Installation Manual

AudioCodes One Voice™ for Microsoft Skype for Business

CloudBond™ 365

Standard/Standard+ Box Edition

Pro Box Edition

Enterprise Box Edition

Virtualized Edition

User Management Pack 365

Version 7.4.5

AudioCodes

CLOUDBOND 365

Tomorrow's UC Today

Table of Contents

This page is intentionally left blank.

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 and other documents as well as software files can be downloaded by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: May-14-2017

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 www.audiocodes.com/support.

Abbreviations and Terminology

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

Related Documentation

Document Name
CloudBond 365 Administration and Maintenance Manual

Document Revision Record

LTRT	Description
26596	Initial document release.
26597	Updates for User Management Pack 365 installation.
26598	Update for indicating that a Windows Server should be configured with a static IPv4 address and not using a DHCP server.

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 http://www.audiocodes.com/downloads.

Part I

Introduction

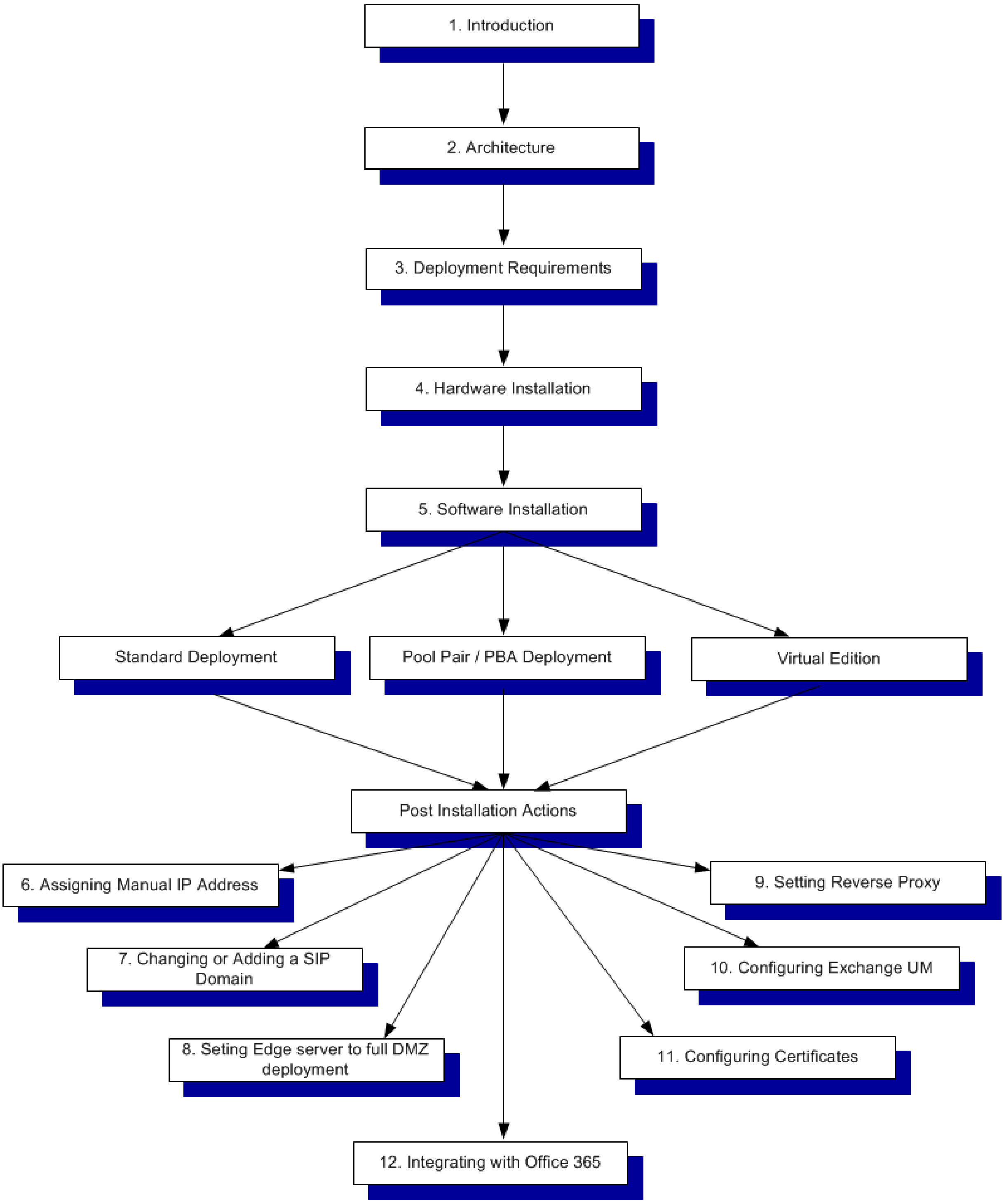
1 Introduction

This document describes AudioCodes' CloudBond 365.

In the document you will find:

- A general description of the AudioCodes CloudBond 365 feature set.
- Hardware/software requirements for installing and using AudioCodes CloudBond 365.

Figure 1-1: Installation Flow


1. Introduction
2. Architecture
3. Deployment Requirements
4. Hardware Installation
5. Software Installation
Standard Deployment
Pool Pair / PBA Deployment
Virtual Edition
Post Installation Actions
6. Assigning Manual IP Address
9. Setting Reverse Proxy
7. Changing or Adding a SIP Domain
10. Configuring Exchange UM
8. Seting Edge server to full DMZ deployment
11. Configuring Certificates
12. Integrating with Office 365

The following describes the steps shown in Figure 6-1 with the corresponding references to each section in the document.

1. Introduction- this Section
2. Architecture- see Chapter 2
3. Deployment Requirements- see Chapter 6
4. Hardware Installation- see Chapter 10
5. Software Installation- see Chapter 11
6. Assigning Manual IP Address- see Chapter 12
7. Changing or Adding a SIP Domain- see Chapter 13
8. Setting Edge Server to Full DMZ deployment- see Chapter 14
9. Settings Reverse Proxy - see Chapter 16
10. Configuring Exchange UM- see Chapter 18
11. Configuring Certificates- see Chapter 17
12. Integrating with Office 365- see Chapter 15

Note: Throughout this document *Skype for Business Server* and *Lync Server 2013* are used interchangeably.

2 Architecture

AudioCodes' CloudBond 365 is built on top of a single server using Microsoft's advanced Virtualization and Security techniques. Due to its single-server design, the CloudBond appliance is limited by the underlying hardware in the number of simultaneous client connections it can support.

- CloudBond 365 Standard Box Edition - 200 clients
- CloudBond 365 Standard+ Box Edition - 200 clients
- CloudBond 365 Pro Box Edition - 500 clients
- CloudBond 365 Enterprise Box Edition - 5000 clients

CloudBond 365 runs in its own Active Directory resource forest and offers an easy Web based management console for administering the CloudBond environment.

With the CloudBond 365 Active Directory connector, enterprise Active Directory users can be added to the appliance without needing to extend the enterprise Active Directory Schema.

Note that the Active Directory connector requires a bidirectional forest trust with one or more enterprise Active Directory environments. Microsoft Windows Small Business Server (SBS) edition does not support forest trusts so importing users is not possible in those environments. CloudBond Appliance's advantage is that Skype for Business can be used with SBS but requires dual user maintenance.

2.1 Microsoft Skype for Business Product Description

In response to today's changing work styles and the need for real-time collaboration, organizations are looking for integrated productivity tools that enable users to communicate from anywhere in a cost-effective and secure manner.

Microsoft Skype for Business Server delivers a fresh, intuitive user experience that brings together the different ways people communicate in a single interface. This unified experience facilitates rapid user adoption, while the ability to support a full range of Communications from a single platform reduces both capital and operational costs.

2.2 New Connected Experience

- Find and communicate with the right person, naturally.

  With native Active Directory integration, Skype for Business Server helps users find the right person to connect with, view their presence, and then communicate with them in the most effective way - via communications, video, or sharing an application or PowerPoint. If required, users can initiate these connections directly from the new Contact Card. With Skill Search powered by SharePoint, users are also able to search for others based on skills, expertise, and group information.

- Stay connected from virtually anywhere, with just a standard internet connection.

  Microsoft Skype for Business offers the same rich functionality and security features outside the firewall without requiring a Virtual Private Network (VPN) connection, and enables mobile and Web access across leading browsers and platforms.

- Build social connections and stay up to date on colleagues' activities.

  Skype for Business encourages closer social connections with a new Activity Feed that shows updates from contacts when they change status note, picture, title, or office location.

2.3 Integration with Microsoft Office

- Communicate with context from Microsoft Office applications.

  Skype for Business Server works with Microsoft Exchange Server, Microsoft SharePoint Server, and Microsoft Office applications for a richer collaborative experience with consistent presence, click-to-call options, and a new Contact Card.

- Office Backstage integration.

  The new Office Backstage view integrates various communication options so users can share documents and presentations via instant messaging (IM), share the application itself, or click to call directly from the application.

2.4 Converged Communications

- Enhanced virtual meetings for improved productivity.

  Users can schedule a meeting from Microsoft Outlook and join through Skype for Business via the PC, phone, or Web interface. Skype for Business Server provides a meeting user interface with integrated audio and video that enables participants to share presentations, annotate slides, superimpose text, and use visual pointers for more effective discussions. Additionally, users have the option to create ad hoc meetings, moving from an IM conversation, for example, to a Live Meeting, directly from the Skype for Business interface.

- Complete set of enterprise-grade Communications features.

  Skype for Business Server delivers a standalone Communications offering to enhance or replace traditional PBX systems, and extends these capabilities outside the office via Internet access without requiring a VPN connection. This includes common calling features such as answer, forward, transfer, hold, divert, release, and park, and support for legacy devices and a broader range of IP and USB user devices from partners. The solution is designed to support high availability through Call Admission Control, and extended options for data resiliency.

2.5 Interoperable and Extensible

- Connect across networks.

  Skype for Business Server supports federation with public IM networks such as Windows Live, AOL, Yahoo!, and, through the XMPP Gateway, Google Talk, allowing workers to use their corporate identities to connect to customers and partners. Skype for Business Server supports audio and video calls with users on Windows Live Messenger.

- Utilize existing A/V infrastructure.

  Conferencing interoperability enables organizations to use existing infrastructure including room systems and high-end conferencing solutions.

- Integrate with existing PBX systems.

  Skype for Business Server works with almost any PBX system either through Session Initiation Protocol (SIP) or qualified gateways, and integrates with qualified third-party SIP Trunking Service Providers.

- Embed communications in business processes.

  New and improved client-side APIs allow developers to embed Skype for Business functionality into Microsoft Windows and Microsoft Silverlight-based applications with supported, ready- to-use code snippets. Enhanced server-side APIs make it easy to instantiate and deliver alerts via IM or phone, find experts, enable Web chat, and provide automated self-service using query-response bots and IVR.

2.6 Simpler Deployment

- Easily deploy systems of any scale, and manage with ease.

  Skype for Business Server can provide presence, IM, and conferencing for organizations of literally any size, with up to 10,000 users per server, 100,000 users per pool, and an unlimited number of pools. Automated tools not only simplify capacity planning and topology design, but also automatically push configuration information and changes to all servers in the network, thus eliminating manual work and the associated chance for errors. The new Skype for Business Server Control Panel consolidates scenario-driven tasks in a single interface, while PowerShell support allows administrators to automate repetitive tasks using a familiar tool. Skype for Business Server relies on Active Directory, eliminating the need for separate user and policy databases, and uses Role Based Access Control (RBAC) to allow the assignment of appropriate management roles and scopes to different administrators.

- Support for on-premises and hosted environments.

  Skype for Business Server can be deployed on-premises or in a service-based (hosted) or hybrid environment. It offers full and seamless integration with Exchange Online and SharePoint Online, allowing customers to choose how to best deliver enterprise messaging and collaboration capabilities to end users.

This page is intentionally left blank.

3 CloudBond 365 Appliances

This chapter describes the available CloudBond 365 Appliances platform.

3.1 CloudBond 365 Standard / Standard+ Box Edition

CloudBond 365 is a complete hardware and software solution.

CloudBond 365 Standard / Standard+ Box Edition is delivered pre-installed on an AudioCodes Mediant 800 device.

CloudBond 365 Standard /Standard+ Box Edition includes both CloudBond 365 software for full Skype for Business capabilities, as well as full AudioCodes Mediant 800 gateway hardware for external Skype for Business Enterprise Voice connectivity.

CloudBond 365 is limited to 200 users.

3.2 CloudBond 365 Pro and Enterprise Editions

CloudBond 365 Pro and Enterprise Editions are delivered with various HP Server device configurations pre-installed.

The HP Server devices include redundant power supplies and raid HDD storage, and can support up to 5000 users on the Enterprise edition.

The Pro and Enterprise Editions can optionally include a Software SBC for PSTN access via external SIP Trunk support. They can also include a Reverse Proxy server if required.

This page is intentionally left blank.

4 Licensing

This chapter describes the CloudBond 365 licensing.

4.1 CloudBond

CloudBond - Skype for Business product is built on top of Microsoft Sever 2012 R2 Standard Edition and Microsoft Skype for Business Server Standard edition and requires the appropriate Microsoft server and CAL licenses in addition to the CloudBond license itself, as described in the sections below.

The CloudBond 365 Sysadmin is licensed by system ID.

To activate your CloudBond 365 system you will need both a “Product Key” and a “System ID” (Fingerprint). Once you have both keys you can activate your product through AudioCodes License Activation tool at http://www.audiocodes.com/swactivation.

An e-mail will subsequently be sent to you with your Product License.

4.2 Windows Server 2012 Licensing Overview

Microsoft offers flexible, cost-effective options for licensing the Windows Server 2012 family of products. Prior to running an instance of Windows Server software (loading it into memory and executing one or more of its instructions), customers must assign a Windows Server license to a physical server. Assignment/reassignment rules for original equipment manufacturer (OEM) licenses are different from Volume Licensing and retail license rights. With a license purchased with a server from an OEM, the Windows Server license is already assigned to that specific server, and lives and dies with that server. The OEM end customer is not allowed to reassign that OEM license to another server.

4.3 Client Access Licensing

Windows Server is licensed using the Server + CAL model. The CAL that accesses the instance of Windows Server must be equivalent or higher in version than the server being accessed. An exception to this rule was introduced with Windows Server 2008 and continued with Windows Server 2008 R2. Under that exception, customers must still license the appropriate CAL version to access the version of the server software running in each virtual operating system environment, but they are not required to upgrade their CALs based on the version of Windows Server that is running in the physical operating system environment. In this scenario, the Hyper-V server role must be the only role running in the physical operating system environment.

A Windows Server 2012 R2 Client Access License (CAL) must be purchased for every user or device that accesses or uses the Windows Server 2012 R2 server software, except under the following circumstances:

- If the instances of the server software are accessed only through the Internet, without access being authenticated or otherwise individually identified by the server software or through any other means
- If external users are accessing the instances of the server software and a Windows Server 2012r2 External Connector license for each server being accessed has been acquired
- If up to two devices or users are accessing the instances of the server software for the purpose of administering those instances
- If Windows Server 2012 R2 serves solely as a virtualization host (CALs for the appropriate edition of Windows Server running in the virtual machine(s) are still required)

4.3.1 Device-based or User-based Windows Client Access Licenses

There are two types of Windows Client Access Licenses from which to choose: device-based or user based, also known as Windows Device CALs or Windows User CALs. This means you can choose to acquire a Windows CAL for every device (used by any user) accessing your servers, or you can choose to acquire a Windows CAL for every named user accessing your servers (from any device).

The option to choose between the two types of Windows CALs offers you the flexibility to use the licensing that best suits the needs of your organization. For example:

- Windows Device CALs might make most economic and administrative sense for an organization with multiple users for one device, such as shift workers

  whereas

- Windows User CALs might make most sense for an organization with many employees who need access to the corporate network from unknown devices (for example, when traveling) and/or an organization with employees who access the network from multiple devices.

4.3.2 Client Access Licensing Modes

After you have selected a license type - Windows Device CAL or Windows User CAL, you have the option to use the server software in two different modes: Per User/Per Device mode or Per Server mode. Both modes are available for either type of license.

4.3.2.1 Per User or Per Device Mode

Per User/Per Device mode is defined as follows:

- A separate Windows CAL (of either type) is required for each user or device that accesses or uses the server software on any of your servers.
- The number of Windows CALs required equals the number of users or devices accessing the server software.
- If you choose this licensing mode, your choice is permanent. You can, however, reassign a Windows CAL from one device to another device, or from one user to another user, provided the reassignment is made either (a) permanently away from the one device or user or (b) temporarily to accommodate the use of the Windows CAL either by a loaner device, while a permanent device is out of service, or by a temporary worker, while a regular employee is absent.

Per User/Per Device mode tends to be the most economical designation for Windows CALs in distributed computing environments where multiple servers within an organization provide services across most devices or users.

Note: Per User/Per Device mode replaces Per Seat mode, used in previous licensing models.

4.3.2.2 Per Server Mode

Per Server mode is defined as follows:

- A separate Windows CAL (of either type) is required for each user or device that accesses or uses the server software on any of your servers. (This does not change the per server connection allowance of one CAL per one connection.)
- The number of Windows CALs required equals the maximum number of users or devices that may simultaneously access or use the server software running on a particular server. The Windows CALs you acquire are designated for use exclusively with a particular server.
- If you choose this licensing mode, you have a one-time right to switch to the other licensing mode—Per User/Per Device mode. Your Windows CALs (of either type) would then be used in Per User/Per Device mode instead.

Per Server mode tends to be the most economical designation for Windows CALs in computing environments where a small number of servers have limited access requirements.

4.3.3 Virtualization

A customer licensed with Windows Server 2012R2 standard edition may run one instance of the server software in the physical operating system environment (POSE) and up to two instances of the server software in the virtual operating system environment (VOSE). If more VOSE instances are required, then additional Windows 2012R2 standard edition licenses are required. Each additional server license allows two additional VOSE instances to be run.

4.4 Skype for Business

Skype for Business Server follows the Server/Client Access License (CAL) model. Under this model, a Skype for Business Server license is required for each operating system environment running Skype for Business Server Front End role. A CAL is required for each user or device accessing the Skype for Business Server. You can acquire Skype for Business Server client access licenses as standalone server and Client Access licenses (CAL) or you can purchase the CALs as part of the Microsoft Enterprise CAL (ECAL) Suite.

4.4.1 CloudBond 365 - Skype for Business Server Standard Edition

Skype for Business Server Standard Edition requires that primary server components, as well as the database for storing user and conference information, be configured on a single computer. Skype for Business Standard Edition is recommended for organizations that do not require higher availability through load balancing.

4.4.2 Skype for Business Server Client Access Licenses Offerings

A CAL is required for each user or device accessing the Skype for Business Server. There are three CALs offered with Skype for Business Server:

- Skype for Business Server Standard CAL
- Skype for Business Server Enterprise CAL
- Skype for Business Server Plus CAL

The table below illustrates the features contained within the Skype for Business Server CAL offerings:

4.4.2.1 Instant Messaging and Presence (Standard CAL Feature)

Table 4-1: Instant Messaging and Presence

Feature	Standard CAL
PC-to-PC and multi-party IM	✓
PC-to-PC and multi-party File Transfer	✓
PC-to-PC computer audio	✓
PC-to-PC computer video	✓
Rich Presence	✓
Persistent Group Chat	✓
Skill Search	✓
IM/P from Office applications	✓
PC-to-PC IM, audio, and video with users at federated organizations & Public IM Networks	✓
Conference Attendee Experience: Join an ad hoc or scheduled meeting; Send/receive audio/video; View shared application; View/Write whiteboard; all this as *an authenticated user*.	✓
Conference Presenter Experience: Upload and advance PowerPoint slides; Initiate Recording; Share application; Manage Roster; Manage Meeting lobby; Use DTMF controls; all this as *an authenticated user*.	✓
View application sharing session (Attendee experience)	✓

4.4.2.2 Audio, Video, & Web Conf. (Requires: Enterprise and/or Plus CAL)

Table 4-2: Audio, Video, and Web Conference

Feature	Enterprise CAL	Plus CAL
Initiate/Schedule ad-hoc multi-party (3+) audio conference (including dial-out to PSTN and/or PBX user)	✓	✓
Initiate ad-hoc multi-party video conference	✓	
Initiate ad-hoc application Sharing (P2P or multi-party)	✓	
Initiate ad-hoc white boarding (P2P or multi-party)	✓	
Schedule and host conferences on the audio conferencing bridge(CAA)	✓	
Schedule Web conferences	✓	
Automatically join meeting audio from PBX or other phone number	✓	
Dial out to PSTN		✓
Receive calls from PSTN		✓

4.4.2.3 Enterprise Communication Technology (Requires: Enterprise and/or Plus CAL)

Table 4-3: Enterprise Communications Technology

Feature	Enterprise CAL	Plus CAL
Ad-hoc multi-party (3+) audio conference (including dial-out to PSTN and/or PBX user)	✓	✓
UC and PBX Call Control (click to call, answer, hold, resume, transfer, park, and retrieve)		✓
Visual access to Voice mail (requires Exchange UM for Voice mail)		✓
Additional telephony features (call park and receive, report malicious call, inbound private line)		✓
Routing Rules (includes team call, call forward, simul- ring)		✓
E911 capabilities		✓
Delegation		✓
Response Group Agent and Agent Anonymity		✓
Office Communicator - OC Phone Edition based phone devices "better together"		✓
Survivable Branch Appliance		✓

Note: The Skype for Business Server Standard CAL is a prerequisite to both the Skype for Business Server Enterprise CAL and Skype for Business Server Plus CAL. Additionally, both Skype for Business Server Standard and Enterprise CALs are components of the Microsoft Enterprise CAL Suite, and the Plus CAL can only be acquired standalone.

4.4.3 Client Software

Skype for Business is the client software used to interact with the Skype for Business Server.

Skype for Business is available as both a standalone product and is also included in Microsoft Office Professional Plus 2013 and later versions.

4.5 Other Offerings

4.5.1 Office 365 Licensing

When CloudBond 365 is deployed with Microsoft Office 365, customers will have to purchase the Office 365 E4/E5 license per user.

For more Office 365 pricing offerings, see: https://products.office.com/en/business/compare-more-office-365-for-business-plans

4.6 Additional Microsoft Skype for Business Server Software Components

The following additional software components are associated with the Skype for Business Server license:

- Archiving and Monitoring Server Role
- Audio/Video Conferencing Server Role
- Central Management Server Role
- Skype for Business Web Application Server Role
- Director Role
- Edge Server Role
- Group Chat Server Role
- Mediation Server Role
- Reach Application Sharing Server Role
- Survivable Branch Appliance Role
- Unified Communications Application Server Role
- Web Conferencing Server Role
- Microsoft Skype for Business Server Control Panel
- Microsoft Skype for Business Server Web App Plug-In
- Microsoft Skype for Business Server Group Chat Administration Tool
- Microsoft Skype for Business in UI Suppression Mode
- Topology Builder
- Administrative Tools
- Microsoft PowerShell Snap-In

Part II

Deployment Requirements

5 Introduction

This part describes the deployment of AudioCodes' CloudBond 365 within an existing corporate domain network.

The guide provides information to technicians on how to perform on-site installation of CloudBond 365. The guide provides:

- Guidelines for preparing the customer enterprise network
- CloudBond 365 application installation procedure
- Basic system and site configuration information
- Concepts and procedures for Microsoft Exchange UM Integration
- Maintenance procedures for the server and the client applications

This page is intentionally left blank.

6 Deployment Requirements

This chapter describes the CloudBond 365 deployment requirements.

6.1 Before Deploying CloudBond 365

Before deploying CloudBond 365 make sure:

- You possess all deployment-related information
- Enterprise customer staff can be available if necessary to perform specific tasks within the existing corporate enterprise network
- You 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 information about the Domain Controller, DHCP and DNS, Microsoft Exchange, etc.

6.2 Public Key Infrastructure

Microsoft Skype for Business uses a Public Key Infrastructure (certificates) to enable secure MTLS and TLS communication between servers and clients.

For further information about CloudBond 365, Skype for Business and Certificates, see the *AudioCodes CloudBond 365 Certificates Configuration Note.*

The Note includes instructions for various Certification deployment options.

All CloudBond 365 Editions contain only private certificates issued by the CloudBond 365 controller. You will need to generate new certificates to access CloudBond 365 internally from a corporate network.

To access CloudBond 365 externally, you will need to deploy public certificates.

6.3 IP Addresses

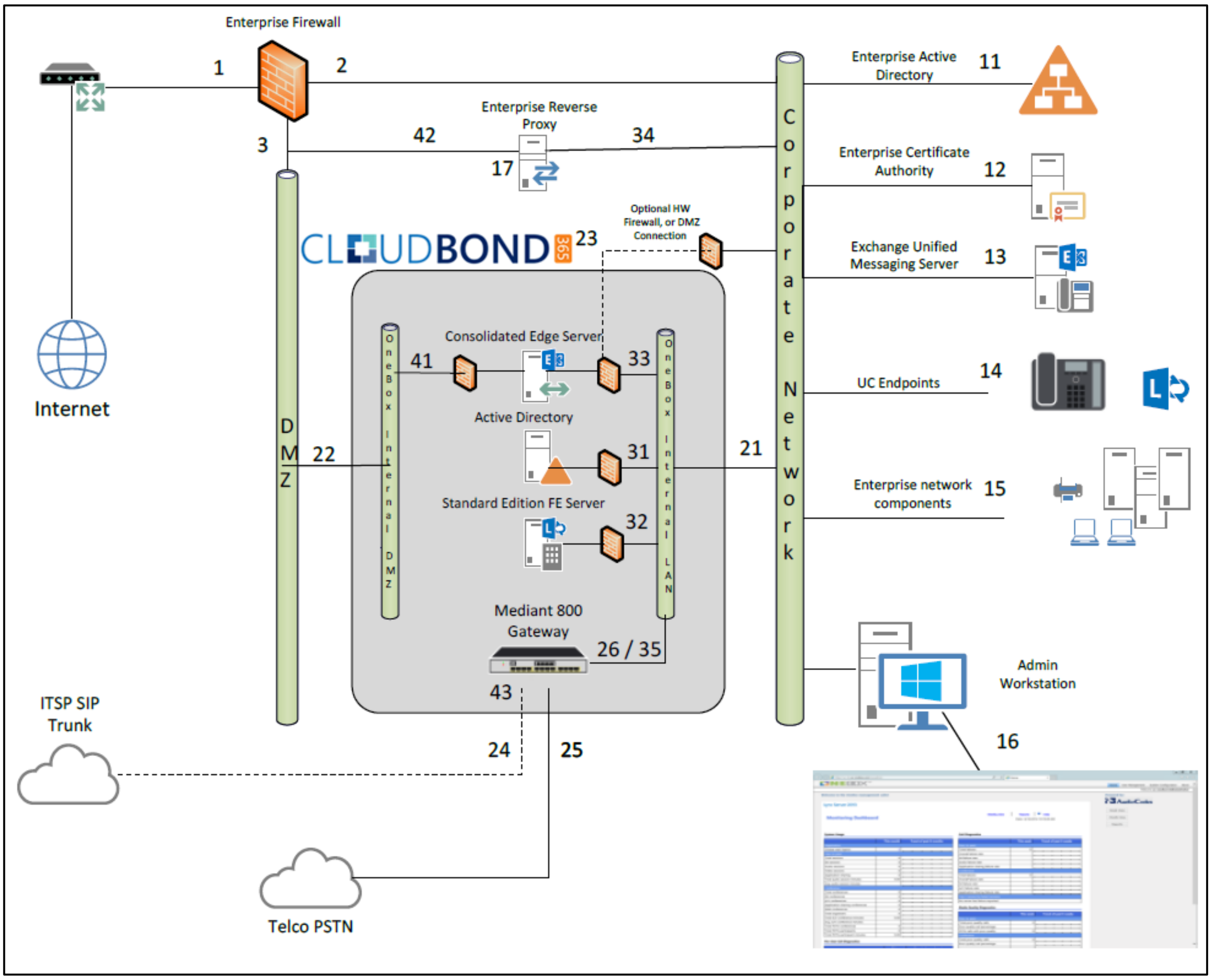
CloudBond 365 is connected to the enterprise network using at least three internal IP addresses. More IP addresses are needed for optional components such as the AudioCodes Mediant 800 gateway, AudioCodes SBC, Office Web Apps Server, Reverse Proxy server, etc.

On the Internet side, one (optionally NAT-ed) public IP Address is required. Some optional components such as Reverse Proxy server, AudioCodes SBC, etc., may require additional IP Addresses.

Figure 6-1 shows the location of CloudBond 365 in the network. For more information on the required ports and firewall configuration, see Chapter 9 on page 67

Note: To provide external access to web meetings and the corporate address book, a Reverse Proxy, demanding its own internal and external IP addresses, is required. Alternatively, a corporate firewall can be used to forward HTTPS traffic from port 443 external to 4443 internal.

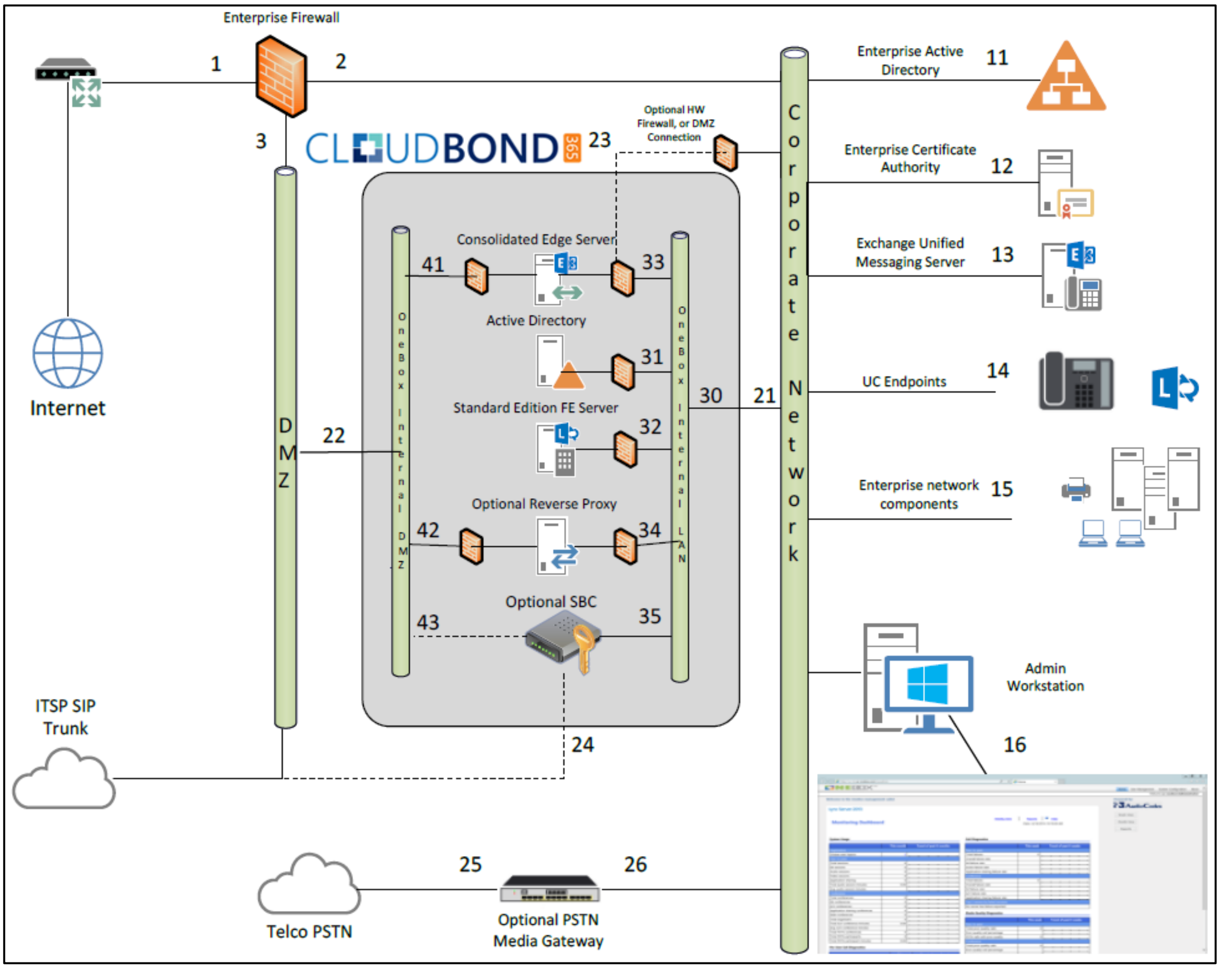
Figure 6-1: CloudBond 365 Standard Edition Located in the Network



All IP addresses will be set to default on a new CloudBond 365 Standard Edition system. You may need to use the CloudBond 365 SysAdmin utility to change IP addresses if the defaults are unsuitable.

The corporate Domain Controller should be able to ping all three CloudBond 365 servers (Controller, Front End, Edge) by IP address. This is a reasonable test to perform for correct network connectivity.

Figure 6-2: CloudBond 365 Pro / Enterprise Edition Located in the Network



All IP addresses will be set to default on a new CloudBond 365 Pro and Enterprise Editions system.

The corporate Domain Controller should be able to ping all three CloudBond 365 servers (Controller, Front End, Edge) by IP address. This is a reasonable test to perform for correct network connectivity. If deploying optional components such as AudioCodes SBC, Reverse Proxy, or Office Web Apps Server, these should also be checked.

6.4 DNS

DNS records play a very important part in the correct functioning of Microsoft Skype for Business and the CloudBond 365.

DNS Records are required:

- To establish a two way trust between the enterprise domain and the CloudBond 365 resource forest
- To allow Skype for Business clients to locate Skype for Business services and to automatically log on
- To allow Skype for Business services to be access externally, such as external users, conferencing, and federation.

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, depending on the CloudBond 365 features required.

Typically, the following will be 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 enterprise DNS server, a primary zone matching the FQDN of the default SIP domain specified for the CloudBond 365 topology. If any additional SIP domains are supported, they may need additional DNS zones. These DNS zones contain the internal DNS records which permit automatic logon of Skype for Business clients to the Skype for Business Front End server.
- 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 or Reverse Proxy servers.

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 those permissions in the enterprise environment, a customer enterprise administrator should be available to assist.

Chapter 8 contains the details of required 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. See also Chapter 13.

6.5 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 provides the steps needed and some background information on how to get to 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 will assume 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.

This page is intentionally left blank.

7 Integrating CloudBond 365

This chapter describes the integration of CloudBond 365 in the Enterprise.

7.1 Connecting CloudBond 365 to the Enterprise Domain

To allow CloudBond 365 to integrate with the enterprise's Active Directory:

1. Verify the time and time zone settings for each CloudBond 365 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
9. Add DHCP entries for Skype for Business Phone edition devices

The following sections cover these steps.

7.2 Verify the Time and Time Zone Settings for CloudBond 365 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 365 servers and hardware components are set to the same time zone, and same time.

CloudBond 365 will typically default to **GMT +1:00 hour**. All servers (CloudBond 365 Controller, Front End, Edge, and Mediant 800 will need to be synchronized accordingly.

7.3 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 presents no problems, it's a known issue when establishing Forest Trusts and some other DNS-based Active Directory activities.

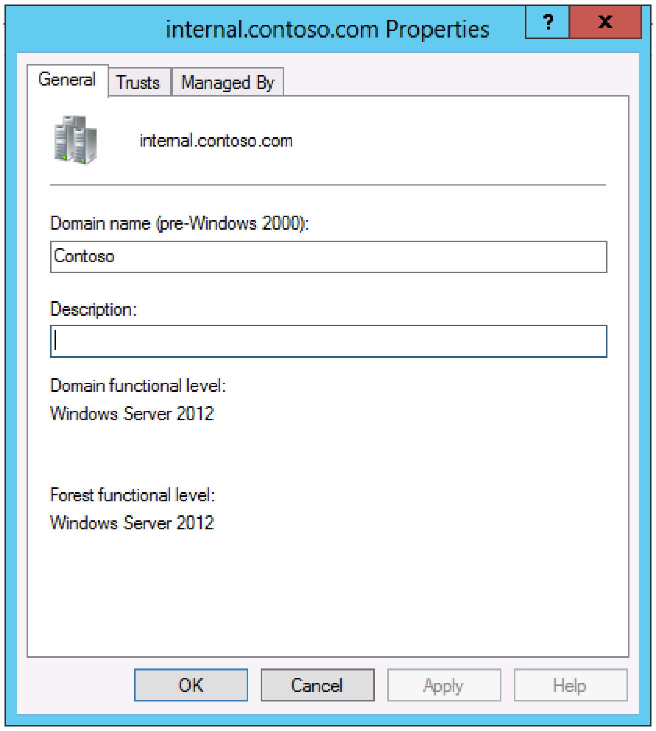
To avoid any issues, make sure the Primary DNS setting on NICs on both the Corporate Domain Controller and CloudBond 365 Controller are set to the IP address of the box rather than to 127.0.0.1. Failure to change these DNS entries will result in a Forest Trust that appears to be configured correctly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

7.4 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.

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 will be displayed.
3. Make sure both domain and forest functional levels are **2003** or higher.

Figure 7-1: Verifying Forest and Domain Functional Levels



internal.contoso.com

Domain name (pre-Windows 2000):
Contoso

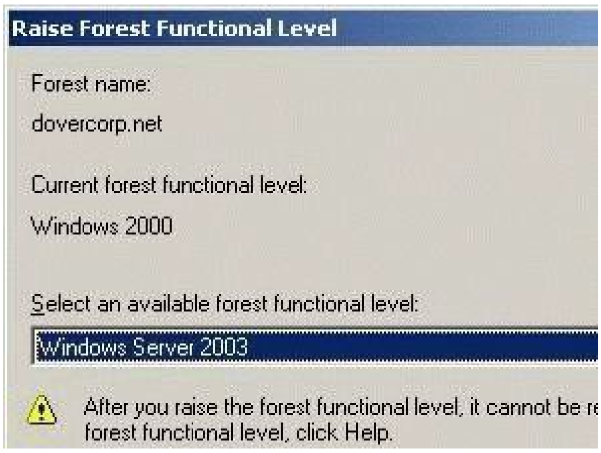
Description:

Domain functional level:
Windows Server 2012

Forest functional level:
Windows Server 2012

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

Figure 7-2: Raising Forest Functional Level



Forest name:
dovercorp.net

Current forest functional level:
Windows 2000

Select an available forest functional level:
Windows Server 2003

After you raise the forest functional level, it cannot be re
forest functional level, click Help.

➢ To raise the domain functional level for a domain:

1. Open the Active Directory Domains And Trusts console
2. Right-click the domain whose functional level you want 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:

5. Open the Active Directory Domains and Trusts console.
6. 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.
7. Click **Raise** and then click **OK**.

7.5 Setting up Cross Forest DNS Stub Zones

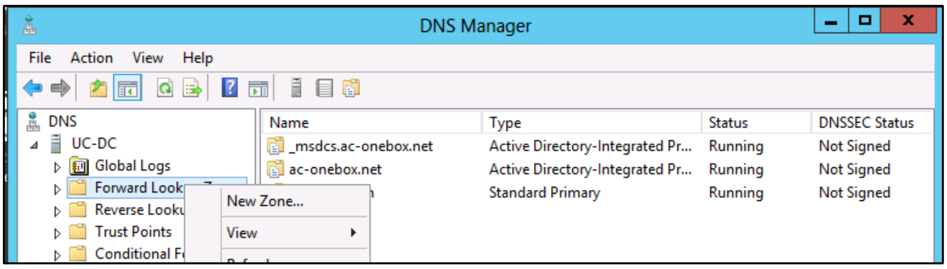
The CloudBond 365 Active Directory connector relies on a bidirectional forest trust between CloudBond 365's Active Directory and enterprise Active Directory.

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.

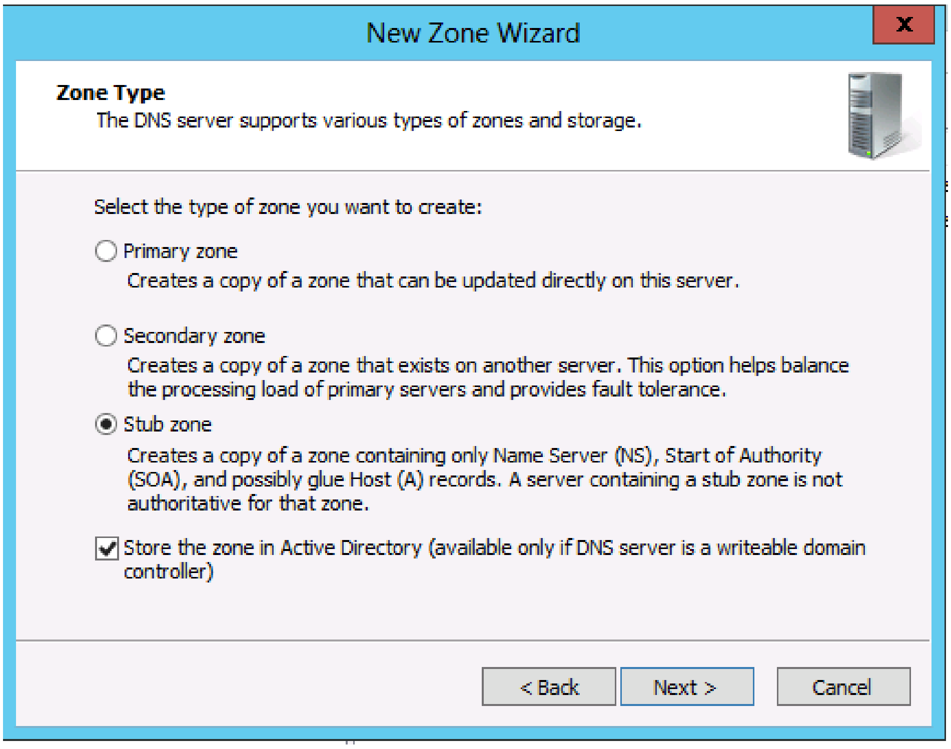
Figure 7-3: Creating DNS Stub Zone



Name	Type	Status	DNSSEC Status
_msdcs.ac-onebox.net	Active Directory-Integrated Pr...	Running	Not Signed
ac-onebox.net	Active Directory-Integrated Pr...	Running	Not Signed
h	Standard Primary	Running	Not Signed

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

Figure 7-4: Creating DNS Stub Zone



New Zone Wizard

Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

○ Primary zone
Creates a copy of a zone that can be updated directly on this server.

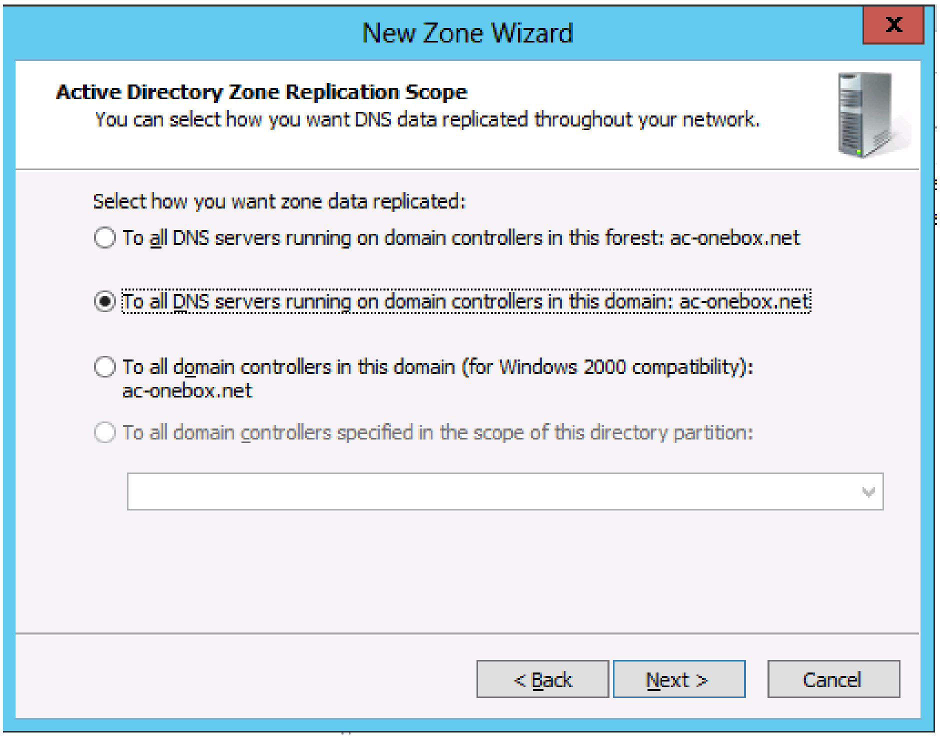
○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

● 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.

☑ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

3. Set replication to all servers within the domain.

Figure 7-5: DNS New Zone Wizard – Replication



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:

○ To all DNS servers running on domain controllers in this forest: ac-onebox.net

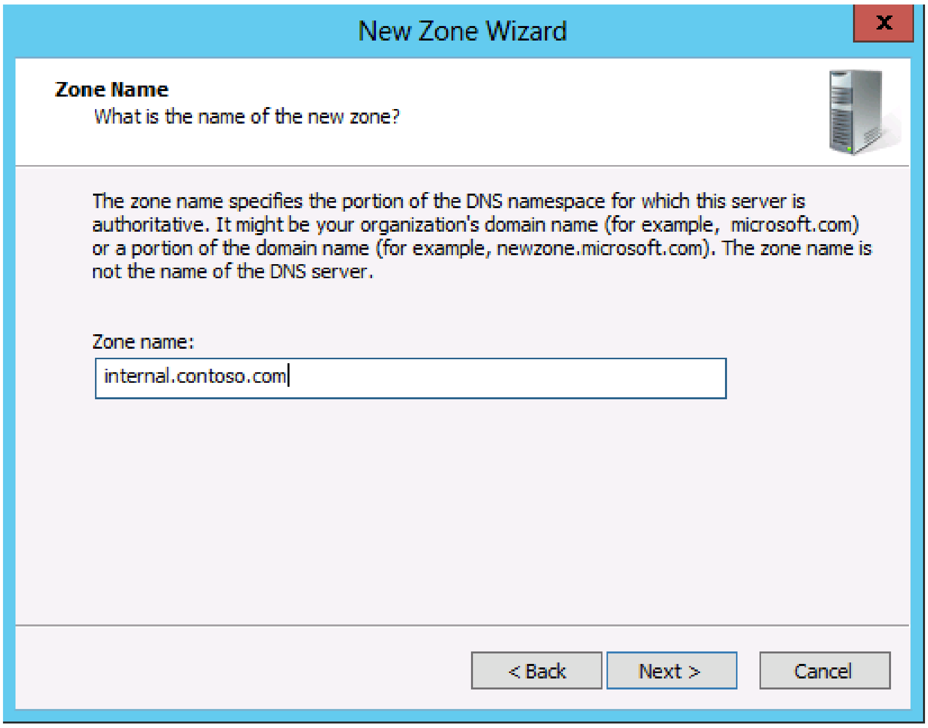
● To all DNS servers running on domain controllers in this domain: ac-onebox.net

○ To all domain controllers in this domain (for Windows 2000 compatibility): ac-onebox.net

○ To all domain controllers specified in the scope of this directory partition:

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

Figure 7-6: DNS Stub Zone – FQDN



New Zone Wizard

Zone Name

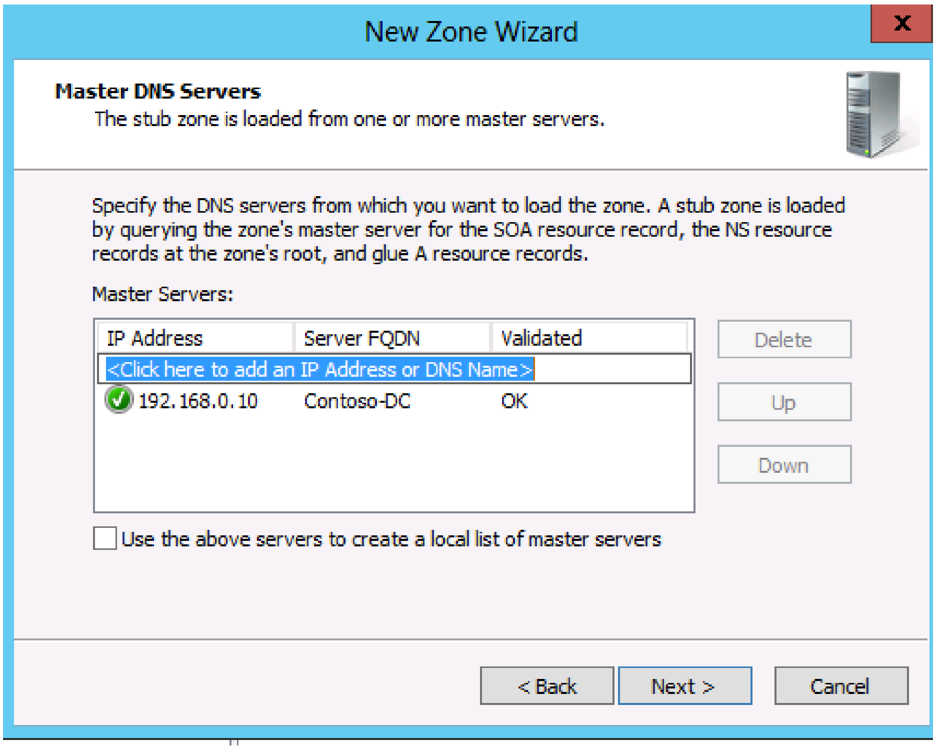
What is the name of the new zone?

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

Zone name: internal.contoso.com

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

Figure 7-7: DNS Stub Zone - Master DNS Server



New Zone 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.

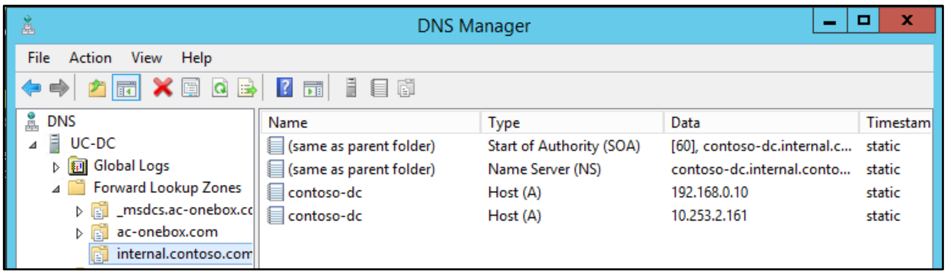
Master Servers:

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

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

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 7-8: Results of Creating DNS Stub Zone



DNS Manager

File Action View Help

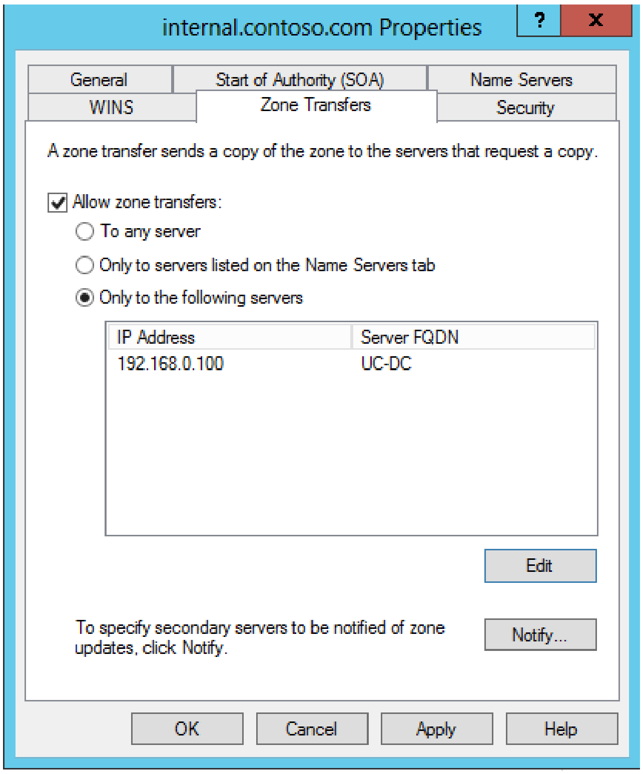
- DNS
  - UC-DC
    - Global Logs
    - Forward Lookup Zones
      - _msdcs.ac-onebox.cc
      - ac-onebox.com
      - internal.contoso.com

Name	Type	Data	Timestam
(same as parent folder)	Start of Authority (SOA)	[60], contoso-dc.internal.c...	static
(same as parent folder)	Name Server (NS)	contoso-dc.internal.conto...	static
contoso-dc	Host (A)	192.168.0.10	static
contoso-dc	Host (A)	10.253.2.161	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 7-9: DNS Stub Zone - Restricting Zone Transfers



internal.contoso.com Properties

Tabs: General | Start of Authority (SOA) | Name Servers | WINS | Zone Transfers | Security

A zone transfer sends a copy of the zone to the servers that request a copy.

☑ Allow zone transfers:

○ To any server

○ Only to servers listed on the Name Servers tab

● Only to the following servers

IP Address	Server FQDN
192.168.0.100	UC-DC

Edit

To specify secondary servers to be notified of zone updates, click Notify.

Notify...

OK Cancel Apply Help

9. Perform the same steps on a DNS server in the enterprise forest, where the forward lookup stub zone should point to the CloudBond 365 FQDN instead (cloudbond365.local).

10. If the enterprise environment has multiple DNS servers that are not Active Directory integrated, there will be no default replication between them. Make sure all enterprise DNS servers are aware of the new Stub zone just created.

11. Repeat steps 1-10 for all other (child-) domains that require a trust with the CloudBond 365 domain.

7.6 Setting up a Forest Trust

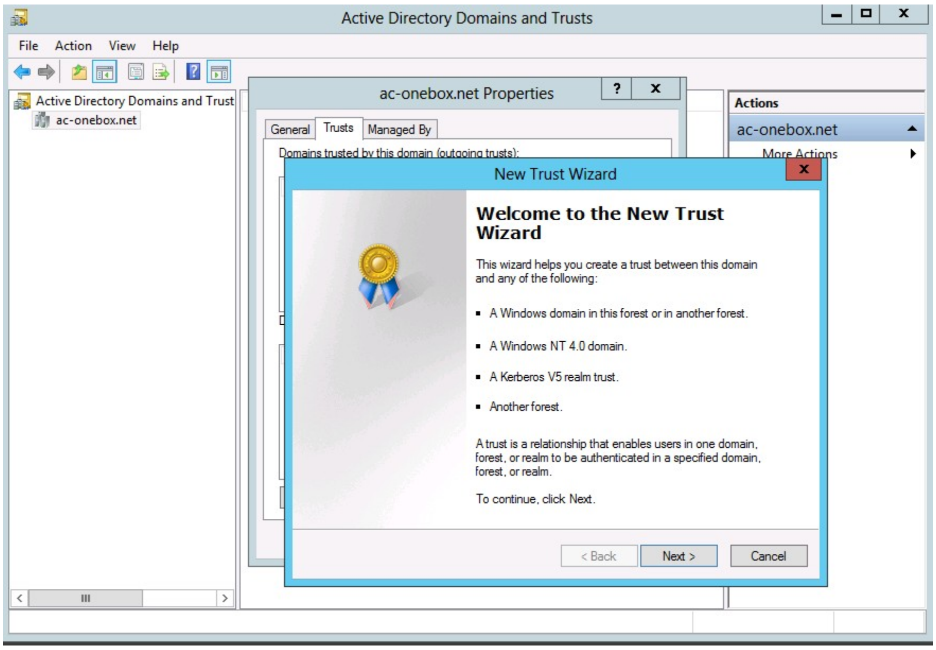
Note: Make sure 127.0.0.1 is not in use as the Primary DNS entry on the NIC of both CloudBond 365 controller and corporate Domain Controller. If you don't, the result may be a forest Trust which appears correct but fails to work.

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

➢ **To set up a Forest Trust:**

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

Figure 7-10: Creating a Trust



Welcome to the New Trust Wizard

This wizard helps you create a trust between this domain and any of the following:

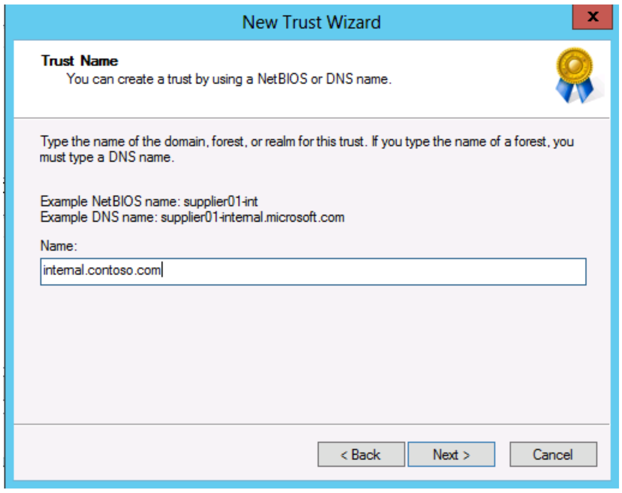
- A Windows domain in this forest or in another forest.
- A Windows NT 4.0 domain.
- A Kerberos V5 realm trust.
- Another forest.

A trust is a relationship that enables users in one domain, forest, or realm to be authenticated in a specified domain, forest, or realm.

To continue, click Next.

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

Figure 7-11: Creating a Trust - Specify the Domain



New Trust Wizard

Trust Name
You can create a trust by using a NetBIOS or DNS name.

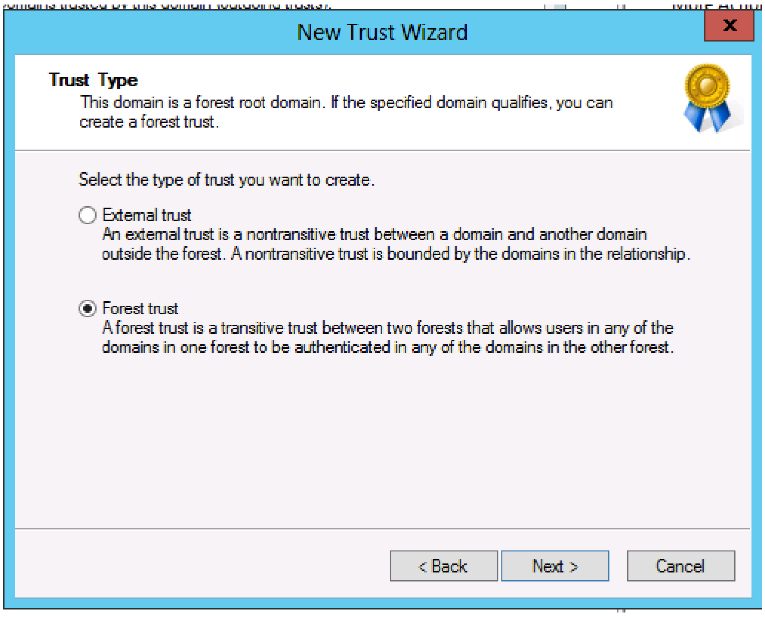
Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.

Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com

Name: internal.contoso.com

4. Select **Forest trust**.

Figure 7-12: 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.

Select the type of trust you want to create.

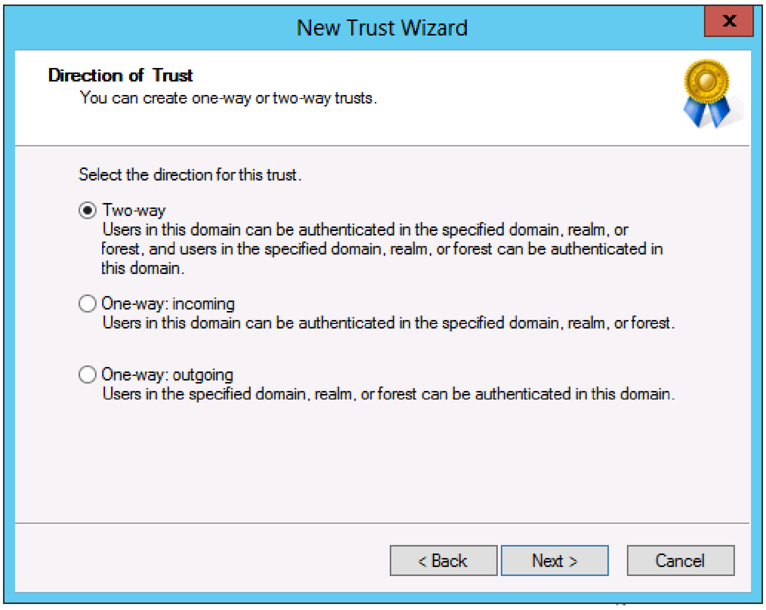
○ External trust
An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.

● 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.

5. Specify an account with sufficient rights in the enterprise forest.

6. Select **Two-way**.

Figure 7-13: Creating a Trust - Two Way Trust



Direction of Trust
You can create one-way or two-way trusts.

Select the direction for this trust.

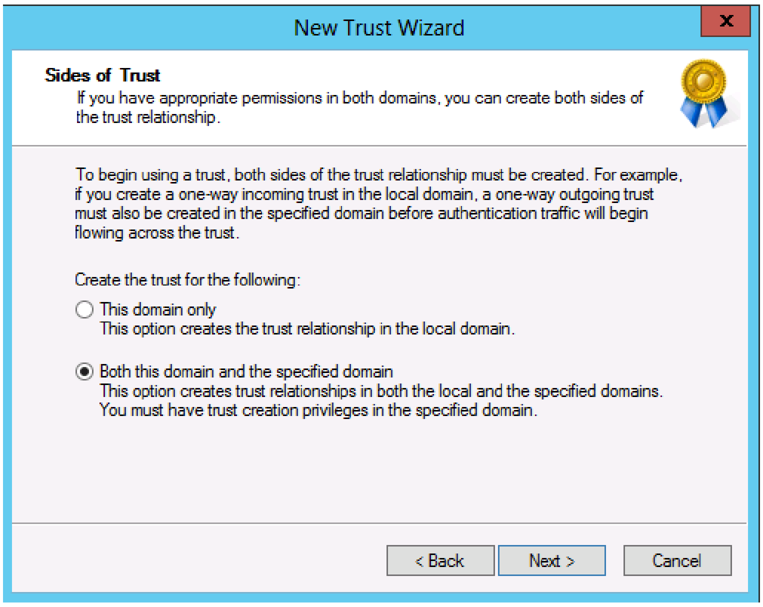
● Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.

○ One-way: incoming
Users in this domain can be authenticated in the specified domain, realm, or forest.

○ One-way: outgoing
Users in the specified domain, realm, or forest can be authenticated in this domain.

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

Figure 7-14: Creating a Trust - Create Both Sides of the Trust



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 example, 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.

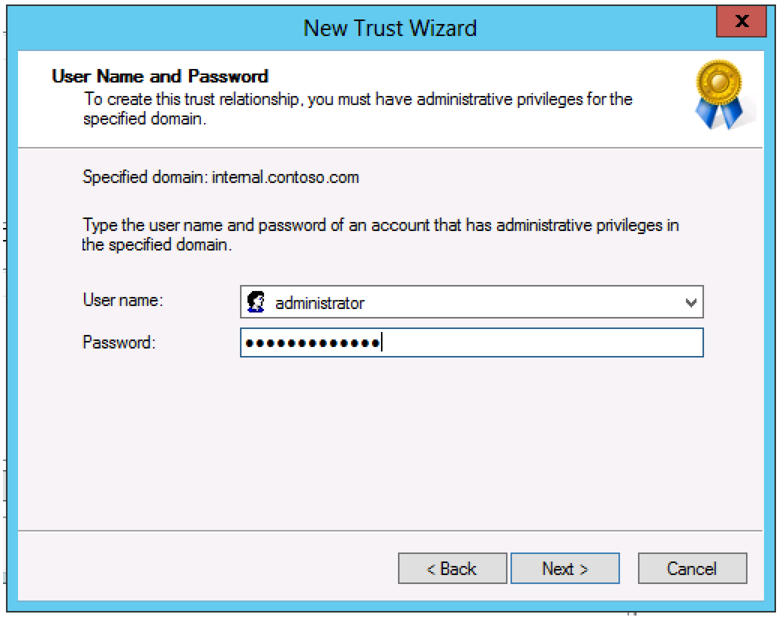
Create the trust for the following:

○ This domain only
This option creates the trust relationship in the local domain.

● 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.

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

Figure 7-15: Creating a Trust - Enter Credentials for the Other Side



New Trust Wizard

User Name and Password

To create this trust relationship, you must have administrative privileges for the specified domain.

Specified domain: internal.contoso.com

Type the user name and password of an account that has administrative privileges in the specified domain.

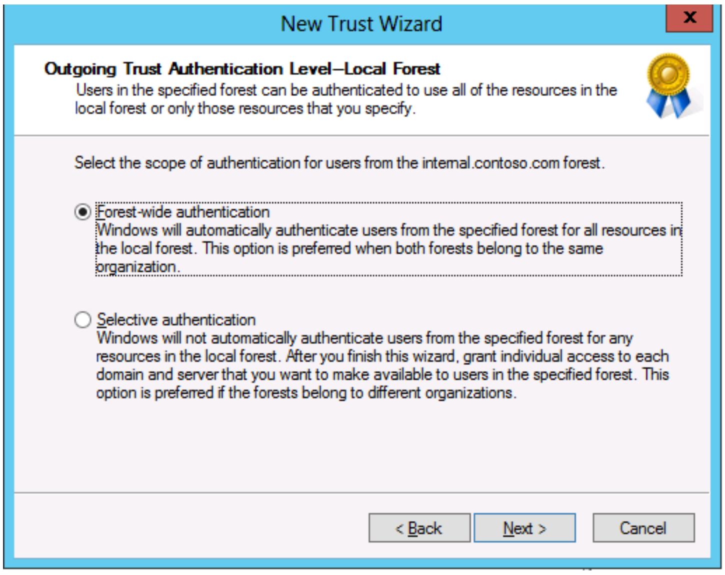
User name: administrator

Password: •••••••••••••

9. Select Forest-wide authentication for both:

- Outgoing Trust Authentication Level – Local Forest
- Outgoing Trust Authentication Level – Specified Forest

Figure 7-16: Creating a Trust - Forest Wide



New Trust Wizard

Outgoing Trust Authentication Level--Local Forest

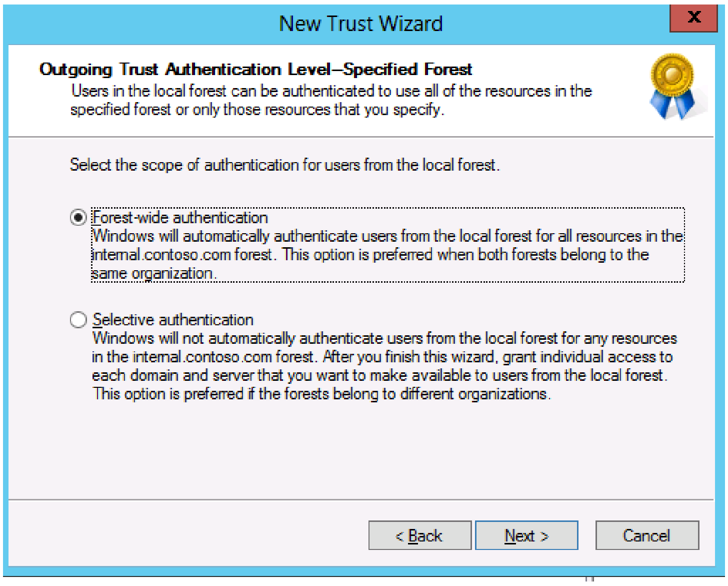
Users in the specified forest can be authenticated to use all of the resources in the local forest or only those resources that you specify.

Select the scope of authentication for users from the internal.contoso.com forest.

● Forest-wide authentication
Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.

○ 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 each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.

Figure 7-17: Creating a Trust - Forest Wide



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.

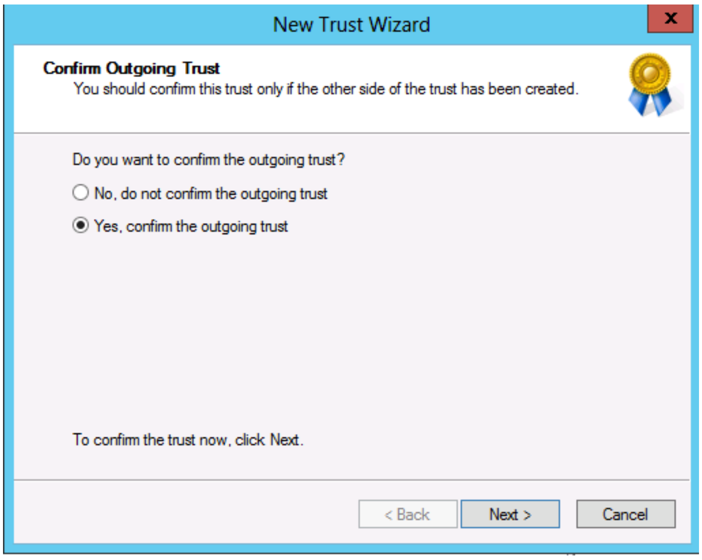
Select the scope of authentication for users from the local forest.

● 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.

○ 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.

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 7-18: Confirming the Trust



Confirm Outgoing Trust
You should confirm this trust only if the other side of the trust has been created.

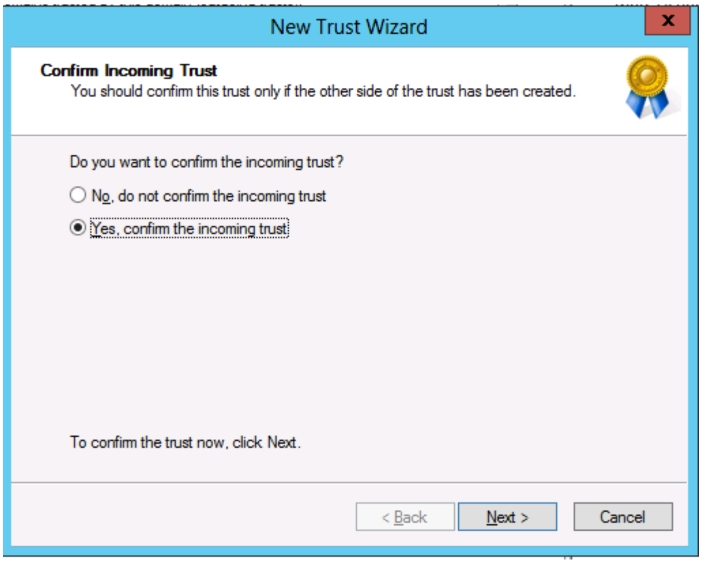
Do you want to confirm the outgoing trust?

○ No, do not confirm the outgoing trust

● Yes, confirm the outgoing trust

To confirm the trust now, click Next.

Figure 7-19: Confirming the Trust



New Trust Wizard

Confirm Incoming Trust
You should confirm this trust only if the other side of the trust has been created.

Do you want to confirm the incoming trust?

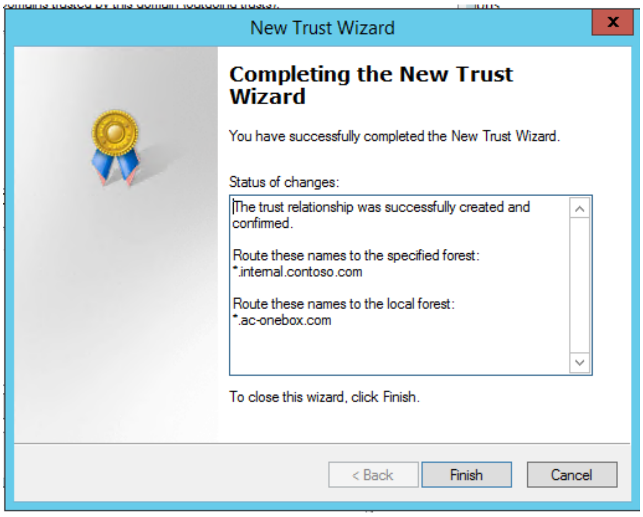
○ No, do not confirm the incoming trust

● Yes, confirm the incoming trust

To confirm the trust now, click Next.

12. A successful Trust Creation page should appear.

Figure 7-20: Completing the New Trust Wizard



New Trust Wizard

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.

7.7 Active Directory Synchronization

For complete integration of CloudBond 365 Skype for Business with Microsoft Exchange and SharePoint, 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

For more information, see Chapter 15.

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.

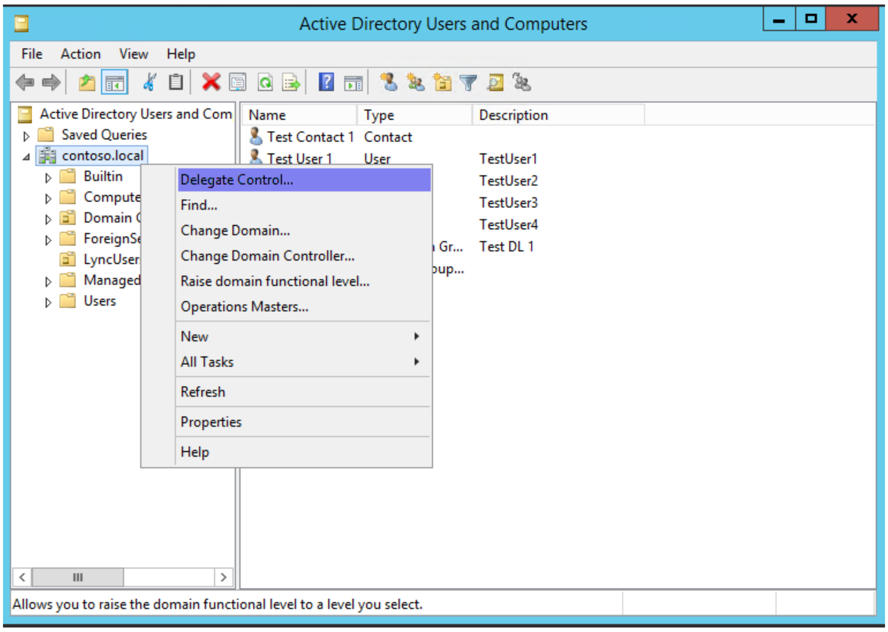
7.8 Delegate Control

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 7-21: Delegate Control

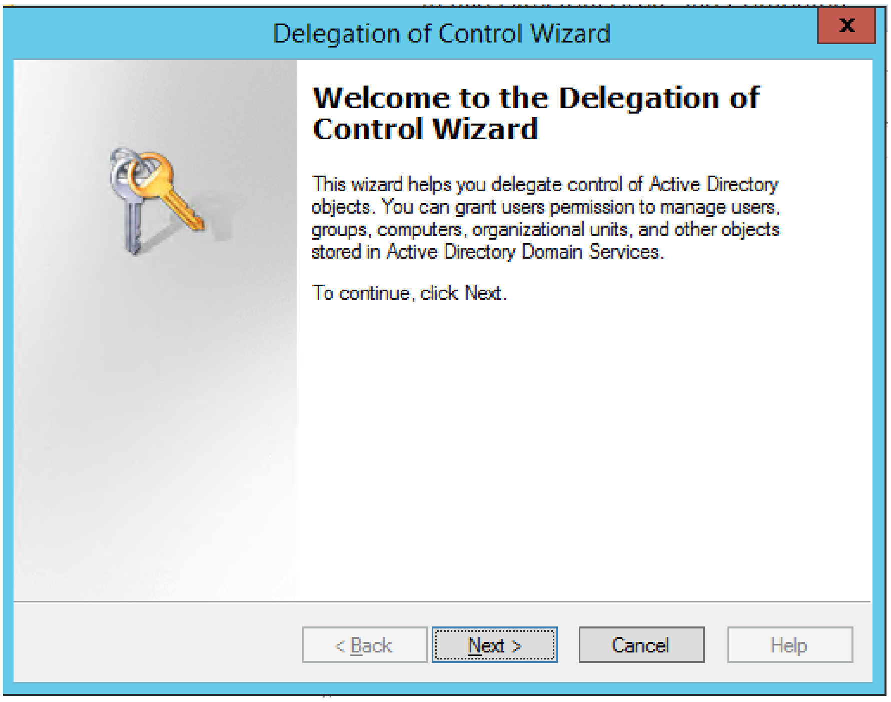


Name	Type	Description
Test Contact 1	Contact	
Test User 1	User	TestUser1
		TestUser2
		TestUser3
		TestUser4
	Gr...	Test DL 1
	oup...	

Allows you to raise the domain functional level to a level you select.

3. Click **Next**.

Figure 7-22: Delegate Control Wizard



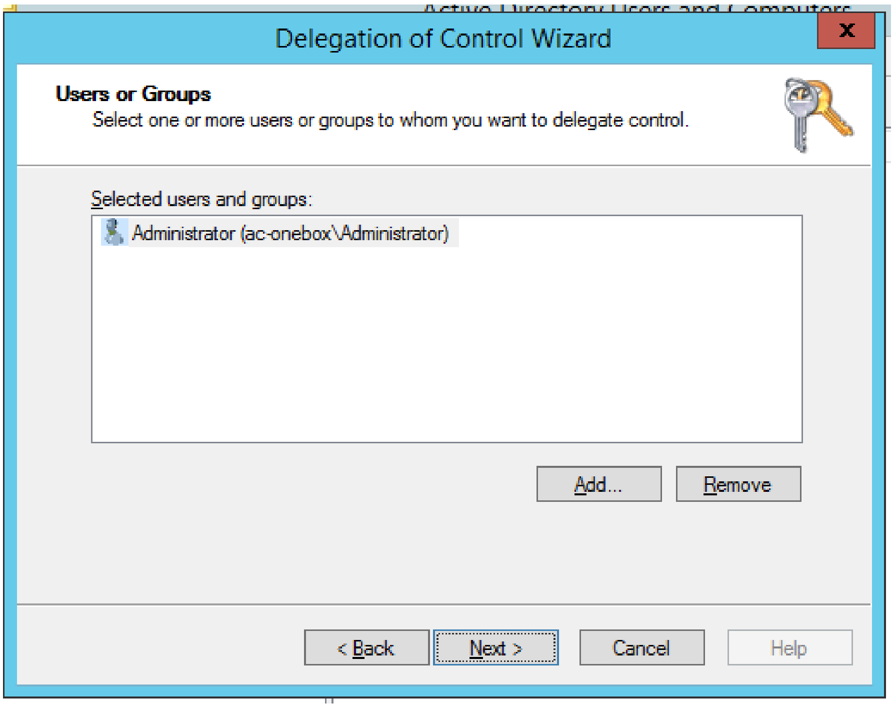
Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.

4. Click **Add**.

Figure 7-23: Delegate to CloudBond 365 Administrator



Delegation of Control Wizard

Users or Groups

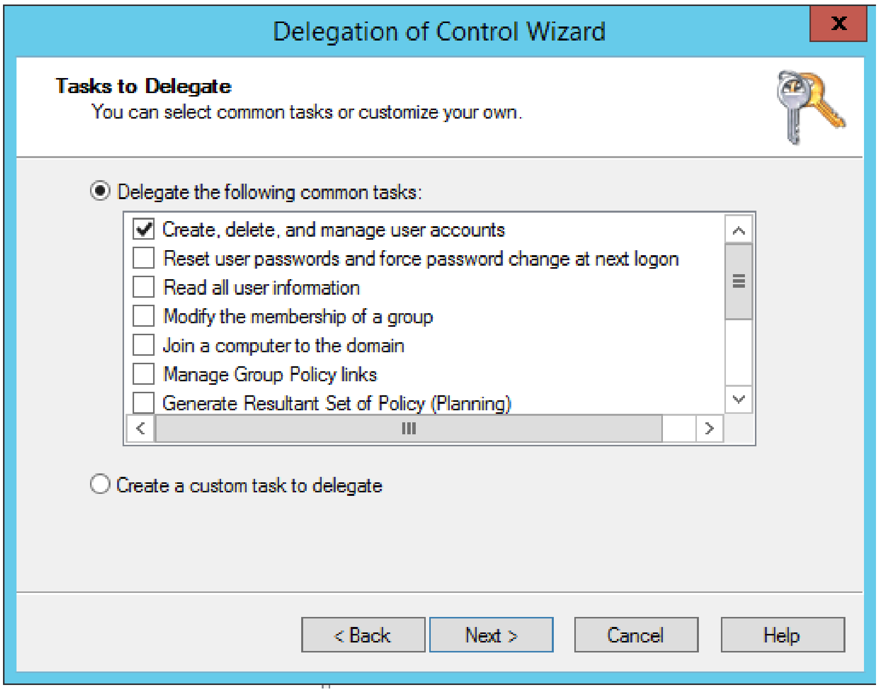
Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

Administrator (ac-onebox\Administrator)

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

Figure 7-24: Delegate Rights



Delegation of Control Wizard

Tasks to Delegate

You can select common tasks or customize your own.

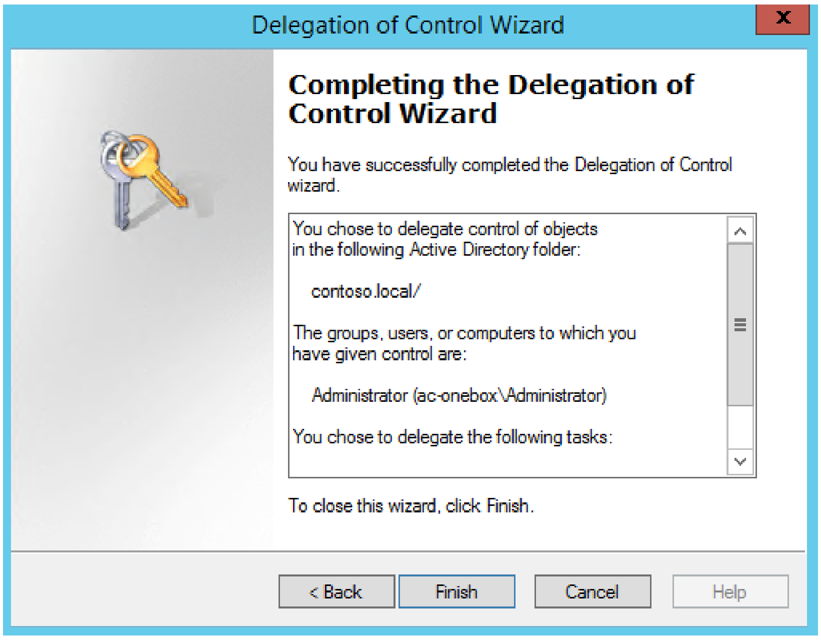
● Delegate the following common tasks:

- ☑ 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)

○ Create a custom task to delegate

6. Click **Finish**.

Figure 7-25: Complete the Wizard



Delegation of Control Wizard

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:

contoso.local/

The groups, users, or computers to which you have given control are:

Administrator (ac-onebox\Administrator)

You chose to delegate the following tasks:

To close this wizard, click Finish.

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)

7.9 Certificates

In all CloudBond 365 Editions, 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 will need to issue new certificates.

For more information, see Configuring Certificates on page 299

8 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.

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 authorative 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 publically available.

Other DNS configurations are possible.

8.1 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)

8.2 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 Skype for Business Phone Edition

Skype for Business phone edition devices are primarily for internal use within the enterprise network. (Skype for Business Mobile Clients are software clients for mobile devices, usually mobile phones, which are primarily intended for use outside the enterprise network.)

If Skype for Business Phone Edition devices are used, an NTP time source is required. (Windows time servers can be found with the command **`net time`** within the enterprise network. Widows Domain Controllers typically provide an NTP time source).

- SRV: _*ntp.*_udp.<FQDN> over port 123 to an enterprise NTP server

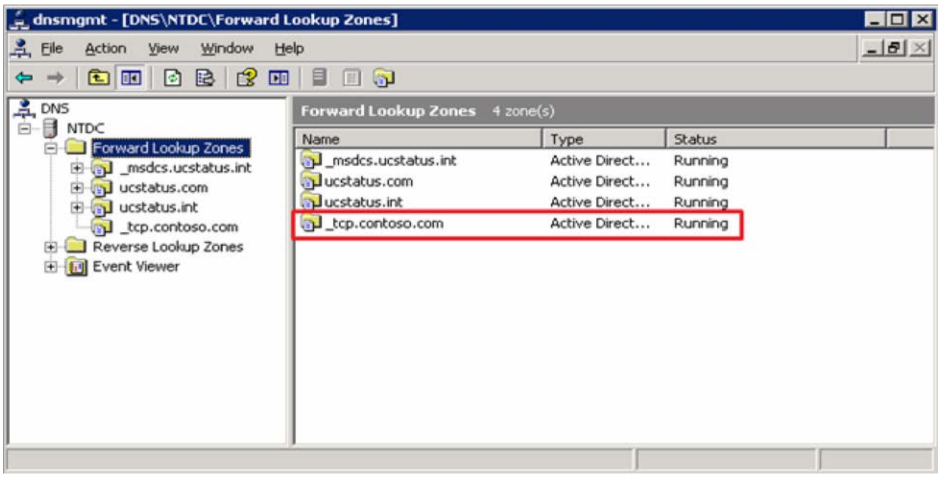
8.4 Skype for Business DNS Records without the Entire DNS Zone

When customers are unable to or unwilling to create a DNS Zone of the Public namespace internally in their AD environment, 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 how the finished domain will look.

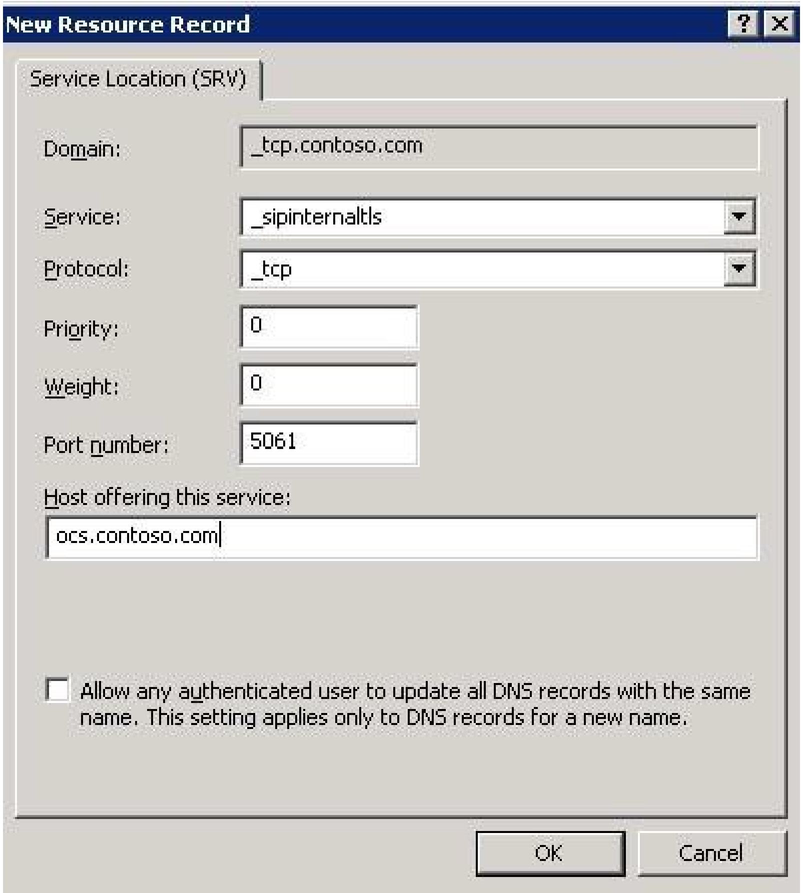
Figure 8-1: Forward Lookup Zones



Name	Type	Status
_msdcs.ucstatus.int	Active Direct...	Running
ucstatus.com	Active Direct...	Running
ucstatus.int	Active Direct...	Running
_tcp.contoso.com	Active Direct...	Running

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

Figure 8-2: New Resource Record



New Resource Record

Service Location (SRV)

Domain: _tcp.contoso.com

Service: _sipinternaltls

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 5061

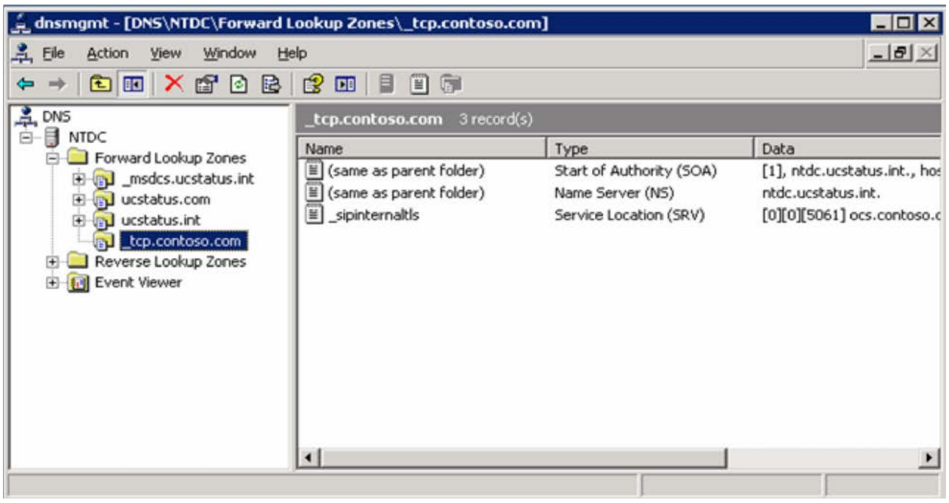
Host offering this service:

ocs.contoso.com

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

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

Figure 8-3: Forward Lookup Zones - _tcp.contoso.com



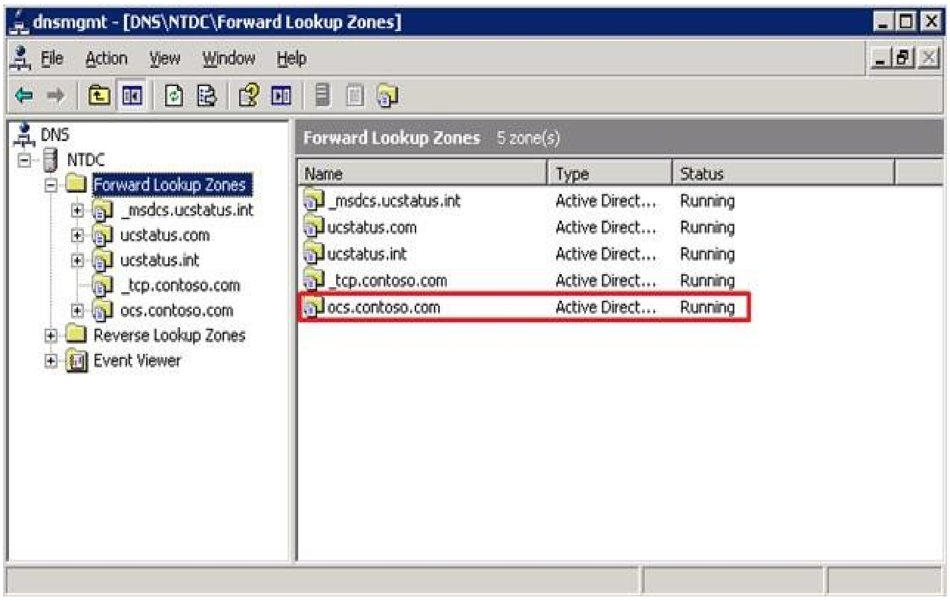
dnsmgmt - [DNS\NTDC\Forward Lookup Zones_tcp.contoso.com]

_tcp.contoso.com 3 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], ntdc.ucstatus.int., hos
(same as parent folder)	Name Server (NS)	ntdc.ucstatus.int.
_sipinternaltls	Service Location (SRV)	[0][0][5061] ocs.contoso.c

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 8-4: ocs.contoso.com



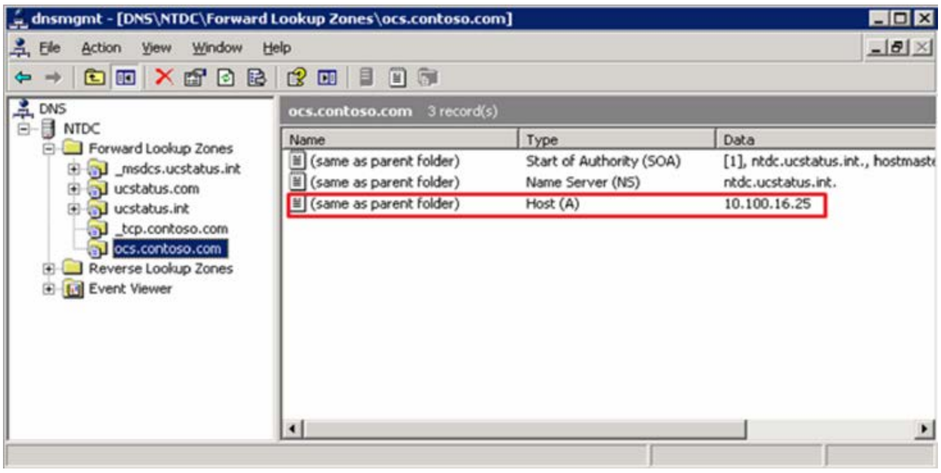
- DNS
  - NTDC
    - Forward Lookup Zones
      - _msdcs.ucstatus.int
      - ucstatus.com
      - ucstatus.int
      - _tcp.contoso.com
      - ocs.contoso.com
    - Reverse Lookup Zones
    - Event Viewer

Forward Lookup Zones 5 zone(s)

Name	Type	Status
_msdcs.ucstatus.int	Active Direct...	Running
ucstatus.com	Active Direct...	Running
ucstatus.int	Active Direct...	Running
_tcp.contoso.com	Active Direct...	Running
ocs.contoso.com	Active Direct...	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.

Figure 8-5: ocs.contoso.com – 3 records



- DNS
  - NTDC
    - Forward Lookup Zones
      - _msdcs.ucstatus.int
      - ucstatus.com
      - ucstatus.int
      - _tcp.contoso.com
      - ocs.contoso.com
    - Reverse Lookup Zones
    - Event Viewer

ocs.contoso.com 3 record(s)

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], ntdc.ucstatus.int., hostmaste
(same as parent folder)	Name Server (NS)	ntdc.ucstatus.int.
(same as parent folder)	Host (A)	10.100.16.25

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.

8.4.1 DNS Records for Non-Windows Clients

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

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

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

8.5 Add DHCP Entries for Skype for Business Phone Edition Devices

Skype for Business Phone Edition devices come in many varieties. They may be used to log in existing Skype for Business users, or they may be configured as 'Common Area Phones' which do not have authenticated Skype for Business users.

Skype for Business Phone Edition devices require additional configuration beyond that required for standard Skype for Business clients. Specifically, they require configuration to enable them to locate the Skype for Business front end servers.

This configuration may be performed directly on some model phones, or via special entries made in a DHCP server.

Definition of Skype for Business PIN policies and common area phones can only be performed through the Skype for Business Control panel and Skype for Business PowerShell environments.

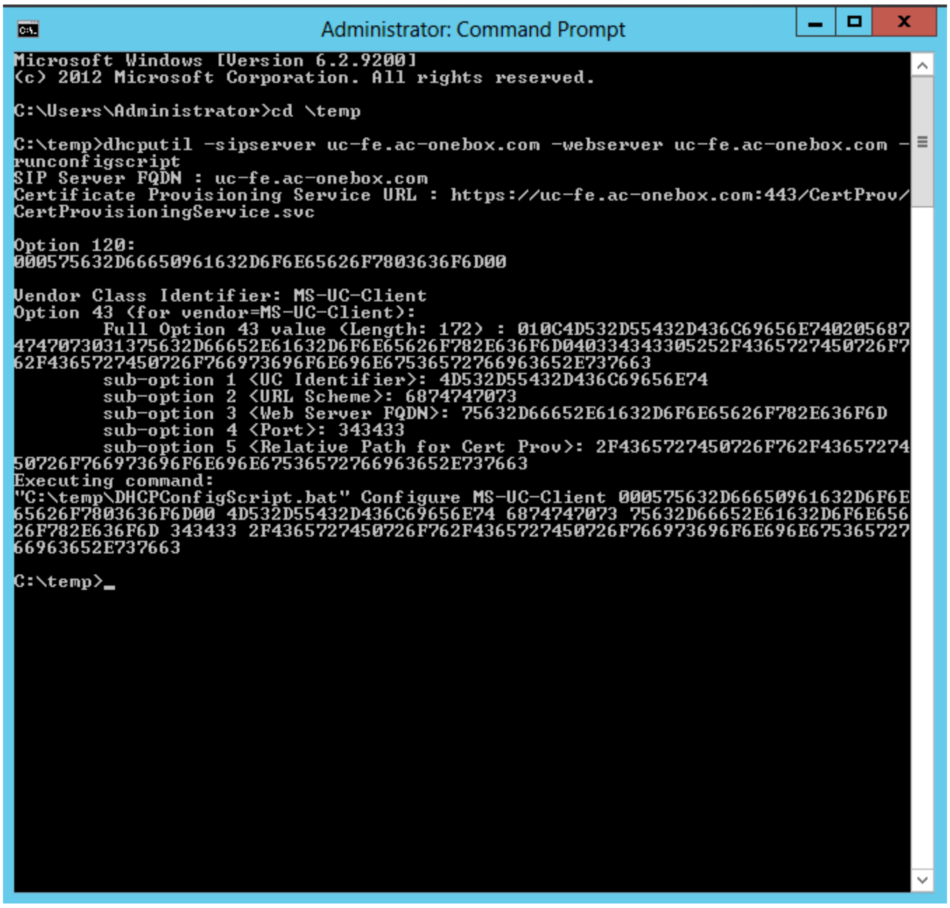
The following assumes a Microsoft DHCP server is available within the enterprise

1. Go to the enterprise's DHCP server
2. Download and Install VC++ from http://support.microsoft.com/kb/2019667
3. Copy Skype for Business DHCP utilities from CloudBond 365 FE server to the DHCP server
    - \\[FE]\c$\Program Files\Common Files\Microsoft Skype for Business Server \DHCPUtil.exe and
    - \\[FE]\c$\Program Files\Common Files\Microsoft Skype for Business Server \DHCPConfigScript.bat

4. Run the utilities (use CloudBond 365 FE FQDN names, not SIP FQDN names) with the following command:

```
DHCPUtil -SipServer UC-FE.cloudbond365.local -WebServer UC-
FE.cloudbond365.local
-RunConfigScript
```

Figure 8-6: Using DHCPUtil

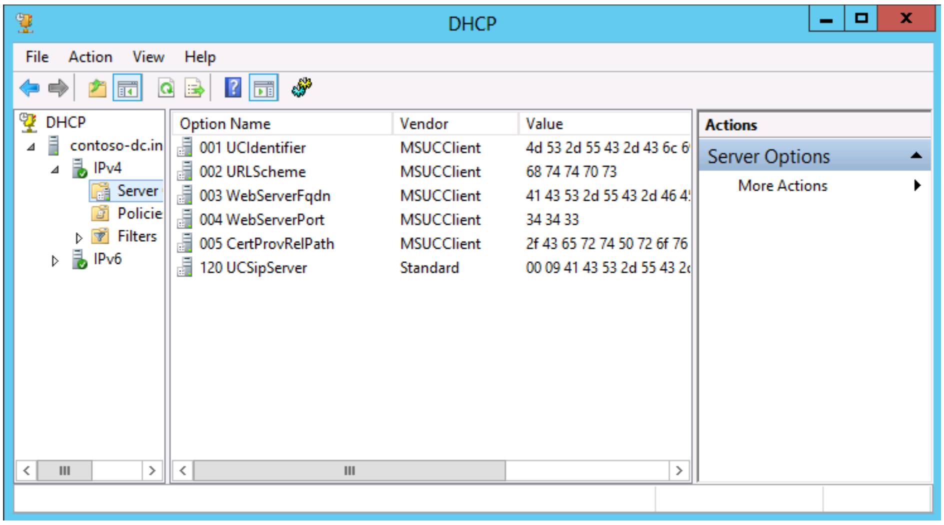


```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd \temp

C:\temp>dhcputil -sipserver uc-fe.ac-onebox.com -webserver uc-fe.ac-onebox.com -
runconfigscript
SIP Server FQDN : uc-fe.ac-onebox.com
Certificate Provisioning Service URL : https://uc-fe.ac-onebox.com:443/CertProv/
CertProvisioningService.svc

Option 120:
000575632D66650961632D6F6E65626F7803636F6D00

Vendor Class Identifier: MS-UC-Client
Option 43 (for vendor=MS-UC-Client):
        Full Option 43 value (Length: 172) : 010C4D532D55432D436C69656E740205687
474707303137563 2D66652E61632D6F6E65626F782E636F6D0403343433305252F4365727450726F7
62F4365727450726F766973696F6E696E6753657276696363652E737663
        sub-option 1 <UC Identifier>: 4D532D55432D436C69656E74
        sub-option 2 <URL Scheme>: 6874747073
        sub-option 3 <Web Server FQDN>: 75632D66652E61632D6F6E65626F782E636F6D
        sub-option 4 <Port>: 343433
        sub-option 5 <Relative Path for Cert Prov>: 2F4365727450726F762F43657274
50726F766973696F6E696E6753657276696363652E737663
Executing command:
"C:\temp\DHCPConfigScript.bat" Configure MS-UC-Client 000575632D66650961632D6F6E
65626F7803636F6D00 4D532D55432D436C69656E74 6874747073 75632D66652E61632D6F6E656
26F782E636F6D 343433 2F4365727450726F762F4365727450726F766973696F6E696E675365727
66963652E737663

C:\temp>_
```

5. Open the DHCP utility and verify DHCP server settings for:

- 120 UCSipServer
- 043 (001-005)

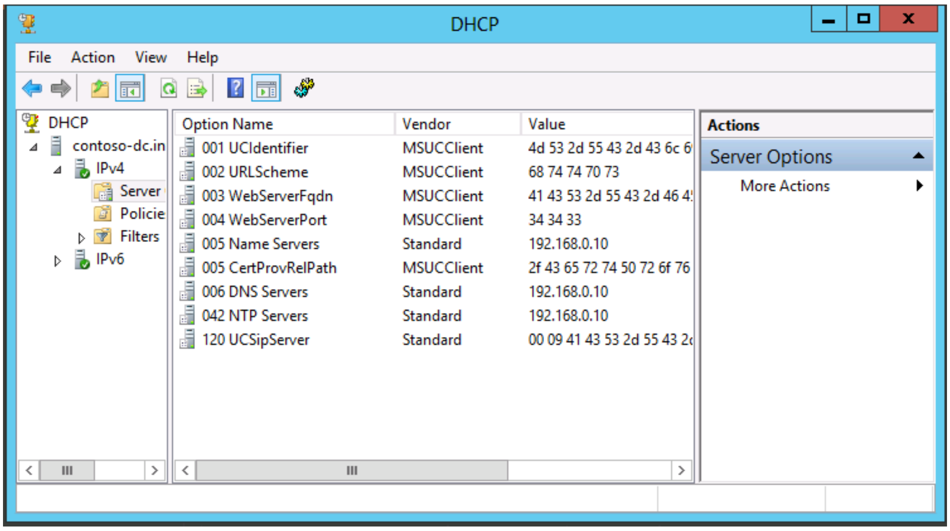
Figure 8-7: DHCP Settings



Option Name	Vendor	Value
001 UCIdentifier	MSUCClient	4d 53 2d 55 43 2d 43 6c 6
002 URLScheme	MSUCClient	68 74 74 70 73
003 WebServerFqdn	MSUCClient	41 43 53 2d 55 43 2d 46 4
004 WebServerPort	MSUCClient	34 34 33
005 CertProvRelPath	MSUCClient	2f 43 65 72 74 50 72 6f 76
120 UCSipServer	Standard	00 09 41 43 53 2d 55 43 2

6. Add Server options for the following
    - 005 Names Servers
    - 006 DNS Servers
    - 042 NTP Server.

Figure 8-8: DHCP Settings



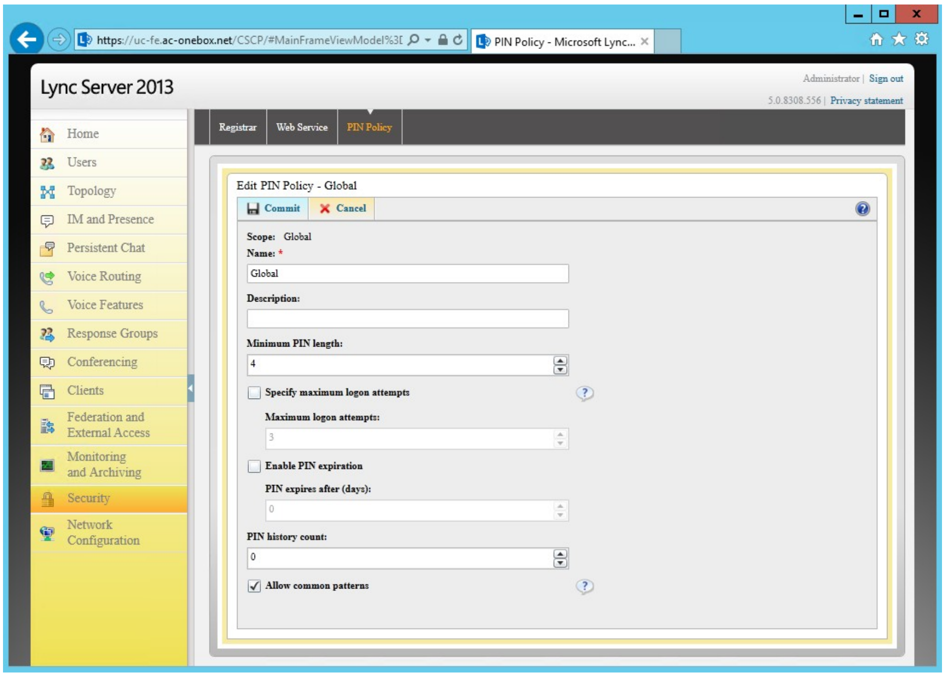
Option Name	Vendor	Value
001 UCIdentifier	MSUCClient	4d 53 2d 55 43 2d 43 6c 6
002 URLScheme	MSUCClient	68 74 74 70 73
003 WebServerFqdn	MSUCClient	41 43 53 2d 55 43 2d 46 4
004 WebServerPort	MSUCClient	34 34 33
005 Name Servers	Standard	192.168.0.10
005 CertProvRelPath	MSUCClient	2f 43 65 72 74 50 72 6f 76
006 DNS Servers	Standard	192.168.0.10
042 NTP Servers	Standard	192.168.0.10
120 UCSipServer	Standard	00 09 41 43 53 2d 55 43 2

7. Set pin policy

8. Open Skype for Business control panel https://UC-FE.cloudbond365.local/CSCP

9. Set pin policy via **Security** > **Pin Policy**
    a. Note the Minimum Pin Length and Allow common Pattern settings

Figure 8-9: Skype for Business PIN Policy



Edit PIN Policy - Global

Scope: Global

Name: *

Global

Description:

Minimum PIN length:

4

□ Specify maximum logon attempts

Maximum logon attempts:

3

□ Enable PIN expiration

PIN expires after (days):

0

PIN history count:

0

☑ Allow common patterns

    b. Commit the changes.

10. Allow Hot desking:

    a. On the CloudBond 365 Controller server, open the Skype for Business Server Management Shell, and enter the command:

    ```
    Set-CsClientPolicy -Identity Global -EnableHotdesking $TRUE
    ```

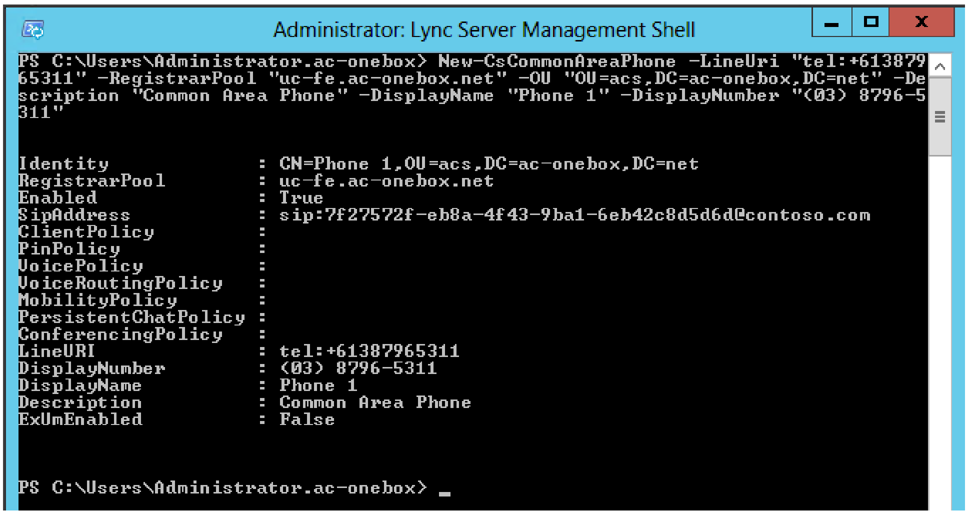
11. Create a common area phone.

> **Note:** Common Area Phones may now be defined using the **SysAdmin** > **Create Device** page. This page replaces the New-csCommonAreaPhone command below. See also *AudioCodes CloudBond 365 Administration Guide*.

    a. On the CloudBond 365 Controller server, open the Skype for Business Server Management Shell, and enter the command:

    ```
    New-CsCommonAreaPhone -LineUri "tel:+61387965111" -
    RegistrarPool "uc-fe.cloudbond365.local" -OU "OU=acs,DC=ac-
    onebox,DC=com" -Description "Common Area Phone" -
    DisplayName
    "Phone 1" -DisplayNumber "(03) 8796-5311"
    ```

Figure 8-10: Common Area Phones



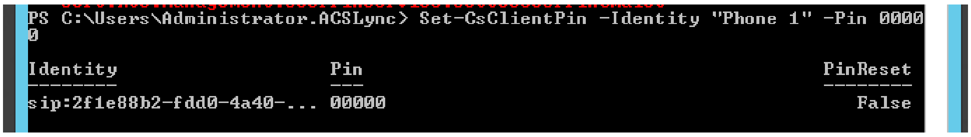
```
PS C:\Users\Administrator.ac-onebox> New-CsCommonAreaPhone -LineUri "tel:+613879
65311" -RegistrarPool "uc-fe.ac-onebox.net" -OU "OU=acs,DC=ac-onebox,DC=net" -De
scription "Common Area Phone" -DisplayName "Phone 1" -DisplayNumber "(03) 8796-5
311"


Identity                : CN=Phone 1,OU=acs,DC=ac-onebox,DC=net
RegistrarPool           : uc-fe.ac-onebox.net
Enabled                 : True
SipAddress              : sip:7f27572f-eb8a-4f43-9ba1-6eb42c8d5d6d@contoso.com
ClientPolicy            :
PinPolicy               :
VoicePolicy             :
VoiceRoutingPolicy      :
MobilityPolicy          :
PersistentChatPolicy    :
ConferencingPolicy      :
LineURI                 : tel:+61387965311
DisplayNumber           : (03) 8796-5311
DisplayName             : Phone 1
Description             : Common Area Phone
ExUmEnabled             : False



PS C:\Users\Administrator.ac-onebox> _
```

12. Set the phones pin

    - On the CloudBond 365 Controller server, open the Skype for Business Server Management Shell, and enter the command:

    ```
    Set-CsClientPin –I denti ty “Phone 1 ” -Pin 00000
    ```

Figure 8-11: Setting Common Area Phone PIN



```
PS C:\Users\Administrator.ACSLync> Set-CsClientPin -Identity "Phone 1" -Pin 0000
0

Identity                     Pin                                        PinReset
--------                     ---                                        --------
sip:2f1e88b2-fdd0-4a40-...   00000                                         False
```

13. Plug in a phone and test.

> **Note:** For more info about configuring AudioCodes Skype for Business IP Phone See also *AudioCodes CloudBond 365 Administration Guide*.

This page is intentionally left blank.

9 Firewall Port Requirements

This chapter describes the port requirements for placing the AudioCodes CloudBond 365™ system behind a firewall.

This guide provides:

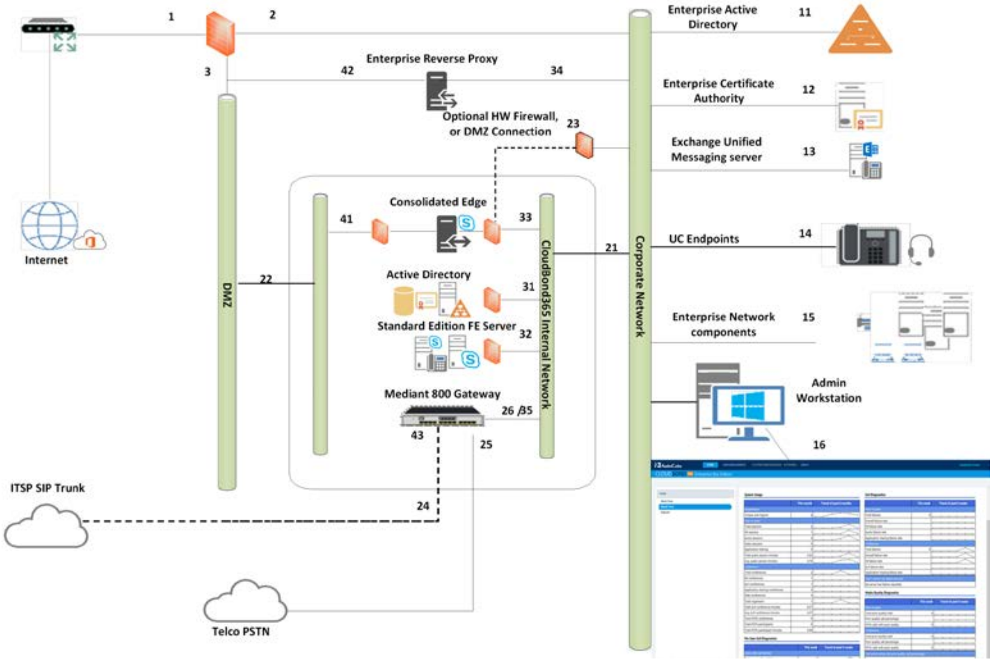
- Overview of AudioCodes CloudBond 365™ Deployment
- Perimeter Network port requirements for Reverse Proxy and Consolidated Edge
- Port Requirements if internal firewalls are deployed

Throughout this guide, AudioCodes CloudBond 365 will be referred to as CloudBond 365.

9.1 CloudBond 365 Deployment Overview

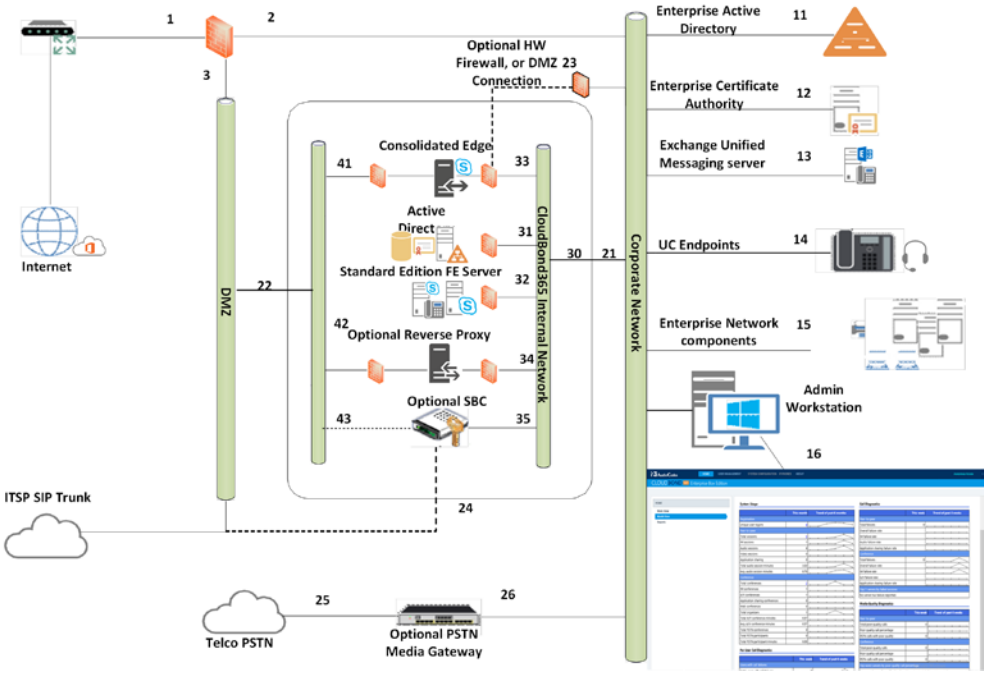
A network diagram for CloudBond 365 Standard Edition deployed in an enterprise network is shown below:

Figure 9-1: CloudBond 365 Standard Edition



A network diagram for CloudBond 365 Pro / Enterprise Edition deployed in an enterprise network is shown below:

Figure 9-2: CloudBond 365 Pro / Enterprise Edition


1
2
3
Optional HW Firewall, or DMZ 23 Connection
Enterprise Active Directory
11
Enterprise Certificate Authority
12
Exchange Unified Messaging server
13
Consolidated Edge
41
33
Active Direct
31
Standard Edition FE Server
32
30
21
UC Endpoints
14
Internet
22
DMZ
42
Optional Reverse Proxy
34
CloudBond365 Internal Network
Corporate Network
Enterprise Network components
15
Optional SBC
43
35
Admin Workstation
16
ITSP SIP Trunk
24
25
26
Telco PSTN
Optional PSTN Media Gateway

9.1.1 References

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

9.1.1.1 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 365 installation will need to be adapted to suit the customer environment.

1. 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
2. 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
3. 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.

9.1.1.2 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 Voice 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
17. Enterprise Revers Proxy Server (not available in the diagram)
    - A Reverse Proxy server is required for some external connectivity functions of Skype for Business, such as Skype for Business Mobile Clients. Microsoft best practice recommends a Reverse Proxy server rather than allowing direct external connections to the FE server.
    - If the customer has an existing Reverse Proxy server, it should be used in preference to the internal CloudBond 365 Reverse Proxy

9.1.1.3 CloudBond 365 Physical Connections

All CloudBond 365 Editions require an internal network connection (21) for clients to connect. It is highly recommended that an external network connection (22) is provided to maximize the features and usability of CloudBond 365.

All versions of CloudBond 365 have “space” network adapters (23, 24) which can optionally be used to separate network traffic and enhance network security where required.

21. Corporate LAN Connection (trusted network)
    - CloudBond 365 Standard Edition uses front GE1 connector
    - CloudBond 365 Pro / Enterprise Edition uses rear NIC # 1
22. DMZ Connector (untrusted public network)
    - CloudBond 365 Standard Edition uses rear GE1 connector
    - CloudBond 365 Pro / Enterprise Edition uses rear NIC # 2
23. Optional Edge firewall connector
    - CloudBond 365 Standard Edition uses rear GE2 connector
    - CloudBond 365 Pro / Enterprise Edition uses rear NIC # 3
24. Optional SBC ITSP Connection
    - CloudBond 365 Standard Edition uses front GE3 connector or WAN connector
    - CloudBond 365 Pro / Enterprise Edition uses rear NIC # 4
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

9.1.1.4 CloudBond 365 Internal Connections

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

9.1.1.4.1 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, but doing so requires additional manual configuration of the CloudBond 365 component affected.

30. Hyper-V Host IP address (Optional)
    - Applies only to CloudBond 365 Pro/Enterprise Edition
    - For CloudBond 365 Standard Edition, this is the same as 31
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. Optional Reverse Proxy Server
    - Available in CloudBond 365 Pro / Enterprise Edition only
    - May exist as external Enterprise server
    - Used for Mobile clients, web conferencing, address book expansion etc.
    - Default 192.168.0.104
35. Optional AudioCodes SBC
    - Available as optional server in CloudBond 365 Pro / Enterprise
        - ♦ Default address 192.168.0.1
    - Available as SBC component of Mediant 800 gateway in CloudBond 365 standard edition
        - ♦ Default address 192.168.0.2

9.1.1.4.2 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.
42. Reverse Proxy external address
    - Used for Mobile clients, conferencing, address book expansion, etc.
    - Entry required in Public DNS and Certificates. Typically meet.contoso.com
    - Skype for Business traffic forwarded to Front End server (UC-FE)
43. SBC External Address
    - Used as SIP Trunk endpoint from ITSP

9.1.1.4.3 EMS Management Network

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

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

9.1.1.4.4 Internet Access

In general, each of the CloudBond 365 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, if you choose to deploy the optional CloudBond 365 Office365 connector, the CloudBond 365 Controller (DC) will need internet access to retrieve user information from Office365, via port 443.

9.2 Perimeter Network Port Requirements

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

9.2.1 Reverse Proxy

The Reverse Proxy (RP) server passes traffic between the external network (Internet) and the CloudBond 365 Front End server. This traffic allows dial-in conferencing, mobile clients, desktop sharing amongst other features. It is largely Web based traffic.

9.2.1.1 Firewall Details for Reverse Proxy Server: External Interface #42

Figure 9-3: Reverse Proxy

Protocol/Port	Use for
HTTP 80 (in)	(Optional) Redirection to HTTPS if user accidentally enters HTTP instead of HTTPS *N.B. Used by some Skype for Business Mobile Clients*
HTTPS 443 (in)	Address book downloads, Address Book Web Query service, client updates, meeting content, device updates, group expansion, dial-in conferencing, and meetings.

9.2.1.2 Firewall Details for Reverse Proxy Server: Internal Interface #34

Figure 9-4: Reverse Proxy

Protocol/Port	Used for
HTTPS 4443 (in)	Traffic sent to 443 on the reverse proxy external interface is redirected to a pool on port 4443 from the reverse proxy internal interface so that the pool web services can distinguish it from internal web traffic

9.2.2 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.

9.2.2.1 Determining External A/V Firewall and Port Requirements

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

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

When reading the tables, *(in)* refers to traffic going 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 going 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. And, *(in/out)* refers to traffic that is going both directions.

9.2.2.1.1 Inbound/Outbound Edge Traffic

Figure 9-5: Edge Server

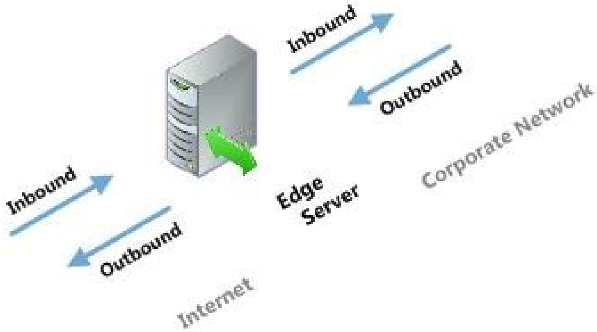
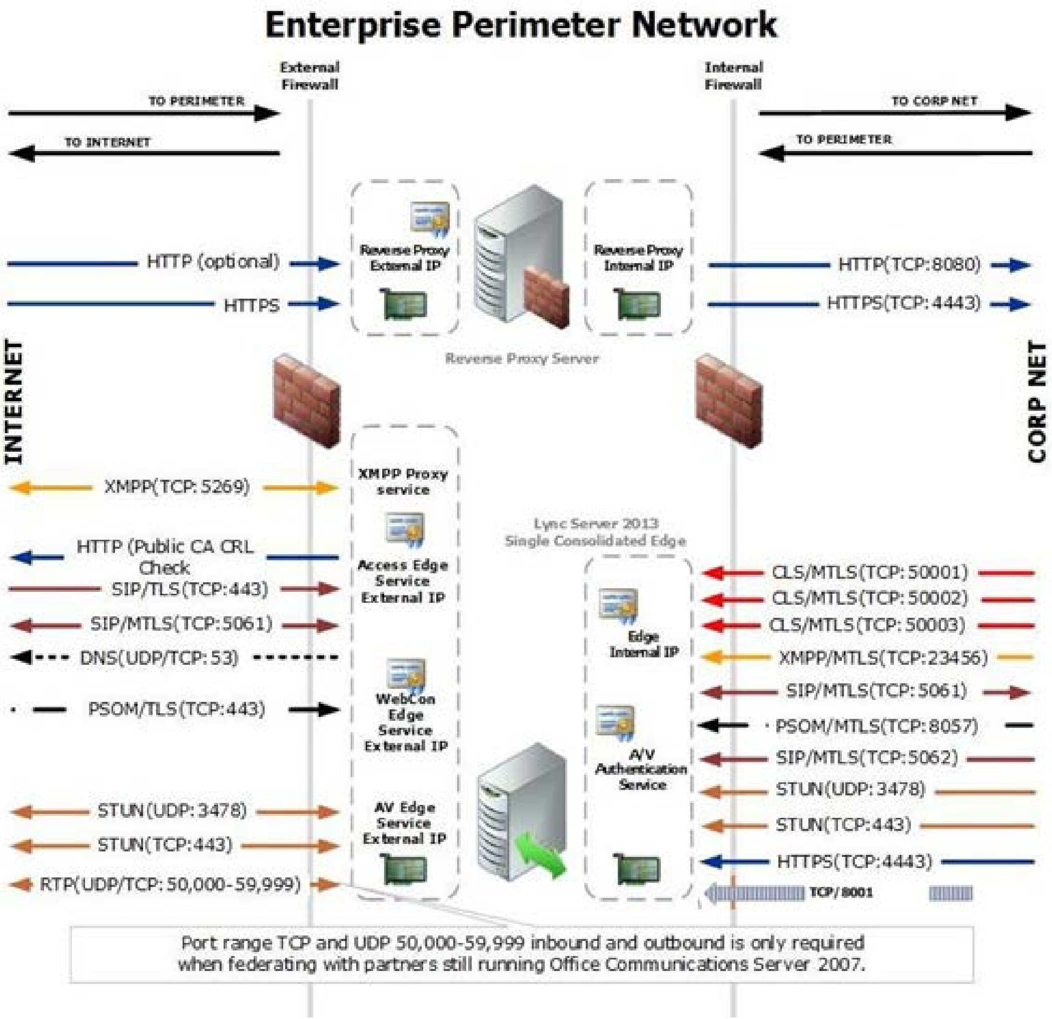


Figure 9-6: Edge Server



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

Table 9-1: Edge Server

Protocol/Port	Used for
XMPP/TCP/5269 (in/out)	XMPP Proxy service accepts traffic from XMPP contacts in defined XMPP federations
HTTP 80 (out)	Checking certificate revocation lists
DNS 53 (out)	External DNS queries
SIP/TLS/MTLS/5061 (in/out)	Client to server SIP traffic for remote user access Federation and connectivity with a hosted Exchange service
PSOM/TLS/444 (in)	Remote user access to conferences for anonymous and federated users
RTP/TCP/50K range (in)	Media exchange and Windows Live Messenger if public IM connectivity is enabled. Required for Office Communications Server 2007 R2 interoperability
RTP/TCP/50K range (out)	Media exchange. Required for Office Communications Server 2007 R2 interoperability Required for Office Communications Server 2007 R2 desktop sharing and federation Required for Lync 2010 application sharing, file transfer, or A/V with Windows Live Messenger
RTP/UDP/50K range (in)	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)

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

Table 9-2: Edge Server

Protocol/Port	Used for
XMPP/MTLS/TCP (out)	Outbound XMPP traffic from XMPP Gateway service running on Front End Server or Front End pool
SIP/MTLS/5061 (in/out)	SIP traffic
PSOM/MTLS/8057 (out)	Web conferencing traffic from pool to Edge Server
SIP/MTLS/5062 (out)	Authentication of A/V users (A/V authentication service)

Protocol/Port	Used for
STUN/MSTURN/UDP/3478 (out)	Preferred path for media transfer between internal and external users (UDP)
STUN/MSTURN/TCP/443 (out)	Alternate path for media transfer between internal and external users (TCP)
HTTPS 4443 (out)	Pushing Central Management store updates to Edge Servers
TCP 8001 (out)	CloudBond 365 Edge worker process
MTLS/TCP/50001 (out)	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50002 (out)	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection
MTLS/TCP/50003 (out)	Centralized Logging Service controller using Skype for Business Server Management Shell and Centralized Logging Service cmdlets, ClsController command line (ClsController.exe) or agent (ClsAgent.exe) commands and log collection

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

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

9.2.3 Management Server

These firewall settings are required only if your CloudBond 365 is to be managed and monitored by the AudioCodes Element Management Server (EMS)

- On CloudBond 365 Standard/Standard Plus Edition apply to Hyper-V Host
- On CloudBond 365 Pro/Enterprise Edition apply to Domain Controller server.

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

Table 9-3: Hyper-V Host Server

Protocol/Port	Used to
HTTPS 443 (out)	Connect to the EMS Server to retrieve updates from the License Pool Manager, for example, to retrieve the latest license.

SNMP (UDP) 162 (out)	Connect to the EMS 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 EMS Server to send keep-alive traps that are used for the EMS to add CloudBond devices to the EMS, and for the CloudBond 365 keep-alive status.

9.2.3.2 Firewall Details for Domain-Controller Server: Internal Interface #21

Table 9-4: Domain Controller Server

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

9.3 Other Port Requirements

This section 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.

9.3.1 Network Ports Used by Trusts

Because 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.

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

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

Table 9-3: AD Trust

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

9.3.1.2 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

9.3.1.2.1 Ports REG_MULTI_SZ

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.

9.3.1.2.2 PortsInternetAvailable REG_SZ

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.

9.3.1.2.3 UseInternetPorts REG_SZ

Y or N (not case-sensitive) 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.

9.3.2 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

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

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

Table 9-4: 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.

Server Ports	Service name	Notes
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).
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
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.

Server Ports	Service name	Notes
5064/TCP	Skype for Business Server Conferencing Attendant service (dial-in conferencing)	Used for incoming SIP requests for dial-in conferencing.
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 (that is, 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.

Server Ports	Service name	Notes
8057/TCP	Skype for Business Server Web Conferencing service	Used to listen for Persistent Shared Object Model (PSOM) connections from client.
8058/TCP	Skype for Business Server Web Conferencing Compatibility service	Used to listen for Persistent Shared Object Model (PSOM) connections from the Live Meeting client and previous versions of Communicator.
8404/TCP	Skype for Business Server Response Group service	Used for incoming SIP requests for the Response Group application.
8861/TCP	EMS Agent	Used for report components alarms from the EMS Monitor Agents to the EMS main agent.
8863/TCP	EMS Agent	Used by the EMS main agent to retrieve the status from the EMS Monitor Agents.
49152-65335/TCP	Skype for Business Server Application Sharing service	Media port range used for application sharing. This range can be restricted with the Set-CSWebServer <FQDN of Web Server> -AppSharingPortCount <at least 100> -AppSharingPortStart <port start> cmdlet
49152- 57500/TCP/UDP	Various	Media port range used for audio conferencing on all internal servers. Used by all servers that terminate audio: Front End Servers (for Skype for Business Server Conferencing Attendant service, Skype for Business Server Conferencing Announcement service, and Skype for Business Server Audio/Video Conferencing service), and Mediation Server. This range can be restricted with the Set-CSWebServer <FQDN of Web Server> - AudioPortCount <at least 100> -AudioPortStart <port start> cmdlet
57501- 65335/TCP/UDP	Skype for Business Server Audio/Video Conferencing service	Media port range used for video conferencing. This range can be restricted with the Set-CSWebServer <FQDN of Web Server> -VideoPortCount <at least 100> -VideoPortStart <port start> cmdlet

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

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

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

Table 9-7: Skype for Business Clients

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

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

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

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

9.3.3 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.

9.3.4 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.

9.3.4.1 Unified Messaging Protocols and Services

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

Warning:. On Exchange 2010 Unified Messaging servers, Exchange setup creates the **SESWorker (TCP-In)** and **SESWorker (GFW) (TCP-In)** rules which allow inbound communication without any TCP port restrictions. We recommend you disable these two rules after you’ve setup the Unified Messaging server, and create a new rule to allow only the ports required for the SESWorker process which include 5065 and 5067 for TCP (unsecured). 5066 and 5068 for mutual TLS (secured). For details, see Exchange Network Port Reference.

9.3.4.1.1 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).

9.3.4.1.2 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.

9.3.4.1.3 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 Web services:

- 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 that have the Unified Messaging server role installed.

9.3.4.1.4 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 9-8: 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.

Protocol	TCP Port	UDP Port	Can Ports be Changed?
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.

9.3.4.1.4.1 Unified Messaging Server Data Paths

Table 9-9: Unified Messaging

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

Data Path	Required Ports	Default Authentication	Supported Authentication	Encryption Supported?	Encrypted by Default?
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
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

Part III

Installing CloudBond 365

This part includes the following:

- Hardware installation (see Chapter 10)
- Software installation (see Chapter 11)

10 Hardware Installation

This part provides a hardware description and step-by-step cabling procedures for AudioCodes' CloudBond 365 Pro and Enterprise Box Editions.

10.1 Specifications

The table below shows the CloudBond 365 specifications.

Table 10-1: CloudBond 365 Specifications

Resource	Specifications	
	CloudBond 365 Pro Box Edition	CloudBond 365 Enterprise Box Edition
Chassis Type	1RU system	1RU system
CPU	6 Core Processor	2 Processors with 12 Cores
Memory	32GB RAM	64GB RAM
Network	4 x 1 GbE ports	4 x 1 GbE ports
Disk	2HDD with RAID 1	4HDD with RAID 5
CD/DVD	SATA CD/DVD R/W	SATA CD/DVD R/W
Installation Interface	VGA Monitor and Keyboard	VGA Monitor and Keyboard

10.2 Physical Description

This chapter provides a physical description of the device.

10.2.1 Physical Dimensions

The device's physical dimensions are listed in the table below.

Table 10-2: Physical Dimensions

Item	Description
Physical Dimensions	1U x 445 mm x 743 mm (HxWxD)
Weight	27.27 kg (60.00 lb)
Environmental	Operational: 10 to 35°C

10.2.2 Front Panel

The CloudBond 365 features an 8-SFF (Small Form Factor) cage for standard internal storage hard drives. The device's front panel is shown in the figures below and described in the subsequent table.

Figure 10-1: Front Panel

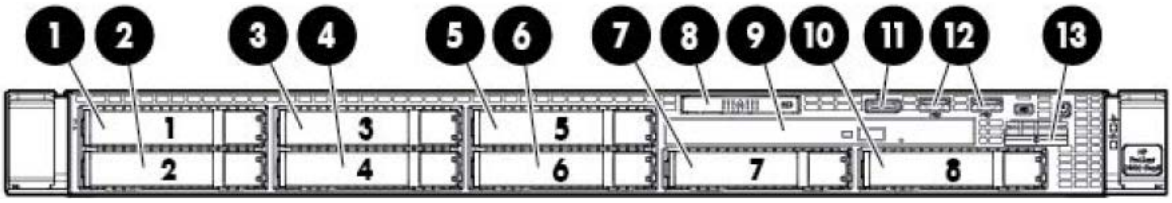


Table 10-3: Front Panel

Item #	Description
1	SAS/SATA/SSD drive bay 1
2	SAS/SATA/SSD drive bay 2
3	SAS/SATA/SSD drive bay 3
4	SAS/SATA/SSD drive bay 4
5	SAS/SATA/SSD drive bay 5
6	SAS/SATA/SSD drive bay 6
7	SAS/SATA/SSD drive bay 7
8	Systems Insight Display
9	DVD-ROM drive (optional)
10	SAS/SATA/SSD drive bay 8 (optional)
11	Front video connector (front video port adapter required)
12	USB connectors (2)
13	Serial number tab

10.2.2.1 Front Panel LEDs

The front panel LEDs are shown in the figure below and described in the subsequent table.

