UC Connector 8.0

Genesys Lync Integration

Deployment Guide

The information contained herein is proprietary and confidential and cannot be disclosed or duplicated without the prior written consent of Genesys Telecommunications Laboratories, Inc.

Copyright © 2013 Genesys Telecommunications Laboratories, Inc. All rights reserved.

About Genesys

Genesys is the world's leading provider of customer service and contact center software—with more than 4,000 customers in 80 countries. Drawing on its more than 20 years of customer service innovation and experience, Genesys is uniquely positioned to help companies bring their people, insights and customer channels together to effectively drive today's customer conversation. Genesys software directs more than 100 million interactions every day, maximizing the value of customer engagement and differentiating the experience by driving personalization and multi-channel customer service—and extending customer service across the enterprise to optimize processes and the performance of customer-facing employees. Go to www.genesyslab.com for more information.

Each product has its own documentation for online viewing at the Genesys Technical Support website or on the Documentation Library DVD, which is available from Genesys upon request. For more information, contact your sales representative.

Notice

Although reasonable effort is made to ensure that the information in this document is complete and accurate at the time of release, Genesys Telecommunications Laboratories, Inc., cannot assume responsibility for any existing errors. Changes and/or corrections to the information contained in this document may be incorporated in future versions.

Your Responsibility for Your System's Security

You are responsible for the security of your system. Product administration to prevent unauthorized use is your responsibility. Your system administrator should read all documents provided with this product to fully understand the features available that reduce your risk of incurring charges for unlicensed use of Genesys products.

Trademarks

Genesys and the Genesys logo are registered trademarks of Genesys Telecommunications Laboratories, Inc. All other company names and logos may be trademarks or registered trademarks of their respective holders. © 2013 Genesys Telecommunications Laboratories, Inc. All rights reserved.

The Crystal monospace font is used by permission of Software Renovation Corporation, www.SoftwareRenovation.com.

Technical Support from VARs

If you have purchased support from a value-added reseller (VAR), please contact the VAR for technical support.

Technical Support from Genesys

If you have purchased support directly from Genesys, please contact Genesys Technical Support. Before contacting technical support, please refer to the ***Genesys Care Program Guide*** for complete contact information and procedures.

Ordering and Licensing Information

Complete information on ordering and licensing Genesys products can be found in the ***Genesys Licensing Guide.***

Released by

Genesys Telecommunications Laboratories, Inc. www.genesyslab.com

Document Version: 80ucc_dep_lync_06-2013_v.8.0.301.00

Table of Contents

List of Procedures

Preface

Welcome to the *Genesys Lync Integration 8.0 Deployment Guide*. This document describes a deployment configuration for the Genesys Voice platform in conjunction with Microsoft Lync 2010, for voice and presence integration.

Note: For versions of this document created for other releases of this product, visit the Genesys Technical Support website, or request the Documentation Library DVD, which you can order by e-mail from Genesys Order Management at orderman@genesyslab.com.

This preface contains the following sections:

For information about related resources and about the conventions that are used in this document, see the supplementary material starting on page 125.

About Genesys Lync Integration

Microsoft Lync 2010 provides an all-software, IP-based voice infrastructure to enterprises, including contact center deployments. This architecture has been qualified by Tekvizion, an independent interoperability testing lab, to support the Microsoft Contact Center applications interop specifications. Testing occurred in June / July 2012.

Intended Audience

This document is primarily intended for system engineers and other members of an implementation team who will complete the deployment and integration

of the Microsoft Lync 2010 into the Genesys environment. It has been written with the assumption that you have a basic understanding of:

- Computer-telephony integration (CTI) concepts, processes, terminology, and applications
- Unified Communications (UC) generally, as well as the specifics of the third-party UC platform deployed on the Enterprise side.
- The Genesys Management Framework architecture and functions that support T-Server, SIP Server, and Genesys routing.
- Network design and operation
- Your own network configurations

Making Comments on This Document

If you especially like or dislike anything about this document, feel free to e-mail your comments to Techpubs.webadmin@genesyslab.com.

You can comment on what you regard as specific errors or omissions, and on the accuracy, organization, subject matter, or completeness of this document. Please limit your comments to the scope of this document only and to the way in which the information is presented. Contact your Genesys Account Representative or Genesys Technical Support if you have suggestions about the product itself.

When you send us comments, you grant Genesys a nonexclusive right to use or distribute your comments in any way it believes appropriate, without incurring any obligation to you.

Contacting Genesys Technical Support

If you have purchased support directly from Genesys, please contact Genesys Technical Support.

Before contacting technical support, please refer to the *Genesys Care Program Guide* for complete contact information and procedures.

Document Change History

This is the first release of the *UC Connector 8.0 Genesys Lync Integration Deployment Guide.* In future releases of this document, this section will list topics that are new or that have changed significantly since the first release of this document.

Chapter

1 Overview

Genesys integrates with Microsoft Lync 2010 using the Genesys SIP Server, deployed in front of the Lync server. Lync users presence is monitored through the Genesys UC Connector, which acts as a gateway between Lync and Genesys presence status.

This chapter contains the following sections:

General Architecture

Figure 1 shows the general architecture of a Lync deployment.

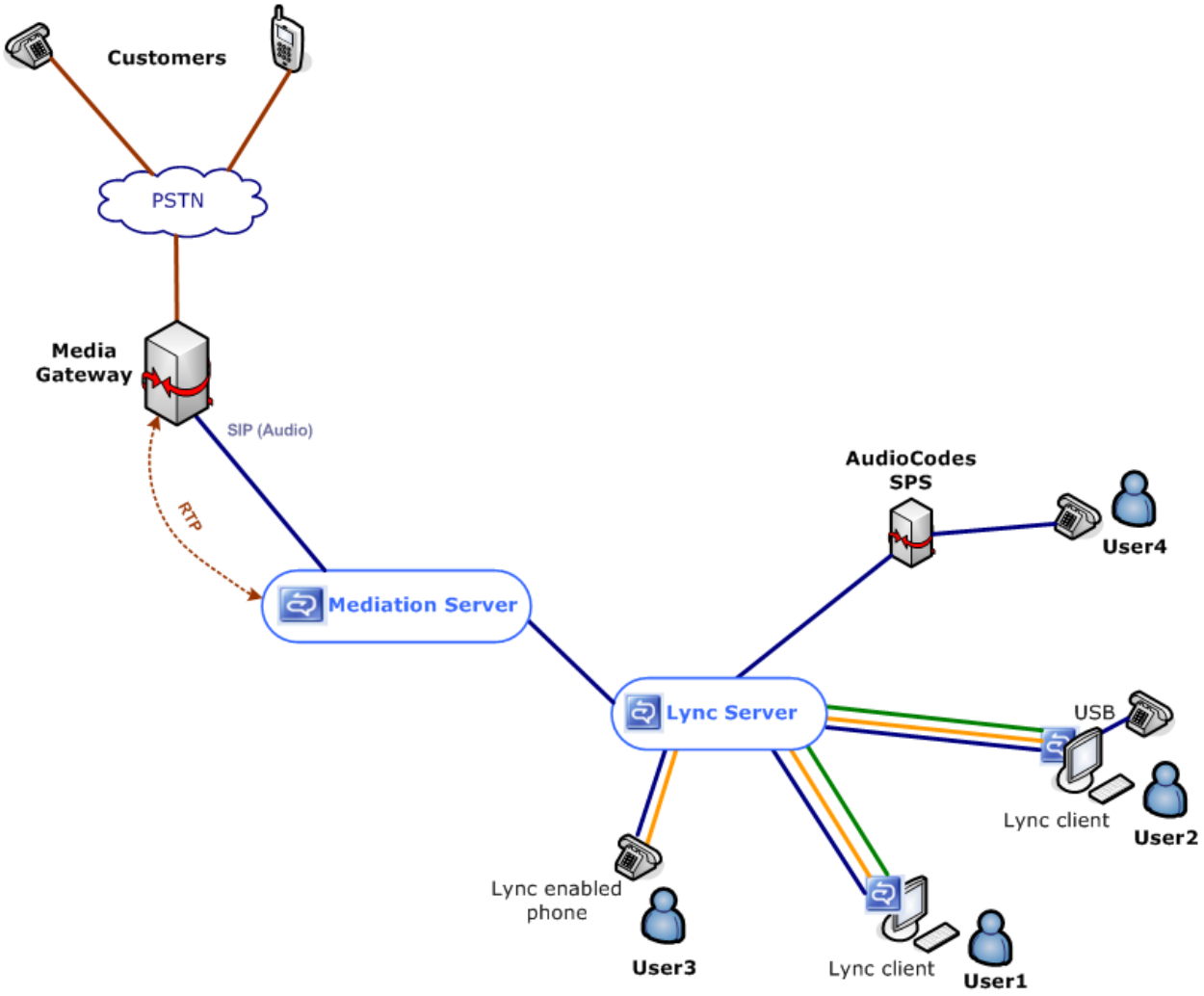

Figure 1: General Lync Voice architecture

The major functions shown in Figure 1 are:

- Public switched telephone network (PSTN) calls come in through a media gateway, which processes signaling and converts it to SIP from whatever protocol it uses in the telephone network, samples the media and converts it to RTP, and then converts it back again.
- The Lync Mediation Server terminates and processes all external voice and signaling connections, policing and throttling the media.
- The Lync Front End Server manages logins, presence, and signaling for all Lync users.

- Lync users have a Lync client on their desktop. This software application provides presence, voice, IM, and video capabilities locally.
- Remote users may go through a SIP trunk or another SIP-to-PSTN conversion managed, for instance, by an AudioCodes gateway.

Environment Information

Figure 2 shows how Genesys integrates with Lync at several levels.

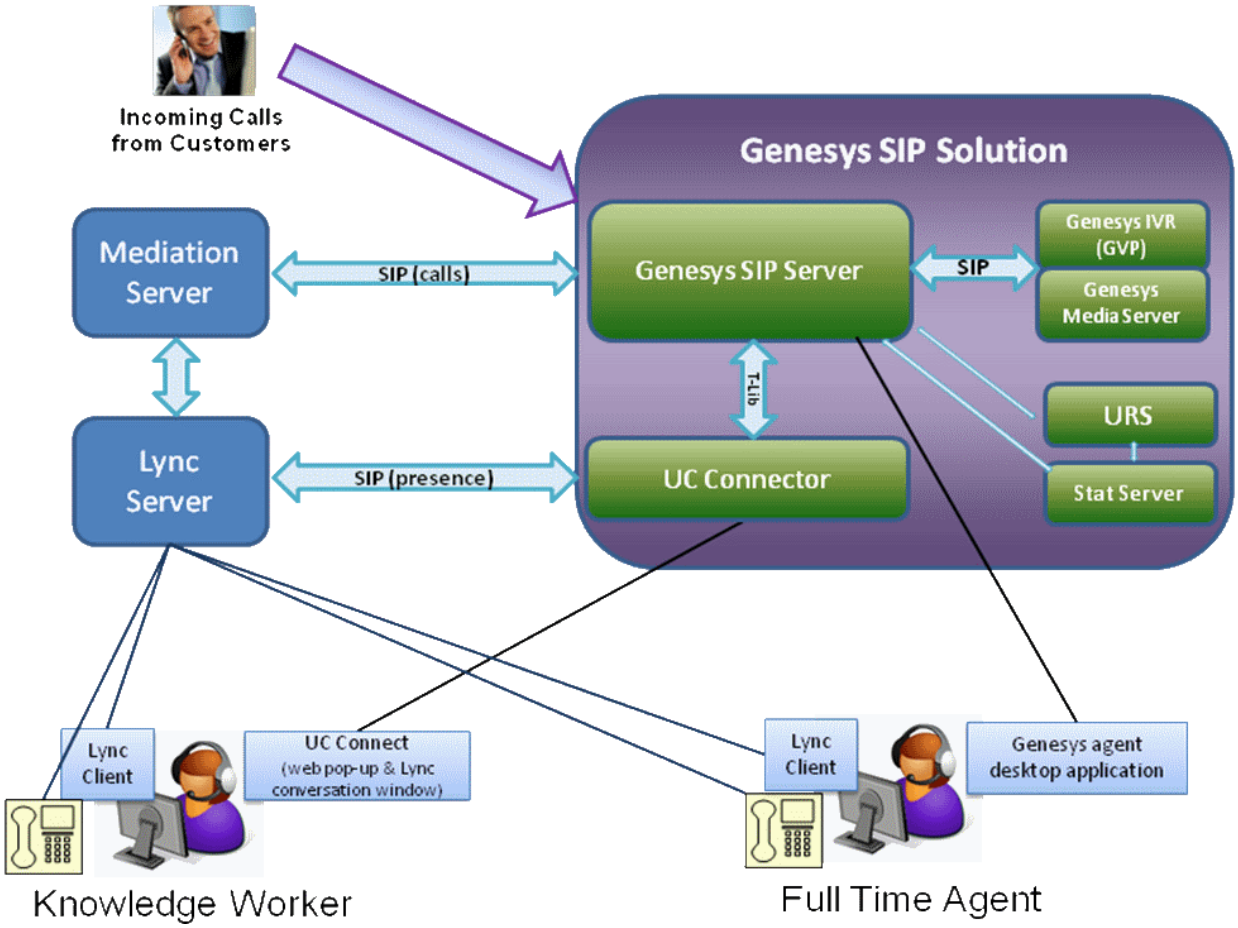

Figure 2: Genesys integration with Lync modules

The integration levels in Figure 2 are:

- From Lync's point of view, Genesys SIP Server acts as an external gateway as it receives incoming calls and forwards them to available agents. This is done through a connection with the Lync Mediation Server.
- Genesys UC Connector subscribes to Lync users' (agents and knowledge workers) presence, to make their status available to Stat Server. This allows routing of interactions to available personnel.

- Agents can use either Genesys Interaction Workspace as their desktop client along with the Interaction Workspace Plug-in for Lync, or another Genesys desktop client with Genesys Lync Agent, in addition to the Lync client on their desktop. Genesys integrates with the Lync client to allow third-party call control and, in particular, answering calls from the Genesys desktop. For more information on Genesys Lync Agent, see Appendix , "Genesys Lync Agent," on page 107.

Lync Enterprise Voice integration

Figure 3 shows the architecture for Genesys SIP Server and Lync Voice for contact center integration.

The SIP Server is positioned in front of Lync Voice, and manages the initial queuing and qualification of calls, transferring the call to Media Server as necessary. The calls are then forwarded to the Lync Mediation Server, depending on agents' availability.

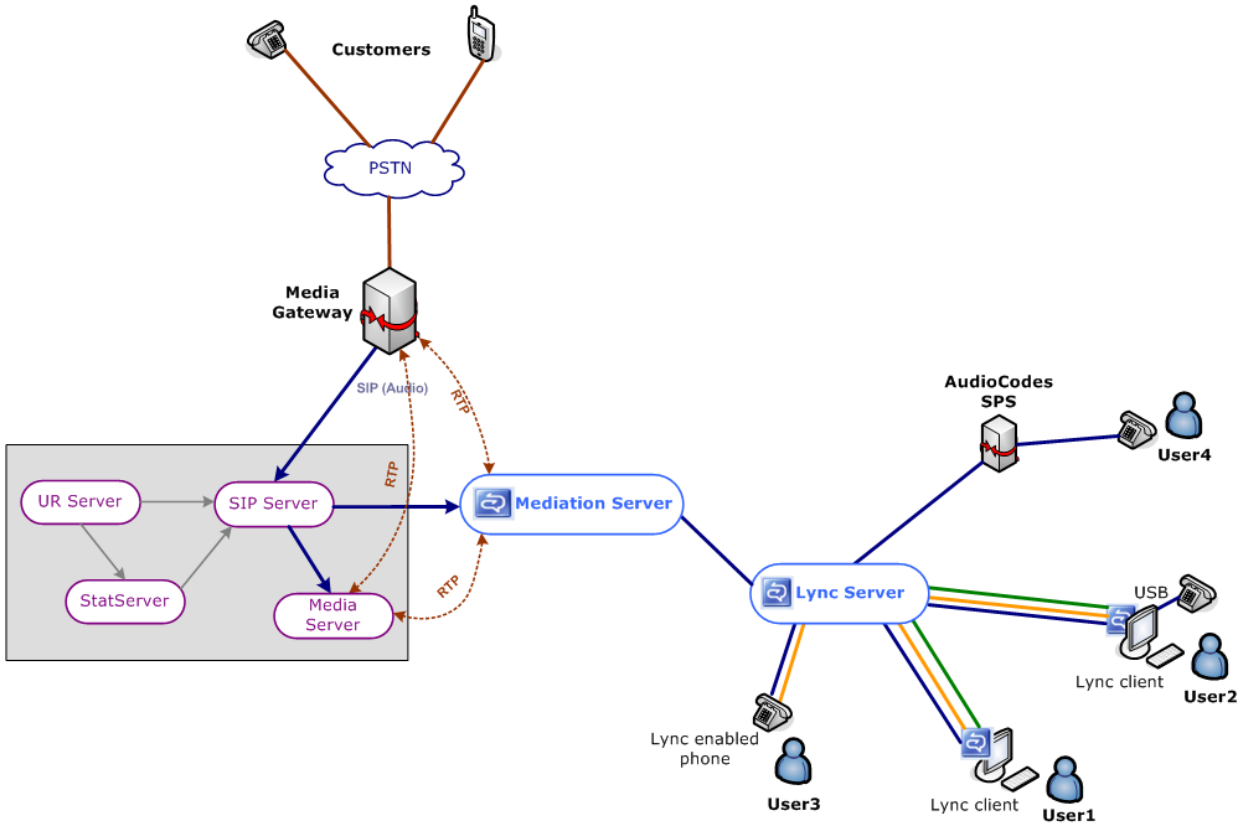

Figure 3: Genesys integration with Lync general architecture

Chapter

2 Deployment Task Flow

This chapter guides you through the various actions you must take to deploy Microsoft Lync 2010 and Genesys components.

This chapter contains the following sections:

Deployment Overview

Complete the following tasks to deploy and integrate Lync and Genesys components.

Task Summary: Deploying Lync and Genesys components

Objective	Actions
1. Complete prerequisites.	Verify that all prerequisite components are in place: • "Installing Active Directory Domain Services" on page 17 • "Installing Active Directory Certificate Services" on page 27
2. Install and configure Microsoft Lync 2010.	Install, connect and configure Lync and Lync-related components. Complete these steps: 1. "Building the Environment" on page 37 2. "Creating the New Topology" on page 54 3. "Lync Server Front End Setup" on page 65 4. "Defining Users in Lync" on page 75 5. "Genesys-Specific Lync Configurations" on page 83
5. Generate certificate for Genesys applications.	1. First generate a client certificate to trust the Lync Front End Server. See "Generate Client Certificate" on page 87 for details. 2. Next generate a server certificate using one of three methods. See "Generate Server Certificate" on page 89 for details.

Task Summary: Deploying Lync and Genesys components (Continued)

Objective	Actions
6. Configure Genesys components for Lync interoperability.	To configure SIP Server, see "SIP Server Configuration Tasks" on page 94. To configure UC Connector, see "UC Connector Configuration Tasks" on page 99. The Interaction Workspace Plug-in for Lync must be installed for agents deployed with the Lync integration. See "Interaction Workspace Plug-in for Lync" on page 102 for details.
7. Review current Lync integration limitations.	For details about how the limitations affect the Phase 1 version of Lync integration, see "Current Limitations" on page 104.

Chapter

3 Deployment Prerequisites

This chapter discusses prerequisites to installing Microsoft Lync on the server. In order to do this, Active Directory must also be installed and configured, together with Active Directory Certificate Services.

This chapter contains the following sections:

Installing Active Directory Domain Services

The process of installing Active Directory on your Windows Server 2008 environment consists of two steps: the first step is to install Active Directory and the second step is to configure your installation. Once this is complete, your Windows server will become a Domain Controller.

Procedure: Installing Active Directory

Purpose: To install Active Directory on a Windows Server 2008 environment.

Start of procedure

1. Access the Server Manager screen. From the Windows taskbar, select `Start > Administrative Tools > Server Manager`.
2. Under Roles Summary, click `Add Roles`.
3. At the welcome page for the wizard, click `Next`.

4. On the Select Server Roles screen, select `Active Directory Domain Services`.

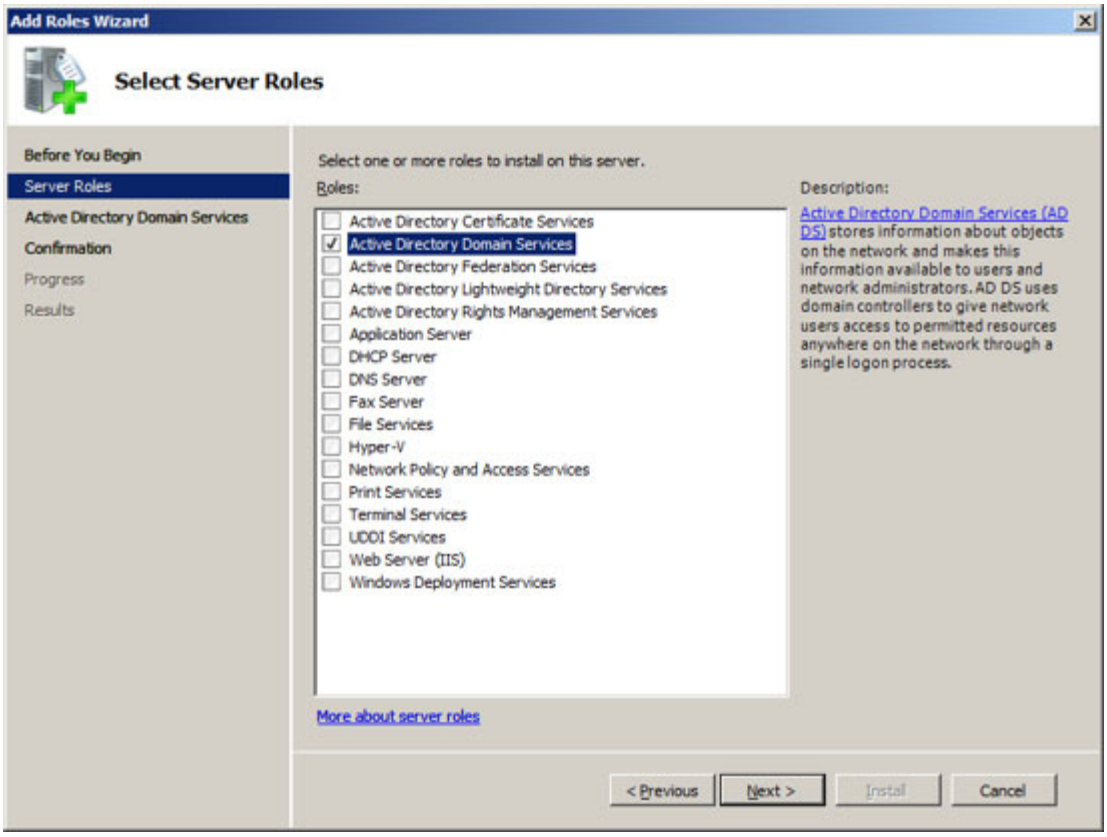

Figure 4: Selecting Active Directory Domain Service

5. In the new dialog, click `Add Required Features`.

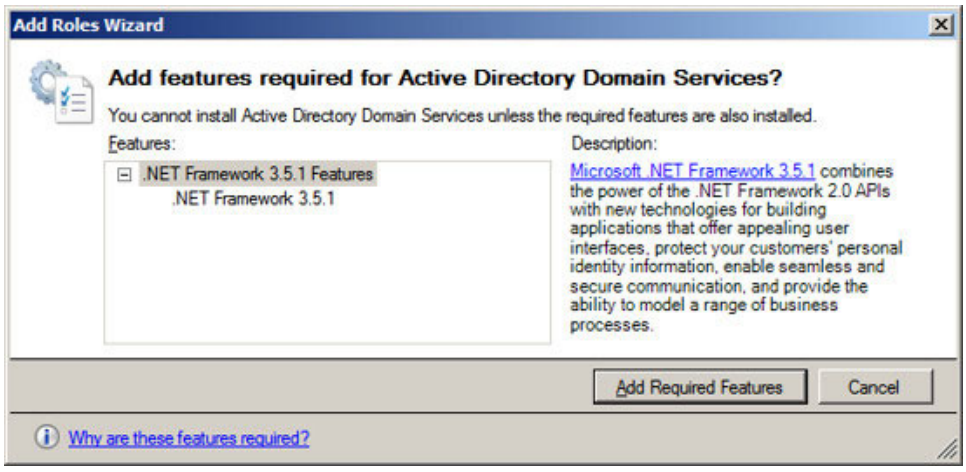

Figure 5: Add Required Features

6. Click `Next`.

7. Review the information presented in the Active Directory Domain Services screen, and click `Next`.

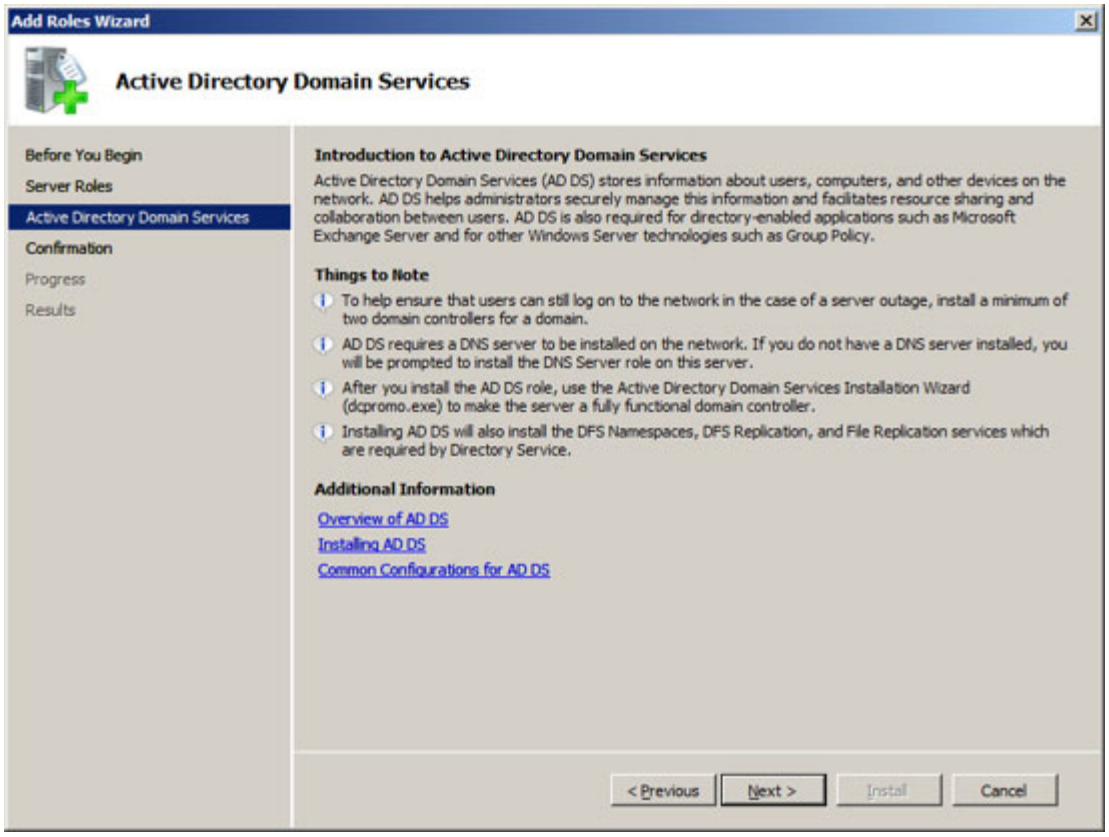

Figure 6: Active Directory Domain Services

8. Review the information on the Confirm Installation Selections screen, and click `Install`.

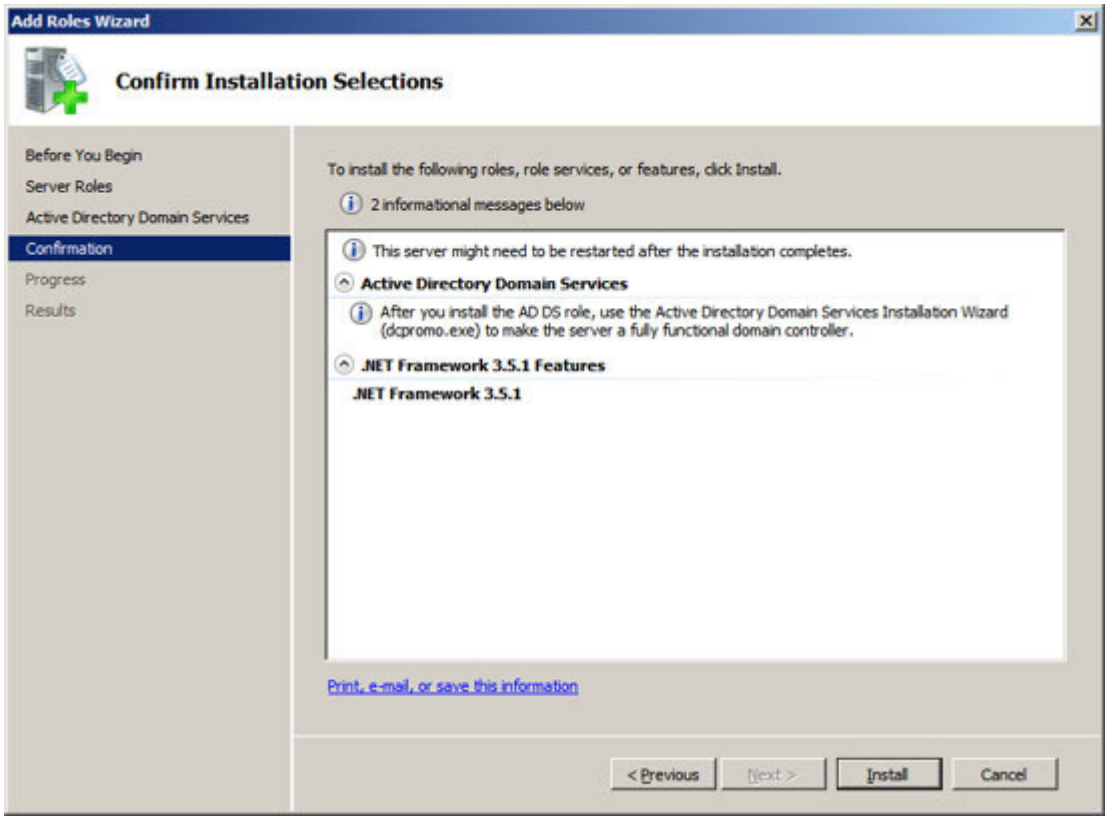

Figure 7: Confirm Installation Selections

9. On the Installation Results screen, click `Close`.

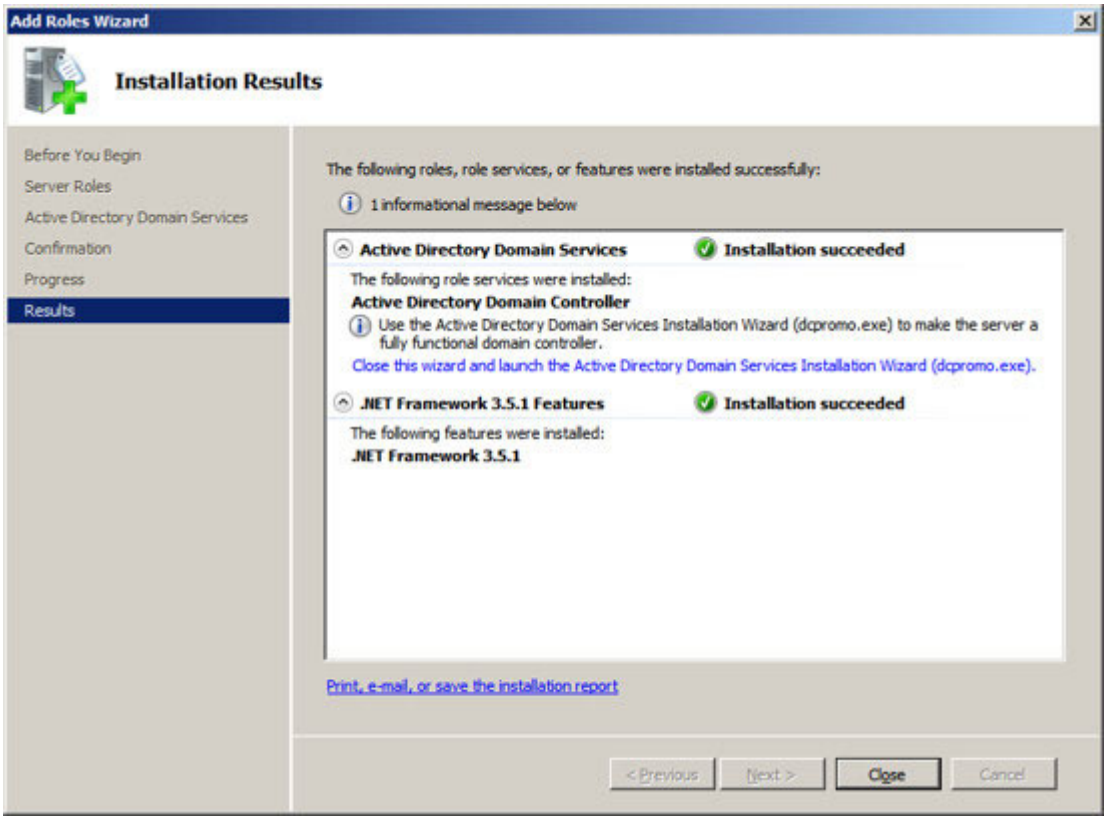

Figure 8: Installation Results

End of procedure

Next Steps

- Procedure: Configuring Active Directory

Procedure: Configuring Active Directory

Purpose: To configure Active Directory in a Windows Server 2008 environment.

Prerequisites

- Procedure: Installing Active Directory

Start of procedure

1. Access the Server Manager screen. From the Windows taskbar, select `Start > Administrative Tools > Server Manager`.
2. Confirm that the Role added in Procedure: Installing Active Directory is displayed under "Roles Summary".

Note: The Active Directory Domain Services may indicate errors because the software is installed but is not yet configured.

3. Click the Windows Start button and select Run.
4. Type dcpromo.exe in the box and click OK. This will launch the Active Directory Domain Services Installation Wizard.
5. On the welcome page, click `Next`.
6. On the Operating System Compatibility page, click `Next`.
7. On the Choose a Deployment Configuration page, select the `Create a new domain in a new forest` option, and click `Next`.

