

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 multichannel 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

7 7
7
7
8
8
8
9
10
11
12
13
14
17
17
27
37
37
54
65
69
69 75

Chapter 5	Certificate Generation for Genesys Applications	87
	Generate Client Certificate	87
	Generate Server Certificate	89
Chapter 6	Genesys Component Configuration for Lync Interoperability	93
	SIP Server Configuration Tasks	94
	UC Connector Configuration Tasks	99
	Interaction Workspace Plug-in for Lync	. 102
	Current Limitations	
	Multiple Front End Server support on the same subnet	. 104
	IP Phone support	. 104
	Early Media support should be disabled	. 104
Appendix	Genesys Lync Agent	107
	What is Genesys Lync Agent?	. 108
	Redundancy.	
	High Availability Support	. 109
	Localization	. 109
	Deploying Genesys Lync Agent	. 110
	Centralized Administration of Host and Port Settings	
	for all GLA Users	. 112
	Using Genesys Lync Agent	
	How GLA Connects to UC Connector	
	Understanding GLA window controls	. 120
Supplements	Related Documentation Resources	. 125
	Document Conventions	. 127
Index		129



List of Procedures

Installing Active Directory	17	7
Configuring Active Directory	2′	1
Installing Active Directory Certificate Services	28	3
Installing Lync Server 2010	37	7
Granting Setup Permissions	4	5
Granting Administrative Permissions	47	7
Adding DNS Records	49	9
Creating the Lync File Share	52	2
Creating a Topology	54	4
Configuring the Administrative URL	6′	1
Publishing the Topology	62	2
Installing the local configuration store	6	5
Installing the Front End Server	68	3
Requesting, installing and assigning certificates	69	9
Creating users in Active Directory		5
Configuring users through the Lync Control Panel	77	7
Configuring voice routing for users	79	9
Creating a new PSTN Gateway	83	3
Configuring UC Connector as a trusted application	8	5
Generating the Client Certificate	87	7
Processing the Client Certificate	88	3
Generating the Server Certificate Using Lync Management Shell	89	9
Generating the Server Certificate Using Microsoft Management Console or CA Web Access	9	1
Configuring a soft switch DN for Lync	9	5
Creating a Trunk DN for Mediation Server	97	7
Creating a DN for MSML VoIP Service	98	3
Creating a DN for Recorder VoIP Service	99	9
Configuring UC Connector for the Front End Server	. 100)
Configuring UC Connector for multiple Front End Server hosts	. 101	1

Prepare the UC Connector Solution	110
Installing Genesys Lync Agent	112
Set up Administrator access to the Domain Controller	113
Run script when the computer starts up	114
Change registry entries directly	115



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 <u>orderman@genesyslab.com</u>.

This preface contains the following sections:

- About Genesys Lync Integration, page 7
- Intended Audience, page 7
- Making Comments on This Document, page 8
- Contacting Genesys Technical Support, page 8
- Document Change History, page 8

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 <u>Techpubs.webadmin@genesyslab.com</u>.

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.



O

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, page 10

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



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, page 14

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
 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
	 "Defining Users in Lync" on page 75
	 "Genesys-Specific Lync Configurations" on page 83
5. Generate certificate for Genesys applications.	 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.

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.

Task Summary: Deploying Lync and Genesys components (Continued)





Chapter



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, page 17
- Installing Active Directory Certificate Services, page 27

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

- 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.

Before You Begin Server Roles	Select one or more roles to install on this server. Roles:	Description:
Active Directory Domain Services Confirmation Progress Results	Active Directory Certificate Services Active Directory Pederation Services Active Directory Federation Services Active Directory Rights Management Services DHCP Server DHCP Server BHS Server File Services File Services UDOI Services UDOI Services UDOI Services Web Server (IIS) Windows Deployment Services	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
	More about server roles	

Figure 4: Selecting Active Directory Domain Service

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

Add features required for Active You cannot install Active Directory Domain Service	
Features:	Description:
INET Framework 3.5.1 Features INET Framework 3.5.1	Microsoft NET Framework 3.5.1 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, and provide the ability to model a range of business processes.
	Add Required Features Cancel

Figure 5: Add Required Features

6. Click Next.

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

Add Roles Wizard	×
Active Director	y Domain Services
Before You Begin Server Roles Active Directory Domain Services Confirmation Progress Results	 Introduction to Active Directory Domain Services Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and colaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy. Things to Note The policy provides a DNS server to be installed on the network in the case of a server outage, install a minimum of two domain controllers for a domain. A Ds requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this server. After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dormon-exe) to make the server a fully functional domain controller. Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by Directory Service. Additional Information Merview of AD DS Installing AD DS Magains AD DS
	< Previous Next > Instal Cancel

Figure 6: Active Directory Domain Services

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

Before You Begin Server Roles Active Directory Domain Services	To install the following roles, role services, or features, click Install.
Confirmation	(1) This server might need to be restarted after the installation completes.
Progress	Active Directory Domain Services
Results	After you install the AD DS role, use the Active Directory Domain Services Installation Wizard (dcpromo.exe) to make the server a fully functional domain controller. JIET Framework 3.5.1 Features
	JNET Framework 3.5.1

Figure 7: Confirm Installation Selections

9. On the Installation Results screen, click Close.

Before You Begin Server Roles Active Directory Domain Services	The following roles, role services, or features we (i) 1 informational message below	re installed successfully:
Confirmation Progress Results	fully functional domain controller.	Installation succeeded Installation Wizard (dcpromo.exe) to make the server a tory Domain Services Installation Wizard (dcpromo.exe).
	 .NET Framework 3.5.1 Features The following features were installed: .NET Framework 3.5.1 	Installation succeeded

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

- 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.

Active Directory Domain Services Installation Wizard	Í
Choose a Deployment Configuration You can create a domain controller for an existing forest or for a new forest.	
C Existing forest	
C. Add a domain controller to an existing domain	
C Create a new domain in an existing forest This server will become the first domain controller in the new domain	
Create a new domain in a n x forest	
More about possible deployment configurations	

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.

		100
Name the Forest Root Do The first domain in the for the forest.	omain rest is the forest root domain. Its name is also the name of	10000
Type the fully qualified do	main name (FQDN) of the new forest root domain.	
EQDN of the forest root d	lomain:	
LyncDCO.lab		
Example: corp.contoso.co	om	

Figure 10: Name the Forest Root Domain Page

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

Active Directory Domain Services Installation Wizard	3
Set Forest Functional Level Select the forest functional level.	
Forest functional level:	
Windows Server 2008 R2	•
Details:	
The Windows Server 2008 R2 forest functional level provides all the features that are available in the Windows Server 2008 forest functional level, plus the following additional feature: - Recycle Bin, which, when it is enabled, provides the ability to restore deleted objects in their entirety while Active Directory Domain Services is running. Any new domains that are created in this forest will operate by default at the Windows Server 2008 R2 domain functional level.	ন
You will be able to add only domain controllers that are running Windows Server 2008 R2 or later to this forest.	
More about domain and forest functional levels	
< Back Nept >	Cancel

Figure 11: Set Forest Functional Level Page

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

Active Directory Domain Services Installation Wizard	×
Additional Domain Controller Options	
Select additional options for this domain controller.	1
DNS server	
🔽 Global catalog	
Fead only domain controller (RODC)	
Additional information:	
cannot be an RODC. We recommend that you install the DNS Server service on the first domain controller.	
	-
More about additional domain controller options	

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.

Active Directory Domain Services Installation Wizard Location for Database, Log Files, and SYSVOL Specify the folders that will contain the Active Directory doma database, log files, and SYSVOL	in controller
For better performance and recoverability, store the database volumes.	and log files on separate
Database folder:	
C:\Windows\NTDS	Browse
Log files folder:	
C:\Windows\NTDS	Browse
SYSVOL folder:	
C:\Windows\SYSVOL	Browse
More about <u>placing Active Directory Domain Services files</u>	
< Back	Next > Cancel

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.

Directory Services Resto	ore Mode Administrator Password	
		1
The Directory Services F Administrator account.	Restore Mode Administrator account is different from the	e domain
	e Administrator account that will be used when this dor ectory Services Restore Mode. We recommend that yo rd.	
Password:	•••••	1
Confirm password:		
More about Directory Ser	vices Restore Mode password	

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.

