



ALTIGEN
COMMUNICATIONS

410 East Plumeria Drive • San Jose, CA 95134
www.altigen.com • +1 (408) 597-9000

MaxACD for Lync/Skype Release 6.5.8

Upgrade Guide

November 30, 2015



AltiGen Communications, Inc.
679 River Oaks Parkway, San Jose, CA 95134
Telephone: 888-AltiGen (258-4436) Fax: 408-597-9020
E-mail: info@altigen.com | Web site: www.altigen.com
Copyright © AltiGen Communications, Inc. 2015. All rights reserved.



Contents

Introduction	5
Operational Notes	5
New Features in Release 6.5.8	6
Requirements	7
Server Requirements	7
MaxAgent Requirements	8
VRM (Voice Recording Manager) Requirements	8
MaxReports Requirements	8
Architecture	9
Changes from MaxACD 6.5.7	10
Upgrade from MaxACD 6.5.7 to Release 6.5.8 on Lync 2010	11
Step 1: Make a Backup.....	11
Step 2: Create a New Trusted Application Pool on the Lync Server.....	11
Step 3: Install the Server SDK Proxy on each Lync Front-end Server.....	12
Step 4: Check Each Lync Front-end Server's Firewall Exception List	14
Step 5: Make the MaxACD System a Lync Application Server	15
Step 6: Install MaxACD 6.5.8.....	20
Step 7: Install the UCMA Application Service on the MaxACD System	23
Step 8: Check the MaxACD System's Firewall Exception List	25
Upgrade MaxACD 6.5.8 From an Earlier Version of Lync to either Lync 2013 or Skype for Business	26
Overview of the Upgrade Process	26
Step 1: Plan and Prepare.....	28
Step 2: Make a Backup.....	29
Step 3: Create a New Trusted Application Pool on the New Platform	29
Step 4: Make the MaxACD System a Lync 2013/Skype for Business Application Server	30
Step 5: Install MaxACD 6.5.8.....	35
Step 6: Install the UCMA Application Service on the MaxACD System	38
Step 7: Check the MaxACD System's Firewall Exception List	40
Step 8: Perform a Restore on the New MaxACD System	41
Step 9: Register Your System Key in MaxACD.....	41
Step 10: Change the System ID on the new MaxACD System	41
Step 11: Check the External Logger Service	41
Step 12: Verify MaxACD Interaction with Lync 2013/Skype for Business	42
Step 13: Install the Server SDK Proxy on Each Lync/Skype Front-end Server	43
Step 14: Check Each Lync/Skype Front-end Server's Firewall Exception List	45
Step 15: Configure Call Routing from Lync/Skype Server to MaxACD	46
Step 16: Configure Outbound Workgroup Call Rules.....	49
Step 17: Move Users to the New Platform and Adjust User Voice Policies	51
Step 18: Reconfigure Altigen Applications.....	51



Step 19: Remove Connections to the Original MaxACD System 51

Troubleshooting 52

Performance..... 53

Introduction

This guide provides instructions for the following tasks:

- Upgrading a MaxACD 6.5.7 installation to MaxACD 6.5.8 (page 11)
- Upgrading a MaxACD installation from Lync 2010 to Lync 2013, or from Lync 2013 to Skype for Business 2015 (page 26)

This guide does not include instructions for performing a first-time installation of MaxACD. If you are installing MaxACD for the first time, follow the instructions in the *MaxACD for Lync Release 6.5.8 Deployment Guide*.

Operational Notes

- MaxAgent cannot see (and does not display) calls that do not route through the MaxACD server.
- Personal caller ID is not displayed in MaxSupervisor.
- Supervisors can record*, silently monitor, barge in, or coach two types of calls:
 - » Inbound PSTN workgroup calls.
 - » Outbound PSTN calls made through an agent's extension with an outbound workgroup configured.
- * Supervisors cannot record on demand when "Auto-record to central location" has been enabled for that workgroup.
- Only single-call handling is available for agents. This means that an agent cannot receive a new workgroup call by placing an existing workgroup call on hold. The current call must be completed, transferred, or otherwise handled before the agent will be able to handle a new workgroup call.
- When a workgroup call is transferred out of MaxACD, it becomes a personal call.
- Conference calls are logged as personal calls.
- Statistics are calculated from the active server only. Because of this, after a redundancy switchover occurs, group statistics values will restart from zero.
- In MaxReports, if you want to export the charts in reports 1301 through 1304 and reports 2301 through 2319, generate the reports in PDF format. The Excel reports do not support those charts.
- In MaxAgent, if an agent is already on a call, the agent cannot click the Pickup button to pick up a queued call. This is because only single-call handling is available.
- In a configuration with multiple Lync Front-end servers, if one FE server goes down, calls may intermittently fail. This happens because the Front-end servers are each listed in the DNS, and when calls go through MaxACD, the server will still try to connect to the FE server listed in the DNS table.
- If you change the password for Manager Extension, you will break the connection to MaxReports.
- If an agent's outbound workgroup call status does not appear in MaxAgent, check the URI configuration for that extension:
 - » The extension's URI must match the URI configured in Lync and in Active Directory
 - » The Mediation Service IP must match the FQDN configured in MaxAdministrator
- When an agent's presence is set to Busy, any outbound call will be considered a non-workgroup call. Because of this, extension Caller IDs will not be transmitted; the system trunk number or main number will be used for the call.

- If an agent tries to blind transfer a workgroup call to an invalid trunk number, the agent may not hear an error tone. In addition, the trunk call and the held party may both drop, leaving the agent no indication that the transfer failed. Because of this possibility, we recommend that agents use the supervised transfer method instead of performing blind call transfers.
- If an agent does a supervised transfer using the secondary pop-up window, and the transferred call is routed to a voice messaging number (either directly or indirectly), the transfer may not be handled properly. If this occurs, a message will be displayed indicating that the transfer did not complete. We recommend that agents transfer calls using the primary (first) pop-up window instead of the secondary window.
- Caller ID is not updated when users make supervised federated transfers. In other words, the call will show the Caller ID of the transferring agent, not the Caller ID of the original inbound call.
- Do not change Workgroup call distribution settings during peak call hours. If you do, it may affect system performance.
- If a MaxAgent client fails to auto-update, this can be the result of a redundant environment where the two servers are running different builds of MaxACD.

To ensure that both the active server and standby server are on the same build, follow this process:

1. Update the standby server to the new version.
 2. Switch MaxACD control to the standby server.
 3. Update the other server to the new version. If you like, you can switch control back to the original server.
- If you must uninstall the AltiGen Lync Proxy, we recommend that you stop the AltiGen Proxy service beforehand. If you do not stop the service first, you will need to restart the MaxACD server afterwards.
 - If your deployment is on Lync Server 2013, and a Lync Front-end server is restarted, MaxAgent will not be able to play workgroup voicemail. This situation occurs, because the AltiGen UCMA Proxy server is no longer connected to that Front-end server. To resolve this issue, restart the AltiGen UCMA Proxy service.
 - If you experience issues in a configuration where multiple mediation servers are behind a hardware load balancer, consider adding a registry entry for the mediation IP addresses. This way, MaxACD will read the registry and add those IP addresses to the matching list.

New Features in Release 6.5.8

The following enhanced features are included in this release:

- Lync 2013 support. MaxACD now supports the following Lync configuration:
 - » A Lync 2010 environment
 - » A Lync 2013 environment
 - » A Skype for Business 2015 environment
 - » A mixed Lync 2010/2013 environment **that is deployed on a Lync 2013 server.**
- Windows 8 (32-bit and 64-bit) support for client applications.
- A method for customizing workgroup greetings via AltiGen Custom Phrase Manager.
- A new AA choice lets you forward calls to a SIP address.



- A new Customer Relationship Management (CRM) Integration seat license. See the separate guide, *Application Notes: Salesforce.com Configuration for MaxACD*, for details.
- A new Workgroup voicemail indicator in MaxAgent.
- New Lync Presence mapping – You can now map Lync presence states to agent *Ready* or *Not Ready* states. When the Lync Presence state is changed, the agent state will be changed accordingly.

For example, if the agent changes his or her Lync Presence to *Busy*, the agent's state will be changed to *Not Ready* and no workgroup calls will be sent to this agent. When the agent's Lync Presence is changed back to *Available*, the agent state changes to *Ready* and the agent will receive workgroup inbound calls again. Lync presence mappings are configured in MaxAdministrator, under **Call Center > Agent Activity**.

Note: Do not set *Ready* or *Not Ready* in the Agent Presence Mapping window if you want agents to have full control of the *Ready/Not Ready* state.

- Agents are now automatically logged out of workgroups when they close MaxAgent.
- Users must enter the appropriate workgroup numbers and passwords when they first log into MaxInsight and MaxSupervisor.
- MaxAgent now displays the Workgroup status window by default. In addition, the user interface has been simplified.
- MaxAgent and MaxSupervisor now minimize to the taskbar.

Requirements

This section lists the requirements your system needs in order to run MaxACD release 6.5.8; for Lync hardware and software requirements, refer to your Lync documentation.

Make sure that all AltiGen-approved Lync Server Cumulative updates (CUs) have been deployed on your system before you begin. Contact your AltiGen representative or Sales Engineer for this information.

Server Requirements

Server Hardware Requirements

Note: An Advanced Micro Devices (AMD) CPU does not support the instruction set necessary for HMCP.

- Dedicated Windows Server 2008 or 2008 R2 Standard running on a 64-bit, Quad-core Intel processor @2GHz, 4GB memory, 160GB hard drive.
- Virtual Server – VMware ESX 5.0 or 5.1, or Hyper-V 6.0.6002.18005. Allocate four Intel cores @ 2GHz each, 4GB memory, and 160GB hard drive.

