



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

UC Connector Genesys Lync Integration Deployment Guide

UC Connector 8.0.3

12/31/2021

Table of Contents

| | |
|--|-----------|
| UC Connector 8.0.3 Lync Integration Deployment Guide | 3 |
| Architecture | 5 |
| Lync / Skype for Business Call Flow and Components | 6 |
| Environment Information | 8 |
| Lync Enterprise Voice Integration | 9 |
| Lync Integration Overview | 10 |
| Supported Lync / Skype for Business Deployments | 12 |
| Task Flow | 16 |
| Deployment Prerequisites | 17 |
| Creating a New PSTN Gateway | 35 |
| Adding UCC as Trusted Host | 39 |
| Security Procedures | 40 |
| Configuration Options | 54 |
| UC Connector Application Options | 55 |
| SIP Server Configuration Options | 56 |
| Genesys Component Configuration for Lync Interoperability | 57 |
| SIP Server Configuration | 58 |
| UC Connector Configuration | 62 |
| Workspace Plugin for Skype for Business | 65 |
| Current Limitations | 66 |
| Genesys Lync Agent | 68 |

UC Connector 8.0.3 Lync Integration Deployment Guide

Welcome to the *UC Connector 8.0.3 Lync Integration Deployment Guide*. This document describes integrating the Unified Communications (UC) Connector with the Genesys Voice platform in conjunction with Microsoft Lync / Skype for Business, for voice and presence integration, based on SIP integration.

Note that Genesys also offers a "native" integration with Skype for Business and Lync 2013, which allows the use of additional media types - video and full-featured IM sessions. To learn more about the native integration, please see the [Multimedia Connector for Skype for Business Deployment Guide](#).

Note: This document is valid for the 8.0.301 release(s) of UC Connector.

Important

As of March 31, 2021, Genesys announced the [End of Platform Support for Skype for Business Online](#). It will reach End of Platform Support on July 31, 2021. This impacts **UC Connector 8.0.3 Lync Integration**. If you have questions, contact your account representative.

About Genesys Lync Integration

Find out about Genesys Lync:

[Overview and Architecture](#)

[Task Flow](#)

Deployment

Find out about the actions you must take to deploy Microsoft Lync / Skype for Business and the Genesys components:

[Installation and Configuration](#)

Other Topics

Find out about other important

information for:

Certificate Generation for Genesys
Applications

Genesys Component Configuration for
Lync Interoperability

Genesys Lync Agent

Architecture

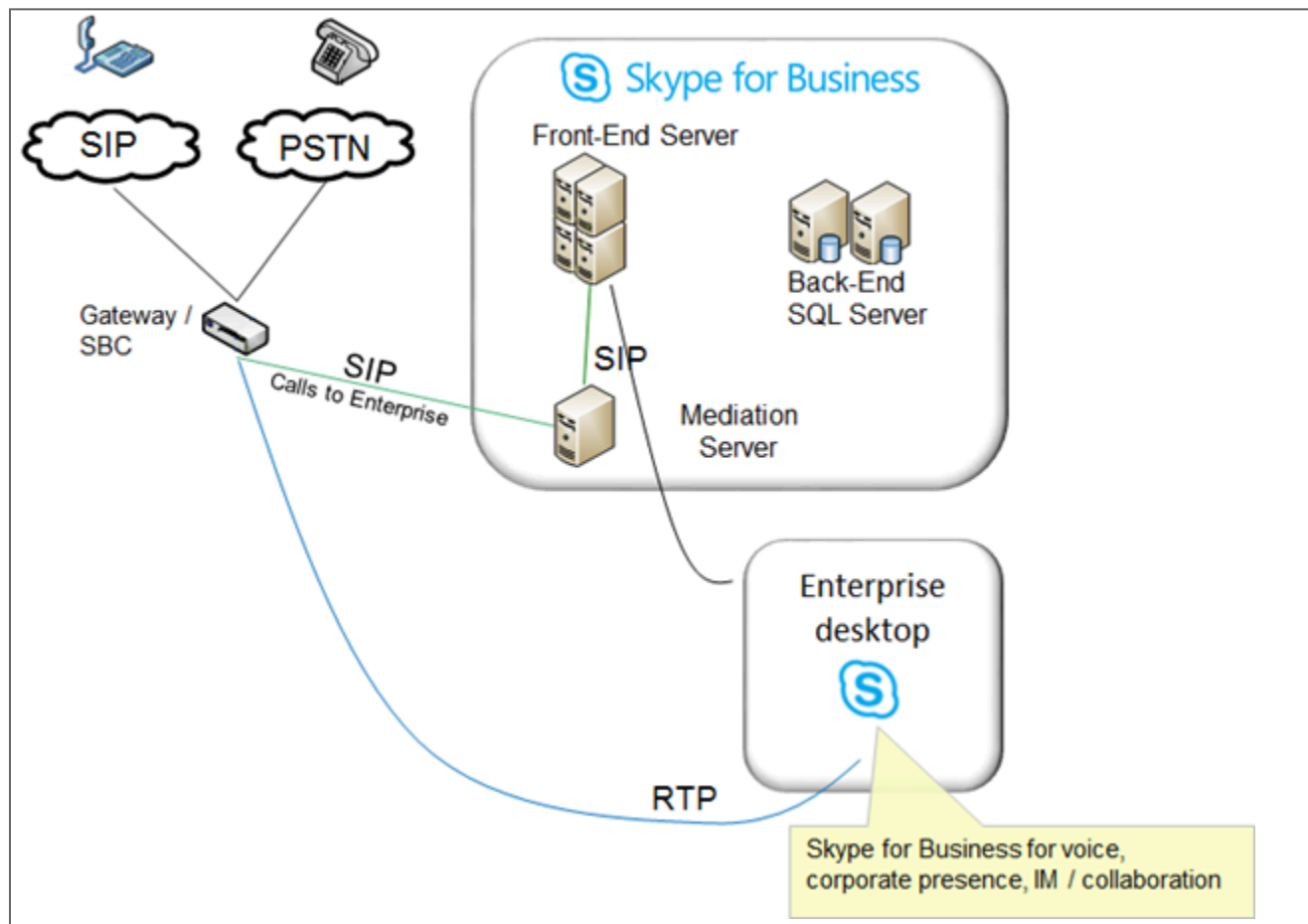
One way that Genesys uses in order to integrate with Microsoft Lync 2010, 2013 and Skype for Business is by using the Genesys SIP Server, deployed in front of the Lync or Skype for Business server. Lync / Skype for Business users' presence is monitored through the Genesys UC Connector, which acts as a gateway between Microsoft and Genesys presence status. This section contains the following topics:

- [Lync / Skype for Business Callflow and Components](#)
- [Environment Information](#)
- [Lync Enterprise Voice Integration](#)

Lync / Skype for Business Call Flow and Components

This page introduces the pure Lync / Skype for Business Enterprise Voice call flow and components. This is before any Genesys integration. Note that a prerequisite of any Genesys integration with Lync / Skype for Business is the Microsoft platform is up and running independently, and processing voice calls.

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, while doing the opposite for media going to the telephone network. Or calls can come in directly on SIP, through a Session Border Controller (SBC). In this case conversion is not necessary.

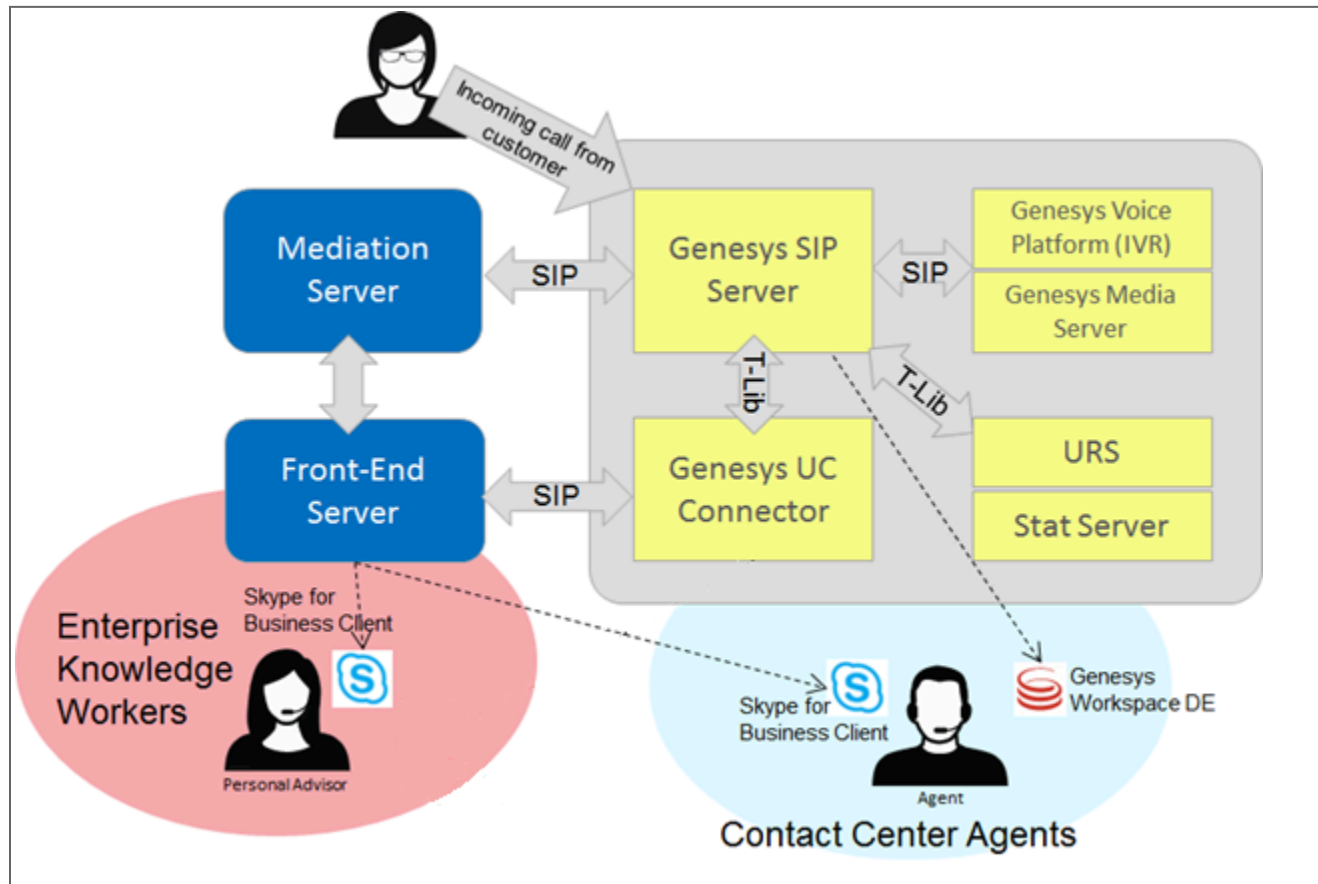


- The Lync / Skype for Business Mediation Server terminates and processes all external voice and signaling connections, policing and throttling the media.

- The Lync / Skype for Business Front End Server manages logins, presence, and signaling for all users.
- Users have a Lync / Skype for Business 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

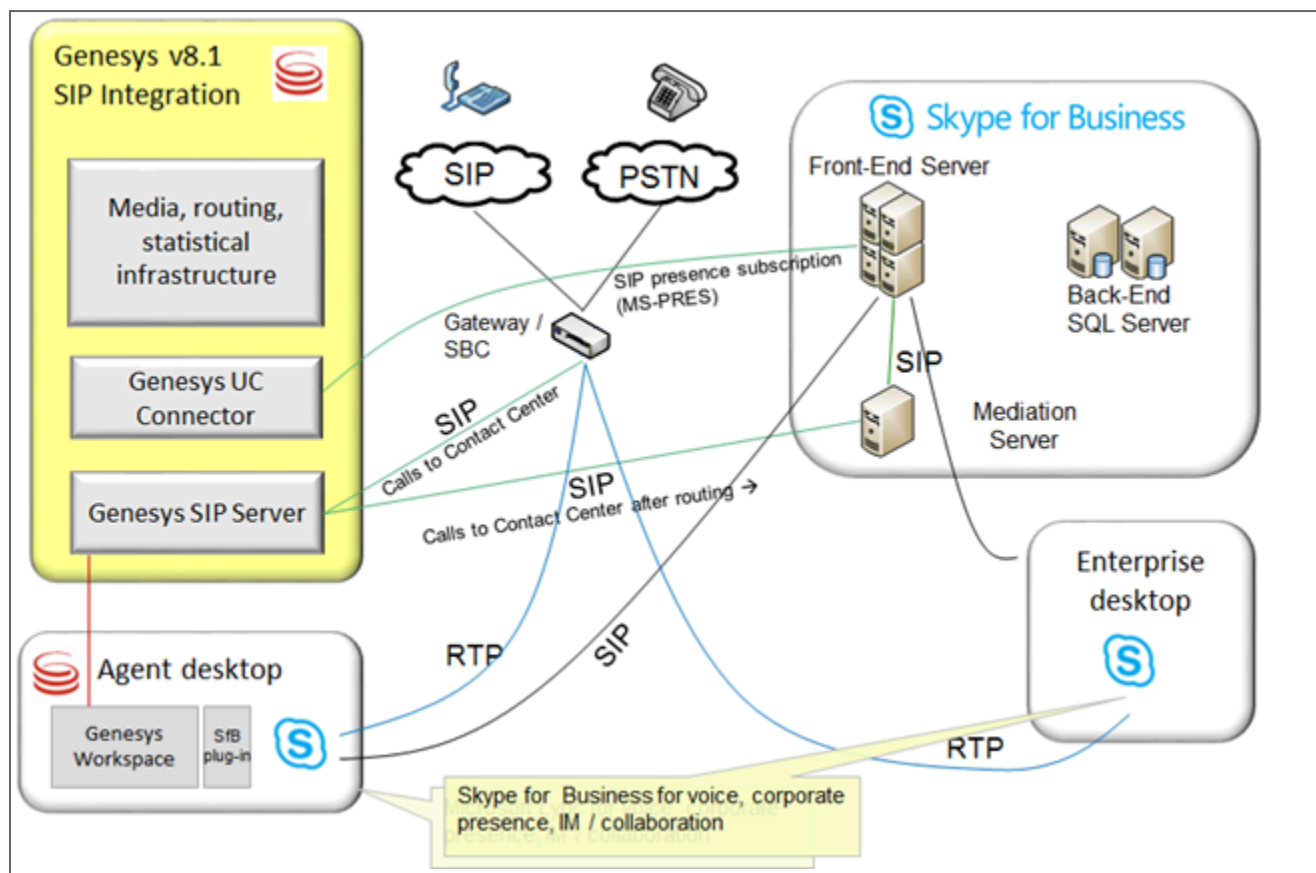
From the Lync / Skype for Business point of view, Genesys SIP Server acts as an external gateway as it receives incoming calls and forwards them to available agents. This is done through a connection with the Mediation Server.



- Genesys UC Connector subscribes to the users' presence, to make their status available to Stat Server. This allows routing of interactions to available personnel.
- Agents can use either Genesys Workspace Desktop Edition as their desktop client along with the Interaction Workspace Plug-in for Skype for Business, or another Genesys desktop client with Genesys Lync Agent (GLA) working together with the Lync / Skype for Business client on their desktop. The option of using Workspace with the Plug-in is more featureful and offers a better user experience, as all functions are performed through the Workspace GUI.
- Using GLA, Genesys integrates with the Lync / Skype for Business client to allow third-party call control and, in particular, answering calls from the Genesys desktop. For detailed information, see [Genesys Lync Agent](#).

Lync Enterprise Voice Integration

The figure below shows the architecture for Genesys SIP Server and Skype for Business (or Lync) Voice for contact center integration.



The SIP Server is positioned in front of the Microsoft platform, 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 / Skype for Business Mediation Server, depending on agents' availability.

Lync Integration Overview

The information below summarizes the various actions you must take to deploy Microsoft Lync / Skype for Business and Genesys components.

Complete Prerequisites

Verify that all prerequisite components are in place:

- [Installing Active Directory Domain Services](#)
- [Installing Active Directory Certificate Services](#)

Note: both these procedures should not be necessary if you are deploying the Genesys SIP Server-based integration on a functioning Lync / Skype for Business environment. Please see this only if you are also installing Lync / Skype for Business from scratch (for instance, in a new lab environment). However, please mostly refer to the Microsoft documentation in this case.

Install and configure Microsoft Lync / Skype for Business

Configure the [Genesys-Specific Lync components](#).

Generate certificate for Genesys applications

1. First generate a client certificate to trust the Lync Front End Server. See [Adding UCC as Trusted Host](#) for details.
2. Next generate a server certificate using one of three methods. Start with [Generating the Client Certificate](#) for details.

Configure Genesys components for Lync interoperability

To configure SIP Server, see [SIP Server Configuration](#).

To configure UC Connector, see [UC Connector Configuration](#).

The Workspace Plugin for Skype for Business must be installed for agents deployed with the Lync / Skype for Business integration. See [Workspace Plugin for Skype for Business](#) for details.

Review current Lync/Skype for Business integration limitations

For details about the limitations of the SIP Server-based architecture of Lync / Skype for Business integration, see [Current Limitations](#).

Supported Lync / Skype for Business Deployments

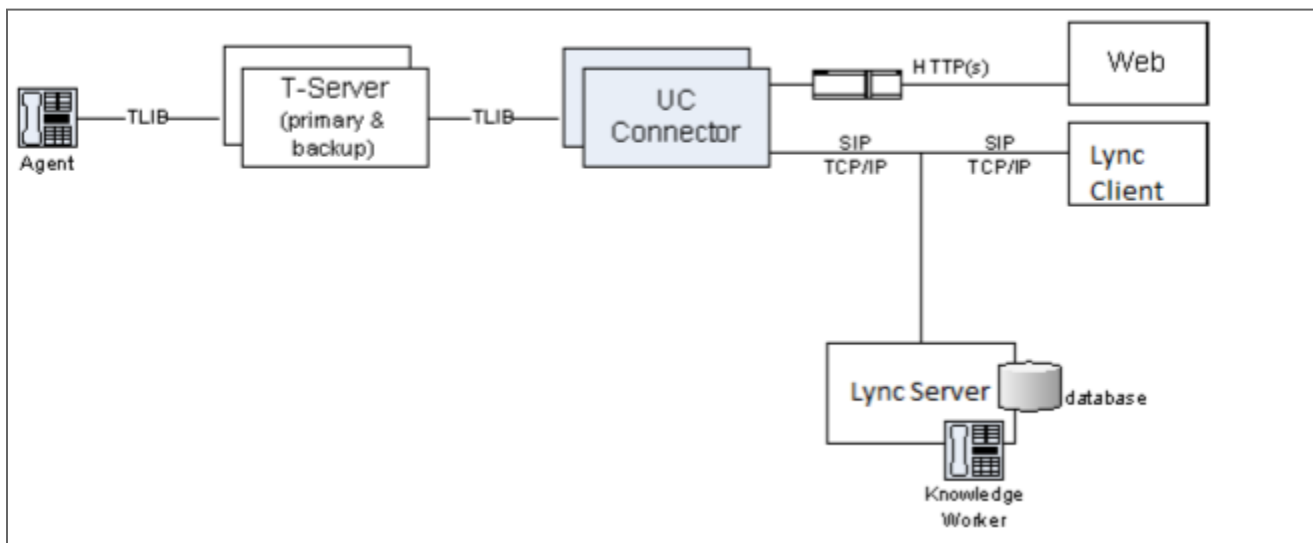
Supported deployments with Microsoft Lync / Skype for Business include:

- Deployment with Microsoft Lync Skype for Business Standard Edition
- Deployment with Microsoft Lync Skype for Business Enterprise Edition
- Deployment with Microsoft Lync / Skype for Business Enterprise via Edge Server

Each of the above deployments is summarized below.

Deployment with Microsoft Lync / Skype for Business Standard Edition

The diagram below shows a UC Connector integration with Microsoft Lync or Skype for Business Standard Edition.