Figure 10-2: Front Panel LEDs

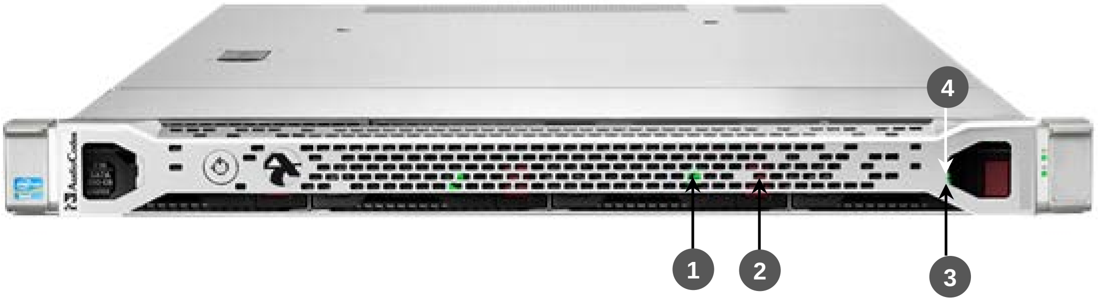


Table 10-4: Front-Panel LEDs

Item #	Description	Status
1	UID LED/button	- Solid blue = Identification is activated. - Flashing blue = System is being managed remotely. - Off = Identification is deactivated.
2	Power On/Standby button/LED	- Solid green = System is On. - Flashing green = Waiting for server power sequence. - Solid amber = System is in standby, but power is still applied. - Off = Power cord is not attached, power supply failure has occurred, no power supplies are installed, facility power is not available, or the power button cable is disconnected
3	Health LED	- Solid green = System health is normal. - Flashing amber = System health is degraded. - Flashing red = System health is critical. - Fast flashing red = Power fault (check system and devices).
4	Aggregate network LED	- Solid green = Link to network. - Flashing green = Network activity. - Off = No network connection.

10.2.3 Rear Panel

The rear panel is displayed in the figure below and described in the subsequent table.

Figure 10-3: Rear Panel

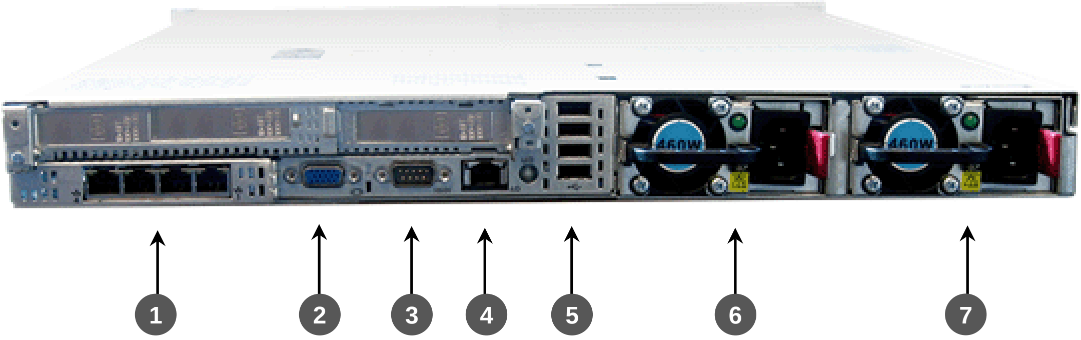


Table 10-5: Rear Panel

Item #	Description
1	4 GbE ports
2	Video connector
3	Serial connector
4	HP iLO port (see http://www8.hp.com/us/en/products/servers/ilo/)
5	USB connectors (4)
6	Power supply bay 1 (primary and redundant power supply supported)

Item #	Description
7	Power supply bay 2 (primary and redundant power supply supported)

10.2.3.1 Rear Panel LEDs

The rear panel LEDs are shown in the figure below and described in the subsequent table.

Figure 10-4: Rear Panel LEDs

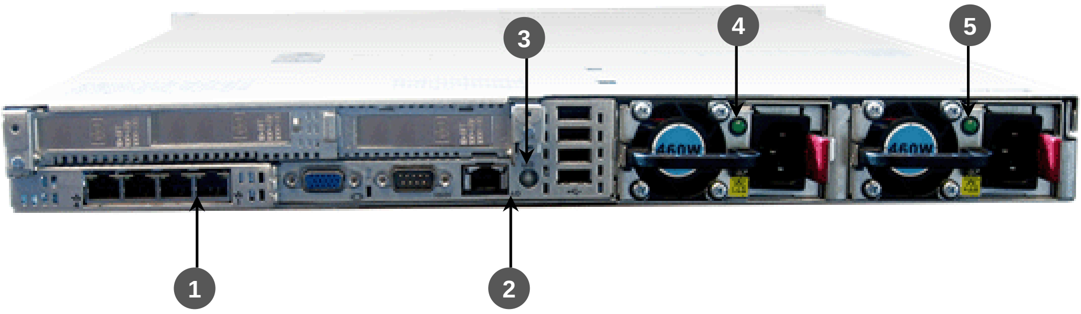


Table 10-6: Rear Panel LEDs

Item #	Description	Status
1	Standard NIC activity LED	• Solid green = Activity exists. • Flashing green = Activity exists. • Off = No activity exists.
2	iLO NIC link LED	• Solid green = Link exists. • Off = No link exists.
3	UID button/LED	• Solid blue = Identification is activated. • Flashing blue = System is being managed remotely. • Off = Identification is deactivated.
4	Power Supply 2 LED	• Solid green = Normal. • Off = One or more of the following conditions exists: ✓ AC power unavailable. ✓ Power supply failed. ✓ Power supply in standby mode. ✓ Power supply exceeded current limit.
5	Power Supply 1 LED	• Solid green = Normal. • Off = One or more of the following conditions exists: ✓ AC power unavailable. ✓ Power supply failed. ✓ Power supply in standby mode. ✓ Power supply exceeded current limit.

10.3 Deploying the Device

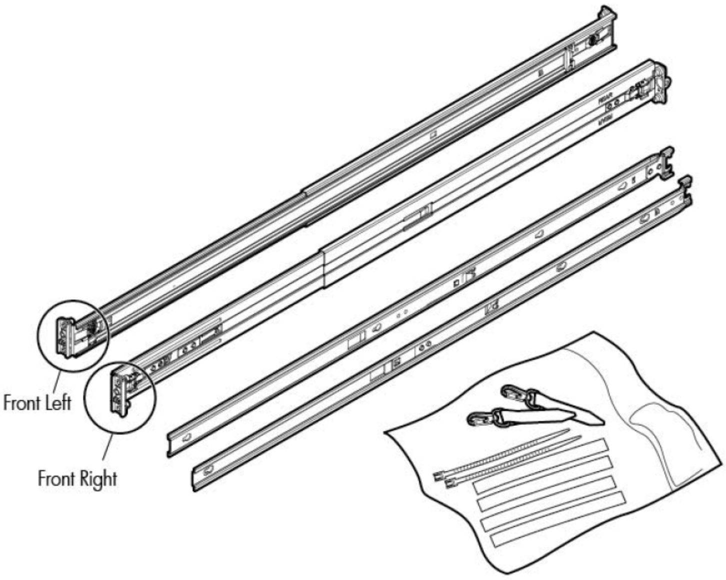
This chapter shows how to deploy the device in a commercial rack mount kit.

10.3.1 Hardware Kit Contents

Warning: To reduce the risk of personal injury or damage to the equipment, at least two people are required to lift the server during installation or removal.

Note: When installing the rack rails, be sure they are oriented Front Left and Front Right, as indicated on the rails.

Figure 10-5: Hardware Kit Contents



You must provide:

- Screws to secure the slide mounting bracket assemblies in a threaded-hole rack
- Cage nuts for a round-hole rack
- Screws that fit a threaded-hole rack
- The appropriate screwdriver for the screws

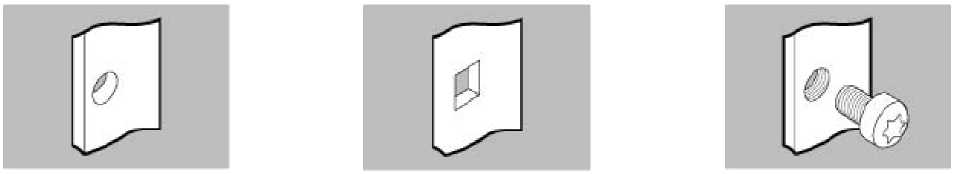
10.3.2 Overview

This rack hardware kit supports a variety of products in round-, square-, or threaded-hole racks. Use the legend to identify installation steps appropriate to the type of rack.

Note: If you are shipping the server installed in a rack, see the additional instructions located in "Preparing the product for integrated shipping in a rack" before proceeding.

10.3.3 Rack Identification Legend

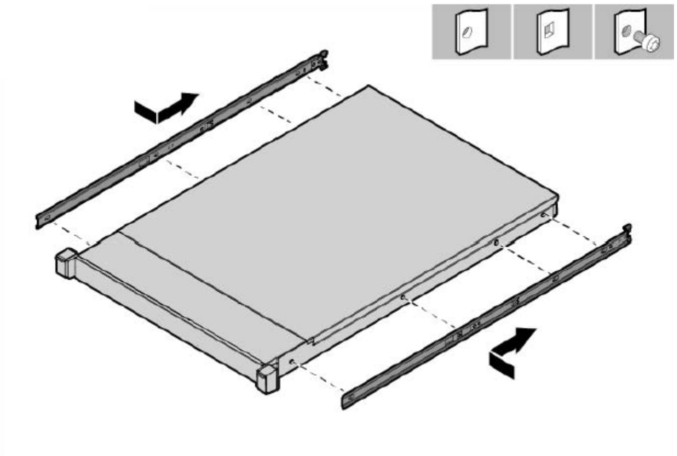
Figure 10-6: Rack Identification Legend



Round-hole racks	Square-hole racks	Threaded-hole racks
No tools required	No tools required	-

10.3.4 Installing the Rail Kit into a Rack

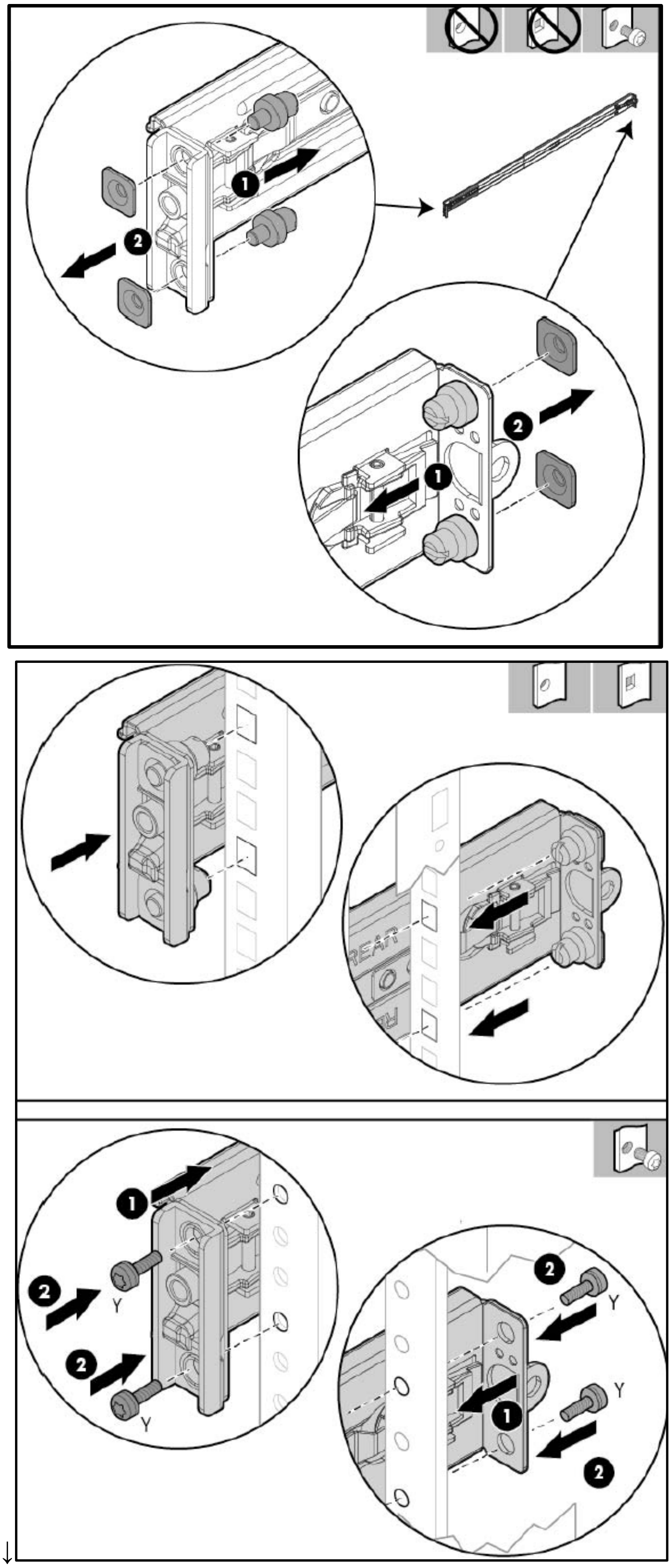
Figure 10-7: Rail Kit



Warning: To avoid risk of personal injury or damage to the equipment, do not stack anything on top of rail-mounted equipment or use it as a work surface when extended from the rack.

Caution: Always plan the rack installation so that the heaviest item is on the bottom of the rack. Install the heaviest item first, and continue to populate the rack from the bottom to the top.

Figure 10-8: Installing Rail Kit

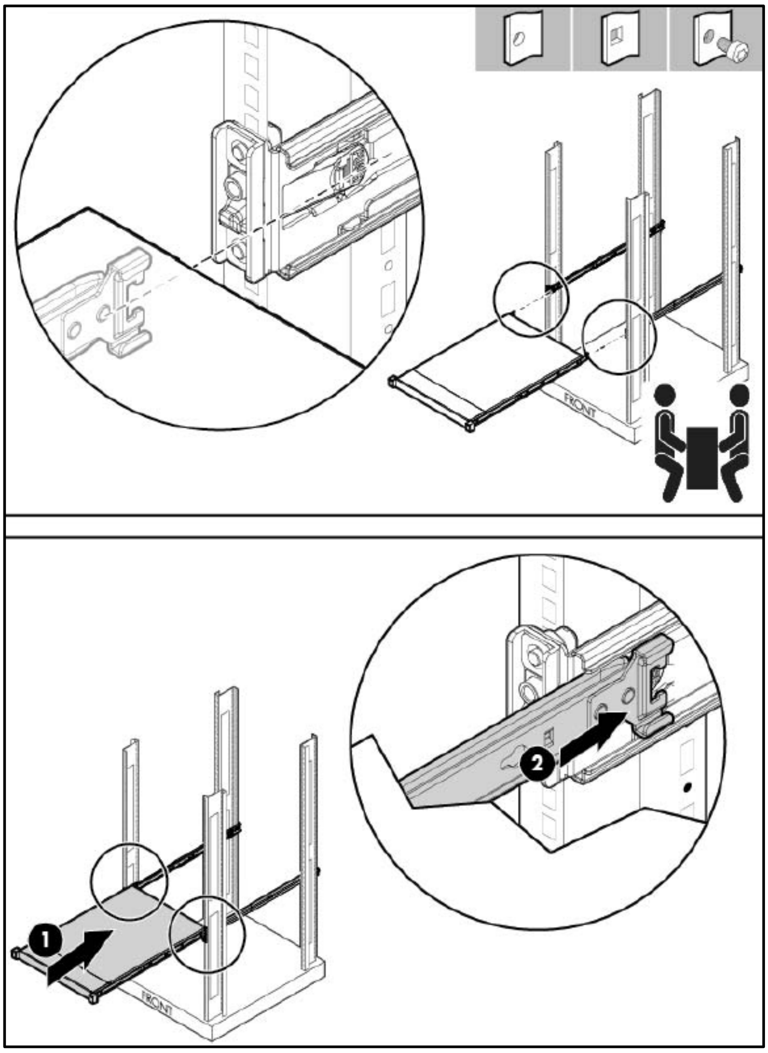


Warning: To reduce the risk of personal injury or equipment damage, be sure that the rack is adequately stabilized before sliding the inner slides into the slide mounting bracket assemblies.

Warning: To reduce the risk of personal injury or damage to the equipment, at least two people are required to lift the server during installation or removal.

Caution: Be sure to keep the product parallel to the floor when sliding the inner slides into the slide mounting bracket. Tilting the product up or down could result in damage to the slides.

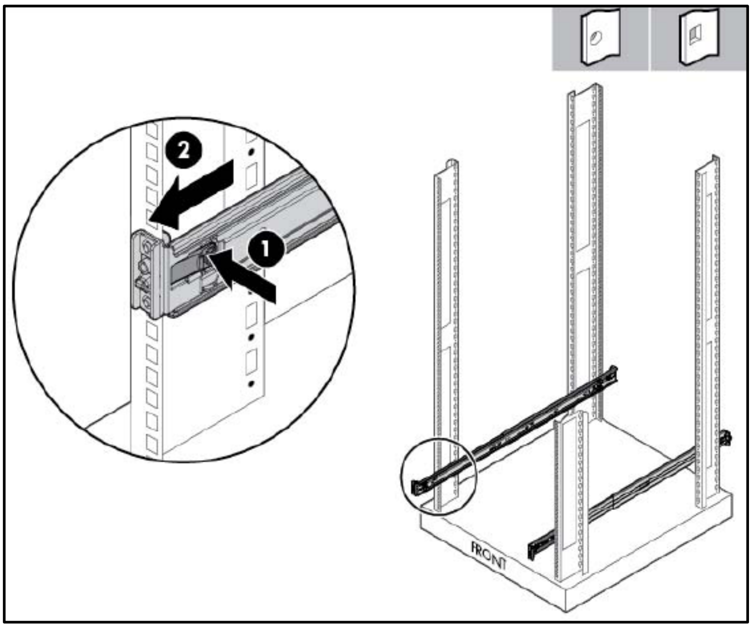
Figure 10-9: Installing Rail Kit Cont'd



10.3.5 Removing the Rail

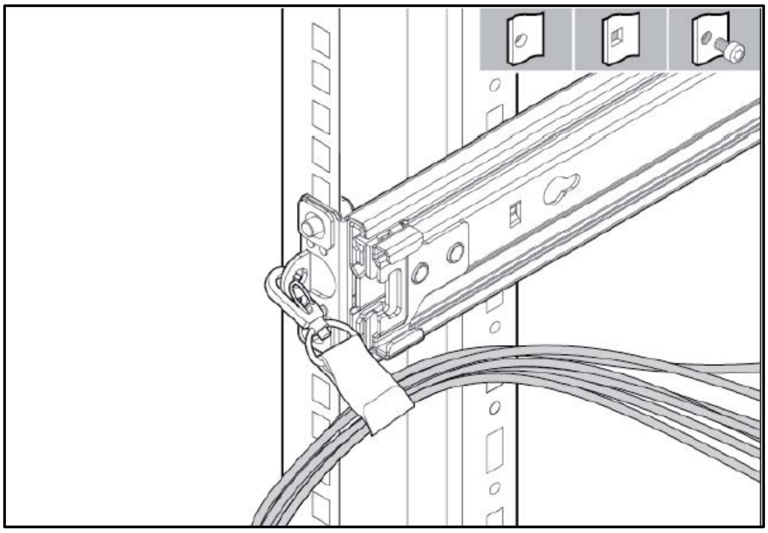
When removing the rail from the rack, always remove the front of the rail first.

Figure 10-10: Removing the Rail



10.3.6 Securing the Cables

Figure 10-11: Securing the Cables



10.3.7 Connecting the Power Cords

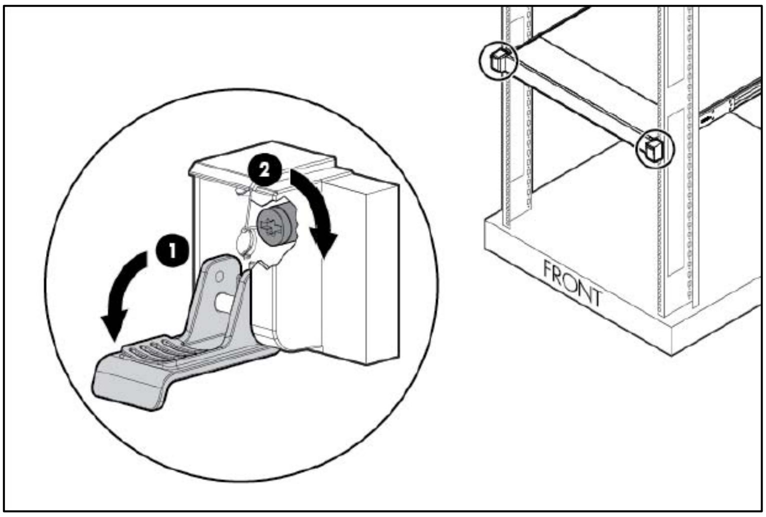
After completing all installation and cable management procedures, you can connect the power cords to the facility power source. See Section 10.4.2 on page 99 for detailed information. The installation is complete.

10.3.8 Preparing the Product for Integrated Shipping in a Rack

Note: You must provide screws to secure the slide mounting bracket assemblies in a threaded-hole rack.

Note: Use the integrated shipping hardware included with this kit to prepare a square-hole rack for integrated shipping.

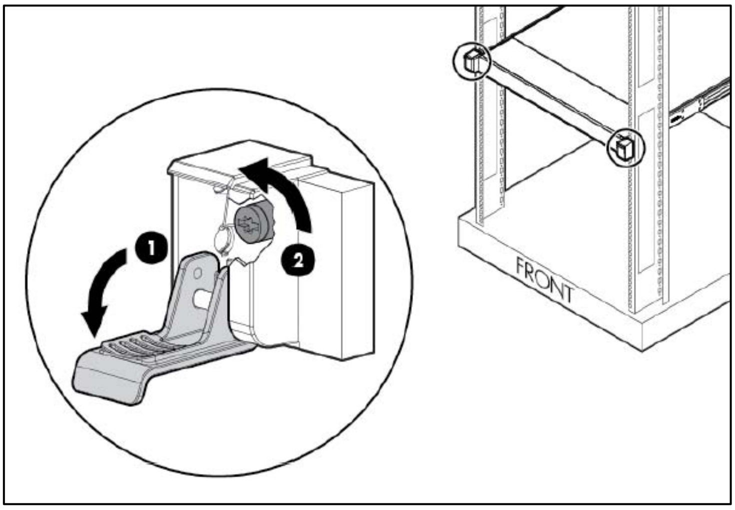
Figure 10-12: Preparing Product for Integrated Shipping in Rack



10.3.9 Loosening the Shipping Screws

To slide the server out of the rack, open the latches and loosen the shipping screws.

Figure 10-13: Loosening Shipping Screws



10.4 Cabling

This chapter shows how to cable the device. Intra-building connections of the device require the use of shielded cables grounded at both ends.

Caution: The intra-building ports of the equipment are suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building ports of the equipment must not be metallically connected to interfaces that connect to the Outside Plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports, as described in GR-1089–CORE, Issue 4) and requires isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

10.4.1 Grounding

The device is intended for use in both common bonding networks and isolated bonding networks. Grounding must comply with local, national, and other applicable government codes and regulations. Dedicated safety grounds are implemented on the product. The product uses a standard three wire cord that includes a safety ground for each power supply.

Warning: To ensure the safety ground, at least one power supply with an appropriately terminated ground lead must be installed at all times.

Tip: To ensure the safety ground, at least one power supply with an appropriately terminated ground lead must be installed at all times.

10.4.2 Connecting to Power

This section shows how to connect the device to the power supply. The device can be connected to an AC power source.

You can connect both Power Supply modules (1 and 2), for 1+1 power load-sharing and redundancy. Each module provides a power socket on the device's rear panel. If both power modules are used, make sure that you connect each one to a different power supply socket.

Note: When connecting both Power Supply modules, the two AC power sources must have the same ground potential.

Warning: The device must be connected (by service personnel) to a socket-outlet with a protective earthing connection.

10.4.2.1 Connecting to AC Power Source

The AC power supply specifications are listed in the table below.

Table 10-7: AC Power Supply Specifications

Specification	Value
Input requirements	**-**
Rated input voltage	100 V AC–240 V AC
Rated input frequency	50 Hz or 60 Hz
Rated input current	3.5 - 8.5A
Rated input power	▪ 843 W at 100 V AC input ▪ 811 W at 200 V AC input
Btus per hour	▪ 2878 at 100 V AC input ▪ 2769 at 200 V AC input
Power supply output	**-**
Rated steady-state power	▪ 750 W at 100 V to 120 V AC input ▪ 750W at 200 V to 240 V AC input
Maximum peak power	▪ 750W at 100 V to 120 V AC input ▪ 750W at 200 V to 240 V AC input

Warning: Use only the AC power cord supplied with the device.

Caution: To reduce the risk of electric shock or damage to the equipment:

- Do not disable the power cord grounding plug. The grounding plug is an important safety feature.
- Plug the power cord into a grounded (earthed) electrical outlet that is easily accessible at all times.
- Unplug the power cord from the power supply to disconnect power to the equipment.
- Do not route the power cord where it can be walked on or pinched by items placed against it. Pay particular attention to the plug, electrical outlet, and the point where the cord extends from the server.

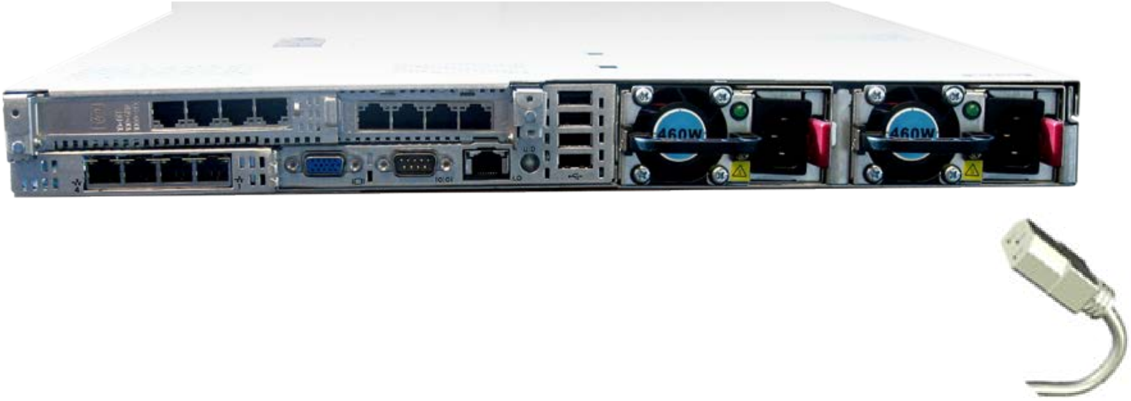
Note:

- This equipment is intended for installation where the NEC (National Electrical Code) applies.
- The safety ground of the AC power cord must terminate the chassis to the interior equipment grounding system.

➢ **To connect the device to the AC power supply:**

1. Connect the AC power cord (supplied) to one of the power sockets located on the rear panel.

Figure 10-14: Connecting AC Power Cords to AC Electrical Outlets



2. Connect the other end of the power cord to a standard AC electrical outlet (100-240V~50-60 Hz).
3. For load sharing and power redundancy, repeat steps 1 through 2, but using the power socket of the second Power Supply module and connecting this to a different supply circuit.
4. Turn on the power at the power source (if required).
5. Check that the **POWER** LED on each Power Supply module (front panel) is lit green. This indicates that the device is receiving power.

10.4.3 Connecting Display and Keyboard

To perform initial configuration, display and keyboard are required.

- Connect the display to the 15-pin HD D-Sub (HD-15) VGA port on the CloudBond 365.
- Connect the keyboard to the USB port.

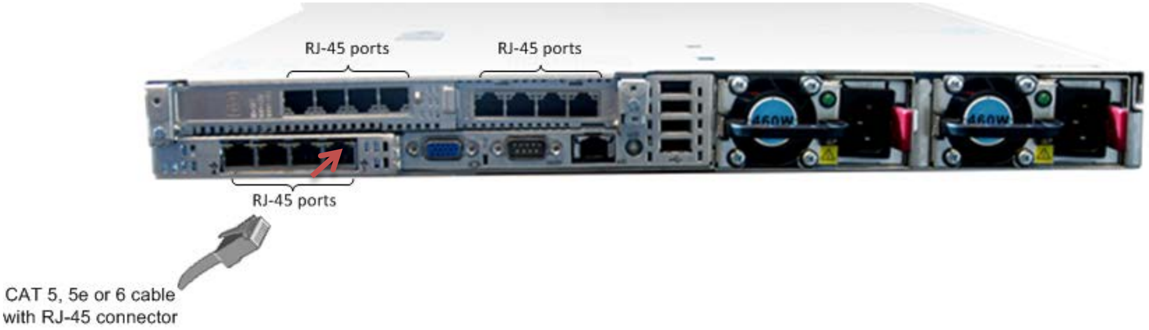
10.4.4 Connecting the Device to the IP Network

This section shows how to connect the device to the IP network.

➢ **To connect the device to the IP network:**

- Use an Ethernet cable to connect an RJ-45 network port on the server's rear panel to the LAN.

Figure 10-15: Connecting the Device to the IP Network



Notes:

- The first port used for OAM&P is located on the lowermost right of the CloudBond 365 chassis.
- The HP iLO port is not used for management of the CloudBond 365 application; it's used only for hardware management.
  For more information, see also http://www8.hp.com/us/en/products/servers/ilo/.

10.5 Initial Configuration

See the *AudioCodes CloudBond 365 - Pro-Enterprise Box Edition - Quick Start* for software configuration.

10.6 Setting up iLO

The CloudBond 365 Pro and Enterprise Box Edition server are equipped with the HP Integrated Lights-Out (iLO) interface and are shipped with the 'iLO Advanced' license key.

The iLO subsystem is a standard component of HP ProLiant servers that simplifies initial server setup, server health monitoring, power and thermal optimization, and remote server administration. The iLO subsystem includes an intelligent microprocessor, secure memory, and a dedicated network interface. This design makes iLO independent of the host server and its operating system.

iLO monitors all key internal subsystems. When enabled, SNMP alerts are sent directly by iLO, regardless of the host operating system or whether a host operating system is installed. Embedded remote support software is available on HP ProLiant servers with iLO 4, regardless of the operating system software and without installing OS agents on the server.

For more information on how to set up and use the iLO advanced capabilities, see the *HP iLO User Guide* available at http://h10032.www1.hp.com/ctg/Manual/c03334051.

➢ **To use the HP iLO interface:**

1. Connect to the iLO interface; refer to *Section Connecting iLO to the network in the HP iLO User Guide*.
2. Log in to the iLO web interface; refer to *Section Setting up iLO by using the iLO web interface in the HP iLO User Guide*.
3. Activate the iLO advanced license; refer to *Section Activating iLO licensed features in the HP iLO User Guide*. Use the iLO advanced license key shipped with the CloudBond 365 Pro and Enterprise Box Edition servers.

Note: The CloudBond 365 servers may be shipped with the iLO advanced license already activated and therefor there is no need to manually activate it.

10.7 Hardware Maintenance

In case hardware maintenance or repair is required for this device, contact AudioCodes RMA at http://www.audiocodes.com/support.

10.7.1 Prerequisites

Before performing any maintenance procedures, read this section.

10.7.1.1 Grounding the Device

Before performing any maintenance procedures, ensure that your device is properly grounded.

10.7.1.2 Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) due to improper handling of the device's modules and components can cause irreversible damage to the equipment. Adhere to the following guidelines for preventing ESD:

- When handling modules, always wear a grounded ESD wrist strap or ankle strap at a grounded work area to prevent ESD. Connect the equipment end of the strap to a grounded workstation or computer chassis.
- To prevent static electrical damage to the module, do not touch the electrical components of the module. Instead, hold the module only on the edges where no electrical components are located.
- Ensure that the modules are securely installed in the chassis.

➢ **To attach an ESD wrist strap to the chassis:**

1. Attach the ESD wrist strap to your body (typically, the wrist) so that it is in direct contact with your skin.
2. Attach the other end of the wrist strap (e.g., an alligator clip) to a grounded workstation or computer chassis.

10.7.2 Replacing Power Supply Modules

This section shows how to replace the power supply modules.

10.7.2.1 Replacing AC Power Supply

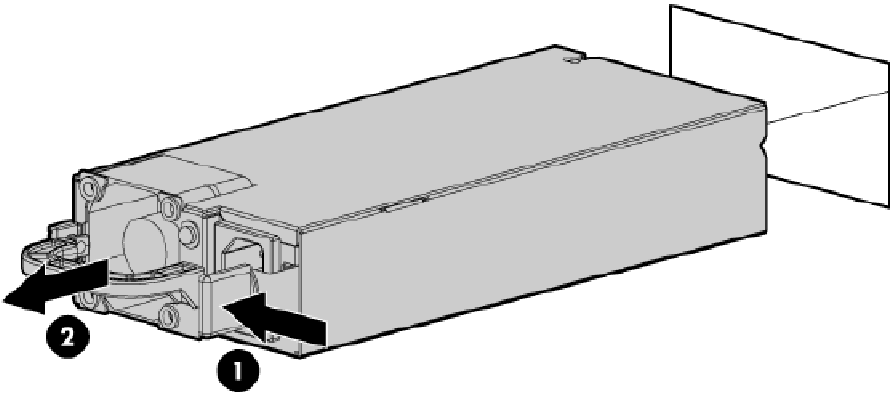
Caution: To prevent improper cooling and thermal damage, do not operate the server unless all bays are populated with either a component or a blank.

➢ **To remove the component:**

1. Power down the server.
2. Remove all power:
   a. Disconnect each power cord from the power source.
   b. Disconnect each power cord from the server.
3. Access the product rear panel.
4. Remove the power supply.

Warning: To reduce the risk of personal injury from hot surfaces, allow the power supply or power supply blank to cool before touching it.

Figure 10-16: Removing Component



To replace the component, reverse the removal procedure.

10.7.3 Troubleshooting Device Failures

Contact AudioCodes RMA at www.audiocodes.com/support to troubleshoot device failures (such as fan alarms).

11 Software Installation

This chapter describes how to install the CloudBond 365 Software. It is intended primarily for AudioCodes staff and dealers; however, may also be used as a guide for re-loading software onto existing AudioCodes hardware, such as for system recovery.

The Software Install Wizard described in the guide is capable of installing software for:

- CloudBond 365 Standard Box Edition
- CloudBond 365 Standard+ Box Edition
- CloudBond 365 Pro Box Edition
- CloudBond 365 Enterprise Box Edition
- CloudBond 365 Virtualized Edition
- User Management Pack 365

The Software Install Wizard can optionally install the following:

- Skype for Business Consolidated Edge Server on Branch / Paired Pool Deployment
- AudioCodes SBC software
- A Reverse Proxy Server

The Software Install Wizard can also deploy CloudBond 365 in two forms:

- Standalone Deployment
- Branch / Paired Pool Deployment

11.1 Software Installer

The software installer consists of several components:

- A bootable USB drive containing a WinPE environment
- An ISO image of the CloudBond 365 Software
- A Software Configuration Wizard to gather data for installation
- An automated software installer to install the CloudBond 365 software to match a requested configuration

11.2 Configurations

The Software installer and Configuration Wizard allow for installation of multiple configurations of the CloudBond 365 software.

The Software installer and Configuration Wizard allow the CloudBond 365 software to be installed onto a Bare Metal hardware platform, or onto one with Windows 2012 R2 operating system already installed.

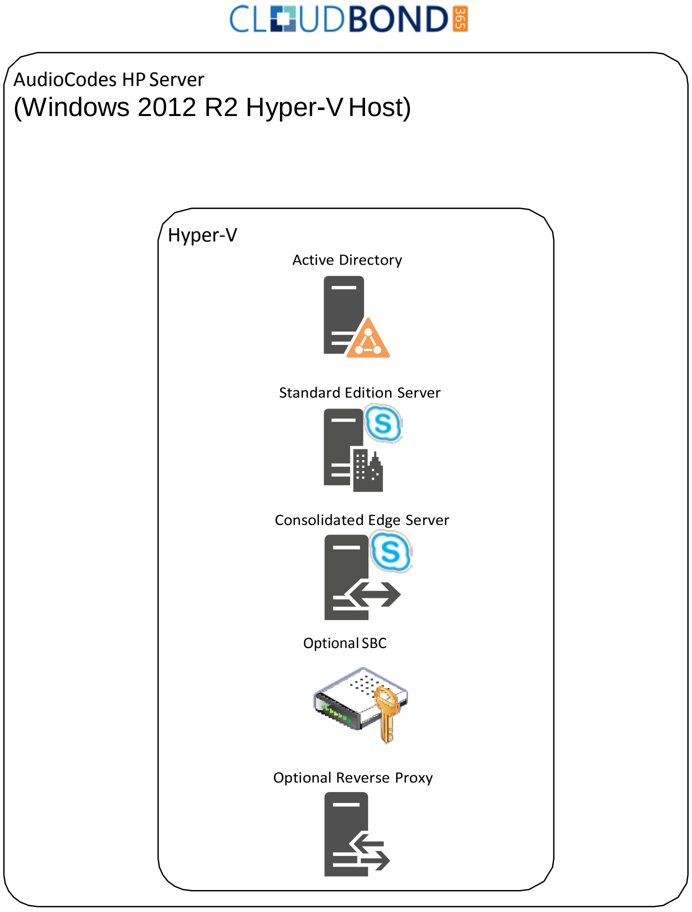
The software installer supports only the approved AudioCodes hardware.

11.2.1 Hyper-V Host with Virtual Machines

The **Hyper-V Host with Virtual Machines** deployment model installs Hyper-V on the selected host machine, and the three CloudBond 365 Servers (Controller, Fe, and Edge) as three separate virtual machines within Hyper-V.

This option is suitable for CloudBond 365 Pro Box and Enterprise Box Editions. (e.g., AudioCodes HP Servers).

Figure 11-1: Hyper-V Host with Virtual Machines

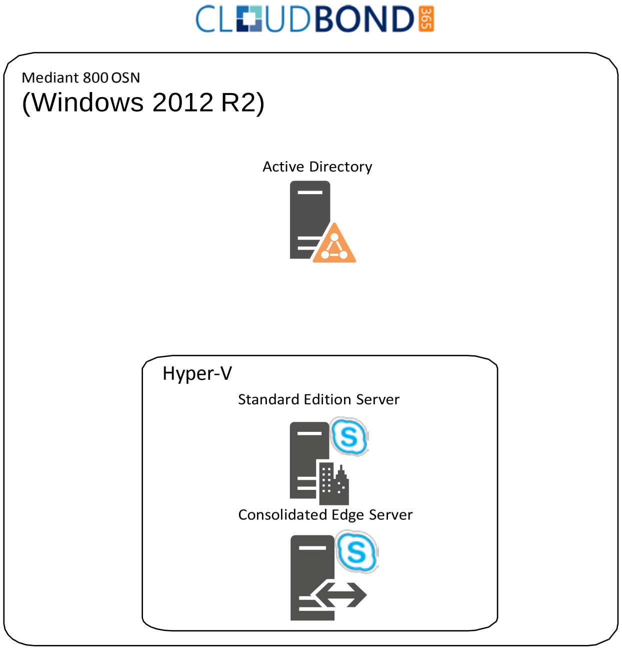


11.2.2 Co-located Hyper-V / Domain Controller with Virtual Machines

The co-located Hyper-V / Domain Controller with Virtual Machines install the CloudBond 365 Controller (DC) and Hyper-V within the host machine, with the remaining CloudBond 365 Servers (FE and Edge) as Hyper-V virtual machines.

This option is suitable for CloudBond 365 Standard / Standard+ Box Editions (e.g. AudioCodes Mediant 800B OSN server).

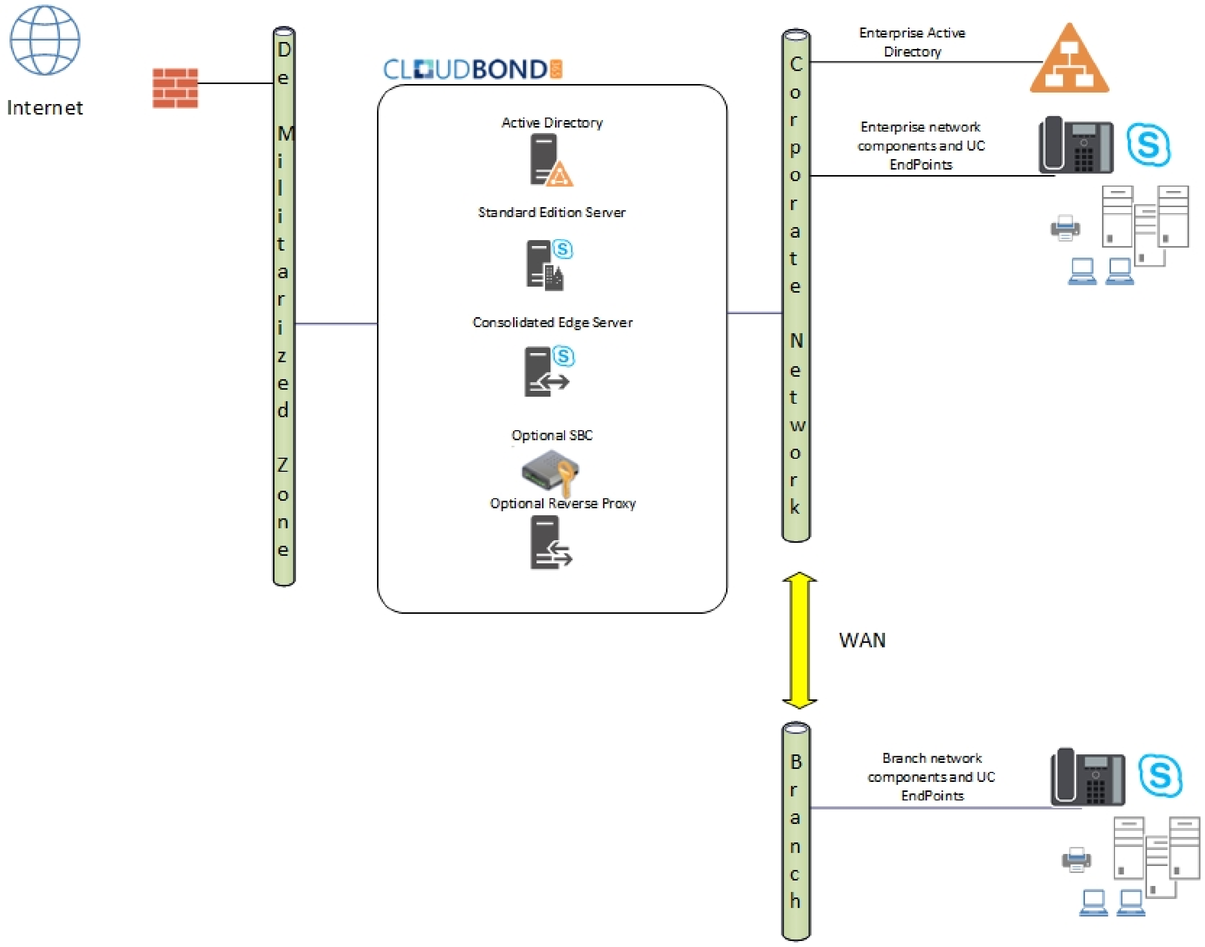
Figure 11-2: Co-Located DC and Hyper-V



11.2.3 Standalone Deployment

A standalone deployment is typically used for the first CloudBond 365 system installed for a customer.

Figure 11-3: Standalone Deployment



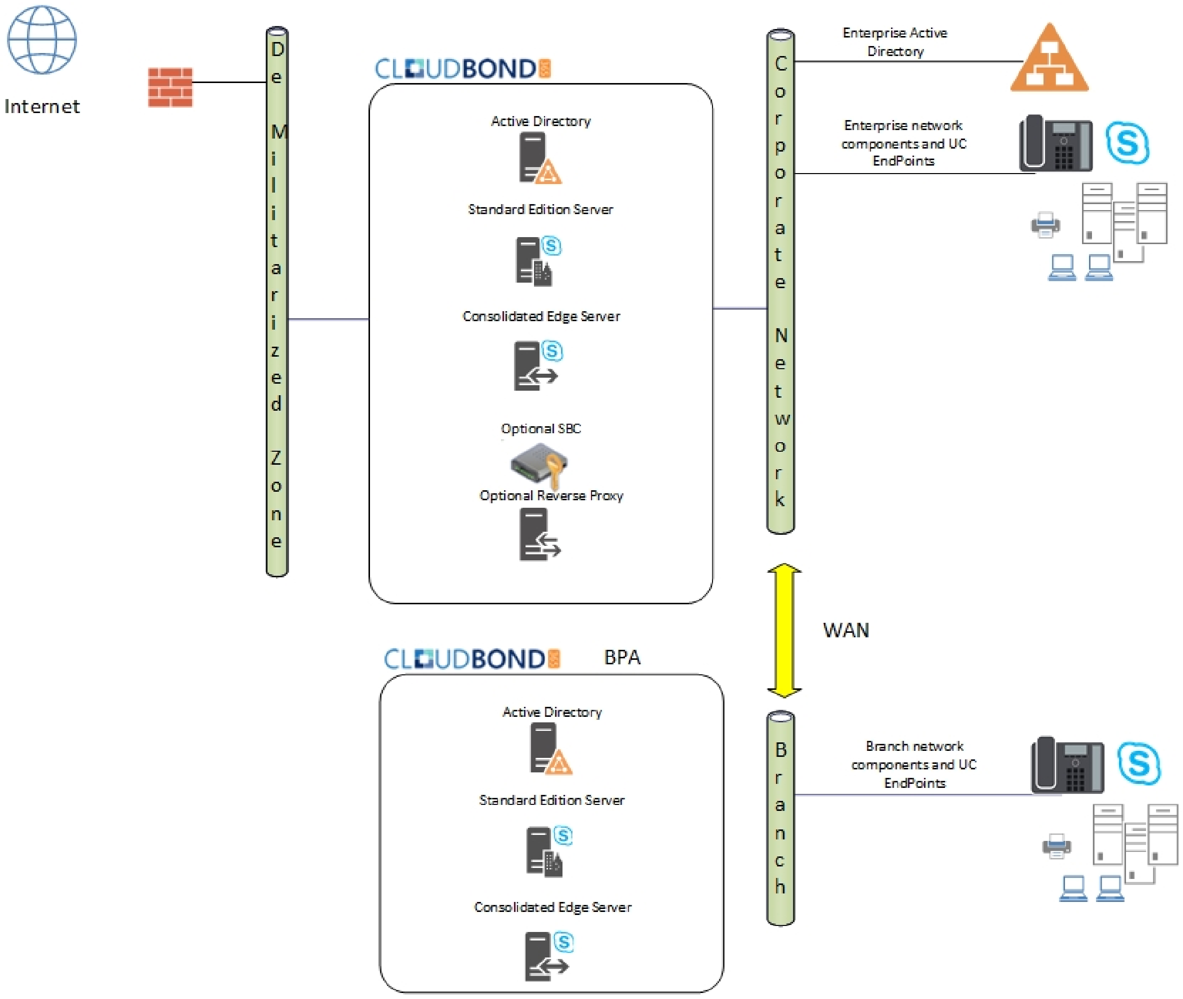
11.2.4 Branch / Paired Pool Deployment

A Branch / Paired Pool Appliance Deployment (BPA) is used where the customer already has an existing CloudBond 365 system deployed. A BPA deployment is used for the second and subsequent CloudBond 365 Deployments within the same customer environment.

There are many possible configurations and reasons for installing a BPA. Typically, it is to provide either:

- Continuous service to a Branch site with slow or unreliably WAN links. This is similar to a Skype for Business Survivable Branch Appliance, but with more features.
- Failover capability within the corporate site using Skype for Business Paired pools.

Figure 11-4: BPA Deployment



11.2.5 User Management Pack 365

The User Management Pack 365 deployment type enables the installation of only the management layer within an existing Lync Server 2013 or Skype for Business Server environment. This option can also be used to upgrade an older version of the CloudBond 365 Management Suite.

11.3 Software Media

CloudBond 365 software is normally supplied on a specially prepared USB key. The key is bootable and must be inserted into the device as part of the installation procedure. It allows CloudBond 365 software to be installed onto the following:

- Bare Metal server hardware
- Windows 2012 R2 operating system already installed on the hardware

Warning: If booting from the USB key, all data will be wiped from the hardware device during installation. The software presents a warning and prompts for permission to continue before wiping data.

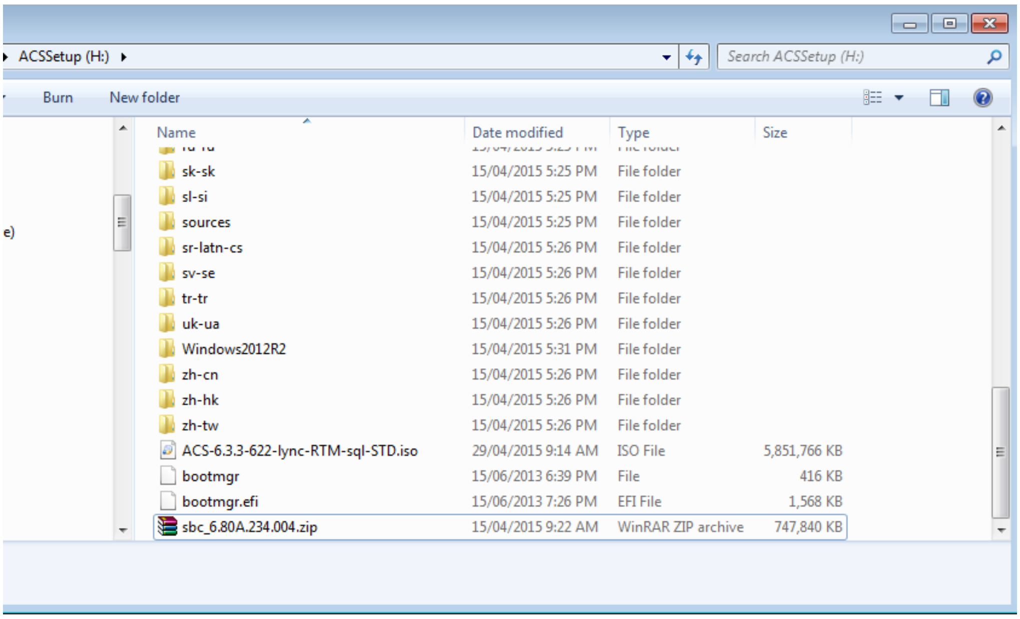
11.3.1 USB Drive

The USB Drive directory structure should be as shown in the image below. The drive contains:

- WinPE environment files
- Windows 2012 R2 directory
- ACS-X.X.x ISO image
- sbc_X.X.X.zip file containing the AudioCodes Software SBC

The USB drive is formatted as NTFS and is bootable. Additionally, the label of the USB Drive **must be** 'ACSSetup'.

Figure 11-5: USB Drive Contents



Name	Date modified	Type	Size
sk-sk	15/04/2015 5:25 PM	File folder	
sl-si	15/04/2015 5:25 PM	File folder	
sources	15/04/2015 5:25 PM	File folder	
sr-latn-cs	15/04/2015 5:26 PM	File folder	
sv-se	15/04/2015 5:26 PM	File folder	
tr-tr	15/04/2015 5:26 PM	File folder	
uk-ua	15/04/2015 5:26 PM	File folder	
Windows2012R2	15/04/2015 5:31 PM	File folder	
zh-cn	15/04/2015 5:26 PM	File folder	
zh-hk	15/04/2015 5:26 PM	File folder	
zh-tw	15/04/2015 5:26 PM	File folder	
ACS-6.3.3-622-lync-RTM-sql-STD.iso	29/04/2015 9:14 AM	ISO File	5,851,766 KB
bootmgr	15/06/2013 6:39 PM	File	416 KB
bootmgr.efi	15/06/2013 7:26 PM	EFI File	1,568 KB
sbc_6.80A.234.004.zip	15/04/2015 9:22 AM	WinRAR ZIP archive	747,840 KB

Warning: Under no circumstances must any .ISO image, file or folder containing the letters 'sbc' be present besides the zip file, as shown in the figure above (the exact version might differ from the figure above).

11.4 Preparation

The CloudBond 365 Software may only be loaded onto hardware certified by AudioCodes. This will primarily be:

- AudioCodes HP Server for CloudBond 365 Pro and Enterprise Box Editions
- AudioCodes Mediant 800B with OSN for the CloudBond 365 Standard / Standard+ Box Edition

The hardware device must be prepared for the new software prior to installation. The preparation steps include:

- Ensuring no Ethernet cables are attached

Warning: If booting from the USB key, all data will be wiped from the device during installation. The software presents a warning and prompts for permission to continue before wiping data.

11.4.1 Partitioning

If performing a 'bare metal' installation, the following partitions will be automatically configured on the machine as part of the installation:

Table 11-1: Configured Partitions

Drive	Label	File System	Size (GB)
C	Windows	NTFS	80
D	Data	NTFS	At least 215 + 5 for Session Border Controller + 55 for Reverse Proxy
E	Recovery	NTFS	15

11.4.2 General Server Hardware

Do not connect any network cables during installation!!

11.5 Bare Metal Install

This section describes the process for installing the CloudBond 365 software without a pre-installed Operating System on the server hardware (also known as *Bare Metal Install*).

The process boots into a Windows 2012 R2 Pre-installation Environment (WinPE) on the connected server hardware.

> **Warning:** All data will be wiped from the hardware device during installation. The software presents a warning and prompts for permission to continue before wiping data.

The Installation program then partitions and formats the HDD storage of the hardware devices, installs Windows 2012 R2, and copies the contents of the USB key to the Recovery partition.

Once Windows 2012 is installed on the host, you can remove the USB Key, and continue with the installation as described in the next chapter.

11.5.1 Bare Metal Install – AudioCodes HP Server

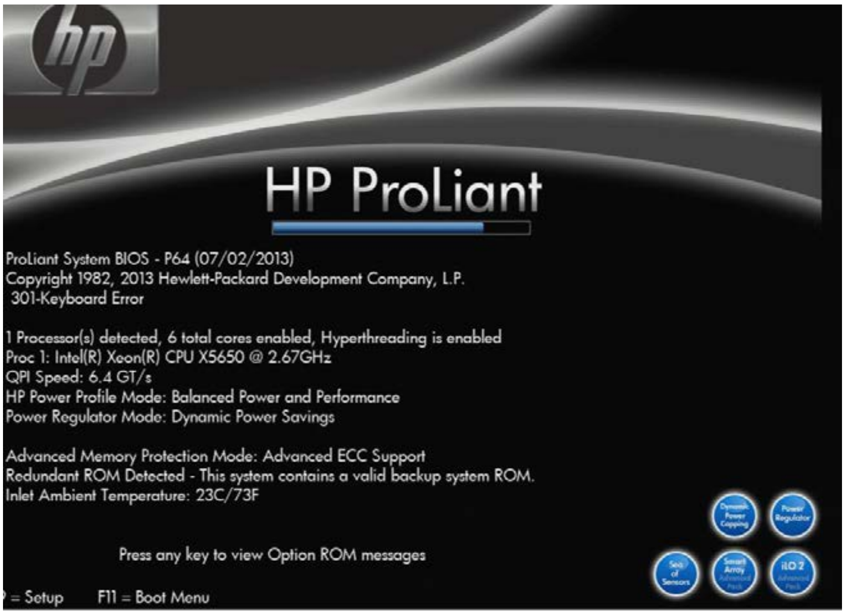
This section describes how to install the software on the AudioCodes HP Server platform.

The CloudBond 365 Pro and Enterprise Box Editions are shipped with the software pre-installed.

If installing on an AudioCodes Mediant 800, see Section 11.5.2 on page 115.

1. Insert the USB Drive in the front USB port.
2. Power on the server.
3. When the HP Splash screen appears, click F11 for Boot Menu.

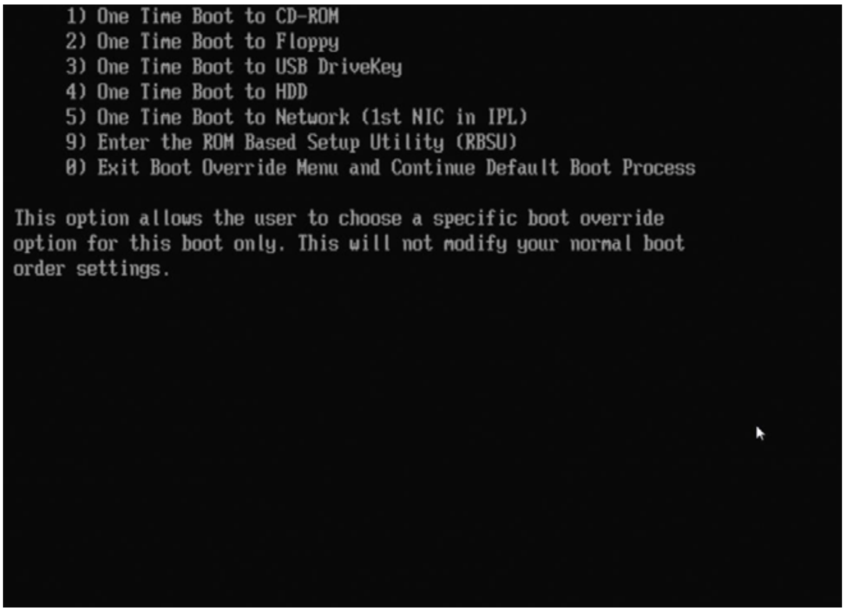
Figure 11-6: HP Splash Screen



```
ProLiant System BIOS - P64 (07/02/2013)
Copyright 1982, 2013 Hewlett-Packard Development Company, L.P.
 301-Keyboard Error

1 Processor(s) detected, 6 total cores enabled, Hyperthreading is enabled
Proc 1: Intel(R) Xeon(R) CPU X5650 @ 2.67GHz
QPI Speed: 6.4 GT/s
HP Power Profile Mode: Balanced Power and Performance
Power Regulator Mode: Dynamic Power Savings

Advanced Memory Protection Mode: Advanced ECC Support
Redundant ROM Detected - This system contains a valid backup system ROM.
Inlet Ambient Temperature: 23C/73F

              Press any key to view Option ROM messages

= Setup     F11 = Boot Menu
```

4. Select a manual One Time Boot to USB.

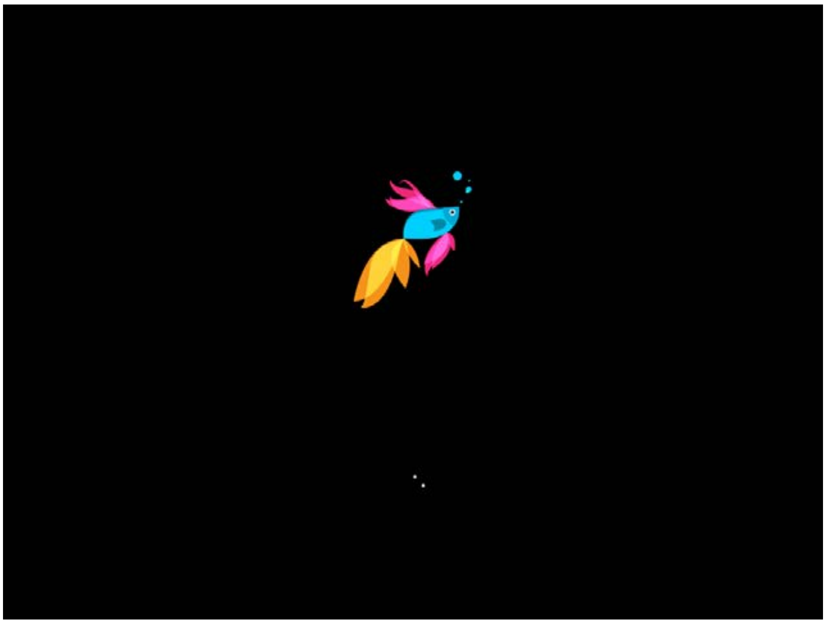
Figure 11-7: One Time Boot



```
      1) One Time Boot to CD-ROM
      2) One Time Boot to Floppy
      3) One Time Boot to USB DriveKey
      4) One Time Boot to HDD
      5) One Time Boot to Network (1st NIC in IPL)
      9) Enter the ROM Based Setup Utility (RBSU)
      0) Exit Boot Override Menu and Continue Default Boot Process

 This option allows the user to choose a specific boot override
 option for this boot only. This will not modify your normal boot
 order settings.
```

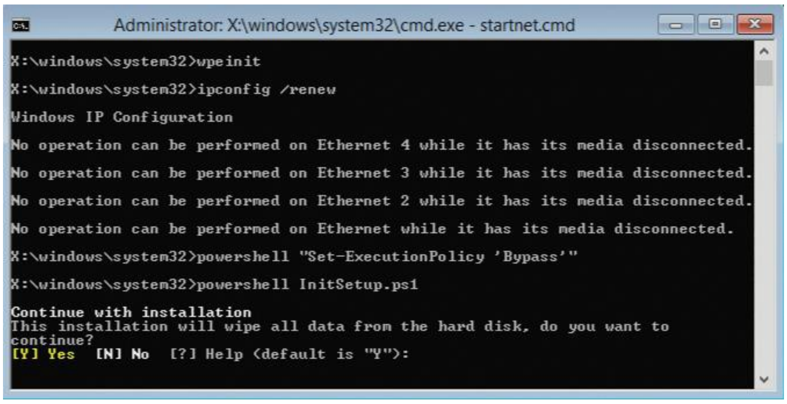
5. After selecting the USB key to boot from, the WinPE Splash screen appears.

Figure 11-8: WinPE Splash Screen



6. After WinPE starts, you will see a command line window, asking if you wish to Continue with installation. Click <Enter>, or <Y> followed by <Enter>, to continue the installation process.

Figure 11-9: Continue with installation



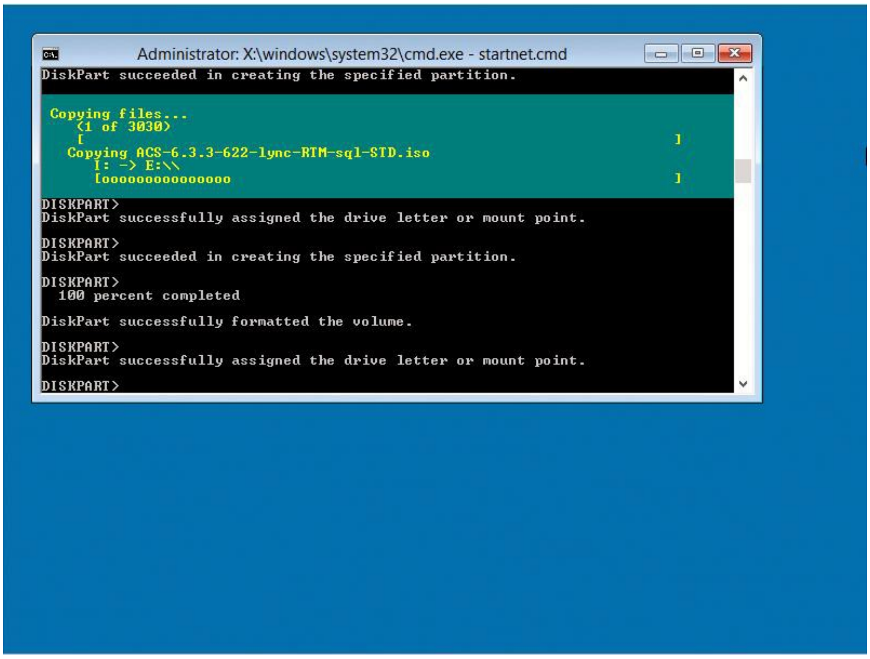
Administrator: X:\windows\system32\cmd.exe - startnet.cmd

```
X:\windows\system32>wpeinit

X:\windows\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet 4 while it has its media disconnected.

No operation can be performed on Ethernet 3 while it has its media disconnected.

No operation can be performed on Ethernet 2 while it has its media disconnected.

No operation can be performed on Ethernet while it has its media disconnected.

X:\windows\system32>powershell "Set-ExecutionPolicy 'Bypass'"

X:\windows\system32>powershell InitSetup.ps1

Continue with installation
This installation will wipe all data from the hard disk, do you want to
continue?
[Y] Yes  [N] No  [?] Help (default is "Y"):
```

Warning: All data will be wiped from the device during installation.

The installer software will now partition and format the HDD storage of the hardware platform, and copy the contents of the USB key to the recovery partition. The software will install Windows 2012 R2 as the operating system and may reboot several times.

Figure 11-10: Copying files from USB to Recovery



Administrator: X:\windows\system32\cmd.exe - startnet.cmd

```
DiskPart succeeded in creating the specified partition.

 Copying files...
    (1 of 3030)
    [                                                                    ]
   Copying ACS-6.3.3-622-lync-RTM-sql-STD.iso
      I: -> E:\\
      [oooooooooooooooo                                                  ]

DISKPART>
DiskPart successfully assigned the drive letter or mount point.

DISKPART>
DiskPart succeeded in creating the specified partition.

DISKPART>
  100 percent completed

DiskPart successfully formatted the volume.

DISKPART>
DiskPart successfully assigned the drive letter or mount point.

DISKPART>
```

Once Windows 2012 R2 has been installed, you may remove the USB key.

11.5.2 Bare Metal Install – Mediant 800 OSN

This section describes how to install or re-install the software on the AudioCodes Mediant 800 OSN platform. The CloudBond 365 Standard Box / Standard+ Box Edition is normally supplied with the software already installed.

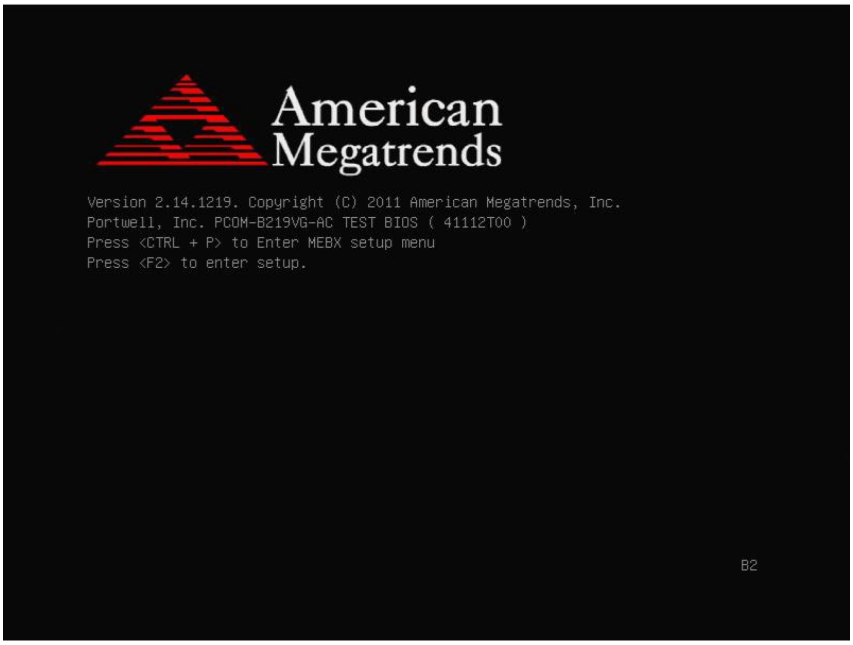
Warning: You may need to upgrade the BIOS on older Mediant 800 OSN models before proceeding. See the latest Product Notice – AudioCodes CloudBond 365 BIOS Update. The minimum required BIOS version for Standard Box Edition is now American Megatrends Inc. 60104T00. The minimum required BIOS version for Standard+ Box Edition is now American Megatrends Inc. 51214T00.

➢ **To perform a Bare Metal install:**

1. Insert the USB Drive in the rear USB port.
2. Power on the server.
3. When the AMI BIOS Splash screen appears, click F2 for Setup Menu.

Note: The BIOS version is displayed on the splash screen. In the example below, the version is (41112T00), and requires updating.

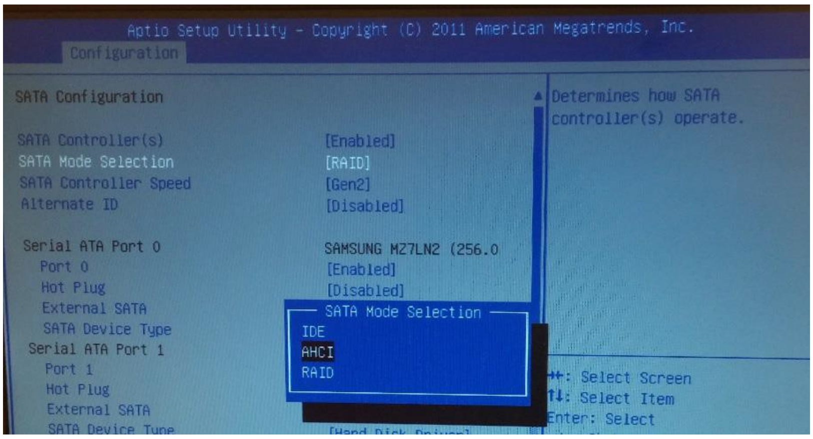
Figure 11-11: AMI BIOS Splash Screen



```
Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.
Portwell, Inc. PCOM-B219VG-AC TEST BIOS ( 41112T00 )
Press <CTRL + P> to Enter MEBX setup menu
Press <F2> to enter setup.
```

4. Navigate to the Configuration page, and then ensure that SATA mode is set to AHCI.

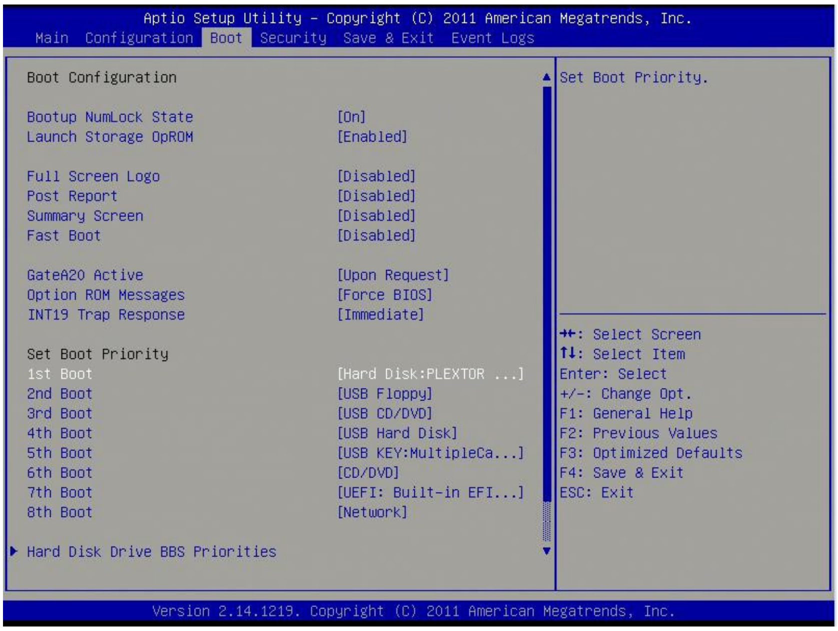
Figure 11-12: SATA Mode



```
        Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
    Configuration

SATA Configuration                                      Determines how SATA
                                                        controller(s) operate.
SATA Controller(s)              [Enabled]
SATA Mode Selection             [RAID]
SATA Controller Speed           [Gen2]
Alternate ID                    [Disabled]

Serial ATA Port 0               SAMSUNG MZ7LN2 (256.0
  Port 0                        [Enabled]
  Hot Plug                      [Disabled]
  External SATA               ─ SATA Mode Selection ─
  SATA Device Type             IDE
Serial ATA Port 1              AHCI
  Port 1                       RAID                     ↔: Select Screen
  Hot Plug                                              ↑↓: Select Item
  External SATA                                         Enter: Select
  SATA Device Type              [Hard Disk Driver]
```

5. Navigate to the Boot page, and then ensure the internal HDD (usually PLEXTOR) is set as the first boot device.

Figure 11-13: M800 First boot device

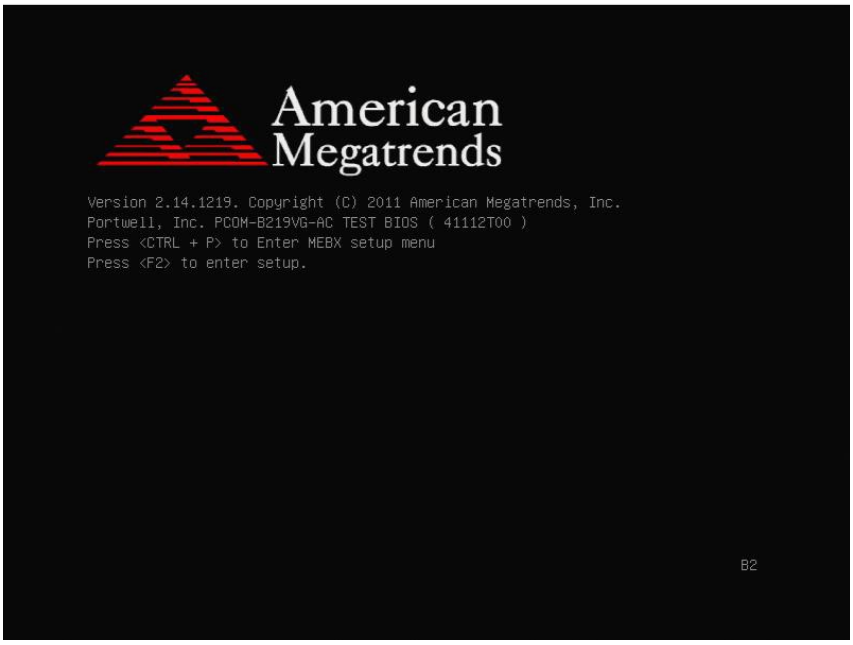


```
        Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
  Main  Configuration  Boot  Security  Save & Exit  Event Logs

 Boot Configuration                                   Set Boot Priority.

 Bootup NumLock State           [On]
 Launch Storage OpROM           [Enabled]

 Full Screen Logo               [Disabled]
 Post Report                    [Disabled]
 Summary Screen                 [Disabled]
 Fast Boot                      [Disabled]

 GateA20 Active                 [Upon Request]
 Option ROM Messages            [Force BIOS]
 INT19 Trap Response            [Immediate]
                                                      ↔: Select Screen
 Set Boot Priority                                    ↑↓: Select Item
 1st Boot                       [Hard Disk:PLEXTOR ...] Enter: Select
 2nd Boot                       [USB Floppy]          +/-: Change Opt.
 3rd Boot                       [USB CD/DVD]          F1: General Help
 4th Boot                       [USB Hard Disk]       F2: Previous Values
 5th Boot                       [USB KEY:MultipleCa...] F3: Optimized Defaults
 6th Boot                       [CD/DVD]              F4: Save & Exit
 7th Boot                       [UEFI: Built-in EFI...] ESC: Exit
 8th Boot                       [Network]

▶ Hard Disk Drive BBS Priorities

        Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.
```

6. Navigate to the **Save & Exit** page, and then select **Save Changes** and **Exit**; the Mediant 800 OSN reboots.

7. When the AMI BIOS Splash screen appears, click **F2** for the Setup Menu.

Figure 11-14: AMI BIOS Splash Screen

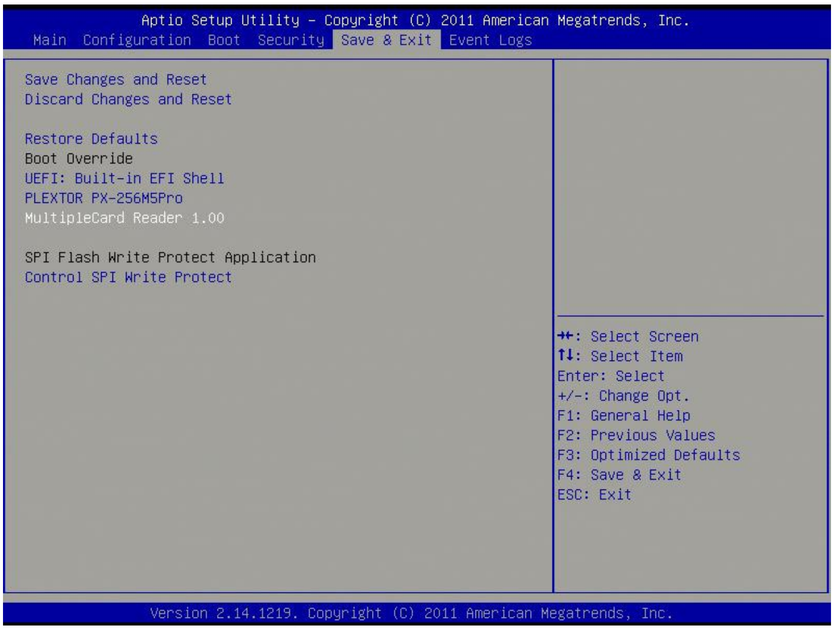


```
Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.
Portwell, Inc. PCOM-B219VG-AC TEST BIOS ( 41112T00 )
Press <CTRL + P> to Enter MEBX setup menu
Press <F2> to enter setup.

                                                             B2
```

8. Navigate to the Save & Exit page. This time move the cursor down to Boot Override, and select the USB key. In the example below, the USB device appears as **MultipleCard Reader**.

9. Click **Enter**; the Mediant 800 OSN restarts.

Figure 11-15: M800 Boot Override

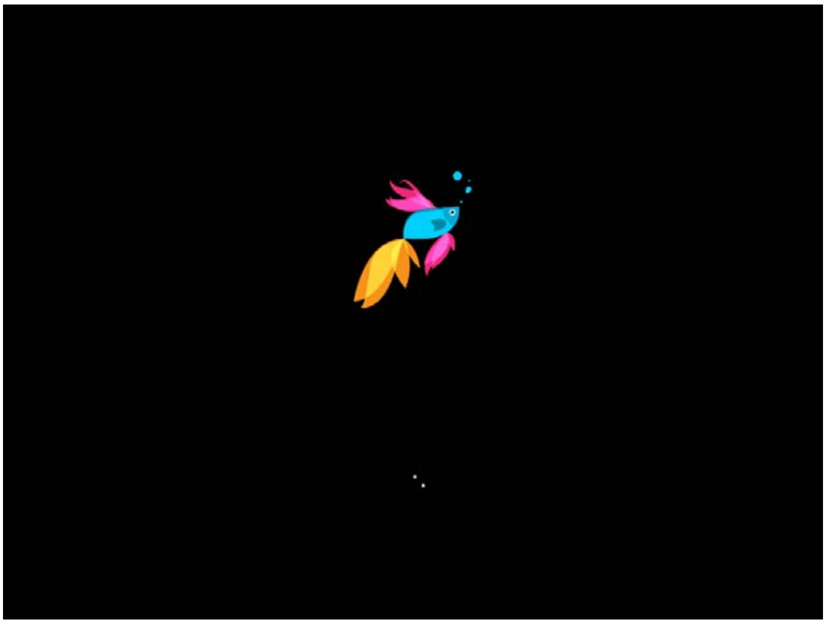


```
        Aptio Setup Utility – Copyright (C) 2011 American Megatrends, Inc.
  Main  Configuration  Boot  Security  Save & Exit  Event Logs

  Save Changes and Reset
  Discard Changes and Reset

  Restore Defaults
  Boot Override
  UEFI: Built-in EFI Shell
  PLEXTOR PX-256M5Pro
  MultipleCard Reader 1.00

  SPI Flash Write Protect Application
  Control SPI Write Protect
                                                ↔: Select Screen
                                                ↑↓: Select Item
                                                Enter: Select
                                                +/-: Change Opt.
                                                F1: General Help
                                                F2: Previous Values
                                                F3: Optimized Defaults
                                                F4: Save & Exit
                                                ESC: Exit

        Version 2.14.1219. Copyright (C) 2011 American Megatrends, Inc.
```

Warning: Failure to set the First Boot device and Boot Override correctly can result in the server performing an endless loop, constantly rebooting from USB (partitioning, formatting, and installing Windows each time.).

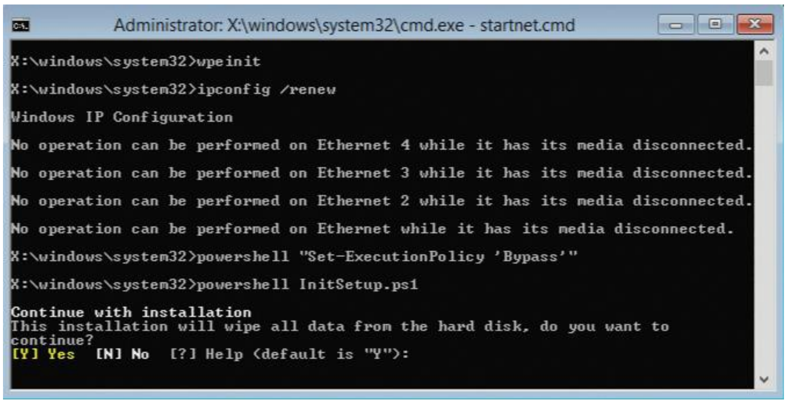
10. After restarting, the Mediant 800 OSN boots from the USB key (one time only) and the WinPE Splash screen appears:

Figure 11-16: WinPE Splash Screen



11. After WinPE starts, you will see a command line window, asking if you wish to Continue with installation. Click **Enter**, or **Y** followed by **Enter** to continue the installation process.

Figure 11-17: Continue with Installation



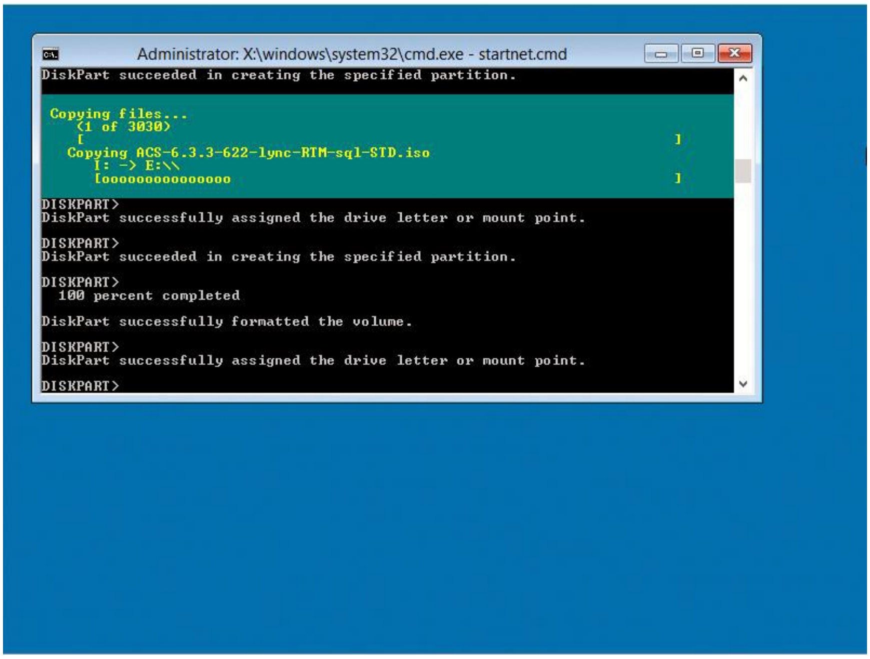
Administrator: X:\windows\system32\cmd.exe - startnet.cmd

```
X:\windows\system32>wpeinit

X:\windows\system32>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet 4 while it has its media disconnected.

No operation can be performed on Ethernet 3 while it has its media disconnected.

No operation can be performed on Ethernet 2 while it has its media disconnected.

No operation can be performed on Ethernet while it has its media disconnected.

X:\windows\system32>powershell "Set-ExecutionPolicy 'Bypass'"

X:\windows\system32>powershell InitSetup.ps1

Continue with installation
This installation will wipe all data from the hard disk, do you want to
continue?
[Y] Yes  [N] No  [?] Help (default is "Y"):
```

Warning: All data will be wiped from the device during installation.

12. The installer software will now partition and format the HDD storage of the hardware platform, and copy the contents of the USB key to the recovery partition. The software will install Windows 2012 R2 as the operating system and may reboot several times.

Figure 11-18: Copying Files from USB to Recovery



```
DiskPart succeeded in creating the specified partition.

 Copying files...
    (1 of 3030)
    [                                                                          ]
   Copying ACS-6.3.3-622-lync-RTM-sql-STD.iso
      I: -> E:\\
      [oooooooooooooooo                                                        ]
DISKPART>
DiskPart successfully assigned the drive letter or mount point.

DISKPART>
DiskPart succeeded in creating the specified partition.

DISKPART>
  100 percent completed

DiskPart successfully formatted the volume.

DISKPART>
DiskPart successfully assigned the drive letter or mount point.

DISKPART>
```

13. Once Windows 2012 R2 has been installed, you may remove the USB key.

11.6 Installing from Windows 2012 R2

If performing a Bare Metal installation by booting from the USB key, Windows 2012 R2 will be installed for you and the contents of the USB key copied to the Recovery partition.

Once the Windows 2012 R2 operating system has been installed, you can continue the software installation with the steps in the following sections.

Before continuing, make sure:

- The HDD storage has been partitioned and formatted correctly
- The contents of the USB Key have been copied to the Recovery partition
- The date, time, and time zone are set correctly within Windows

Note: After Windows 2012 R2 is installed, drive letters for the various partitions are randomly assigned and may vary from those in the following screenshots. The CloudBond software installer standardizes the drive letters during installation.

Warning: Failure to set the date, time, and time zone correctly prior to software installation will result in issues which may only become apparent sometime after installation.

Warning: If you choose to install a Branch / Paired Pool Appliance deployment type, you will need to prepare the existing CloudBond 365 environment before installing the additional BPA server. These steps are detailed in Section 0 on page 138. Do not start the Configuration Wizard before completing these steps.

To commence the remaining installation steps, mount the ISO image from the Recovery partition and start the Configuration Wizard, as described below.

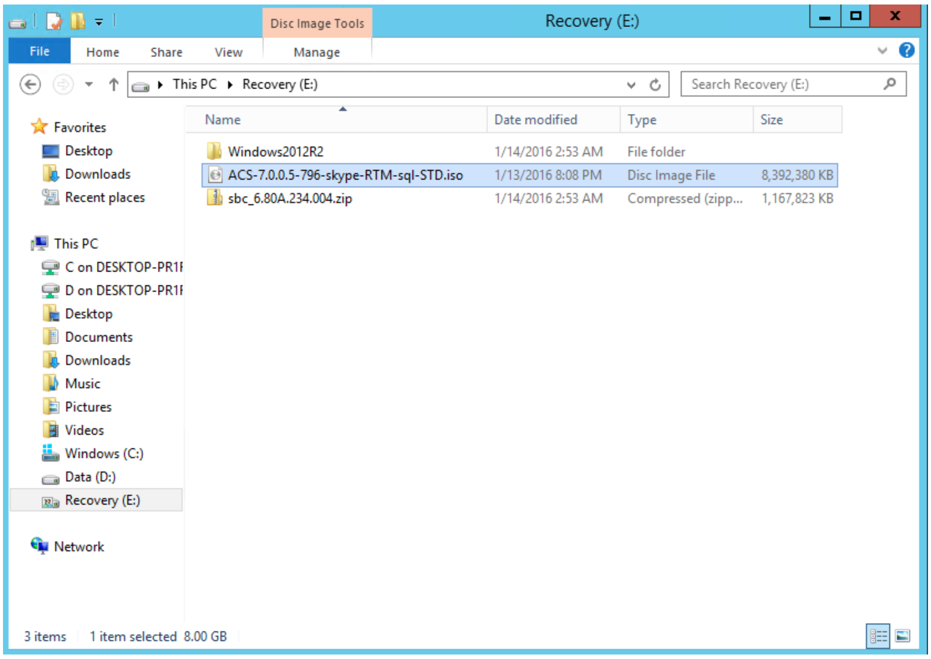
11.6.1 Recovery Partition

The Recovery partition should have a copy of selected contents from the USB key. The Recovery partition contains the following:

- Windows 2012 R2 directory
- ACS-X.0.x ISO image
- sbc_x.x.x zip file containing the AudioCodes Software SBC

The directory structure of the 'Recovery' Partition should appear as in the image below.

Figure 11-19: USB Drive Contents



Name	Date modified	Type	Size
Windows2012R2	1/14/2016 2:53 AM	File folder	
ACS-7.0.0.5-796-skype-RTM-sql-STD.iso	1/13/2016 8:08 PM	Disc Image File	8,392,380 KB
sbc_6.80A.234.004.zip	1/14/2016 2:53 AM	Compressed (zipp...	1,167,823 KB

3 items 1 item selected 8.00 GB

Warning: Under no circumstances, should there be any files or folders containing the letters 'sbc' present besides the zip file as shown in the image (the exact version might differ from the image).

If the Configuration Wizard has been previously run, you may find the following additional files in the root of the recovery partition:

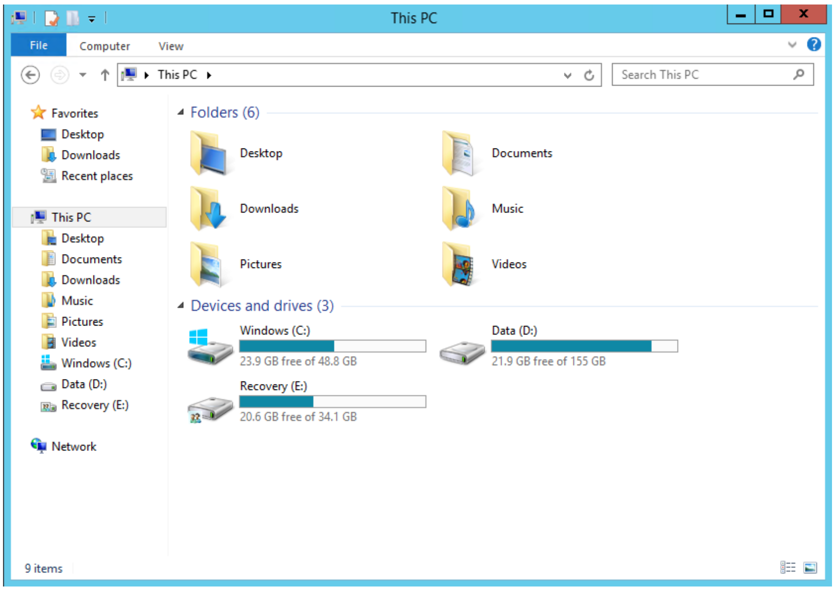
- configuration.xml
- Host.xml
- identities.txt

11.6.2 Mounting the ISO Image

If you have not already done so, remove the USB key from the system.

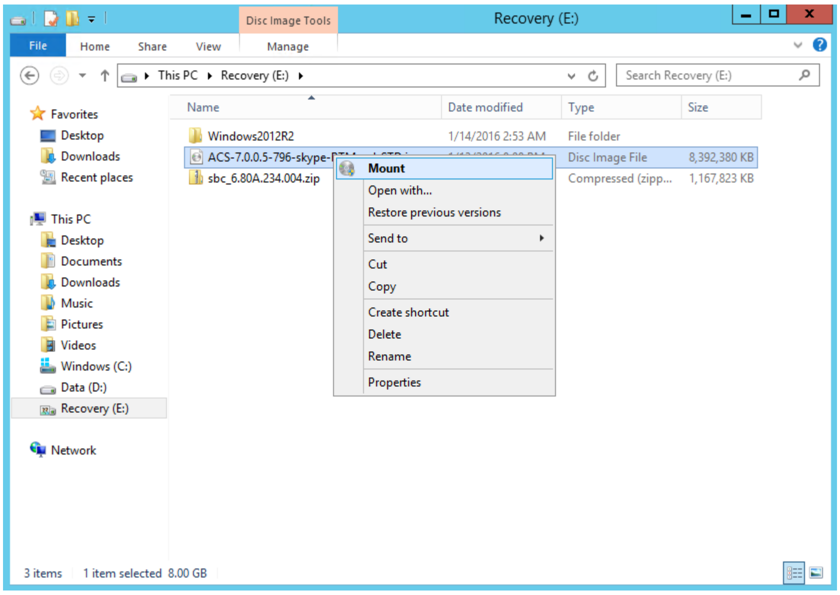
1. Open the Windows File Explorer.
2. Open the Recovery partition (double click).

Figure 11-20: Open the Recovery partition



3. Locate the ACS-7.x.x ISO image.
4. Mount the image by double clicking, or right-click and select mount.

Figure 11-21: Mounting the ISO image



Name	Date modified	Type	Size
Windows2012R2	1/14/2016 2:53 AM	File folder	
ACS-7.0.0.5-796-skype-[illegible]	[illegible]	Disc Image File	8,392,380 KB
sbc_6.80A.234.004.zip		Compressed (zipp...	1,167,823 KB

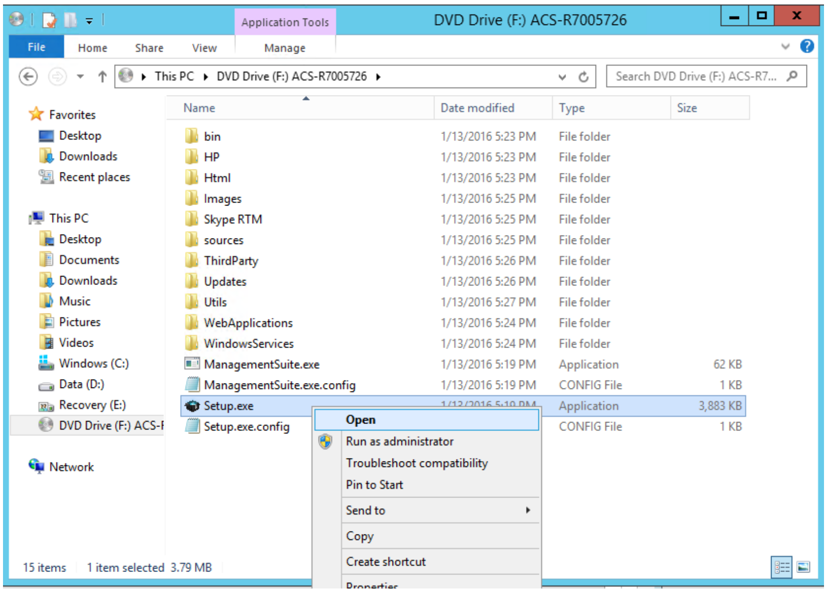
5. The ISO image will be mounted and assigned an available drive letter.
6. Windows File Explorer will automatically open a window showing the contents of the mounted ISO image.

11.6.3 Starting the Configuration Wizard

Warning: Do not start the Configuration Wizard before reading the following chapter regarding Deployment Types.

1. Locate the Setup application within the mounted ISO image.
2. Double Click, or right click and select open, to start the Configuration Wizard.

Figure 11-22: Starting the Configuration Wizard



Name	Date modified	Type	Size
bin	1/13/2016 5:23 PM	File folder	
HP	1/13/2016 5:23 PM	File folder	
Html	1/13/2016 5:23 PM	File folder	
Images	1/13/2016 5:25 PM	File folder	
Skype RTM	1/13/2016 5:25 PM	File folder	
sources	1/13/2016 5:25 PM	File folder	
ThirdParty	1/13/2016 5:26 PM	File folder	
Updates	1/13/2016 5:26 PM	File folder	
Utils	1/13/2016 5:27 PM	File folder	
WebApplications	1/13/2016 5:24 PM	File folder	
WindowsServices	1/13/2016 5:24 PM	File folder	
ManagementSuite.exe	1/13/2016 5:19 PM	Application	62 KB
ManagementSuite.exe.config	1/13/2016 5:19 PM	CONFIG File	1 KB
Setup.exe	1/13/2016 5:19 PM	Application	3,883 KB
Setup.exe.config		CONFIG File	1 KB

15 items 1 item selected 3.79 MB

11.7 Software Configuration Wizard

The Software Configuration Wizard will guide you through the options available for installing the CloudBond 365 software product.

When completed, the Wizard will store your configuration choices in a configuration file on the local HDD storage, in both the Recovery partition, and the c:\acs\installtmp directory.

Each time the Configuration Wizard is started, it will search for an existing configuration file. If one is located, the Configuration Wizard will proceed straight to the final summary page in readiness to perform the software installation.

11.7.1 Deployment Type

Shortly after starting the configuration wizard, you must choose from two deployment types:

- Standalone
- Branch / Paired Pool Appliance (BPA)
- User Management Pack 365

The three deployment types have completely different installation results, and are detailed in separate sections.

Warning: Once a Deployment Type is chosen, it is not possible to change the Deployment Type without restarting the Configuration Wizard.

11.7.1.1 Standalone Deployment Type

Note: A Standalone Deployment creates the first CloudBond 365 system for a customer.

A Standalone deployment type is for a standalone, CloudBond 365 Skype for Business deployment.

This is generally the first Skype for Business install for a site, and uses the Resource Forest model. It will automatically install a Domain Controller (DC) with the CloudBond 365 Management Suite (SysAdmin), Front-End server, and Edge Server, all within the Resource Forest.

The customer can then either operate the CloudBond 365 system by itself in standalone mode, or, join the Resource Forest to their existing Domain using a forest trust. For more information, see Section Standalone Deployment Type on page124

If performing a Standalone Deployment Type, continue with the Section 11.8 on page 124.

11.7.1.2 Branch / Paired Pool DeploymentType

Note: A Branch / Paired Pool deployment can only be added to an existing CloudBond 365 system or any other Microsoft Skype for Business customer deployment.

A Branch / Paired Pool Appliance deployment type is for adding a CloudBond 365 Skype for Business device to an existing CloudBond 365 or Microsoft Skype for Business environment. It will create an additional SysAdmin Management Server, which can optionally be deployed as an additional full domain controller for resiliency / branch authentication and an FE server within the existing Skype for Business Topology. Optionally other components, like consolidated Edge server, SBC and Reverse Proxy can also be installed in the BPA depending on the hardware used.

If performing a Branch / Paired Pool Deployment Type, skip to Section 11.9 on page 138.

11.7.1.3 User Management Pack 365

The User Management Pack 365 deployment type enablesthe installation of only the management layer within an existing Lync Server 2013 or Skype for Business Server environment. This option can also be used to upgrade an older version of the CloudBond 365 Management Suite.

11.8 Standalone Deployment Type

A Standalone deployment type is for a standalone, CloudBond 365 Skype for Business deployment.

This is generally the first Skype for Business installation for a site and will automatically install a Domain Controller (DC) with the CloudBond 365 Management Suite, a Front-End server and an Edge Server in the Resource Forest model.

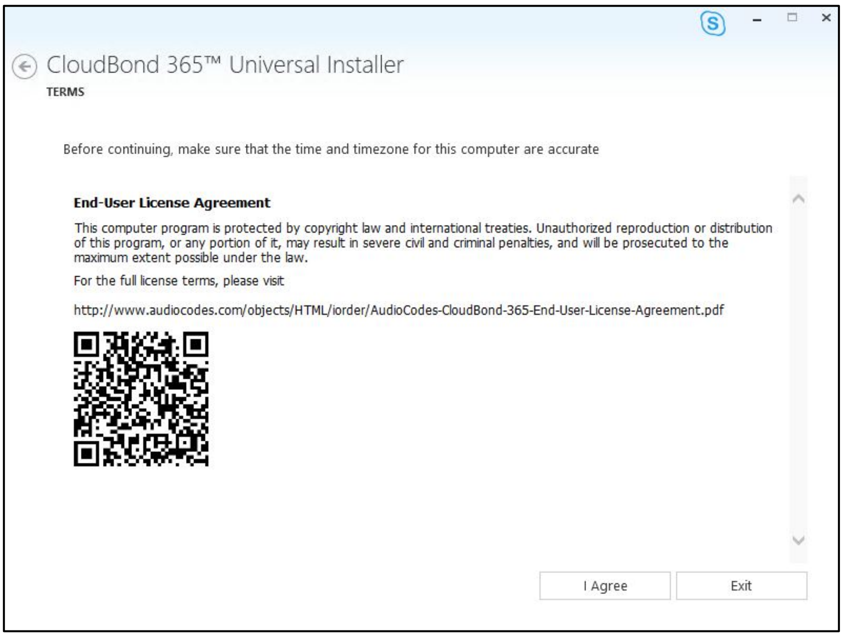
The customer can then either operate the CloudBond 365 system in Standalone mode by itself, or, join the Resource Forest to their existing Domain using a forest trust. For more information, see Section 6.5 on page 39.

11.8.1 License Agreement

If you are running the Configuration Wizard for the first time, or an existing configuration file is not found, a license agreement page is presented. You must agree to the license terms before proceeding with the software installation.

This page offers a short copy write text, a link to the full license agreement, and a QR code which contains said link. Click I Agree to continue setup, or Exit to abort.

Figure 11-23: License Agreement



Before continuing, make sure that the time and timezone for this computer are accurate

End-User License Agreement

This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

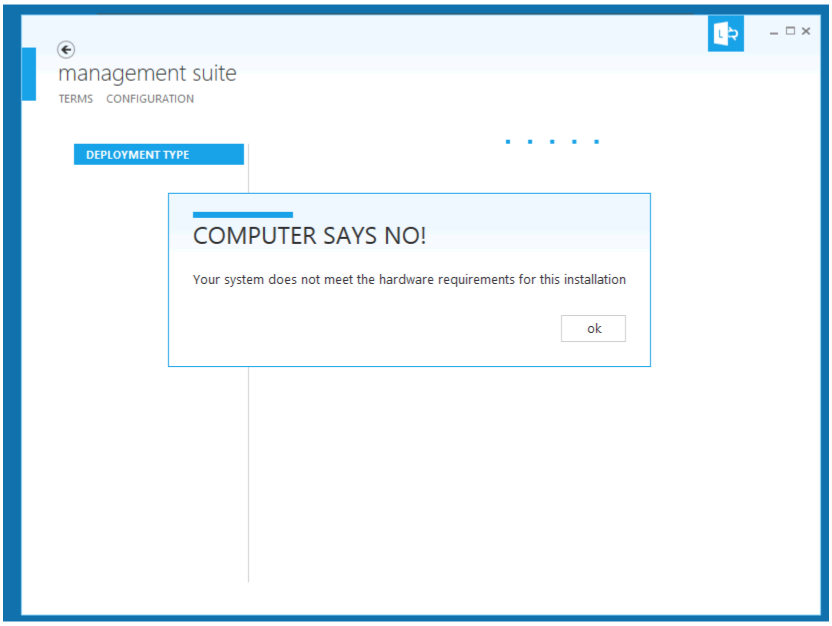
For the full license terms, please visit

http://www.audiocodes.com/objects/HTML/iorder/AudioCodes-CloudBond-365-End-User-License-Agreement.pdf

11.8.2 Hardware Check

The Configuration Wizard will first verify the hardware platform that it is running on. The hardware detected will influence the options presented within the Configuration Wizard. When the system running the setup does not meet the hardware requirements, the following message is shown.

Figure 11-24: Hardware Check



COMPUTER SAYS NO!

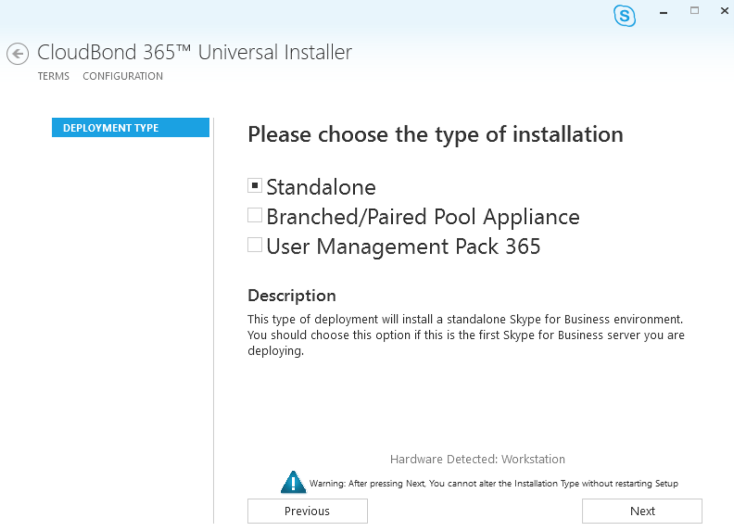
Your system does not meet the hardware requirements for this installation

11.8.3 Deployment Type

You must choose the Standalone deployment type, for the first CloudBond 365 system for a customer.

This page also shows which hardware level was detected.

Figure 11-25: Choosing Deployment Type



Please choose the type of installation

- ■ Standalone
- □ Branched/Paired Pool Appliance
- □ User Management Pack 365

Description

This type of deployment will install a standalone Skype for Business environment. You should choose this option if this is the first Skype for Business server you are deploying.

Hardware Detected: Workstation

Warning: After pressing Next, You cannot alter the Installation Type without restarting Setup

11.8.4 Deployment Model

There are currently three Deployment Models on the Configuration Wizard to choose from:

- Virtual Edition
- Hyper-V Host with Virtual Machines
- Co-Located Hyper-V / Domain Controller with Virtual Machines

If you're not installing the Virtual Edition, you can optionally install:

- Session Border Controller (SBC)
- Reverse Proxy Server (RP)

Note:

- The hardware detected by the Configuration Wizard determines which Deployment Models are available, e.g., on a Mediant 800 OSN with 16/32GB RAM, only the Co-Located Hyper-V / Domain Controller with Virtual Machines is offered.
- The Skype for Business Consolidated Edge server is mandatory for a Standalone Deployment Type, but optional for a BPA Deployment Type.
- The optional SBC and RP are not available on CloudBond 365 Standard Box Edition (Mediant 800 OSN).
- If both the SBC and RP additional machines are checked, the Front-End Server will start with reduced memory to accommodate the two extra machines.

11.8.4.1 Virtual Edition

The Virtual Edition allows you to install the CloudBond 365 application onto your own (virtual) hardware. The installer must run the installation file on three individual Windows Server 2012 R2 Operating System environments, in this order:

1. On the server that hosts the CloudBond 365 management server
2. On the server that hosts the CloudBond 365 FrontEnd server
3. On the server that hosts the CloudBond 365 Edge server

11.8.4.1.1 Virtual Machine Specification

When CloudBond 365 is deployed as Virtualized Edition, you need to prepare the following Virtualized environment. The minimum specification is shown in the table below. Virtualization is supported on Hyper-V or VMware.

Table 11-2: Minimum Specification of the Virtualized Environment

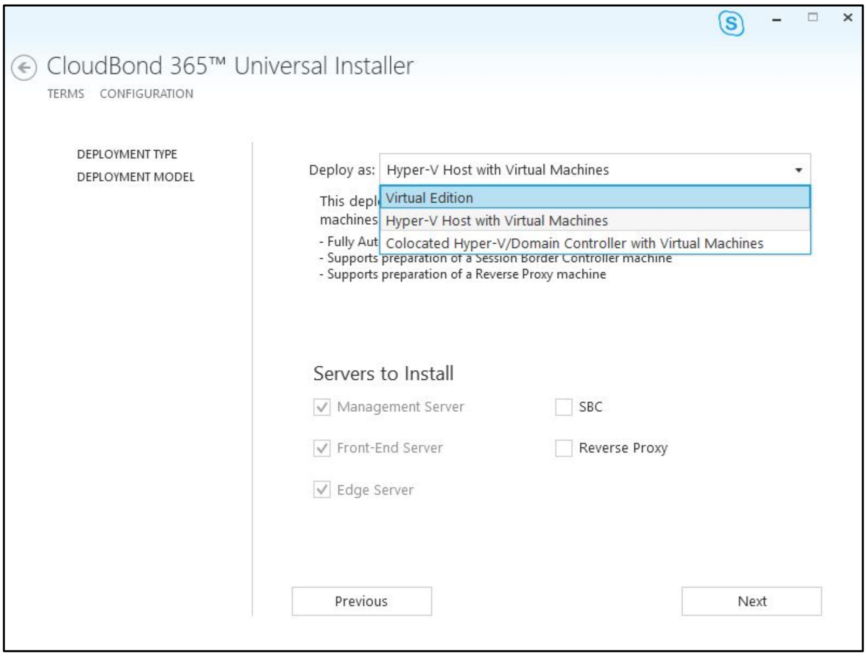
Server	Use	OS***	CPU (Virtual Core)	RAM* in GB	HDD in GB	NIC**
1	Domain Controller & Management	Win 2012 R2	4/4/4	4/8/8	80	1
2	Front End	Win 2012 R2	6/12/16	10/20/24	80	1
3	Edge	Win 2012 R2	4/6/6	8/16/16	50	2

* RAM assigned according to number of users: 500/2000/5000

** NIC can be shared

*** Windows Server 2012 R2 must be licensed

Figure 11-26: Deployment Model – Virtual Edition



CloudBond 365™ Universal Installer

TERMS
CONFIGURATION
DEPLOYMENT TYPE
DEPLOYMENT MODEL

Deploy as: Hyper-V Host with Virtual Machines

Virtual Edition
Hyper-V Host with Virtual Machines
Colocated Hyper-V/Domain Controller with Virtual Machines

This depl
machines
- Fully Aut
- Supports preparation of a Session Border Controller machine
- Supports preparation of a Reverse Proxy machine

Servers to Install

☑ Management Server
☑ Front-End Server
☑ Edge Server
□ SBC
□ Reverse Proxy

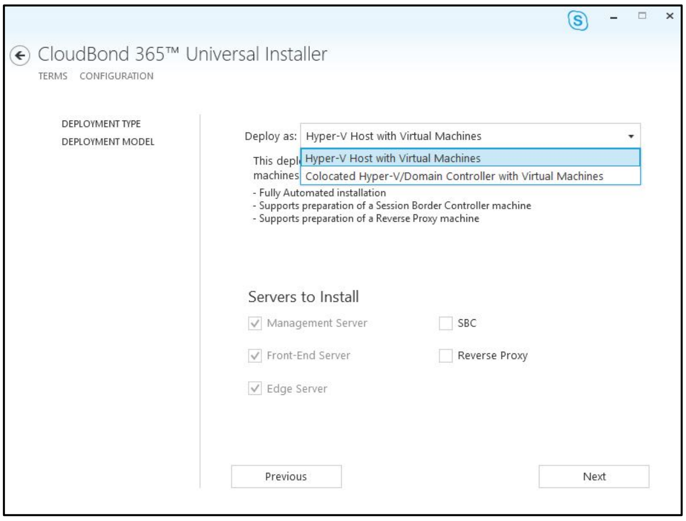
11.8.4.2 Hyper-V Host with Virtual Machines

The Hyper-V Host with Virtual Machines installs Hyper-V on the selected host machine, and the three CloudBond 365 Servers (Controller, FE, and Edge) as three separate virtual machines within Hyper-V.

You may also choose to add an SBC server and Reverse Proxy server.

This option is suitable for CloudBond 365 Pro, and CloudBond 365 Enterprise. (e.g., AudioCodes HP Servers).

Figure 11-27: Deployment Model - Pro and Enterprise



Deploy as: Hyper-V Host with Virtual Machines

Hyper-V Host with Virtual Machines
Colocated Hyper-V/Domain Controller with Virtual Machines

This depl
machines
- Fully Automated installation
- Supports preparation of a Session Border Controller machine
- Supports preparation of a Reverse Proxy machine

Servers to Install

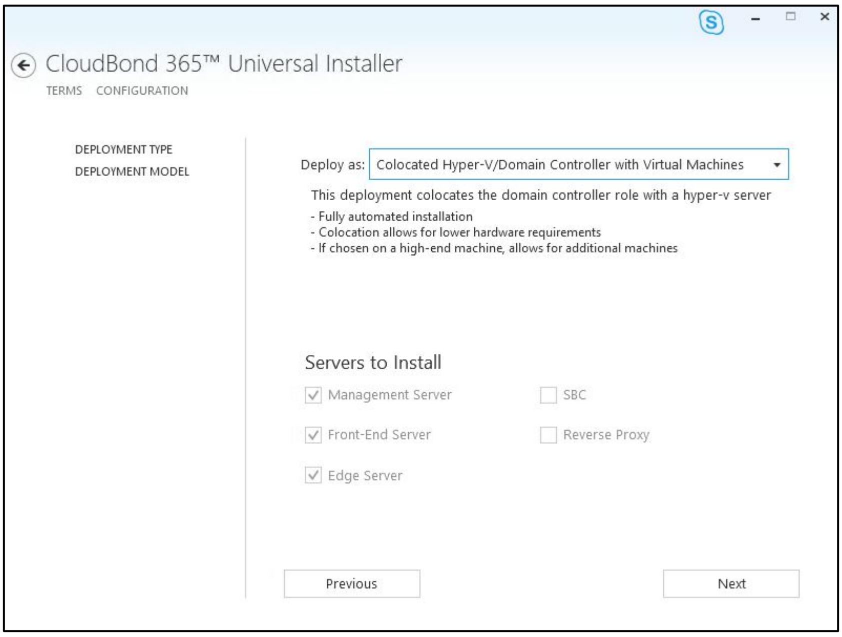
☑ Management Server
☑ Front-End Server
☑ Edge Server
□ SBC
□ Reverse Proxy

11.8.4.3 Co-located Hyper-V / Domain Controller with Virtual Machines

The Co-Located Hyper-V / Domain Controller with Virtual Machines installs the CloudBond 365 Controller (DC) and Hyper-V within the host machine, with the remaining CloudBond 365 Servers (FE and Edge) as Hyper-V virtual machines.

This option is suitable for CloudBond 365 Standard Box Edition (e.g., AudioCodes Mediant 800B OSN server).

Figure 11-28: Deployment Model - Mediant 800



Deploy as: Colocated Hyper-V/Domain Controller with Virtual Machines

This deployment colocates the domain controller role with a hyper-v server
- Fully automated installation
- Colocation allows for lower hardware requirements
- If chosen on a high-end machine, allows for additional machines

Servers to Install

☑ Management Server
☑ Front-End Server
☑ Edge Server
□ SBC
□ Reverse Proxy

11.8.5 Credentials for Standalone Deployment

If performing a Standalone Deployment, you will be asked to confirm or change the login credentials for the CloudBond 365 Administrator.

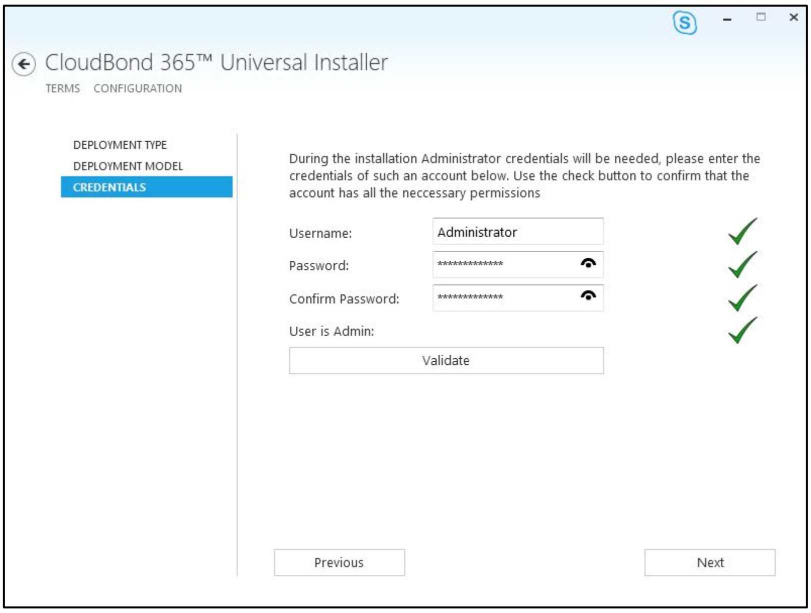
The credential page requires you to enter the credentials of an Administrator account to verify you have the required permissions to continue the installation process.

If the configuration is being entered for a Bare Metal install, the entered username and password will be created.

If running the installer from pre-installed Windows2012 R2, the entered credentials must already be present on the system.

Click **Validate** to verify the information you entered is correct.

Figure 11-29: Credentials



During the installation Administrator credentials will be needed, please enter the credentials of such an account below. Use the check button to confirm that the account has all the neccessary permissions

Username: Administrator ✓

Password: ************* ✓

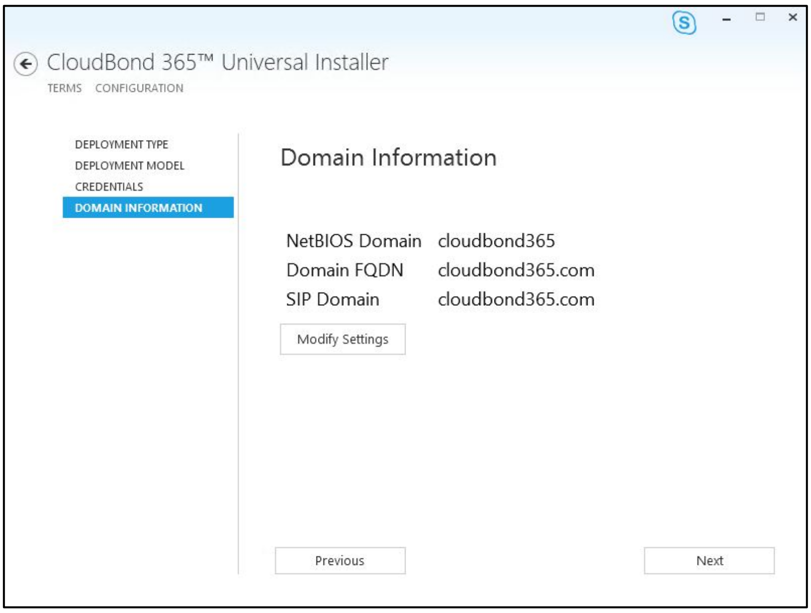
Confirm Password: ************* ✓

User is Admin: ✓

11.8.6 Domain Information (Standalone Deployment)

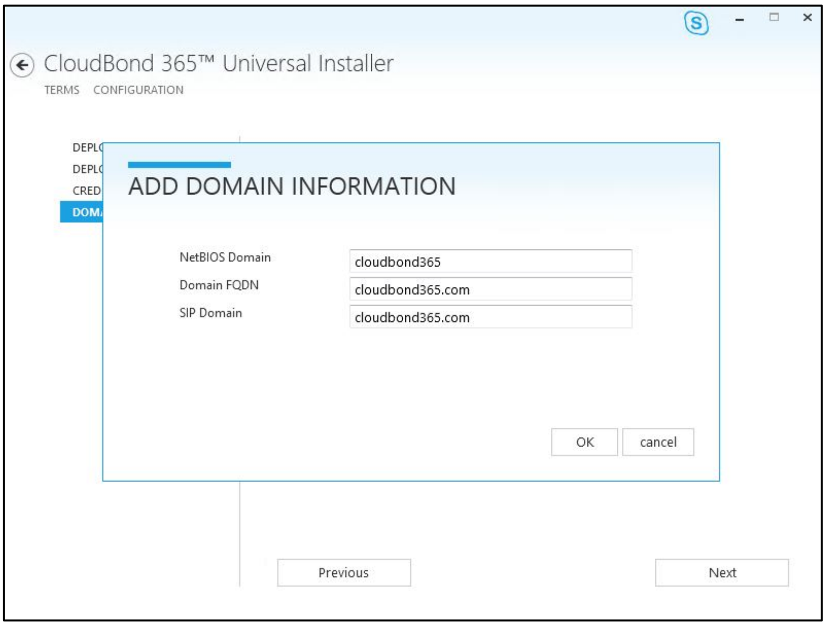
If you selected a Standalone Deployment Type, you will be prompted to confirm or change the new Domain information, including NetBIOS domain name, the Domain FQDN, and the default SIP Domain within Skype for Business. You may leave these values at their default settings, or modify them as required.

Figure 11-30: Standalone Deployment Domain



NetBIOS Domain cloudbond365
Domain FQDN cloudbond365.com
SIP Domain cloudbond365.com

Figure 11-31: Modifying Domain Details



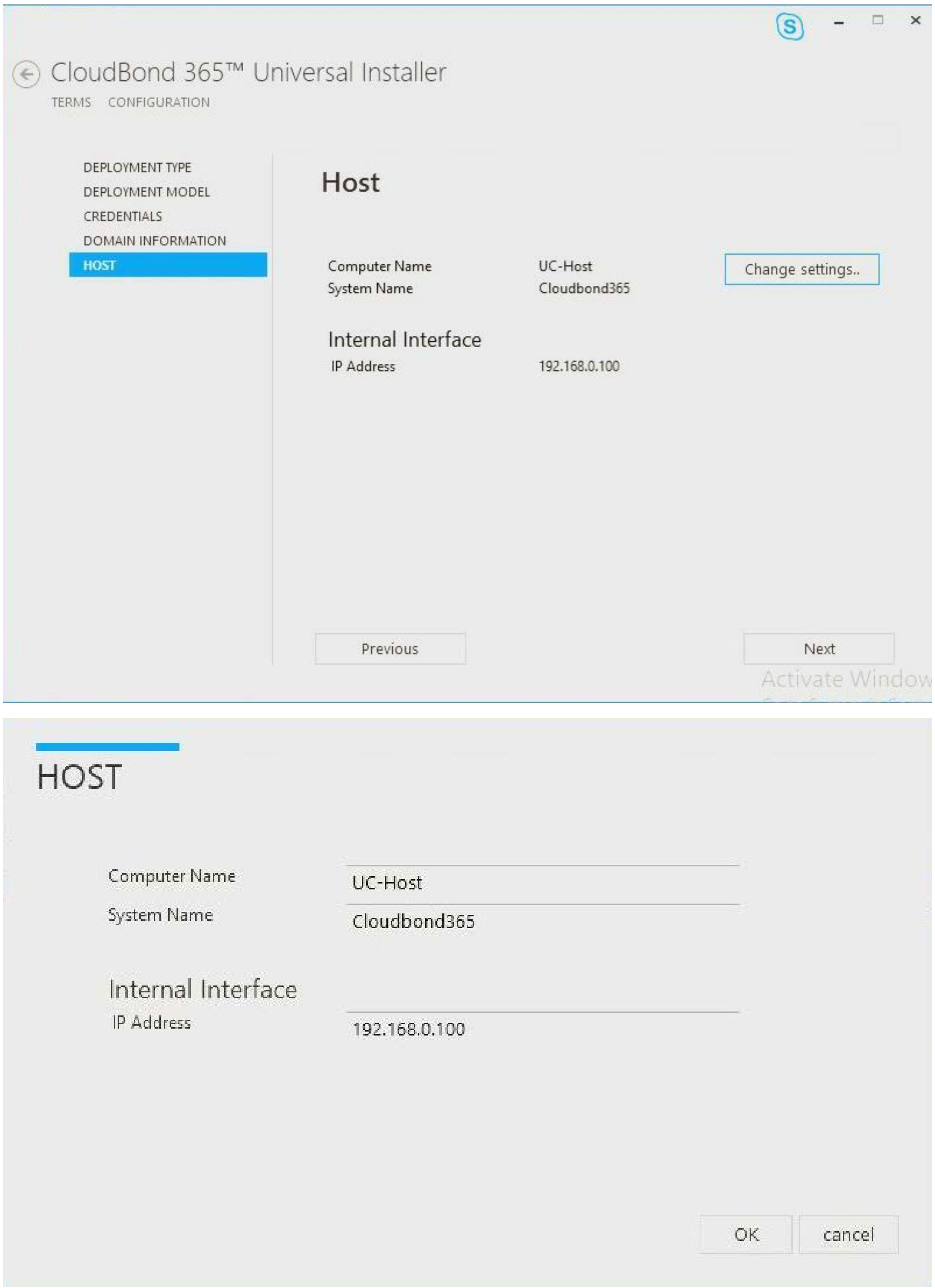
NetBIOS Domain: cloudbond365
Domain FQDN: cloudbond365.com
SIP Domain: cloudbond365.com

11.8.7 Host Server

For the Hyper-V Host with Virtual Machines deployment model, you'll be prompted to confirm or change the details for the Host server.

Note: This is relevant only for the CloudBond 365 Pro/Enterprise Edition.

Figure 11-32: Host Server



Host

Computer Name UC-Host
System Name Cloudbond365

Internal Interface
IP Address 192.168.0.100

HOST

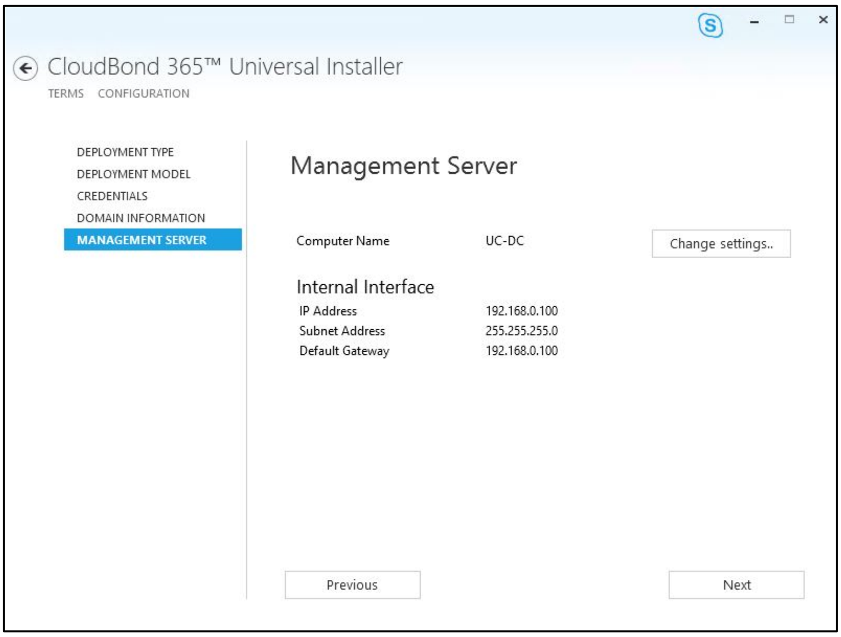
Computer Name UC-Host
System Name Cloudbond365

Internal Interface
IP Address 192.168.0.100

11.8.8 Domain Controller

If you selected a Standalone Deployment Type, you will be asked to verify or change the Management Server information. The wizard will automatically create a new Forest and Domain controller with the information specified, and install the SysAdmin suite and Archiving and Monitoring database on the controller.

Figure 11-33: Specify the DC (Standalone)



Management Server

Computer Name UC-DC

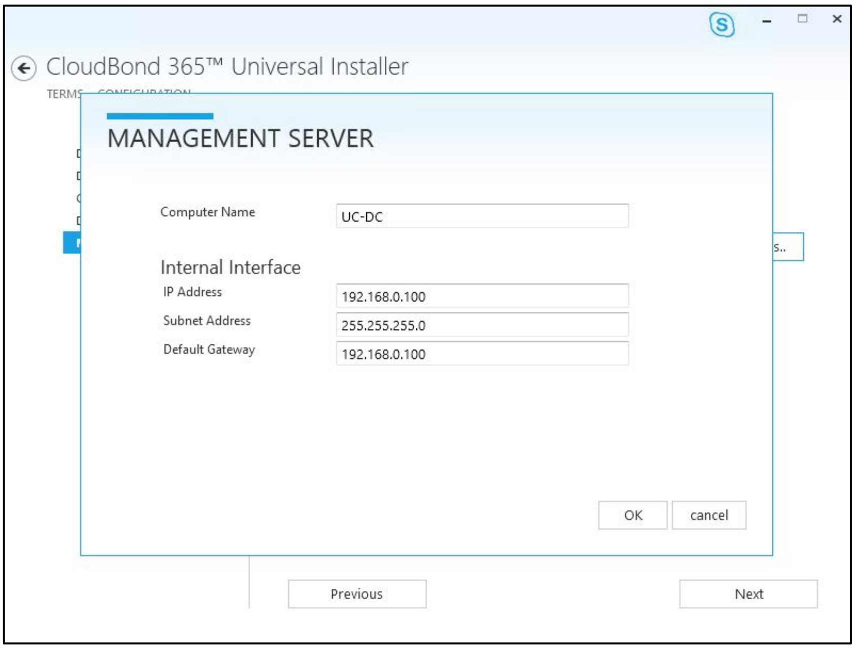
Internal Interface

IP Address 192.168.0.100

Subnet Address 255.255.255.0

Default Gateway 192.168.0.100

Figure 11-34: Changing the Controller Settings



MANAGEMENT SERVER

Computer Name UC-DC

Internal Interface

IP Address 192.168.0.100

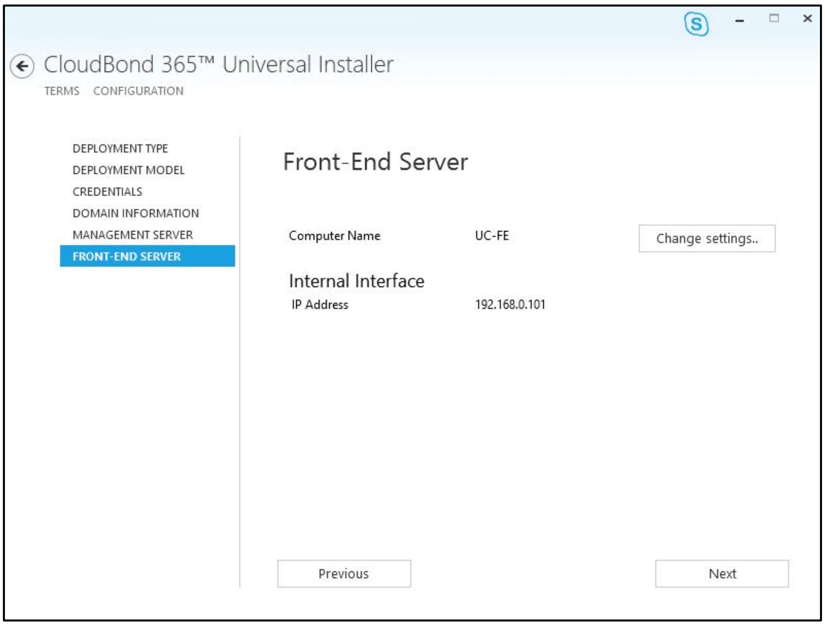
Subnet Address 255.255.255.0

Default Gateway 192.168.0.100

11.8.9 Front-End Server

For all deployment types, you will be asked to confirm or change the details for the Front-End server.

Figure 11-35: Front-End server



CloudBond 365™ Universal Installer

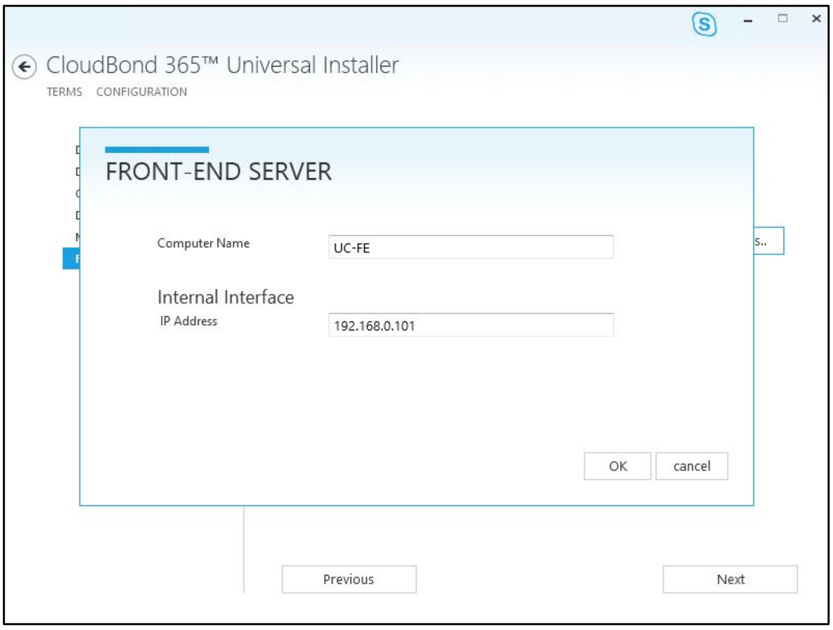
Front-End Server

Computer Name UC-FE

Internal Interface

IP Address 192.168.0.101

Figure 11-36: Changing the FE settings



CloudBond 365™ Universal Installer

FRONT-END SERVER

Computer Name UC-FE

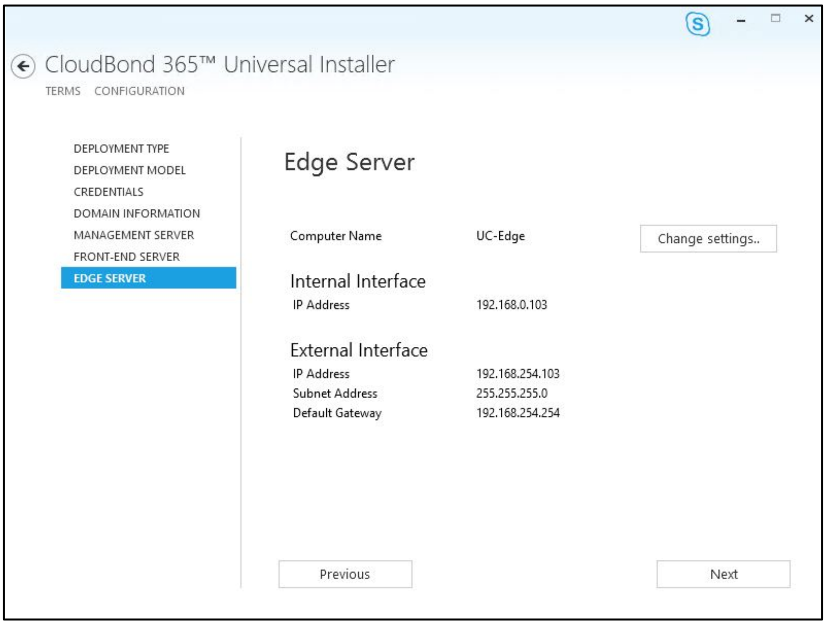
Internal Interface

IP Address 192.168.0.101

11.8.10 Edge Server

For Standalone Deployment Type, you will be asked to confirm or change the details of the Edge Server.