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

Figure 16: Add Roles Wizard

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

Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Active Directory Certificate Services Active Directory Domain Services (Installed) Active Directory Pederation Services (Installed) Active Directory Rights Management Services Active Directory Rights Management Services Application Server DHCP Server ONS Server (Installed) File Services Hyper-V Network Policy and Access Services Print and Document Services Web Server (IIS) Windows Server Update Services	Description: Active Directory Certificate Service (AD CS) is used to create certificati authorities and related role service that allow you to issue and manag- certificates used in a variety of applications.

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.

Before You Begin Server Roles	Select the role services to install for Active Directory Certific Role services:	cate Services: Description:
AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Certification Authority Certification Authority Web Enrolment Online Responder Network Device Enrolment Service Certificate Enrolment Web Service Certificate Enrolment Policy Web Service	Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
	More about role services	

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.

Add Roles Wizard		×
Configure Cry	yptography for CA	
Before You Begin Server Roles AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	To create a new private key, you must first select a cryptographic service provide; hash algorithm, and key length that are appropriate for the intended use of the certificates that you issue. Selecting a higher operations.	
	More about cryptographic options for a CA	
	<pre>< Previous Next > LostalCancel</pre>	

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.

Add Roles Wizard	llation Selections	×
Before You Begin Server Roles AD CS	To install the following roles, role servic 1 varning, 1 informational messa	ges below
AD CS Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	Active Directory Certificate S Certification Authority	of this computer cannot be changed after Certification Authority has Enterprise Root RSA#Microsoft Software Key Storage Provider SHA1 2048 Disabled 2/28/2016 1:32 PM CN= LyncDCO-DCOLYNC2-CA,DC= LyncDCO,DC=local C:\Windows\pystem32\CertLog
	Print, e-mail, or save this information	<previous next=""> Instal Cancel</previous>

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



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, page 37
- Creating the New Topology, page 54
- Lync Server Front End Setup, page 65
- Defining Users in Lync, page 75
- Genesys-Specific Lync Configurations, page 83

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.

Microsoft Lync Server 2010		X
In order to run the software on this CD, the Microsoft Visual C+ Redistributable - x64 9.0.30729.4148 Package must be installed wish to install it?		
Yes	No	

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.

B Hicrosoft Lync Server 2010	×
Lync Server 2010	
Specify the location for the installation files. Any additional Lync Server components th also go to this folder.	at you install will
To install Lync Server 2010, Core Components and start the Deployment Wizard, click	Install.
Installation Location:	10.12 M
C:\Program Files\Microsoft Lync Server 2010	Browse
Install	Cancel

Figure 25: Microsoft Lync Server 2010 Installation Location

7. On the License Agreement page, accept the end–user license agreement, and then click 0K.

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.

Lync S	erver 2010 - Deployment Wizard	×
	Prepare Active Directory for Lync Server These tasks prepare Active Directory for your Lync Server installation.	
aploy > A	Active Directory Preparation	4
Step 1:	Prepare Schema Run once per deployment. Extends the schema for Lync Server.	-
	Prerequisites + Run	
	Verify Replication of Schema Partition Verify that the schema partition has been replicated before preparing the forest. Help •	
Step 3:	Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components.	
	Not Available: The schema must be prepared before you can prepare the forest. Prerequisites Help Run	
	Verify Replication of Global Catalog Verify that settings in the global catalog have been replicated before preparing a domain. Help >	
Step 5:	Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups.	-
	Not Available: The schema and forest must be prepared before you can prepare the domain. Prerequisites Help Run	
		-

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.

Prepare Schema			2
Executing Commands			
> Prepare Schema			
Install-CSAdServerSchema -Confirm:\$false -Verbos \Temp\Install-CSAdServerSchema-[2011_02_28][1 Creating new log file "C:\Users\Administrator.LYNC CSAdServerSchema-2097b930-87de-4b64-a557-90 Modify the Active Directory schema to support Lync Creating new log file "C:\Users\Administrator.LYNC [2011_02_28][16_24_06].html". "Install-CSAdServerSchema" processing has compl Detailed results can be found at "C:\Users\Administ CSAdServerSchema-[2011_02_28][16_24_06].html	16_24_06].html" CDC0\AppData\Local\Temp\ c38058bbdc7.xml". hc Server 2010. CDC0\AppData\Local\Temp\ leted successfully. strator.LYNCDC0\AppData\L	Install- Install-CSAdServerScl	
Task status: Completed.			
Prepare Schema			View Log

Figure 29: Task Status Completed

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

1	Prepare Active Directory for Lync Server	
2	These tasks prepare Active Directory for your Lync Server installation.	
eploy > A	ctive Directory Preparation	
	Prepare Schema Run once per deployment. Extends the schema for Lync Server.	
	Prerequisites Help Complete	Run
Manual	Verify Replication of Schema Partition Verify that the schema partition has been replicated before preparing the forest. Help >	
100	Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components.	
	Prerequisites + Help +	Run
Manual	Verify Replication of Global Catalog Verify that settings in the global catalog have been replicated before preparing a domain. Help •	
	Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal gro	oups.
	Not Available: The schema and forest must be prepared before you can prepare the domain.	
	Prerequisites +	
	Help •	Run
Step 6:	Verify Replication in the Domain	
and the second division of the second divisio	and dealer of the second states of the second state	

Figure 30: Prepare Schema Completed

14. On the Prepare Forest window, click Next.

🛜 Prepare Forest		
Prepare Forest		
Run once per deployment to create global settings an	d universal groups for Lync Server com	ponents.
Help	Back Next	Cancel

Figure 31: Prepare Forest Window

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

🛜 Pi	Prepare Forest	X
	Universal Group Location	
wa	pecify the domain where the universal groups will be created. By default, the local domain is used. If you do n ant the universal groups to be created in the local domain, please specify the FQDN of the domain where you ould like the universal groups to be created.	ot
•	Local domain	
C	Domain FQDN	_
	Example: domain.contoso.com Help Back Next Cancel	

Figure 32: Universal Group Location Page

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

Prepare Forest		Contract of the second second	
Executing Comma	nds		
> Prepare Forest			
Enable-CSAdForest -Verbose -Confirm:: \Enable-CSAdForest-[2011_02_28][16_; Creating new log file "C:\Users\Administ b806-4841-b174-ee8008f55e2d.xml". Enable the Active Directory forest to ho: Creating new log file "C:\Users\Administ [2011_02_28][16_29_35].html". "Enable-CSAdForest" processing has cor Detailed results can be found at "C:\User [2011_02_28][16_29_35].html".	29_35].html" trator. LYNCDCO\A st Lync Server 2010 trator. LYNCDCO\A mpleted successful	ppData\Local\Temp\Er 0 deployments. ppData\Local\Temp\Er ly.	able-CSAdForest-37d892fd- able-CSAdForest-
ask status: Completed.			
repare Forest			View Log
Help		Back	Finish Cancel