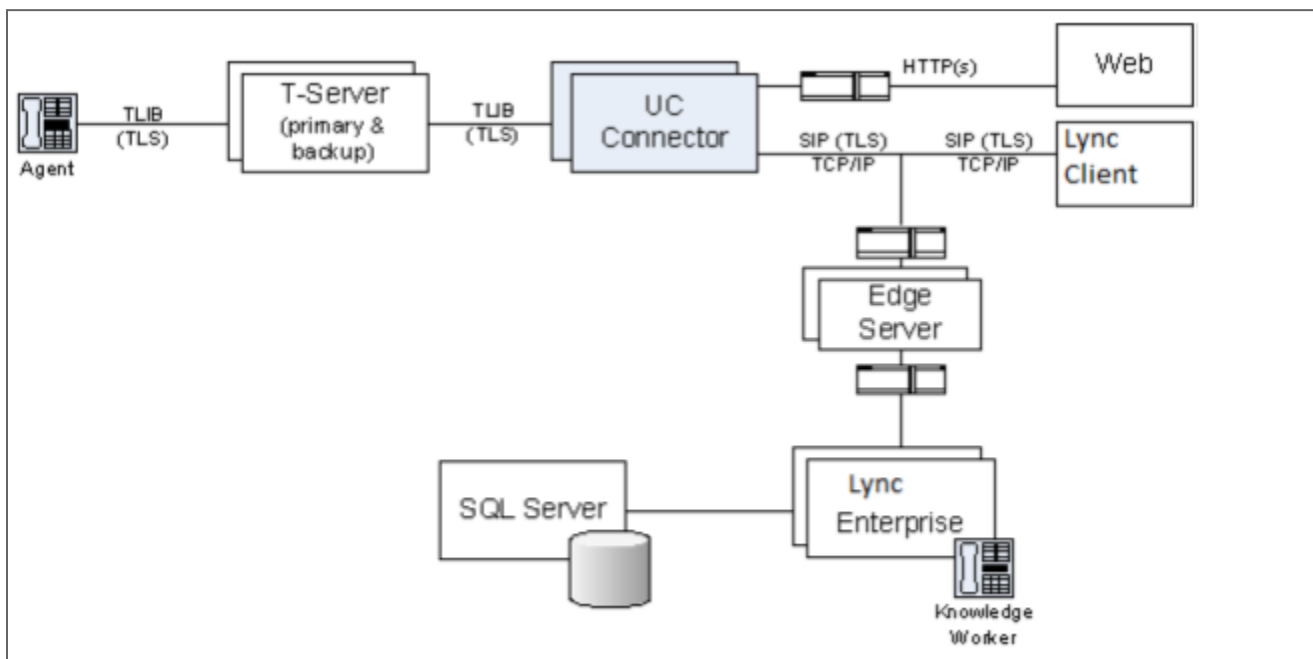
Integrations with the Standard Edition of Microsoft Lync / Skype for Business require that the main server components, as well as the database for storing user and conference information, be deployed on a single Front End Server. This integration is used for organizations with less than 5000 users, and which do not require High Availability through clustering for the Lync / Skype for Business Server part of the system. In essence due to the lack of High Availability, Standard Edition is seldom used in real deployments - but mostly in lab settings.

Database

For the Standard Edition, the real-time communications (RTC) database must be kept locally on a Microsoft SQL Server Express instance.

Deployment with Microsoft Lync / Skype for Business Enterprise Edition

The diagram below shows a UC Connector integration with Microsoft Lync / Skype for Business Enterprise Edition, where the Microsoft platform is deployed on multiple servers, the database is deployed on a separate server, and a third-party load balancer is deployed to balance the load across the Front End servers.



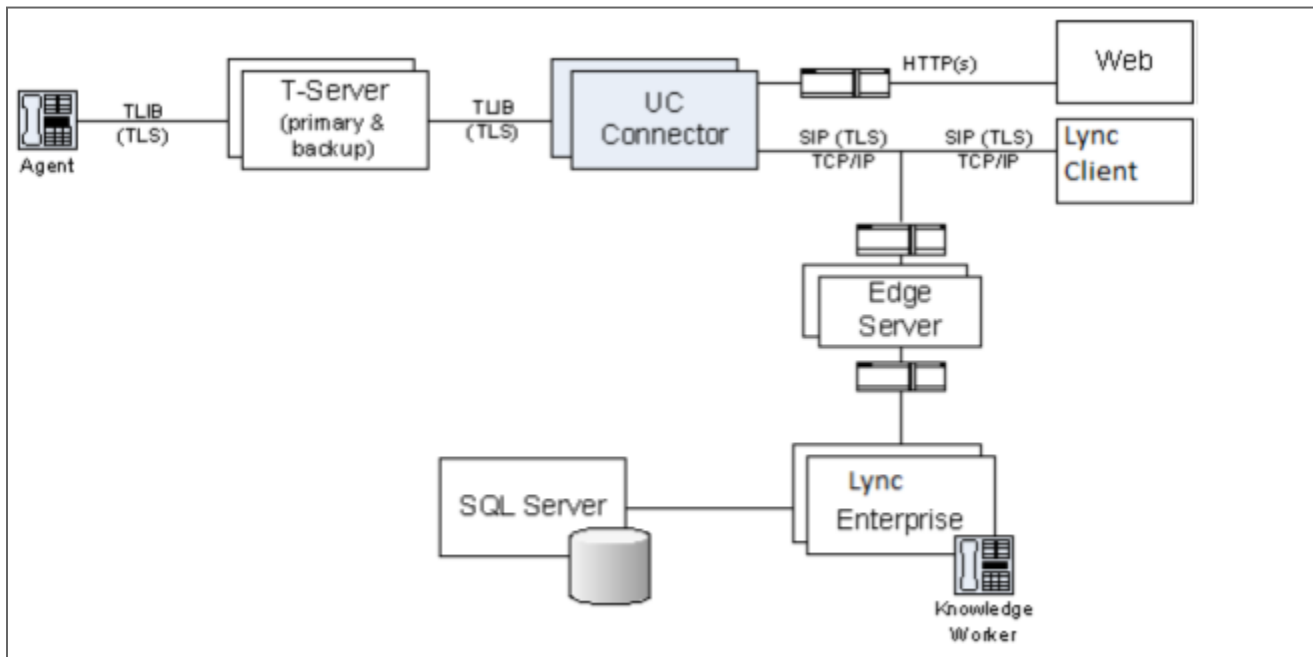
With the Enterprise Edition, you can separate the server functions from the database functions as a way to increase capacity and availability. This edition is recommended for organizations that require higher availability through clustering of server roles.

Database

The Enterprise Editions enables you to specify a remote database server. This dedicated Microsoft SQL Server back-end database must be located on a computer that is separate from any of the Enterprise Edition servers.

Deployment with Microsoft Lync / Skype for Business Enterprise via Edge Server

The diagram below shows a UC Connector integration with Microsoft Lync / Skype for Business Enterprise Edition, where the Microsoft platform is deployed on multiple servers, the database is located on a separate server, and a Microsoft Lync / Skype for Business Edge Server is deployed in front of the primary Front End servers.



About the Edge Server

Installed at the perimeter of the enterprise network where the Lync / Skype for Business servers are located, the edge server is used to authorize users from outside of the enterprise firewall before they can access the Lync / Skype for Business deployment.

For more information about deployments that use the Lync / Skype for Business Edge Server, see the Microsoft documentation for the product: <https://technet.microsoft.com/en-us/library/mt346417.aspx>

Reporting in Microsoft Lync / Skype for Business Integrations

When integrated with Microsoft Lync / Skype for Business, the four standard Microsoft presence states are mapped to user-specific `AttributeReason` parameters. These `KW_UC_STATUS` parameters are used to provide Genesys Reporting with additional information about routing requests involving UC Connector users.

The table below shows the mapping between Microsoft presence states and Genesys `AttributeReason` parameters.

| Communicator Presence | KW_UC_STATUS |
|-----------------------|--|
| Busy | RequestAgentNotReady with KW_UC_STATUS of busy. |
| Do Not Disturb | RequestAgentNotReady with KW_UC_STATUS of dnd. |
| Be Right Back | RequestAgentNotReady with KW_UC_STATUS of be-right-back. |
| Away | RequestAgentNotReady with KW_UC_STATUS of away. |
| Available | RequestAgentReady with KW_UC_STATUS of ready. |

Task Flow

Complete the following tasks to deploy and integrate Lync / Skype for Business and Genesys components.

| Objective | Actions | Details |
|---|---|--|
| 1. Complete prerequisites. | Verify that all prerequisite components are in place. There should be nothing to do if Lync / Skype for Business is up and running and processing calls. | <ul style="list-style-type: none"> • Installing Active Directory Domain Services • Installing Active Directory Certificate Services |
| 2. Enable communication between SIP Server and Lync / Skype for Business. | Create a new public switched telephone network (PSTN) gateway. | <ul style="list-style-type: none"> • Creating a New PSTN Gateway |
| 3. UCC as a Trusted Host. | Add UCC as a Trusted Host in Lync / Skype for Business. | <ul style="list-style-type: none"> • Adding UC as a Trusted Host in Lync / Skype for Business |
| 4. Generate certificates for Genesys applications. | First generate a client certificate to trust the Front End Server. Next, generate a server certificate using one of two methods. | <ul style="list-style-type: none"> • See the topics on generating the client and server certificates. |
| 5. Configure Genesys components for Lync / Skype for Business interoperability. | Configure SIP Server. Configure UC Connector. Install the Workspace Plug-in for Skype for Business. | <ul style="list-style-type: none"> • SIP Server Configuration Tasks • UC Connector Configuration Tasks • Workspace Plug-in for Skype for Business |
| 6. Deploying and Using the Lync Agent. | Use Genesys Lync Agent (GLA) to allow the use of Microsoft Lync or Skype for Business for voice interactions, regardless of the type of Genesys agent desktop client in use.. | <ul style="list-style-type: none"> • Deploying the Lync Agent |
| 7. Review current SIP Server-based integration limitations. | Review limitations that affect this architecture for the Lync / Skype for Business integration. | <ul style="list-style-type: none"> • See Current Limitations. |

Deployment Prerequisites

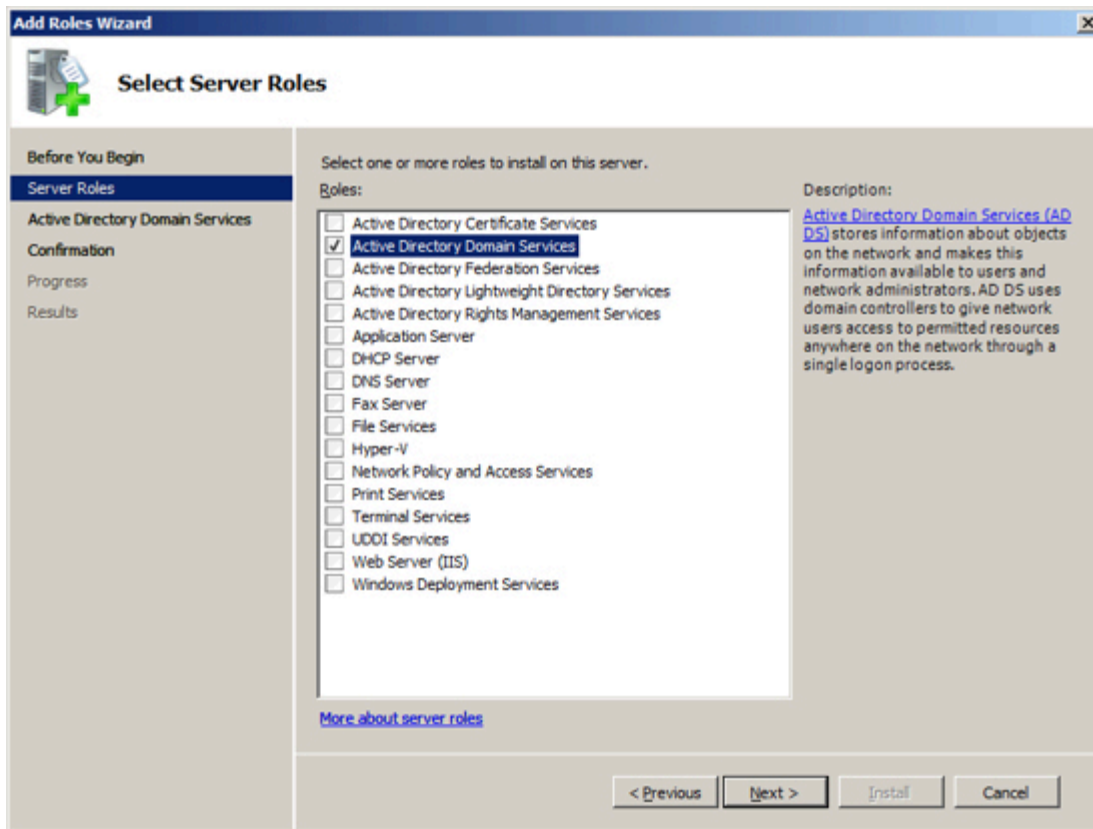
This section discusses prerequisites to installing Microsoft Lync on the server. In order to do this, Active Directory must also be installed and configured, together with Active Directory Certificate Services.

If you are deploying the SIP Server / UC Connector - based integration on a active Lync or Skype for Business Enterprise Voice installation the procedures described in this page are not necessary, as Active Directory will already have been configured. But you may need to perform these tasks if installing Lync / Skype for Business from scratch, for instance in a lab setting.

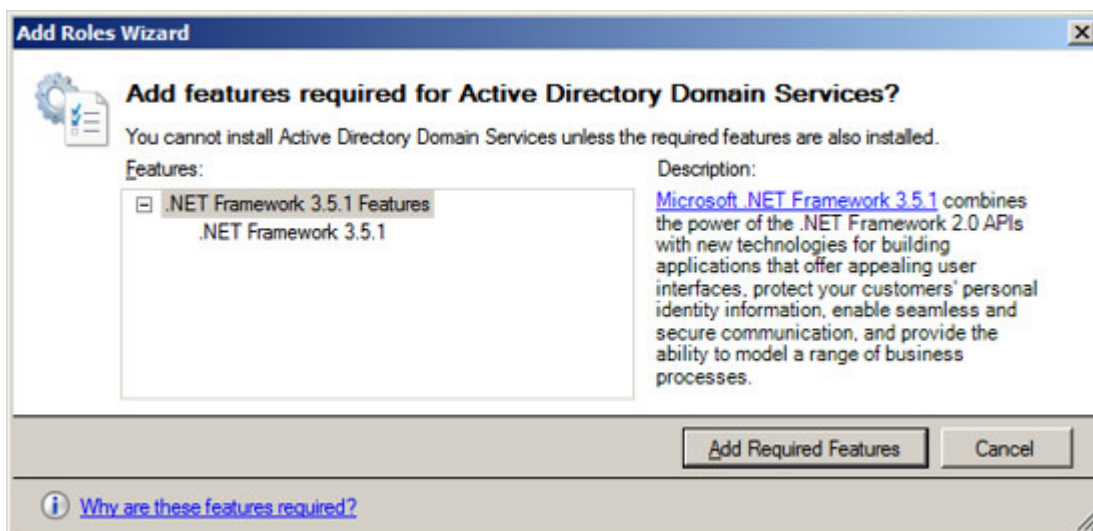
Active Directory Domain Services

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.

1. Access the Server Manager screen. From the Windows taskbar, select Start > Administrative Tools > Server Manager.
2. Under Roles Summary, click Add Roles.
3. At the welcome page for the wizard, click Next.
4. On the Select Server Roles screen, select Active Directory Domain Services.

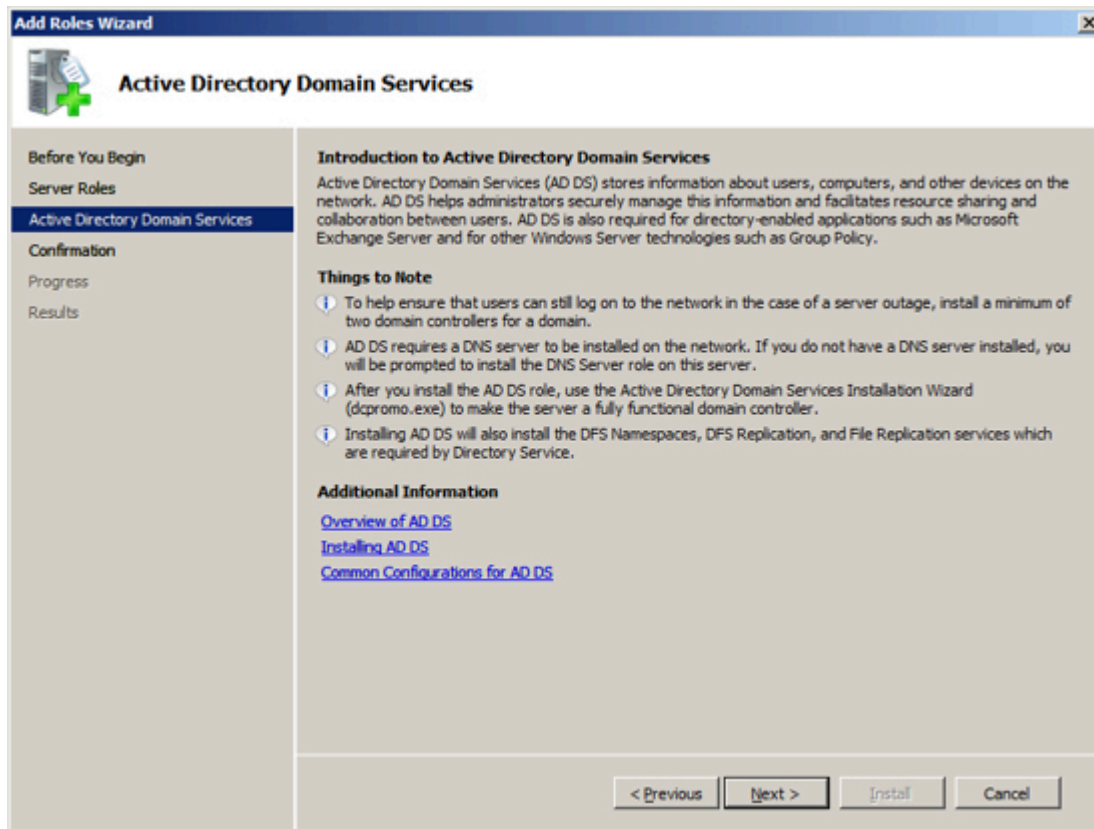


5. In the new dialog, click Add Required Features.

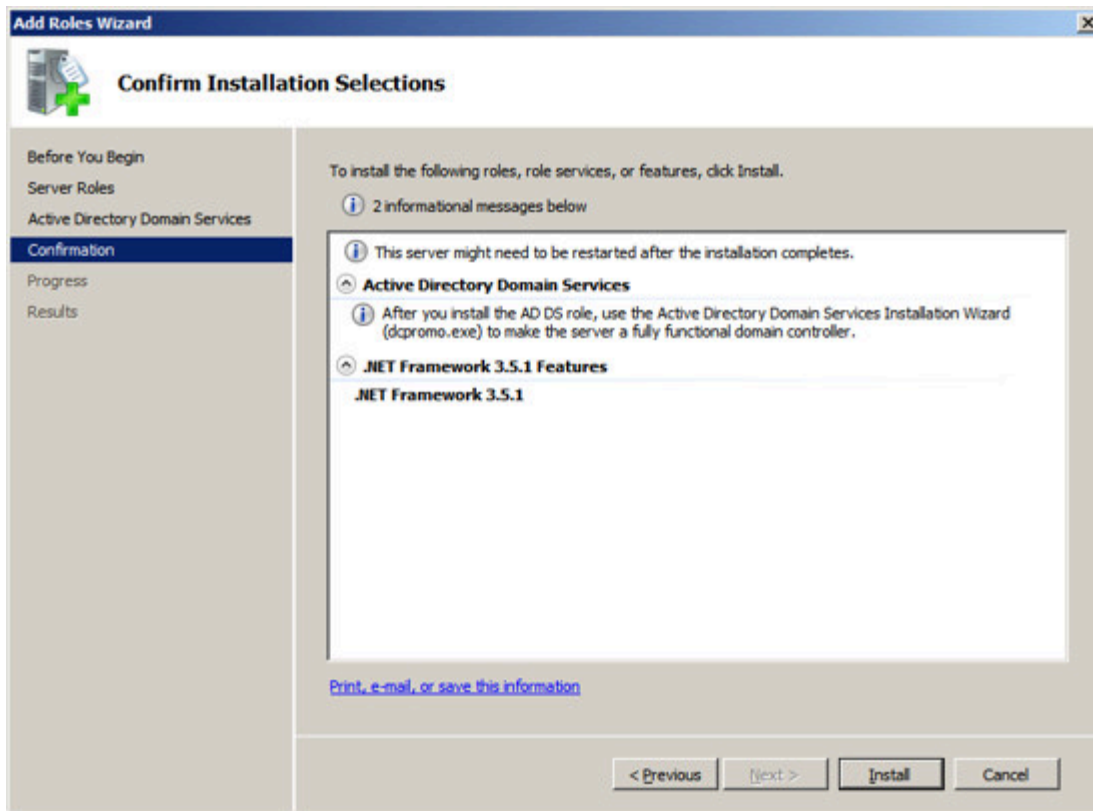


6. Click Next.

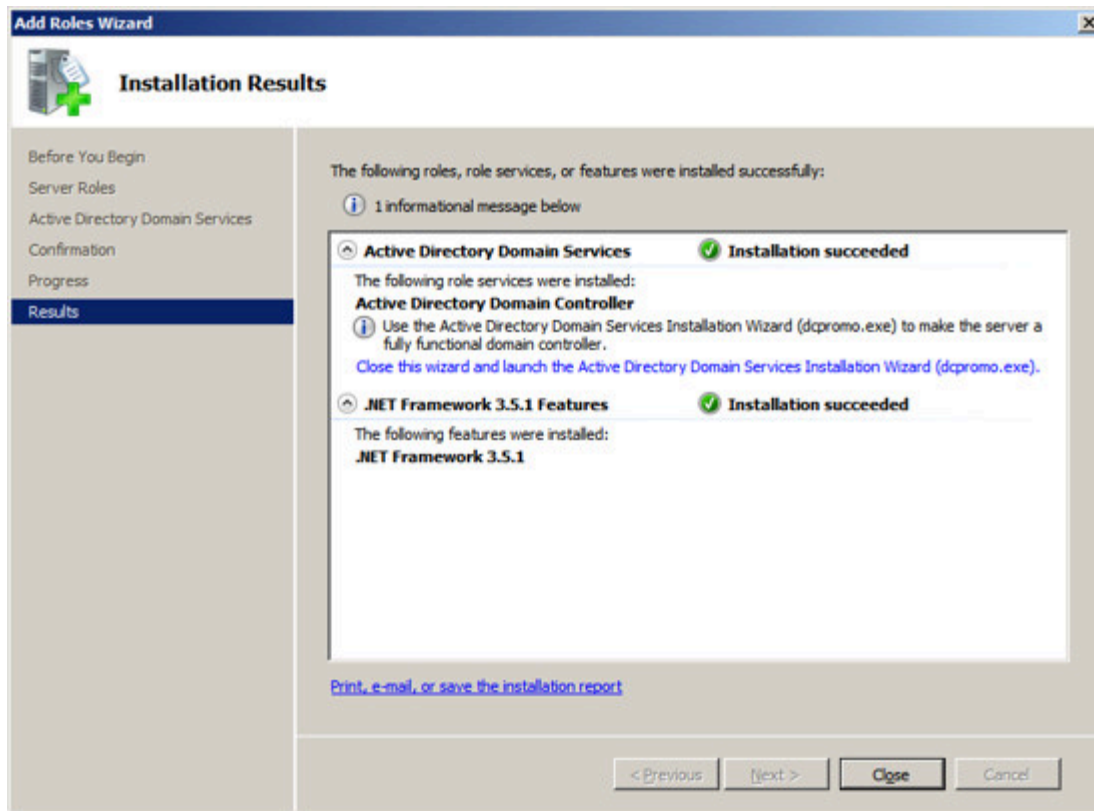
7. Review the information presented in the Active Directory Domain Services screen, and click Next.