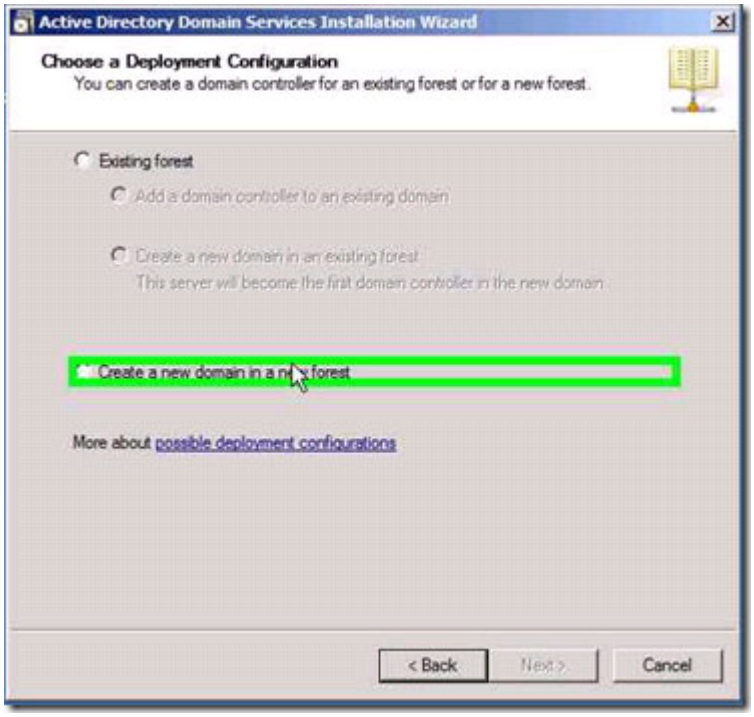

Figure 9: Choose a Deployment Configuration Page

8. On the Name the Forest Root Domain page, enter the fully qualified domain name (FQDN) of the forest root domain and click `Next`.

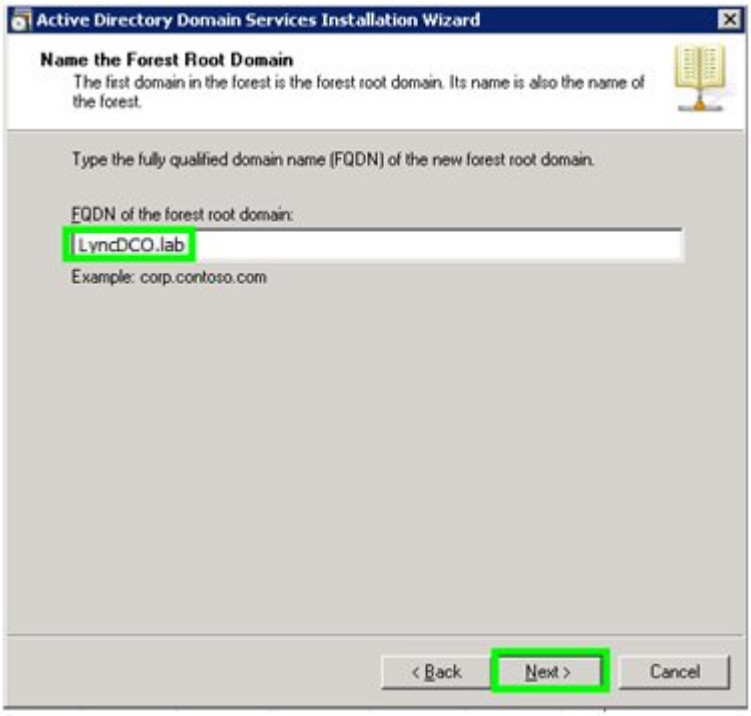

Figure 10: Name the Forest Root Domain Page

9. On the Set Forest Functional Level page, select Windows Server 2008 R2 and click `Next`.

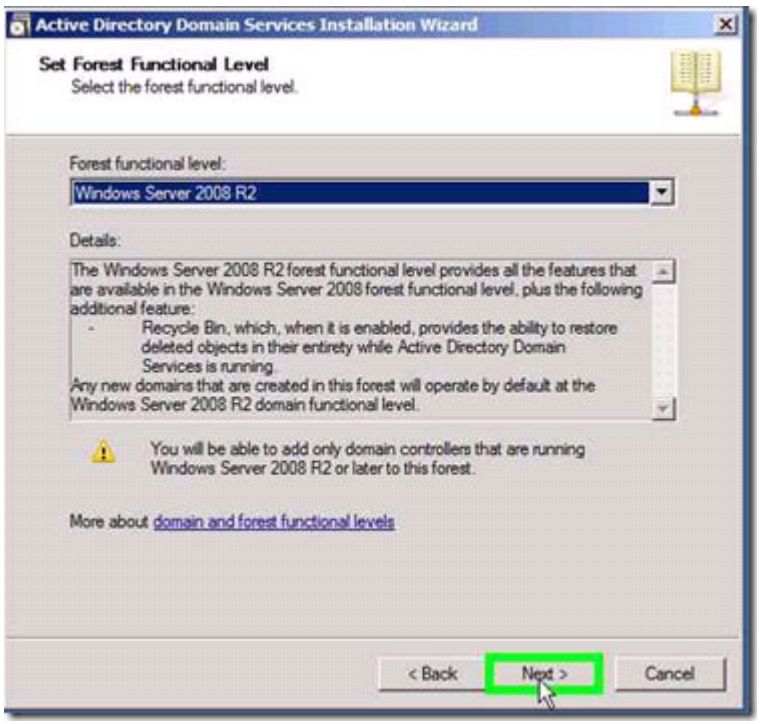

Figure 11: Set Forest Functional Level Page

10. On the Additional Domain Controller Options page, ensure that `DNS server` is selected, and click `Next`.

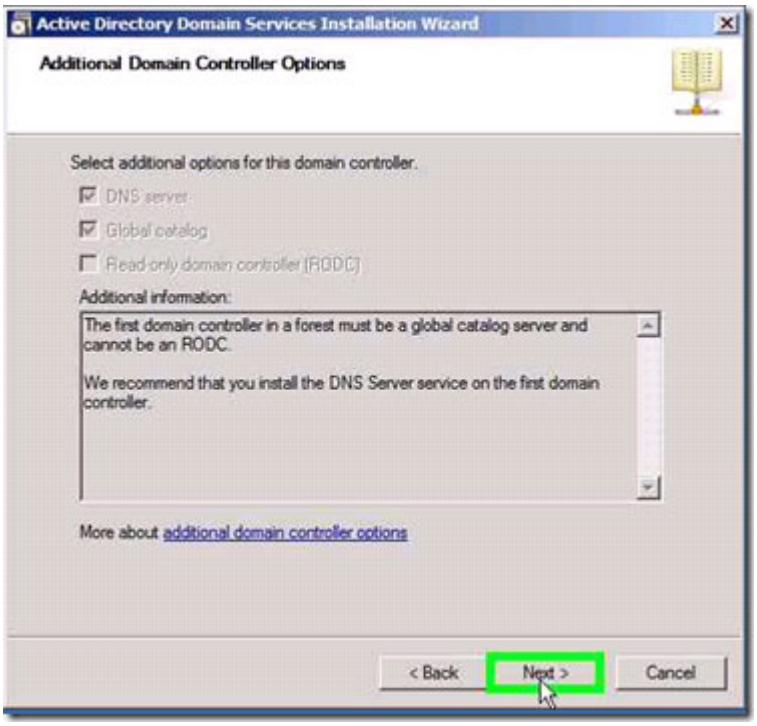

Figure 12: Additional Domain Controller Options Page

11. Click `Yes` on the delegation for DNS server warning.

Figure 13: DNS Server Warning

12. On the Location for Database, Log files, and SYSVOL page, accept the defaults, and click `Next`.

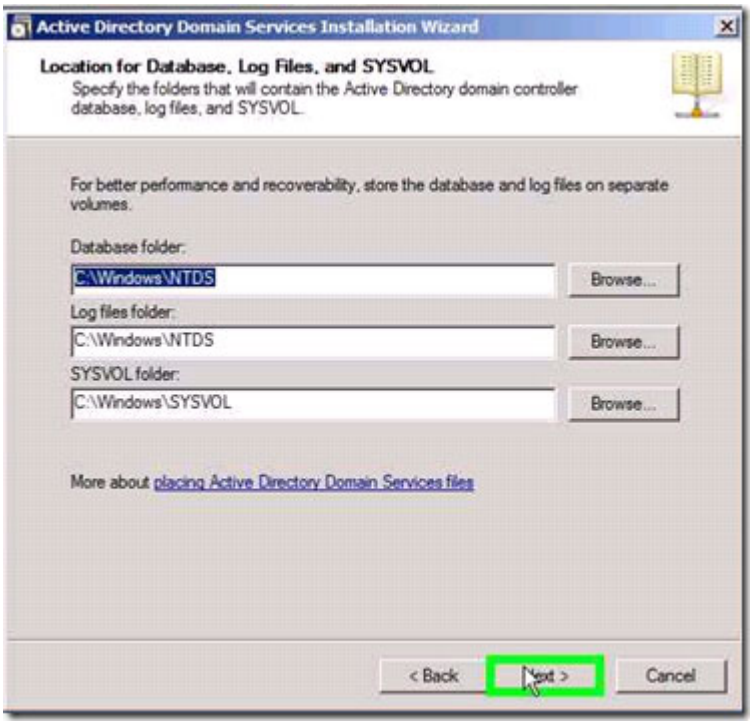

Figure 14: Location for Database, Log Files, and SYSVOL Page

13. On the Directory Services Restore Mode Administrator Password page, enter and confirm a password, and click `Next`.

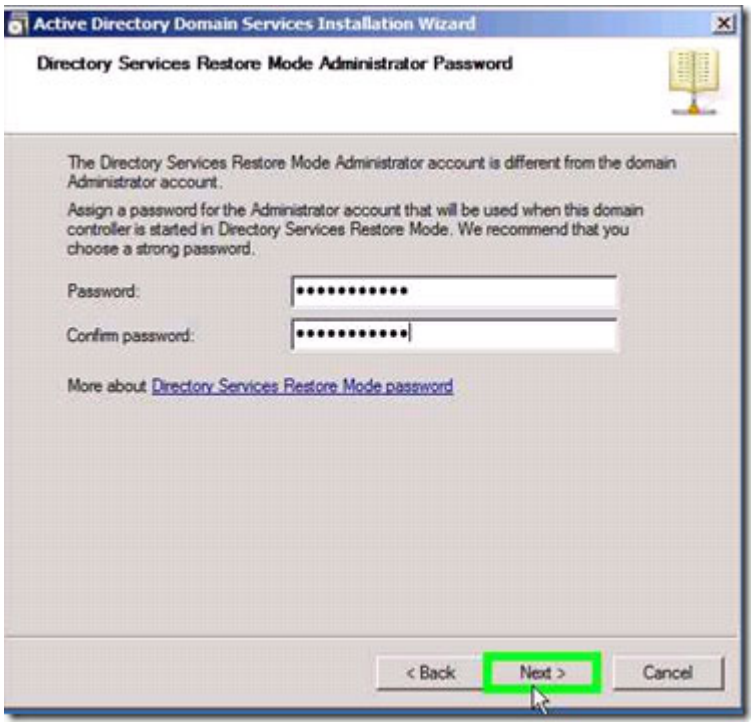

Figure 15: Directory Services Restore Mode Administrator Password Page

14. On the Summary page, verify the information and click `Next`.
15. Select the `Reboot on completion` option to reboot the server when the installation is complete.

End of procedure

Next Steps

- Procedure: Installing Active Directory Certificate Services

Installing Active Directory Certificate Services

Once your Windows server is configured as a Domain Controller (see Procedure: Installing Active Directory Domain Services), you must install the Active Directory Certificate Services.

Procedure:
Installing Active Directory Certificate Services

Purpose: To install Active Directory Certificate Services on the domain.

Prerequisites

- Procedure: Configuring Active Directory

Start of procedure

1. Log on to the Domain Controller as `[server name]\Administrator`.
2. Go to `Start > Administrative Tools > Server Manager`.
3. Access the Server Manager screen. From the Windows taskbar, select `Start > Administrative Tools > Server Manager`.
4. Under Roles Summary, click `Add Roles`.
5. At the welcome page for the wizard, click `Next`.

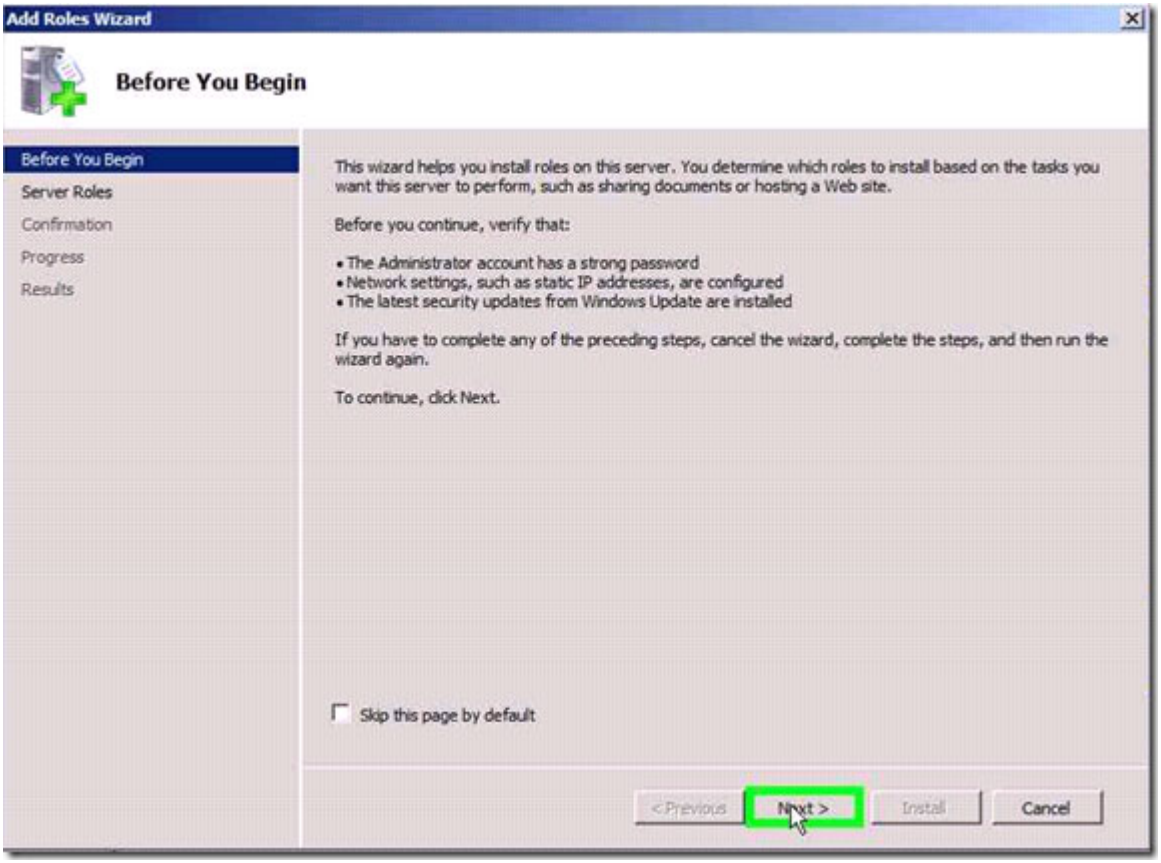

Figure 16: Add Roles Wizard

6. On the Select Server Roles page, select `Active Directory Certificate Services` and click `Next`.

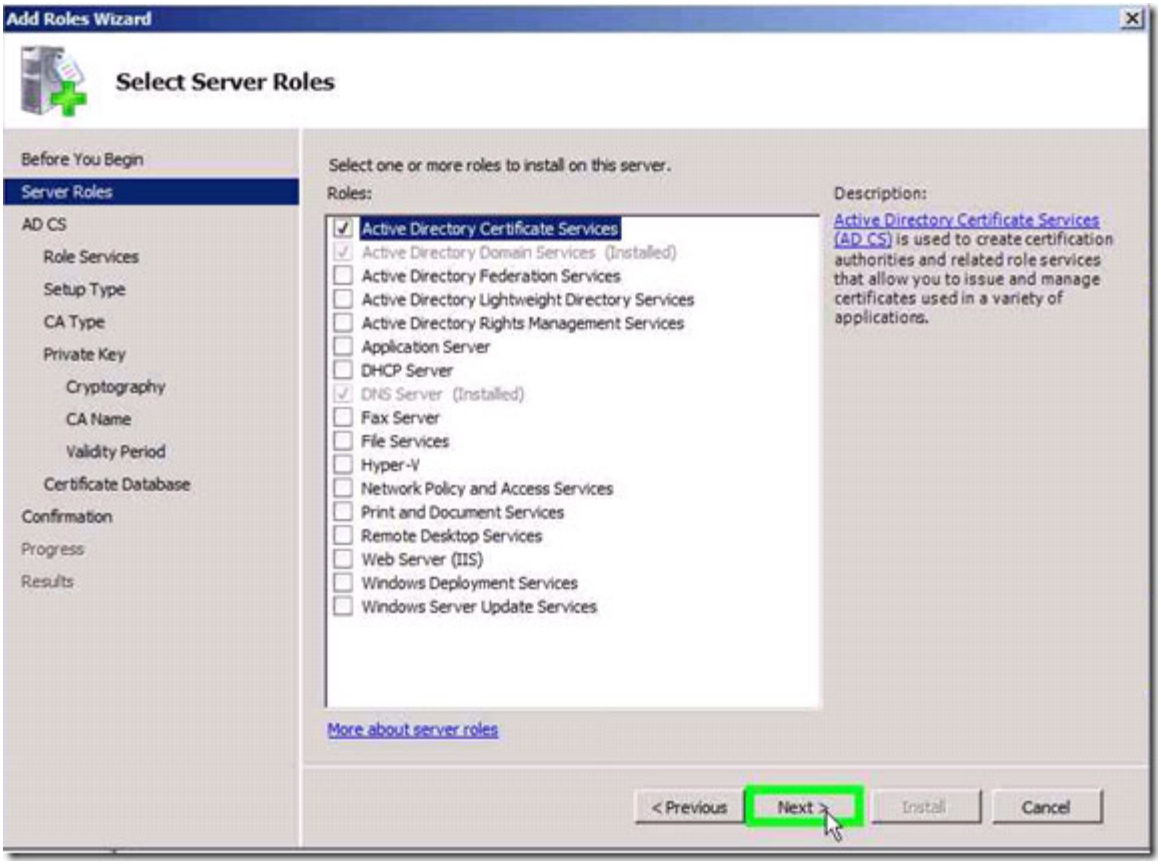

Figure 17: Select Server Roles Page

7. On the Introduction to Active Directory Certificate Services page, click `Next`.

8. On the Select Role Services page, ensure that both Certification Authority and Certification Authority Web Enrollment are selected, and click `Next`.

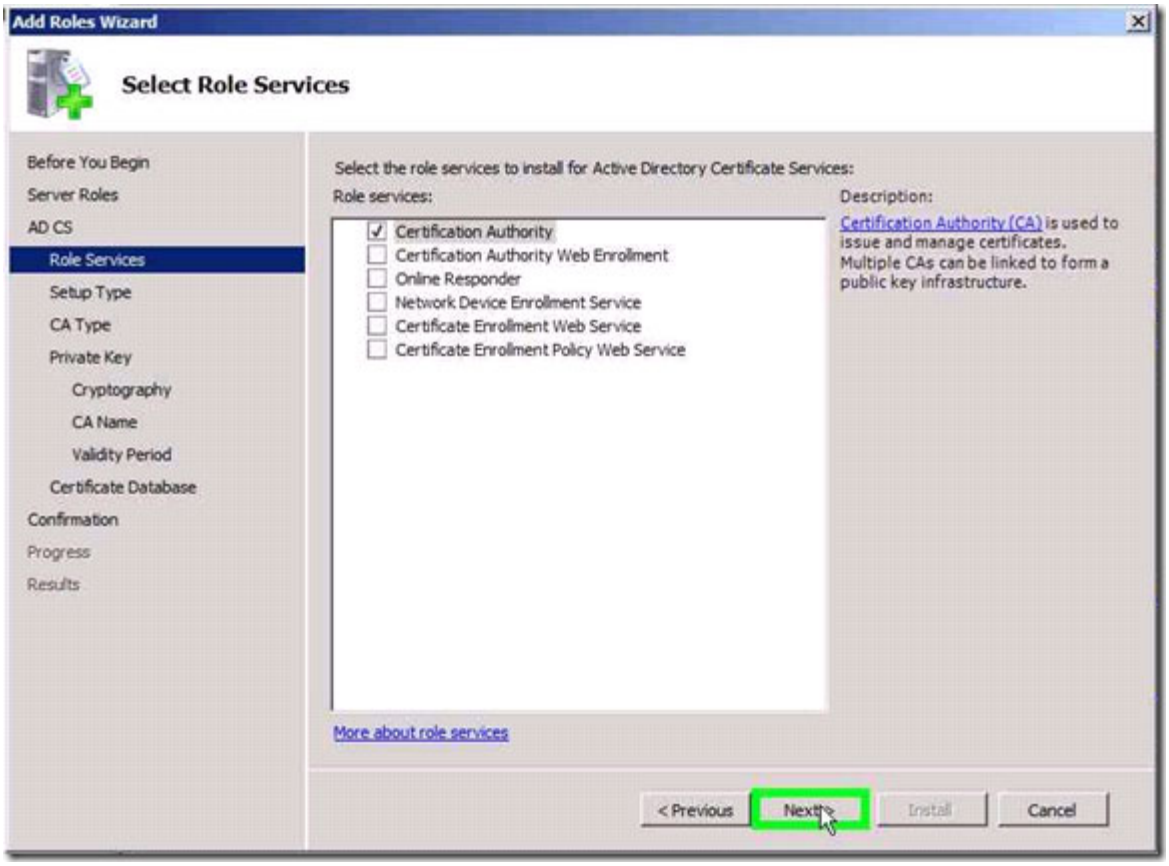

Figure 18: Select Role Services Page

9. On the Specify Setup Type page, ensure that Enterprise is selected and click `Next`.

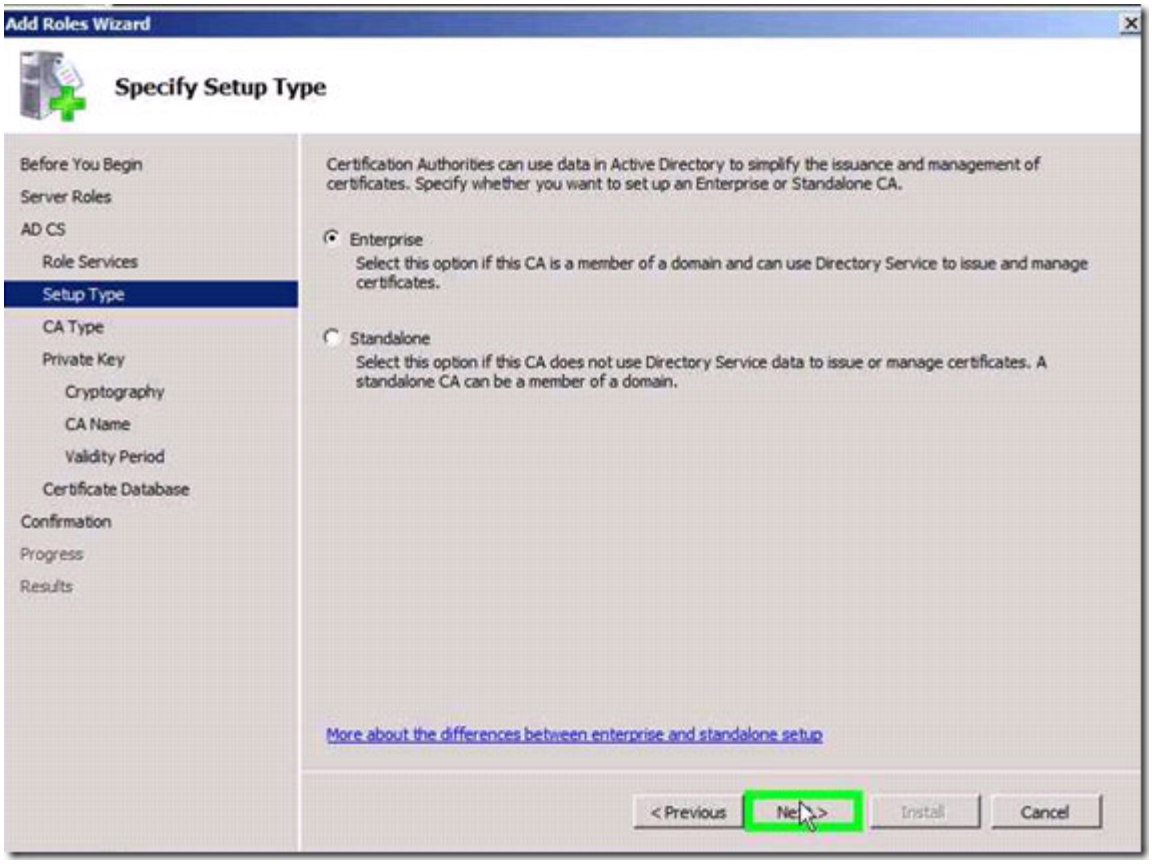

Figure 19: Specify Setup Type Page

10. On the Specify CA Type page, ensure that Root CA is selected and click `Next`.

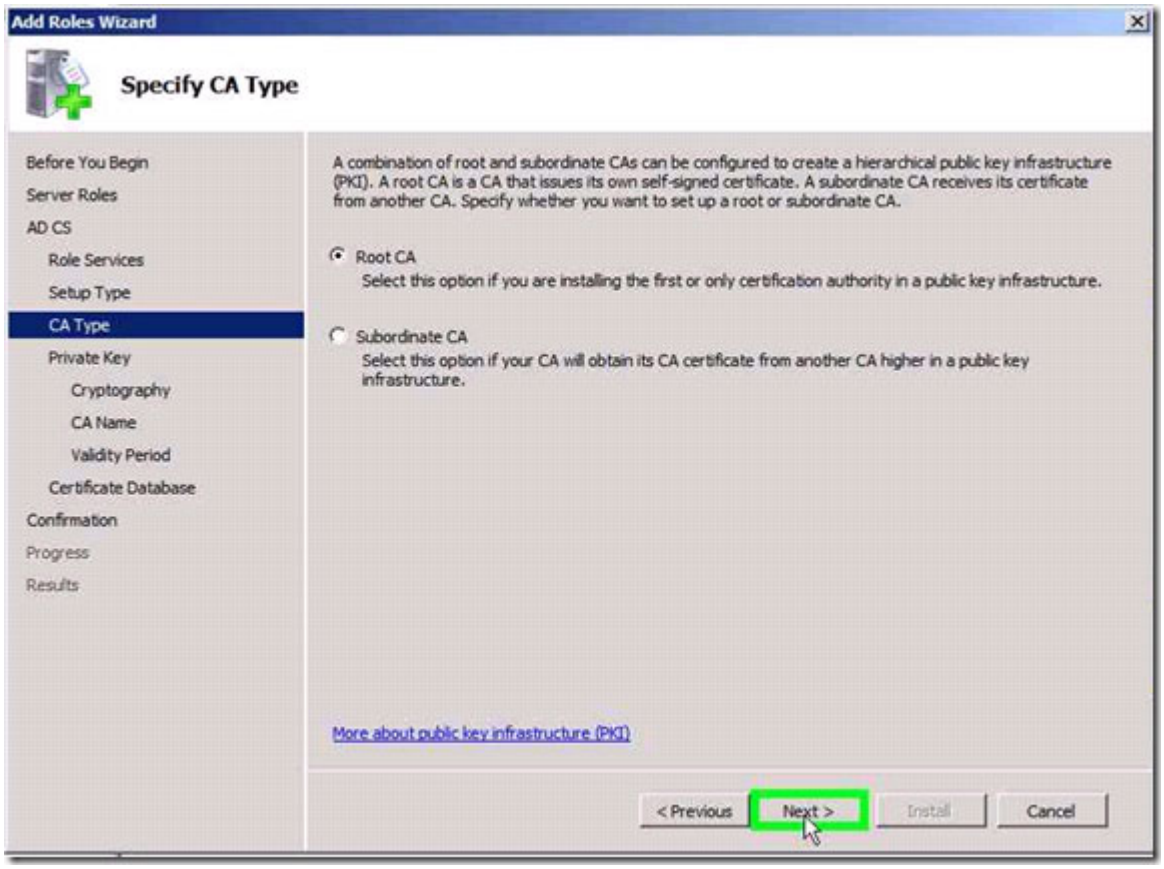

Figure 20: Specify CA Type Page

11. On the Set Up Private Key page, ensure that Create a new private key is selected, and click `Next`.

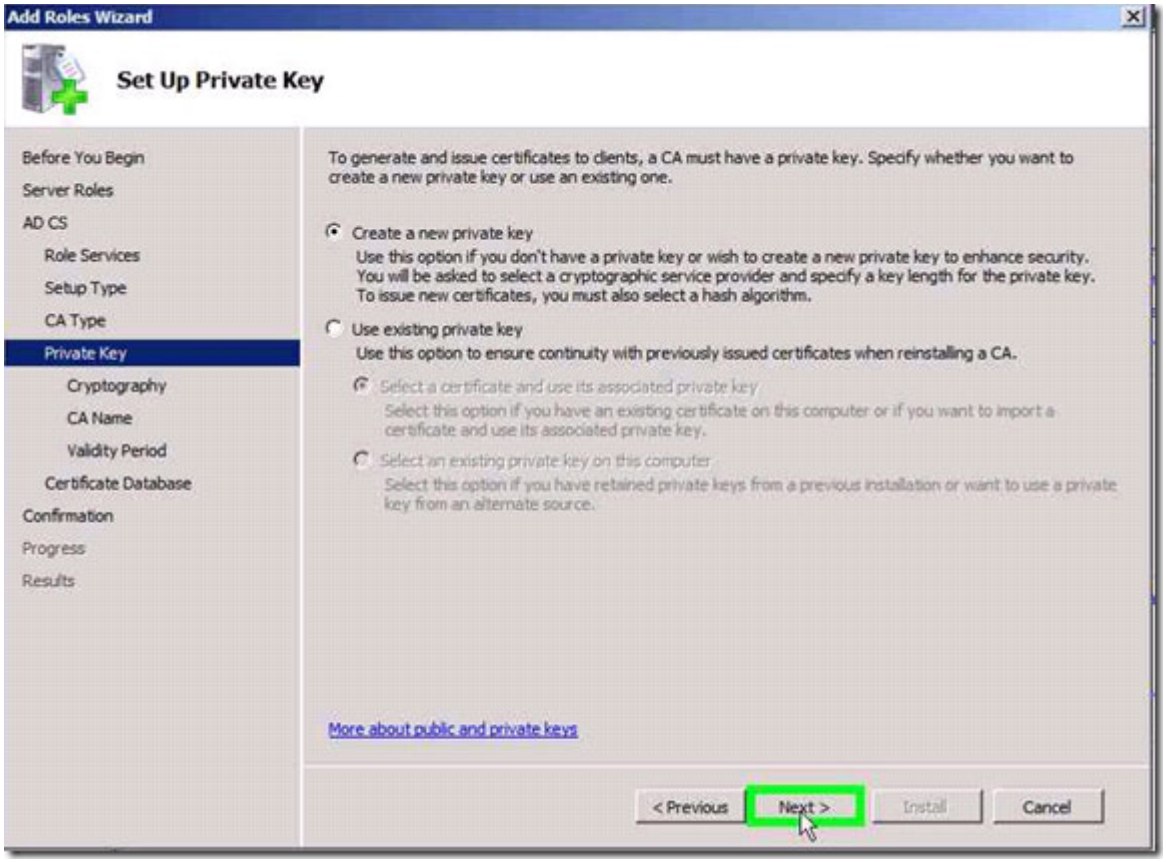

Figure 21: Set Up Private Key Page

12. On the Configure Cryptography for CA page, accept the defaults and click `Next`.

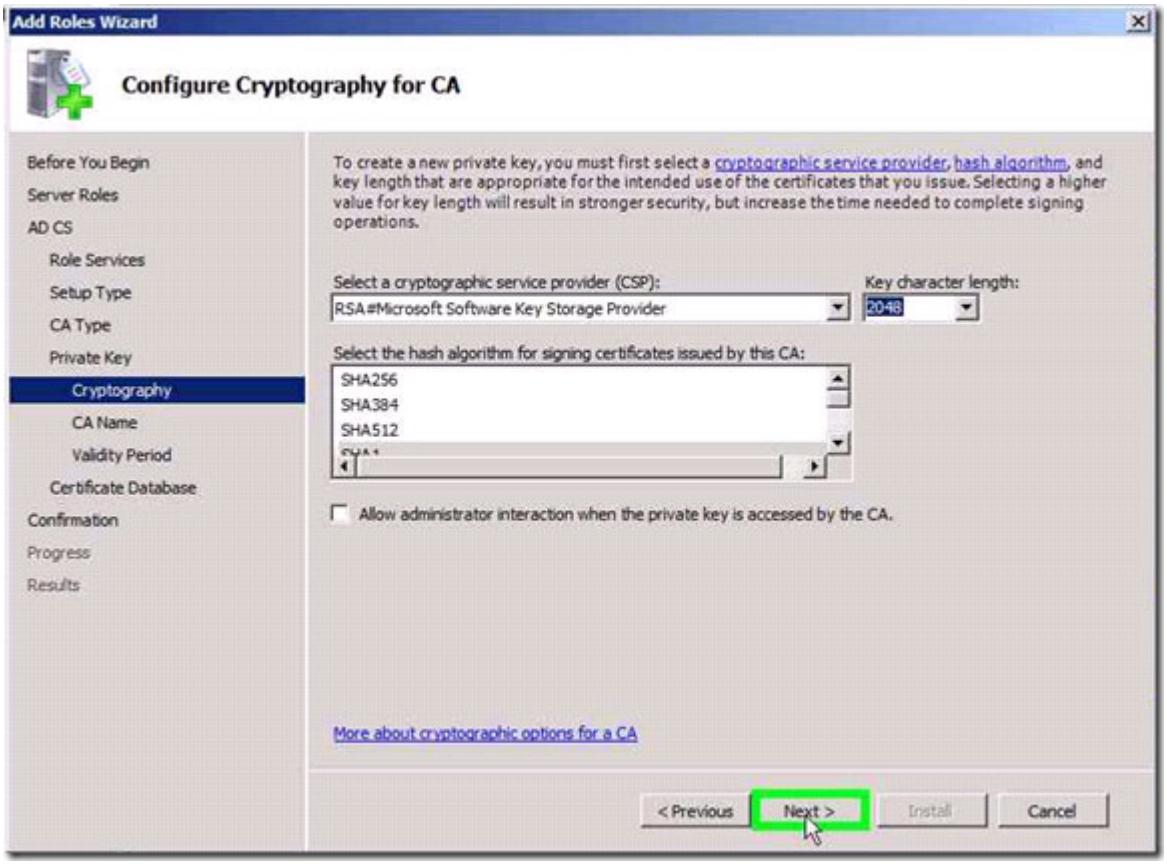

Figure 22: Configure Cryptography for CA Page

13. On the Configure CA Name page, accept the defaults and click `Next`.
14. On the Set Validity Period page, accept the defaults and click `Next`.
15. On the Configure Certificate Database page, accept the defaults and click `Next`.