Figure 33: Task Status Completed

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

Prepare Active Directory for your Lync Server Installation. ploy > Active Directory Preparation Step 1: Prepare Schema Run once per deployment. Extends the schema for Lync Server. Prerequisites > Help > Step 2: Verify Replication of Schema Partition Manual Verify that the schema partition has been replicated before preparing the forest. Help > Step 3: Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components. Prerequisites > Help > Step 4: Verify Replication of Global Catalog Manual Verify that settings in the global catalog have been replicated before preparing a domain. Help > Step 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help > Step 6: Verify Replication in the Domain Manual Verify that the domain has finished replicating ACEs before deploying Lync Server machines.		erver 2010 - Deployment Wizard Prepare Active Directory for Lync Server		
Blay > Active Directory Preparation Step 1: Prepare Schema Run once per deployment. Extends the schema for Lync Server. Prerequisites > Help > Step 2: Verify Replication of Schema Partition Hanual Verify that the schema partition has been replicated before preparing the forest. Help > Step 3: Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components. Help > Step 4: Verify Replication of Global Catalog Hanual Verify that settings in the global catalog have been replicated before preparing a domain. Help > Step 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help > Step 6: Verify Replication in the Domain	14			
Sitep 1: Prepare Schema Run once per deployment. Extends the schema for Lync Server. Prerequisites > Help > ✓ Complete Run Sitep 2: Verify Replication of Schema Partition Nanual Verify that the schema partition has been replicated before preparing the forest. Help > ✓ Complete Run Sitep 3: Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components. Prerequisites > Help > ✓ Complete Run Sitep 4: Verify Replication of Global Catalog Hanual Verify that settings in the global catalog have been replicated before preparing a domain. Help > Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help > Sitep 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help > Sitep 6: Verify Replication in the Domain	20	unne menn burbure unerer surgerer ben bue en un untererer u		
Run once per deployment. Extends the schema for Lync Server. Prerequisites > Help > Step 2: Verify Replication of Schema Partition famual Verify that the schema partition has been replicated before preparing the forest. Help > Step 3: Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components. Prerequisites > Help • Step 4: Verify Replication of Global Catalog Manual Verify that settings in the global catalog have been replicated before preparing a domain. Help • Step 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help • Step 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help • Run	ploy > /	Active Directory Preparation		
Prerequisites >	tep 1:	Prepare Schema		
Help → ✓ Complete Run Step 2: Verify Replication of Schema Partition Nanual Verify that the schema partition has been replicated before preparing the forest. Help → Step 3: Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components. Prerequisites > Help > Step 4: Verify Replication of Global Catalog Nanual Verify that settings in the global catalog have been replicated before preparing a domain. Help > Step 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help > Step 6: Verify Replication in the Domain		Run once per deployment. Extends the schema for Lync Server.		
Atep 2: Verify Replication of Schema Partition Ianual Verify that the schema partition has been replicated before preparing the forest. Help > Help > Atep 3: Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components. Prerequisites > Image: Complete in the global catalog Ianual Verify Replication of Global Catalog Ianual Verify that settings in the global catalog have been replicated before preparing a domain. Help > Image: Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help > Run once per Lync Server user or server domain. Run Atep 6: Verify Replication in the Domain				
Ianual Verify that the schema partition has been replicated before preparing the forest. Help → tep 3: Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components. Prerequisites → ✓ Complete Help → ✓ Complete Run Verify Replication of Global Catalog Ianual Verify that settings in the global catalog have been replicated before preparing a domain. Help → tep 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites → Run Help → Run		Help • Comple	te Run	
Ianual Verify that the schema partition has been replicated before preparing the forest. Help → tep 3: Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components. Prerequisites → ✓ Complete Help → ✓ Complete Run Verify Replication of Global Catalog Ianual Verify that settings in the global catalog have been replicated before preparing a domain. Help → tep 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites → Run Help → Run	tep 2:	Verify Replication of Schema Partition		
tep 3: Prepare Current Forest Run once per deployment. Creates global settings and universal groups for Lync Server server components. Prerequisites • Help • tep 4: Verify Replication of Global Catalog Ianual Verify that settings in the global catalog have been replicated before preparing a domain. Help • tep 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites • Help • Run Run Run Etc 6: Verify Replication in the Domain				
Run once per deployment. Creates global settings and universal groups for Lync Server server components. Prerequisites > Help > Werify Replication of Global Catalog Ianual Verify Replication of Global Catalog have been replicated before preparing a domain. Help > Help		Help •		
Prerequisites → ✓ Complete Run Help → ✓ Complete Run tep 4: Verify Replication of Global Catalog Image: Complete Run Help → Image: Complete Run tep 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites → Run Help → Run	tep 3:		its.	
Itep 4: Verify Replication of Global Catalog Ianual Verify that settings in the global catalog have been replicated before preparing a domain. Help > Itep 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help > Help > Run				
tanual Verify that settings in the global catalog have been replicated before preparing a domain. Help > Step 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help > Step 6: Verify Replication in the Domain		Help • Completion	te Run	
Step 5: Prepare Current Domain Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help > Run				
Run once per Lync Server user or server domain. Sets access control entries (ACEs) for Lync Server universal groups. Prerequisites > Help > Run		Help •		
Help Run	tep 5:		ersal groups.	
tep 6: Verify Replication in the Domain		Prerequisites +		
		Help •	Run	
Ianual Verify that the domain has finished replicating ACEs before deploying Lync Server machines.				
	lanual	Verify that the domain has finished replicating ACEs before deploying Lync Server machines.		
Back Ex			Back	Exit

Figure 34: Prepare Current Forest Completed

18. On the Prepare Domain window, click Next.

👩 Prepare Domain	×
Prepare Domain	
Run once per Lync Server user domain or server domain to set universal groups	t access control entries (ACEs) for Lync Server
Help	Back Next Cancel

Figure 35: Prepare Domain Window

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

Executing Commands Prepare Domain Enable-CSAdDomain -Verbose -Confirm:\$false -Report "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp \Enable-CSAdDomain-[2011_02_28][16_31_38].html" Creating new log file "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp \Enable-CSAdDomain-c98e2832-607f-420b-b528-3d8a5daa4ea5.xml". Enable an Active Directory domain to host Lync Server 2010 deployments. Creating new log file "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain-[2011_02_28][16_31_38].html". Enable an Active Directory domain to host Lync Server 2010 deployments. Creating new log file "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain-[2011_02_28][16_31_38].html". Enable-CSAdDomain" processing has completed successfully. Detailed results can be found at "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain-[2011_02_28][16_31_38].html".	Prepare Domain	
Enable-CSAdDomain -Verbose -Confirm:\$false -Report "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp \Enable-CSAdDomain-[2011_02_28][16_31_38].html" Creating new log file "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain- c98e2832-607f-420b-b528-3d8a5daa4ea5.xml". Enable an Active Directory domain to host Lync Server 2010 deployments. Creating new log file "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain- [2011_02_28][16_31_38].html". "Enable-CSAdDomain" processing has completed successfully. Detailed results can be found at "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain-	Executing Comma	ands
\Enable-CSAdDomain-[2011_02_28][16_31_38].html" Creating new log file "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain- c98e2832-607F-420b-b528-3d8a5daa4ea5.xml". Enable an Active Directory domain to host Lync Server 2010 deployments. Creating new log file "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain- [2011_02_28][16_31_38].html". "Enable-CSAdDomain" processing has completed successfully. Detailed results can be found at "C:\Users\Administrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain-	> Prepare Domain	
	\Enable-CSAdDomain-[2011_02_28][1 Creating new log file "C:\Users\Admin c98e2832-607f-420b-b528-3d8a5daa4 Enable an Active Directory domain to I Creating new log file "C:\Users\Admin [2011_02_28][16_31_38].html". "Enable-CSAdDomain" processing has Detailed results can be found at "C:\U	I6_31_38].html" istrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain- tea5.xml". host Lync Server 2010 deployments. istrator. LYNCDC0\AppData\Local\Temp\Enable-CSAdDomain- completed successfully.
Prepare Domain View Log	Prepare Domain	▼ View Log

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.

CUniversalReadOnlyAdmins Properties			
ieneral	Members	Member Of Ma	naged By UNIX Attributes
Member	'S:		
Name			Active Directory Domain Services Fc
& RT	CSBAUniv	ersalServices	LyncDCO.lab/Users
SRT 8	CUniversal	SBATechnicians	LyncDCO.lab/Users
St. BT	CUniversal	UserAdmins	LyncDCO.lab/Users
0.00			
I			
I			

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.

Select this object type:	
Users, Service Accounts, Groups, or Other objects	Object Types
From this location:	
LyncDCO.lab	Locations
	Check Names
Enter the object names to select (<u>examples)</u> : Administrator	Check Names

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

- 8. On the RtcUniversalReadOnlyAdmins Properties page, click 0K.
- 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.

CSAdmini	strator Pro	operties			? ×
General	Members	Member Of	Managed I	By	
Membe	rs:				
Name		Active Dir	ectory Doma	ain Services Fold	er
Ad	d	Remove	1		
	<u> </u>	Helliove	J		
			ОК	Cancel	Apply

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.