Figure 11-37: Edge Server (Standalone)



Edge Server

Computer Name UC-Edge

Internal Interface

IP Address 192.168.0.103

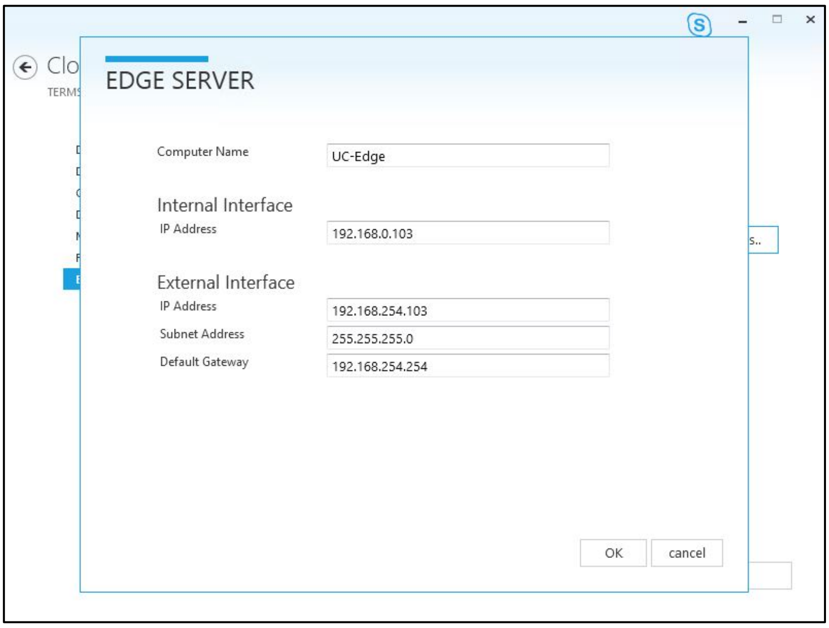
External Interface

IP Address 192.168.254.103

Subnet Address 255.255.255.0

Default Gateway 192.168.254.254

Figure 11-38: Changing the Edge Settings



EDGE SERVER

Computer Name UC-Edge

Internal Interface

IP Address 192.168.0.103

External Interface

IP Address 192.168.254.103

Subnet Address 255.255.255.0

Default Gateway 192.168.254.254

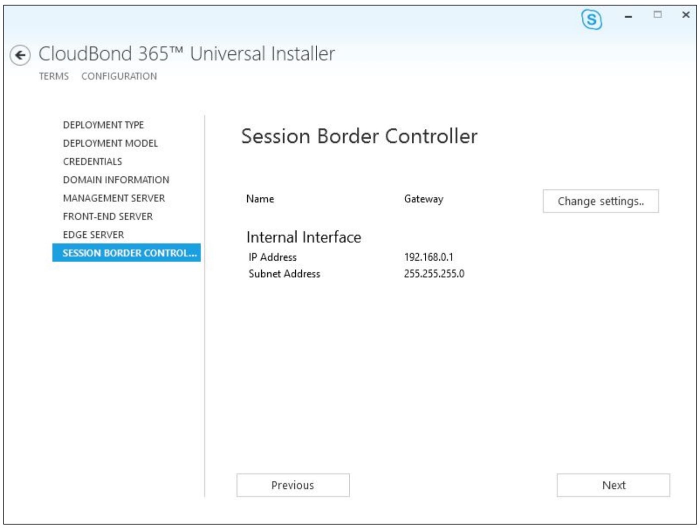
Note: To prevent complex networking scenarios during installation, the wizard only allows for a single public Edge IP Address and requires the Edge internal leg to be on the same subnet as the other servers installed. If different deployment scenarios are needed, it is just a small change to be made in Skype for Business Topology Builder after the installation wizard has finished.

For more information see Section 17.5.1.4, Chapter 14 and Chapter 17.

11.8.11 Session Border Controller

This option installs the AudioCodes SBC software on the nominated server. See the *AudioCodes Mediant Virtual Edition SBC Installation Manual* for more information.

Figure 11-39: SBC Settings



CloudBond 365™ Universal Installer

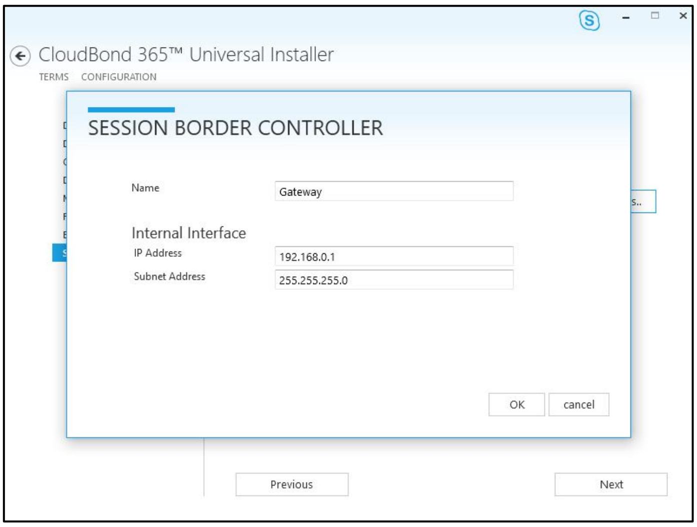
Session Border Controller

Name: Gateway

Internal Interface
IP Address: 192.168.0.1
Subnet Address: 255.255.255.0

Note: The optional SBC is not available on CloudBond 365 Standard / Standard+ Box Edition (Mediant 800 OSN).

Figure 11-40: Changing the SBC settings



CloudBond 365™ Universal Installer

SESSION BORDER CONTROLLER

Name: Gateway

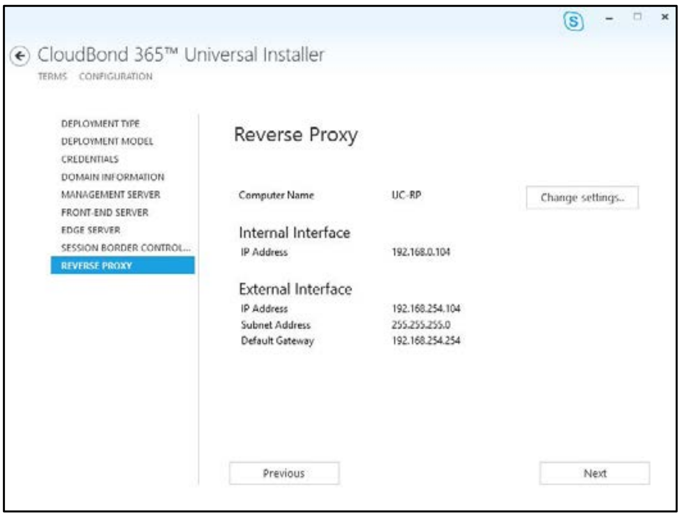
Internal Interface
IP Address: 192.168.0.1
Subnet Address: 255.255.255.0

Note: There are many possible network configurations for the SBC. You may need to modify the Hyper-V network adapter requirements after software installation to meet your requirements.

11.8.12 Reverse Proxy Server

This option creates a Windows 2012 R2 virtual machine suitable for use as a Reverse Proxy using Internet Information Server and Application Request Routing (IIS + ARR). Further details on this Reverse Proxy solution can be found in chapter Installing IIS and ARR on page 282.

Figure 11-41: Reverse Proxy Settings



Reverse Proxy

Computer Name UC-RP

Internal Interface

IP Address 192.168.0.104

External Interface

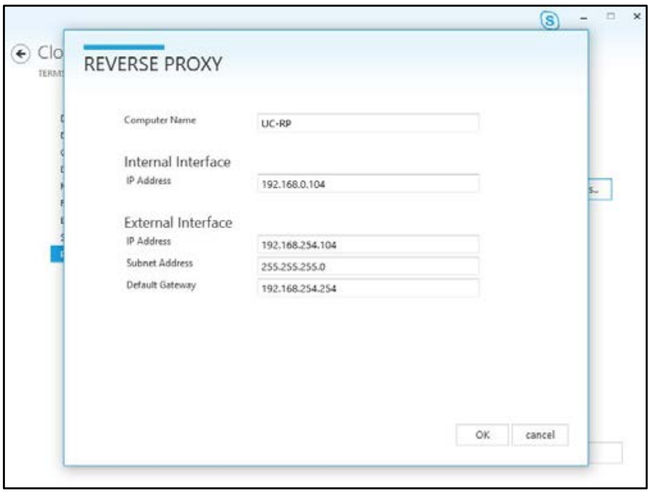
IP Address 192.168.254.104

Subnet Address 255.255.255.0

Default Gateway 192.168.254.254

Note: The optional RP is not available on CloudBond 365 Standard Box Edition (Mediant 800 OSN), or if the Branch / Paired Pool deployment type is chosen.

Figure 11-42: Changing the RP Settings



REVERSE PROXY

Computer Name UC-RP

Internal Interface

IP Address 192.168.0.104

External Interface

IP Address 192.168.254.104

Subnet Address 255.255.255.0

Default Gateway 192.168.254.254

Note: There are many possible network configurations for the RP. You may need to modify the Hyper-V network adapter requirements after software installation to meet your requirements.

11.8.13 SBC Configuration

To manage the SBC with the EMS Agent, the following changes are required in the SBC ini file settings.

- Enable internal OSNInternalVLAN – This option enables the EMS Agent in CloudBond to access the SBC. You can change the value either from the CLI or from the ini file, to OSNInternalVLAN = **1**.

11.8.14 Summary

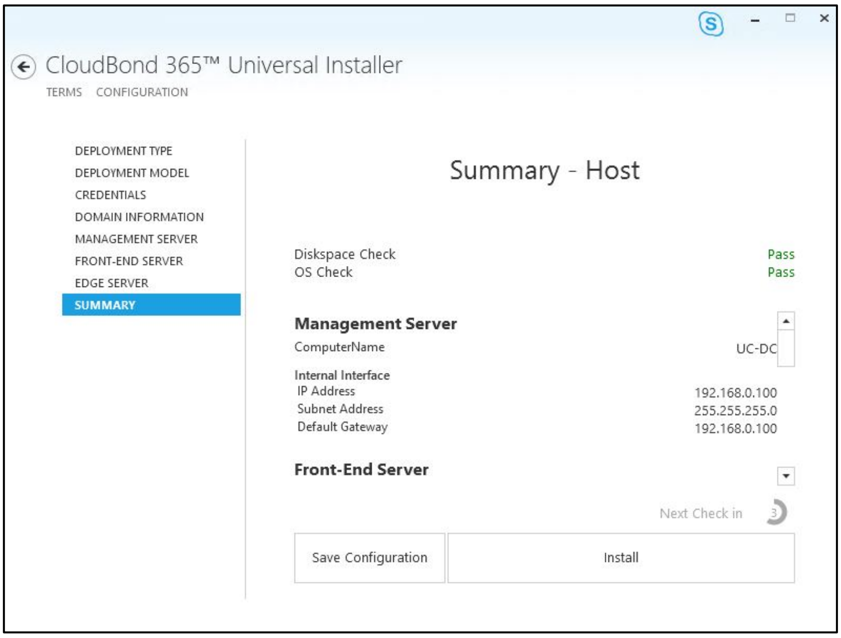
The Summary page shows details of the selections made during the Wizard, as well as various pre-checks performed on the hardware.

If all information meets requirements, an **Install** button will appear below.

The summary page allows you to manually save the entered configuration by clicking on the Save Configuration button. This will prompt you for a location to save the file.

Click the **Install** button to begin the Software Install process only once the checks show **Pass.** The OS Check specifically will sometimes need more time to be validated. The rotating wheel above the **Install** Button gives a time indication when the next validation check will be performed.

Figure 11-43: Wizard Summary



Summary - Host

Diskspace Check Pass
OS Check Pass

Management Server

ComputerName UC-DC

Internal Interface
IP Address 192.168.0.100
Subnet Address 255.255.255.0
Default Gateway 192.168.0.100

Front-End Server

Next Check in 3

11.9 Branch / Paired Pool Deployment Type

A Branch / Paired Pool Appliance (BPA) deployment type is for adding a CloudBond 365 Skype for Business device to an existing CloudBond 365 or Microsoft Skype for Business deployment. It will create a Management Server with the SysAdmin suite, which can optionally be enabled as an additional DC. It will also install an FE server within the existing Skype for Business Topology, and optionally install an additional Edge server.

If you choose to install a Branch / Paired Pool Appliance deployment type, you will need to prepare some items before starting the configuration wizard.

- During the Configuration Wizard, the software must be able to contact the existing CloudBond 365 installation, and specifically the existing domain controller. You must ensure that the Host IP address, gateway, and DNS settings are correct before proceeding.

Note: If multiple Active Directory Sites exist within the environment, make sure that the correct IP Subnet information is configured to prevent installation failures. Active Directory assigns a domain controller for domain-based actions by checking the IP Subnet information and if a wrong domain controller is assigned (in a different subnet) you might experience Active Directory replication issues.

In such a case, one domain controller will know about the computer object that is currently being installed, but another domain controller does not know that computer object yet. Actions like *join domain* or *promote to domain controller* will fail due to the fact that the computer object is not found, or there are no logon servers to process the logon request.

By default, all domain controllers will replicate every 15 minutes within an Active Directory site and every 180 minutes between sites. More information on Active Directory replication can be found at: https://technet.microsoft.com/en-us/library/cc961788.aspx.

- In addition to setting the correct IP information, an Ethernet cable must be connected to the front GE1 port of the Mediant 800 gateway, or to the Corporate LAN NIC of the HP Server when using Pro / Enterprise hardware.
- The configuration wizard will also ask you to supply a copy of the existing Topology as a zip file, created using the Export-csConfiguration command. It is a much smoother process if this Topology file is prepared ahead of time.

11.9.1 Planning Your BPA

There are many possible configuration combinations for CloudBond 365 BPA Deployments, depending upon network layout, WAN links, and desired outcomes.

Configurations can vary from the relatively simple, such as a Management Server with local FE at a branch location, to a Full DC with paired pool FE and alternate Edge connector at a remote site.

Exact details for each configuration are not covered in this guide. See the *Microsoft Skype for Business Planning information* for further details.

For a BPA install to be successful, you should plan ahead, at a minimum allowing for new server names and IP addresses for the Management Server and FE. If planning an additional Edge Server, consideration must be given to many aspects of Skype for Business External connectivity, including internet domain names, public geographic based DNS servers, hardware load balancers, federation requirements, etc.

Note:

- The default server names and IP addresses presented by the Wizard are the same as those used for a Standalone Deployment Type. Rarely are these values suitable for a BPA deployment. You should be prepared to enter new values for Server Names and IP addresses, according to your planned configuration.
- As the BPA will be joined into an existing Active Directory forest topology, the server running the CloudBond 365 Hyper-V host will need to have a DNS IP address assigned that is capable of resolving a domain controller for the domain to which the BPA will need to be joined. The same DNS will need to be used in the Wizard on the Management Server Configuration page.

11.9.2 Preparing the Topology

Within the existing CloudBond 365 Topology, there will be a single site defined, containing the existing FE and Edge Servers.

To add a BPA system, it is necessary to add another FE server, and optionally, an Edge server definition within the Topology.

You may also wish to add the new servers to the existing Site, or create a new Site.

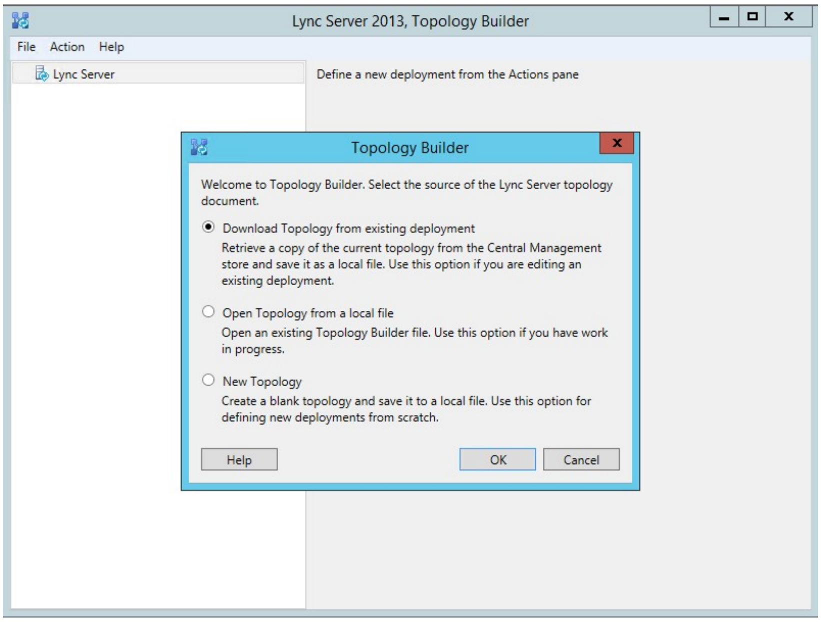
Note: Skype for Business Topology Sites are not related to AD Sites and Services, or to MS Exchange Sites. You may optionally wish to update your AD Sites and Services to match Skype for Business Sites for consistency.

11.9.2.1 Editing the Topology

To prepare the Topology file:

1. Logon to the existing CloudBond 365 Controller (or Skype for Business FE Server).
2. Open Topology Builder.
3. Download the current topology (and save it when it prompts you to).

Figure 11-44: Downloading Existing Topology



Define a new deployment from the Actions pane

Topology Builder

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.

○ Open Topology from a local file

Open an existing Topology Builder file. Use this option if you have work in progress.

○ New Topology

Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.

11.9.2.2 Adding a New Site (Optional)

Adding a new site to the Skype for Business topology is optional. You must add a new FE server to the existing topology, but that FE server may be within an existing site, or within a newsite.

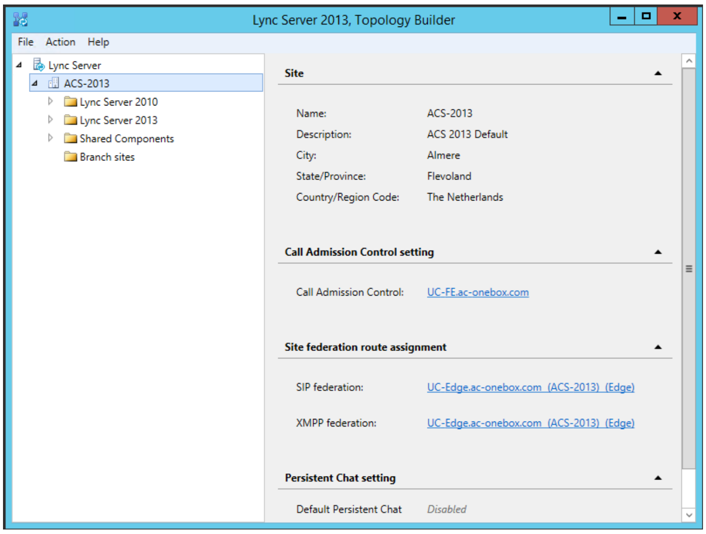
Typically, you would add a new site for a “Branch” install, but add to an existing site for a central Paired Pool.

Note: The Skype for Business Topology uses “Branch Sites” for definition of Survivable Branch Appliances (SBAs). A BPA is not a SBA, and is defined within a Central Site, not within the Branch Sites area.

➢ To Add a new site:

1. Right-click the ‘Lync Server’ node and select ‘New Central Site’.

Figure 11-45: Existing Topology



Site

Name: ACS-2013

Description: ACS 2013 Default

City: Almere

State/Province: Flevoland

Country/Region Code: The Netherlands

Call Admission Control setting

Call Admission Control: UC-FE.ac-onebox.com

Site federation route assignment

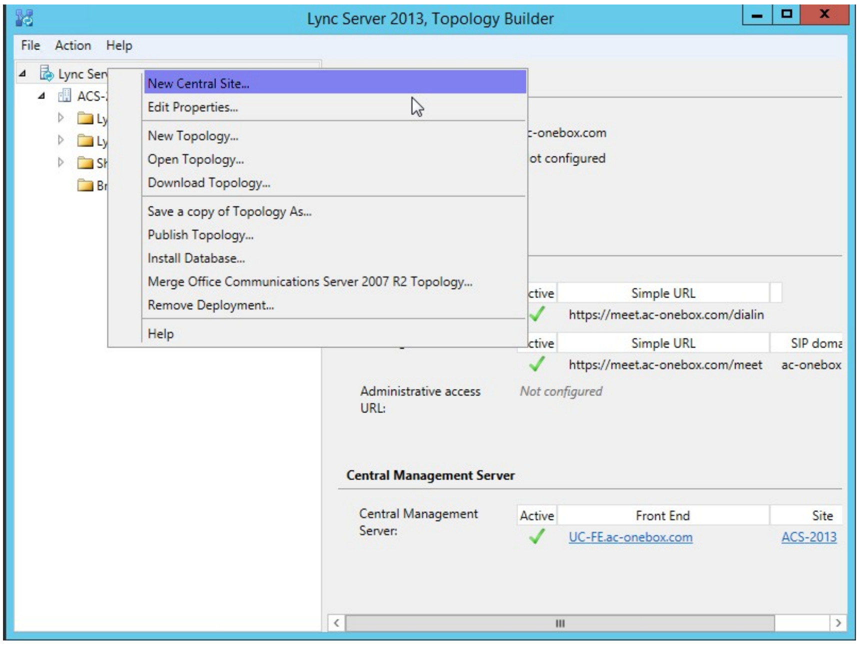
SIP federation: UC-Edge.ac-onebox.com (ACS-2013) (Edge)

XMPP federation: UC-Edge.ac-onebox.com (ACS-2013) (Edge)

Persistent Chat setting

Default Persistent Chat *Disabled*

Figure 11-46: Adding New Central Site



Simple URL: https://meet.ac-onebox.com/dialin

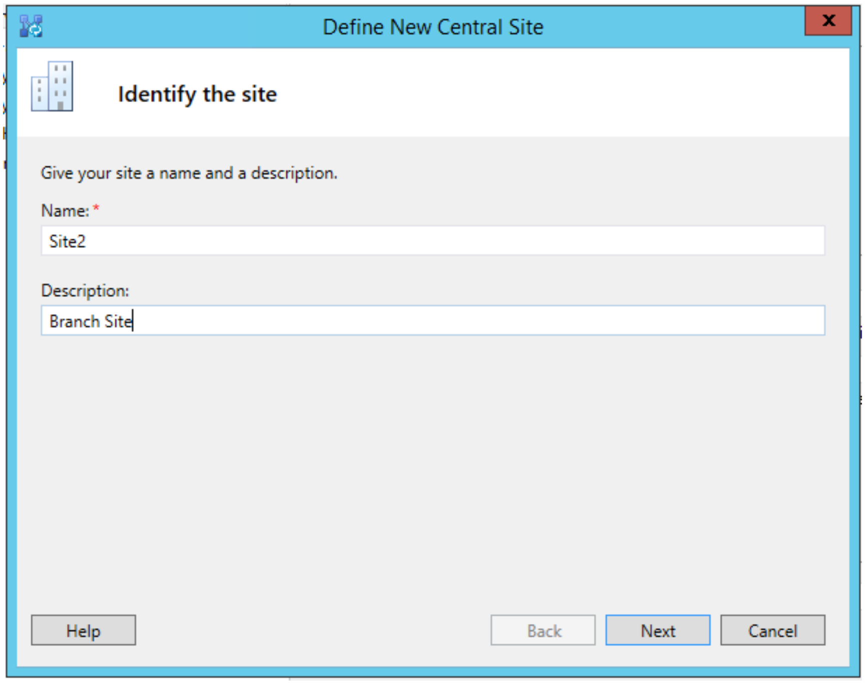
Simple URL: https://meet.ac-onebox.com/meet

Administrative access URL: *Not configured*

Central Management Server: Front End UC-FE.ac-onebox.com, Site ACS-2013

2. Give the new site a name (and optionally a description).

Figure 11-47: Defining a Central Site



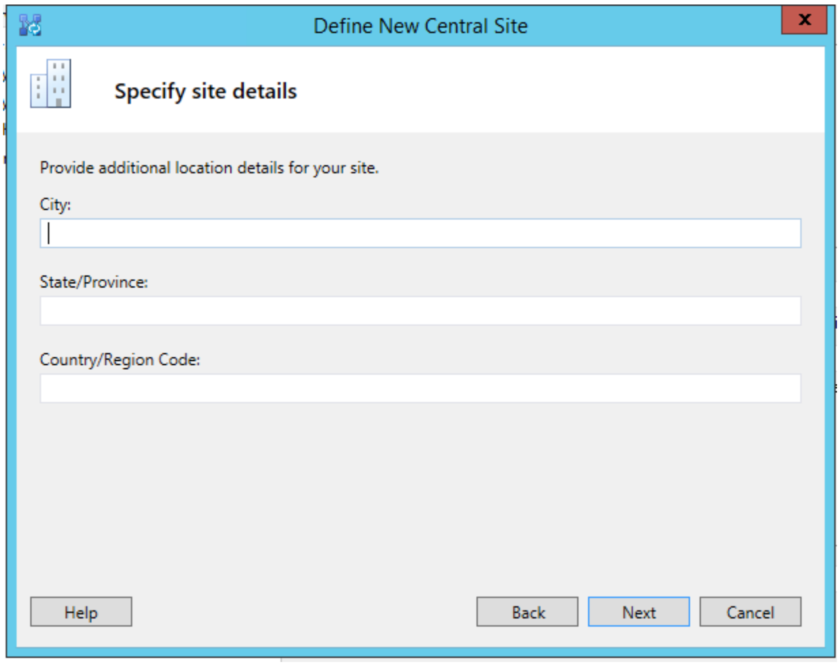
Give your site a name and a description.

Name:* Site2

Description: Branch Site

3. Enter the City, State/Province and Country/Region Code details.

Figure 11-48: Defining a Central Site



Define New Central Site

Specify site details

Provide additional location details for your site.

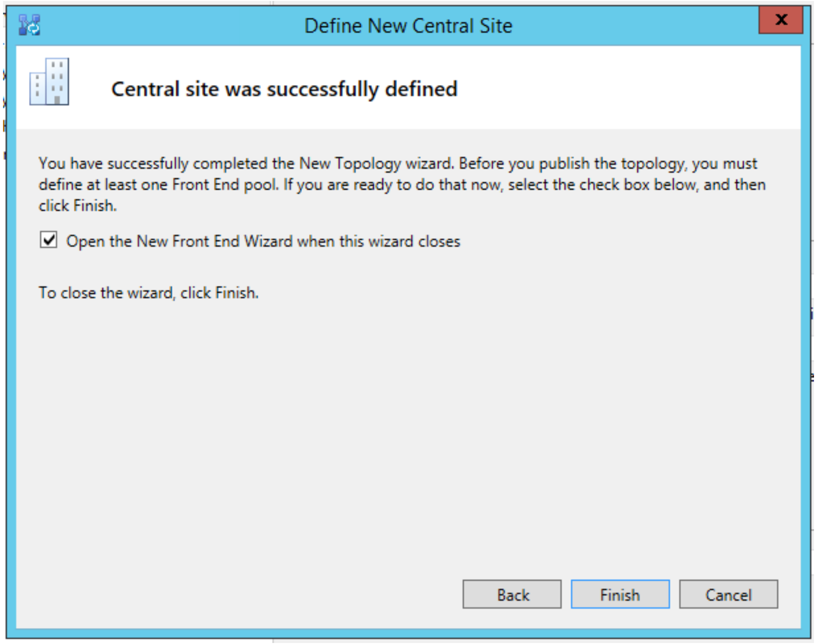
City:

State/Province:

Country/Region Code:

4. Leave the **Open the New Front End Wizard….** check-box selected and then click **Finish**.

Figure 11-49: Defining a Central Site



Define New Central Site

Central site was successfully defined

You have successfully completed the New Topology wizard. Before you publish the topology, you must define at least one Front End pool. If you are ready to do that now, select the check box below, and then click Finish.

☑ Open the New Front End Wizard when this wizard closes

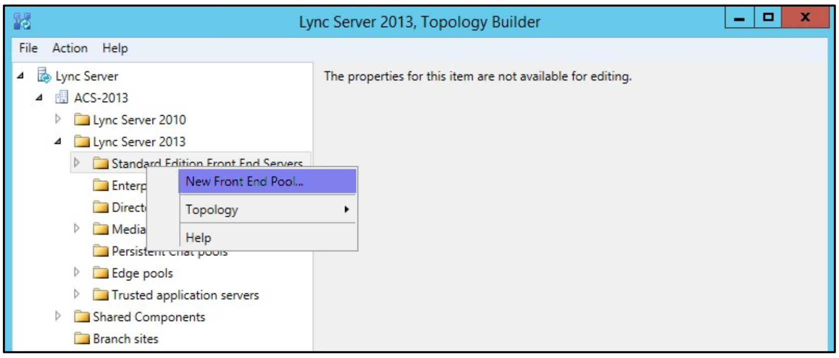
To close the wizard, click Finish.

11.9.2.3 Adding a New Front-End Server

You must add a new Front-End server to the existing topology. As CloudBond 365 uses Skype for Business Standard Edition FE Servers, this means adding a new FE Pool to a site.

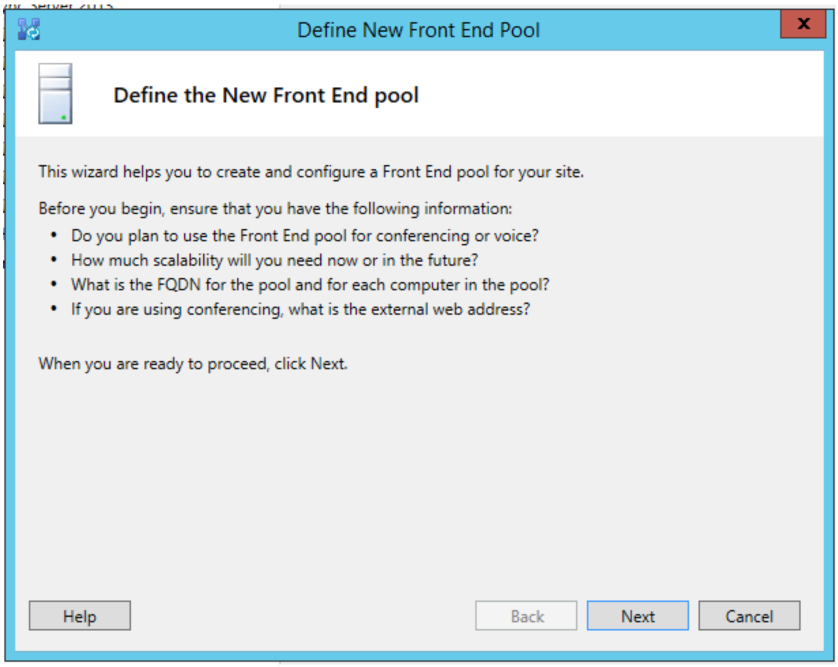
If you did not define a new site, you can add a new FE Pool by navigating to the server (**Skype for Business Server 2015/Lync Server 2013)** → **Standard Edition Front End Servers** within an existing site, right clicking, and selecting **New Front End Pool**.

Figure 11-50: Creating New FE Pool



The properties for this item are not available for editing.

Figure 11-51: Creating New FE Pool



Define the New Front End pool

This wizard helps you to create and configure a Front End pool for your site.

Before you begin, ensure that you have the following information:

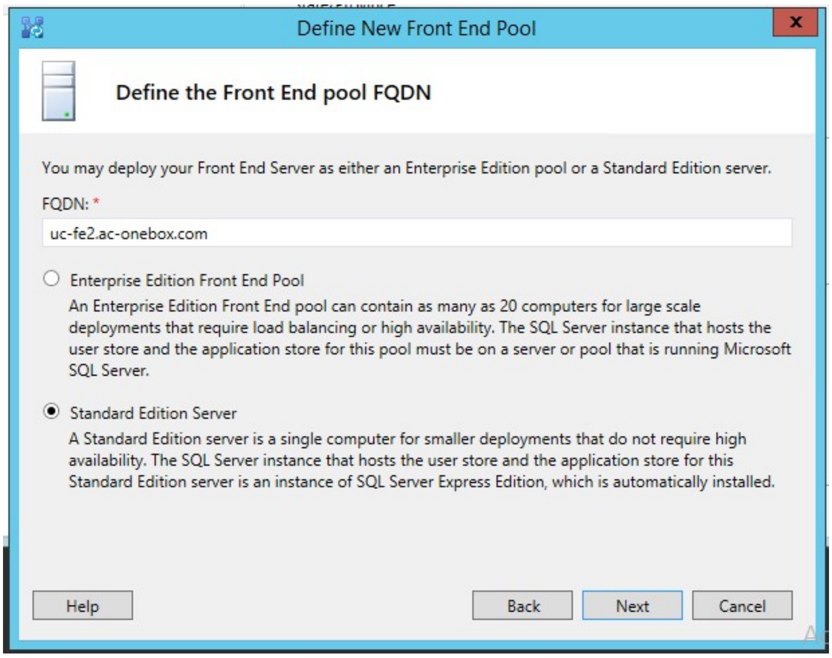
- Do you plan to use the Front End pool for conferencing or voice?
- How much scalability will you need now or in the future?
- What is the FQDN for the pool and for each computer in the pool?
- If you are using conferencing, what is the external web address?

When you are ready to proceed, click Next.

➢ To define the new FE server:

1. Define a new front-end server FQDN (example: uc-fe2.ac-onebox.com).
2. Make sure that the **Standard Edition Server** option is selected.

Figure 11-52: FE Server FQDN



Define New Front End Pool

Define the Front End pool FQDN

You may deploy your Front End Server as either an Enterprise Edition pool or a Standard Edition server.

FQDN: *

uc-fe2.ac-onebox.com

○ Enterprise Edition Front End Pool

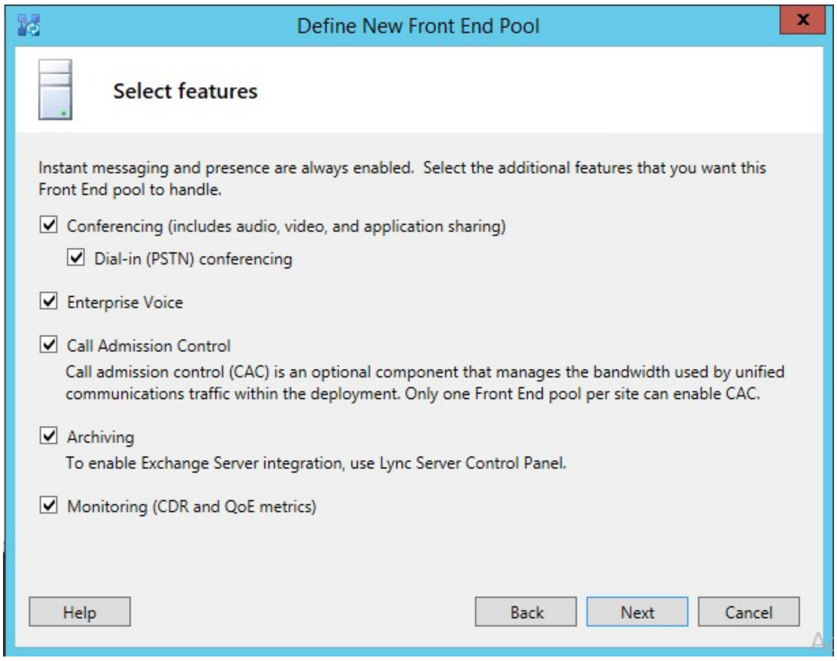
An Enterprise Edition Front End pool can contain as many as 20 computers for large scale deployments that require load balancing or high availability. The SQL Server instance that hosts the user store and the application store for this pool must be on a server or pool that is running Microsoft SQL Server.

● Standard Edition Server

A Standard Edition server is a single computer for smaller deployments that do not require high availability. The SQL Server instance that hosts the user store and the application store for this Standard Edition server is an instance of SQL Server Express Edition, which is automatically installed.

3. Select the features you want to use on this Front-End Server (we usually select all. Call Admission Control requires separate sites).

Figure 11-53: FE Server Features



Define New Front End Pool

Select features

Instant messaging and presence are always enabled. Select the additional features that you want this Front End pool to handle.

☑ Conferencing (includes audio, video, and application sharing)

☑ Dial-in (PSTN) conferencing

☑ Enterprise Voice

☑ Call Admission Control

Call admission control (CAC) is an optional component that manages the bandwidth used by unified communications traffic within the deployment. Only one Front End pool per site can enable CAC.

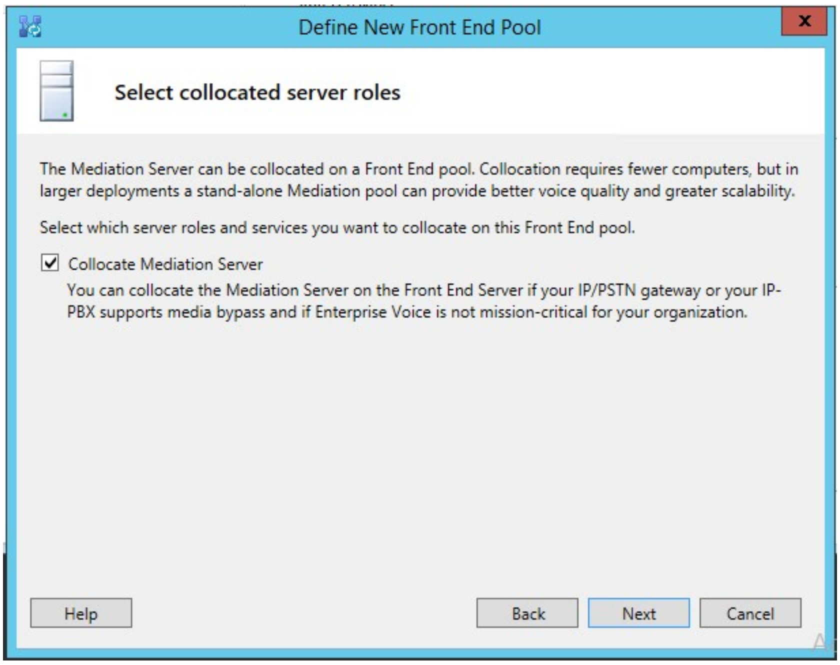
☑ Archiving

To enable Exchange Server integration, use Lync Server Control Panel.

☑ Monitoring (CDR and QoE metrics)

4. Leave the ‘Collocate Mediation Server’ check box enabled.

Figure 11-54: FE and Mediation Server



Select collocated server roles

The Mediation Server can be collocated on a Front End pool. Collocation requires fewer computers, but in larger deployments a stand-alone Mediation pool can provide better voice quality and greater scalability.

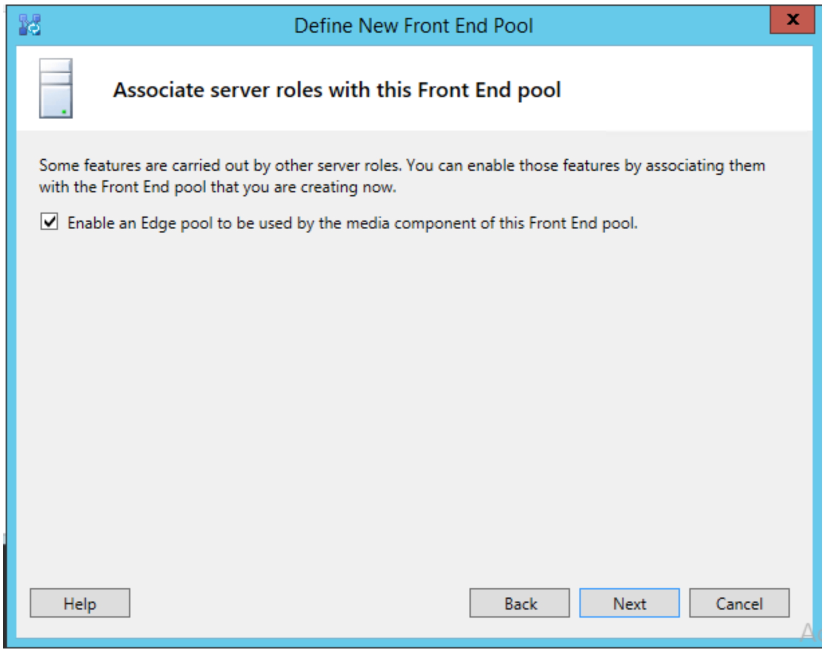
Select which server roles and services you want to collocate on this Front End pool.

☑ Collocate Mediation Server

You can collocate the Mediation Server on the Front End Server if your IP/PSTN gateway or your IP-PBX supports media bypass and if Enterprise Voice is not mission-critical for your organization.

5. Leave the ‘Enable and Edge pool to be used…’ check box enabled.

Figure 11-55: FE and Edge



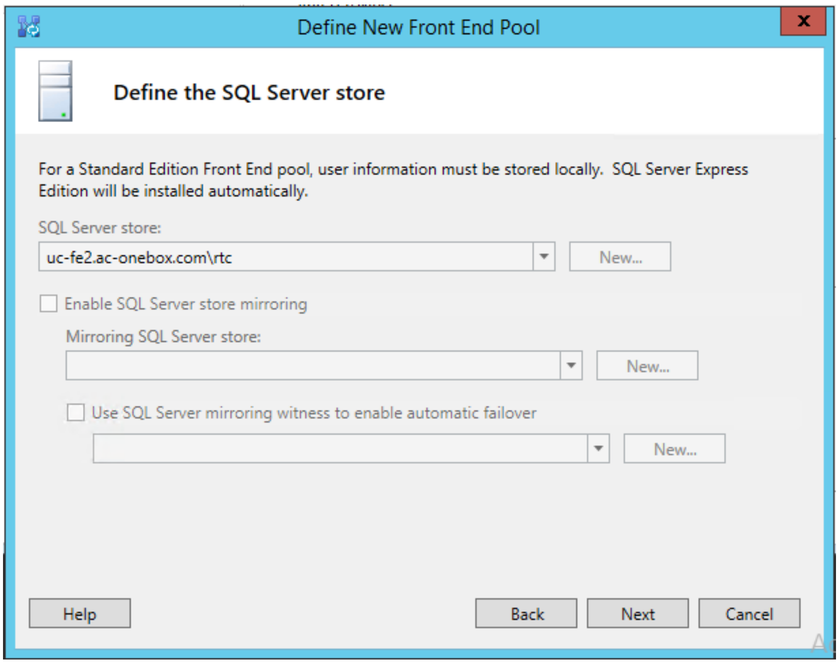
Associate server roles with this Front End pool

Some features are carried out by other server roles. You can enable those features by associating them with the Front End pool that you are creating now.

☑ Enable an Edge pool to be used by the media component of this Front End pool.

6. Leave the SQL Server store page as it is (it cannot be edited anyway).

Figure 11-56: FE SQL Store



Define New Front End Pool

Define the SQL Server store

For a Standard Edition Front End pool, user information must be stored locally. SQL Server Express Edition will be installed automatically.

SQL Server store: uc-fe2.ac-onebox.com\rtc

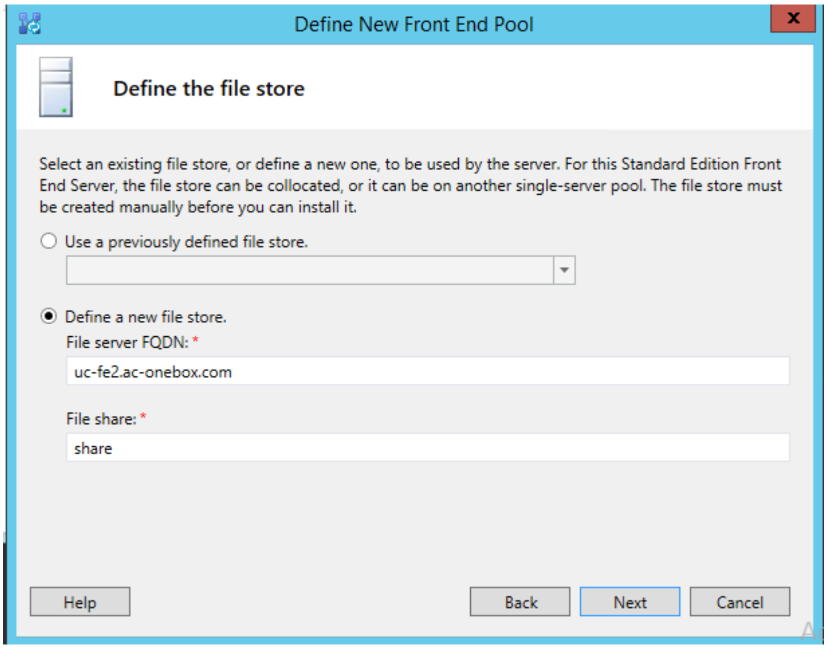
□ Enable SQL Server store mirroring

Mirroring SQL Server store:

□ Use SQL Server mirroring witness to enable automatic failover

7. Leave the file store on default settings.

Figure 11-57: FE Local Store



Define New Front End Pool

Define the file store

Select an existing file store, or define a new one, to be used by the server. For this Standard Edition Front End Server, the file store can be collocated, or it can be on another single-server pool. The file store must be created manually before you can install it.

○ Use a previously defined file store.

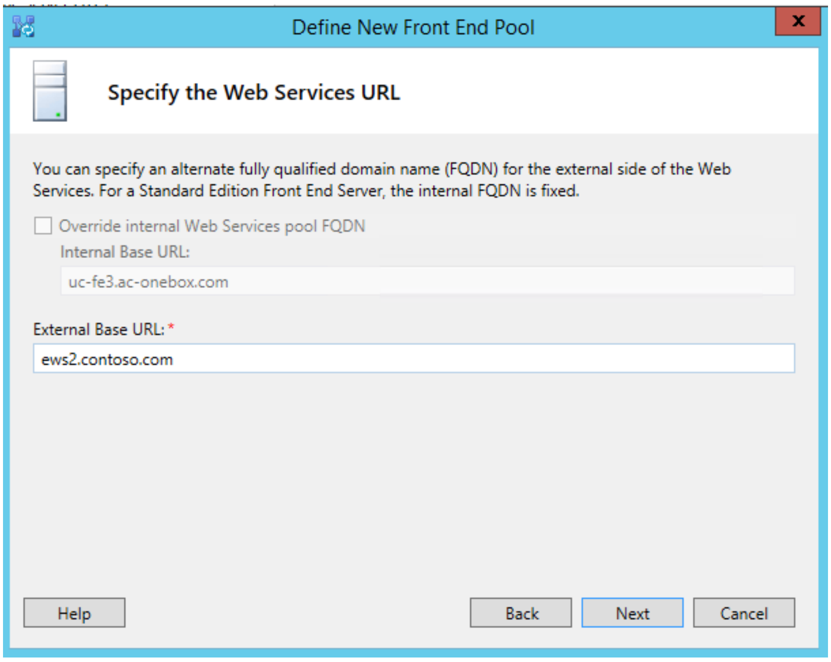
● Define a new file store.

File server FQDN: * uc-fe2.ac-onebox.com

File share: * share

8. Define an 'External Base URL' (example: ews2.contoso.com).

Figure 11-58: FE External Web Access



Define New Front End Pool

Specify the Web Services URL

You can specify an alternate fully qualified domain name (FQDN) for the external side of the Web Services. For a Standard Edition Front End Server, the internal FQDN is fixed.

□ Override internal Web Services pool FQDN

Internal Base URL:

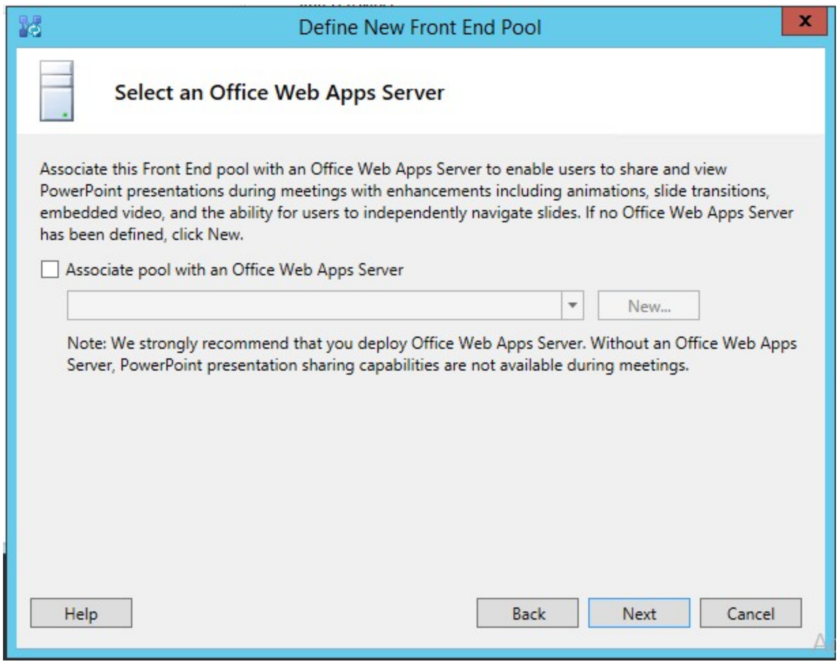
uc-fe3.ac-onebox.com

External Base URL: *

ews2.contoso.com

9. Clear the 'Associate pool with an Office Web Apps Server' check box.

Figure 11-59: FE OWA server



Define New Front End Pool

Select an Office Web Apps Server

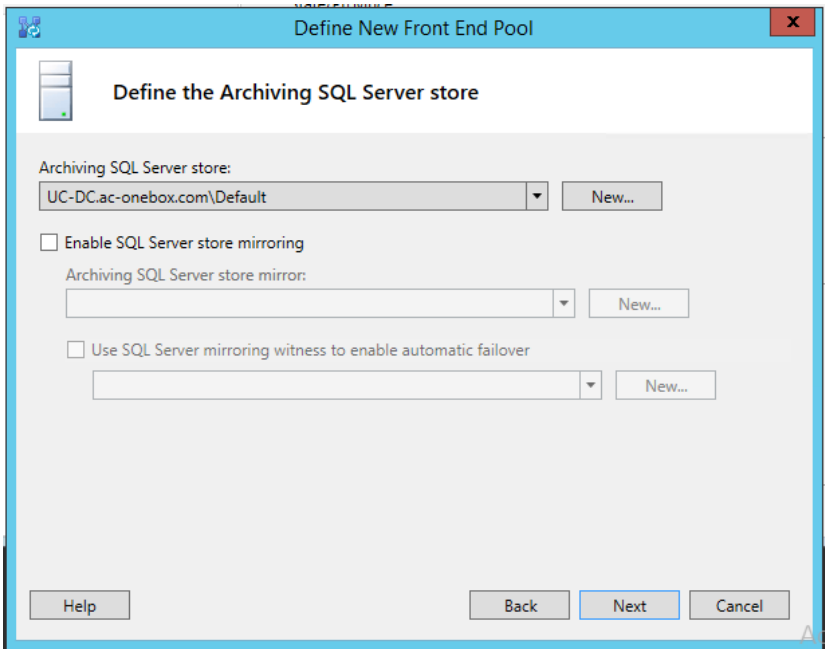
Associate this Front End pool with an Office Web Apps Server to enable users to share and view PowerPoint presentations during meetings with enhancements including animations, slide transitions, embedded video, and the ability for users to independently navigate slides. If no Office Web Apps Server has been defined, click New.

□ Associate pool with an Office Web Apps Server

Note: We strongly recommend that you deploy Office Web Apps Server. Without an Office Web Apps Server, PowerPoint presentation sharing capabilities are not available during meetings.

10. Either use the Archiving SQL Store already defined or define a new one (we usually use the existing one).

Figure 11-60: Archiving SQL Server



Define New Front End Pool

Define the Archiving SQL Server store

Archiving SQL Server store: UC-DC.ac-onebox.com\Default

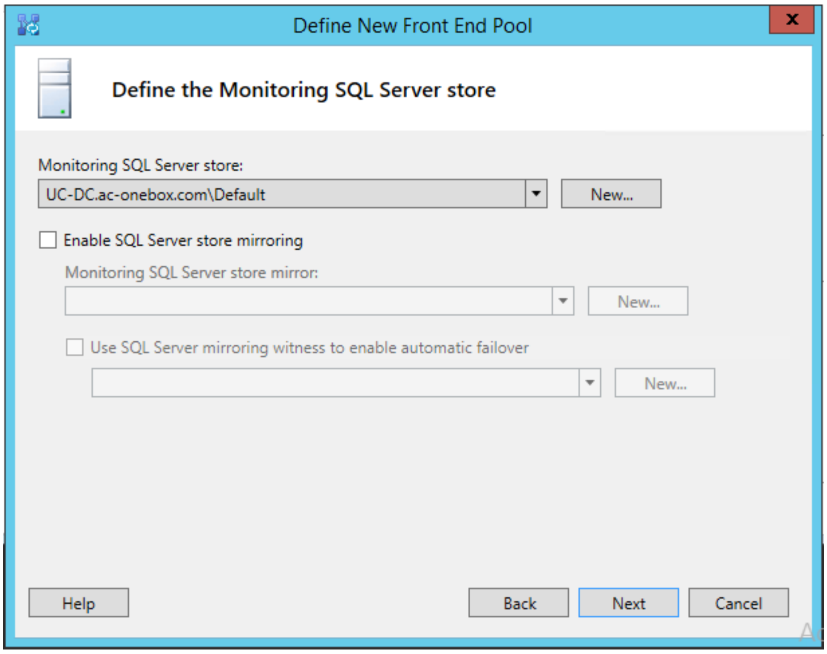
☐ Enable SQL Server store mirroring

Archiving SQL Server store mirror:

☐ Use SQL Server mirroring witness to enable automatic failover

11. Same for the Monitoring SQL Server Store.

Figure 11-61: Monitoring SQL Server



Define New Front End Pool

Define the Monitoring SQL Server store

Monitoring SQL Server store: UC-DC.ac-onebox.com\Default

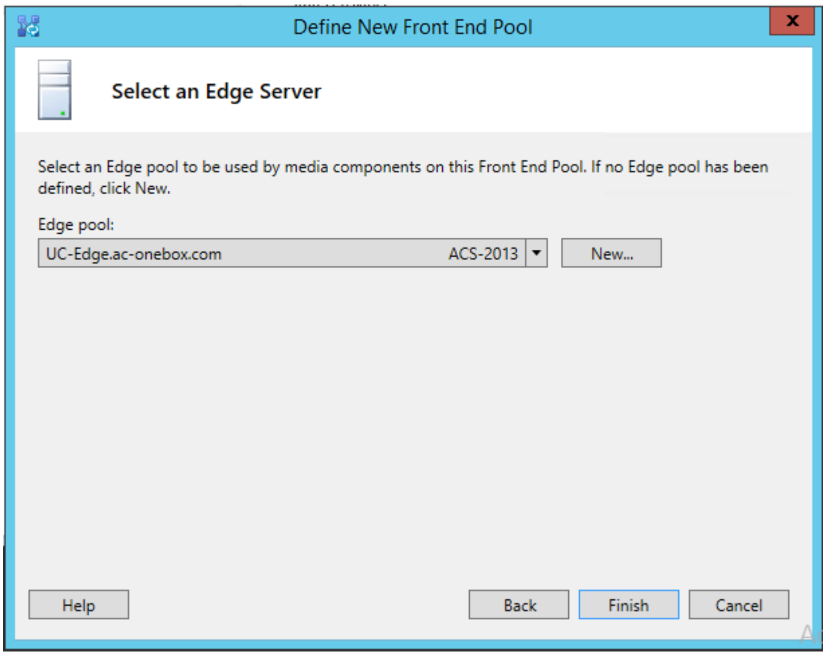
☐ Enable SQL Server store mirroring

Monitoring SQL Server store mirror:

☐ Use SQL Server mirroring witness to enable automatic failover

12. Select the Edge pool to be used (Select the existing Edge Server, or click **New** to start the wizard for defining a new Edge Server).

Figure 11-62: Assigning Edge to FE



Define New Front End Pool

Select an Edge Server

Select an Edge pool to be used by media components on this Front End Pool. If no Edge pool has been defined, click New.

Edge pool: UC-Edge.ac-onebox.com ACS-2013

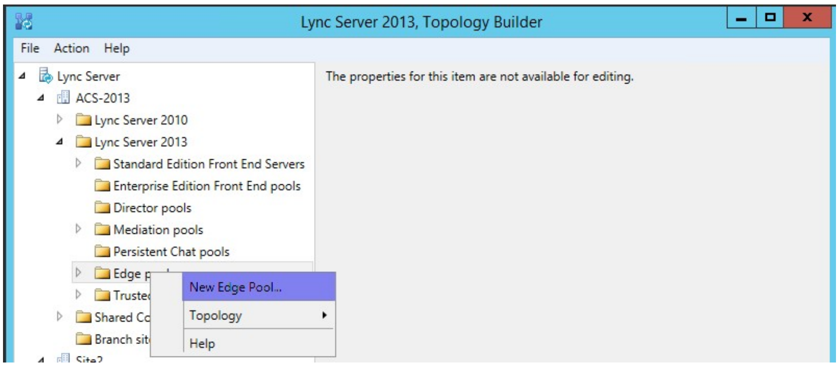
13. Click **Finish**.

11.9.3 Defining an Edge Server

You can optionally add a new Edge server to the existing topology.

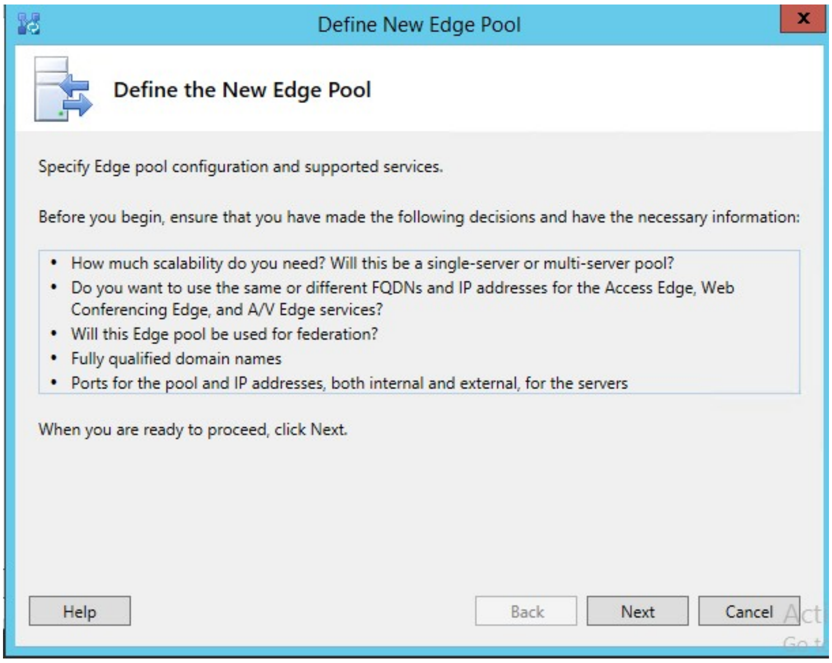
If you did not define a new Edge Pool when defining the FE Server, you can add a new Edge Pool by navigating to the server (**Skype for Business Server 2015**/**Lync Server 2013**)> **Edge Pools** within an existing site, right clicking, and selecting **New Edge Pool**.

Figure 11-63: Defining a New Edge Pool



The properties for this item are not available for editing.

Figure 11-64: Defining a New Edge Pool



Define the New Edge Pool

Specify Edge pool configuration and supported services.

Before you begin, ensure that you have made the following decisions and have the necessary information:

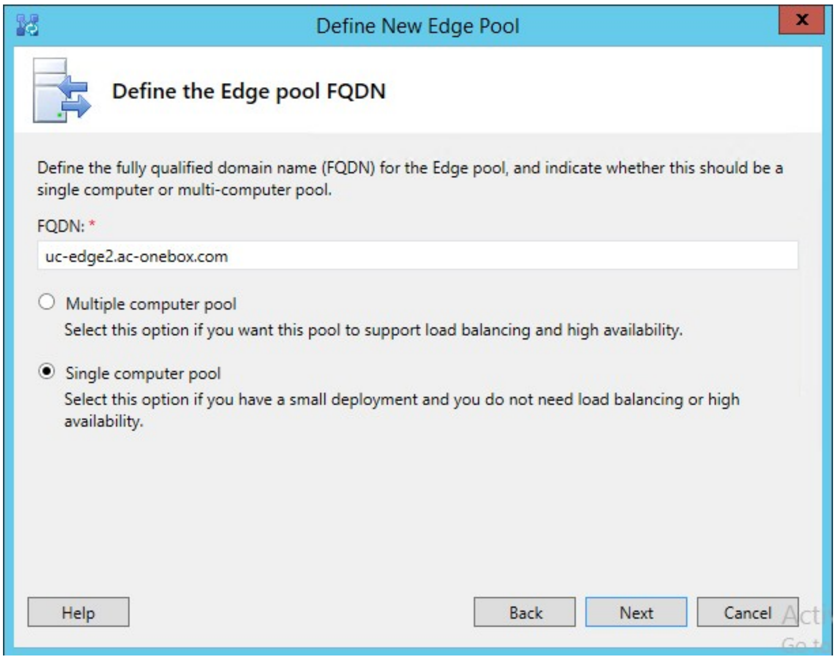
- How much scalability do you need? Will this be a single-server or multi-server pool?
- Do you want to use the same or different FQDNs and IP addresses for the Access Edge, Web Conferencing Edge, and A/V Edge services?
- Will this Edge pool be used for federation?
- Fully qualified domain names
- Ports for the pool and IP addresses, both internal and external, for the servers

When you are ready to proceed, click Next.

➢ To define the New Edge Server:

1. Specify the Edge server internal FQDN.

Figure 11-65: Define Edge Internal FQDN



Define New Edge Pool

Define the Edge pool FQDN

Define the fully qualified domain name (FQDN) for the Edge pool, and indicate whether this should be a single computer or multi-computer pool.

FQDN: *

uc-edge2.ac-onebox.com

○ Multiple computer pool

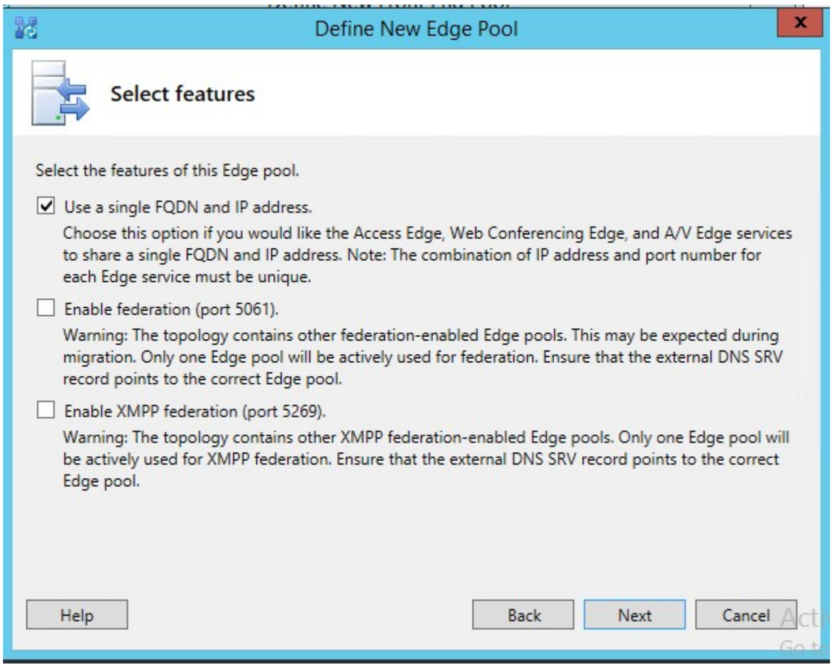
Select this option if you want this pool to support load balancing and high availability.

● Single computer pool

Select this option if you have a small deployment and you do not need load balancing or high availability.

2. Select the features required.

Figure 11-66: Select Edge Features



Define New Edge Pool

Select features

Select the features of this Edge pool.

☑ Use a single FQDN and IP address.

Choose this option if you would like the Access Edge, Web Conferencing Edge, and A/V Edge services to share a single FQDN and IP address. Note: The combination of IP address and port number for each Edge service must be unique.

☐ Enable federation (port 5061).

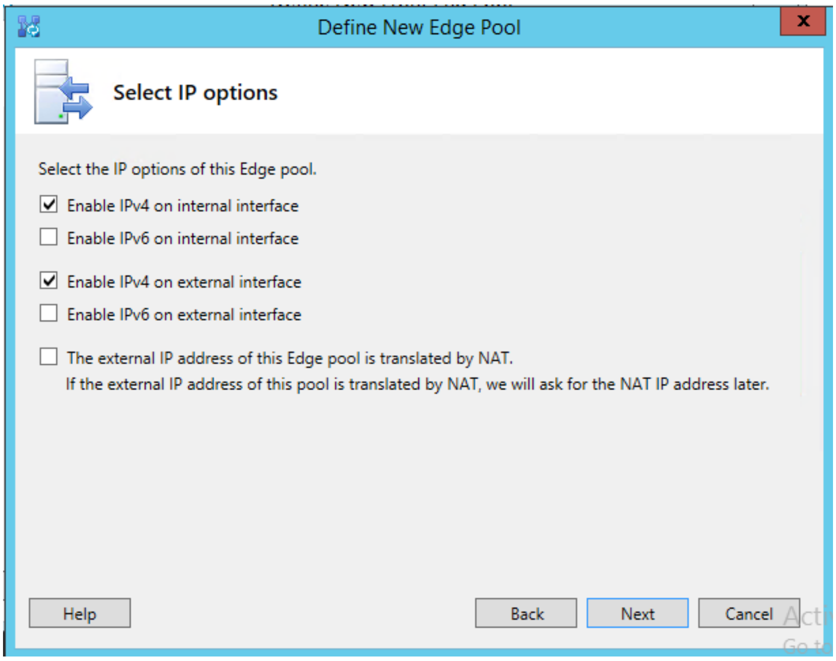
Warning: The topology contains other federation-enabled Edge pools. This may be expected during migration. Only one Edge pool will be actively used for federation. Ensure that the external DNS SRV record points to the correct Edge pool.

☐ Enable XMPP federation (port 5269).

Warning: The topology contains other XMPP federation-enabled Edge pools. Only one Edge pool will be actively used for XMPP federation. Ensure that the external DNS SRV record points to the correct Edge pool.

3. Select the IP Options required.

Figure 11-67: Select Edge IP options



Select IP options

Select the IP options of this Edge pool.

☑ Enable IPv4 on internal interface

□ Enable IPv6 on internal interface

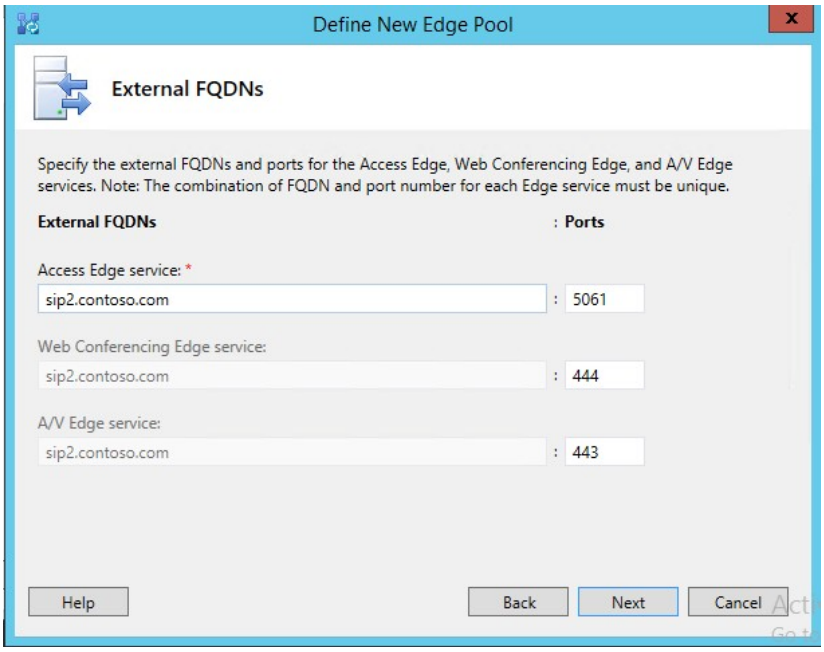
☑ Enable IPv4 on external interface

□ Enable IPv6 on external interface

□ The external IP address of this Edge pool is translated by NAT.
If the external IP address of this pool is translated by NAT, we will ask for the NAT IP address later.

4. Specify the External FQDN.

Figure 11-68: Define Edge External FQDN



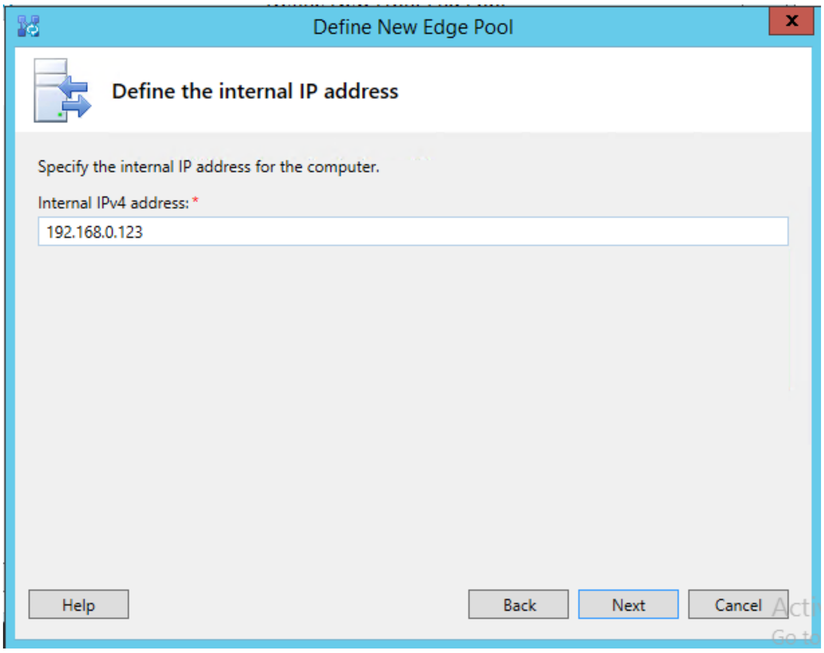
External FQDNs

Specify the external FQDNs and ports for the Access Edge, Web Conferencing Edge, and A/V Edge services. Note: The combination of FQDN and port number for each Edge service must be unique.

External FQDNs	: Ports
Access Edge service: * sip2.contoso.com	5061
Web Conferencing Edge service: sip2.contoso.com	444
A/V Edge service: sip2.contoso.com	443

5. Specify the internal IP address.

Figure 11-69: Define Edge Internal IP address



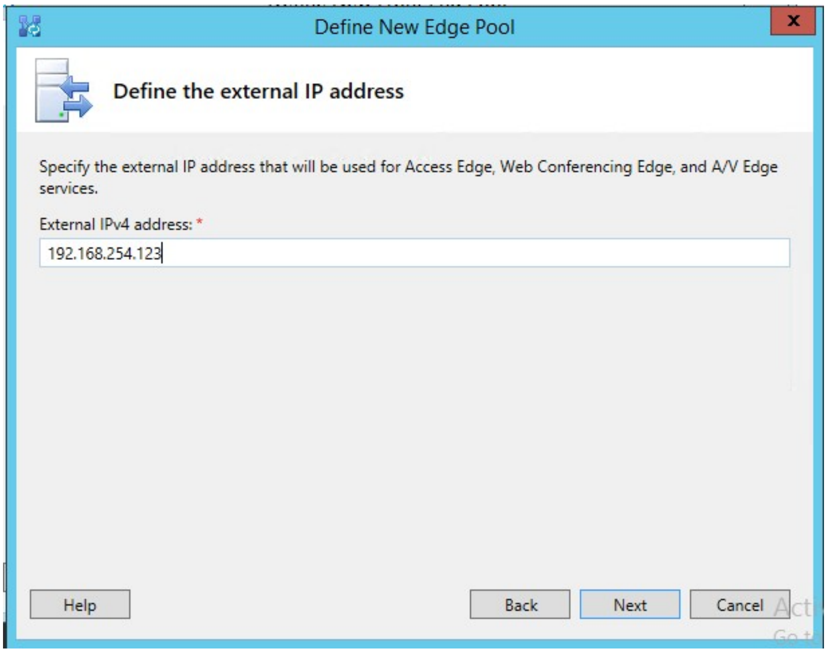
Specify the internal IP address for the computer.

Internal IPv4 address: *

192.168.0.123

6. Specify the external IP address.

Figure 11-70: Define Edge external IP address



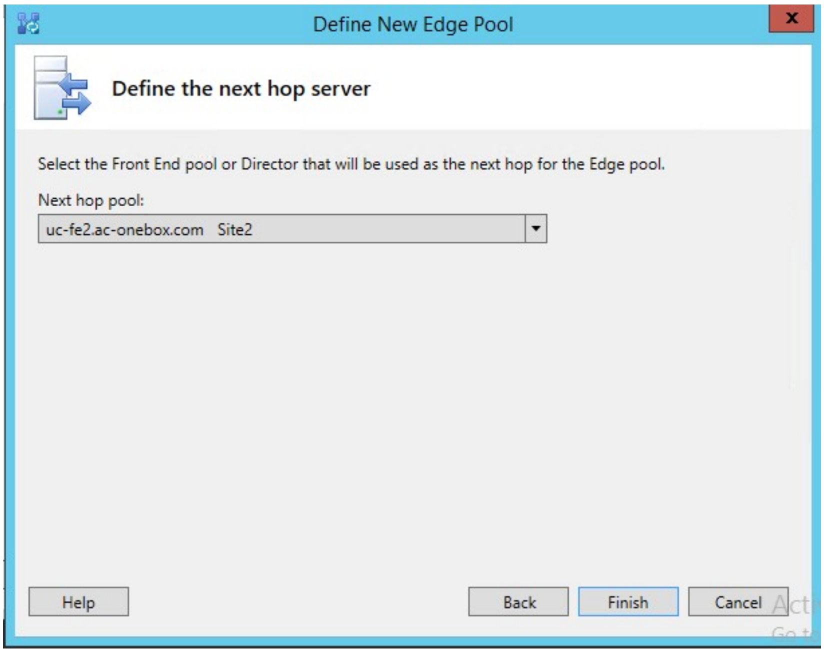
Specify the external IP address that will be used for Access Edge, Web Conferencing Edge, and A/V Edge services.

External IPv4 address: *

192.168.254.123

7. Specify the FE pool for this Edge server.

Figure 11-71: Specify the Associated FE Server



Define New Edge Pool

Define the next hop server

Select the Front End pool or Director that will be used as the next hop for the Edge pool.

Next hop pool: uc-fe2.ac-onebox.com Site2

8. Click **Finish**.

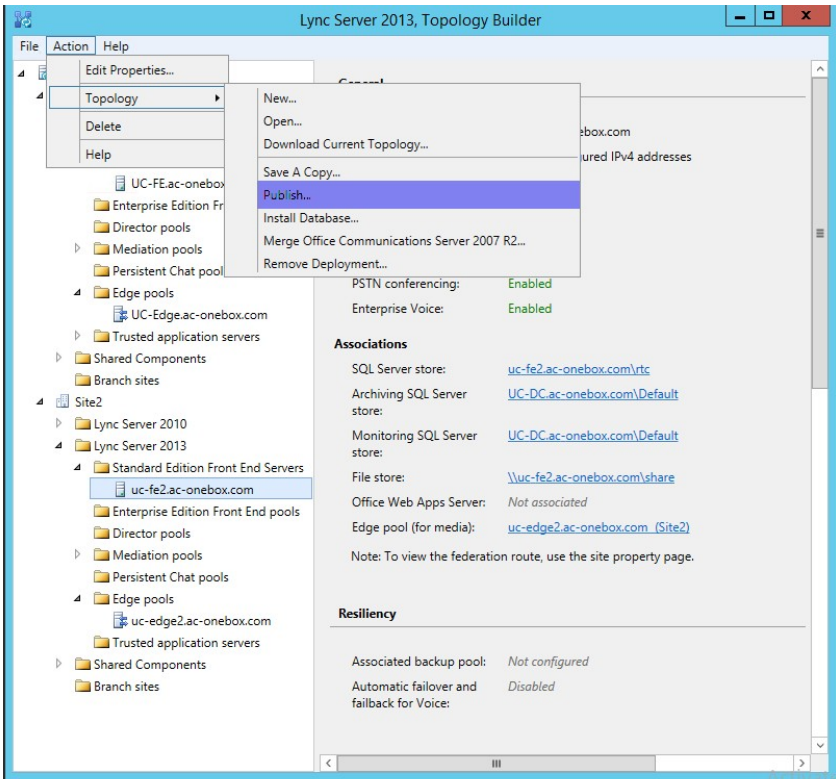
Note: To prevent complex networking scenarios during installation, the wizard only allows for a single public edge IP Address and requires the Edge internal leg to be on the same subnet as the other servers installed. If different deployment scenarios are needed, it is just a small change to be made in Skype for Business Topology Builder after the installation wizard has finished.

For more information see Section 17.5.1.4, Chapter 14 and Chapter 17.

11.9.3.1 Publish the Topology

1. Click **Action** at the top of Topology Builder.
2. Open the **Topology** sub-menu.
3. Click **Publish,** and then click **Next** in the wizard that pops up.

Figure 11-72: Publish the Topology



ebox.com
ured IPv4 addresses

PSTN conferencing: Enabled
Enterprise Voice: Enabled

Associations

SQL Server store: uc-fe2.ac-onebox.com\rtc
Archiving SQL Server store: UC-DC.ac-onebox.com\Default
Monitoring SQL Server store: UC-DC.ac-onebox.com\Default
File store: \\uc-fe2.ac-onebox.com\share
Office Web Apps Server: Not associated
Edge pool (for media): uc-edge2.ac-onebox.com (Site2)

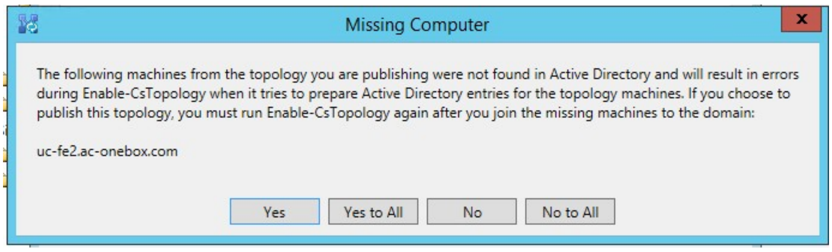
Note: To view the federation route, use the site property page.

Resiliency

Associated backup pool: Not configured
Automatic failover and failback for Voice: Disabled

4. You will receive a warning that the machine(s) you just defined cannot be found in Active Directory, Click **Yes to All**.

Figure 11-73: Warning - Servers do not Exist



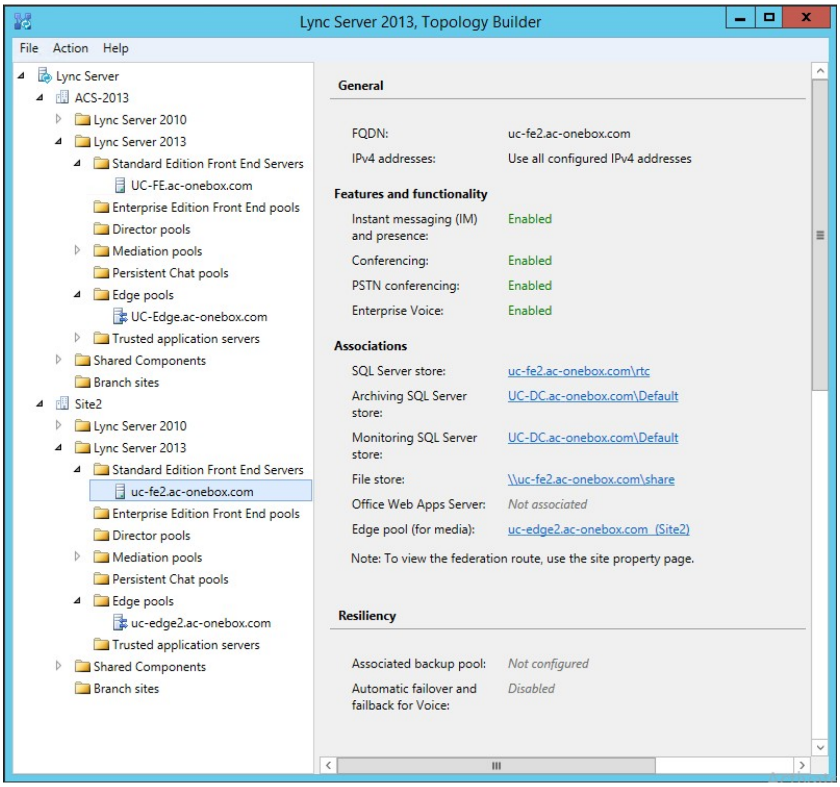
The following machines from the topology you are publishing were not found in Active Directory and will result in errors during Enable-CsTopology when it tries to prepare Active Directory entries for the topology machines. If you choose to publish this topology, you must run Enable-CsTopology again after you join the missing machines to the domain:

uc-fe2.ac-onebox.com

5. During ‘Enabling topology’ it will encounter errors, the summary screen will show status: Completed with warnings.
6. If you view logs for publishing you will find that the warning generated comes from the fact that the machines do not exist yet. This warning can be safely ignored.

7. Click **Finish**; You now have a second Central Site defined in your topology and are ready to export the file.

Figure 11-74: Finished Topology Changes



Lync Server 2013, Topology Builder

- Lync Server
  - ACS-2013
    - Lync Server 2010
    - Lync Server 2013
      - Standard Edition Front End Servers
        - UC-FE.ac-onebox.com
      - Enterprise Edition Front End pools
      - Director pools
      - Mediation pools
      - Persistent Chat pools
      - Edge pools
        - UC-Edge.ac-onebox.com
      - Trusted application servers
    - Shared Components
    - Branch sites
  - Site2
    - Lync Server 2010
    - Lync Server 2013
      - Standard Edition Front End Servers
        - uc-fe2.ac-onebox.com
      - Enterprise Edition Front End pools
      - Director pools
      - Mediation pools
      - Persistent Chat pools
      - Edge pools
        - uc-edge2.ac-onebox.com
      - Trusted application servers
    - Shared Components
    - Branch sites

General

FQDN: uc-fe2.ac-onebox.com
IPv4 addresses: Use all configured IPv4 addresses

Features and functionality

Instant messaging (IM) and presence: Enabled
Conferencing: Enabled
PSTN conferencing: Enabled
Enterprise Voice: Enabled

Associations

SQL Server store: uc-fe2.ac-onebox.com\rtc
Archiving SQL Server store: UC-DC.ac-onebox.com\Default
Monitoring SQL Server store: UC-DC.ac-onebox.com\Default
File store: \\uc-fe2.ac-onebox.com\share
Office Web Apps Server: *Not associated*
Edge pool (for media): uc-edge2.ac-onebox.com (Site2)

Note: To view the federation route, use the site property page.

Resiliency

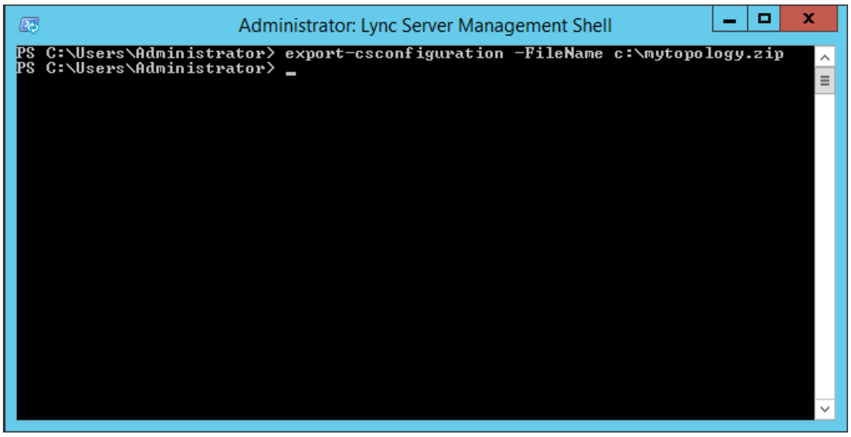
Associated backup pool: *Not configured*
Automatic failover and failback for Voice: *Disabled*

11.9.4 Exporting the Topology

➢ To prepare the Topology file:

1. Log on to the existing CloudBond 365 Controller (or Skype for Business FE Server).
2. Open the Skype for Business Management Shell.
3. Enter the command Export-CsConfiguration –Filename c:\mytopology.zip.
4. Copy the mytopology.zip file to a convenient location on the new host operating system.

Figure 11-75: Exporting the Topology



Administrator: Lync Server Management Shell

```
PS C:\Users\Administrator> export-csconfiguration -FileName c:\mytopology.zip
PS C:\Users\Administrator> _
```

11.9.5 Commencing the BPA Configuration

To commence the remaining installation steps, mount the ISO image from the Recovery partition, and start the Configuration Wizard as described in Section 11.6 on page 119.

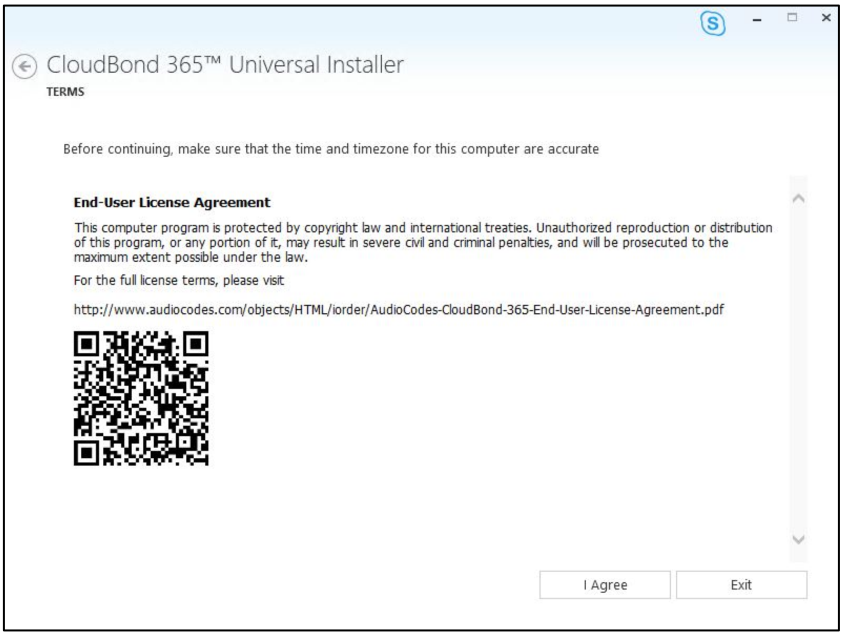
Ensure that there is network connectivity between the new BPA Hardware, and the existing CloudBond 365 servers.

11.9.6 License Agreement

If you are running the Configuration Wizard for the first time, or an existing configuration file is not found, a license agreement page is presented. You must agree to the license terms before proceeding with the software installation.

This page offers a short copy write text, a link to the full license agreement, and a QR code which contains said link. Click I Agree to continue setup, or Exit to abort.

Figure 11-76: License Agreement



Before continuing, make sure that the time and timezone for this computer are accurate

End-User License Agreement

This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

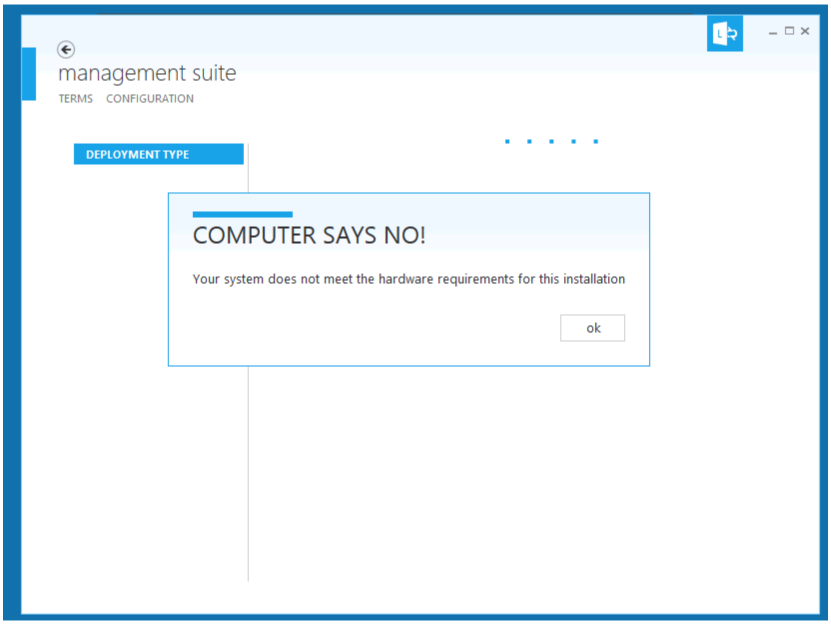
For the full license terms, please visit

http://www.audiocodes.com/objects/HTML/iorder/AudioCodes-CloudBond-365-End-User-License-Agreement.pdf

11.9.7 Hardware Check

The Configuration Wizard will first verify the hardware platform that it is running on. The hardware detected will influence the options presented within the Configuration Wizard. When the system running the setup does not meet the hardware requirements, the following message is shown.

Figure 11-77: Hardware Check



COMPUTER SAYS NO!

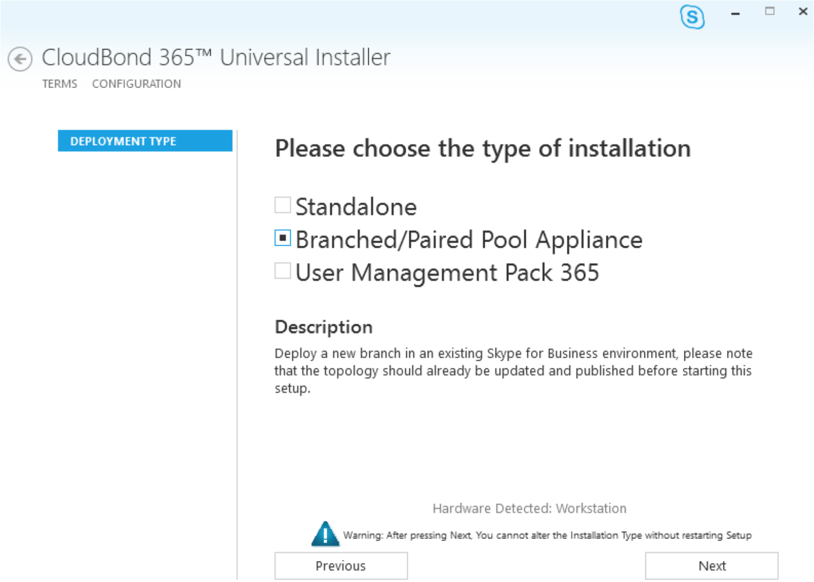
Your system does not meet the hardware requirements for this installation

11.9.8 Deployment Type

You must choose the Branch / Paired Pool Appliance (BPA) Deployment Type. This page also shows which hardware level was detected.

Once a Deployment Type is chosen, it is not possible to change the Deployment Type without restarting the Configuration Wizard.

Figure 11-78: Deployment Type



Please choose the type of installation

□ Standalone
☑ Branched/Paired Pool Appliance
□ User Management Pack 365

Description

Deploy a new branch in an existing Skype for Business environment, please note that the topology should already be updated and published before starting this setup.

Hardware Detected: Workstation

Warning: After pressing Next, You cannot alter the Installation Type without restarting Setup

11.9.9 Deployment Model

There are currently three Deployment Models on the Configuration Wizard to choose from:

- Virtual Edition
- Hyper-V Host with Virtual Machines
- Co-Located Hyper-V / Domain Controller with Virtual Machines

Notes:

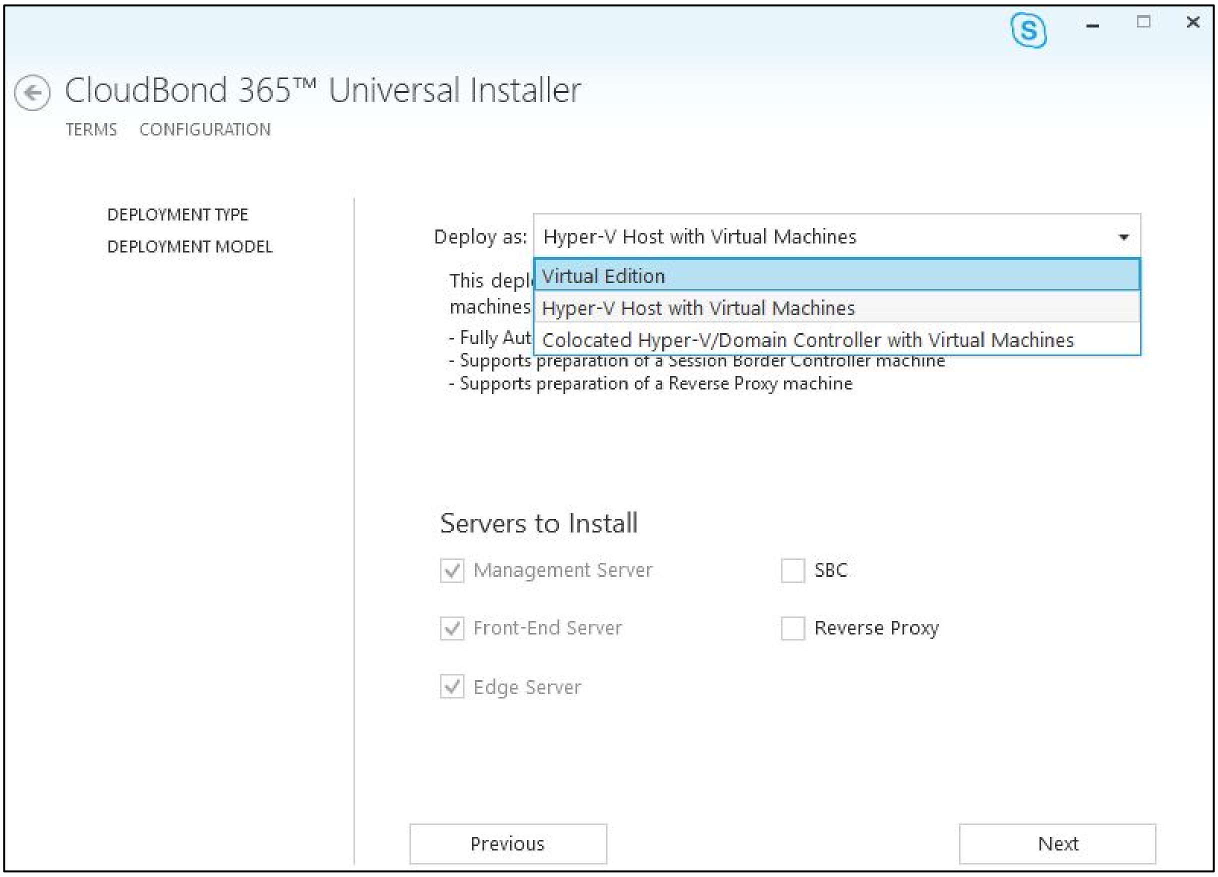
- The hardware detected by the Configuration Wizard determines which Deployment Models are available. For example, on a Mediant 800 OSN with 16/32GB RAM, only the Co-Located Hyper-V / Domain Controller with Virtual Machines is offered.
- The optional SBC and RP are unavailable on CloudBond 365 Standard Box Edition hardware.

11.9.9.1 Virtual Edition

The Virtual Edition allows you to install the CloudBond 365 application onto your own (virtual) hardware. This installation should be started three times on individual Windows Server 2012 R2 Operating System environments, in the following order:

- On the server that will be hosting the CloudBond 365 management server
- On the server that will be hosting the CloudBond 365 FrontEnd server
- On the server that will be hosting the CloudBond 365 Edge server

Figure 11-36: Deployment Model – Virtual Edition



CloudBond 365™ Universal Installer

TERMS CONFIGURATION

DEPLOYMENT TYPE

DEPLOYMENT MODEL

Deploy as: Hyper-V Host with Virtual Machines

- Virtual Edition
- Hyper-V Host with Virtual Machines
- Colocated Hyper-V/Domain Controller with Virtual Machines

This depl
machines
- Fully Aut
- Supports preparation of a Session Border Controller machine
- Supports preparation of a Reverse Proxy machine

Servers to Install

☑ Management Server ☐ SBC

☑ Front-End Server ☐ Reverse Proxy

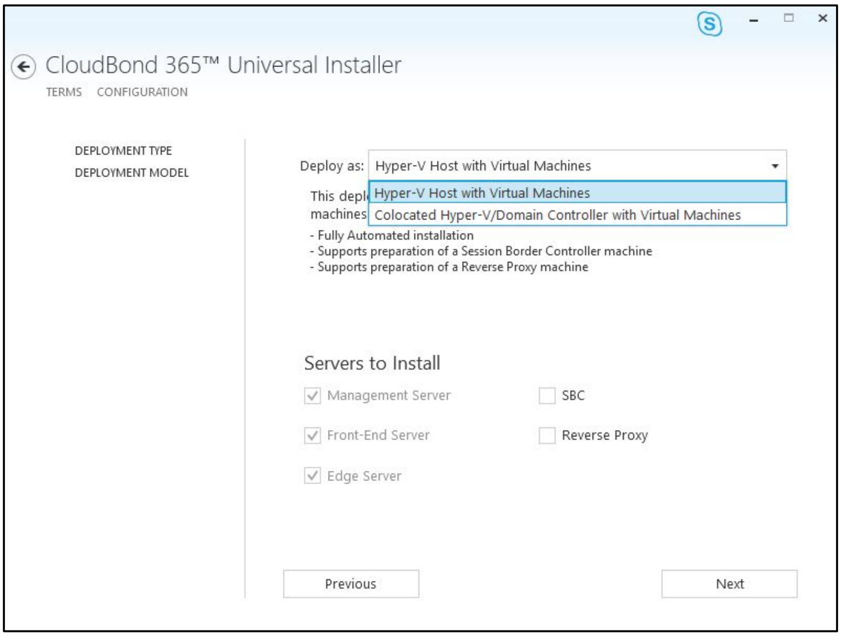
☑ Edge Server

11.9.9.2 Hyper-V Host with Virtual Machines

The Hyper-V Host with Virtual Machines installs Hyper-V on the selected host machine, and the three CloudBond 365 Servers (Controller, FE, and optional Edge) as three separate virtual machines within Hyper-V.

This option is suitable for CloudBond 365 Pro, and CloudBond 365 Enterprise. (e.g. AudioCodes HP Servers).

Figure 11-79: Deployment Model - Pro and Enterprise



CloudBond 365™ Universal Installer

TERMS CONFIGURATION

DEPLOYMENT TYPE
DEPLOYMENT MODEL

Deploy as: Hyper-V Host with Virtual Machines

Hyper-V Host with Virtual Machines
Colocated Hyper-V/Domain Controller with Virtual Machines

This depl[...]
machines

- Fully Automated installation
- Supports preparation of a Session Border Controller machine
- Supports preparation of a Reverse Proxy machine

Servers to Install

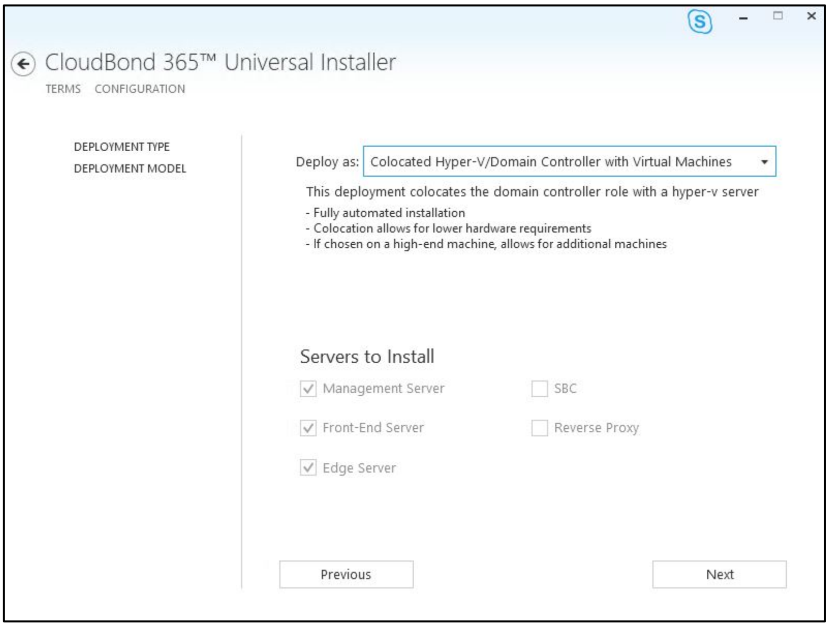
☑ Management Server
☑ Front-End Server
☑ Edge Server
□ SBC
□ Reverse Proxy

11.9.9.3 Co-located Hyper-V / Domain Controller, with VirtualMachines

The Co-Located Hyper-V / Domain Controller with Virtual Machines installs the CloudBond 365 Controller (DC) and Hyper-V within the host machine, with the remaining CloudBond 365 Servers (FE and optional Edge) as Hyper-V virtual machines.

This option is suitable for CloudBond 365 Standard / Standard+ Box Edition (e.g. AudioCodes Mediant 800B OSN server).

Figure 11-80: Deployment Model - Mediant 800



CloudBond 365™ Universal Installer

TERMS CONFIGURATION

DEPLOYMENT TYPE

DEPLOYMENT MODEL

Deploy as: Colocated Hyper-V/Domain Controller with Virtual Machines

This deployment colocates the domain controller role with a hyper-v server

- Fully automated installation
- Colocation allows for lower hardware requirements
- If chosen on a high-end machine, allows for additional machines

Servers to Install

☑ Management Server ☐ SBC

☑ Front-End Server ☐ Reverse Proxy

☑ Edge Server

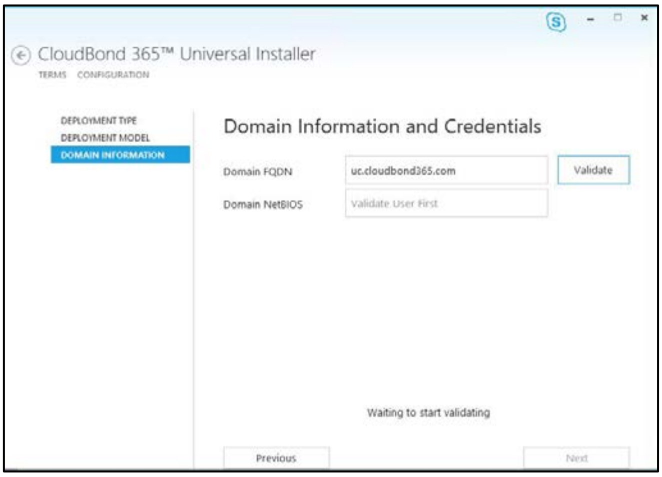
11.9.10 Domain Information and Credentials (Branch / Paired Pool Deployment)

If performing a Branch / Paired Pool deployment, you will be asked to change and verify the domain, and, administrator login credentials for the existing CloudBond 365 Administrator, to verify you have the required permissions to continue the installation process.

The configuration wizard uses a multistep process to verify first, the domain details, and secondly the administrator credentials in that domain. The wizard will validate the information provided, and also that the user is a member of specific Skype for Business security groups with sufficient privileges to perform the installation.

Click **Validate** to verify the Domain Information you entered is correct.

Figure 11-81: Validate Domain



Domain Information and Credentials

Domain FQDN: uc.cloudbond365.com

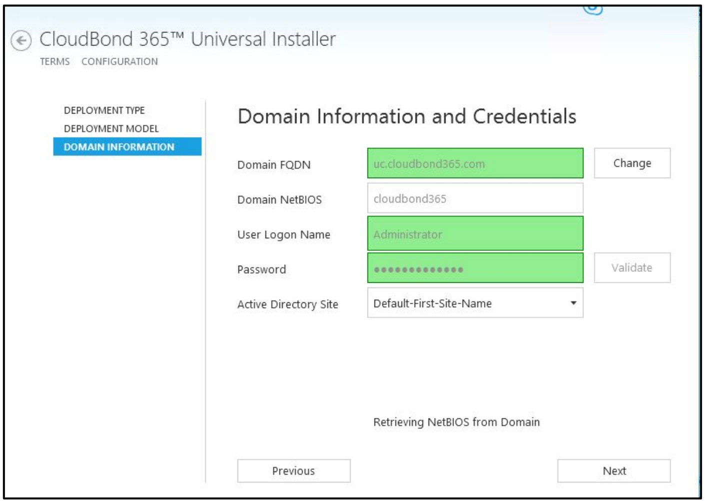
Domain NetBIOS: Validate User First

Waiting to start validating

If the domain validation is successful, it will be highlighted in green.

Click **Validate** to confirm the Administrator Credentials you entered.

Figure 11-82: Domain and Credentials Validated



Domain Information and Credentials

Domain FQDN: uc.cloudbond365.com

Domain NetBIOS: cloudbond365

User Logon Name: Administrator

Password: ●●●●●●●●●●●●●

Active Directory Site: Default-First-Site-Name

Retrieving NetBIOS from Domain

If the credential validation is successful, it will be highlighted in green and the NetBIOS field will be populated. Click **Next** to continue the installation.

11.9.11 Management Server

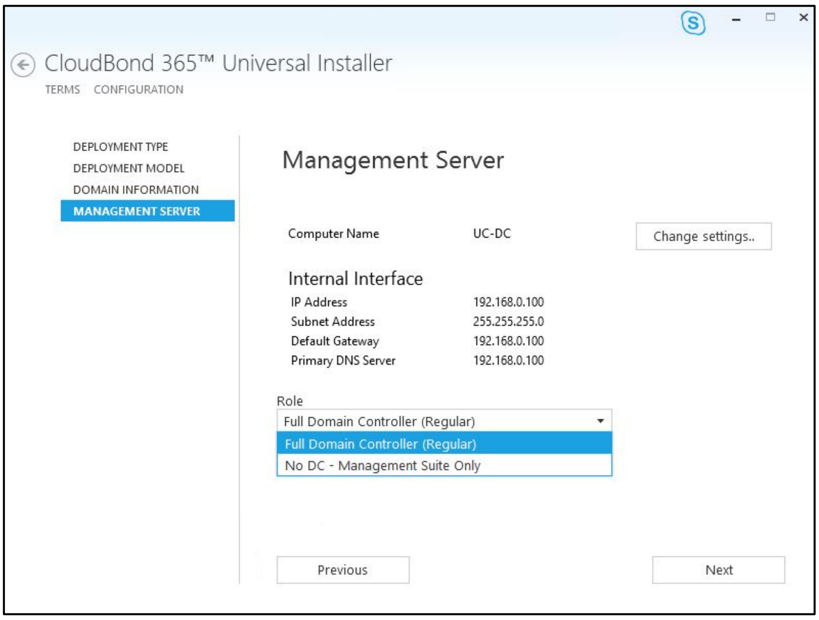
If you selected a Branch / Paired Pool Deployment Type, you will be asked to specify the new Management Server information. If installed as a second Domain Controller, it provides resiliency within the Branch, should the WAN link to the existing CloudBond 365 system be lost.

You will also need to select whether the Domain Controller is a:

- No Domain Controller (Management Suite only)
- Full Domain Controller (Read / Write)

The wizard will automatically create a new Domain controller with the information specified, and insert it into the existing Active Directory Resource Forest. It will also install the SysAdmin suite onto the Controller.

Figure 11-83: Domain Controller (BPA)



Management Server

Computer Name UC-DC

Internal Interface

IP Address 192.168.0.100

Subnet Address 255.255.255.0

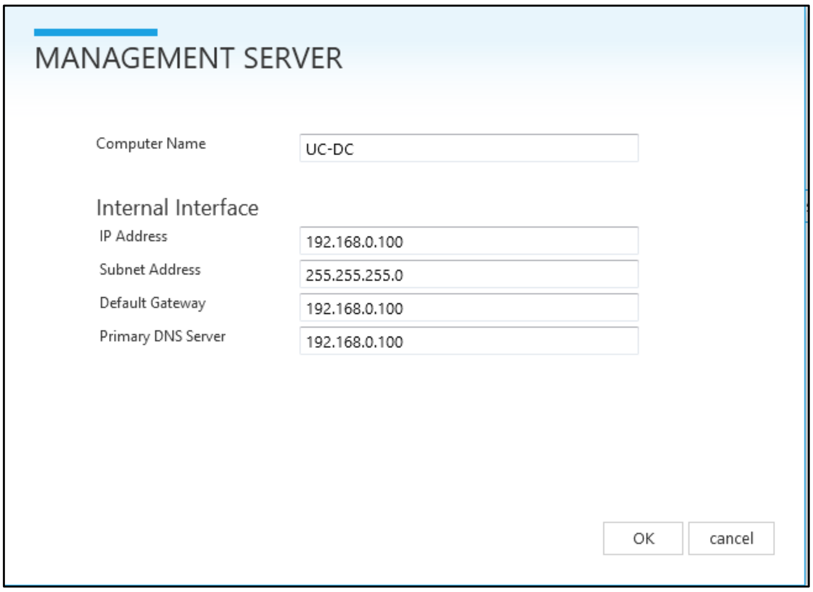
Default Gateway 192.168.0.100

Primary DNS Server 192.168.0.100

Role: Full Domain Controller (Regular)

- Full Domain Controller (Regular)
- No DC - Management Suite Only

Figure 11-84: Changing the Controller Settings



MANAGEMENT SERVER

Computer Name: UC-DC

Internal Interface

IP Address: 192.168.0.100

Subnet Address: 255.255.255.0

Default Gateway: 192.168.0.100

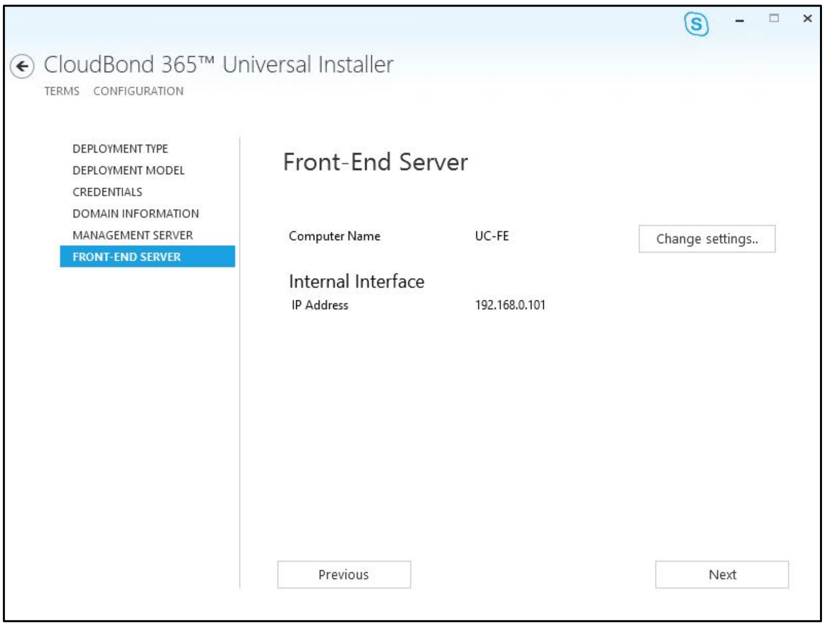
Primary DNS Server: 192.168.0.100

Note: As the BPA will be joined into an existing Active Directory forest topology, the Management Server DNS Server IP address needs to be a DNS server that is capable of resolving a domain controller for the domain to which the BPA will need to be joined.

11.9.12 Front-End Server

For all deployment types, you will be asked to specify the details for the Front-End server.

Figure 11-85: Front-End server



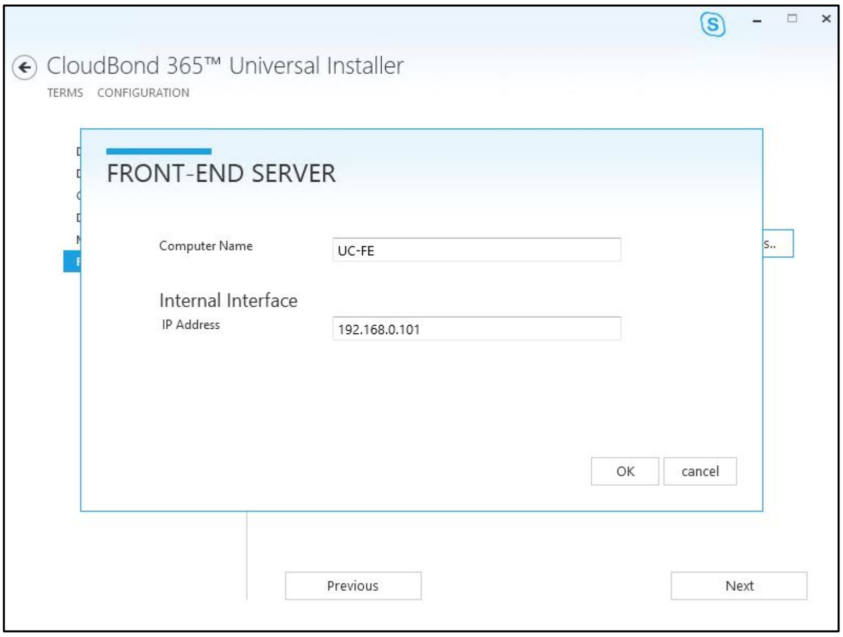
Front-End Server

Computer Name UC-FE

Internal Interface

IP Address 192.168.0.101

Figure 11-86: Changing the FE Settings



FRONT-END SERVER

Computer Name: UC-FE

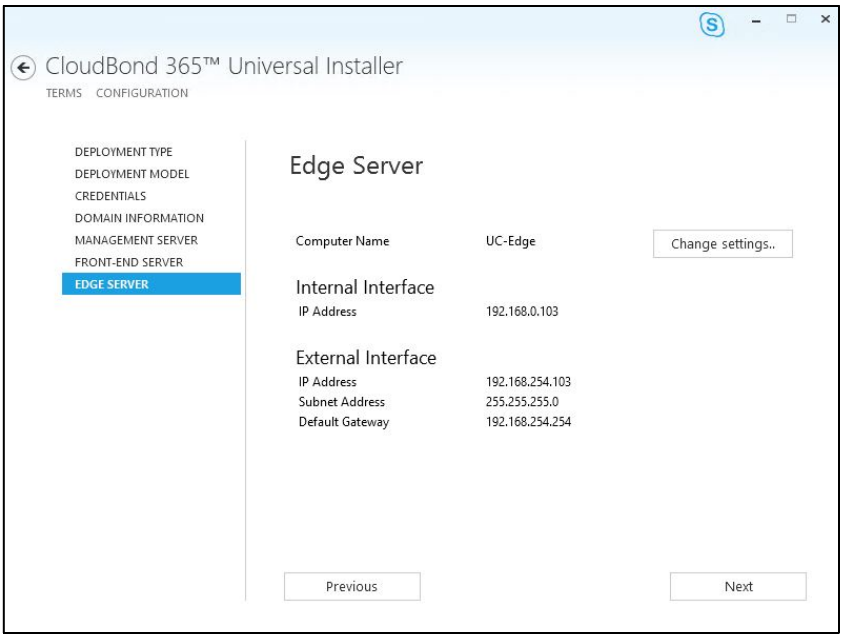
Internal Interface

IP Address: 192.168.0.101

11.9.13 Edge Server

For Branch / Paired Pool deployment type, installation of the additional Edge server is optional.

Figure 11-87: Edge Server (BPA)



CloudBond 365™ Universal Installer

TERMS CONFIGURATION

- DEPLOYMENT TYPE
- DEPLOYMENT MODEL
- CREDENTIALS
- DOMAIN INFORMATION
- MANAGEMENT SERVER
- FRONT-END SERVER
- EDGE SERVER

Edge Server

Computer Name UC-Edge

Change settings..

Internal Interface

IP Address 192.168.0.103

External Interface

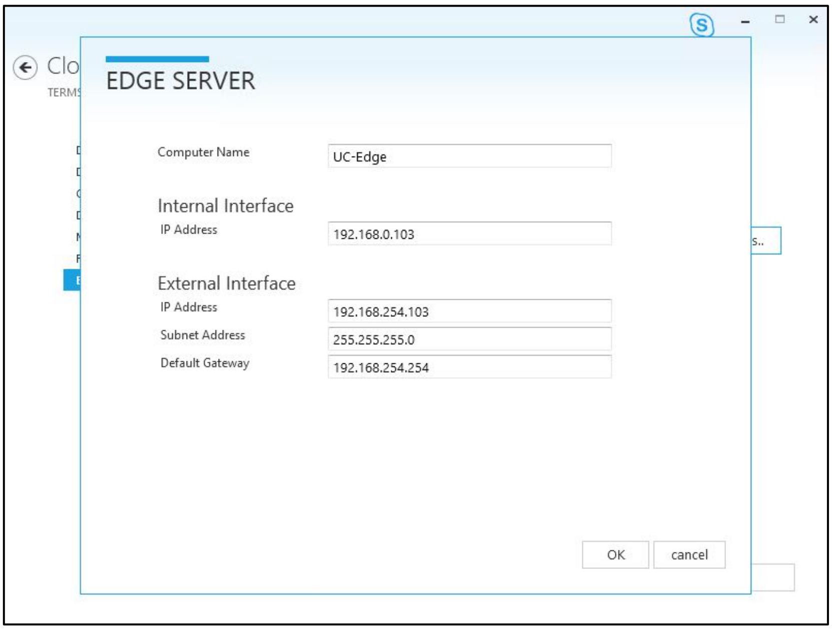
IP Address 192.168.254.103

Subnet Address 255.255.255.0

Default Gateway 192.168.254.254

Previous Next

Figure 11-88: Changing the Edge Settings



EDGE SERVER

Computer Name UC-Edge

Internal Interface

IP Address 192.168.0.103

External Interface

IP Address 192.168.254.103

Subnet Address 255.255.255.0

Default Gateway 192.168.254.254

OK cancel

Note: To prevent complex networking scenarios during installation, the wizard only allows for a single public edge IP Address and requires the Edge Internal leg to be on the same subnet as the other servers installed. If different deployment scenarios are needed, it is just a small change to be made in Skype for Business Topology Builder after the installation wizard has finished.

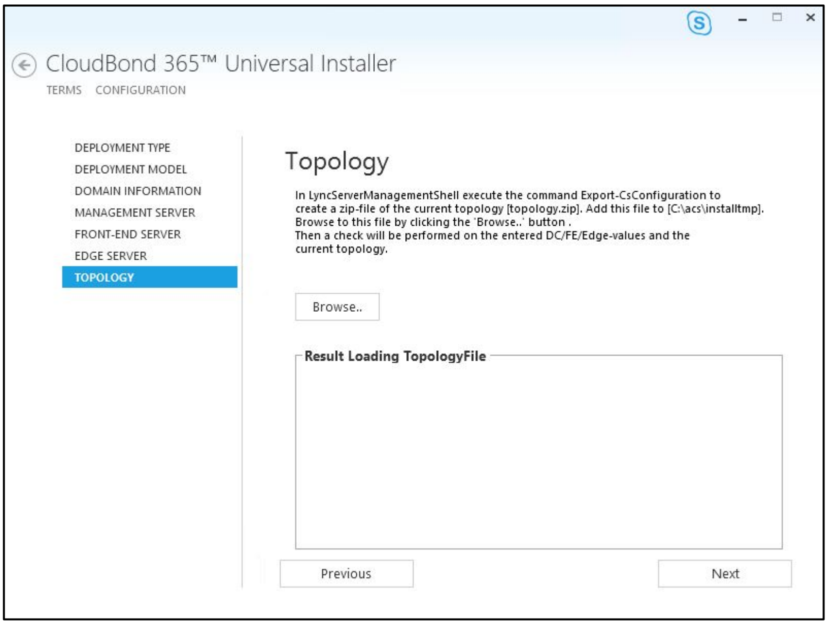
For more information see Section 17.5.1.4, Chapter 14 and Chapter 17.

11.9.14 Topology

If installing a Branch / Paired Pool deployment, you will be asked to provide a copy of the existing topology in a zip file.

This can be retrieved from the existing CloudBond Controller using the Skype for Business Management Shell command **Export-csConfiguration** as describer at the start of this chapter.

Figure 11-89: Loading the Topology



Topology

In LyncServerManagementShell execute the command Export-CsConfiguration to create a zip-file of the current topology [topology.zip]. Add this file to [C:\acs\installtmp]. Browse to this file by clicking the 'Browse..' button .
Then a check will be performed on the entered DC/FE/Edge-values and the current topology.

The wizard will scan the topology for information and report results.

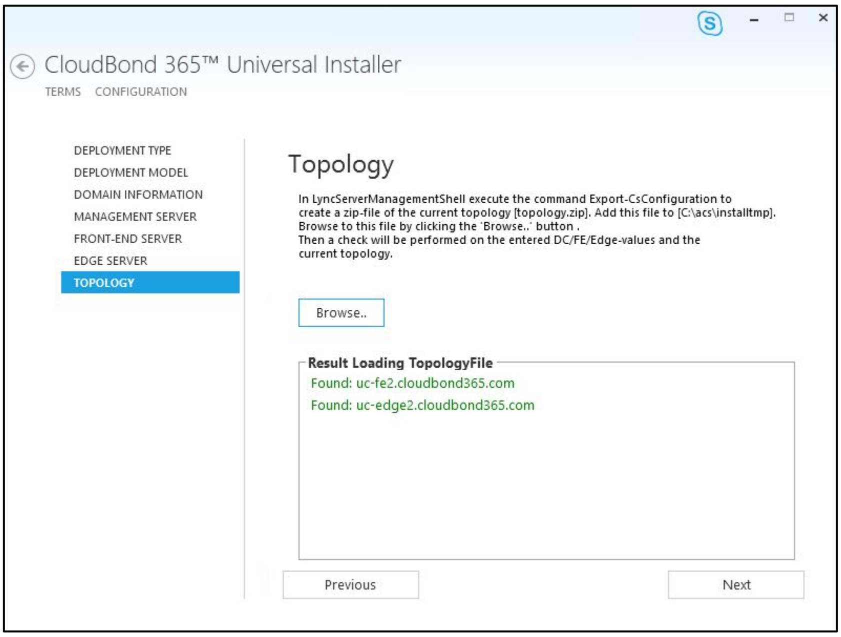
11.9.14.1 Topology Scan Results

The Wizard will scan the supplied topology file and attempt to match the required FE and Edge servers against the data you have entered so far.

If it fails to find matching entries, it will highlight the results in Red. You may need to return to the existing CloudBond 365 installation, and modify the topology, or change the data you have entered in the BPA wizard by going to previous screens.

If the wizard is able to match your entries against the topology, the results will be highlighted in green, and you may proceed with the installation.

Figure 11-90: Topology Scan Results – Pass



Topology

In LyncServerManagementShell execute the command Export-CsConfiguration to
create a zip-file of the current topology [topology.zip]. Add this file to [C:\acs\installtmp].
Browse to this file by clicking the 'Browse..' button .
Then a check will be performed on the entered DC/FE/Edge-values and the
current topology.

Result Loading TopologyFile

Found: uc-fe2.cloudbond365.com
Found: uc-edge2.cloudbond365.com

11.9.15 Summary

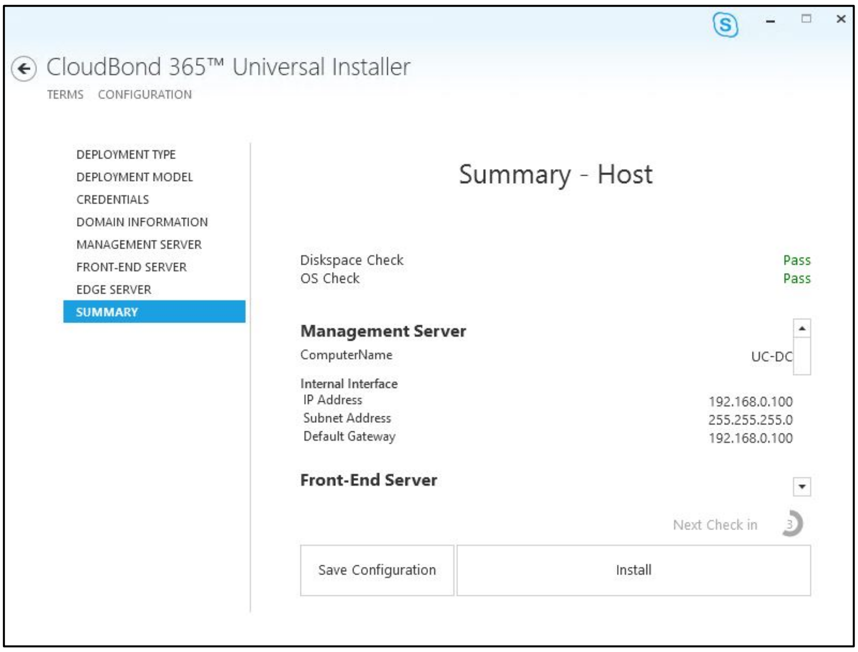
The Summary page shows details of the selections made during the Wizard, as well as various pre-checks performed on the hardware.

If all information meets requirements, an **Install** button will appear below.

The summary page allows you to manually save the entered configuration by clicking the Save Configuration button. This will show display a standard “Save As” dialog, allowing you to specify where the file is saved.

Click the **Install** button to begin the Software Install process only once the checks show **Pass.** The OS Check specifically will sometimes need more time to be validated. The rotating wheel above the **Install** Button gives a time indication when the next validation check will be performed.

Figure 11-91: Wizard Summary



CloudBond 365™ Universal Installer

Summary - Host

Diskspace Check Pass
OS Check Pass

Management Server
ComputerName UC-DC
Internal Interface
IP Address 192.168.0.100
Subnet Address 255.255.255.0
Default Gateway 192.168.0.100

Front-End Server

Warning: After the installation is finished, scheduled tasks will have been created on the management server. If multiple management servers are installed in the environment for redundancy, the scheduled tasks on the redundant servers should be disabled and only enabled if the primary server goes down to prevent duplicated objects from being created in the Active Directory.

11.10 User Management Pack 365

The User Management Pack 365 can be installed in any existing CloudBond 365, Lync Server 2013 or Skype for Business Server environment, to either upgrade the older version of the management layer to the latest version or to just only install the User Management Pack 365 to enhance the administrative features for any Microsoft or competitive native deployment of Lync Server 2013 or Skype for Business Server .

Note: AudioCodes support policy for CloudBond / User Management Pack is N-1;this implies that Lync 2010 server backend environments are no longer supported.

11.10.1 Prerequisites for Standalone Deployments

The Installation of the User Management Pack 365 requires a Windows Server 2012 R2 (virtual) server environment for installation. This server needs to be domain joined to the existing Skype for Business environment and should be added as a trusted application server within the Skype for Business topology.

The service account used for the installation of the Management Pack should be a member of the following security groups:

- Domain Admins
- CSAdministrator
- RTCUniversalServerAdmins
- RTCUniversalUserAdmins

Note:

- The Windows Server should be configured with a static IPv4 address and not using a DHCP server (DHCP server is not allowed in this configuration).
- Even though Lync Server 2013 is supported as a backend environment, the Skype for Business Administration tools should be installed on the server running the User Management Pack application.

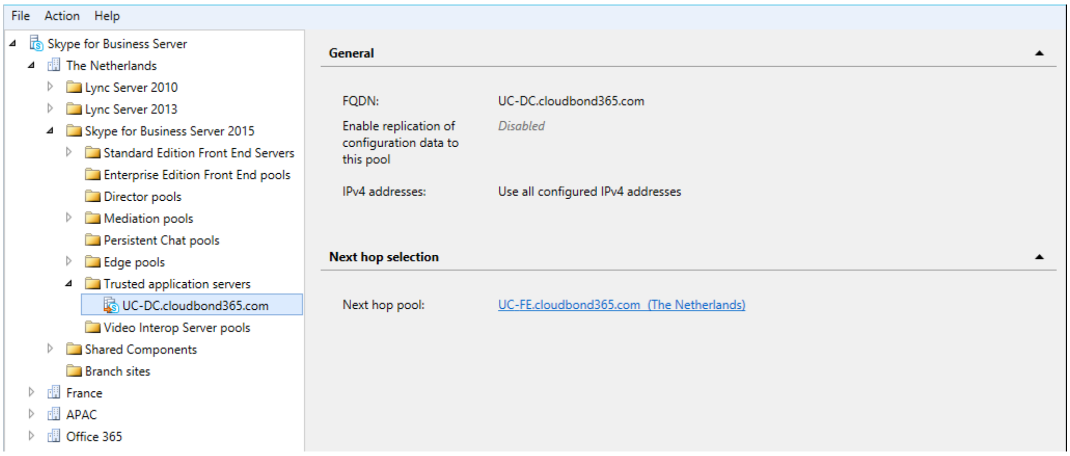
11.10.1.1 Prepare the Skype for Business Environment

Note: When upgrading an existing CloudBond 365 environment continue with step: Installing User Management Pack 365.

Before the User Management Pack 365 can be installed, the the Skype for Business Environment must be prepared for a new trusted application. To do this, perform the following steps:

1. Create a trusted application pool for the server that will be used to install the CloudBond 365 Management Pack in the Skype for Business topology. In the example screenshot below, this computer is named UC-DC.cloudbond365.com instead of the default UC-DC.cloudbond365.local.

Figure 11-92: Add Trusted Application Server



FQDN: UC-DC.cloudbond365.com

Enable replication of configuration data to this pool: Disabled

IPv4 addresses: Use all configured IPv4 addresses

Next hop pool: UC-FE.cloudbond365.com (The Netherlands)

2. Add a new trusted application to this application pool named presenceservice using the following cmdlet in the Skype for Business Management Shell:

   ```
   New-CsTrustedApplication -ApplicationId presenceservice -
   TrustedApplicationPoolFqdn uc-dc.cloudbond365.local –Port 6001
   ```

   Where uc-dc.cloudbond365.local reflects the FQDN from the computer where the management pack will be installed.

Note: Another trusted application name and port can be chosen, but will require a change in the c:\acs\UCMAWebService\SysAdmin.UCMAService.exe.config file to reflect the same parameters.

3. Enable the new trusted application with the following cmdlet:

   ```
   Enable-CsTopology
   ```

11.10.1.2 Prepare the Server that will run the Management Pack Application

The server that is used for the installation of the CloudBond 365 Management Pack requires the enabling of specific Windows Roles and Features. For this, perform the following steps:

1. Make sure the computer is joined to the Active Directory domain that hosts the Skype for Business environment.
2. Make sure that the service account used to logon to the server is a member of the following security groups:
   a. Domain Admins
   b. CSAdministrator
   c. RTCUniversalServerAdmins
   d. RTCUniversalUserAdmins
3. Install the Windows Roles and features required by the Management Pack by issuing the following cmdlet in a Windows Powershell window:

   ```
   Install-WindowsFeature Telnet-Client, SMTP-Server, Web-Server,
   RSAT-ADCS-Mgmt, RSAT-AD-Tools, Web-Mgmt-Tools, Web-Mgmt-
   Console, Web-WebServer, Web-Common-Http, Web-Default-Doc, Web-
   Static-Content, Web-Performance, Web-Stat-Compression, Web-
   Dyn-Compression, Web-Security, Web-Filtering, Web-Windows-
   Auth, Web-App-Dev, Web-Net-Ext45, Web-Asp-Net45, Web-ISAPI-
   Ext, Web-ISAPI-Filter, Web-Includes,
   ```

```
InkandHandwritingServices, Web-Net-Ext, Web-Asp-Net, Server-
Media-Foundation, rsat
```

Note: Some features might require access to the Windows server installation media. For these features, you should add the following parameter to the end of the cmdlet, where D is the driveletter assigned to the drive holding the Windows server media:

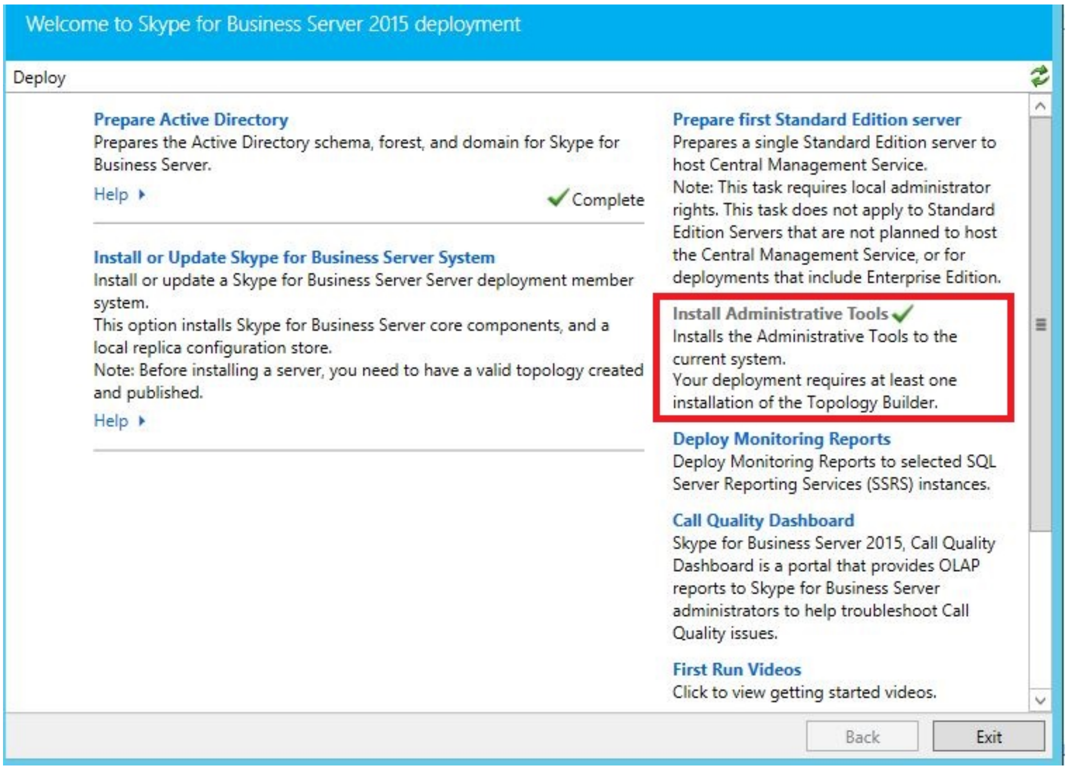
```
Source D:\Sources\sxs
```

4. Set the execution policy for PowerShell Scripts to Bypass mode, by issuing the following cmdlet in a Windows PowerShell window:

```
Set-ExecutionPolicy Bypass
```

5. Install the Skype for Business Administration tools using the Skype for Business installation media:

Figure 11-93: Skype for Business Administration Tools



Welcome to Skype for Business Server 2015 deployment

Deploy

Prepare Active Directory
Prepares the Active Directory schema, forest, and domain for Skype for Business Server.
Help ▸ ✓ Complete

Install or Update Skype for Business Server System
Install or update a Skype for Business Server Server deployment member system.
This option installs Skype for Business 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 to the current system.
Your deployment requires at least one installation of the Topology Builder.

Deploy Monitoring Reports
Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances.

Call Quality Dashboard
Skype for Business Server 2015, Call Quality Dashboard is a portal that provides OLAP reports to Skype for Business Server administrators to help troubleshoot Call Quality issues.

First Run Videos
Click to view getting started videos.

6. Install the latest Skype for Business Server updates using Microsoft's SkypeServerUpdateInstaller.exe, which can be found in the \Updates folder on the CloudBond 365 Management Pack installation media.