Server Software Requirements

- MaxACD for Lync Release 6.5.8
- Microsoft Lync Server 2010 or 2013
- Microsoft 2010 or 2013 Mediation Server
- Microsoft Exchange 2010 with Unified Messaging (UM) installed (for voice mail integration). Make sure the Exchange and Outlook versions match. For example, you must use Exchange 2010 with Outlook 2010. You must install Microsoft Outlook on the MaxACD system. Only the 32-bit version of Outlook is supported.
- AltiGen Lync Server Proxy 6.5.8 (running on the Front-end Server and on the MaxACD Server)



MaxAgent Requirements

MaxAgent Client Hardware Requirements

- 2GHz CPU
- 1GB available hard drive disk space
- 2GB RAM
- SVGA monitor (1024 x 768) with 256 color display

MaxAgent Client Software Requirements

- MaxAgent for Lync Release 6.5.8
- Lync 2010 or 2013 client
- Windows XP Professional (32-bit only), Vista Business Edition (32-bit or 64-bit), Windows 7 (32-bit or 64-bit), or Windows 8 (32-bit or 64-bit)
- Microsoft .NET 3.5 framework

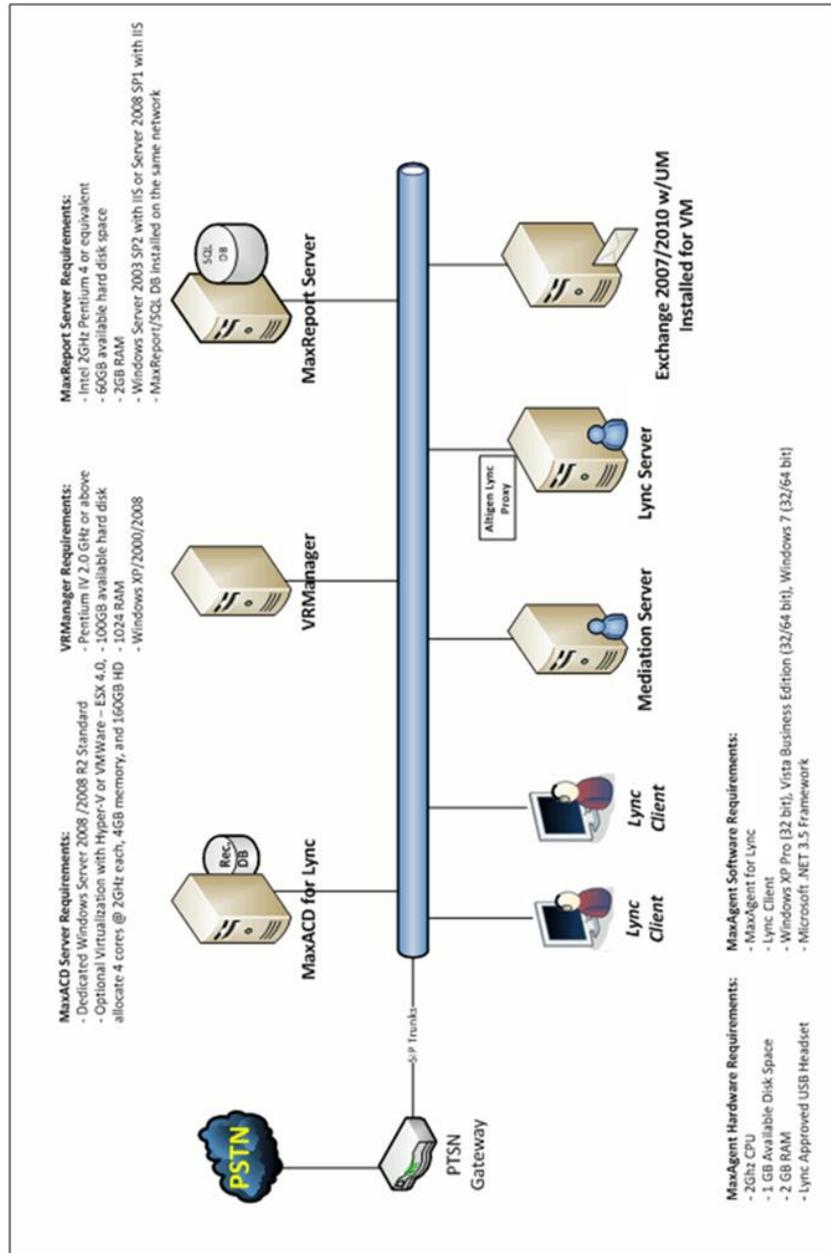
VRM (Voice Recording Manager) Requirements

- Windows Server 2003, 2008, or 2008 R2
- 2GHz CPU with 2GB RAM
- 100GB available hard drive disk space

MaxReports Requirements

- Windows Server 2003, 2008, or 2008 R2
- Intel 2GHz Pentium 4 or equivalent CPU with 2GB RAM
- 100GB available hard drive disk space

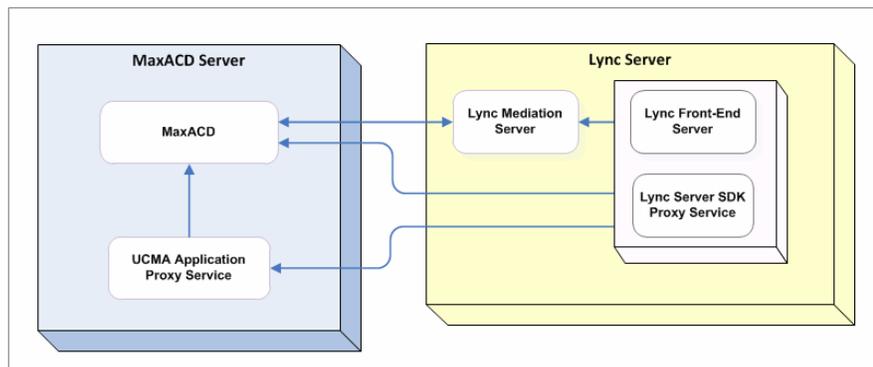
Architecture



Changes from MaxACD 6.5.7

One of the changes in MaxACD 6.5.8 was made in order to support Lync 2013. The MaxACD Lync Proxy Service has been divided into two separate services in release 6.5.8:

- **UCMA Application Proxy Service**, which provides Lync user presence information and is installed on the MaxACD server
- **Lync Server SDK Proxy Service**, which provides Lync user call information and is installed on each Lync Front-end server



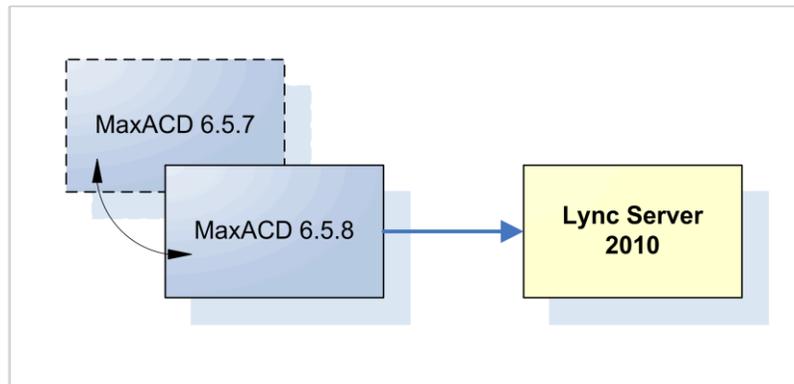
Both of these services are installed by the AltiGen Lync Proxy installation program.

There are various scenarios for upgrading from release 6.5.7 to release 6.5.8. These processes are described in the next few sections.

- To upgrade to MaxACD release 6.5.8 and stay on Lync Server 2010, follow the steps in the next section, starting on page 11.
- To upgrade a deployment of MaxACD 6.5.8 on Lync Server 2010 to Lync Server 2013, follow the steps on page 26.

Upgrade from MaxACD 6.5.7 to Release 6.5.8 on Lync 2010

To upgrade to release 6.5.8 and stay on Lync Server 2010, follow this process.



Step 1: Make a Backup

Make a backup of your MaxACD 6.5.7 system.

You can use the **Backup and Restore** utility to do this; refer to Chapter 23 of the *MaxACD Administrator Manual*.

If MaxACD is on a virtual machine, it is a good idea to take a snapshot of the image.

Step 2: Create a New Trusted Application Pool on the Lync Server

- 1 Log into the Lync Front-end server as a Domain user with Administrative privileges.
- 2 Open Lync Server and download the topology from your existing deployment.
- 3 Run **Topology Builder** and create a new Trusted Application pool.
- 4 Enter a name for this pool. It must be a unique FQDN (Fully Qualified Domain Name). This should be different from the FQDN of the server that will be added to the pool. For example, the server FQDN may be *max-proxy.company.com*, and the pool FQDN may be *max-pool.company.com*.
- 5 Choose **Multiple computer pool**, and then click **Next**.
- 6 The next page is where you add servers to the pool. You need to enter those servers where MaxACD will be running the Proxy role. Enter each server's FQDN and click **Add**. When you are done, click **Next**.
- 7 Select which front-end pool to use as the next hop, and then click **Finish**.
- 8 Publish the revised topology.

Step 3: Install the Server SDK Proxy on each Lync Front-end Server

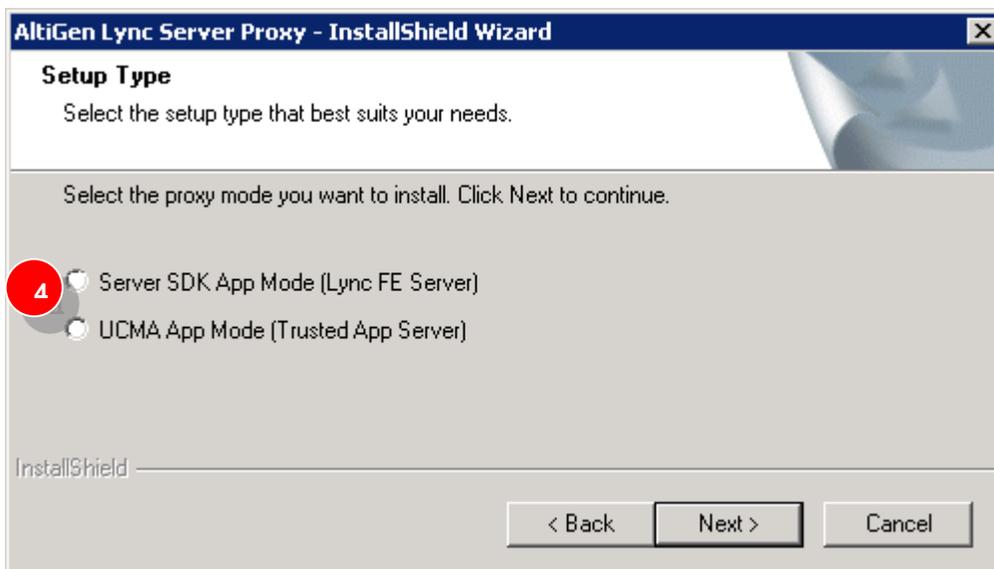
Note: If you have multiple Lync Front-end servers, then the Server SDK Application Proxy must be installed on each one.