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



9. On the Installation Results screen, click Close.



Configuring Active Directory

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

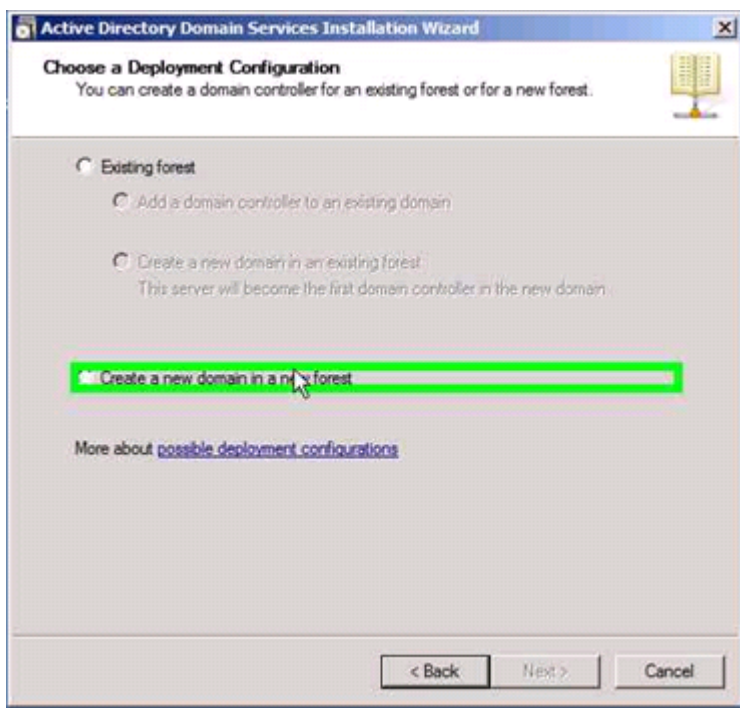
Warning

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

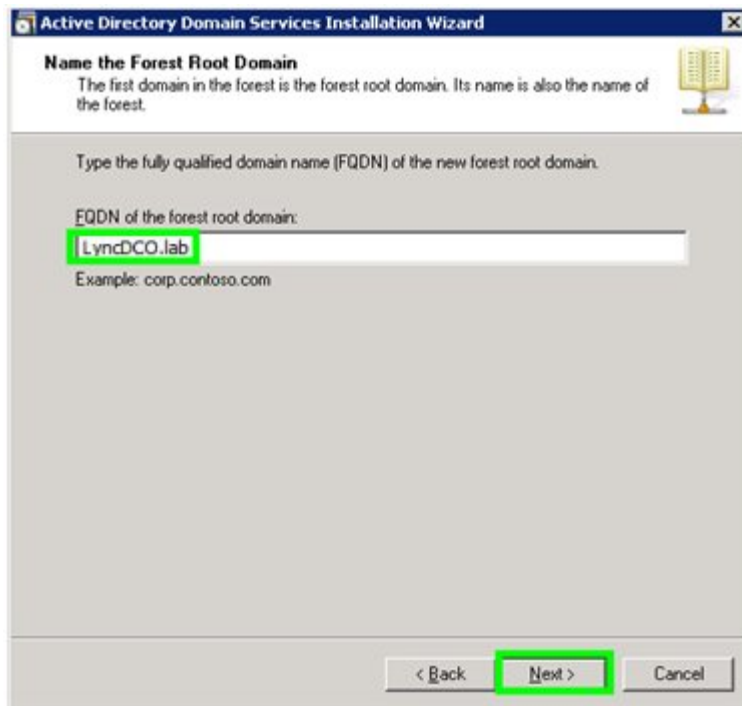
3. Click the Windows Start button and select Run.
4. Type `dcpromo.exe` in the box and click OK. This will launch the Active Directory Domain Services

Installation Wizard.

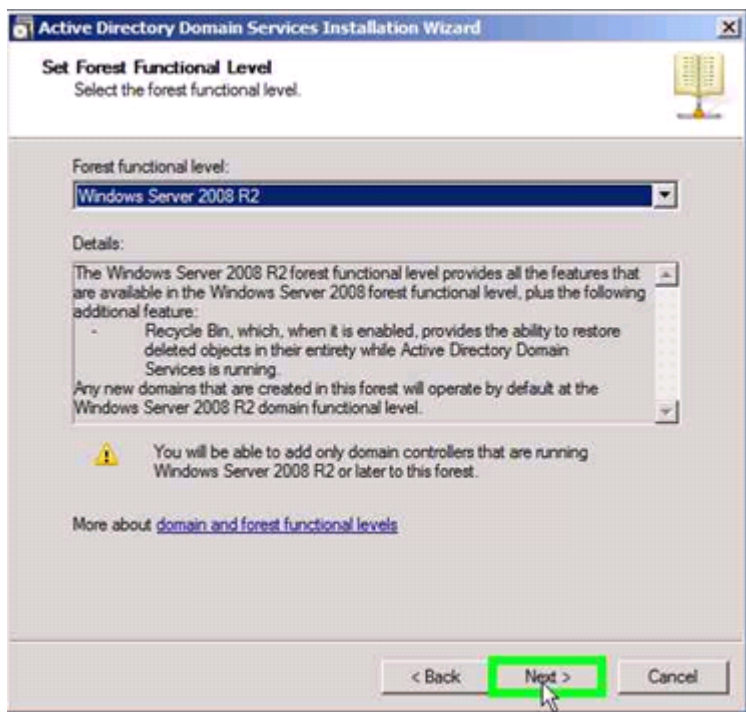
5. On the Welcome page, click Next.
6. On the Operating System Compatibility page, click Next.
7. On the Choose a Deployment Configuration page, select the Create a new domain in a new forest option, and click Next.



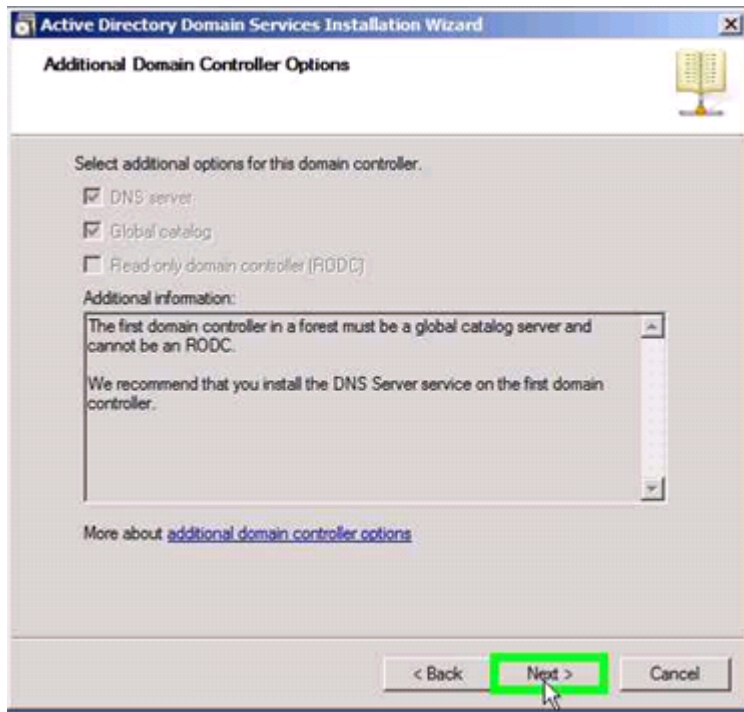
8. On the Name the Forest Root Domain page, enter the fully qualified domain name (FQDN) of the forest root domain and click Next.



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



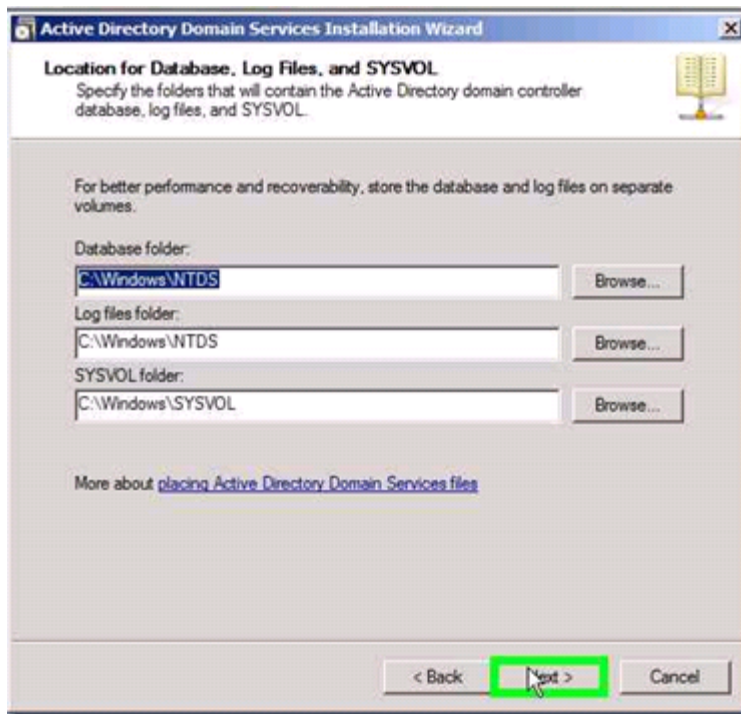
10. On the Additional Domain Controller Options page, ensure that DNS server is selected, and click Next.



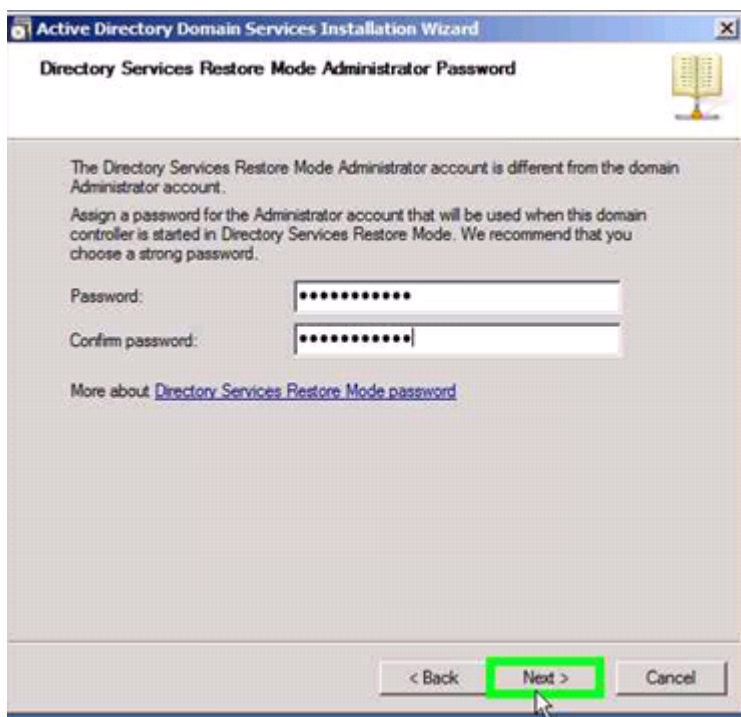
11. Click Yes on the delegation for DNS server warning.



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



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

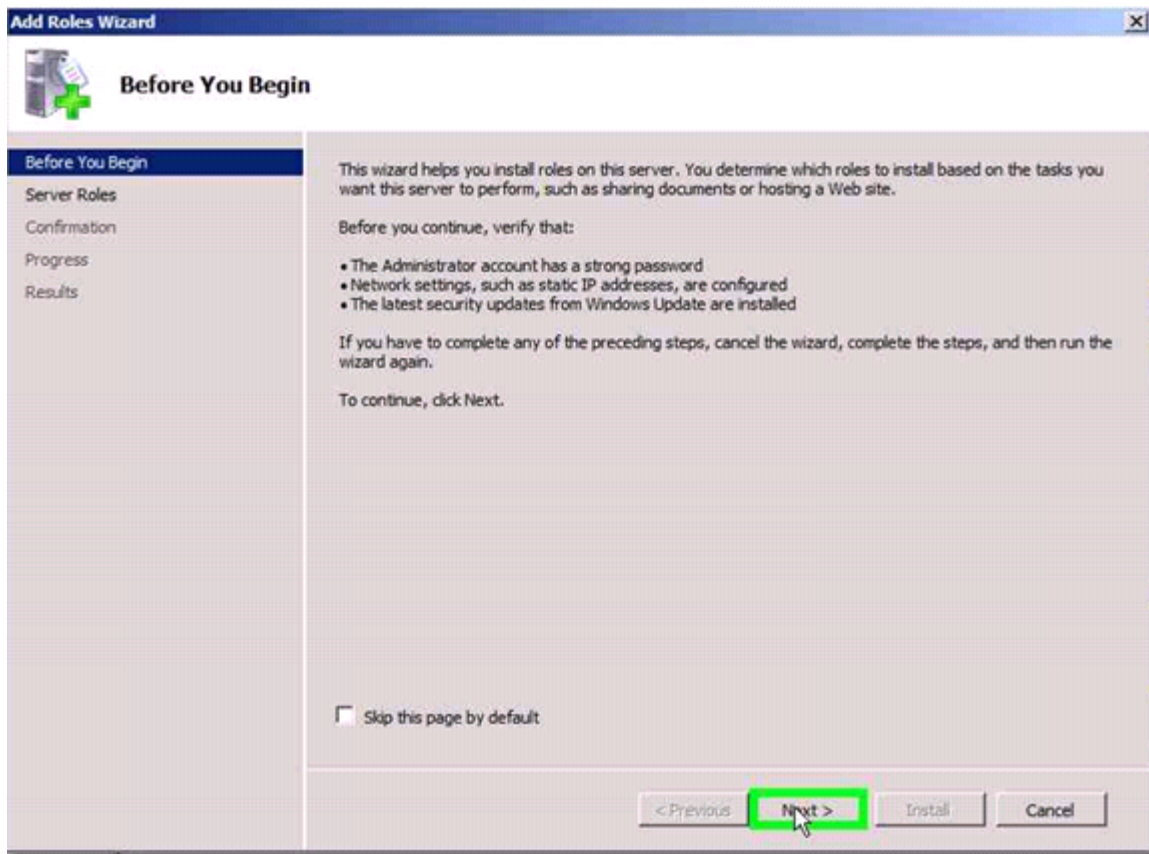


14. On the Summary page, verify the information and click Next.
15. Select the Reboot on completion option to reboot the server when the installation is complete.

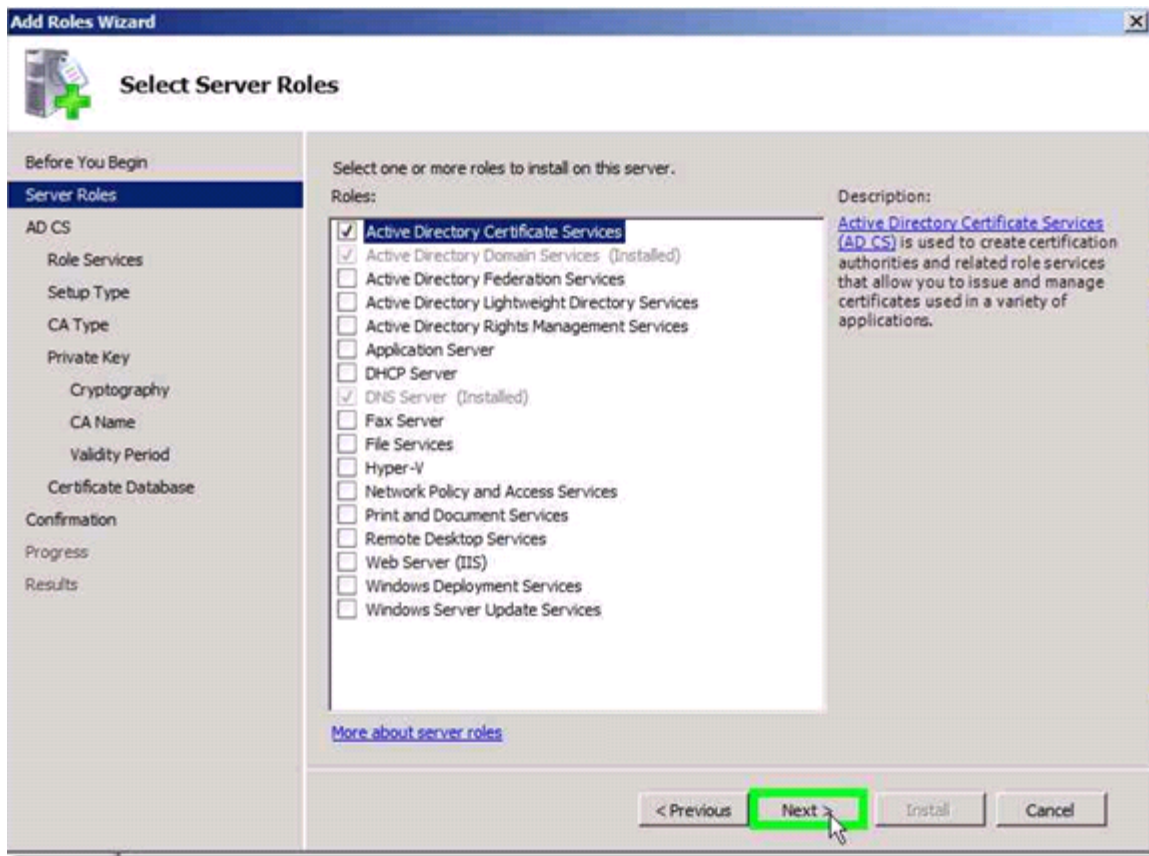
Active Directory Certificate Services

Once your Windows server is configured a **Domain Controller**, you must install the Active Directory Certificate Services.