16. On the Confirm Installation Selections page, click `Install`.

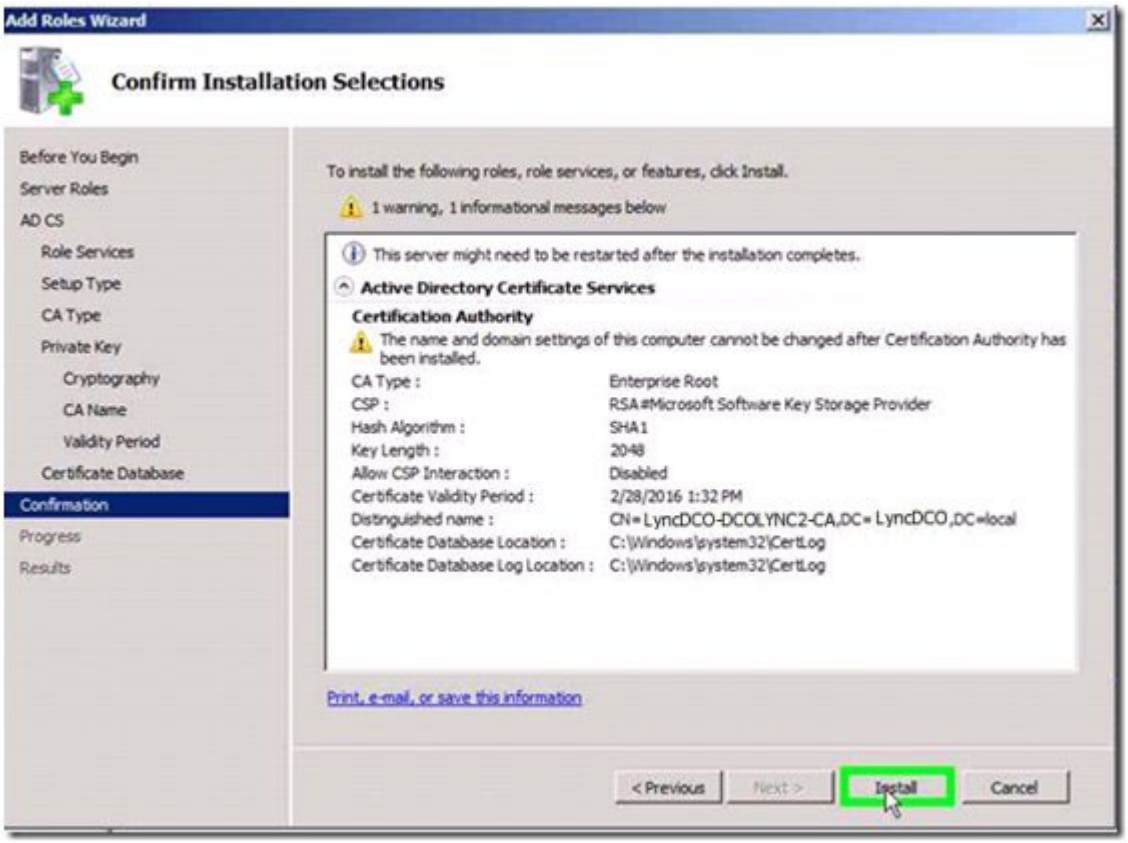

Figure 23: Confirm Installation Selections Page

17. Once the installation is complete, click `Close`.

End of procedure

Next Steps

- Procedure: Installing Lync Server 2010, on page 37

Chapter

4 Lync Installation

This chapter discusses creating and configuring the Lync Server environment on your Windows 2008 server.

This chapter contains the following sections:

Building the Environment

Procedure: Installing Lync Server 2010

Purpose: To install Lync Server 2010 on your Windows 2008 server.

Prerequisites

- Installing Active Directory Certificate Services, page 28

Start of procedure

1. Log on to the host where Lync Server 2010 will be installed. Log in as `[Domain-Name]\Administrator`.
2. Mount the Lync Server 2010 installation media.
3. Navigate to the appropriate hardware-specific directory in the installation media, for example `\Setup\amd64`.

4. Execute the `setup.exe` file to start the Deployment Wizard.
5. If it is not already installed, you will be prompted to install Microsoft Visual C++ 2008. Click `Yes` to install it.

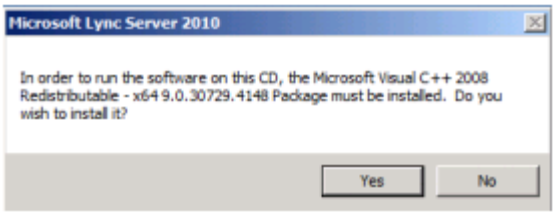

Figure 24: Visual C++ 2008 Installation Prompt

6. You will be presented with the following window. Adjust the installation location if you desire, and then click `Install`.

Figure 25: Microsoft Lync Server 2010 Installation Location

7. On the License Agreement page, accept the end–user license agreement, and then click `OK`.

8. Once the installation of the Deployment Wizard is complete, you will be presented with the Lync Server 2010 Deployment Wizard. Click `Install Topology Builder`. After installation, the Deployment Wizard displays a green check mark next to Install Topology Builder.

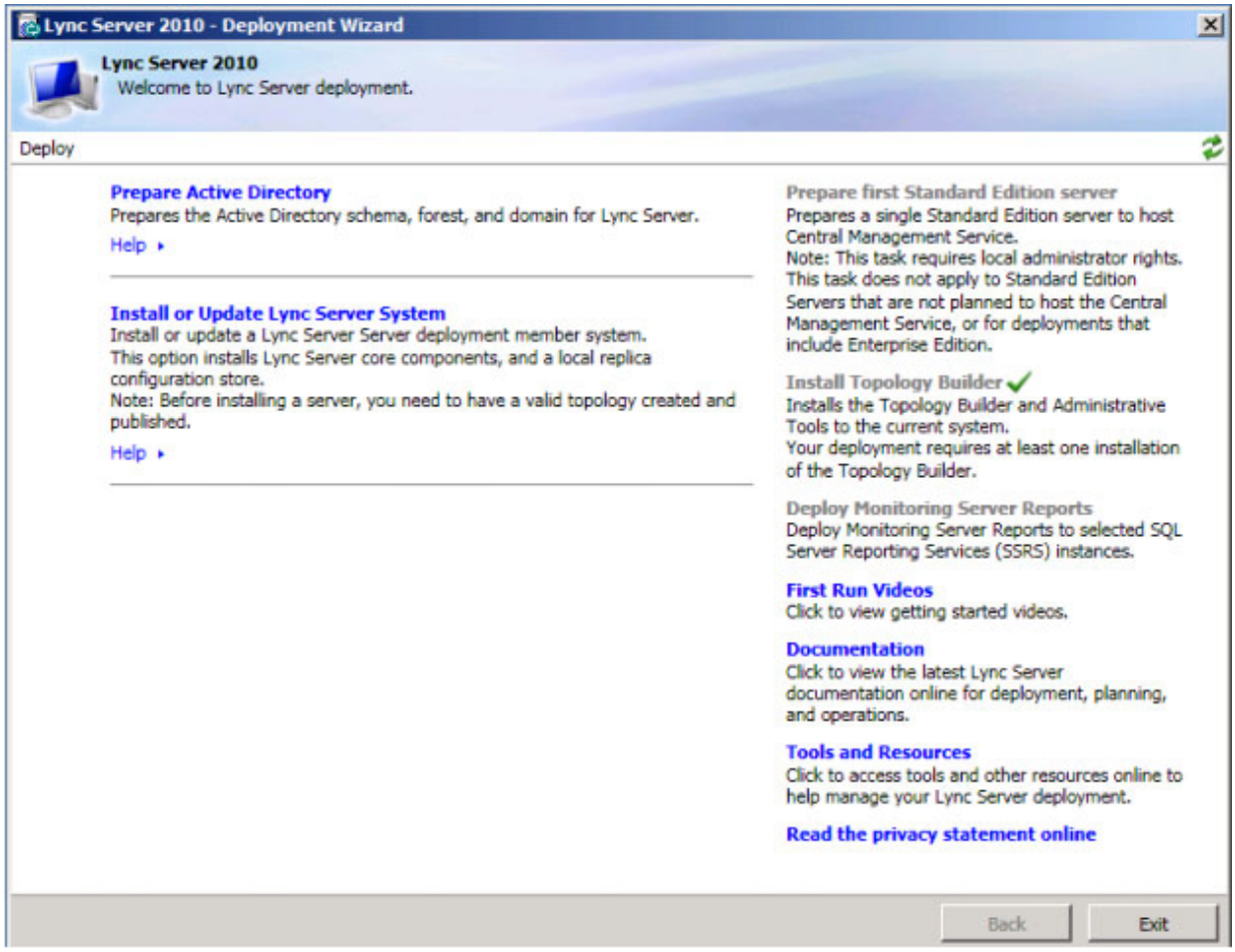

Figure 26: Lync Server 2010 Deployment Wizard

9. Click `Prepare Active Directory`.

10. On the Prepare Active Directory for Lync Server page, click `Run` under `Step 1`.

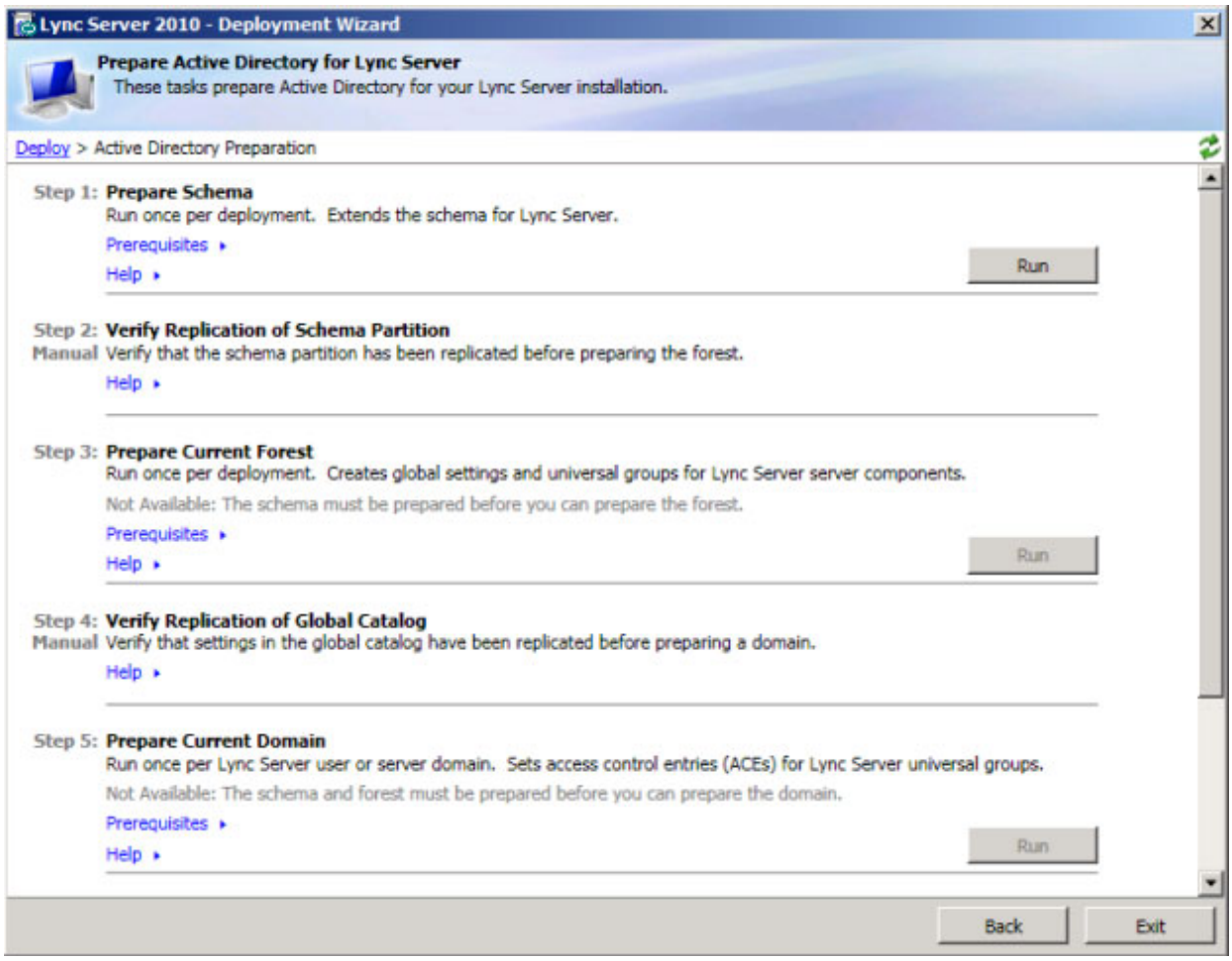

Figure 27: Prepare Active Directory for Lync Server Page

11. On the Prepare Schema window, click `Next`.

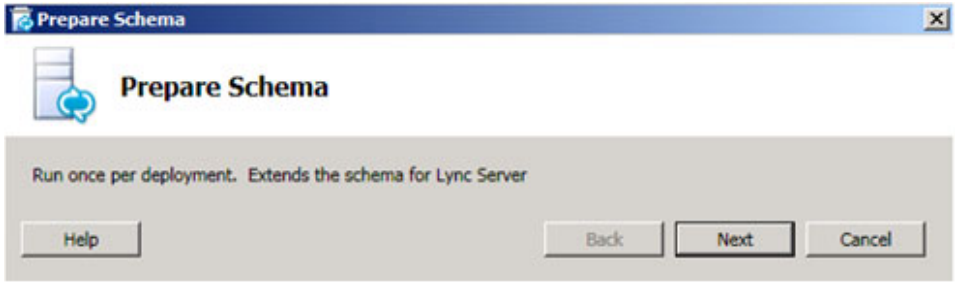

Figure 28: Prepare Schema Window

12. On the Executing Commands page, verify that the Task Status shows Completed, then click `Finish`.

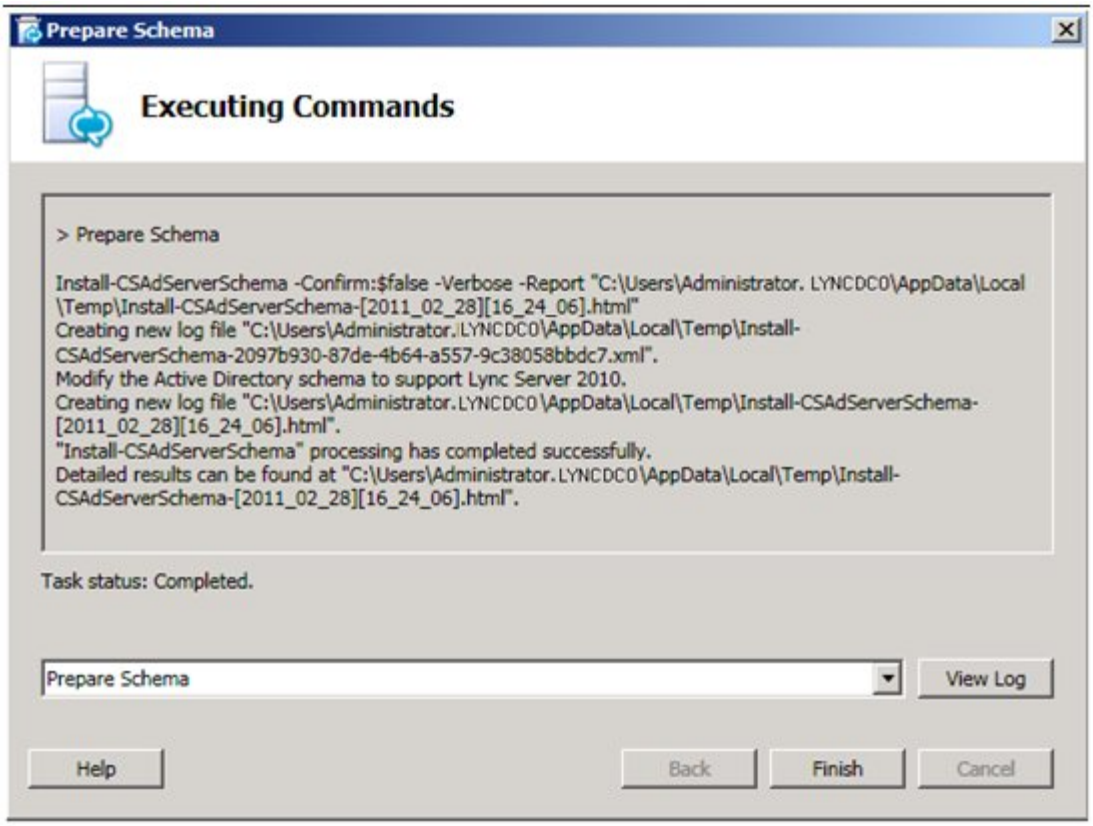

Figure 29: Task Status Completed

13. On the Prepare Active Directory for Lync Server page, click `Run` under `Step 3`.

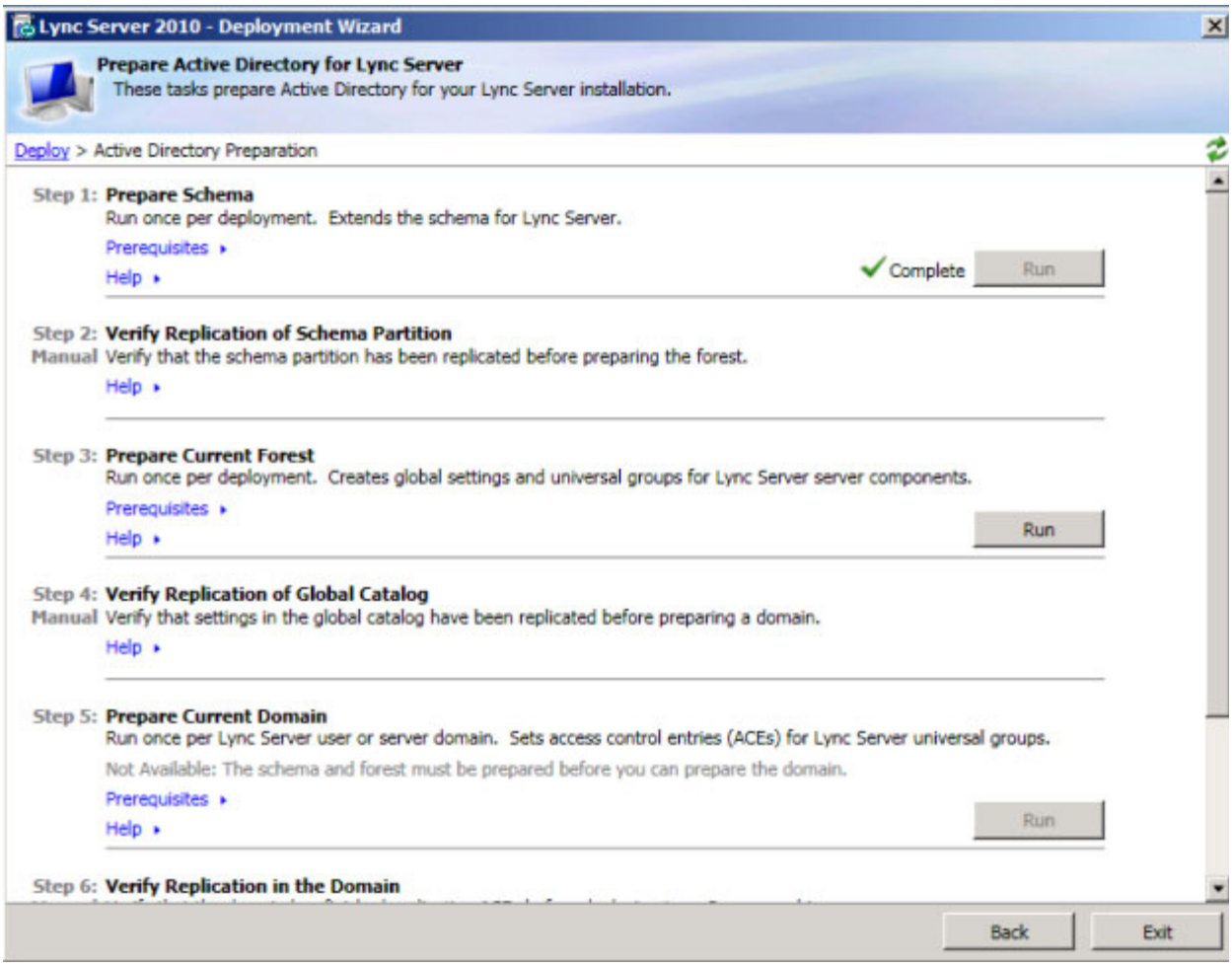

Figure 30: Prepare Schema Completed

14. On the Prepare Forest window, click `Next`.

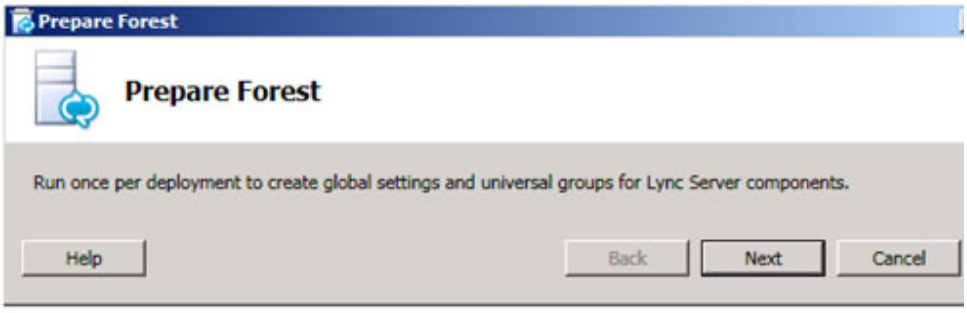

Figure 31: Prepare Forest Window

15. On the Universal Group Location page, leave the `Local domain` option selected and click `Next`.

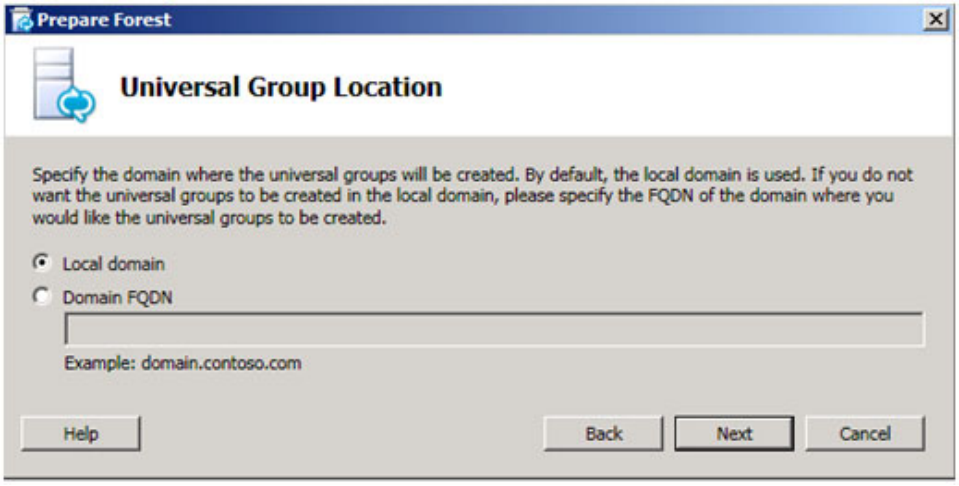

Figure 32: Universal Group Location Page

16. On the Executing Commands page, verify that the Task Status shows Completed and click `Finish`.

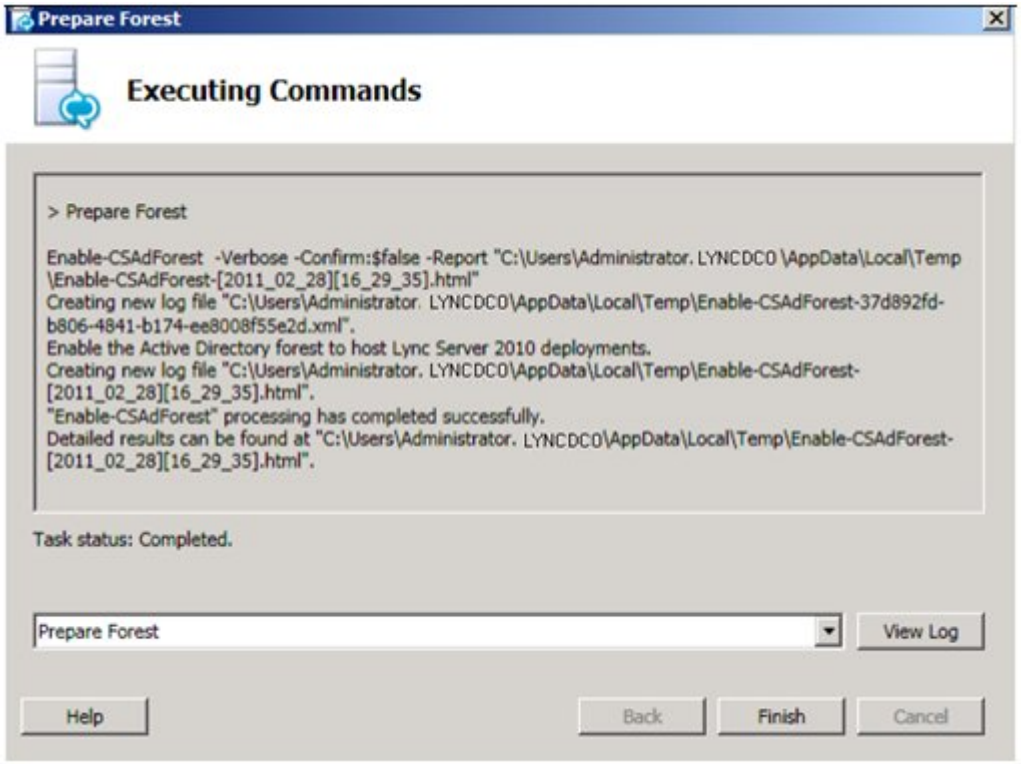

Figure 33: Task Status Completed

17. On the Prepare Active Directory for Lync Server page, click `Run` under `Step 5`.

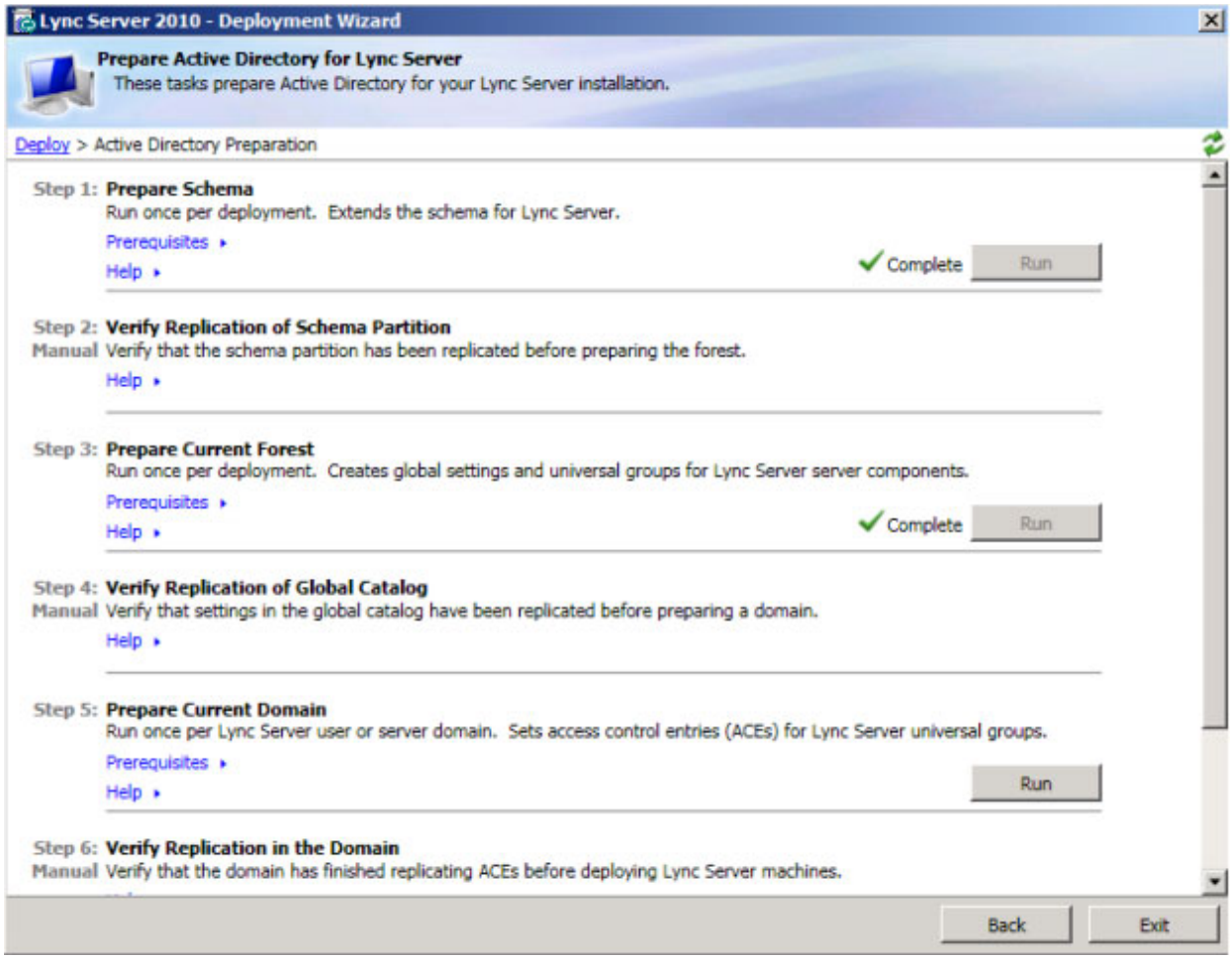

Figure 34: Prepare Current Forest Completed

18. On the Prepare Domain window, click `Next`.

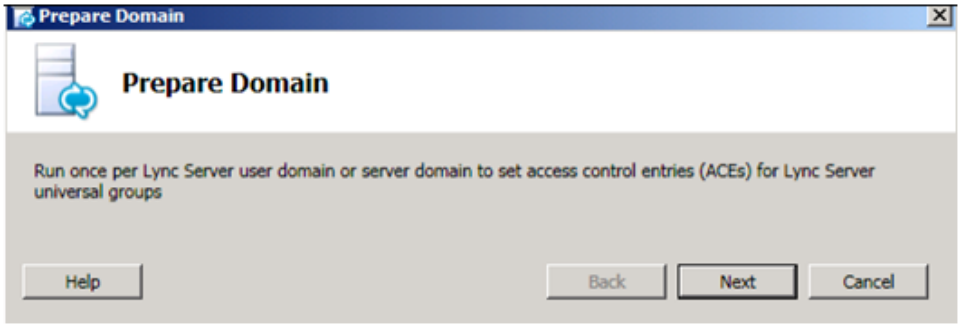

Figure 35: Prepare Domain Window

19. On the Executing Commands page, verify that the Task Status shows Completed, and click `Finish`.

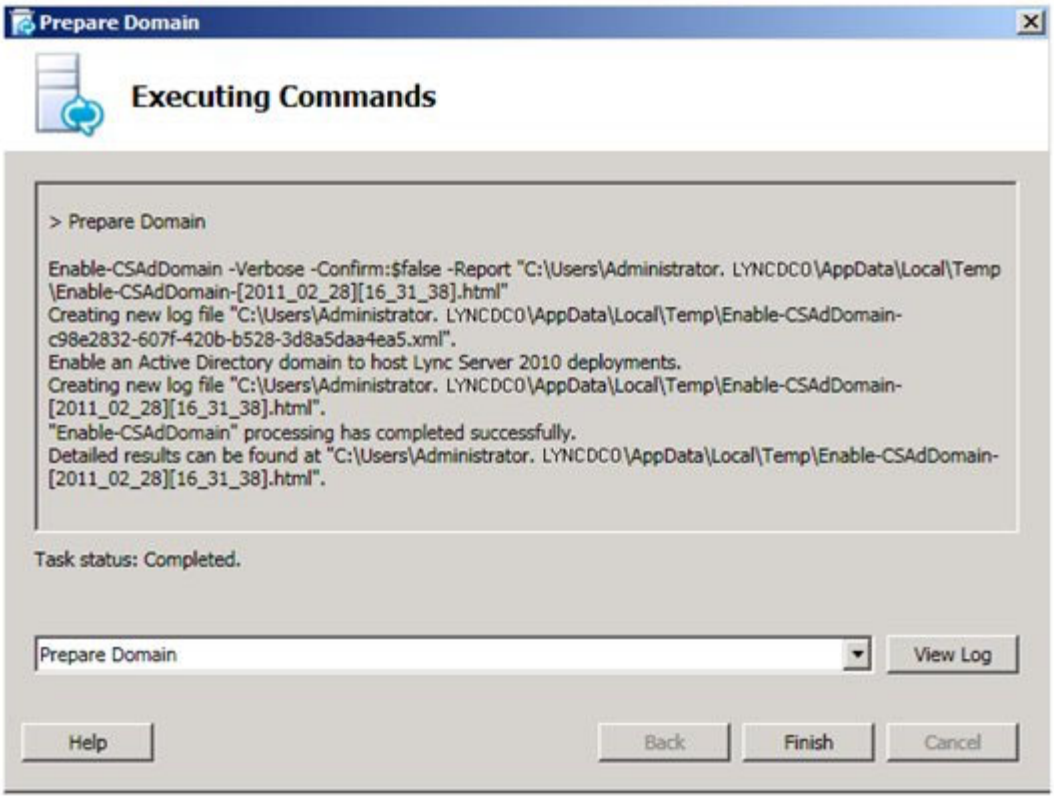

Figure 36: Task Status Completed

End of procedure

Next Steps

- Granting Setup Permissions, page 45

Procedure: Granting Setup Permissions

Purpose: To grant permissions to users so that they can run the Lync Server 2010 setup program.

Note: In this procedure, the machine has a single user account which also happens to have built-in Active Directory elevated permissions. However, this account still needs some specific Lync Server 2010 permissions.

Prerequisites

- Installing Lync Server 2010, page 37

Start of procedure

1. Log into the Lync Server host as `[Domain-name]\Administrator`.
2. Go to `Start > Administrative Tools`, and then click `Active Directory Users and Computers`.
3. In the console tree of Active Directory Users and Computers, expand the domain that you are using for Lync. Select the `Users` container.
4. In the details pane, locate the `RtcUniversalReadOnlyAdmins` group, right-click on it, and select `Properties`.
5. On the RtcUniversalReadOnlyAdmins Properties window, click the `Members` tab.

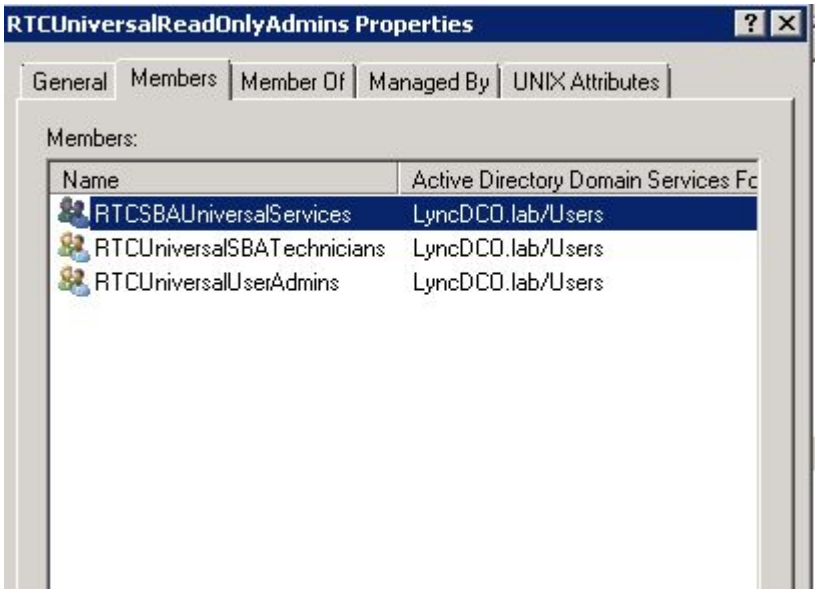

Figure 37: RTCUniversalReadOnlyAdmins Properties Window

6. Click `Add`.

7. On the Select Users, Contacts, Computers, Service Accounts, or Groups window type `Administrator` in the `Enter the object names to select` field, and then click `OK`.