The installation account must be a member of the following groups:

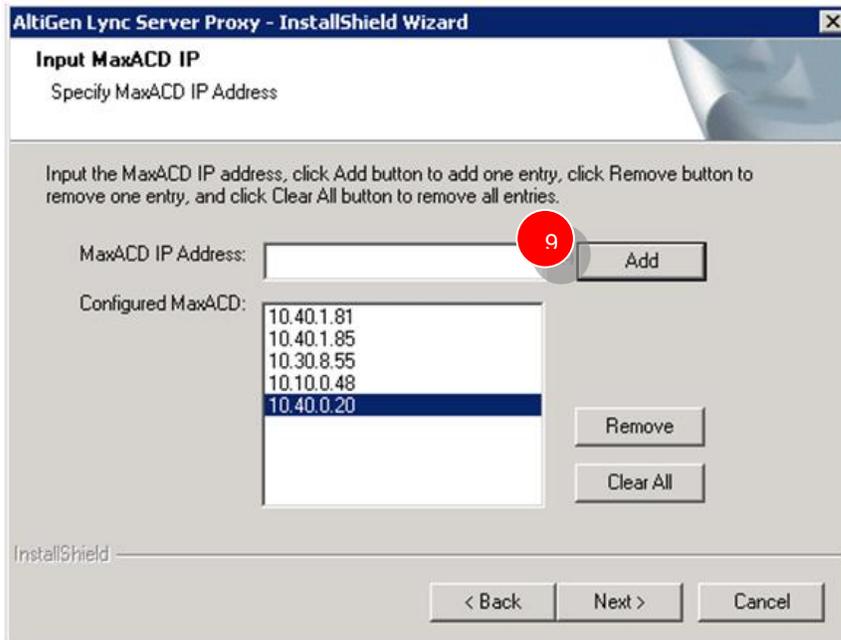
- *RTCUniversalServerAdmins*
- *Account Operator*

In addition, the installation account must be added to the *RTC Server Applications* group on the Lync Front-end server.

- 1 On the Lync 2010 Front-end server, stop the AltiGen 6.5.7 Lync Server Proxy service through Windows Services. Then uninstall the AltiGen Lync Proxy and remove the C:\AltiLyncServProxy folder.
- 2 Log in as a Domain user with Administrator privileges.
- 3 Insert the MaxACD Installation CD and in the **MaxACD Server > AltiGen Lync Proxy** folder, run *setup.exe*.
- 4 When prompted, choose **Server SDK App Mode (Lync FE Server)** and click **Next**.



- 5 Choose **Microsoft Lync 2010** and click **Next**.
- 6 When prompted, enter your user name and company name and click **Next**.
- 7 The setup wizard creates a user account and suggests a random password. If you choose not to use this password, enter a different one (up to 20 characters). Click **Next**.
- 8 We recommend that you accept the default installation location. Click **Next**.



9 Enter the MaxACD server IP address and click **Add**. To connect to multiple MaxACD servers, enter the IP address of each server. Click **Next** when you are done.

10 Enter the FQDN of the Lync Front-end Pool. Click **Next**.

Note: You can run `Get-CsSite` from the Lync Server Management Shell on this system to obtain this information.

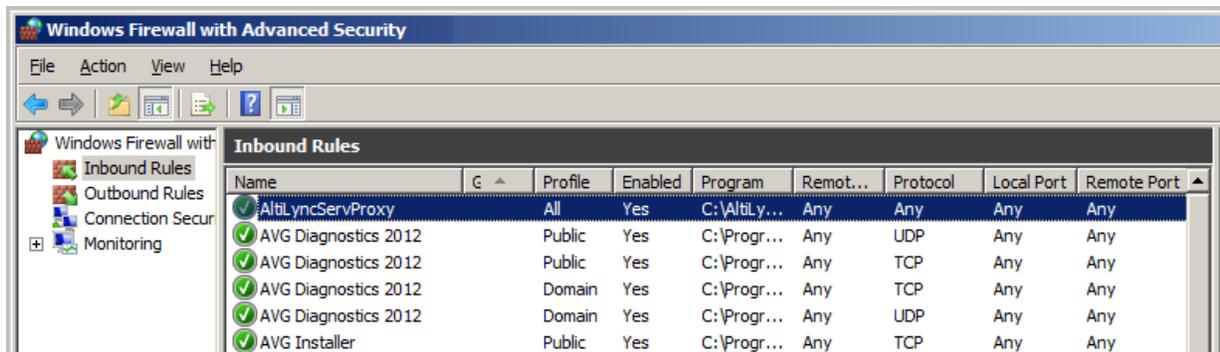
11 Click **Install**. After the process has finished, click **Finish**.

Note: If you need to change the IP addresses in the future, log in as a user with Administrative privileges and run this wizard again. To do this, in Windows, click **Start > All Programs**, then right-click *AltiGen Lync Server Proxy Configuration* and select **Run as Admin**.

Step 4: Check Each Lync Front-end Server's Firewall Exception List

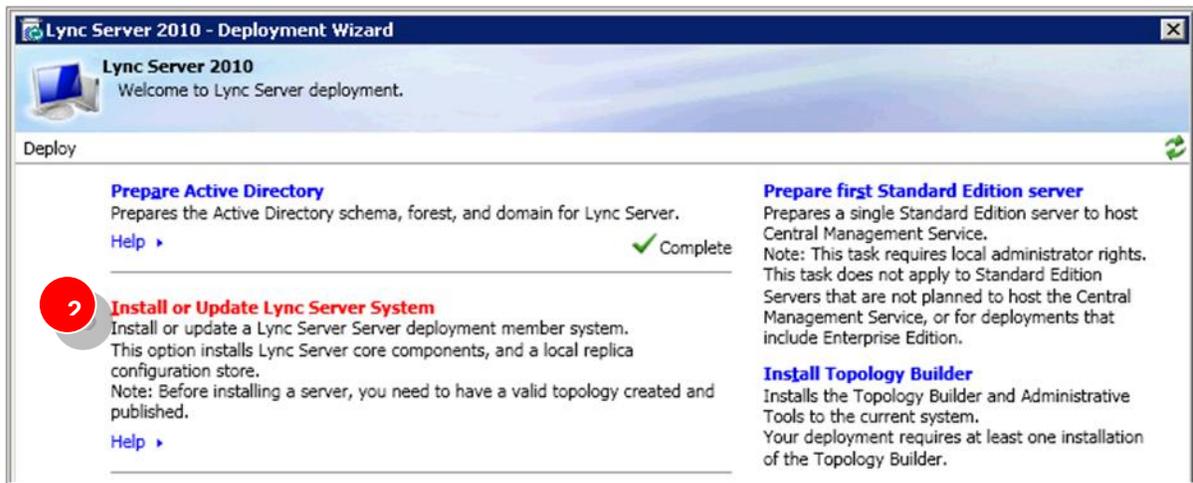
The installation program is designed to update the list of firewall exceptions on each Front-end server. You should confirm this list on each server. The steps may vary from one version of Windows to another.

- 1 On each Lync Front-end server, open Windows Firewall (found in the Windows Control Panel, in **System and Security**).
- 2 Click **Advanced Settings**.
- 3 Select **Inbound Rules**.
- 4 Check that the MaxACD system Components list has inbound routing rules established. If not, manually add a new rule.

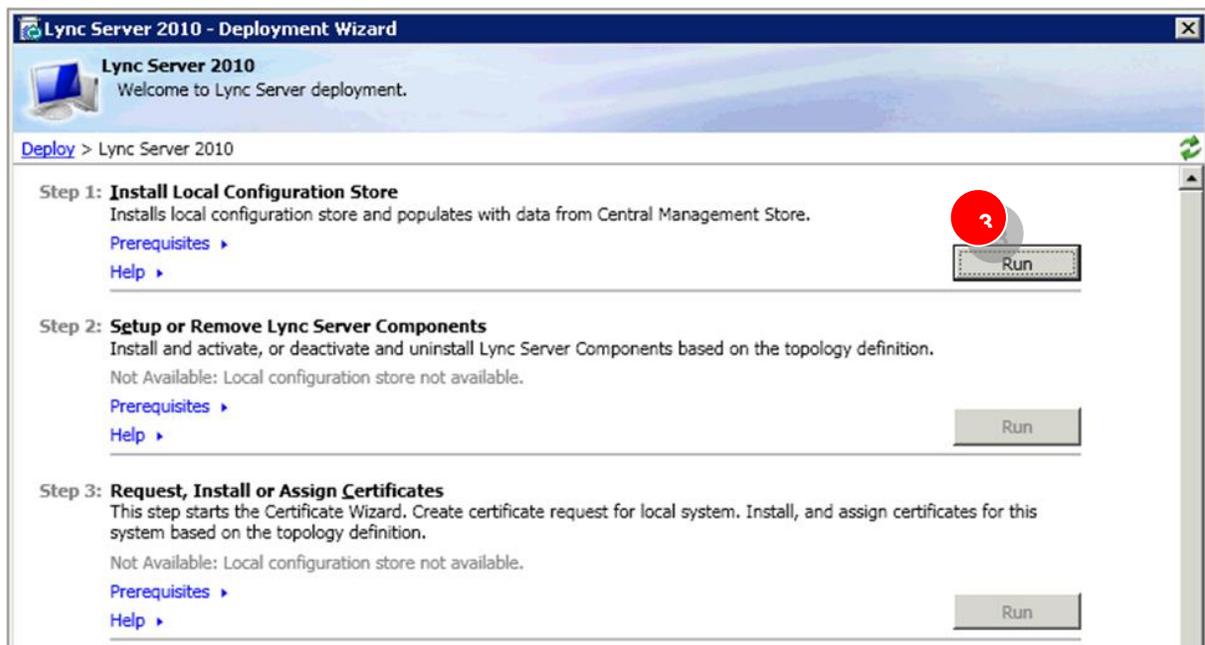


Step 5: Make the MaxACD System a Lync Application Server

- 1 On the MaxACD system, log in as a Domain user with Administrator privileges. Insert your Lync Server Installation CD and run *setup.exe*.
- 2 Choose **Install or Update Lync Server System**.



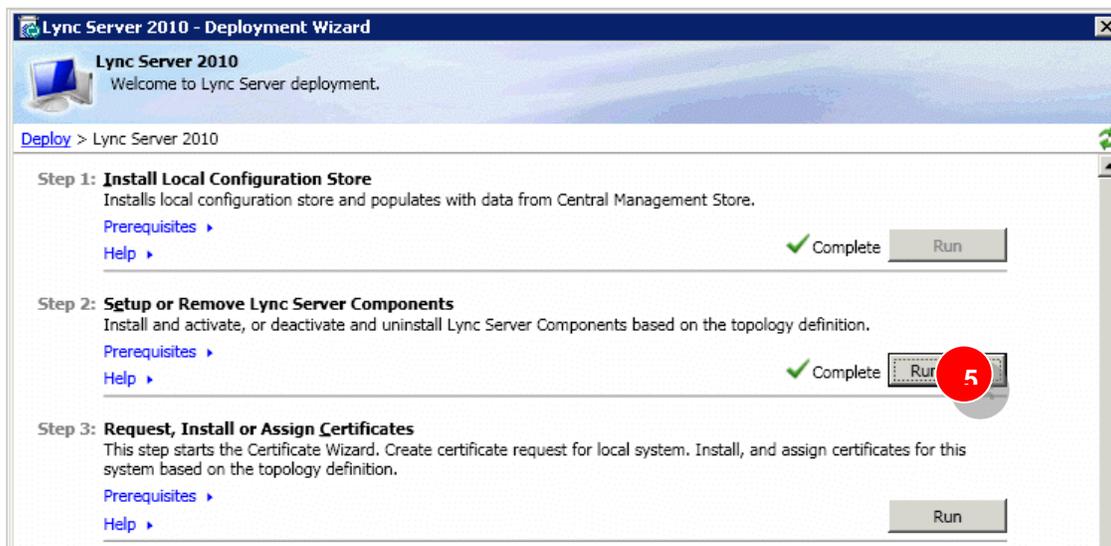
- 3 For "Step 1, Install Local Configuration Store," click **Run**.