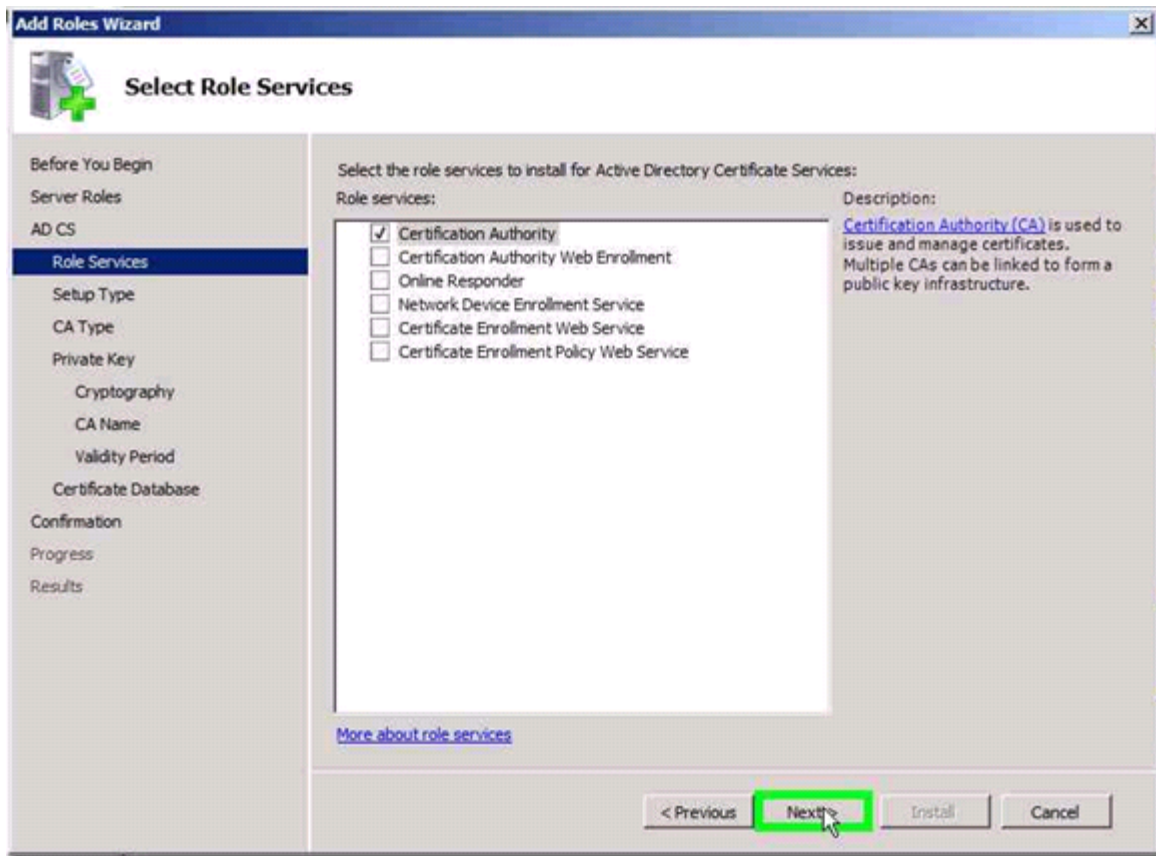
1. Log on to the Domain Controller as [server name]\Administrator.
2. Go to Start > Administrative Tools > Server Manager.
3. Access the Server Manager screen. From the Windows taskbar, select Start > Administrative Tools > Server Manager.
4. Under Roles Summary, click Add Roles.
5. At the welcome page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



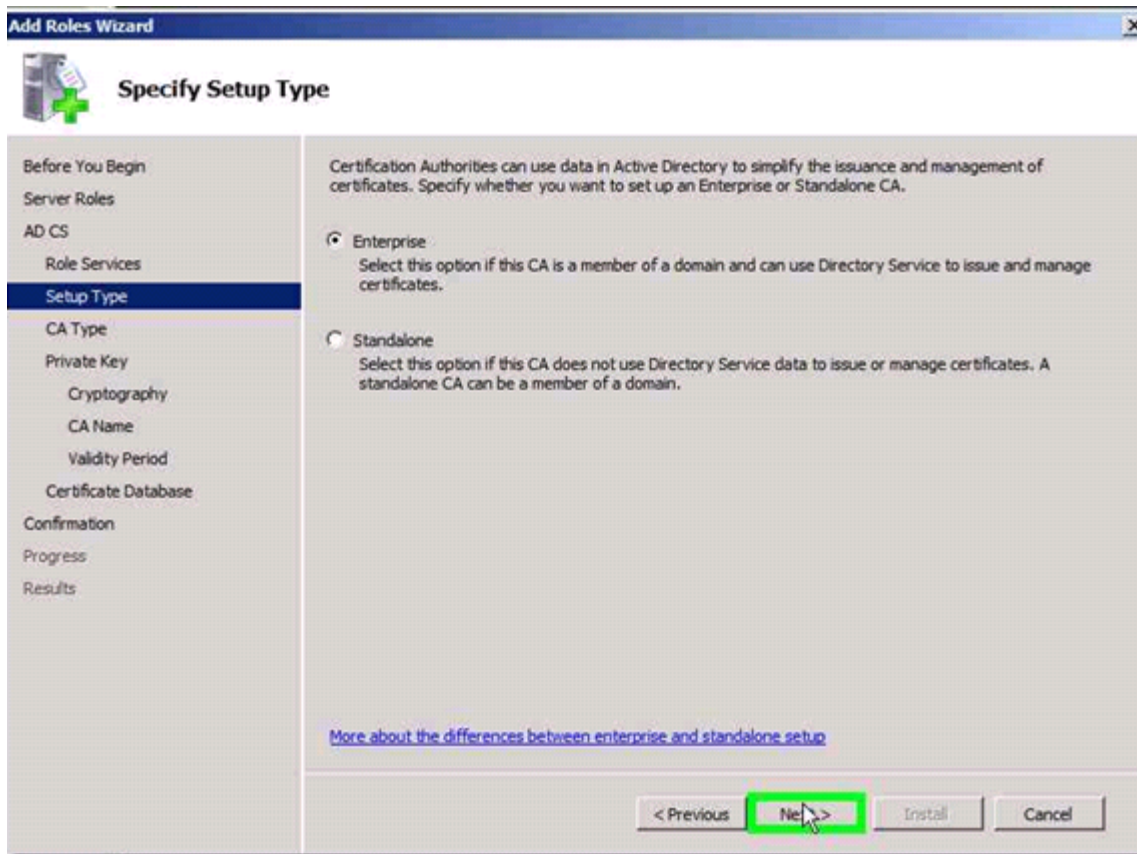
6. On the Select Server Roles page, select Active Directory Certificate Services and click Next.



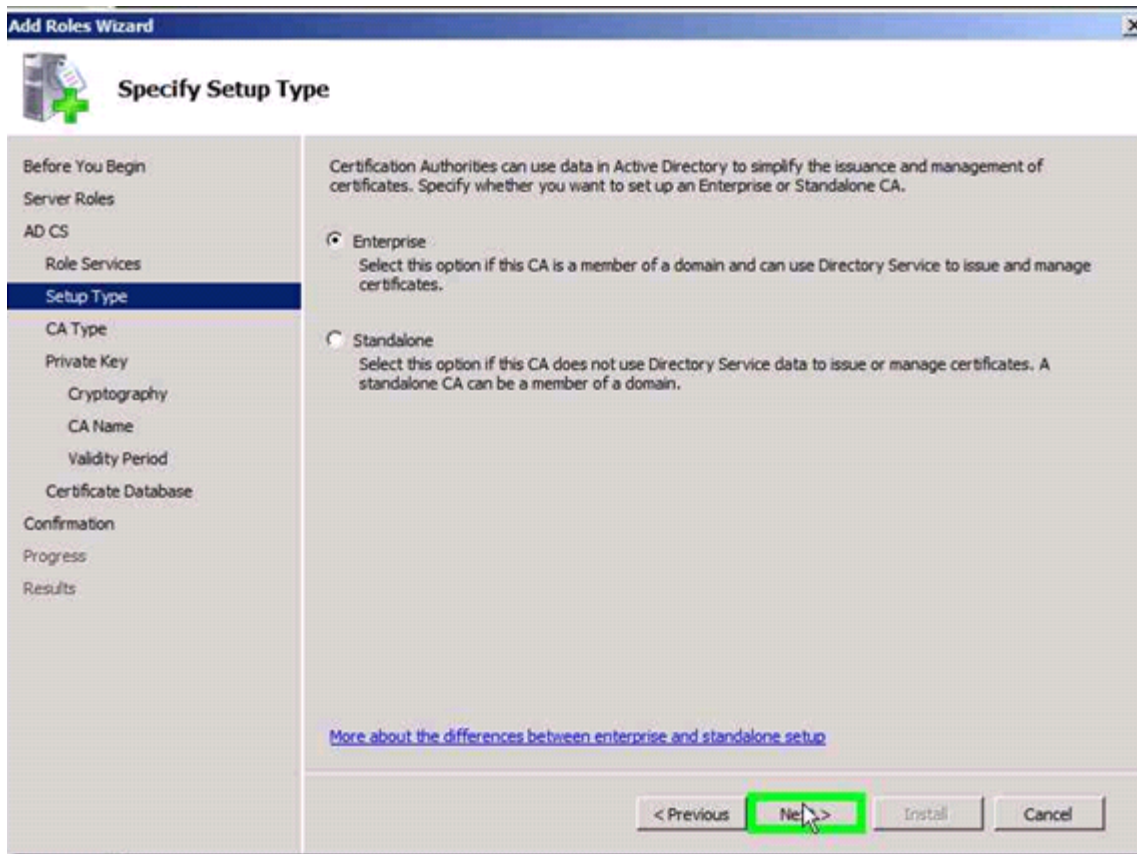
7. On the Introduction to Active Directory Certificate Services page, click Next.
8. On the Select Role Services page, ensure that both Certification Authority and Certification Authority Web Enrollment are selected, and click Next.



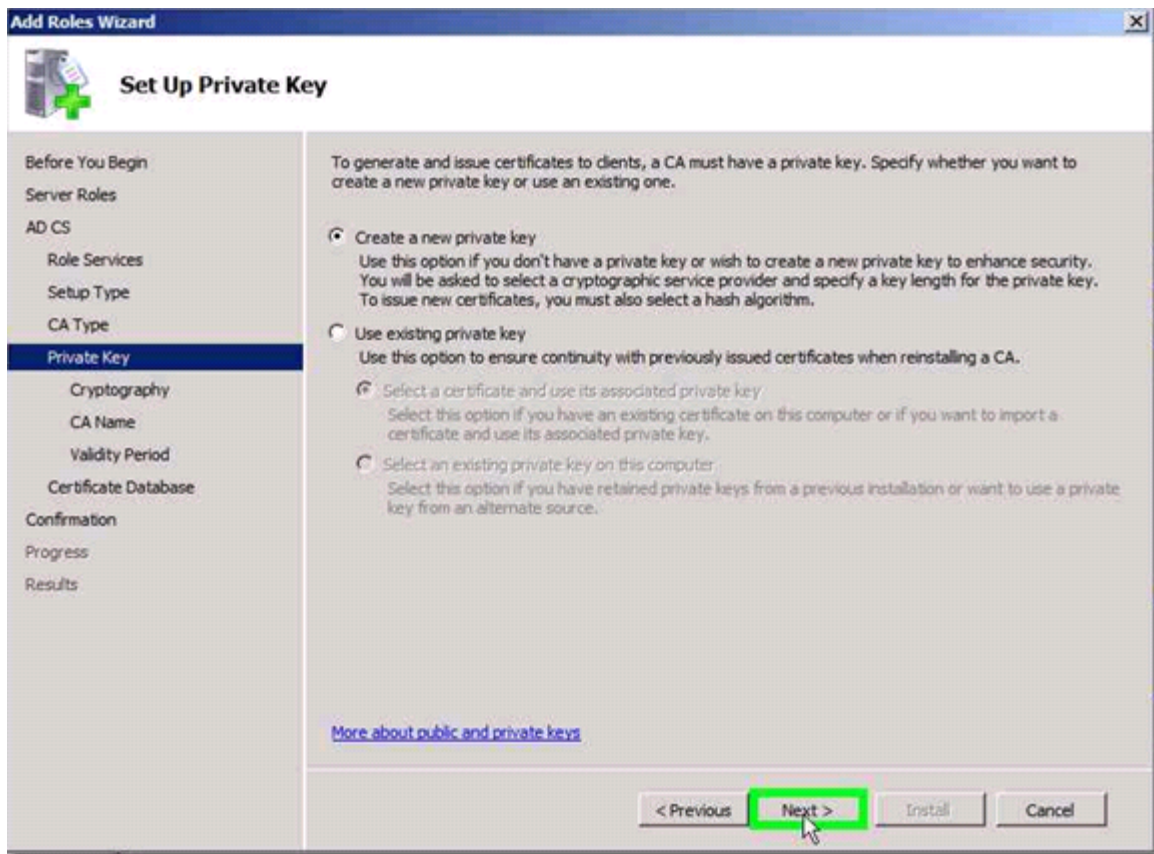
9. On the Specify Setup Type page, ensure that Enterprise is selected and click Next.



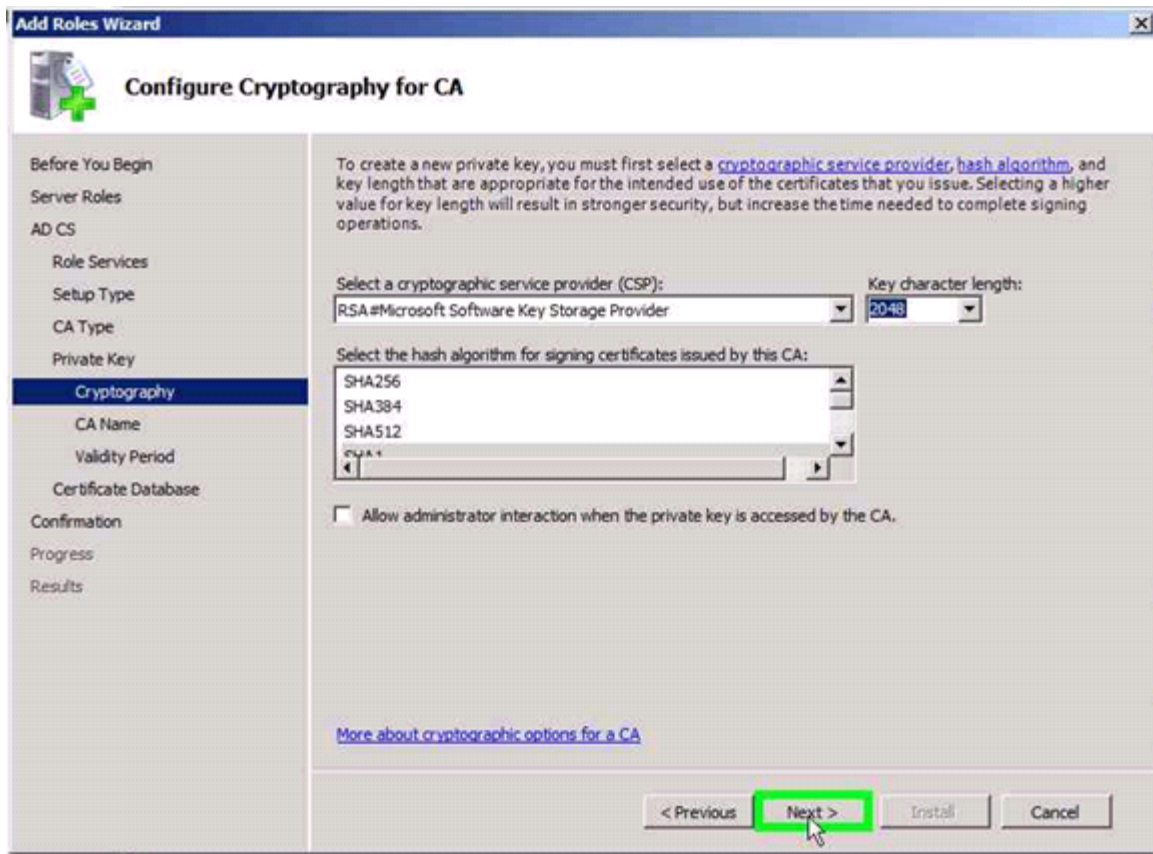
10. On the Specify CA Type page, ensure that Root CA is selected and click Next.



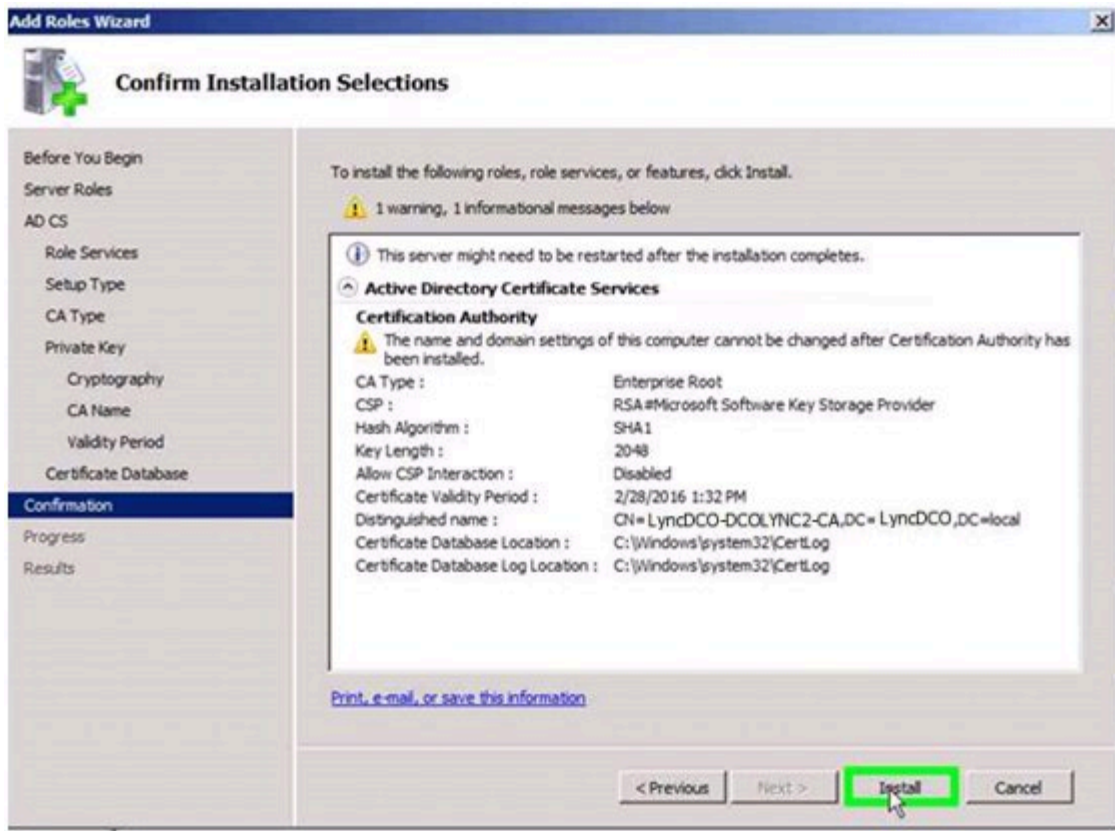
11. On the Set Up Private Key page, ensure that Create a new private key is selected, and click Next.



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



13. On the Configure CA Name page, accept the defaults and click Next.
14. On the Set Validity Period page, accept the defaults and click Next.
15. On the Configure Certificate Database page, accept the defaults and click Next.
16. On the Confirm Installation Selections page, click Install.



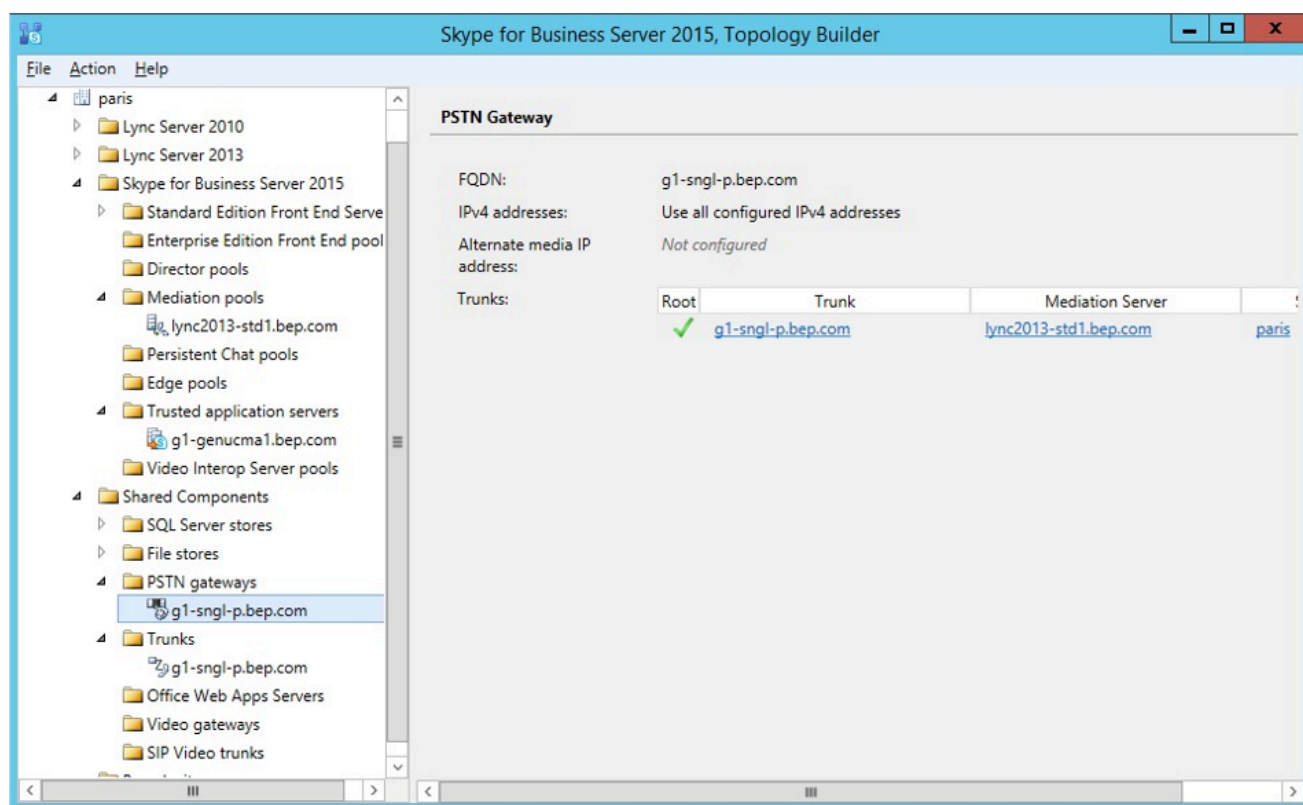
17. Once the installation is complete, click Close.