Figure 38: Select Users, Contacts, Computers, Service Accounts, or Groups Window

8. On the RtcUniversalReadOnlyAdmins Properties page, click `OK`.
9. Leave the Active Directory Users and Computers console open.

End of procedure

Next Steps

- Procedure: Granting Administrative Permissions

Procedure: Granting Administrative Permissions

Purpose: To grant permissions to users so that they can run the Lync Server 2010 administration program.

Prerequisites

- Procedure: Installing Lync Server 2010

Start of procedure

1. In the details pane of the Active Directory Users and Computers console, locate the `CsAdministrator` group, right-click it, and select `Properties`.
2. On the CSAdministrator Properties window, click the `Members` tab.

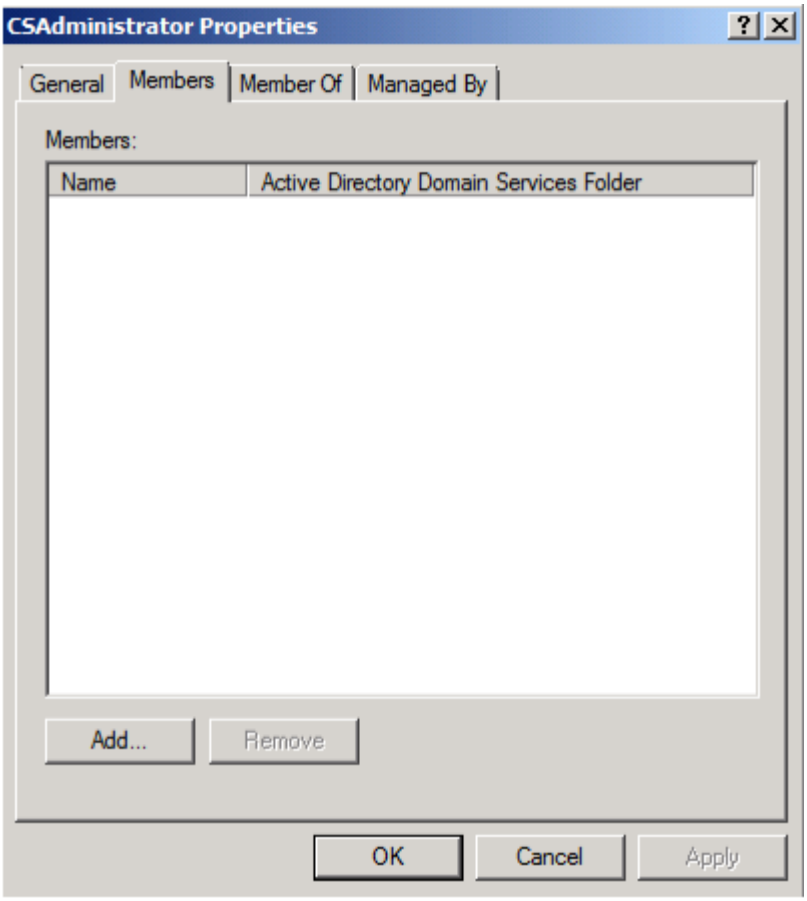

Figure 39: CSAdministrators Properties Page

3. Click `Add`.

4. On the Select Users, Contacts, Computers, Service Accounts or Groups window, type `Administrator` in the `Enter the object names to select field` and then click `OK`.

Figure 40: Select Users, Contacts, Computers, Service Accounts or Groups Window

End of procedure

Next Steps

- Procedure: Adding DNS Records

Procedure: Adding DNS Records

Purpose: To add the following DNS records as part of the infrastructure preparation:

Table 1: DNS Records

Deployment Scenario	DNS Requirement
Standard Edition Server	An internal A record that resolves the fully qualified domain name (FQDN) of the server to its IP address. Note: This record will already exist. It was created when the virtual machine was joined to Active Directory.

Table 1: DNS Records (Continued)

Deployment Scenario	DNS Requirement
Admin URL	An internal A record that resolves to the FQDN of the admin URL to its IP address.
Automatic client sign-in	For each supported SIP domain, you must create a _sipinternals SRV record that maps to the FQDN of the Standard Edition server.

Start of procedure

1. Log on to the Domain Controller host as `[Domain-name]\Administrator`.
2. Go to `Start > Administrative Tools`, and then select `DNS`.
3. In the Console Tree, expand the tree, expand Forward Lookup Zones, and then select your domain
4. Right-click the name of your domain in the Console Tree, and then select `New Host (A or AAA)`.
5. In the New Host window, type `admin` in the `Name` field, enter the IP in the `IP address` field, and then click `Add Host`.

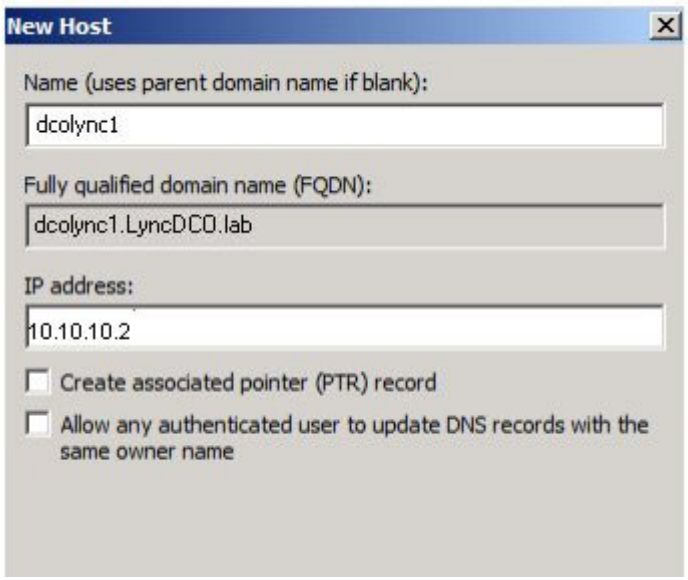

Figure 41: New Host Window

6. On confirmation that the host record was created, click `OK`.
7. In the console tree, right-click the your domain and then select `Other New Records`.

8. On the Resource Record Type window, select `Service Location (SRV)` and then click `Create Record`.

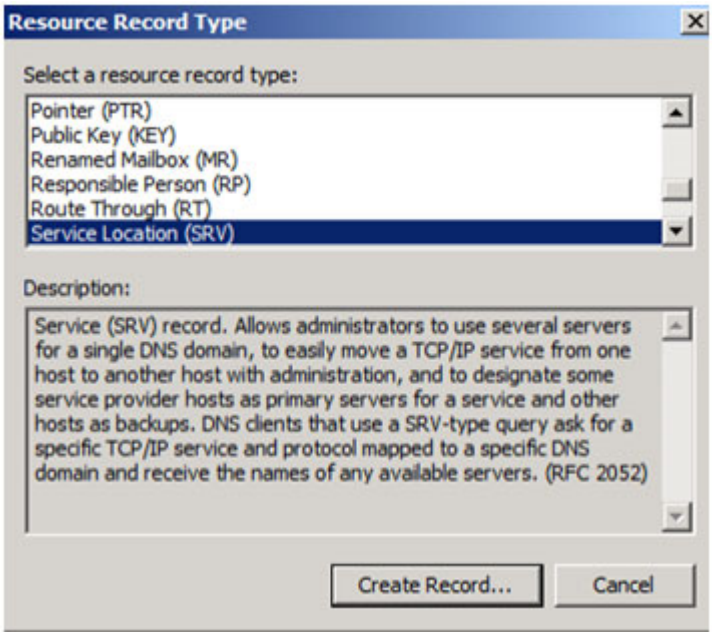

Figure 42: Resource Record Type Window

9. On the New Resource Record window, click `Service` and type `_sipinternaltls`
10. Click `Protocol` and `type _tcp`

11. Click `Port Number` and type `5061`

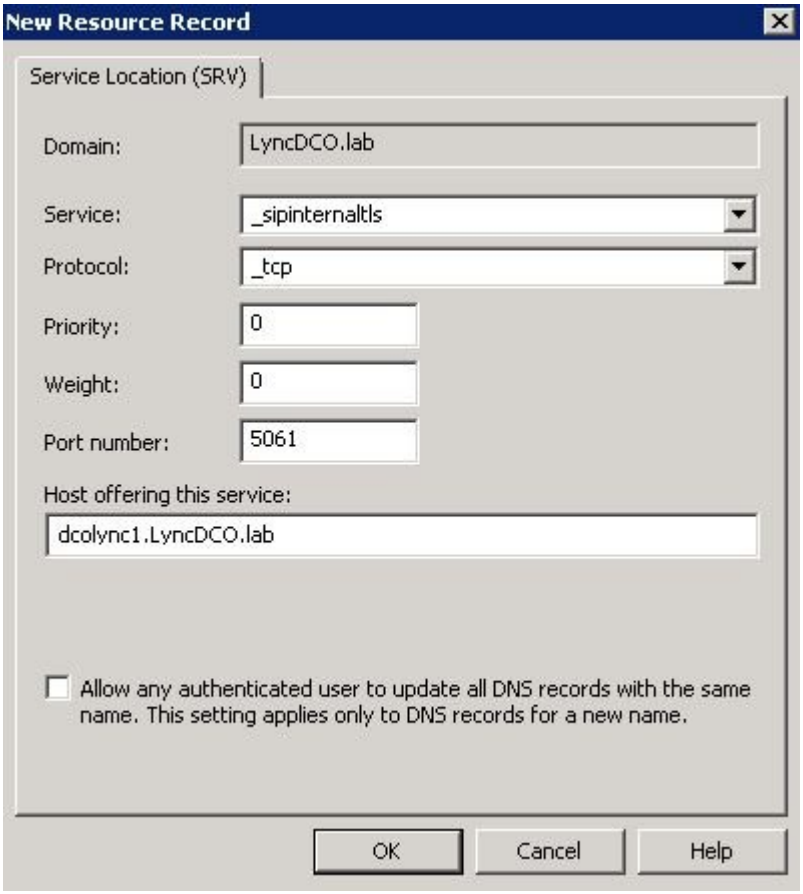

Figure 43: New Resource Record Window

12. In the `Host offering this service field`, type the string corresponding to `[lyncserverhostname].[domain-name].[high-level-domain]`
13. Click `OK`, and then click `Done`.

End of procedure

Next Steps

- Procedure: Creating the Lync File Share

Procedure: Creating the Lync File Share

Purpose: The user account used to publish the topology must have full control (read/write/modify) on the file share in order for Topology Builder to configure the required permissions. In the case of a Standard Edition Server,

the file share resides on the same server. In this example, the Administrator account is used to publish the topology and it already has sufficient NTFS permissions. However, you must still create a file share.

Start of procedure

1. Log on to the Lync Server host as `[Domain-name]\Administrator`.
2. Go to `Start > Computer > Local Disk (C:)`.
3. Right-click in the `Details Pane`, select `New`, and then select `Folder`.
4. Name the new folder `LyncShare`.
5. Right-click the `LyncShare` folder and select `Properties`. Click the `Sharing` tab, and then click `Advanced Sharing`.
6. On the Advanced Sharing window, select the `Share this folder` option and leave the `Share Name` field as `LyncShare`.

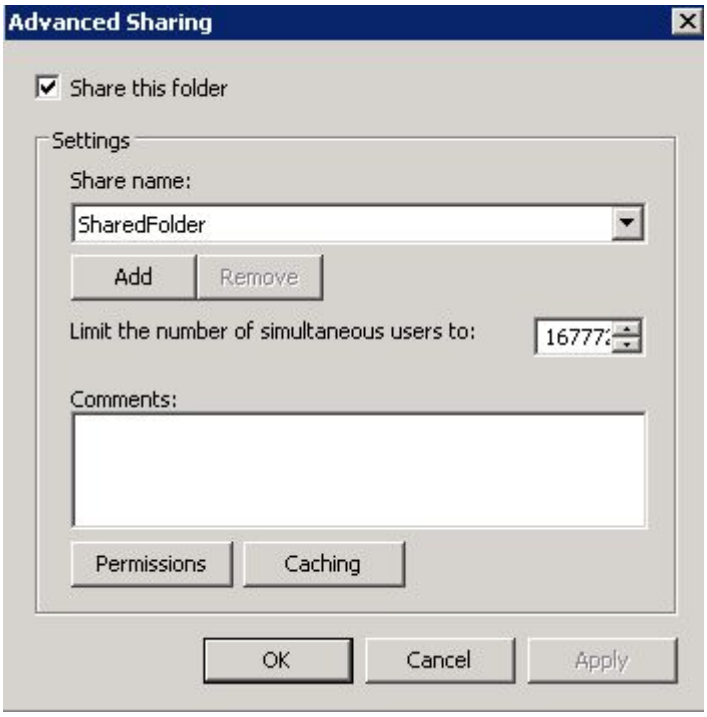

Figure 44: Advanced Sharing Window

7. Click Permissions.
8. On the Permissions for LyncShare window, check `Allow` next to `Full Control` (in addition to `Read` and `Change`) and then click `OK`.
9. Click `OK`, and then click `Close`.

End of procedure

Creating the New Topology

After installing Lync, you must define an initial topology. This section discusses the use of Lync Topology Builder, a Microsoft tool to manage topologies.

Procedure: Creating a Topology

Purpose: To create an initial topology using Lync Topology Builder.

Start of procedure

1. Click `Start > All Programs > Microsoft Lync Server 2010 > Lync Server Topology Builder`.
2. In Topology Builder, select `New Topology` and then save the topology `.tbxml` file.
3. On the Define the primary domain page, enter the `Primary SIP domain` and click `Next`.

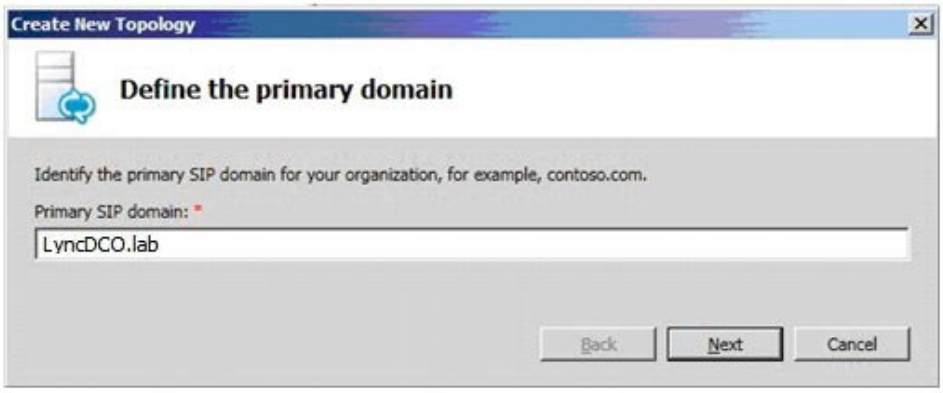

Figure 45: Define the Primary Domain Window

4. On the Specify additional supported domains window, click `Next`.

5. On the Define the first site page, enter a site name into the `Name` field, enter a description into the `Description` field, if desired and click `Next`.

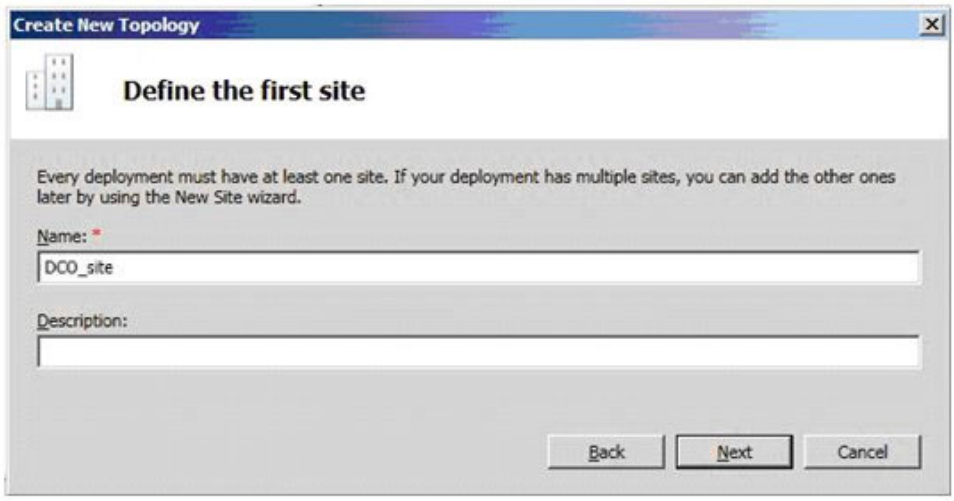

Figure 46: Define the First Site Name

6. On the Specify site details page, enter the location details and click `Next`.

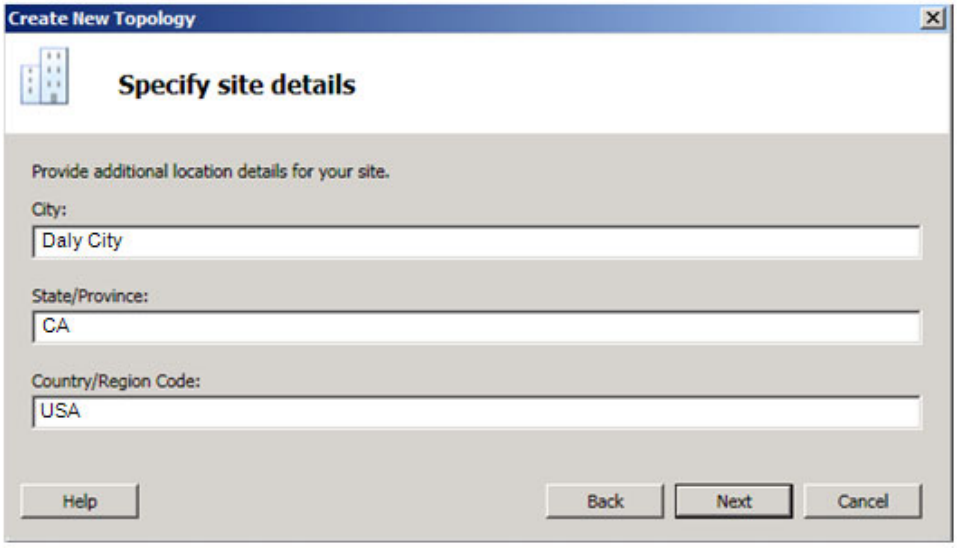

Figure 47: Specify the First Site Details

7. On the New topology was successfully defined page, ensure that the `Open the New Front End Wizard when this wizard closes` option is selected and click `Finish`.

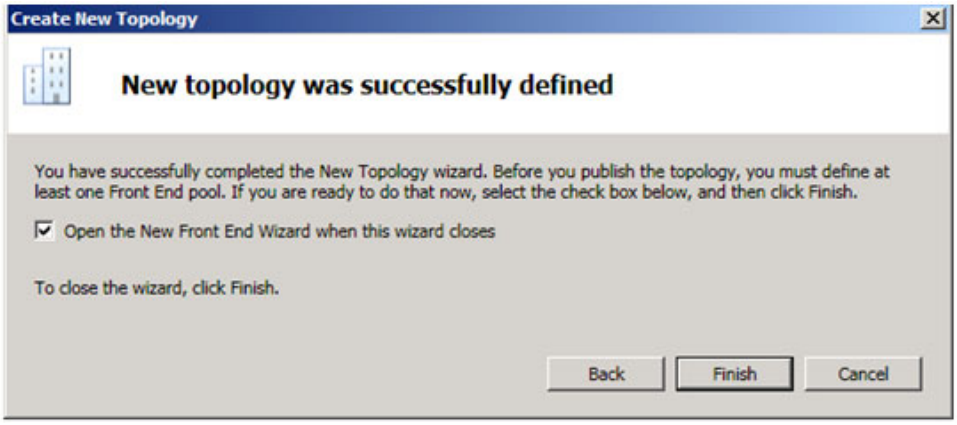

Figure 48: New Topology was Successfully Defined Window

8. On the Define the New Front End Pool wizard, click `Next`.

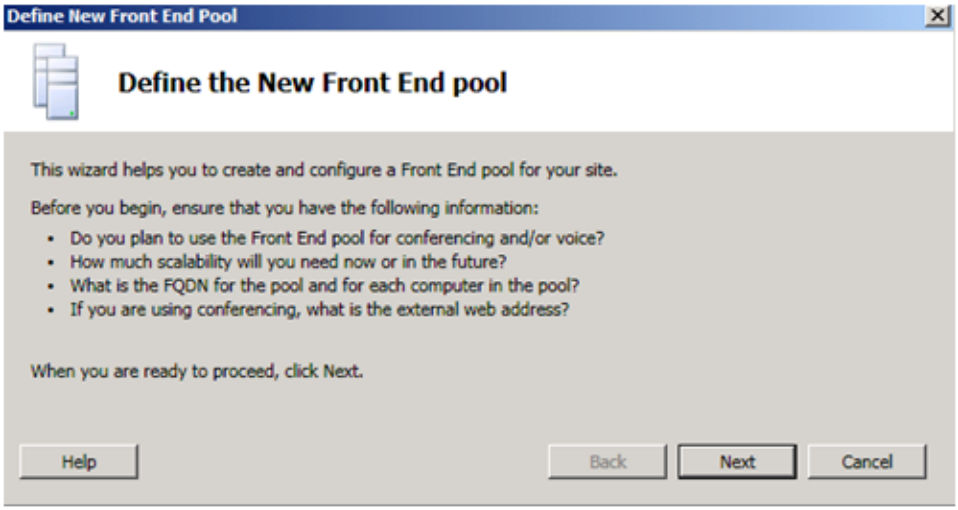

Figure 49: Define the New Front End Pool Wizard

9. On the Define the Front End pool FQDN page, type `[pool-name.domain-name]` into the `Pool FQDN` field. Ensure that the `Enterprise Edition Front End Pool` option is selected and click `Next`.

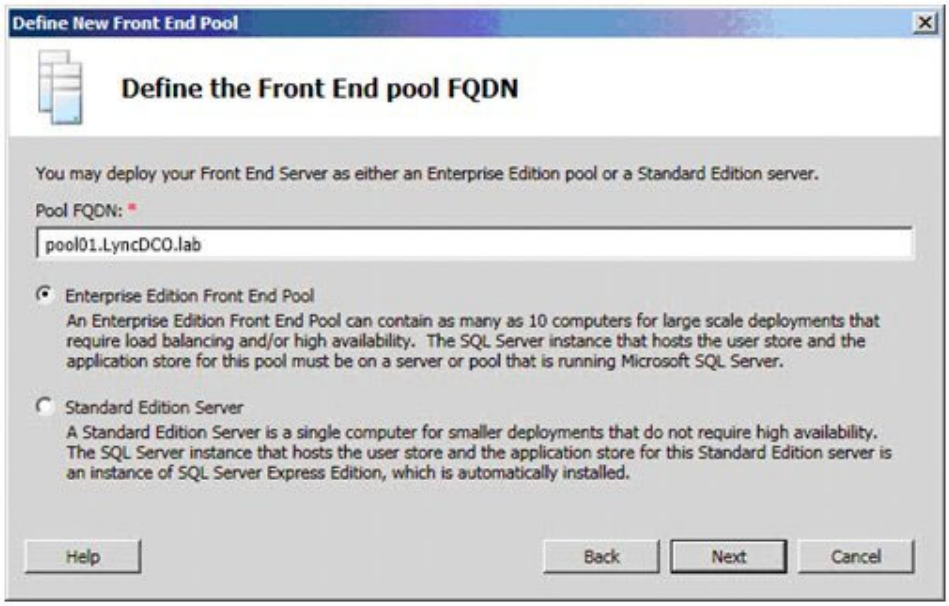

Figure 50: Define the Front End Pool FQDN Page

10. On the Define the computers in this pool page, specify the host where the Front End Server needs to be installed, and then click `Next`.

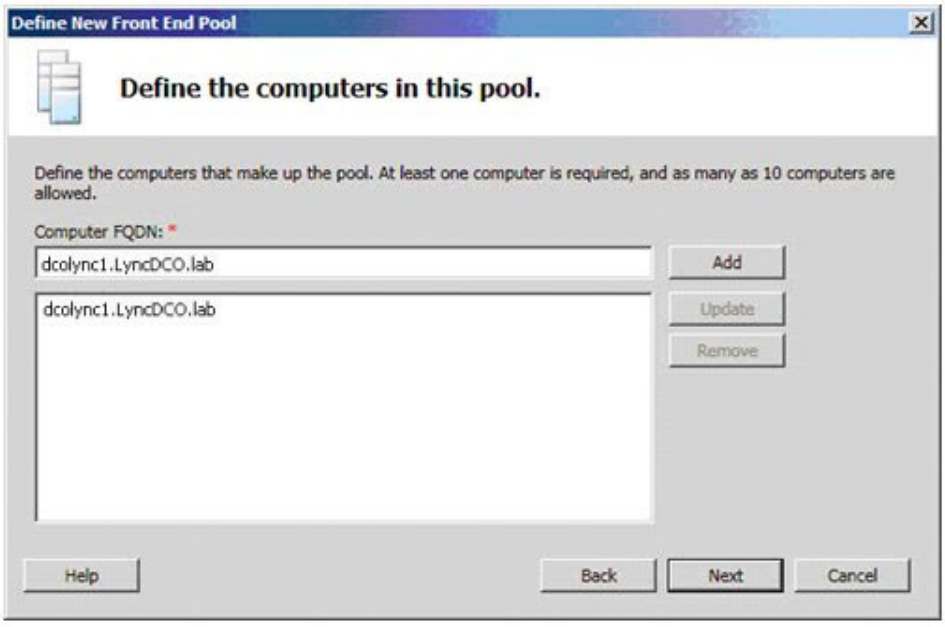

Figure 51: Define the Computers in this Pool Page

11. On the Select features page, leave all options unchecked and click `Next`.

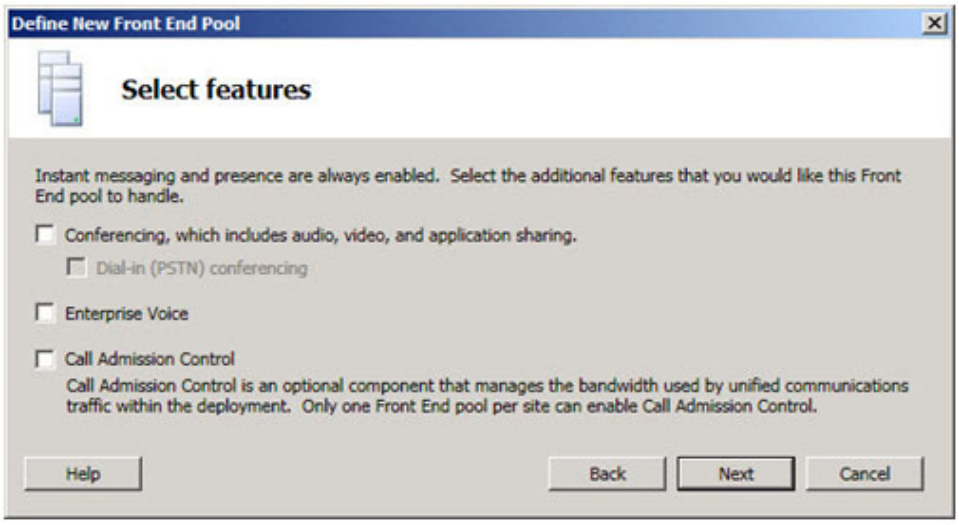

Figure 52: Select Features Page

Notes: The Conferencing option can be enabled later if required. For an example, see http://social.technet.microsoft.com/Forums/en-GB/ocsconferencing/thread/5a005491-72ec-4388-8e67-734f9a69fec8

Lync Enterprise Voice is required, but it will be added later.

12. On the Select collocated server roles page, leave all options unchecked and click `Next`.

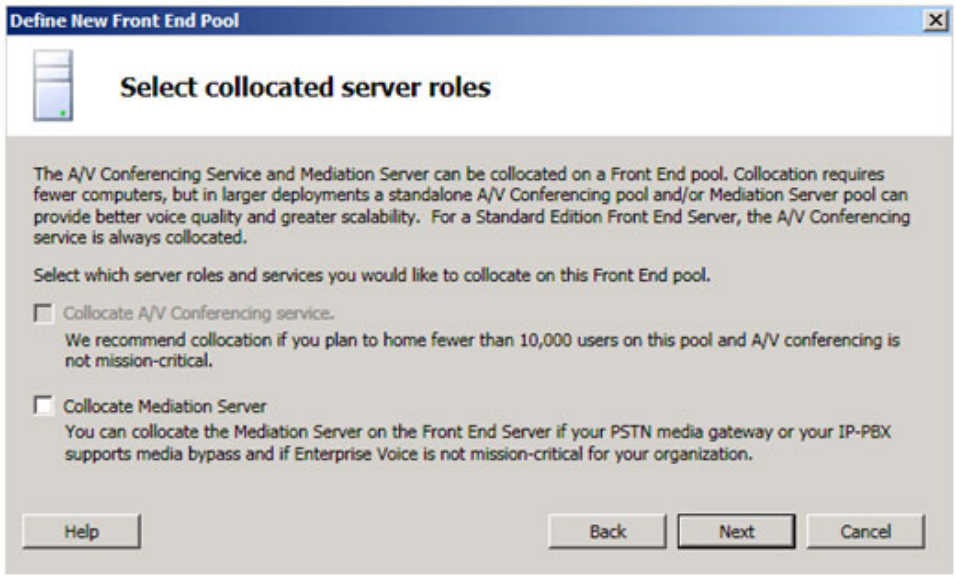

Figure 53: Select Collocated Server Roles Page

13. On the Associate server roles with this Front End pool page, ensure that all options are unchecked and click `Next`.

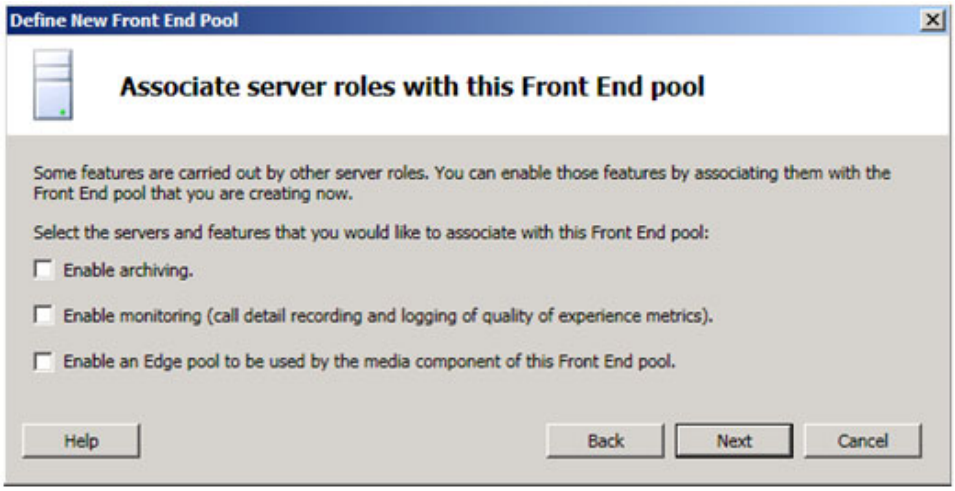

Figure 54: Associate Server Roles with this Front End Pool Page

14. On the Define the SQL store page, point to the location where SQL Server 2008 SP1 is installed and click `Next`.

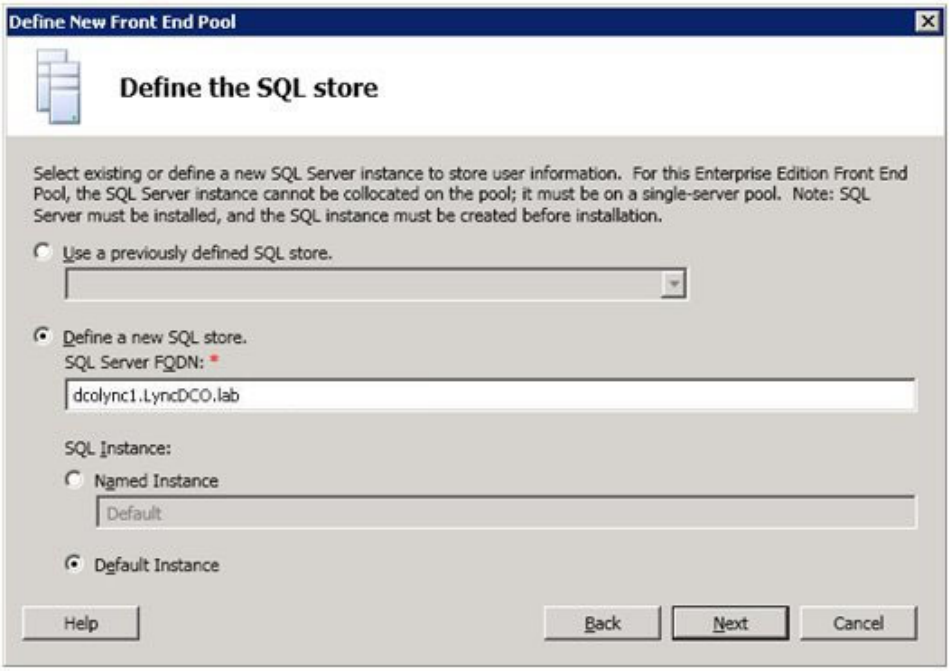

Figure 55: Define the SQL Store Page

15. On the Define the file share page, type `LyncShare` (the name of the share file defined in Procedure: Creating the Lync File Share, on page 52) in the `File Share` field, and click `Next`.