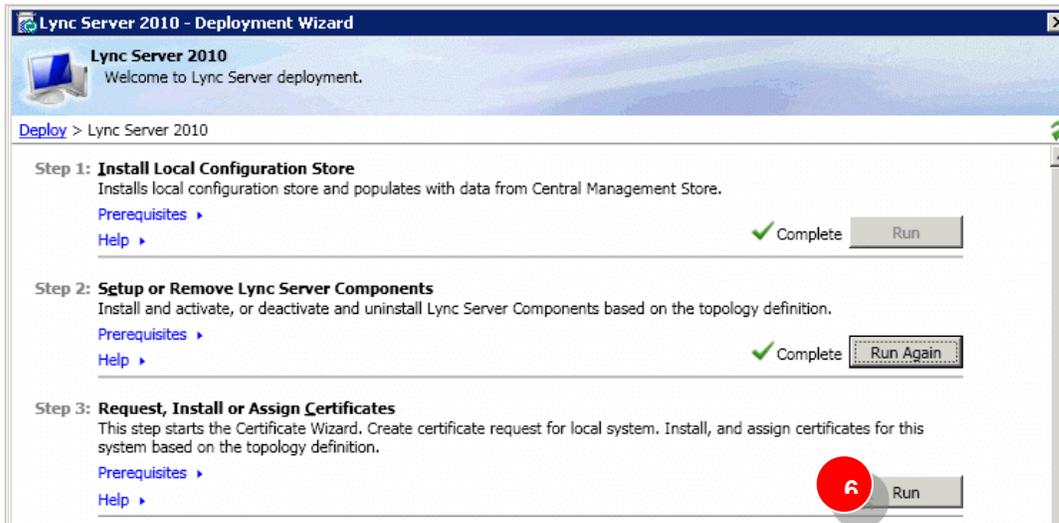
- On the next panel, choose **Retrieve directly from Central Management Store**, and then click **Next**. When processing has completed, click **Finish**.



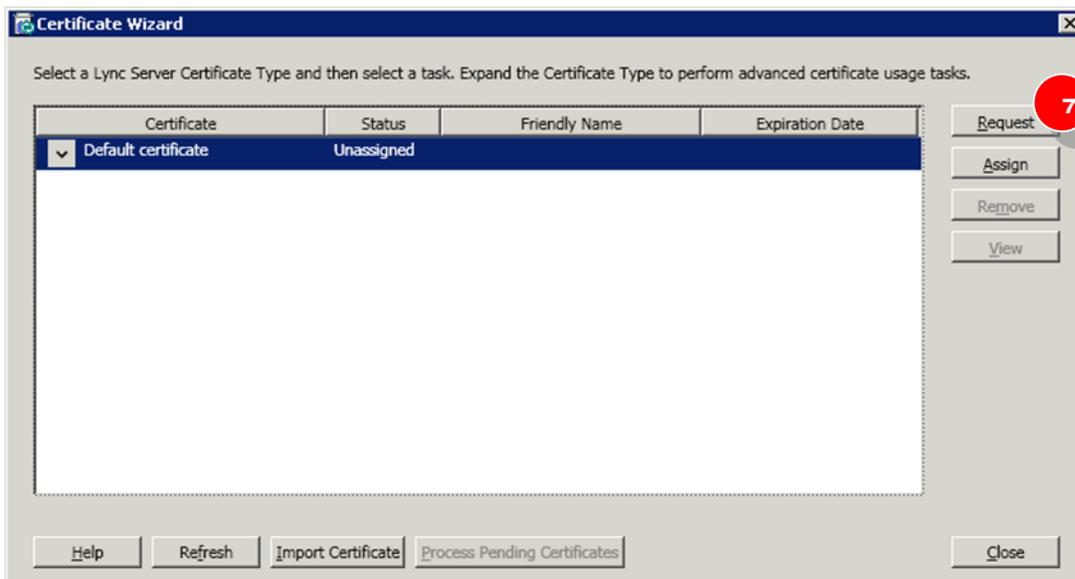
- You return to the main page. For “Step 2, Setup or Remove Lync Server Components,” click **Run** and then click **Next**. When processing has completed, click **Finish**.



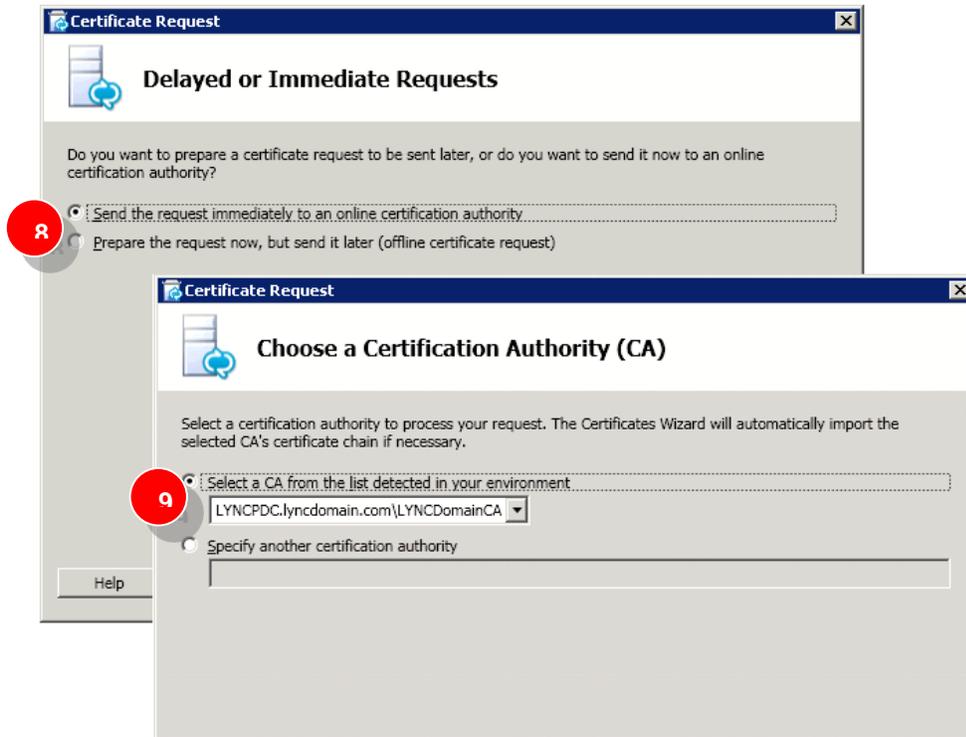
- When you return to the main page of the Wizard, for “Step 3, Request, Install or Assign Certificates,” click **Run**.



- In the Certificate Wizard, click **Request**, and then click **Next**.

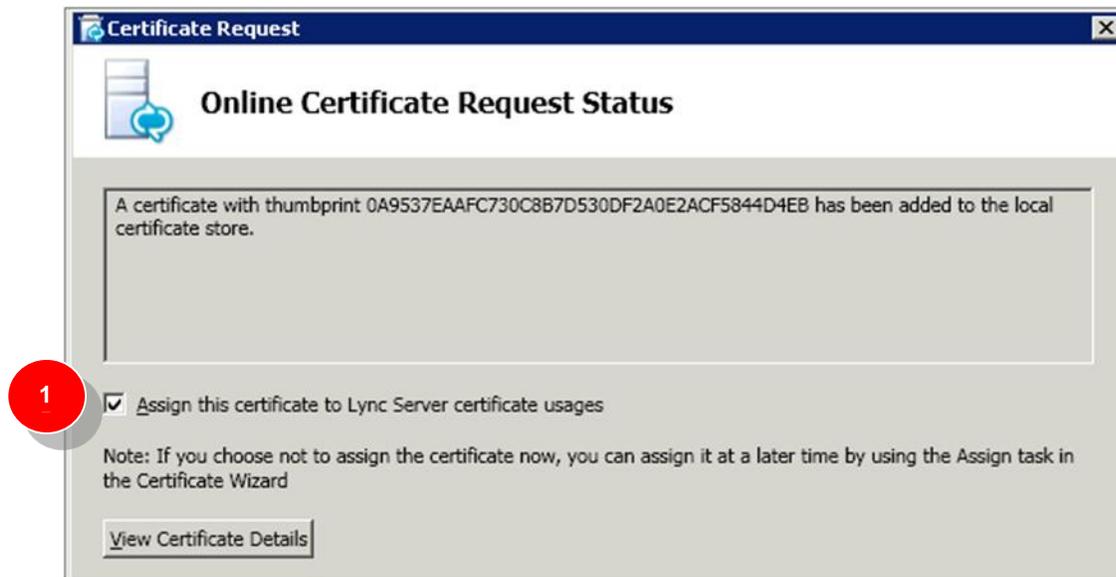


- 8 Select the “Send the request immediately...” option and click **Next**.



- 9 Choose a Certificate Authority (CA) from the list and click **Next**.
- 10 For the next two panels (*Certification Authority Account* and *Specify Alternate Certificate Template*), click **Next** to accept the default settings and continue.
- 11 When you reach the *Name and Security Settings* panel, enter a friendly name. Make sure that the bit length is set to **2048**, and that the **Mark Certificate Private Key As Exportable** checkbox is checked. Click **Next**.

- 12 Continue through the wizard panels. When you reach the *Geographical Information* panel, note that names cannot contain abbreviations.
- 13 Continue through the wizard panels. When you reach the *SIP Domain Setting on Subject Alternate Names* panel, check your SIP domain and click **Next**.
- 14 Continue through the wizard panels. When you reach the *Certificate Request Summary* panel, review all of the information carefully. If necessary, click **Back** to make any changes. When all of the information is correct, click **Next**. This starts the process of requesting the certificate.
- 15 When you reach the *Online Certificate Request Status* panel, we recommend that you check the box to assign the certificate (to save yourself a few steps). Click **Finish**, click **Next** twice, and then click **Finish**.



- 16 If you did not check the box in step 11, click **Assign** in the main Certificate pane and assign the certificate.
- 17 Close the Certificate wizard. When you return to the main page of the Wizard, for “Step 4, Start Services,” click **Run**, click **Next**, and click **Finish**.
- 18 At the bottom of the Deployment window, click **Run** to install any additional Lync updates, and then click **Exit** to close the Deployment wizard.