7. Request a certificate for this computer to be used by the UCMA application, using the following cmdlet in the Skype for Business Management Shell:

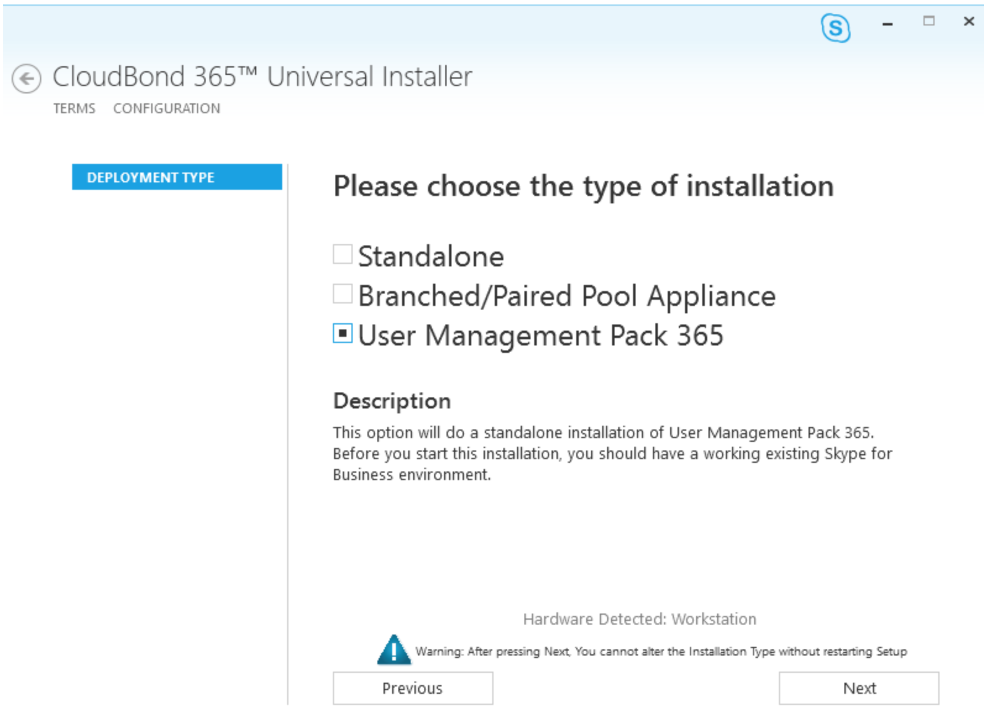
```
Request-CsCertificate -New -Type default -FriendlyName
"trustedapps.contoso.com Pool" -CA ca.contoso.com\ContosoCA -
ComputerFQDN uc-dc.cloudbond365.local
```

More info can be found at http://msdn.microsoft.com/en-us/library/lync/hh347354.aspx

11.10.2 Installing User Management Pack 365

Now that the server is prepared, it is time to install the User Management Pack. If not already mounted, mount the CloudBond 365 installation media and start **setup.exe** and select the **User Management Pack 365** option as the deployment type:

Figure 11-94: Select Deployment Type



Please choose the type of installation

☐ Standalone
☐ Branched/Paired Pool Appliance
☒ User Management Pack 365

Description

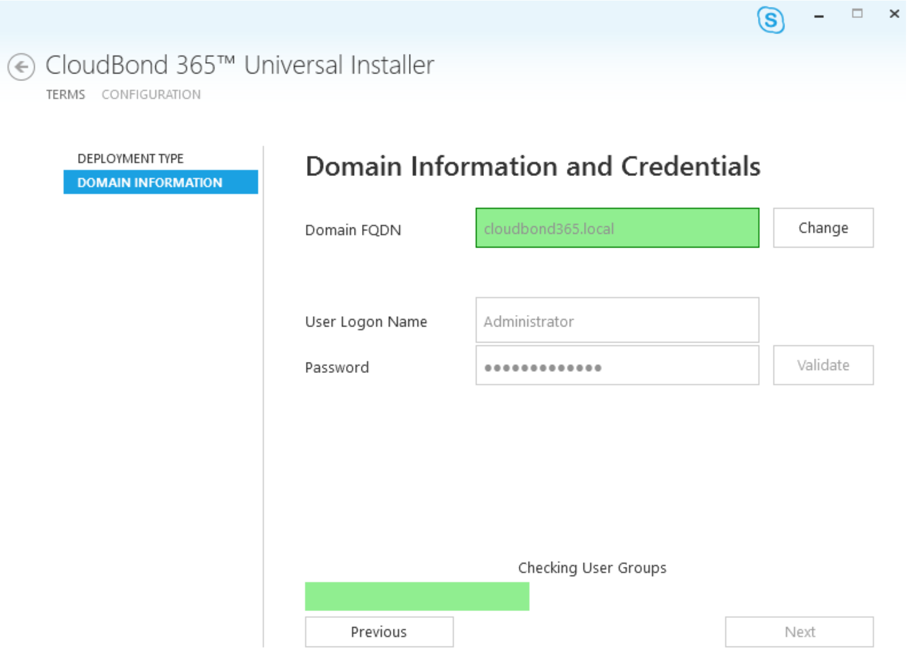
This option will do a standalone installation of User Management Pack 365. Before you start this installation, you should have a working existing Skype for Business environment.

Hardware Detected: Workstation

Warning: After pressing Next, You cannot alter the Installation Type without restarting Setup

8. Click **Next** and validate the domain Information and Credentials:

Figure 11-95: Domain Information and Credentials



Domain Information and Credentials

Domain FQDN: cloudbond365.local

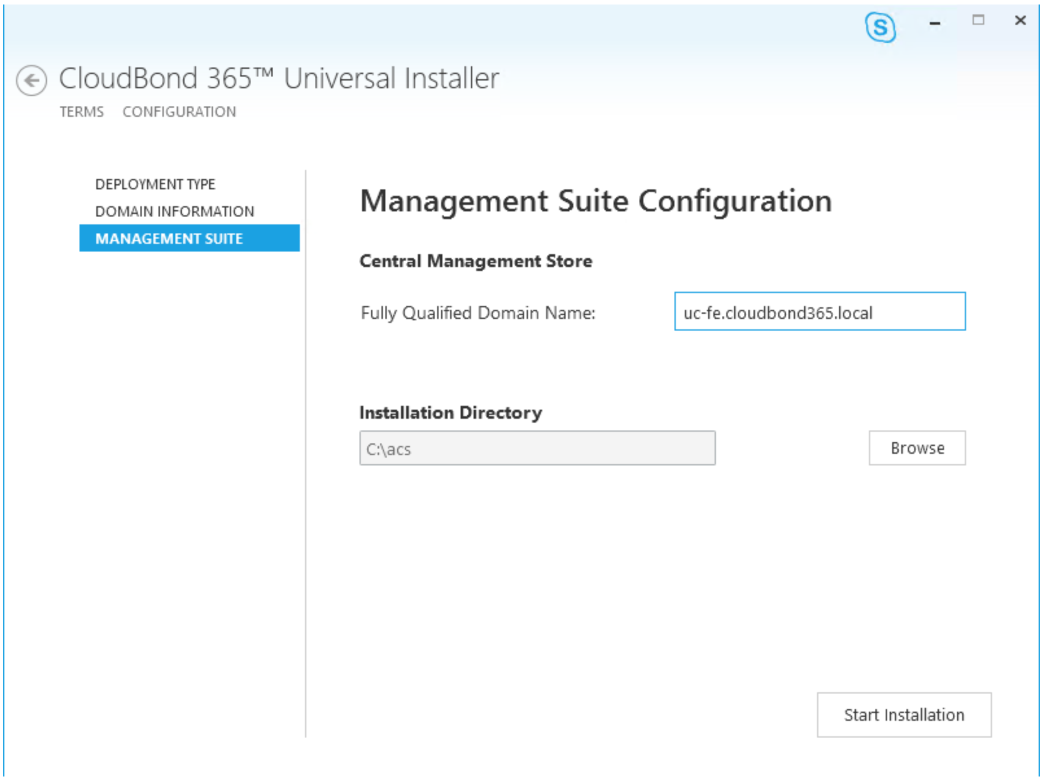
User Logon Name: Administrator

Password: ●●●●●●●●●●●●●

Checking User Groups

9. Click **Next** and specify the name of the Frontend pool:

Figure 11-96: Front End Pool Name



Management Suite Configuration

Central Management Store

Fully Qualified Domain Name: uc-fe.cloudbond365.local

Installation Directory

C:\acs

Note: Even though the wizard mentions Central Management Store, the Fully Qualified Domain Name should point to a server holding the **RTCLocal** database. This will be the pool FQDN for the FrontEnd server(pool).

Some functions within the User Management Pack application require PowerShell functions to be executed on the actual FrontEnd servers in the environment.

For this a proprietary SysAdmin.RemotingSvr service needs to be installed on **every FrontEnd server** in the Skype for Business FrontEnd pools within the environment. This requires the following steps to be performed:

1. Copy the RemotingSvr folder from the \WindowsServices\ location on the CloudBond 365 installation media to a location on every Front End server (in the following example we'll use c:\acs\RemotingSvr as the destination)

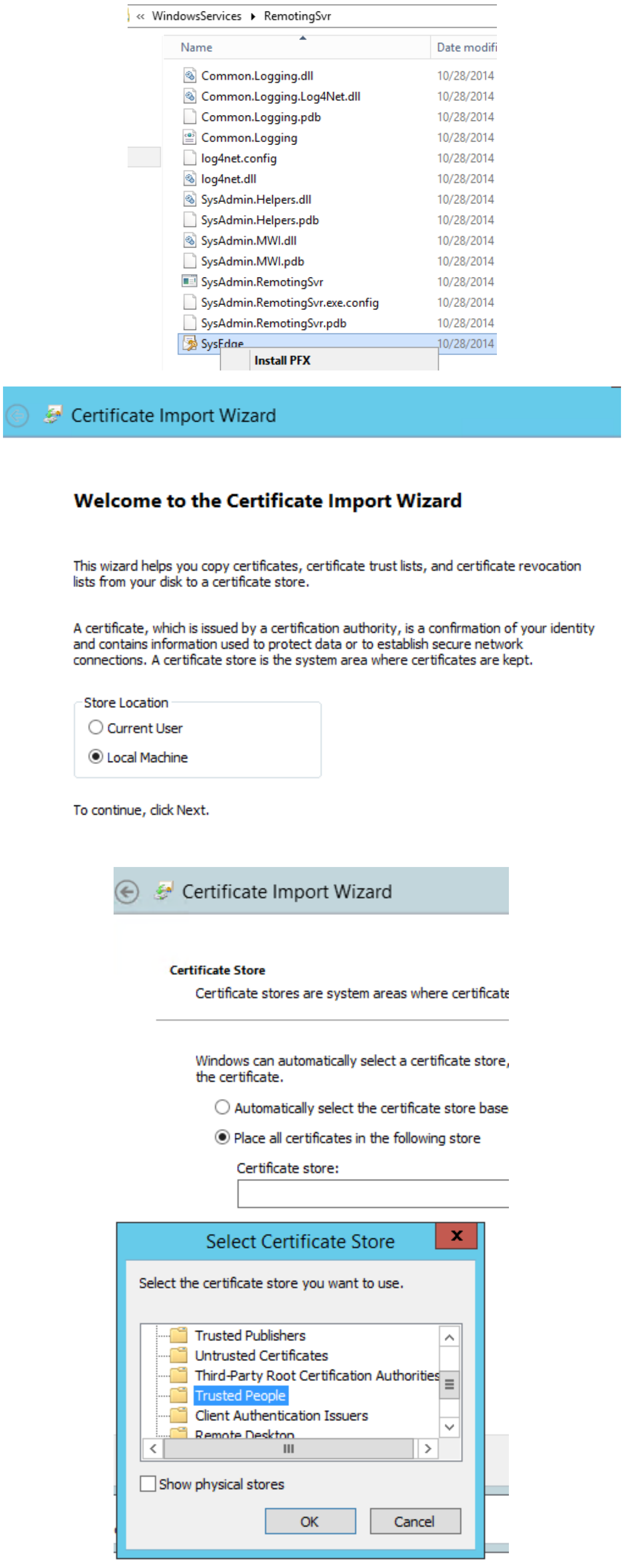
Note: When upgrading an earlier version of the CloudBond 365 environment, you need to stop the sysadmin.remotingsvr service and only copy the new files, replacing the older ones. There is no need to reregister the service and therefore you do not need to proceed with the steps below.

2. Set the execution policy for PowerShell Scripts to Bypass mode, by issuing the following cmdlet in a Windows PowerShell window:

```
Set-ExecutionPolicy Bypass
```

3. Import the c:\acs\RemotingSvr\SysEdge.pfx certificate in the computer\Trusted People certificate store by right clicking the certificate, and selecting **Install PFX**. Choose the Local Machine as the destination and continue to the password page, where the password p@ssw0rd needs to be input. Complete the import wizard according to the following screens:

Figure 11-97: Complete Import Wizard



« WindowsServices ▸ RemotingSvr

Name	Date modifi
Common.Logging.dll	10/28/2014
Common.Logging.Log4Net.dll	10/28/2014
Common.Logging.pdb	10/28/2014
Common.Logging	10/28/2014
log4net.config	10/28/2014
log4net.dll	10/28/2014
SysAdmin.Helpers.dll	10/28/2014
SysAdmin.Helpers.pdb	10/28/2014
SysAdmin.MWI.dll	10/28/2014
SysAdmin.MWI.pdb	10/28/2014
SysAdmin.RemotingSvr	10/28/2014
SysAdmin.RemotingSvr.exe.config	10/28/2014
SysAdmin.RemotingSvr.pdb	10/28/2014
SysEdge	10/28/2014

Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

○ Current User

● Local Machine

To continue, click Next.

Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificate

Windows can automatically select a certificate store, the certificate.

○ Automatically select the certificate store base

● Place all certificates in the following store

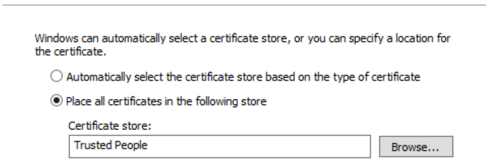
Certificate store:

Select Certificate Store

Select the certificate store you want to use.

- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities
- Trusted People
- Client Authentication Issuers
- Remote Desktop

□ Show physical stores

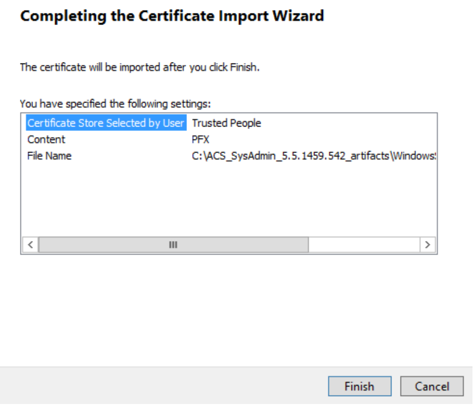


Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted People

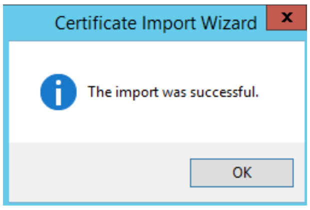


Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted People
Content	PFX
File Name	C:\ACS_SysAdmin_5.5.1459.542_artifacts\Windows\



Certificate Import Wizard

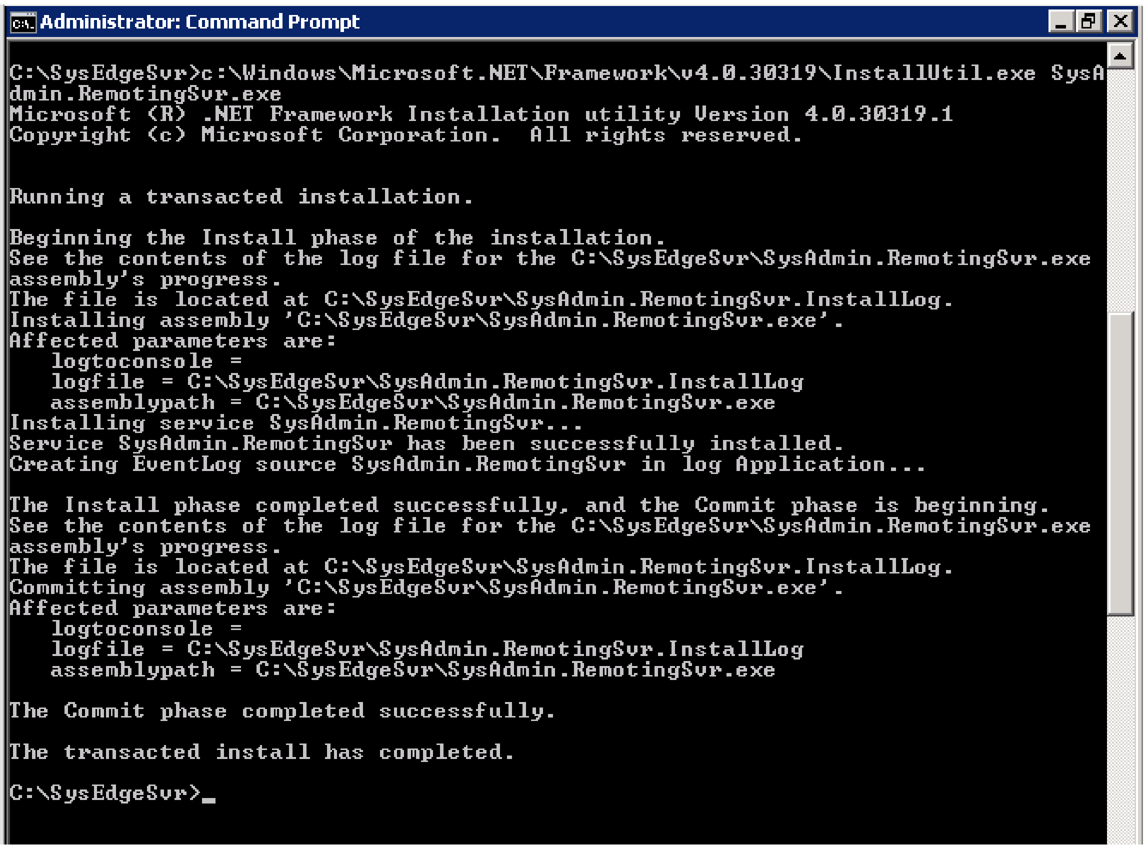
The import was successful.

4. Install the SysAdmin.RemotingSvr service, using the c:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe application by performing the following steps:

   a. Open a Command Prompt as Administrator

   b. Run the following command to install the application as a service: c:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe c:\acs\Remoting Svr\SysAdmin.RemotingSvr.exe

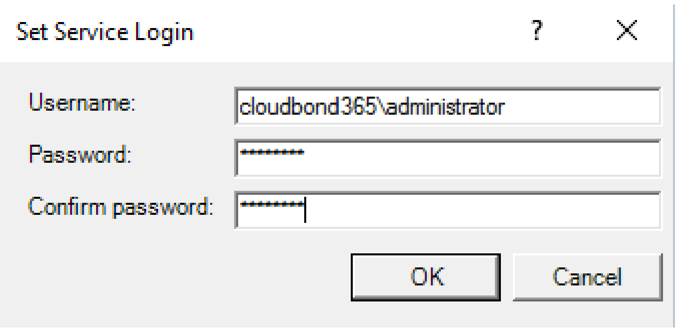
Figure 11-98: Administrator Command Prompt



```
C:\SysEdgeSvr>c:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe SysA
dmin.RemotingSvr.exe
Microsoft (R) .NET Framework Installation utility Version 4.0.30319.1
Copyright (c) Microsoft Corporation.  All rights reserved.


Running a transacted installation.

Beginning the Install phase of the installation.
See the contents of the log file for the C:\SysEdgeSvr\SysAdmin.RemotingSvr.exe
assembly's progress.
The file is located at C:\SysEdgeSvr\SysAdmin.RemotingSvr.InstallLog.
Installing assembly 'C:\SysEdgeSvr\SysAdmin.RemotingSvr.exe'.
Affected parameters are:
   logtoconsole =
   logfile = C:\SysEdgeSvr\SysAdmin.RemotingSvr.InstallLog
   assemblypath = C:\SysEdgeSvr\SysAdmin.RemotingSvr.exe
Installing service SysAdmin.RemotingSvr...
Service SysAdmin.RemotingSvr has been successfully installed.
Creating EventLog source SysAdmin.RemotingSvr in log Application...

The Install phase completed successfully, and the Commit phase is beginning.
See the contents of the log file for the C:\SysEdgeSvr\SysAdmin.RemotingSvr.exe
assembly's progress.
The file is located at C:\SysEdgeSvr\SysAdmin.RemotingSvr.InstallLog.
Committing assembly 'C:\SysEdgeSvr\SysAdmin.RemotingSvr.exe'.
Affected parameters are:
   logtoconsole =
   logfile = C:\SysEdgeSvr\SysAdmin.RemotingSvr.InstallLog
   assemblypath = C:\SysEdgeSvr\SysAdmin.RemotingSvr.exe

The Commit phase completed successfully.

The transacted install has completed.

C:\SysEdgeSvr>_
```

c. This command will prompt for the service account to be used for starting the service. Provide the username in the format domain\serviceaccount as shown below:

Figure 11-99: Set Service Login



Username: cloudbond365\administrator

Password: *********

Confirm password: *********

d. Though the service startup mode will be set to Automatic'. It is required to manually start the service after installation.

11.11 Virtual Edition Install

When all Configuration Wizard options are completed, the installation program starts installing the Skype for Business software components according to the input settings.

11.11.1 Deployment Model using Hyper-V

If you selected a Deployment Model of **Hyper-V Host with Virtual Machines** or

Co-Located Hyper-V / Domain Controller with Virtual Machines, installation will continue automatically on the current hardware platform, requiring minimal intervention. Software installation can take between 3-8 hours, depending on the options chosen.

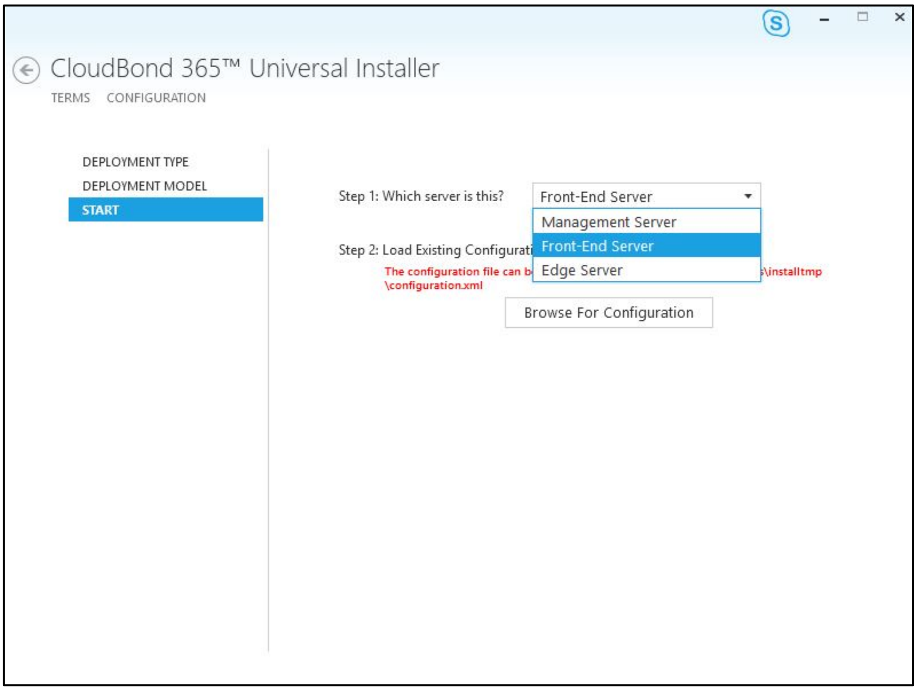
11.11.2 Deployment Model using the Virtual Edition

If you perform a Deployment Model of **Virtual Edition**, Hyper-V and Windows operating systems will not be installed. You'll be required to create your own Windows Server 2012 R2 virtual servers and assign to them IP addresses that will match the IP addresses you'll specify in the installation wizard.

Important: As the installer performs all installation tasks such as creating the Active Directory domain forest, joining the servers to the domain and installing the Skype for Business components, it is mandatory that a clean Windows Server 2012 R2 operating system is used.

You'll be required to log on to each of the three servers (DC, FE, and Edge) and perform the configuration on each. Once configured on the DC, the configuration can be saved and loaded for re-use on the FrontEnd and Edge servers:

Figure 11-100: Configuring DC, FE, and Edge Servers



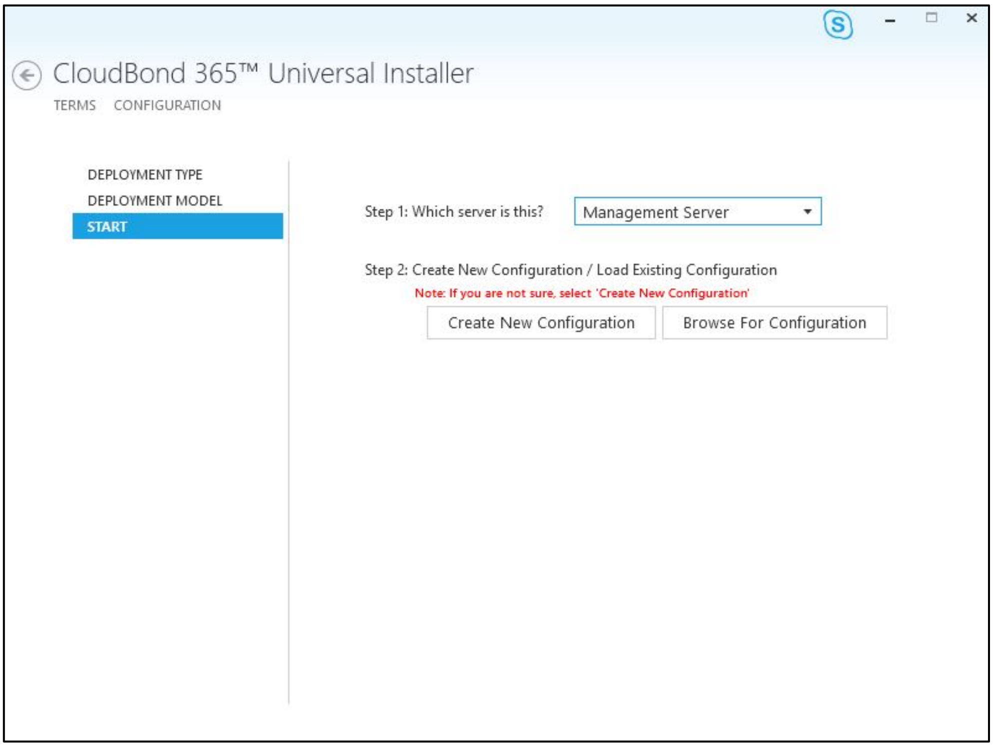
CloudBond 365™ Universal Installer

Step 1: Which server is this? Front-End Server

Step 2: Load Existing Configurati

The configuration file can b \installtmp \configuration.xml

Figure 11-101: Configuring DC, FE, and Edge Servers



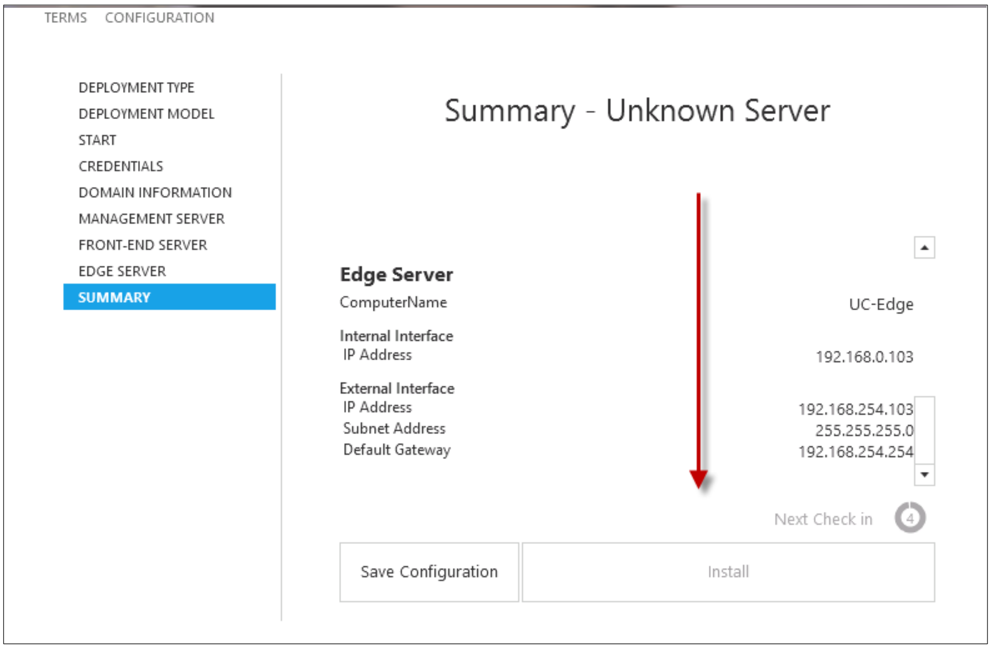
Step 1: Which server is this? Management Server

Step 2: Create New Configuration / Load Existing Configuration

Note: If you are not sure, select 'Create New Configuration'

The installation wizard checks the machine IP with the IP defined in the wizard, to determine which server role will be installed. If there's an IP address mismatch between the wizard and the virtual machine, the **Install** button will be grayed out and the server role is displayed as 'Unknown Server' on the Summary page.

Figure 11-102: Summary – Unknown Server



Summary - Unknown Server

Edge Server

ComputerName UC-Edge

Internal Interface
IP Address 192.168.0.103

External Interface
IP Address 192.168.254.103
Subnet Address 255.255.255.0
Default Gateway 192.168.254.254

11.11.3 Installation Steps

The software installer will perform many steps on each server to build the CloudBond 365 system. The steps will vary depending upon the options chosen in the Configuration Wizard. The major steps include:

- Creating Hyper-V Virtual machines as required
- Installing Windows 2012 R2 on each VM where needed
- Creating a Domain Controller
- Installing a Skype for Business Standard Edition Front End Server
- Installing a Skype for Business Consolidated Edge Server
- Installing Skype for Business utilities on the DC
- Installing SysAdmin and other CloudBond 365 components
- Installing the SBC software if required

The order of building each server VM is important. For example, the FE cannot be installed before the DC build is complete. The servers will be installed in the following order:

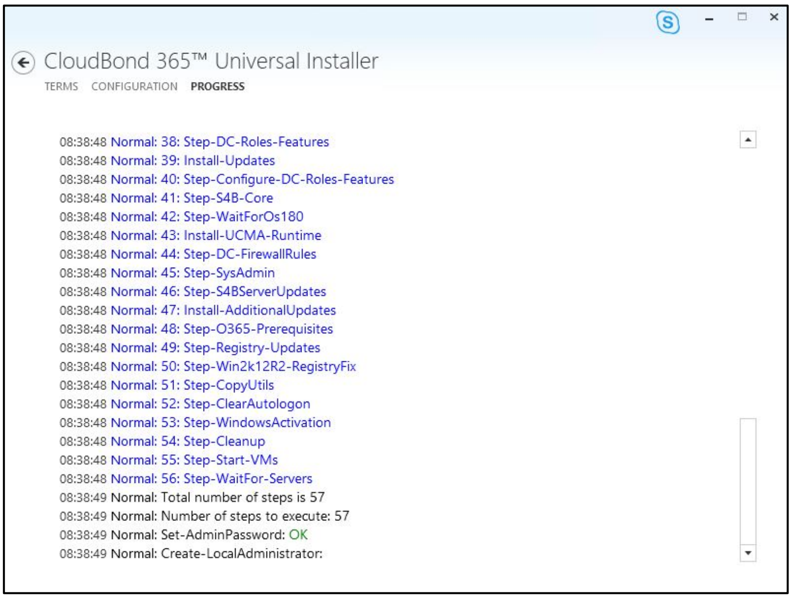
- DC
- FE
- Edge
- SBC
- RP

The Host waits for all VMs to complete before continuing. Each individual server waits for the previous server to complete before continuing.

11.11.4 Installation Progress

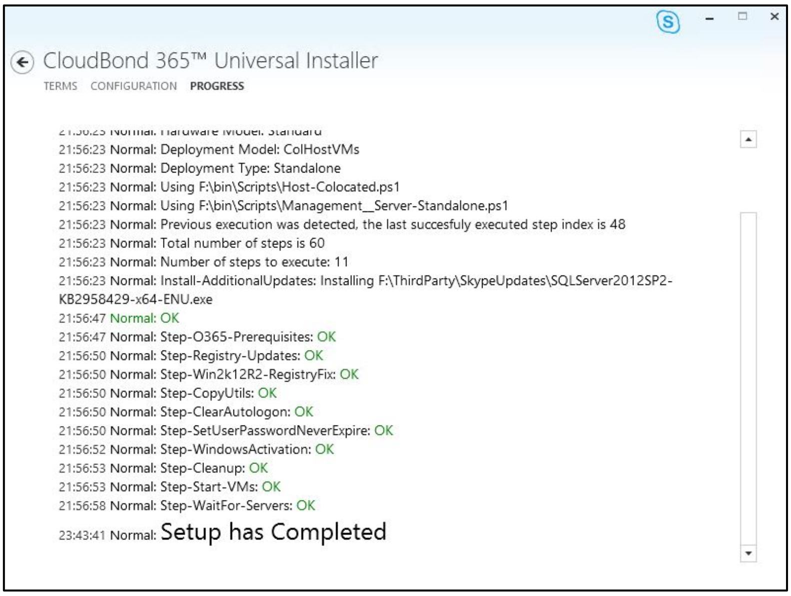
The following screenshots provide examples of the progress visible on each server component of the CloudBond 365 system.

Figure 11-103: Typical Automated Installer screen



```
08:38:48 Normal: 38: Step-DC-Roles-Features
08:38:48 Normal: 39: Install-Updates
08:38:48 Normal: 40: Step-Configure-DC-Roles-Features
08:38:48 Normal: 41: Step-S4B-Core
08:38:48 Normal: 42: Step-WaitForOs180
08:38:48 Normal: 43: Install-UCMA-Runtime
08:38:48 Normal: 44: Step-DC-FirewallRules
08:38:48 Normal: 45: Step-SysAdmin
08:38:48 Normal: 46: Step-S4BServerUpdates
08:38:48 Normal: 47: Install-AdditionalUpdates
08:38:48 Normal: 48: Step-O365-Prerequisites
08:38:48 Normal: 49: Step-Registry-Updates
08:38:48 Normal: 50: Step-Win2k12R2-RegistryFix
08:38:48 Normal: 51: Step-CopyUtils
08:38:48 Normal: 52: Step-ClearAutologon
08:38:48 Normal: 53: Step-WindowsActivation
08:38:48 Normal: 54: Step-Cleanup
08:38:48 Normal: 55: Step-Start-VMs
08:38:48 Normal: 56: Step-WaitFor-Servers
08:38:49 Normal: Total number of steps is 57
08:38:49 Normal: Number of steps to execute: 57
08:38:49 Normal: Set-AdminPassword: OK
08:38:49 Normal: Create-LocalAdministrator:
```

Figure 11-104: Setup has been completed on one of the VMs



```
21:56:23 Normal: Hardware Model: Standard
21:56:23 Normal: Deployment Model: ColHostVMs
21:56:23 Normal: Deployment Type: Standalone
21:56:23 Normal: Using F:\bin\Scripts\Host-Colocated.ps1
21:56:23 Normal: Using F:\bin\Scripts\Management__Server-Standalone.ps1
21:56:23 Normal: Previous execution was detected, the last succesfuly executed step index is 48
21:56:23 Normal: Total number of steps is 60
21:56:23 Normal: Number of steps to execute: 11
21:56:23 Normal: Install-AdditionalUpdates: Installing F:\ThirdParty\SkypeUpdates\SQLServer2012SP2-
KB2958429-x64-ENU.exe
21:56:47 Normal: OK
21:56:47 Normal: Step-O365-Prerequisites: OK
21:56:50 Normal: Step-Registry-Updates: OK
21:56:50 Normal: Step-Win2k12R2-RegistryFix: OK
21:56:50 Normal: Step-CopyUtils: OK
21:56:50 Normal: Step-ClearAutologon: OK
21:56:50 Normal: Step-SetUserPasswordNeverExpire: OK
21:56:52 Normal: Step-WindowsActivation: OK
21:56:53 Normal: Step-Cleanup: OK
21:56:53 Normal: Step-Start-VMs: OK
21:56:58 Normal: Step-WaitFor-Servers: OK
23:43:41 Normal: Setup has Completed
```

11.12 Setup Complete

When the Hyper-V Host server installation is finished and it can communicate to the virtual servers over IP, it will report **Setup has Completed** on the install screen.

You should now proceed with the post-install steps, which include:

- Installing a license code into the CloudBond 365 management suite web pages
- Completing any configuration steps for the SBC and reverse proxy
- To connect to the customer domain, see Part 'Deployment Requirements' on page 31.
- Perform any local customer Skype for Business configuration required.
- Activating Windows 2012 R2 licenses
- Update Windows and Skype for Business updates
- Update HP servers latest service pack updates

If you installed a Branch / Paired Pool Appliance, and wish to configure a paired pool, proceed to the next chapter.

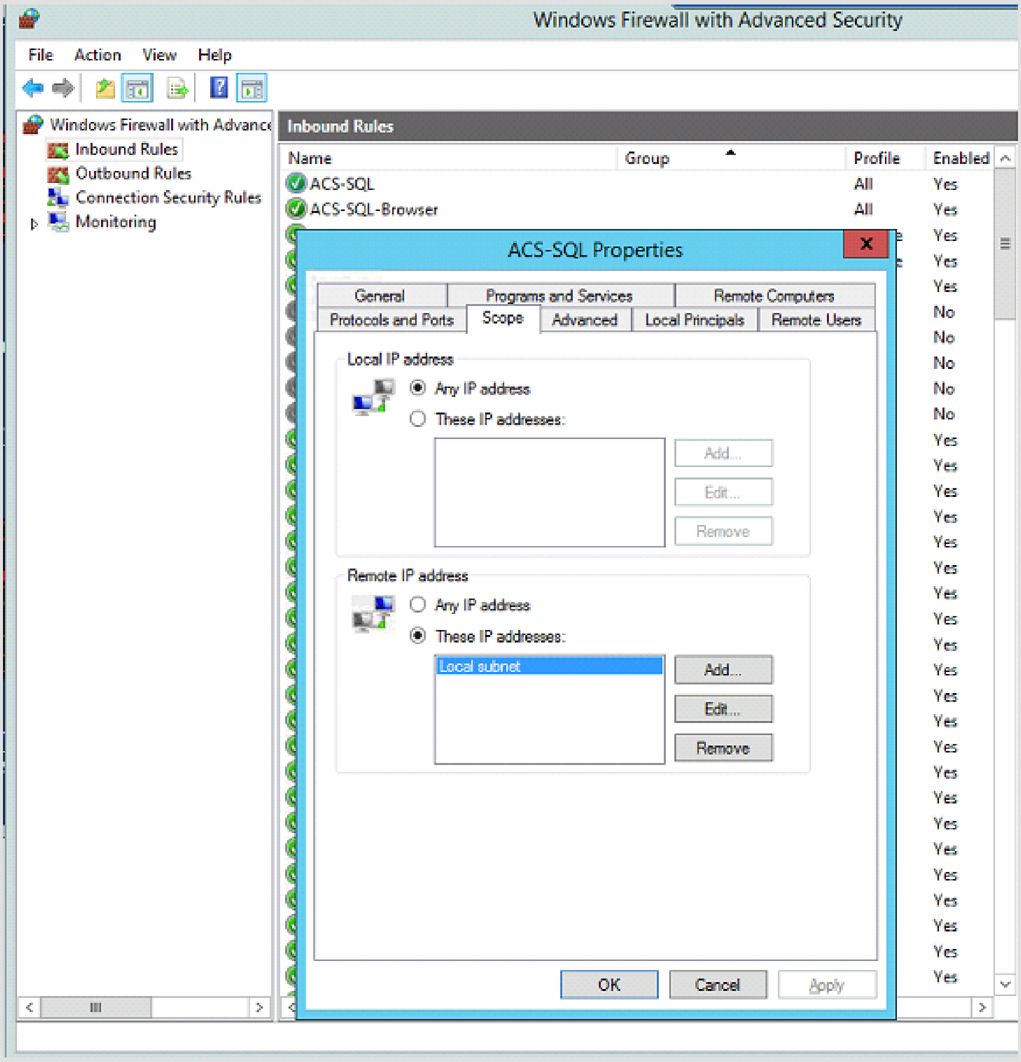
Note: After the CloudBond 365 software has been installed as a BPA or Software Only installation, the IP addresses for the none-domain-joined computers are not registered into DNS dynamically.

Consequently, for full feature functionality you'll need to make sure that the following servers all have a hosts file entry for the UMP management server, and that these servers are added to the DNS that is queried by the management server:

- Edge server
- Host server from a Pro or Enterprise server
- SBC
- Reverse proxy server

Note: After CloudBond 365 software has been installed, you may need to adjust DNS settings to match your network environment. You may either follow the deployment guide to set up DNS, or set the DNS server on the CloudBond 365 Controller (UC-DC) to forward requests to the internet. See Section 11.21 for more details.

Note: The Installation Wizard adds firewall rules to the Windows firewall for opening communication to the SQL environment. For security reasons, these ports are only opened to the local subnet. If communication between multiple IP subnets are required, the Remote IP address on the Scope tab of the ACS SQL Inbound firewall rules should be set to Any IP Address, or IP Addresses have to be added to the “These IP addresses” list as shown below:



ACS-SQL Properties – Scope

Local IP address: ● Any IP address ○ These IP addresses:

Remote IP address: ○ Any IP address ● These IP addresses: Local subnet

11.13 Paired Pools – Post Install

After the BPA software install completes, you may wish to modify the topology so that each FE server has resiliency by Pairing with the other FE server.

A paired pool of servers should only be established after both servers and installed and functioning.

To pair FE servers, they must be of the same type. For CloudBond 365, this means both FE servers must be Skype for Business Standard Edition FE Servers. You cannot pair a Skype for Business Standard Edition FE Pool with a Skype for Business Enterprise Edition FE Pool.

There is a good article about Paired Pool setup at:

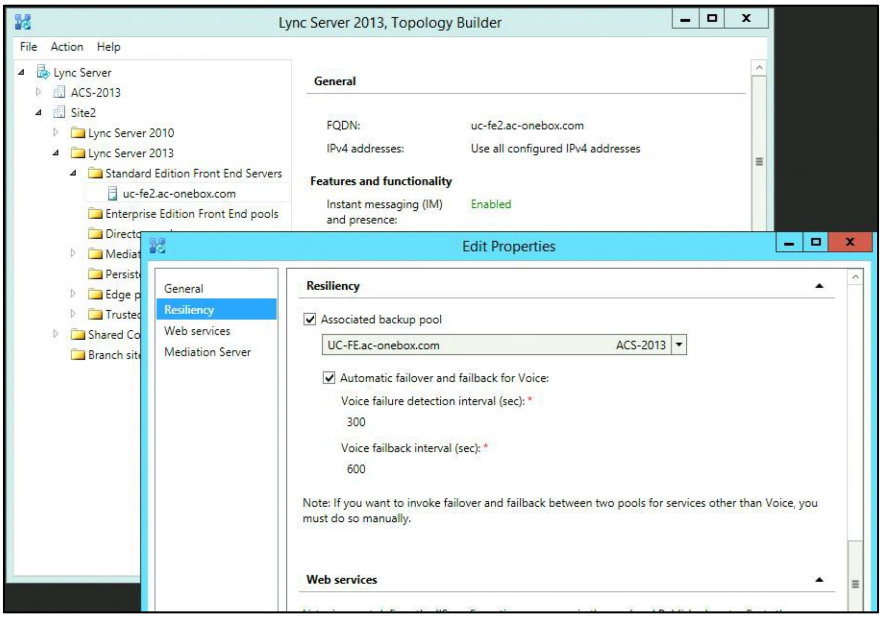
http://www.gecko-studio.co.uk/dont-play-with-fire-play-with-pool-pairing-configuring-testing/

11.13.1 Pairing Pools in Topology

➢ **To pair two FE servers:**

1. Log on to a CloudBond 365 DC.
2. Open the Skype for Business Topology Builder.
3. Right-click an existing Standard Edition FE Server, and select properties.
4. Navigate to the **Resiliency** section.
5. Enable an Associated backup pool, and select the paired FE server.
6. Select **Automatic failover and failback for Voice**.
7. Click **OK**.

Figure 11-105: Edit Properties



General

FQDN: uc-fe2.ac-onebox.com

IPv4 addresses: Use all configured IPv4 addresses

Features and functionality

Instant messaging (IM) and presence: Enabled

Resiliency

☑ Associated backup pool

UC-FE.ac-onebox.com ACS-2013

☑ Automatic failover and failback for Voice:

Voice failure detection interval (sec): *
300

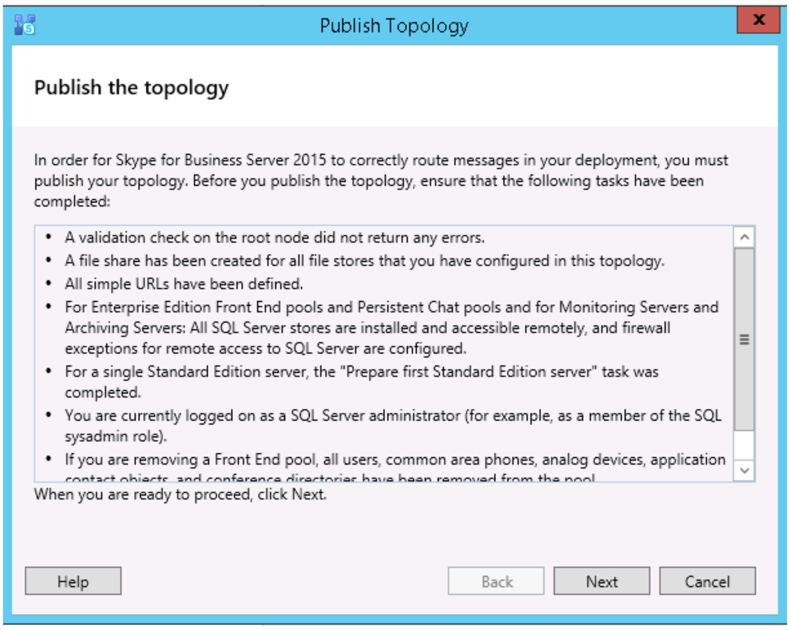
Voice failback interval (sec): *
600

Note: If you want to invoke failover and failback between two pools for services other than Voice, you must do so manually.

8. Publish the topology.

9. On each FE server, run the Skype for Business Deployment Wizard.

Figure 11-106: Publish Topology



Publish the topology

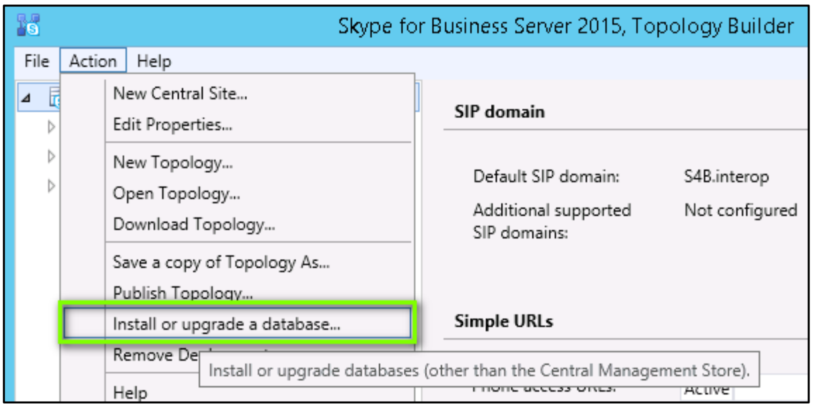
In order for Skype for Business Server 2015 to correctly route messages in your deployment, you must publish your topology. Before you publish the topology, ensure that the following tasks have been completed:

- A validation check on the root node did not return any errors.
- A file share has been created for all file stores that you have configured in this topology.
- All simple URLs have been defined.
- 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.
- For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed.
- You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role).
- 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.

When you are ready to proceed, click Next.

10. Click **Install or update database**.

Figure 11-107: Install or Update Database



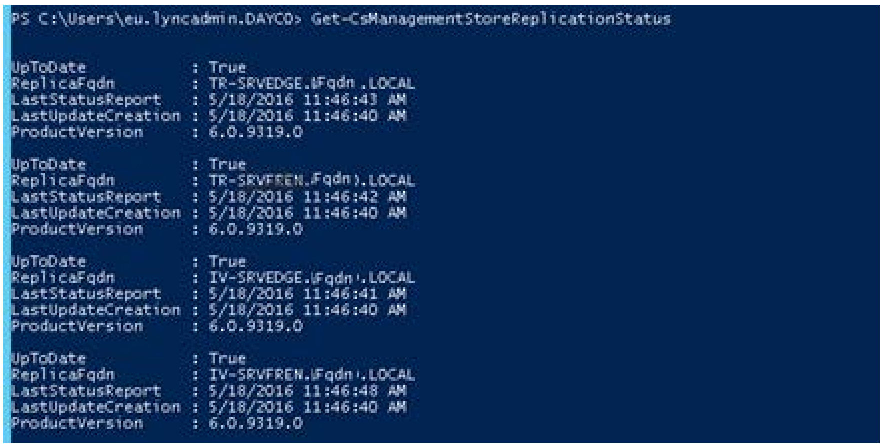
Skype for Business Server 2015, Topology Builder
File
Action
Help
New Central Site...
Edit Properties...
New Topology...
Open Topology...
Download Topology...
Save a copy of Topology As...
Publish Topology...
Install or upgrade a database...
Remove De
Help
Install or upgrade databases (other than the Central Management Store).
SIP domain
Simple URLs
Phone access URLs:
Active

Default SIP domain: S4B.interop

Additional supported SIP domains: Not configured

11. With the Get-CsManagmentReplicationStatus command, make sure the CMS is updated on all servers.

Figure 11-108: Making Sure the CMS is Updated on all Servers

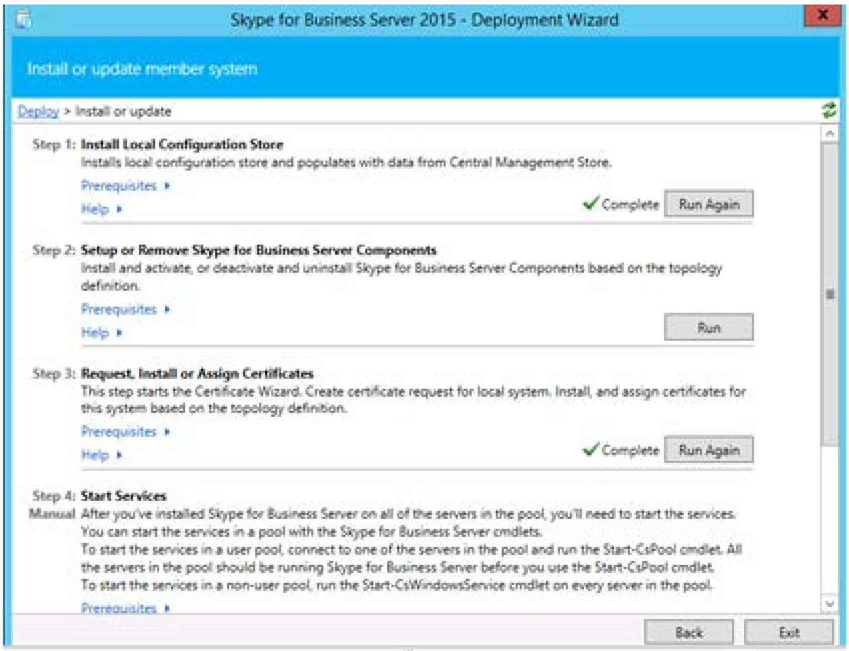


```
PS C:\Users\eu.lyncadmin.DAYCO> Get-CsManagementStoreReplicationStatus


UpToDate            : True
ReplicaFqdn         : TR-SRVEDGE.\Fqdn .LOCAL
LastStatusReport    : 5/18/2016 11:46:43 AM
LastUpdateCreation  : 5/18/2016 11:46:40 AM
ProductVersion      : 6.0.9319.0

UpToDate            : True
ReplicaFqdn         : TR-SRVFREN.Fqdn).LOCAL
LastStatusReport    : 5/18/2016 11:46:42 AM
LastUpdateCreation  : 5/18/2016 11:46:40 AM
ProductVersion      : 6.0.9319.0

UpToDate            : True
ReplicaFqdn         : IV-SRVEDGE.\Fqdn'.LOCAL
LastStatusReport    : 5/18/2016 11:46:41 AM
LastUpdateCreation  : 5/18/2016 11:46:40 AM
ProductVersion      : 6.0.9319.0

UpToDate            : True
ReplicaFqdn         : IV-SRVFREN.\Fqdn'.LOCAL
LastStatusReport    : 5/18/2016 11:46:48 AM
LastUpdateCreation  : 5/18/2016 11:46:40 AM
ProductVersion      : 6.0.9319.0
```

12. On each FE server (not in parallel), run the Skype for Business Deployment Wizard.

13. In the Skype for Business Deployment Wizard, Run 'Step 2' as shown in the figure below.

Figure 11-109: Install or Update Database



Skype for Business Server 2015 - Deployment Wizard

Install or update member system

Deploy > Install or update

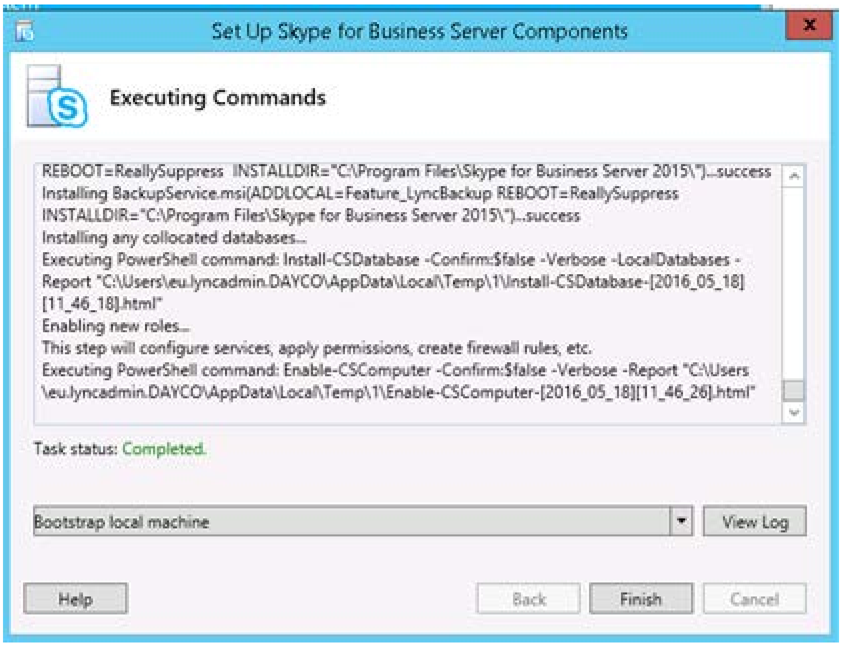
Step 1: **Install Local Configuration Store**
Installs local configuration store and populates with data from Central Management Store.
✓ Complete

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.

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.
✓ Complete

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.

Figure 11-110: Executing Install or Update Database



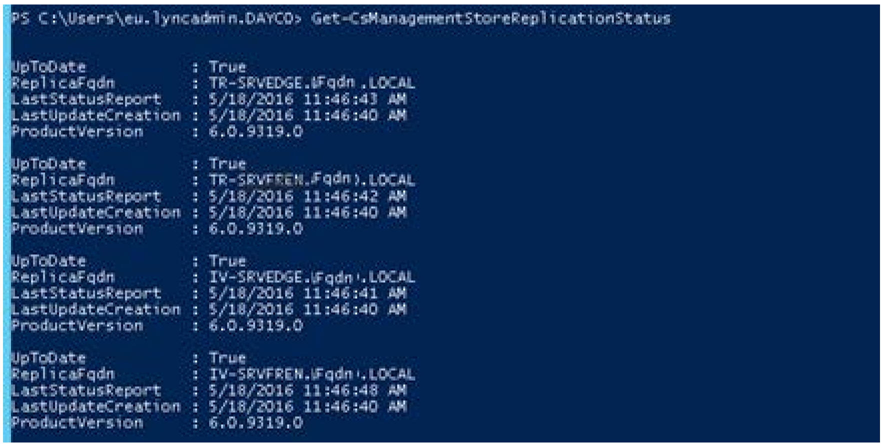
```
REBOOT=ReallySuppress  INSTALLDIR="C:\Program Files\Skype for Business Server 2015\")...success
Installing BackupService.msi(ADDLOCAL=Feature_LyncBackup REBOOT=ReallySuppress
INSTALLDIR="C:\Program Files\Skype for Business Server 2015\")...success
Installing any collocated databases...
Executing PowerShell command: Install-CSDatabase -Confirm:$false -Verbose -LocalDatabases -
Report "C:\Users\eu.lyncadmin.DAYCO\AppData\Local\Temp\1\Install-CSDatabase-[2016_05_18]
[11_46_18].html"
Enabling new roles...
This step will configure services, apply permissions, create firewall rules, etc.
Executing PowerShell command: Enable-CSComputer -Confirm:$false -Verbose -Report "C:\Users
\eu.lyncadmin.DAYCO\AppData\Local\Temp\1\Enable-CSComputer-[2016_05_18][11_46_26].html"
```

Task status: Completed.

Bootstrap local machine

14. With the Get-CsManagmentReplicationStatus command, make sure the CMS is updated on all servers.

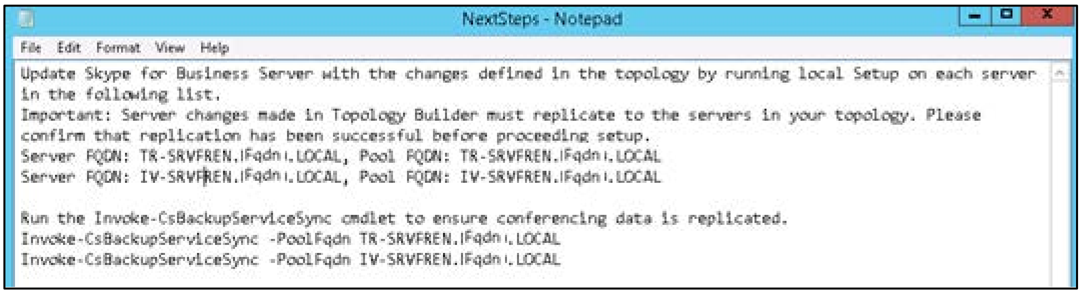
Figure 11-111: Making Sure the CMS is Updated on all Servers



```
PS C:\Users\eu.lyncadmin.DAYCO> Get-CsManagementStoreReplicationStatus


UpToDate            : True
ReplicaFqdn         : TR-SRVEDGE.lFqdn .LOCAL
LastStatusReport    : 5/18/2016 11:46:43 AM
LastUpdateCreation  : 5/18/2016 11:46:40 AM
ProductVersion      : 6.0.9319.0

UpToDate            : True
ReplicaFqdn         : TR-SRVFREN.Fqdn).LOCAL
LastStatusReport    : 5/18/2016 11:46:42 AM
LastUpdateCreation  : 5/18/2016 11:46:40 AM
ProductVersion      : 6.0.9319.0

UpToDate            : True
ReplicaFqdn         : IV-SRVEDGE.lFqdn'.LOCAL
LastStatusReport    : 5/18/2016 11:46:41 AM
LastUpdateCreation  : 5/18/2016 11:46:40 AM
ProductVersion      : 6.0.9319.0

UpToDate            : True
ReplicaFqdn         : IV-SRVFREN.lFqdn'.LOCAL
LastStatusReport    : 5/18/2016 11:46:48 AM
LastUpdateCreation  : 5/18/2016 11:46:40 AM
ProductVersion      : 6.0.9319.0
```

15. Run the Invoke-CsBackupServiceSync cmdlet on each server to make sure conferencing data is replicated. The following commands are listed in the to-do list after publishing the topology:

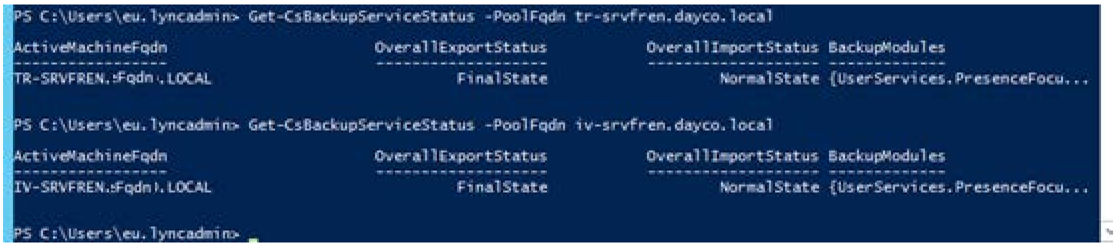
Figure 11-112: Commands Listed in the To-Do List after Publishing the Topology



```
Update Skype for Business Server with the changes defined in the topology by running local Setup on each server
in the following list.
Important: Server changes made in Topology Builder must replicate to the servers in your topology. Please
confirm that replication has been successful before proceeding setup.
Server FQDN: TR-SRVFREN.lFqdnl.LOCAL, Pool FQDN: TR-SRVFREN.lFqdnl.LOCAL
Server FQDN: IV-SRVFREN.lFqdnl.LOCAL, Pool FQDN: IV-SRVFREN.lFqdnl.LOCAL

Run the Invoke-CsBackupServiceSync cmdlet to ensure conferencing data is replicated.
Invoke-CsBackupServiceSync -PoolFqdn TR-SRVFREN.lFqdnl.LOCAL
Invoke-CsBackupServiceSync -PoolFqdn IV-SRVFREN.lFqdnl.LOCAL
```

16. Check the Pool-Pairing status (FinalState) with Get-CSBackupServicesStatus:

Figure 11-113: Checking the Pool-Pairing Status (FinalState)



```
PS C:\Users\eu.lyncadmin> Get-CsBackupServiceStatus -PoolFqdn tr-srvfren.dayco.local

ActiveMachineFqdn                    OverallExportStatus          OverallImportStatus BackupModules
-----------------                    -------------------          ------------------- -------------
TR-SRVFREN.<Fqdn>.LOCAL                       FinalState                  NormalState {UserServices.PresenceFocu...

PS C:\Users\eu.lyncadmin> Get-CsBackupServiceStatus -PoolFqdn iv-srvfren.dayco.local

ActiveMachineFqdn                    OverallExportStatus          OverallImportStatus BackupModules
-----------------                    -------------------          ------------------- -------------
IV-SRVFREN.<Fqdn>.LOCAL                       FinalState                  NormalState {UserServices.PresenceFocu...

PS C:\Users\eu.lyncadmin> _
```

11.13.2 Pairing Pools in DNS

To complete the setup of a paired pool, the DNS records will need to be reviewed and modified so that users can locate the surviving Front End pool in the event of a failure.

The most common way to do this is to add a weighted SRV record pointing to the second FE server. When this method is used, all Skype for Business clients will initially contact the first FE pool indicated by the SRV records. The first FE pool will redirect clients homed on the second FE to that FE Pool, thus some minor additional traffic is encountered by the First FE pool. During a failure, the clients will use the second weighted SRV record to locate the surviving FE Pool.

You may choose other methods to control client logins, such as geographic DNS records. These will redirect client logins to their local FE pool and minimize traffic.

11.13.3 Failing Over

Paired pools offer automatic failover for Enterprise Voice traffic, but not for other features of Skype for Business. Failover between servers is a manual process. After a server fails, and before manual failover is completed, clients will experience restrictions and limited functionality.

Microsoft documentation for the failover process can be found at: https://technet.microsoft.com/en-us/library/jj204678%28v=ocs.15%29.aspx

In the following command examples, it is assumed that uc-fe.ac-onebox.com has failed, and must be switched to the surviving uc-fe2.ac-onebox.com

11.13.3.1 Edge Pool Next Hop

If an Edge server uses the failed FE pool as the next hop, and that edge server has not failed and is still available, you will have to change the Edge server to use a surviving FE pool as the next hop.

```
Set-CsEdgeServer -Identity EdgeServer:uc-edge.ac-onebox.com -
Registrar   Registrar:uc-fe2.ac-onebox.com
```

11.13.3.2 Central Management Store

If your CMS is located on the failed FE server, you will need to fail it over to the remaining server. You can check the CMS location with *Get-CsManagementConnection.*

In the Skype for Business Management Shell on the surviving FE server, enter the commands:

```
Get-CsManagementConnection
Invoke-CsManagementServerFailover –BackupSqlServerFQDN uc-fe2.ac-
onebox.com –BackupSqlServerInstance rtc -force
```

11.13.3.3 Users

To failover the users, enter the command:

```
Invoke-CsPoolFailOver -PoolFqdn uc-fe.ac-onebox.com -DisasterMode
```

11.13.4 Failing Back

Once the failed server has been recovered and brought back online, you can fallback the users and CMS as required.

Note that the CMS location does not need to be changed and can remain in its current location if desired.

11.13.4.1 Edge Pool Next Hop

If an Edge server next hop pool was changed, you can optionally change the Edge next hop value back to its original location. For a paired pool within the same site, this may not be required, but if the FE and Edge are now on separate sites, the next hop should be returned to minimize cross WAN traffic.

```
Set-CsEdgeServer -Identity EdgeServer:uc-edge.ac-onebox.com -
Registrar   Registrar:uc-fe.ac-onebox.com
```

11.13.4.2 Central Management Store

To return the CMS to its original location, in the Skype for Business Management Shell on the repaired a FE server, enter the commands:

```
Get-CsManagementConnection
Invoke-CsManagementServerFailover –BackupSqlServerFQDN uc-fe.ac-
onebox.com
 –BackupSqlServerInstance rtc -force
```

11.13.4.3 Users

To return users to their original home pool, on the repaired FE server, enter the command:

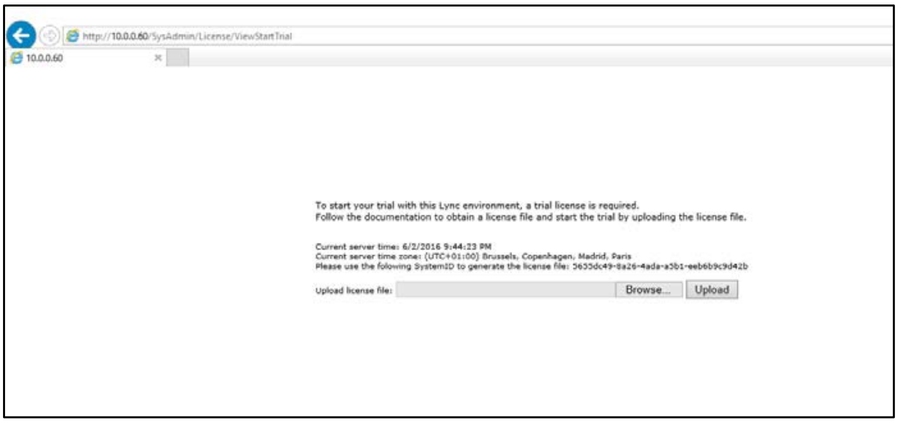
```
Invoke-CsPoolFailBack -PoolFqdn uc-fe.ac-onebox.com
```

11.14 Installing the Product License

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 Enterprise License is based on a unique “System ID” (Fingerprint) which is based on an AD contact field. The “System ID” key is available the first time you try to login to the CloudBond 365 using the CloudBond 365 sysadmin.

Figure 11-114: Uploading License File



To start your trial with this Lync environment, a trial license is required.
Follow the documentation to obtain a license file and start the trial by uploading the license file.

Current server time: 6/2/2016 9:44:23 PM
Current server time zone: (UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Please use the folowing SystemID to generate the license file: 5635dc49-8a26-4ada-a3b1-eeb6b9c9d42b

Upload license file: Browse... Upload

The “System ID” is also available in the CloudBond 365 management tool **System Configuration** -> **Licensing Info** page.

The first time a CloudBond 365 system is ordered for an enterprise the AudioCodes system generated a unique “Product Key” that represents the customer enterprise system. The Product key is sent to the customer/channel upon system ordering via email.

To activate your CloudBond 365 system you will need both a “Product Key” and a “System ID” (Fingerprint). Once you have both keys you can activate your product through AudioCodes License Activation tool at http://www.audiocodes.com/swactivation.

An e-mail will subsequently be sent to you with your Product License.

11.15 Activating Windows

CloudBond 365 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 CloudBond 365 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.

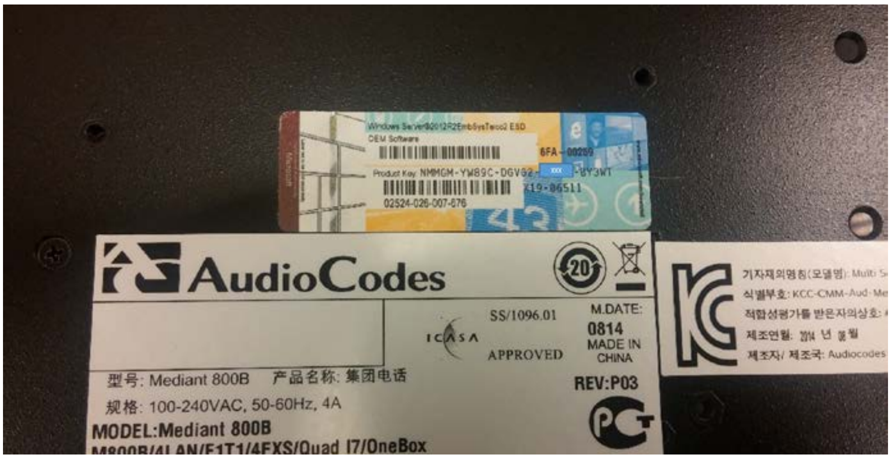
Note: Make sure your host server and all virtual machines have Internet access when activating the Windows license.

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. In the case of CloudBond 365 Pro with three stickers, it allows to activate the host and six virtual machines.

The CloudBond 365 Standard Box Edition contains one Windows 2012 R2 OEM license that allows you to license the Host, FE and Edge servers.

Figure 11-115: CloudBond 365 Standard Box Edition



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 Reverse Proxy server.

The CloudBond 365 Pro and Enterprise Box Editions contain three Windows 2012 R2 OEM license stickers that allows you to license the Host, DC and FE servers with the first sticker product key. The second sticker product key is for licensing the Edge and Reverse Proxy servers. The third sticker is available for licensing additional verified applications to be installed on the server.

Figure 11-116: CloudBond 365 Pro and Enterprise Box Editions

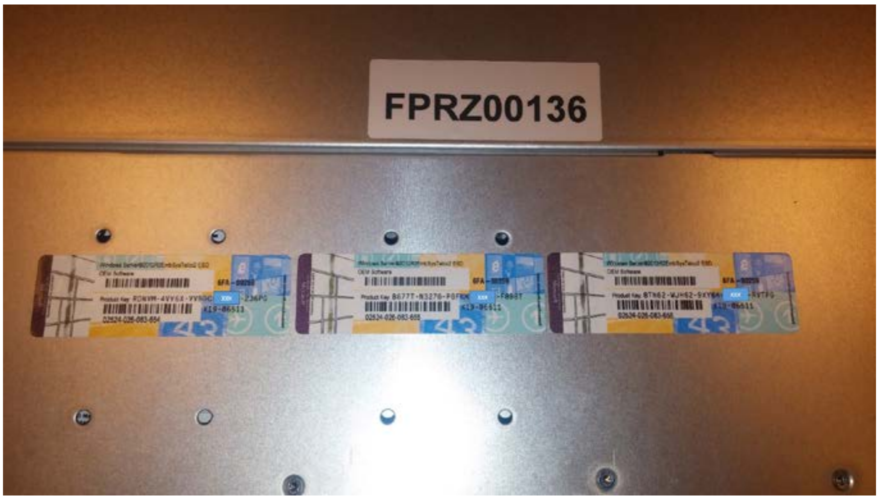
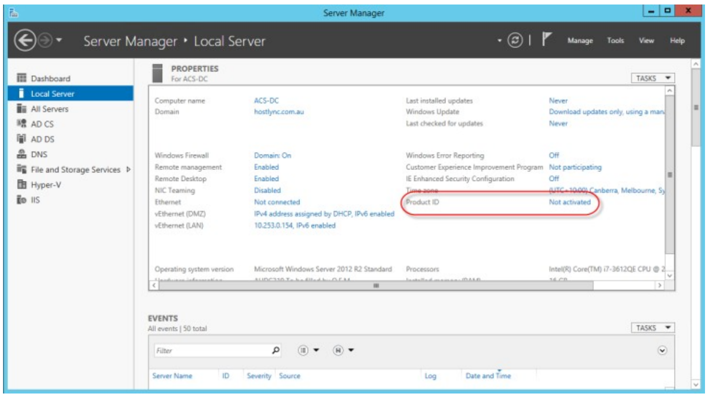


Figure 11-117: Activation using Server Manager



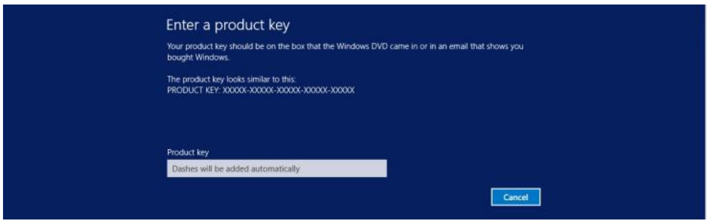
PROPERTIES
For ACS-DC

Computer name	ACS-DC	Last installed updates	Never
Domain	hostlync.com.au	Windows Update	Download updates only, using a man
		Last checked for updates	Never
Windows Firewall	Domain: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Enabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC+10:00) Canberra, Melbourne, Sy
Ethernet	Not connected	Product ID	Not activated
vEthernet (DMZ)	IPv4 address assigned by DHCP, IPv6 enabled		
vEthernet (LAN)	10.253.0.154, IPv6 enabled		
Operating system version	Microsoft Windows Server 2012 R2 Standard	Processors	Intel(R) Core(TM) i7-3612QE CPU @ 2

EVENTS
All events | 50 total

Server Name	ID	Severity	Source	Log	Date and Time

Figure 11-118: 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: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

Product key

Dashes will be added automatically

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.

11.16 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 CloudBond Windows operating system up-to-date with the latest hotfixes.

Refer to the Microsoft best practice guidelines regarding Windows Update: https://technet.microsoft.com/en-us/library/dn518337%28v=ocs.15%29.aspx

Note: If any unsupported or unapproved hotfix is found by the AudioCodes team, AudioCodes will officially publish a Product Notice regarding this issue.

Windows updates are configured to “automatically download updates” on all Windows Servers (Controller, Front End, and Edge) installed as part of a CloudBond 365 system.

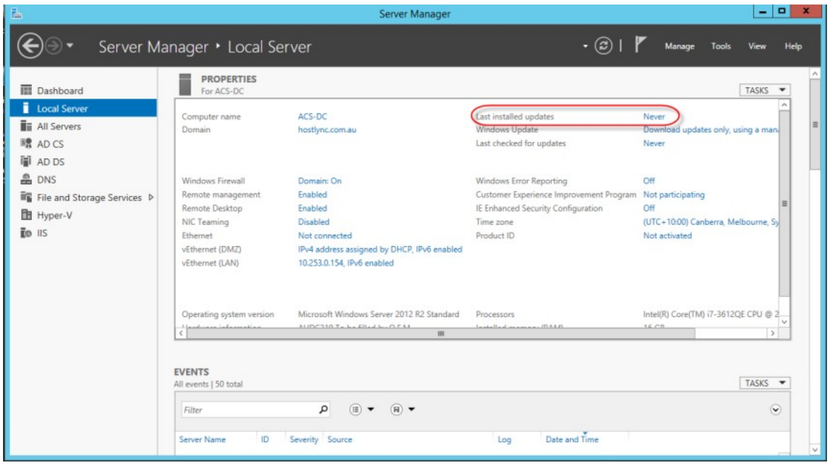
Note: Downloaded updates are not automatically installed. The Administrator should manually run the update at a convenient time e.g., after working hours.

You may modify these Windows Update settings to suit your requirements, or manually install updates at a convenient time.

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 11.21 for more details.

Figure 11-119: Accessing Windows Updates



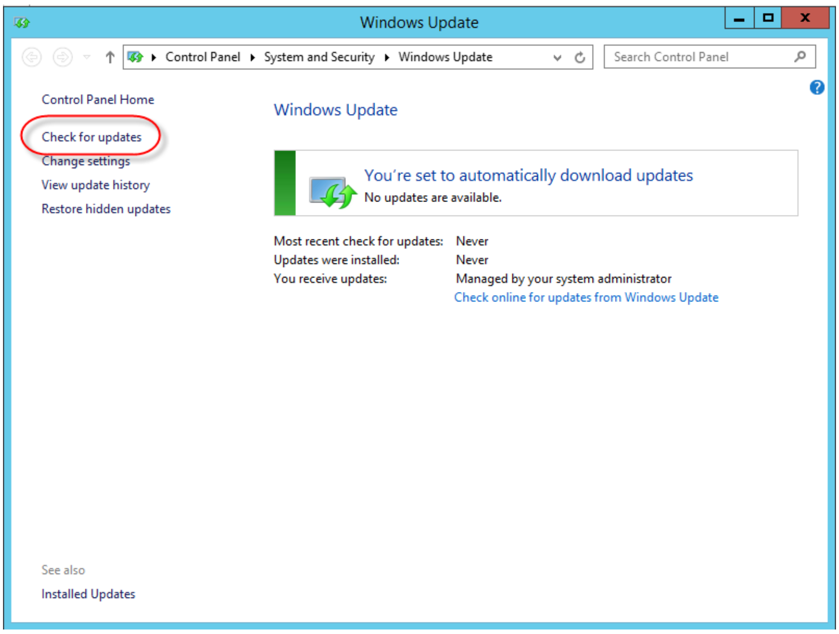
PROPERTIES
For ACS-DC

Computer name	ACS-DC	Last installed updates	Never
Domain	hostlync.com.au	Windows Update	Download updates only, using a man
		Last checked for updates	Never
Windows Firewall	Domain: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Enabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC+10:00) Canberra, Melbourne, Sy
Ethernet	Not connected	Product ID	Not activated
vEthernet (DMZ)	IPv4 address assigned by DHCP, IPv6 enabled		
vEthernet (LAN)	10.253.0.154, IPv6 enabled		
Operating system version	Microsoft Windows Server 2012 R2 Standard	Processors	Intel(R) Core(TM) i7-3612QE CPU @ 2

EVENTS
All events | 50 total

Server Name	ID	Severity	Source	Log	Date and Time

Figure 11-120: Checking for New Updates



Windows Update

You're set to automatically download updates

No updates are available.

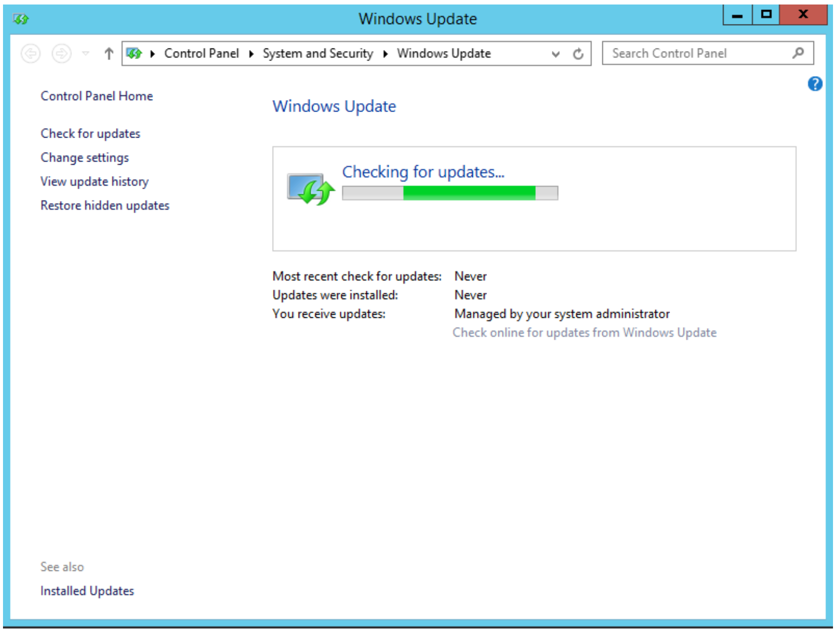
Most recent check for updates: Never

Updates were installed: Never

You receive updates: Managed by your system administrator

Check online for updates from Windows Update

Figure 11-121: Checking for New Updates



Windows Update

Checking for updates...

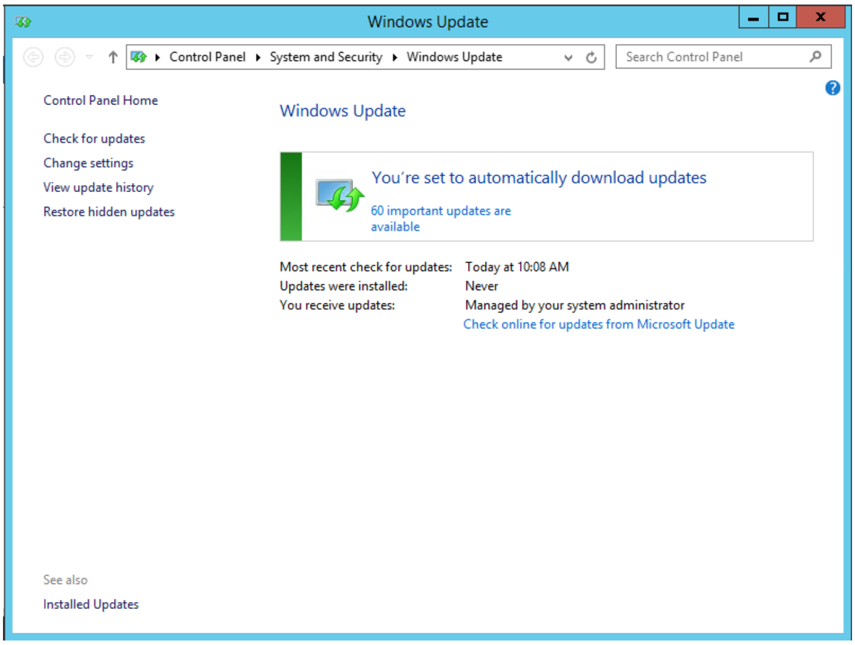
Most recent check for updates: Never

Updates were installed: Never

You receive updates: Managed by your system administrator

Check online for updates from Windows Update

Figure 11-122: New Updates Found



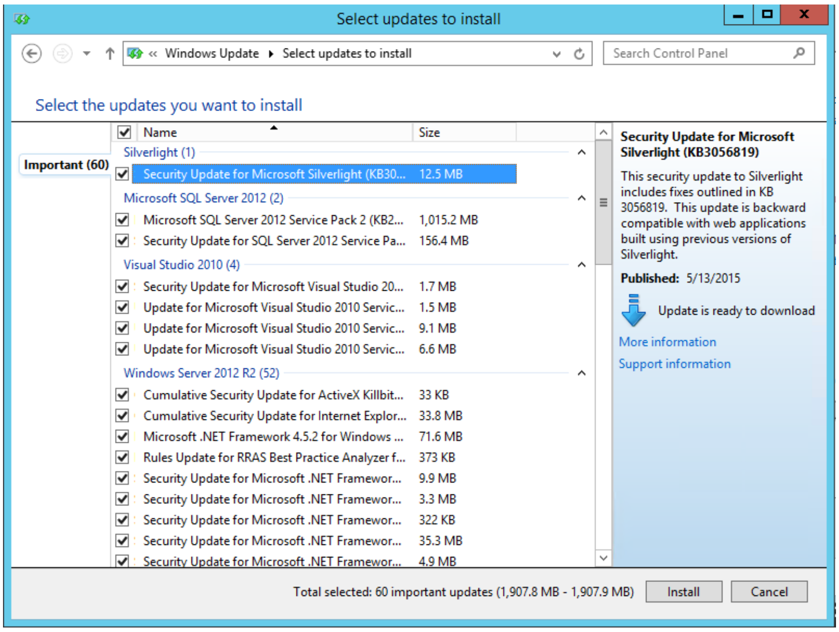
Windows Update

You're set to automatically download updates

60 important updates are available

Most recent check for updates:	Today at 10:08 AM
Updates were installed:	Never
You receive updates:	Managed by your system administrator Check online for updates from Microsoft Update

Figure 11-123: Selecting and Installing Update



Select updates to install
« Windows Update ▸ Select updates to install
Search Control Panel
Important (60)
Install
Cancel

Select the updates you want to install

☑ Name	Size
Silverlight (1)	
☑ Security Update for Microsoft Silverlight (KB30...	12.5 MB
Microsoft SQL Server 2012 (2)	
☑ Microsoft SQL Server 2012 Service Pack 2 (KB2...	1,015.2 MB
☑ Security Update for SQL Server 2012 Service Pa...	156.4 MB
Visual Studio 2010 (4)	
☑ Security Update for Microsoft Visual Studio 20...	1.7 MB
☑ Update for Microsoft Visual Studio 2010 Servic...	1.5 MB
☑ Update for Microsoft Visual Studio 2010 Servic...	9.1 MB
☑ Update for Microsoft Visual Studio 2010 Servic...	6.6 MB
Windows Server 2012 R2 (52)	
☑ Cumulative Security Update for ActiveX Killbit...	33 KB
☑ Cumulative Security Update for Internet Explor...	33.8 MB
☑ Microsoft .NET Framework 4.5.2 for Windows ...	71.6 MB
☑ Rules Update for RRAS Best Practice Analyzer f...	373 KB
☑ Security Update for Microsoft .NET Framewor...	9.9 MB
☑ Security Update for Microsoft .NET Framewor...	3.3 MB
☑ Security Update for Microsoft .NET Framewor...	322 KB
☑ Security Update for Microsoft .NET Framewor...	35.3 MB
☑ Security Update for Microsoft .NET Framewor...	4.9 MB

Security Update for Microsoft Silverlight (KB3056819)

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.

Published: 5/13/2015

Update is ready to download

More information

Support information

Total selected: 60 important updates (1,907.8 MB - 1,907.9 MB)

Unless you wish to avoid a specific update, it is generally easiest to accept the default selections and click Install.

11.17 CloudBond Infrastructure Updates

The CloudBond 365 system is built on top of different infrastructure modules such as Mediant 800, HP server, server BIOS and firmware, Windows OS, hardware and software drivers, Hyper-V, CloudBond 365 applications, etc. CloudBond was fully tested to operate and best perform with all infrastructure modules and together with CloudBond software applications.

It is not allowed to self-upgrade any of the CloudBond infrastructure or application modules without AudioCodes official instruction or without consulting an official AudioCodes representative.

11.17.1 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 CloudBond system.

It is recommended not to install a CU on the CloudBond 365 unless it has been approved by AudioCodes.

11.18 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.

11.19 Antivirus Application

No antivirus application is installed with CloudBond 365. To protect your CloudBond 365 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 https://technet.microsoft.com/en-us/library/mt629173.aspx.

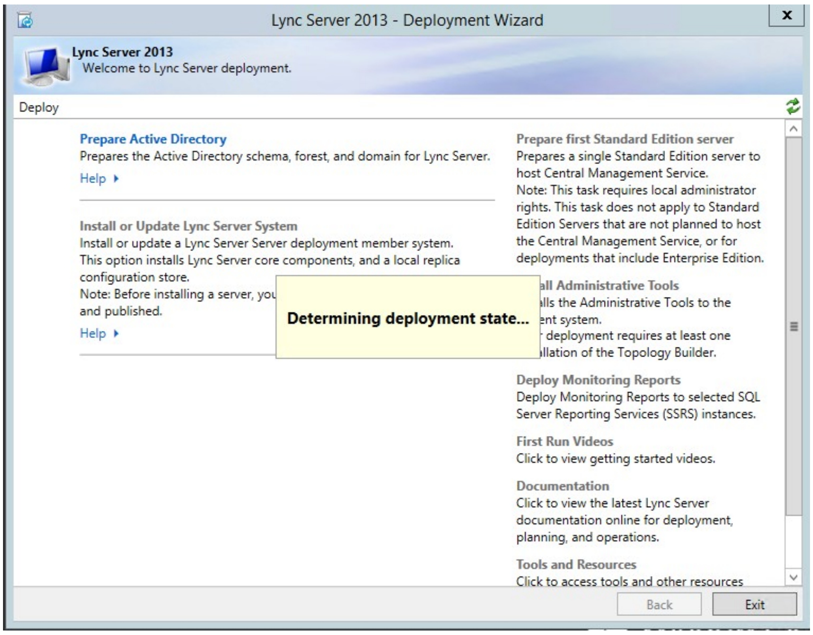
11.20 Running the Skype for Business Deployment Wizard

Normally, the Software Install Wizard will perform all Skype for Business Deployment steps for you automatically.

If creating a paired pool for resiliency purposes, this can only be done after the software install has been completed. For Paired Pools, it is necessary to run the Skype for Business Deployment wizard on each server, so that Topology Changes (paired pools) take effect.

To run the deployment wizard (on each FE and Edge server), locate the Skype for Business Deployment Wizard on the **Start** menu, and open the Utility.

Figure 11-124: Skype for Business Deployment Wizard



Lync Server 2013 - Deployment Wizard

Lync Server 2013
Welcome to Lync Server deployment.

Deploy

Prepare Active Directory
Prepares the Active Directory schema, forest, and domain for Lync Server.
Help ▸

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
and published.
Help ▸

Determining deployment state...

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.

ll Administrative Tools
lls the Administrative Tools to the
ent system.
deployment requires at least one
llation of the Topology Builder.

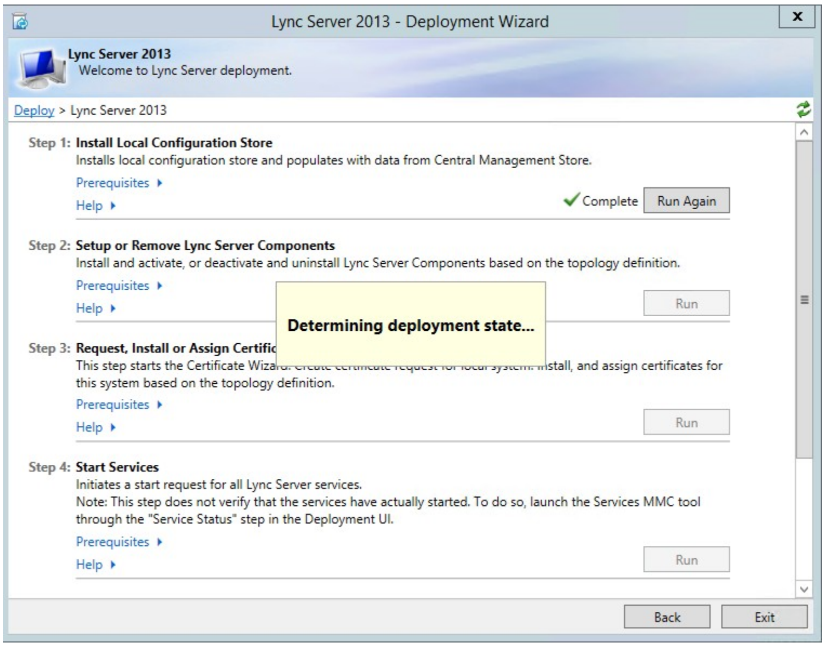
Deploy Monitoring Reports
Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances.

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

Figure 11-125: Setup or Remove Components



Lync Server 2013 - Deployment Wizard

Lync Server 2013
Welcome to Lync Server deployment.

Deploy > Lync Server 2013

Step 1: Install Local Configuration Store
Installs local configuration store and populates with data from Central Management Store.
Prerequisites ▸
Help ▸
✓ Complete Run Again

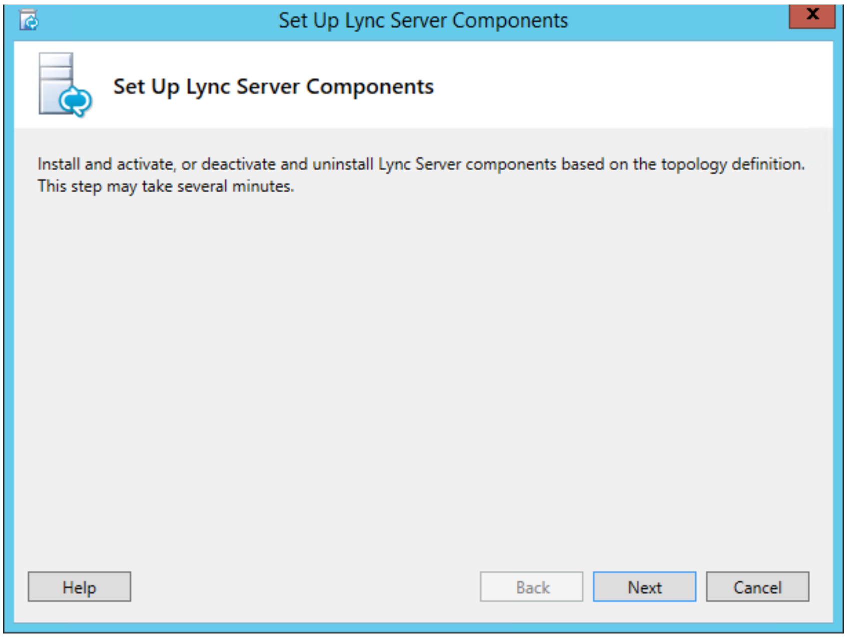
Step 2: Setup or Remove Lync Server Components
Install and activate, or deactivate and uninstall Lync Server Components based on the topology definition.
Prerequisites ▸
Help ▸
Run

Determining deployment state...

Step 3: Request, Install or Assign Certific
This step starts the Certificate Wiza nstall, and assign certificates for this system based on the topology definition.
Prerequisites ▸
Help ▸
Run

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 ▸
Help ▸
Run

Figure 11-126: Updating the Skype for Business Deployment

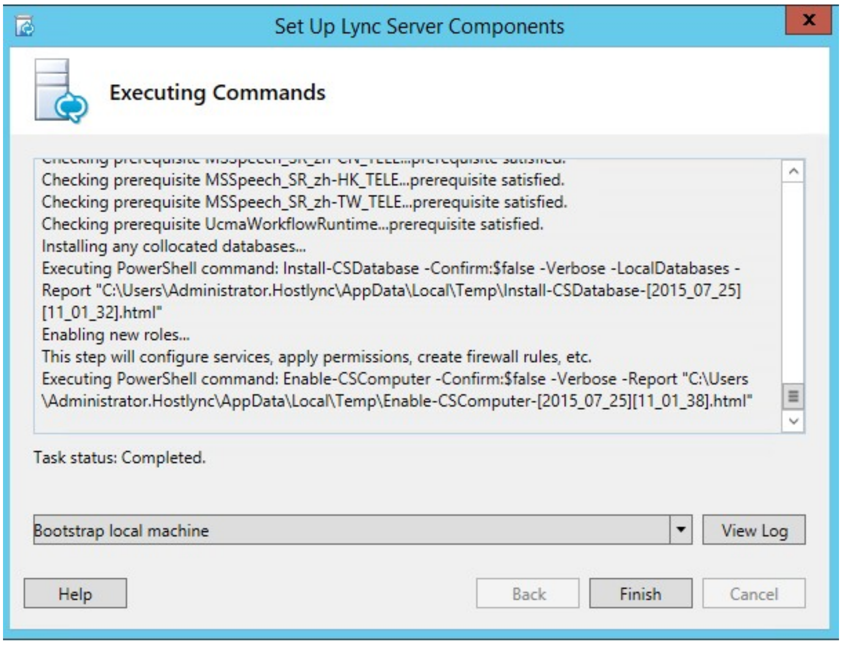


Set Up Lync Server Components

Set Up Lync Server Components

Install and activate, or deactivate and uninstall Lync Server components based on the topology definition. This step may take several minutes.

Figure 11-127: Skype for Business Deployment Results



Set Up Lync Server Components

Executing Commands

```
Checking prerequisite MSSpeech_SR_zh-CN_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_zh-HK_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_zh-TW_TELE...prerequisite satisfied.
Checking prerequisite UcmaWorkflowRuntime...prerequisite satisfied.
Installing any collocated databases...
Executing PowerShell command: Install-CSDatabase -Confirm:$false -Verbose -LocalDatabases -
Report "C:\Users\Administrator.Hostlync\AppData\Local\Temp\Install-CSDatabase-[2015_07_25]
[11_01_32].html"
Enabling new roles...
This step will configure services, apply permissions, create firewall rules, etc.
Executing PowerShell command: Enable-CSComputer -Confirm:$false -Verbose -Report "C:\Users
\Administrator.Hostlync\AppData\Local\Temp\Enable-CSComputer-[2015_07_25][11_01_38].html"
```

Task status: Completed.

Bootstrap local machine

11.21 Forwarding DNS Requests

The CloudBond 365 controller (UC-DC) acts as the DNS master for the CloudBond 365 system. It can resolve all necessary DNS lookup requests within the CloudBond 365 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 CloudBond 365 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.

1. Log on to UC-DC using remote desktop
2. Open the Administrative tools and DNS mmc
3. Right click the DNS server name and select properties
4. One the Forwarders tab, add the IP address of the more authoritative DNS server
5. Close the DNS mmc

DNS requests from the CloudBond 365 servers will now be passed to the CloudBond Controller (UC-DC) as normal. If the request is for an external name, the UC-DC DNS server will be unable to resolve the request, and will relay the request to the more authoritative DNS server for resolution.

Note: Failure to set DNS forwarding correctly will cause Windows Updates to fail.

Figure 11-128: Start -> Administrative Tools

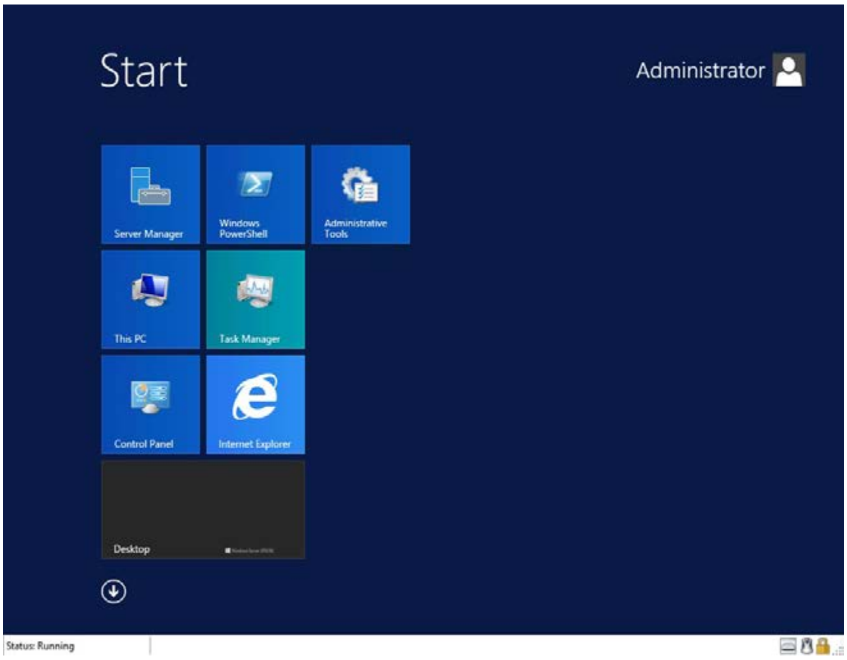
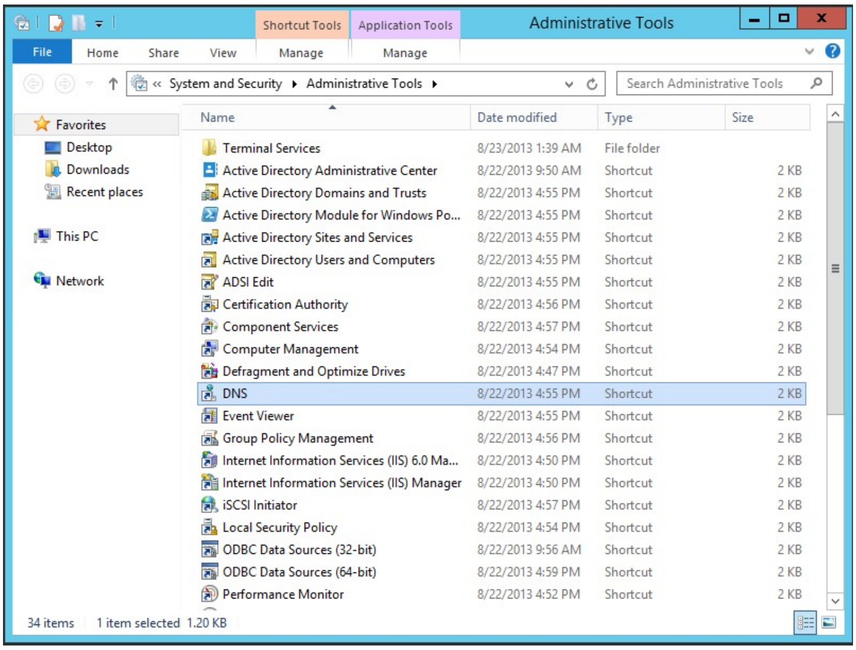


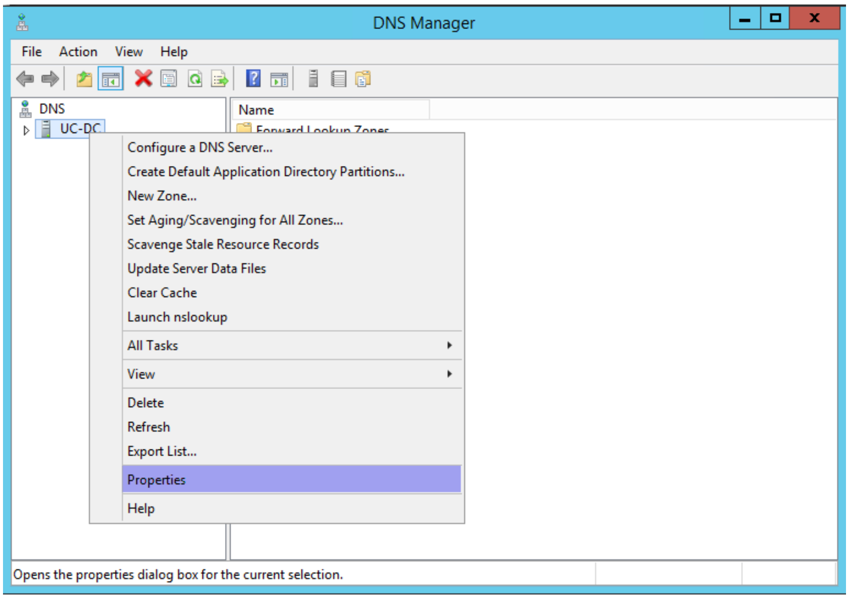
Figure 11-129: DNS MMC Tool



Name	Date modified	Type	Size
Terminal Services	8/23/2013 1:39 AM	File folder	
Active Directory Administrative Center	8/22/2013 9:50 AM	Shortcut	2 KB
Active Directory Domains and Trusts	8/22/2013 4:55 PM	Shortcut	2 KB
Active Directory Module for Windows Po...	8/22/2013 4:55 PM	Shortcut	2 KB
Active Directory Sites and Services	8/22/2013 4:55 PM	Shortcut	2 KB
Active Directory Users and Computers	8/22/2013 4:55 PM	Shortcut	2 KB
ADSI Edit	8/22/2013 4:55 PM	Shortcut	2 KB
Certification Authority	8/22/2013 4:56 PM	Shortcut	2 KB
Component Services	8/22/2013 4:57 PM	Shortcut	2 KB
Computer Management	8/22/2013 4:54 PM	Shortcut	2 KB
Defragment and Optimize Drives	8/22/2013 4:47 PM	Shortcut	2 KB
DNS	8/22/2013 4:55 PM	Shortcut	2 KB
Event Viewer	8/22/2013 4:55 PM	Shortcut	2 KB
Group Policy Management	8/22/2013 4:56 PM	Shortcut	2 KB
Internet Information Services (IIS) 6.0 Ma...	8/22/2013 4:50 PM	Shortcut	2 KB
Internet Information Services (IIS) Manager	8/22/2013 4:50 PM	Shortcut	2 KB
iSCSI Initiator	8/22/2013 4:57 PM	Shortcut	2 KB
Local Security Policy	8/22/2013 4:54 PM	Shortcut	2 KB
ODBC Data Sources (32-bit)	8/22/2013 9:56 AM	Shortcut	2 KB
ODBC Data Sources (64-bit)	8/22/2013 4:59 PM	Shortcut	2 KB
Performance Monitor	8/22/2013 4:52 PM	Shortcut	2 KB

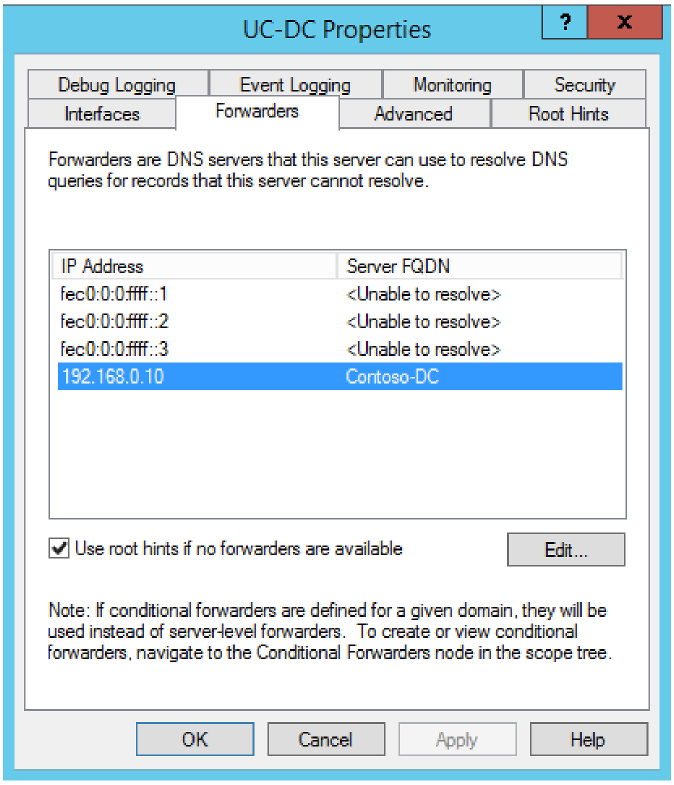
34 items 1 item selected 1.20 KB

Figure 11-130: Setting DNS Server Properties



Opens the properties dialog box for the current selection.

Figure 11-131: Adding Corporate DNS to Forwarders



Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.

IP Address	Server FQDN
fec0:0:0:ffff::1	<Unable to resolve>
fec0:0:0:ffff::2	<Unable to resolve>
fec0:0:0:ffff::3	<Unable to resolve>
192.168.0.10	Contoso-DC

☑ Use root hints if no forwarders are available

Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.

This page is intentionally left blank.

Part IV

Changing the Default Shipped Configuration

This part includes the following:

- Manual IP address assignment (see Chapter 12)
- Changing or adding a SIP domain (see Chapter 13)
- Edge Server to full DMZ deployment (see Chapter 14)

12 Manual IP Address Assignment

This chapter describes how to manually configure the IP addresses used by the AudioCodes CloudBond 365 Servers.

This guide provides:

- Information about manually configuring IP addresses for the AudioCodes CloudBond 365 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.

An AudioCodes CloudBond 365™ 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.

Throughout this guide, AudioCodes CloudBond 365 will be referred to as CloudBond 365.

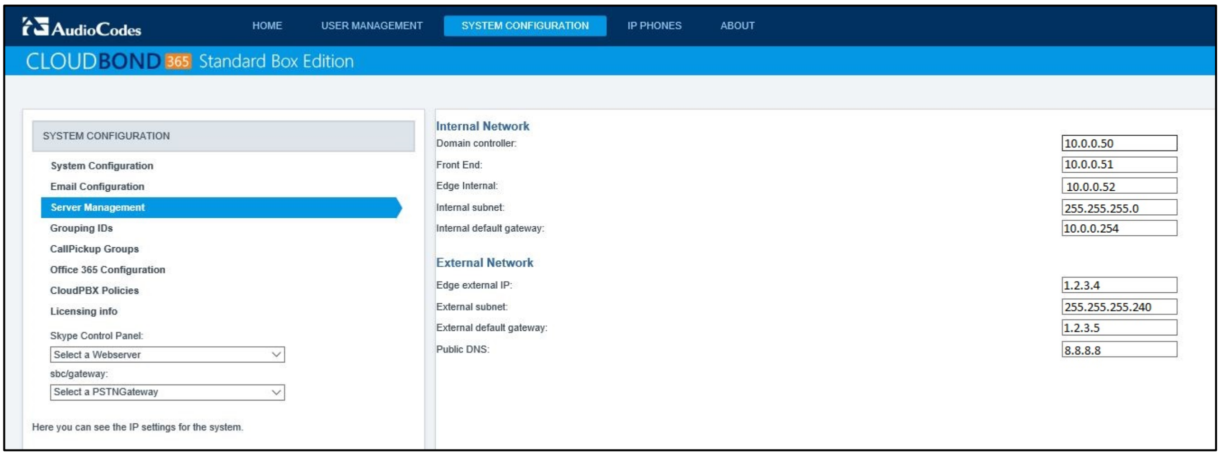
12.1 Why Manual Configuration?

From time to time, it may become necessary to manually change, or confirm, the IP address configuration of the CloudBond 365 Servers.

The CloudBond 365 Standard Box Edition Network settings are normally changed through http://192.168.0.101/sysadmin.

- TAB “system configuration”
- Server Management

Figure 12-1: Server Management (CloudBond 365)



Skype Control Panel: Select a Webserver

sbc/gateway: Select a PSTNGateway

Here you can see the IP settings for the system.

Internal Network

Domain controller:	10.0.0.50
Front End:	10.0.0.51
Edge Internal:	10.0.0.52
Internal subnet:	255.255.255.0
Internal default gateway:	10.0.0.254

External Network

Edge external IP:	1.2.3.4
External subnet:	255.255.255.240
External default gateway:	1.2.3.5
Public DNS:	8.8.8.8

However, this page is not normally available on CloudBond 365 Pro and Enterprise editions, due to the different build architecture used. It is also possible for this page to become unavailable on CloudBond 365 due to misconfiguration etc.

It is useful to know how to verify individual settings within the CloudBond 365 environment.

12.2 Default Configuration

The default configuration of the CloudBond 365 system is detailed below.

12.2.1 AudioCodes Mediant 800 Information (CloudBond 365)

12.2.1.1 Login

- Username: Admin
- Password: Admin

12.2.1.2 IP address information:

- Mediant 800 Gateway 192.168.0.2

12.2.2 CloudBond 365 Server information

12.2.2.1 Login

- Username: cloudbond365\Administrator
- Password: R3m0t3Supp0rt

12.2.2.2 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)
- All subnet masks 255.255.255.0

12.2.2.3 CloudBond 365 Domain Information

- Internal FQDN cloudbond365.local
- NetBIOS domain cloudbond365

12.2.2.4 CloudBond 365 Default Skype for Business Topology

- Default SIP domain
  - cloudbond365.local
- Simple URL's
  - https://meet.cloudbond365.local/dialin
  - https://meet.cloudbond365.local.com/meet
- FE Pool
  - uc-fe.cloudbond365.local
- External Web
  - ewslync.cloudbond365.local
- Edge Pool
  - uc-edge.cloudbond365.local
  - Access Edge sip.cloudbond365.local:5061
  - Web Conferencing sip.cloudbond365.local:444

- A/V Edge sip.cloudbond365.local:443

12.2.3 AudioCodes SBC (Optional)

12.2.3.1 Login

- Username: Admin
- Password: Admin

12.2.3.2 IP Address Information

- network-if 0 192.168.0.1

12.2.4 Reverse Proxy (Optional)

12.2.4.1 Login

- Username: Administrator
- Password: R3m0t3Supp0rt

12.2.4.2 IP Address Information

- Internal LAN 192.168.0.104
- External DMZ 192.168.254.104

12.3 Plan 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 CloudBond 365 system inoperative by misconfiguring the underlying IP network.

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

If you have a CloudBond 365, or you chose the Deployment Model: Co-Located Hyper-V / Domain Controller with Virtual Machines during software installation on CloudBond 365 Pro / Enterprise Edition, you should take extra care. In these cases, the Domain controller hosts the other servers as Hyper-V machine guest servers. Changing the address of the Domain Controller can prevent access to and correct operation of the Guest Virtual Machines.

12.4 How do I Make the Changes?

You may make changes to the CloudBond 365 IP Network by either:

- Attaching a local Monitor, Keyboard, and Mouse to the CloudBond 365 rear panel
- Starting an RDP Session to the CloudBond 365 Controller. Each option has advantages and disadvantages.

12.4.1 Local Monitor, Keyboard, and Mouse

Using a local monitor, keyboard and mouse allows you to make changes to the CloudBond 365 system without the worry of “losing connectivity” should you make an error in configuration. However, it does require physical access to the CloudBond 365, which may be difficult when installed in a server rack etc.

12.4.2 RDP Session

Using RDP sessions to connect to the CloudBond 365 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.

12.5 What Changes are Required?

Changes to IP addresses may be required to both CloudBond 365 core server components, as well as hardware devices and servers external to the CloudBond 365 software. You may also have to update DNS server to reflect the changes.

CloudBond 365 Core Components:

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

Devices and Servers external to the CloudBond 365 software are typically optional components, depending upon your chosen CloudBond 365 product and individual customer configuration.

E.g. CloudBond 365 includes an AudioCodes Mediant 800 gateway device which will probably require an IP Address change.

Keep in mind that these external devices and servers may need address changes.

As these optional devices may not be present, or may not be AudioCodes devices, they will all have individual methods for changing IP address. No attempt will be made to describe the process required. Please consult the individual device or server documentation.

CloudBond 365 External Components:

- Change any Media Gateway addresses, including Mediant 800 IP address
- Change any SBC addresses, including AudioCodes SBC IP address
- Change any Reverse Proxy addresses
- 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 communications are used.

12.5.1 Change the IP Addresses for Each Individual Server

Using RDP Sessions to each server, (or Hyper-V sessions from the CloudBond 365 Controller) you may change the IP address settings in Windows 2012 R2 for all individual servers (as shown in the figure below for the DC).

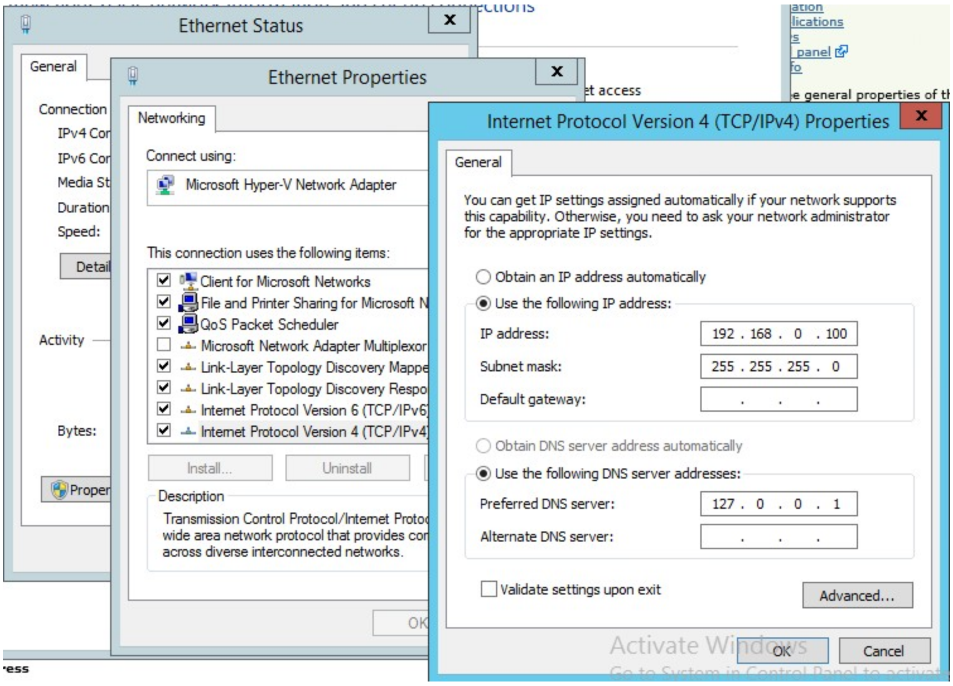
Note: The Edge server will have two interfaces, one for the internal IP and one for the external IP. The external DNS should point to a public DNS provider, such as your ISP. The internal DNS and gateway should be empty, as a Hosts file is used to lookup the internal server addresses.

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

1. In the Network and Sharing Center, click the **Ethernet** button; the Ethernet Status screen is displayed.

2. Select the IP interface and then click **Properties** to change the IP address settings as shown in the figures below.

Figure 12-2: Changing Individual Server Addresses



Connect using:

Microsoft Hyper-V Network Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft N
- ☑ QoS Packet Scheduler
- □ Microsoft Network Adapter Multiplexor
- ☑ Link-Layer Topology Discovery Mappe
- ☑ Link-Layer Topology Discovery Respo
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protoc wide area network protocol that provides co across diverse interconnected networks.

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 127 . 0 . 0 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

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 CloudBond 365 domain. Instead, use the actual Domain Controller IP address, such as 192.168.0.101.

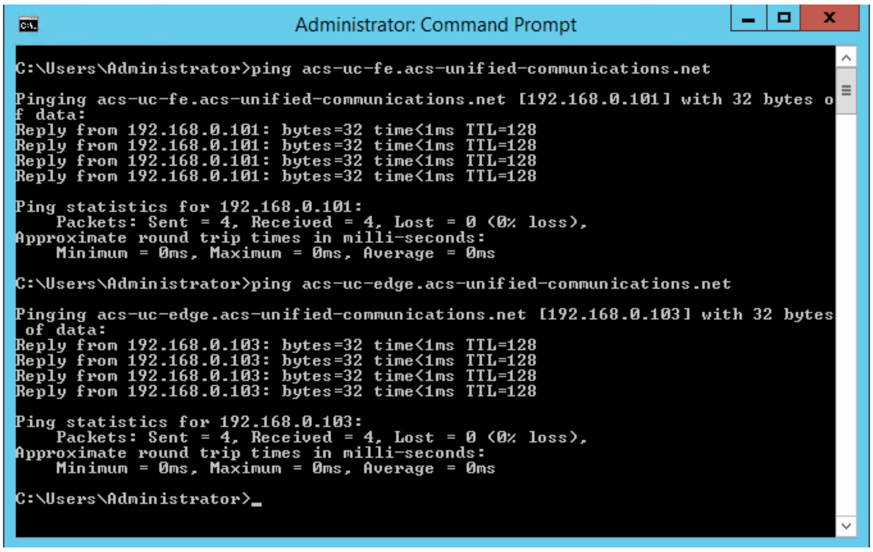
12.5.2 Confirm IP Addresses in DNS Server

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 CloudBond 365 Controller. The ping test should be performed by IP address as well as by DNS name.

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

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

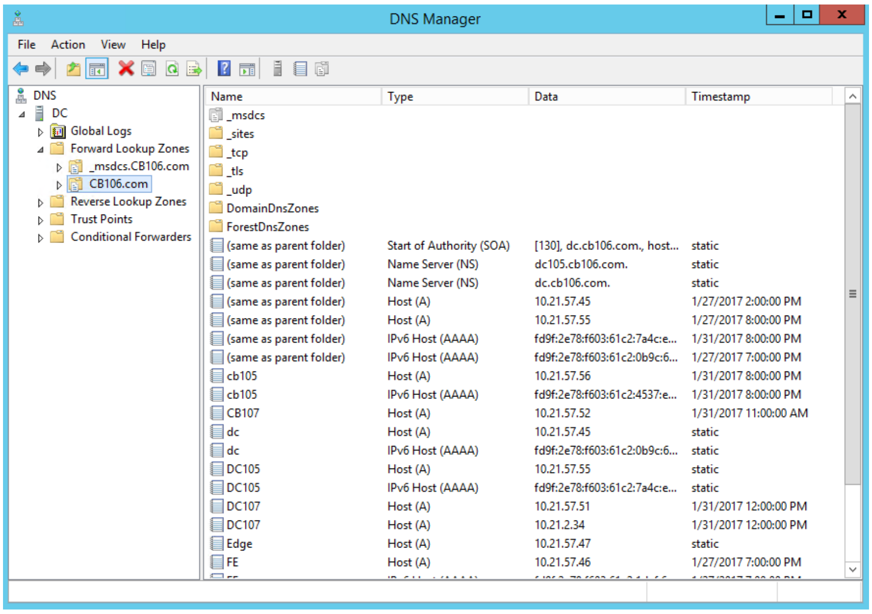
Figure 12-3: PING Tests



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

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

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

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

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

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

C:\Users\Administrator>_
```

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

Figure 12-4: Check DNS Updates



Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_tls			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[130], dc.cb106.com., host...	static
(same as parent folder)	Name Server (NS)	dc105.cb106.com.	static
(same as parent folder)	Name Server (NS)	dc.cb106.com.	static
(same as parent folder)	Host (A)	10.21.57.45	1/27/2017 2:00:00 PM
(same as parent folder)	Host (A)	10.21.57.55	1/27/2017 8:00:00 PM
(same as parent folder)	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:7a4c:e...	1/31/2017 8:00:00 PM
(same as parent folder)	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:0b9c:6...	1/27/2017 7:00:00 PM
cb105	Host (A)	10.21.57.56	1/31/2017 8:00:00 PM
cb105	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:4537:e...	1/31/2017 8:00:00 PM
CB107	Host (A)	10.21.57.52	1/31/2017 11:00:00 AM
dc	Host (A)	10.21.57.45	static
dc	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:0b9c:6...	static
DC105	Host (A)	10.21.57.55	static
DC105	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:7a4c:e...	static
DC107	Host (A)	10.21.57.51	1/31/2017 12:00:00 PM
DC107	Host (A)	10.21.2.34	1/31/2017 12:00:00 PM
Edge	Host (A)	10.21.57.47	static
FE	Host (A)	10.21.57.46	1/27/2017 7:00:00 PM

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

12.5.3 Change Topology Entries

On the CloudBond 365 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 (see Section 12.5.3.1)
- Simple URL's (see Section 12.5.3.2)
- Edge Settings (see Section 12.5.3.3)
- Publish Topology (see Section 12.5.3.4)

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 more information in Chapter 17 on page 299 and Chapter 113 on page 219.

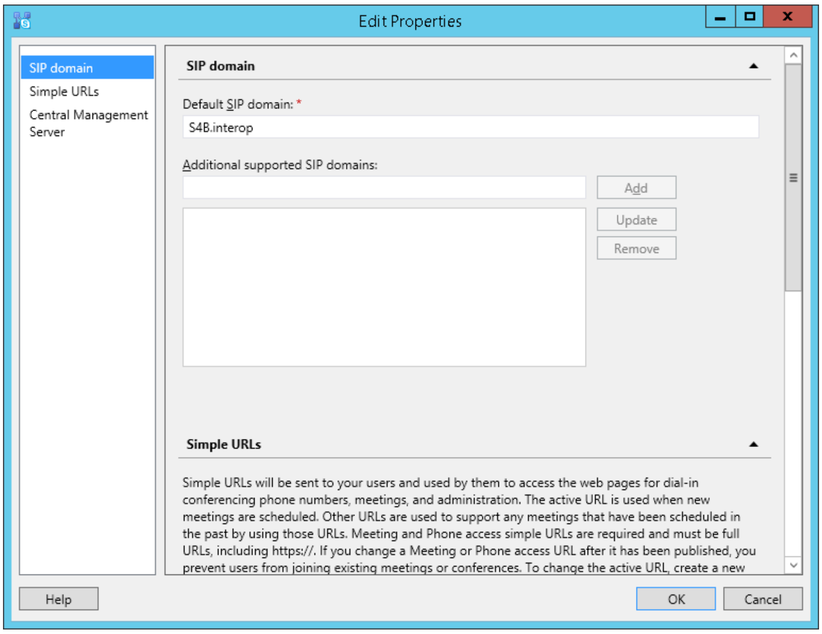
12.5.3.1 Default SIP Domain

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

➢ To change SIP domains:

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

Figure 12-5: Changing SIP Domains



Default SIP domain: *
S4B.interop

Additional supported SIP domains:

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

> **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
> ```

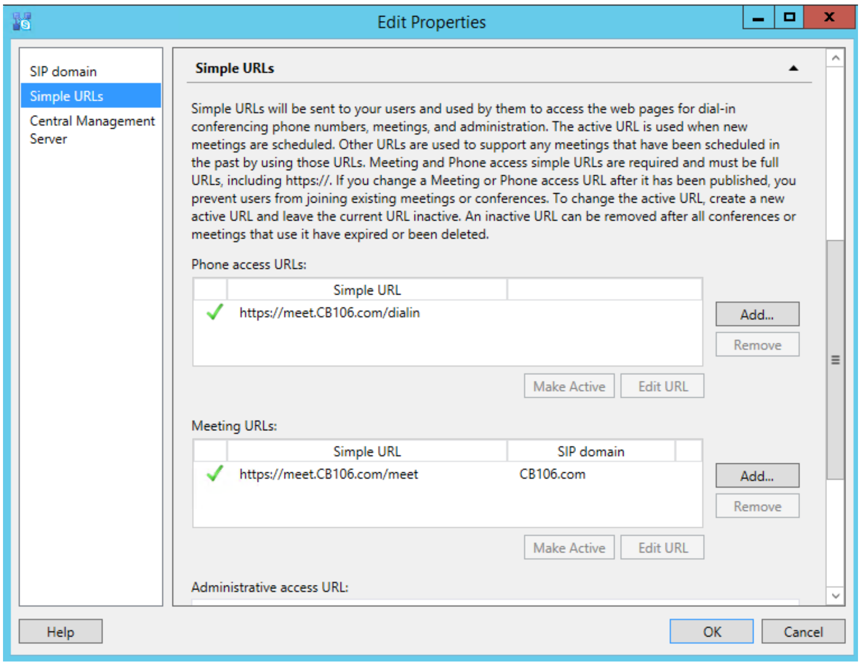
12.5.3.2 Simple URL's

You may need to modify 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 12-6: Changing Simple URL's



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

Phone access URLs:

	Simple URL	
✓	https://meet.CB106.com/dialin	

Meeting URLs:

	Simple URL	SIP domain
✓	https://meet.CB106.com/meet	CB106.com

Administrative access URL:

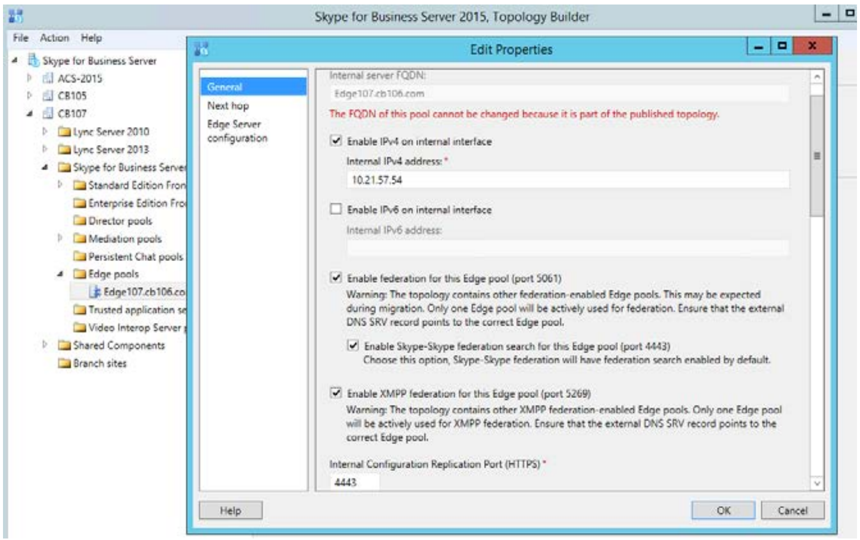
12.5.3.3 Edge Settings

The Edge server settings within the topology usually contain IP addresses 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 12-7: Changing Edge Server



Internal server FQDN:
Edge107.cb106.com
The FQDN of this pool cannot be changed because it is part of the published topology.

☑ Enable IPv4 on internal interface

Internal IPv4 address: *
10.21.57.54

□ Enable IPv6 on internal interface

Internal IPv6 address:

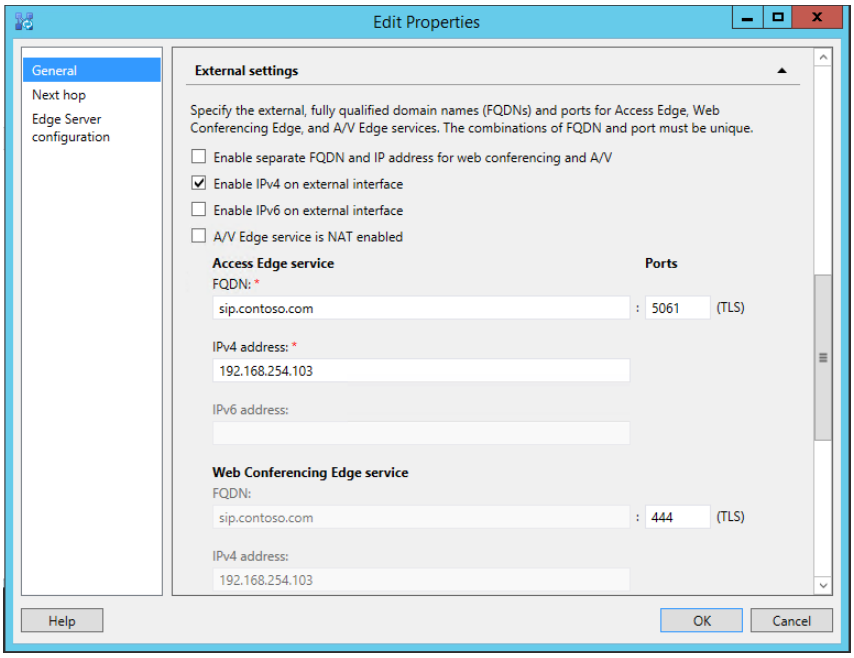
☑ Enable federation for this Edge pool (port 5061)
Warning: The topology contains other federation-enabled Edge pools. This may be expected during migration. Only one Edge pool will be actively used for federation. Ensure that the external DNS SRV record points to the correct Edge pool.

☑ Enable Skype-Skype federation search for this Edge pool (port 4443)
Choose this option, Skype-Skype federation will have federation search enabled by default.

☑ Enable XMPP federation for this Edge pool (port 5269)
Warning: The topology contains other XMPP federation-enabled Edge pools. Only one Edge pool will be actively used for XMPP federation. Ensure that the external DNS SRV record points to the correct Edge pool.

Internal Configuration Replication Port (HTTPS) *
4443

Figure 12-8: Changing Edge Server



External settings

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

□ Enable separate FQDN and IP address for web conferencing and A/V
☑ Enable IPv4 on external interface
□ Enable IPv6 on external interface
□ A/V Edge service is NAT enabled

Access Edge service **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

12.5.3.4 Publish the Topology Changes

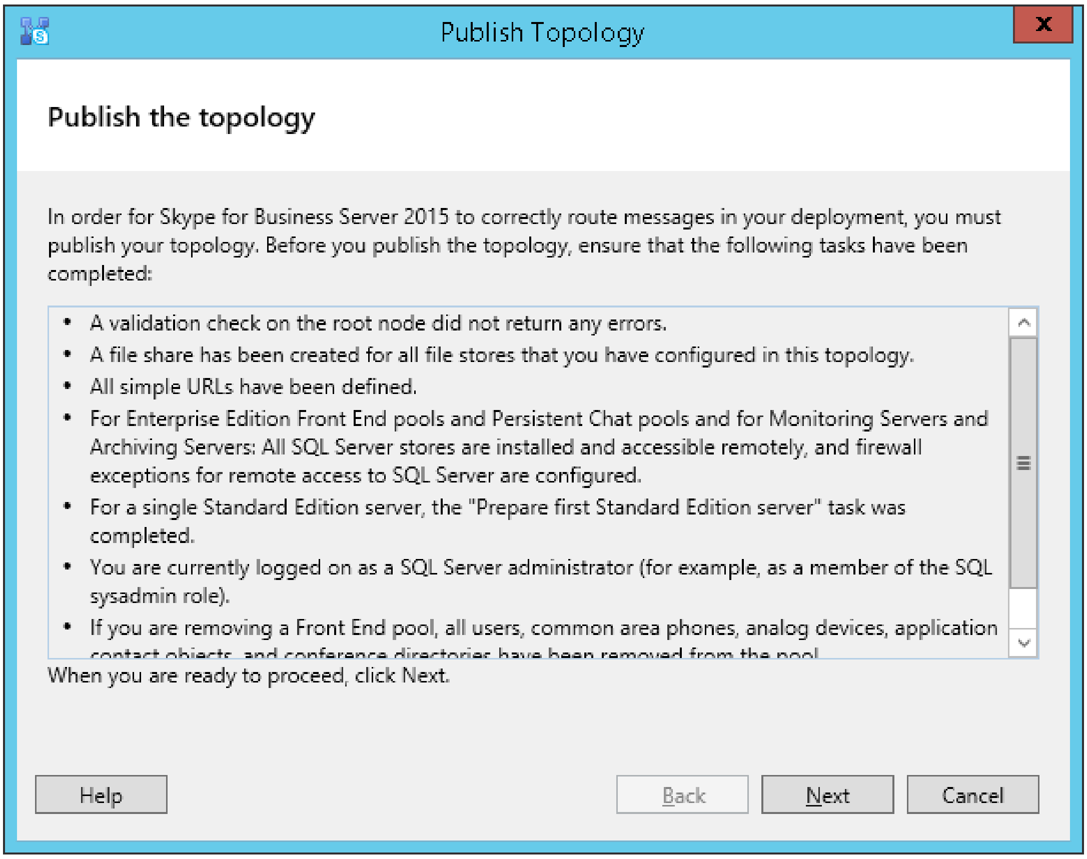
Once all topology changes are complete, publish the Skype for Business topology.

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

➢ **To publish Topology:**

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

Figure 12-9: Publish Topology



Publish the topology

In order for Skype for Business Server 2015 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:

- A validation check on the root node did not return any errors.
- A file share has been created for all file stores that you have configured in this topology.
- All simple URLs have been defined.
- 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.
- For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed.
- You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role).
- 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.

When you are ready to proceed, click Next.

12.5.4 Change Static DNS Records

The CloudBond 365 Edge server, Reverse Proxy server and Host server are not part of the CloudBond 365 domain for security reasons. As such, it uses a static DNS table (Hosts file) to find the IP addresses of the CloudBond 365 servers on the internal network.

Use the DNS entries from the CloudBond 365 Controller to manually update the Hosts file on the following platforms:

- Edge server (see Section 12.5.4.1)
- Reverse Proxy server (see Section 12.5.4.2)
- Host server (see Section 12.5.4.3)

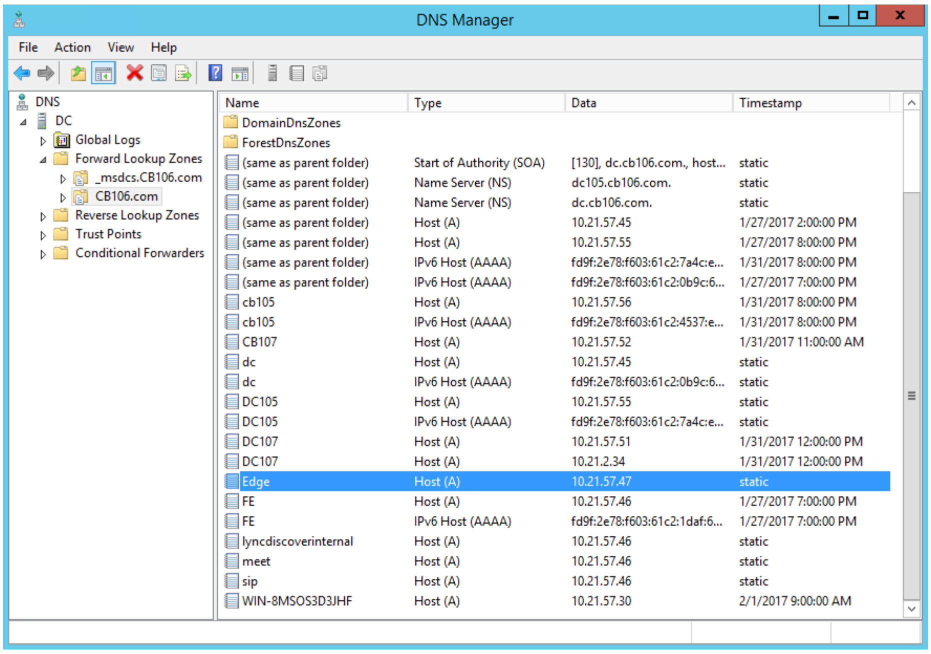
Note:

- The Reverse Proxy and the Host server settings are required only if your CloudBond 365 platform is managed by the AudioCodes Element Management System (EMS).
- The Host server applies to CloudBond 365 Pro Box and Enterprise Box editions.
- The Reverse Proxy server applies to CloudBond 365 Standard+ Box/Pro Box and Enterprise Box editions.

➢ To change static DNS records:

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

Figure 12-10: Change Static IP DNS Entries



Name	Type	Data	Timestamp
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[130], dc.cb106.com., host...	static
(same as parent folder)	Name Server (NS)	dc105.cb106.com.	static
(same as parent folder)	Name Server (NS)	dc.cb106.com.	static
(same as parent folder)	Host (A)	10.21.57.45	1/27/2017 2:00:00 PM
(same as parent folder)	Host (A)	10.21.57.55	1/27/2017 8:00:00 PM
(same as parent folder)	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:7a4c:e...	1/31/2017 8:00:00 PM
(same as parent folder)	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:0b9c:6...	1/27/2017 7:00:00 PM
cb105	Host (A)	10.21.57.56	1/31/2017 8:00:00 PM
cb105	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:4537:e...	1/31/2017 8:00:00 PM
CB107	Host (A)	10.21.57.52	1/31/2017 11:00:00 AM
dc	Host (A)	10.21.57.45	static
dc	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:0b9c:6...	static
DC105	Host (A)	10.21.57.55	static
DC105	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:7a4c:e...	static
DC107	Host (A)	10.21.57.51	1/31/2017 12:00:00 PM
DC107	Host (A)	10.21.2.34	1/31/2017 12:00:00 PM
Edge	Host (A)	10.21.57.47	static
FE	Host (A)	10.21.57.46	1/27/2017 7:00:00 PM
FE	IPv6 Host (AAAA)	fd9f:2e78:f603:61c2:1daf:6...	1/27/2017 7:00:00 PM
lyncdiscoverinternal	Host (A)	10.21.57.46	static
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

12.5.4.1 Modify the Edge Server Hosts File

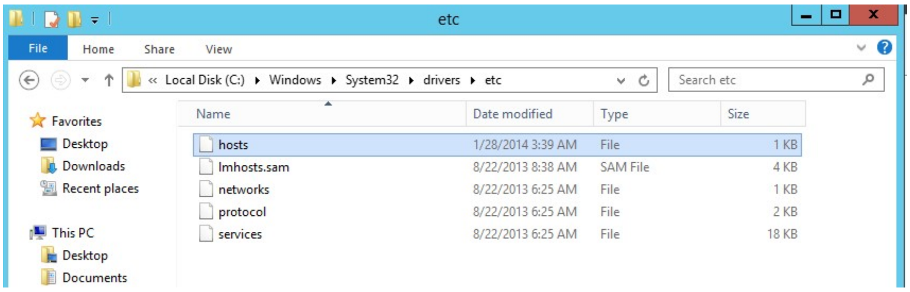
The Edge server is not a domain member, and has no reference to the internal DNS server.

You will need to manually edit the c:\windows\system32\drivers\etc\hosts file, so the Edge server can find the internal server FQDN names.

➢ **To modify the Edge Server Hosts file:**

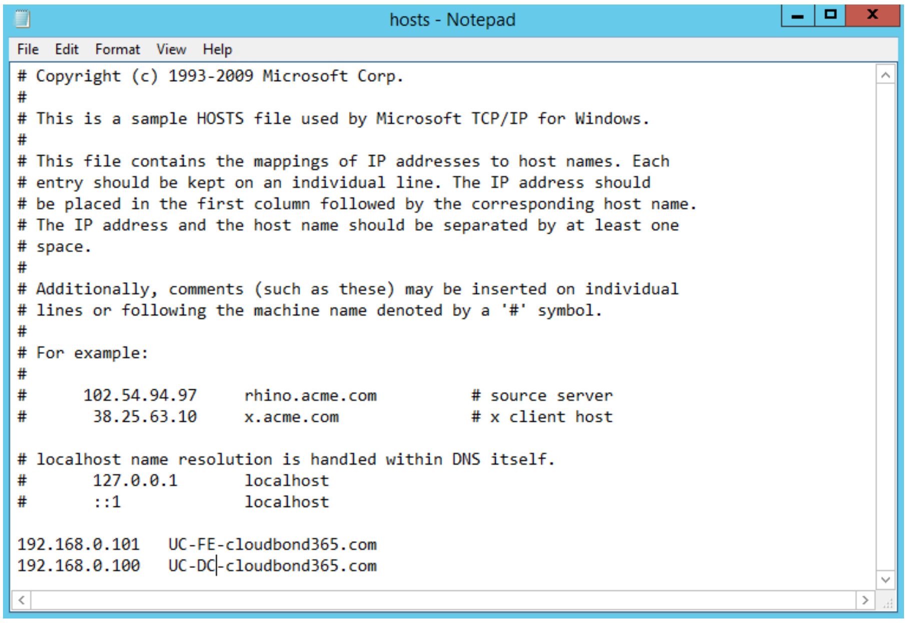
1. On the Edge server, open the Hosts file (C:\Windows\System32\drivers\etc).
2. Edit the file as required.

Figure 12-11: Locating the Hosts file



Name	Date modified	Type	Size
hosts	1/28/2014 3:39 AM	File	1 KB
lmhosts.sam	8/22/2013 8:38 AM	SAM File	4 KB
networks	8/22/2013 6:25 AM	File	1 KB
protocol	8/22/2013 6:25 AM	File	2 KB
services	8/22/2013 6:25 AM	File	18 KB

Figure 12-12: Modifying the Edge Server Hosts File



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

192.168.0.101   UC-FE-cloudbond365.com
192.168.0.100   UC-DC-cloudbond365.com
```

12.5.4.2 Modify the Reverse Proxy Server Hosts File

The Reverse Proxy 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.