Select this object type:	
Users, Service Accounts, Groups, or Other objects	Object Types.
From this location:	
LyncDC0.lab	Locations
Enter the object names to select (<u>examples</u>):	
Administrator	Check Nam
Administratod	Check Name

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.

S records with the

Figure 41: New Host Window

- 6. On confirmation that the host record was created, click 0K.
- 7. In the console tree, right-click the your domain and then select 0ther New Records.

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

Resource Record Type	X
Select a resource record type:	
Pointer (PTR) Public Key (KEY)	-
Renamed Mailbox (MR) Responsible Person (RP) Route Through (RT)	_
Service Location (SRV)	-
Description:	
Service (SRV) record. Allows administrators to use several servers for a single DNS domain, to easily move a TCP/IP service from one host to another host with administration, and to designate some service provider hosts as primary servers for a service and other hosts as backups. DNS clients that use a SRV-type query ask for a specific TCP/IP service and protocol mapped to a specific DNS domain and receive the names of any available servers. (RFC 2052)	*
	-
Create Record Cancel	

Figure 42: Resource Record Type Window

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

w Resource Red	ora			
ervice Location (S	SRV)			
Domain:	LyncDCO,lab			
Service:	_sipinternaltls			-
Protocol:	_tcp			•
Priority:	0			
Weight:	0			
Port number:	5061			
Host offering this	; service;			
dcolync1.LyncD	CO.lab			
Allow any aut name. This se	henticated user to u atting applies only to	pdate all DNS reco	DNS records w ords for a new	vith the same name.
		-	Cancel	Help

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.

ettings	
Share name	
SharedFold	ler 🗾
Add	Remove
Limit the nur	mber of simultaneous users to: 16777;
Limit the nur Comments:	mber of simultaneous users to: 167776
	mber of simultaneous users to: 16777;

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

- 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.

Create New Topology		×
Define the primary doma	in	
Identify the primary SIP domain for your organization	n, for example, contoso.com.	
LyncDCO.lab		
	Back Next	Cancel
	Tory Weyr	Cancer

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.

	eployment must have using the New Site w	at least one site. If your o vizard.	leployment has multiple	e sites, you can add the	other ones
Name: *		n 13 n 25.			
DCO_si					
Descript	ion:				

Figure 46: Define the First Site Name

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

Create No	ew Topology			×
:	Specify site details			
Provide	additional location details for your site.			
City:				
Daly	City			
	rovince:			
CA				
Country	/Region Code:			
USA				
Hel	p	Back	Next	Cancel

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.

Create New	v Topology	×
: :	New topology was successfully defined	
least one	successfully completed the New Topology wizard. Before you publish the topology, you must define at Front End pool. If you are ready to do that now, select the check box below, and then click Finish. The New Front End Wizard when this wizard closes	
To close	the wizard, click Finish. Back Finish Cancel	

Figure 48: New Topology was Successfully Defined Window

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

Define New Front End Pool	×
Define the New Front End pool	
This wizard helps you to create and configure a Front End pool for your site.	
Before you begin, ensure that you have the following information:	
 Do you plan to use the Front End pool for conferencing and/or voice? How much scalability will you need now or in the future? What is the FQDN for the pool and for each computer in the pool? If you are using conferencing, what is the external web address? 	
When you are ready to proceed, click Next.	
Help Back Next Cancel	

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.

efine New Fro	nt End Pool	AND			×
D	efine the Front	End pool FQDN			
You may depl	oy your Front End Serve	r as either an Enterprise E	dition pool or a Sta	ndard Edition serv	ver.
Pool FQDN: *					
pool01.Lync	DCO.lab				
An Enterp require lo applicatio	ad balancing and/or high n store for this pool mus Edition Server	ool can contain as many as n availability. The SQL Ser t be on a server or pool th	rver instance that h hat is running Micro	osts the user store soft SQL Server.	e and the
The SQL S	Server instance that host	gle computer for smaller d ts the user store and the a s Edition, which is automat	pplication store for		
Help			Back	Next	Cancel

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.

Define the computers in the	is pool.	
efine the computers that make up the pool. At least or llowed.	e computer is required, and as many as 10 comput	ters are
omputer FQDN: * dcolync1.LyncDCO.lab	Add	
dcolync1.LyncDCO.lab	Update	
	Remove	

Figure 51: Define the Computers in this Pool Page

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

Define Nev	v Front End Pool	×
	Select features	
	nessaging and presence are always enabled. Select the additional features that you would like this Fro I to handle.	nt
Confi	erencing, which includes audio, video, and application sharing.	
	Dial-in (PSTN) conferencing	
Enter	rprise Voice	
	Admission Control	
	Admission Control is an optional component that manages the bandwidth used by unified communication ic within the deployment. Only one Front End pool per site can enable Call Admission Control.	ns
Help	Back Next Cance	
Help	Back Next Cance	

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/th read/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.

Define Nev	w Front End Pool	x
	Select collocated server roles	
fewer co provide	Conferencing Service and Mediation Server can be collocated on a Front End pool. Collocation requires imputers, but in larger deployments a standalone A/V Conferencing pool and/or Mediation Server pool can better voice quality and greater scalability. For a Standard Edition Front End Server, the A/V Conferencing s always collocated.	
Select w	hich server roles and services you would like to collocate on this Front End pool.	
Colle	cate A/V Conferencing service.	
	recommend collocation if you plan to home fewer than 10,000 users on this pool and A/V conferencing is mission-critical.	
Colle	ocate Mediation Server	
	can collocate the Mediation Server on the Front End Server if your PSTN media gateway or your IP-PBX ports media bypass and if Enterprise Voice is not mission-critical for your organization.	
Help	Back Next Cancel	

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.

Define Ne	w Front End Pool	×
	Associate server roles with this Front End pool	
	satures are carried out by other server roles. You can enable those features by associating them with the ad pool that you are creating now.	
Select t	he servers and features that you would like to associate with this Front End pool:	
Enal	ble archiving.	
Ena	ble monitoring (call detail recording and logging of quality of experience metrics).	
🗖 Ena	ble an Edge pool to be used by the media component of this Front End pool.	
Help	Back Next Cancel	

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.

Defin	e New Front End Pool	×
	Define the SQL store	
Poo	ol, the SQL Server instance cannot be collocated on rver must be installed, and the SQL instance must be	store user information. For this Enterprise Edition Front End the pool; it must be on a single-server pool. Note: SQL e created before installation.
6	Use a previously defined SQL store.	-
c	Define a new SQL store. SQL Server FQDN: *	
	dcolync1.LyncDCO.lab	
	SQL Instance:	
	C Named Instance	
	Default	
	Default Instance	
	Help	Back Next Cancel

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.

Jenne ne	r Front End Pool	×
	Define the file share	
Server, t manually	existing file share, or define a new one, to be used by the server. For this Standard Edition Front End the file share can be collocated, or it can be on another single-server pool. The file share must be created before you can install it. previously defined file share.	
	<u>ت</u>	
	e a new file share. erver FQDN: *	
dco	ync1.LyncDCO.lab	
File	hare: •	
Sha	edFolder	1
Defir File dcc File	e a new file share. erver FQDN: * ync1.LyncDCO.lab hare: *	

Figure 56: Define the File Share Page

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

efine New Front	End Pool				×
. Spe	cify the Web Se	rvices URL			
	an alternate FQDN for the e nal FQDN is fixed.	external side of the We	b Services. For a	Standard Edition	Front End
C Override inte	rnal Web Services pool FQI	DN			
Internal Base	URL:				
pool01.Lync	DCO.lab				
External Base UR	L: •				
pool01.LyncDCO	.lab				
-					
Help			Back	Finish	Cancel
, nonp				- mager	Control

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.