Creating a New PSTN Gateway

This section discusses the configuration on the Lync / Skype for Business Server that needs to be implemented so that the Genesys SIP Server can integrate with it. The prerequisite for the procedure described in this chapter is that Lync / Skype for Business needs to be deployed in the target network, and fielding voice calls through its Enterprise Voice option.

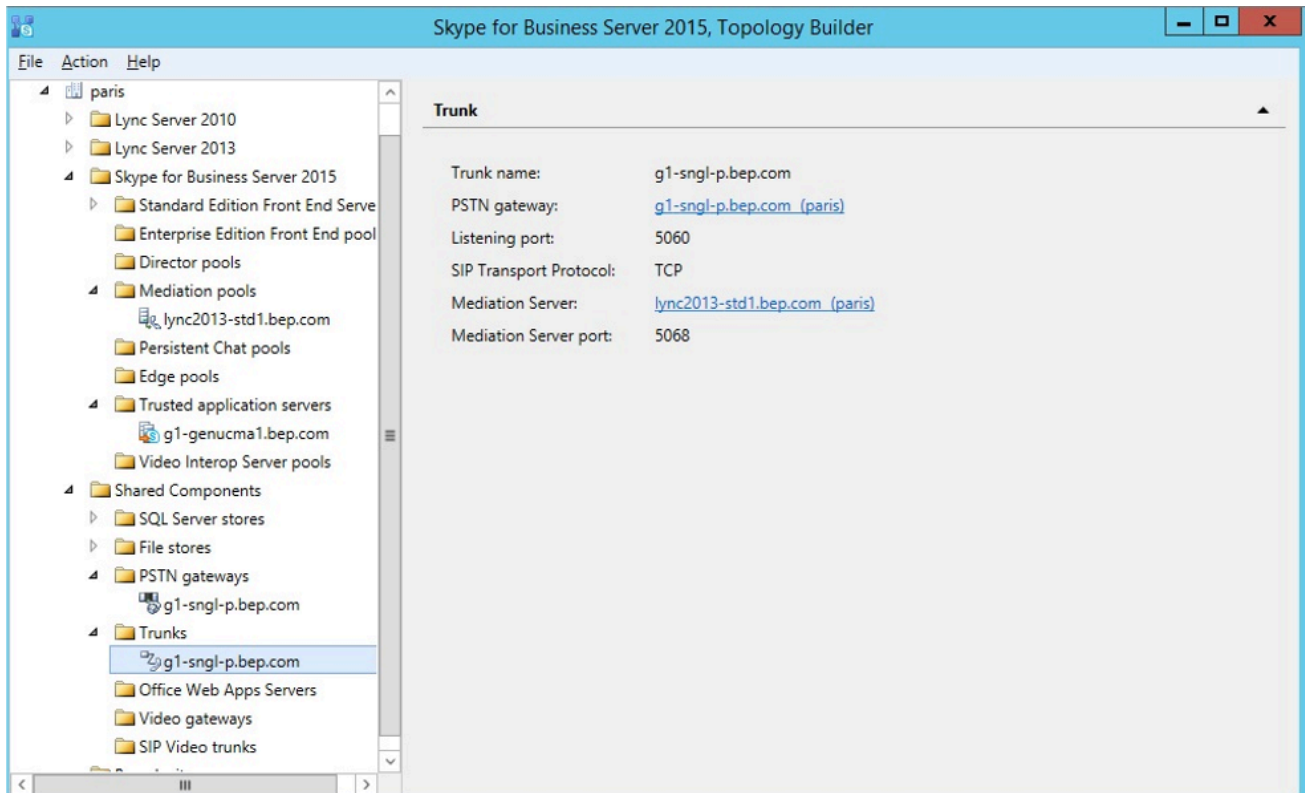
Purpose: To create a new public switched telephone network (PSTN) gateway. The SIP Server is seen by Lync / Skype for Business as a PSTN gateway that talks to the Mediation Server. PSTN gateways are configured in Lync / Skype for Business through the Topology Builder. The following screen shots that illustrate how to create a new PSTN gateway are taken from a Skype for Business deployment. Lync 2013 and 2010 have similar facilities.

1. Declare the host where SIP Server is running as the PSTN Gateway.
2. From the Skype for Business Server 2015 Topology Builder, go to Shared Components > PSTN gateways > New IP/PSTN Gateway.
3. Enter the FQDN of the SIP Server host.



4. Define the root trunk:

- Default trunk name – in the figure, g1-sngl-p.bep.com.
- Listening port for IP/PSTN gateway: 5060 (this port corresponds to the value defined in the SIP Server option sip-port).
- SIP Transport Protocol: TCP.
- Associated Mediation Server: FQDN of Mediation Server.
- Associated Mediation Server port: for example, 5068.

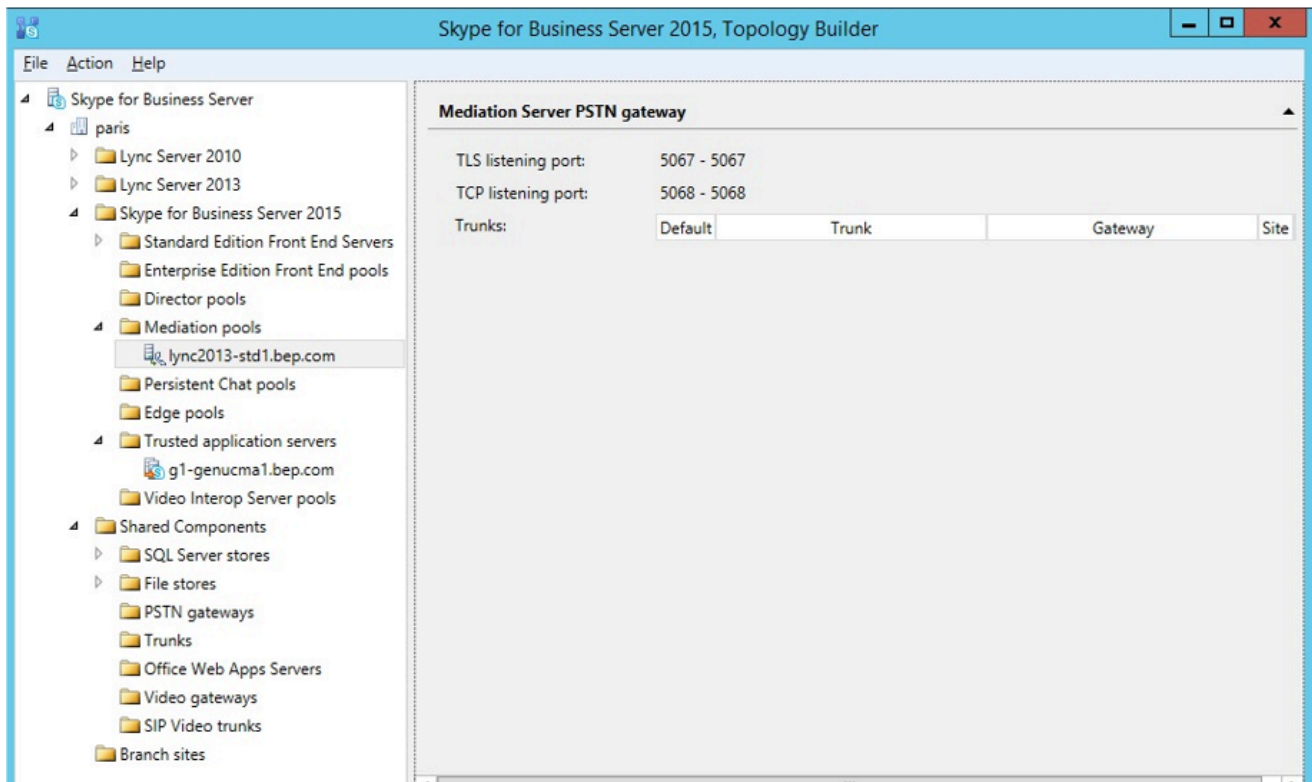


Important

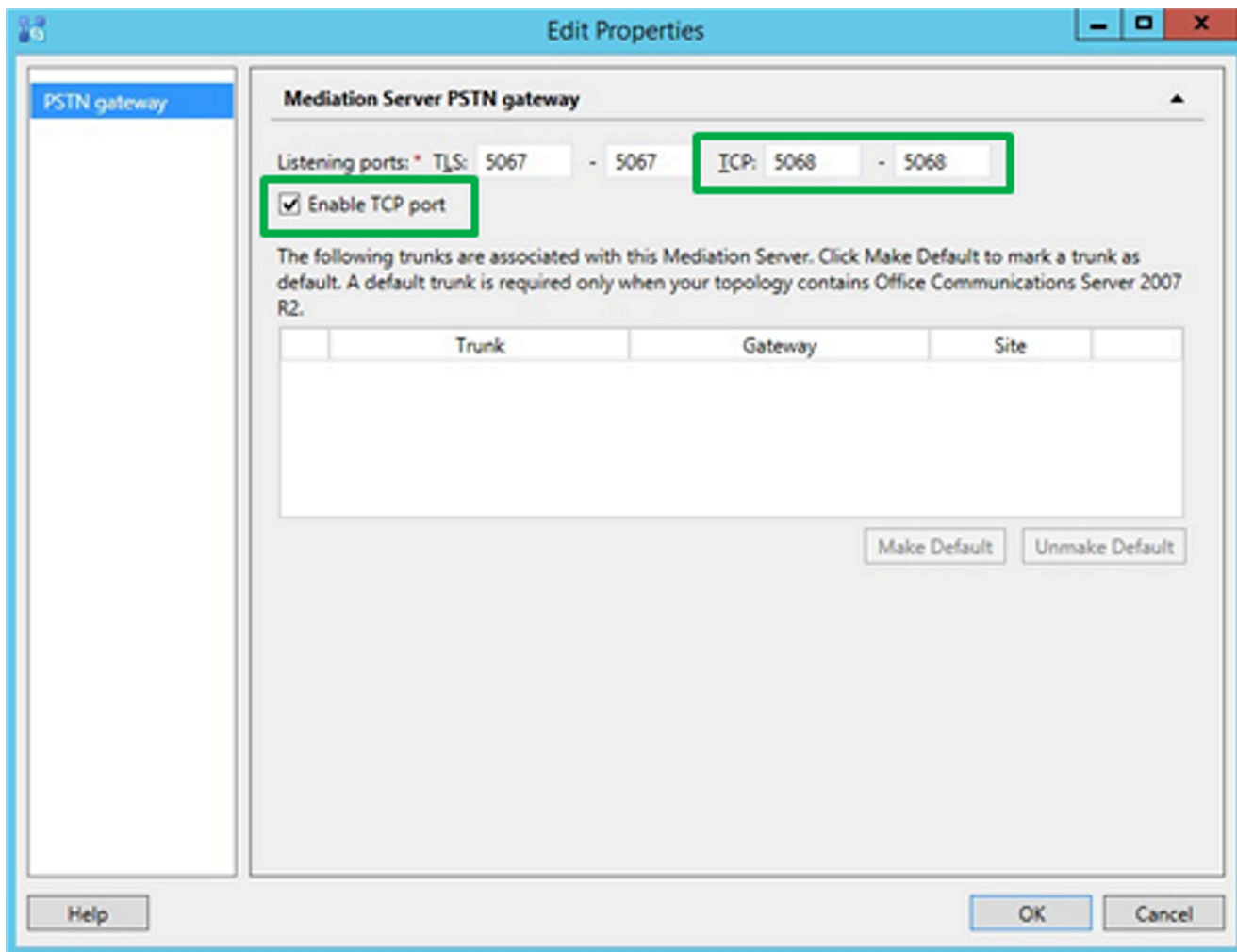
If TCP is not offered as a SIP transport protocol during trunk definition, it means that it has not been enabled on the Mediation Server.

To enable TCP:

1. Go to Skype for Business Server 2015 > Mediation Pool > [FQDN of mediation pool] (as in the following figure):



2. Select the Enable TCP port check box (as shown below).



3. Publish the Topology.

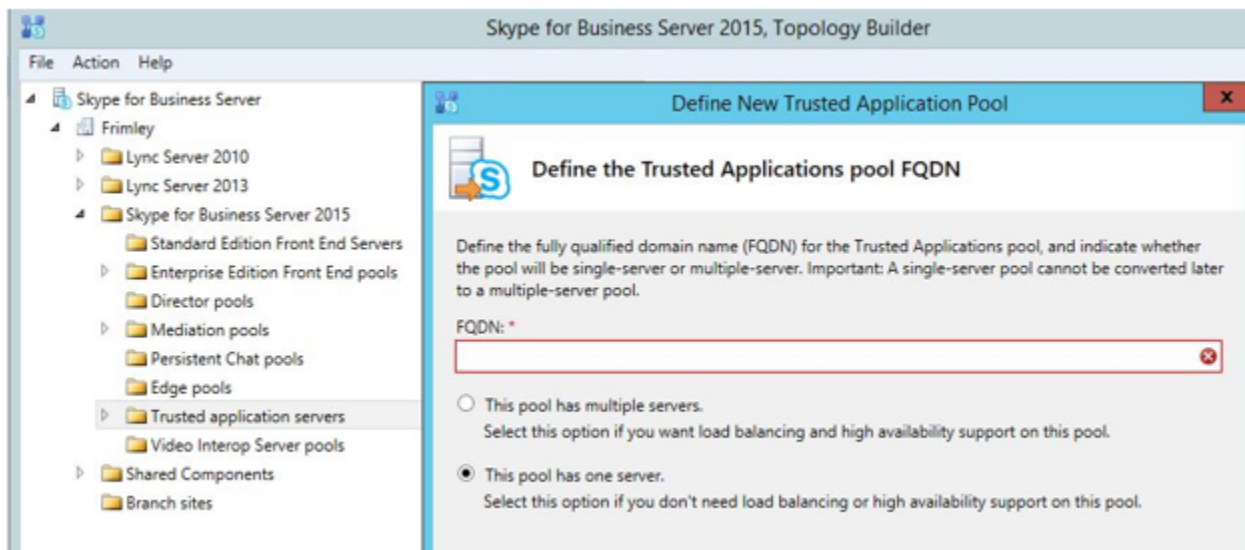
Tip

When you publish the topology, you may have an alert in the Skype for Business Topology Builder if you have used an FQDN that was not declared as a computer in Active Directory. This may happen when you use a second A or a CNAME record used to declare the SIP Server, if it runs on the same host that UC Connector. This is not an error and can be ignored.

Adding UCC as Trusted Host

Purpose: To add the UC Connector host as a Trusted Application Host in the Lync / Skype for Business Topology Builder. On the computer where the Lync / Skype for Business Server is installed:

1. Click Start > All Programs > Microsoft Lync Server 2015 > 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 This pool has one server.
4. Specify the pool, which is selected by default, and click Finish.
5. Publish the Topology.

Note: we are using Skype for Business Topology Builder for this example, Lync 2010/2013 offers a similar tool.

Security Procedures

The procedures below apply to integrations with Lync and Skype for Business relevant for all use cases of UC Connector - whether it is used to exchange presence in Smart Link integrations, or for voice integrations in the Contact Center. For background information see the *UC Connector Deployment Guide*, [Enable Secure Communications](#).

Generating the Client Certificate

Purpose: To generate a regular client/user certificate used to trust servers in the domain, such as the Lync / Skype for Business Front End server(s). This is the same type of certificate that is installed on a user's workstation to start a Lync / Skype for Business client and to connect to the Front End server using TLS connectivity. It is not necessary to export private keys for this certificate or have private keys exportable.

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`

Next Steps:

- On the host computer where Genesys is installed, open the Microsoft Management Console (MMC) or Internet Explorer to retrieve the certificate.
- Continue to one of the following:
 - Generating the Server Certificate using Skype for Business Management Shell
 - Generating the Server Certificate using Microsoft Management Console or CA Web Access.

Generating the Server Certificate Using Skype for Business Management Shell

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

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

```
Request-CsCertificate -New -Type Default -FriendlyName "GenesysServerCertificate" -CA
```

```
"labdc01.companya.com\companya-LABDC01-CA" -ComputerFQDN [server_name] -Verbose
```

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

This will request the certificate through Skype for Business. 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):

- Click Start > Run.
- Type MMC and click OK.

3. Add the certificates snap-in:

- Go to File > Add/Remove Snap-In.
- Click Add.
- Select the Certificates Snap-In and click Add.
- Select Local Computer and click Finish.

4. Find the Genesys Server certificate that you want to export:

- Under the Certificates tree, locate your domain certificate; for example this could be in the Personal folder.
- Click Certificates.
- 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)").

- Choose 'Yes, export the private key'.
- Choose 'Include all certificates in certificate path if possible'.

 Do not select 'Delete Private key'.

- Enter a password (take note of it). (Example: mnopqr)
- Select a location to save the file, then click Finish (Example: GenesysServer_Certificate.pfx)

6. When you get the message "The export was successful", click OK.

Next Steps:

- Place the exported file in a logical location on the UC Connector host machine.
- After the certificate is moved to the UCC host, continue at Configuring a secure SIP port.

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.

Important

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".

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

Next Steps:

- Place the exported file in a logical location on the UC Connector host machine.
- After the certificate is moved to the UCC host, continue at [Configuring a Secure SIP Port](#).

Generating the Front End Server Certificate

Purpose: To generate a server certificate for use in a lab environment.

1. On the host computer where Front End Server is installed, open the Microsoft Management Console (MMC):

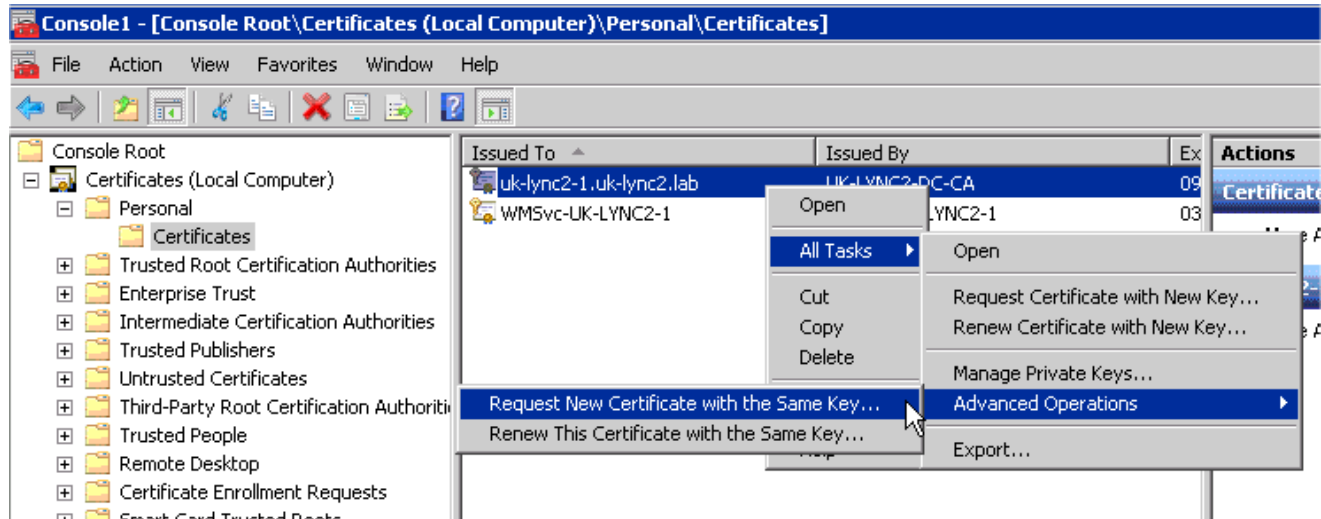
- Click Start > Run.
- Type MMC and click OK.

2. Add the certificates snap-in:

- Go to File > Add/Remove Snap-In.
- Click Add.
- Select the Certificates Snap-In and click Add.
- Select Computer Account and click Finish.
- Select Local Computer and click Finish.