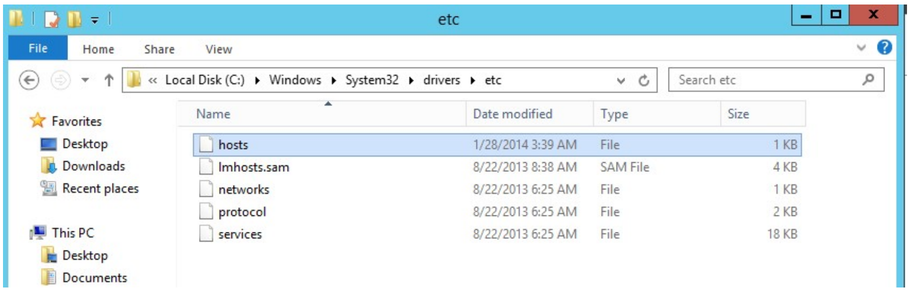
Note:

- This configuration is only required if your CloudBond 365 is managed by the AudioCodes Element Management System (EMS).
- The reverse Proxy is an optional component installed on the CloudBond 365 servers.

➢ **To modify the Reverse Proxy Server Hosts file:**

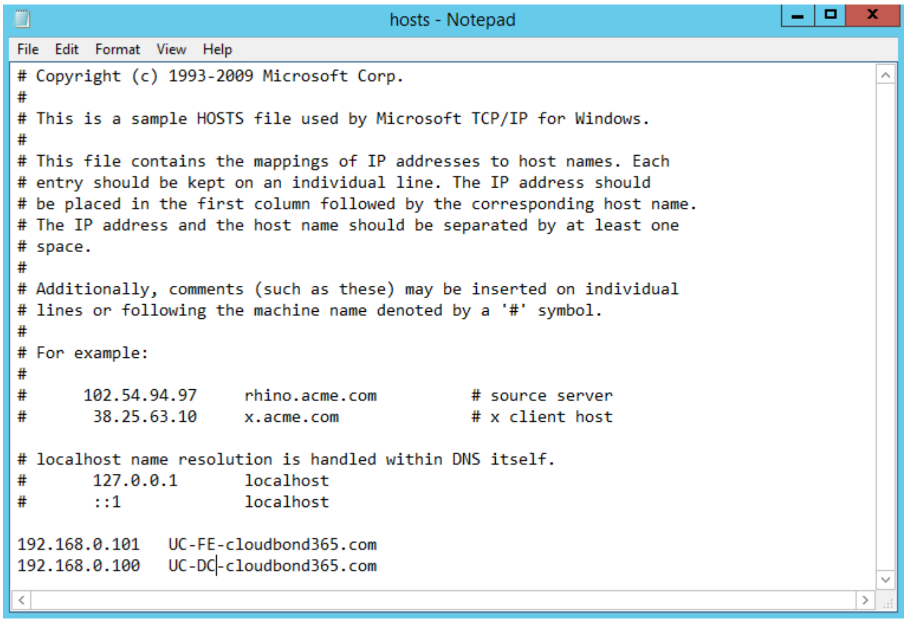
1. On the Reverse Proxy server, open the Hosts file (C:\Windows\System32\drivers\etc).
2. Edit the file as required.

Figure 12-13: Locating the Hosts file



Name	Date modified	Type	Size
hosts	1/28/2014 3:39 AM	File	1 KB
lmhosts.sam	8/22/2013 8:38 AM	SAM File	4 KB
networks	8/22/2013 6:25 AM	File	1 KB
protocol	8/22/2013 6:25 AM	File	2 KB
services	8/22/2013 6:25 AM	File	18 KB

Figure 12-14: Modifying the Reverse Proxy Server Hosts File



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

192.168.0.101   UC-FE-cloudbond365.com
192.168.0.100   UC-DC-cloudbond365.com
```

12.5.4.3 Modify the Host Server Hosts File

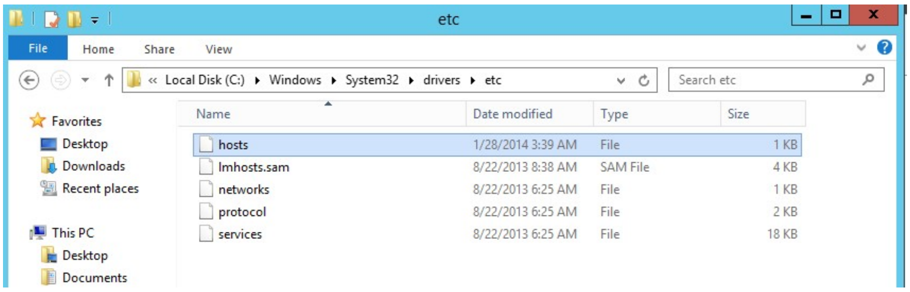
The Host server is not a domain member, and has no reference to the internal DNS server. You will need to manually edit the c:\windows\system32\drivers\etc\hosts file, so the Edge server can find the internal server FQDN names.

> **Note:**
> - This configuration only applies to the CloudBond 365 Pro and Enterprise Editions.
> - This configuration only applies to a CloudBond 365 installation that is managed by the AudioCodes Element Management System (EMS).

➢ **To modify the Host Server Hosts file:**

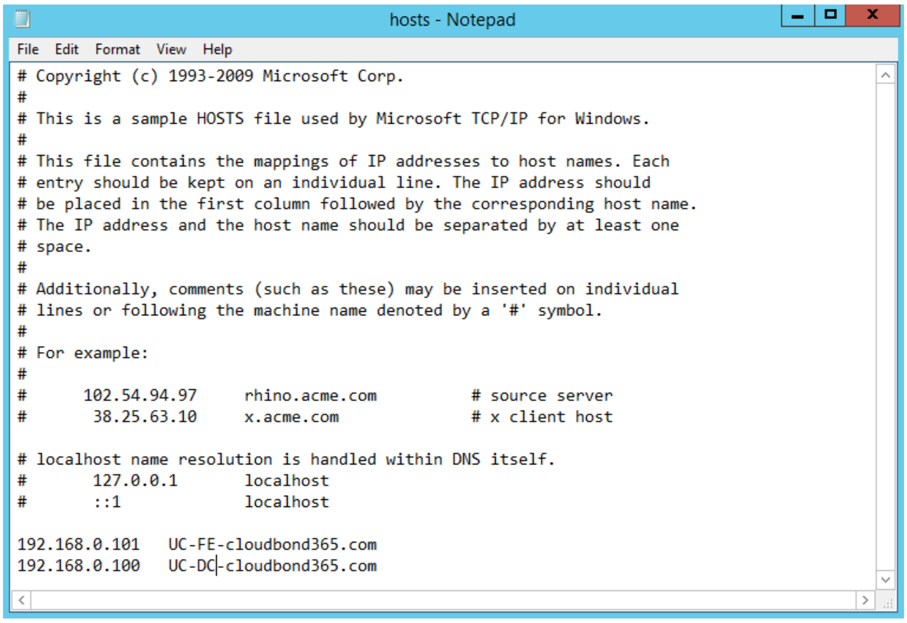
1. On the Host server, open the Hosts file (C:\Windows\System32\drivers\etc).
2. Edit the file as required.

Figure 12-15: Locating the Hosts File



Name	Date modified	Type	Size
hosts	1/28/2014 3:39 AM	File	1 KB
lmhosts.sam	8/22/2013 8:38 AM	SAM File	4 KB
networks	8/22/2013 6:25 AM	File	1 KB
protocol	8/22/2013 6:25 AM	File	2 KB
services	8/22/2013 6:25 AM	File	18 KB

Figure 12-16: Modifying the Host Server Hosts File



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1             localhost

192.168.0.101   UC-FE-cloudbond365.com
192.168.0.100   UC-DC-cloudbond365.com
```

12.5.5 Change the IP Address of the AudioCodes Devices

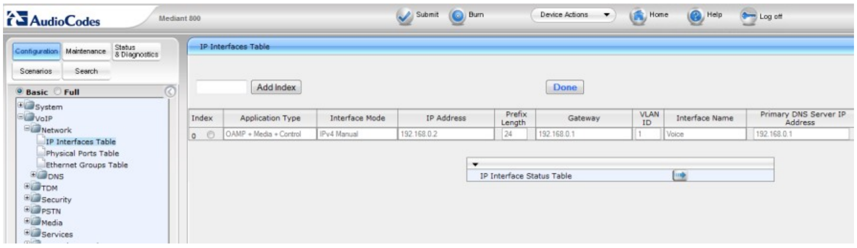
For the system to function correctly, the Mediant 800B and the Mediant VE SBC server should be assigned an address on the same internal network subnet as the CloudBond 365 Controller.

12.5.5.1 Mediant 800B IP Address (CloudBond 365 Standard Edition)

The CloudBond 365 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 365 Controller via the Mediant 800 front panel GE1 connector.

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

Figure 12-17: Changing the Mediant 800B Gateway



IP Interfaces Table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address
0 ○	OAMP + Media + Control	IPv4 Manual	192.168.0.2	24	192.168.0.1	1	Voice	192.168.0.1

12.5.5.2 Change AudioCodes SBC Server (Optional - CloudBond 365 Pro Box/Enterprise Box Editions)

The CloudBond 365 Pro Box and Enterprise Box editions can optionally install the Mediant VE SBC server on a virtual machine as a SIP Trunk gateway. The default address of this virtual machine is 192.168.0.1.

To change the default address for the SBC, please refer to the following guides:

- *Mediant Software SBC User's Manual*
- *Mediant Virtual Edition SBC Installation Manual*

12.5.6 Change Reverse Proxy Server (Optional - CloudBond 365 Standard+ Box/Pro Box/Enterprise Box Editions)

The CloudBond 365 Pro Box and Enterprise Box editions can optionally install an empty Windows 2012 R2 server which can be built as a Reverse Proxy server. The empty machine consists of two network adapters, one in the DMZ, and one on the corporate LAN.

These network adapters can have their IP addresses changed by standard Microsoft methods as described in Section 12.5.1.

Refer to page 203 for further details.

This page is intentionally left blank.

13 Changing or Adding a SIP Domain

This chapter describes how to change or add a SIP domain to the AudioCodes CloudBond 365™ system.

The SIP domain is very important to Skype for Business operations, as it provides the sign on and various other addresses within a Skype for Business environment. As Skype for Business uses TLS as a secured protocol, many other items must match the SIP address.

Throughout this guide, AudioCodes CloudBond 365 will be referred to as CloudBond 365.

> **Note:** CloudBond 365 includes a default certificate. This is a private internal certificate sufficient for CloudBond 365 internal connectivity only. 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 (yourdomain.com) and associated Simple URL's, DNS references, etc. are not suitable for the public internet.

13.1 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.

13.1.1 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.

13.1.2 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 access externally, they will not require public certificate entries.

13.2 CloudBond 365 and the SIP Domain

A CloudBond 365 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 CloudBond 365 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.

13.3 Changing or Adding a SIP Domain

Modifying the CloudBond 365 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

13.3.1 Overview of the Process

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 CloudBond 365 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 CloudBond 365, this will include the UC-FE and UC-Edge servers.

After publishing a topology change, the Skype for Business Deployment Wizard must be re-run on all Skype for Business servers (UC-FE and UC-Edge). For a SIP domain change, this will update the IIS configuration to recognize requests for the new SIP Domain simple URL's.

Changes to the SIP domains and Simple URL's have flow on requirements for DNS entries. We will need to update DNS entries for both internal and external DNS servers to match the new SIP domains. This includes many records, such as those used for Simple URL's, those used for Auto Configuration of Skype for Business Clients, and those used for Federation.

Changes to DNS entries require changes to SSL Certificates in order for the secured HTTPS and TLS protocol to work correctly. Updated Certificates will need to be installed on both the CloudBond 365-FE and CloudBond 365-Edge servers. This may involve a public certificate from your provider.

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

Lastly, you will 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.

13.3.2 Connect to CloudBond 365 Controller using RDP

Connect to the CloudBond controller. As an alternative, Hyper-V Manager on the CloudBond 365 Controller can be used to connect to the console of both the CloudBond 365 Front-End and Edge servers (UC-FE and UC-Edge).

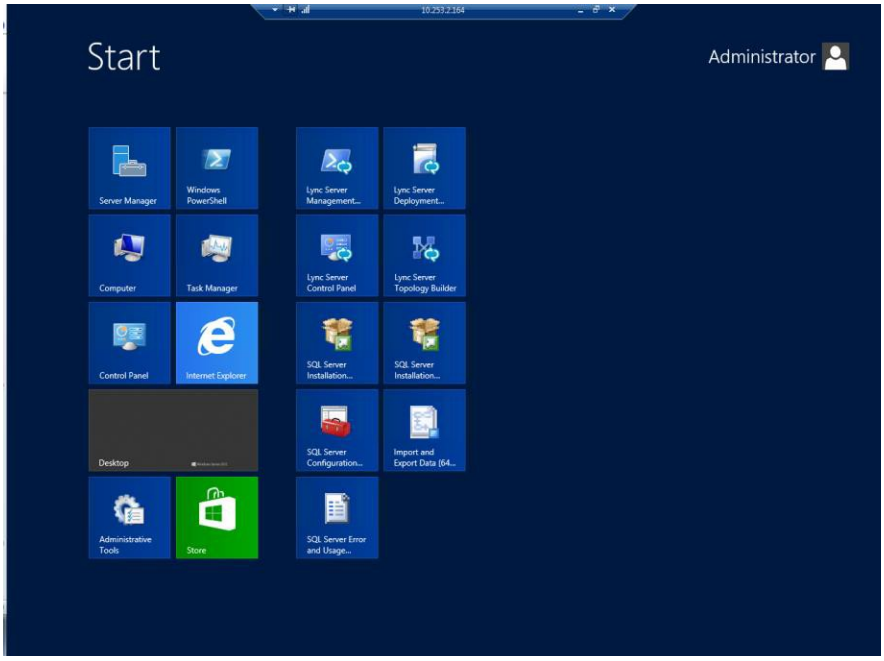
13.3.3 Use the Topology Builder

This section describes how to use the Topology Builder.

➢ **To use the Topology Builder:**

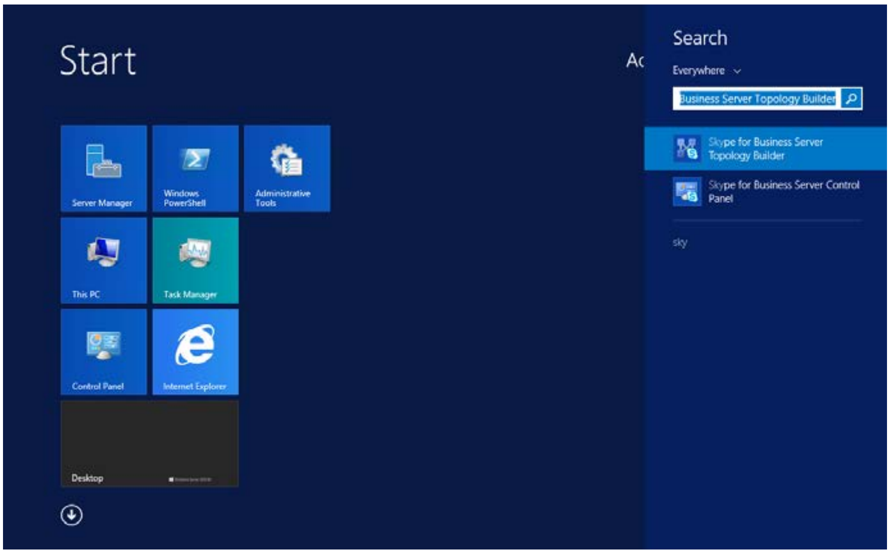
1. Open topology builder.

Figure 13-1: Topology Builder - From the CloudBond 365 Controller


10.253.2.164
Start
Administrator
Server Manager
Windows PowerShell
Lync Server Management...
Lync Server Deployment...
Computer
Task Manager
Lync Server Control Panel
Lync Server Topology Builder
Control Panel
Internet Explorer
SQL Server Installation...
SQL Server Installation...
Desktop
SQL Server Configuration...
Import and Export Data (64...
Administrative Tools
Store
SQL Server Error and Usage...

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

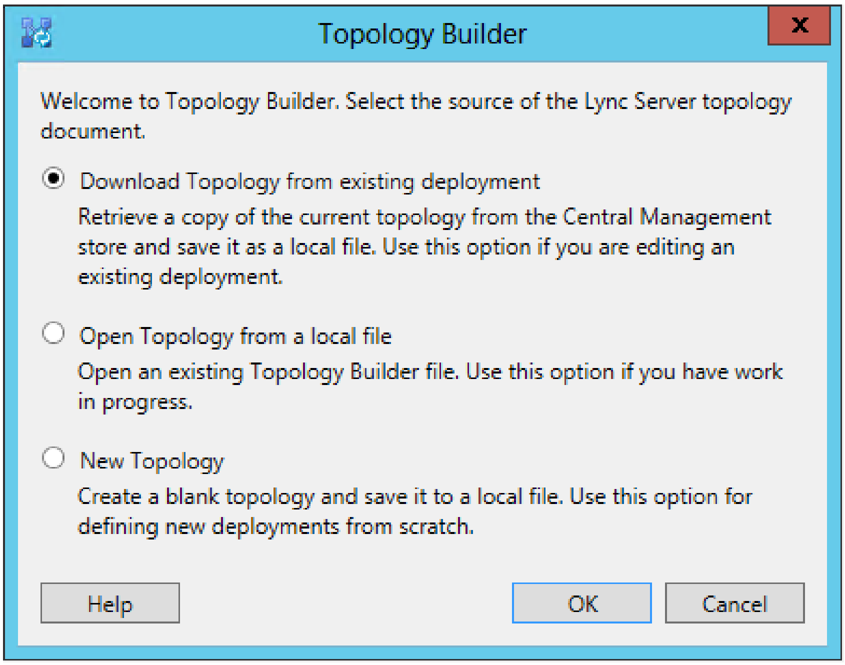
Figure 13-2: Using Search to Open Skype for Business Utilities



Business Server Topology Builder

3. Download and save the current topology.

Figure 13-3: Source of the Topology



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.

○ Open Topology from a local file

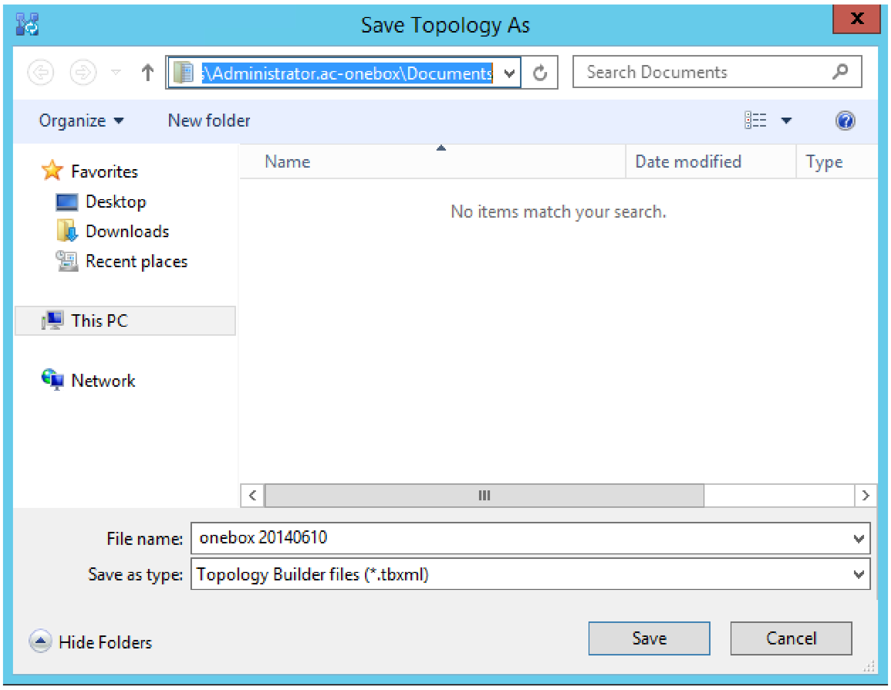
Open an existing Topology Builder file. Use this option if you have work in progress.

○ New Topology

Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.

4. Save the topology.

Figure 13-4: Saving the Topology



Save Topology As

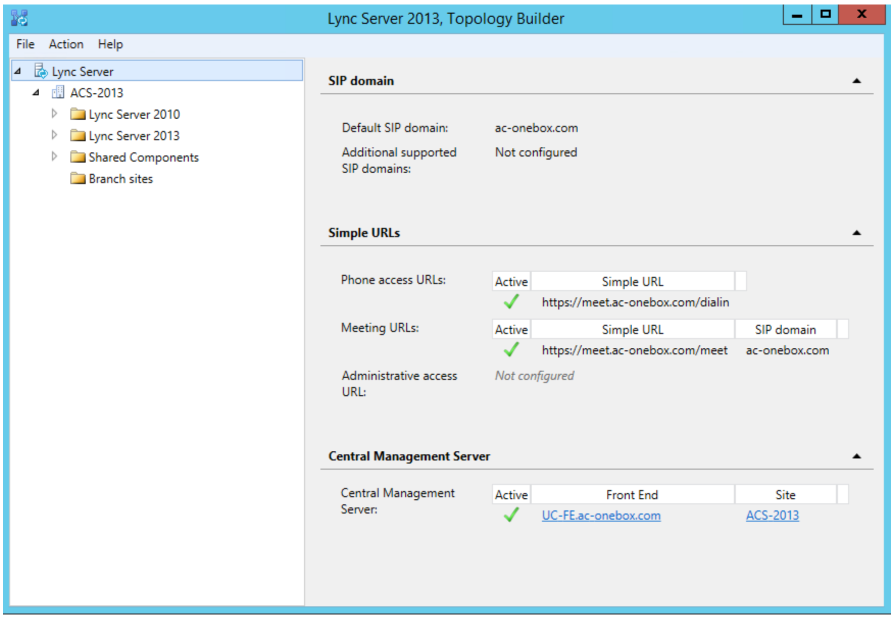
:\Administrator.ac-onebox\Documents

File name: onebox 20140610

Save as type: Topology Builder files (*.tbxml)

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

Figure 13-5: Viewing a Topology



Lync Server 2013, Topology Builder

SIP domain

Default SIP domain: ac-onebox.com

Additional supported SIP domains: Not configured

Simple URLs

Phone access URLs:

Active	Simple URL
✓	https://meet.ac-onebox.com/dialin

Meeting URLs:

Active	Simple URL	SIP domain
✓	https://meet.ac-onebox.com/meet	ac-onebox.com

Administrative access URL: *Not configured*

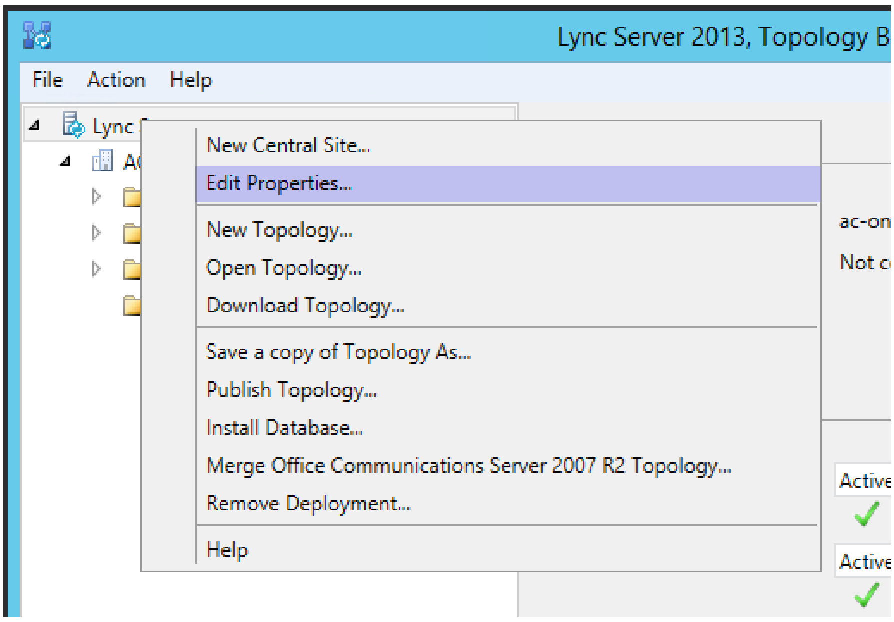
Central Management Server

Central Management Server:

Active	Front End	Site
✓	UC-FE.ac-onebox.com	ACS-2013

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

Figure 13-6: Edit Server Properties

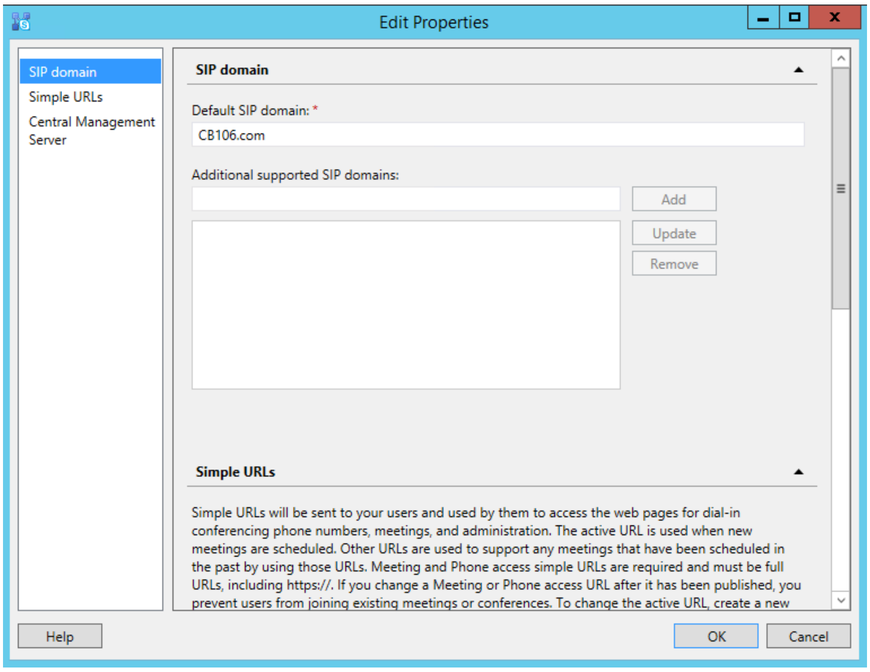


13.3.3.1 Add the New SIP Domain to the Topology

➢ **To add a new SIP domain to the topology:**

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

Figure 13-7: Edit Properties



SIP domain

Default SIP domain: *

CB106.com

Additional supported SIP domains:

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

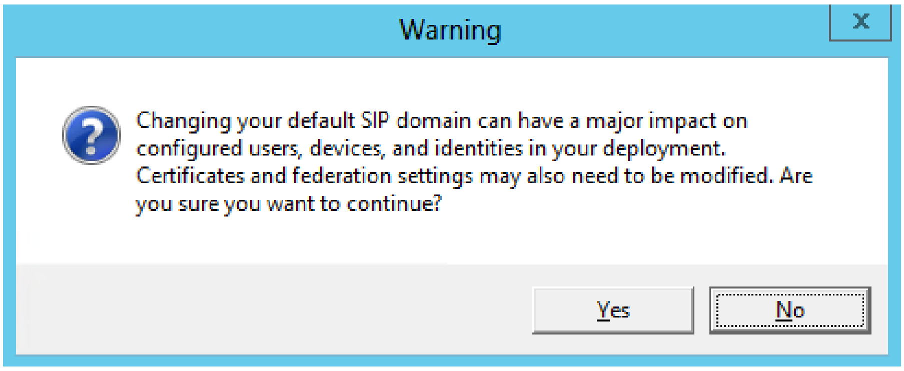
13.3.3.2 Changing the Default (Primary) SIP Domain

If you change the primary SIP domain, you will be presented with the following pop-up, 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 13-8: Warning: Changing the Primary SIP Domain is Complex



Warning

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. Are you sure you want to continue?

Note: Simple URL's, Edge services, and their matching certificates are covered in chapter Configuring Certificates on page 299.

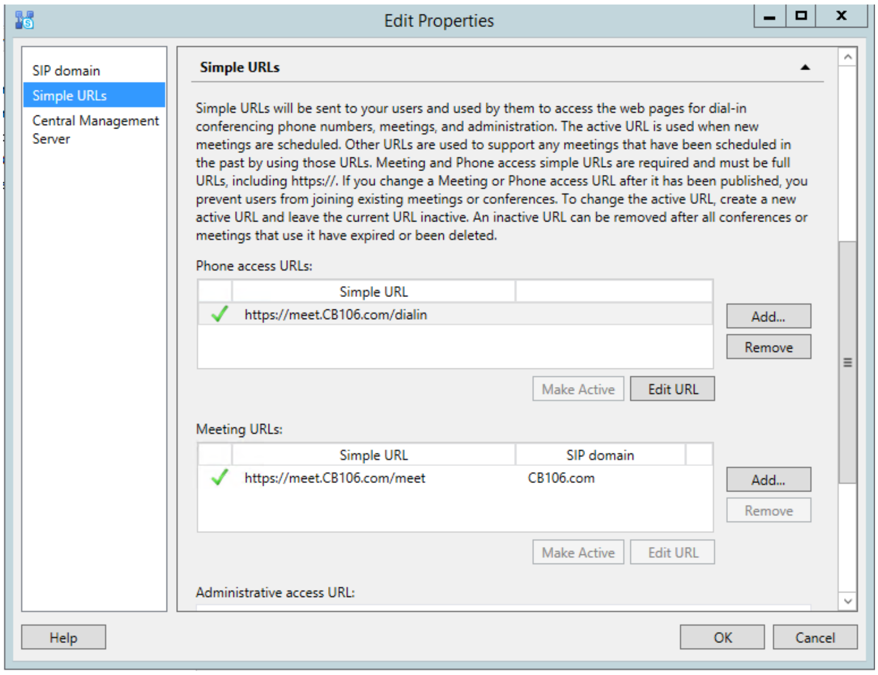
Note: It is also possible to change an existing **Additional SIP domain** to the "Default SIP domain", using the Skype for Business Management shell and the *set-csSipDomain* command.

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

13.3.3.3 Simple URLs

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

Figure 13-9:Simple URL's Using Option 3



Edit Properties

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 in the past by using those URLs. Meeting and Phone access simple URLs are required and must be full URLs, including https://. If you change a Meeting or Phone access URL after it has been published, you prevent users from joining existing meetings or conferences. To change the active URL, create a new active URL and leave the current URL inactive. An inactive URL can be removed after all conferences or meetings that use it have expired or been deleted.

Phone access URLs:

	Simple URL	
✓	https://meet.CB106.com/dialin	

Meeting URLs:

	Simple URL	SIP domain
✓	https://meet.CB106.com/meet	CB106.com

Administrative access URL:

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

Note: Further details on naming options for Simple URLs are covered in chapter Configuring Certificates on page 299.

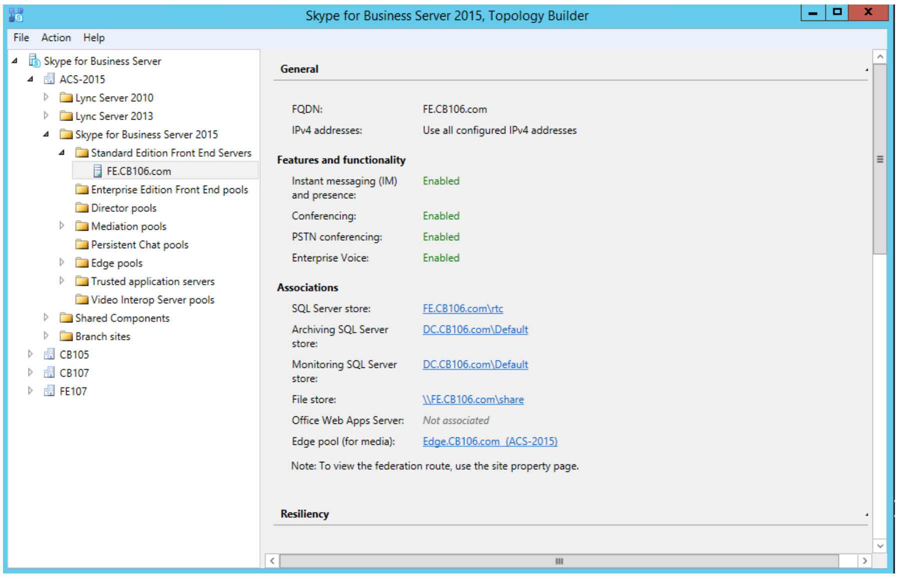
13.3.3.4 External Web Services

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

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

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

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


Skype for Business Server 2015, Topology Builder
File
Action
Help
Skype for Business Server
ACS-2015
Lync Server 2010
Lync Server 2013
Skype for Business Server 2015
Standard Edition Front End Servers
FE.CB106.com
Enterprise Edition Front End pools
Director pools
Mediation pools
Persistent Chat pools
Edge pools
Trusted application servers
Video Interop Server pools
Shared Components
Branch sites
CB105
CB107
FE107

General

FQDN: FE.CB106.com
IPv4 addresses: Use all configured IPv4 addresses

Features and functionality

Instant messaging (IM) and presence: Enabled
Conferencing: Enabled
PSTN conferencing: Enabled
Enterprise Voice: Enabled

Associations

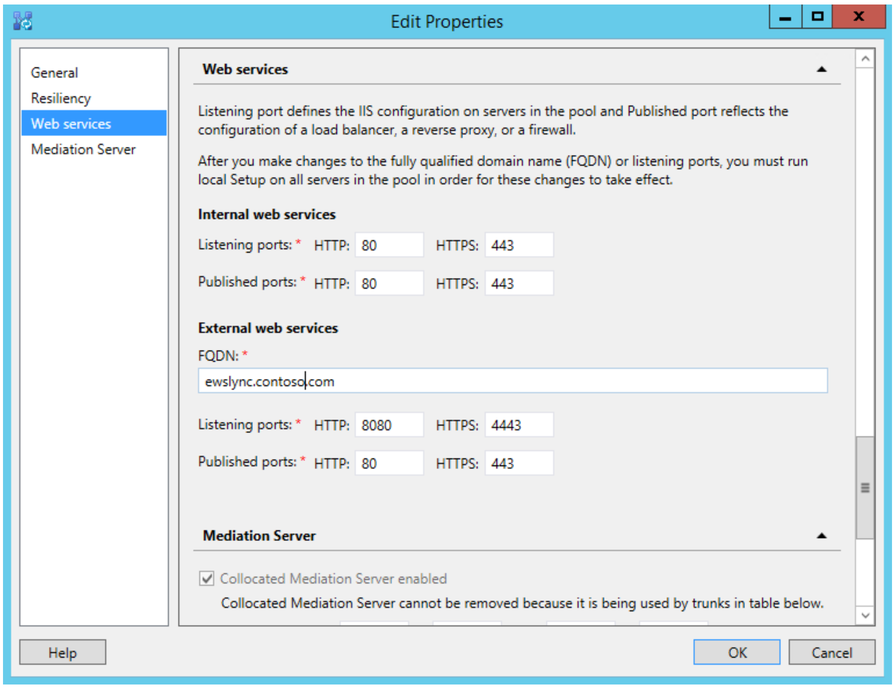
SQL Server store: FE.CB106.com\rtc
Archiving SQL Server store: DC.CB106.com\Default
Monitoring SQL Server store: DC.CB106.com\Default
File store: \\FE.CB106.com\share
Office Web Apps Server: *Not associated*
Edge pool (for media): Edge.CB106.com (ACS-2015)

Note: To view the federation route, use the site property page.

Resiliency

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

Figure 13-11: Edit Properties



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.contoso.com

Listening ports: * HTTP: 8080 HTTPS: 4443
Published ports: * HTTP: 80 HTTPS: 443

Mediation Server

☑ Collocated Mediation Server enabled
Collocated Mediation Server cannot be removed because it is being used by trunks in table below.

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

13.3.3.5 Edge Services

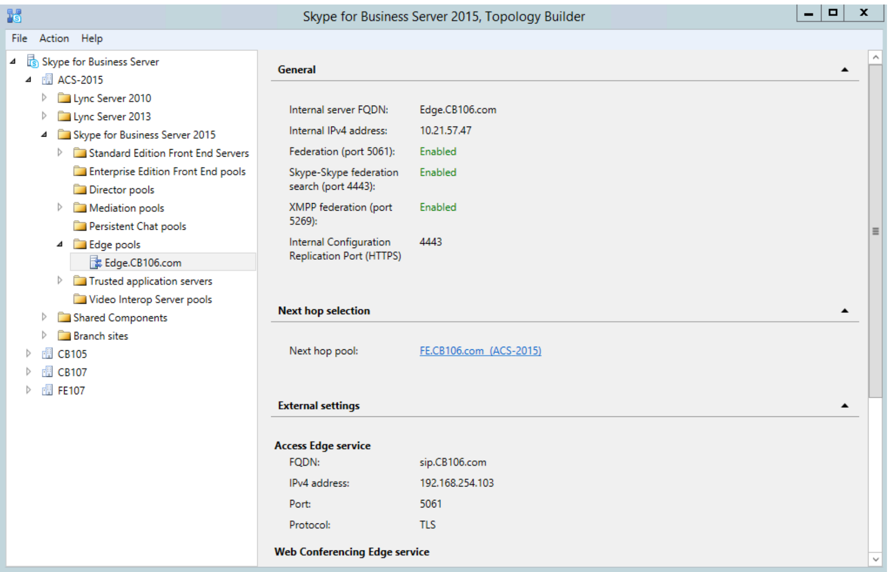
Edge External FQDN's allow users to access your Skype for Business system from outside your organization. This includes Access Edge for external users, Web Conferencing Edge for external conferences, and A/V Edge for voice and video calls.

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

➢ **To edit Edge Services properties:**

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

Figure 13-12: Selecting the Edge Server from the Edge Pool


Skype for Business Server 2015, Topology Builder
File
Action
Help
Skype for Business Server
ACS-2015
Lync Server 2010
Lync Server 2013
Skype for Business Server 2015
Standard Edition Front End Servers
Enterprise Edition Front End pools
Director pools
Mediation pools
Persistent Chat pools
Edge pools
Edge.CB106.com
Trusted application servers
Video Interop Server pools
Shared Components
Branch sites
CB105
CB107
FE107

General

Internal server FQDN: Edge.CB106.com
Internal IPv4 address: 10.21.57.47
Federation (port 5061): Enabled
Skype-Skype federation search (port 4443): Enabled
XMPP federation (port 5269): Enabled
Internal Configuration Replication Port (HTTPS) 4443

Next hop selection

Next hop pool: FE.CB106.com (ACS-2015)

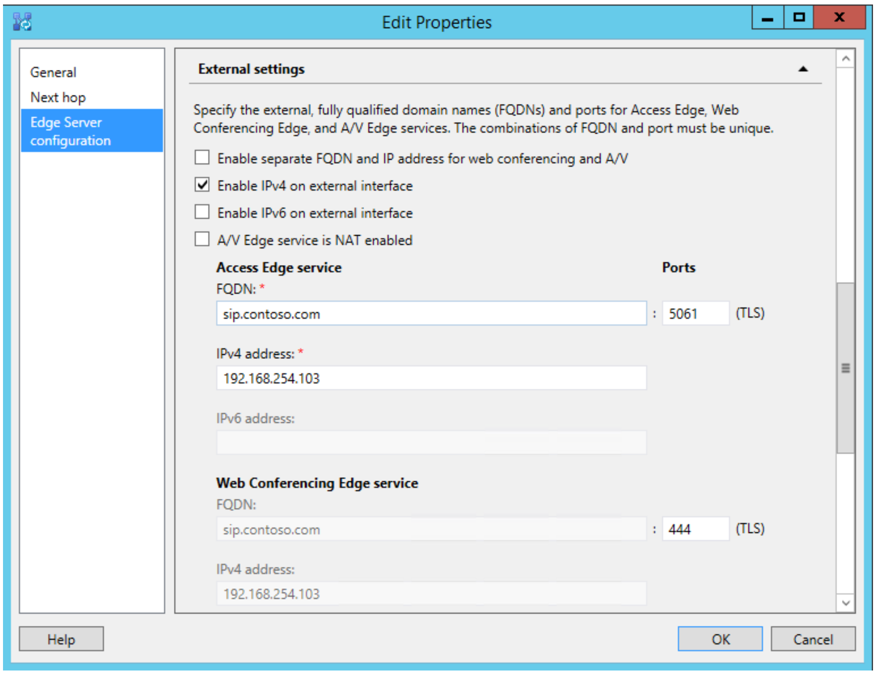
External settings

Access Edge service
FQDN: sip.CB106.com
IPv4 address: 192.168.254.103
Port: 5061
Protocol: TLS

Web Conferencing Edge service

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

Figure 13-13: Edge Server External Access FQDNs



External settings

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

☐ Enable separate FQDN and IP address for web conferencing and A/V
☑ Enable IPv4 on external interface
☐ Enable IPv6 on external interface
☐ A/V Edge service is NAT enabled

Access Edge service — 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

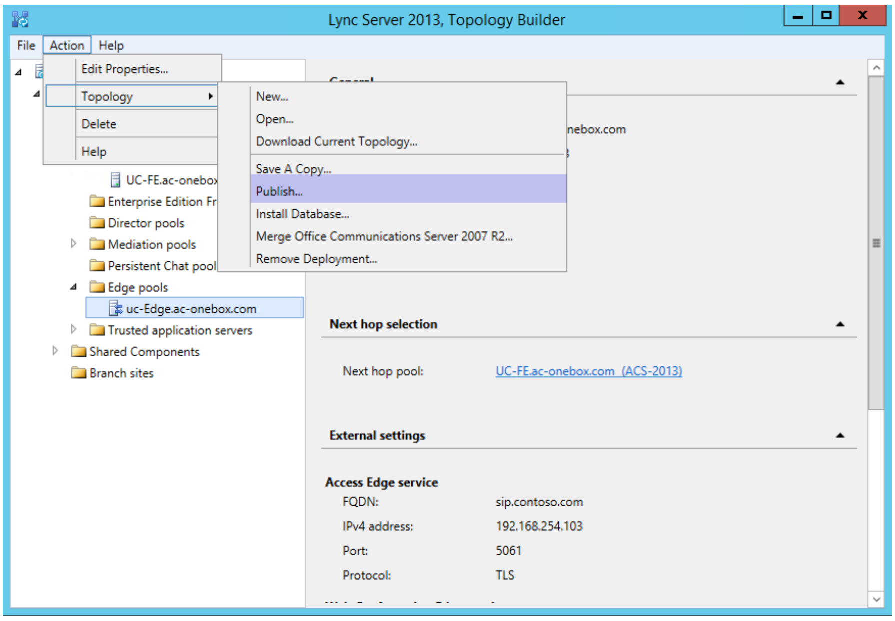
3. Modify the service FQDNs’ as required.
4. Click **OK**.

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.

13.3.3.6 Publish Topology

In Topology Builder, make the required additions, like additional SIP domains or voice gateways for example, and select **Publish Topology**… to continue the installation.

Figure 13-14: Publishing the Topology



Next hop selection

Next hop pool: UC-FE.ac-onebox.com (ACS-2013)

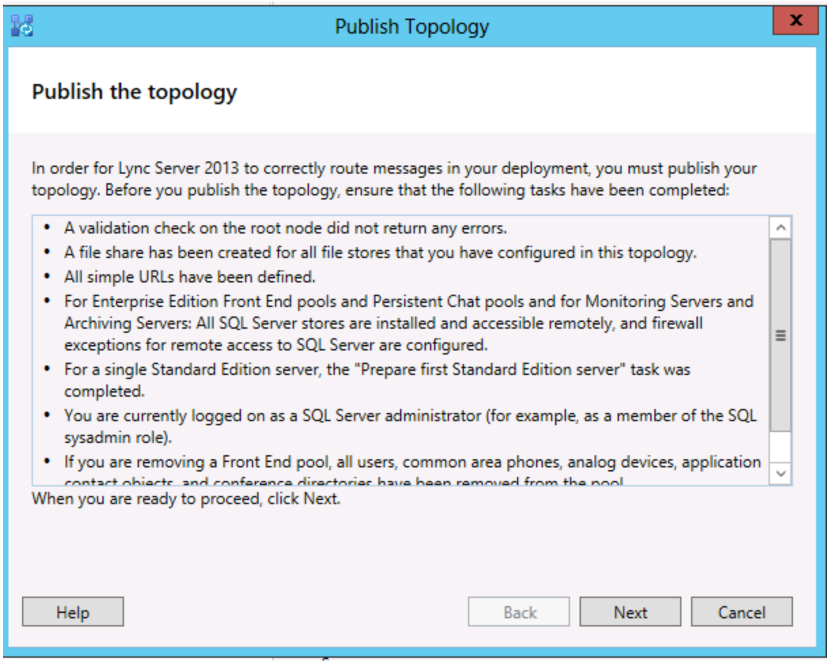
External settings

Access Edge service

FQDN:	sip.contoso.com
IPv4 address:	192.168.254.103
Port:	5061
Protocol:	TLS

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

Figure 1-15: Publishing the Topology



Publish Topology

Publish the topology

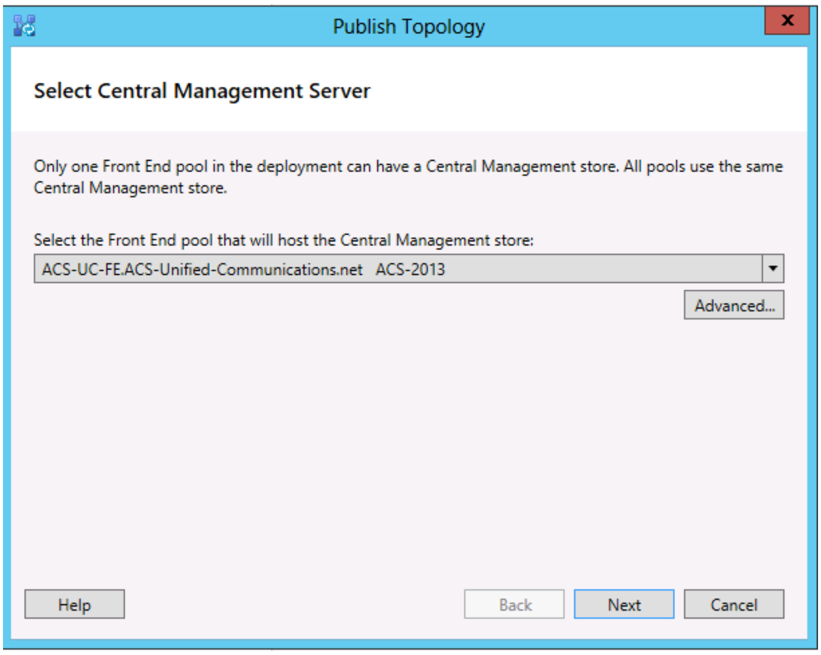
In order for Lync Server 2013 to correctly route messages in your deployment, you must publish your topology. Before you publish the topology, ensure that the following tasks have been completed:

- A validation check on the root node did not return any errors.
- A file share has been created for all file stores that you have configured in this topology.
- All simple URLs have been defined.
- 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.
- For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed.
- You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role).
- 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.

When you are ready to proceed, click Next.

2. Click **Next**.

Figure 13-16: Select Central Management Server



Publish Topology

Select Central Management Server

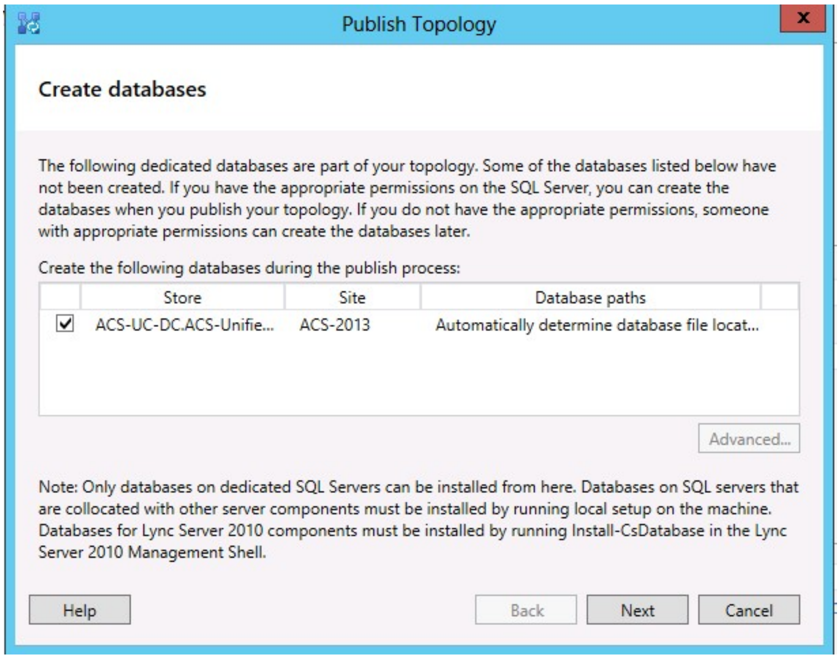
Only one Front End pool in the deployment can have a Central Management store. All pools use the same Central Management store.

Select the Front End pool that will host the Central Management store:

ACS-UC-FE.ACS-Unified-Communications.net ACS-2013

3. Click **Next**.

Figure 13-17: Publishing the topology – Create Databases



Create databases

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

Create the following databases during the publish process:

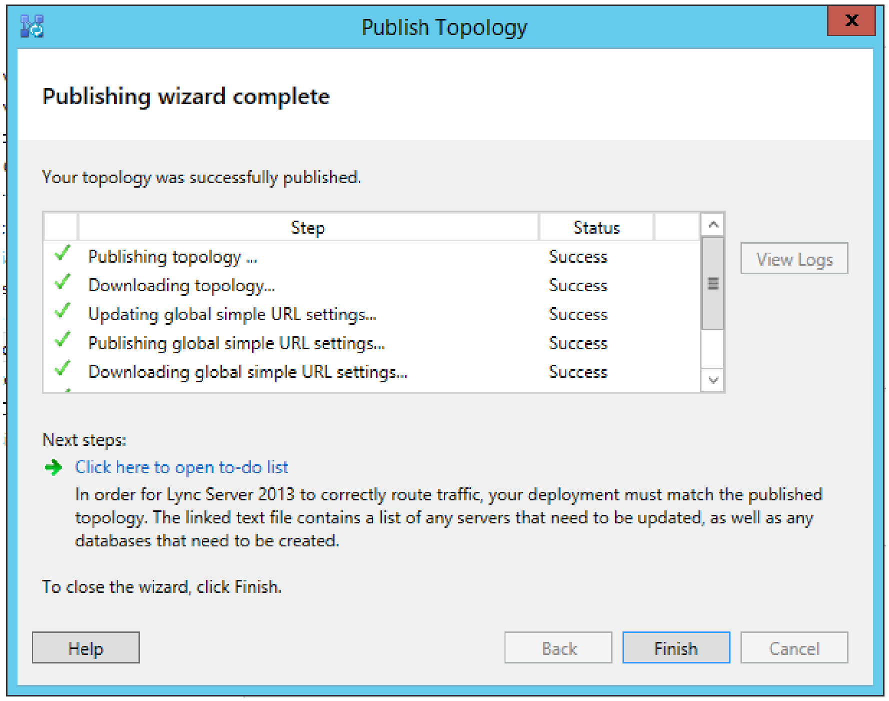
	Store	Site	Database paths
☑	ACS-UC-DC.ACS-Unifie...	ACS-2013	Automatically determine database file locat...

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

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

4. Click **Finish**.

Figure 13-18: Publishing the Topology Completes



Publishing wizard complete

Your topology was successfully published.

	Step	Status
✓	Publishing topology ...	Success
✓	Downloading topology...	Success
✓	Updating global simple URL settings...	Success
✓	Publishing global simple URL settings...	Success
✓	Downloading global simple URL 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.

13.3.4 Run Deployment Wizard

The Deployment wizard implements any changes from the newly published Topology. The Deployment wizard must be run on both the CloudBond 365 Front End and Edge servers.

Figure 13-19: Starting the Deployment Wizard

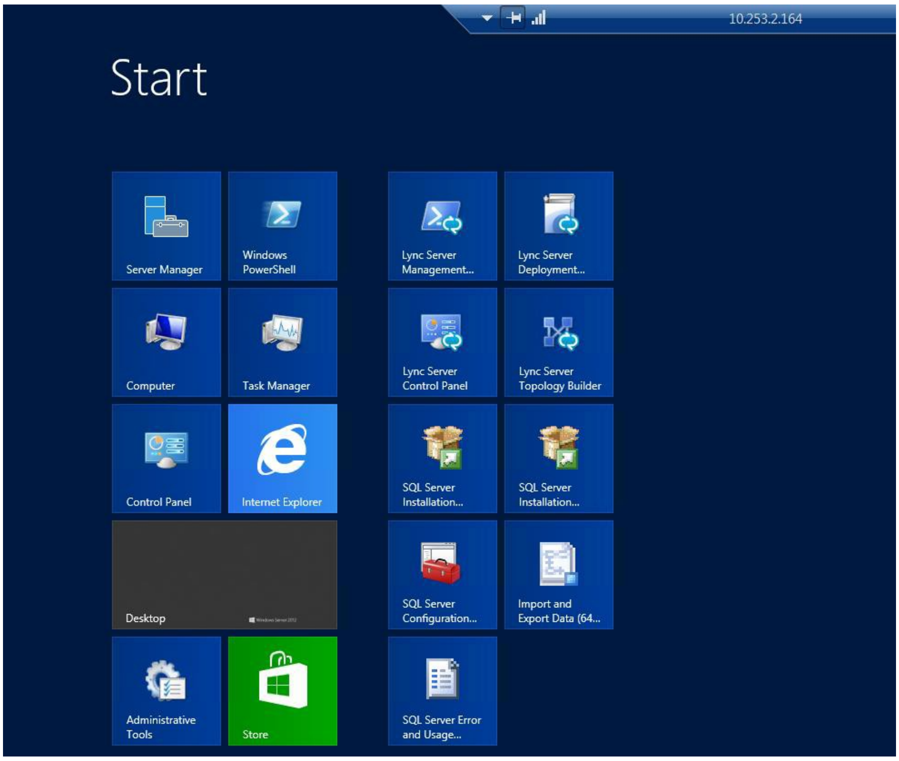
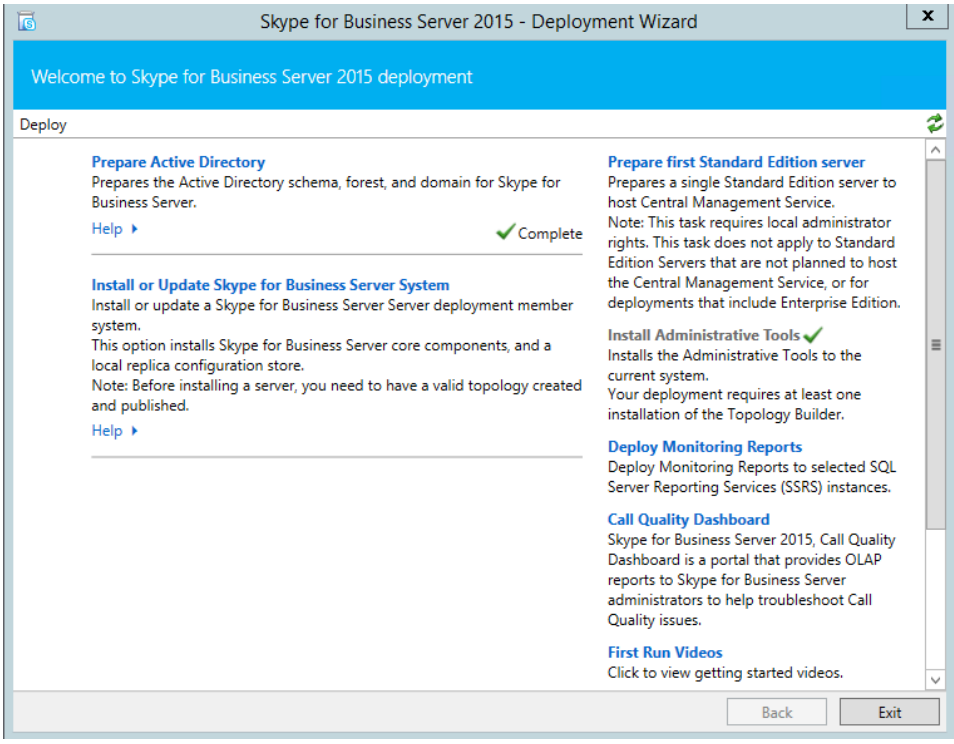

10.253.2.164
Start
Server Manager
Windows PowerShell
Lync Server Management...
Lync Server Deployment...
Computer
Task Manager
Lync Server Control Panel
Lync Server Topology Builder
Control Panel
Internet Explorer
SQL Server Installation...
SQL Server Installation...
Desktop
SQL Server Configuration...
Import and Export Data (64...
Administrative Tools
Store
SQL Server Error and Usage...

Figure 13-20: Deployment Wizard



Skype for Business Server 2015 - Deployment Wizard

Welcome to Skype for Business Server 2015 deployment

Deploy

Prepare Active Directory
Prepares the Active Directory schema, forest, and domain for Skype for Business Server.
Help ▸ ✓ Complete

Install or Update Skype for Business Server System
Install or update a Skype for Business Server Server deployment member system.
This option installs Skype for Business 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 to the current system.
Your deployment requires at least one installation of the Topology Builder.

Deploy Monitoring Reports
Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances.

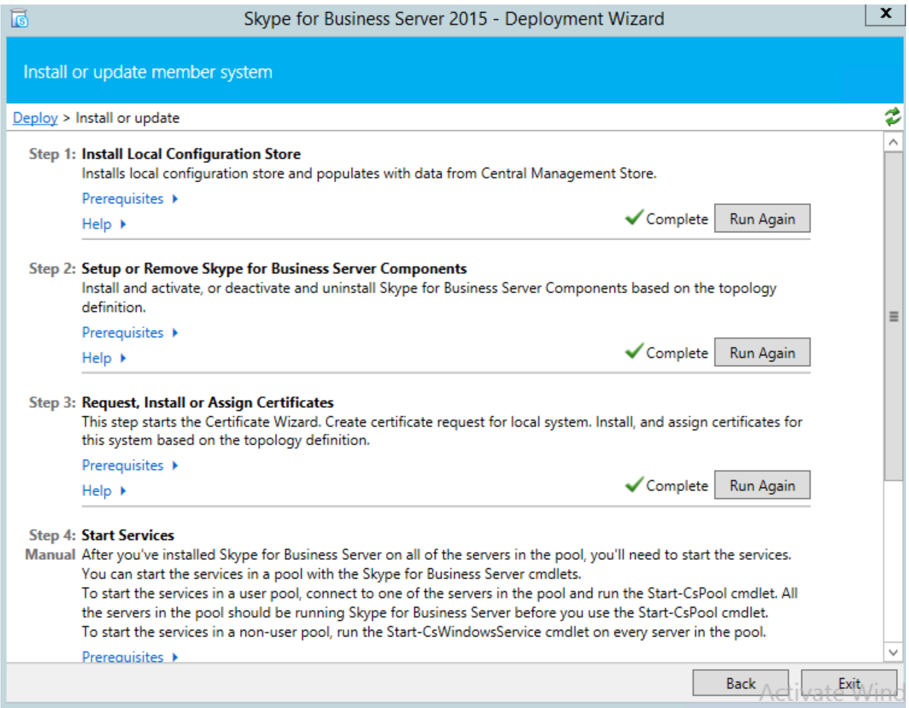
Call Quality Dashboard
Skype for Business Server 2015, Call Quality Dashboard is a portal that provides OLAP reports to Skype for Business Server administrators to help troubleshoot Call Quality issues.

First Run Videos
Click to view getting started videos.

Back Exit

13.3.4.1 Select Install or Update Skype for Business Server System

Figure 13-21: Deployment Wizard Steps



Skype for Business Server 2015 - Deployment Wizard

Install or update member system

Deploy > Install or update

Step 1: Install Local Configuration Store
Installs local configuration store and populates with data from Central Management Store.
Prerequisites ▸
Help ▸
✓ Complete

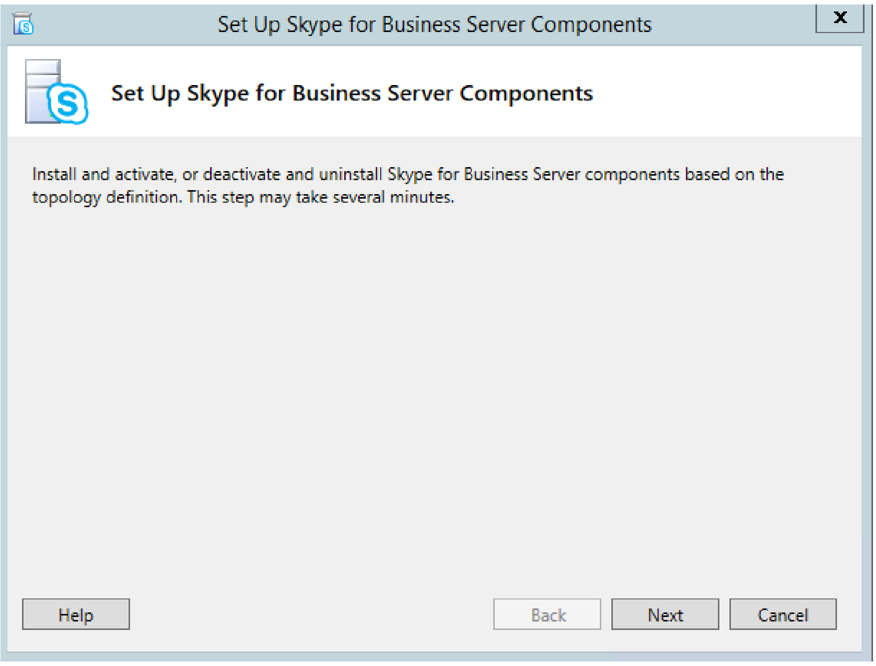
Step 2: Setup or Remove Skype for Business Server Components
Install and activate, or deactivate and uninstall Skype for Business Server Components based on the topology definition.
Prerequisites ▸
Help ▸
✓ Complete

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

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.
Prerequisites ▸

1. Select **Setup or Remove Skype for Business Server Components**.
2. Click **Run Again**.

Figure 13-22: Setup Server Components

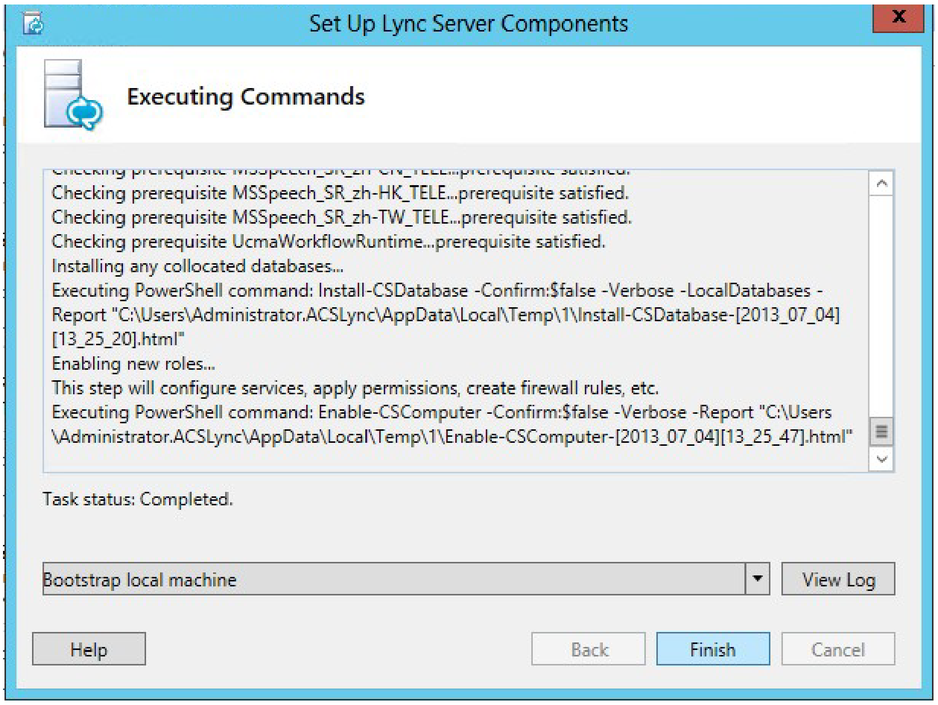


Set Up Skype for Business Server Components

Set Up Skype for Business Server Components

Install and activate, or deactivate and uninstall Skype for Business Server components based on the topology definition. This step may take several minutes.

Figure 13-23: Executing Components



```
Checking prerequisite MSSpeech_SR_zh-CN_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_zh-HK_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_zh-TW_TELE...prerequisite satisfied.
Checking prerequisite UcmaWorkflowRuntime...prerequisite satisfied.
Installing any collocated databases...
Executing PowerShell command: Install-CSDatabase -Confirm:$false -Verbose -LocalDatabases -
Report "C:\Users\Administrator.ACSLync\AppData\Local\Temp\1\Install-CSDatabase-[2013_07_04]
[13_25_20].html"
Enabling new roles...
This step will configure services, apply permissions, create firewall rules, etc.
Executing PowerShell command: Enable-CSComputer -Confirm:$false -Verbose -Report "C:\Users
\Administrator.ACSLync\AppData\Local\Temp\1\Enable-CSComputer-[2013_07_04][13_25_47].html"
```

Task status: Completed.

Bootstrap local machine

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

13.3.5 DNS Entries

DNS entries are covered in Section 6.4 .

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

13.3.5.1 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>

13.3.5.2 Skype for Business External Records

External records refer to public IP addresses.

- SRV: _*sipfederationtls.*_tcp.<FQDN> over port 5061 to sip.<FQDN>
- SRV: _*sip.*_tls.<FQDN> over port 5061 to sip.<FQDN>
- A: sip.<FQDN>
- A: sipexternal.<FQDN>
- A: meet.<FQDN>
- (in a default CloudBond 365 installation, meet is used for both dialing and meet simple URL’s)
- A: ewslync.<FQDN>
- (is assigned to the default CloudBond 365 Skype for Business external web services)
- CNAME: Skype for Businessdiscover.<FQDN> pointing to ewslync.<FQDN>

13.3.6 Certificates

Certificate requirements are covered in:

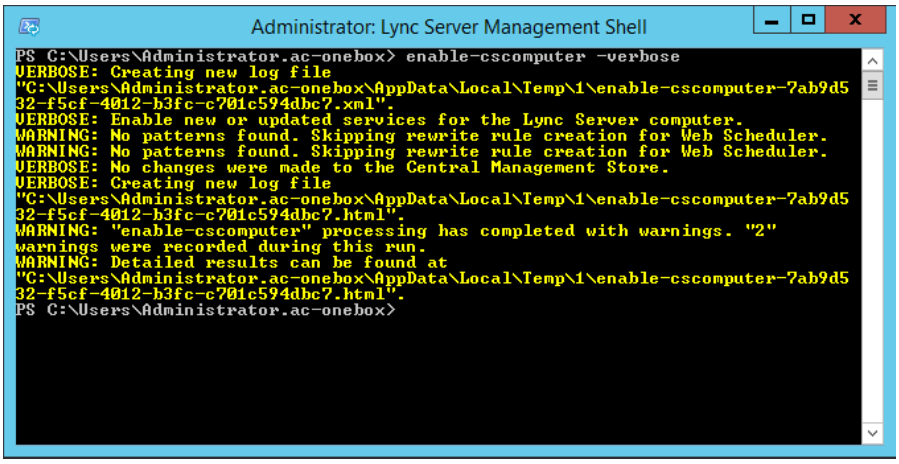
13.3.6.1 AudioCodes CloudBond 365 Certificates Configuration Note

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

13.3.7 Enable Configuration

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

Figure 13-24: Management Shell



```
PS C:\Users\Administrator.ac-onebox> enable-cscomputer -verbose
VERBOSE: Creating new log file
"C:\Users\Administrator.ac-onebox\AppData\Local\Temp\1\enable-cscomputer-7ab9d5
32-f5cf-4012-b3fc-c701c594dbc7.xml".
VERBOSE: Enable new or updated services for the Lync Server computer.
WARNING: No patterns found. Skipping rewrite rule creation for Web Scheduler.
WARNING: No patterns found. Skipping rewrite rule creation for Web Scheduler.
VERBOSE: No changes were made to the Central Management Store.
VERBOSE: Creating new log file
"C:\Users\Administrator.ac-onebox\AppData\Local\Temp\1\enable-cscomputer-7ab9d5
32-f5cf-4012-b3fc-c701c594dbc7.html".
WARNING: "enable-cscomputer" processing has completed with warnings. "2"
warnings were recorded during this run.
WARNING: Detailed results can be found at
"C:\Users\Administrator.ac-onebox\AppData\Local\Temp\1\enable-cscomputer-7ab9d5
32-f5cf-4012-b3fc-c701c594dbc7.html".
PS C:\Users\Administrator.ac-onebox>
```

14 Edge Server to a Full DMZ Deployment

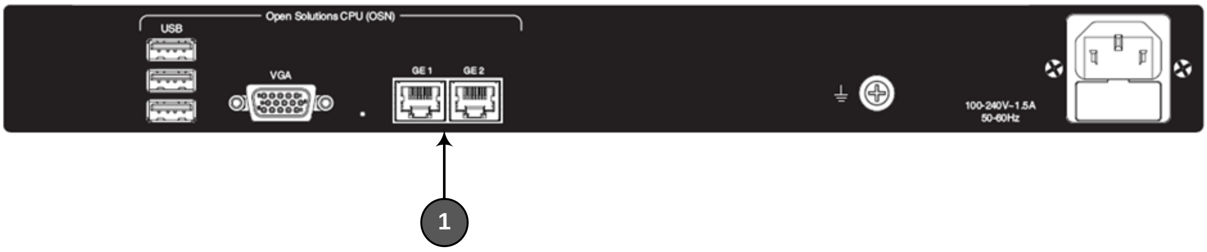
This chapter shows how to connect the AudioCodes CloudBond 365 Edge Server to a full DMZ deployment.

14.1 Connecting the Edge Server

This chapter shows how to connect the CloudBond 365 Edge Server to a full DMZ deployment.

The CloudBond 365 Edge Server by default connects to the external world via a separated Ethernet connection, located on the rear panel of the CloudBond 365, shown in the figure below.

Figure 14-1: Two Gigabit Ethernet Ports on the CloudBond 365 Rear Panel



1	OSN GE1/GE2. Two Gigabit Ethernet ports for connecting directly to the OSN server. For example, one port can be connected to the LAN (to IP phones) and the second to the WAN interface (to an IP PBX).

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 14-2: Utilizing the Second Ethernet Port on the CloudBond 365 Rear Panel

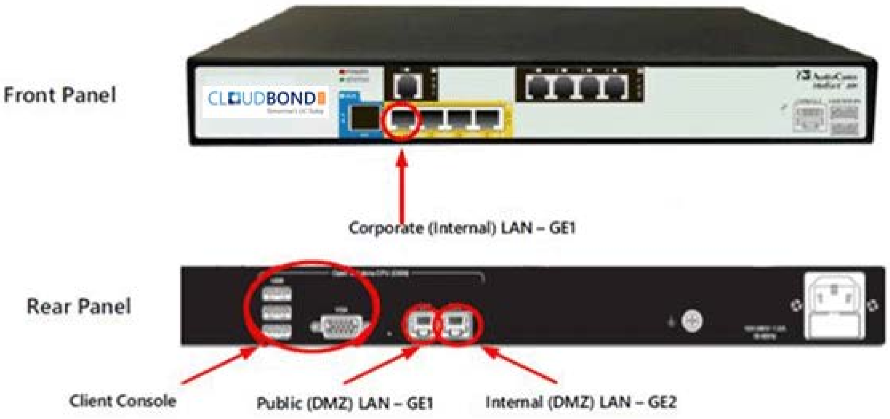
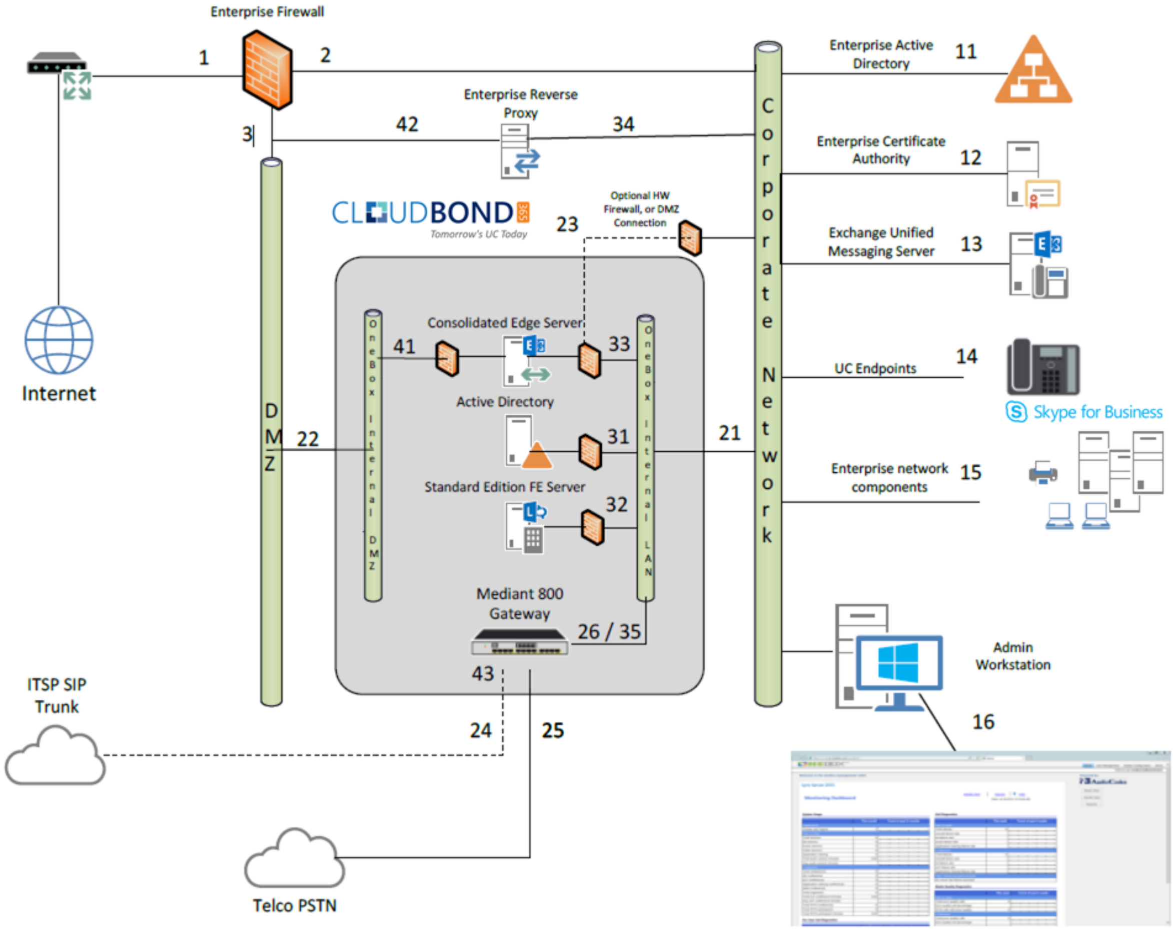


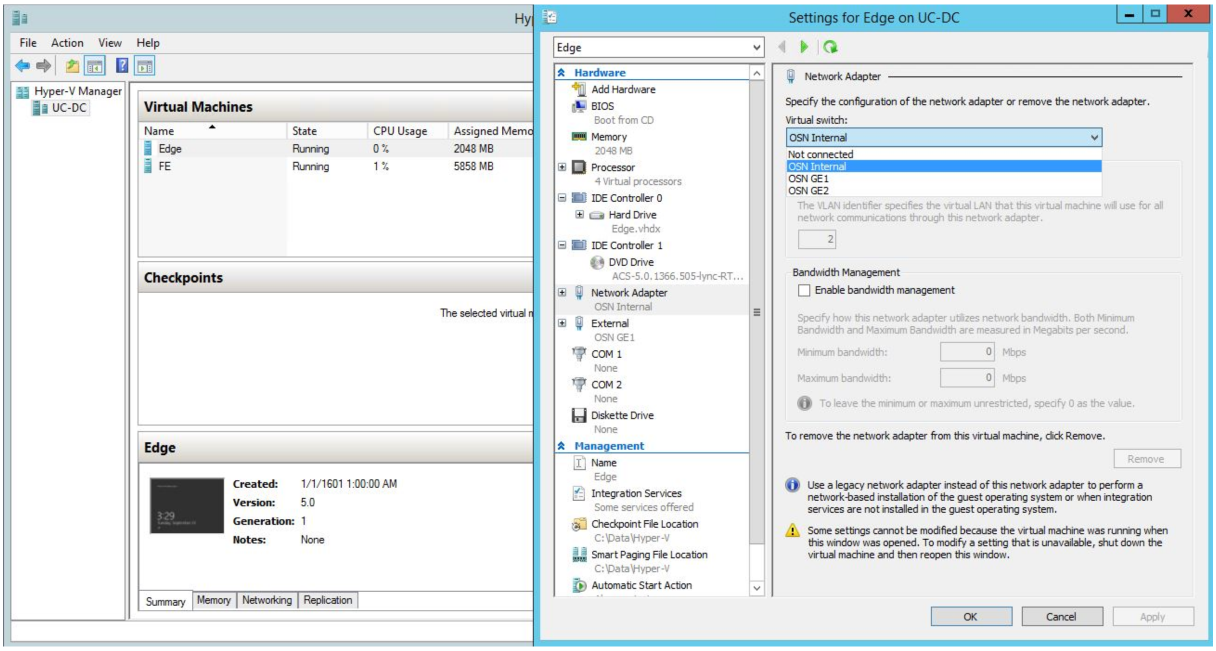
Figure 14-3: Edge Server - Two Legs



➢ **To set up the CloudBond 365 for a deployment like this:**

1. Connect to CloudBond 365 through a locally connected keyboard, mouse and monitor, or through a remote desktop connection to the CloudBond 365 controller.
   The default remote connection information is:
   - IP address: 192.168.0.101
   - Username: ac-CloudBond\administrator
   - Password: R3m0t3Supp0rt
2. Start the Hyper-V Manager application, located on the base Operating System.
3. Open the Edge Server settings through the Action menu, and then select the Network Adapter named **OSN Internal**.
4. Change the virtual switch from **OSN Internal** to **OSN GE2**, and then adapt the VLAN ID accordingly, if necessary.

Figure 14-4: Setup in Hyper-V Manager



Name	State	CPU Usage	Assigned Memo
Edge	Running	0 %	2048 MB
FE	Running	1 %	5858 MB

The selected virtual m

Edge

Created: 1/1/1601 1:00:00 AM
Version: 5.0
Generation: 1
Notes: None

Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch: OSN Internal

Not connected
OSN Internal
OSN GE1
OSN GE2

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

□ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

Some settings cannot be modified because the virtual machine was running when this window was opened. To modify a setting that is unavailable, shut down the virtual machine and then reopen this window.

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 part is intentionally left blank.

Part V

Configuring CloudBond 365

This part includes the following:

- Office 365 integration (see Chapter 15)
- Reverse Proxy (see Chapter 16)
- Certificates (see Chapter 17)
- Exchange UM (see Chapter 18)

15 Office 365 Integration

15.1 Introduction

This part 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.

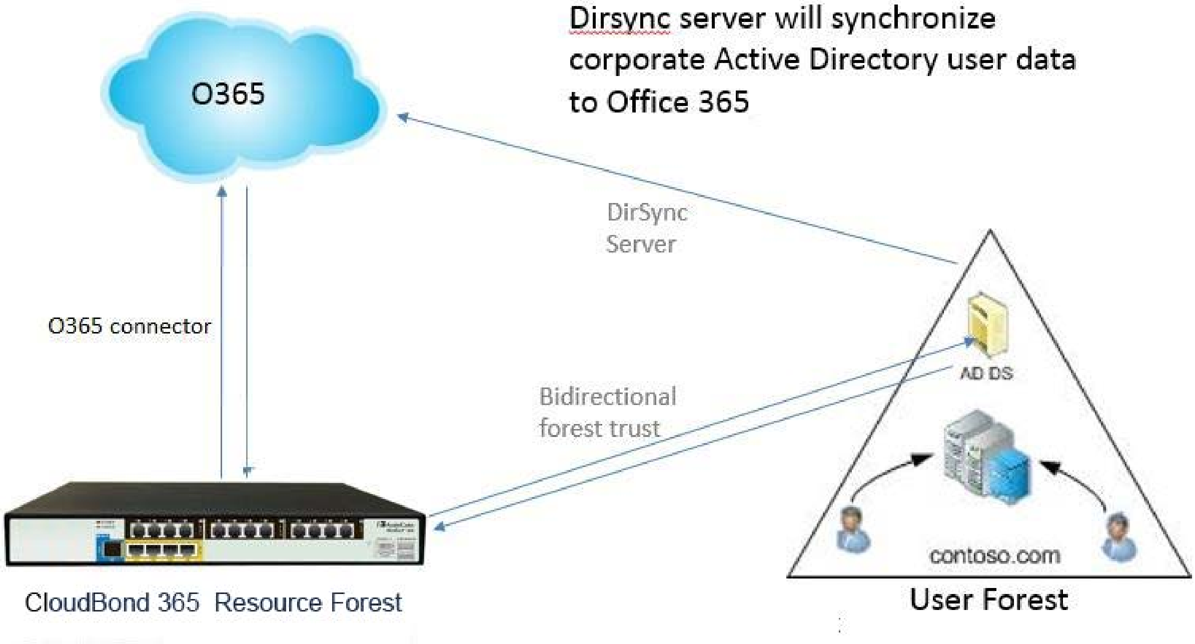
This guide provides:

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

15.2 Overview

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

Figure 15-1: CloudBond 365 and Office 365


Dirsync server will synchronize corporate Active Directory user data to Office 365
O365
DirSync Server
O365 connector
Bidirectional forest trust
AD DS
contoso.com
CloudBond 365 Resource Forest
User Forest

15.2.1 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 have much information about Office 365: http://office.microsoft.com

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

15.2.2 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 15.2.5.1, 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.

15.2.3 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 your larger 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.

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

15.2.4 What is Skype for Business Federation?

Skype for Business Federation is feature which 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, federation allows users in your on-premises deployment to communicate with Office 365 users in your organization.

Skype for Business federation has various security mechanisms included. 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.

15.2.5 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 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

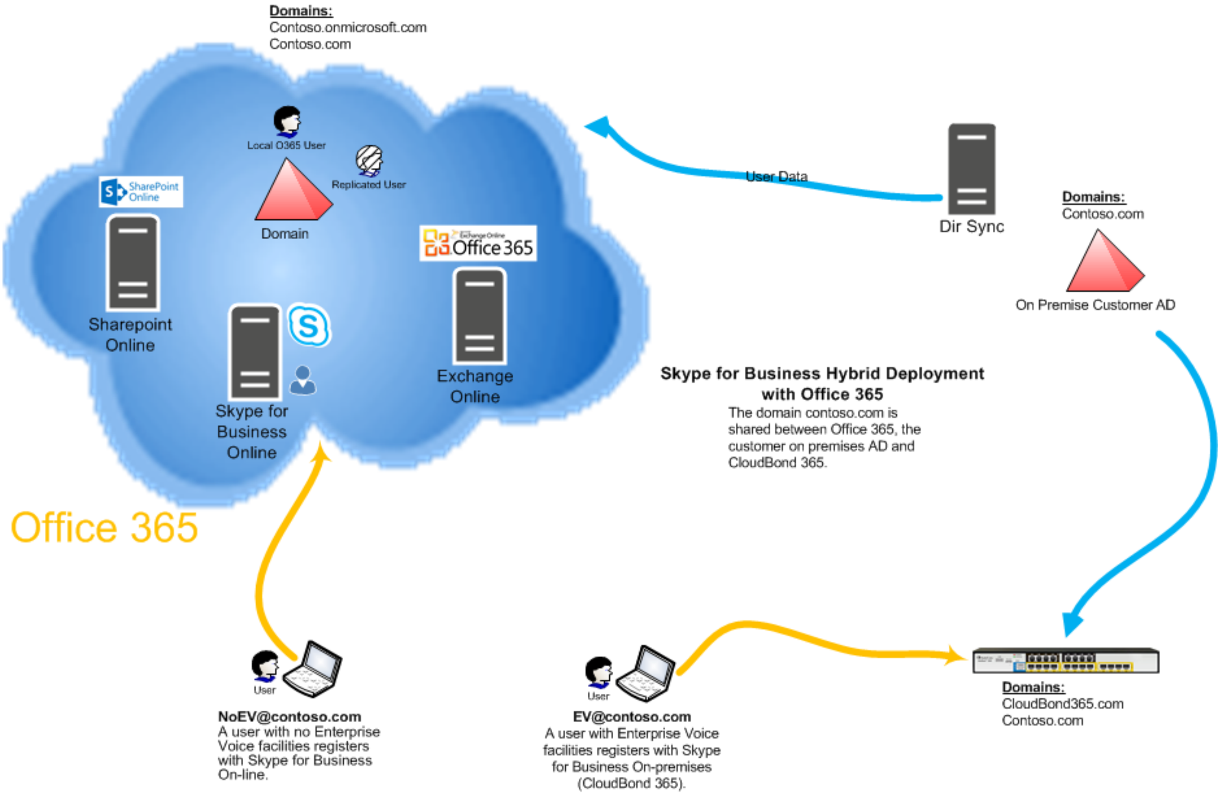
15.2.5.1 Skype for Business Hybrid Deployment

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

In a Skype for Business Hybrid deployment:

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

Figure 15-2: CloudBond 365 Skype for Business Hybrid Deployment


Domains:
Contoso.onmicrosoft.com
Contoso.com
Local O365 User
Replicated User
Domain
SharePoint Online
Sharepoint Online
Office 365
Exchange Online
Skype for Business Online
Office 365
User Data
Dir Sync
Domains:
Contoso.com
On Premise Customer AD
Skype for Business Hybrid Deployment with Office 365
The domain contoso.com is shared between Office 365, the customer on premises AD and CloudBond 365.
User
NoEV@contoso.com
A user with no Enterprise Voice facilities registers with Skype for Business On-line.
User
EV@contoso.com
A user with Enterprise Voice facilities registers with Skype for Business On-premises (CloudBond 365).
Domains:
CloudBond365.com
Contoso.com

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.

15.2.6 Replicating Users

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

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

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

Some good background information on DirSync is available at the following links: http://blogs.office.com/2014/04/15/synchronizing-your-directory-with-office-365-is-easy/

https://blogs.office.com/2013/07/26/password-hash-sync-simplifies-user-management-for-office-365/

15.2.6.1 DirSync

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

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

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

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

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

A recently added option within DirSync allows hashed passwords to also be synchronized from on-premises AD to Office 365 AD. This is the recommended configuration. With 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 supportability 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 Single Sign on. A user logging in will still be prompted for User ID and password in Office 365, even if they are already signed in to the on-premises network.

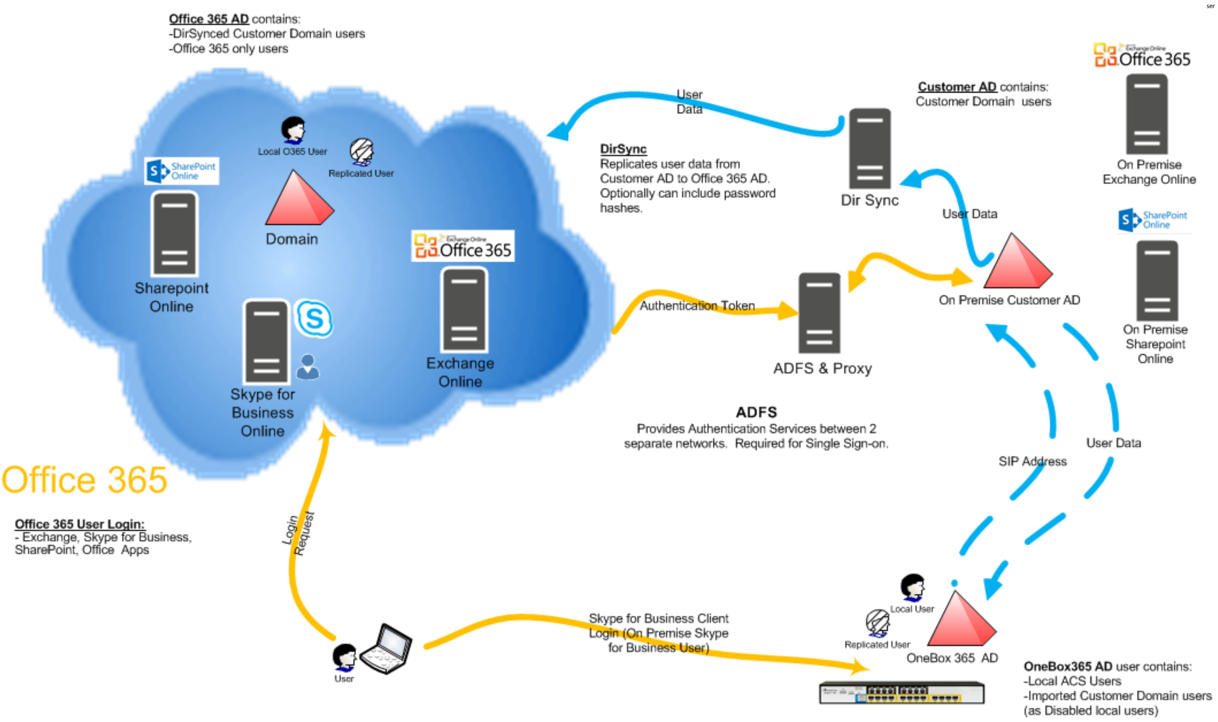
15.2.7 Active Directory Federation Services

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 15-3: ADFS Single Sign On


Office 365 AD contains:
-DirSynced Customer Domain users
-Office 365 only users
Local O365 User
Replicated User
SharePoint Online
Domain
Sharepoint Online
Office 365
Exchange Online
Skype for Business Online
Exchange Online
Office 365
Office 365 User Login:
- Exchange, Skype for Business, SharePoint, Office Apps
Login Request
User
User Data
DirSync
Replicates user data from Customer AD to Office 365 AD. Optionally can include password hashes.
Dir Sync
Customer AD contains:
Customer Domain users
Exchange Online
Office 365
On Premise Exchange Online
User Data
SharePoint Online
Authentication Token
ADFS & Proxy
On Premise Customer AD
On Premise Sharepoint Online
ADFS
Provides Authentication Services between 2 separate networks. Required for Single Sign-on.
User Data
SIP Address
Skype for Business Client Login (On Premise Skype for Business User)
Local User
Replicated User
OneBox 365 AD
OneBox365 AD user contains:
-Local ACS Users
-Imported Customer Domain users
(as Disabled local users)
ser

15.3 Pre-Requisites

This chapter describes the prerequisites for a Skype for Business Server hybrid deployment.

15.3.1 Infrastructure Prerequisites

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

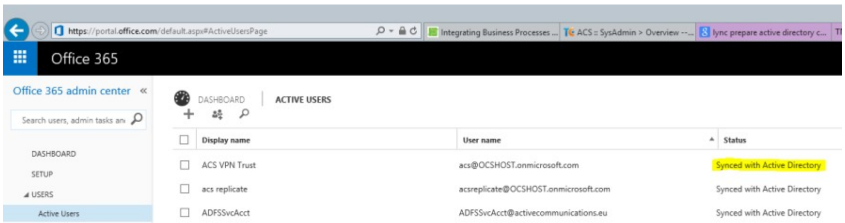
- An Office 365 tenant with Skype for Business Online enabled.
- Optionally, if you want to support Single Sign-on with Office 365, an Active Directory Federation Services (AD FS) Server either on-premises or using Microsoft Azure. For more information about AD FS, see Active Directory Federation Services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

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

15.3.2 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 15-4: Office 365 Users



https://portal.office.com/default.aspx#ActiveUsersPage
Integrating Business Processes ...
ACS :: SysAdmin > Overview --...
lync prepare active directory c...
Office 365
Office 365 admin center
Search users, admin tasks an
DASHBOARD
SETUP
USERS
Active Users
DASHBOARD
ACTIVE USERS

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

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

Following Microsoft best practice, DirSync should be installed on a member server of the domain you wish to replicate users from. 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

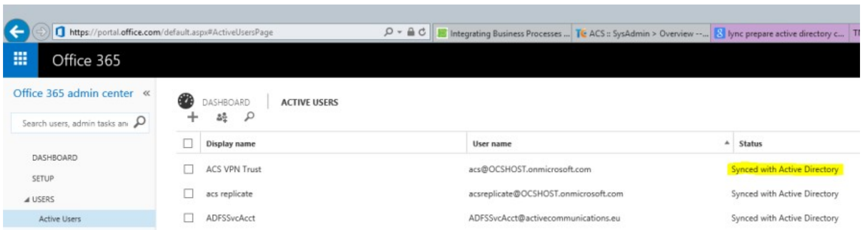
The Setup Wizard will offer you the chance to run the Configuration Wizard after install completes.

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

15.3.3 Ensure DirSync is Functioning

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

Figure 15-5: DirSync Working



https://portal.office.com/default.aspx#ActiveUsersPage

Office 365

Office 365 admin center

Search users, admin tasks an

DASHBOARD

SETUP

USERS

Active Users

DASHBOARD | ACTIVE USERS

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

Integrating Business Processes ...
ACS :: SysAdmin > Overview --...
lync prepare active directory c...

15.3.4 Deploy Skype for Business Schema Attributes

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

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

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

15.3.4.1 Using LDIFDE

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

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

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

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

Copy

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

For example:

Copy

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

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

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

Copy

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

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

15.3.5 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 Part ‘Deployment Requirements’ on page 31.

15.3.6 Prepare the User Forest Active Directory for Write Access

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

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

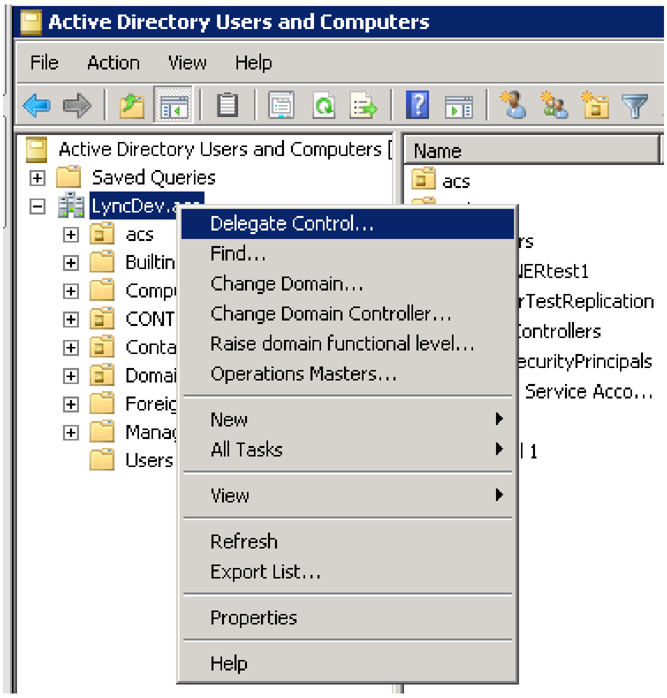
In the screenshots below:

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

➢ **To prepare the User Forest Active Directory for Write Access:**

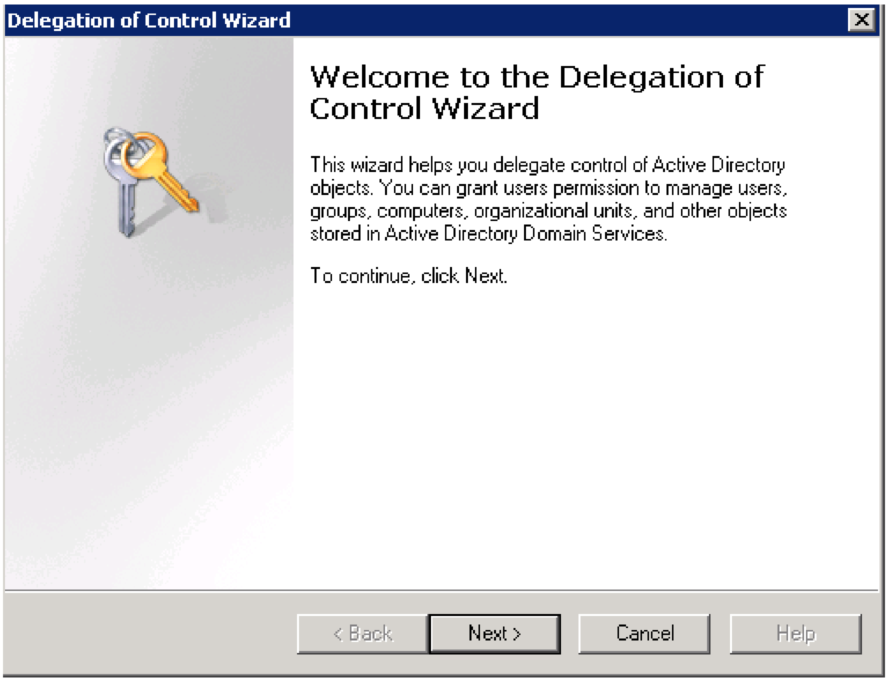
1. On the Customer Corporate DC, open the Active Directory Users and Computers tool.
2. Right-click on the top level domain, and select **Delegate Control**.

Figure 15-6: Delegate Control



3. Click **Next**.

Figure 15-7: Delegate Control Wizard



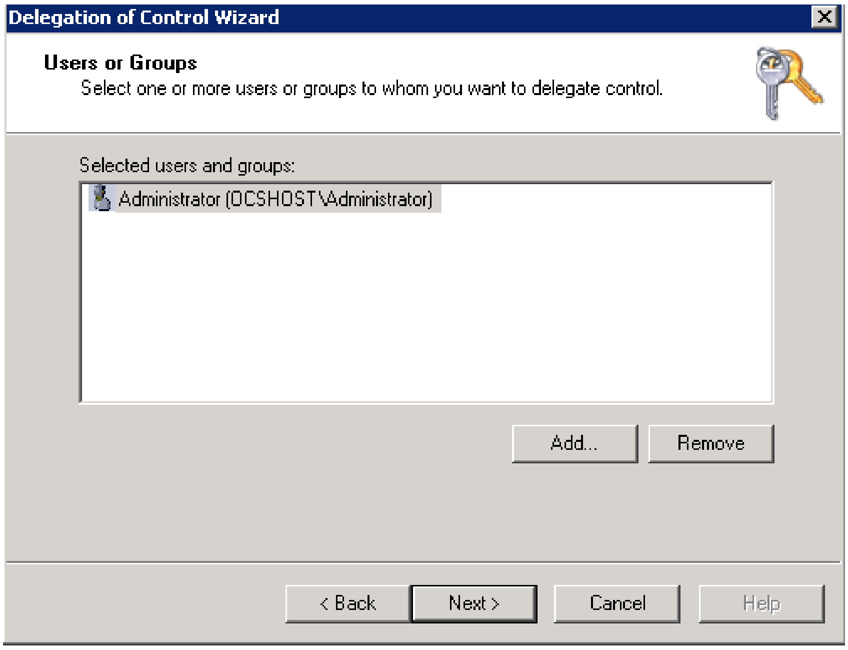
Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.

4. Click **Next**.

Figure 15-8: Delegate to CloudBond 365 Administrator



Delegation of Control Wizard

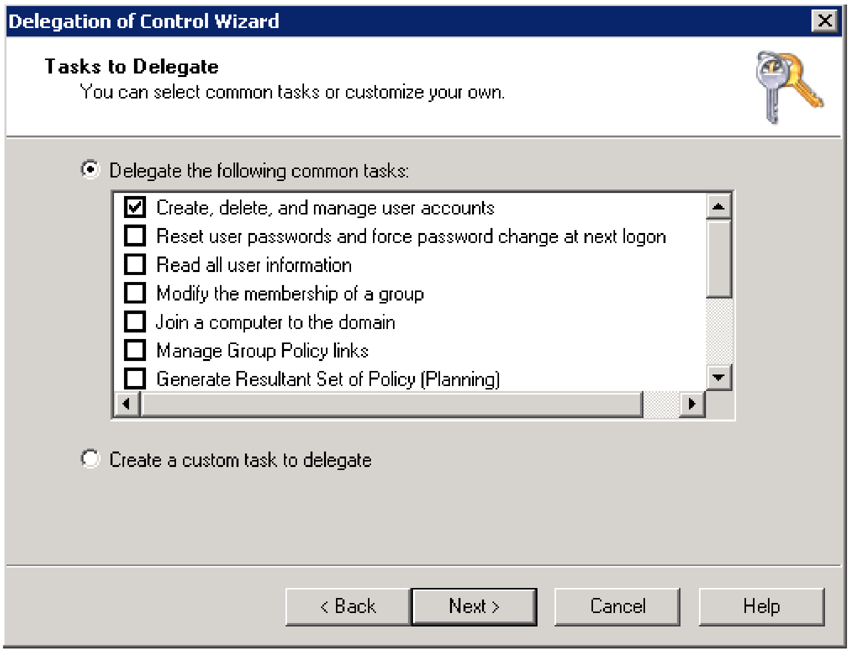
Users or Groups
Select one or more users or groups to whom you want to delegate control.

Selected users and groups:

Administrator (OCSHOST\Administrator)

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

Figure 15-9: Delegate Rights



Delegation of Control Wizard

Tasks to Delegate
You can select common tasks or customize your own.

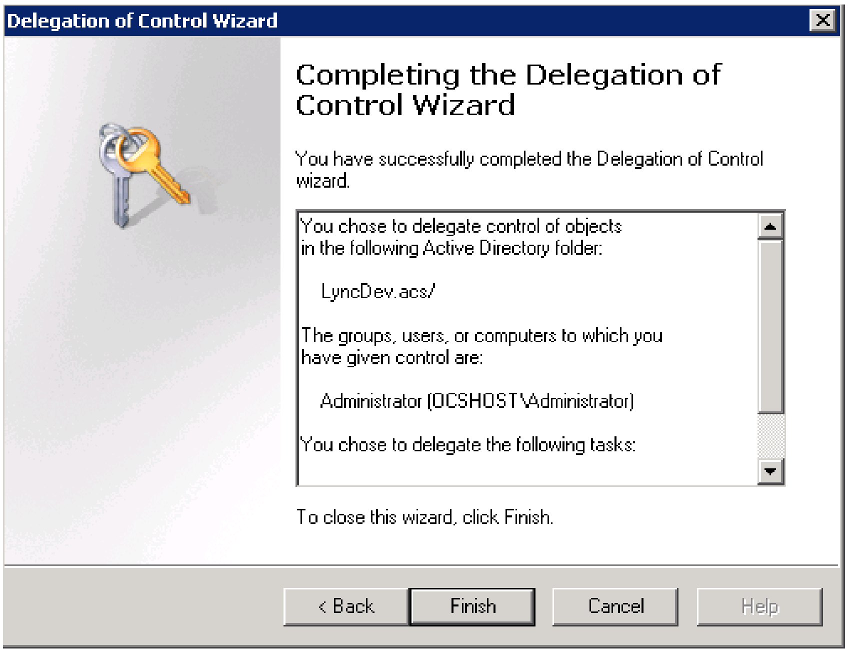
● Delegate the following common tasks:

☑ 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)

○ Create a custom task to delegate

6. Click **Finish**.

Figure 15-10: Complete the Wizard



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.

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 A.

15.4 Configure Office 365 Integration

This chapter describes Office 365 integration.

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

To enable a Skype for Business hybrid deployment, you will need to 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

15.4.1.1 Start a Skype for Business Online PowerShell Session

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

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

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

For more information about using the Skype for Business Online PowerShell module, see Using Windows PowerShell to manage Skype for Business Online.

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

15.4.1.2 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
```

15.4.1.3 Allow 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
```

15.4.1.4 Remove 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
```

15.4.1.5 Create 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:

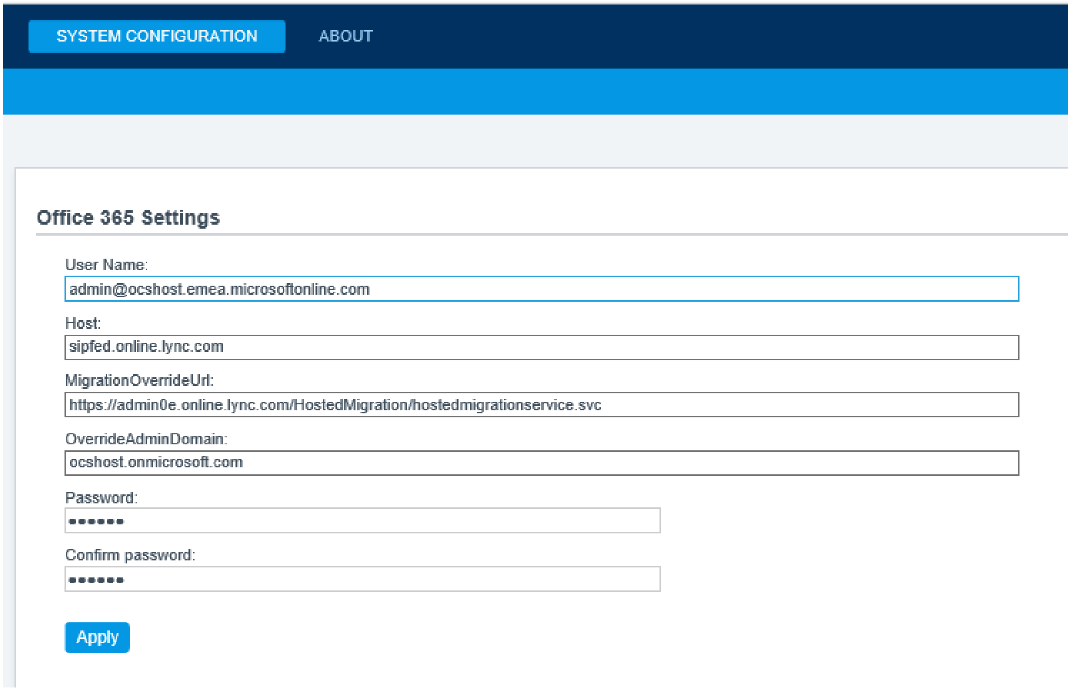
```
New-CSHostingProvider -Identity LyncOnline -ProxyFqdn
"sipfed.online.Lync.com" -Enabled $true -EnabledSharedAddressSpace
$true
-HostsOCSUsers $true -VerificationLevel UseSourceVerification -
IsLocal $false
-AutodiscoverUrl
https://webdir.online.Lync.com/Autodiscover/AutodiscoverService.svc/r
oot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

15.4.2 Obtain the Customer Specific Office 365 Information

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

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

Figure 15-11: CloudBond - Office 365 Connector Information



Office 365 Settings

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

Host: sipfed.online.lync.com

MigrationOverrideUrl: https://admin0e.online.lync.com/HostedMigration/hostedmigrationservice.svc

OverrideAdminDomain: ocshost.onmicrosoft.com

Password: ••••••

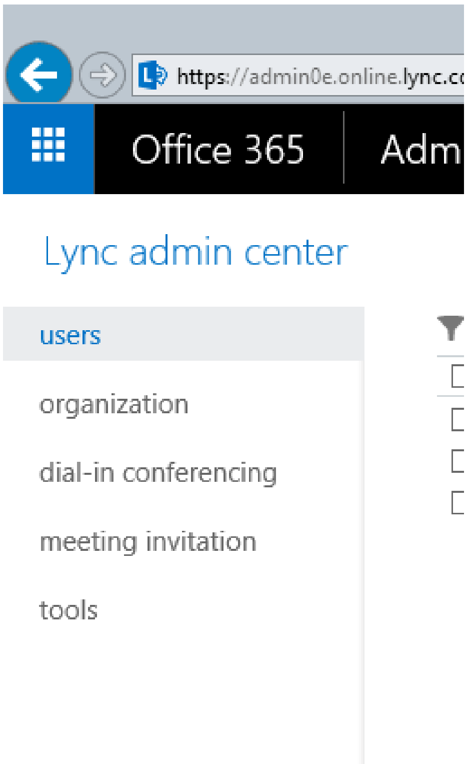
Confirm password: ••••••

15.4.2.1 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 15-12: Office 365 Skype for Business Admin Center



3. With the **Skype for Business admin center** displayed, select and copy the URL in the address bar up to **.com**. An example URL looks similar to the following: https://webdir0e.online.lync.com/lscp/?language=en-US&tenantID=

   Replace "webdir" in the URL with "admin", resulting in the following: `https://admin0e.online.Lync.com`
4. Append the following string to the URL:

   ```
   /HostedMigration/hostedmigrationservice.svc
   ```
5. The resulting URL, which is the value of the **HostedMigrationOverrideUrl**, should look like the following:

   https://admin0e.online.lync.com/HostedMigration/hostedmigrationservice.svc

15.4.2.2 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.

15.4.3 Using Exchange Online for Voicemail

This section describes how to use Exchange Online for Voicemail.

15.4.3.1 Prepare 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 15.7 shows an example of creating a UM Dial Plan for Exchange Online.

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

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

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

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

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

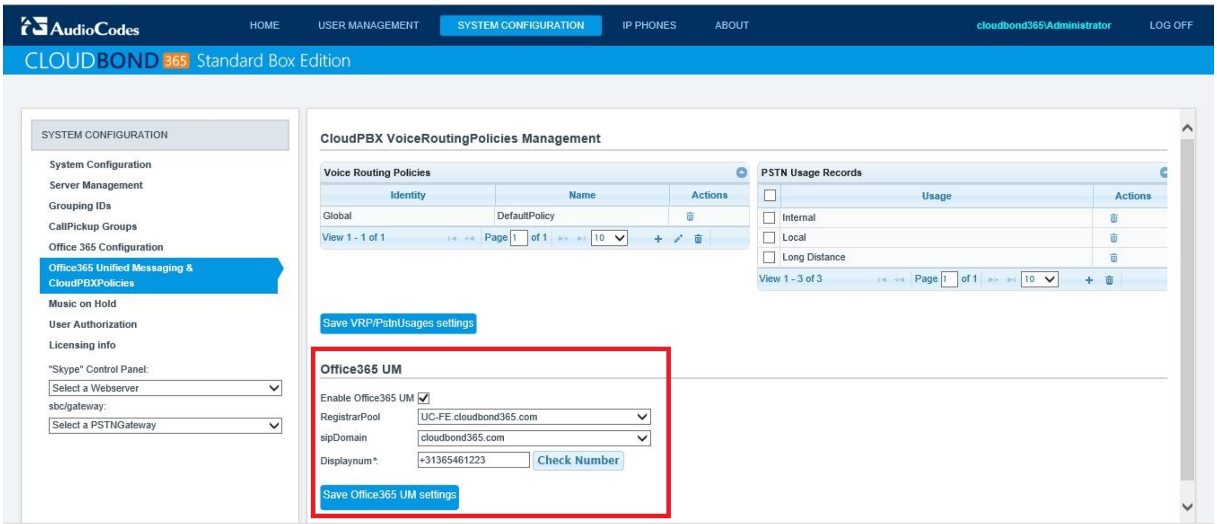
15.4.3.2 Allow Users to Dial-in to Access Exchange Online Voicemail

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 4.1 till 4.3.1 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 15-13: Office 365 UM



"Skype" Control Panel: Select a Webserver

sbc/gateway: Select a PSTNGateway

CloudPBX VoiceRoutingPolicies Management

Voice Routing Policies

Identity	Name	Actions
Global	DefaultPolicy	

View 1 - 1 of 1 Page 1 of 1 10

PSTN Usage Records

□	Usage	Actions
□	Internal	
□	Local	
□	Long Distance	

View 1 - 3 of 3 Page 1 of 1 10

Office365 UM

Enable Office365 UM ☑

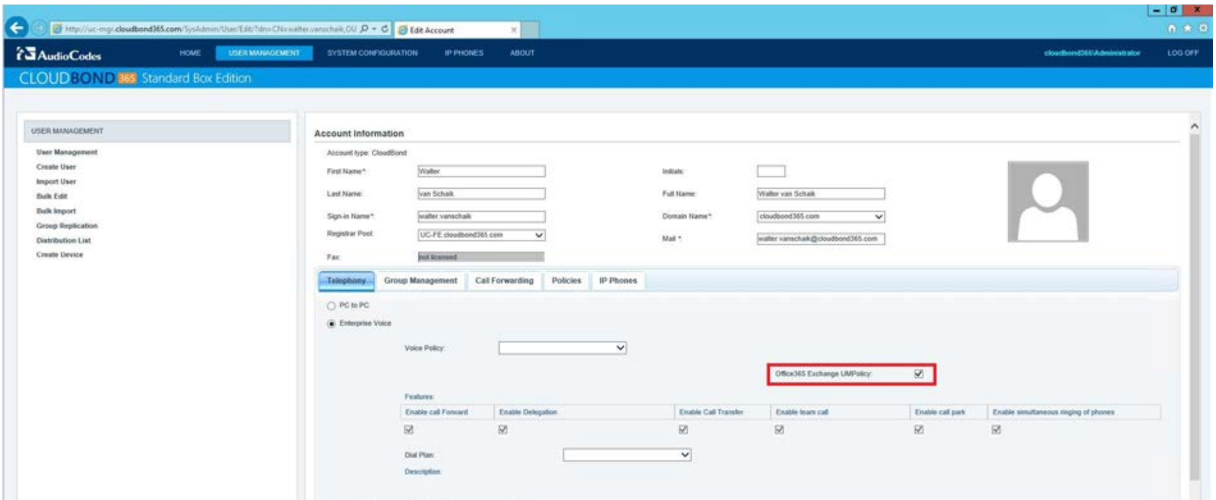
RegistrarPool: UC-FE.cloudbond365.com

sipDomain: cloudbond365.com

Displaynum*: +31365461223

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 15-14: Office 365 Exchange UM Policy



Account Information

Account type: CloudBond

First Name*: Walter

Initials:

Last Name: van Schaik

Full Name: Walter van Schaik

Sign-in Name*: walter.vanschaik

Domain Name*: cloudbond365.com

Registrar Pool: UC-FE.cloudbond365.com

Mail *: walter.vanschaik@cloudbond365.com

Fax: not licensed

○ PC to PC

● Enterprise Voice

Voice Policy:

Office365 Exchange UMPolicy: ☑

Features:

Enable call Forward	Enable Delegation	Enable Call Transfer	Enable team call	Enable call park	Enable simultaneous ringing of phones
☑	☑	☑	☑	☑	☑

Dial Plan:

Description:

15.5 Initial Replication

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

Once the Office 365 Skype for Business enabled users are replicated over to the CloudBond 365 resource forest, they will be 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: http://blog.msresource.net/2014/03/10/windows-azure-active-directory-connector- part-3-immutable-id/, to support more complex and custom build environments as well.

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

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

There are several components to the user replication process.

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

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

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

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

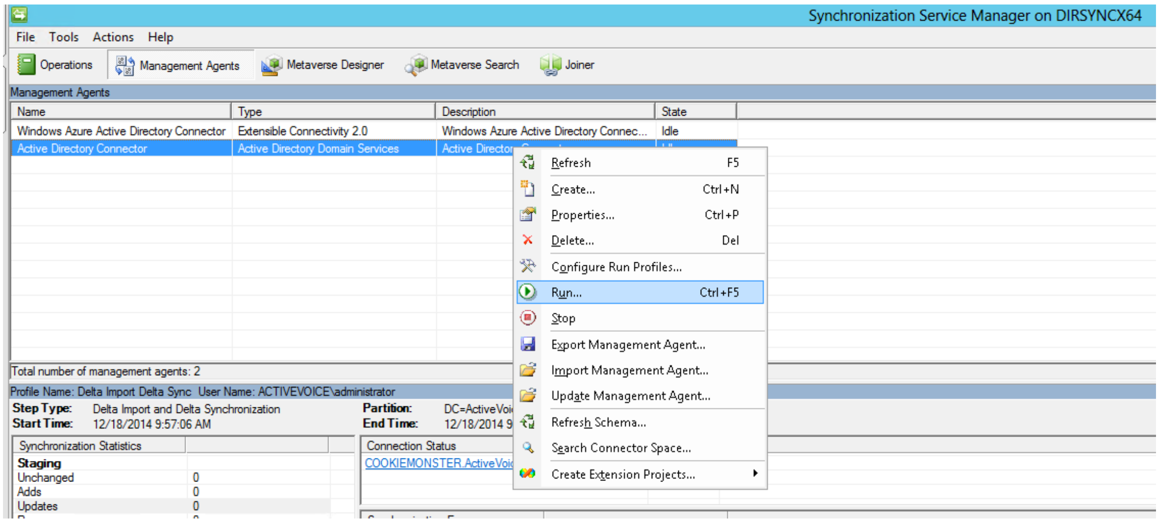
2. Match the objects with the user forest through:

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

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

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

Figure 15-15: DirSync


Synchronization Service Manager on DIRSYNCX64
File
Tools
Actions
Help
Operations
Management Agents
Metaverse Designer
Metaverse Search
Joiner
Refresh F5
Create... Ctrl+N
Properties... Ctrl+P
Delete... Del
Configure Run Profiles...
Run... Ctrl+F5
Stop
Export Management Agent...
Import Management Agent...
Update Management Agent...
Refresh Schema...
Search Connector Space...
Create Extension Projects...

Management Agents

Name	Type	Description	State
Windows Azure Active Directory Connector	Extensible Connectivity 2.0	Windows Azure Active Directory Connec...	Idle
Active Directory Connector	Active Directory Domain Services	Active Director	

Total number of management agents: 2

Profile Name: Delta Import Delta Sync User Name: ACTIVEVOICE\administrator

Step Type: Delta Import and Delta Synchronization
Start Time: 12/18/2014 9:57:06 AM
Partition: DC=ActiveVoi
End Time: 12/18/2014 9

Synchronization Statistics	
Staging	
Unchanged	0
Adds	0
Updates	0

Connection Status

COOKIEMONSTER.ActiveVoi

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

15.5.1 After Initial Replication

Now the initial replication cycle has been performed, the environment is ready to be brought into production. This step requires the public DNS records to be changed, where the specific Skype for Business SRV and A records need to be pointed 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.

15.5.1.1 Update DNS Records

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

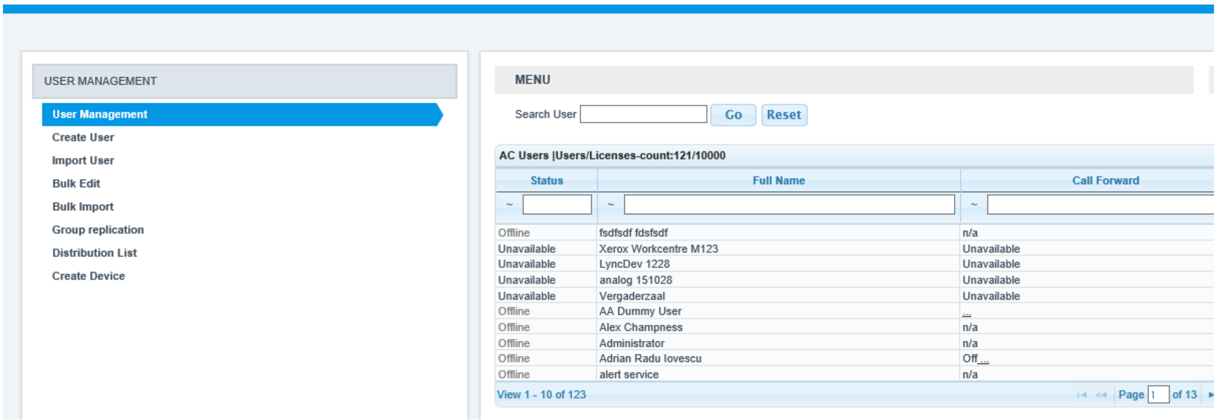
- Update the **lyncdiscover.contoso.com** A record to point to the FQDN of the on-premises reverse proxy server.
- Update the **_*sip*._tls.contoso.com** SRV record to resolve to the public IP or VIP address of the Access Edge service of Skype for Business on-premises.
- Update the **_*sipfederationtls*._tcp.contoso.com**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

15.5.1.2 Assigning User Registrar Pool

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

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

Figure 15-16: User List



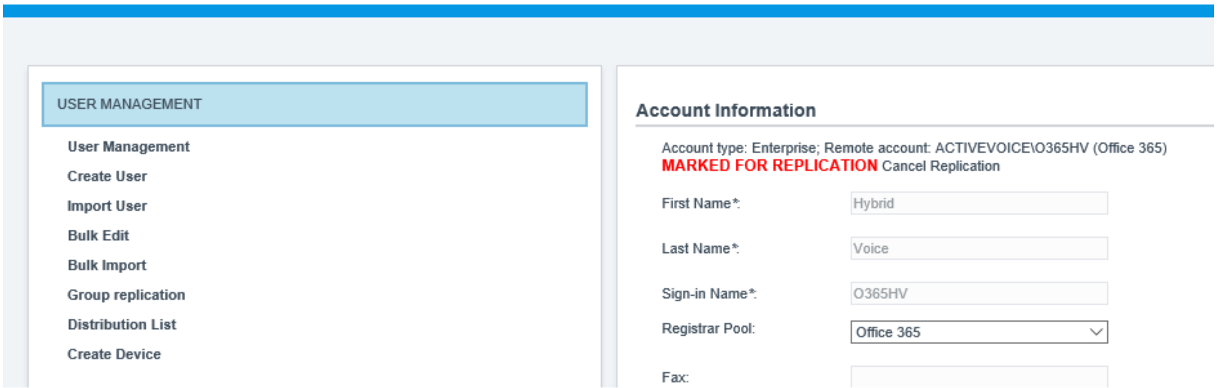
AC Users |Users/Licenses-count:121/10000

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

View 1 - 10 of 123

Assign a destination Frontend pool:

Figure 15-17: Editing a User Registrar Pool



Account Information

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

First Name*:	Hybrid
Last Name*:	Voice
Sign-in Name*:	O365HV
Registrar Pool:	Office 365
Fax:	

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

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

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

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

15.6 Ongoing Replication

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

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

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

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

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

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

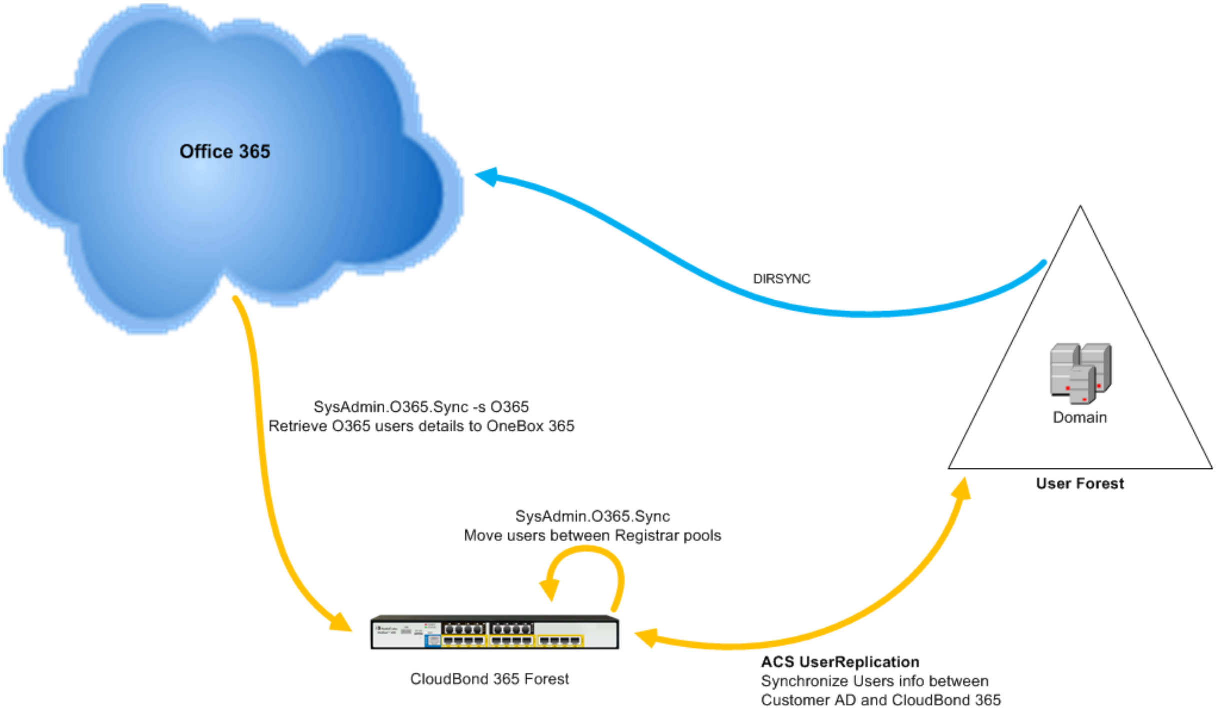
- A Scheduled task occurs at a regular interval (daily)

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

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

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

Figure 15-18: Synchronization Tasks

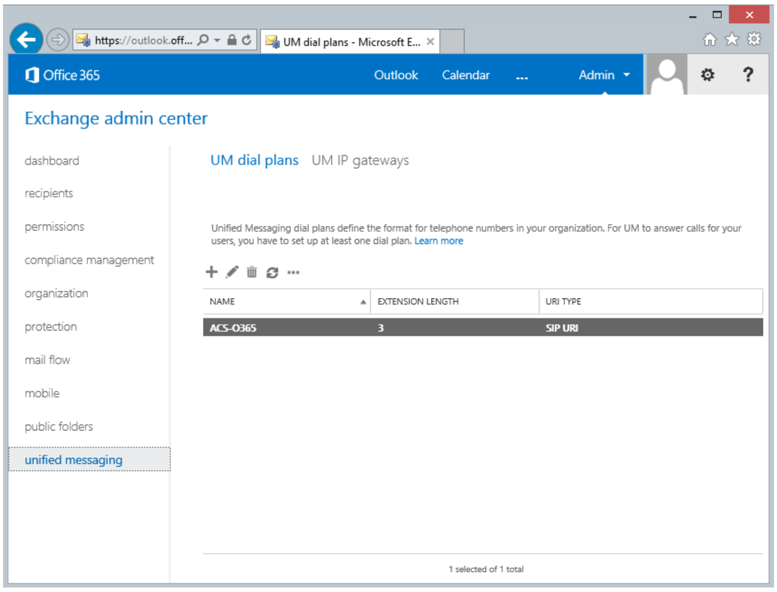

Office 365
DIRSYNC
Domain
User Forest
SysAdmin.O365.Sync -s O365
Retrieve O365 users details to OneBox 365
SysAdmin.O365.Sync
Move users between Registrar pools
CloudBond 365 Forest
ACS UserReplication
Synchronize Users info between
Customer AD and CloudBond 365

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.