💑 Lync Server 2010, Topology Builder				_ 🗆 ×
File Action View Help				
🗢 🔿 🔲 🛛 🖻				
Lync Server 2010	SIP domain			Actions
DCO_site DCO_site Standard Edition Front End Servers	SIP domain			Lync Server 2010 🔺
Contract Contract Contract Contract Contract Contract Contrect Contract Con	Default SIP domain: Additional supported SIP domains: Simple URLs	LyncDCO.lab Not configured	•	Image: New Central Ste Edit Properties New Topology Open Topology Download Topology
The stores Wedshot I. LyncDCO. Jab \SharedFolder Mediation pools FIN gateways Monitoring Servers E Archiving Servers E Edge pools E Edge pools Trusted application servers	Phone access URLs: Meeting URLs:	Active Simple URL https://dialin.LyncDCO.lab Active Simple URL https://meet.LyncDCO.lab	SIP do	Save a copy of Topology As Publish Topology Install Database Merge 2007 or 2007 R2 Topol Remove Deployment
🗷 🦳 Branch sites	Administrative access URL:	Not configured		View
	Central Management Ser	ver	<u> </u>	
	Central Management Server:	pool01.LyncDCO.lab (DCO_site)		

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.

domain	Simple URLs		
ple URLs			1020 02
ntral Management rver	Simple URLs will be sent to your users and use numbers, meetings, and administration. The ac Other URLs are used to support any meetings and Phone access Simple URLs are required an Phone access URL after it has been published v order to change the active URL, you should cree inactive URL can be removed after all conferen Phone access URLs:	trive URL is the one that is used when new me that have been scheduled in the past by using d must be full URLs, including https://. Chang will prevent users from joining existing meeting rate a new active URL and leave the current UR	etings are scheduled. those URLs. Meeting ing a Meeting or is or conferences. In RL inactive. An
	Simple URL		
	https://dialin.LyncDCO.lab		Add
			Remove
	1	Make Active Edit UR	
	Meeting URLs:	Make Active Edit UR	
	Meeting URLs:		
	Simple URL	SIP domain	
	Simple URL	SIP domain	
	Simple URL	SIP domain	Add
	Simple URL	SIP domain LyncDCO.lab	Add
	Simple URL	SIP domain LyncDCO.lab	Add
	Simple URL https://meet.LyncDCO.lab	SIP domain LyncDCO.lab	Add
	Simple URL https://meet.LyncDCO.lab	SIP domain LyncDCO.lab	Add
	Simple URL https://meet.LyncDCO.lab	SIP domain LyncDCO.lab	Add

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.

Publish Topology			×
Publish the topology			
In order for Lync Server 2010 to correctly route messages i Before you publish the topology, ensure that the following to A validation check on the root node did not return any A file share has been created for all file stores that you All simple URLs have been defined. For Enterprise Edition Front End pools and for Monitor installed and accessible remotely; firewall exceptions f For a single Standard Edition server: The task "Prepar You are currently logged on as a SQL administrator, fo If you are removing a Front End pool, all users, comm objects, and conference directories have been remove When you are ready to proceed, click Next. Help	tasks have been completed or errors. u have configured in this to ing Servers and Archiving S or remote access to SQL S e first Standard Edition ser or example, as a member o on area phones, analog de	: pology. Servers: All SQL stores are erver are configured. ver" was run. f the SQL sysadmin role.	

Figure 60: Publish Topology Window

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

re	ate databases				
eate Iblis eate	ed. If you have the appropr	iate permissions not have the app	ur topology. Some of the data on the SQL Server, you can o propriate permissions, someo	create the databas	es when you
	Store FQDN	Site			
~	dcolync1.LyncDCO.lab	DCO_site			
			an be installed from here. Da installed by running local se		

Figure 61: Create Databases Page

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

Select Central M	lanagement Serve	er			
Only one Front End pool in	n the deployment can have a	Central Management	Store, All	pools will us	se the same store
			Store, All	pools will u	se the same store
Select the Front End pool	n the deployment can have a that will host the Central Mar DCO_site		Store, All	pools will u	se the same store
	that will host the Central Mar		Store. All	pools will u	se the same store

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.

rour	topology was successfully published.			_
2	Step	Status		
1	Creating Central Management Store	Success		View Logs
~	Setting Central Management Store location	Success		
1	Publishing topology	Success		
√.	Downloading topology	Success		-
√.	Updating global simple URL settings	Success		
Υ.	Publishing global simple URL settings	Success	-	
•	steps: Click here to open to-do list In order for Lync Server 2010 to correctly route The linked text file contains a list of any servers to be created. ose the wizard, 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.

Lync Server 2010 Welcome to Lync Server deployment.	
hadress Long Screen 2010	
Deploy > Lync Server 2010	2
Step 1: Install Local Configuration Store Installs local configuration store and populates with data from Central Management Store.	
Prerequisites >	
Help • Run	
Step 2: Setup or Remove Lync Server Components Install and activate, or deactivate and uninstall Lync Server Components based on the topology definition. Not Available: Local configuration store not available.	
Prerequisites +	
Help +	
Step 3: Request, Install or Assign Certificates This step starts the Certificate Wizard. Create certificate request for local system. Install, and assign certificates for thi system based on the topology definition. Not Available: Local configuration store not available.	•
Prerequisites +	_
Help • Run	0.
Step 4: Start Services Initiates a start request for all Lync Server services. Note: This step does not verify that the services have actually started. To do so, launch the Services MMC tool through "Service Status" step in the Deployment UI.	the
Not Available: Local configuration store not available.	
Prerequisites +	-
Help • Run	1
Back	Exit

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.

Setup Lync	Server compo	onents				×
E E	xecuting (Commands				
Checking pr Checking pr Checking pr Checking pr Checking pr Checking pr Checking pr Checking pr	rerequisite Suppor rerequisite IISp rerequisite IIS7Fe rerequisite SqlExp rerequisite VCred rerequisite SqlBa rerequisite SqlBa rerequisite Ucmal	rsneil2prerequisite sa prtedServerOSprerequ prerequisite satisfied. eaturesprerequisite sa pressRtcLocalprerequi listprerequisite satisfie tiveClientprerequisite ckcompatprerequisite Redistprerequisite sati eModuleinstallingsi	isite satisfied. atisfied. isite satisfied. ed. satisfied. satisfied. isfied.			*
Checking pr Checking pr The server has restarte	rerequisite Wmf2 rerequisite Wmf2 must be restarter ed, start the Depl	008prerequisite satisf 008prerequisite satisf 008R2installingfailu d before installation car loyment Wizard and cor	fied. Ire code 3010 1 continue. To		tallation after the	e server
Bootstrap lo	cal machine					<u>V</u> iew Log
Help]			<u>B</u> ack	<u>F</u> inish	Cancel

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.

ault certificate Unassigned Assign Remov	Certificate	Status	Friendly Name	Expiration Date	Reque
	Default certificate	Unassigned			Assig
View					Remo
					View

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

Select a certification authority to process your request. The Certificates Wizard will automatically import the selected CA's certificate chain if necessary.	E	Certificate Request	-
selected CA's certificate chain if necessary. Select a CA from the list detected in your environment LyncDCO-DCOLYNC1-CA	L	Choose a Certification Authority (CA)	
	90	elected CA's certificate chain if necessary. Select a CA from the list detected in your environment	
	C		

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.

🗟 Certific	ate Request					×
¢	Name a	nd Security	Settings			
Type a n	ame for the nev	certificate. The n	ame should be easy	for you to refer to ar	d remember.	
					e determined automa	tically
		usages on this ma				
Friendly	Name:					
Lync Po	ool1 Cert					
Bit lengt	h:					
2048		•				
-						
I Mark	the certificates	private key as exp	ortable			
Help				Back	<u>N</u> ext C	ancel

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.

🎖 Certificate Request	<u>×</u>
Subject Name / Subject Alternate Na	mes
The following will be automatically populated for the Subject Name and Subject Name:	Subject Alternate Name (SAN)
pool1/ynedco.lab	
Subject Alternate Name:	
pool1 lynodoo.lab dialin.lynodoo.lab admin.lynodoo.lab	
Help E	ack Next Cancel

Figure 71: Subject Name / Subject Alternate Names Page

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

Certificate Request			×
SIP Do	main setting on Su	bject Alternate N	ames (SANs)
domain: • Your deployment use • Your deployment per	s automatic sign-in without DN forms strict domain matching udes devices that run Lync Pho	S SRV configuration	I SANs for each configured SIP
LyncDCO.lab	-		
Select one or more SIP	domains for which a sip. <sipdo< td=""><td>omain> entry is to be added</td><th>to the SAN list.</th></sipdo<>	omain> entry is to be added	to the SAN list.
Help		Back	Next Cancel
			······································

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.

ertificate Requ	est		
<u> </u>	ficate Request Summary		
Property	value	lext	
Certificate Use	Server default,Web services internal,Web services external		
Country/Region State/Province City/Locality	internal, web services external		
Friendly Name Key Size	Lync Pool1 Cert 2048		-
Exportable Organization Organizational Unit	False		
Subject Name	LyncDCO.lab		

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.