Step 6: Install MaxACD 6.5.8

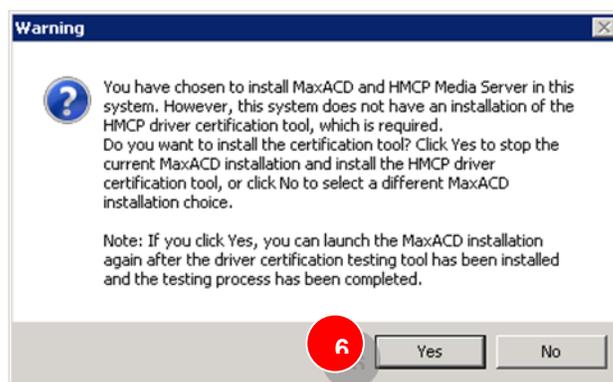
Follow these steps to install MaxACD. (You do **not** need to uninstall MaxACD 6.5.7.)

- 1 First, obtain a system key and license activation file from your account manager.
- 2 Log into the system as a Domain or Local user with local administrator privileges, and make sure that the server is already joined to the domain where your Lync Server is installed. If you plan to run Exchange Integration, you must have Domain administrator privileges.
- 3 Insert the MaxACD CD. In the **MaxACD Server > MaxACD for Lync** folder, run *setup.exe*.
- 4 Accept the license agreement, and continue to follow the instructions in the wizard.
- 5 When prompted, select a setup type:
 - **All-in-one (MaxACD + HMCP) System** – Select this if MaxACD will be operating on a single server. (This is the default configuration.)
 - **MaxACD Server with Separate HMCP Server** – Select this if the MaxACD server and HMCP servers will be running on different chassis in an enterprise deployment. You will select which components to install:
 - » **MaxACD Server** – Select this option to install MaxACD on the server. You will need a dongle for the MaxACD server.
 - » **HMCP Media Server** – If you have a small- to medium-size call center (no more than about 200 agents), you can install MaxACD and HMCP Media Server in the same machine. You can also install them in different machines, especially if you plan to grow your call centers.

If you have more than 200 agents, we recommend that you install the HMCP Media Server and MaxACD on two different servers.

- 6 Before installing the HMCP Media server, the installation program scans the system to determine whether the HMCP Certification Tool has already been installed on that system.

During an All-in-one installation, if the tool is not detected, you must either select **Yes** to install the Certification Tool and automatically restart the MaxACD installation, or select **No** to return to step 5 and select the other installation choice.



- 7 Continue through the remaining installation panels, entering information as prompted. During this process, the wizard will create a password account for Altigen services. We recommend that you accept this default password.

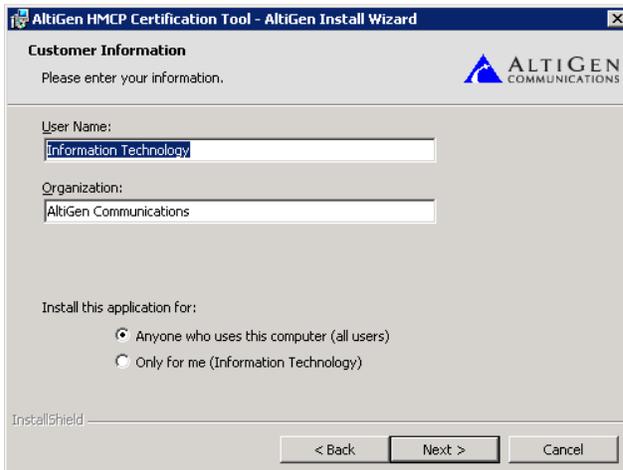
Note: If a window prompts whether to install KEYLOK during the installation process, click **Install**.
- 8 After the installation process has been completed, you must reboot the system.

Note: If you are using Exchange Integration, check the Exchange Integration Service to ensure that it has Domain Administrator privileges and that the service is running.

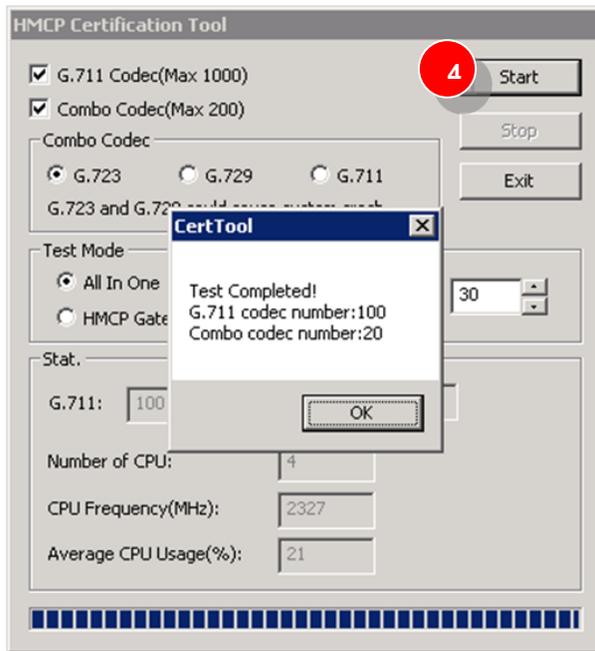
HMCP Certification Tool Installation

During installation, if you are prompted to install the HMCP certification tool, follow these steps:

- 1 Click **Next** through the HMCP tool installation panels, entering information as prompted.



- 2 On the final panel, click **Finish**. Then click **Yes** to restart the system.
- 3 After the system restarts, in Windows select **Start > All Programs > AltiGen HMCP Certification Tool > AltiGen HMCP Certification Tool**.
- 4 In the tool, click **Start**. After the assessment, the tool shows the results. For future configuration, write down the recommended quantities for G711 and combo codecs. Click **OK**, and then click **Exit**.



- 5 You can now restart the MaxACD installation. Return to *Step 6: Install MaxACD 6.5.8* on page 20 and begin the installation process again.

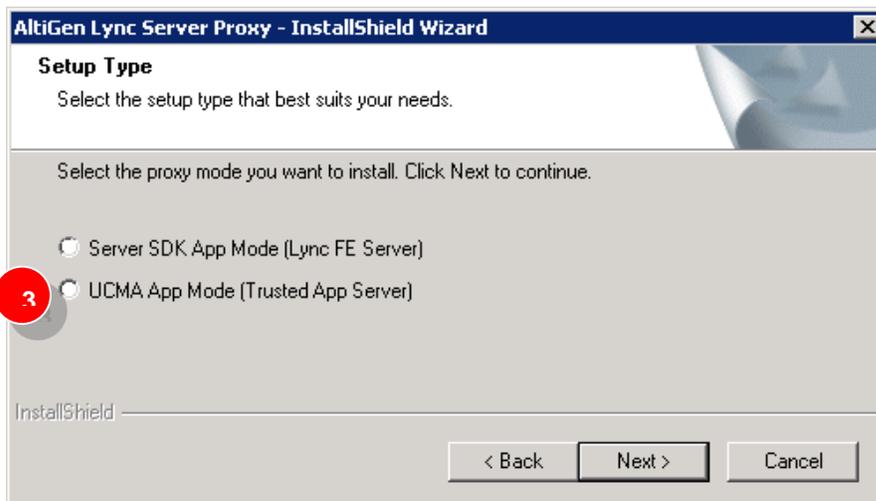
Step 7: Install the UCMA Application Service on the MaxACD System

The next step is to run the AltiGen Lync Server Proxy installation program to install the UCMA Application Service on the system where you installed MaxACD.

Note: The UCMA Application Proxy can be installed on a different server than the MaxACD server.

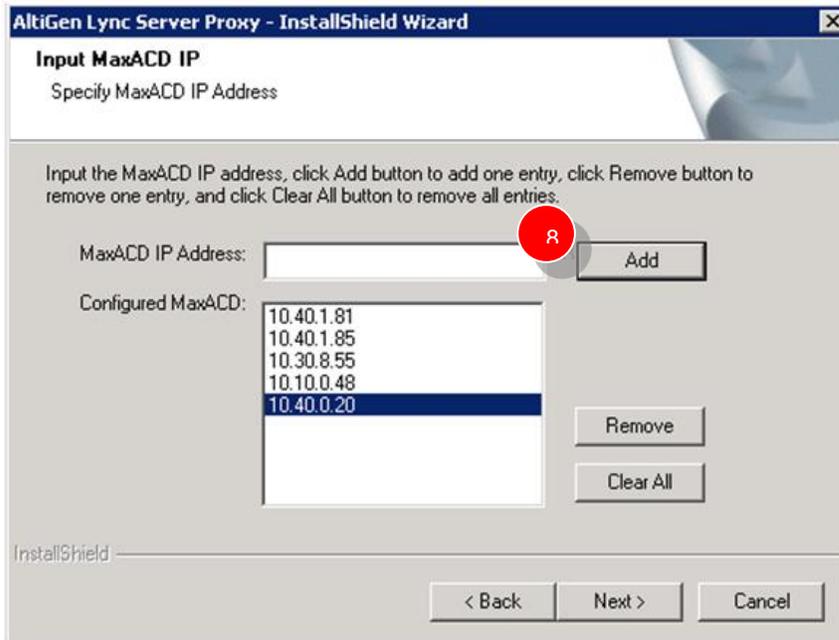
The only system that must be added to the Lync Trusted Application Pool and must have Lync deployed to it is the system that is running the UCMA Application Proxy. Therefore, if the UCMA Application Proxy will be installed on a different server than the MaxACD server, then the MaxACD server does not need to be added to the Lync Trusted Application Pool.

- 1 Log into the system as a Domain user with local Administrator privileges.
- 2 Insert the MaxACD Installation CD, and in the **MaxACD Server > AltiGen Lync Proxy** folder, run *setup.exe*.
- 3 When prompted, choose **UCMA App Mode (Trusted App Server)** and click **Next**.



- 4 Choose **Microsoft Lync 2010** and click **Next**.
- 5 When prompted, enter your user name and company name and click **Next**.
- 6 The setup wizard creates a user account and suggests a random password. If you choose not to use this password, enter a different one (up to 20 characters). Click **Next**.
- 7 We recommend that you accept the default installation location. Click **Next**.

- 8 Enter the MaxACD server IP address and click **Add**. To connect to multiple MaxACD servers, enter the IP address of each server. Click **Next** when you are done.