Figure 56: Define the File Share Page

16. On the Specify the Web Services URL page, click `Finish`.

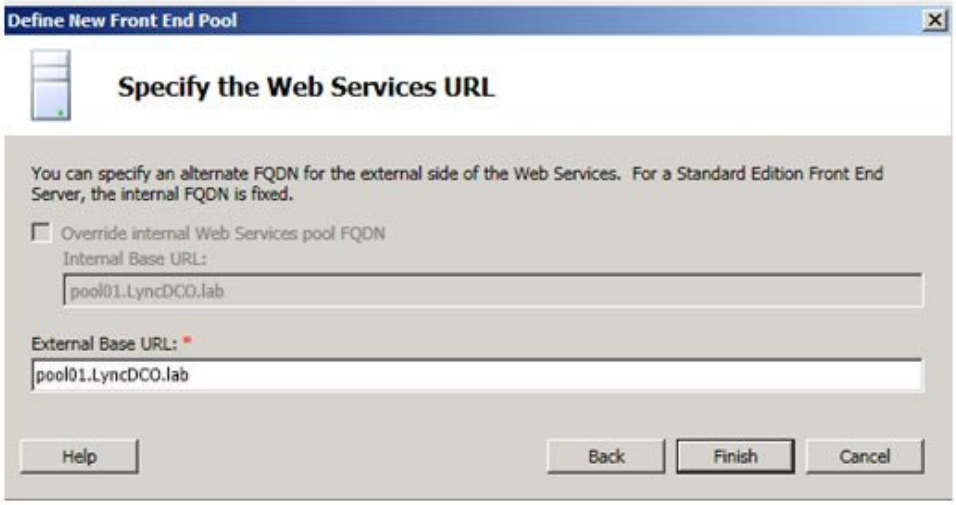

Figure 57: Specify the Web Services URL Page

17. On the Topology Builder page, view and modify the topology that was just created, if desired.

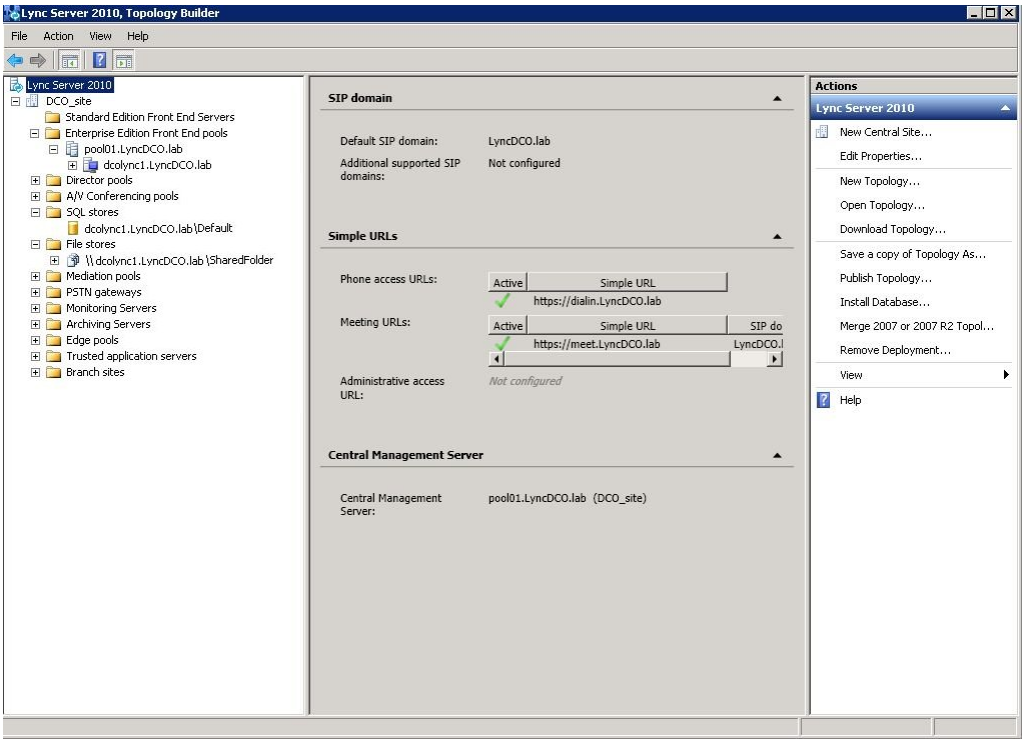

Figure 58: Review the new topology

End of procedure

Procedure:
Configuring the Administrative URL

Purpose: To configure the Administrative URL in order to access services through the Web. Three simple URLs can be created, but this procedure focuses on the third URL type:

1. Meet—Helps users connect to Conferencing Service.
2. Dial-in—Helps users access dial-in Conferencing Service.
3. Admin—Helps users connect to Lync Server 2010 Control Panel as an Administrator (optional).

Start of procedure

1. In the Topology Builder window, select the `Lync Server 2010` node in the console tree.
2. In the `Actions` pane, click `Edit Properties`.

3. In the Edit Properties dialog box, click `Simple URLs`.
4. In the `Administrative access URL` text box, specify the URL as `https://admin.[domain-name]` and click `OK`.

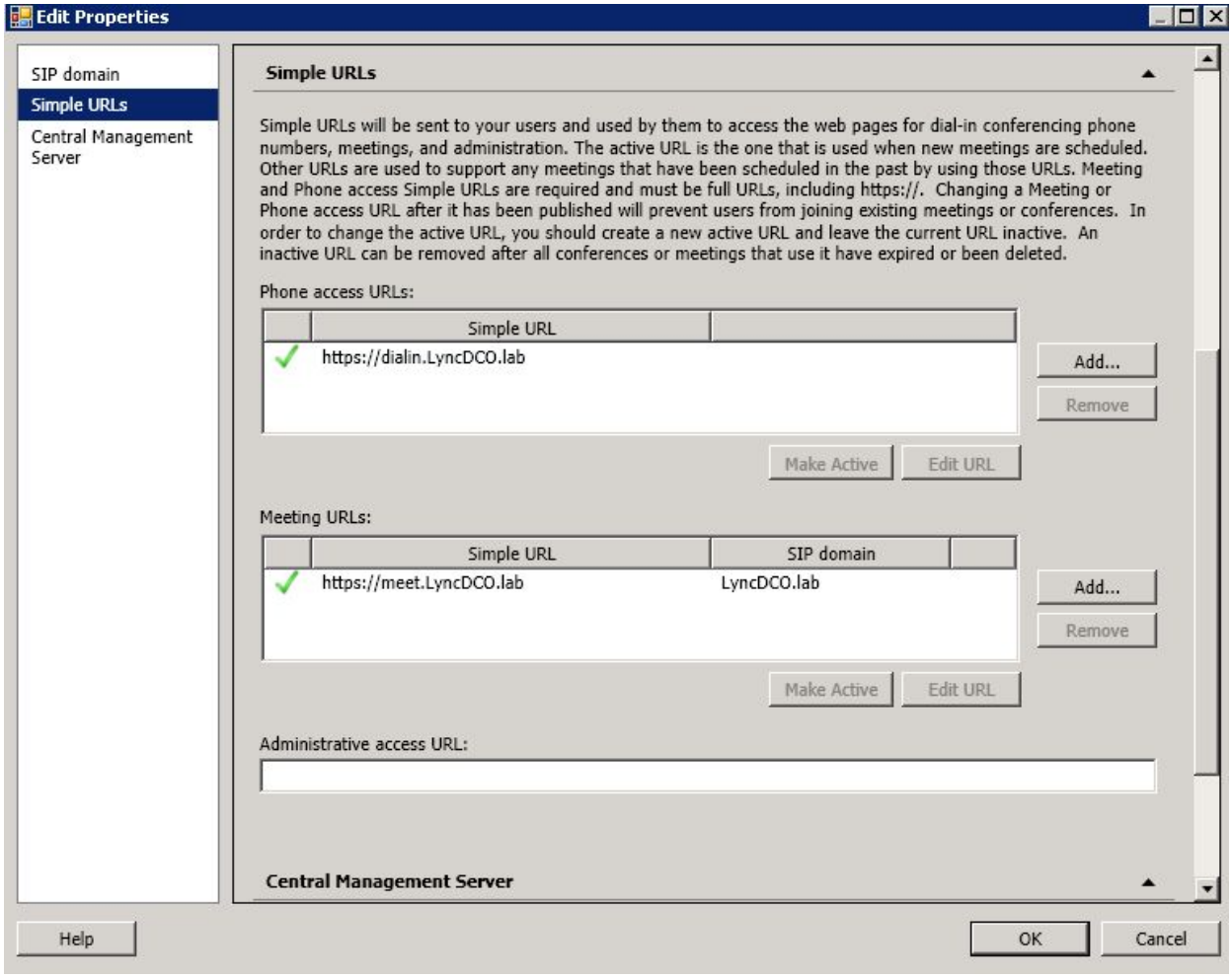

Figure 59: Simple URLs Page

End of procedure

Next Steps

- Procedure: Publishing the Topology

Procedure: Publishing the Topology

Purpose: In order to take effect, the topology that you have created needs to be published in a Central Data Store.

Prerequisites

- Procedure: Creating a Topology
- Procedure: Configuring the Administrative URL

Start of procedure

1. In the Topology Builder window, open the topology created in Procedure: Creating a Topology, on page 54.
2. In the console tree, right-click on the `Lync Server 2010` node, and then choose the `Publish the Topology` option.
3. On the Publish the Topology window, click `Next`.

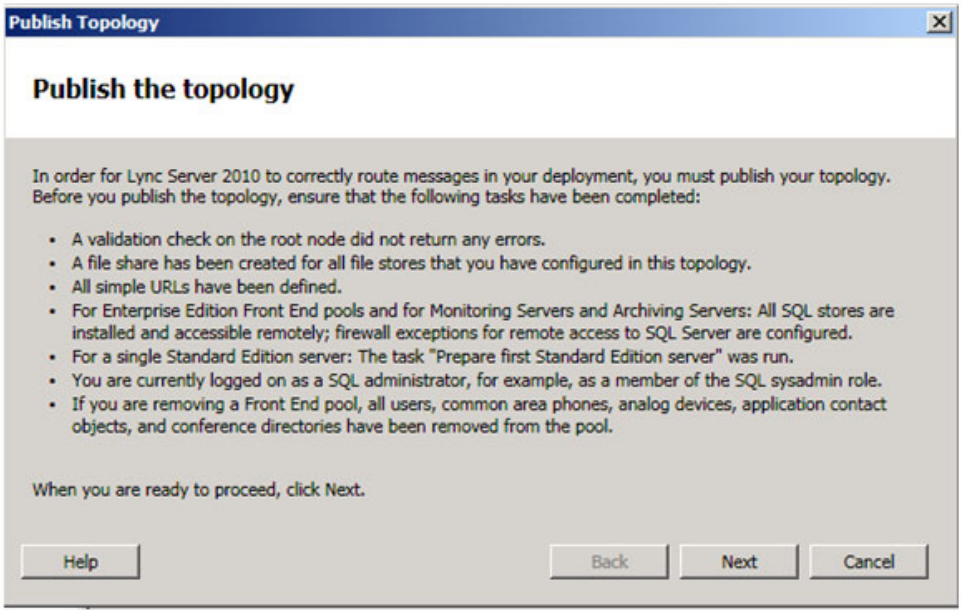

Figure 60: Publish Topology Window

4. On the Create Databases page, check that the back-end database is selected and click `Next`.

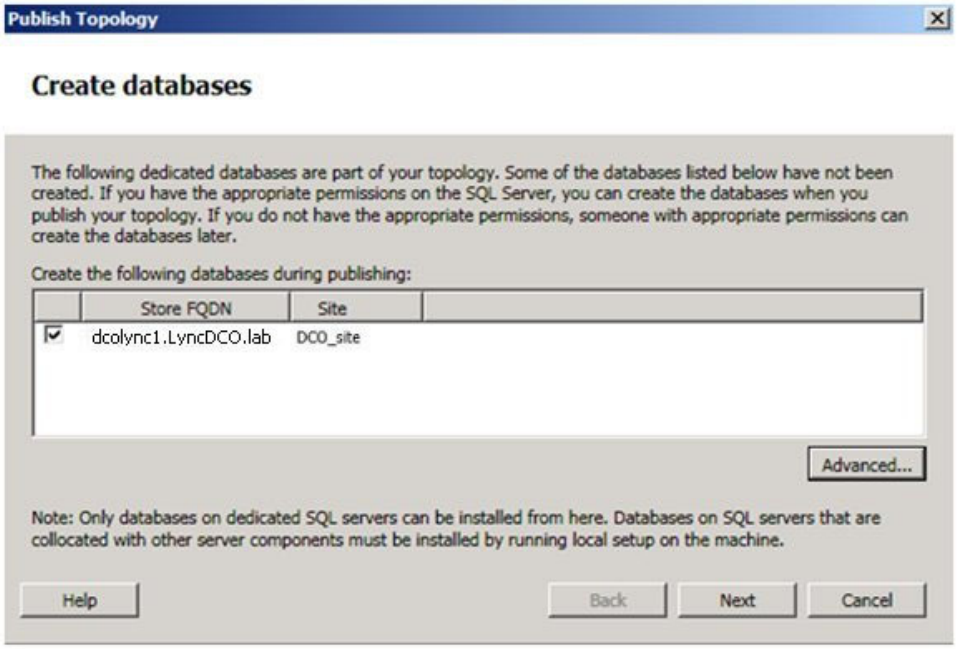

Figure 61: Create Databases Page

5. On the Select Central Management Server page, ensure that the Front End Pool is selected and click `Next`.

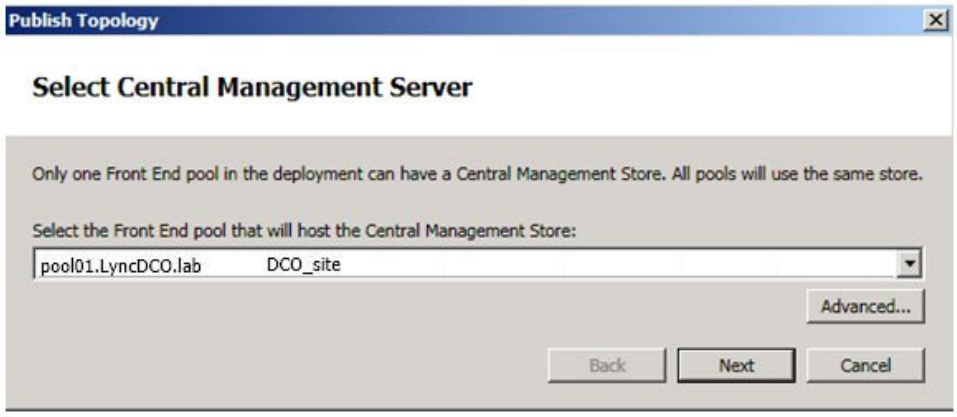

Figure 62: Select Central Management Server Page

6. Publish the Topology. When the Topology Builder shows Complete Status, ensure that each step shows a Success status. Click `Finish`.

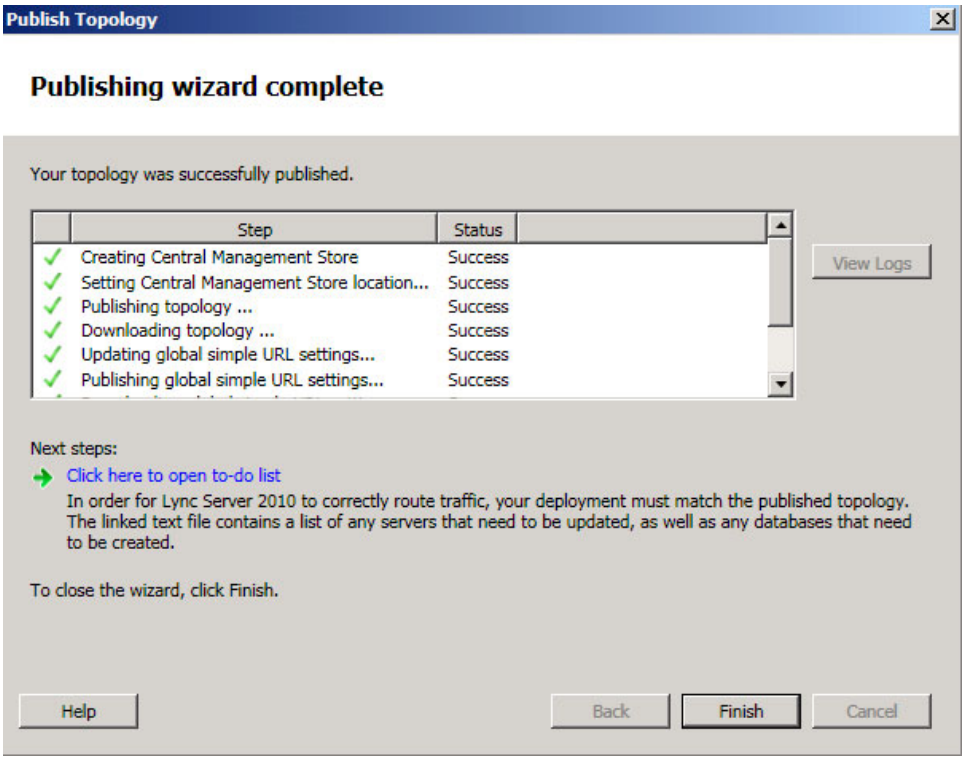

Figure 63: Publish Topology Complete

End of procedure

Next Steps

- Procedure: Installing the local configuration store

Lync Server Front End Setup

This section explains how to setup and configure the Lync Front End Server.

Procedure: Installing the local configuration store

Purpose: To install the local configuration store for the Lync Front End Server.

Start of procedure

1. On the Lync Server 2010 Deployment Wizard window, click the `Install or Update Lync Server System` link.

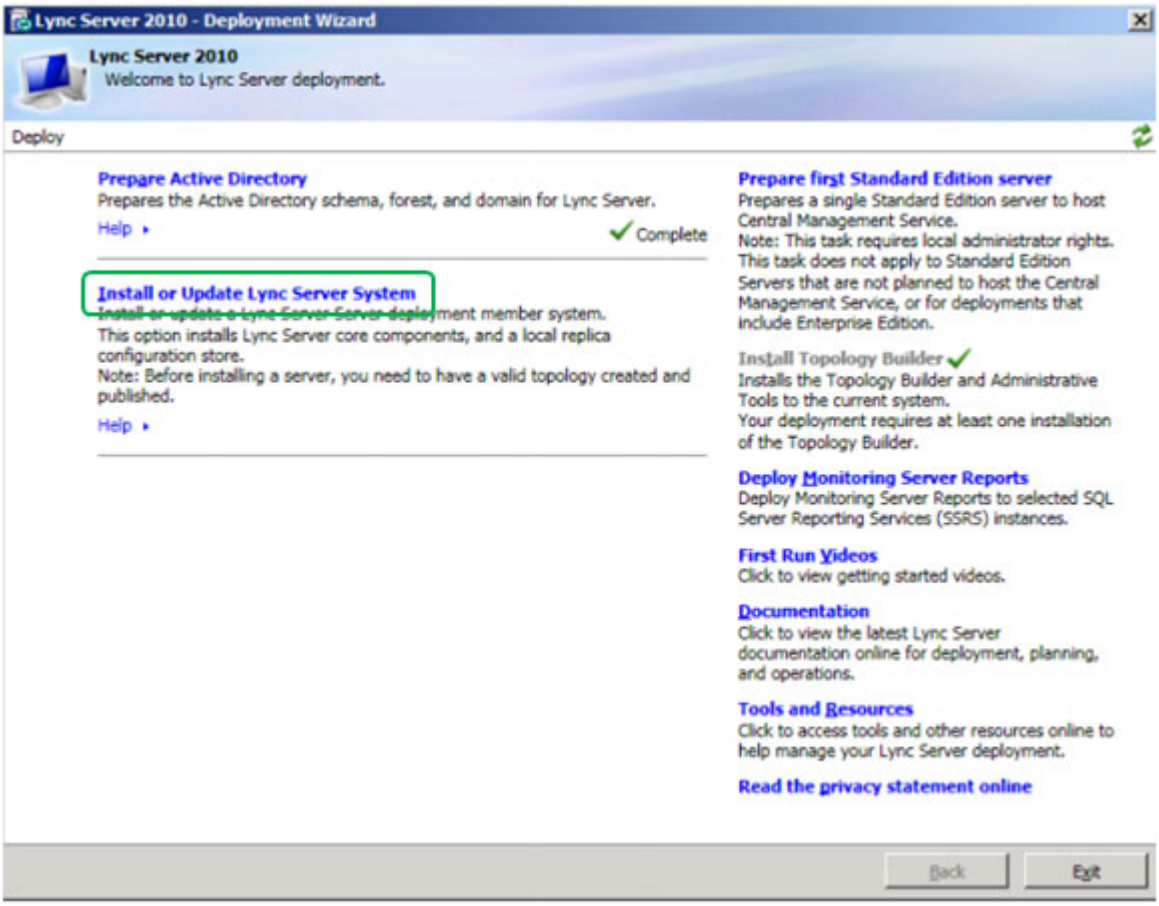

Figure 64: Lync Server 2010 Deployment Wizard Window

2. On the Lync Server 2010 page, click `Run` under `Step 1`.

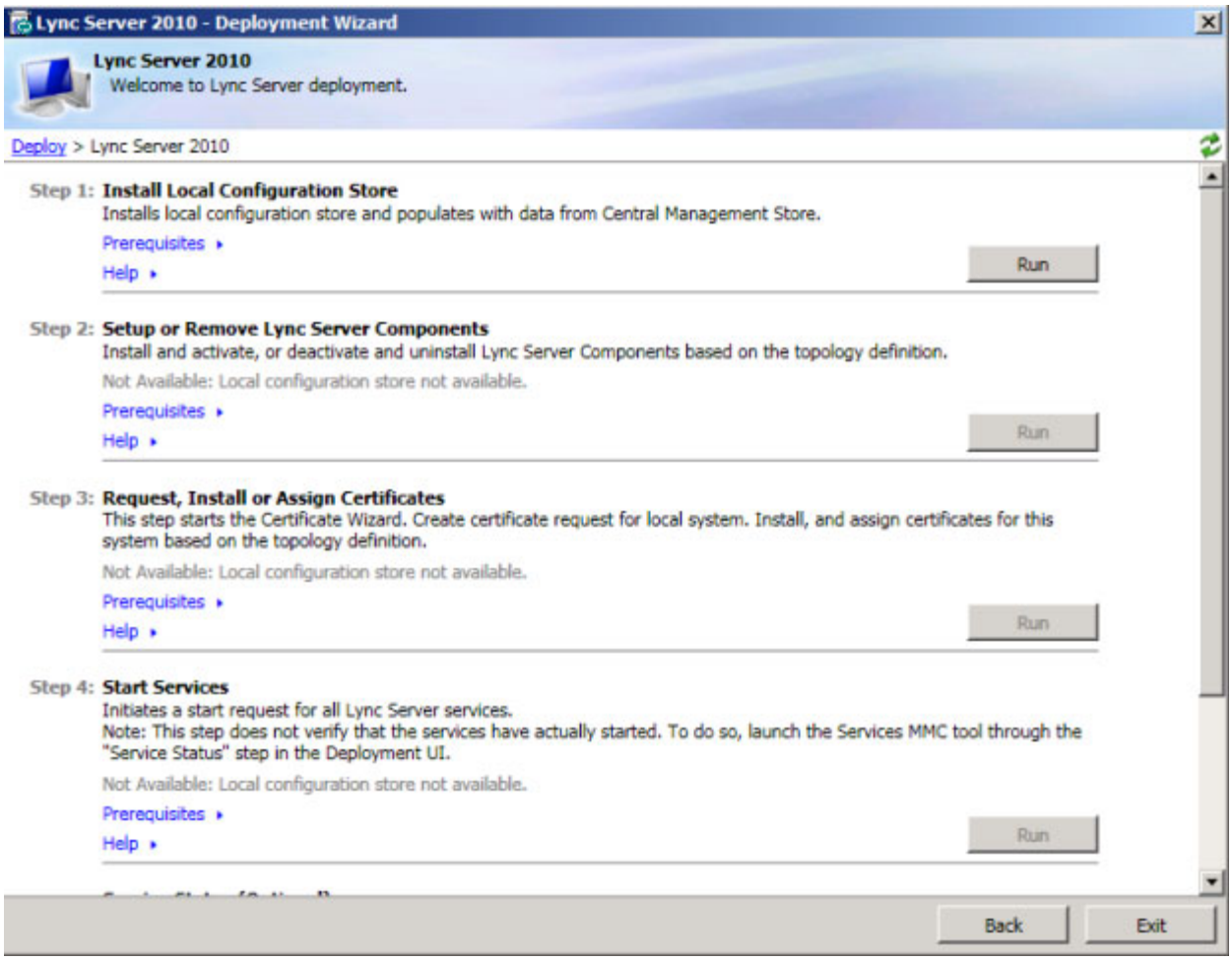

Figure 65: Lync Server 2010 Page

3. On the Configure Local Replica of Central Management Store window, select `Retrieve directly from the Central Management Store` option and click `Next`. When prompted, provide the location of the Lync Server installation media.
4. When the task is completed, click `Finish`.

End of procedure

Next Steps

- Procedure: Installing the Front End Server

Procedure:
Installing the Front End Server

Purpose: To install the Lync Front End Server.

Prerequisites

- Procedure: Installing the local configuration store

Start of procedure

1. On the Lync Server 2010 Deployment Wizard window, click the `Install or Update Lync Server System` link.
2. On the Lync Server 2010 page, click `Run` under `Step 2`.
3. On the Setup Lync Server Components window, click `Next`.
4. Once the installation is completed and the host machine is restarted, complete the installation by clicking `Finish`.

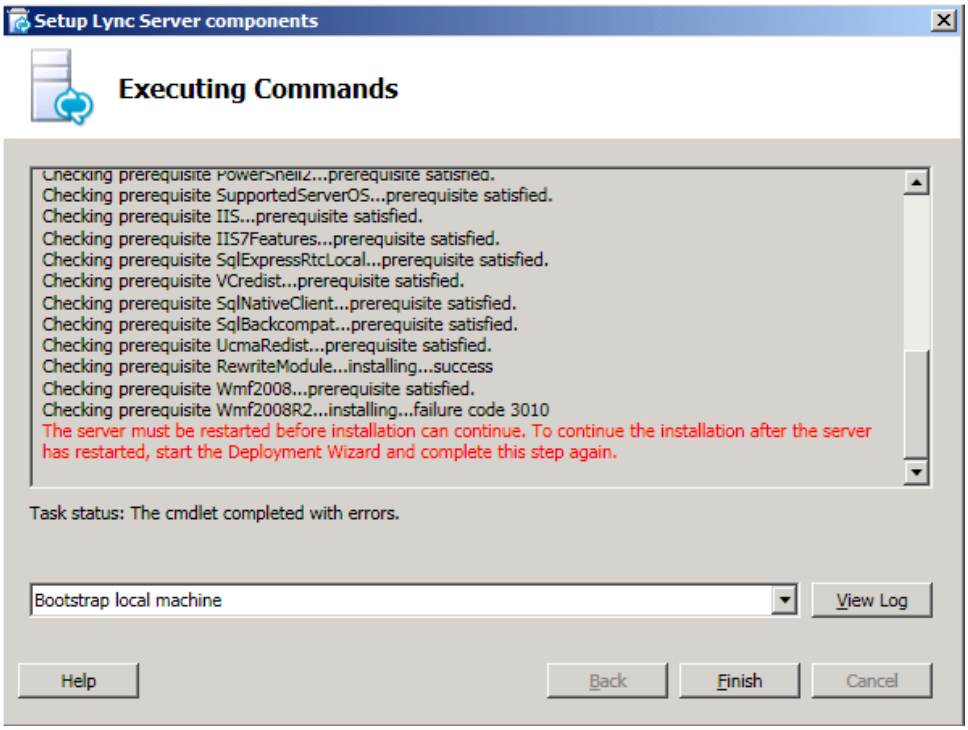

Figure 66: Setup Lync Server Components Completed

End of procedure

Requesting, installing and assigning certificates

All communication within Lync is done over TLS, which means that a security certificate issued by a proper Certificate Authority is necessary for Lync installations. Lync includes a facility to automate the process of requesting, installing, and assigning certificates. This section explains how to manage the installation of a suitable certificate.

Procedure: Requesting, installing and assigning certificates

Purpose: To request, install, and assign certificates on the Lync installation.

Prerequisites

- Procedure: Installing the Front End Server

Start of procedure

1. On the Lync Server 2010 Deployment Wizard window, click the `Install or Update Lync Server System` link.
2. On the Lync Server 2010 page, click `Run` under `Step 3`.
3. On the Certificate Wizard window, click `Request`.

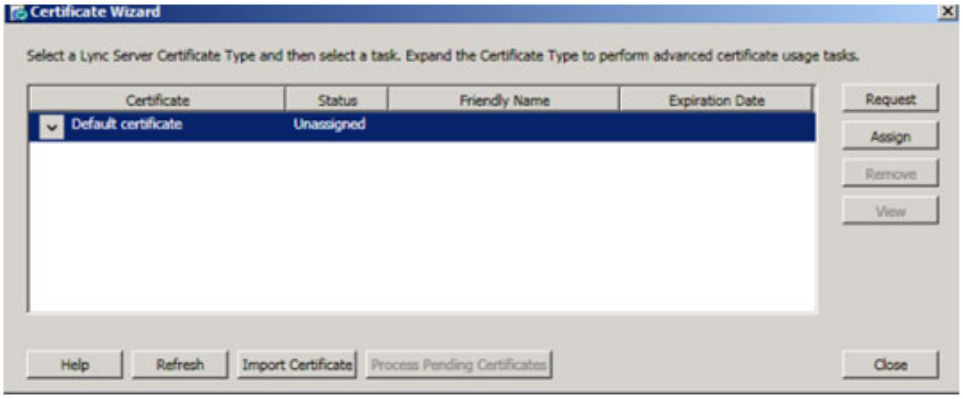

Figure 67: Certificate Wizard Window

4. On the Certificate Request page, click `Next`.

5. On the Delayed or Immediate Requests page, select the `Send the request immediately` option and click `Next`.

Figure 68: Delayed or Immediate Requests page

6. On the Choose Certificate Authority page, select the CA for which the certificate needs to be requested and click `Next`

Figure 69: Choose a Certification Authority (CA) Page

7. On the Certificate Authority Account page, click `Next`.
8. On the Specify Alternate Certificate Template page, leave the `Use Alternate Certificate` option unchecked and click `Next`.

9. On the Name and Security Settings page, specify a friendly name and click `Next`.

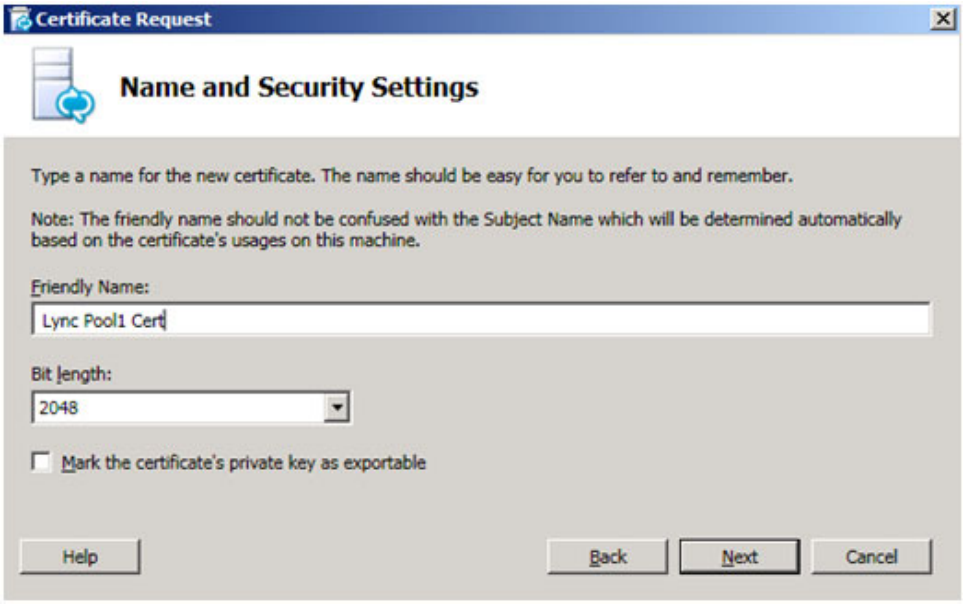

Figure 70: Name and Security Settings Page

10. Specify the Organization and Geographic information, and click `Next`.
11. On the Subject Name / Subject Alternate Names page, click `Next`.

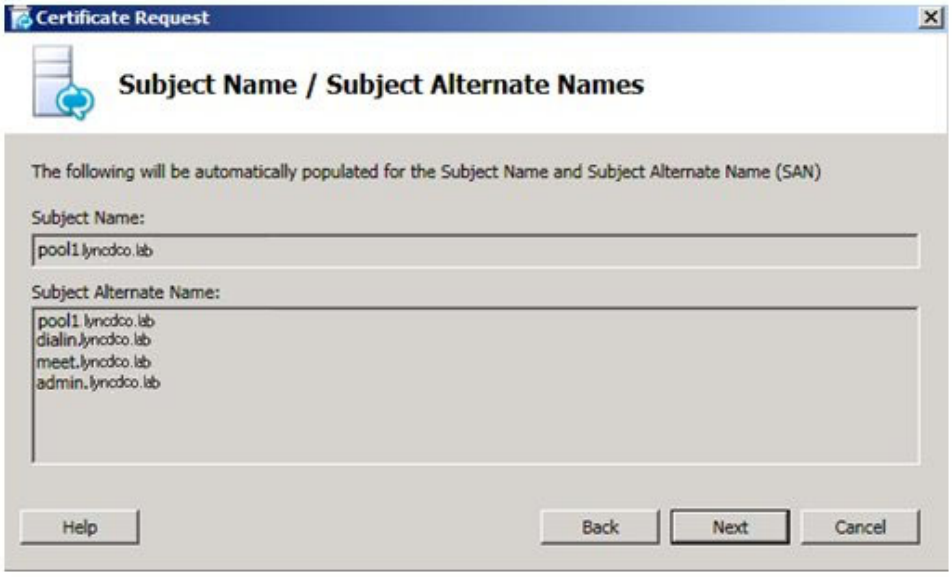

Figure 71: Subject Name / Subject Alternate Names Page

12. On the SIP Domain Setting page, select the SIP domain and click `Next`.

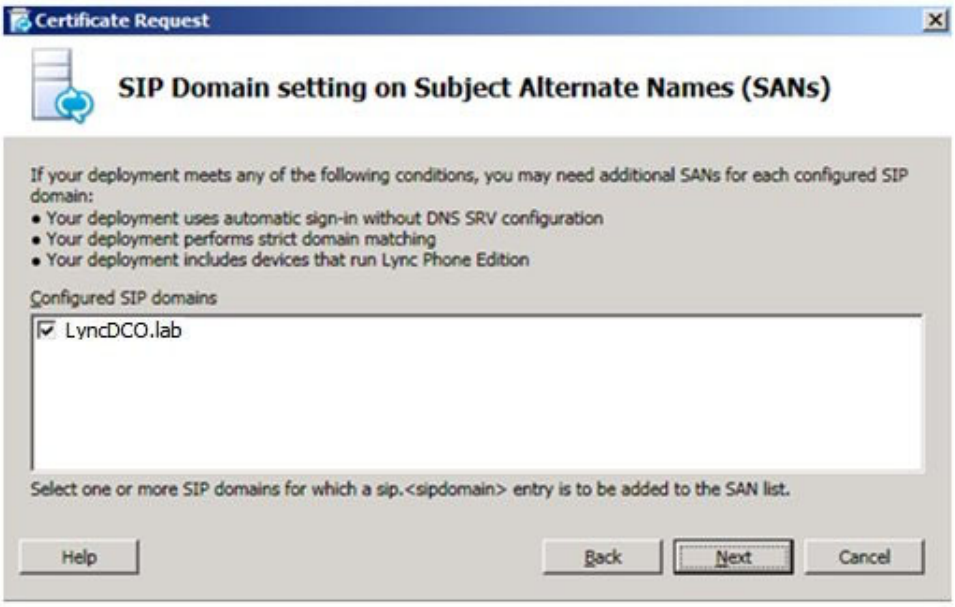

Figure 72: SIP Domain Setting on Subject Alternate Names Page

13. On the Configure Additional Subject Alternate Names page, click `Next`.
14. On the Summary page, review the content and click `Next`.
15. On the Executing Commands page, ensure that the `Task Status` shows as Completed and click `Next`.

16. On the Online Certificate Request Status page, check that the `Assign this Certificate to the Lync Server Certificate` option is selected and click `Finish`.