Property	ing certificate to the Lync Server usages lis	NOUY SINCK HEAL	
Friendly Name	Lync Pool1 Cert		
Thumbprint	B813CEC61B63348A0E44A1BD00DAC 51AFE6F74C6		
Contribution I los	Server default, Web services		
Certificate Use	internal,Web services external		
Issue date Expiration date	10/1/201110:31:03 PM 9/30/2013 10:31:03 PM		
Subject Name (SN)	pool1.LyncDCO.lab		
Subject Alternate Names (SANs)	sip. LyncDCO.lab		
Names (SANS)	pool1.LyncDCO.lab		
	dial LyncDCO.lab		

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.

Status	Friendly Name	Expiration Date	Request
Assigned	Lync Pool1 Cert	9/30/2013 10:31:03 PM	Aurice
Assigned	Lync Pool1 Cert	9/30/2013 10:31:03 PM	Assign
Assigned	Lync Pool1 Cert	9/30/2013 10:31:03 PM	Remove
Assigned	Lync Pool1 Cert	9/30/2013 10:31:03 PM	100000
			View
	Assigned Assigned Assigned	Assigned Lync Pool1 Cert Assigned Lync Pool1 Cert Assigned Lync Pool1 Cert	Assigned Lync Pool1 Cert 9/30/2013 10:31:03 PM Assigned Lync Pool1 Cert 9/30/2013 10:31:03 PM Assigned Lync Pool1 Cert 9/30/2013 10:31:03 PM

Figure 75: Certificate Wizard Window

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.

Vladimir Nabokov Properties ? >							
Dial-in Environment Sessions Remote control Remote Desktop Services Profile Personal Virtual Desktop COM+ General Address Account Profile Telephones Organization Member Of							
User logon name: vnabokov @companya.com User logon name (pre-Windows 2000): COMPANYA\ vnabokov Log On Hours Log On Io Unlock account							
Account options:							
OK Cancel Apply Help							

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

- 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.

Select URL	to connect Lync Server Control Pane
https://pool01.lyr	ncdco.lab/Cscp

Figure 77: Select URL Window

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

I Home 22 Users 23 Users 24 Topology 25 Topology 26 Noice Routing 27 Nonce Routing 28 Response Groups 29 Conferencing 21 Conferencing 22 Cients 23 Response Groups 24 Conferencing 25 Conferencing 26 Colients 27 Conternoing 28 Response Groups 29 Conferencing 20 Conferencing 21 View Monitoring Server reports 22 Restormang 23 Response Groups 24 View Monitoring Server reports 25 Cocmunity 26 Counce and Archiving	ator Sign ou 4.0.7577.
Image: Second secon	
Image: Section 2 Intervention 2 Intervention 2 Image: Section 2 Intervention 2 Intervention 2 Image: Section 2 Voice Reatures Intervention 2 Image: Section 2 Image: Section 2 Intervention 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Section 2 Image: Sec	
 View your roles View your roles Vice Routing Vice Routing Vice Features Response Groups Conferencing Conferencing Clients External User Access Monitoring 	
 Voice Routing Voice Features Response Groups Conferencing Conferencing Clients External User Access Monitoring 	
Voice Features Top Actions Image: Second	
Response Groups Conferencing Downloadable Documentation Documentation Online Documentation on TechNet Library Uiew topology status View topology status View Monitoring Server reports Community Forums Blogs	
Conferencing C	
Clients Lync Server Management Shell Script Library Lync Server Management Shell Script Library Lync Server Resource Kit Tools Community Forums Blogs	
External User Access Monitoring	
Access Forums Blogs	
in the second seco	
A Security	
Network Configuration	

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.

R	Microsoft*	Admini	strator Sign o				
E.	Lync Server 2010		4.0.757				
	Home	User Search					
22	Users	Î					
ĸ	Topology	• Search DDAP search					
Ð	IM and Presence	Search for users by typing a user's name or clicking Add filter Find 🛱 🔒 + Add filter	*				
3	Voice Routing	🏽 Enable users 🔻 🥖 Edit 🔻 Action 🔻	0				
6	Voice Features	Display name A Enabled SIP address Registrar pool Telephony					
12	Response Groups						
Þ	Conferencing	Select the type of search that you want to perform.					
	Clients	IMPORTANT: Search returns users already enabled for Lync Server, but					
1	External User Access	does not include users enabled for previous versions. To see these users, select Legacy users in the search filter query.					
	Monitoring and Archiving						
0	Security						
ę	Network Configuration						

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.

Edit Lync Server User - LyncKW1

lay name:			
:KW1			
nabled for Lync Server			
sip:LyncKW1	@	LyncDCO.lab	•
Registrar pool:			
pool01.LyncDCO.lab			
elephony:			

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.

	Home	Dial Plan	Voice Policy	Route	PSTN Usage	Trunk Configuration	Test Voice Rout
33	Users	Create					
×	Topology						
Ş	IM and Presence	Edit D	Dial Plan - Glob	al			
ષ્ટ	Voice Routing	√	OK X Cance	el			
2	Voice Features	Nar	ne:*				
23	Response Groups	Glo					
Þ	Conferencing	Sim					
	Clients	Des					
許	External User Access						
	Monitoring	Dia	-in conferencing	region:			
	and Archiving	che	ennai				?
	Security	Exte	ernal access prefi	х:			?



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.

Associated Normalization Rules New Copy Paste Select... Show details... Remove Image: Copy Normalization rule State Pattern to match Extension Dialing 10xx Committed ^(10\d(2))\$ Extension Dialing 60xx Committed ^(60\d(2))\$ Custom Prefix All Committed \+?[\s0\-\./]*1?[\s0\\-\./]*\(?\s*([2-9]\d\d)\s*\)?[\s()\-\./]*



		010	Dial Plan	Voice Policy R	oute	PSTN Usage	Trunk Configura	ation Test Voice Routing	4.0.75
_	Home	-		pice routing test ca		-			*
12	Users		Create v	bice routing test ca	ise inforr	nation			~
X	Topology		[م	
	IM and Presence								
8	Voice Routing			🥖 Edit 🔻 👚 N	love up	-	wn Action T		
6	Voice Features		Local			State Committed	PSTN usage	Pattern to match	
\$	Response Groups		CCRo			Committed	Local	^(\+1999[0-9]{7})\$	
\$	Conferencing			alRoute		Committed	Internal	^(\+1865[0-9](7))\$	
3	Clients		GWR			Committed	Local	^(\+1650[0-9]{7})\$	
\$	External User Access		01114			committee	2000	((
_	Monitoring								
	and Archiving	4							
	Security								
P	Network								
	Configuration								

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

Microsoft'		Administrator S
Lync Server 2010		4.0
Home	Dial Plan Voice Policy Route PSTN Usage Trunk Configuration Test Voice Routing	
Users	Create voice routing test case information	
Topology		
IM and Presence	Edit Voice Route - CCRoute	
		0
Voice Routing	Name:*	-
Voice Features	CCRoute	
Response Groups	Description:	
Conferencing		
Clients	Build a Pattern to Match	
External User	Add the starting digits that you want this route to handle, or create	
Access	the expression manually by clicking Edit.	
Monitoring	Starting digits for numbers that you want to allow:	
and Archiving	Type a valid number and then click Add.	
Security	+1999[0-9](7) Exceptions	
Network	Remove	
Configuration		
	Match this pattern:*	
	^(\+1999[0-9](7))\$	
	Edit Reset 🧭	
	Suppress caller ID Alternate caller ID:	
	Associated gateways: PstnGateway:192.168.10.199 Add	
	Remove	
	Associated PSTN Usages	
	Select Remove 👚 🥾	
	PSTN usage record Associated voice policies	
	Local 💮 Global	
	Translated number to test:	
	Go	
		•

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

- 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.