15.7 Adding a Dial Plan to Exchange Online

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

Figure 15-19: Exchange Online - UM Dial Plans



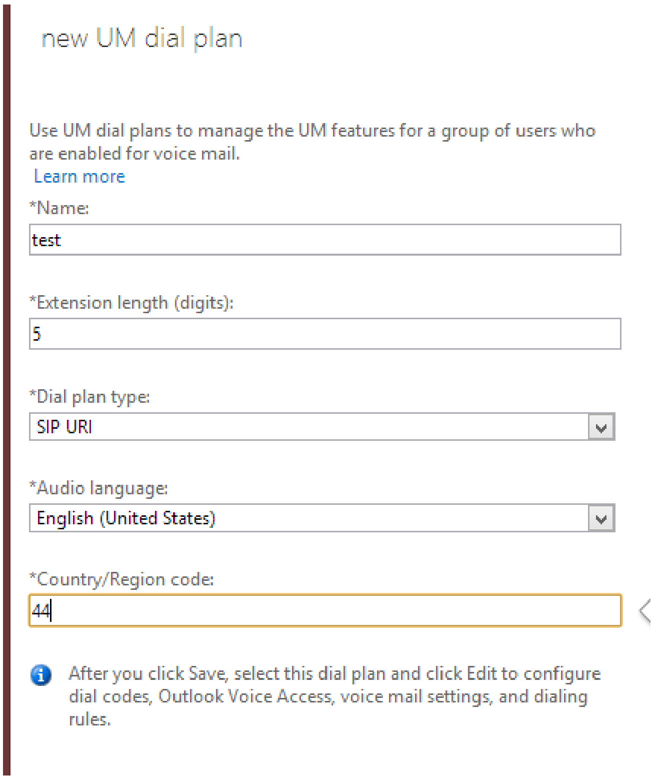
Unified Messaging dial plans define the format for telephone numbers in your organization. For UM to answer calls for your users, you have to set up at least one dial plan. Learn more

NAME	EXTENSION LENGTH	URI TYPE
ACS-O365	3	SIP URI

1 selected of 1 total

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

Figure 15-20: New Dial Plan



new UM dial plan

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

*Name:
test

*Extension length (digits):
5

*Dial plan type:
SIP URI

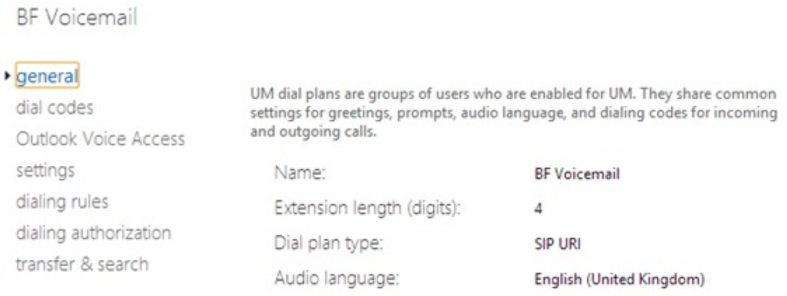
*Audio language:
English (United States)

*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 15-21: Edit the Dial Plan



BF Voicemail

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

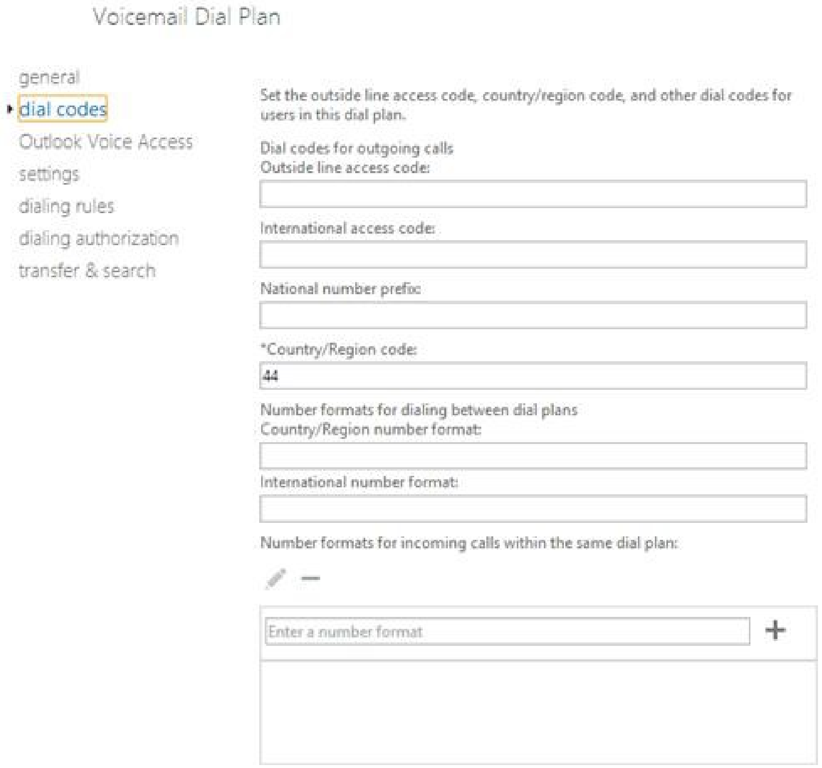
Name: BF Voicemail

Extension length (digits): 4

Dial plan type: SIP URI

Audio language: English (United Kingdom)

Figure 15-22: Dial Codes



Voicemail Dial Plan

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

Dial codes for outgoing calls

Outside line access code:

International access code:

National number prefix:

*Country/Region code: 44

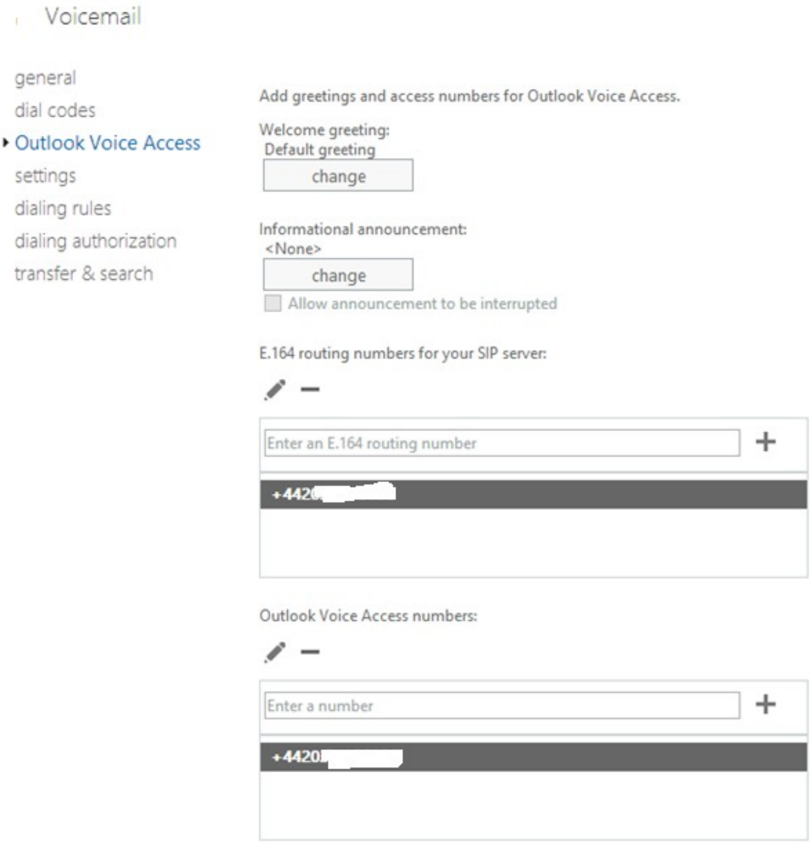
Number formats for dialing between dial plans

Country/Region number format:

International number format:

Number formats for incoming calls within the same dial plan:

Figure 15-23: Voice Access



Add greetings and access numbers for Outlook Voice Access.

Welcome greeting:
Default greeting

Informational announcement:
<None>

□ Allow announcement to be interrupted

E.164 routing numbers for your SIP server:

Enter an E.164 routing number

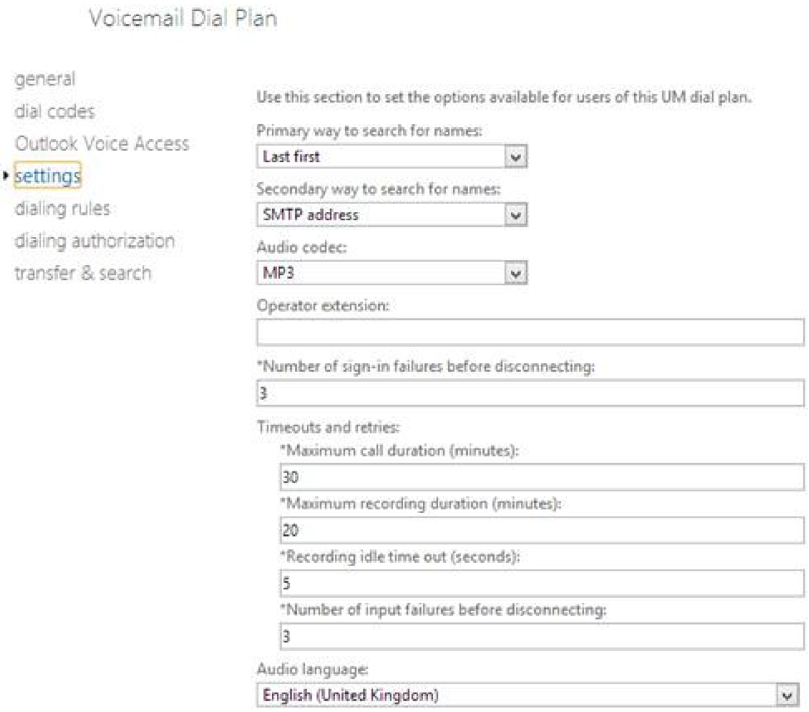
+4420[redacted]

Outlook Voice Access numbers:

Enter a number

+4420[redacted]

Figure 15-24: Settings



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

Primary way to search for names: Last first

Secondary way to search for names: SMTP address

Audio codec: MP3

Operator extension:

*Number of sign-in failures before disconnecting: 3

Timeouts and retries:

*Maximum call duration (minutes): 30

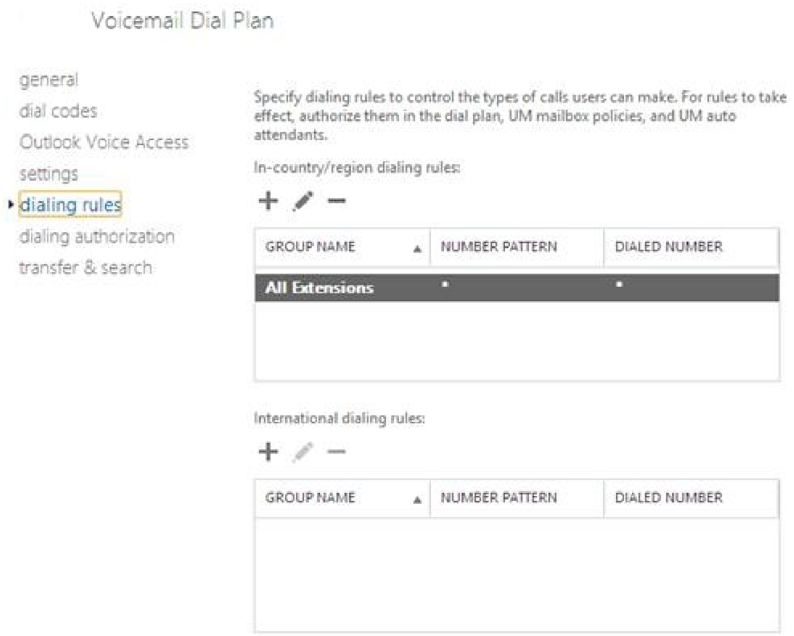
*Maximum recording duration (minutes): 20

*Recording idle time out (seconds): 5

*Number of input failures before disconnecting: 3

Audio language: English (United Kingdom)

Figure 15-25: Dialing Rules



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

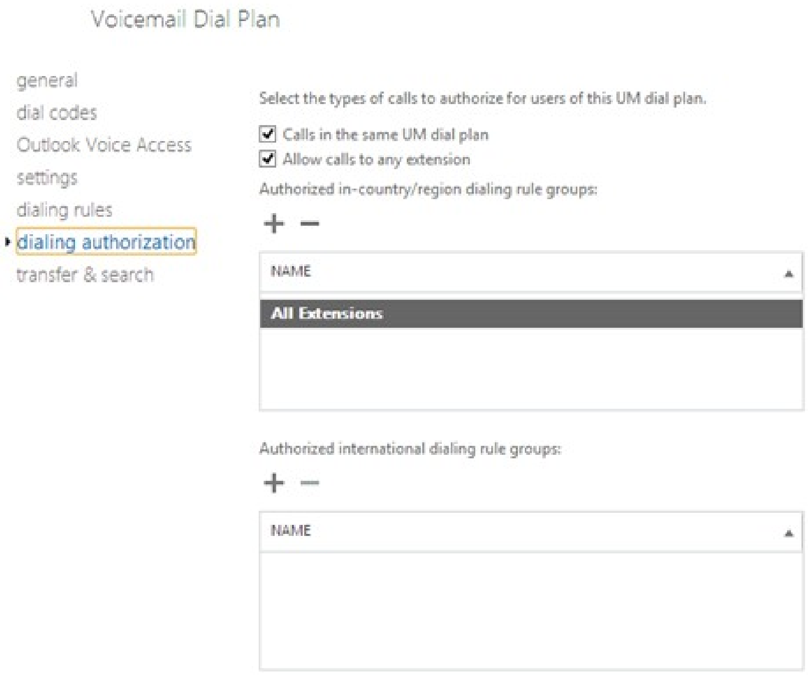
In-country/region dialing rules:

GROUP NAME ▲	NUMBER PATTERN	DIALED NUMBER
All Extensions	*	*

International dialing rules:

GROUP NAME ▲	NUMBER PATTERN	DIALED NUMBER

Figure 15-26: Dialing Authorizations



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

☑ Calls in the same UM dial plan

☑ Allow calls to any extension

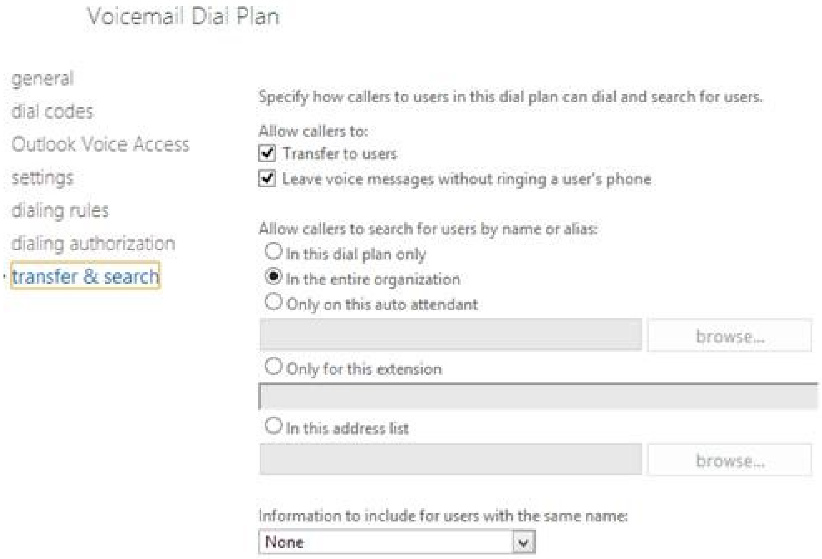
Authorized in-country/region dialing rule groups:

NAME ▲
All Extensions

Authorized international dialing rule groups:

NAME ▲

Figure 15-27: Transfer and Search



Voicemail Dial Plan

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

Allow callers to:

☑ Transfer to users

☑ Leave voice messages without ringing a user's phone

Allow callers to search for users by name or alias:

○ In this dial plan only

● In the entire organization

○ Only on this auto attendant

○ Only for this extension

○ In this address list

Information to include for users with the same name:

None

15.8 Skype for Business PowerShell

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

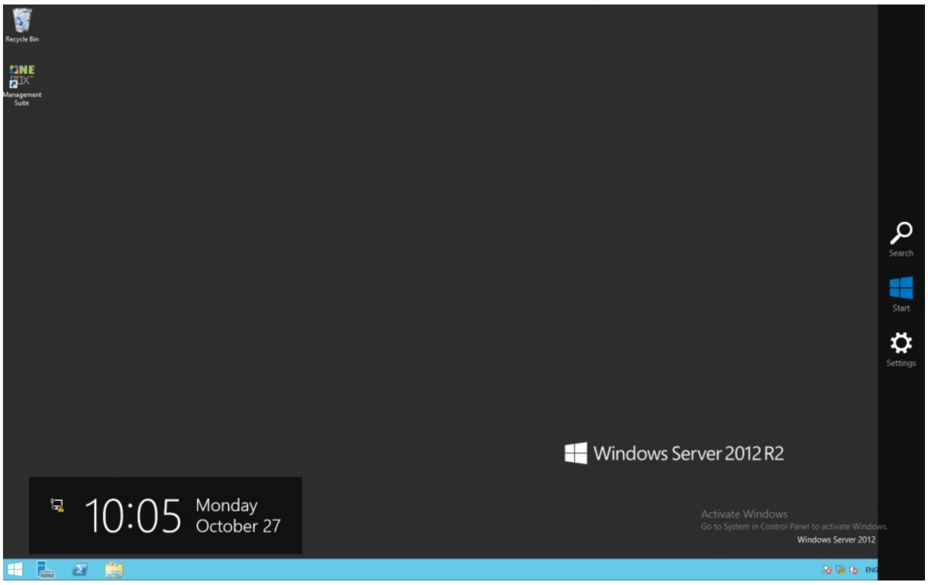
The Skype for Business Server Management Shell is a PowerShell environment with a Skype for Business specific command extension module added, which enables you to manage the Skype for Business environment from the command line. Similar modules are available for other products, such as Exchange.

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 15-28: Windows Server 2012 R2



5. Open the charms bar.

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

Figure 15-29: Searching for Skype for Business

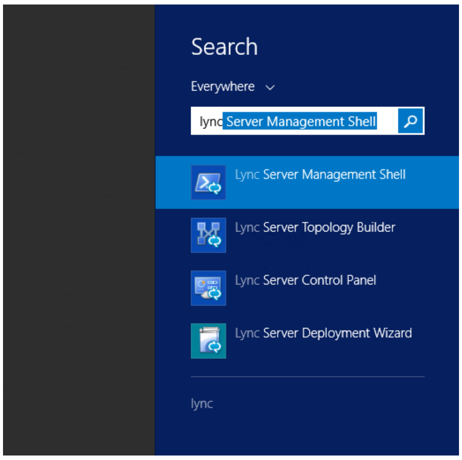
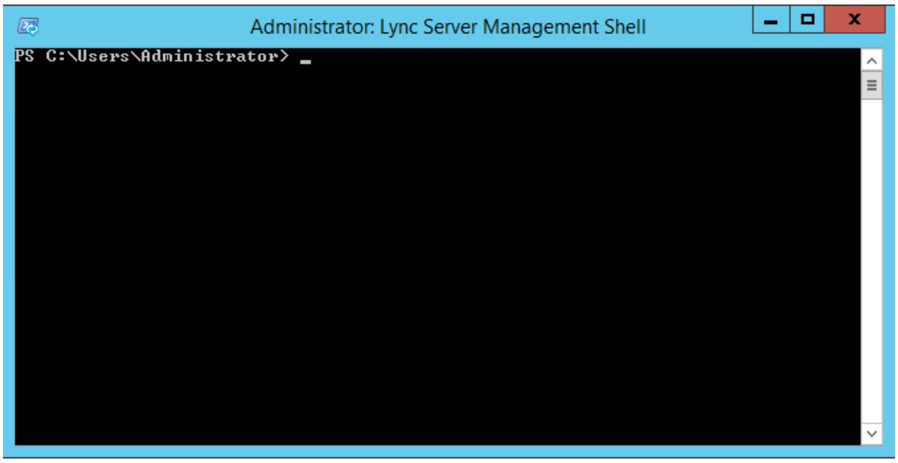

Search
Everywhere
lync Server Management Shell
Lync Server Management Shell
Lync Server Topology Builder
Lync Server Control Panel
Lync Server Deployment Wizard
lync

Figure 15-30: The Skype for Business Server Management Shell



```
PS C:\Users\Administrator> _
```

15.9 PowerShell for Skype for Business Online

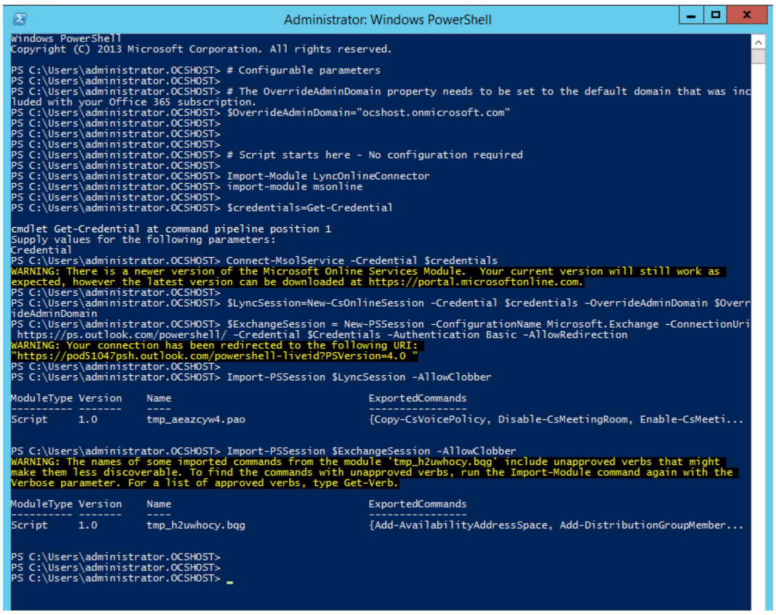
This chapter provides a sample PowerShell script which connects to Skype for Business On-Line to allow entering PowerShell command line configuration items. You will need to satisfy the pre-requisites detailed in the following links, prior to using PowerShell for online components:

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

15.9.1 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.)
```

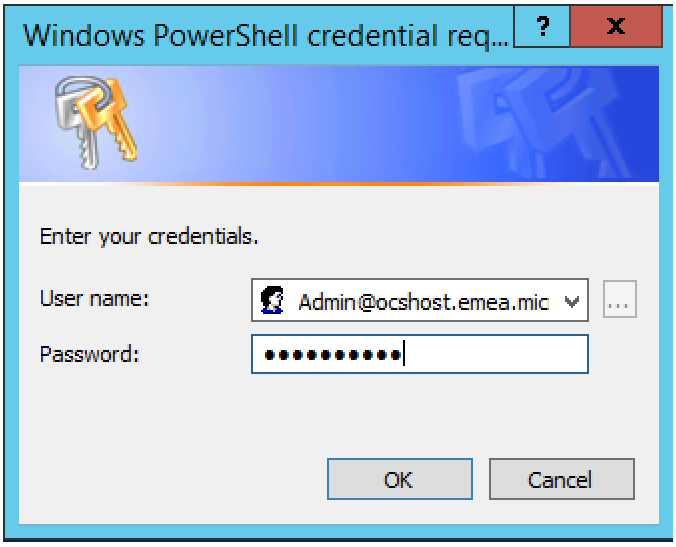
Figure 15-31: Windows PowerShell



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

PS C:\Users\administrator.OCSHOST> # Configurable parameters
PS C:\Users\administrator.OCSHOST>
PS C:\Users\administrator.OCSHOST> # The OverrideAdminDomain property needs to be set to the default domain that was inc
luded with your Office 365 subscription.
PS C:\Users\administrator.OCSHOST> $OverrideAdminDomain="ocshost.onmicrosoft.com"
PS C:\Users\administrator.OCSHOST>
PS C:\Users\administrator.OCSHOST>
PS C:\Users\administrator.OCSHOST>
PS C:\Users\administrator.OCSHOST> # Script starts here - No configuration required
PS C:\Users\administrator.OCSHOST>
PS C:\Users\administrator.OCSHOST> Import-Module LyncOnlineConnector
PS C:\Users\administrator.OCSHOST> import-module msonline
PS C:\Users\administrator.OCSHOST>
PS C:\Users\administrator.OCSHOST> $credentials=Get-Credential

cmdlet Get-Credential at command pipeline position 1
Supply values for the following parameters:
Credential
PS C:\Users\administrator.OCSHOST> Connect-MsolService -Credential $credentials
WARNING: There is a newer version of the Microsoft Online Services Module.  Your current version will still work as
expected, however the latest version can be downloaded at https://portal.microsoftonline.com.
PS C:\Users\administrator.OCSHOST>
PS C:\Users\administrator.OCSHOST> $LyncSession=New-CsOnlineSession -Credential $credentials -OverrideAdminDomain $Overr
ideAdminDomain
PS C:\Users\administrator.OCSHOST> $ExchangeSession = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri
 https://ps.outlook.com/powershell/ -Credential $Credentials -Authentication Basic -AllowRedirection
WARNING: Your connection has been redirected to the following URI:
"https://pod51047psh.outlook.com/powershell-liveid?PSVersion=4.0 "
PS C:\Users\administrator.OCSHOST>
PS C:\Users\administrator.OCSHOST> Import-PSSession $LyncSession -AllowClobber

ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Script     1.0        tmp_aeazcyw4.pao                    {Copy-CsVoicePolicy, Disable-CsMeetingRoom, Enable-CsMeeti...


PS C:\Users\administrator.OCSHOST> Import-PSSession $ExchangeSession -AllowClobber
WARNING: The names of some imported commands from the module 'tmp_h2uwhocy.bqg' include unapproved verbs that might
make them less discoverable. To find the commands with unapproved verbs, run the Import-Module command again with the
Verbose parameter. For a list of approved verbs, type Get-Verb.

ModuleType Version    Name                                ExportedCommands
---------- -------    ----                                ----------------
Script     1.0        tmp_h2uwhocy.bqg                    {Add-AvailabilityAddressSpace, Add-DistributionGroupMember...


PS C:\Users\administrator.OCSHOST>
PS C:\Users\administrator.OCSHOST>
PS C:\Users\administrator.OCSHOST> _
```

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

Figure 15-32: Login Credentials



Windows PowerShell credential req...

Enter your credentials.

User name: Admin@ocshost.emea.mic

Password: ●●●●●●●●●●

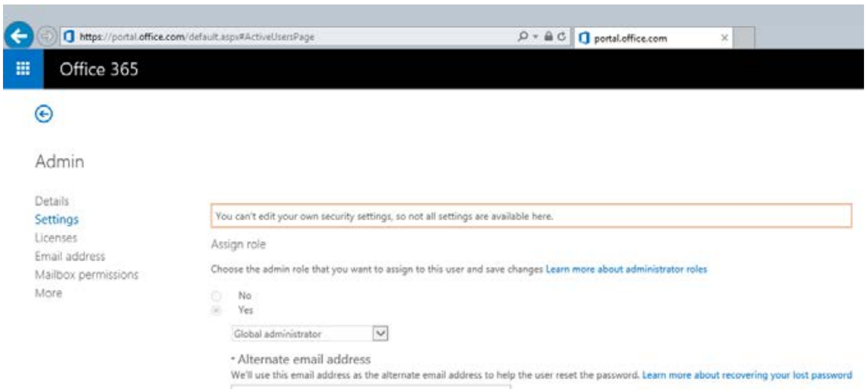
When the script completes, you can enter Skype for Business Online PowerShell commands to configure your Skype for Business Online environment.

15.10 Troubleshooting

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

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

Figure 15-33: Admin Settings



https://portal.office.com/default.aspx#ActiveUsersPage

portal.office.com

Office 365

Admin

You can't edit your own security settings, so not all settings are available here.

Assign role

Choose the admin role that you want to assign to this user and save changes Learn more about administrator roles

○ No
● Yes

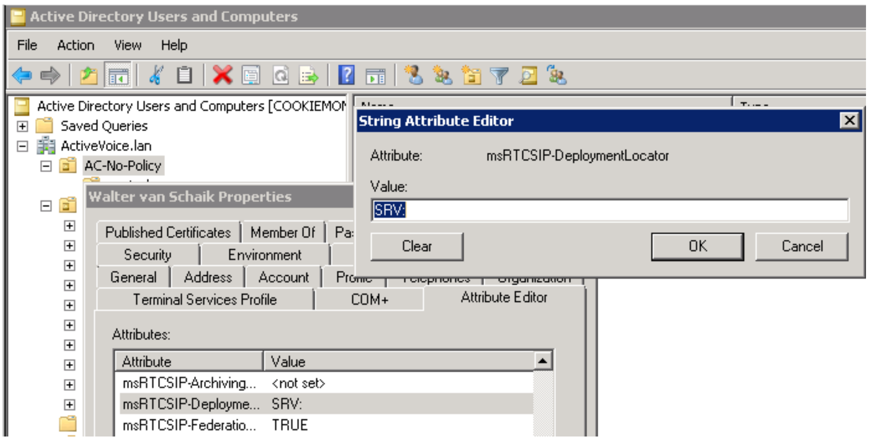
Global administrator

* 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

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

Figure 15-34: String Attribute Editor



Attribute: msRTCSIP-DeploymentLocator

Value: SRV:

Attributes:

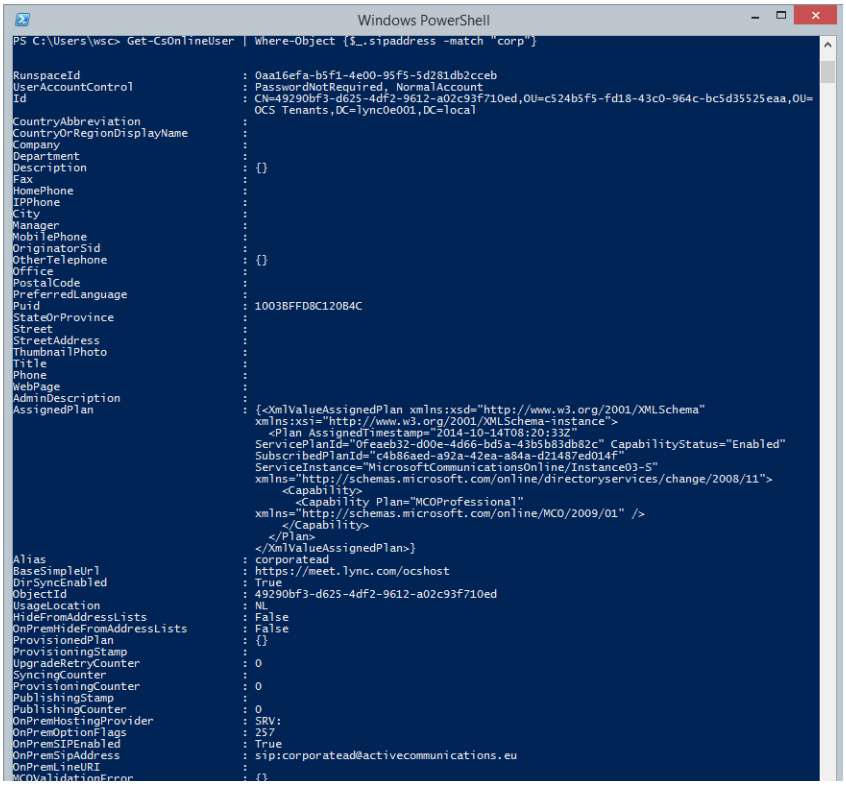
Attribute	Value
msRTCSIP-Archiving...	<not set>
msRTCSIP-Deployme...	SRV:
msRTCSIP-Federatio...	TRUE

3. 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 premise data to the cloud:

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

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

Figure 15-35: Get-csOnlineUser Attributes



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


RunspaceId                         : 0aa16efa-b5f1-4e00-95f5-5d281db2cceb
UserAccountControl                 : PasswordNotRequired, NormalAccount
Id                                 : CN=49290bf3-d625-4df2-9612-a02c93f710ed,OU=c524b5f5-fd18-43c0-964c-bc5d35525eaa,OU=
                                     OCS Tenants,DC=lync0e001,DC=local
CountryAbbreviation                :
CountryOrRegionDisplayName         :
Company                            :
Department                         :
Description                        : {}
Fax                                :
HomePhone                          :
IPPhone                            :
City                               :
Manager                            :
MobilePhone                        :
OriginatorSid                      :
OtherTelephone                     : {}
Office                             :
PostalCode                         :
PreferredLanguage                  :
Puid                               : 1003BFFD8C120B4C
StateOrProvince                    :
Street                             :
StreetAddress                      :
ThumbnailPhoto                     :
Title                              :
Phone                              :
WebPage                            :
AdminDescription                   :
AssignedPlan                       : {<XmlValueAssignedPlan xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
                                       <Plan AssignedTimestamp="2014-10-14T08:20:33Z"
                                     ServicePlanId="0feaeb32-d00e-4d66-bd5a-43b5b83db82c" CapabilityStatus="Enabled"
                                     SubscribedPlanId="c4b86aed-a92a-42ea-a84a-d21487ed014f"
                                     ServiceInstance="MicrosoftCommunicationsOnline/Instance03-S"
                                     xmlns="http://schemas.microsoft.com/online/directoryservices/change/2008/11">
                                         <Capability>
                                           <Capability Plan="MCOProfessional"
                                     xmlns="http://schemas.microsoft.com/online/MCO/2009/01" />
                                         </Capability>
                                       </Plan>
                                     </XmlValueAssignedPlan>}
Alias                              : corporatead
BaseSimpleUrl                      : https://meet.lync.com/ocshost
DirSyncEnabled                     : True
ObjectId                           : 49290bf3-d625-4df2-9612-a02c93f710ed
UsageLocation                      : NL
HideFromAddressLists               : False
OnPremHideFromAddressLists         : False
ProvisionedPlan                    : {}
ProvisioningStamp                  :
UpgradeRetryCounter                : 0
SyncingCounter                     :
ProvisioningCounter                : 0
PublishingStamp                    :
PublishingCounter                  : 0
OnPremHostingProvider              : SRV:
OnPremOptionFlags                  : 257
OnPremSIPEnabled                   : True
OnPremSipAddress                   : sip:corporatead@activecommunications.eu
OnPremLineURI                      :
MCOValidationError                 : {}
```

We are specifically interested in the following attributes:

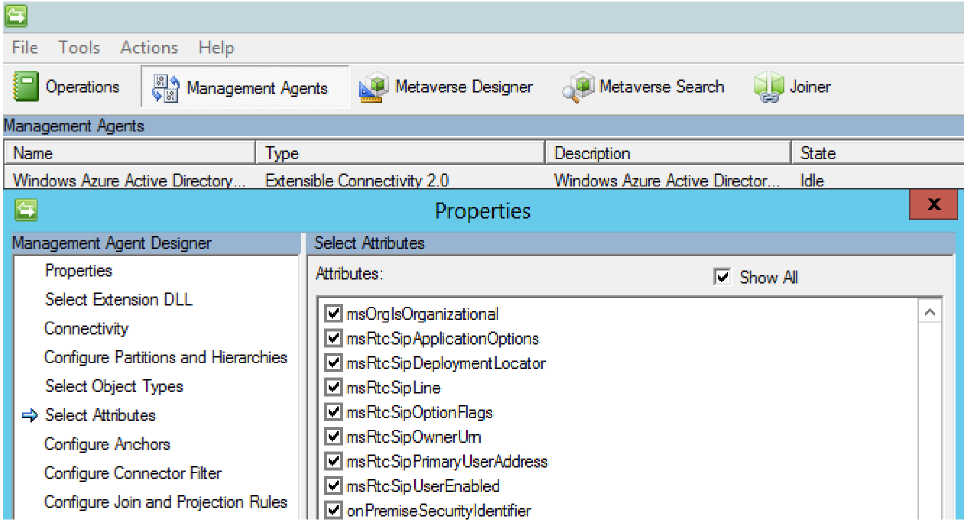
- OnPremHostingProvider: SRV:
- OnPremOptionFlags 257
- OnPremSIPEnabled : True
- OnPremSipAddress : sip:corporatead@activecommunications.eu

This tells 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 will hold 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 those attributes are showing up empty, perform the manual steps as described in Initial Replication chapter for the particular user and make sure that the Office 365 Directory Synchronization agents replicate those values by right-clicking those properties and verifying the Properties.z.

Figure 15-36: Windows Azure AD Properties



Management Agents

Name	Type	Description	State
Windows Azure Active Directory...	Extensible Connectivity 2.0	Windows Azure Active Director...	Idle

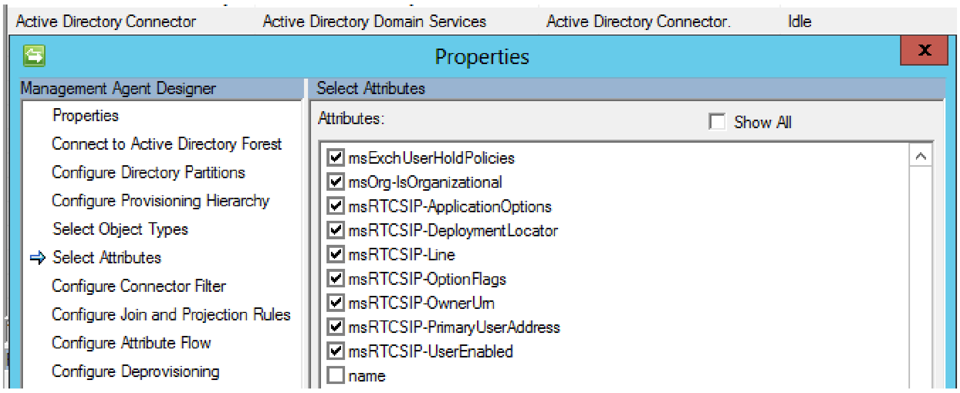
Management Agent Designer
- Properties
- Select Extension DLL
- Connectivity
- Configure Partitions and Hierarchies
- Select Object Types
- ⇨ Select Attributes
- Configure Anchors
- Configure Connector Filter
- Configure Join and Projection Rules

Select Attributes

Attributes: ☑ Show All

- ☑ msOrgIsOrganizational
- ☑ msRtcSipApplicationOptions
- ☑ msRtcSipDeploymentLocator
- ☑ msRtcSipLine
- ☑ msRtcSipOptionFlags
- ☑ msRtcSipOwnerUrn
- ☑ msRtcSipPrimaryUserAddress
- ☑ msRtcSipUserEnabled
- ☑ onPremiseSecurityIdentifier

Figure 15-37: DirSync AD Connector properties



Active Directory Connector	Active Directory Domain Services	Active Directory Connector.	Idle

Management Agent Designer
- Properties
- Connect to Active Directory Forest
- Configure Directory Partitions
- Configure Provisioning Hierarchy
- Select Object Types
- ⇨ Select Attributes
- Configure Connector Filter
- Configure Join and Projection Rules
- Configure Attribute Flow
- Configure Deprovisioning

Select Attributes

Attributes: □ Show All

- ☑ msExchUserHoldPolicies
- ☑ msOrg-IsOrganizational
- ☑ msRTCSIP-ApplicationOptions
- ☑ msRTCSIP-DeploymentLocator
- ☑ msRTCSIP-Line
- ☑ msRTCSIP-OptionFlags
- ☑ msRTCSIP-OwnerUrn
- ☑ msRTCSIP-PrimaryUserAddress
- ☑ msRTCSIP-UserEnabled
- □ name

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

15.11 Custom User IDs for Cross Domain Updates

This chapter describes the Custom User IDs for Cross Domain updates.

15.11.1 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.

15.11.2 Retrieving User Data from Office 365

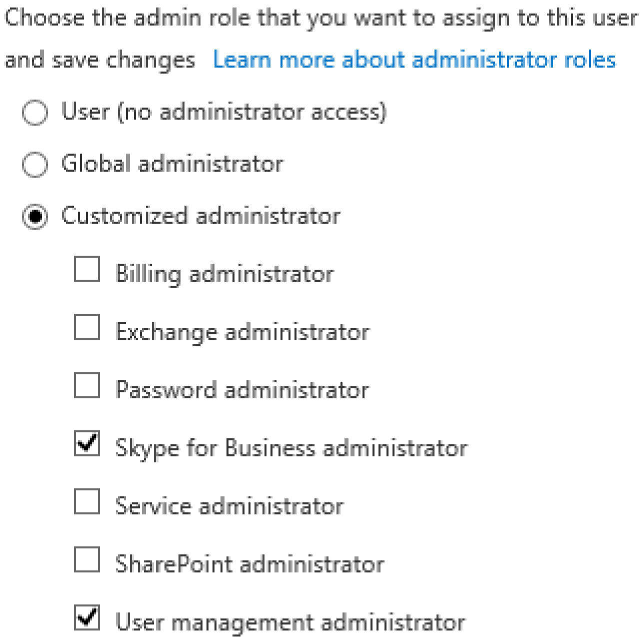
The updates to the cloudbond365 directory from Office 365 are performed by a scheduled task. The scheduled task runs the following:

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

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

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

Figure 15-38: 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

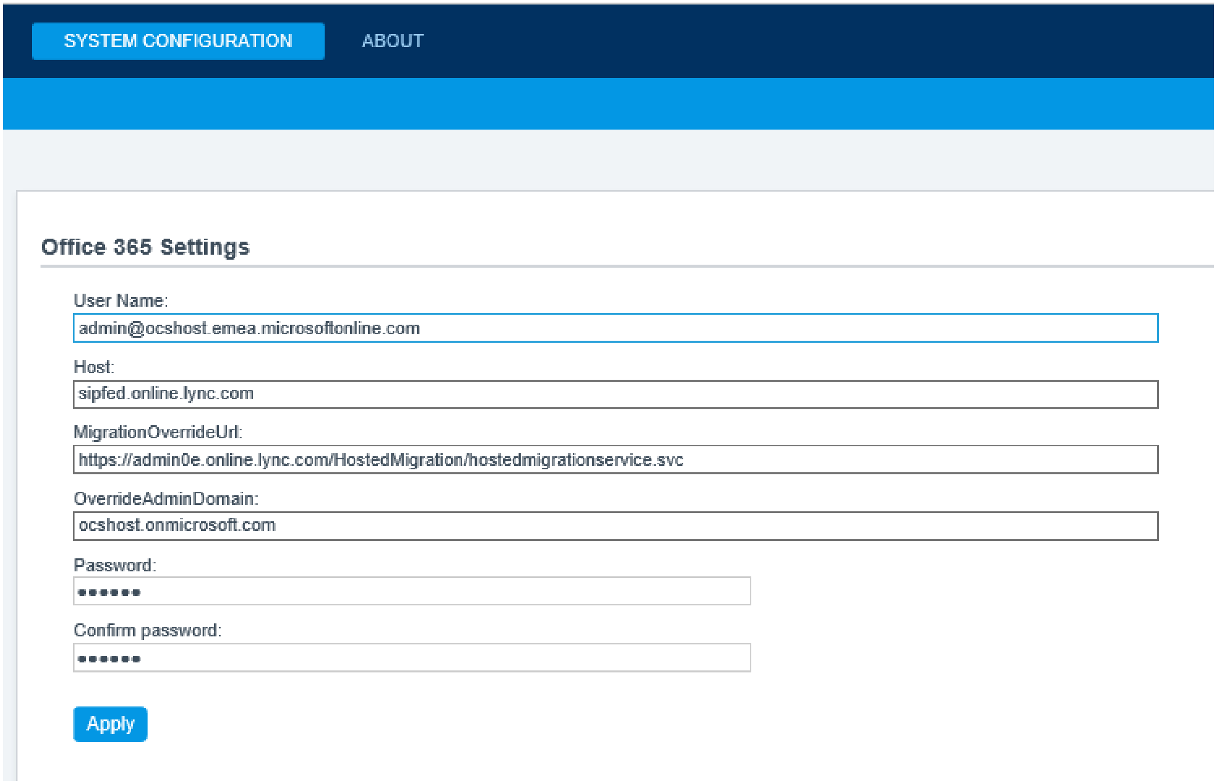
● Customized administrator

- ☐ 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 15-39: Office 365 Settings



Office 365 Settings

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

Host: sipfed.online.lync.com

MigrationOverrideUrl: https://admin0e.online.lync.com/HostedMigration/hostedmigrationservice.svc

OverrideAdminDomain: ocshost.onmicrosoft.com

Password: ••••••

Confirm password: ••••••

This page is intentionally left blank.

16 Reverse Proxy using IIS ARR

16.1 Introduction

This chapter describes using Microsoft IIS (Internet Information Server) and ARR (Application Request Routing) as a Reverse Proxy solution for AudioCodes CloudBond 365 deployments.

This guide provides:

- Background information on Skype for Business and Reverse Proxies
- Recommendations for installing IIS and ARR
- Configuring IIS and ARR

Further information can be found at:

http://blogs.technet.com/b/nexthop/archive/2013/02/19/using-iis-arr-as-a-reverse-proxy-for-lync-server-2013.aspx

http://www.iis.net/learn/install/installing-iis-85/installing-iis-85-on-windows-server-2012-r2
http://www.jaapwesselius.com/2014/03/16/using-arr-for-reverse-proxy-with-lync-2013/

16.2 Proxy Servers

This chapter describes the Proxy servers used in the Reverse Proxy installation.

16.2.1 What is a Reverse Proxy?

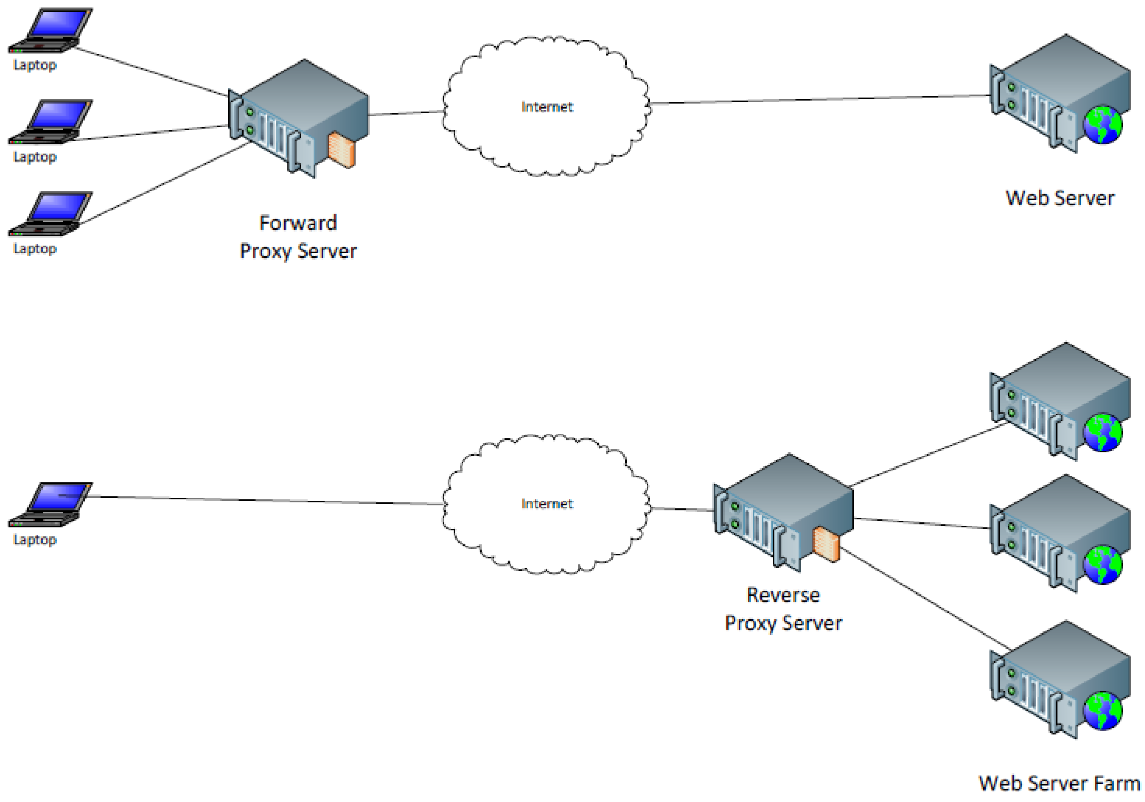
A proxy server is typically an intermediate server for web (HTTP) traffic, located between the web browser (client) and the web server.

Some readers will be familiar with forward proxy servers. These are typically employed by large companies and ISPs to provide access control, authorization and caching of internet data, i.e., the proxy server keeps copies of web site information for recently visited web sites. The web browser will often download information from the local proxy server, which is much faster and cheaper in traffic terms rather than go to the original remote web site each time to retrieve information.

A reverse proxy performs some similar tasks, but at the web server end, not the client end. A reverse proxy server is deployed for security, rerouting, caching, and load balancing, i.e., the web browser request is received by the reverse proxy and forwarded to one of many web servers hosting the same data, to achieve load balancing.

Both forms of proxy server are usually invisible to the end user. Both forms of proxy may be used at the same time.

Figure 16-1: Proxy Servers



For more information on proxy servers, see:

http://stackoverflow.com/questions/224664/difference-between-proxy-server-and-reverse-proxy-server

16.2.2 Why have a Reverse Proxy Server for Skype for Business?

Skype for Business is designed to operate with a Reverse Proxy server for external communications.

The Skype for Business Edge server handles external SIP and RTC traffic used in Access, Web Conferencing, and A/V, but does not handle Web based HTTP traffic. The Edge server can be considered a SIP proxy server handling login, presence, and audio. The Edge server is specifically designed to minimize security risks through exposure to the internet, and for this reason, should not be a member of the internal domain.

All Web based HTTP traffic is handled by the Skype for Business FE servers. However, the FE server must be a domain member to function correctly, so it's a security risk to expose the FE servers directly to the internet.

To overcome the security risks, a reverse proxy server is used to filter external web (HTTP) traffic before routing it to the FE server.

More information can be found at: http://www.lyncinsider.com/tag/reverse-proxy/

16.2.3 Skype for Business Reverse Proxy Functions

To use any of the following Skype for Business features, you will need to deploy a Reverse Proxy server.

- Enabling external users to download meeting content for your meetings.
- Enabling external users to expand distribution groups.
- Enabling remote users to download files from the Address Book service.
- Accessing the Skype for Business Web App client.
- Accessing the Dial-in Conferencing Settings webpage.
- Enabling external devices to connect to Device Update web service and obtain updates.
- Enabling mobile applications to automatically discover and use the mobility (Mcx) URLs from the Internet.
- Enabling the Skype for Business client, Skype for Business Windows Store app and Skype for Business Mobile client to locate the Skype for Business Discover (autodiscover) URLs and use the Unified Communications Web API (UCWA).

See https://technet.microsoft.com/en-au/library/gg398069.aspx for more information.

16.2.4 What is ARR?

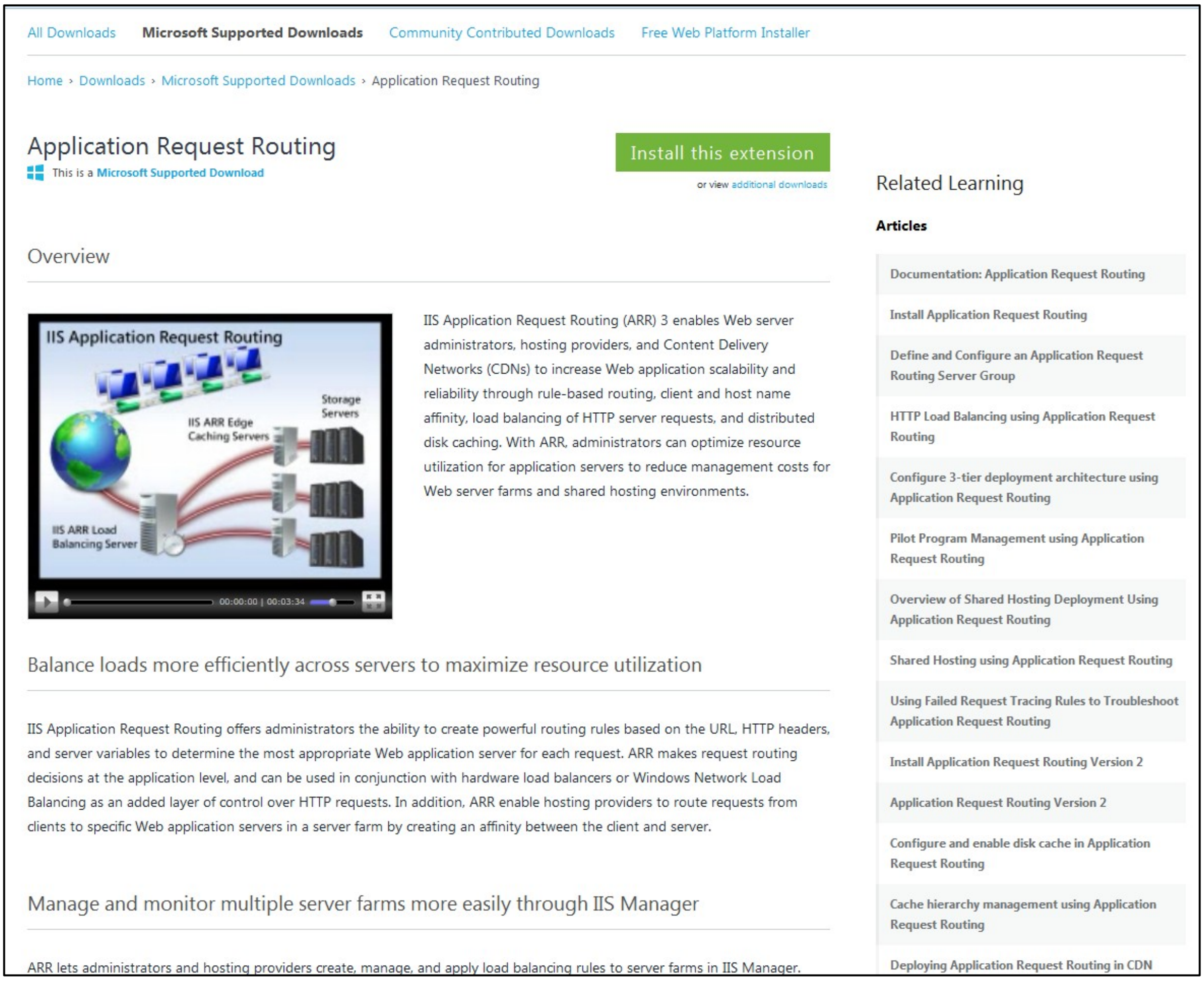
ARR is a component of the IIS which allows the Web server to function as a Reverse Proxy server. The IIS and ARR combination is a relatively inexpensive way to provide a Reverse Proxy server for Skype for Business (IIS and ARR are free components of Windows 2012).

The IIS and ARR combination is only one possible Reverse Proxy solution for Skype for Business. There are many others, ranging from the free, Linux-based Pound or Apache software, to dedicated hardware solutions such as F5 or Kemp, and expensive corporate scale software solutions.

Note: Microsoft's former solution, Threat Management Gateway (TMG), was withdrawn in 2012.

For further details about ARR, see http://www.iis.net/downloads/microsoft/application-request-routing.

Figure 16-2: Application Request Routing (ARR)


IIS Application Request Routing
Storage Servers
IIS ARR Edge Caching Servers
IIS ARR Load Balancing Server
00:00:00 | 00:03:34

All Downloads · **Microsoft Supported Downloads** · Community Contributed Downloads · Free Web Platform Installer

Home › Downloads › Microsoft Supported Downloads › Application Request Routing

Application Request Routing

This is a **Microsoft Supported Download**

Install this extension

or view additional downloads

Overview

IIS Application Request Routing (ARR) 3 enables Web server administrators, hosting providers, and Content Delivery Networks (CDNs) to increase Web application scalability and reliability through rule-based routing, client and host name affinity, load balancing of HTTP server requests, and distributed disk caching. With ARR, administrators can optimize resource utilization for application servers to reduce management costs for Web server farms and shared hosting environments.

Balance loads more efficiently across servers to maximize resource utilization

IIS Application Request Routing offers administrators the ability to create powerful routing rules based on the URL, HTTP headers, and server variables to determine the most appropriate Web application server for each request. ARR makes request routing decisions at the application level, and can be used in conjunction with hardware load balancers or Windows Network Load Balancing as an added layer of control over HTTP requests. In addition, ARR enable hosting providers to route requests from clients to specific Web application servers in a server farm by creating an affinity between the client and server.

Manage and monitor multiple server farms more easily through IIS Manager

ARR lets administrators and hosting providers create, manage, and apply load balancing rules to server farms in IIS Manager.

Related Learning

Articles

- Documentation: Application Request Routing
- Install Application Request Routing
- Define and Configure an Application Request Routing Server Group
- HTTP Load Balancing using Application Request Routing
- Configure 3-tier deployment architecture using Application Request Routing
- Pilot Program Management using Application Request Routing
- Overview of Shared Hosting Deployment Using Application Request Routing
- Shared Hosting using Application Request Routing
- Using Failed Request Tracing Rules to Troubleshoot Application Request Routing
- Install Application Request Routing Version 2
- Application Request Routing Version 2
- Configure and enable disk cache in Application Request Routing
- Cache hierarchy management using Application Request Routing
- Deploying Application Request Routing in CDN

16.3 Installing IIS and ARR

IIS and ARR must be installed on a separate Windows 2012 R2 server, located in your network DMZ. Since the server is located in your DMZ and is therefore exposed to internet traffic, the server should be a standalone installation and should not be made a member of any domain.

The preferred installation method for IIS and ARR is to use the Microsoft Web Platform Installer. This will install all components required, as a single package:

http://www.microsoft.com/web/downloads/platform.aspx

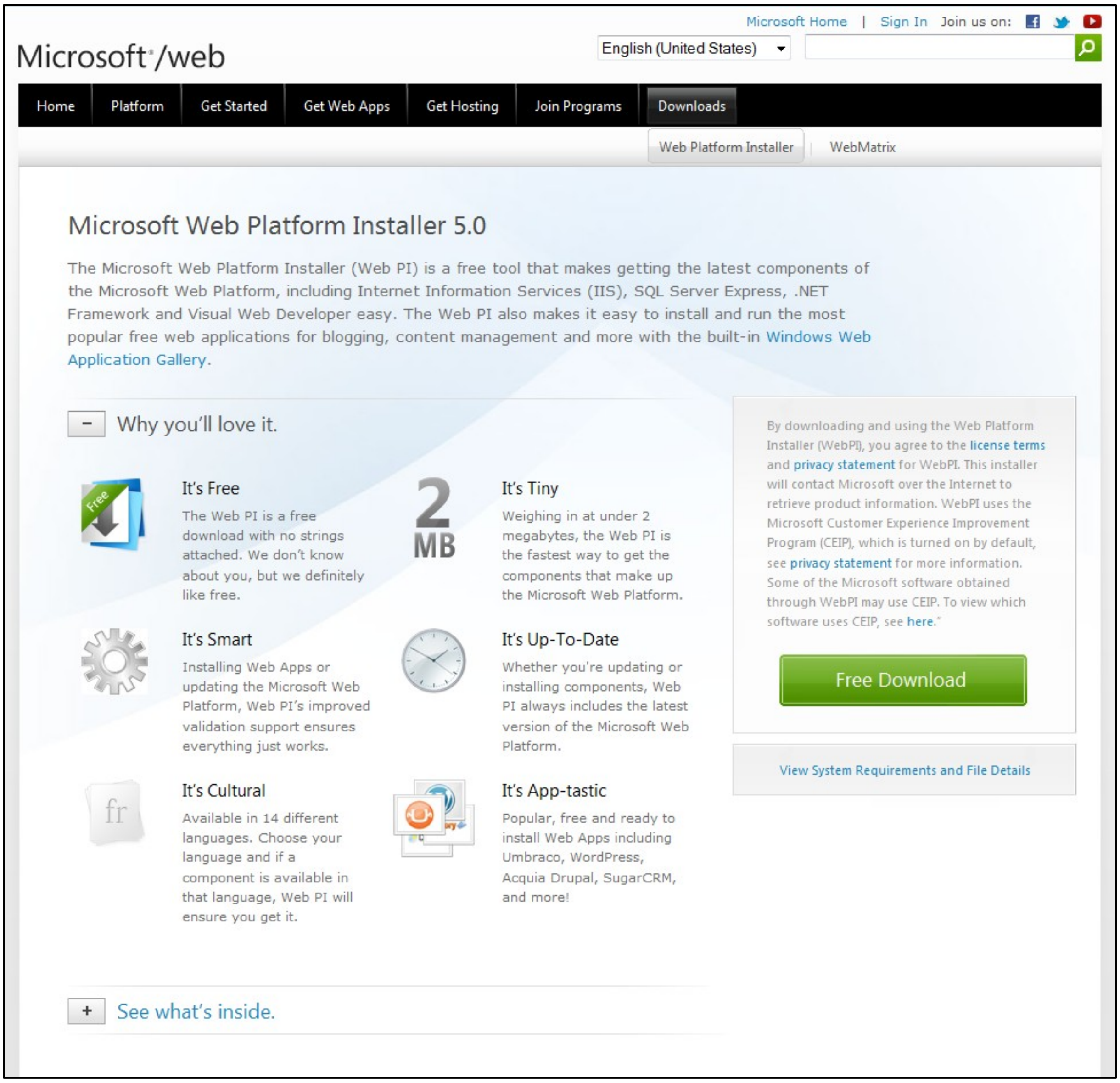
ARR 3.0 is the current release.

Though ARR components can be manually added to an existing IIS installation, it's not recommended. It can be difficult to get the installation sequence and package dependencies correct. To manually install ARR, see:

http://blogs.iis.net/wonyoo/archive/2011/04/20/how-to-install-application-request-routing-arr-2-5- without-web-platform-installer-webpi.aspx

http://blogs.technet.com/b/erezs_iis_blog/archive/2013/11/27/installing-arr-manually-without- webpi.aspx

Figure 16-3: MS Web Platform Installer



Microsoft Web Platform Installer 5.0

The Microsoft Web Platform Installer (Web PI) is a free tool that makes getting the latest components of the Microsoft Web Platform, including Internet Information Services (IIS), SQL Server Express, .NET Framework and Visual Web Developer easy. The Web PI also makes it easy to install and run the most popular free web applications for blogging, content management and more with the built-in Windows Web Application Gallery.

− Why you'll love it.

It's Free

The Web PI is a free download with no strings attached. We don't know about you, but we definitely like free.

It's Tiny

Weighing in at under 2 megabytes, the Web PI is the fastest way to get the components that make up the Microsoft Web Platform.

It's Smart

Installing Web Apps or updating the Microsoft Web Platform, Web PI's improved validation support ensures everything just works.

It's Up-To-Date

Whether you're updating or installing components, Web PI always includes the latest version of the Microsoft Web Platform.

It's Cultural

Available in 14 different languages. Choose your language and if a component is available in that language, Web PI will ensure you get it.

It's App-tastic

Popular, free and ready to install Web Apps including Umbraco, WordPress, Acquia Drupal, SugarCRM, and more!

By downloading and using the Web Platform Installer (WebPI), you agree to the license terms and privacy statement for WebPI. This installer will contact Microsoft over the Internet to retrieve product information. WebPI uses the Microsoft Customer Experience Improvement Program (CEIP), which is turned on by default, see privacy statement for more information. Some of the Microsoft software obtained through WebPI may use CEIP. To view which software uses CEIP, see here.*

+ See what's inside.

16.4 Prerequisites

This chapter describes the prerequisites for deploying the Reverse Proxy configuration.

16.4.1 Certificates

The Reverse Proxy server must publish certificate information externally for HTTPS traffic, as well as trust certificates used by the FE server.

The full certificate chain, including trusted root certificates, must be installed to make a certificate valid.

For public certificates, the root certificates for the issuing Certificate Authority may already be included by default by Microsoft, or you may need to download the certificate chain from the CA.

Though internal certificates could be used for External access, the practice is not recommended.

Where internal certifcates are used, domain member computers are normally provisioned automatically with the root CA certificate via group policy.

If the Reverse Proxy server is not a domain member, the corporate Root CA should be installed manually.

Use mmc.exe and the certificates snap-in to verify that the appropriate root certificates are installed on the Reverse Proxy server.

You will need to copy the Certificates used by your Skype for Business FE server for External communications to the Reverse Proxy server, and install them as described in this guide.

See chapter Configuring Certificates on page 299 for further details about Skype for Business Certificates.

16.4.2 DNS Lookup

The Reverse Proxy server will need to contact both internal and external servers using their DNS name. It will certainly not be possible to contact the internal servers using an external or public DNS server.

For this reason, you may decide to use a suitably configured internal DNS server, or, add entries to the Hosts file to represent your internal servers. Entries in the Hosts file would normally contain:

- Any Skype for Business FE servers
- Any WAC / OWA servers

16.5 Configuring IIS and ARR for Skype for Business

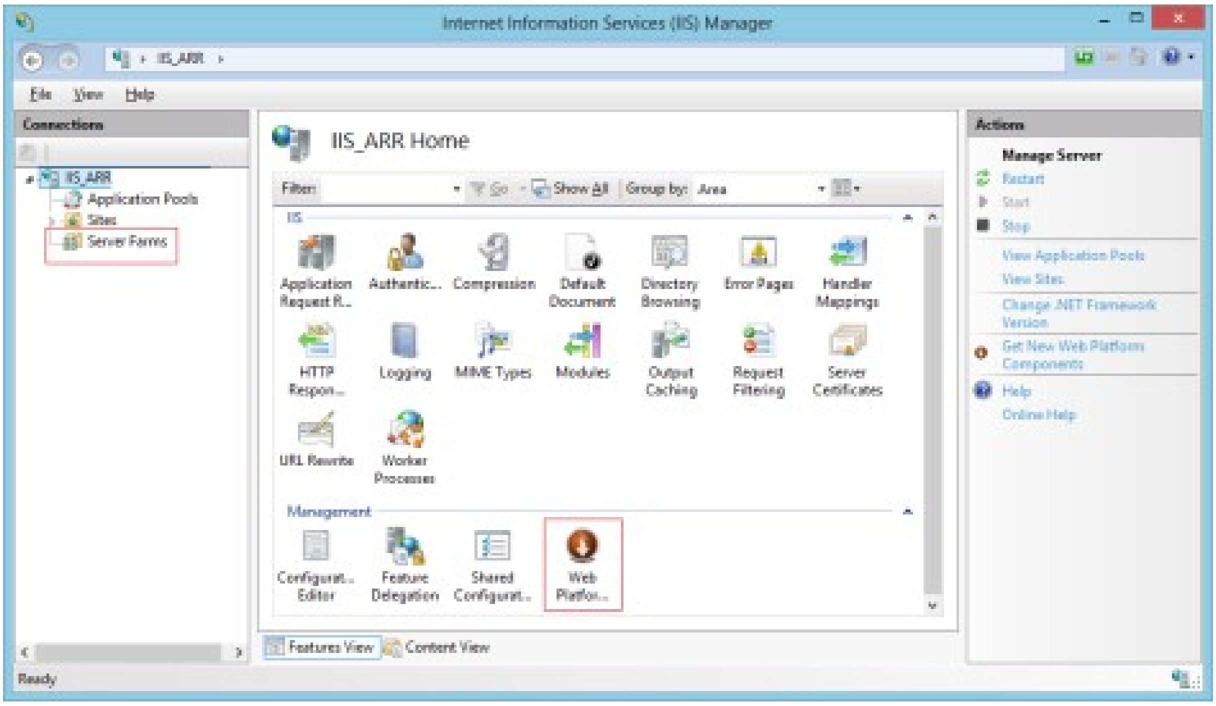
For a summary of the configuration process, see the internet article:

http://www.ucguys.com/2014/08/using-iis-arr-30-on-windows-server-2012r2-as-a-reverse-proxy-for-lync-server-2013.html.

After configuration, open the IIS Manager; you'll see you have two new ARR features:

- 'Server Farms' under the server node
- 'Web Platform Installer' in the management node

Figure 16-4: IIS Manager



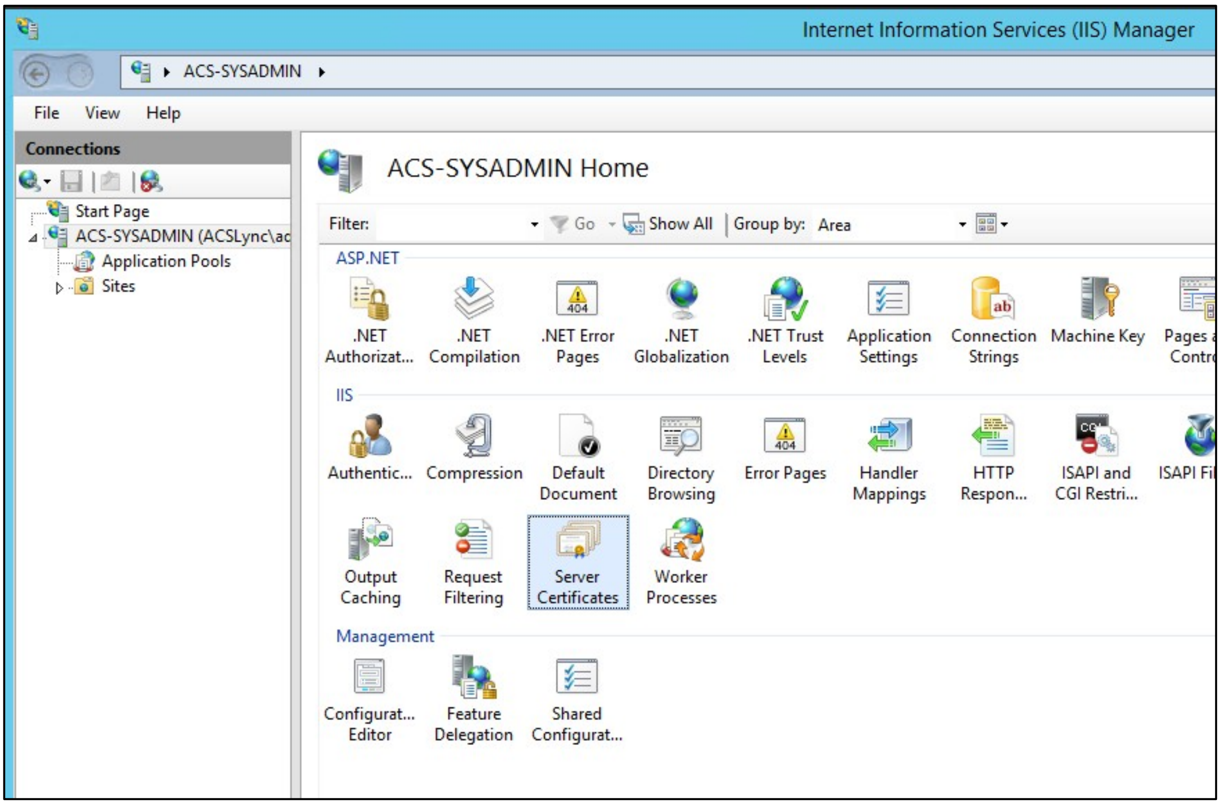
16.5.1 Importing Skype for Business FE External Certificate

This section shows how to import Skype for Business FE External Certificate.

➢ **To import a Skype for Business FE External Certificate:**

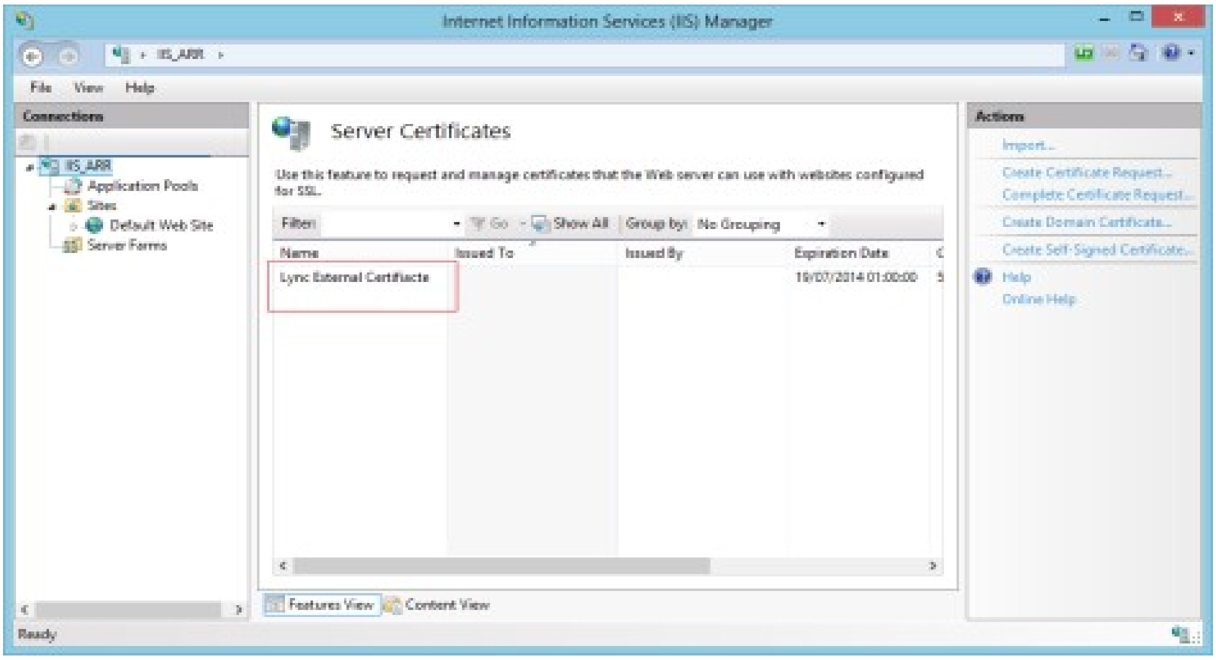
1. Open the IIS Manager.
2. Select the server located uppermost left in the navigation panel.
3. Double-click **Server Certificates** in the middle panel.

Figure 16-5: IIS Certificates



4. Click **Import** in the upper right panel.

Figure 16-6: Import FE External Certificate



Server Certificates

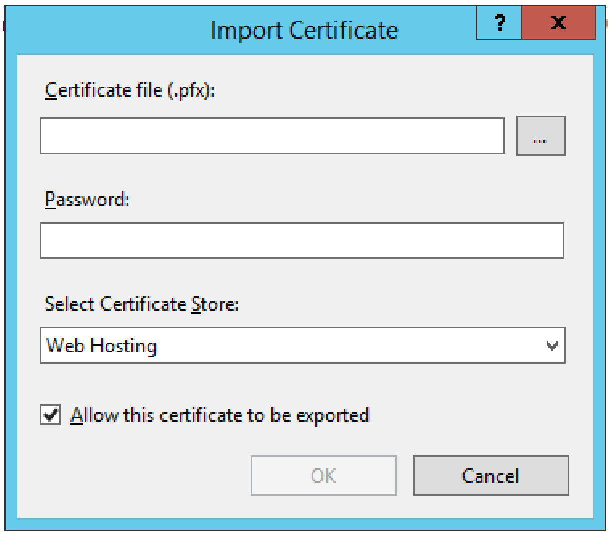
Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Group by: No Grouping

Name	Issued To	Issued By	Expiration Date
Lync External Certifiacte			19/07/2014 01:00:00

5. Supply the details to import your Skype for Business FE External Certificate.

Figure 16-7: Import FE External Certificate



Certificate file (.pfx):

Password:

Select Certificate Store: Web Hosting

☑ Allow this certificate to be exported

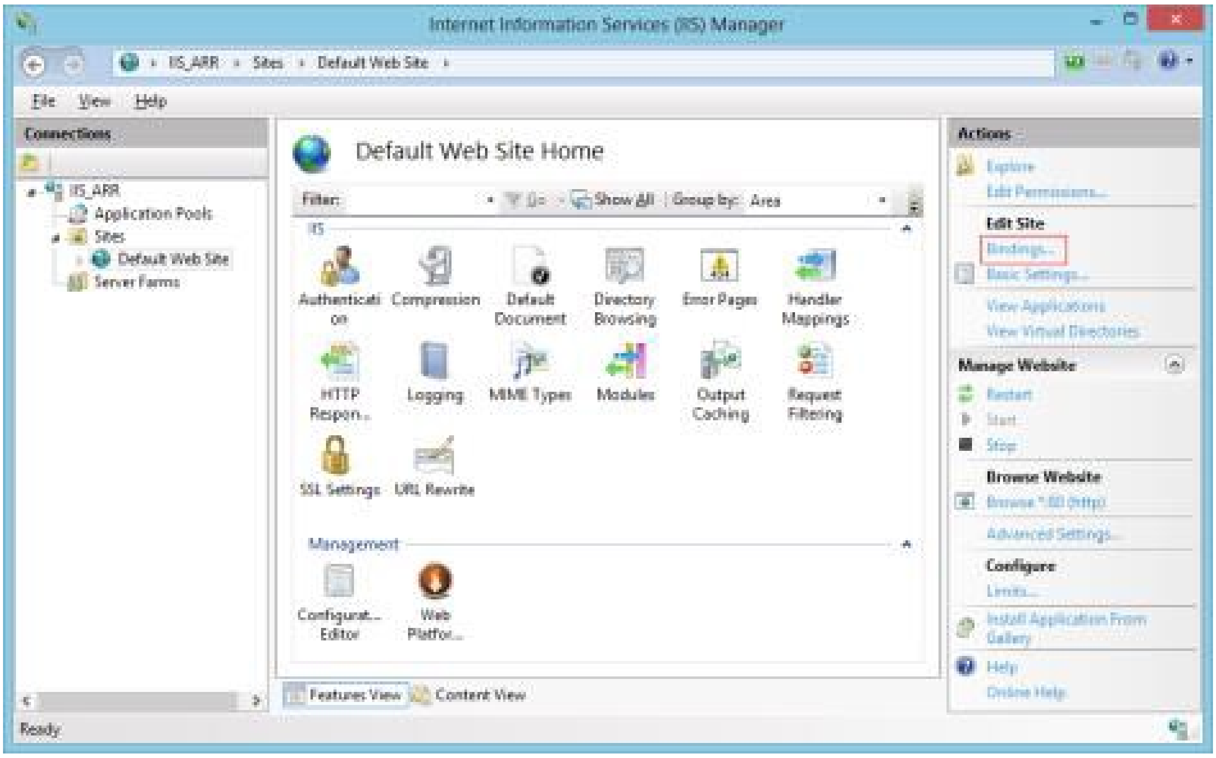
16.5.2 Configuring the Website

This section shows how to configure the website.

➢ **To configure the website.**

1. Navigate to your default website in the IIS Manager and click **Bindings**:

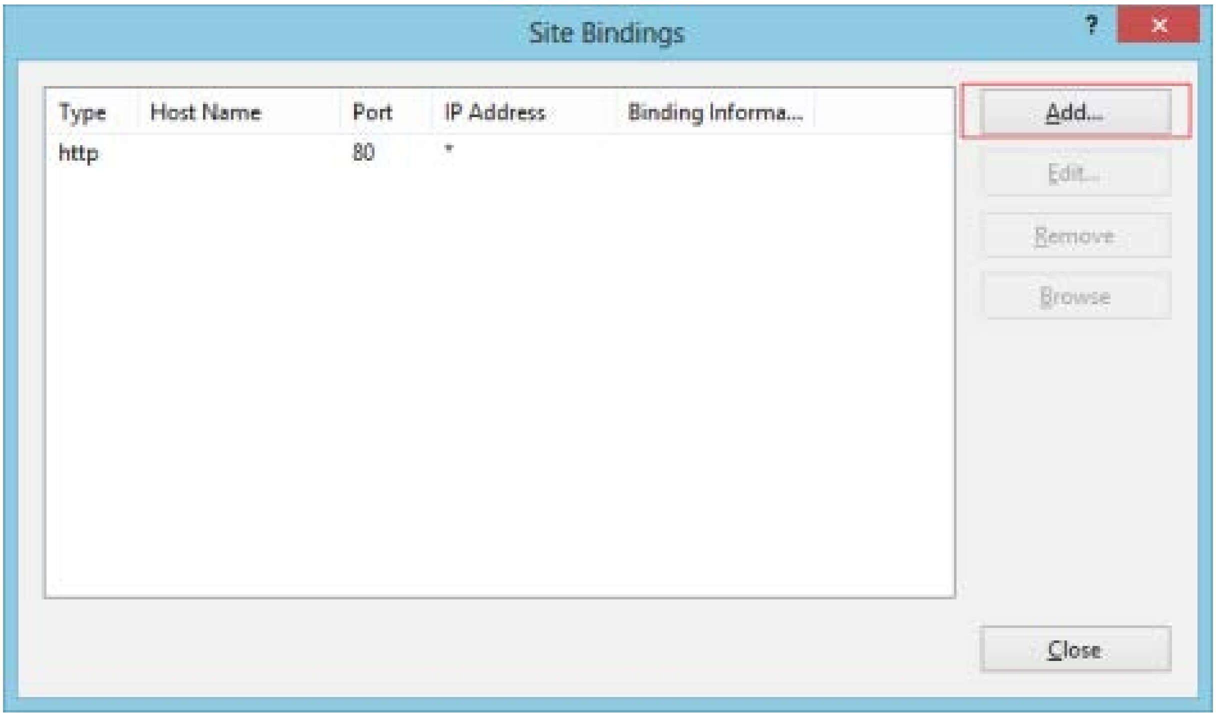
Figure 16-8: Default Web Site - Bindings



You'll see it has only the HTTP binding.

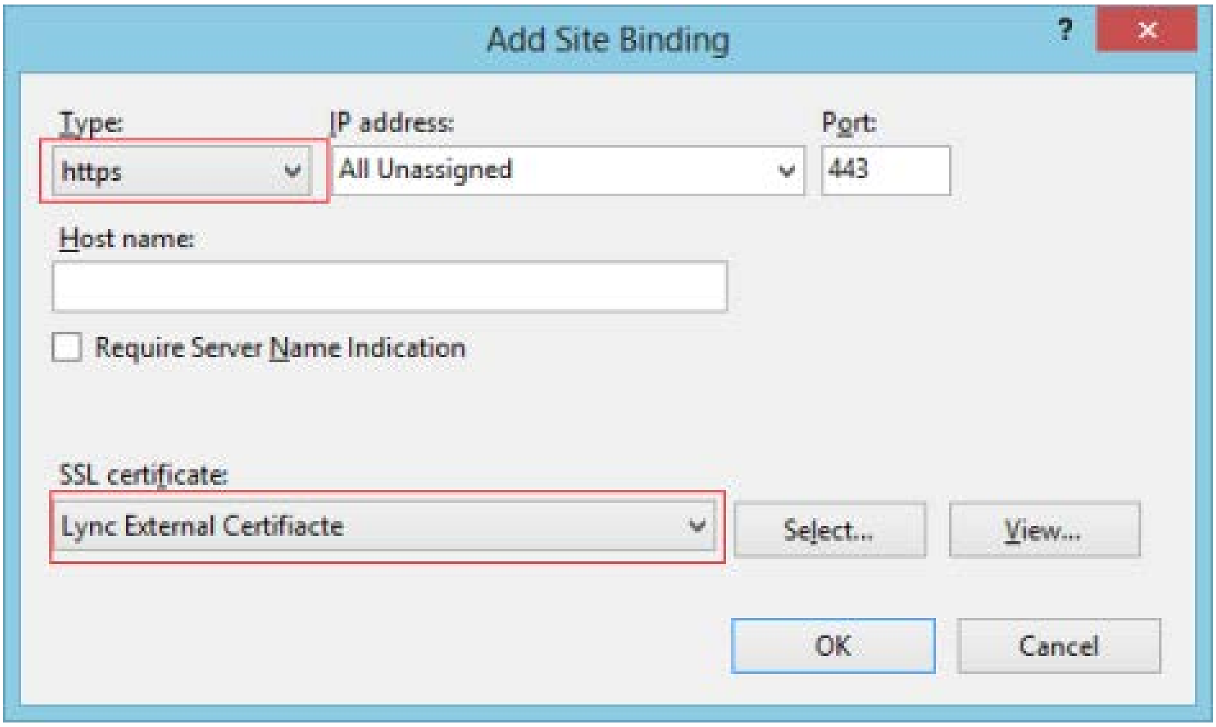
2. Click **Add** to edit the HTTPS binding:

Figure 16-9: Add HTTPS Binding



3. In the next window, choose **HTTPS** from the dropdown, then choose your Skype for Business external certificate, and press **OK**.

Figure 16-10: Configure HTTPS Binding



Add Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

□ Require Server Name Indication

SSL certificate: Lync External Certifiacte

This completes the configuration of the website.

16.5.3 Creating Server Farms

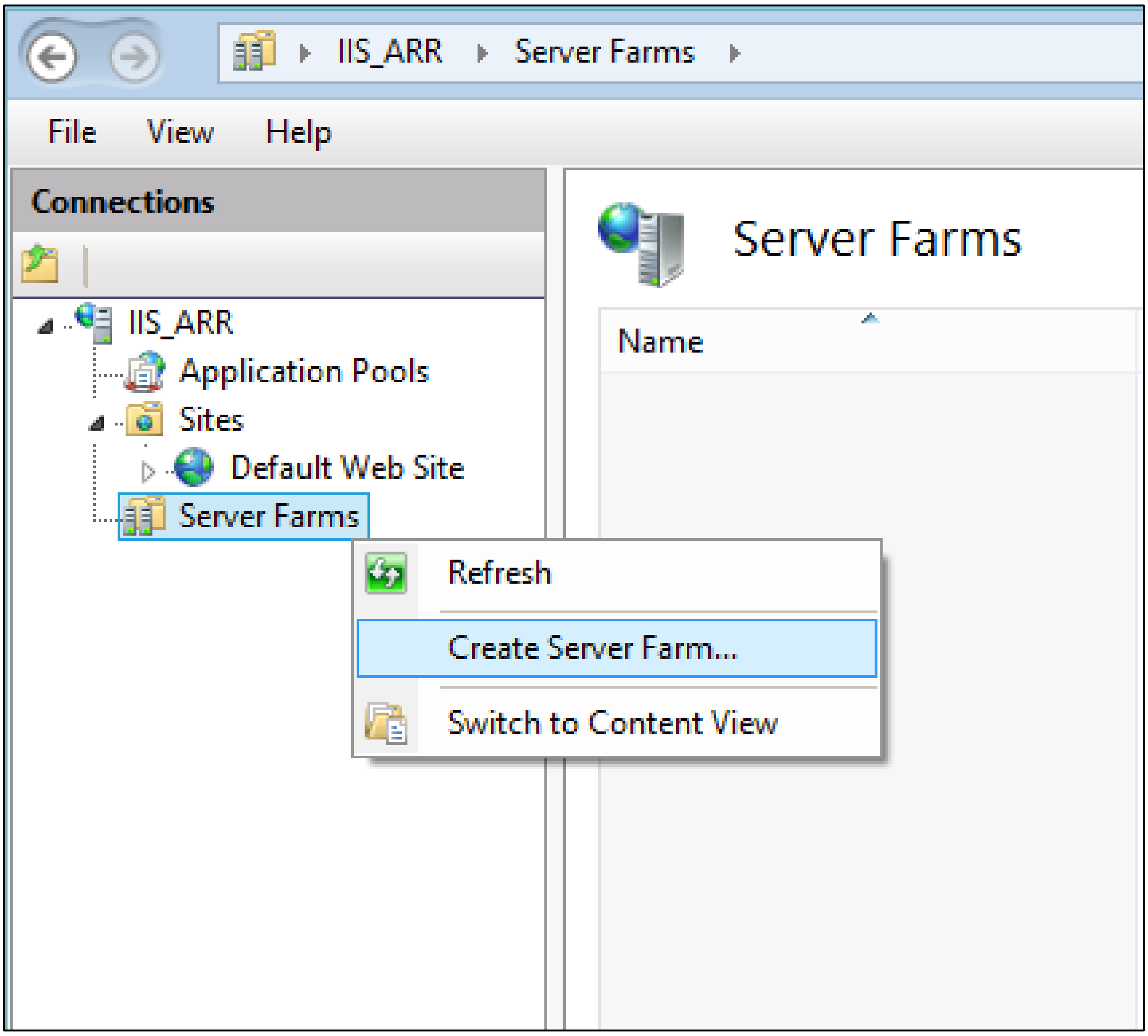
Follow these guidelines on how to create server farms:

- A server farm must be created for each name to be published.
- The Internal root CA (the one used for signing the internal Skype for Business certificates) must be placed in the 'Trusted Root Certification Authorities' container in your IIS-ARR machine.
- The Internal names of your Skype for Business servers and WAC servers must be resolvable from this server, so remember to add them to your hosts file.

➢ **To build the first Server Farm:**

1. Right-click **Server Farms** and from the popup menu choose **Create Server Farm**:

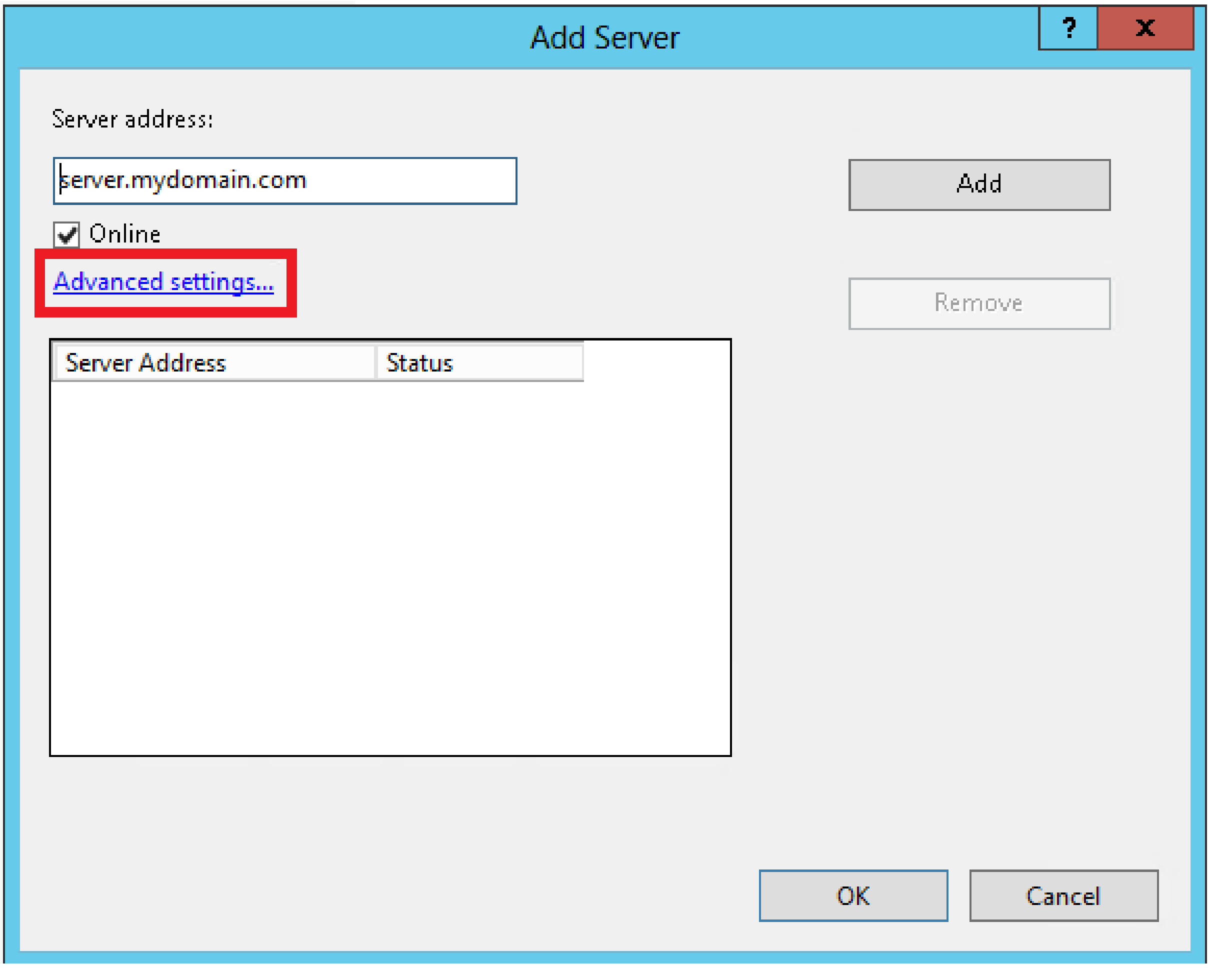
Figure 16-11: Create Server Farm



2. In 'Server Farm Name' field, enter the FQDN of the Skype for Business Server , and then click **Next**.
3. In the Add Server window, enter the name of the server to publish, and then click **Advanced settings…** The server name should be the Skype for Business FE FQDN.

Remember to click **Advanced settings…** *before* you click **Add**. You need to add the server to the farm only after you set the advanced settings for the server.

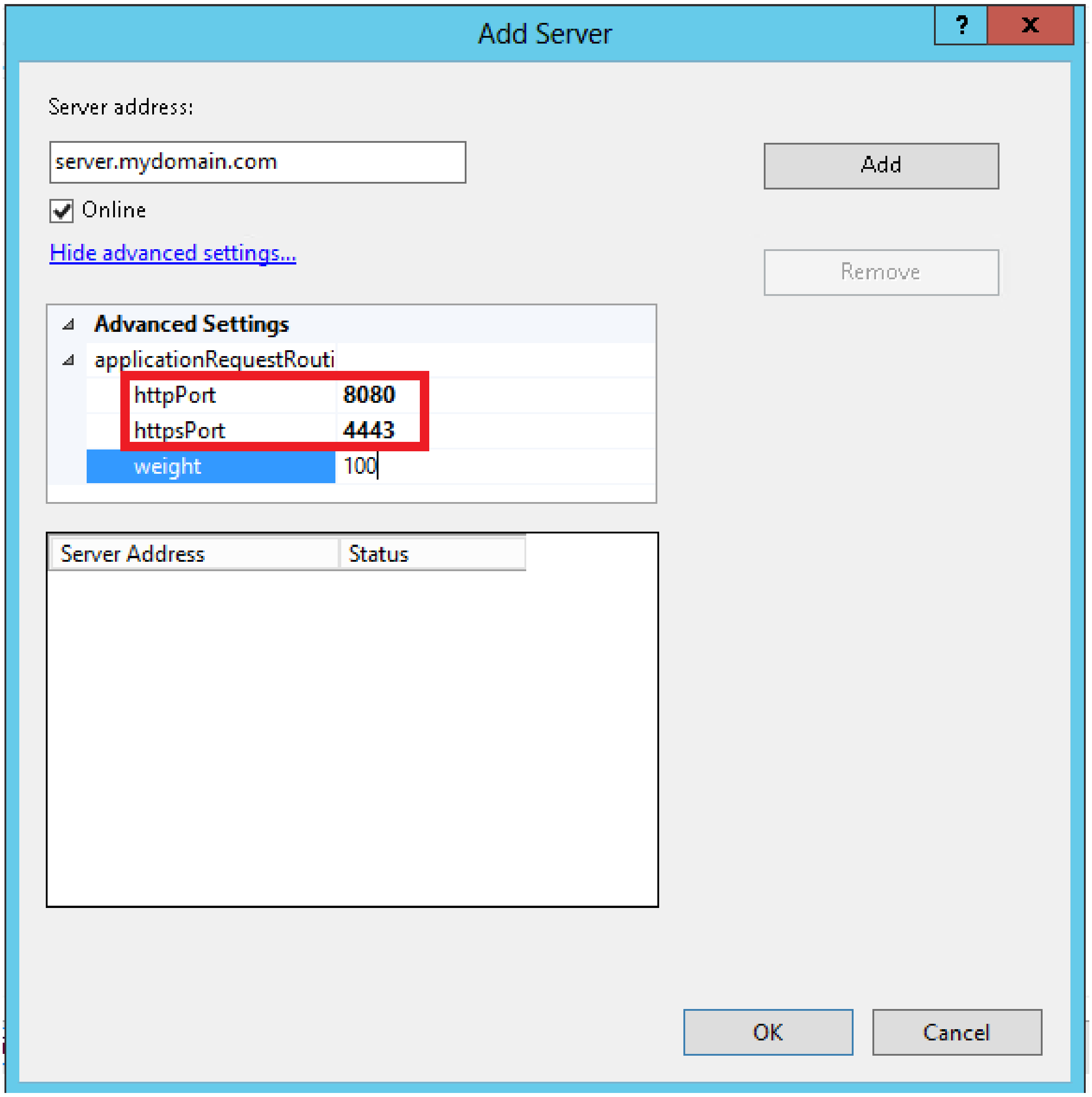
Figure 16-12: Add Server to Farm



Advanced settings… is where the port bridging rules from 443 to 4443 are set.

4. Set the HTTP port to 8080 and the HTTPS port to 4443, then click **Add**; the screen shown in Figure 16-13 opens.

Figure 16-13: Advanced Settings



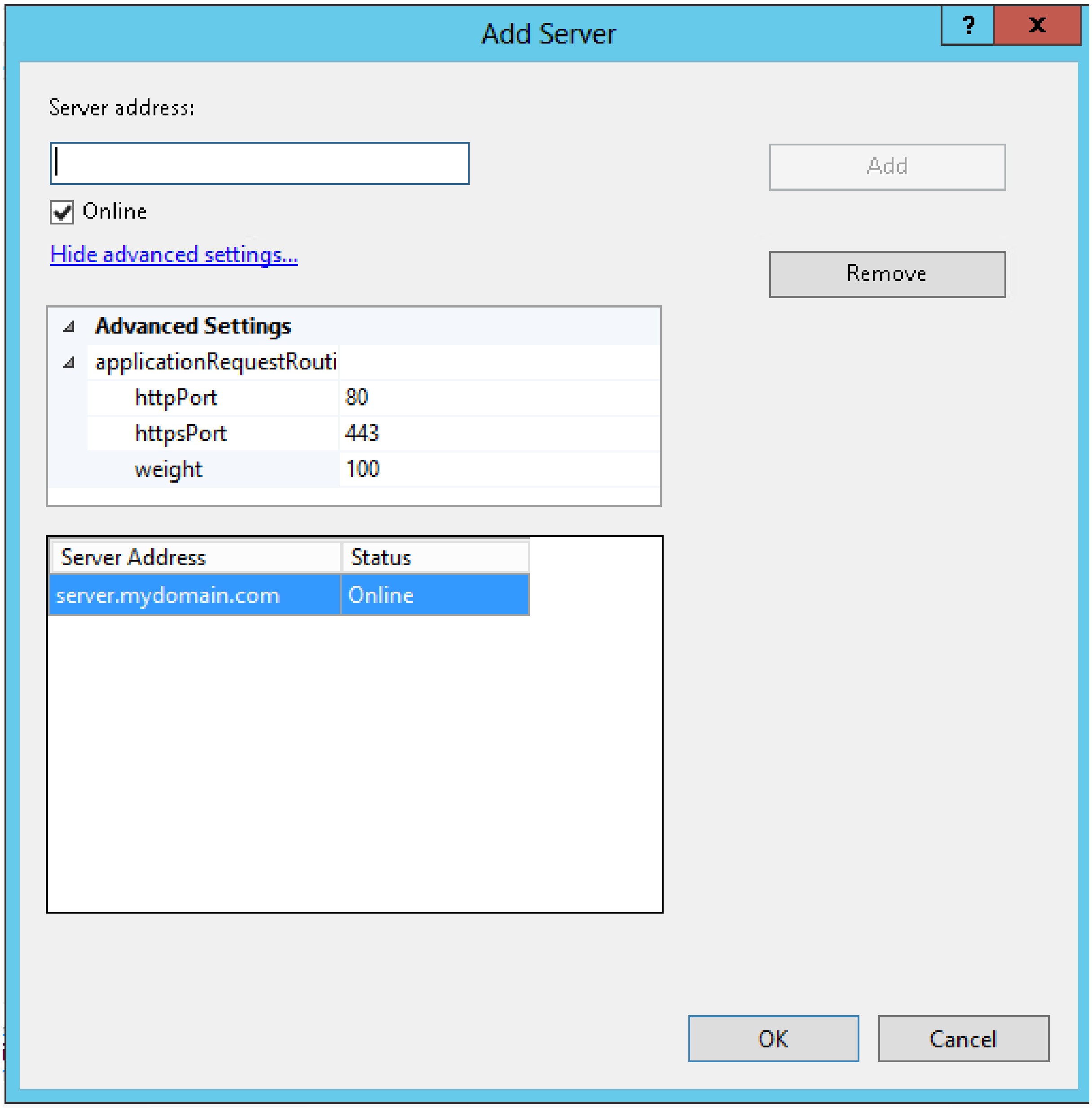
Server address: server.mydomain.com

☑ Online

applicationRequestRouti	
httpPort	8080
httpsPort	4443
weight	100

5. View the server in the server farm:

Figure 16-14: Viewing the Server in the Server Farm



Server address:

☑ Online

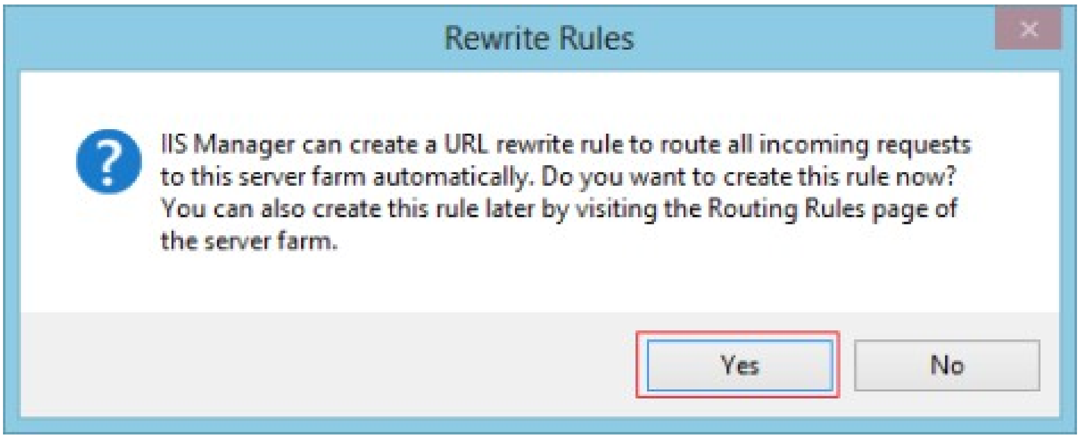
Advanced Settings

applicationRequestRouti	
httpPort	80
httpsPort	443
weight	100

Server Address	Status
server.mydomain.com	Online

6. After clicking **OK**, you'll be prompted to create a URL rewrite rule:

Figure 16-15: URL Rewrite Rule Prompt



IIS Manager can create a URL rewrite rule to route all incoming requests to this server farm automatically. Do you want to create this rule now? You can also create this rule later by visiting the Routing Rules page of the server farm.

7. Click **Yes**.

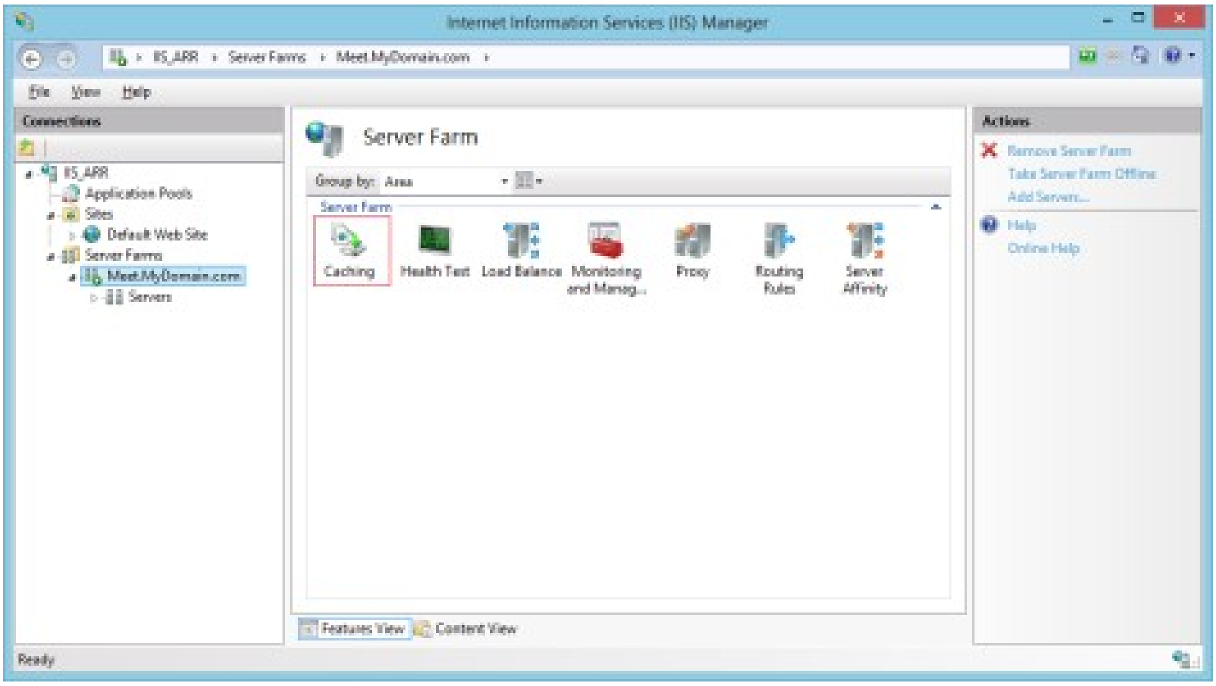
16.5.4 Adjusting Server Farm Settings

A few adjustments need to be made for correct operation with Skype for Business. Perform the steps shown in the sections below.

16.5.4.1 Step 1: Disable Caching

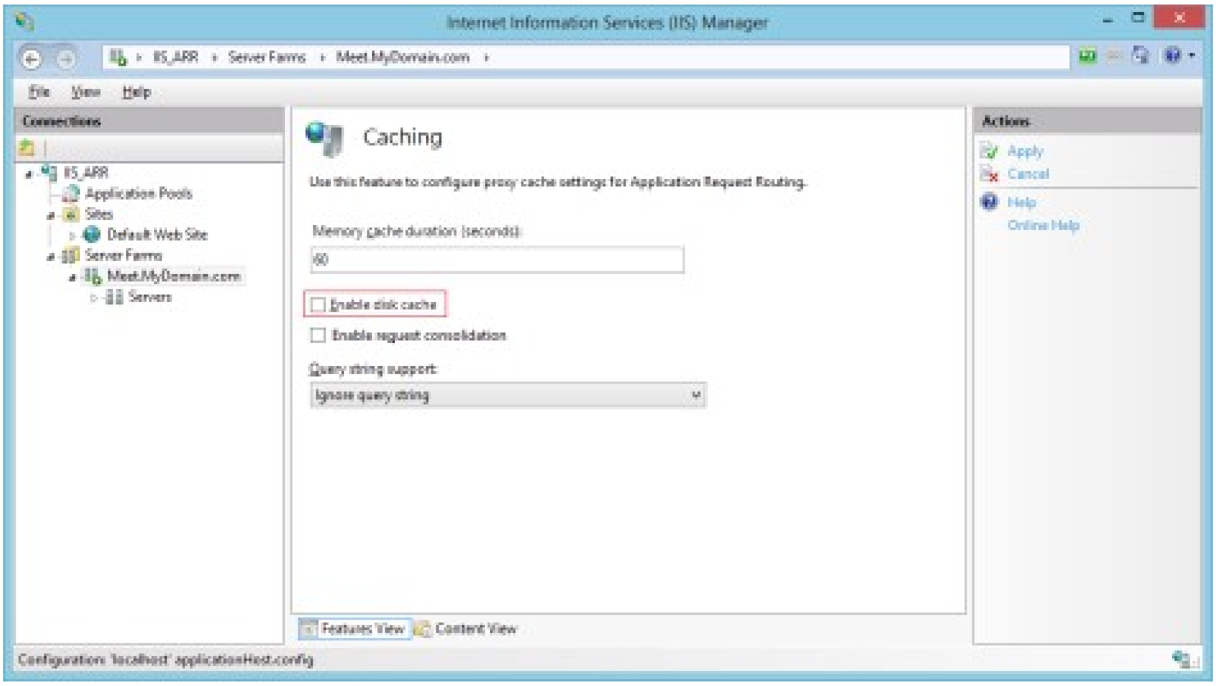
1. Click the server farm and choose **Caching**.

Figure 16-16: Caching



2. In Caching, clear the 'Enable disk cache' option.

Figure 16-17: Disable Caching



Caching

Use this feature to configure proxy cache settings for Application Request Routing.

Memory cache duration (seconds): 60

☐ Enable disk cache

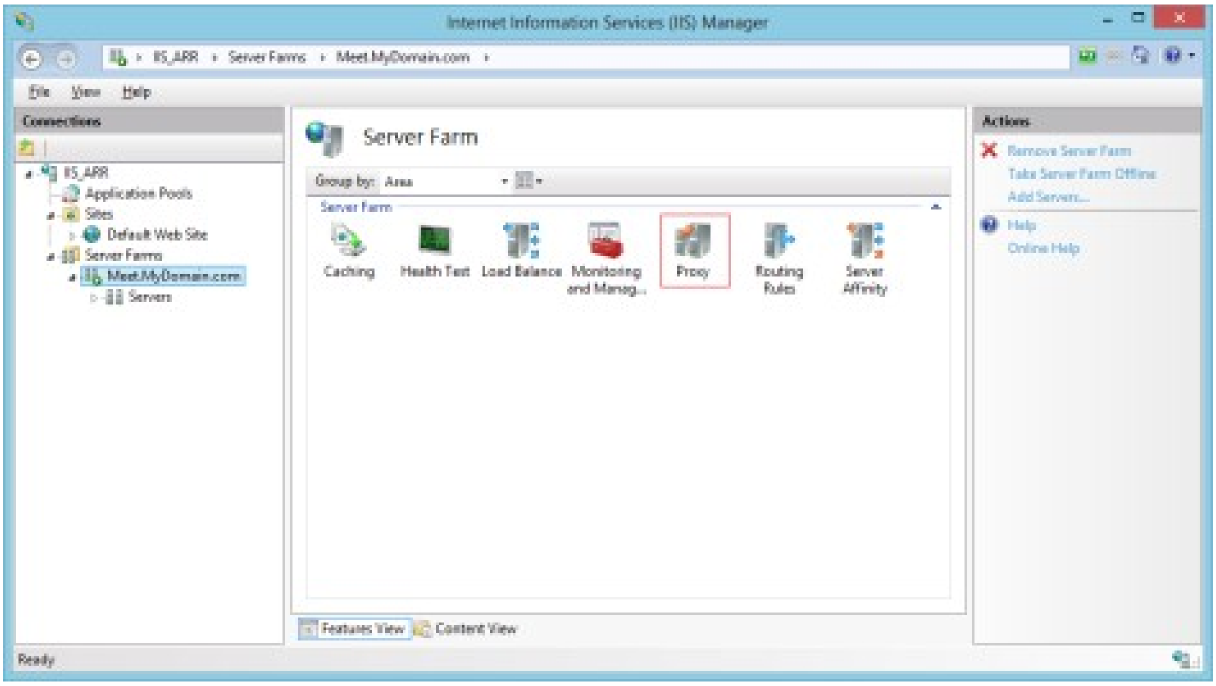
☐ Enable request consolidation

Query string support: Ignore query string

16.5.4.2 Step 2: Change the Proxy Timeout

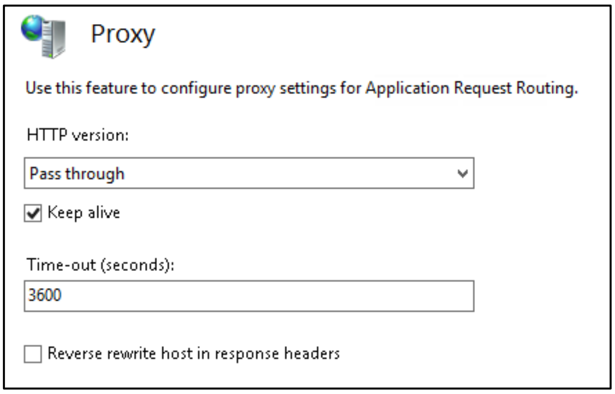
1. Click the server farm and choose **Proxy**.

Figure 16-18: Proxy



2. In the Proxy screen, change the Time-out to **3600**.

Figure 16-19: Proxy Timeout



Proxy

Use this feature to configure proxy settings for Application Request Routing.

HTTP version:

Pass through

☑ Keep alive

Time-out (seconds):

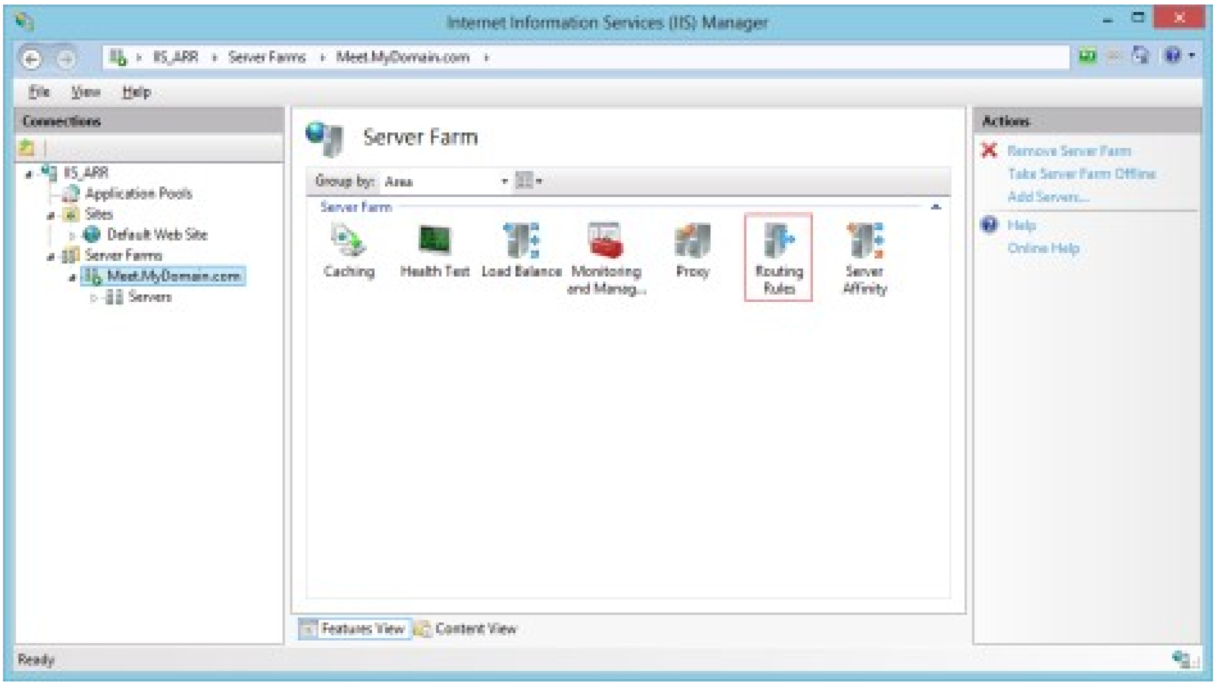
3600

□ Reverse rewrite host in response headers

16.5.4.3 Step 3: Disable SSL Offloading in the Routing Rules

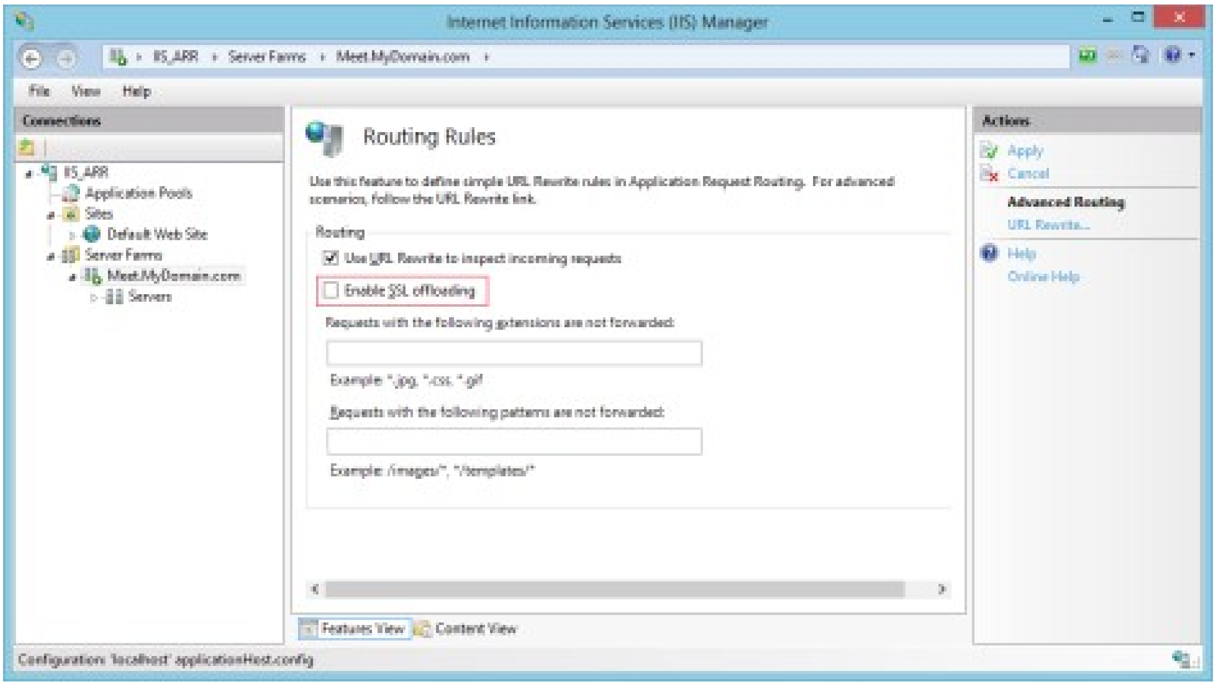
1. Click the server farm and choose **Routing Rules**.

Figure 16-20: Routing Rules



2. In the Routing Rules screen, clear the 'Enable SSL offloading' option.

Figure 16-21: Disable SSL Offloading



Routing Rules

Use this feature to define simple URL Rewrite rules in Application Request Routing. For advanced scenarios, follow the URL Rewrite link.

Routing

☑ Use URL Rewrite to inspect incoming requests

☐ Enable SSL offloading

Requests with the following extensions are not forwarded:

Example: *.jpg, *.css, *.gif

Requests with the following patterns are not forwarded:

Example: /images/*, */templates/*

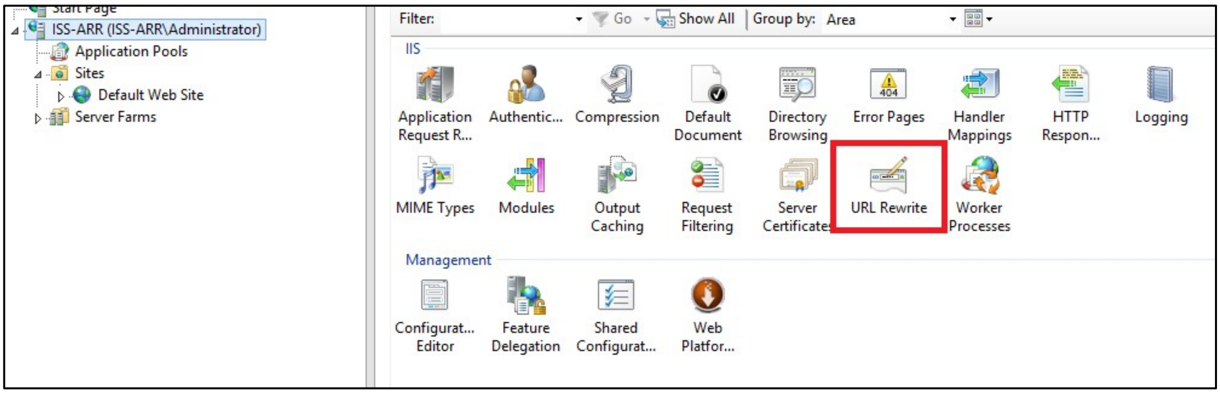
Configuration: 'localhost' applicationHost.config

16.5.5 URL Rewrite

After completing the three Server Farm steps in the previous sections, you must configure rules to rewrite the URLs of incoming requests.

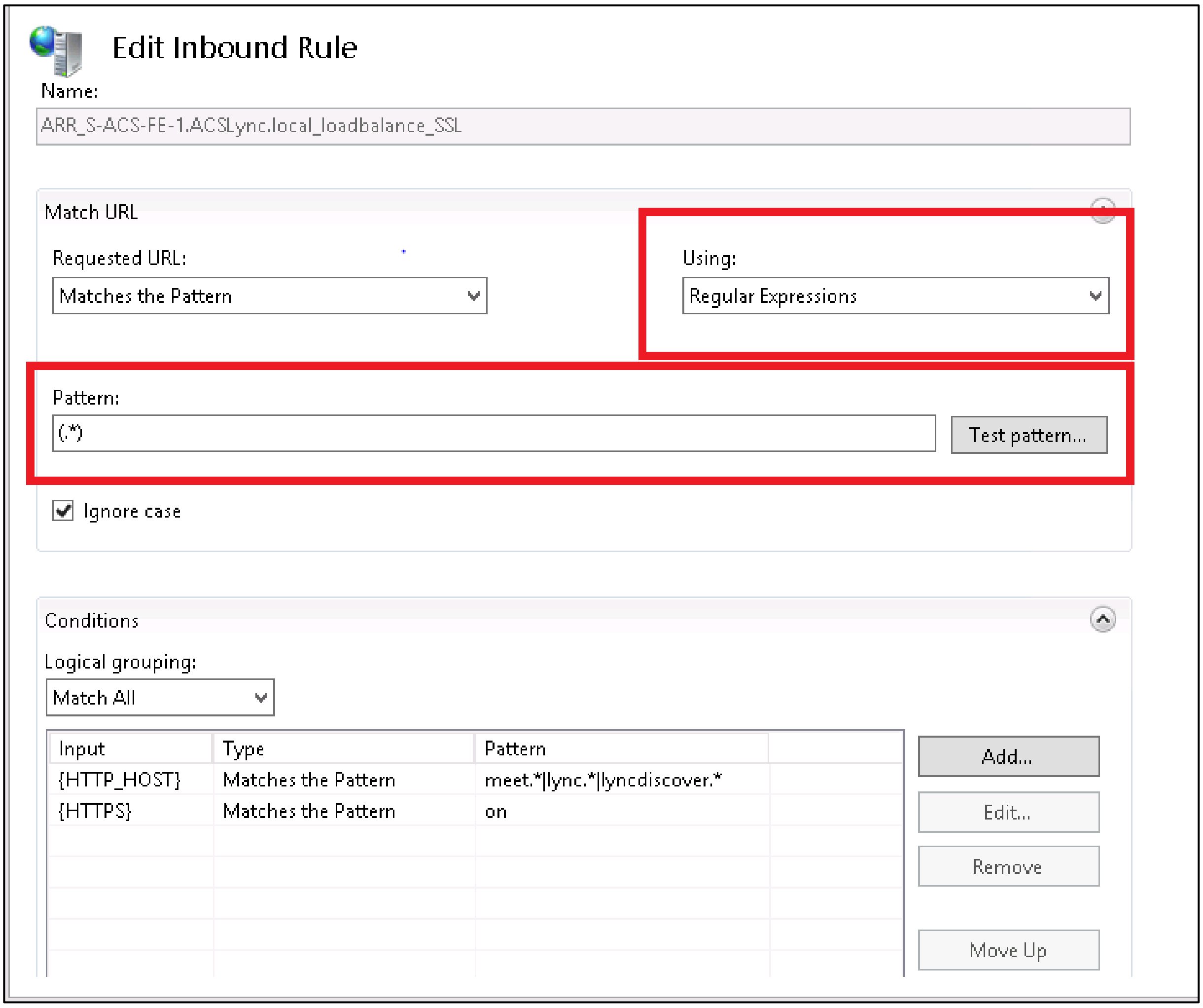
1. Go to the IIS Server Home and click **URL Rewrite**.

Figure 16-22: URL Rewrite



2. The next window shows the server farm with the URL rewrite rules that were created earlier. Click the **+** sign to the left of the server farm to display the existing URL Rewrite options. One is for HTTP, the other for HTTPS.
3. Since HTTP is not used, remove the HTTP rule (the rule *without* the suffix **_SSL**). This leaves only the HTTPS Rewrite rule.
4. Click **Add** to add a condition to the HTTPS rule.
5. Start entering '**{HTTP_**' and choose the {HTTP_HOST} option from the dropdown. In the 'Pattern' field, enter the beginning of the FQDN followed by a star, for example, "Meet.*", lyncdiscover.*"

Figure 16-23: URL Rewrite Rules



Edit Inbound Rule

Name:

ARR_S-ACS-FE-1.ACSLync.local_loadbalance_SSL

Match URL

Requested URL: Matches the Pattern

Using: Regular Expressions

Pattern: (.*)

☑ Ignore case

Conditions

Logical grouping: Match All

Input	Type	Pattern
{HTTP_HOST}	Matches the Pattern	meet.*|lync.*|lyncdiscover.*
{HTTPS}	Matches the Pattern	on

Note: When installed manually on Windows 2008 R2, Windows 2008 R2 does not support multiple Patterns. To resolve this on Windows 2008 R2, create multiple server farms with individual Patterns.

This page is intentionally left blank.

17 Configuring Certificates

This chapter gives 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 Chapter 13.

17.1 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.

17.1.1 Public Key Infrastructure

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

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

17.1.2 What Purpose does Certificates Serve?

Certificates within Microsoft perform two major functions. They allow different computer services to verify they are communicating with the server they intended to communicate with (trust), and they allow that communication to be encrypted with public and private keys if required (privacy).

17.1.3 Trust

Certificate trust works on a third party system. i.e. The two communicating computers may not trust each other directly, but they must ultimately trust a 3rd 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 that server by its name, and for security, will request 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 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.

17.1.3.1 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.

N.B. The subject field will be depreciated in future, and no longer used.

17.1.3.2 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, but may introduce complexities with Federation and other external access. They are generally not suitable for CloudBond 365 deployments with multiple SIP domains.

17.1.4 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.

17.1.5 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 3rd 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.

17.1.5.1 Where to Obtain Certificates?

Certificates can be obtained from private corporate Certificate Authorities (free, but 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.

17.1.5.2 How to Obtain a Certificate?

The exact process for obtaining a certificate varies from vendor to vendor. Please 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.

17.2 CloudBond 365 Default Certificates

17.2.1 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 will be required for most external connections to CloudBond 365.

17.2.2 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 Chapter 13.

17.3 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.

More commonly, a single Public certificate will be used for the External roles, whilst a single or multiple private certificate(s) will be used for the internal roles.

More information on Certificate requirements can be found in Chapter 17.11 on page 350.

17.3.1 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.

17.4 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.

17.4.1 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.

17.4.2 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.

17.4.2.1 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 13.

An 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.

e.g.

- 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)

17.4.2.2 Minimize the Variations in Simple URLs

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

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

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

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

Skype for Business allows 3 main methods of configuring Simple URL's, which have varying economies on DNS entries and SSL Certificate SAN's.
See http://technet.microsoft.com/en-us/library/gg398287.aspx for details.

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

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

As a quick summary:

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

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

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

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

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

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

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

17.4.2.3 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.

17.4.2.4 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.

17.4.2.5 What About LyncDiscover?

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

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

However…

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

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

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

For further information, see:

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

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

17.4.2.6 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.

17.4.2.7 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:

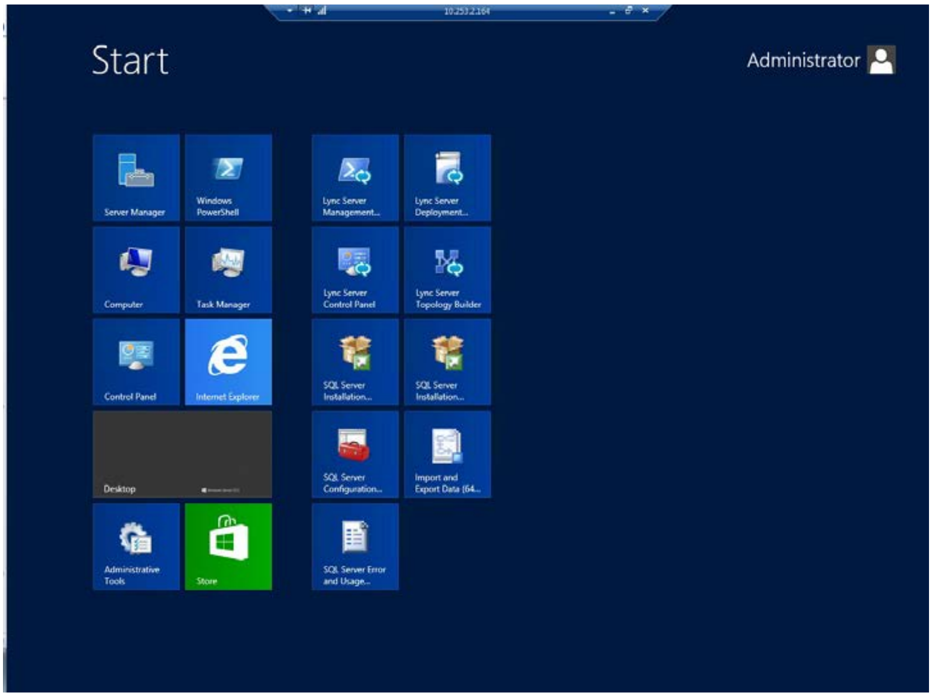
- Mobile client access is configured for secured connections
- Certificate is to be used internally
- PIC Integration is to be configured

17.5 Verify the Topology

17.5.1 Using the Topology Builder

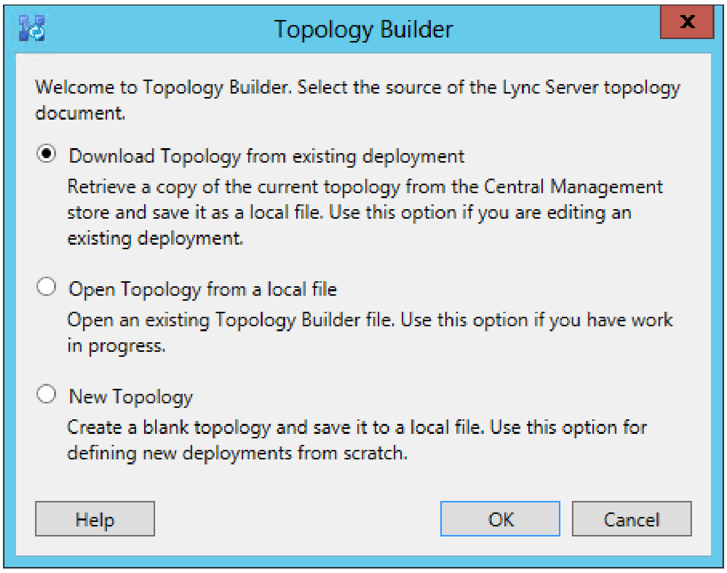
1. Open topology builder.

Figure 17-1: Topology builder is available on the CloudBond 365-Controller


10.253.2.164
Start
Administrator
Server Manager
Windows PowerShell
Lync Server Management...
Lync Server Deployment...
Computer
Task Manager
Lync Server Control Panel
Lync Server Topology Builder
Control Panel
Internet Explorer
SQL Server Installation...
SQL Server Installation...
Desktop
SQL Server Configuration...
Import and Export Data (64...
Administrative Tools
Store
SQL Server Error and Usage...

2. Download current topology.

Figure 17-2: Source of the Topology



Topology Builder

Welcome to Topology Builder. Select the source of the Lync Server topology document.

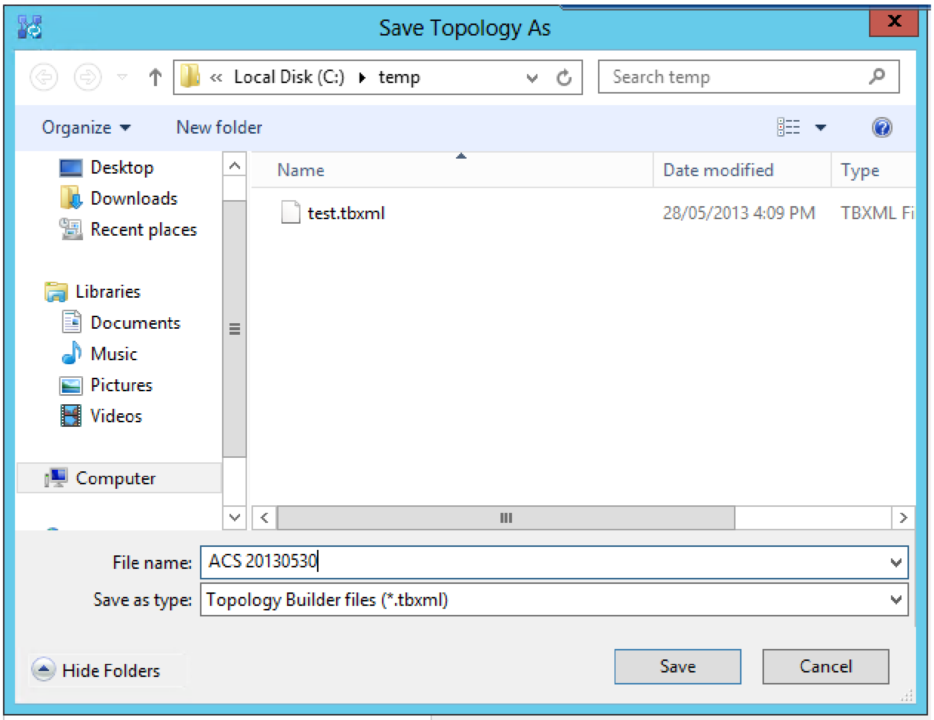
● Download Topology from existing deployment
Retrieve a copy of the current topology from the Central Management store and save it as a local file. Use this option if you are editing an existing deployment.

○ Open Topology from a local file
Open an existing Topology Builder file. Use this option if you have work in progress.

○ New Topology
Create a blank topology and save it to a local file. Use this option for defining new deployments from scratch.

3. Save the topology.

Figure 17-3: Saving the Topology



Save Topology As

« Local Disk (C:) ▸ temp

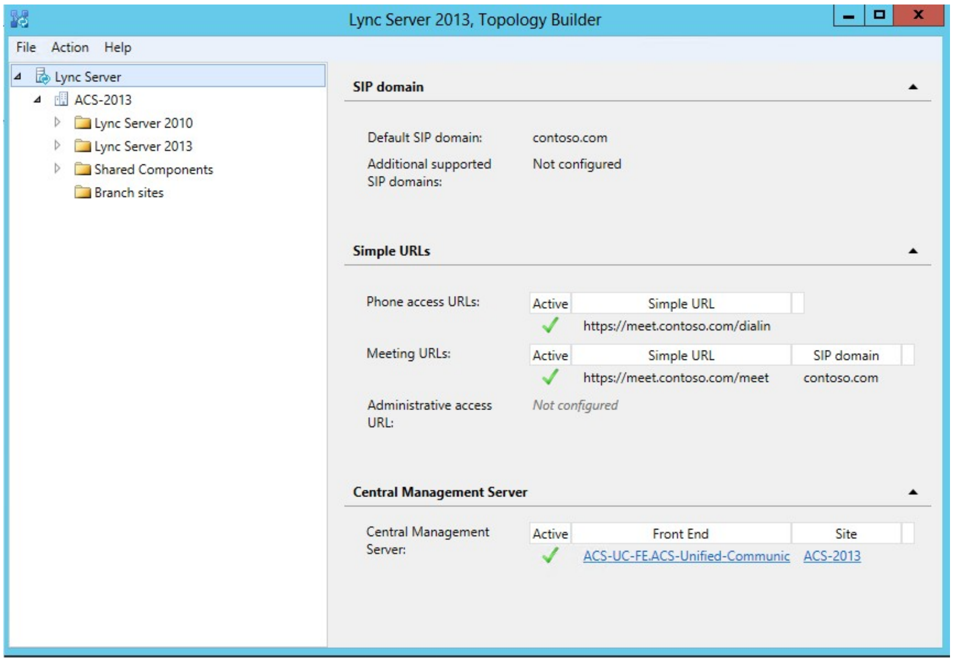
Name	Date modified	Type
test.tbxml	28/05/2013 4:09 PM	TBXML Fi

File name: ACS 20130530

Save as type: Topology Builder files (*.tbxml)

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

Figure 17-4: Topology Builder



SIP domain

Default SIP domain: contoso.com

Additional supported SIP domains: Not configured

Simple URLs

	Active	Simple URL	SIP domain
Phone access URLs:	✓	https://meet.contoso.com/dialin	
Meeting URLs:	✓	https://meet.contoso.com/meet	contoso.com

Administrative access URL: *Not configured*

Central Management Server

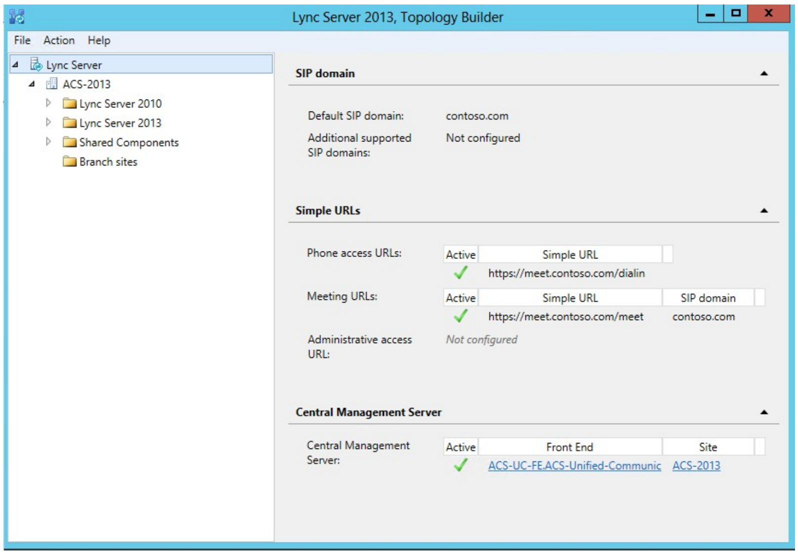
	Active	Front End	Site
Central Management Server:	✓	ACS-UC-FE.ACS-Unified-Communic	ACS-2013

17.5.1.1 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**), and then select **Edit Properties**.

Figure 17-5: Viewing a Topology



SIP domain

Default SIP domain: contoso.com

Additional supported SIP domains: Not configured

Simple URLs

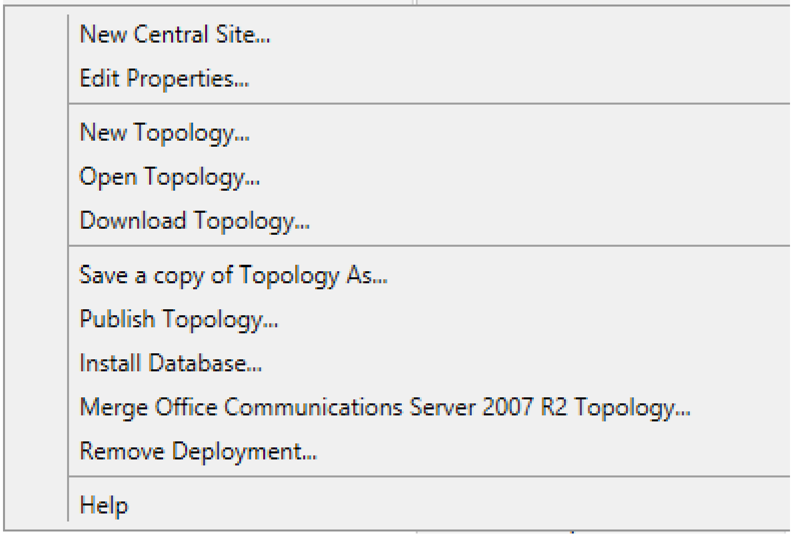
	Active	Simple URL	SIP domain
Phone access URLs:	✓	https://meet.contoso.com/dialin	
Meeting URLs:	✓	https://meet.contoso.com/meet	contoso.com

Administrative access URL: *Not configured*

Central Management Server

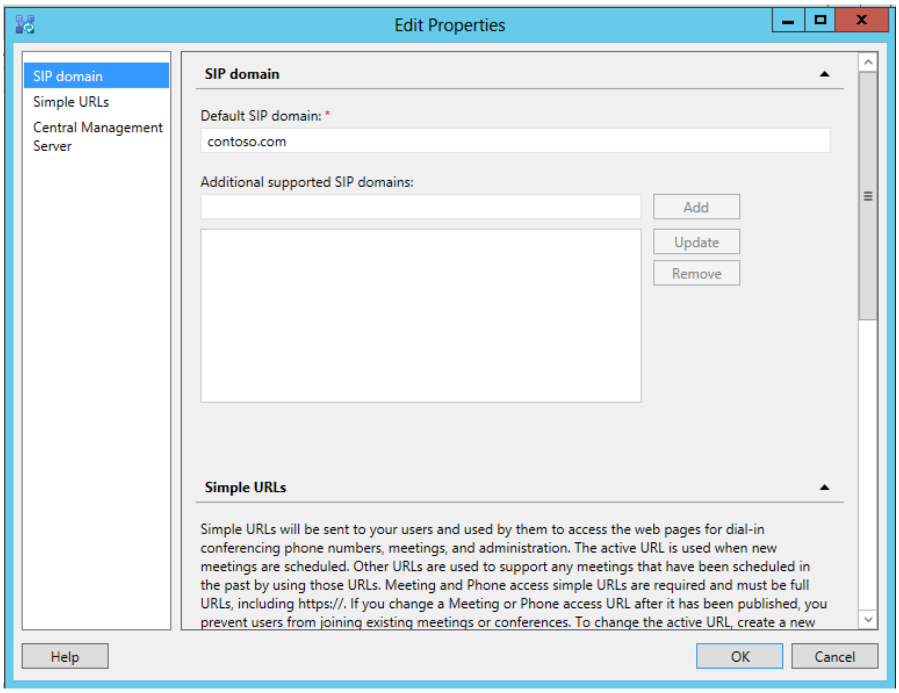
	Active	Front End	Site
Central Management Server:	✓	ACS-UC-FE.ACS-Unified-Communic	ACS-2013

Figure 17-6: Edit Properties of the Server



17.5.1.1.1Add the New SIP Domain to the Topology

Figure 17-7: Additional SIP Domains



SIP domain

Default SIP domain: *

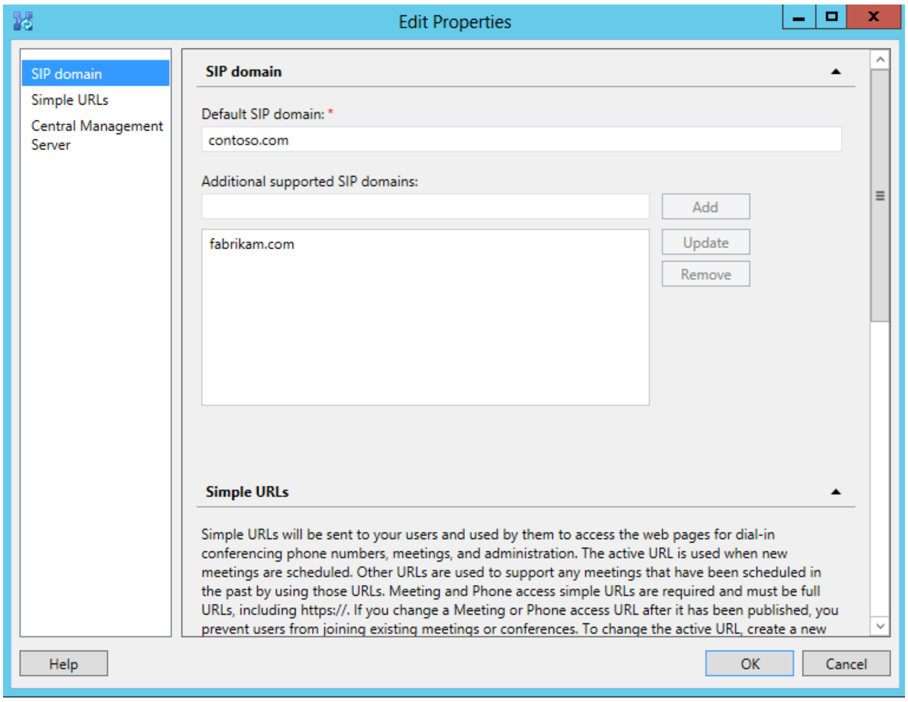
contoso.com

Additional supported SIP domains:

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

Figure 17-8: Adding fabrikam.com as an additional SIP domain



SIP domain

Default SIP domain: * contoso.com

Additional supported SIP domains:

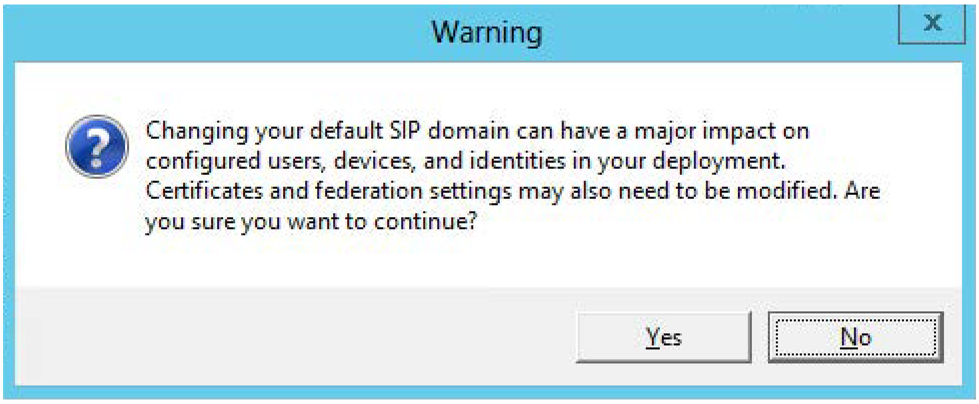
fabrikam.com

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

17.5.1.1.2Changing the Default (Primary) SIP Domain

Figure 17-9: Warning: Changing the Primary SIP Domain is Complex



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. Are you sure you want to continue?

If you change the primary SIP domain, you will be presented with the following pop-up, 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.

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:

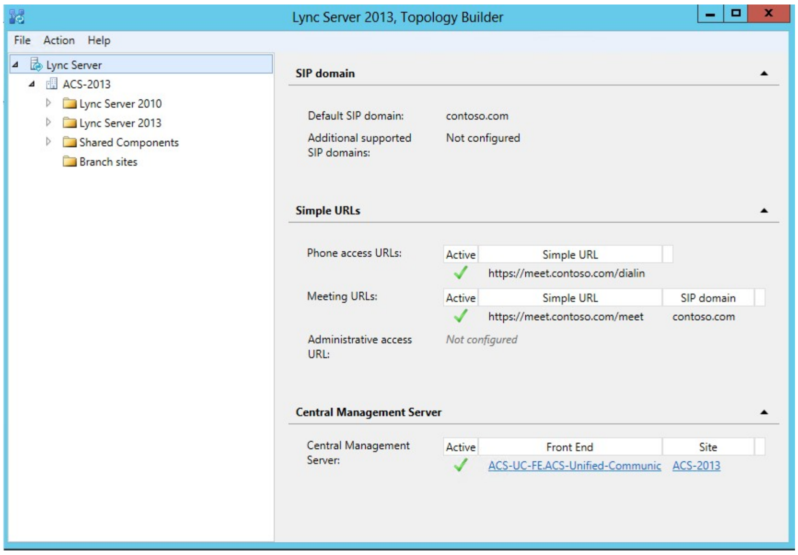
Set-CsSipDomain –Identity fabrikam.com –IsDefault $True

17.5.1.2 Simple URL’s

Simple URL’s are also properties of the whole server Topology.

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

Figure 17-10: Viewing a Topology



SIP domain

Default SIP domain: contoso.com

Additional supported SIP domains: 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*

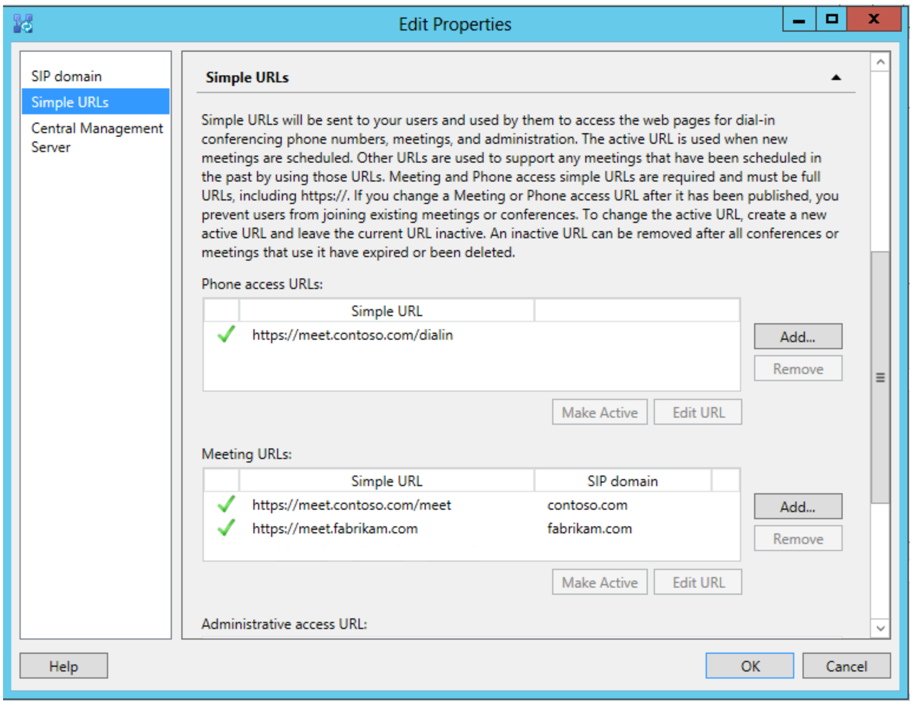
Central Management Server

Central Management Server:

Active	Front End	Site
✓	ACS-UC-FE.ACS-Unified-Communic	ACS-2013

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 17-11: Topology Simple URLs – Using Option 2



Simple URLs

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

Phone access URLs:

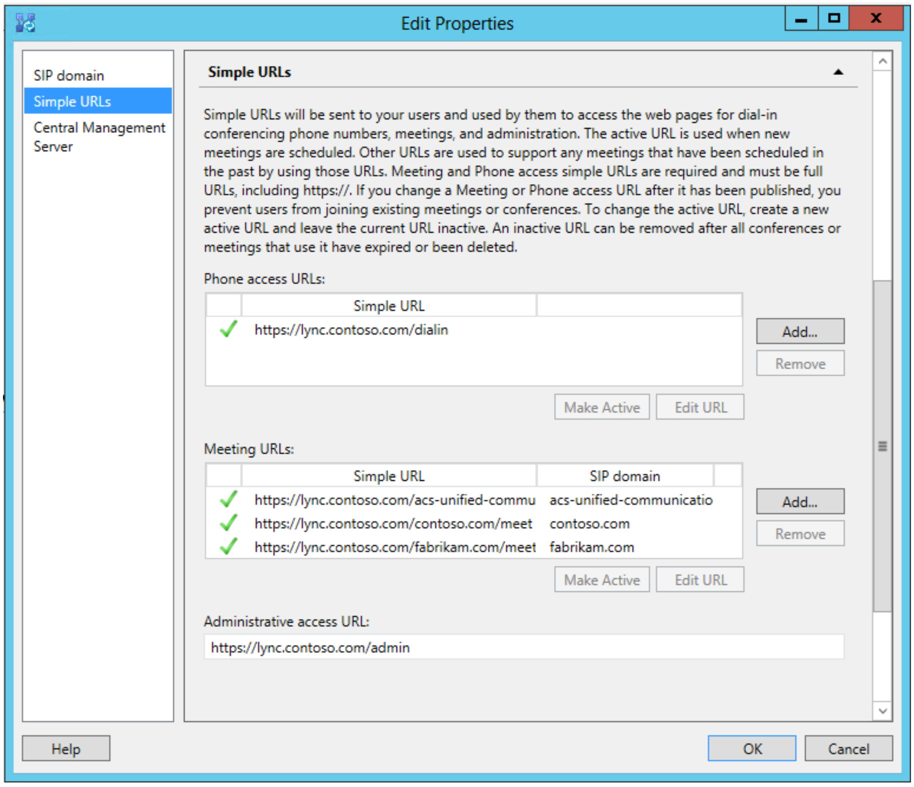
	Simple URL
✓	https://meet.contoso.com/dialin

Meeting URLs:

	Simple URL	SIP domain
✓	https://meet.contoso.com/meet	contoso.com
✓	https://meet.fabrikam.com	fabrikam.com

Administrative access URL:

Figure 17-12: Simple URL's Using Option 3



Simple URLs

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

Phone access URLs:

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

Meeting URLs:

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

Administrative access URL:

https://lync.contoso.com/admin

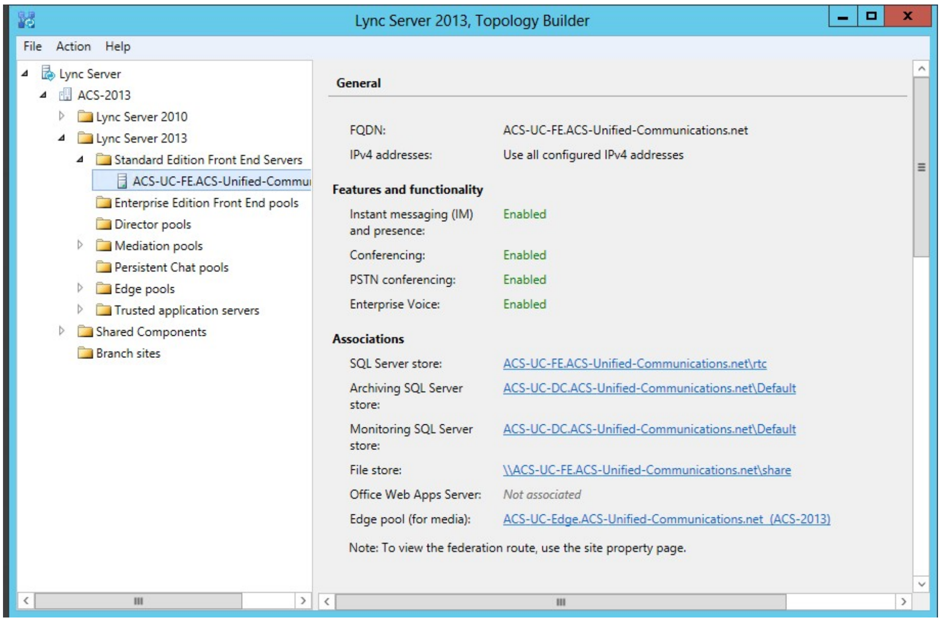
Warning: The Topology builder will check for conflicting URL's. The Simple URL's base component must be unique from that used for External Web Services on the FE Pool, even though they will point to the same server within CLOUDBOND 365.

17.5.1.3 External Web Services

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

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

Figure 17-13: Selecting the Standard Edition Front End Pool



- Lync Server
  - ACS-2013
    - Lync Server 2010
    - Lync Server 2013
      - Standard Edition Front End Servers
        - ACS-UC-FE.ACS-Unified-Commu
      - Enterprise Edition Front End pools
      - Director pools
      - Mediation pools
      - Persistent Chat pools
      - Edge pools
      - Trusted application servers
    - Shared Components
    - Branch sites

General

FQDN: ACS-UC-FE.ACS-Unified-Communications.net

IPv4 addresses: Use all configured IPv4 addresses

Features and functionality

Instant messaging (IM) and presence: Enabled

Conferencing: Enabled

PSTN conferencing: Enabled

Enterprise Voice: Enabled

Associations

SQL Server store: ACS-UC-FE.ACS-Unified-Communications.net\rtc

Archiving SQL Server store: ACS-UC-DC.ACS-Unified-Communications.net\Default

Monitoring SQL Server store: ACS-UC-DC.ACS-Unified-Communications.net\Default

File store: \\ACS-UC-FE.ACS-Unified-Communications.net\share

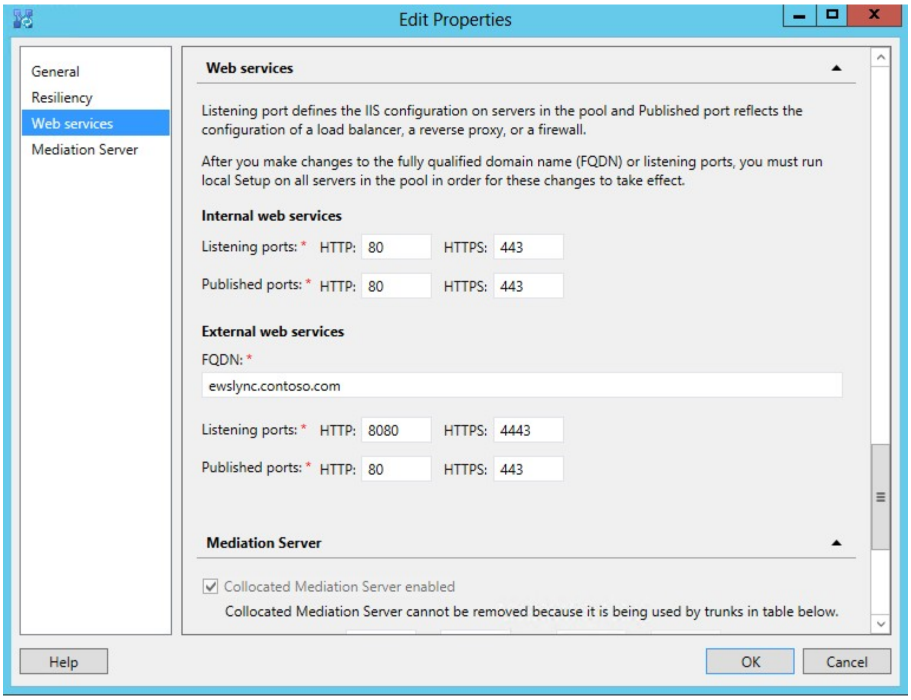
Office Web Apps Server: *Not associated*

Edge pool (for media): ACS-UC-Edge.ACS-Unified-Communications.net (ACS-2013)

Note: To view the federation route, use the site property page.

2. Scroll down, or select Web Services from the left pane.

Figure 17-14: The External Web Services URL must be unique from the Simple URL's



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.contoso.com

Listening ports: * HTTP: 8080 HTTPS: 4443

Published ports: * HTTP: 80 HTTPS: 443

Mediation Server

☑ Collocated Mediation Server enabled

Collocated Mediation Server cannot be removed because it is being used by trunks in table below.

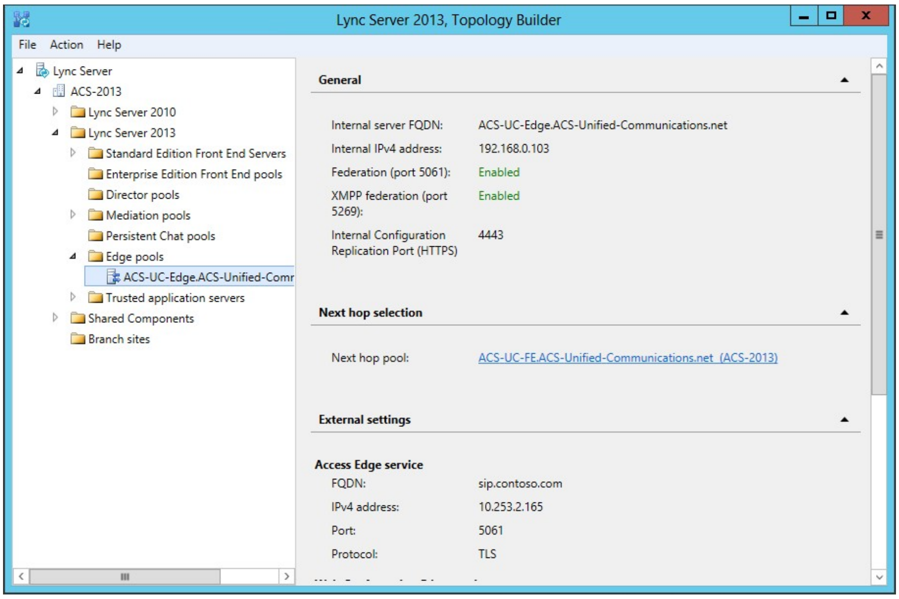
3. Modify the External Web Services FQDN as required. Click **OK**.

17.5.1.4 Edge Services

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

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

Figure 17-15: Selecting the Edge Server from the Edge Pool



- Lync Server
  - ACS-2013
    - Lync Server 2010
    - Lync Server 2013
      - Standard Edition Front End Servers
      - Enterprise Edition Front End pools
      - Director pools
      - Mediation pools
      - Persistent Chat pools
      - Edge pools
        - ACS-UC-Edge.ACS-Unified-Comr
      - Trusted application servers
    - Shared Components
    - Branch sites

General

Internal server FQDN: ACS-UC-Edge.ACS-Unified-Communications.net
Internal IPv4 address: 192.168.0.103
Federation (port 5061): Enabled
XMPP federation (port 5269): Enabled
Internal Configuration Replication Port (HTTPS) 4443

Next hop selection

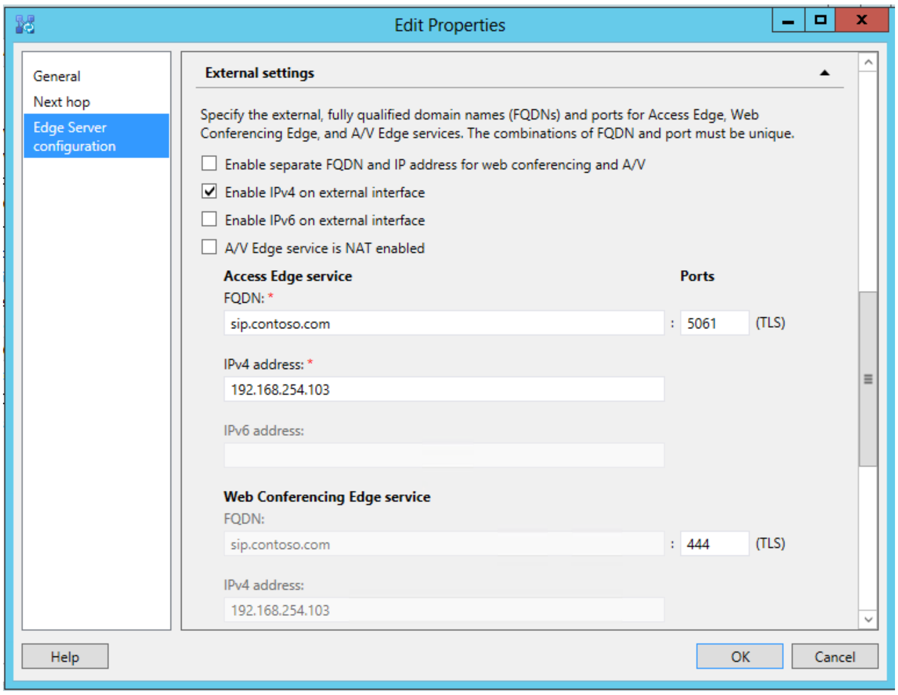
Next hop pool: ACS-UC-FE.ACS-Unified-Communications.net (ACS-2013)

External settings

Access Edge service
FQDN: sip.contoso.com
IPv4 address: 10.253.2.165
Port: 5061
Protocol: TLS

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

Figure 17-16: Edge Sever External Access FQDNs



External settings

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

☐ Enable separate FQDN and IP address for web conferencing and A/V
☑ Enable IPv4 on external interface
☐ Enable IPv6 on external interface
☐ A/V Edge service is NAT enabled

Access Edge service **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

3. Modify the service FQDNs' as required. 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.

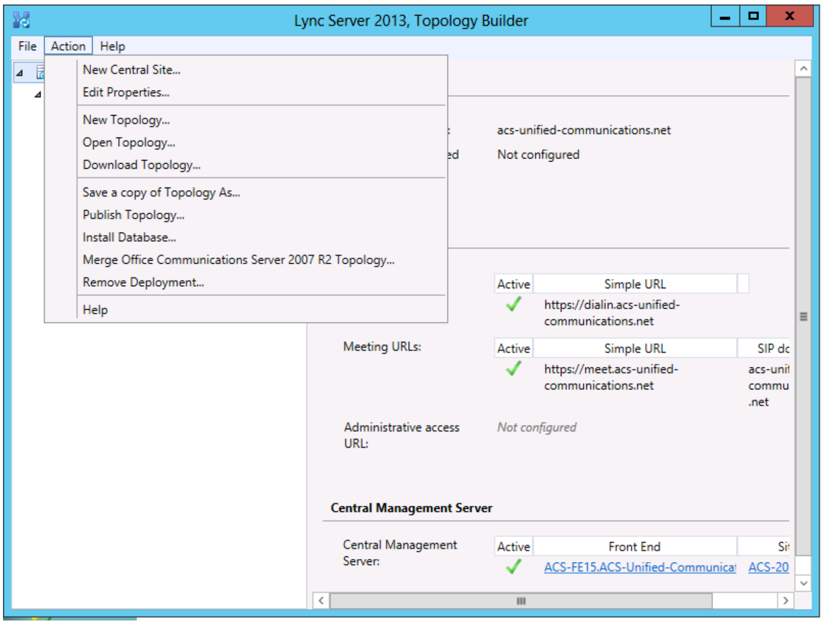
17.5.1.5 Publish Topology and Deploy

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.

17.5.1.5.1 Publish Topology

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

Figure 17-17: Publishing the Topology - Actions



acs-unified-communications.net

Not configured

Active	Simple URL
✓	https://dialin.acs-unified-communications.net

Meeting URLs:

Active	Simple URL	SIP dc
✓	https://meet.acs-unified-communications.net	acs-unif commu .net

Administrative access URL: *Not configured*

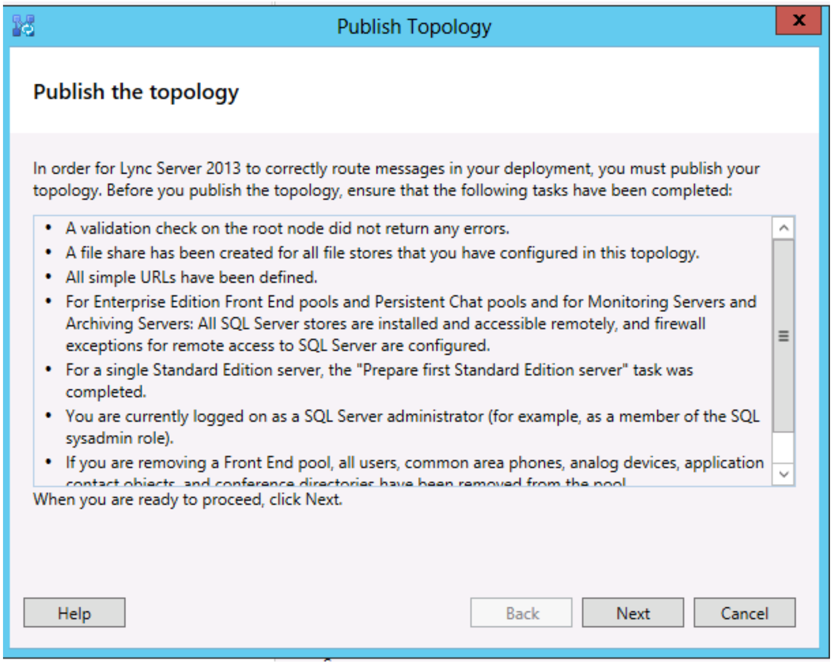
Central Management Server

Central Management Server:

Active	Front End	Si
✓	ACS-FE15.ACS-Unified-Communica	ACS-20

4. Continue the wizard by clicking **Next**, **Next**, and **Finish**:

Figure 17-18: Publishing the Topology



Publish Topology

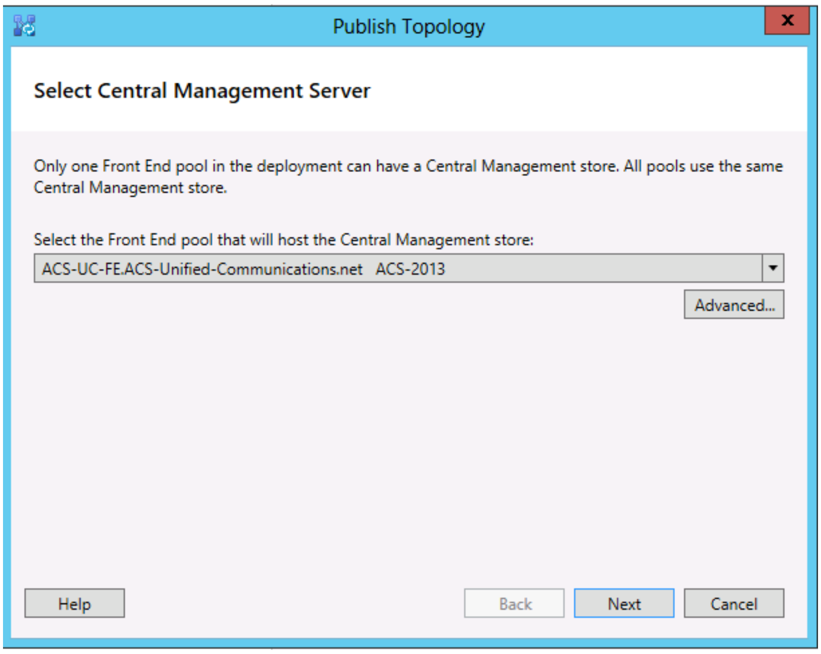
Publish the topology

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:

- A validation check on the root node did not return any errors.
- A file share has been created for all file stores that you have configured in this topology.
- All simple URLs have been defined.
- 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.
- For a single Standard Edition server, the "Prepare first Standard Edition server" task was completed.
- You are currently logged on as a SQL Server administrator (for example, as a member of the SQL sysadmin role).
- 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.

When you are ready to proceed, click Next.

Figure 17-19: Select Central Management Server



Publish Topology

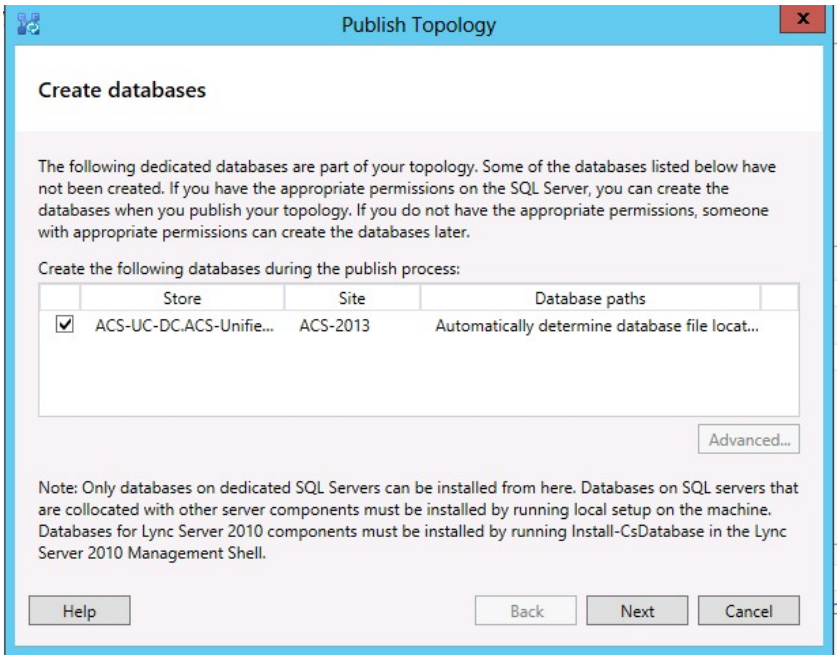
Select Central Management Server

Only one Front End pool in the deployment can have a Central Management store. All pools use the same Central Management store.

Select the Front End pool that will host the Central Management store:

ACS-UC-FE.ACS-Unified-Communications.net ACS-2013

Figure 17-20: Create Databases



Publish Topology

Create databases

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

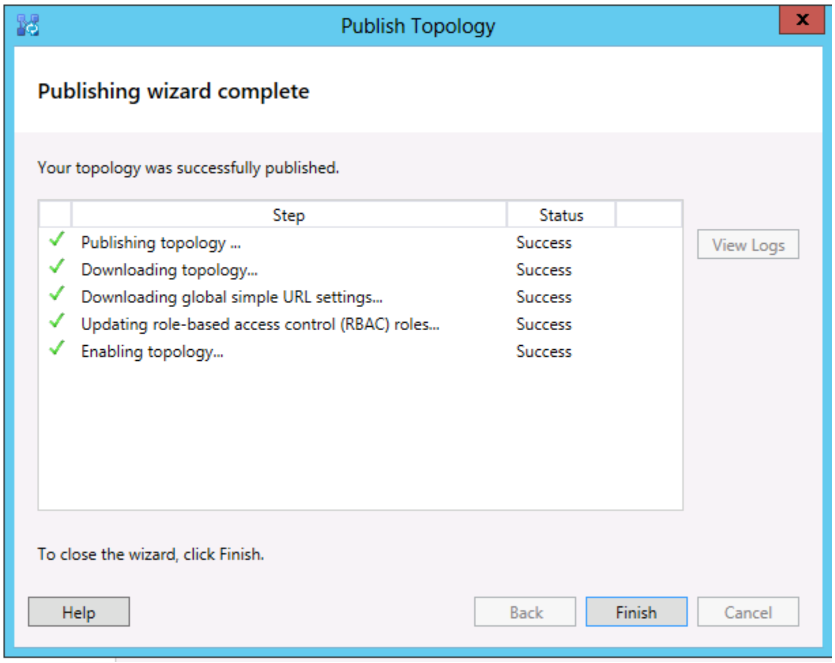
Create the following databases during the publish process:

	Store	Site	Database paths
☑	ACS-UC-DC.ACS-Unifie...	ACS-2013	Automatically determine database file locat...

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

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

Figure 17-21: Publishing the Topology Completes



Publish Topology

Publishing wizard complete

Your topology was successfully published.

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

To close the wizard, click Finish.

17.5.1.5.2 Run 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.

Figure 17-22: Starting the Deployment Wizard

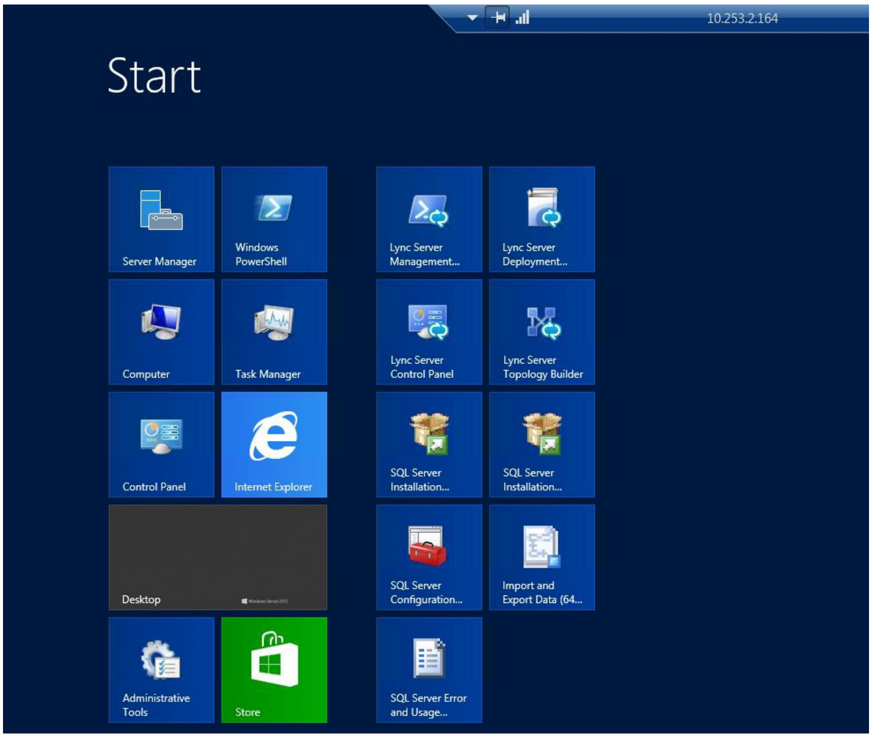
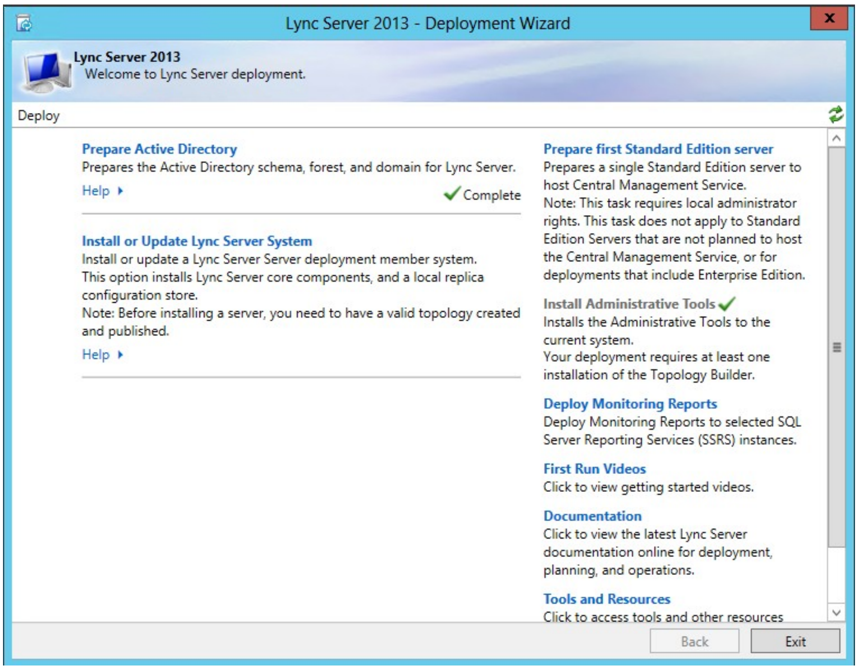

10.253.2.164
Start
Server Manager
Windows PowerShell
Lync Server Management...
Lync Server Deployment...
Computer
Task Manager
Lync Server Control Panel
Lync Server Topology Builder
Control Panel
Internet Explorer
SQL Server Installation...
SQL Server Installation...
Desktop
SQL Server Configuration...
Import and Export Data (64...
Administrative Tools
Store
SQL Server Error and Usage...

Figure 17-23: Skype for Business Deployment Wizard



Lync Server 2013 - Deployment Wizard

Lync Server 2013
Welcome to Lync Server deployment.

Deploy

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 to the current system.
Your deployment requires at least one installation of the Topology Builder.

Deploy Monitoring Reports
Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances.

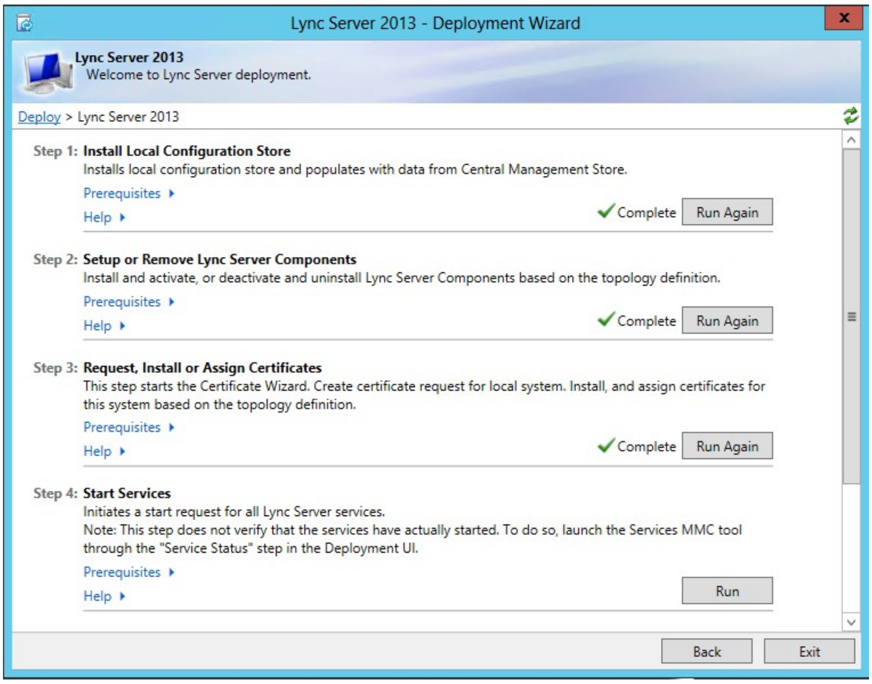
First Run Videos
Click to view getting started videos.

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

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

Figure 17-24: Updating Skype for Business Components



Lync Server 2013 - Deployment Wizard

Lync Server 2013
Welcome to Lync Server deployment.

Deploy > Lync Server 2013

Step 1: **Install Local Configuration Store**
Installs local configuration store and populates with data from Central Management Store.
Prerequisites ▸
Help ▸
✓ Complete | Run Again

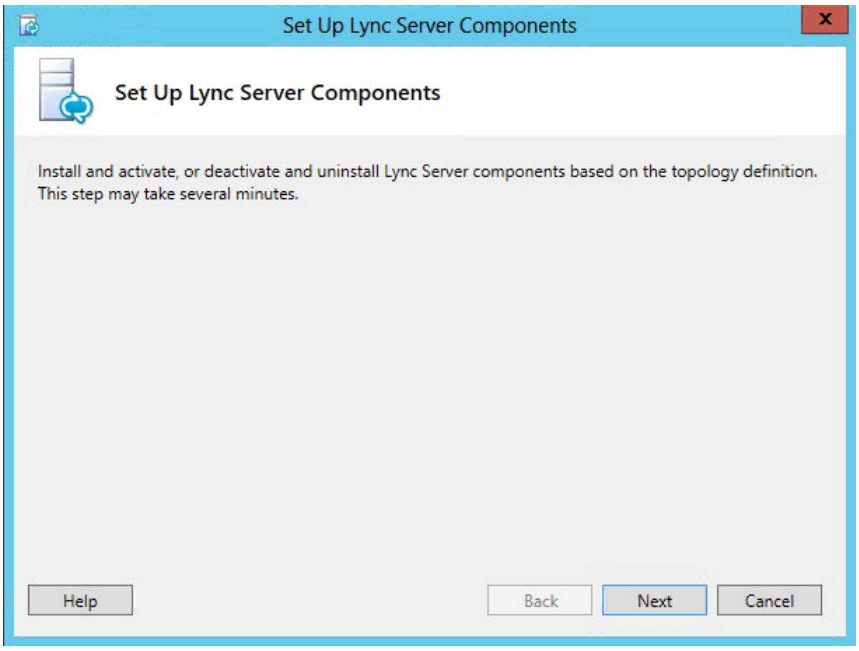
Step 2: **Setup or Remove Lync Server Components**
Install and activate, or deactivate and uninstall Lync Server Components based on the topology definition.
Prerequisites ▸
Help ▸
✓ Complete | Run Again

Step 3: **Request, Install or Assign Certificates**
This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.
Prerequisites ▸
Help ▸
✓ Complete | Run Again

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 ▸
Help ▸
Run

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

Figure 17-25: Setup Server Components

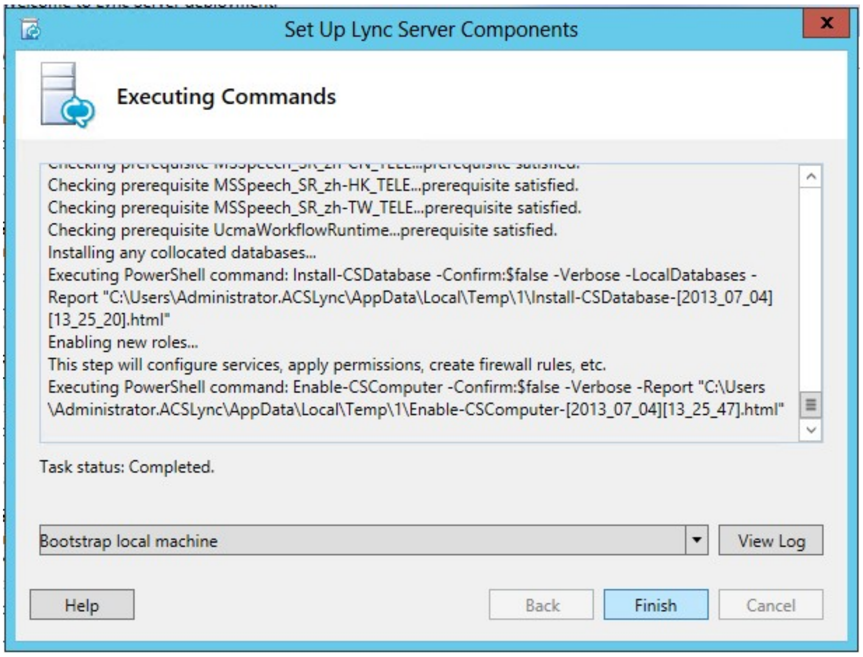


Set Up Lync Server Components

Set Up Lync Server Components

Install and activate, or deactivate and uninstall Lync Server components based on the topology definition.
This step may take several minutes.

Figure 17-26: Finishing the Wizard