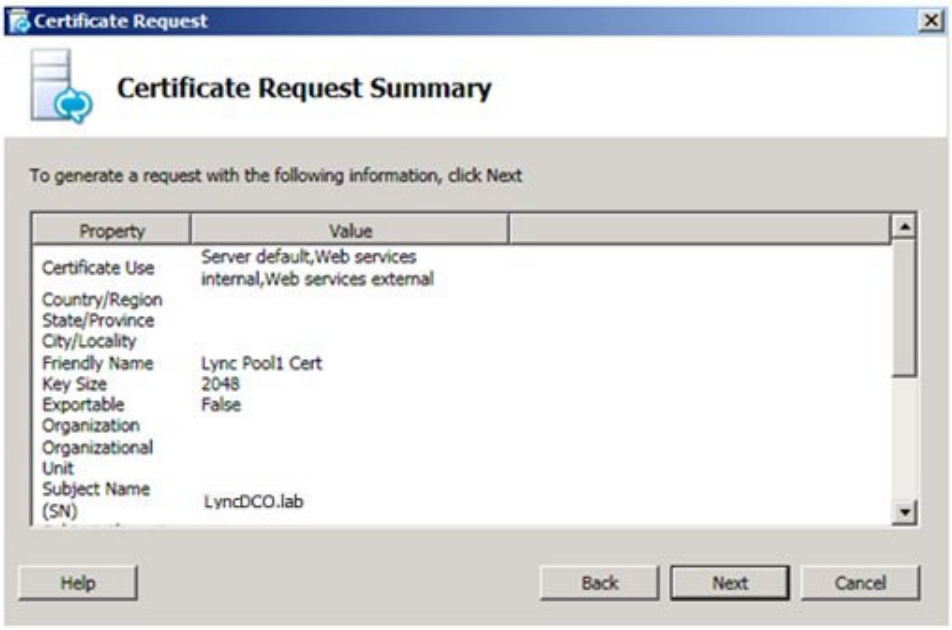

Figure 73: Certificate Request Summary Page

17. On the Certificate Assignment page, click `Next`.

18. On the Certificate Assignment Summary page, review the information and click `Next`.

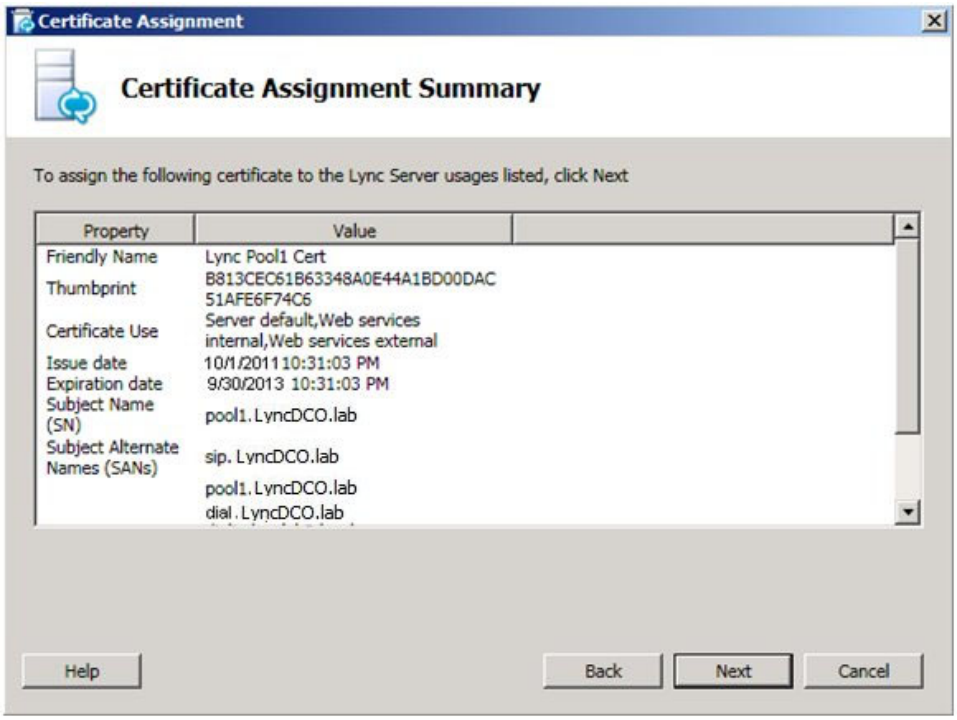

Figure 74: Certificate Assignment Summary Page

19. On the Executing Commands page, check that the `Task Status` is Completed and then click `Finish`.
20. In the Certificate Wizard window, review the list of assigned certificates and click `Close`.

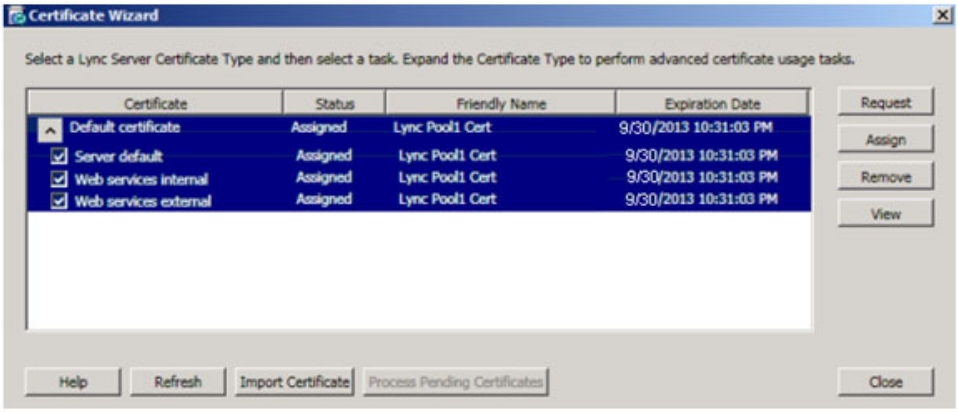

Figure 75: Certificate Wizard Window

End of procedure

Next Steps

- Procedure: Creating users in Active Directory

Defining Users in Lync

Once the environment is set up, you will need to create users who will be both Lync users and Genesys agents. This section describes the manual user creation process in Lync. This is appropriate for smaller deployments.

Procedure: Creating users in Active Directory

Purpose: Since Lync uses AD for user data, users need to be created in Active Directory.

Start of procedure

1. Open Active Directory Users and Computers.
2. In the console tree, right-click the folder in which you want to add a user account. Point to `New` and click `User`.
3. On the `General` tab, enter the first and last name, display name, and e-mail.

4. On the `Account` tab, enter the user login name and account options.

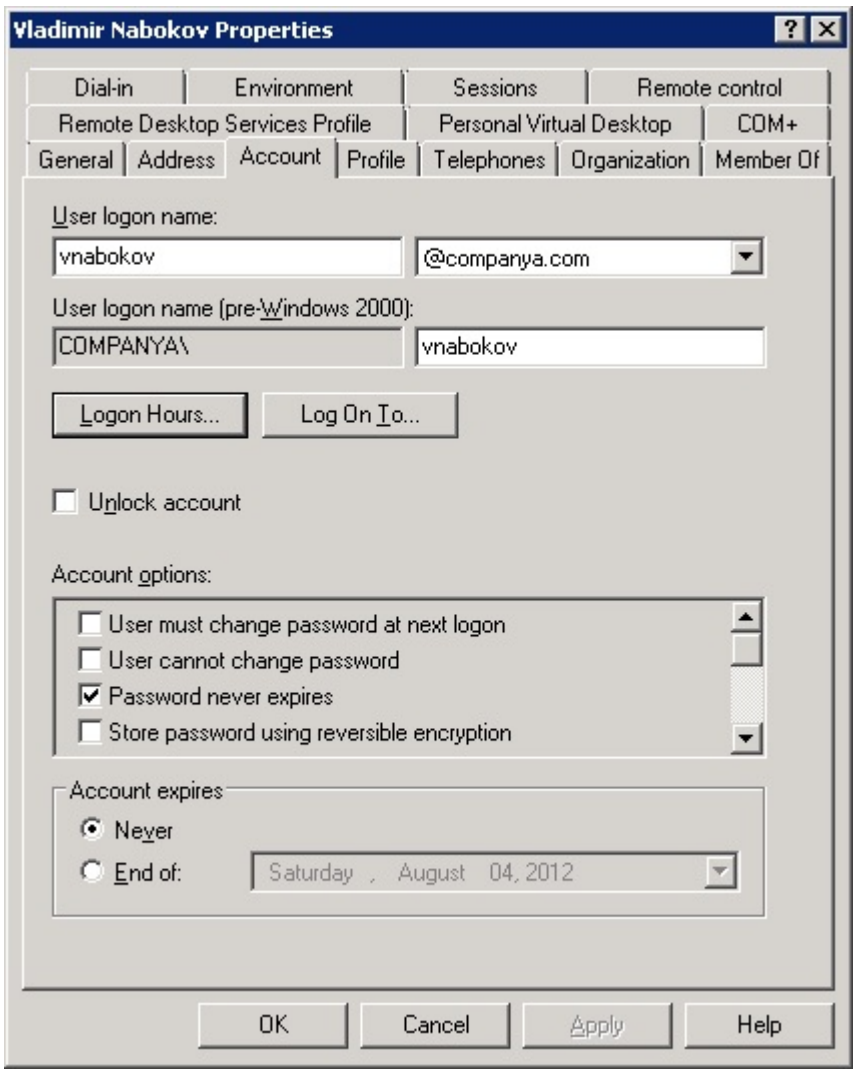

Figure 76: User Properties for Account Tab

5. On the `Telephones` tab, enter the user telephone number(s).
6. Click `OK`.

End of procedure

Next Steps

- Procedure: Configuring users through the Lync Control Panel

Procedure:
Configuring users through the Lync Control Panel

Purpose: Further configuration can be done from the Lync Control Panel. The control panel allows you to edit/modify users, although it cannot create new Active Directory users.

Prerequisites

- Procedure: Creating users in Active Directory

Start of procedure

1. To launch the Lync Control Panel, open a browser window and enter the Lync Admin URL (https://admin.[domain-name]). Alternatively, on the Lync Front End Server, go to `Start > All Programs > Microsoft Lync Server 2010 > Lync Server Control Panel`.
2. Select the pool that you would like to connect to.

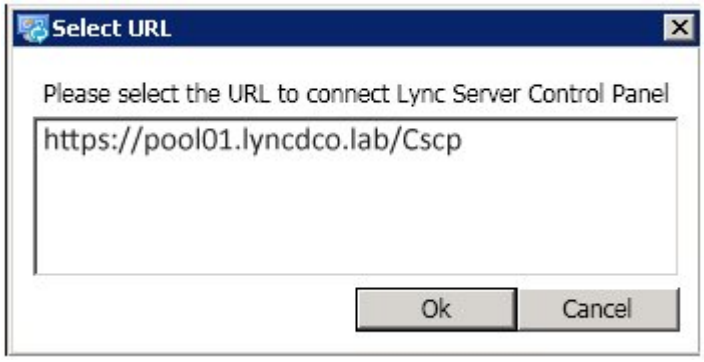

Figure 77: Select URL Window

3. Specify the `[Domain-Name]/Administrator` login credentials and click `OK` to open the Lync Control Panel.

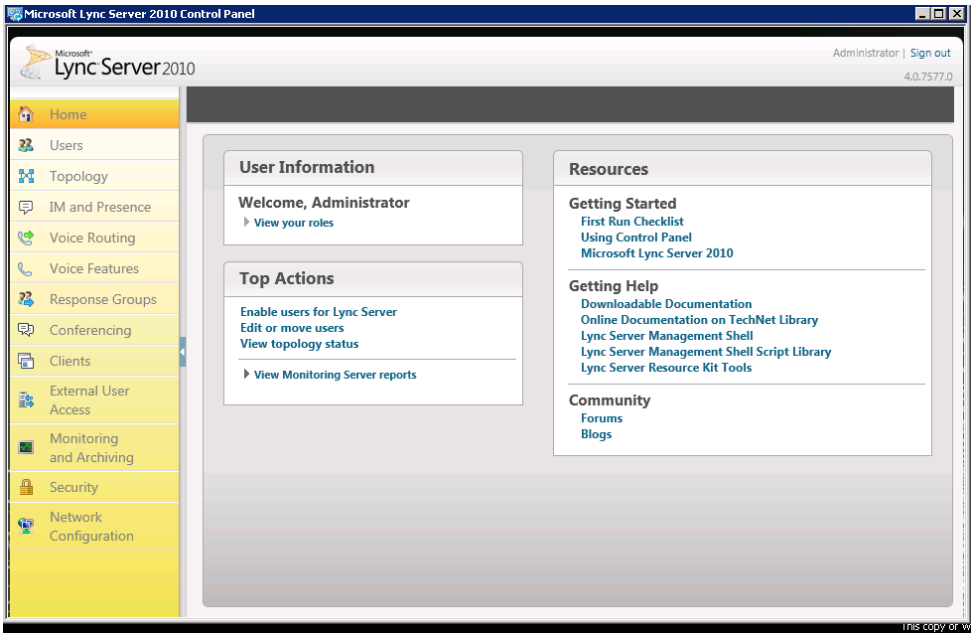

Figure 78: The Lync Control Panel

4. Click `Users` in the left-hand side options list. The window displays a list of users who have already been created. To enable a new user, the user must already exist in Active Directory. Select `Enable Users` from the `Users Tab`.

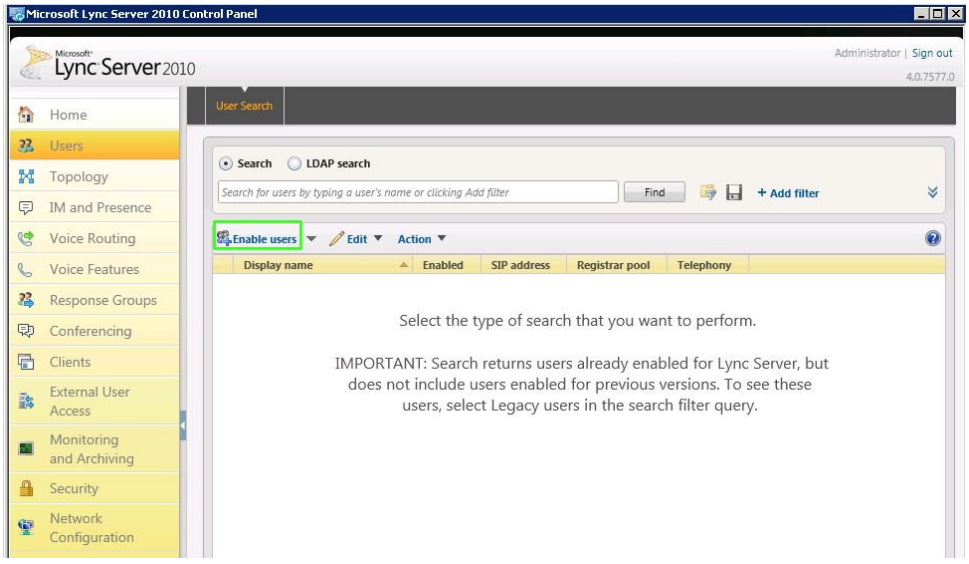

Figure 79: Lync Control Panel Enable Users

5. Search to find the user(s) to add and select the `Enabled for Lync Server` check box. Click each user to edit the user's properties. Initially, the other options such as the `Dial plan policy`, `voice policy`, `conferencing policy`, `Client Version policy`, `Pin policy`, `External access policy`, `archiving policy`, `Location and client policy` can be left as automatic.

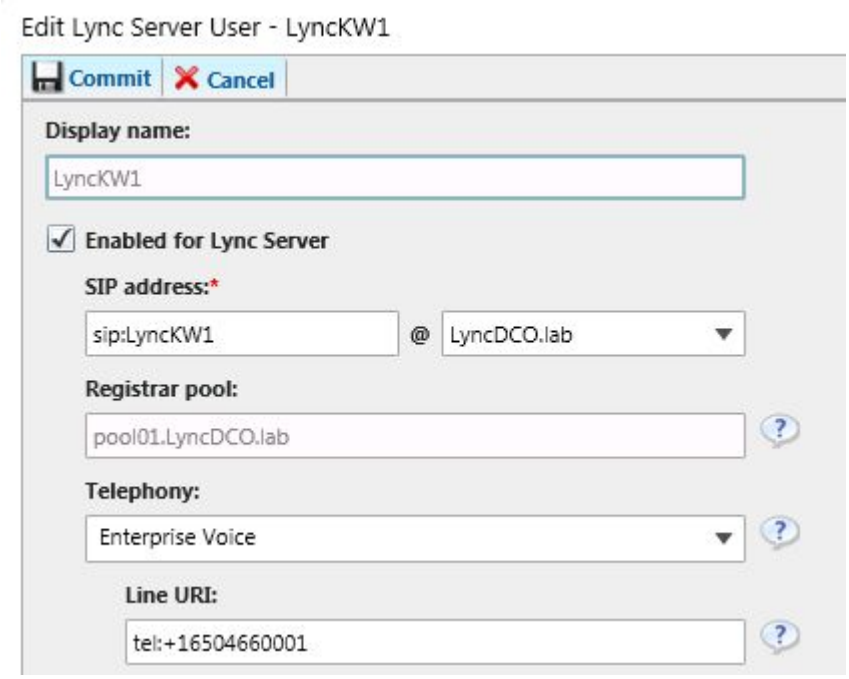

Figure 80: Edit Lync Server User Window

6. Click `Commit`.

End of procedure

Next Steps

- Procedure: Configuring voice routing for users

Procedure: Configuring voice routing for users

Purpose: To configure voice routing for users on the Lync Control Panel.

Start of procedure

1. In the Lync Control Panel, click `Voice Routing` in the left navigation bar.

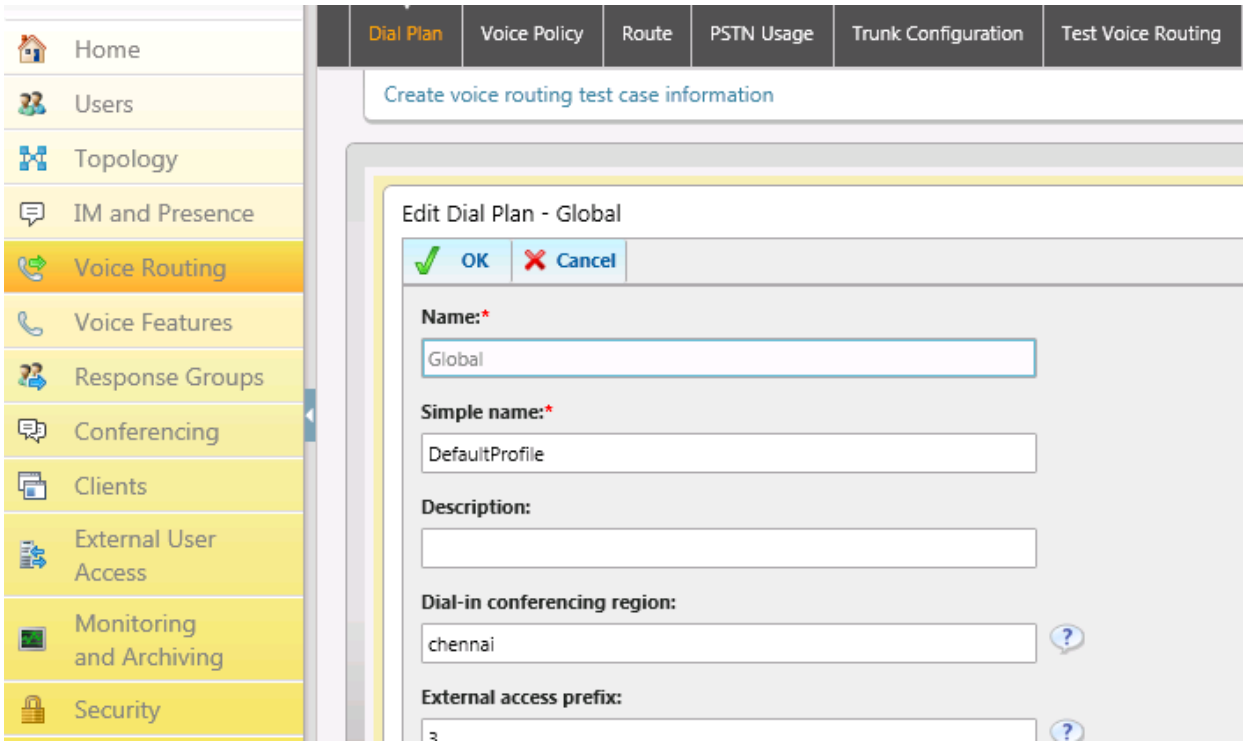

Figure 81: Voice Routing Page

2. In the `Dialed number` field, type in the phone number you want to use. This number will be normalized and displayed in the `Normalized number` field of the `Results` pane.

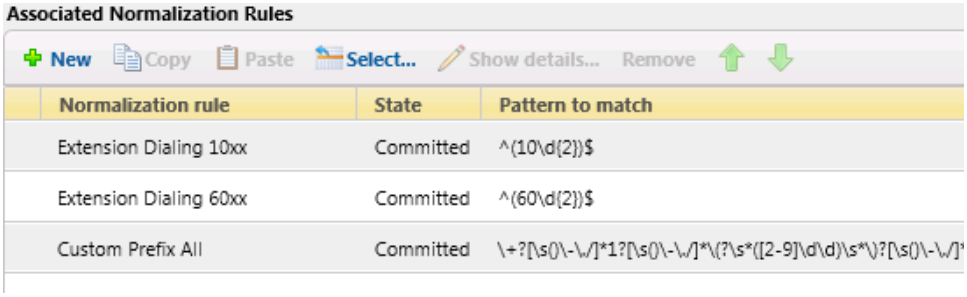

Figure 82: Associated Normalized Rules

3. Click the `Route` tab to configuring route details.

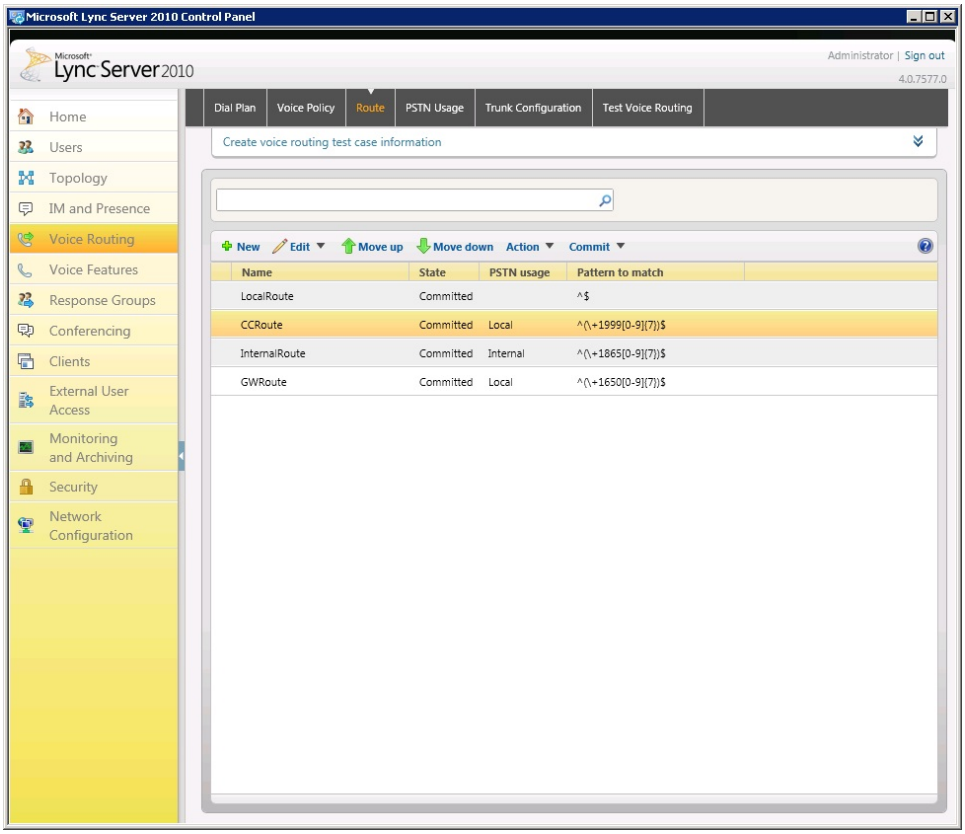

Figure 83: Voice Routing—Route Tab

4. If required, change the route by moving each route up and down in the list. To specify the detailed route configuration, click `Edit`

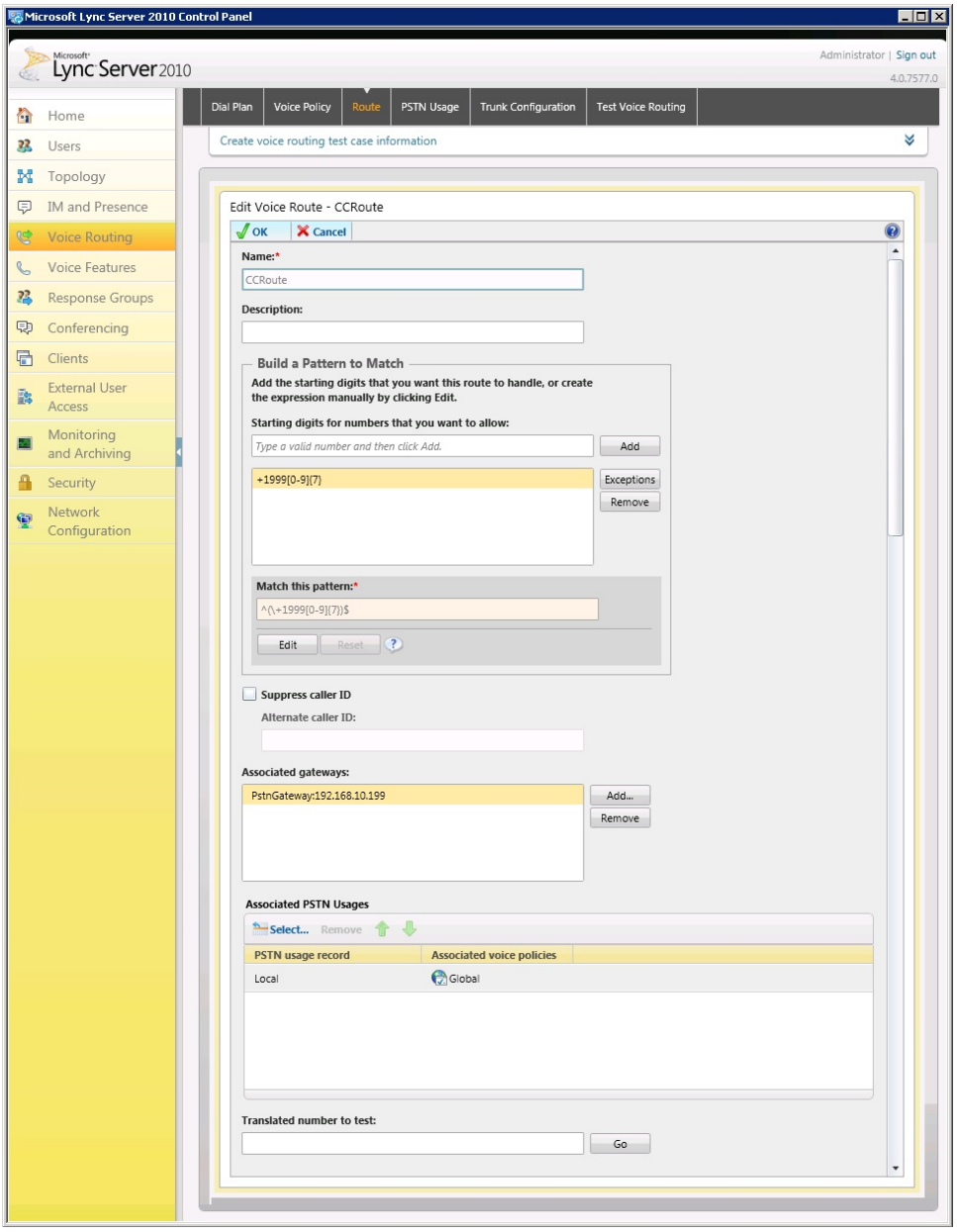

Figure 84: Edit Voice Route Window

End of procedure

Next Steps

- Procedure: Creating a new PSTN Gateway

Genesys-Specific Lync Configurations

This section discusses specific Lync configurations that allow SIP Server and UC Connector to integrate with Lync.

Procedure: Creating a new PSTN Gateway

Purpose: To create a new public switched telephone network (PSTN) gateway. The SIP Server is seen by Lync as a PSTN gateway that talks to the Mediation Server. PSTN gateways are configured in Lync through the Topology Builder.

Start of procedure

1. Click `Start > All Programs > Microsoft Lync Server 2010 > Lync Server Topology Builder`.
2. In the site tree on the left-hand panel, right-click `PSTN gateways` and select `New`.

3. In the Define New IP/PSTN Gateway window, specify the `Host`, `Port` and `Transport`.

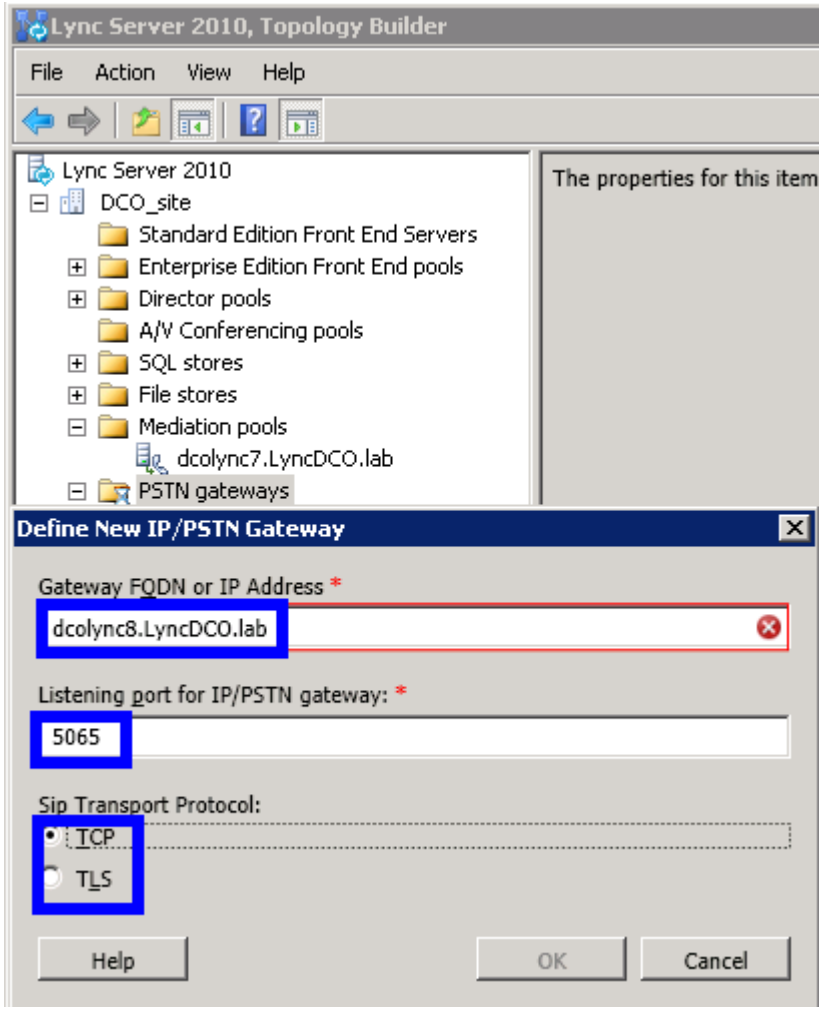

Figure 85: Define New IP/PSTN Gateway Window

Note: When TLS is the transport chosen for SIP Server, the configuration option `TServer\sip-tls-cert` should be set to SIP Server's host certificate thumbprint that is issued by Lync CA. You should also set the `TServer\sip-port-tls` to the port.

4. Right-click the Mediation Server pool host and select the `PSTN Gateway` tab. The newly created PSTN Gateway (the SIP Server) should be added to the associated list of the Mediation Server, and selected as the Default Gateway.

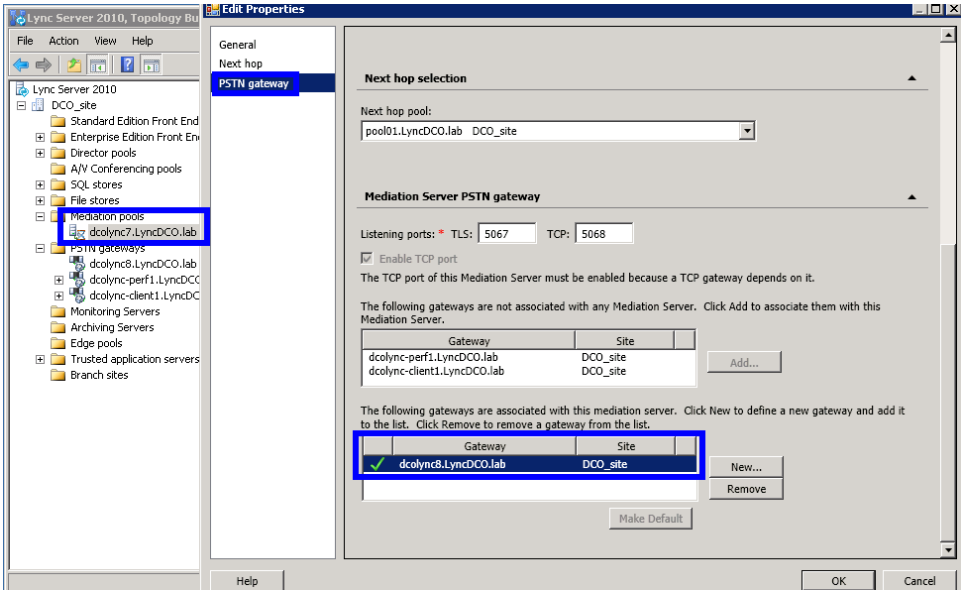

Figure 86: Mediation Pool PSTN Gateway

Note: In this sample configuration, Mediation Server uses ports `5067` for SIP TLS and `5068` for SIP TCP.

5. Publish the Topology.

End of procedure

Next Steps

- Procedure: Configuring UC Connector as a trusted application

Procedure:
Configuring UC Connector as a trusted application

Purpose: To add the UC Connector host as a Trusted Application Host in the Lync Topology Builder.

Start of procedure

1. Click `Start > All Programs > Microsoft Lync Server 2010 > Lync Server Topology Builder`.
2. Right-click the `Trusted Application Servers` item on the left-hand-side panel and click `New`.
3. Enter the `FQDN` for the UC Connector host and select `Single computer pool`.