Kunc Server 2010, Topology Builder	
File Action View Help	
🗢 🔿 🙍 🖬 🛛 🖬	
 Lync Server 2010 DCO_site Standard Edition Front End Servers Enterprise Edition Front End pools Director pools A/V Conferencing pools SQL stores File stores Mediation pools dcolync7.LyncDCO.lab PSTN gateways 	The properties for this item
Define New IP/PSTN Gateway	×
Gateway FQDN or IP Address * dcolync8.LyncDCO.lab	8
Listening port for IP/PSTN gateway: *	
Sip Transport Protocol: • : TCP • : TLS	
Help	OK Cancel

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.

File Action Weth Help Ceneral Next hop PSTM gateway PSTM gateway PSTM gateway PSTM gateway Next hop selection Selection Selection Selection Next. Selection Next. Selection Next. Next. Next. Next. Next. Next. Next.	Lync Server 2010, Topology Bu	Edit Properties	×
	Constant Server 2010 File Action View Help Constant Server 2010 Constant Server 2010 Constant Edition Front End Decost Server 2010 Constant Edition Front End Decost Server 2010 Constant Server 2010 Constan	General Next hop PSTN gateway Next hop selection Next hop pool: pool011.jvncDCO.lab Pool011.jvncDCO.lab Mediation Server PSTN gateway Listening ports: * TLS: 5067 TCP: 5068 Image: Server PSTN gateway Image: Server	×
Help OK Cancel		Make Default	•

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

- 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.

File Action View Help	
🗢 🔿 🖄 🖬 🛛 🖬	Define New Trusted Application Pool
Upto Server 2010 DCO_site Standard Edition Front End Servers Enterprise Edition Front End pools Comparison Fr	
Director pools Director pools Director pools Director pools Director pools Directores Directores Directores	Define the fully qualified domain name (FQDN) for the Trusted Applications pool, and indicate whether the pool will be single-server or multiple-server. Important: A single-server pool cannot be converted later to a multiple-server pool.
 Imediation pools PSTN gateways Imediation pools Imediation pools	FQDN: * dcolync-cme.lyncdco.lab
 Edge pools Trusted application servers Branch sites 	Multiple computer pool Select this option if you want this pool to support load balancing and high availability. Single computer pool
	Select this option if you have a small deployment and you do not need load balancing or high availability.
	Help Back Next Cancel

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.



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, page 87
- Generate Server Certificate, page 89

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.
- 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)
- Place this file in a logical location. For example: <ucc_root>\etc\CompanyA_Store.jks

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 0k.
- 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

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)
- 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





Chapter



Genesys Component Configuration for Lync Interoperability

This chapter contains the following sections:

- SIP Server Configuration Tasks, page 94
- UC Connector Configuration Tasks, page 99
- Interaction Workspace Plug-in for Lync, page 102
- Current Limitations, page 104

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

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.

Task Summary: Configuring SIP Server

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.

	Lync_55 - \Switches\Switch_Lync_1\DNs\				
×	Cancel 🚽 Save & Close 🚽 Save	s 🛃 Save 🕄	& New 🛛 🛃 Reload		
C	onfiguration Options		Permissions	Dependencies	
	New 🙀 Delete ځ Export 주 In	nport	View:	Advanced View (Annex)	
	Name 🔺	Section	Option	Value	
T	Filter	Filter	Filter	Filter	
∃ TServer (6 Items)					
	TServer/contact	TServer	contact	dcolync7:5068;transport=tcp	
	TServer/dual-dialog-enabled	TServer	dual-dialog-enabled	false	
	TServer/make-call-rfc3725-flow	TServer	make-call-rfc3725-flow	1	
	TServer/refer-enabled	TServer	refer-enabled	false	
	TServer/reuse-sdp-on-reinvite	TServer	reuse-sdp-on-reinvite	true	
	TServer/service-type	TServer	service-type	softswitch	

Figure 89: Configuration options for the soft switch DN

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:

Trunk_Mediation - \Switches\Switch_Lync_1\DNs\				
🔀 Cancel 🚽 Save & Close 🚽 Save	e 🛃 Save	& New 🛛 🔀 Reload		
Configuration Options		Permissions	Dependencies	
📰 New 🙀 Delete 💆 Export 🏹 In	nport	View: Advanc	ed View (Annex)	
Name 🔺	Section	Option	Value	
T Filter	Filter	Filter	Filter	
🗉 TServer (6 Items)				
TServer/contact	TServer	contact	dcolync7:5068;transport=tcp	
TServer/dual-dialog-enabled	TServer	dual-dialog-enabled	false	
TServer/make-call-rfc3725-flow	TServer	make-call-rfc3725-flow	1	
TServer/prefix	TServer	prefix	+1415466	
TServer/refer-enabled	TServer	refer-enabled	false	
TServer/reuse-sdp-on-reinvite	TServer	reuse-sdp-on-reinvite	true	

Figure 90: Configuration options for the trunk DN

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:

MSML_VoIP_partition - \Switches\Switch_Lync_1\DNs\Outbound\				
Cancel 🚽 Save & Close 🚽 Save			boana (
Configuration Options		Permissions	Dependencies	
📄 New 🙀 Delete ځ Export 🐴 In	nport	View: Adv	anced View (Annex)	
Name 🔺	Section	Option	Value	
T				
🗉 TServer (8 Items)				
TServer/contact	TServer	contact	172.21.81.198:5060	
TServer/cpd-capability	TServer	cpd-capability	mediaserver	
TServer/make-call-rfc3725-flow	TServer	make-call-rfc3725-flow	/ 1	
TServer/prefix	TServer	prefix	msml=	
TServer/refer-enabled	TServer	refer-enabled	false	
TServer/ring-tone-on-make-call	TServer	ring-tone-on-make-call	false	
TServer/service-type	TServer	service-type	msml	
TServer/subscription-id	TServer	subscription-id	Lync	

Figure 91: DN configuration options

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:

Recorder_VoIP - \Switches\Switch_Lync_1\DNs\					
×	Cancel 🛃 Save & Clo	ise 🛃 Save 🛛	🚽 Save & New 🕴 🔀 🛛	Reload	
C	onfiguration	Options	Permission	s	Dependencies
New 🙀 Delete 💆 Export 🚡 Import View: Advanced View (Annex)					
	Name 🔺	Section	Option	Value	
T	Filter	Filter	Filter	Filter	
TServer (3 Items)					
	TServer/contact	TServer	contact	10.10.11.7:5	5070
	TServer/request-uri	TServer	request-uri	annc@10.10	0.11.7:5070;record=recording/call-
	TServer/service-type	TServer	service-type	recorder	

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.

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.