```
Checking prerequisite MSSpeech_SR_zh-CN_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_zh-HK_TELE...prerequisite satisfied.
Checking prerequisite MSSpeech_SR_zh-TW_TELE...prerequisite satisfied.
Checking prerequisite UcmaWorkflowRuntime...prerequisite satisfied.
Installing any collocated databases...
Executing PowerShell command: Install-CSDatabase -Confirm:$false -Verbose -LocalDatabases -
Report "C:\Users\Administrator.ACSLync\AppData\Local\Temp\1\Install-CSDatabase-[2013_07_04]
[13_25_20].html"
Enabling new roles...
This step will configure services, apply permissions, create firewall rules, etc.
Executing PowerShell command: Enable-CSComputer -Confirm:$false -Verbose -Report "C:\Users
\Administrator.ACSLync\AppData\Local\Temp\1\Enable-CSComputer-[2013_07_04][13_25_47].html"
```

Task status: Completed.

Bootstrap local machine

17.6 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.

17.6.1 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.

17.6.2 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.

17.6.3 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.

17.6.4 Assigning a Certificate to a Skype for Business Role

This can easily be achieved from the Skype for Business Certificate Wizard.

17.7 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 Chapter 17.12.3 on page 357 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.

17.7.1 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 get this root certificate installed, 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.

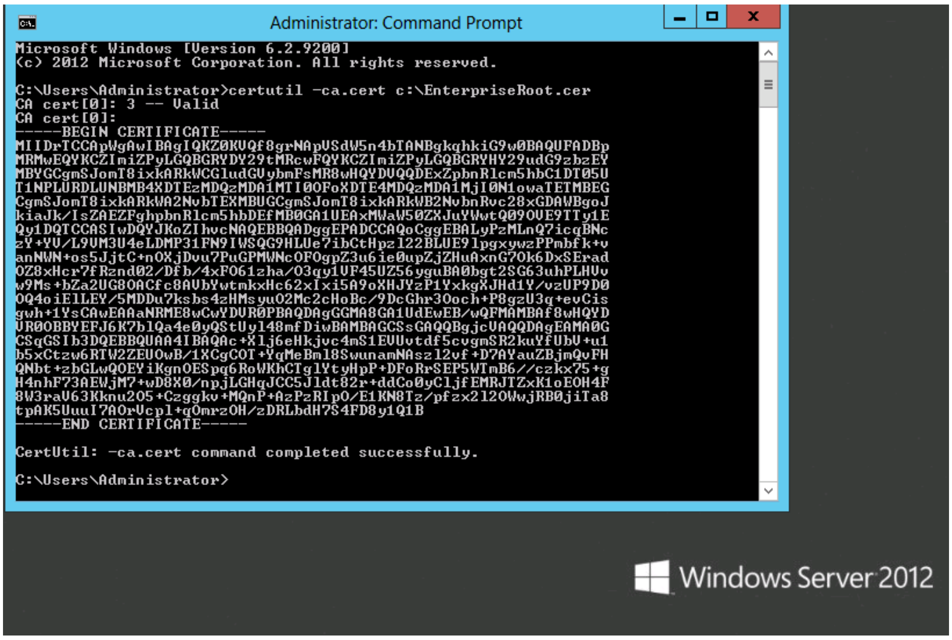
Note: Private Internal Certificates cannot be used for any external connectivity features of CloudBond 365, such as external users, federation, or external conferencing, and mobile clients. A public certificate is required for these features.

17.7.1.1 Obtain the Enterprise Root Certificate

To get the enterprise root certificate, log on to the enterprise Certificate Authority server and issue the following command from a command window:

```
certutil -ca.cert c:\EnterpriseRoot.cer
```

Figure 17-27: Obtaining the CA Root Certificate



```
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>certutil -ca.cert c:\EnterpriseRoot.cer
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDrTCCApWgAwIBAgIQKZ0KVQf8grNApVSdW5n4bTANBgkqhkiG9w0BAQUFADBp
MRMwEQYKCZImiZPyLGQBGRYDY29tMRcwFQYKCZImiZPyLGQBGRYHY29udG9zbzEY
MBYGCgmSJomT8ixkARkWCGludGVybmFsMR8wHQYDVQQDExZpbnRlcm5hbC1DT05U
T1NPLURDLUNBMB4XDTEzMDQzMDA1MTI0OFoXDTE4MDQzMDA1MjI0N1owaTETMBEG
CgmSJomT8ixkARkWA2NvbTEXMBUGCgmSJomT8ixkARkWB2NvbnRvc28xGDAWBgoJ
kiaJk/IsZAEZFghpbnRlcm5hbDEfMB0GA1UEAxMWaW50ZXJuYWwtQ09OVE9TTy1E
Qy1DQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALyPzMLnQ7icqBNc
zY+YV/L9VM3U4eLDMP31FN9IWSQG9HLUe7ibCtHpzl22BLUE9lpgxywzPPmbfk+v
anNWN+os5JjtC+nOXjDvu7PuGPMWNcOFOgpZ3u6ie0upZjZHuAxnG7Ok6DxSErad
OZ8xHcr7fRznd02/Dfb/4xFO61zha/O3qy1VF45UZ56yguBA0bgt2SG63uhPLHVv
w9Ms+bZa2UG8OACfc8AVbYwtmkxHc62xIxi5A9oXHJYzP1YxkgXJHd1Y/vzUP9D0
OQ4oiElLEY/5MDDu7ksbs4zHMsyuO2Mc2cHoBc/9DcGhr3Ooch+P8gzU3q+evCis
gwh+1YsCAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYD
VR0OBBYEFJ6K7blQa4e0yQStUyl48mfDiwBAMBAGCSsGAQQBgjcVAQQDAgEAMA0G
CSqGSIb3DQEBBQUAA4IBAQAc+Xlj6eHkjvc4mS1EVUvtdf5cvgmSR2kuYfUbV+u1
b5xCtzw6RTW2ZEUOwB/1XCgCOT+YqMeBml8SwunamNAszl2vf+D7AYauZBjmQvFH
QNbt+zbGLwQOEYiKgnOESpq6RoWKhCTglYtyHpP+DFoRrSEP5WTmB6//czkx75+g
H4nhF73AEWjM7+wD8X0/npjLGHqJCC5Jldt82r+ddCo0yCljfEMRJTZxK1oEOH4F
8W3raV63Kknu2O5+Czggkv+MQnP+AzPzRIpO/E1KN8Tz/pfzx2l2OWwjRB0jiTa8
tpAK5UuuI7AOrVcpl+qOmrzOH/zDRLbdH7S4FD8y1Q1B
-----END CERTIFICATE-----

CertUtil: -ca.cert command completed successfully.

C:\Users\Administrator>
```

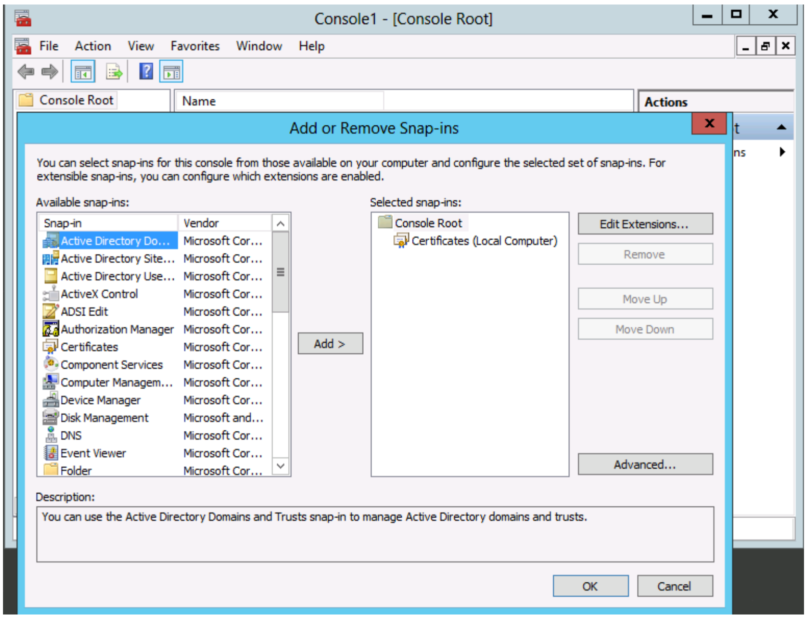
17.7.1.2 Install the Enterprise Root Certificate on CloudBond 365

Copy the file “EnterpriseRoot.cer” from this server to the CloudBond 365 system and perform the following steps to import the enterprise CA as a trusted authority:

On all CloudBond 365 Servers (Frontend, Edge, and Controller), perform the following steps:

1. Open the MMC utility.

Figure 17-28: Install the Root Certificate – Add or Remove Snap-ins



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
Active Directory Do...	Microsoft Cor...
Active Directory Site...	Microsoft Cor...
Active Directory Use...	Microsoft Cor...
ActiveX Control	Microsoft Cor...
ADSI Edit	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
DNS	Microsoft Cor...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...

Selected snap-ins:

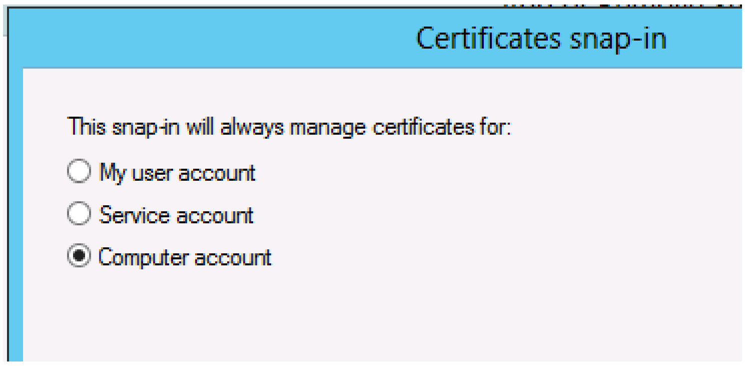
- Console Root
  - Certificates (Local Computer)

Description:

You can use the Active Directory Domains and Trusts snap-in to manage Active Directory domains and trusts.

2. Click **File** -> **Add/Remove Snap-in**.
3. Select **Certificates** -> click **Add**.
4. Select **Computer account**.

Figure 17-29: Install the Root Certificate – Computer Account



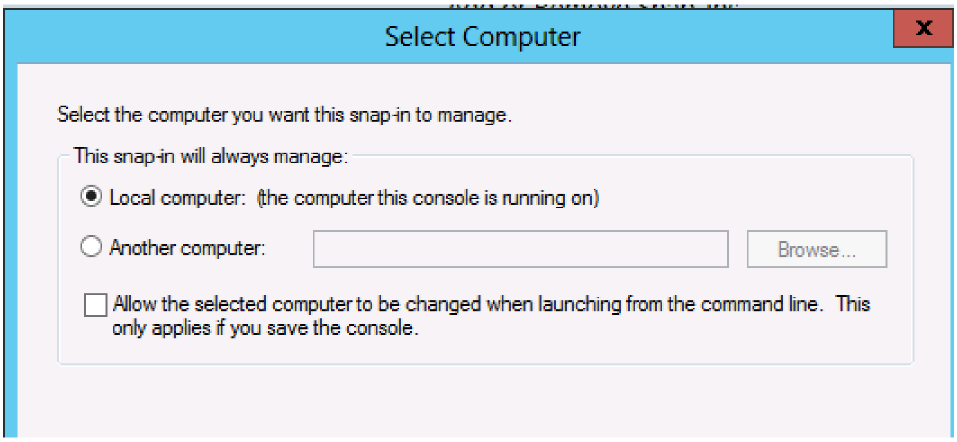
Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

5. Select **Local computer**.

Figure 17-30: Select Computer



Select Computer

Select the computer you want this snap-in to manage.

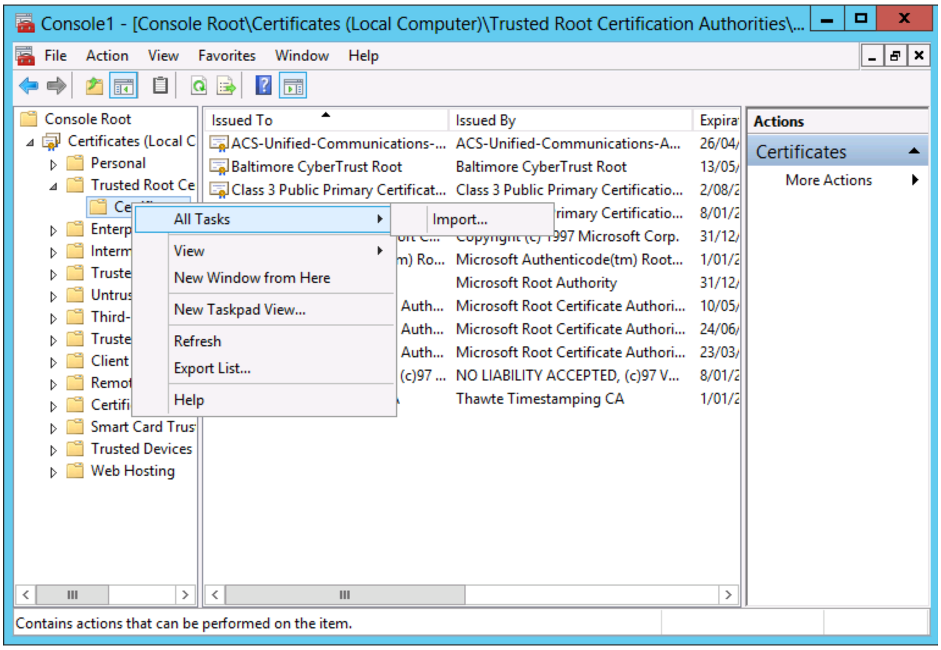
This snap-in will always manage:

● Local computer: (the computer this console is running on)
○ Another computer: Browse...

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

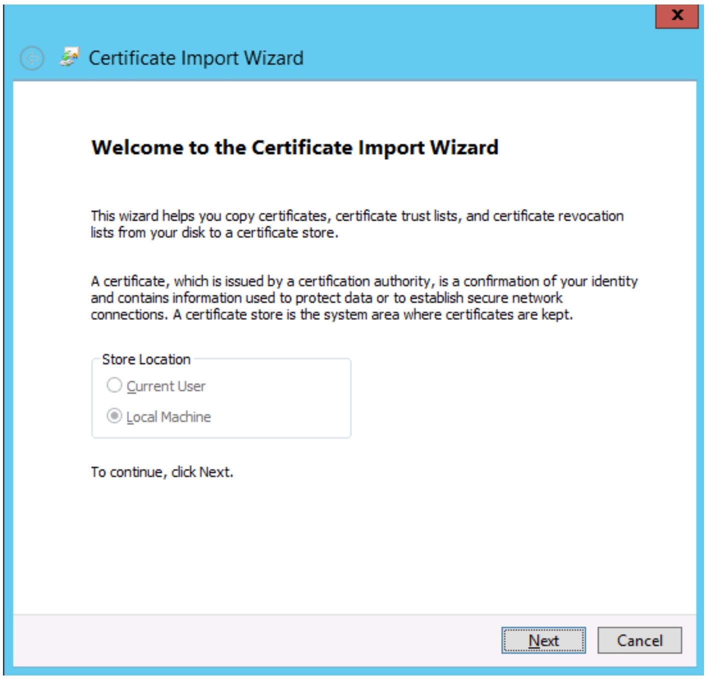
6. Click **Finish**, then click **OK**.
7. Right click **Trusted Root Certification Authorities** -> **All Tasks** and select **Import**.

Figure 17-31: Trusted Root Certificates


Console1 - [Console Root\Certificates (Local Computer)\Trusted Root Certification Authorities\...
File Action View Favorites Window Help
Console Root
Certificates (Local C
Personal
Trusted Root Ce
Ce
Enterp
Interm
Truste
Untrus
Third-
Truste
Client
Remot
Certifi
Smart Card Trus
Trusted Devices
Web Hosting
Issued To
Issued By
Expira
ACS-Unified-Communications-... ACS-Unified-Communications-A... 26/04/
Baltimore CyberTrust Root Baltimore CyberTrust Root 13/05/
Class 3 Public Primary Certificat... Class 3 Public Primary Certificatio... 2/08/2
rimary Certificatio... 8/01/2
Copyright (c) 1997 Microsoft Corp. 31/12/
m) Ro... Microsoft Authenticode(tm) Root... 1/01/2
Microsoft Root Authority 31/12/
Auth... Microsoft Root Certificate Authori... 10/05/
Auth... Microsoft Root Certificate Authori... 24/06/
Auth... Microsoft Root Certificate Authori... 23/03/
(c)97 ... NO LIABILITY ACCEPTED, (c)97 V... 8/01/2
Thawte Timestamping CA 1/01/2
All Tasks
Import...
View
New Window from Here
New Taskpad View...
Refresh
Export List...
Help
Actions
Certificates
More Actions
Contains actions that can be performed on the item.

8. Complete the import wizard, importing the root certificate.

Figure 17-32: Importing the Certificate



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

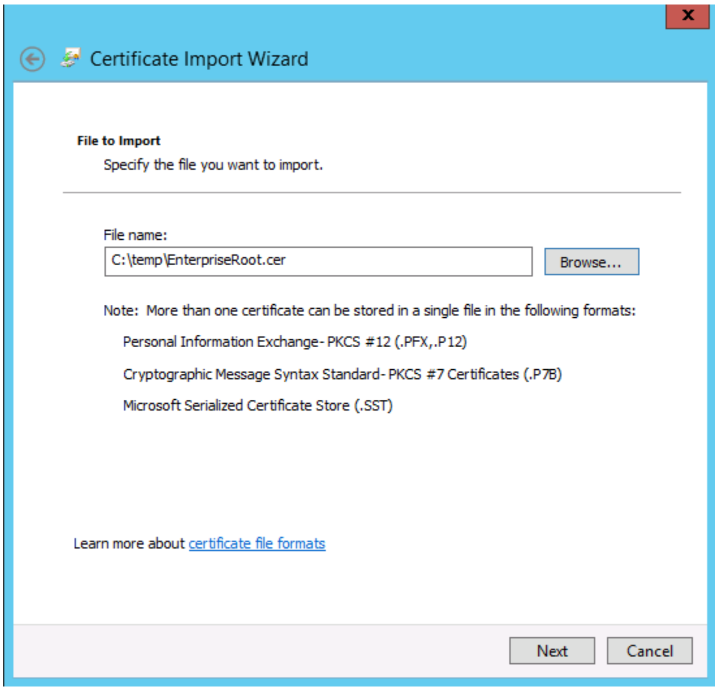
○ Current User

● Local Machine

To continue, click Next.

9. Specify the certificate file copied from the Enterprise CA.

Figure 17-33: Certificate Import Wizard



File to Import

Specify the file you want to import.

File name:

C:\temp\EnterpriseRoot.cer

Note: More than one certificate can be stored in a single file in the following formats:

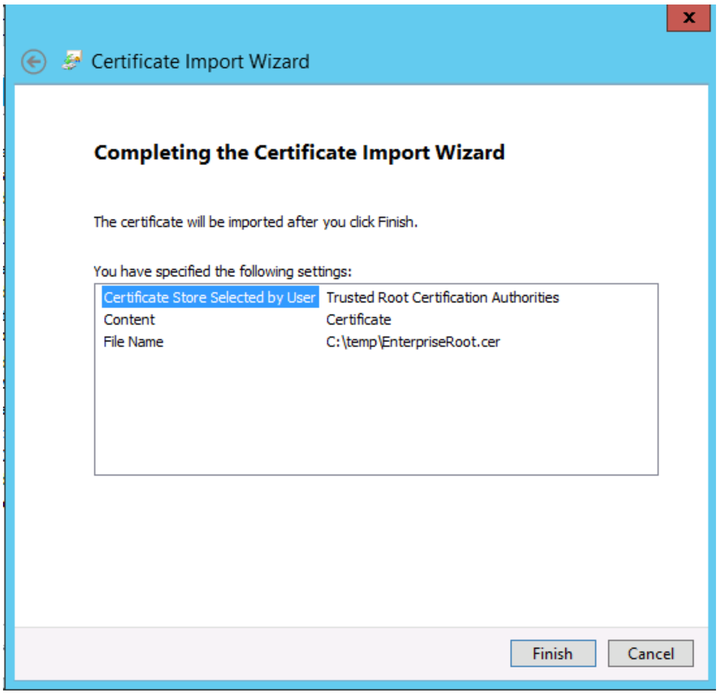
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Figure 17-34: Completing Certificate Import Wizard



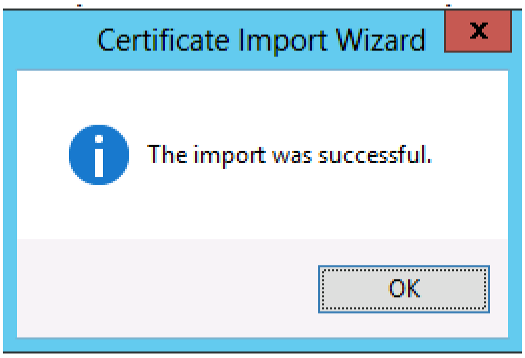
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\temp\EnterpriseRoot.cer

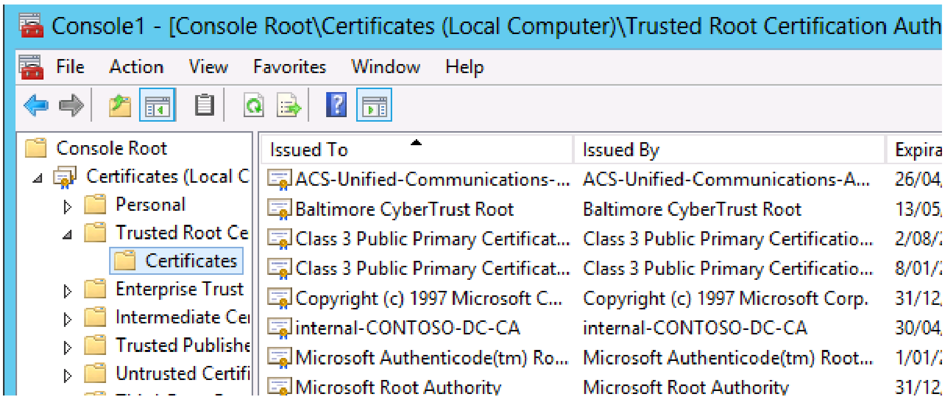
Figure 17-35: Successful Import



The import was successful.

10. The Enterprise root certificate will now appear in the list of trusted root certificates.

Figure 17-36: Trusted Root Certificates



Issued To	Issued By	Expira
ACS-Unified-Communications-...	ACS-Unified-Communications-A...	26/04,
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13/05,
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	2/08/
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/01/
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31/12,
internal-CONTOSO-DC-CA	internal-CONTOSO-DC-CA	30/04,
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	1/01/
Microsoft Root Authority	Microsoft Root Authority	31/12,

17.8 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.

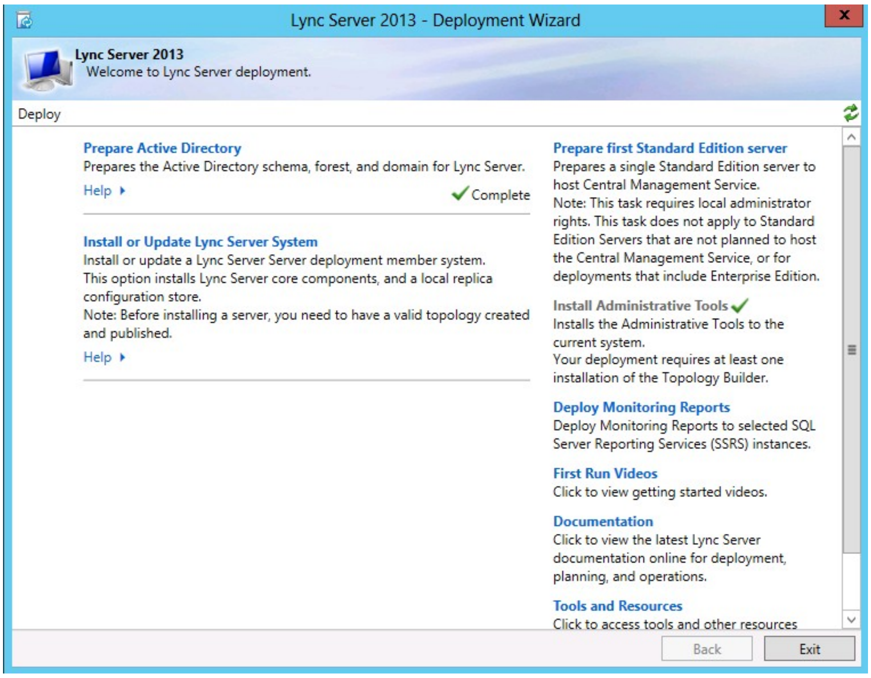
17.8.1 Using the Certificate Wizards

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.

17.8.1.1 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 17-37: Skype for Business Deployment Wizard



Lync Server 2013 - Deployment Wizard
Lync Server 2013
Welcome to Lync Server deployment.
Deploy
Back
Exit

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 to the current system.
Your deployment requires at least one installation of the Topology Builder.

Deploy Monitoring Reports
Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances.

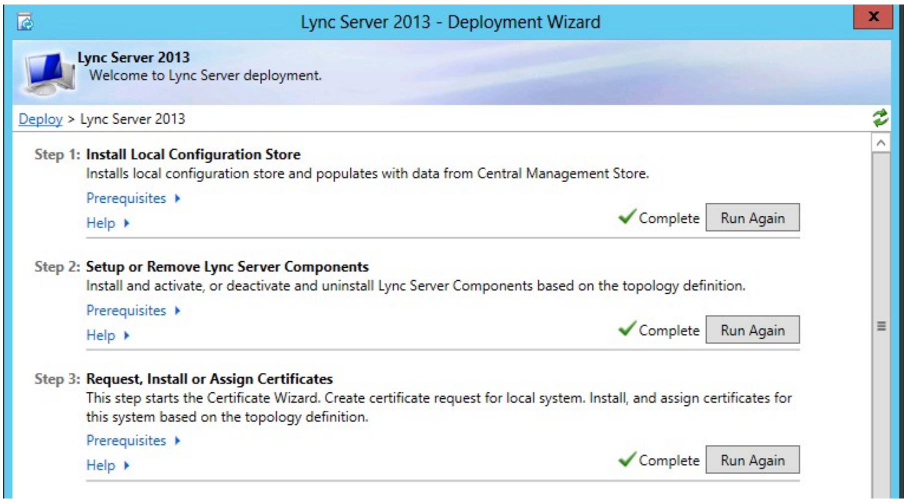
First Run Videos
Click to view getting started videos.

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

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

Figure 17-38: Requesting a certificate



Lync Server 2013 - Deployment Wizard
Lync Server 2013
Welcome to Lync Server deployment.
Deploy > Lync Server 2013

Step 1: **Install Local Configuration Store**
Installs local configuration store and populates with data from Central Management Store.

Step 2: **Setup or Remove Lync Server Components**
Install and activate, or deactivate and uninstall Lync Server Components based on the topology definition.

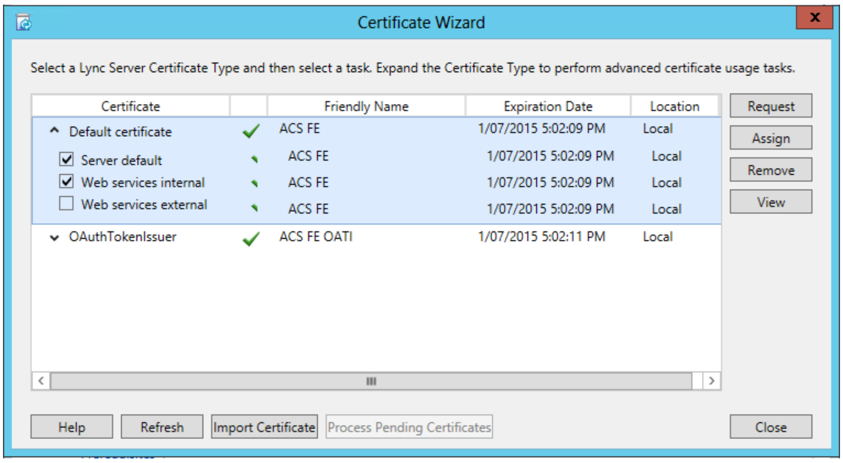
Step 3: **Request, Install or Assign Certificates**
This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for this system based on the topology definition.

You will see the Certificate Wizard screen similar to one of those below. Expand the Section for the certificate you wish to work with, and select the roles.

- Front End – Server default and Internal Web Services
- Front End – External Web Services
- Edge – Internal
- Edge – External

The OAuthTokenIssuer is used for Microsoft Exchange 2013 integration.

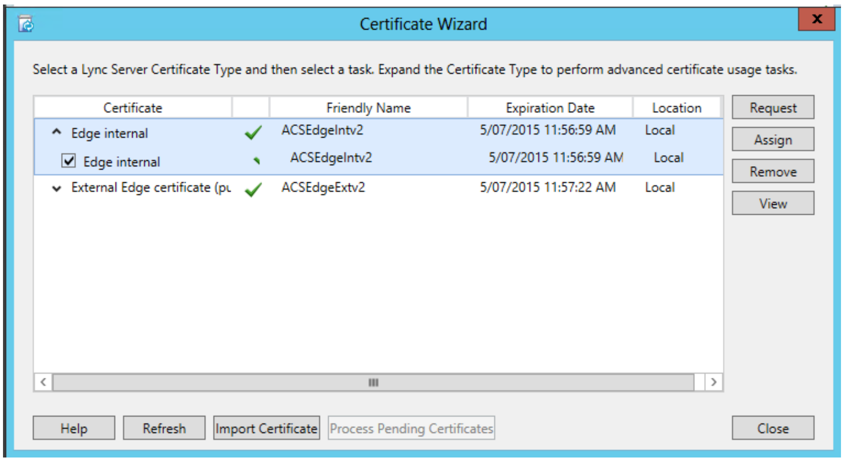
Figure 17-39: Front-End Certificate for Internal Use



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
^ Default certificate	✓	ACS FE	1/07/2015 5:02:09 PM	Local
☑ Server default	✓	ACS FE	1/07/2015 5:02:09 PM	Local
☑ Web services internal	✓	ACS FE	1/07/2015 5:02:09 PM	Local
□ Web services external	✓	ACS FE	1/07/2015 5:02:09 PM	Local
˅ OAuthTokenIssuer	✓	ACS FE OATI	1/07/2015 5:02:11 PM	Local

Figure 17-40: Edge Certificate for Internal Use



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
^ Edge internal	✓	ACSEdgeIntv2	5/07/2015 11:56:59 AM	Local
☑ Edge internal	✓	ACSEdgeIntv2	5/07/2015 11:56:59 AM	Local
˅ External Edge certificate (pu	✓	ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local

17.9 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.

17.9.1 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 will be 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.

17.9.2 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.

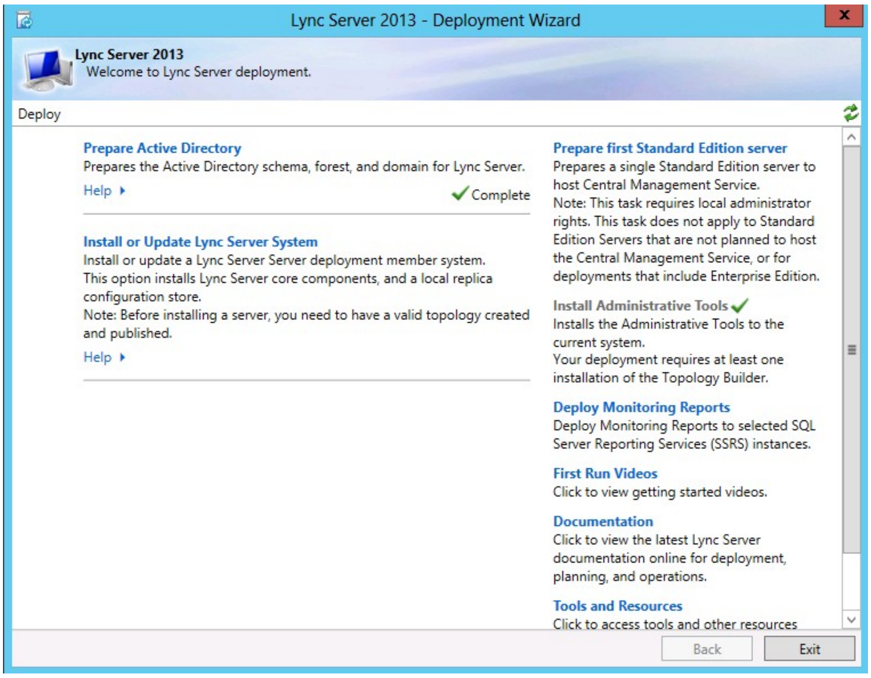
Note: Skype for Business introduced a new Authorization method for server to server communications. This includes a new certificate requirement for an OAuth certificate on the Skype for Business Front End server. This OAuth certificate is only used for communicating with Exchange 2013 and SharePoint 2013, and can also be used with Office 365.

17.9.3 Requesting Certificates (CA Accessible)

17.9.3.1 Generating the Certificate Request

1. Start the Deployment Wizard.
2. Select **Install or Update Lync Server System**.

Figure 17-41: Deployment Wizard



Lync Server 2013
Welcome to Lync Server deployment.

Deploy

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 to the current system.
Your deployment requires at least one installation of the Topology Builder.

Deploy Monitoring Reports
Deploy Monitoring Reports to selected SQL Server Reporting Services (SSRS) instances.

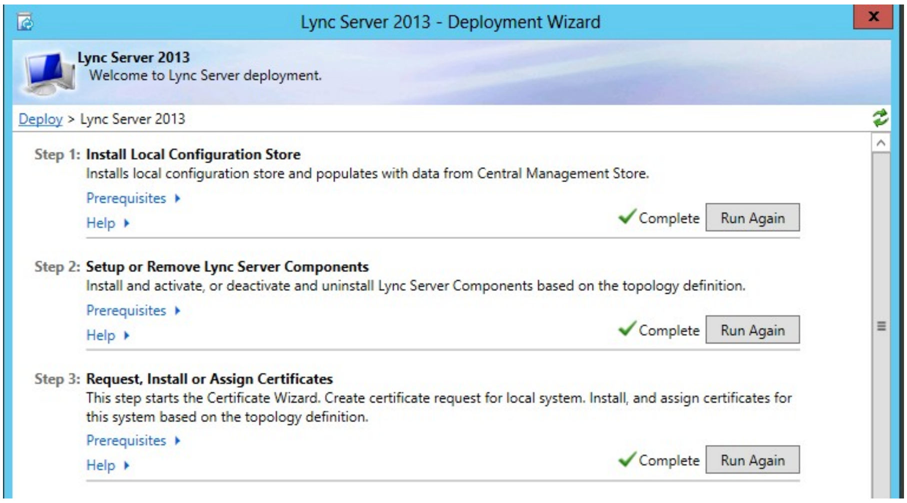
First Run Videos
Click to view getting started videos.

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

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

Figure 17-42: Requesting a certificate



Lync Server 2013
Welcome to Lync Server deployment.

Deploy > Lync Server 2013

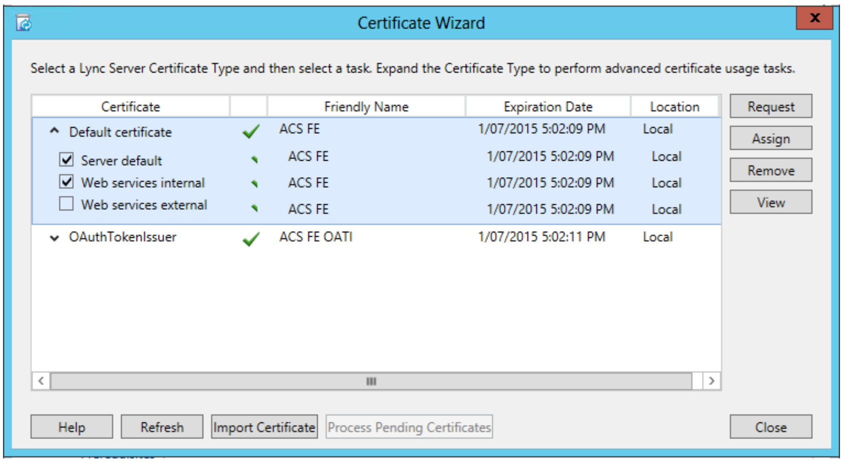
Step 1: **Install Local Configuration Store**
Installs local configuration store and populates with data from Central Management Store.
Prerequisites ▸
Help ▸ ✓ Complete Run Again

Step 2: **Setup or Remove 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 request for local system. Install, and assign certificates for this system based on the topology definition.
Prerequisites ▸
Help ▸ ✓ Complete Run Again

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

Figure 17-43: Front-End Certificate for Internal Use

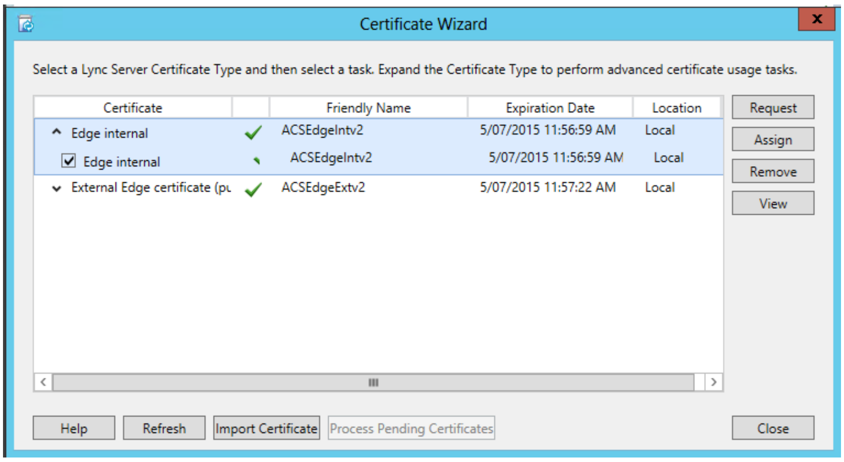


Certificate Wizard

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
^ Default certificate	✓	ACS FE	1/07/2015 5:02:09 PM	Local
☑ Server default		ACS FE	1/07/2015 5:02:09 PM	Local
☑ Web services internal		ACS FE	1/07/2015 5:02:09 PM	Local
□ Web services external		ACS FE	1/07/2015 5:02:09 PM	Local
⌄ OAuthTokenIssuer	✓	ACS FE OATI	1/07/2015 5:02:11 PM	Local

Figure 17-44: Edge Certificate for Internal Use



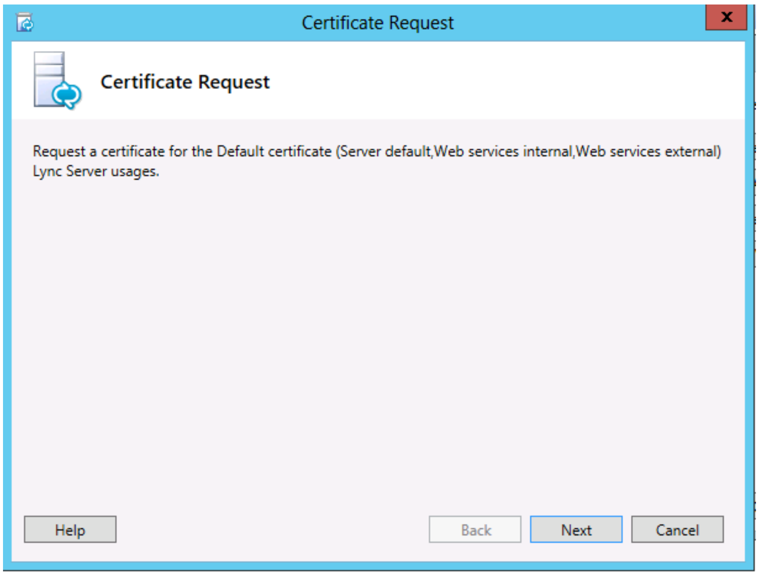
Certificate Wizard

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
^ Edge internal	✓	ACSEdgeIntv2	5/07/2015 11:56:59 AM	Local
☑ Edge internal		ACSEdgeIntv2	5/07/2015 11:56:59 AM	Local
⌄ External Edge certificate (pu	✓	ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local

5. Complete the Wizard.

Figure 17-45: Certificate Request



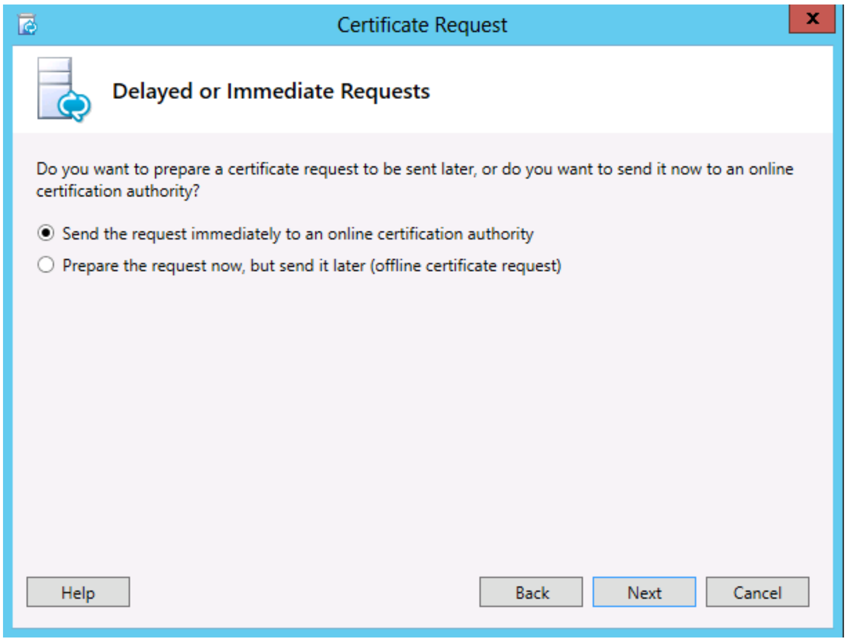
Certificate Request

Certificate Request

Request a certificate for the Default certificate (Server default,Web services internal,Web services external) Lync Server usages.

6. Select **Send the request immediately**.

Figure 17-46: Delayed or Immediate Requests



Delayed or Immediate Requests

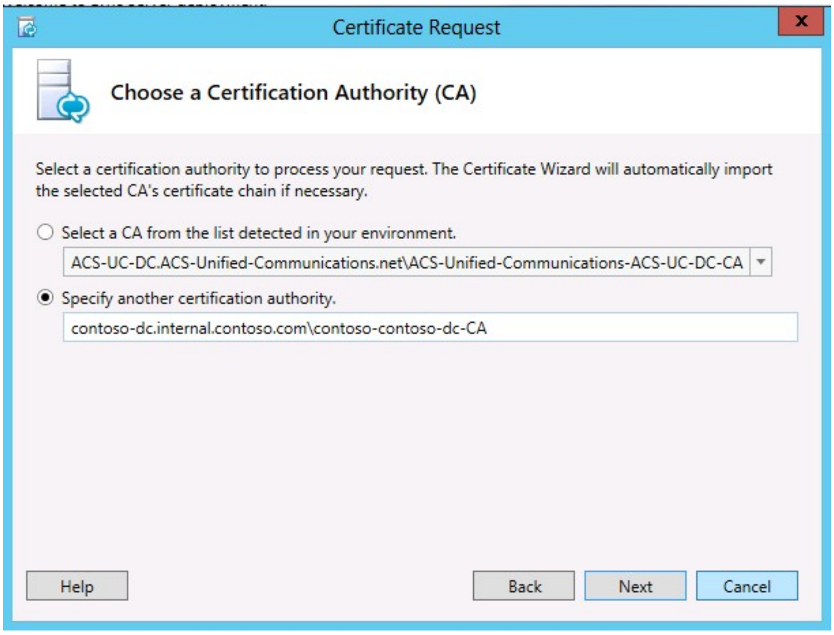
Do you want to prepare a certificate request to be sent later, or do you want to send it now to an online certification authority?

● Send the request immediately to an online certification authority

○ Prepare the request now, but send it later (offline certificate request)

7. Specify the Enterprise CA.

Figure 17-47: Creating Certificate Requests



Choose a Certification Authority (CA)

Select a certification authority to process your request. The Certificate Wizard will automatically import the selected CA's certificate chain if necessary.

○ Select a CA from the list detected in your environment.

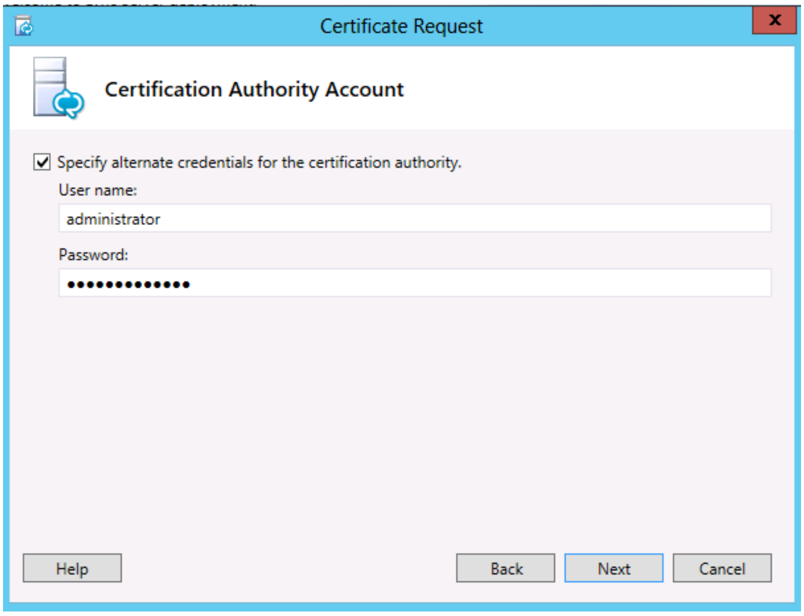
ACS-UC-DC.ACS-Unified-Communications.net\ACS-Unified-Communications-ACS-UC-DC-CA

● Specify another certification authority.

contoso-dc.internal.contoso.com\contoso-contoso-dc-CA

8. Enter Enterprise Domain credentials.

Figure 17-48: Certification Authority Account



Certificate Request

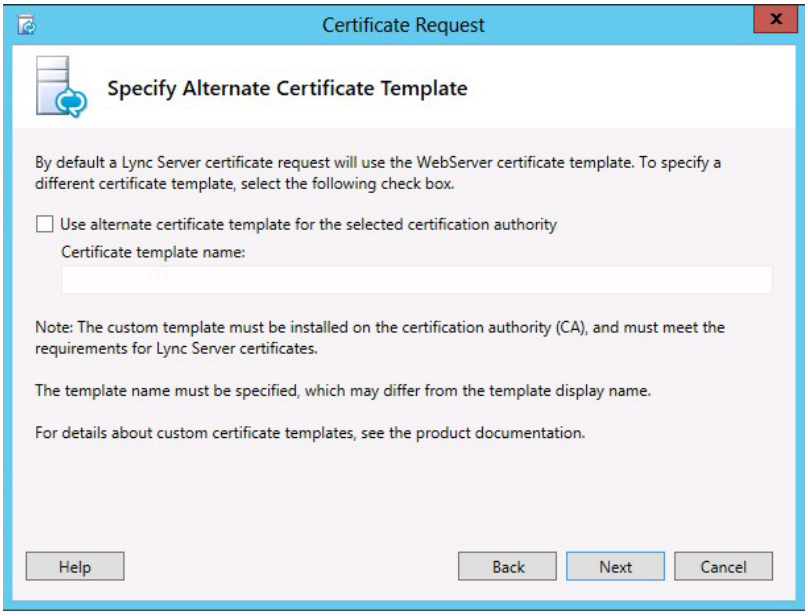
Certification Authority Account

☑ Specify alternate credentials for the certification authority.

User name: administrator

Password: •••••••••••••

Figure 17-49: Specify Alternate Certificate Template



Certificate Request

Specify Alternate Certificate Template

By default a Lync Server certificate request will use the WebServer certificate template. To specify a different certificate template, select the following check box.

☐ Use alternate certificate template for the selected certification authority

Certificate template name:

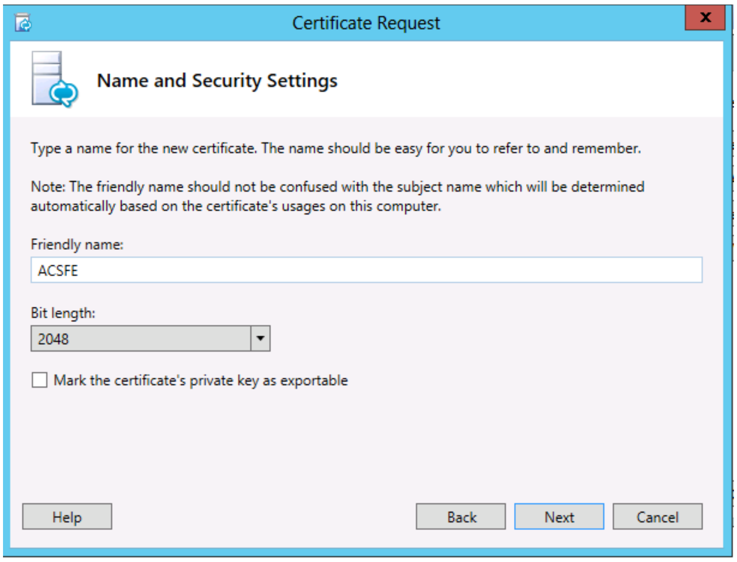
Note: The custom template must be installed on the certification authority (CA), and must meet the requirements for Lync Server certificates.

The template name must be specified, which may differ from the template display name.

For details about custom certificate templates, see the product documentation.

9. Enter a friendly name.

Figure 17-50: Name and Security Settings



Certificate Request

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.

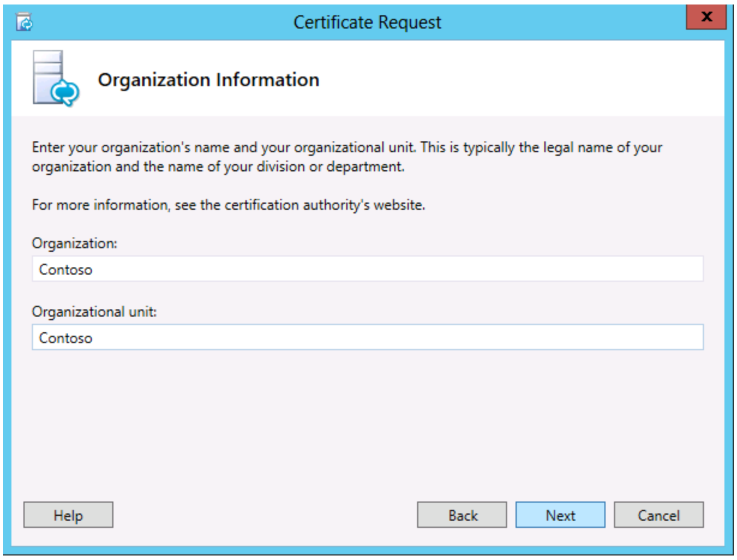
Friendly name:
ACSFE

Bit length:
2048

□ Mark the certificate's private key as exportable

10. Enter the organization details.

Figure 17-51: Organization Information



Certificate Request

Organization Information

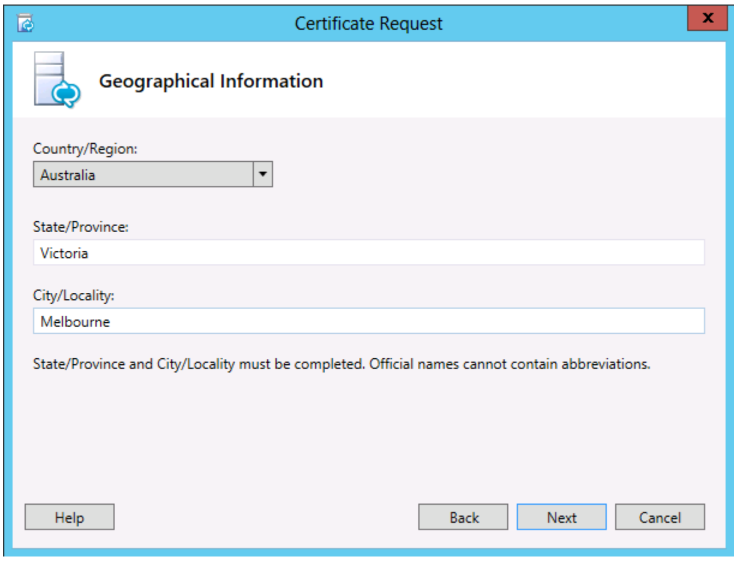
Enter your organization's name and your organizational unit. This is typically the legal name of your organization and the name of your division or department.

For more information, see the certification authority's website.

Organization:
Contoso

Organizational unit:
Contoso

Figure 17-52: Geographical Information



Certificate Request

Geographical Information

Country/Region: Australia

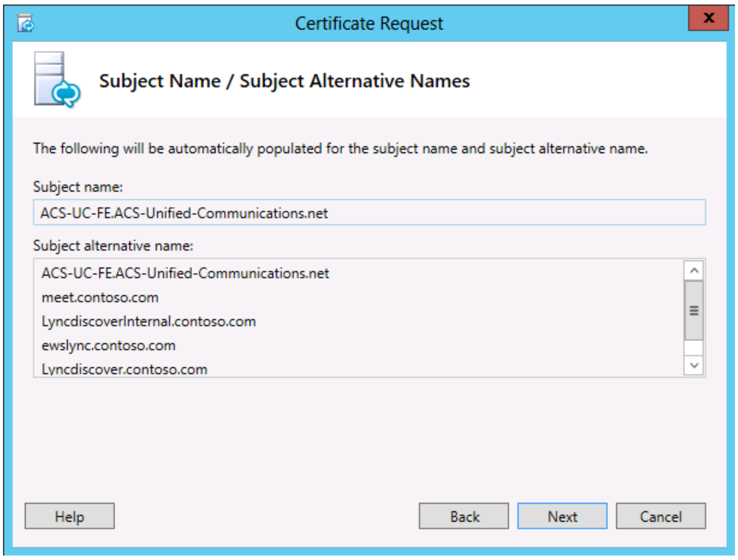
State/Province: Victoria

City/Locality: Melbourne

State/Province and City/Locality must be completed. Official names cannot contain abbreviations.

11. 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 17-53: Subject Name / Subject Alternative Names



Certificate Request

Subject Name / Subject Alternative Names

The following will be automatically populated for the subject name and subject alternative name.

Subject name:

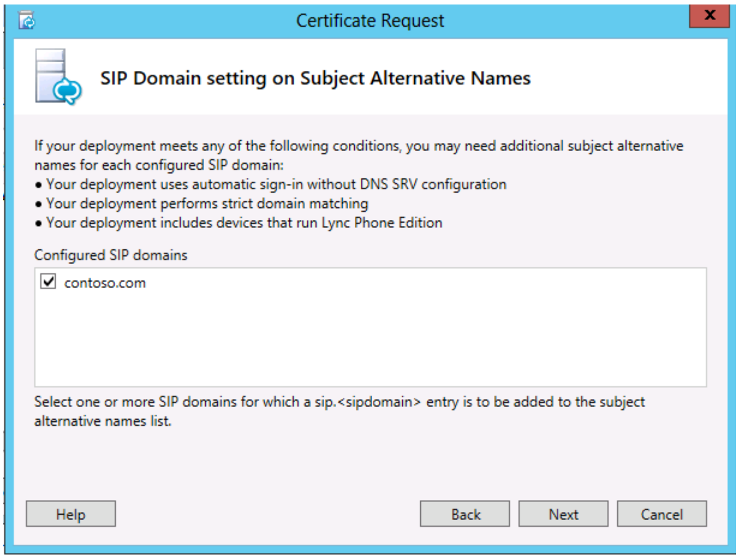
ACS-UC-FE.ACS-Unified-Communications.net

Subject alternative name:

ACS-UC-FE.ACS-Unified-Communications.net
meet.contoso.com
LyncdiscoverInternal.contoso.com
ewslync.contoso.com
Lyncdiscover.contoso.com

12. Enable any SIP domains.

Figure 17-54: SIP Domain Setting on Subject Alternative Names



Certificate Request

SIP Domain setting on Subject Alternative Names

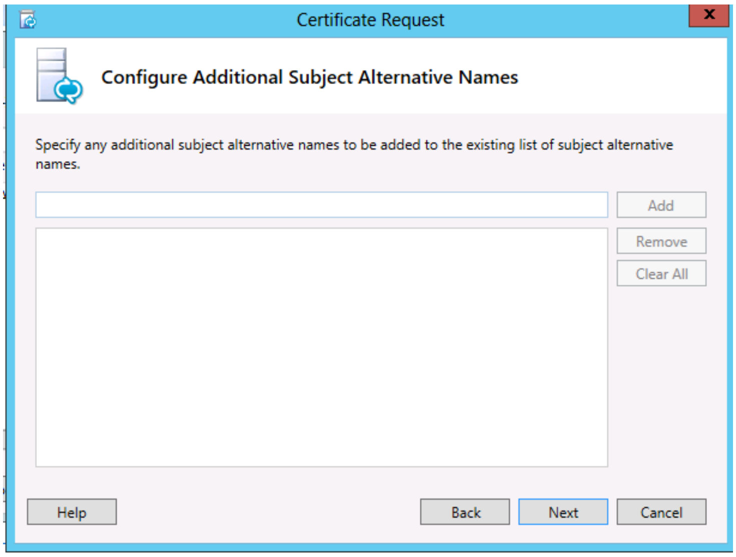
If your deployment meets any of the following conditions, you may need additional subject alternative names for each configured SIP domain:
- Your deployment uses automatic sign-in without DNS SRV configuration
- Your deployment performs strict domain matching
- Your deployment includes devices that run Lync Phone Edition

Configured SIP domains

☑ contoso.com

Select one or more SIP domains for which a sip.<sipdomain> entry is to be added to the subject alternative names list.

Figure 17-55: Configure Additional Subject Alternative Names

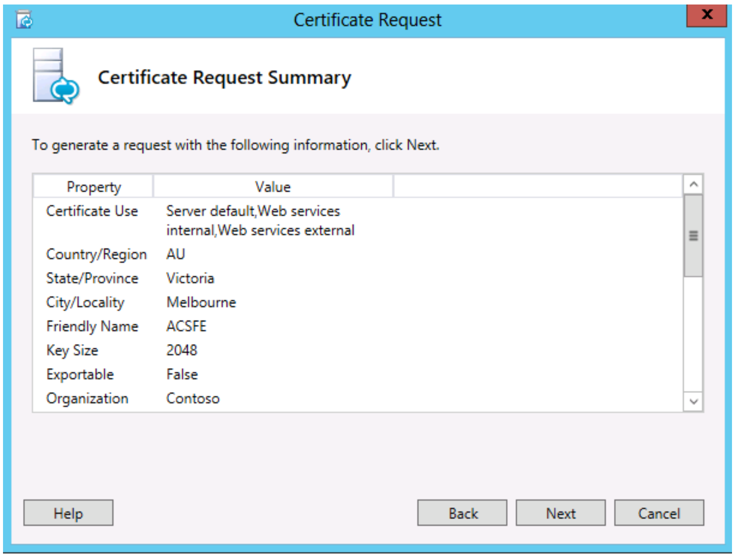


Certificate Request

Configure Additional Subject Alternative Names

Specify any additional subject alternative names to be added to the existing list of subject alternative names.

Figure 17-56: Certificate Request Summary



Certificate Request Summary

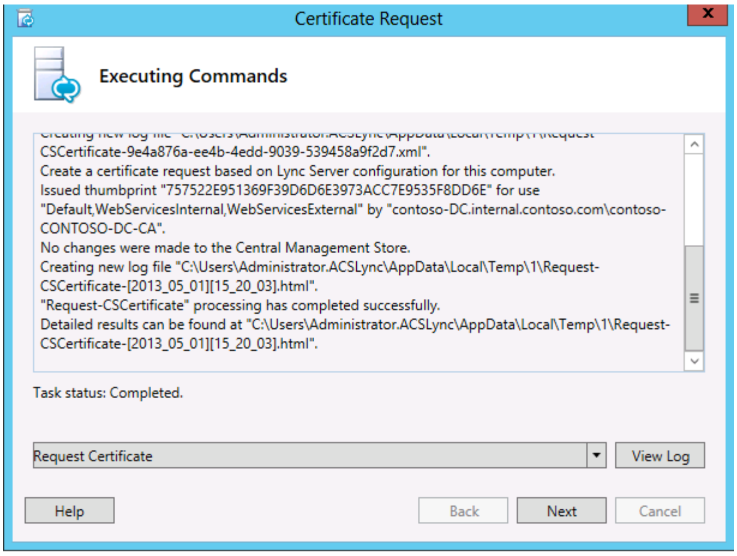
To generate a request with the following information, click Next.

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
Organization	Contoso

17.9.3.2 Generating and Installing the Certificate

The certificate request is sent to the nominated CA, where a matching Certificate is generated. The Certificate is returned to the requestor and imported automatically as part of the process.

Figure 17-57: Executing Commands



Executing Commands

```
Creating new log file "C:\Users\Administrator.ACSLync\AppData\Local\Temp\1\Request-
CSCertificate-9e4a876a-ee4b-4edd-9039-539458a9f2d7.xml".
Create a certificate request based on Lync Server configuration for this computer.
Issued thumbprint "757522E951369F39D6D6E3973ACC7E9535F8DD6E" for use
"Default,WebServicesInternal,WebServicesExternal" by "contoso-DC.internal.contoso.com\contoso-
CONTOSO-DC-CA".
No changes were made to the Central Management Store.
Creating new log file "C:\Users\Administrator.ACSLync\AppData\Local\Temp\1\Request-
CSCertificate-[2013_05_01][15_20_03].html".
"Request-CSCertificate" processing has completed successfully.
Detailed results can be found at "C:\Users\Administrator.ACSLync\AppData\Local\Temp\1\Request-
CSCertificate-[2013_05_01][15_20_03].html".
```

Task status: Completed.

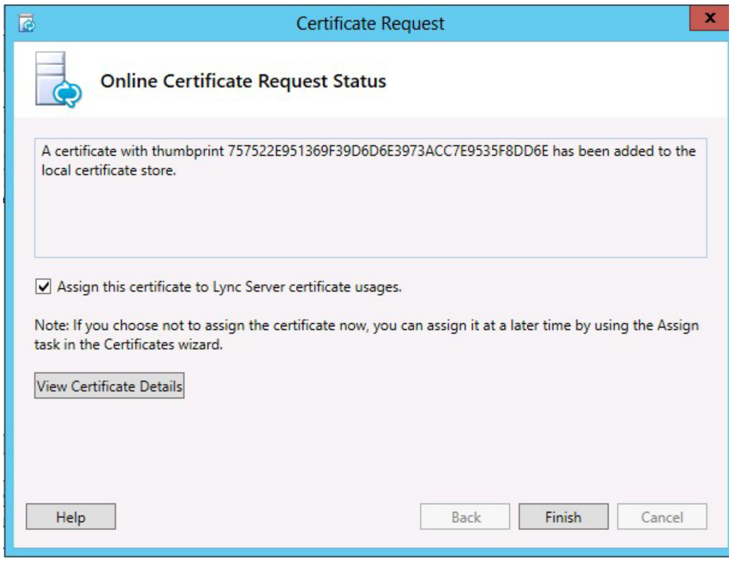
Request Certificate

The certificate has now been generated and imported into the server certificate store.

17.9.3.3 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 17-58: Online Certificate Request Status



Certificate Request

Online Certificate Request Status

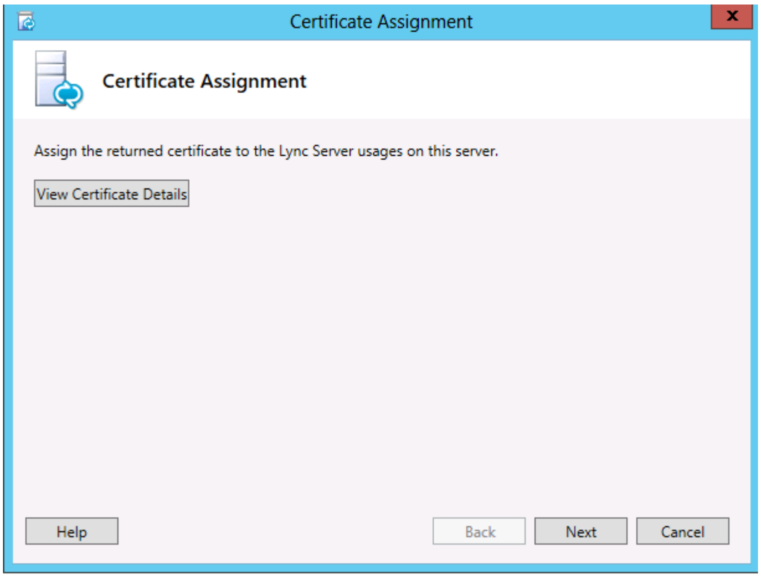
A certificate with thumbprint 757522E951369F39D6D6E3973ACC7E9535F8DD6E has been added to the local certificate store.

☑ Assign this certificate to Lync Server certificate usages.

Note: If you choose not to assign the certificate now, you can assign it at a later time by using the Assign task in the Certificates wizard.

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

Figure 17-59: Certificate Assignment

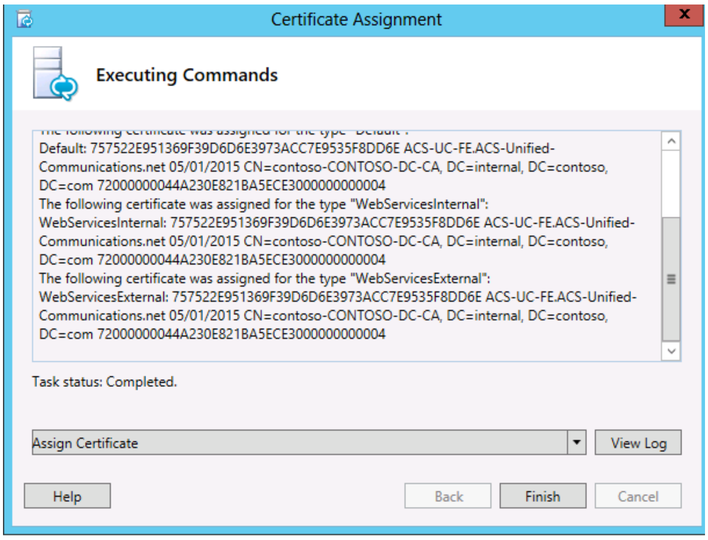


Certificate Assignment

Certificate Assignment

Assign the returned certificate to the Lync Server usages on this server.

Figure 17-60: Executing Commands



```
The following certificate was assigned for the type "Default":
Default: 757522E951369F39D6D6E3973ACC7E9535F8DD6E ACS-UC-FE.ACS-Unified-
Communications.net 05/01/2015 CN=contoso-CONTOSO-DC-CA, DC=internal, DC=contoso,
DC=com 72000000044A230E821BA5ECE3000000000004
The following certificate was assigned for the type "WebServicesInternal":
WebServicesInternal: 757522E951369F39D6D6E3973ACC7E9535F8DD6E ACS-UC-FE.ACS-Unified-
Communications.net 05/01/2015 CN=contoso-CONTOSO-DC-CA, DC=internal, DC=contoso,
DC=com 72000000044A230E821BA5ECE3000000000004
The following certificate was assigned for the type "WebServicesExternal":
WebServicesExternal: 757522E951369F39D6D6E3973ACC7E9535F8DD6E ACS-UC-FE.ACS-Unified-
Communications.net 05/01/2015 CN=contoso-CONTOSO-DC-CA, DC=internal, DC=contoso,
DC=com 72000000044A230E821BA5ECE3000000000004
```

Task status: Completed.

Assign Certificate

3. Repeat the above steps on the CloudBond 365 Edge server internal network to assign an Enterprise CA certificate.

17.9.4 Requesting Certificates (CA is Not Available)

This section describes how to requesting certificates when the CA is not available.

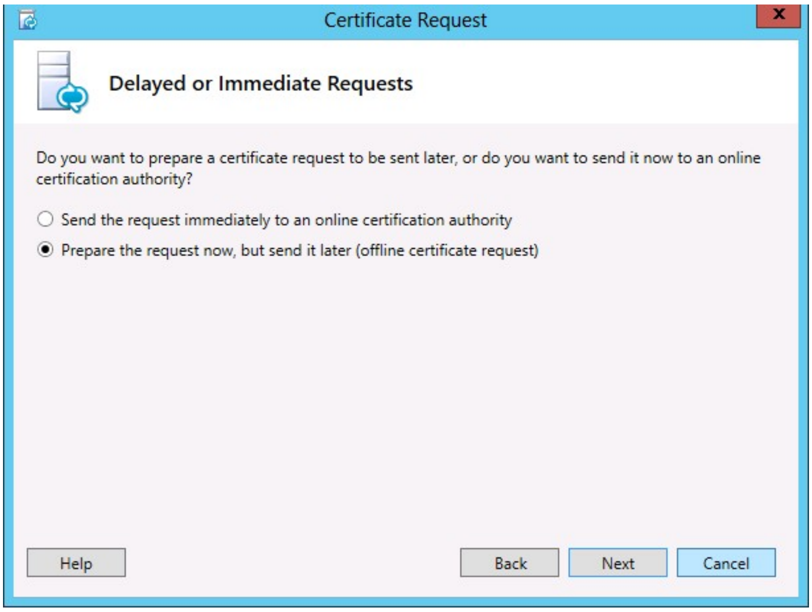
17.9.4.1 Generating the Certificate Request

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.

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**, but send it later.

Figure 17-61: Delayed or Immediate Requests



Delayed or Immediate Requests

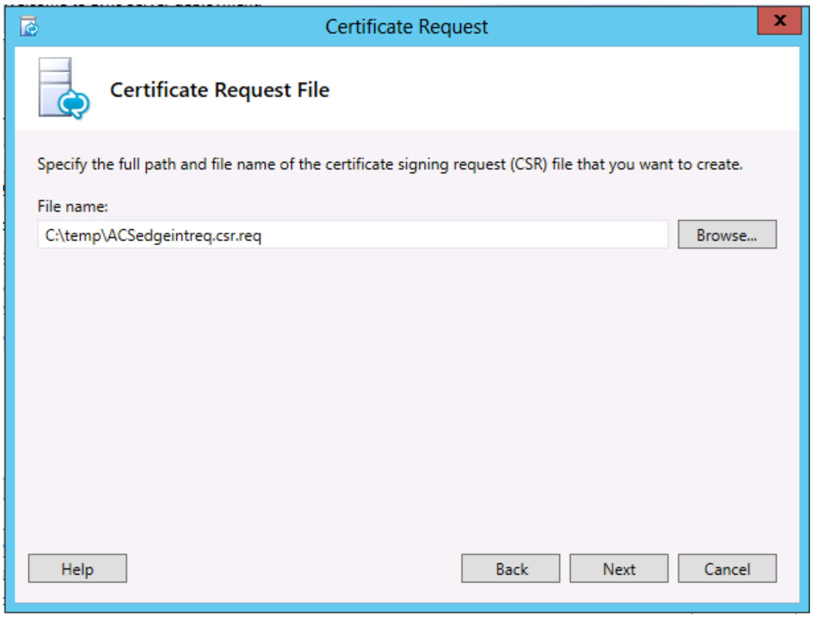
Do you want to prepare a certificate request to be sent later, or do you want to send it now to an online certification authority?

○ Send the request immediately to an online certification authority

● Prepare the request now, but send it later (offline certificate request)

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

Figure 17-62: Certificate Request File

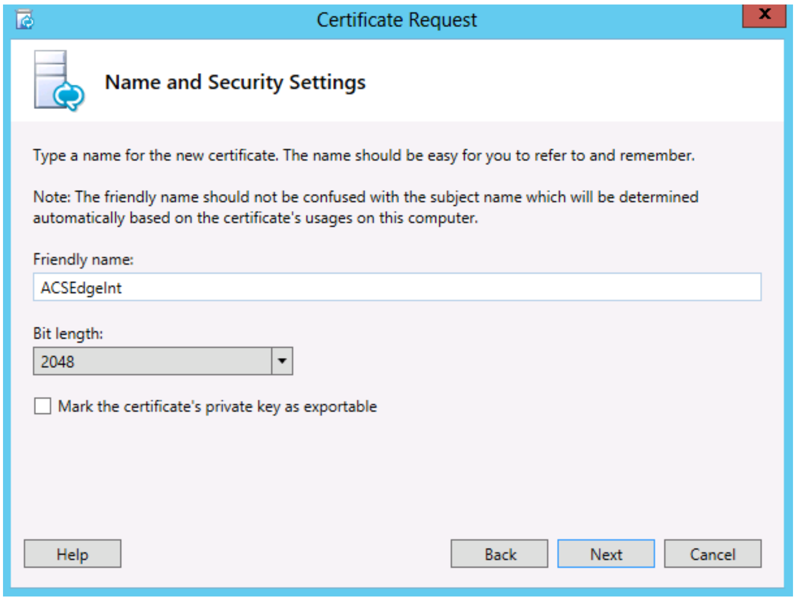


Certificate Request File

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

Figure 17-63: Name and Security Settings



Certificate Request

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.

Friendly name: ACSEdgeInt

Bit length: 2048

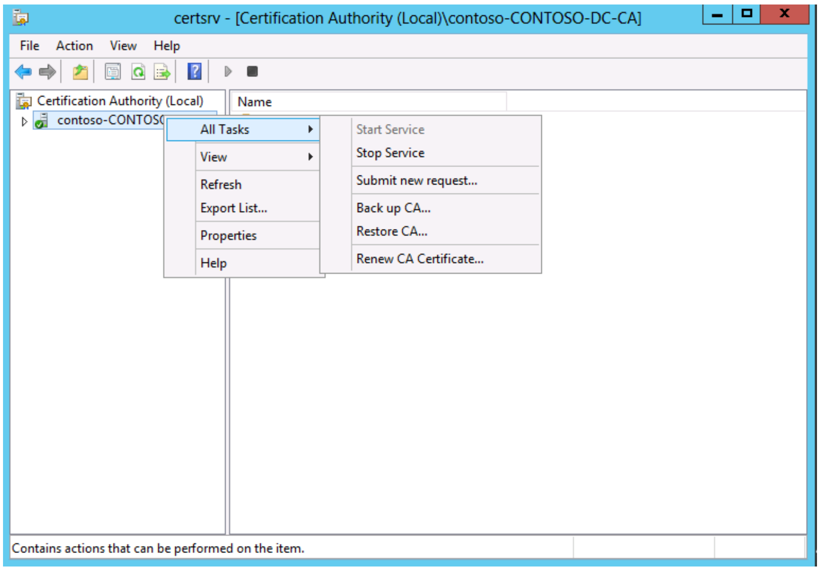
□ Mark the certificate's private key as exportable

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.

17.9.4.2 Generating the Certificate

1. Copy the Certificate Signing Request File that was just created to the enterprise Certification Authority server and start the Certificate Authority management console.
2. Right-click the server and select **All Tasks** -> **Submit new request**.

Figure 17-64: Manually Generating a Certificate – All Tasks

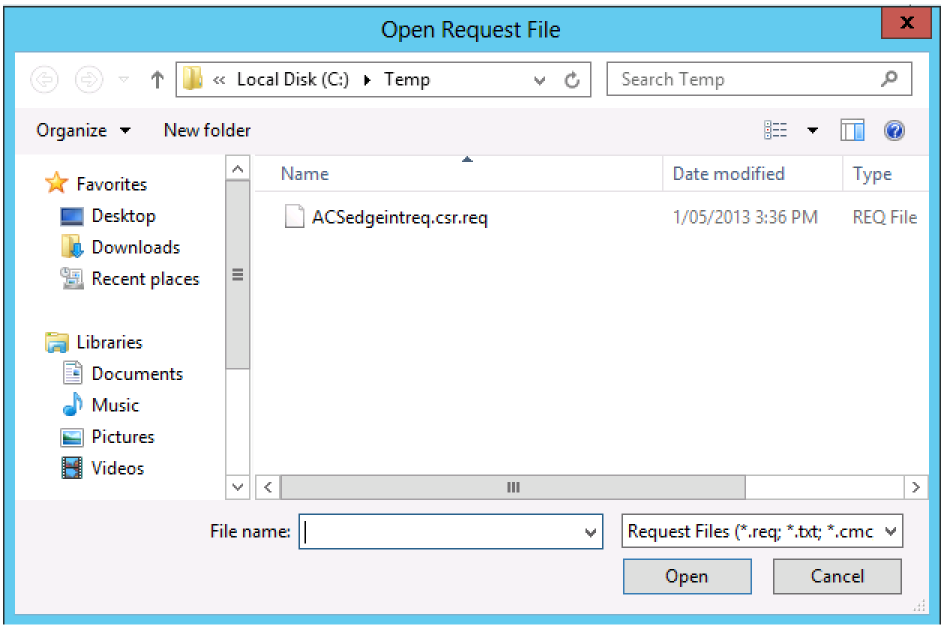


certsrv - [Certification Authority (Local)\contoso-CONTOSO-DC-CA]

Contains actions that can be performed on the item.

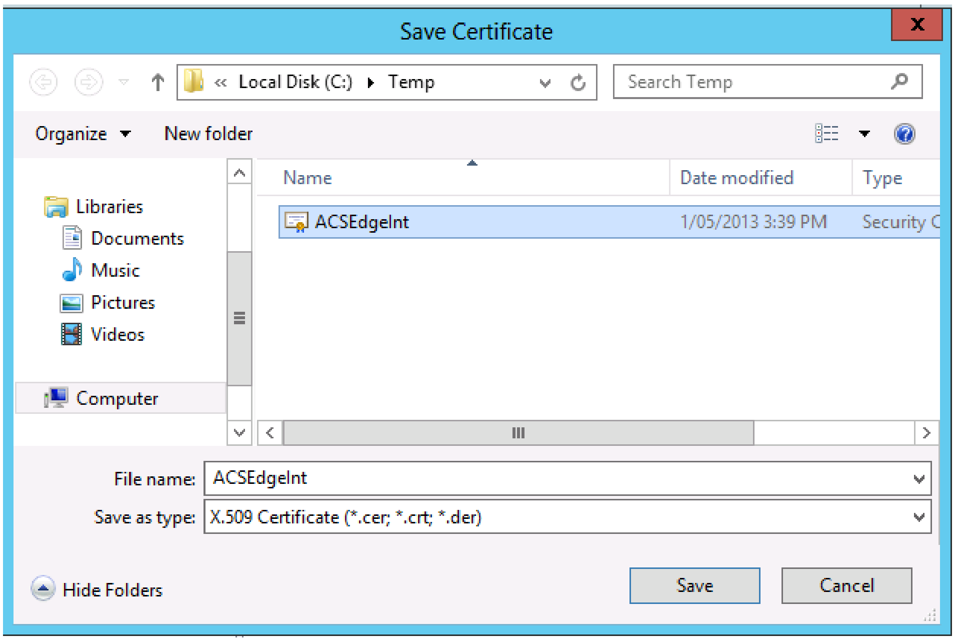
3. Open the request file and click **Open**.

Figure 17-65: Manually Generating a Certificate



4. A similar window appears to save the requested certificate.

Figure 17-66: Manually Generating a Certificate – Save Request



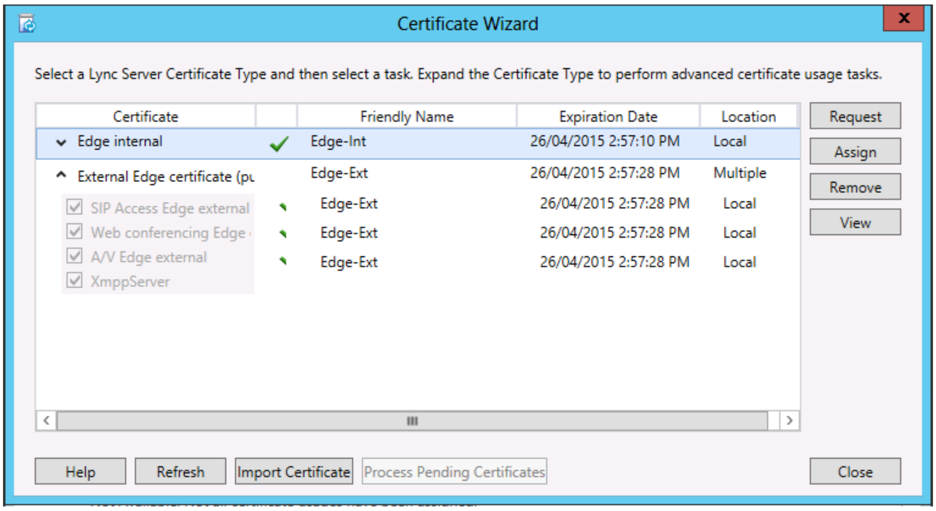
File name: ACSEdgeInt

Save as type: X.509 Certificate (*.cer; *.crt; *.der)

17.9.4.3 Install the Certificate on the CloudBond 365 Server

1. Copy the generated .cer file back to the CloudBond 365 system.
2. In the **Skype for Business Certificate Wizard**, select **Import Certificate** to import the just created Certificate file.

Figure 17-67: Certificate Wizard

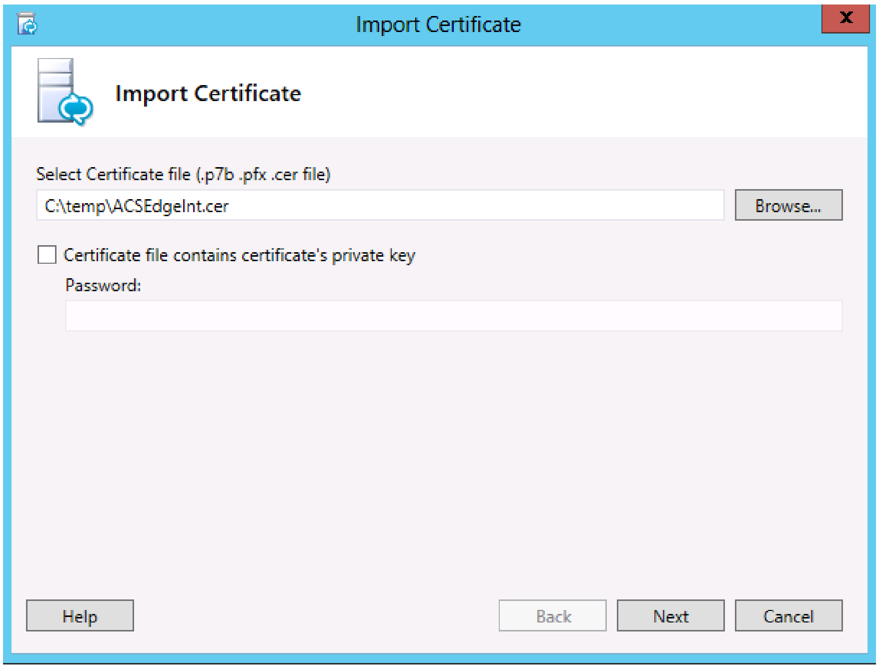


Select a Lync Server Certificate Type and then select a task. Expand the Certificate Type to perform advanced certificate usage tasks.

Certificate		Friendly Name	Expiration Date	Location
⌄ Edge internal	✓	Edge-Int	26/04/2015 2:57:10 PM	Local
^ External Edge certificate (pu		Edge-Ext	26/04/2015 2:57:28 PM	Multiple
☑ SIP Access Edge external	✓	Edge-Ext	26/04/2015 2:57:28 PM	Local
☑ Web conferencing Edge	✓	Edge-Ext	26/04/2015 2:57:28 PM	Local
☑ A/V Edge external	✓	Edge-Ext	26/04/2015 2:57:28 PM	Local
☑ XmppServer				

3. Specify the certificate file copied from the CA.

Figure 17-68: Import Certificate



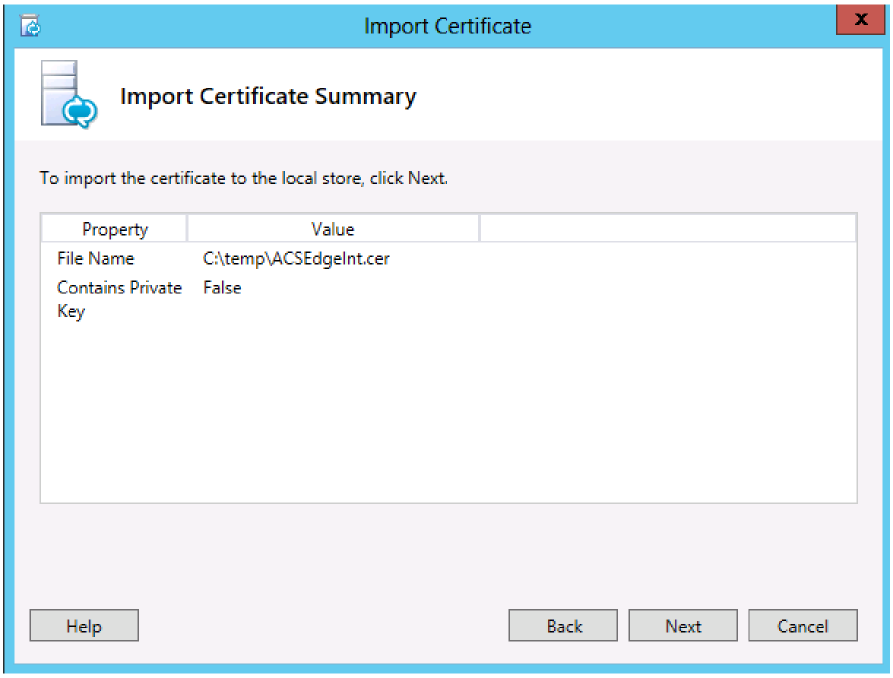
Select Certificate file (.p7b .pfx .cer file)

C:\temp\ACSEdgeInt.cer

☐ Certificate file contains certificate's private key

Password:

Figure 17-69: Import Certificate Summary

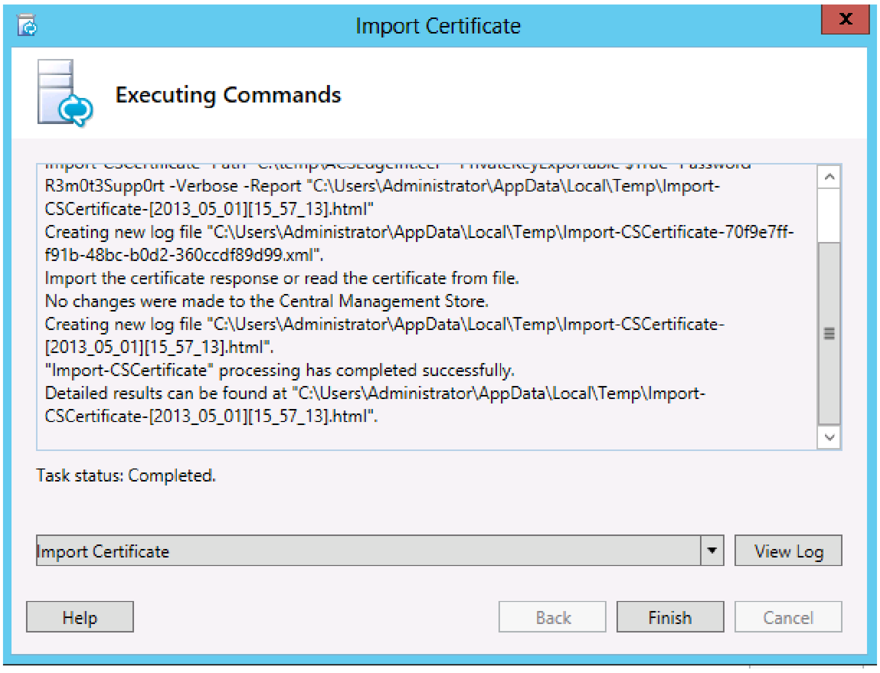


Import Certificate Summary

To import the certificate to the local store, click Next.

Property	Value	
File Name	C:\temp\ACSEdgeInt.cer	
Contains Private Key	False	

Figure 17-70: Executing Commands



Executing Commands