3. Find the Domain certificate that you want to export.

- Under the Certificates tree, locate your domain certificate, for example in the Personal folder.
- Click Certificates.
- Right-click the certificate you want to export, select All Tasks > Advanced Operations > Request New Certificate with the Same Key.



4. Follow the wizard to export the certificate to a .pfx file.

- Choose 'Yes, export the private key'.
- Choose 'Include all certificates in certificate path if possible'.

⚠ Do not select 'Delete Private key'.

- Enter a password (take note of it).
- Select a location to save the file, then click Finish.

5. When you get the message "The export was successful", click OK.

Next Steps:

- Place the exported file in a logical location on the UC Connector host machine.
- After the certificate is moved to the UCC host, continue at [Configuring a Secure SIP Port](#).

Modifying Command Line Arguments for MTLS

Prerequisites

- You noted the password that you created in Generating the Front End Server Certificate.
- You noted the file location where you placed the .pfx file.

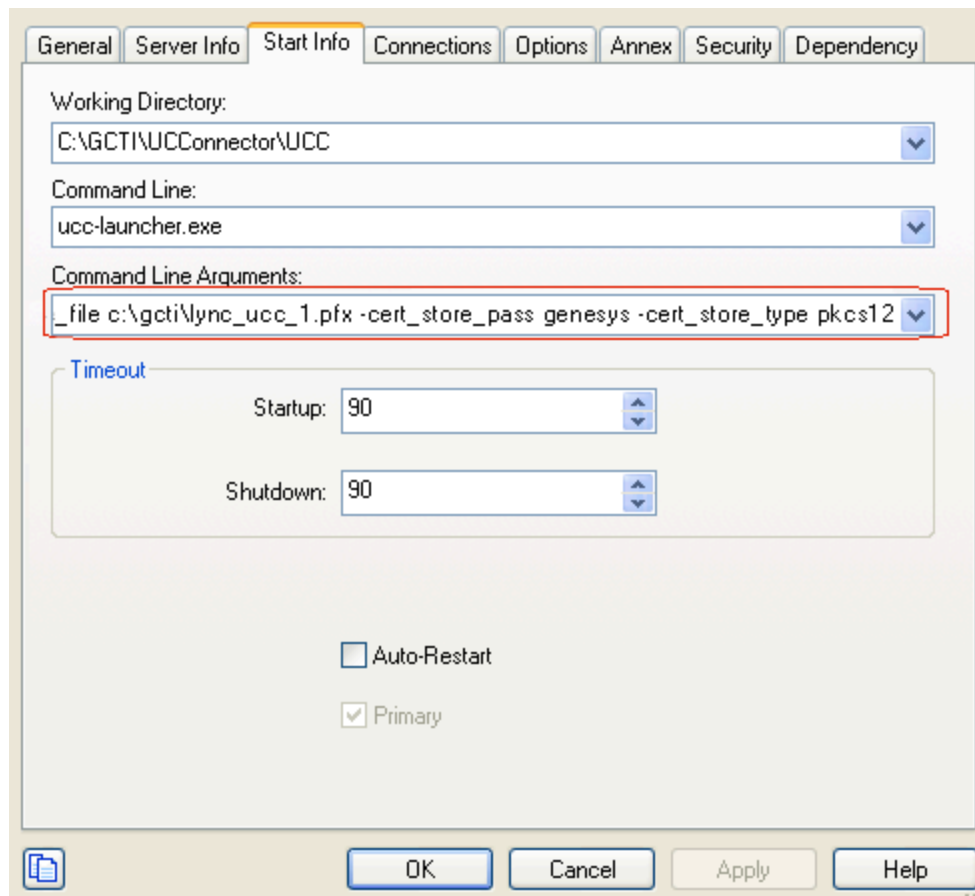
1. Go to Start Info tab > Command Line Arguments in the UC Connector application.

2. Add the following parameters to the existing command line argument:

```
-cert_store_<path to .pfx file on UCC host>  
-cert_store_pass <password generated in Generating the Front End Server Certificate.  
-cert_store_type pkcs12  
-key_store_file <path to the Java keystore file>—This file contains the collection of CA  
certificates trusted by the application process (trust store). If a trust store location is not specified,  
the SunJSSE implementation uses a keystore file in the following locations (in order):
```

- \$JAVA_HOME/lib/security/jssecacerts
- \$JAVA_HOME/lib/security/cacerts

```
-key_store_pass <password to unlock the keystore file>  
-ket_store_type jks
```



3. Click OK to save.

4. If you are planning on starting UC Connector from the batch file, you must also modify the startup.bat file with the certificate parameters.
For example, the following startup.bat is appended with these sample certificate values:

```
-cert_store_file c:\gcti\lync_ucc_1.pfx
-cert_store_pass genesys
```

```
@echo off
```

```
rem -----
rem Copyright (C) 2011 Genesys Telecommunications Laboratories, Inc.
rem
rem startServer.bat file for UC Connector, version 8.0.100.12
rem -----
```

```
@TITLE UC Connector v. 8.0.100.12: Application UCC_Saran
ucc-launcher.exe -host 10.10.10.0 -port 2020 -app UCC_Saran -l 7260@135.80.170.120 -http_port 6060 -cert_store_file
c:\gcti\lync_ucc_1.pfx -cert_store_pass genesys -cert_store_type pkcs12
```

Next Steps:

- If you came to this task from the Lync / Skype for Business procedures, you might still need to integrate with Genesys Routing. If so, see the *Genesys UC Connector Deployment Guide*, [Integrating with Genesys Routing](#).
- Otherwise, configure the routing strategies used to deliver interactions to the Knowledge Worker. See the *Genesys UC Connector Deployment Guide*, [Configuring the Routing Strategies](#).

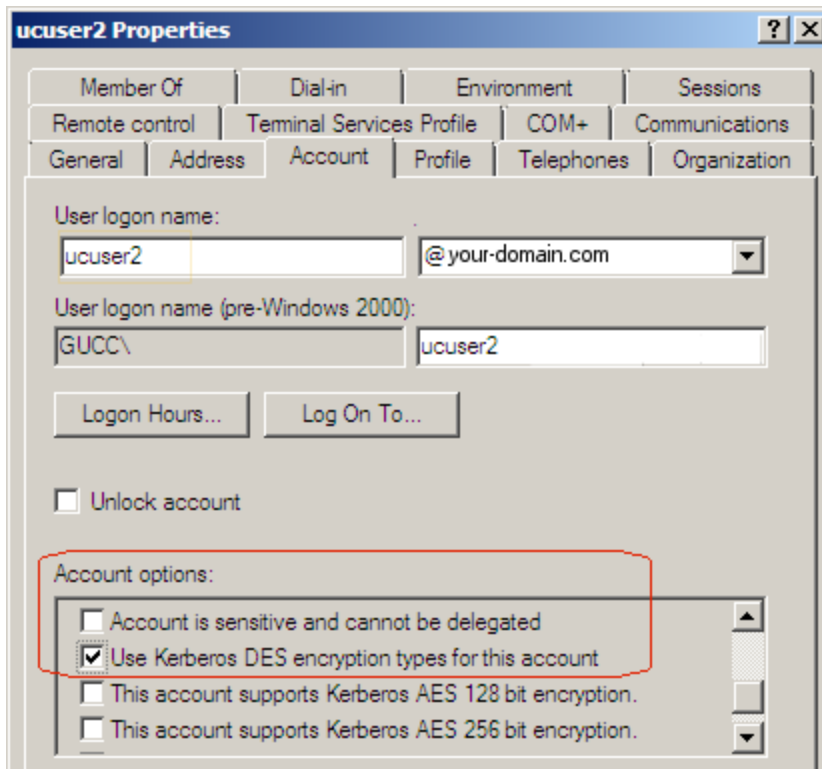
Enabling Kerberos Security Between UCC and Lync Skype for Business

See the *Genesys UCC Connector Deployment Guide*, Enable TLS/Kerberos in [Enable Secure Communications](#)

Configuring Kerberos Security in Active Directory

Purpose: To configure Kerberos security for the user that represents the UC Connector environment in the Microsoft Lync / Skype for Business deployment.

1. Access the user properties in Active Directory.
2. Locate the OCS user that represents your UC Connector environment, right-click this user, and then select Properties.
3. On the Account tab, under the Account options field, select Use Kerberos DES encryption for this account.



Creating a Password for Kerberos Security

Prerequisites

- You are logged in to Configuration Manager.
- A UC Connector Application object, which has been configured according to Creating the UC Connector Application Object.
- An account/user that represents the UC Connector has been created in Microsoft OCS. For example, ocs-ucc.
- You will need the password configured for this user in Active Directory. If you do not know the password, you might have to reset it. Right-click the user in Active Directory and select reset password.

1. Go to Environment > Applications and double-click the UC Connector Application object.

2. Go to the Options tab.

3. In the Microsoft-OCS section, set the password option to String. Set this option to the password configured for the OCS user in Active Directory. This is your Kerberos password, required for Kerberos authentication between the components.

Next Steps:

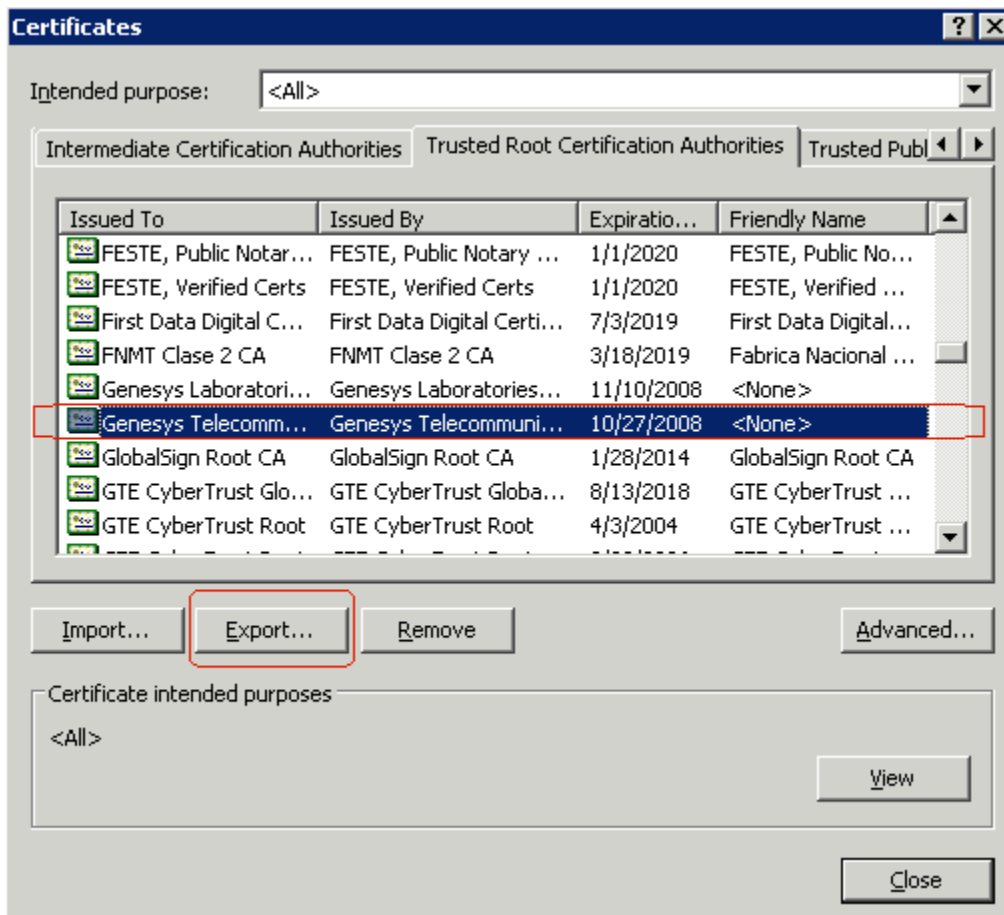
- Exporting the trusted certificate from the Lync / Skype for Business host.

Exporting the Trusted Certificate from the Lync Skype for Business Host

Prerequisites

- A valid certificate to authenticate the OCS server has been installed as part of the domain configuration. This can be obtained using internal Certificate Authorities (CA), a domain configuration utility, or from a third party (for example, Verisign), according to your security policy.

1. On the host computer for Microsoft OCS, open Internet Explorer.
2. Go to Tools > Internet Options > Content > Certificates and select the Trusted Root Certification Authorities tab.
3. Highlight the certificate that has been issued to this host computer, then click Export.



4. When you are prompted to do so during the export operation, under Export format, select DER Encoded Binary x.509 (*.cer).

5. When asked to enter a name for the certificate, enter any useful name. There are no mandatory formats. For example, if you enter `UCC_certificate`, the export operation will create a file called `UCC_certificate.cer`.

Next Step:

- Adding the certificate to the UC Connector installation.

Adding the Certificate to the UC Connector Installation

Prerequisites

- The trusted certificate has been exported from the Microsoft OCS host computer.


1. Copy the certificate that you created in Exporting the trusted certificate from the Lync / Skype for Business host.

2. Place this certificate in the `JDK\bin` directory of your prerequisite JDK installation.

3. From the `JDK\bin` directory, run the following command:


```
keytool -import -alias "certificate_name" -file <certificatefile.cer> -keystore  
<output_file.jks>
```

For example, `keytool -import -alias "ucc-cert" -file UCC_Certificate.cer -keystore UCC_store.jks`

 Take note of the password that was generated during the keytool process. You will add this later to the Command Line Parameters of the UC Connector application.

- `-alias`—Enter an alias for the certificate. It can be anything; there are no restrictions.
- `-file`—Enter a file name of the exported certificate.
- `-keystore`—Enter the name of the file that will be created as a result of running this keytool command.

4. Place this file in a logical location. For example: `<ucc_root>\etc\MYSTORE.jks`.

 Take note of the location where you save this file. You will need to add a parameter for this path to the Command Line Arguments of the UC Connector application.

Next Step: Creating the Configuration File for Kerberos Security

Creating the Configuration File for Kerberos security

1. If Kerberos is not already configured for your environment, on the UC Connector host computer, navigate to the `etc` folder in the installation directory and open the sample `krb5.conf` file. For example, the default path to the `etc` folder would be: `C:\GCTI\`

UCConnector\<your_UC_Connector>\etc


2. Modify the krb5.conf file with the following information:

```
[libdefaults]
    default_realm = YOUR-OCS-DOMAIN.COM
#    default_checksum = rsa-md5
[realms]
    YOUR-OCS-DOMAIN.COM = {
        kdc = SERVER1.YOUR-OCS-DOMAIN.COM
    }
[domain_realm]
    .your-ocs-domain.com = YOUR-OCS-DOMAIN.COM
```

The following table provides more information about the parameters used in this file.

| Parameter | Description |
|----------------|---|
| default_realm | Set this option to the OCS domain as per the UCC setup. This is used in cases where a user in Active Directory is configured without a specified domain. For example, in cases where clients are connecting from computers that are not part of the domain. |
| [realms] | This is a list of all the domain names included in the OCS environment. |
| kdc= | Set this option to the FQDN or IP address for the Key Distribution Center (KDC), typically the same computer hosting the domain or domain controller. |
| [domain_realm] | Use this to map domains to realms in which Kerberos authentication is running (typically used in multi-domain environments). In our sample, the realm .your-ocs-domain.com is mapped to the domain YOUR-OCS-DOMAIN.COM. |

3. Save the krb5.conf file.

 Take note of the location where you save this file. You will need to add a parameter for this path to the Command Line Arguments of the UC Connector application.

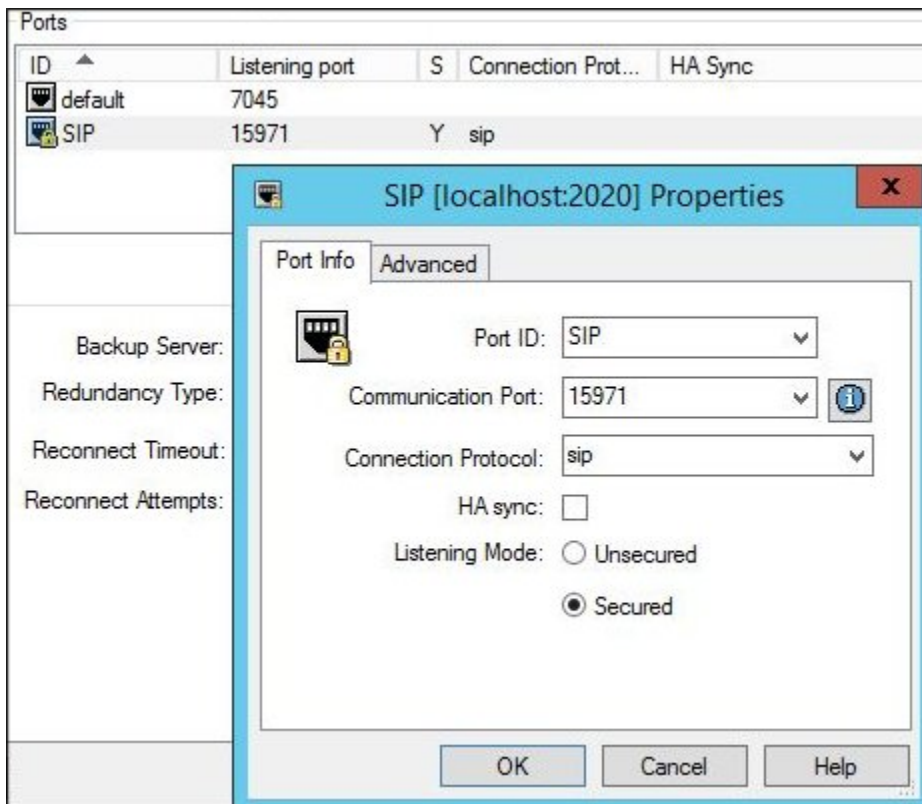
Configuring a Secure SIP Port

Purpose: To configure the UC Connector Application object to connect to Lync / Skype for Business using a secure port.

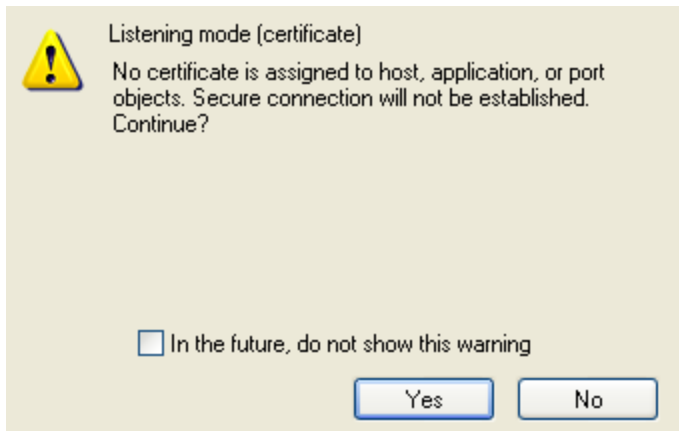
Lync / Skype for Business requires a secure connection for communication with UC Connector.

1. In the UC Connector Application object, on the Server Info tab, add a new port for SIP communication with Lync / Skype for Business.

- Port ID—Enter a useful name for this port.
- Communication Port—Enter the SIP communication port to be used. Any free port on the UC Connector host may be used.
- Connection Protocol—Select sip from the drop-down list.
- Listening Mode—Select the Secured option.



2. On adding this port, you may see the following Warning. For this configuration, you can ignore this warning. Click Yes to continue.

**Next Steps:**

- For TLS/Kerberos, continue at Modifying Command Line Parameters for TLS.
- For Mutual Transport Layer Security (MTLS), continue at Modifying Command Line Arguments for MTLS. Or go back to Modify Command Line Arguments for MTLS.