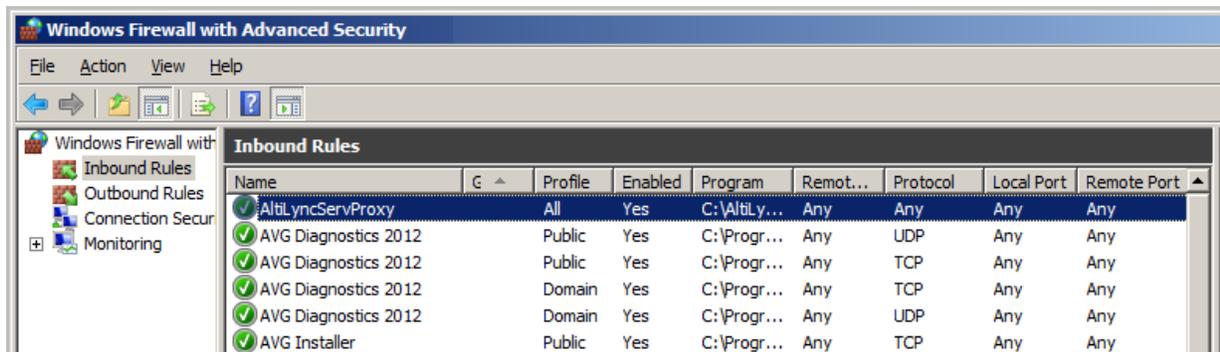
- 9 Enter the FQDN of the Trusted Application Pool. Click **Next**.
- 10 Click **Install**. After the process has finished, click **Finish**.

Note: If you need to change the IP addresses in the future, log in as a user with Administrative privileges and run this wizard again. To do this, in Windows, click **Start > All Programs**, then right-click *AltiGen Lync Server Proxy Configuration* and select **Run as Admin**.

Step 8: Check the MaxACD System's Firewall Exception List

The installation program is designed to update the list of firewall exceptions on the MaxACD system. You should confirm this list. The steps may vary from one version of Windows to another.

- 1 On the server where you installed MaxACD, open Windows Firewall (found in the Windows Control Panel, in **System and Security**).
- 2 Click **Advanced Settings**.
- 3 Select **Inbound Rules**.
- 4 Check that the MaxACD system Components list has inbound routing rules established. If not, manually add a new rule.



Upgrade MaxACD 6.5.8 From an Earlier Version of Lync to either Lync 2013 or Skype for Business

This section provides an overview of the process of upgrading your MaxACD 6.5.8 deployment:

- From Lync Server 2010 to Lync Server 2013, or
- From Lync Server 2013 to Skype for Business

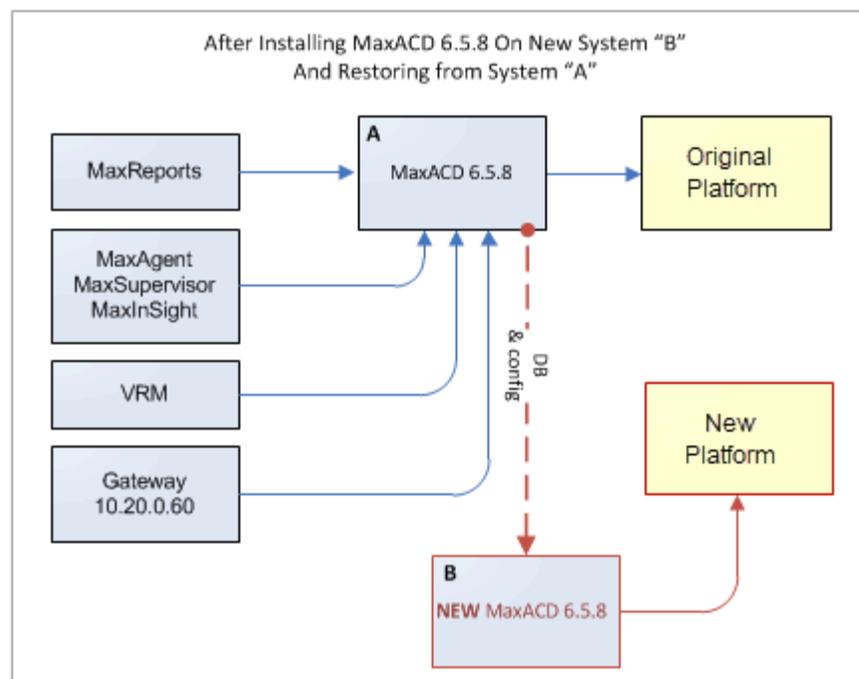
The instructions in this guide apply to either type of upgrade unless noted otherwise. The term “original platform” refers to the current version of Lync; the term “new platform” refers to the deployment that you are moving onto (either Lync 2013 or Skype for Business).

Essentially, you will run two instances of MaxACD 6.5.8 side-by-side for a period of time, migrating batches of users to the new platform. This gives you control over how quickly (or slowly) you migrate users from an older platform to the newer one.

Overview of the Upgrade Process

The next figure illustrates how systems are typically configured in release 6.5.8.

While your configuration may differ slightly from this example, you probably have clients and a gateway pointing to your current MaxACD 6.5.8 system, which, in turn, is configured to work with your original Lync platform.

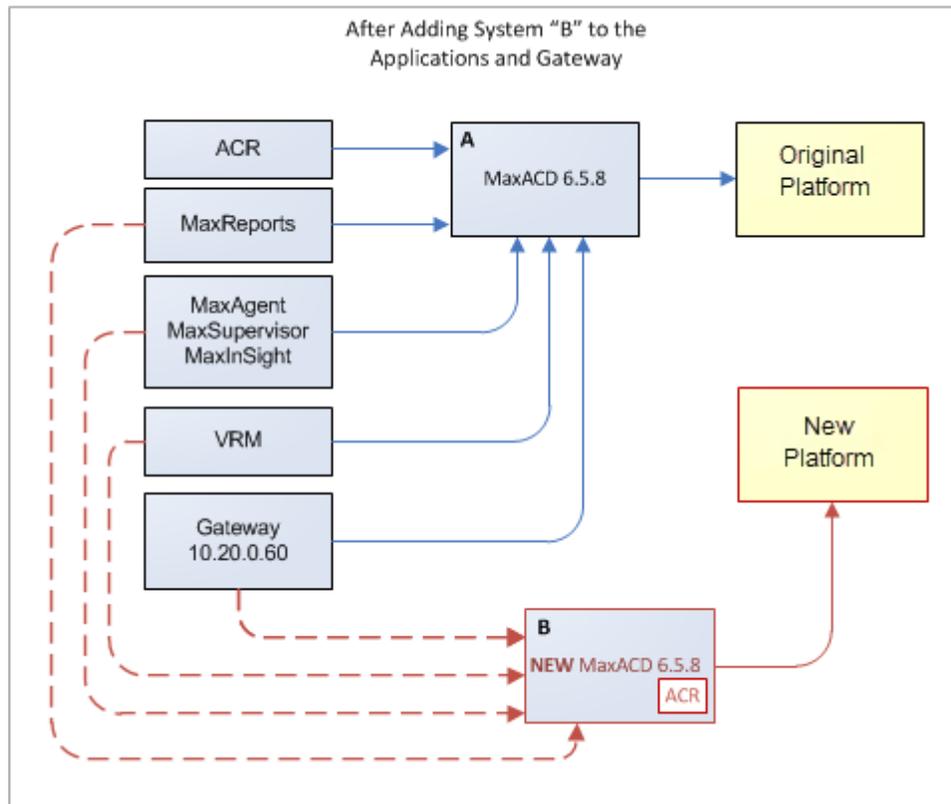


Here is an overview of the upgrade process:

First, you will create a backup of your current MaxACD 6.5.8 deployment.

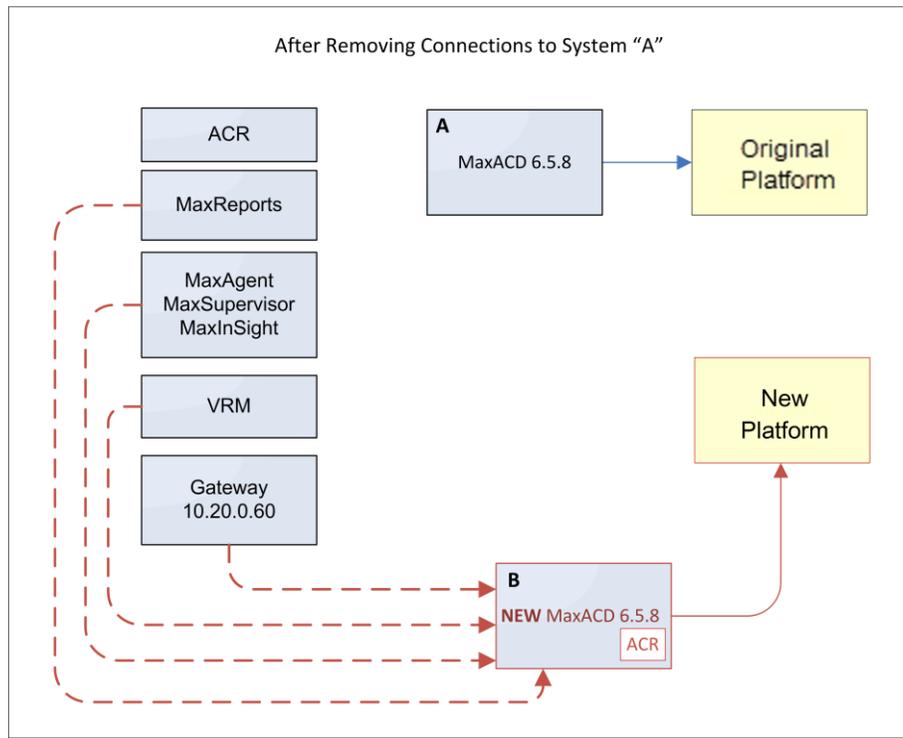
Then you will create a new installation of MaxACD 6.5.8, on a different system (B in the next figure). This second deployment will be configured for the new platform (Lync 2013 or Skype for Business 2015).

Next, you will restore the configuration of your original MaxACD 6.5.8 installation (on A in the next figure) onto the new MaxACD 6.5.8 system (B), and configure some routing rules on Lync Server/Skype for Business Server. At this point, you will add the address of the new MaxACD 6.5.8 system (B) to various applications, and modify your gateway configuration to route some calls through the new MaxACD system.



Then you can migrate users to the new 6.5.8 system. Users can be migrated as needed, a few at a time, or all at once.

Once all users are on the new platform, you can update the gateway and client applications to remove the connections to the original MaxACD 6.5.8 system (A).



Step 1: Plan and Prepare

Before you can begin this process, you must do the following:

- Deploy the new platform (Lync 2013 or Skype for Business) in your environment.
- Make sure the new system or virtual machine meets all of the requirements listed on page 7.
- Perform the following steps on the new 6.5.8 system:
 - Install Windows Server 2008 R2, and apply Service Pack 1 (if it is not already installed).
 - Join the server to the same domain as your Lync 2013 or Skype for Business Server.
 - Install .NET 4.5
 - Install Windows Management Framework 3.0 (which includes Powershell Script V3.0)
 - Install Windows Identity Foundation (KB974405)
- Work with your AltiGen representative to schedule the upgrade to the new platform. AltiGen will need to reset your system key so that you can run both instances of MaxACD 6.5.8 side-by-side during the upgrade process.