Task Summary: Configuring UC Connector

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 j ava 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 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
Start UC Connector with the following arguments in command line:
```

- Start OC Connector with the following arguine
- for j ava 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.

Customer1 - Interaction Workspace	
Case Information	
Origin: Inbound call to 1000 Queue: 1000	
	Accept Reject

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.

customer1 - External - Interaction Workspace _
customer1 🕥 (00:02:08)
Case Information
Origin: Inbound call to 1000 Queue: 1000
▼ customer1 🕥 Connected
G G G F F F III O F SF F
📲 Anonymous Caller 📃 🗖 🔀
Anonymous Caller Guest (Other)
IM Call - Video - 🖉 - 🕖 »
🖉 🐠 🏭 💷 - 🛛 1:55 📊 🕲 🏕 -

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?, page 108 Deploying Genesys Lync Agent, page 110 Using Genesys Lync Agent, page 116

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.
- Select Forest > Domains > <your domain> > Group Policy Objects and double-click Default Domain Policy.

🔜 Group Policy Management		_ 🗆 🗙
📓 File Action View Window Help		_ 8 ×
🗢 🔿 🙍 🖬 🛍 💢 🧟 👔		
Group Policy Management Forest: LyncDCO.lab □ Domains □ Default Domain Policy □ Domain Controllers □ Default Domain Controllers □ Default Domain Controllers □ Default Domain Controller: □ Default Domain Controller: □ Default Domain Policy □ Default Domain Policy □ Starter GPOs □ Sites □ Group Policy Modeling □ Group Policy Results	Default Domain Policy Scope Details Settings Delegation Links Display links in this location: LyncDC0.lab The following sites, domains, and OUs are linked to this GPO: Location Enforced Link Enabled Path Image: Location Enforced Link Enabled Path Path Path Image: LyncDC0.lab No Yes LyncDC0.lab Image: LyncDc0.lab No Yes LyncDc0.lab	

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

- 2. Select Startup.
- 3. On the Scripts tab, use the Add button to add the following

tartup Properties			? >		
Scripts PowerShell Scrip	pts				
Startup Scri	pts for Default Domai	n Policy			
Name	Parameters				
regedit.exe	/s 1.reg		Up		
			Down		
			Add		
			Edit		
			Remove		
,					
To view the script files stored in this Group Policy Object, press the button below. Show Files					
	OK	Cancel	Apply		

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.

Image: Second secon	yncDCO.lab)Policies1(3182F940-016D-11D2-	945F-00004F6984F9}{Ma Date modified 1/29/2013 11:00 AM	thinalScripts/Startup	Size KB	Search S
	·				8≡ ▼ (
Pavorites Powiloads Powiloads Powiloads Powiloads Documents Pictures Pictures Pictures Videos					
 ▶ Downloads ₩ Recent Places ▷ Libraries ▷ Documents → Music ► Pictures ▼ Videos 		1/29/2013 11:00 AM	Registration Entries	1 KB	
Local Disk (C:)					
I item					

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

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

🧾 Group Policy Management Editor										_ 🗆 ×
File Action View Help										
(~ ~) 2 📷 🤞 🖬 🗙 🗉 🗭 0	🗟 📝 📅 🗟 🔕 + 1	t 🖡								
Default Domain Policy [DCOLVNC2.LVNCDC0.L]	Constant of the second se	/	Host 1	L F	Action Replace Replace	Hive HKEY_LOCAL_MACHINE HKEY_LOCAL_MACHINE	Key SOFTWAREIGCTI\GenesysLyncAger& SOFTWAREIGCTI\GenesysLyncAgerR	Value Name Host Port	Type REG_EVEAND_SZ REG_DWORD	Valus Data Sbhanderi-PC 00001F90
	Preferences $\sqrt{\text{Extended}}$ Sta	andard /								
Last changed: 1/29/2013 11:55:56 AM			_		_				J	

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.



Configure—Opens GLA. Exit—Terminates GLA. About—Displays details about GLA.

	×
Genesys Lync Agent Version : 8.0.0.0 Contact : genesys support <support@genesyslab.com> Copyright © 2012 Genesys Telecommunications Laboratories, All Right Reserved.</support@genesyslab.com>	ts
	(

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.

	Genesys Lync Agent	
1. The "Edit" or "Save" button lets you modify and save the configuration	UC Connector Host Name: Sbhanderi-PC	6. Host name 7. Host port in use
	Edit Cancel Test Connection	 8. Test connection
2. Cancel changes and close to the system tray	Connected to server:	
3. Lync connection state	5. Status string	

4. Test connection progress

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.

😗 Use	🛞 User Account Control 🧮				
Do you want to allow the following program from an unknown publisher to make changes to this computer?					
	Program name: Publisher: File origin:	GenesysLyncAgent.exe Unknown Hard drive on this computer			
💌 s	how details	Yes No			
		Change when these notifications appear			

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.

🛞 User Account Control 🛛 💽			
Do you want to allow the following program from an unknown publisher to make changes to this computer?			
Program name: GenesysLyncAgent.exe Verified publisher: Unknown File origin: Hard drive on this computer			
To continue, type an administrator password, and then click Yes.			
User name Password Domain: LYNCDCO			
Show details			

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 <u>system level</u> <u>documents by release</u> 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 <u>http://docs.genesyslab.com/</u>.
- 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 <i>Genesys Migration</i> <i>Guide</i> for more information. Do <i>not</i> use this value for this option. A <i>customary and usual</i> practice is one that is widely accepted and used within a particular industry or profession. The formula, $x + 1 = 7$ where x stands for

Type Style	Used For	Examples
Monospace font (Looks like teletype or typewriter text)	 All programming identifiers and GUI elements. This convention includes: The <i>names</i> 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⟩

Table 4: Type Styles (Continued)



Index

Symbols

[] (square brackets).					2	2	. 128
< > (angle brackets)			2		÷		. 128

A

Active Directory	.45,49
Active Directory Certificate Services	
Active Directory Domain Services	17
Active Directory Users and Computers .	46
Administrative URL.	61
Agent Desktop Client.	108
angle brackets	128
audience, for document	7

В

brackets													
angle.				÷			÷				2		128
square	÷	÷	÷	÷			÷		÷	÷			128

С

CA
Central Data Store
Client certificate
client certificate
commenting on this document
contact
contact (Microsoft-OCS)
conventions
in document
type styles
cpd-capability
CTI

D

DN options	
contact)
cpd-capability	3
dual-dialog-enabled	7
make-call-rfc3725-flow	3
prefix	
refer-enabled	3
request-uri	
reuse-sdp-on-reinvite	
ring-tone-on-make-call	
service-type	
subscription-id	
DNS records	
_sipinternals SRV record	
internal A record	
document	
audience	7
change history	3
conventions	7
errors, commenting on	3
version number	
Domain Controller	2
dual-dialog-enabled	

Е

Early Media																		104	ł
-------------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	-----	---

F

font styles	
italic.	. 127
monospace	. 128
Forward Lookup Zones	
FQDN	

G

Genesys Agent Desktop	102
Genesys Interaction Workspace	12
Genesys Lync Agent	108
Genesys Lync Agent options	
gla-call-match-window.	111
gla-kpl-response-time	111
gla-kpl-time	111
invite-message	111

Н

heartbeat / keep alive			÷			. 118
high availability						. 109

Install Topology Builder
for Lync
italics

J

Java Development Kit					. 88, 102
Java keystore					102
JDK					. 88, 102
JKS					88

Κ

keystores	102
Java keystore	
pkcs12 keystore	
keytool.exe	88, 102

L

Lync 2010 desktop client	
Lync certificates	69
Lync Enterprise Voice	12
Lync file share	52
Lync Front End Server	D, 14, 65
Lync Mediation Server	, 11, 104
Lync Server 2010	47
Lync Server 2010 Control Panel	
Lync topology.	.52, 54
Lync Topology Builder	54
Lync users	75
LyncShare	

Μ

make-call-rfc3725-flow Microsoft Lync Client API						
MMC						
msml-support						

Ρ

permiss	sio	ns																		
Lync	ad	mi	nis	str	at	iv	е	ре	err	ni	ss	io	ns	5					. 4	47
Lync																				
Lync	se	tup) p	er	m	is	si	or	าร										. 4	45
pkcs12	ke	eys	to	re					2	1				1			ι.		1()2
prefix .																				
PSTN						2		1								1	0,	11	1,8	33

R

redundancy				109
refer-enabled				
registrar-uri (Microsoft-OCS).				
request-uri .`				99
reuse-sdp-on-reinvite				

S

server certificate
SIP Server options
msml-support
sip-enable-100rel
sip-enable-moh
sip-port-tls
sip-tls-cert
sip-enable-100rel
sip-enable-moh
sip-port-tls
sip-tls-cert
SQL Server 2008 SP1
square brackets
Stat Server
subscription-id

Т

TLS	۰.	۰.	۰.	۰.	۰.	۰.	۰.	۰.	۰.	۰.	۰.	۰.	۰.	۰.	. 87
Topology Builder.				۰.			۰.			5	52 ,	6	1,	63	3, <mark>65</mark>
type styles															
conventions	2	2				2			2				2	2	127

italic							. 12	27
monospace							. 12	28
typographical styles								

U

UAC	:						. 8
UC Connector opt contact (Microso registrar-uri (Mic	oft-C	CC					

V

Index