Modifying Command Line Parameters for TLS

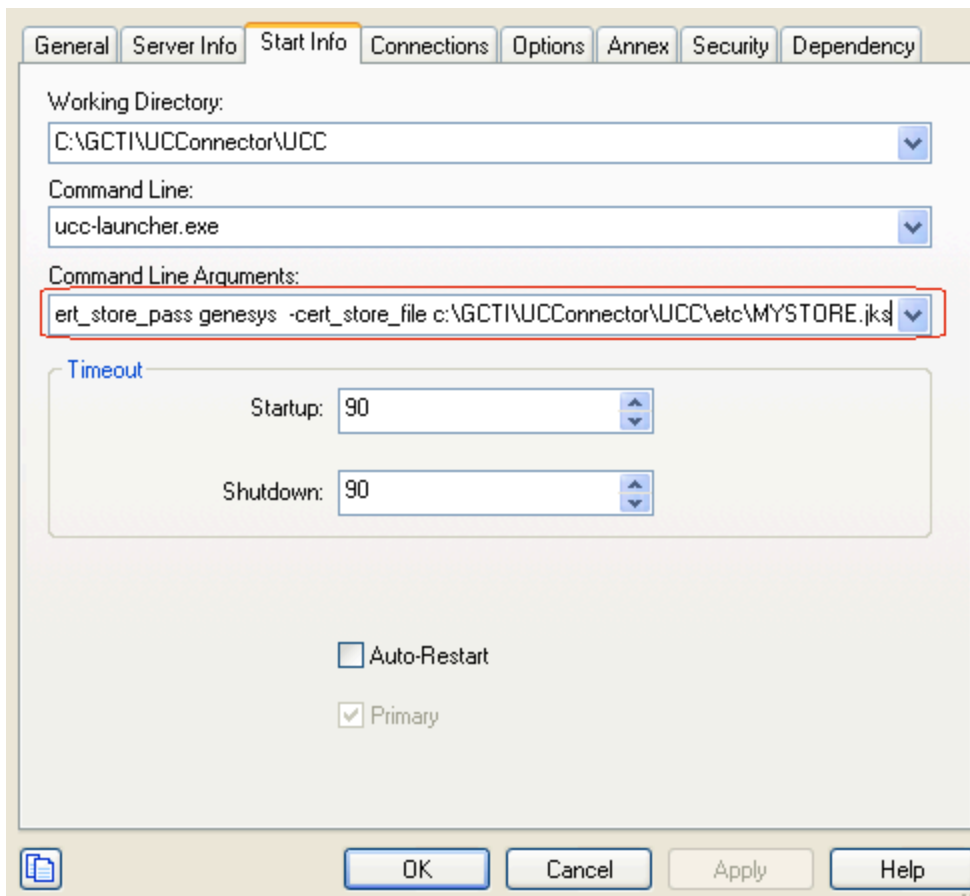
Prerequisites

- You noted the password that you created in Adding the certificate to the UC Connector installation.
- You noted the file location where you placed the keystore file in Adding the certificate to the UC Connector installation

1. Go to Start Info tab > Command Line Arguments in the UC Connector application.

2. Add the following parameters to the existing command line argument:

- -krb_conf_file <path to krb5.conf file>
- -cert_store_pass <password generated in Add certificate file to the UC Connector Installation>
- -cert_store_file <path to keystore file moved in Add Certificate File to the UC Connector Installation>



3. Click OK to save.

Configuration Options

This section describes the configuration options that are modified during Lync / Skype for Business integration. Options are organized according to component type, and include the following:

- [UC Connector Application Options](#)
- [SIP Server Options](#)

Tip

For a complete list of all UC Connector options, see the *UC Connector 8.0.3 Deployment Guide*.

UC Connector Application Options

Options specific to Lync / Skype for Business integration are listed below.

UC-Connector Section

GLA refers to the Genesys Lync Agent.

- `gla-call-match-window`
- `gla-kpl-time`
- `gla-kpl-response-time`
- `presence-gateway-mode`

Microsoft-OCS Section

The Microsoft-OCS section of the UCC Application object contains the options that allow integration with Microsoft Lync and Skype for Business. Note that the name of the section refers to an older Microsoft product (the Office Communications Server); however, the options govern the integration with the newer Microsoft UC platforms.

- `agent-status-ready`
- `agent-status-notready`
- `agent-status-logout`
- `contact`
- `presence-acw-note`
- `presence-acw-status`
- `presence-lg-note`
- `presence-lg-status`
- `presence-sync-mode`
- `registrar-uri`

SIP Server Configuration Options

Certain SIP Server options need to be configured for Lync / Skype for Business integration. No changes have been made in SIP Server to integrate with Lync / Skype for Business; however, a specific configuration is necessary. For detail on these options, see [SIP Server Configuration](#).

Genesys Component Configuration for Lync Interoperability

This section describes the Genesys components that are configured for UC Connector Lync integration to work properly.

- [SIP Server Configuration](#)
- [UC Connector Configuration](#)
- [Interaction Workspace Plug-in for Lync](#)
- [Current Limitations](#)

SIP Server Configuration

This section describes the list of **SIP Server** options that need to be configured for Lync / Skype for Business integration. No software changes are necessary in SIP Server in order to integrate with Lync / Skype for Business; however, a specific configuration is necessary as described below.

Set up MSML-Enabled Treatments

Set the following configuration option on the SIP Server Application level:
`TServer\msml-support = true`

Enable 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`

Disable Early Media Support

In integration with Microsoft Lync / Skype for Business, early media support should be disabled in the SIP Server. For details, see **Current Limitations**.

On the SIP Server Application level, set the following configuration option:
`TServer\sip-enable-100rel = false`

Set Softswitch Properties

Purpose: To set up a softswitch DN for Lync or Skype for Business.

A softswitch 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 Skype for Business Enterprise Agent's Phone number, with no sections added to them specifically.

These options are configured in **Genesys Administrator** under the **Switch > DNs** associated with a SIP Server. For detailed information on these options, consult the **SIP Server Deployment Guide**.

Under the **Options** tab, select **Advanced View (Annex)** and add the following options:

- `TServer/contact`—The contact should point to the Mediation Server host and port, which by default

uses port 5068 for TCP transport, and port 5067 for TLS transport.

- `TServer/dual-dialog-enabled`—The dual-dialog setting should be set to `false`. As with most PSTN devices, 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 consultation call INVITE message without the SDP.
- `TServer/make-call-rfc3725-flow`—The call flow should be set to 1, to make third-party call control calls without sending an initial INVITE with the black hole SDP to the Mediation Server.
- `TServer/refer-enabled`—The REFER support is set to `false`, to make the RFC 3725 call flow effective.
- `TServer/reuse-sdp-on-reinvite`—The Mediation Server does not 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`.

Create 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.

These options are configured in Genesys Administrator under the Switch > DNs associated with a SIP Server. For detailed information on these options, consult the [SIP Server Deployment Guide](#).

Under the Options tab, select `Advanced View (Annex)` and add the options as shown below:

- `TServer/contact`—The contact should point to the Mediation Server host and port, which by default uses port 5068 for TCP transport, and port 5067 for TLS transport.
- `TServer/dual-dialog-enabled`—The dual-dialog setting should be set to `false`.
- `TServer/make-call-rfc3725-flow`—The call flow should be set to 1.
- `TServer/prefix`—A string should contain any characters allowed in a user part of the SIP URI (according to RFC 3261). When configured on a Trunk DN, the value of this option is used by SIP Server to select the proper Trunk for an outgoing call. For each available Trunk, SIP Server compares the value of this option with the initial characters of the call's destination name; the Trunk with the longest possible match is selected.
- `TServer/refer-enabled`—The REFER support is set to `false`, to make the RFC 3725 call flow effective.
- `TServer/reuse-sdp-on-reinvite`—The Mediation Server does not 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`.

Create a DN for MSML VoIP Service

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

These options are configured in **Genesys Administrator** under the Switch > DNs associated with a SIP Server. For detailed information on these options, consult the ***SIP Server Deployment Guide***.

Under the Options tab, select Advanced View (Annex) and add the following options:

- TServer/contact—The contact should point to the Resource Manager IP address and port.
- TServer/cpd-capability—This should be set to mediaserver.
- TServer/make-call-rfc3725-flow—The call flow should be set to 1.
- TServer/prefix—This should be set to msml=.
- TServer/refer-enabled—The REFER support is set to false, in order to make the RFC 3725 call flow effective.
- TServer/ring-tone-on-make-call—This should be set to false.
- TServer/service-type—This should be set to msml.
- TServer/subscription-id—This should be set to the name of the tenant to which SIP Server switch belongs.

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 Skype for Business. Additional and more advanced recording capabilities can be configured, but were not tested officially during the qualification tests.

These options are configured in Genesys Administrator under the Switch > DNs associated with a SIP Server. For detailed information on these options, consult the ***SIP Server Deployment Guide***.

Under the Options tab, select Advanced View (Annex) and add the following options:

- TServer/contact—The contact (SIP URI) should point to the recorder server.
- TServer/request-uri—The value of the Request-URI address to be used in the INVITE message, if that address is different from the address where the message will be sent.
- TServer/service-type—The service type is set to recorder.

Create a Routing Point DN

When a call is made from a Skype for Business Client to a SIP Endpoint, the call progresses through the Skype for Business Server and lands on a SIP Server's Routing Point.

Create a DN of type Routing Point and set the Register property to true.

UC Connector Configuration

The Genesys UC Connector is used in integration with Lync / Skype for Business to provide presence synchronization of users, who act as contact center agents for the Genesys solution. To do this, UC Connector subscribes to the Lync / Skype for Business 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 Front End Server notifies Genesys when there are any status changes to the Microsoft presence status of Agents.

Configure UC Connector for the Front End Server

Purpose: To configure UC Connector to register with the Front End Pool and Subscribe for Lync / Skype for Business Users.

Prerequisites:

- [Generating the Client Certificate](#)
- One of the following:
 - [Generating the Server Certificate Using Skype for Business Management Shell](#)
 - [Generating the Server Certificate Using Microsoft Management Console or CA Web Access](#)

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 / Skype for Business User URI.

- For example:

`sip:lync_user1@lync-domain.com`

3. Set the value of the Microsoft-OCS\registrar-uri option to the IP address or FQDN of the Front End Pool.

4. Click the Configuration tab. In the Command Line Arguments field, and add following information:

```
-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>" -key_store_type pkcs12
```

Note:

- <client_certificate_path>—location of the client certificate created in [Generating the Client Certificate](#).
- <client_certificate_password>—the client certificate password created in [Generating the Client Certificate](#).
- <server_certificate_path>—location of the server certificate created in either [Generating the Server Certificate Using Skype for Business Management Shell](#) or [Generating the Server Certificate Using Microsoft Management Console or CA Web Access](#).
- <server_certificate_password>—the server certificate password created in either [Generating the Server Certificate Using Skype for Business Management Shell](#) or [Generating the Server Certificate Using Microsoft Management Console or CA Web Access](#).

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 / Skype for Business Enterprise Edition.

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

Important

In order to provide the correct security certificates for different Front End Servers in the same Pool, the certificate keystore must contain two (or more) entries corresponding to each of the Front End Servers in the same Pool.

1. Export the pfx (pkcs12) files from both Front End Server hosts using mmc on Windows (for example, certificate1.pfx and certificate2.pfx). During the export a password will be specified for each file (for example, pwd1 and pwd2).

2. Import the files from Step 1 into a new keystore with a new password (for example, pwd_final):

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

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

```
Type: keytool.exe -importkeystore -v -srckeystore certificate2.pfx
```

```
-destkeystore final_certificate.jks -srcstoretype pkcs12  
-deststoretype jks -srcstorepass pwd2 -deststorepass pwd_final
```

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

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

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

3. Start UC Connector with the following arguments in command line:

- for java keystore:

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

- for pkcs12 keystore:

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

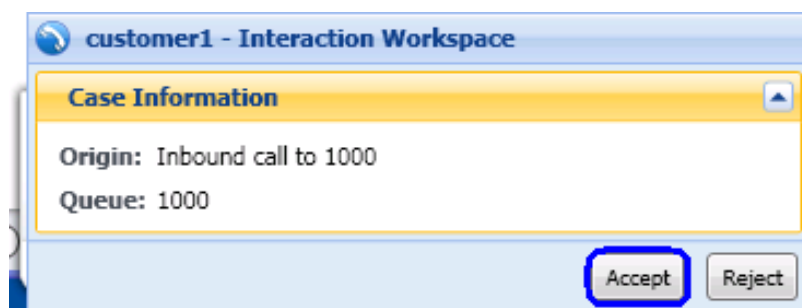
Important

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 / Skype for Business must be in the same subnet.

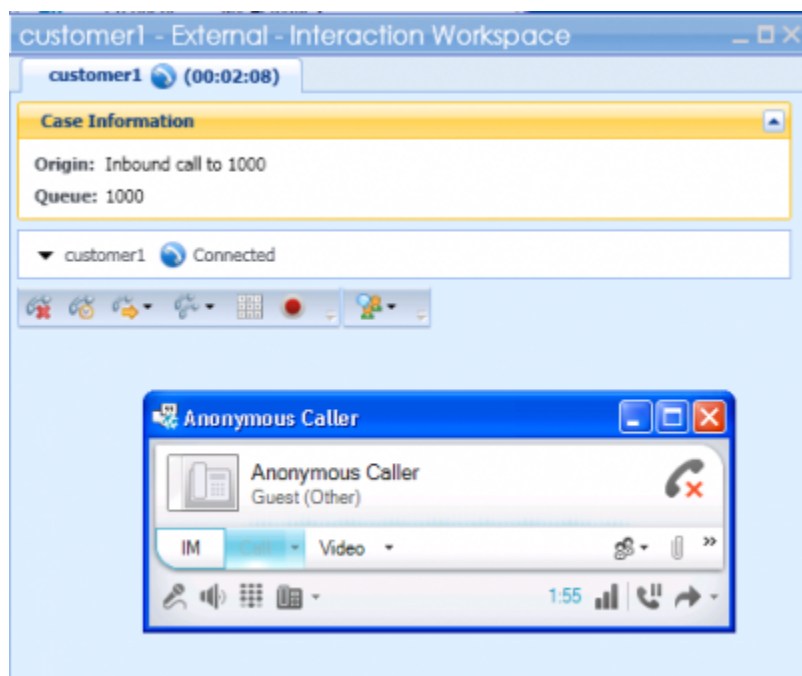
Workspace Plugin for Skype for Business

Workspace Desktop Edition (formerly Interaction Workspace), the Genesys agent desktop application, includes a **plugin** for Lync / Skype for Business. This plug-in is distributed through the UC Connector CD, since UC Connector is necessary for integration with Lync / Skype for Business.

Installation of this plug-in is mandatory for an Agent deployed with Lync / Skype for Business Integration. The plug-in exercises the Lync Client SDK locally to allow answering calls from the Workspace GUI.



In effect, the Answer Call Interaction Workspace toast, shown above, implements a first-party call control answer command on the Lync / Skype for Business Client residing in the same host. Clicking it also opens up the Workspace Call Control window.



Current Limitations

This section describes the current limitations in the SIP Server integration with Microsoft Lync / Skype for Business.

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 or Skype for Business desktop clients as soft-phones for voice communication.

This Genesys deployment does not interoperate with Lync- or Skype for Business-supported IP hard phones, such as Polycom CX series. Use of these phones has the following limitations:

- The AnswerCall option through Interaction Workspace cannot be used to answer the call on the a physical 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 Workspace-based 3pcc call control through should be used.

Early Media support should be disabled

When a SIP User Agent supporting Early Media (such as the SIP Server) contacts the 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/Skype for Business Client— this call is Early Media enabled. When the Client responds with its Early Media SDP, the Mediation Server attempts to update the UAC with the Client's Early Media SDP; however, the 2nd 183 Session Progress response does not contain an incremented RSeq header value—the UAC doesn't process it. This is not compliant with the RFC 3262 guideline.

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

Conversation Extension Window

The Conversation Extension Window functionality does not work when using the Skype For Business client on the Knowledge Worker desktop.

Genesys Lync Agent

Genesys Lync Agent (GLA) is a piece of software that allows the use of Microsoft Lync or Skype for Business for voice interactions, 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 / Skype for Business 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 or Skype for Business Enterprise Voice.

Workspace Desktop Edition Alternative

Genesys Lync Agent runs on the same machine as the Microsoft Lync / Skype for Business Client, communicating with UC Connector to allow agents to answer incoming calls and perform call control. This is an alternative to installing Workspace Desktop Edition on the agent's computer, with the Workspace plug-in for Lync / Skype for Business. Genesys realizes that not all of its customers can use Workspace, either because of previous architecture choices or because of environment constraints. While the Workspace plug-in controls communication with the local Lync / Skype for Business client and runs some call control commands through it, without it there is a need to at least answer calls from the Genesys desktop – since the Lync / Skype for Business client does not allow remote answer commands.

Genesys Lync Agent solves this problem by accepting remote call control commands and executing them using the Microsoft Lync Client SDK (which also works with the Skype for Business Client). 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 SDK call.

Interface to UC Connector

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

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.

Localization

Genesys Lync Agent supports the following languages:

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

Deploying Genesys Lync Agent

This section describes the steps required to deploy the Genesys Lync Agent.

Prerequisites

- UC Connector 8.0.301.04+ is installed.
- SIP Server 8.1.0.001+ is installed.
- The Lync / Skype for Business client has been installed, and operates correctly.
- The Lync Client SDK redistribution has been installed.
- A valid desktop to connect to the Genesys environment exists.

Preparation

Prepare the UCC Solution

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:
-

| 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, in milliseconds, 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 Microsoft-OCS section, configure the following option:

| 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. |

For more information about these options, see the *UC Connector 8.0.3 Deployment Guide, Configuration Options*.

5. Click Save.

Install Genesys Lync Agent

Install Genesys Lync Agent

1. On the UC Connector 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.
3. In the final Installation Complete page, click Finish.

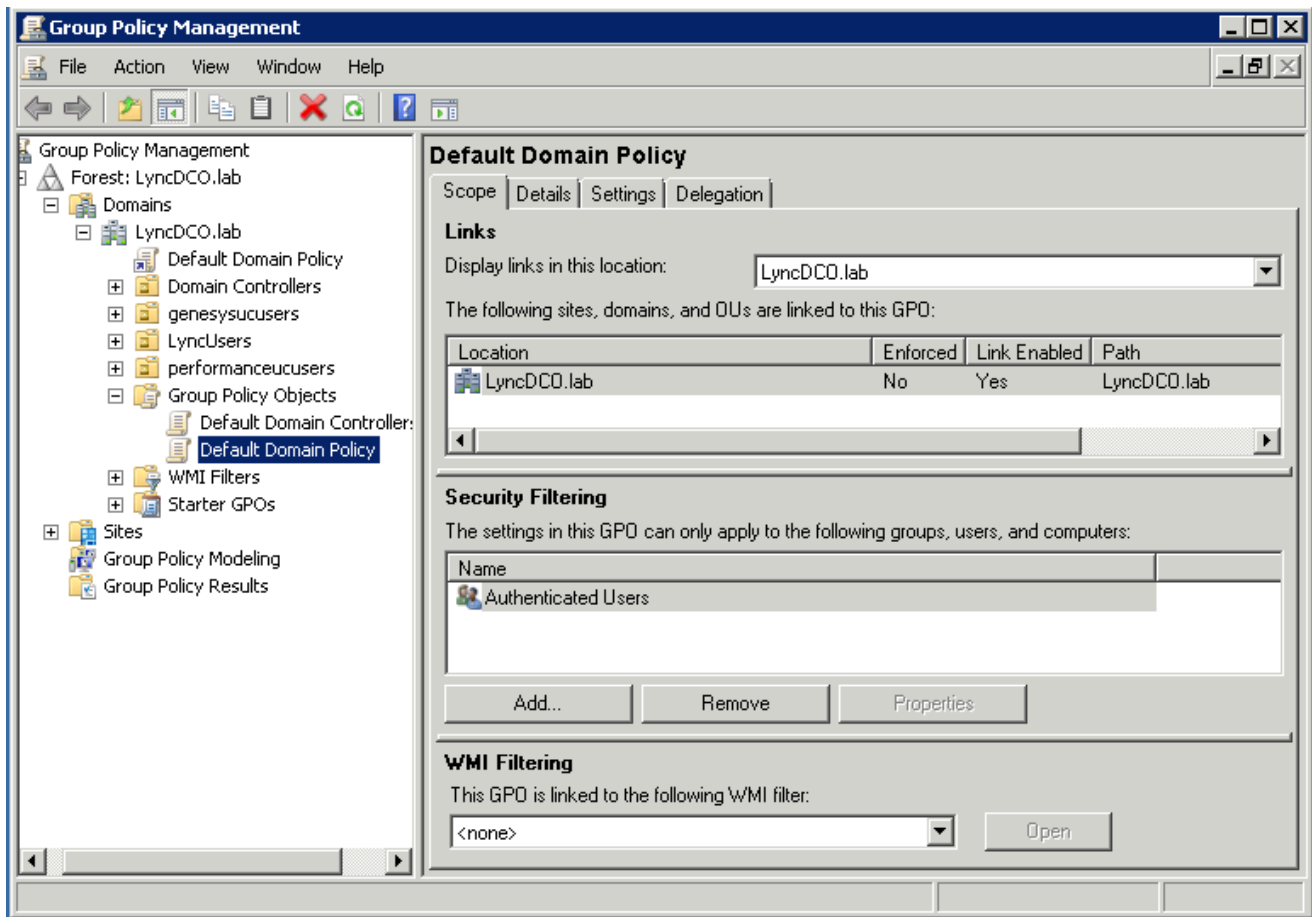
Set Host and Port

Set Host and Port for Lync Agent 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.