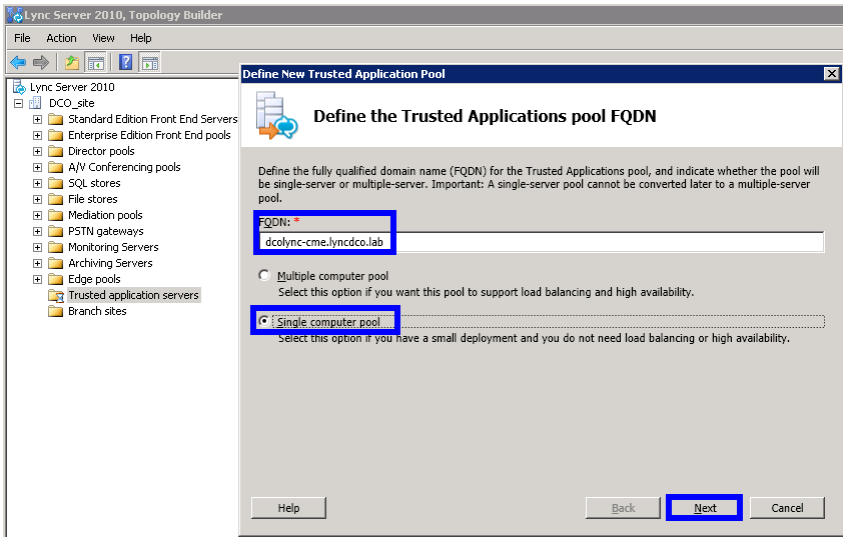

Figure 87: Define the Trusted Applications Pool FQDN Window

4. Specify the pool, which is selected by default, and click `Finish`.

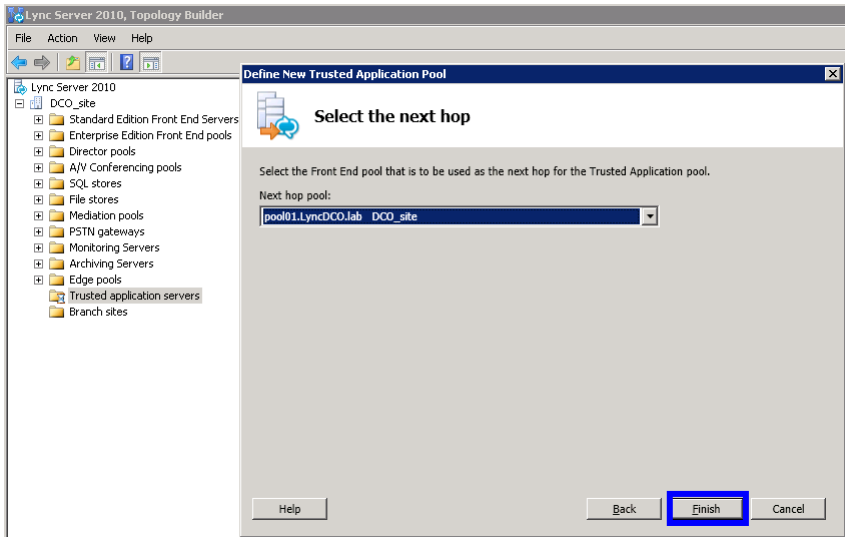

Figure 88: Select the Next Hop Window

5. Publish the Topology.

End of procedure

Chapter

5 Certificate Generation for Genesys Applications

To enable connections between the Genesys application (SIP Server for IM, UC Connector for Contact Center Agents, UC Connector for Experts) and the Lync Front End Server, Lync Enterprise requires the use of TLS. MTLS (mutual TLS) is used for this.

In order to enable MTLS, both server and client need to obtain certificates. In a lab setting, certificates can be self-signed, while in public deployments they need to be issued by a Certificate Authority (CA), such as Verisign.

This chapter contains the following sections:

Generate Client Certificate

The first certificate is a regular client/user certificate, used to trust servers of the domain, like the Lync Front End Server(s). It is not necessary to export private keys for this certificate, or to have private keys exportable.

This is the same type of certificate that would have to be installed on a user's workstation to start a Lync client and to connect to Lync server (TLS connectivity).

Procedure: Generating the Client Certificate

Purpose: To generate a client certificate used to trust the Lync Front End server.

Start of procedure

1. Request the certificate through Certification Authority (CA) Web Access
   `https://[server_name]/certsrv`
2. Select 'Download a CA certificate, certificate chain, or CRL'
3. Select 'Download CA certificate'
4. Save the certificate as "DER encoded binary X.509 (.CER)." For example, `CompanyA_Certificate.cer`

End of procedure

Next Steps

- Procedure: Processing the Client Certificate

Procedure: Processing the Client Certificate

Purpose: To convert the .cer certificate file to JKS format (Java keystore).

> **Note:** keytool.exe is a tool provided by the Java Development Kit and can be found in the `bin` directory of the JDK installation

Prerequisites

- Procedure: Generating the Client Certificate

Start of procedure

1. Copy the certificate that you created in the previous procedure (for example, `CompanyA_Certificate.cer`)
2. Place this certificate in the `JDK\bin` directory of your prerequisite JDK installation.
3. From the `JDK\bin` directory, run the following command:
   ```
   keytool -import -alias "CompanyA_Certificate" -file
   CompanyA_Certificate.cer -keystore CompanyA_Store.jks
   ```
4. Note the keystore password requested during keytool procedure (for example, `ghijkl`)
5. Place this file in a logical location. For example:
   `<ucc_root>\etc\CompanyA_Store.jks`

End of procedure

Next Steps

- Continue to one of the following:
  - Procedure: Generating the Server Certificate Using Lync Management Shell
  - Procedure: Generating the Server Certificate Using Microsoft Management Console or CA Web Access

Generate Server Certificate

This is a server certificate (enhanced key usage: Server Authentication - Private keys exportable), the same type of certificate that is required by any server belonging to a Lync infrastructure (such as A/V MCU, Edge Server, Mediation Server).

As a MTLS (mutual TLS) connection is to be established between the Genesys application (SIP Server and / or UC Connector) and Lync Front End Server, each side needs to have its own server certificate, which establishes trust between the two servers. This is a standard Lync procedure.

Procedure: Generating the Server Certificate Using Lync Management Shell

Purpose: To generate a server certificate. This is the same type of certificate required by any server belonging to a Lync infrastructure (A/V MCU, Edge Server, Mediation Server).

Start of procedure

1. On the host computer where the Lync Front End Server is installed, open the Microsoft Lync Shell and type

```
Request-CsCertificate -New -Type Default -FriendlyName
"GenesysServerCertificate" -CA
"labdc01.companya.com\companya-LABDC01-CA" -ComputerFQDN
[server_name]-Verbose
```

Note: The [server_name] must match the FQDN of the host where UC Connector is running.

This will request the certificate through Lync. If authorized/granted, it will be installed on the Certificate Store (Personal) of the host where the request was issued.

2. Open the Microsoft Management Console (MMC):
   a. Click `Start > Run`.
   b. Type `MMC` and click `Ok`.
3. Add the certificates snap-in:
   a. Go to `File > Add/Remove Snap-In`.
   b. Click `Add`.
   c. Select the `Certificates Snap-In` and click `Add`.
   d. Select `Local Computer` and click `Finish`.
4. Find the Genesys Server certificate that you want to export:
   a. Under the `Certificates` tree, locate your domain certificate; for example this could be in the `Personal` folder.
   b. Click `Certificates`.
   c. Right-click the certificate you want to export, select `All Tasks > Advanced Operations > Export`.
5. Follow the wizard to export the certificate to a .pfx file ("Personal Information Exchange - PKCS #12 (.PFX)").
   a. Choose `'Yes, export the private key'`.
   b. Choose `'Include all certificates in certificate path if possible'`.

Note: Do NOT select `'Delete Private key'`.

   c. Enter a password (take note of it). (Example: mnopqr)
   d. Select a location to save the file, then click `Finish` (Example: GenesysServer_Certficate.pfx)
6. When you get the message "`The export was successful`", click `OK`.
7. Copy the certificate file on to the UC Connector host and place it in a logical location. For example:
   `<ucc_root>\etc\GenesysServer_Certificate.pfx`

End of procedure

Procedure:
Generating the Server Certificate Using Microsoft Management Console or CA Web Access

Purpose: To generate a certificate for the host running UC Connector with the Microsoft Management Console or Certification Authority (CA) Web Access.

Note: Note that such a certificate template may not exist by default at the Certification Authority level (certificate template including Server Authentication as enhanced key usage and allowing Private keys to be exported). If operational policies permit it, a copy of the "Web Server" certificate template can be made, adding permission to export Private keys. This can be achieved on the Certification Authority host running the client tool "certtmpl.msc".

Start of procedure

1. On the host computer where Genesys is installed, request the certificate through CA Web Access:
   `https://[server_name]/certsrv`
2. Select `Request a certificate`
3. Select `Advanced certificate request`
4. Select `Create and submit a request to this CA`
   - Type - Select a `Server Template with Private Keys exportable`
   - (NDLR: custom Server template with Private Keys exportable)
   - Name: `demosrv.genesyslab.com` (Subject)
   - New keyset: Microsoft RSA, Key Size 2048, Mark Keys as exportable
   - Friendly Name: (Example: GenesysServerCertificate)
5. Export the certificate and save it into a .pfx file (Example: `GenesysServer_Certficate.pfx`). [password - Example: `mnopqr`)]
6. Copy the certificate file on to the UC Connector host and place it in a logical location. For example:
   `<ucc_root>\etc\GenesysServer_Certificate.pfx`

End of procedure

Chapter

6 Genesys Component Configuration for Lync Interoperability

This chapter contains the following sections:

SIP Server Configuration Tasks

This section describes the list of SIP Server options that need to be configured for Lync integration. No changes have been made in SIP Server to integrate with Lync; however, a specific configuration is necessary.

Task Summary: Configuring SIP Server

Objectives	Actions
Set up MSML-enabled treatments.	Set the following configuration option on the SIP Server application level: `TServer\msml-support = true`
Set up music on hold.	To enable music to be played when the caller is on hold, set the following configuration option on the SIP Server application level: `TServer\sip-enable-moh = true`
Set up early media support.	In integration with Microsoft Lync, early media support should be disabled in the SIP Server. For details, see “Current Limitations” on page 104. On the SIP Server application level, set the following configuration option: `TServer\sip-enable-100rel = false`
Set soft switch properties.	A soft switch configuration simplifies the common configuration required on Endpoint DNs. Use a DN of type Voice over IP Service, with `TServer\service-type = softswitch`. Create Extension DNs with the number corresponding to the Lync Enterprise Agent's Phone number, with no sections added to them specifically. See Procedure: Configuring a soft switch DN for Lync.
Create a trunk for Mediation Server.	Since SIP Server is seen by the Lync Mediation Server as a media gateway, a trunk needs to be created on SIP Server pointing to the IP address and port of the Mediation Server.
Create a DN for MSML VoIP Service.	See Procedure: Creating a DN for MSML VoIP Service

Task Summary: Configuring SIP Server

Objectives	Actions
Create a DN for Recorder VoIP Service.	Call recording can be configured using NETANN. This is how the recording test cases were tested during the SIP Server qualification tests with Lync. Additional and more advanced recording capabilities can be configured, but were not tested officially during the qualification tests. Configure the `request-uri` section in NETANN format, as shown in Procedure: Creating a DN for Recorder VoIP Service
Configure a route point.	When a call is made from a Lync Client to a SIP Endpoint, the call progresses through the Lync Server and lands on SIP Server on a route point. Create a Routing Point DN and set `Register` to `true`.

Procedure: Configuring a soft switch DN for Lync

Purpose: To set up a soft switch DN for Lync.

Start of procedure

1. In Genesys Administrator, create a new extension DN. Under the Options tab, select Advanced View (Annex) and add the following options:
   - `TServer/contact`—The contact should point to the Mediation Server, which by default runs on port `5068` for TCP transport, and port `5067` for TLS transport.
   - `TServer/dual-dialog-enabled`—The dual-dialog setting should be `false`. As with most PSTN devices, Lync Mediation Server handles one call at a time. This makes SIP Server reuse the same dialog for the Consultation call. This is also required to have a Media bypass applied to the consult call. Otherwise, by default SIP Server sends a Consult Call INVITE message without SDP.
   - `TServer/make-call-rfc3725-flow`—The call flow should be set to `RFC 3725 flow 1`, in order to make third-party call control calls without sending an Initial INVITE with Black Hole SDP to Lync Mediation Server.

- `TServer/refer-enabled`—The refer support is set to `false`, in order to make the RFC 3725 call flow effective.
- `TServer/reuse-sdp-on-reinvite`—Lync Mediation Server doesn't apply Media Bypass for calls, which go by Late Media. In order for a valid SDP from the caller to reach the Mediation Server, the SDP is reused. The value for this option should be set to `true`.
- `TServer/service-type`—The service type is set to `softswitch`.

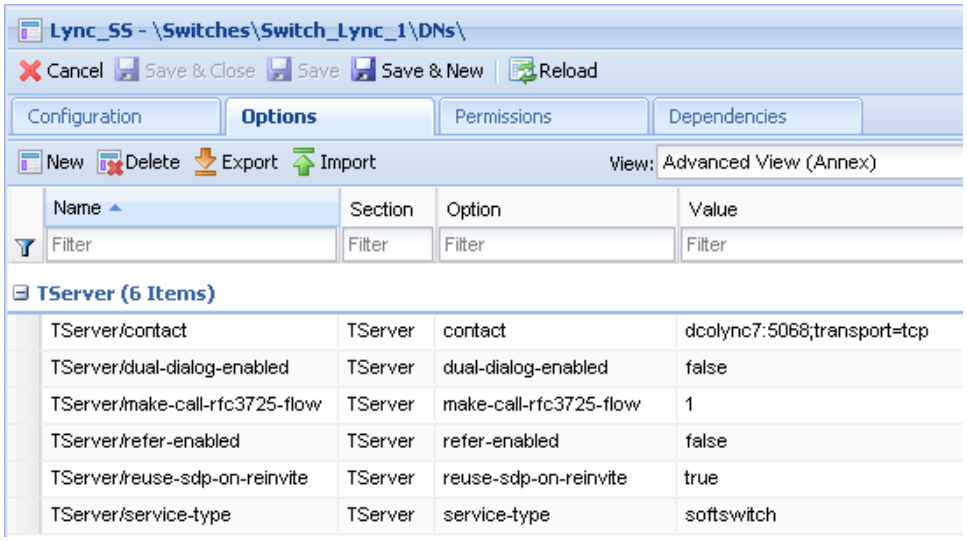

Figure 89: Configuration options for the soft switch DN

End of procedure

Procedure:
Creating a Trunk DN for Mediation Server

Purpose: To create a trunk DN on SIP Server pointing to the IP address and port of the Mediation Server.

Start of procedure

1. In Genesys Administrator, create a new trunk DN. Under the Options tab, select Advanced View (Annex) and add the options as shown in the figure below:

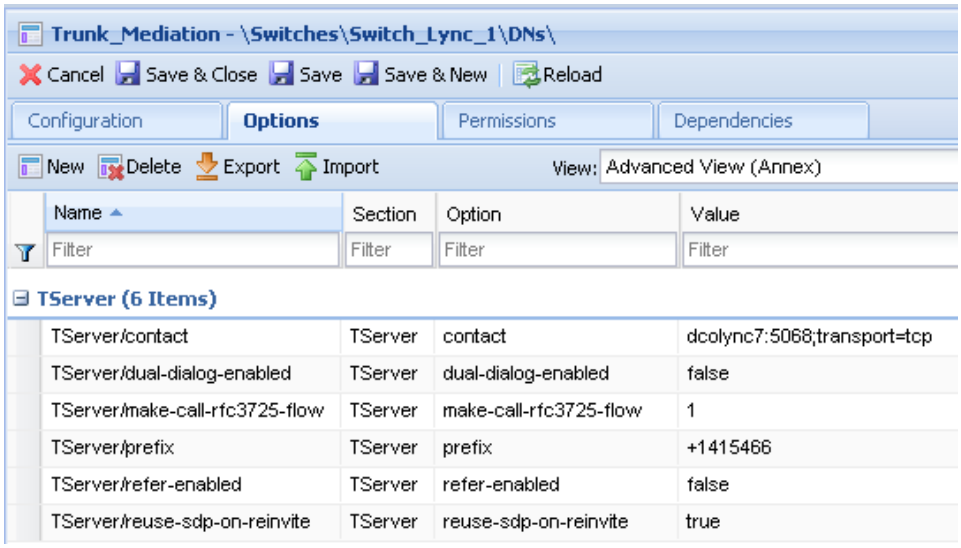

Figure 90: Configuration options for the trunk DN

End of procedure

Procedure:
Creating a DN for MSML VoIP Service

Purpose: To provision GVP/Media Server for Treatment of the Inbound Calls.

Start of procedure

1. In Genesys Administrator, create a new DN. Under the Options tab, select Advanced View (Annex) and add the options as shown in the figure below:

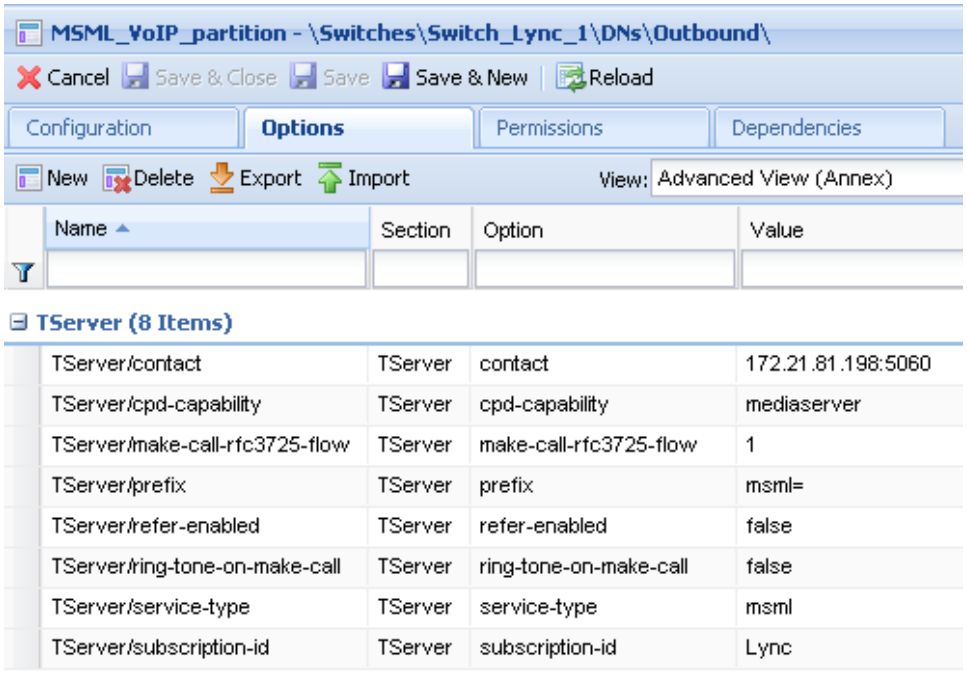

Figure 91: DN configuration options

End of procedure

Procedure:
Creating a DN for Recorder VoIP Service

Purpose: To create a DN for Recorder VoIP Service.

Start of procedure

1. In Genesys Administrator, create a new DN. Under the Options tab, select Advanced View (Annex) and add the options as shown in the figure below:

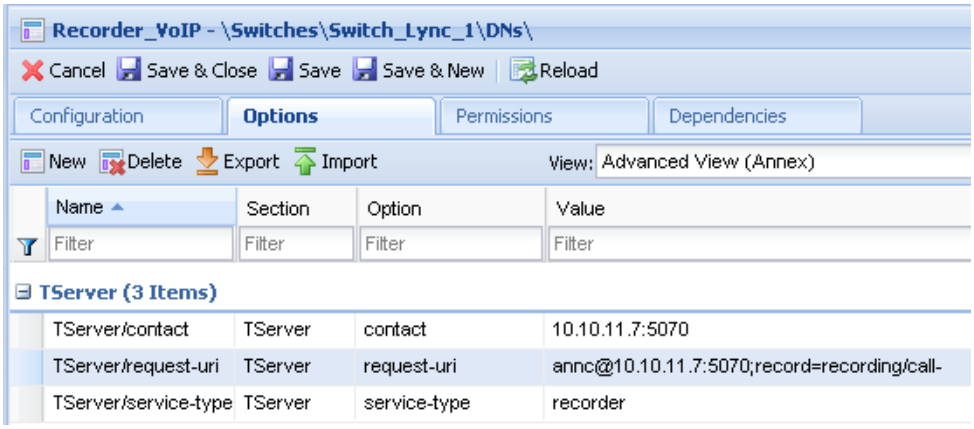

Figure 92: Configuration options for Recorder VoIP Service DN

End of procedure

UC Connector Configuration Tasks

The Genesys UC Connector is used in integration with Lync to provide presence synchronization of remote Lync users, who act as contact center agents for the Genesys solution. To do this, UC Connector subscribes to the Lync presence service and monitors presence events for all registered users. It reports presence status variations to Stat Server through a configurable mapping filter.

UC Connector connects with the Front End Pool and subscribes to Agent statuses periodically. The Lync Front End Server notifies Genesys when there are any status changes to the Lync Contact Center Agents.

Task Summary: Configuring UC Connector

Objectives	Actions
Configure UC Connector for the Front End Server.	UC Connector registers with the Front End Server, and then Subscribes to each Lync Agent Status separately. See Procedure: Configuring UC Connector for the Front End Server.
Configure UC Connector for multiple Front End Server hosts.	UC Connector can be provisioned to connect to multiple Front End Server hosts belonging to the same pool. This is compulsory when connecting to Lync Enterprise Edition. See Procedure: Configuring UC Connector for multiple Front End Server hosts.

Procedure: Configuring UC Connector for the Front End Server

Purpose: To configure UC Connector to register with the Front End Server and Subscribe to each Lync Agent Status separately.

Prerequisites

- Procedure: Processing the Client Certificate
- One of the following:
  - Procedure: Generating the Server Certificate Using Lync Management Shell
  - Procedure: Generating the Server Certificate Using Microsoft Management Console or CA Web Access

Start of procedure

1. In Genesys Administrator, open the UC Connector application and click the `Options` tab.
2. Set the value of the `Microsoft-OCS\contact` option to a valid Lync User URI.
3. Set the value of the `Microsoft-OCS\registrar-uri` option to the Lync Pool at the UC Connector application level.
4. Click the `Configuration` tab. In the Command Line Arguments field, enter the following information:

```
ucc-launcher.exe -host demosrv.genesyslab.com -port 2020 -app
UCConnector_AG -l 7260@demosrv -http_port 8092 -cert_store_file
"<client_certificate_path>" -cert_store_pass
<client_certificate_password> -cert_store_type jks -key_store_file
"<server_certificate_path>" -key_store_pass
<server_certificate_password>" -ket_store_type pkcs12
```

Note: `<client_certificate_path>`—location of the client certificate created in Procedure: Processing the Client Certificate.

`<client_certificate_password>`—the client certificate password created in Procedure: Processing the Client Certificate.

`<server_certificate_path>`—location of the server certificate created in either Procedure: Generating the Server Certificate Using Lync Management Shell or Procedure: Generating the Server Certificate Using Microsoft Management Console or CA Web Access.

`<server_certificate_password>`—the server certificate password created in either Procedure: Generating the Server Certificate Using Lync Management Shell or Procedure: Generating the Server Certificate Using Microsoft Management Console or CA Web Access.

End of procedure

Procedure: Configuring UC Connector for multiple Front End Server hosts

Purpose: To configure UC Connector to connect to multiple Front End Server hosts in the same pool.

Note: In order to provide the correct security certificates for different front ends in the same pool, the certificate keystore must contain two (or more) entries corresponding to the front ends in the same pool.

Start of procedure

1. Export `pfx (pkcs12)` files from both front ends using `mmc` on Windows (so you would have `certificate1.pfx` and `certificate2.pfx`). To export, you must set a password for each file.
2. Import the files from Step 1 into a new keystore with a new password (for example `pwd_final`):

- If the final keystore is `java` keystore, use the following commands:

Type: `keytool.exe -importkeystore -v -srckeystore certificate1.pfx -destkeystore final_certificate.jks -srcstoretype pkcs12 -deststoretype jks -srcstorepass pwd1 -deststorepass pwd_final`

Type: `keytool.exe -importkeystore -v -srckeystore certificate2.pfx -destkeystore final_certificate.jks -srcstoretype pkcs12 -deststoretype jks -srcstorepass pwd2 -deststorepass pwd_final`

- If the final keystore is `pkcs12` keystore, use the following commands:

Type: `keytool.exe -importkeystore -v -srckeystore certificate1.pfx -destkeystore final_certificate.pfx -srcstoretype pkcs12 -deststoretype pkcs12 -srcstorepass pwd1 -deststorepass pwd_final`

Type: `keytool.exe -importkeystore -v -srckeystore certificate2.pfx -destkeystore final_certificate.pfx -srcstoretype pkcs12 -deststoretype pkcs12 -srcstorepass pwd2 -deststorepass pwd_final`

3. Start UC Connector with the following arguments in command line:
   - for `java` keystore:

```
-cert_store_file final_certificate.jks -cert_store_pass pwd_final
-cert_store_type jks
```

   - for `pkcs12` keystore

```
-cert_store_file final_certificate.pfx -cert_store_pass pwd_final
-cert_store_type pkcs12
```

Notes: `keytool.exe` is a tool provided by the Java Development Kit and can be found in the `bin` directory of the JDK installation

For multiple Front End Server support, UC Connector and Lync must be in the same subnet.

End of procedure

Interaction Workspace Plug-in for Lync

Interaction Workspace, Genesys' Agent Desktop application, includes a plug-in for Lync 2010. This plug-in is distributed through the UC Connector CD, since UC Connector is necessary for integration with Lync.

Installation of this plug-in is mandatory for an Agent deployed with Lync Integration. The plug-in exercises the Lync Client local APIs to allow answering calls from Interaction Workspace.

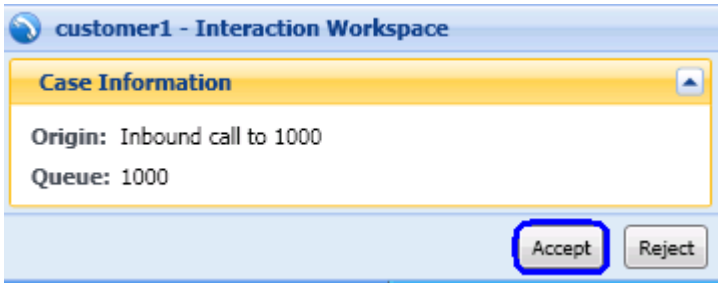

Figure 93: Answer Call Interaction Workspace toast

In effect the Answer Call Interaction Workspace toast, shown in Figure 93, implements a third-party call control answer command on the Lync 2010 Client residing in the same host. Clicking it also opens up the Interaction Workspace Call Control window, as shown in Figure 94.

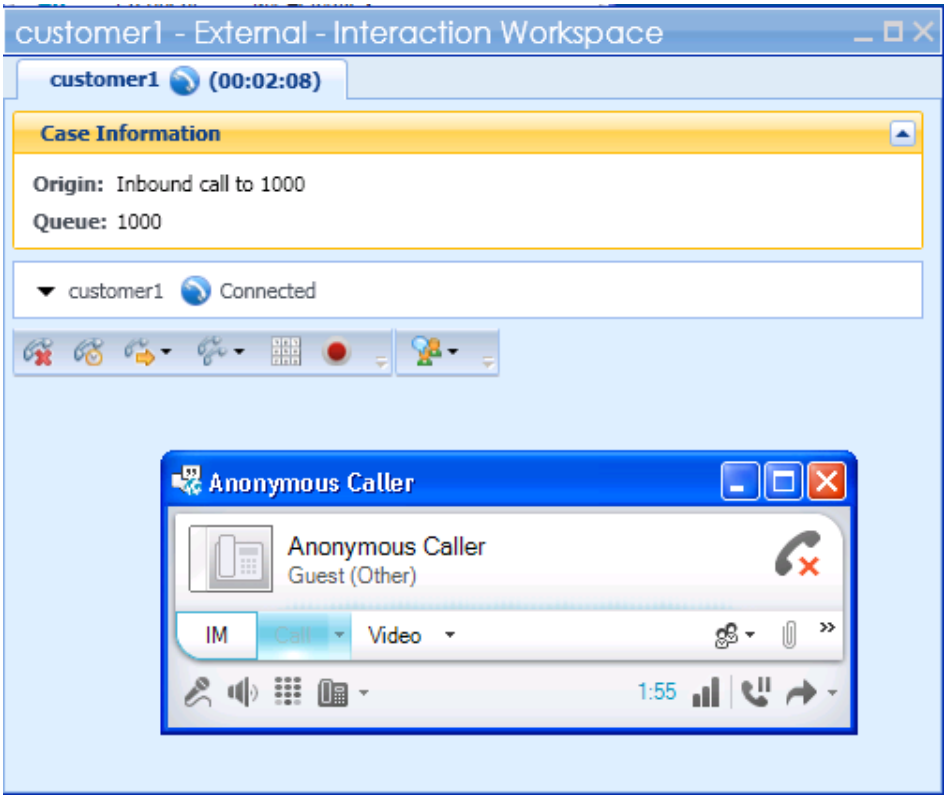

Figure 94: Interaction Workspace Call Control Window

Current Limitations

This section describes the current limitations in the SIP Server integration with Microsoft Lync 2010. This is Phase 1 of the integration with Lync Server—as the support evolves this section of the document will change and shrink.

Multiple Front End Server support on the same subnet

The Multiple Front End Server support of UC Connector depends on the mechanism used by the Windows host's DNS Client to resolve the pool's Front End IPs.

First pick from the set of resolved IPs is the default DNS Client behavior in Windows 2003 Server, usually with the DNS Server re-ordering in round-robin fashion.

Windows 2008 R2 Host DNS Client complies with the RFC3484 Rule of Destination Address selection; the unreachable destinations are automatically avoided. This is limited to hosts within the same subnet.

Genesys UC Connector is limited to provide Front End Failover support when provisioned on a Windows 2008 R2 host, and has to be in the same subnet as the Lync.

IP Phone support

Genesys only supports the use of the Lync 2010 desktop client as a soft-phone for voice communication.

This Genesys deployment does not interoperate with Lync-supported IP hard phones, such as Polycom CX 600. Currently, use of these phones has the following limitations:

- The AnswerCall option through Interaction Workspace cannot be used to answer the call on the Lync IP phone.
- 1pcc call handling, such as transfers and conference done using the IP phone, does not coordinate with the call control on the Genesys suite. Only Interaction Workspace-based 3pcc call control through Interaction Workspace should be used.

Early Media support should be disabled

When a SIP User Agent supporting Early Media (such as the SIP Server) contacts the Lync Mediation Server, the Mediation Server does not apply Media bypass condition for the call. The Mediation Server responds with a 183 Session Progress containing its own SDP, Required:100rel and an RSeq header. The SIP Server sends a RAck in the PRACK.

The Mediation Server contacts the Front End Server to reach the Lync Client—this call is Early Media enabled. When the Lync Client responds with its Early Media SDP, the Mediation Server attempts to update the UAC with the Lync Client's Early Media SDP; however, the 2nd 183 Session Progress response doesn't contain an incremented RSeq header value—the UAC doesn't process it. This is no compliant with RFC 3262 guideline.

As a result, SIP early media does not work with the Lync Mediation Server, and should be disabled as a SIP Server option.

Appendix

Genesys Lync Agent

This appendix contains the following sections:

What is Genesys Lync Agent?

Genesys Lync Agent (GLA) is a piece of software that allows the use of Microsoft Lync for voice interaction, regardless of the type of Genesys agent desktop client in use. Genesys Lync Agent is installed on an agent's machine where it runs in the background and executes remote answer commands for Microsoft Lync calls on behalf of the agent. This enables third-party call control from Genesys desktop applications. In particular, GLA supports the use of web-based Agent Desktop Clients with Microsoft Lync Enterprise Voice.

Genesys Lync Agent when running on the same machine as the Microsoft Lync Client, communicates with UC Connector to allow agents to answer incoming calls and perform call control.

When Microsoft Lync is used as Enterprise Voice, Genesys offers an integration solution which conducts telephony through Genesys SIP Server and Lync presence synchronization through UC Connector. Full Genesys desktop functionality is not supported with this solution because Microsoft Lync does not support third-party answer call and make call. The calls can only be initiated and answered using the endpoint, because neither the standard SIP nor Microsoft SIP extensions provide the means to send the command to the endpoint to accept the call.

Genesys Lync Agent solves this problem by accepting remote call control commands and executing them using the Microsoft Lync Client API. When GLA is installed on each agent desktop, it runs at the same permission level as the logged in Windows user. GLA works in the background, where it waits for the answer command and invokes the appropriate Lync Client API calls.

Genesys Lync Agent is an interface to UC Connector through cometD, and to Lync client through the Lync 2010 SDK. When a Lync client conversation window pops up, GLA signals UC Connector. UC Connector then instructs GLA to answer the active conversation.

Under normal operations, GLA is only visible as the Genesys icon in the system tray.

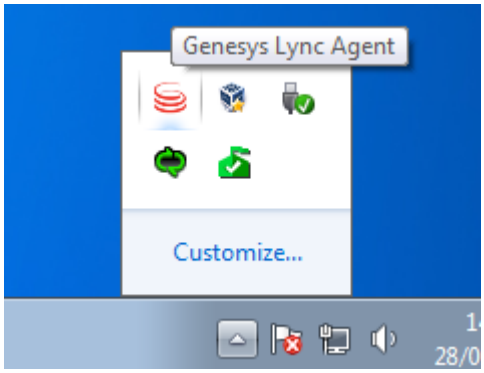

Figure 95: GLA in the system tray.

Redundancy

Genesys Lync Agent supports redundant UC Connectors in the traditional HTTP redundancy mode, which means that no special measures are made to support UC Connector redundancy in the application itself.

If the cometD connection attempt fails, GLA initiates another connection to the same URL. The minimum interval between two connection attempts is 1 second to avoid network flooding.

GLA only supports active connections to UC Connector; it does not support the warm standby redundancy method for high availability.

High Availability Support

Genesys Lync Agent only supports active connections to UC Connector. It does not support warm UC Connector standby.

Localization

Genesys Lync Agent supports the following languages:

- English (en)
- French (fr)
- Germany (de)
- Italian (it)
- Spanish (es)
- Russian (ru)

Deploying Genesys Lync Agent

Complete the following tasks to install and configure Genesys Lync Agent:

Task Summary: Deploying Genesys Lync Agent

Objective	Actions
1. Complete prerequisites.	• UC Connector 8.0.300.04+ is installed • SIP Server 8.1.0.001+ is installed. • The Lync client has been installed, and operates correctly. • The Lync SDK redistribution has been installed. • A valid desktop to connect to the Genesys environment exists. • Procedure: Prepare the UC Connector Solution
2. Install Genesys Lync Agent.	Procedure: Installing Genesys Lync Agent
3. Set the host and port for all Genesys Lync Agent users.	Centralized Administration of Host and Port Settings for all GLA Users

Procedure: Prepare the UC Connector Solution

Start of procedure

1. In Genesys Administration, go to `Environment > Applications` and double-click on the UC Connector `Application` object.
2. Go to the `Options` tab.

3. In the `UC-Connector` section, configure the following options (see *UC Connector 8.0 Deployment Guide* for more information on the configuration options):

Table 2: UC Connector—UC-Connector Section

Option Name	Default Value	Description
gla-kpl-time	30	The interval, in seconds, between keep alive messages sent from GLA to UC Connector. This value must be greater than the value for the gla-kpl-response-time option. The valid values range from 4 to any integer greater than the kpl-response-time.
gla-kpl-response-time	4	The expected time, in seconds, for UC Connector to respond to the keep alive messages sent by GLA. This value must be less than the value for the gla-kpl-time option. The valid values range from 3 to any integer less than the kpl-time.
gla-call-match-window	4000	The time window during which a T-Lib call is matched against a Lync call reported by GLA. Lync and T-Lib call events do not have a common reference and can only be matched by coincidence in time. The valid values range from 2000-15000.

4. In the In the `Microsoft-OCS` section, configure the following option:

Table 3: UC Connector—Microsoft-OCS Section

Option Name	Default Value	Description
invite-message	“Please use the window on the right to access data about current interactions”	Configure this option to be blank/no value in Genesys Administrator. This prevents an additional Lync IM conversation window from appearing on the desktop.

5. Click Save.

End of procedure

Next Steps

- See Procedure: Installing Genesys Lync Agent.