Step 2: Make a Backup

Make a backup of your current MaxACD 6.5.8 system. You can use the **Backup and Restore** utility to do this, refer to Chapter 23 of the MaxACD Administrator Manual.

If MaxACD is on a virtual machine, we recommend that you take a snapshot of the image as well.

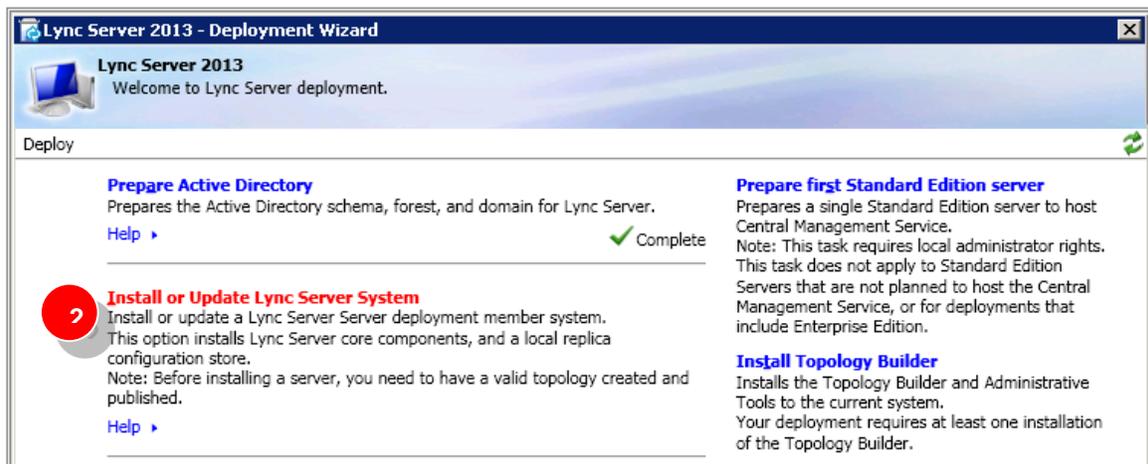
Step 3: Create a New Trusted Application Pool on the New Platform

Create a new Trusted Application Pool for Lync 2013 or Skype for Business. This name *must be different* from the name of the pool that you configured for your original platform. While creating the new pool, add the new MaxACD system to it.

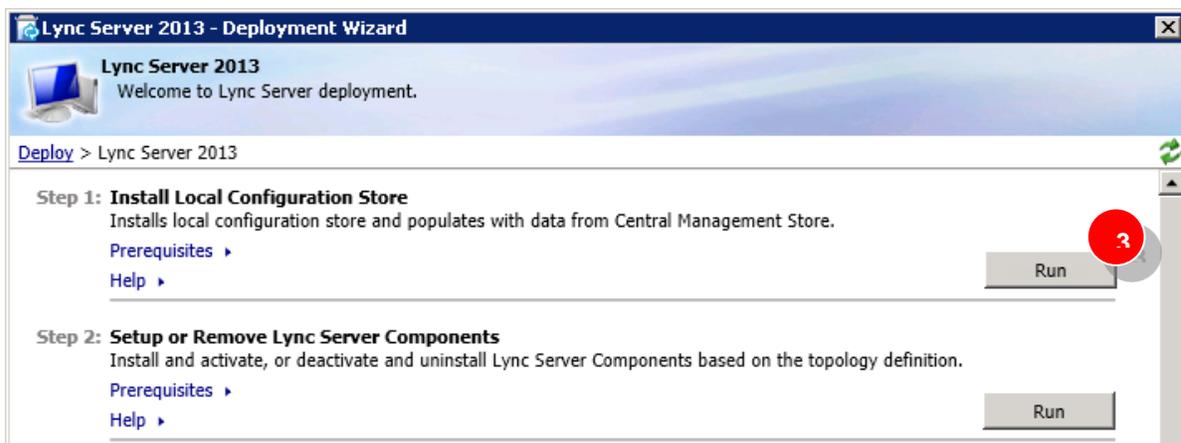
- 1 Log into a Lync Front-end server as a Domain user with Administrative privileges.
- 2 Open Lync Server/Skype for Business and download the topology from your existing deployment.
- 3 Run **Topology Builder** and create a new Trusted Application pool.
- 4 Enter a name for this pool. It must be a unique FQDN. This should be different from the FQDN of the server that will be added to the pool. For example, the server FQDN may be *max-proxy.company.com*, and the pool FQDN may be *max-pool.company.com*.
- 5 Choose **Multiple computer pool**, and then click **Next**.
- 6 The next page is where you add servers to the pool. You need to enter those servers where MaxACD will be running the Proxy role. Enter each server's FQDN and click **Add**. When you are done, click **Next**.
- 7 Select which front-end pool to use as the next hop, and then click **Finish**.
- 8 Before publishing these updates, open the *PSTN Gateways* and *Trunks* folders in Topology Builder and make sure that the IP address of the new MaxACD 6.5.8 server is listed in each folder. If the IP address is not listed there, then add it manually.
- 9 Publish the revised topology.

Step 4: Make the MaxACD System a Lync 2013/Skype for Business Application Server

- 1 On the system where you want to install MaxACD, log in as a Domain user with Administrator privileges. Insert your Lync Server 2013/Skype for Business Installation CD and run *setup.exe* to launch the Deployment wizard.
- 2 Choose **Install or Update Lync/Skype Server System**.



- 3 For “Step 1, Install Local Configuration Store,” click **Run**.
Note: If you see a warning that a prerequisite step has not been satisfied, you must stop and install ‘Windows Identity Foundation’ as noted on page 28.



- On the next panel, choose **Retrieve directly from Central Management Store**, and then click **Next**. When processing has completed, click **Finish**.

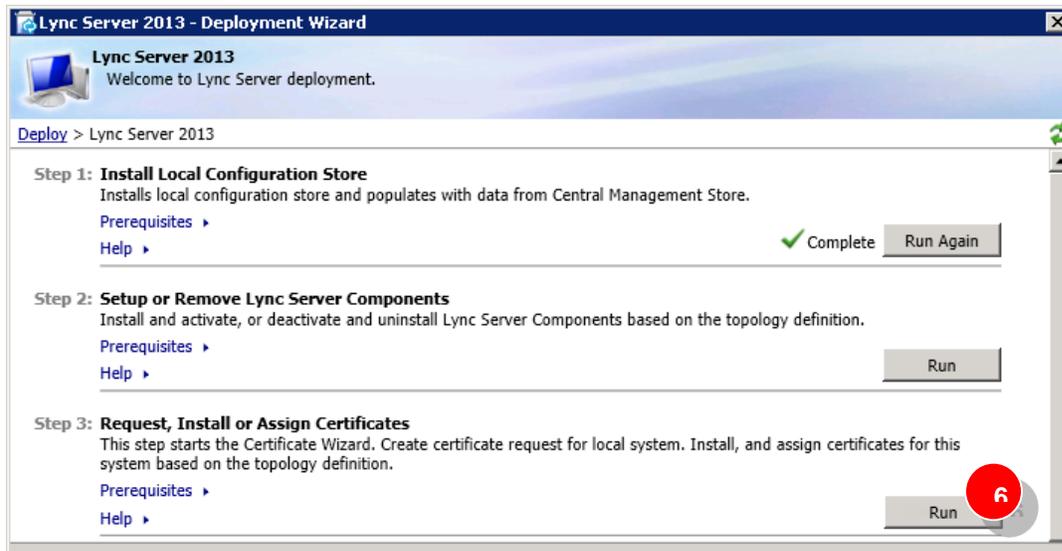


- You return to the main page. For “Step 2, Setup or Remove Lync/Skype Server Components,” click **Run** and then click **Next**. When processing has completed, click **Finish**.

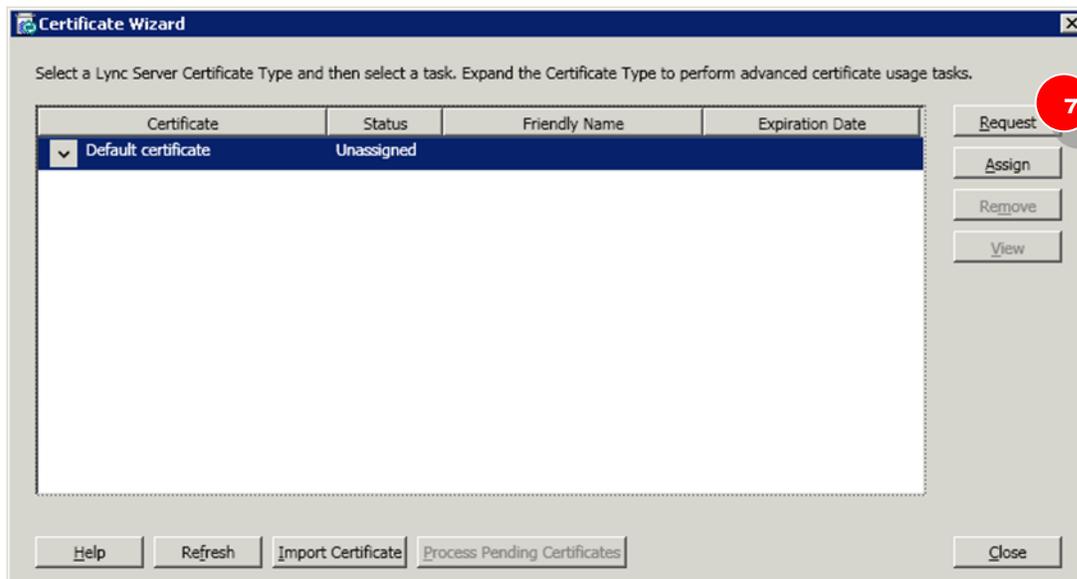
Note: You may or may not see the green checkmark when Step 2 is complete.