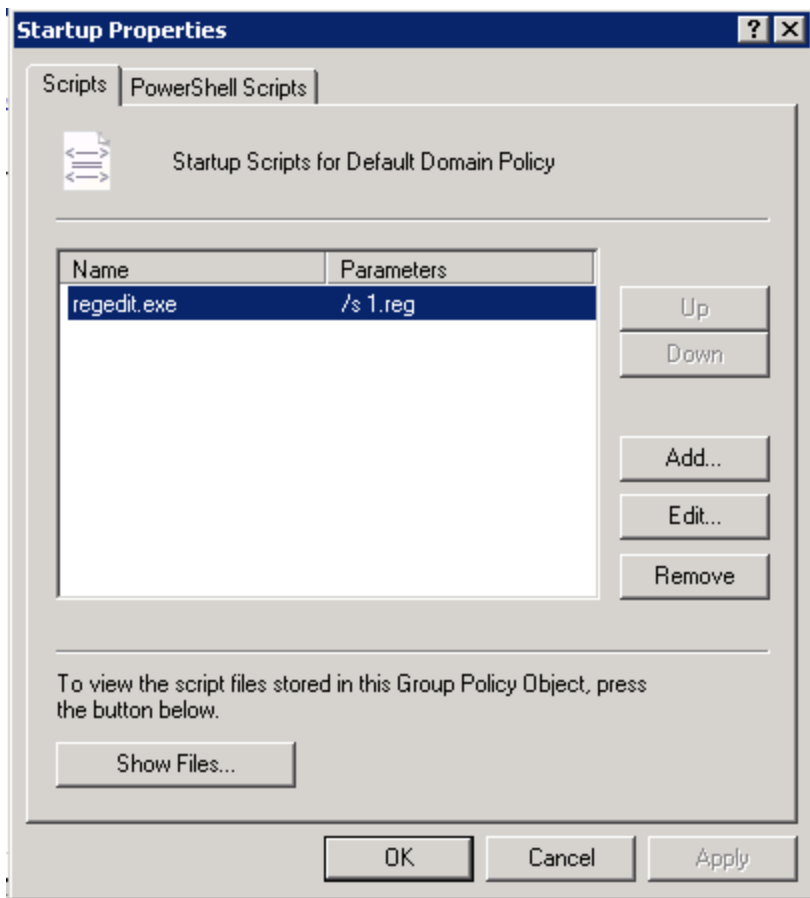
Set up Administrator Access to the Domain Controller

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



Run Script When the Computer Starts Up

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



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

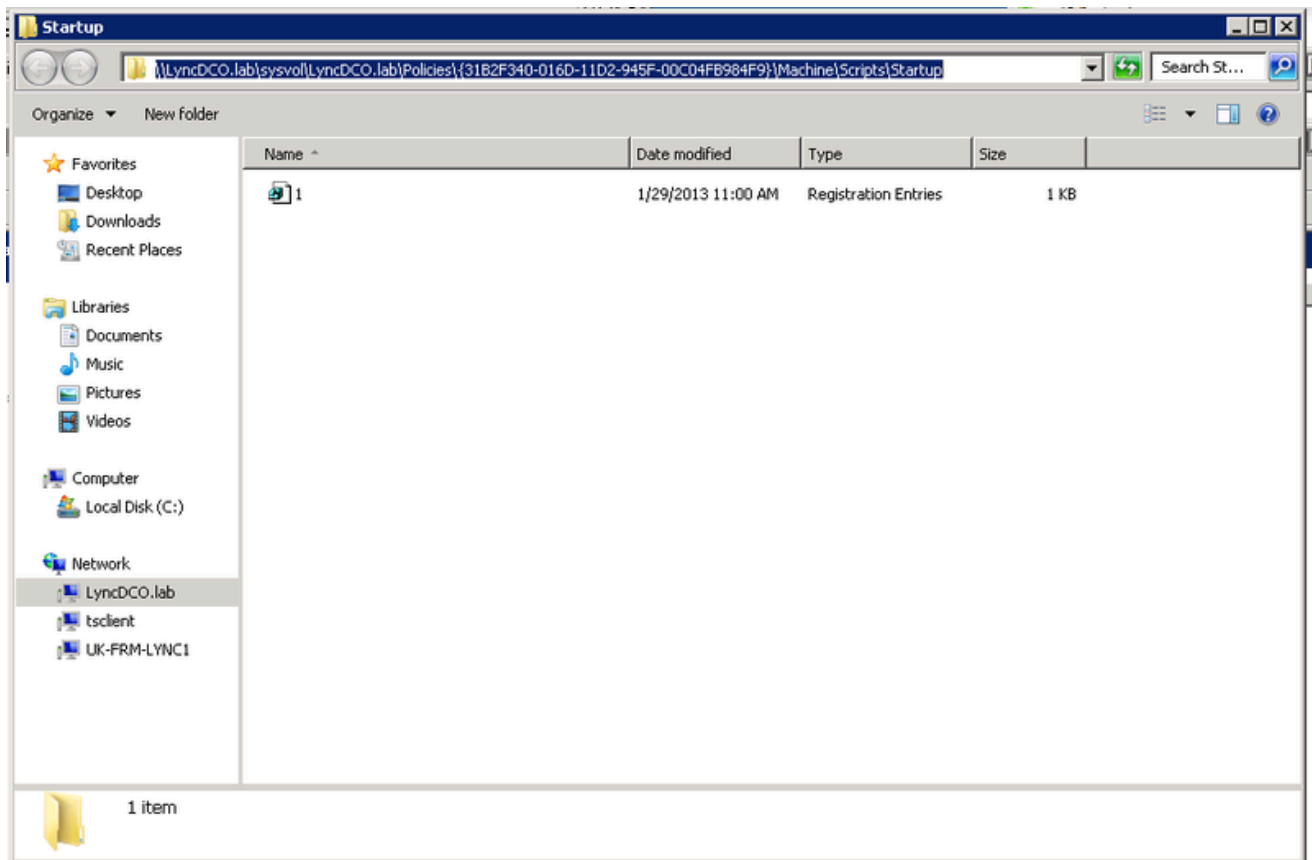
[HKEY_LOCAL_MACHINE\SOFTWARE\GCTI]

[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

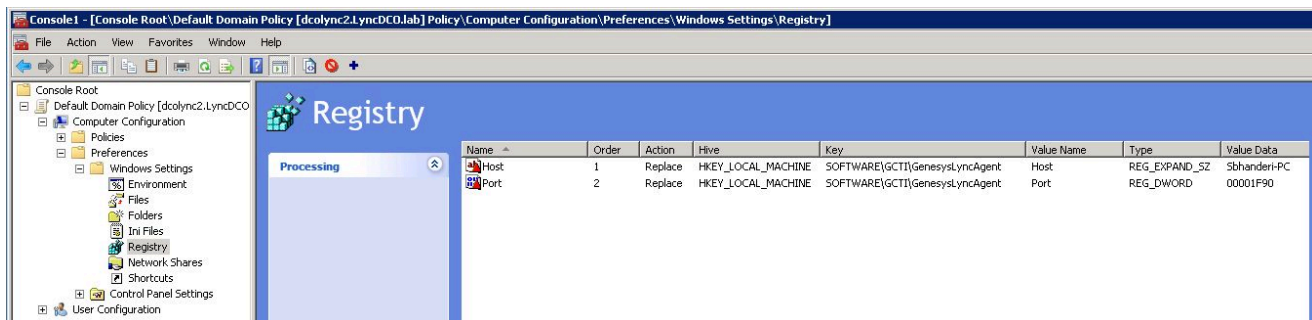
"Port"=dword:00001f90

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



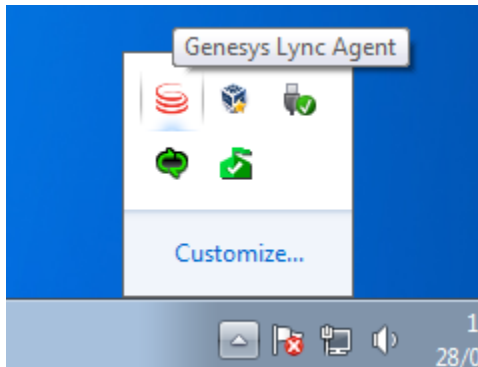
Change registry entries directly

1. Select Computer Configuration > Preferences > Windows Settings > Registry.
2. Add the entries as shown in the figure below (click to expand):

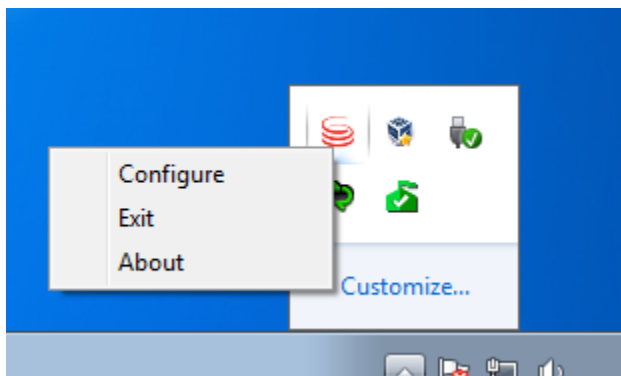


Using Genesys Lync Agent

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



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

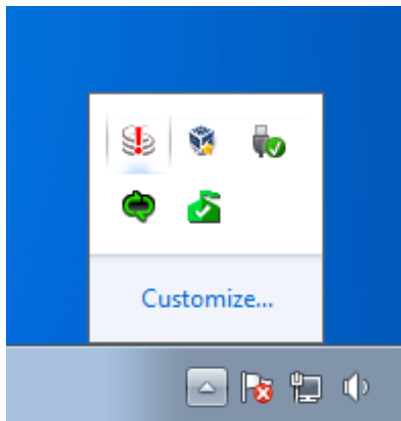


- Configure—Opens GLA.
- Exit—Terminates GLA.
- About—Displays details about GLA.

Connecting to UC Connector

How GLA Connects to UC Connector

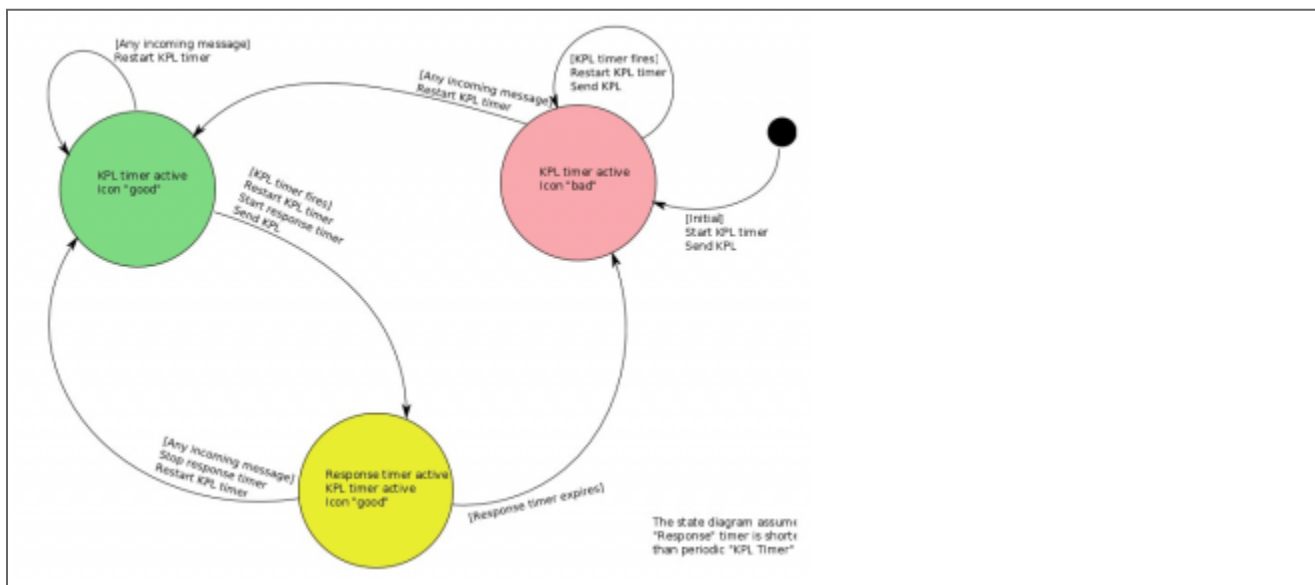
At the start, GLA tries to check the connection to UC Connector by sending a "test" message. If successful, UC Connector acknowledges the message and the tray icon changes to indicate the results of the test.



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 this GUI is closed, the heartbeat process will be restarted.

Heartbeat (Keep Alive) to UC Connector

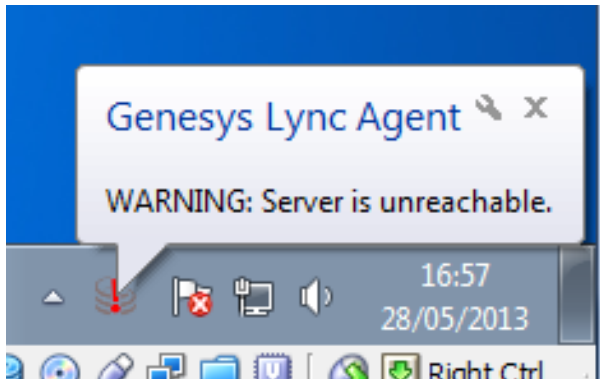
The UC Connector option `gla-kpl-time` is set to 30 seconds, which is the heartbeat rate. The UC Connector option `gla-kpl-response-time` is set to 4 seconds, the time in which a response must be received.



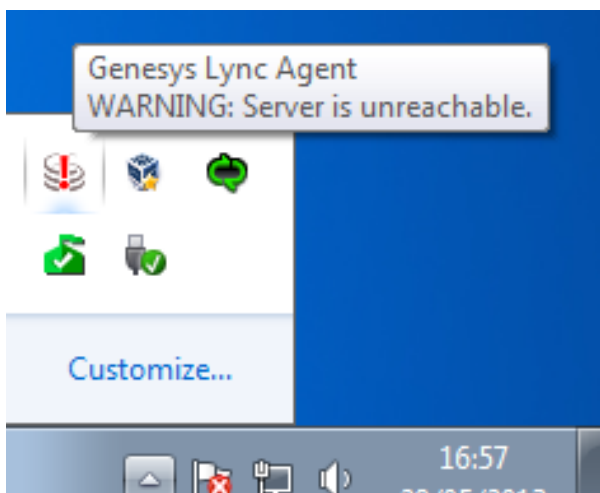
This diagram shows how the keep alive mechanism interacts with UC Connector.

Heartbeat Failure

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



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



Understanding Controls

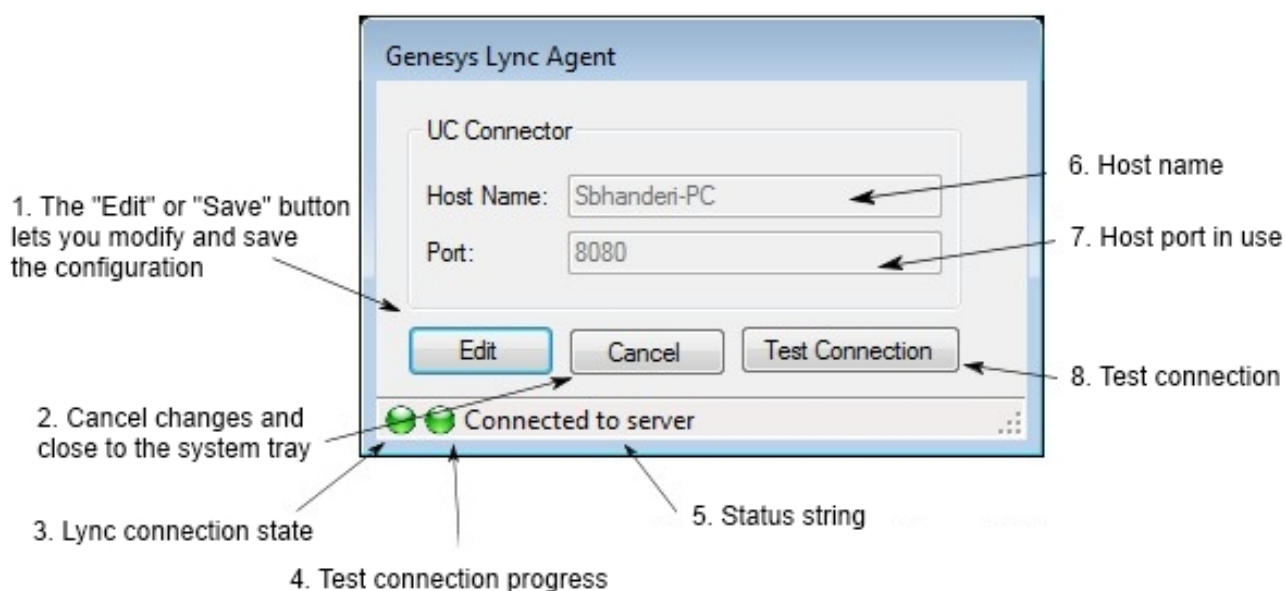
Understanding GLA Window Controls

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

- Business client is not started.

- The Lync / Skype for Business 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.

The Genesys Lync Agent dialog box is shown below.



The numbers below are keyed to the above diagram.

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 / Skype for Business Client connection state. The icon is green if GLA is connected to the Client. The icon is red if:

- The Lync / Skype for Business client user is not logged in.
- The Lync / Skype for Business client is not started.
- Genesys Lync Agent cannot connect to the Lync / Skype for Business 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 / Skype for Business 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 / Skype for Business 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.

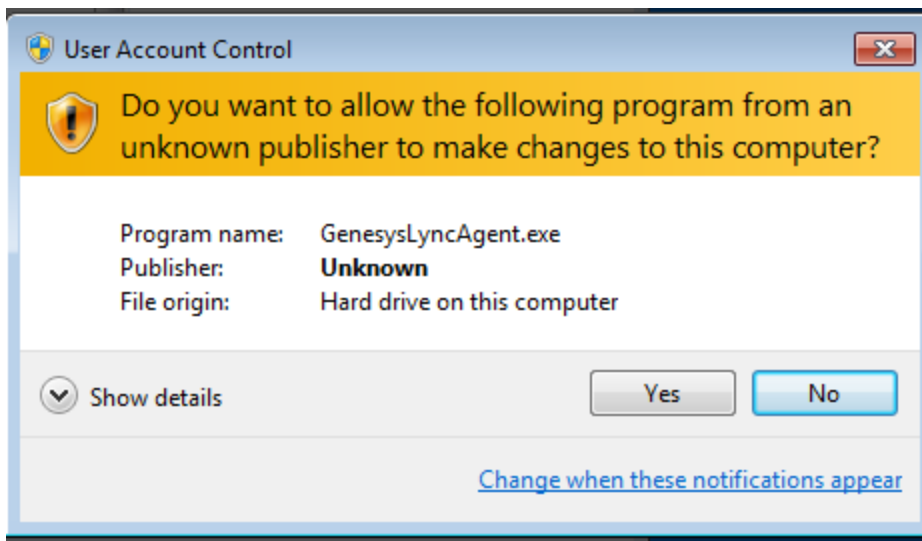
Warning

The Lync / Skype for Business client must be running and the user must be logged in before attempting to test the connection.

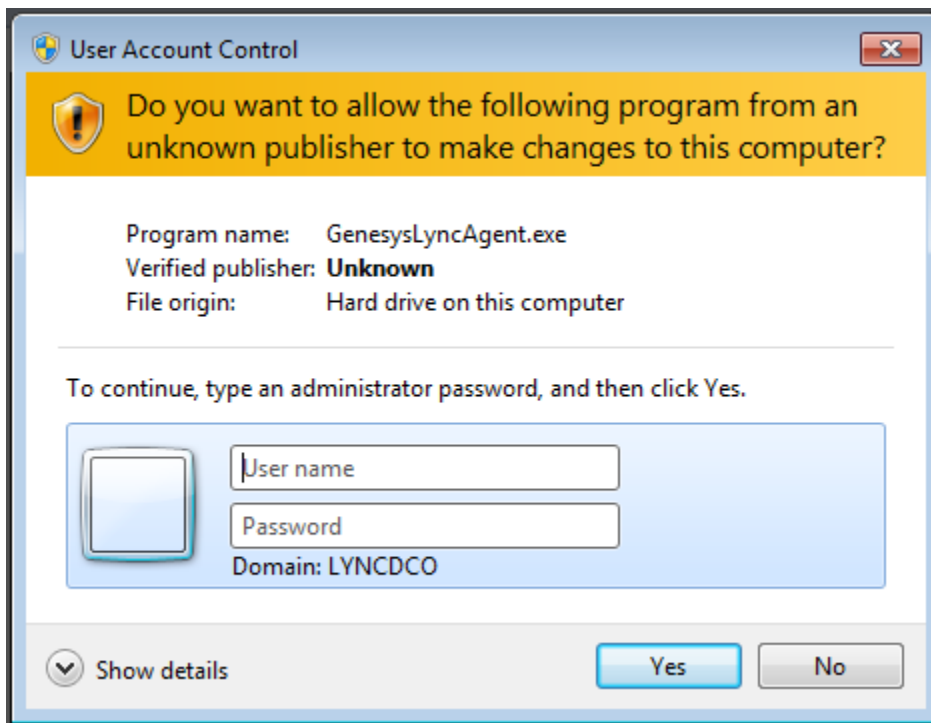
Modifying the Host and Port Entries

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.
- 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.



Important

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.