```
Import-CSCertificate -Path "C:\temp\ACSEdgeInt.cer" -PrivateKeyExportable $True -Password
R3m0t3Supp0rt -Verbose -Report "C:\Users\Administrator\AppData\Local\Temp\Import-
CSCertificate-[2013_05_01][15_57_13].html"
Creating new log file "C:\Users\Administrator\AppData\Local\Temp\Import-CSCertificate-70f9e7ff-
f91b-48bc-b0d2-360ccdf89d99.xml".
Import the certificate response or read the certificate from file.
No changes were made to the Central Management Store.
Creating new log file "C:\Users\Administrator\AppData\Local\Temp\Import-CSCertificate-
[2013_05_01][15_57_13].html".
"Import-CSCertificate" processing has completed successfully.
Detailed results can be found at "C:\Users\Administrator\AppData\Local\Temp\Import-
CSCertificate-[2013_05_01][15_57_13].html".
```

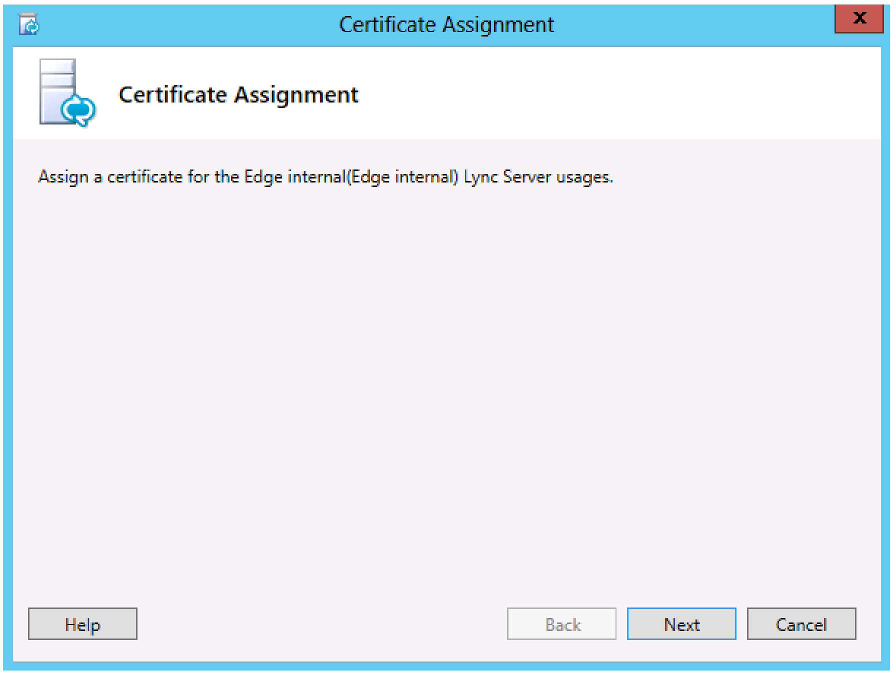
Task status: Completed.

17.9.4.4 Assign the Certificate to a Skype for Business Role

The imported certificate must now be assigned to a Skype for Business Role.

1. Once the certificate has been imported, highlight the Skype for Business role for the certificate (Edge Internal) then select **Assign**.

Figure 17-71: Certificate Assignment

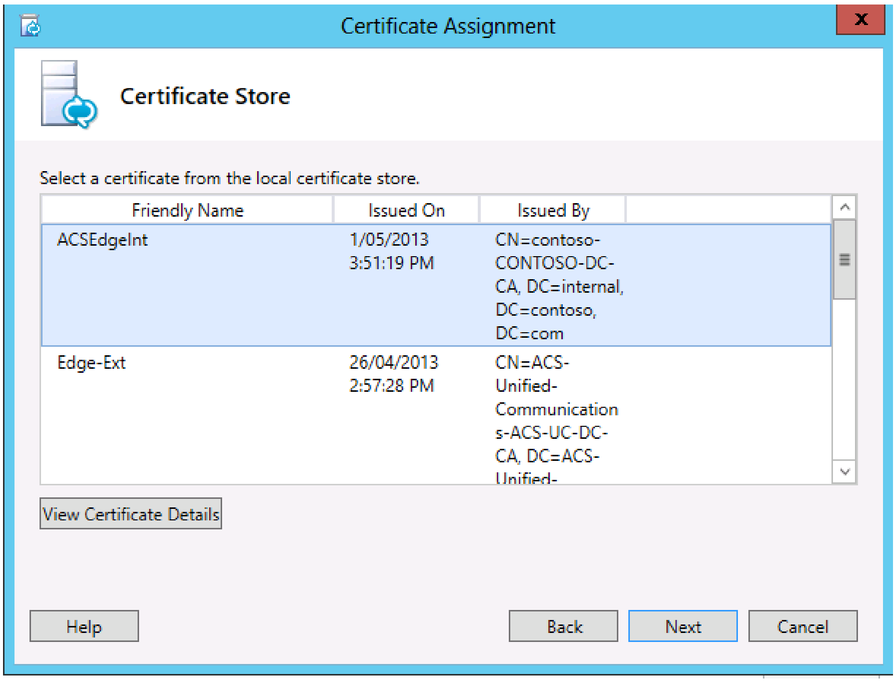


Certificate Assignment

Assign a certificate for the Edge internal(Edge internal) Lync Server usages.

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

Figure 17-72: Certificate Assignment – Certificate Store



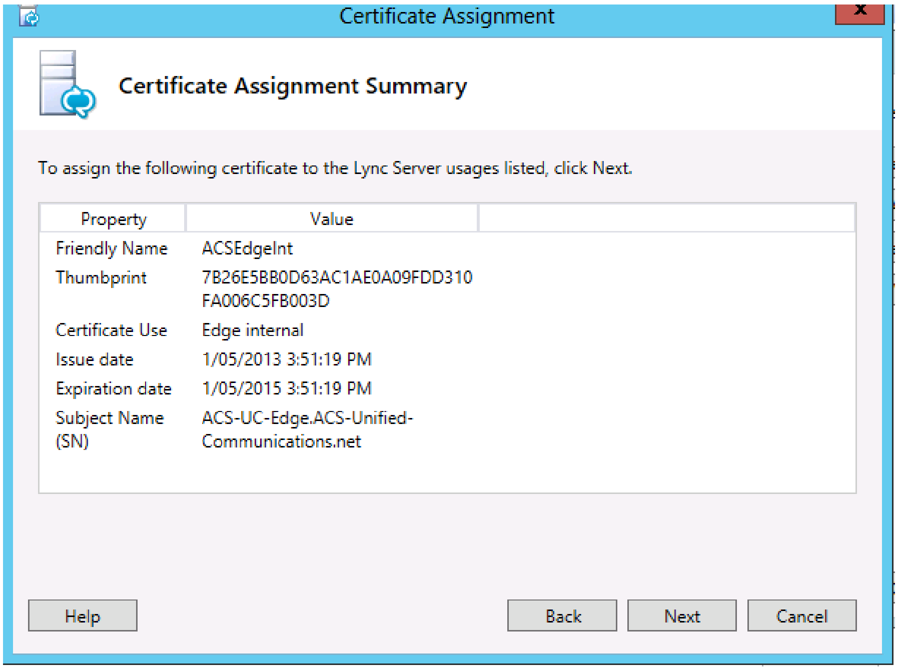
Certificate Store

Select a certificate from the local certificate 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-Communications-ACS-UC-DC-CA, DC=ACS-Unified-

If your certificate does not appear in the list, then the certificate is not suitable for assigning to the chosen roles.

Figure 17-73: Certificate Assignment Summary

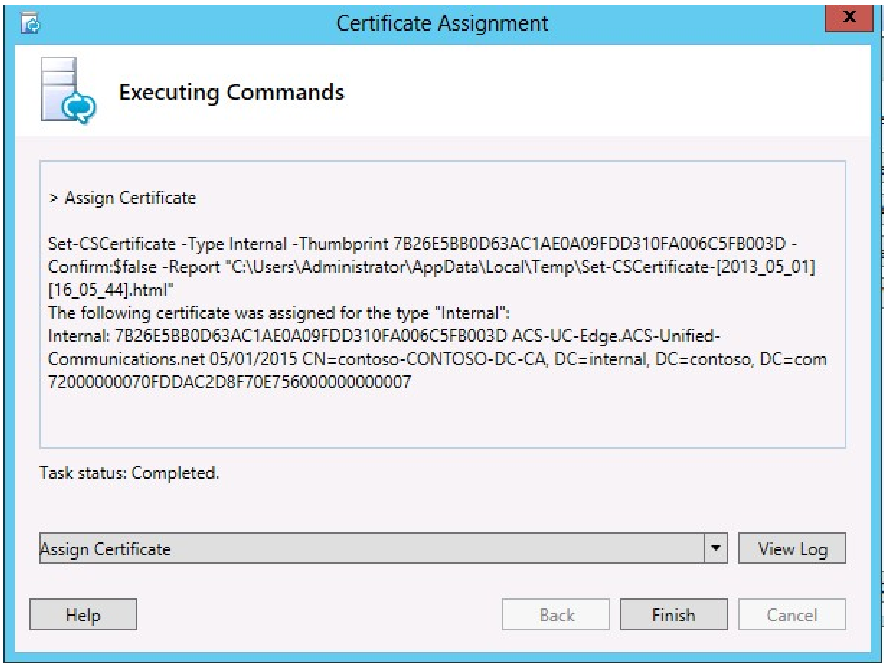


Certificate Assignment Summary

To assign the following certificate to the Lync Server usages listed, click Next.

Property	Value
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

Figure 17-74: Executing Commands



Executing Commands

```
> Assign Certificate

Set-CSCertificate -Type Internal -Thumbprint 7B26E5BB0D63AC1AE0A09FDD310FA006C5FB003D -
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: 7B26E5BB0D63AC1AE0A09FDD310FA006C5FB003D ACS-UC-Edge.ACS-Unified-
Communications.net 05/01/2015 CN=contoso-CONTOSO-DC-CA, DC=internal, DC=contoso, DC=com
72000000070FDDAC2D8F70E756000000000007
```

Task status: Completed.

3. Click **Close** to close the certificate wizard, followed by **exit** to close the deployment wizard.
4. 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.

17.10 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.

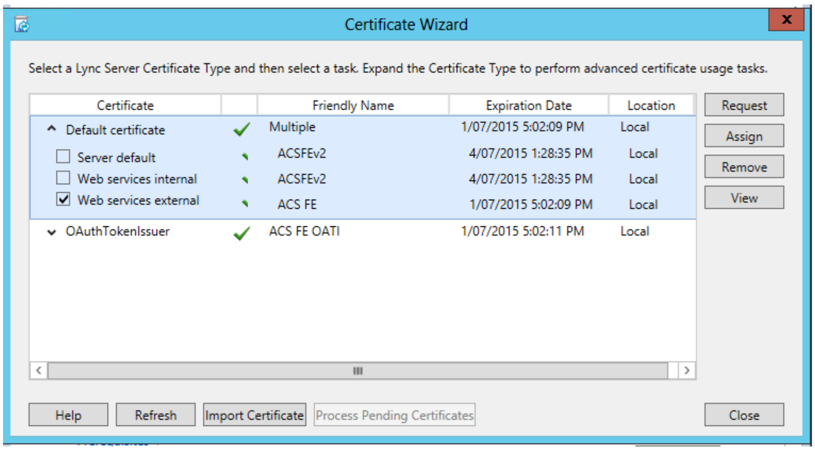
The certificate wizard must be run on both FE and Edge servers, and will create two separate certificate requests, one for each of the servers.

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 17-75: Front-End certificate for External (Public) use via Reverse Proxy

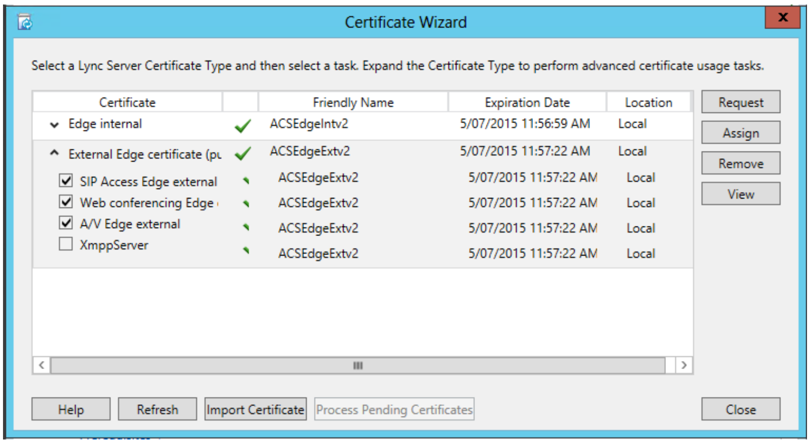


Certificate Wizard

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
^ Default certificate	✓	Multiple	1/07/2015 5:02:09 PM	Local
□ Server default		ACSFEv2	4/07/2015 1:28:35 PM	Local
□ Web services internal		ACSFEv2	4/07/2015 1:28:35 PM	Local
☑ Web services external		ACS FE	1/07/2015 5:02:09 PM	Local
⌄ OAuthTokenIssuer	✓	ACS FE OATI	1/07/2015 5:02:11 PM	Local

Figure 17-76: Edge Certificate for External (public) use



Certificate Wizard

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
⌄ Edge internal	✓	ACSEdgeIntv2	5/07/2015 11:56:59 AM	Local
^ External Edge certificate (pu	✓	ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local
☑ SIP Access Edge external		ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local
☑ Web conferencing Edge		ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local
☑ A/V Edge external		ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local
□ XmppServer		ACSEdgeExtv2	5/07/2015 11:57:22 AM	Local

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.

17.11 Certificate Summary

Update: Public certificate authorities will no longer issue public certificates valid from 1 Nov 2015, which contain private DNS name spaces or reserved IP address ranges. Additionally, any name or IP address entered in the Subject common name field must also appear as an entry in the Subject Alternate Name (SAN) list. The intent is to depreciate the Subject common name at some point in future.

The certificates listed in the following table are required to support the edge topology shown in the Single Consolidated Edge Topology figure.

There are three certificates shown for the reverse proxy server to highlight the certificate requirements for dedicated simple URLs (for example, https://dial-in.contoso.com).

For deployments that have a single pool or where multiple pools share the same dial-in conferencing and meeting simple URLs, you could create a single publishing rule and corresponding certificate.

For example, URLs defined in topology builder as lync.contoso.com/dialin and lync.contoso.com/meet could share a single publishing rule and certificate with a subject name of lync.contoso.com.

Note: The following table shows a second SIP entry in the subject alternative name list for reference. For each SIP domain in your organization, you need a corresponding FQDN listed in the certificate subject alternative name list.

Table 17-1: Certificates Required for Single Consolidated Edge Topology

Component	Subject Name	Subject Alternative Name Entries/Order	Certification Authority (CA)	Enhanced key usage (EKU)	Comments
Single consolidated Edge	access.contoso.com	webcon.contoso.com sip.contoso.com sip.fabrikam.com	Public	Server*	Assign to the following Edge Server roles: External interface: SIP Access Edge Web Conferencing Edge A/V Edge

Component	Subject Name	Subject Alternative Name Entries/Order	Certification Authority (CA)	Enhanced key usage (EKU)	Comments
Single consolidated Edge	lsedge.contoso.net	N/A	Private	Server	Assign to the following Edge Server roles: **Internal interface:** Edge
Single consolidated Edge	lsedge.contoso.net	N/A	Private	Server	Assign to the following Edge Server roles: **Internal interface:** Edge
Reverse proxy	lsrp.contoso.com	lswebext.contoso.com dialin.contoso.com meet.contoso.com	Public	Server	Address Book Service, distribution group expansion and Skype for Business IP Device publishing rules. Subject alternative name includes: External Web Services FQDN
					Dial-in conferencing Online meeting publishing rule
Next hop pool (on Front End)	fe01.contoso.net (on Front End)	sip.contoso.com sip.fabrikam.com lsweb.contoso.net lswebext.contoso.com admin.contoso.com dialin.contoso.com meet.contoso.com fe01.contoso.net	Private	Server	Assign to the following servers and roles in the next hop pool: Front End 01

Note: Client EKU is required if public internet connectivity with AOL isenabled.

17.12 Setting Up a Certificate Authority

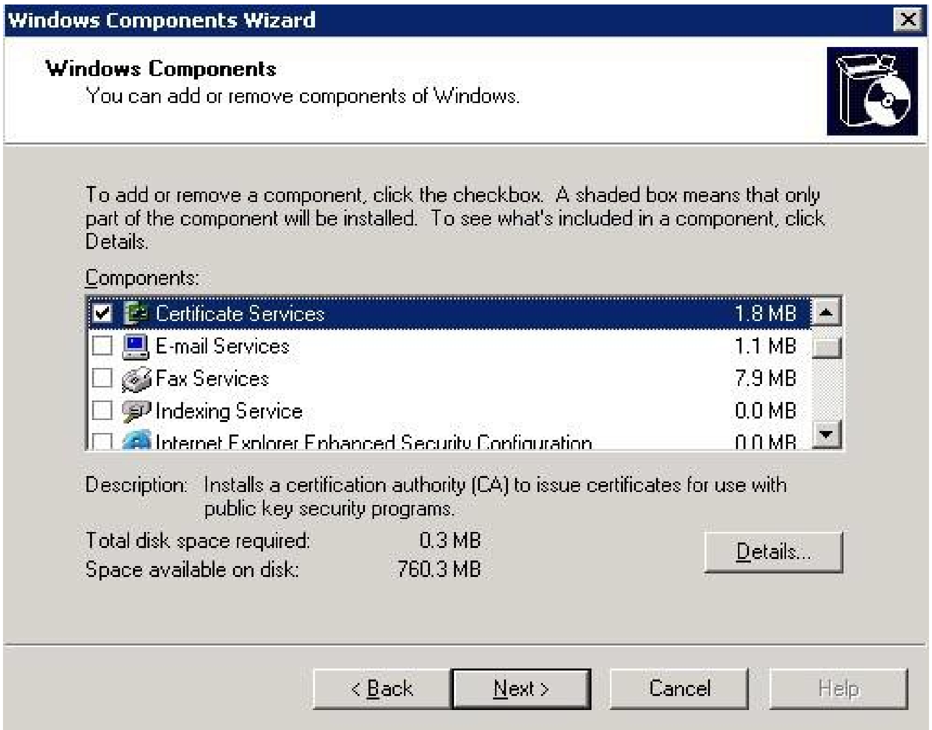
This section describes how to setup a certificate authority.

17.12.1 Setting Up a Certificate Authority on Windows Server 2003

To set up a Certificate Authority on a Microsoft Windows Server 2003 edition, perform the following steps:

1. Open **Add or Remove Programs** in Windows Control Panel.
2. Select **Add/Remove Windows components**.
3. Select **Certificate Services**.

Figure 17-77: Windows Components



Windows Components Wizard

Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

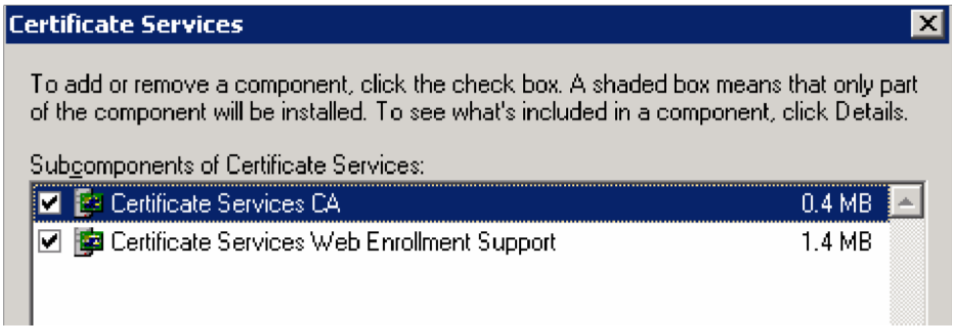
☑	Certificate Services	1.8 MB
□	E-mail Services	1.1 MB
□	Fax Services	7.9 MB
□	Indexing Service	0.0 MB
□	Internet Explorer Enhanced Security Configuration	0.0 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 0.3 MB
Space available on disk: 760.3 MB

4. Click **Details** and make sure that both the Certificate Services CA and the Certificate Services Web Enrollment Support are enabled.

Figure 17-78: Certificate Services



Certificate Services

To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Certificate Services:

☑	Certificate Services CA	0.4 MB
☑	Certificate Services Web Enrollment Support	1.4 MB

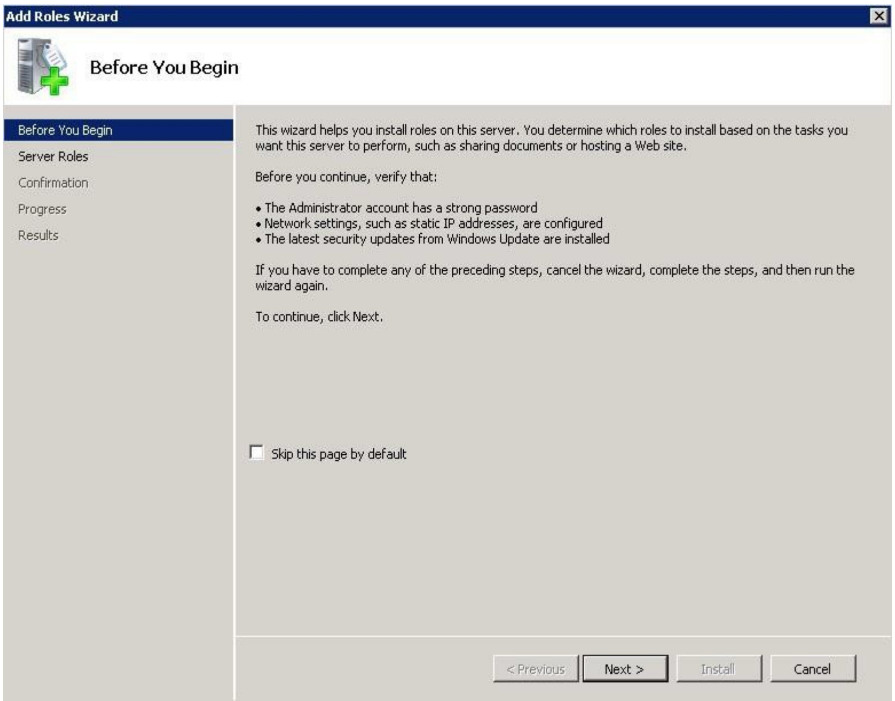
5. Click **OK** followed by **Next** to finish the installation.

17.12.2 Setting up a Certificate Authority on Windows server 2008

To set up a Certificate Authority on a Microsoft Windows server 2008 or 2008R2 edition, perform the following steps:

1. Open Server Manager through **Start** -> **All Programs** -> **Administrative Tools**.
2. Select **Roles**, then Add Roles in the right screen of the Roles Summary section.
3. Follow the screens as shown below:

Figure 17-79: Before You Begin



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

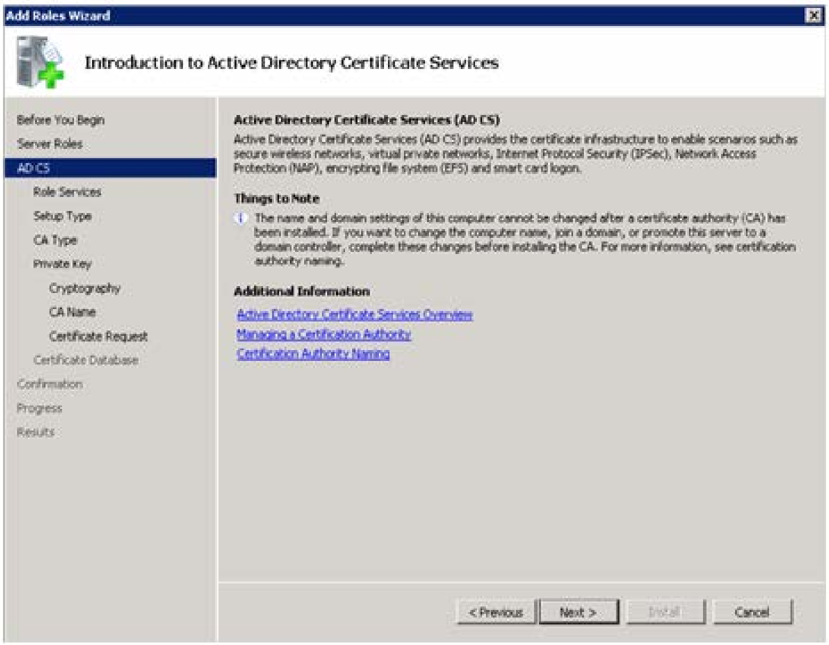
If you have to complete any of the preceding steps, cancel the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

4. Select **Active Directory Certificate Services**:

Figure 17-80: Introduction to Active Directory Certificate Services



Active Directory Certificate Services (AD CS)

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card logon.

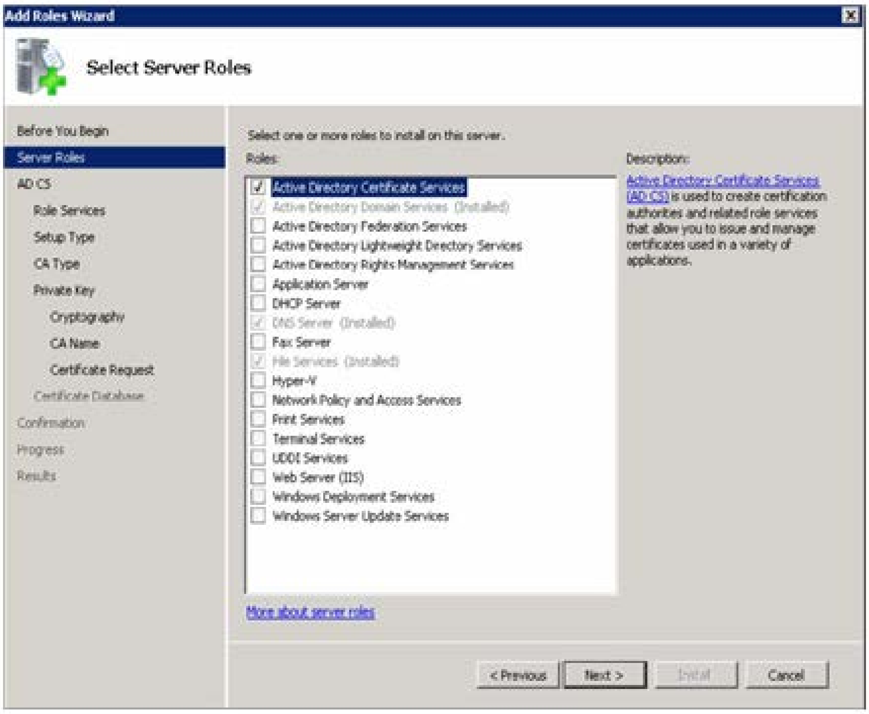
Things to Note

The name and domain settings of this computer cannot be changed after a certificate authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

Additional Information

Active Directory Certificate Services Overview
Managing a Certification Authority
Certification Authority Naming

Figure 17-81: Select Server Roles



Add Roles Wizard

Select Server Roles

Select one or more roles to install on this server.

Roles:

☑ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Application Server
□ DHCP Server
☑ DNS Server (Installed)
□ Fax Server
☑ File Services (Installed)
□ Hyper-V
□ Network Policy and Access Services
□ Print Services
□ Terminal Services
□ UDDI Services
□ Web Server (IIS)
□ Windows Deployment Services
□ Windows Server Update Services

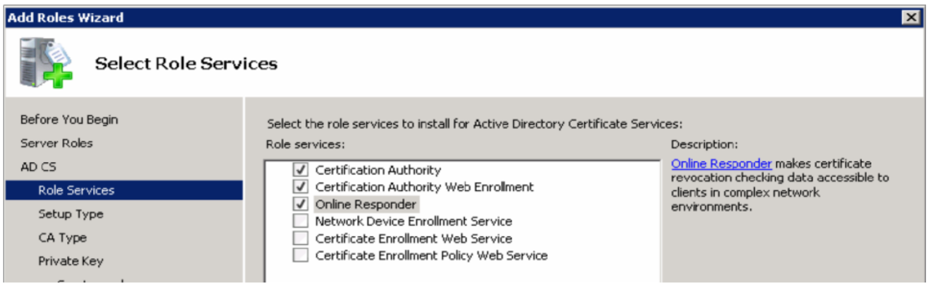
Description:

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

More about server roles

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

Figure 17-82: Select Role Services



Add Roles Wizard

Select Role Services

Select the role services to install for Active Directory Certificate Services:

Role services:

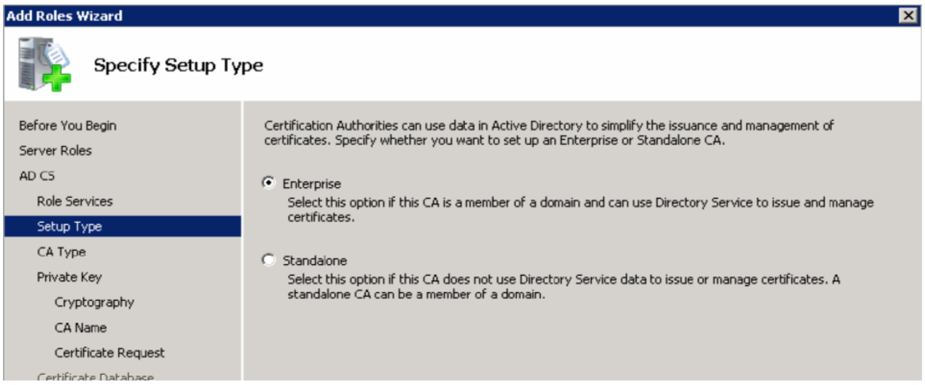
☑ Certification Authority
☑ Certification Authority Web Enrollment
☑ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

Description:

Online Responder makes certificate revocation checking data accessible to clients in complex network environments.

6. Select **Enterprise**.

Figure 17-83: Specify Setup Type



Add Roles Wizard

Specify Setup Type

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.

● Enterprise

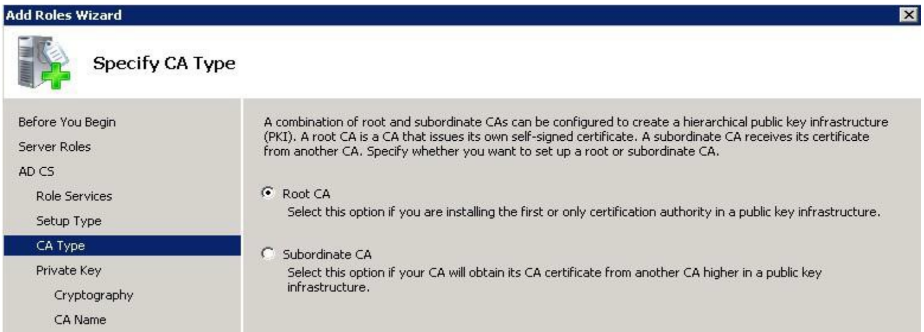
Select this option if this CA is a member of a domain and can use Directory Service to issue and manage certificates.

○ Standalone

Select this option if this CA does not use Directory Service data to issue or manage certificates. A standalone CA can be a member of a domain.

7. Select **Root CA**.

Figure 17-84: Specify CA Type



Specify CA Type

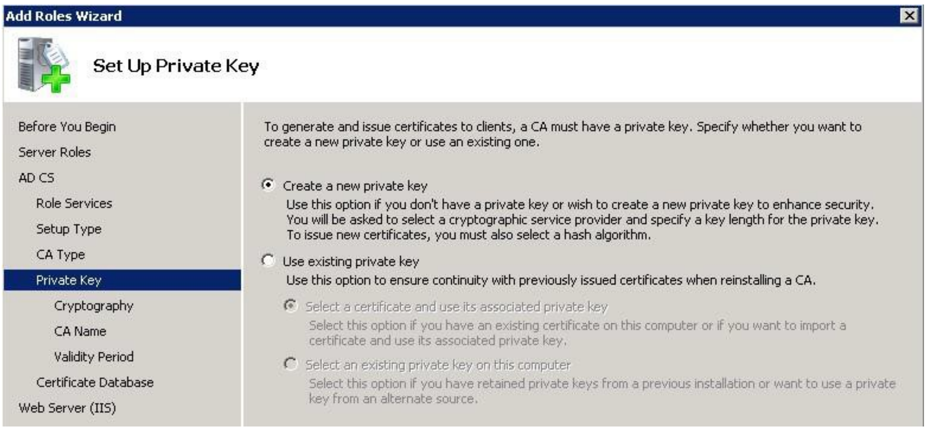
A combination of root and subordinate CAs can be configured to create a hierarchical public key infrastructure (PKI). A root CA is a CA that issues its own self-signed certificate. A subordinate CA receives its certificate from another CA. Specify whether you want to set up a root or subordinate CA.

● Root CA
Select this option if you are installing the first or only certification authority in a public key infrastructure.

○ Subordinate CA
Select this option if your CA will obtain its CA certificate from another CA higher in a public key infrastructure.

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

Figure 17-85: Set Up Private Key



Set Up Private Key

To generate and issue certificates to clients, a CA must have a private key. Specify whether you want to create a new private key or use an existing one.

● Create a new private key
Use this option if you don't have a private key or wish to create a new private key to enhance security. You will be asked to select a cryptographic service provider and specify a key length for the private key. To issue new certificates, you must also select a hash algorithm.

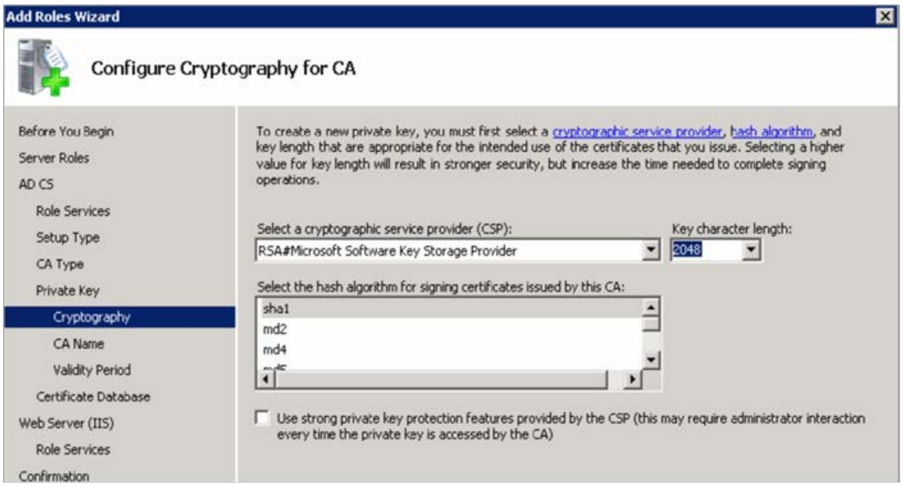
○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

● Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

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

Figure 17-86: Configure Cryptography for CA



Configure Cryptography for CA

To create a new private key, you must first select a cryptographic service provider, hash algorithm, and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher value for key length will result in stronger security, but increase the time needed to complete signing operations.

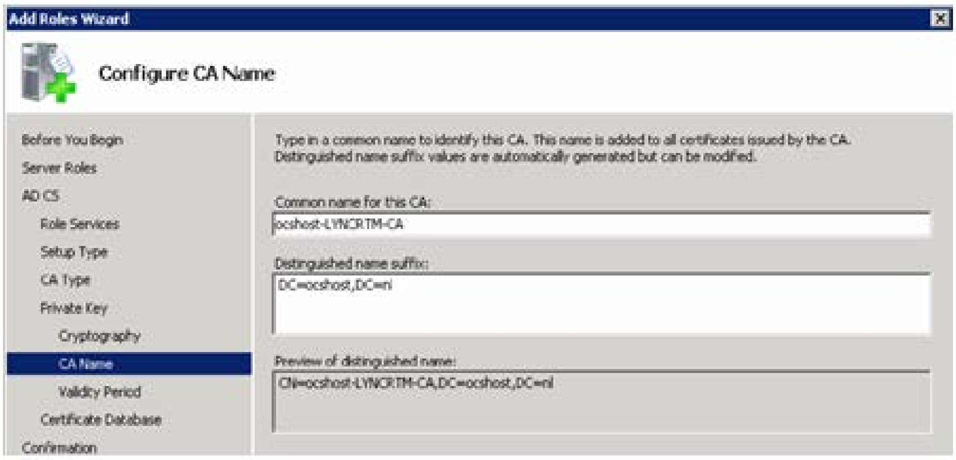
Select a cryptographic service provider (CSP): RSA#Microsoft Software Key Storage Provider

Key character length: 2048

Select the hash algorithm for signing certificates issued by this CA:
sha1
md2
md4
md5

□ Use strong private key protection features provided by the CSP (this may require administrator interaction every time the private key is accessed by the CA)

Figure 17-87: Configure CA Name



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.

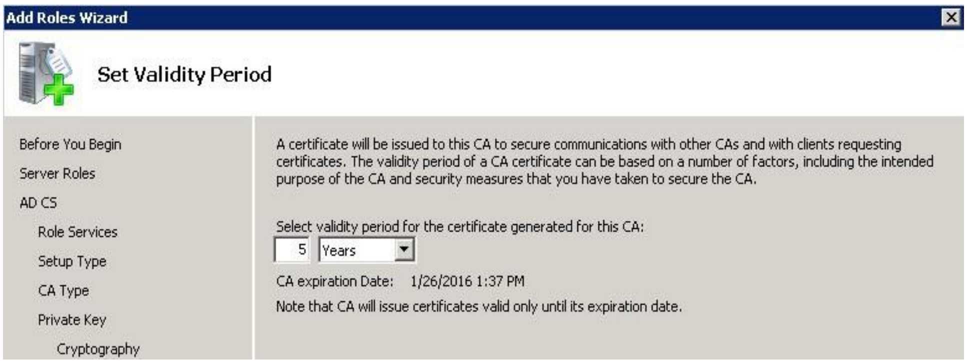
Common name for this CA: ocshost-LYNCRTM-CA

Distinguished name suffix: DC=ocshost,DC=nl

Preview of distinguished name: CN=ocshost-LYNCRTM-CA,DC=ocshost,DC=nl

10. Choose a Validity Period for the CA.

Figure 17-88: Set Validity Period



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.

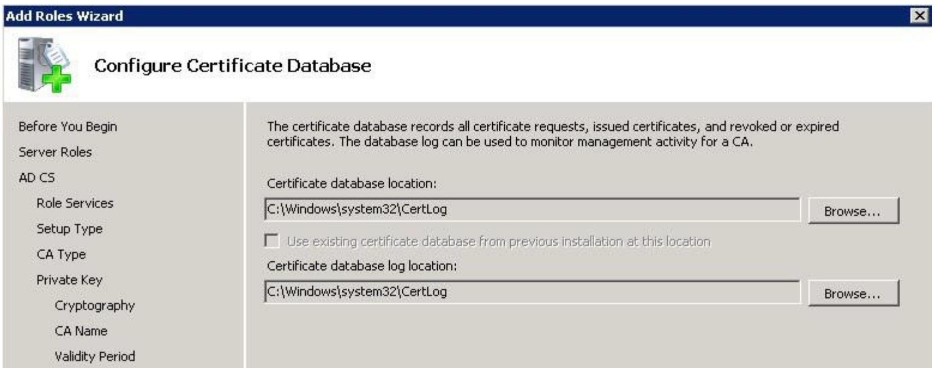
Select validity period for the certificate generated for this CA: 5 Years

CA expiration Date: 1/26/2016 1:37 PM

Note that CA will issue certificates valid only until its expiration date.

11. Stick with the default data location.

Figure 17-89: Configure Certificate Database



The certificate database records all certificate requests, issued certificates, and revoked or expired certificates. The database log can be used to monitor management activity for a CA.

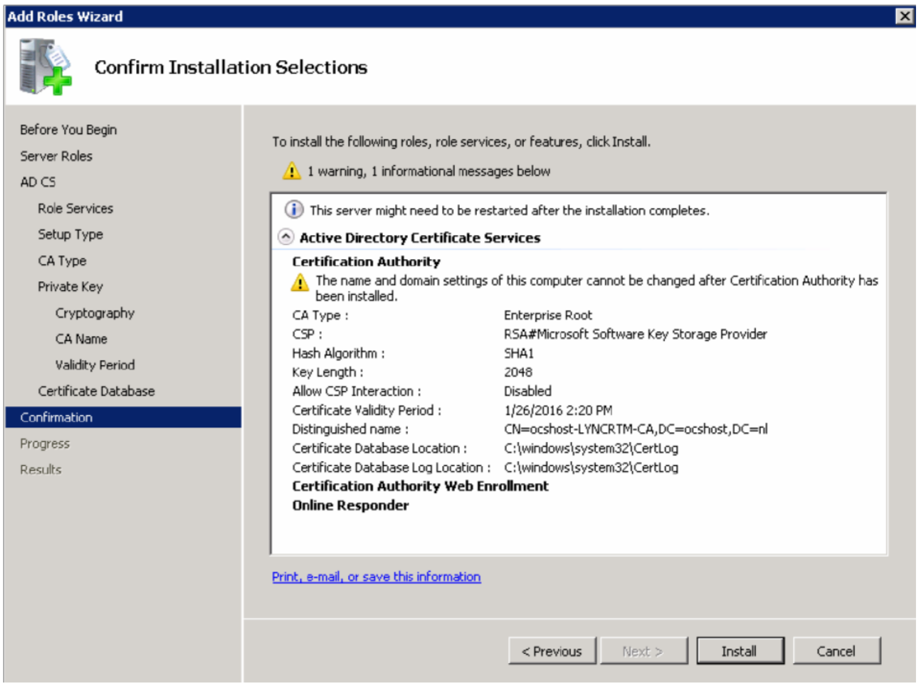
Certificate database location: C:\Windows\system32\CertLog

□ Use existing certificate database from previous installation at this location

Certificate database log location: C:\Windows\system32\CertLog

12. If IIS roles are added by the Add Roles Wizard, accept those by clicking next and finish the Wizard by clicking Install on the Confirmation page.

Figure 17-90: Confirm Installation Selections



Add Roles Wizard

Confirm Installation Selections

To install the following roles, role services, or features, click Install.

1 warning, 1 informational messages below

This server might need to be restarted after the installation completes.

Active Directory Certificate Services

Certification Authority

The name and domain settings of this computer cannot be changed after Certification Authority has been installed.

CA Type : Enterprise Root
CSP : RSA#Microsoft Software Key Storage Provider
Hash Algorithm : SHA1
Key Length : 2048
Allow CSP Interaction : Disabled
Certificate Validity Period : 1/26/2016 2:20 PM
Distinguished name : CN=ocshost-LYNCRTM-CA,DC=ocshost,DC=nl
Certificate Database Location : C:\windows\system32\CertLog
Certificate Database Log Location : C:\windows\system32\CertLog

Certification Authority Web Enrollment

Online Responder

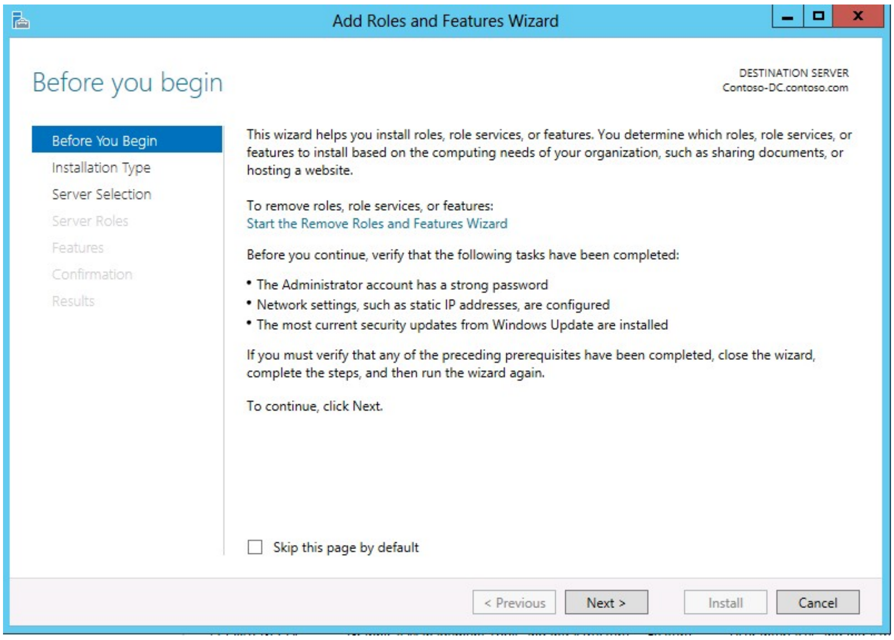
Print, e-mail, or save this information

17.12.3 Setting Up a Certificate Authority on Windows Server 2012

To set up a Certificate Authority on a Microsoft Windows server 2012, perform the following steps:

1. Open the Server Manager.
2. Select the Local Server.
3. Scroll down to **Roles and Features**.
4. Click **Tasks** -> Add Roles and Features
5. Follow the screens as shown below:

Figure 17-91: Add Roles and Features Wizard



Add Roles and Features Wizard

Before you begin

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:

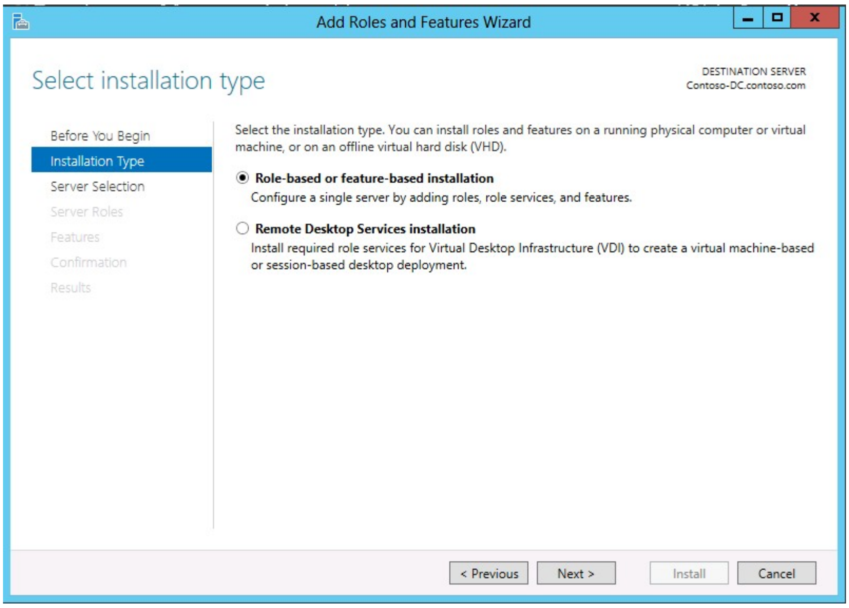
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Figure 17-92: Select Installation Type



Add Roles and Features Wizard

Select installation type

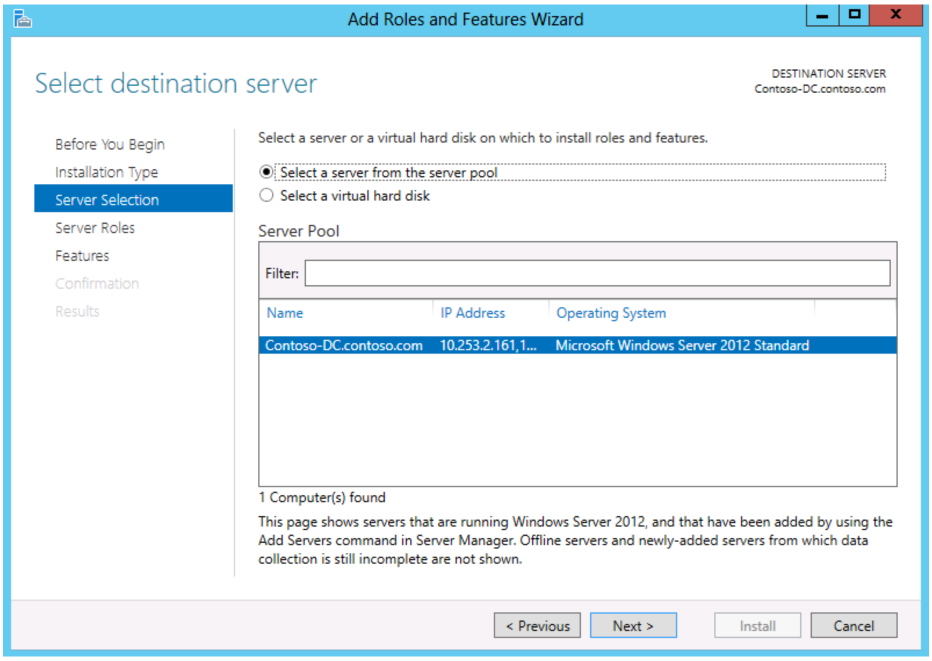
DESTINATION SERVER
Contoso-DC.contoso.com

Select the installation type. You can install roles and features on a running physical computer or virtual 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.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Figure 17-93: Select Destination Server



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
Contoso-DC.contoso.com

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 Pool

Filter:

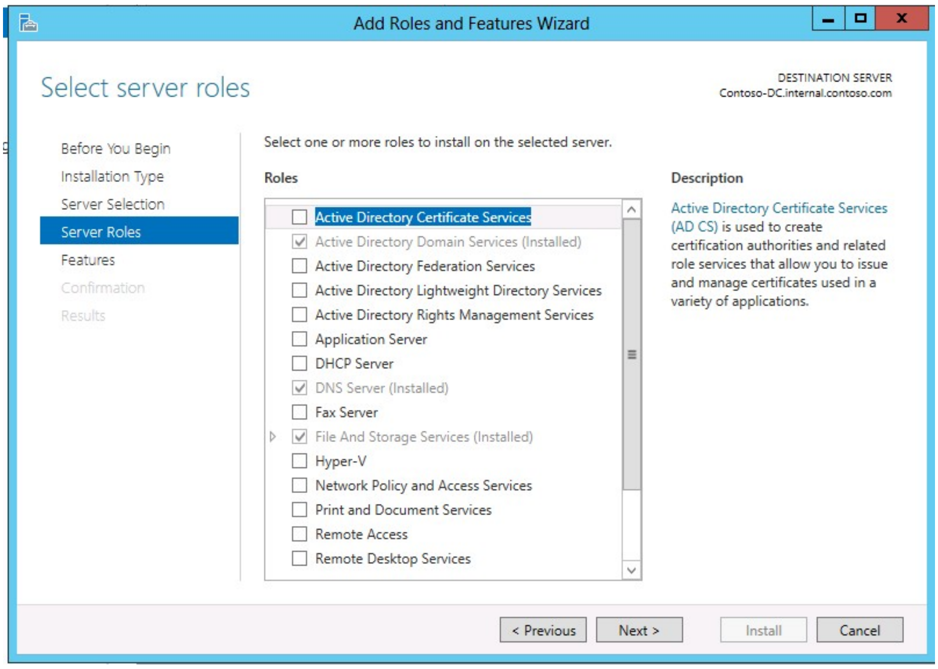
Name	IP Address	Operating System
Contoso-DC.contoso.com	10.253.2.161,1...	Microsoft Windows Server 2012 Standard

1 Computer(s) 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.

6. Select **Active Directory Certificate Services**:

Figure 17-94: Select Server Roles



Select server roles

DESTINATION SERVER
Contoso-DC.internal.contoso.com

Select one or more roles to install on the selected server.

Roles

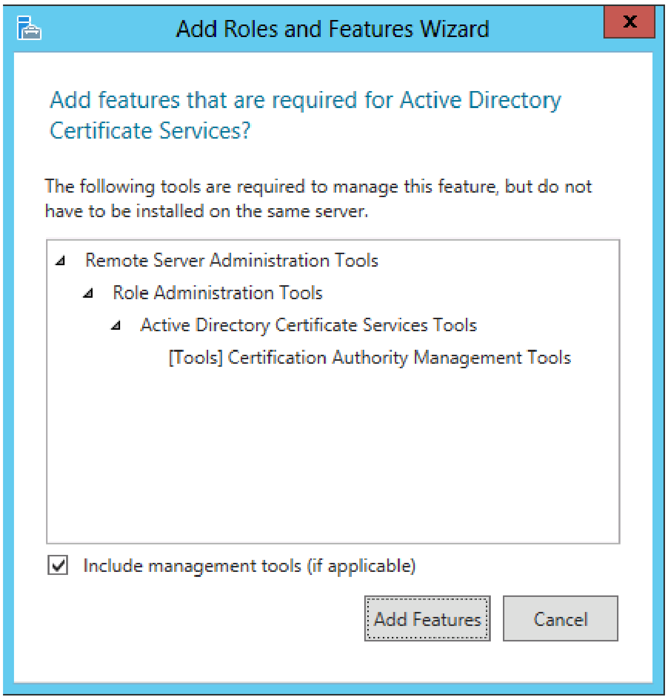
- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- ☑ DNS Server (Installed)
- □ Fax Server
- ☑ File And Storage Services (Installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

7. Click **Add Features**.

Figure 17-95: Add Features that are Required



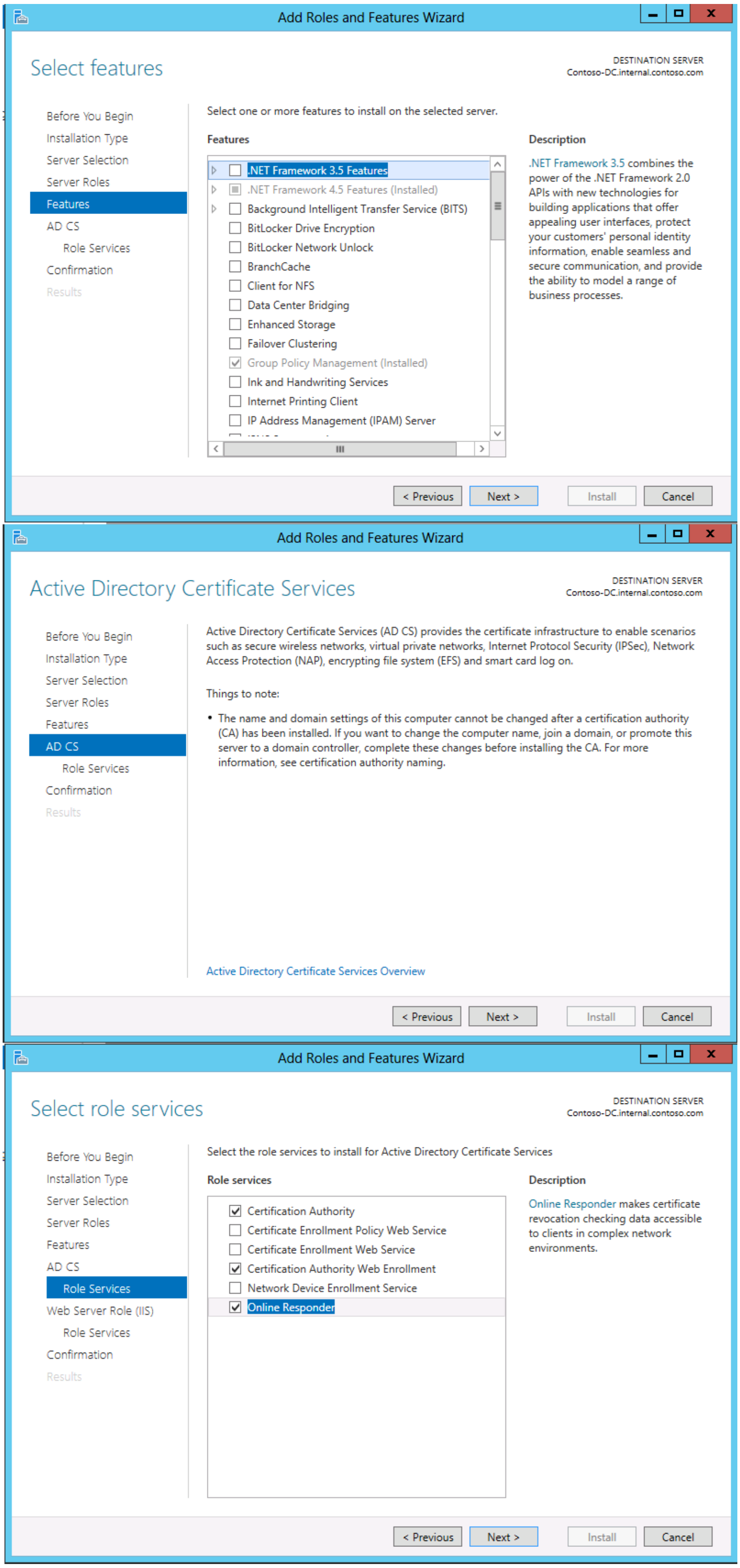
Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Certification Authority Management Tools

☑ Include management tools (if applicable)

Figure 17-96: Select Features



Select features

DESTINATION SERVER
Contoso-DC.internal.contoso.com

Select one or more features to install on the selected server.

Features

- □ .NET Framework 3.5 Features
- ▣ .NET Framework 4.5 Features (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Enhanced Storage
- □ Failover Clustering
- ☑ Group Policy Management (Installed)
- □ Ink and Handwriting Services
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Active Directory Certificate Services

DESTINATION SERVER
Contoso-DC.internal.contoso.com

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

Things to note:

- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

Active Directory Certificate Services Overview

Select role services

DESTINATION SERVER
Contoso-DC.internal.contoso.com

Select the role services to install for Active Directory Certificate Services

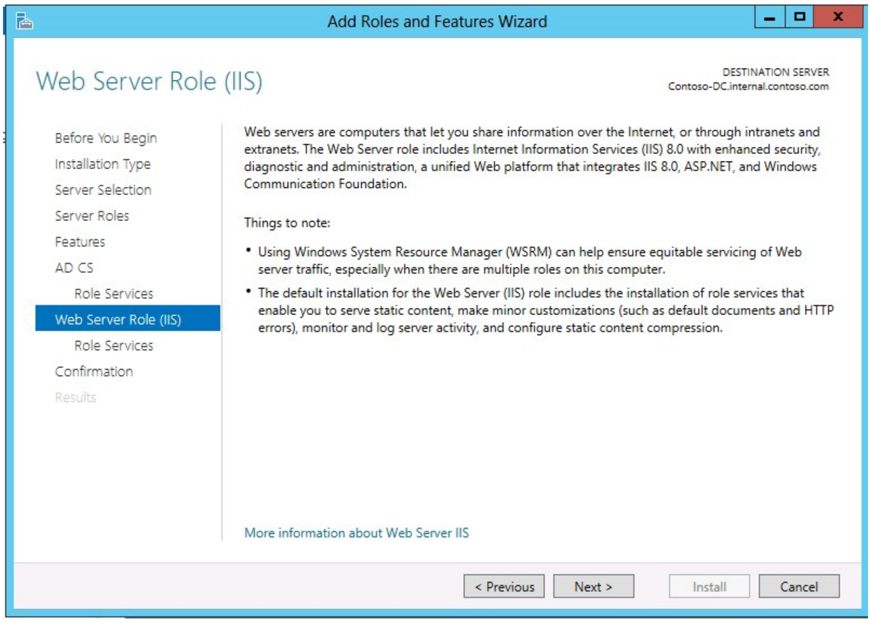
Role services

- ☑ Certification Authority
- □ Certificate Enrollment Policy Web Service
- □ Certificate Enrollment Web Service
- ☑ Certification Authority Web Enrollment
- □ Network Device Enrollment Service
- ☑ Online Responder

Description

Online Responder makes certificate revocation checking data accessible to clients in complex network environments.

Figure 17-97: Web Server Role (IIS)

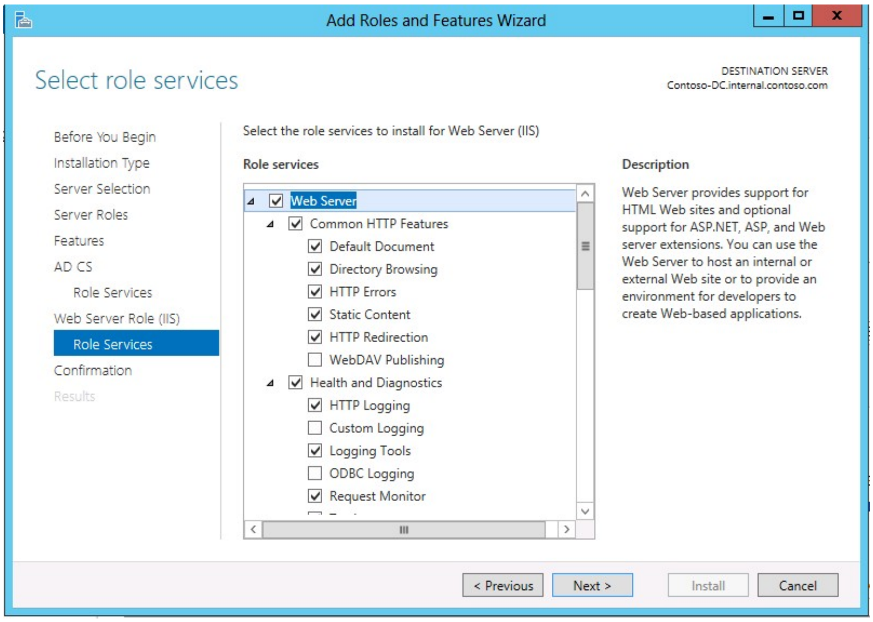


Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 8.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 8.0, ASP.NET, and Windows Communication Foundation.

Things to note:

- Using Windows System Resource Manager (WSRM) can help ensure equitable servicing of Web server traffic, especially when there are multiple roles on this computer.
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

Figure 17-98: Select Role Services



Select the role services to install for Web Server (IIS)

Role services

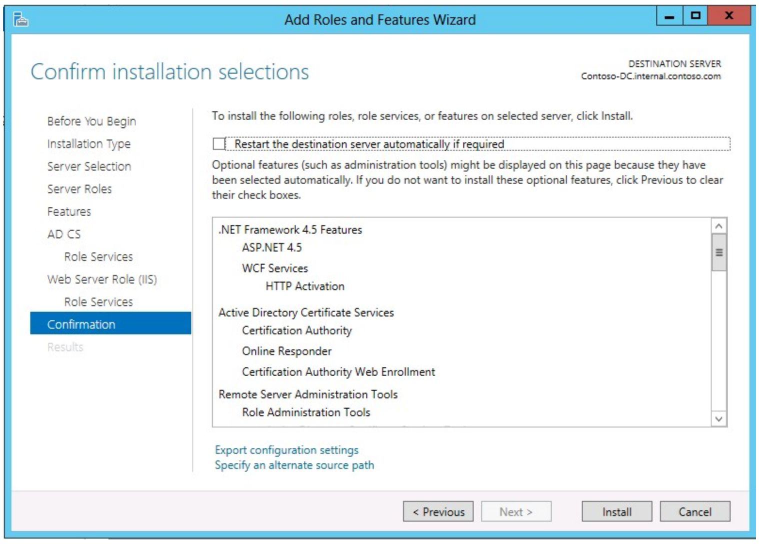
- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - ☑ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Custom Logging
    - ☑ Logging Tools
    - □ ODBC Logging
    - ☑ Request Monitor

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.

8. Click **Install** to complete the Wizard.

Figure 17-99: Confirm Installation Selection



Confirm installation selections

DESTINATION SERVER
Contoso-DC.internal.contoso.com

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

.NET Framework 4.5 Features
  ASP.NET 4.5
  WCF Services
    HTTP Activation
Active Directory Certificate Services
  Certification Authority
  Online Responder
  Certification Authority Web Enrollment
Remote Server Administration Tools
  Role Administration Tools

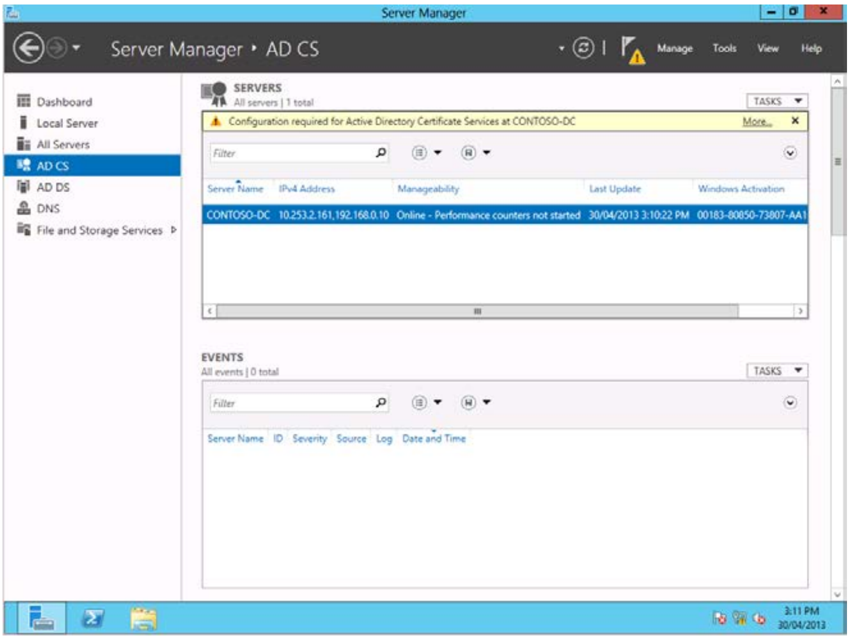
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

17.12.3.1 Configure the Certificate Services

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

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

Figure 17-100: Server Manager AD CS

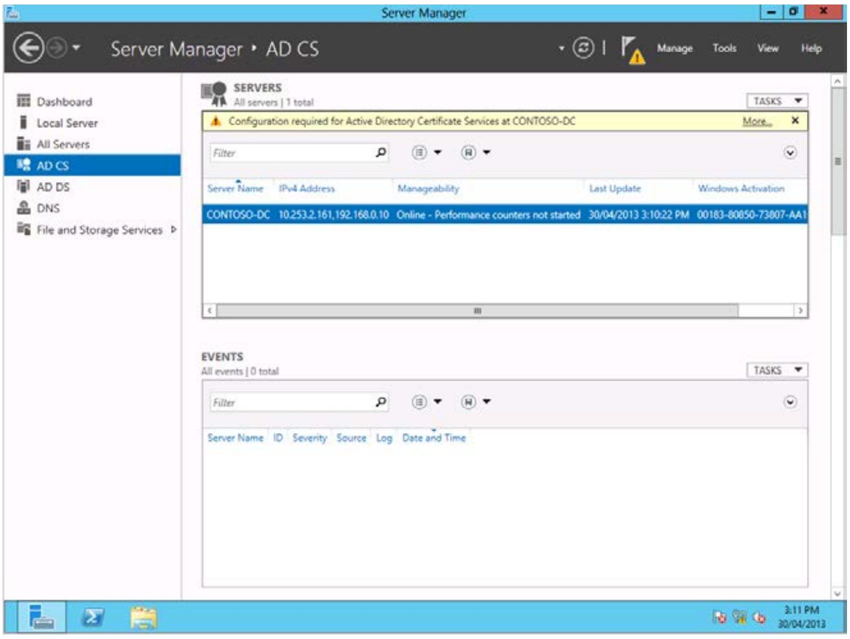


⚠ Configuration required for Active Directory Certificate Services at CONTOSO-DC More...

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
CONTOSO-DC	10.253.2.161,192.168.0.10	Online - Performance counters not started	30/04/2013 3:10:22 PM	00183-80850-73807-AA1

3. Click **Configure Active Directory Certificate Services…** in the action column

Figure 17-101: Server Manager AD CS - Servers

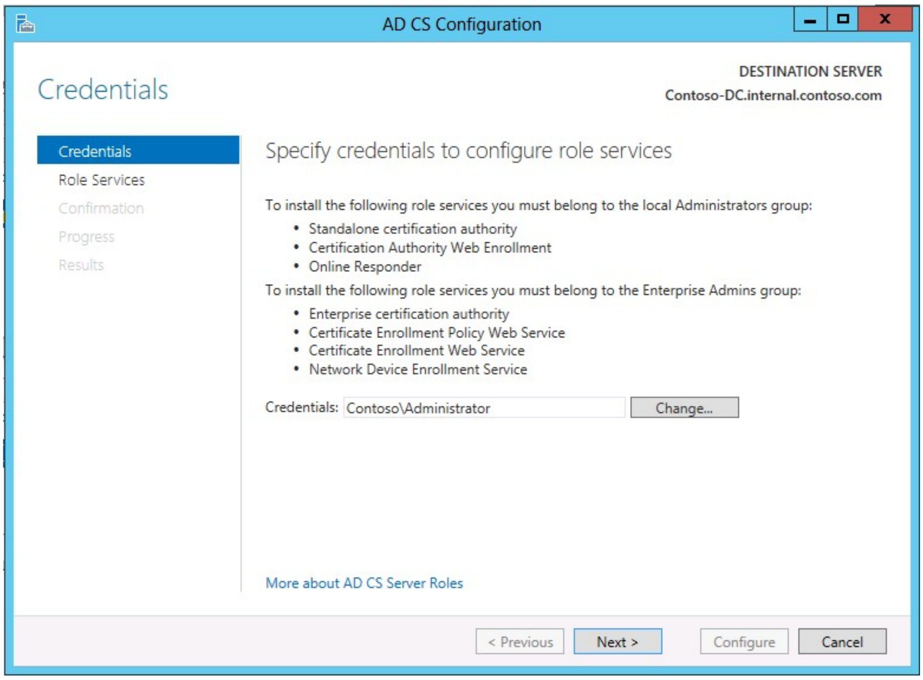


Configuration required for Active Directory Certificate Services at CONTOSO-DC More... ✕

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
CONTOSO-DC	10.253.2.161,192.168.0.10	Online - Performance counters not started	30/04/2013 3:10:22 PM	00183-80850-73807-AA1

4. Follow the screens.

Figure 17-102: AD CS Configuration - Credentials



DESTINATION SERVER
Contoso-DC.internal.contoso.com

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:

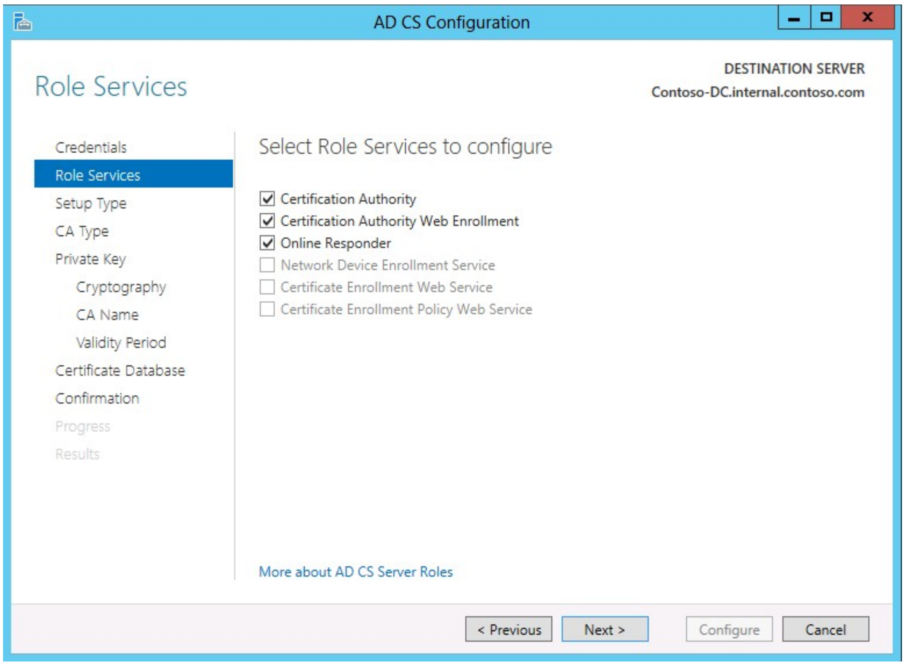
- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: Contoso\Administrator Change...

More about AD CS Server Roles

5. Select **Certification Authority**, **Web Enrollment**, and **Online Responder**.

Figure 17-103: AD CS Configuration – Role Services



AD CS Configuration

Role Services

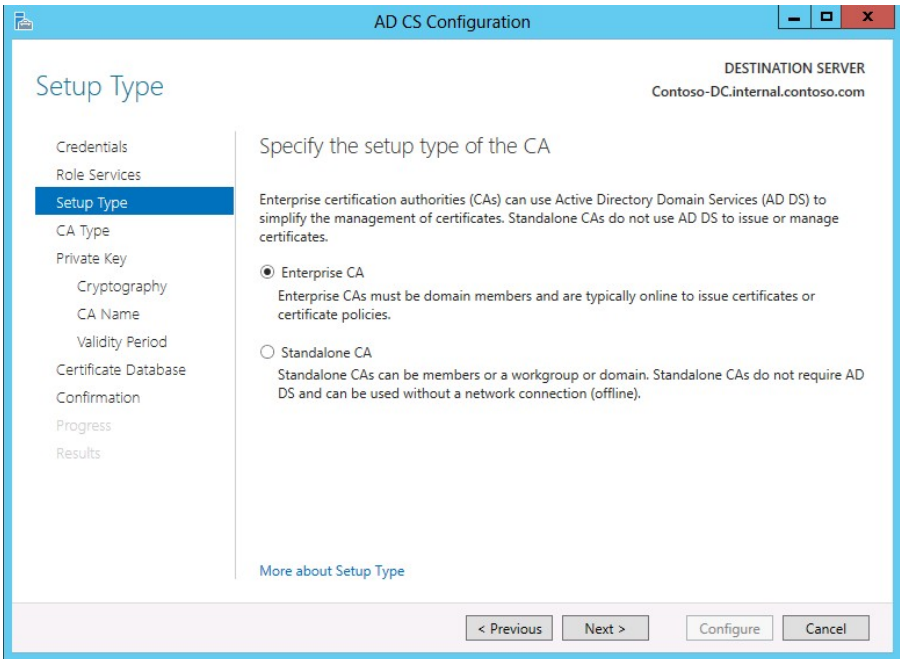
DESTINATION SERVER
Contoso-DC.internal.contoso.com

Select Role Services to configure

☑ Certification Authority
☑ Certification Authority Web Enrollment
☑ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

More about AD CS Server Roles

Figure 17-104: AD CS Configuration – Setup Type



AD CS Configuration

Setup Type

DESTINATION SERVER
Contoso-DC.internal.contoso.com

Specify the setup type of the CA

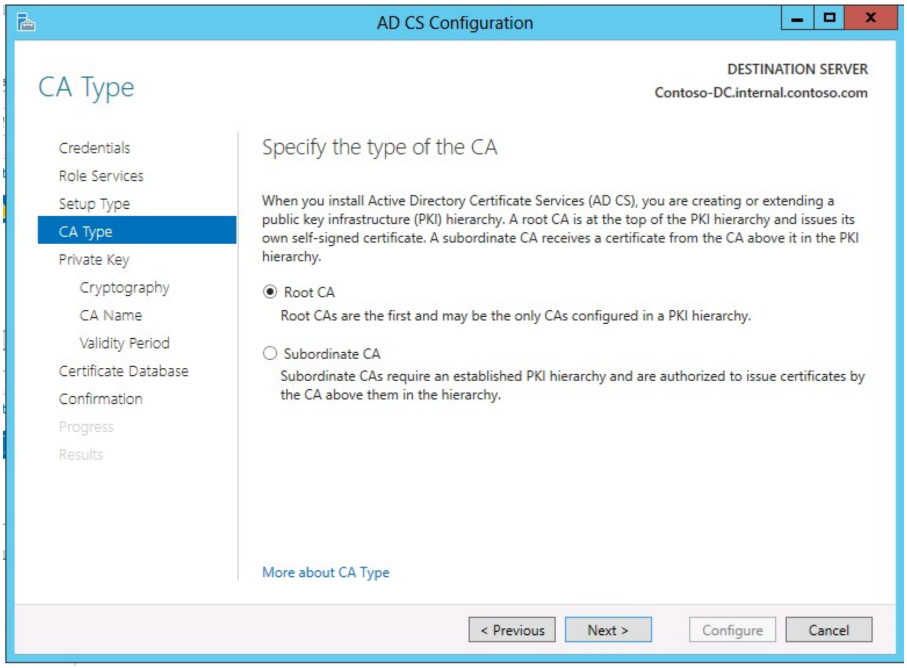
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ 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).

More about Setup Type

Figure 17-105: AD CS Configuration – CA Type



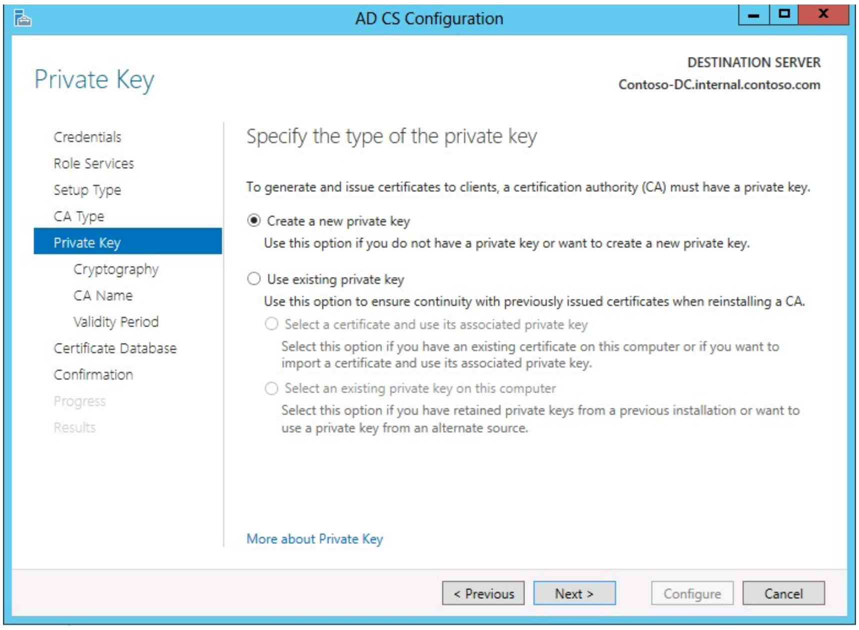
Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

Figure 17-106: AD CS Configuration – Private Key



Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

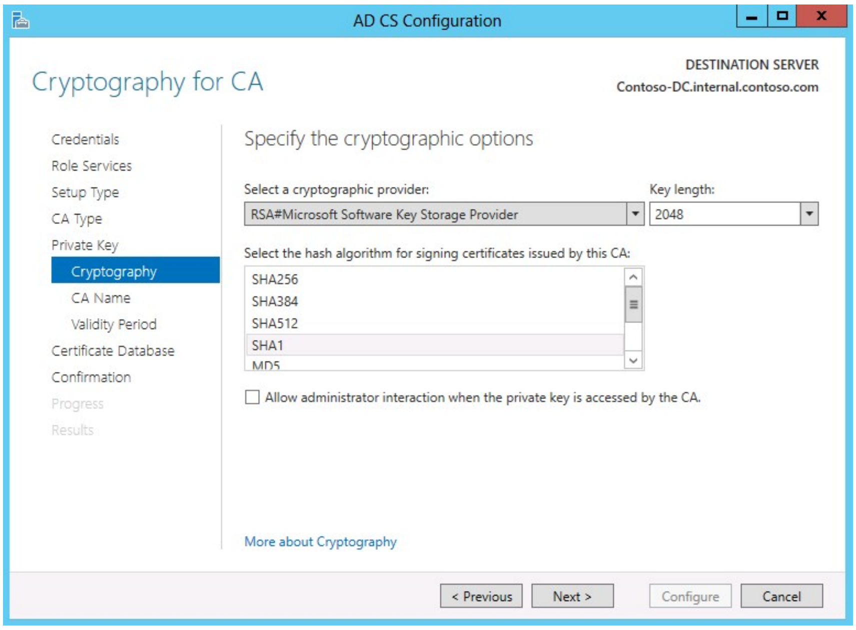
● Create a new private key
Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

Figure 17-107: AD CS Configuration – Cryptography for CA



Cryptography for CA

DESTINATION SERVER
Contoso-DC.internal.contoso.com

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

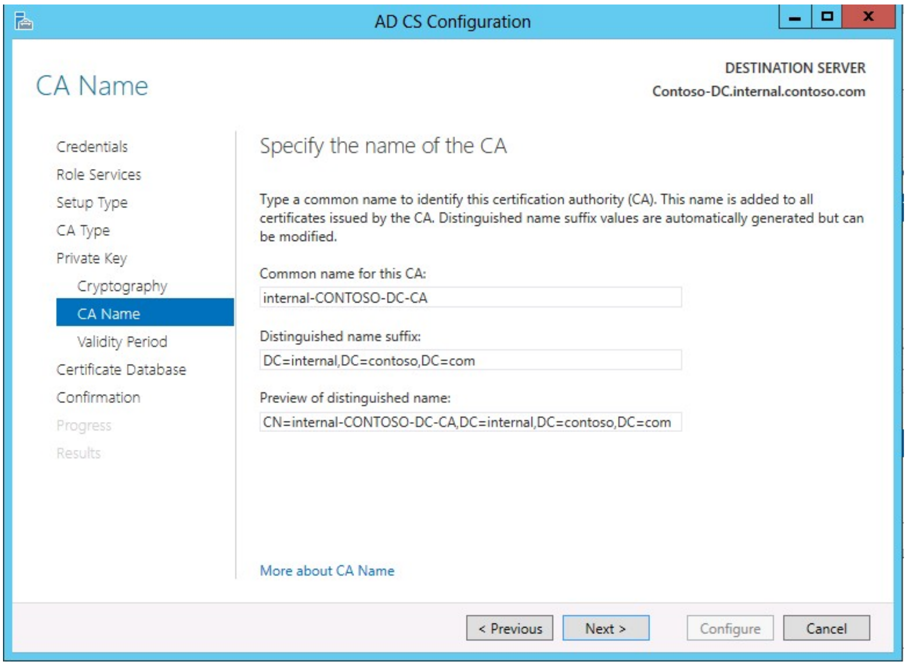
Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

□ Allow administrator interaction when the private key is accessed by the CA.

More about Cryptography

Figure 17-108: AD CS Configuration – CA Name



CA Name

DESTINATION SERVER
Contoso-DC.internal.contoso.com

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

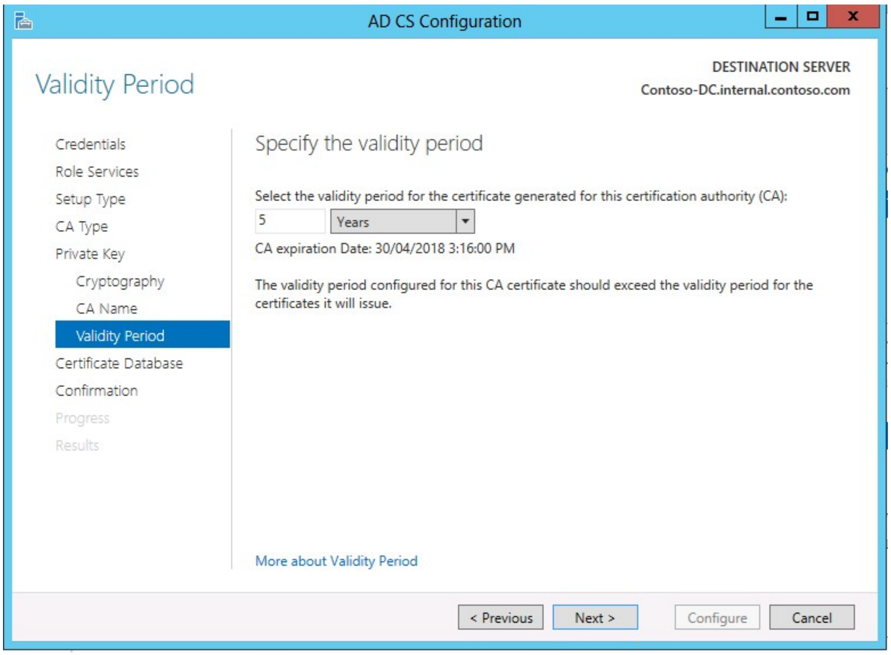
Common name for this CA: internal-CONTOSO-DC-CA

Distinguished name suffix: DC=internal,DC=contoso,DC=com

Preview of distinguished name: CN=internal-CONTOSO-DC-CA,DC=internal,DC=contoso,DC=com

More about CA Name

Figure 17-109: AD CS Configuration – Validity Period



Specify the validity period

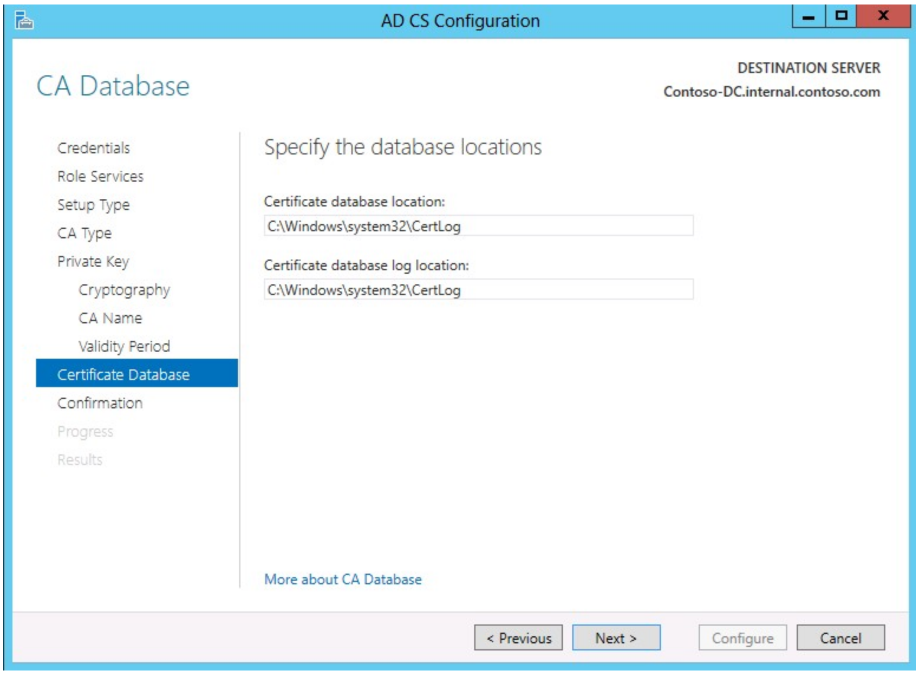
Select the validity period for the certificate generated for this certification authority (CA):

5 Years

CA expiration Date: 30/04/2018 3:16:00 PM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

Figure 17-110: AD CS Configuration – CA Database



Specify the database locations

Certificate database location:

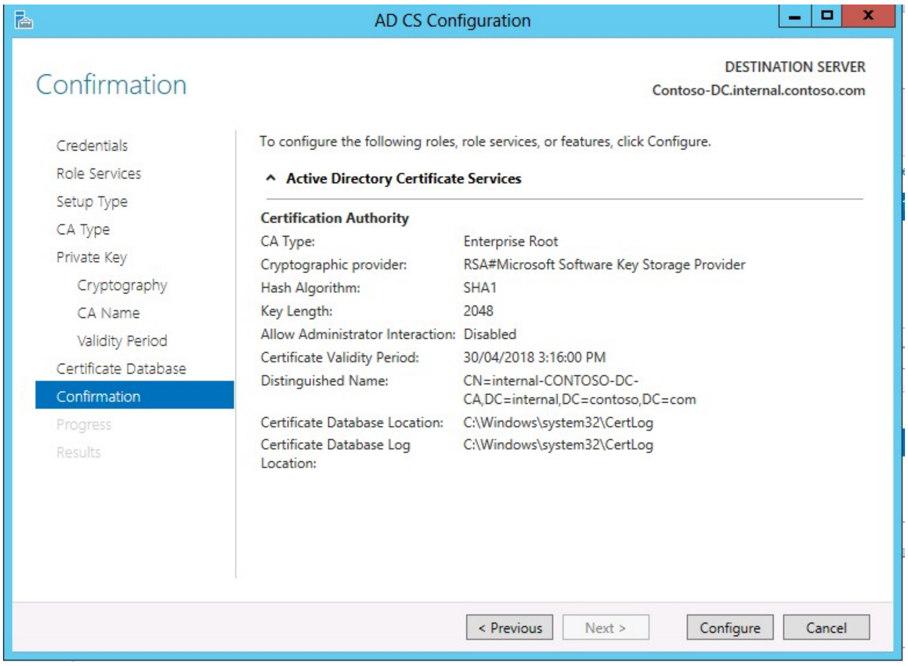
C:\Windows\system32\CertLog

Certificate database log location:

C:\Windows\system32\CertLog

6. Click **Configure** to complete the wizard.

Figure 17-111: AD CS Configuration - Confirmation



DESTINATION SERVER
Contoso-DC.internal.contoso.com

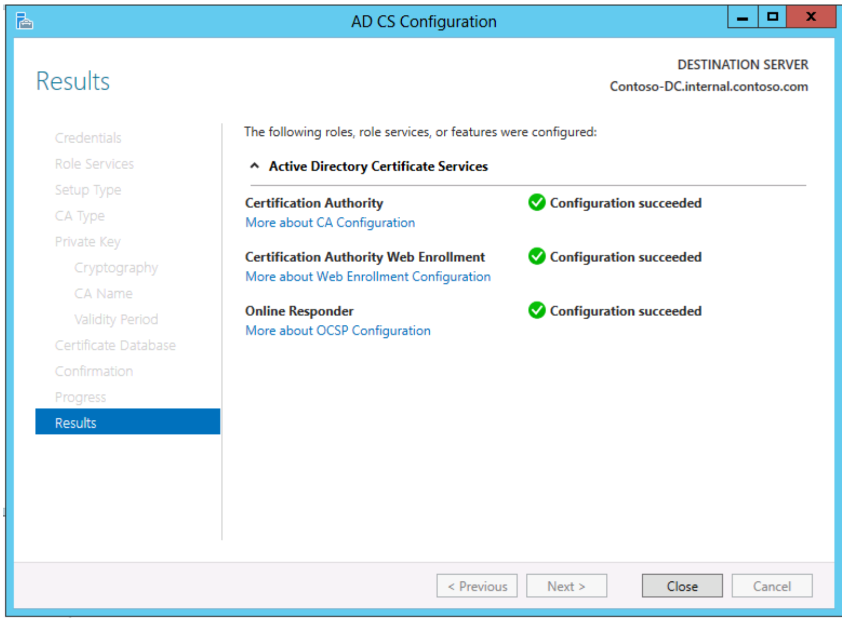
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA1
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	30/04/2018 3:16:00 PM
Distinguished Name:	CN=internal-CONTOSO-DC-CA,DC=internal,DC=contoso,DC=com
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Figure 17-112: AD CS Configuration - Results



DESTINATION SERVER
Contoso-DC.internal.contoso.com

The following roles, role services, or features were configured:

Active Directory Certificate Services

Certification Authority More about CA Configuration	✓ Configuration succeeded
Certification Authority Web Enrollment More about Web Enrollment Configuration	✓ Configuration succeeded
Online Responder More about OCSP Configuration	✓ Configuration succeeded

18 Configuring Exchange Enterprise UM

This section shows how to integrate CloudBond 365 within an Enterprise Exchange 2007 or 2010 Unified Messaging (UM) environment.

Though the steps required for Exchange Server 2013 are not different, Microsoft has significantly changed the Exchange Server 2013 Management Console. See https://technet.microsoft.com/en-us/library/bb676409(v=exchg.150).aspx for a step-by-step guide on deploying Exchange 2013 UM.

18.1 Overview

➢ **To integrate CloudBond 365, follow this procedure:**

1. Deploy Exchange Server 2010 SP1 in the enterprise forest as a consolidated server with the Unified Messaging role included.
2. Replace the self-signed certificate with one from an internal Windows Enterprise Certificate Authority and reassign all Exchange roles to it.
3. Create a new SIP Dial Plan in Exchange.
4. Configure the UM Dial Plan, Policy, and Auto Attendant settings.
5. Enable Unified Messaging on at least one mailbox.
6. Run the *exchucutil.ps1* PowerShell script on the Exchange server.
7. Configure Skype for Business Server Dial Plan or verify that the existing configuration is sufficient.
8. Run the *ocsumutil.exe* tool on the Skype for Business Server .

18.2 Configuration

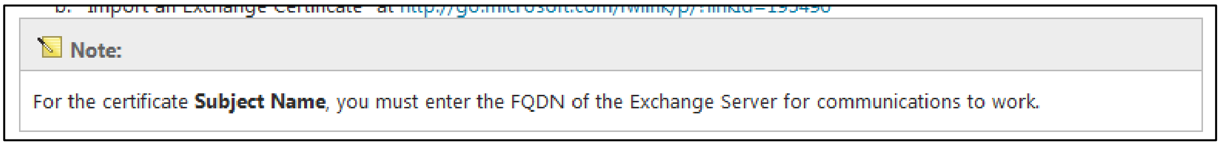
This section describes how to configure the Exchange Enterprise UM.

18.2.1 Deploy Exchange Server

Deploying Exchange Server 2010 SP1 is outside the scope of this *Deployment Guide* but there are many official and unofficial walkthroughs available online to help anyone unfamiliar with the Exchange Server deployment process. The best starting point is: http://technet.microsoft.com/en-us/library/dd351084.aspx.

18.2.2 Generate New Certificate

This step is a common Exchange deployment task and official instructions can be found at http://technet.microsoft.com/en-us/library/dd351057.aspx. Note that the statement 'You must use a public certificate if you are using Unified Messaging with Office Communications Server' is not entirely correct. It should state that a ‘trusted certificate’ is required, because a private certificate issued by an internal enterprise Windows CA can be used and will function flawlessly if both the Skype for Business and Exchange servers trust the same Certificate Authority. Also, make sure that the UM service is assigned to the new certificate after it is installed, and that the UM service is restarted.



b. Import an Exchange Certificate at http://go.microsoft.com/fwlink/p/?linkid=195490

Note:

For the certificate **Subject Name**, you must enter the FQDN of the Exchange Server for communications to work.

See http://technet.microsoft.com/en-au/library/gg398564.aspx for more information.

When collocating the UM role on a consolidated Exchange Server, the easiest configuration is to use a single SAN certificate for all Exchanges services with the server's FQDN set as the *Subject Name* with any other required names added to the *Subject Alternative Names* field.

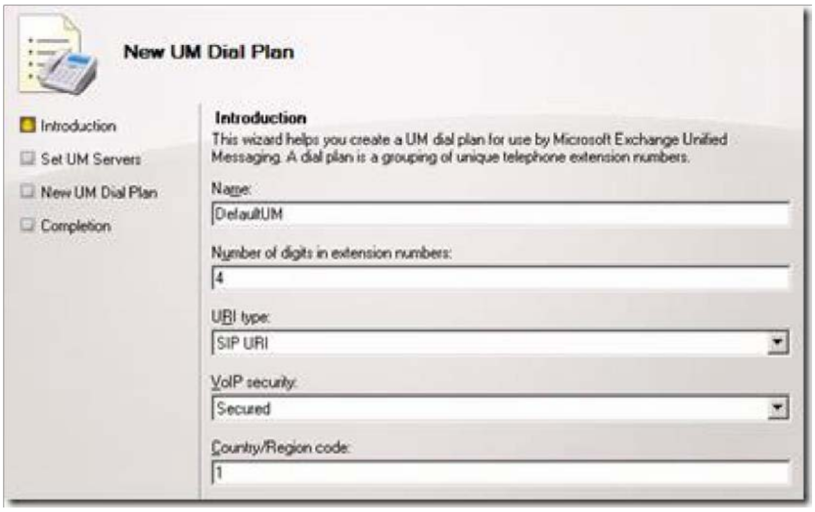
18.2.3 Create an Exchange UM Dial Plan

You need to create an Exchange UM Dial Plan.

➢ **To create an Exchange UM Dial Plan:**

1. In the Exchange Management Console, navigate to the **UM Dial Plans** tab under **Organization Configuration** > **Unified Messaging**.
2. Create a new UM Dial Plan with any **Name** you like (e.g., **DefaultUM**), and any valid **PIN length** (e.g. **4**). The dropdown 'URI Type' must be set to **SIP URI** and 'VOIP Security' must be set to **Secured**. 'Country/Region Code' in the example below is set to **1** (the North American dialing plan).

Figure 18-1: New UM Dial Plan



New UM Dial Plan

Introduction

This wizard helps you create a UM dial plan for use by Microsoft Exchange Unified Messaging. A dial plan is a grouping of unique telephone extension numbers.

Name: DefaultUM

Number of digits in extension numbers: 4

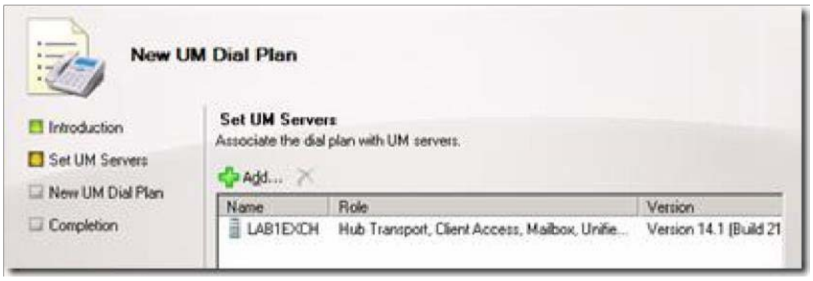
URI type: SIP URI

VoIP security: Secured

Country/Region code: 1

3. In Exchange Server 2010 the wizard prompts which UM server to associate with the new dial plan. If Exchange Server 2007 is deployed, this step must be performed afterwards manually.
4. Select the consolidated Exchange server running the UM role, and then complete the wizard.

Figure 18-2: Complete Wizard



New UM Dial Plan

Set UM Servers

Associate the dial plan with UM servers.

Name	Role	Version
LAB1EXCH	Hub Transport, Client Access, Mailbox, Unifie...	Version 14.1 (Build 21

When completing the wizard, the error below may appear because the default UM service startup mode is set to TCP and is incompatible with the VoIP Security option selected. This will also prevent the UM service from starting on the Exchange server.

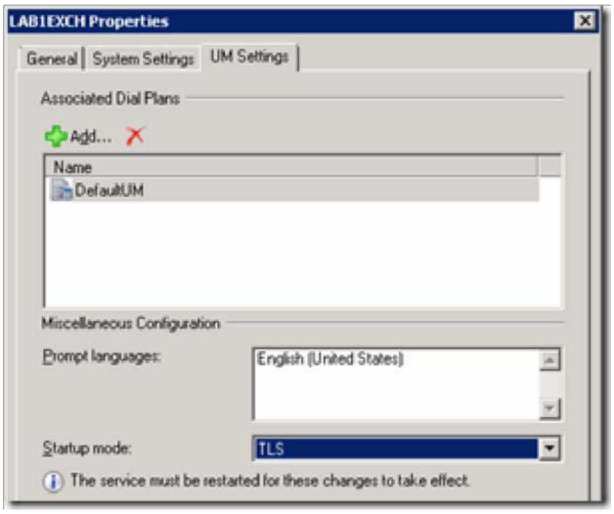
Error:

The VoIPSecurity type of dial plan(s) ‘DefaultUM’ does not match the UMStartupMode of Unified Messaging server ‘LAB1EXCH’. Please ensure that if the UMStartupMode of the Unified Messaging server is TCP, the dial plan has a VoIPSecurity type of Unsecured. If the UMStartupMode of the Unified Messaging server is TLS, the dial plan should have a VoIPSecurity type of either SIPSecured or Secured.

To resolve this issue, complete the wizard and then use the Exchange Management Console to navigate to the **UM Settings** tab on the UM server properties located under **Server Configuration** > **Unified Messaging**. Change the **Startup Mode** to **TLS**.

(**Dual** can also be selected but for Skype for Business all communications use TLS so there is no reason for the UM service to listen over TCP as well.)

Figure 18-3: LABTEXCH Properties



DefaultUM

Prompt languages: English (United States)

Startup mode: TLS

The service must be restarted for these changes to take effect.

To apply this change, the *Microsoft Exchange Unified Messaging* service must be started (it should not be running at this point).

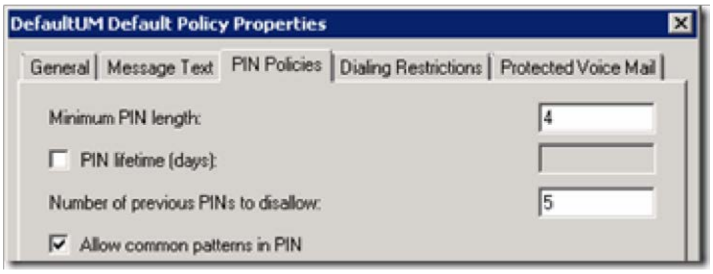
Alternatively, the Exchange Management Shell can be used with the following PowerShell cmdlets to perform all of the steps shown above in this section.

```
New-UMDialPlan -Name ‘DefaultUM’ -NumberOfDigitsInExtension ’4’
-URIType
‘SipName’ -VoIPSecurity ‘Secured’ -CountryOrRegionCode ’1’ Set-
UMServer -Identity ‘LAB1EXCH’ -DialPlans ‘DefaultUM’ -
UMStartupMode ‘TLS’ Start-Service MSExchangeUM
```

18.2.4 Configure UM Settings

To allow for common PIN patterns like ‘1234’ or ‘1111’, change the **PIN policies** tab on the default UM Mailbox Policy and enable **Allow common patterns in PIN**.

Figure 18-4: Default Policy Properties



Minimum PIN length: 4

□ PIN lifetime (days):

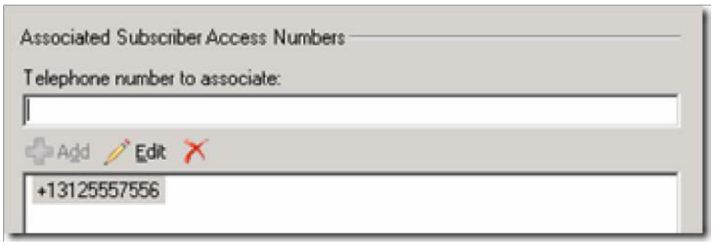
Number of previous PINs to disallow: 5

☑ Allow common patterns in PIN

Next is the Exchange Subscriber Access and Auto Attendant configuration. In this example **312-55575xx** is used in the Skype for Business Dial Plan, where **7556** and **7557** are used for the SA and AA telephone numbers.

Enter the required telephone number on the **Subscriber Access** tab of the newly created UM Dial Plan (e.g., **+13125557556**).

Figure 18-5: Subscriber Access Numbers



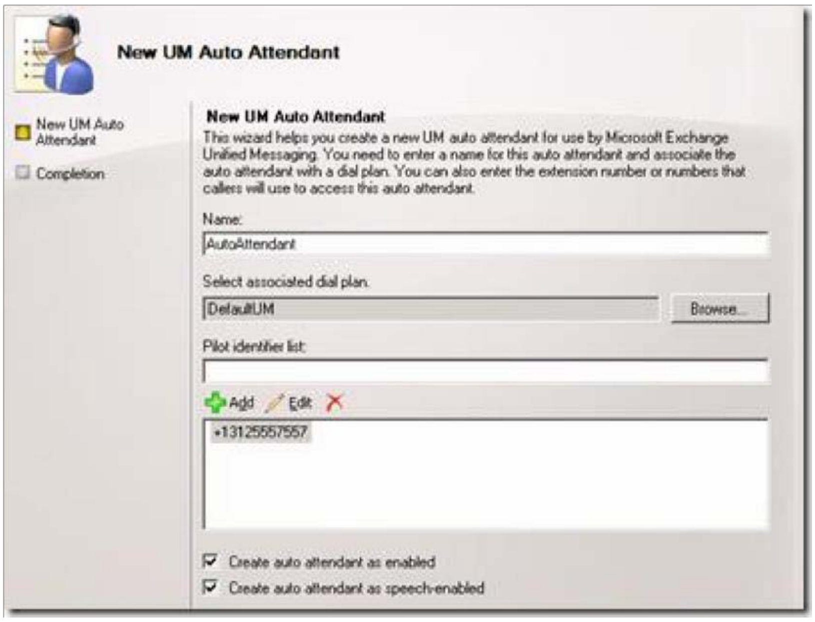
Associated Subscriber Access Numbers

Telephone number to associate:

+13125557556

Create a new *UM Auto Attendant* with any Name (e.g., *AutoAttendant*) (no spaces) and enter the required phone number in the **Pilot Identifier List** (e.g., **+13125557557**). Select the new UM Dial Plan as the associated dial plan and select both settings to enable and speech-enable the Auto Attendant.

Figure 18-6: New UM Auto Attendant



New UM Auto Attendant

New UM Auto Attendant

This wizard helps you create a new UM auto attendant for use by Microsoft Exchange Unified Messaging. You need to enter a name for this auto attendant and associate the auto attendant with a dial plan. You can also enter the extension number or numbers that callers will use to access this auto attendant.

Name: AutoAttendant

Select associated dial plan: DefaultUM

Pilot identifier list:

+13125557557

☑ Create auto attendant as enabled

☑ Create auto attendant as speech-enabled

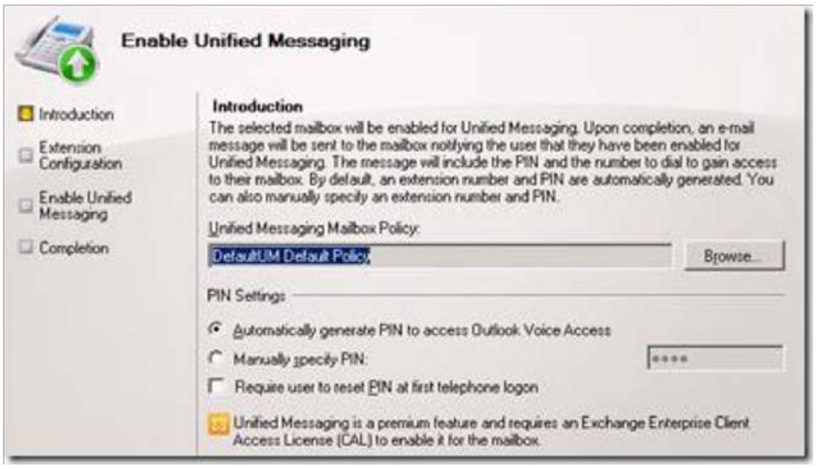
Alternatively, the PowerShell cmdlet shown below can be used to create the new UM Auto Attendant with the setting described above.

```
New-UMAutoAttendant -Name ‘AutoAttendant’ -UMDialPlan
‘DefaultUM’ -Status
‘Enabled’ -SpeechEnabled $true -PilotIdentifierList
‘+13125557557’
```

18.2.5 Enable Mailboxes for UM

Select at least one mailbox using the Exchange Management Console and enable Unified Messaging on it. Run the Enable Unified Messaging wizard on the mailbox and select the default policy. Retain the automatic settings but verify that the displayed extension and SIP address match the settings required for that user.

Figure 18-7: Enable Unified Messaging - Introduction



Enable Unified Messaging

- Introduction
- Extension Configuration
- Enable Unified Messaging
- Completion

Introduction

The selected mailbox will be enabled for Unified Messaging. Upon completion, an e-mail message will be sent to the mailbox notifying the user that they have been enabled for Unified Messaging. The message will include the PIN and the number to dial to gain access to their mailbox. By default, an extension number and PIN are automatically generated. You can also manually specify an extension number and PIN.

Unified Messaging Mailbox Policy: DefaultUM Default Policy [Browse...]

PIN Settings

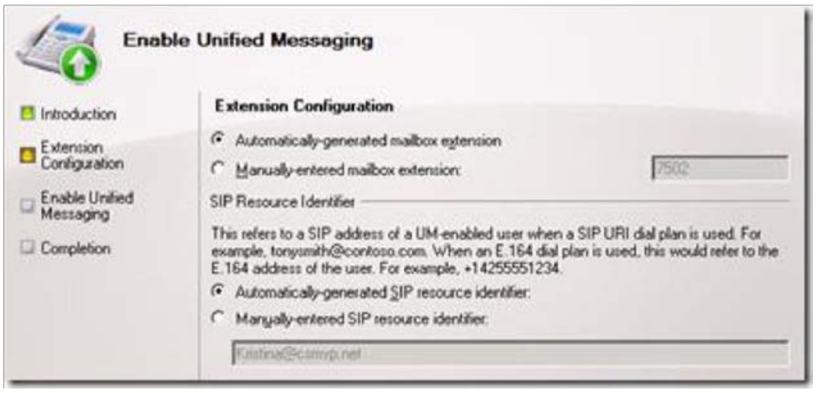
● Automatically generate PIN to access Outlook Voice Access

○ Manually specify PIN: ****

□ Require user to reset PIN at first telephone logon

Unified Messaging is a premium feature and requires an Exchange Enterprise Client Access License (CAL) to enable it for the mailbox.

Figure 18-8: New UM Auto Attendant – Extension Configuration



Enable Unified Messaging

- Introduction
- Extension Configuration
- Enable Unified Messaging
- Completion

Extension Configuration

● Automatically-generated mailbox extension

○ Manually-entered mailbox extension: 7502

SIP Resource Identifier

This refers to a SIP address of a UM-enabled user when a SIP URI dial plan is used. For example, tonysmith@contoso.com. When an E.164 dial plan is used, this would refer to the E.164 address of the user. For example, +14255551234.

● Automatically-generated SIP resource identifier:

○ Manually-entered SIP resource identifier:

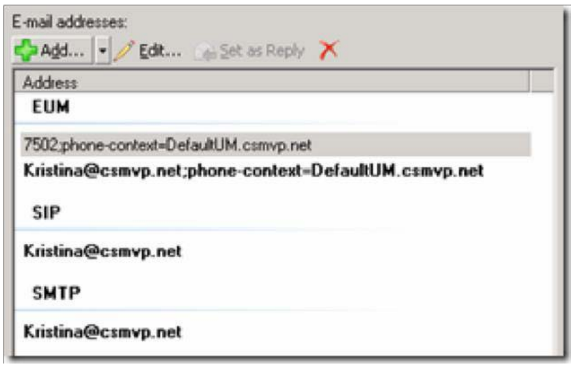
Kristina@csmvp.net

The Exchange Management Shell can be used to perform the same step, as shown by the following cmdlet.

```
Enable-UMMailbox –Identity ‘kristina’ -PinExpired $false -
UMMailboxPolicy ‘DefaultUM Default Policy’ -Extensions ’7502’ -
SIPResourceIdentifier ‘Kristina@csmvp.net’
```

Make sure the EUM and SIP addresses are correctly configured on the mailbox after the wizard completes.

Figure 18-9: E-mail Addresses



Address
EUM
7502;phone-context=DefaultUM.csmvp.net
Kristina@csmvp.net;phone-context=DefaultUM.csmvp.net
SIP
Kristina@csmvp.net
SMTP
Kristina@csmvp.net

18.2.6 Run Exchange UC Configuration Script

This script is basically unchanged in SP1 and performs the same actions: creating the UM IP Gateway and IP Hunt Group as well as granting permissions to Skype for Business Server to read specific UM-related objects in Active Directory.

Make sure to allow for any outstanding AD replication to complete before running this script so that the newly created UM dial plan and any other changes are read by the script in their updated state. If run too soon, the *Dial Plans* listed in the last line of the script output will sometimes display as “not found” even though the configuration would typically be functional at that point. If this happens, it is safe to re-run the script multiple times as it will identify any successful previous changes and thus report that no new changes were applied in those cases.

Using the Exchange Management Shell, execute the **exchucutil.ps1** script located in the Exchange Server’s 'Scripts' directory, as shown in the path below.

```
[PS] C:\Program Files\Microsoft\Exchange
Server\v14\Scripts>.\ExchUCUtil.ps1 –Forest:”network- cyvmq4j.acs”
(where network-cyvmq4j.acs is the forest name from the Lync
appliance)
Using Global Catalog: GC://DC=csmvp,DC=net
Configuring permissions for csmvp.net\RTCUniversalServerAdmins …
CSMVP Net: The appropriate permissions haven’t been granted for
the Office Communications Servers and Administrators to be able to
read the UM dial plan and auto attendants container objects
in Active Directory. The correct permissions are being added to
the container objects.
UM DialPlan Container: The appropriate permissions haven’t been
granted for the Office Communications Servers and Administrators
to be able to read the UM dial plan and auto attendants container
objects in Active Directory. The correct permissions are being
added to the container objects.
UM AutoAttendant Container: The appropriate permissions haven’t
been granted for the Office Communications Servers and
Administrators to be able to read the UM dial plan and auto
attendants container objects in Active Directory. The correct
permissions are being added to the container objects.
Configuring permissions for
csmvp.net\RTCComponentUniversalServices …
CSMVP Net: The appropriate permissions haven’t been granted for
the Office Communications Servers and Administrators to be able to
read the UM dial plan and auto attendants container objects in
Active Directory. The correct permissions are being added to the
container objects.
UM DialPlan Container: The appropriate permissions haven’t been
granted for the Office Communications Servers and Administrators
to be able to read the UM dial plan and auto attendants container
objects in Active Directory. The correct permissions are being
added to the container objects.
UM AutoAttendant Container: The appropriate permissions haven’t
been granted for the Office Communications Servers and
Administrators to be able to read the UM dial plan and auto
attendants container objects in Active Directory. The correct
permissions are being added to the container objects.
Configuring UM IP Gateway objects…
Pool: lab1ls.csmvp.net
A UMIPGateway doesn’t exist in Active Directory for the Office
Communications Server Pool. A new UM IP gateway is being created
for the Pool.
```

```
IsBranchRegistrar: False MessageWaitingIndicatorAllowed: True
OutcallsAllowed: True
WARNING: The command completed successfully but no settings of
’1:1’ have
been modified.
Dial plans: DefaultUM
```

```
Permissions for group csmvp.net\RTCUniversalServerAdmins
ObjectName AccessRights Configured
```

```
———-       —————   ———-
CSMVP Net ListChildren True UM DialPlan Container
ListChildren, ReadProperty     True UM AutoAttendant Container
ListChildren, ReadProperty
True
Permissions for group csmvp.net\RTCComponentUniversalServices
ObjectName AccessRights Configured
———-       —————   ———-
CSMVP Net ListChildren True UM DialPlan Container     ListChildren,
ReadProperty
True  UM AutoAttendant Container     ListChildren, ReadProperty
True
PoolFqdn  UMIPGateway  DialPlans
——– ———-  ————
lab1ls.csmvp.net 1:1   {DefaultUM}
```

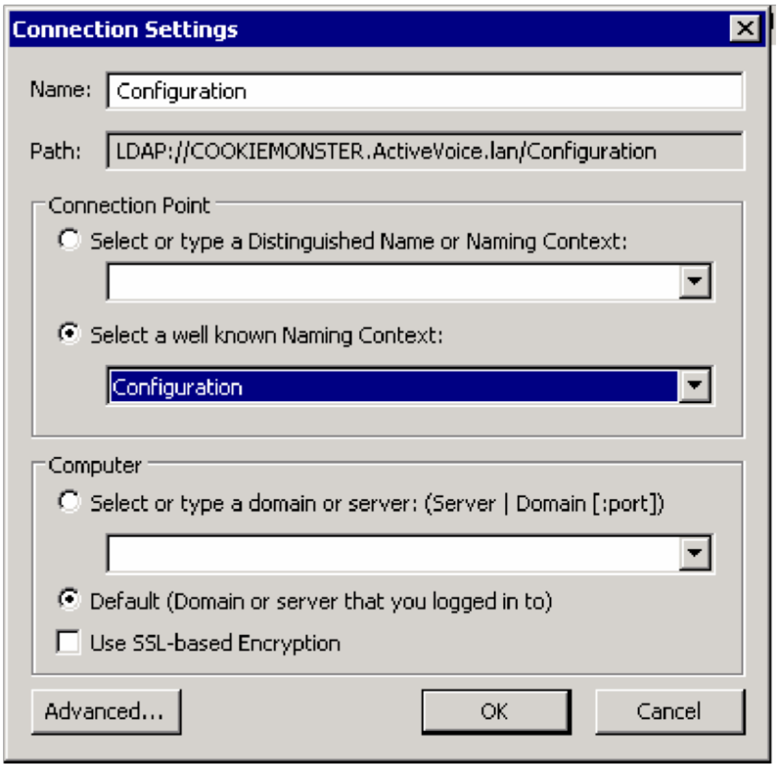
18.2.7 Prepare Administrative Access Rights for the Skype for Business Administrator

To be able to run the Skype for Business UM Configuration tool from a trusted resource forest (where Skype for Business resides), minimum read permissions must be assigned to the Skype for Business Administrator account in the Exchange environment (the **`ocsumutil`** command will need to be run by this administrator).

An automated installer will be created at some point but for now an enterprise administrator is needed to set these permissions through the configuration partition in ADSIEdit.msc within the enterprise domain where Exchange is installed.

1. After starting ADSIEdit.msc, select the configuration partition as shown in the figure below.

Figure 18-10: Connection Settings



Connection Settings

Name: Configuration

Path: LDAP://COOKIEMONSTER.ActiveVoice.lan/Configuration

Connection Point

○ Select or type a Distinguished Name or Naming Context:

● Select a well known Naming Context: Configuration

Computer

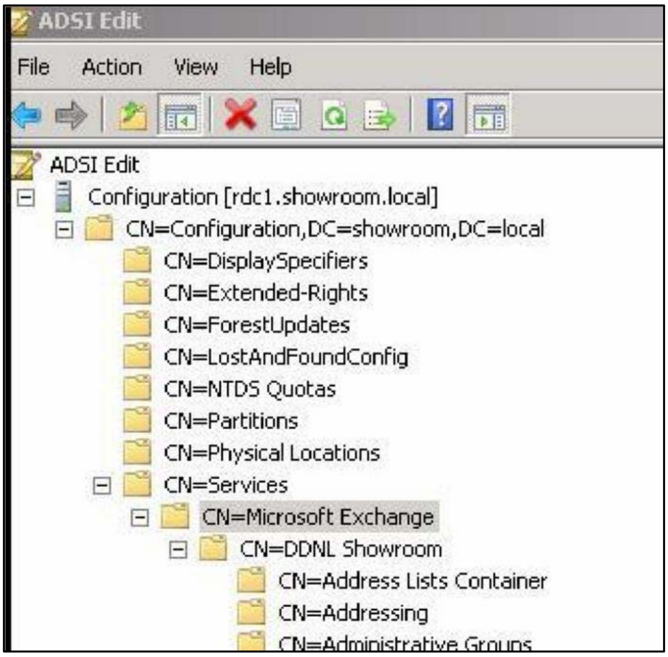
○ Select or type a domain or server: (Server | Domain [:port])

● Default (Domain or server that you logged in to)

□ Use SSL-based Encryption

2. Right-click the **CN=Microsoft Exchange** object under **CN=Services** in the CN=localdomain (CN=Configuration,DC=Showroom,DC=local as examplified in the figure below) and select **Properties**.

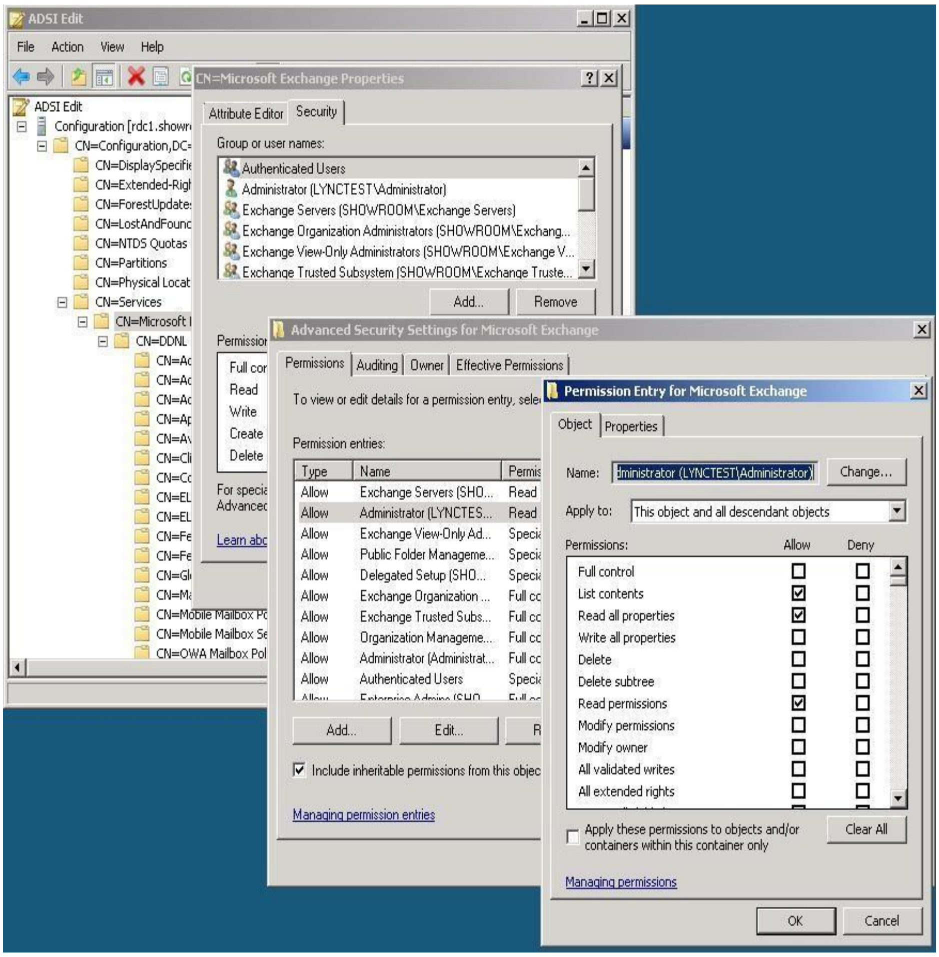
Figure 18-11: New UM Auto Attendant



ADSI Edit
Configuration [rdc1.showroom.local]
CN=Configuration,DC=showroom,DC=local
CN=DisplaySpecifiers
CN=Extended-Rights
CN=ForestUpdates
CN=LostAndFoundConfig
CN=NTDS Quotas
CN=Partitions
CN=Physical Locations
CN=Services
CN=Microsoft Exchange
CN=DDNL Showroom
CN=Address Lists Container
CN=Addressing
CN=Administrative Groups

3. Select the **Security** tab and click **Advanced**.

Figure 18-12: Security Tab



Name: dministrator (LYNCTEST\Administrator)

Apply to: This object and all descendant objects

Permissions:	Allow	Deny
Full control	□	□
List contents	☑	□
Read all properties	☑	□
Write all properties	□	□
Delete	□	□
Delete subtree	□	□
Read permissions	☑	□
Modify permissions	□	□
Modify owner	□	□
All validated writes	□	□
All extended rights	□	□

□ Apply these permissions to objects and/or containers within this container only

ADSI Edit
CN=Microsoft Exchange Properties
Attribute Editor
Security
Advanced Security Settings for Microsoft Exchange
Permission Entry for Microsoft Exchange
Object
Properties
Change...
Clear All
Managing permissions
OK
Cancel

4. Click **Add…** and select the Skype for Business administrator from the (trusted Skype for Business) Resource forest. Select **Allow** in order to:
   - List contents
   - Read all Properties
   - Read permissions
5. Click **OK** three times to leave those properties
6. Close ADSIEdit.msc

18.2.8 Run Skype for Business UM Configuration Tool

This utility is used to create the AD contact objects for Skype for Business Server to resolve and locate the Exchange Subscriber Access and Auto Attendant services.

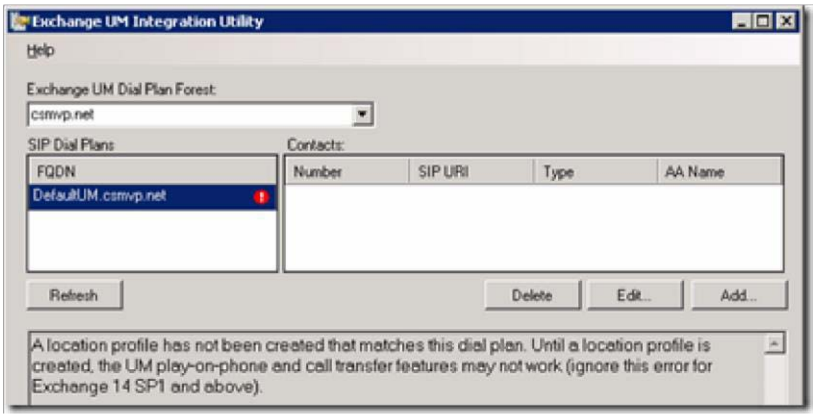
In Exchange 2007, it was always required to configure the UM Dial Plan name to be the identical FQDN to that of the OCS Location Profile. With Exchange Server 2010 SP1, this is no longer required, as indicated by the informational text in the figure below (lowermost).

1. Run the **OcsUmUtil.exe** program located in the Skype for Business Server's 'Support' directory shown in this path:

```
C:\Program Files\Common Files\Microsoft Lync Server 2010\Support\OcsUmUtil.exe
```

2. Click **Load Data**; the Active Directory forest name populates the 'Exchange UM Dial Plan Forest' field. If no Dial Plan is displayed, there is a permissions issue with the account running OcsUmUtil.exe. Verify the steps from the previous item for the account running OcsUmUtil.exe.

Figure 18-13: Exchange UM Integration Utility



Exchange UM Integration Utility

Help

Exchange UM Dial Plan Forest: csmvp.net

SIP Dial Plans:

FQDN
DefaultUM.csmvp.net

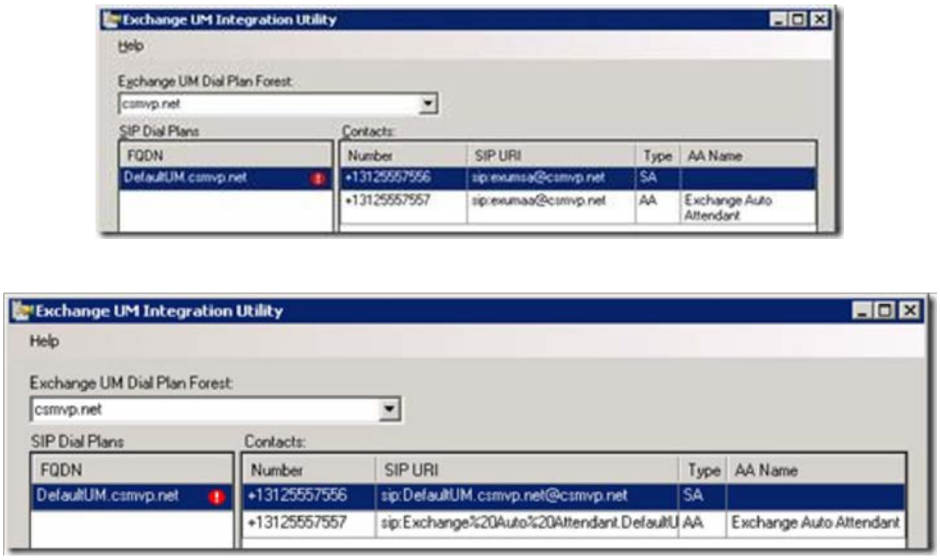
Contacts:

Number	SIP URI	Type	AA Name

A location profile has not been created that matches this dial plan. Until a location profile is created, the UM play-on-phone and call transfer features may not work (ignore this error for Exchange 14 SP1 and above).

3. Click **Add** to create the Subscriber Access contact first. Select the required 'Organizational Unit' and 'Name'. The defaults can be used for the rest of the settings.
4. Click **Add** again to create another contact, and select **Auto-Attendant** as 'Contact Type'. Select the requried 'Organizational Unit' and ' Name'. The defaults can be used for the rest of the settings as well.

Figure 18-14: Exchange UM Integration Utility - Contacts



Exchange UM Integration Utility

Help

Exchange UM Dial Plan Forest: csmvp.net

SIP Dial Plans:

FQDN
DefaultUM.csmvp.net

Contacts:

Number	SIP URI	Type	AA Name
+13125557556	sip:exumsa@csmvp.net	SA	
+13125557557	sip:exumaa@csmvp.net	AA	Exchange Auto Attendant

Exchange UM Integration Utility

Help

Exchange UM Dial Plan Forest: csmvp.net

SIP Dial Plans:

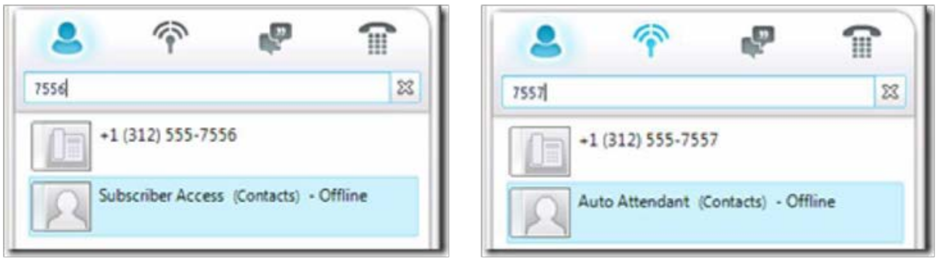
FQDN
DefaultUM.csmvp.net

Contacts:

Number	SIP URI	Type	AA Name
+13125557556	sip:DefaultUM.csmvp.net@csmvp.net	SA	
+13125557557	sip:Exchange%20Auto%20Attendant.DefaultU	AA	Exchange Auto Attendant

5. Close the Exchange UM Integration Utility and force an address book update in a Skype for Business client to verify the new Exchange contacts. Depending on the AD forest configuration replication may need to complete before attempting the address book update process.

Figure 18-15: Address Book Update



7556

+1 (312) 555-7556

Subscriber Access (Contacts) - Offline

7557

+1 (312) 555-7557

Auto Attendant (Contacts) - Offline

Calls to Auto Attendant will now function and Voice Mail access for enabled users will be available from Outlook and Skype for Business clients.

This page is intentionally left blank.

Part VI

Appendix

A Script to Set Writeback Permissions to Enterprise Users

This appendix shows an example script for setting writeback permissions to Enterprise Users.

```
# This script sets the minimum required write access permissions
for a Skype for Business resource forest service account when
deployed in hybrid mode with Office 365.
#
# The user forests in a resource forest model will require Skype
for Business schema updates if Dirsync or AADSync are used to
replicate changes to Office365.
# If AADConnect (Microsoft released October 2015) is used and
deployed in a resource forest model, there is no need for those
schema updates.
#
# Users that are member of an administrator group within Active
Directory have special protection on the Access Controll
Permissions.
# To also include those users in the replication logic (enable
them for Skype for Business) the -IncludeAdministrators parameter
need to be used.
# more info can be found at:
#
https://blogs.technet.microsoft.com/asiasupp/2006/11/15/regarding-
adminsdholder/
# more on security mechanism: https://technet.microsoft.com/en-
us/library/2009.09.sdadminholder.aspx
#
# To reset the user forest to the default security permissions of
Active Directory, use Dsacls /S /T on an OU
# for example, to reset the EnterpriseUsers OU, including all sub-
OUs and objects within it, use the command:
# Dsacls "OU=EnterpriseUsers,DC=enterpriseusers,DC=local" /S /T
#
#
# Usage:
#
# Run the script with the following parameters:
# -Target, representing the target OU in the user forest
# -Trustee, being the service account that is given write
perissions on the Skype for Business attributes in the user forest
# -ForReal, without this parameter, the script will run in demo
mode
# -IncludeAdministrators, needs to be present if Administrartor
accounts are also used for regular use with Skype for Business
(which is against Microsoft Best Practice Security Rules)
#
# Example:
# To assign write permissions for the CloudBond365\Administrator
to the EnterpriseUsers OU users, including the Administrative
users within it, run:
#
```

```
# DirSyncHybridACLPermissions.ps1 -Target
"OU=EnterpriseUsers,DC=enterpriseusers,DC=local" -Trustee
"CloudBond365\Administrator" -ForReal -IncludeAdministrators
#


param
(
    [Parameter(Mandatory = $true)]
    [String]$Target,

    [Parameter(Mandatory = $true)]
    [String]$Trustee,

    [Parameter(Mandatory = $false)]
    [Switch]$ForReal = ![Switch]::Present,

    [Parameter(Mandatory = $false)]
    [Switch]$IncludeAdministrators = ![Switch]::Present
);


$objectDomain = ($Target -replace "(.*?)DC=(.*)",'$2')
$adminSDHolder="cn=adminsdholder,cn=system,dc="+$objectDomain


Write-Host "'nTarget:        $Target`nTrustee:
$Trustee`nAdminSDHolder: $adminSDHolder`n";


if($ForReal.IsPresent)
{
    Write-Host "Granting the following permissions...";
}
else
{
    Write-Host `
        "Running in informational mode.  To actually submit
changes use the -ForReal switch.`n" `
        -ForegroundColor Yellow;
}


[String[]]$objectTypes = @(
    "contact",
    "group",
    "user"
);


[String[]]$SkypeHybridWriteBackAttributes = @(
    "proxyAddresses;user",
    "msRTCSIP-UserEnabled;user",
    "msRTCSIP-OptionFlags;user",
    "msRTCSIP-DeploymentLocator;user",
    "msRTCSIP-Line;user",
    "msRTCSIP-PrimaryUserAddress;user"
);



foreach($objectClass in $objectTypes)
{
    Write-Host "Object type:" $objectClass;
    foreach($attribute in $SkypeHybridWriteBackAttributes)
    {
        [String[]]$scopedAttrs = $attribute.Split(";",
[StringSplitOptions]::None);
        [String]$attr = $scopedAttrs[0];
        [String]$ttype = $scopedAttrs[1];

        if( ($ttype.ToLower() -eq $objectClass.ToLower()) -or
            ($ttype.ToLower() -eq "all"))
        {
            Write-Host "`tWrite Property (WP) $attr on descendent
user objects";
            # [String]$cmd1 = "dsacls '$Target' /I:S /P:N";
            [String]$cmd1 = "dsacls '$Target' /I:S /G
'`"$Trustee`":WP;$attr;$objectClass'";
            if($ForReal.IsPresent)
            {
                Invoke-Expression $cmd1 |Out-File
DirSyncHibridPermissions.log.txt -Append
                # Invoke-Expression $cmd2 |Out-File
DirSyncHibridPermissions.log.txt -Append
            }
        }
    }
}


if($IncludeAdiministrators.IsPresent)
{
    # Set ACLs on adminSDholder object
    # this should replicate to admin users (where admincount =1)
    # dsacls
"cn=adminsdholder,cn=system,dc=enterpriseusers,dc=local" /G
"CloudBond365\Administrator:WP;msRTCSIP-PrimaryUserAddress"
    dsacls $adminSDHolder /G $Trustee + ":WP;proxyAddresses"
    dsacls $adminSDHolder /G $Trustee + ":WP;msRTCSIP-UserEnabled"
    dsacls $adminSDHolder /G $Trustee + ":WP;msRTCSIP-OptionFlags"
    dsacls $adminSDHolder /G $Trustee + ":WP;msRTCSIP-
DeploymentLocator"
    dsacls $adminSDHolder /G $Trustee + ":WP;msRTCSIP-Line"
    dsacls $adminSDHolder /G $Trustee + ":WP;msRTCSIP-PrimaryUserAddress"
}


Write-Host "`nScript complete.`n`n";
```

This page is intentionally left blank.

International Headquarters
1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/contact
Website: www.audiocodes.com