Procedure: Installing Genesys Lync Agent

Start of procedure

1. On the UC Connector 8.0 product CD, locate the Genesys Lync Agent setup.exe file in the lync folder.
2. Follow the Wizard instructions, clicking Next through each of the following pages:
   a. Choose Destination Location—Select the path where Genesys Lync Agent will be installed.
   b. Genesys Lync Agent Parameters—Enter the host name where UC Connector is running and the UC Connector HTTP port.
   c. Ready to Install—Click Install to proceed.
4. In the final Installation Complete page, click Finish.

End of procedure

Next Steps

- See Centralized Administration of Host and Port Settings for all GLA Users.

Centralized Administration of Host and Port Settings for all GLA Users

The two procedures below are examples of ways to centralize the set-up of host and port registry settings for a Genesys Lync Agent user.

To complete either of these procedures, you must first have Administrator access to the Domain Controller within your network. See Procedure: Set up Administrator access to the Domain Controller.

Procedure:
Set up Administrator access to the Domain Controller

Start of procedure

1. Open the Group Policy Management Console.
   - Click `Start` > `All Programs` > `Accessories` > `Run` and type `gpmc.msc` in the text box. Click `OK`.
2. Select `Forest` > `Domains` > `<your domain>` > `Group Policy Objects` and double-click `Default Domain Policy`.

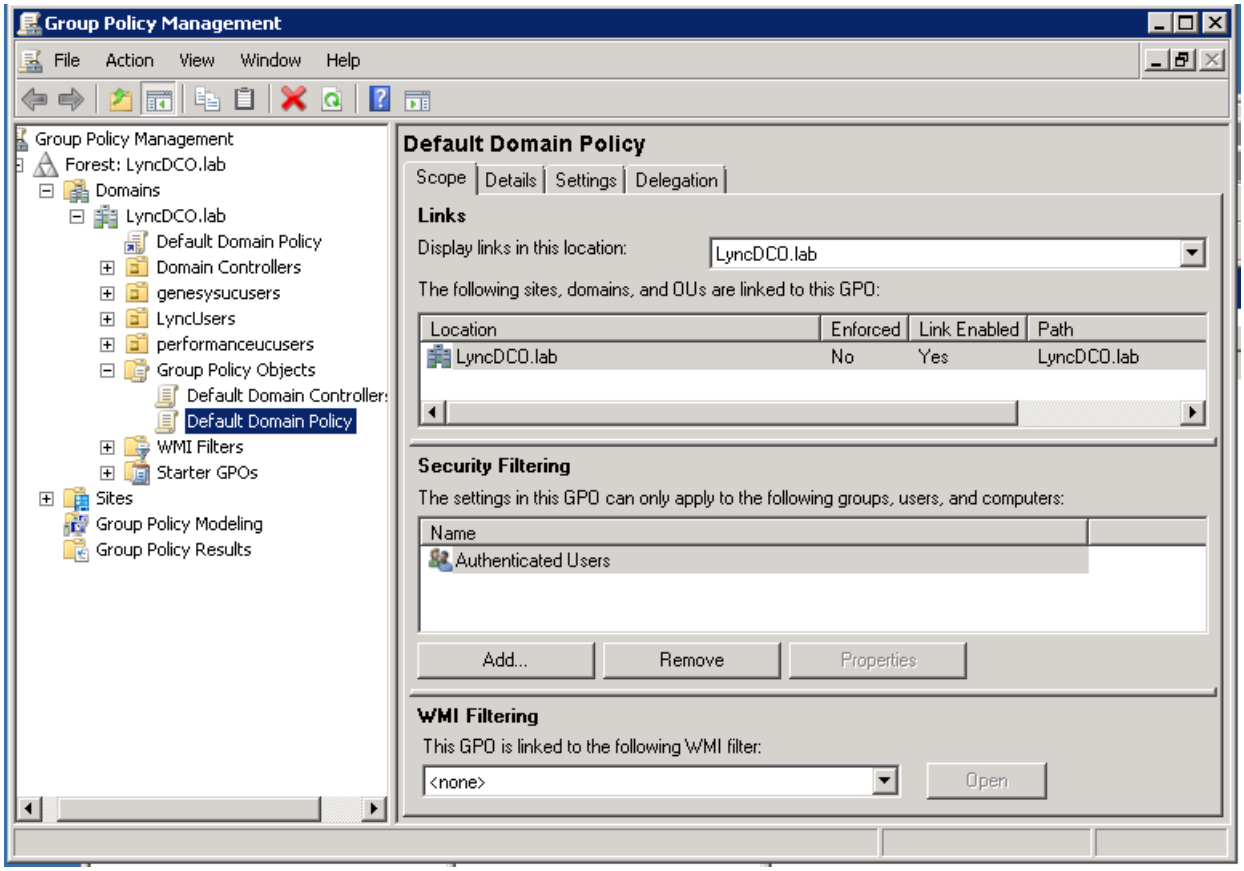

Figure 96: Group Policy Management window.

End of procedure

Next Steps

- Complete one of the following:
  - Procedure: Run script when the computer starts up
  - Procedure: Change registry entries directly

Procedure:
Run script when the computer starts up

Prerequisites

- Procedure: Set up Administrator access to the Domain Controller

Start of procedure

1. Select Computer `Configuration > Policies >Windows Settings >Scripts (Start-up/Shut-down).`
2. Select `Startup`.
3. On the `Scripts` tab, use the `Add` button to add the following

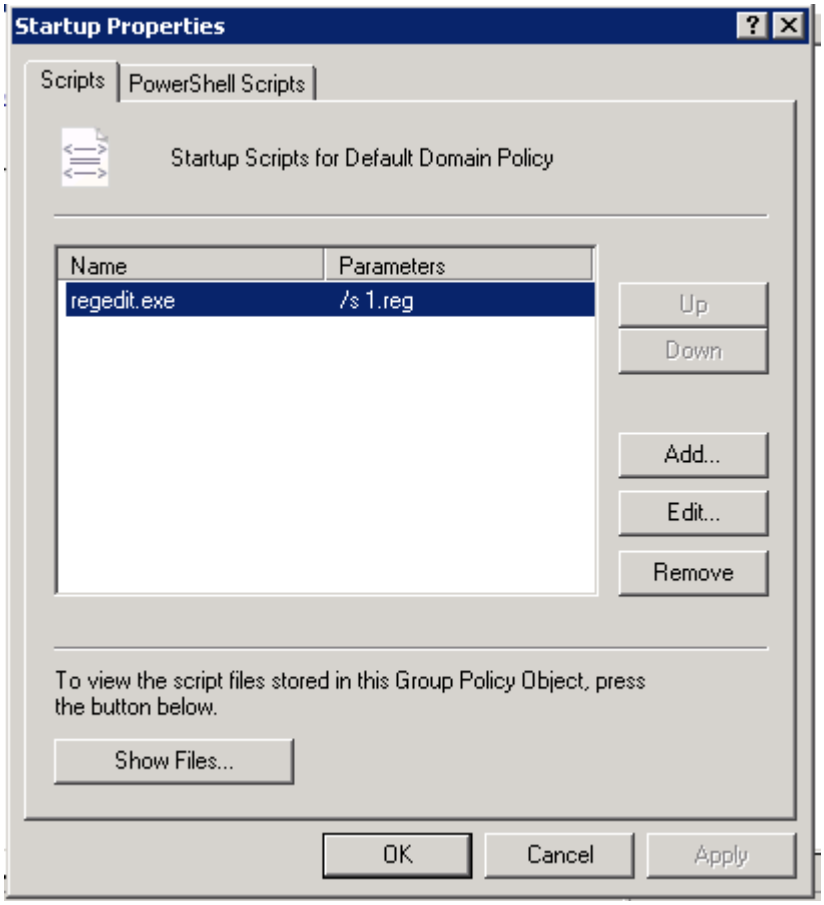

Figure 97: Startup Properties.

4. The script will run a single line to modify the registry with the parameters in 1.reg. The contents of 1.reg are:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\GCTI]
[HKEY_LOCAL_MACHINE\SOFTWARE\GCTI\GenesysLyncAgent]
```

```
"Host"=hex(2):53,00,62,00,68,00,61,00,6e,00,64,00,65,00,72,00,69,00
,2d,00,50,\
 00,43,00,00,00
"Port"=dword:00001f90
```

5. Add this file to the group policy object. Select `Show Files...` and add the file at the same location.

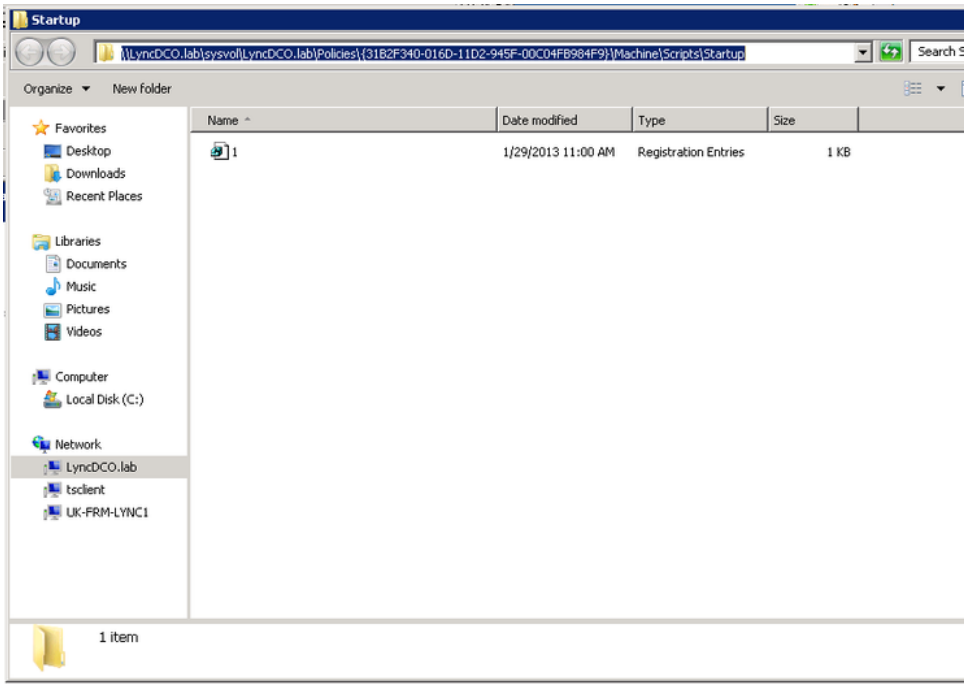

Figure 98: Startup file location.

End of procedure

Procedure:
Change registry entries directly

Prerequisites

- Procedure: Set up Administrator access to the Domain Controller

Start of procedure

1. Select `Computer Configuration > Preferences > Windows Settings > Registry`.
2. Add the entries in the figure below:

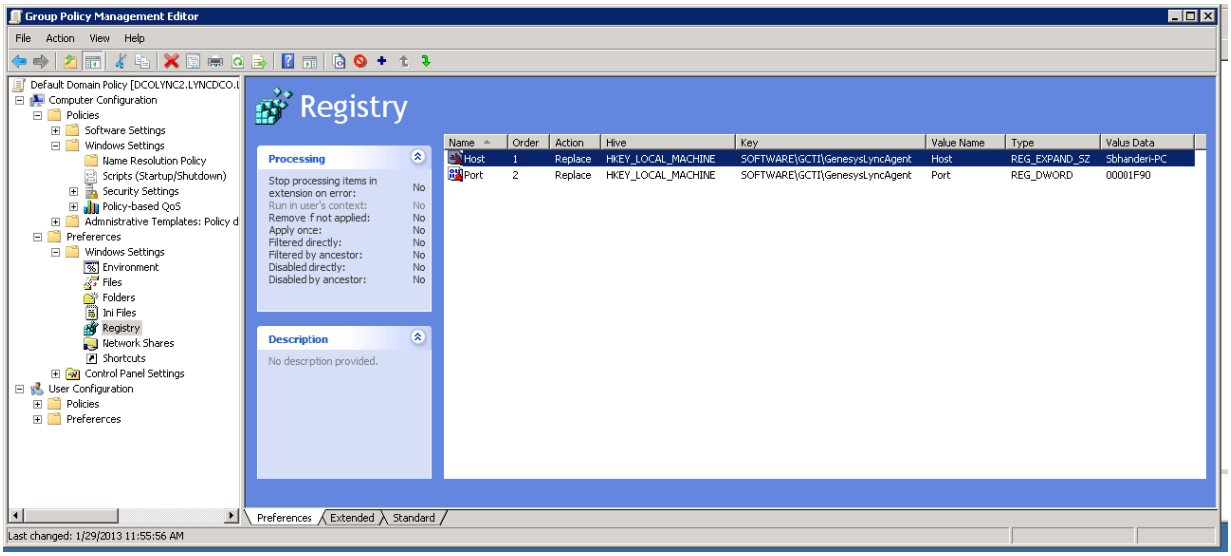

Figure 99: Scripts Registry.

End of procedure

Using Genesys Lync Agent

Under normal operations, Genesys Lync Agent is only visible as the Genesys icon in the system tray.

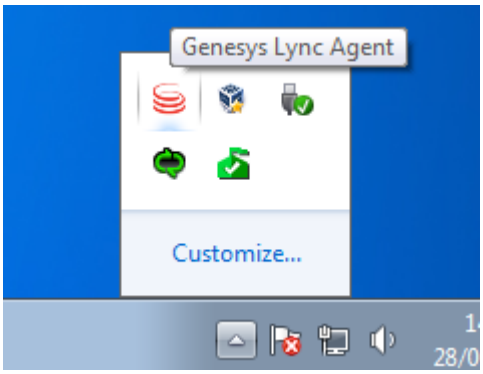

Figure 100:GLA in the system tray.

To see the menu options, right-click the GLA application in the system tray.

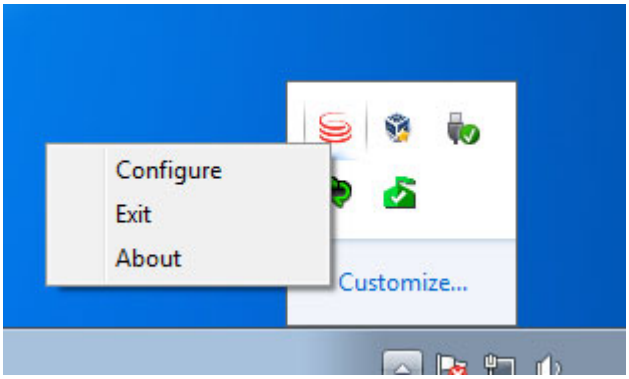

Figure 101:GLA menu options.

Configure—Opens GLA.

Exit—Terminates GLA.

About—Displays details about GLA.

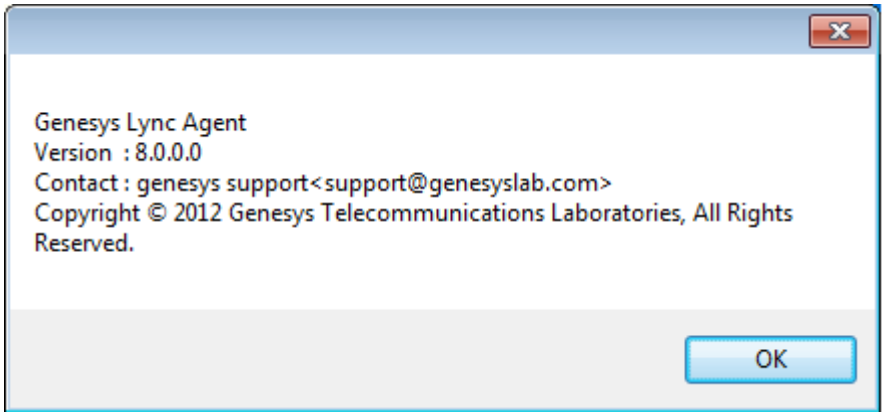

Figure 102:GLA About window.

How GLA Connects to UC Connector

At the start, GLA tries to check the connection to UC Connector by sending a "test" message. If successful, UC Connector acknowledges the message and the tray icon changes to indicate the results of the test.

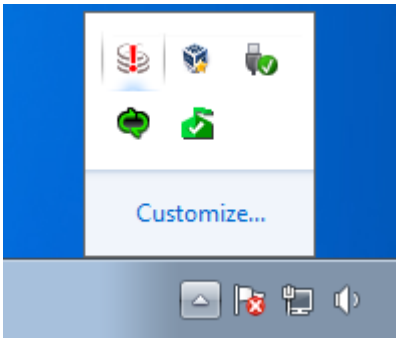

Figure 103:A bad connection icon.

As soon as GLA starts running, it begins the heartbeat process with UC Connector. If UC Connector responds, the connection is good and the corresponding icon is shown in the system tray. If there is no response, the connection is bad and the corresponding icon is shown in the system tray. A bad connection will also open the Genesys Lync Agent GUI; once you close this GUI, the heartbeat process will be restarted.

Heartbeat (Keep Alive) to UC Connector

Figure 104 shows how the keep alive mechanism interacts with UC Connector. The UC Connector option `gla-kpl-time` is set to 30 seconds, which is the

heartbeat rate. The UC Connector option `gla-kpl-response-time` is set to 4 seconds, the time in which a response must be received.

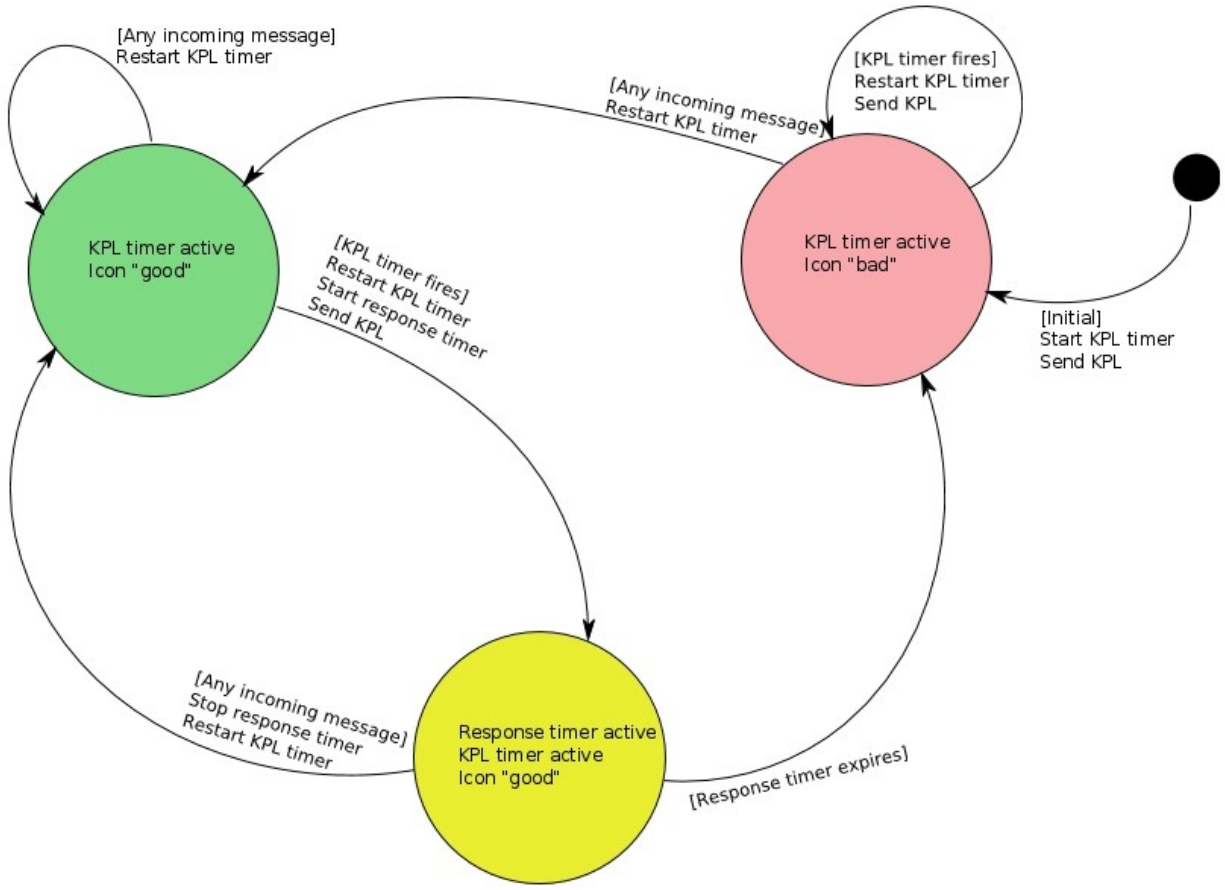

Figure 104:Keep alive and UC Connector.

Heartbeat failure

If Genesys Lync Agent's attempt to connect to UC Connector fails (the heartbeat fails), GLA displays a balloon tip.

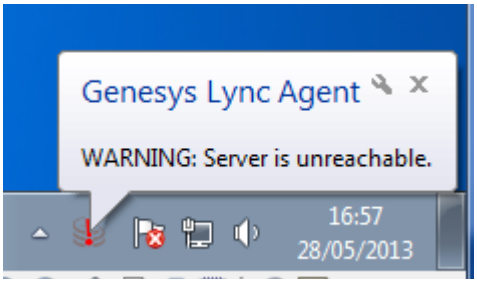

Figure 105:No response from UC Connector warning.

In the system tray, GLA changes its icon to a grey Genesys icon with a red exclamation mark and displays a warning message.

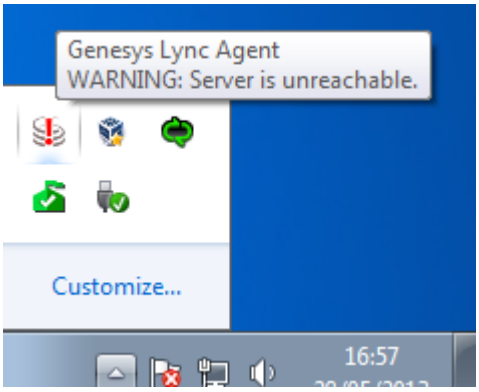

Figure 106:No response from UC Connector system tray warning.

Understanding GLA window controls

Genesys Lync Agent is normally minimized to the system tray, but it is displayed on the desktop in the following scenarios:

- The Lync client is not started.
- The Lync client user is not logged in.
- The Host and Port are not available in the GLA registry entry.
- The user double-clicks `Configure` in the GLA menu.

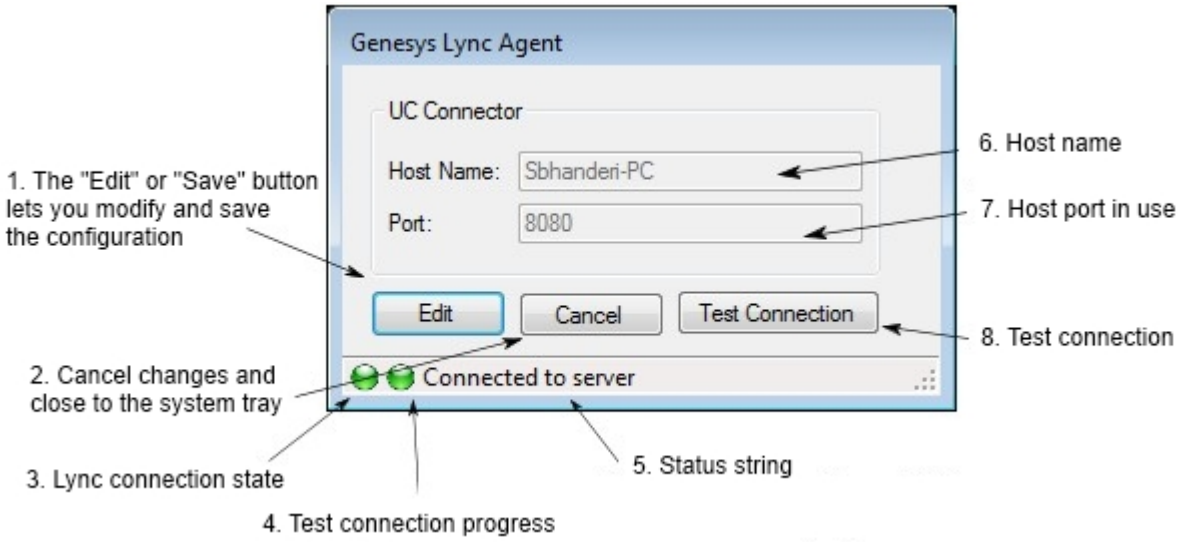

Figure 107:GLA window controls.

In Figure 107:

1. Click `Edit` to modify the `Host Name` and `Port`, then click `Save`. See Modifying the Host and Port Entries.

2. Click `Cancel` to cancel the changes to `Host Name` and `Port`, or to minimize GLA to the system tray without making any changes.
3. Shows the Lync client connection state. The icon is green if GLA is connected to the Lync client. The icon is red if:
   - The Lync client user is not logged in.
   - The Lync client is not started.
   - Genesys Lync Agent cannot connect to the Lync client.
4. Shows the test connection progress when the user clicks `Test Connection`. The icon can be one of three colors:
   - Yellow—GLA has sent a message to UC Connector.
   - Red—The message response from UC Connector is invalid or the connection cannot be established.
   - Green—The connection has been established.
   - Blue—The host and port details have been modified and saved, but `Test Connection` has not been clicked.
5. Displays the Lync user name, if available, or the test connection progress state if the user clicks `Test Connection`.
6. The host name of the machine where UC Connector is running.
7. The UC Connector HTTP port.
8. Click `Test Connection` to test the connection to UC Connector. The Lync client must be running and the user must be logged in. When testing the connection, normal operations to UC Connector will be suspended, so the answer call and make call features will not work.

Note: The Lync Client must be running and the user must be logged in before attempting to test the connection.

Modifying the Host and Port Entries

When the GLA user is not an Administrator, the following changes are seen in the GLA window:

- The `Save` button is replaced with `Edit`.
- The `Host Name` field is disabled and modifications are not allowed.
- The `Port` field is disabled and modifications are not allowed.

If the user is in the Administrator group and User Account Control (UAC) is enabled, then GLA can be promoted to Administrator by clicking `Edit` in GLA.

The UAC menu appears and, if successful, the button name will change to `Save` in GLA.

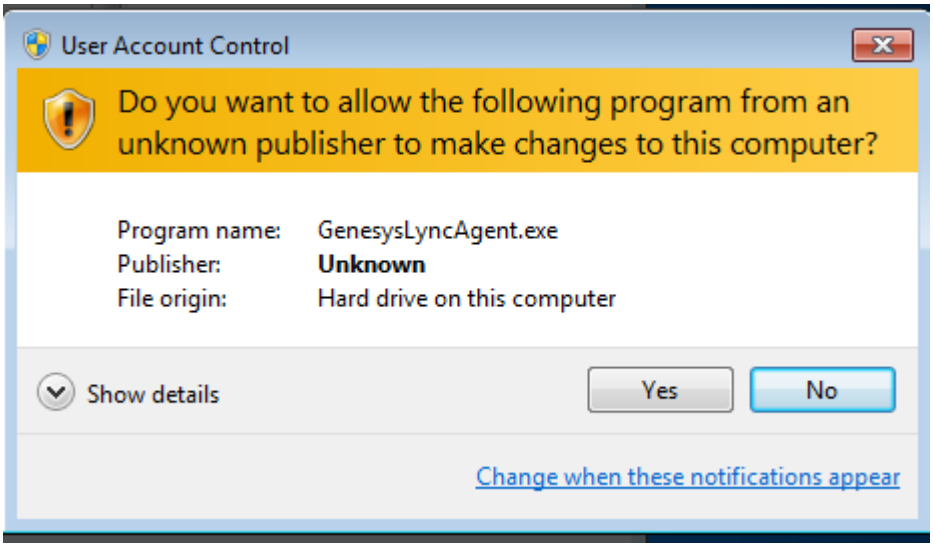

Figure 108:User Account Control window for a user in the Administrator group.

If the user is not in the Administrator group and clicks `Edit`, UAC displays a window asking the user to login to the application as Administrator. If successful, the button name will change to `Save` in GLA.

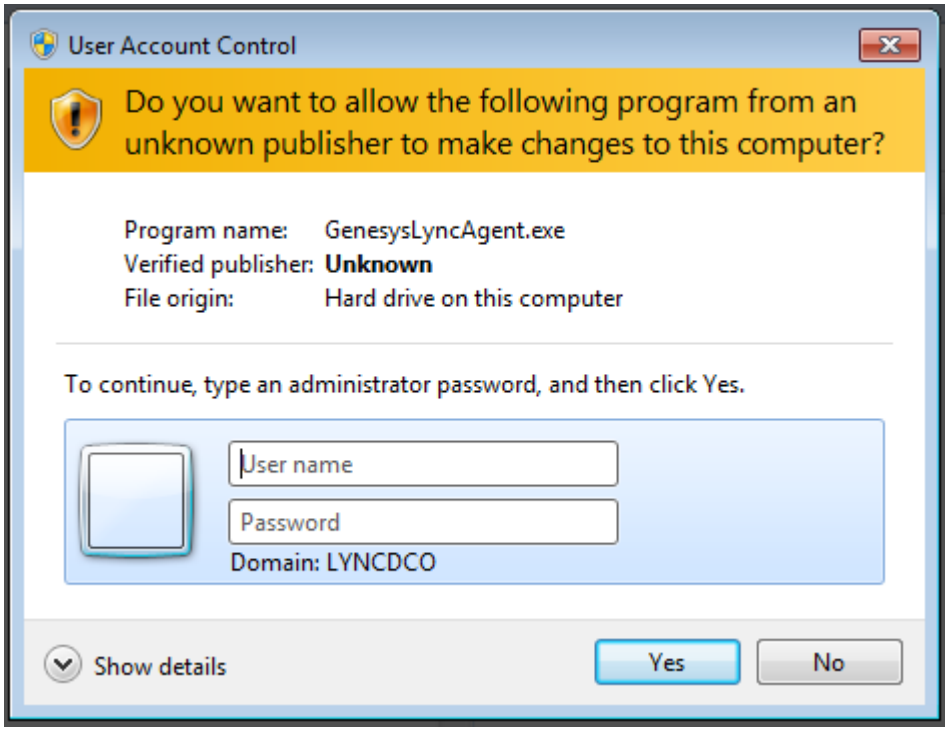

Figure 109:User Account Control window for a user not in the Administrator group.

Note: If the user is not in the Administrator group and GLA is running as Administrator, then it is possible that GLA will not be able to communicate with the Lync client.

When the user successfully accesses GLA as Administrator, the `Host Name` and `Port` fields are editable.

Supplements

Related Documentation Resources

The following resources provide additional information that is relevant to this software. Consult these additional resources as necessary.

UC Connector

- *UC Connector 8.0 Deployment Guide*, which provides information to configure and install UC Connector.

T-Server

- *Framework 8.1 SIP Server Deployment Guide*, which provides information to configure and install SIP Server.

Microsoft Lync Server 2010

- Microsoft Lync Server 2010 Documentation Help File. This download contains a compiled help file (chm) of all the available Lync Server 2010 IT professional documentation on the Technical Library.
  `http://www.microsoft.com/download/en/details.aspx?id=23888`

Open Standards

- *RFC 3261 SIP: Session Initiation Protocol*
- *RFC 3863 Presence Information Data Format (PIDF)*
- *RFC 3265 Session Initiation Protocol (SIP)-Specific Event Notification*

Genesys

- *Genesys Technical Publications Glossary,* which ships on the Genesys Documentation Library DVD, provides a comprehensive list of the Genesys and computer-telephony integration (CTI) terminology and acronyms used in this document.
- *Genesys Migration Guide*, which ships on the Genesys Documentation Library DVD, provides documented migration strategies for Genesys product releases. Contact Genesys Technical Support for more information.

Information about supported hardware and third-party software is available on the Genesys Technical Support website in the following documents:

- *Genesys Supported Operating Environment Reference Guide*
- *Genesys Supported Media Interfaces Reference Manual*

Consult the following additional resources as necessary:

- *Genesys Hardware Sizing Guide,* which provides information about Genesys hardware sizing guidelines for the Genesys 8.x releases.
- *Genesys Interoperability Guide,* which provides information on the compatibility of Genesys products with various Configuration Layer Environments; Interoperability of Reporting Templates and Solutions; and Gplus Adapters Interoperability.
- *Genesys Licensing Guide,* which introduces you to the concepts, terminology, and procedures that are relevant to the Genesys licensing system.
- *Genesys Database Sizing Estimator 8.x Worksheets,* which provides a range of expected database sizes for various Genesys products.

For additional system-wide planning tools and information, see the release-specific listings of System Level Documents on the Genesys Technical Support website. These documents are accessible from the `system level documents by release` tab in the Knowledge Base `Browse Documents` Section.

Genesys product documentation is available on the:

- Genesys Technical Support website at `http://genesyslab.com/support`.
- Genesys Documentation wiki at `http://docs.genesyslab.com/`.
- Genesys Documentation Library DVD and/or the Developer Documentation CD, which you can order by e-mail from Genesys Order Management at `orderman@genesyslab.com`.

Document Conventions

This document uses certain stylistic and typographical conventions—introduced here—that serve as shorthands for particular kinds of information.

Document Version Number

A version number appears at the bottom of the inside front cover of this document. Version numbers change as new information is added to this document. Here is a sample version number:

80fr_ref_06-2008_v8.0.001.00

You will need this number when you are talking with Genesys Technical Support about this product.

Screen Captures Used in This Document

Screen captures from the product graphical user interface (GUI), as used in this document, may sometimes contain minor spelling, capitalization, or grammatical errors. The text accompanying and explaining the screen captures corrects such errors *except* when such a correction would prevent you from installing, configuring, or successfully using the product. For example, if the name of an option contains a usage error, the name would be presented exactly as it appears in the product GUI; the error would not be corrected in any accompanying text.

Type Styles

Table 4 describes and illustrates the type conventions that are used in this document.

Table 4: Type Styles

Type Style	Used For	Examples
Italic	• Document titles • Emphasis • Definitions of (or first references to) unfamiliar terms • Mathematical variables Also used to indicate placeholder text within code samples or commands, in the special case where angle brackets are a required part of the syntax (see the note about angle brackets on page 128).	Please consult the *Genesys Migration Guide* for more information. Do *not* use this value for this option. A *customary and usual* practice is one that is widely accepted and used within a particular industry or profession. The formula, $x + 1 = 7$ where x stands for . . .

Table 4: Type Styles (Continued)

Type Style	Used For	Examples
Monospace font (Looks like `teletype` or `typewriter text`)	All programming identifiers and GUI elements. This convention includes: • The *names* of directories, files, folders, configuration objects, paths, scripts, dialog boxes, options, fields, text and list boxes, operational modes, all buttons (including radio buttons), check boxes, commands, tabs, CTI events, and error messages. • The values of options. • Logical arguments and command syntax. • Code samples. Also used for any text that users must manually enter during a configuration or installation procedure, or on a command line.	Select the `Show variables on screen` check box. In the `Operand` text box, enter your formula. Click `OK` to exit the `Properties` dialog box. T-Server distributes the error messages in `EventError` events. If you select `true` for the `inbound-bsns-calls` option, all established inbound calls on a local agent are considered business calls. Enter `exit` on the command line.
Square brackets ([ ])	A particular parameter or value that is optional within a logical argument, a command, or some programming syntax. That is, the presence of the parameter or value is not required to resolve the argument, command, or block of code. The user decides whether to include this optional information.	`smcp_server -host [/flags]`
Angle brackets (< >)	A placeholder for a value that the user must specify. This might be a DN or a port number specific to your enterprise. **Note:** In some cases, angle brackets are required characters in code syntax (for example, in XML schemas). In these cases, italic text is used for placeholder values.	`smcp_server -host <confighost>`

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

P

R

S

T

U

V