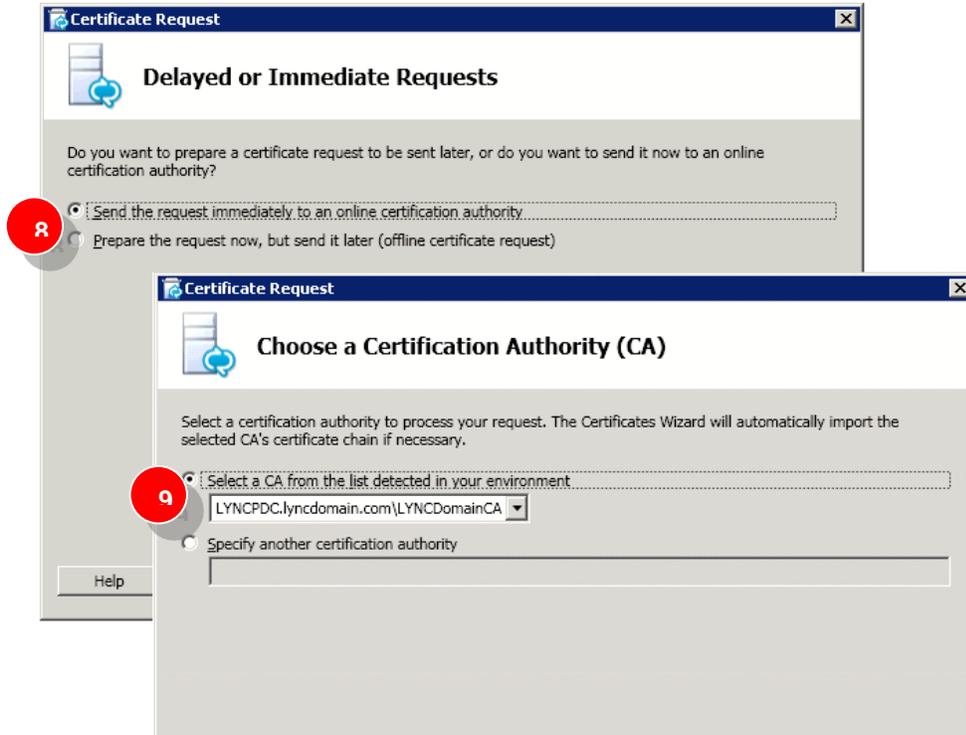
- When you return to the main page of the Wizard, for “Step 3, Request, Install or Assign Certificates,” click **Run**.



- In the Certificate Wizard, click **Request**, and then click **Next**.

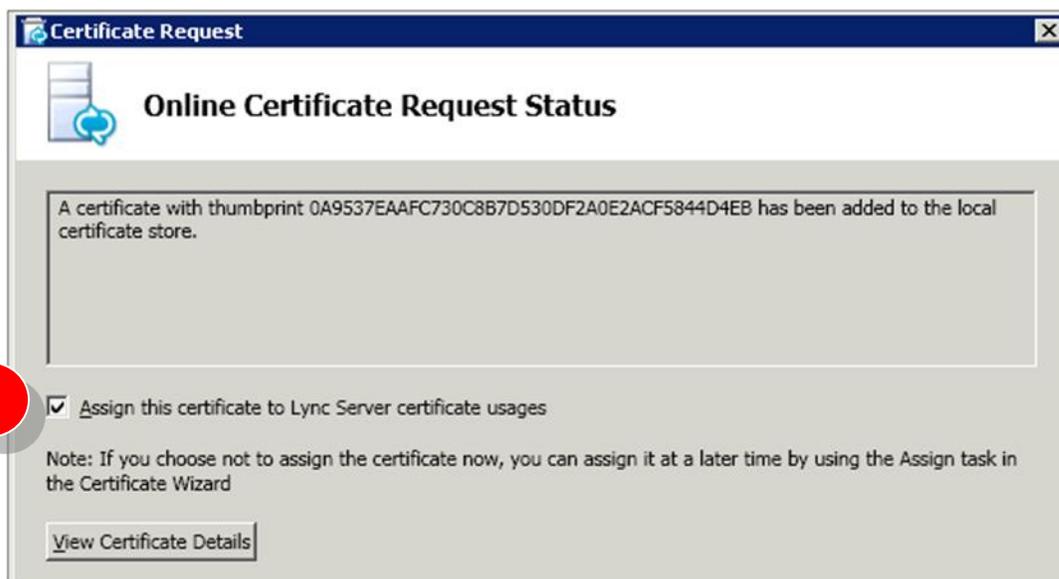


- 8 Select the “Send the request immediately...” option and click **Next**.



- 9 Choose a Certificate Authority (CA) from the list and click **Next**.
- 10 For the next two panels (*Certification Authority Account* and *Specify Alternate Certificate Template*), click **Next** to accept the default settings and continue.
- 11 When you reach the *Name and Security Settings* panel, enter a friendly name. Make sure that the bit length is set to **2048**, and that the **Mark Certificate Private Key As Exportable** checkbox is checked. Click **Next**.

- 12 Continue through the wizard panels. When you reach the *Geographical Information* panel, note that the City, State, and Country names cannot contain abbreviations. For example, enter *San Jose* rather than *SJ*.
- 13 Continue through the wizard panels. When you reach the *SIP Domain Setting on Subject Alternate Names* panel, check your SIP domain and click **Next**.
- 14 Continue through the wizard panels. When you reach the *Certificate Request Summary* panel, review all of the information carefully. If necessary, click **Back** to make any changes. When all of the information is correct, click **Next**. This starts the process of requesting the certificate.
- 15 When you reach the *Online Certificate Request Status* panel, we recommend that you check the box to assign the certificate (to save yourself a few steps). Click **Finish**, click **Next** twice, and then click **Finish**.



- 16 If you did not check the box in step 11, click **Assign** in the main Certificate pane and assign the certificate.
- 17 Close the Certificate wizard. When you return to the main page of the Wizard, for “Step 4, Start Services,” click **Run**, click **Next**, and click **Finish**.
- 18 At the bottom of the Deployment window, click **Run** to install any additional Lync updates, and then click **Exit** to close the Deployment wizard.

Step 5: Install MaxACD 6.5.8

On the new system, follow these steps to install MaxACD.

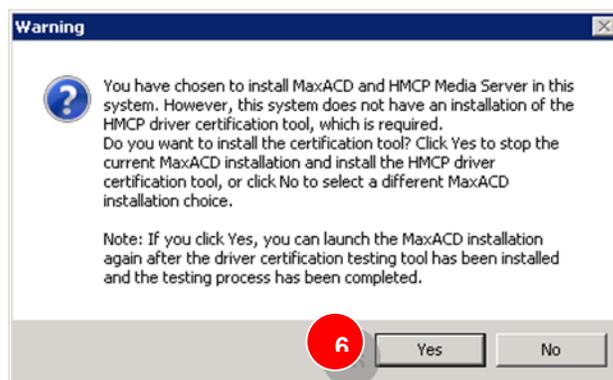
Note: During this installation process, if a message appears asking whether to install KEYLOK, click **Install** to continue.

- 1 Obtain a system key and license activation file from your AltiGen account manager.
- 2 Log into the system as a Domain or Local user with local administrator privileges, and make sure that the server is already joined to the domain where your Lync 2013 Server/Skype for Business Server is installed. If you plan to run Exchange Integration, you must have Domain administrator privileges.
- 3 Insert the MaxACD installation CD. In the **MaxACD Server > MaxACD for Lync** folder, run *setup.exe*.
- 4 Accept the license agreement, and continue to follow the instructions in the wizard.
- 5 When prompted, select a setup type:
 - **All-in-one (MaxACD + HMCP) System** – Select this if MaxACD will be operating on a single server. (This is the default configuration.)
 - **MaxACD Server with Separate HMCP Server** – Select this if the MaxACD server and HMCP servers will be running on different chassis in an enterprise deployment. You will select which components to install:
 - » **MaxACD Server** – Select this option to install MaxACD on the server. You will need a dongle for the MaxACD server.
 - » **HMCP Media Server** – If you have a small- to medium-size call center (no more than about 200 agents), you can install MaxACD and HMCP Media Server in the same machine. You can also install them in different machines, especially if you plan to grow your call centers.

If you have more than 200 agents, we recommend that you install the HMCP Media Server and MaxACD on two different servers.

- 6 Before installing the HMCP Media server, the installation program scans the system to determine whether the HMCP Certification Tool has already been installed on that system.

During an All-in-one installation, if the tool is not detected, you must either select **Yes** to install the Certification Tool and automatically restart the MaxACD installation, or select **No** to return to step 5 and select the other installation choice.



- 7 Continue through the remaining installation panels, entering information as prompted. During this process, the wizard will create a password account for AltiGen services. We recommend that you accept this default password.

Note: If a window prompts whether to install KEYLOK during the installation process, click **Install**.

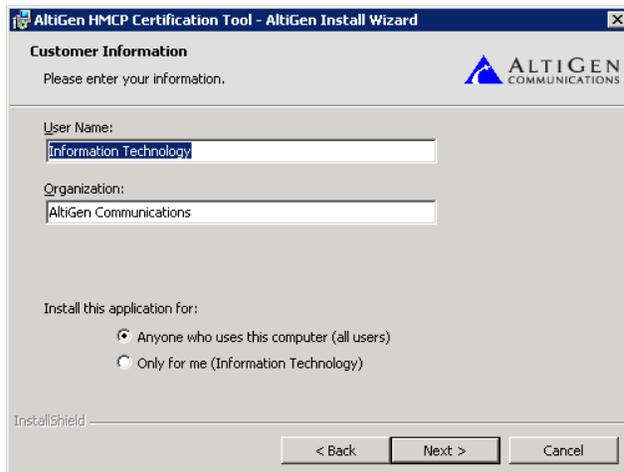
- 8 After the installation process has been completed, you must reboot that system.

Note: If you are using Exchange Integration, check the Exchange Integration Service to ensure that it has Domain Administrator privileges and that the service is running.

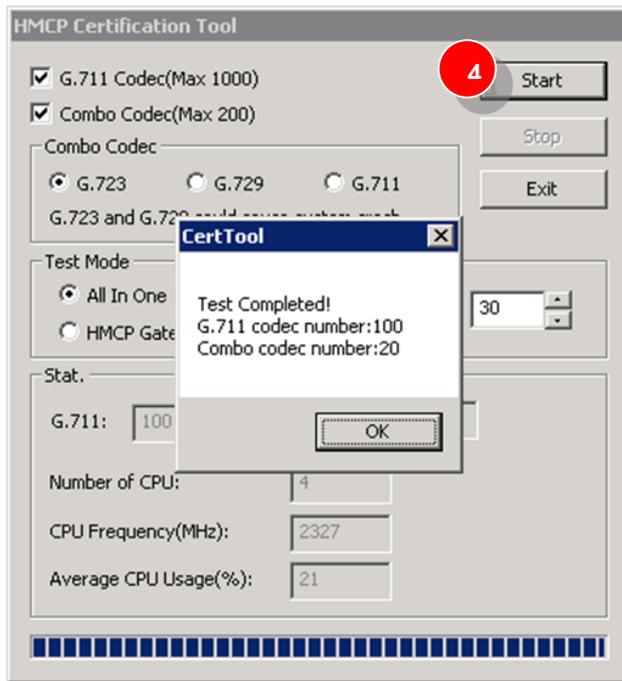
HMCP Certification Tool Installation

During installation, if you are prompted to install the HMCP certification tool, follow these steps:

- 1 Click **Next** through the HMCP tool installation panels, entering information as prompted.



- 2 On the final panel, click **Finish**. Then click **Yes** to restart the system.
- 3 After the system restarts, in Windows select **Start > All Programs > AltiGen HMCP Certification Tool > AltiGen HMCP Certification Tool**.
- 4 In the tool, click **Start**. After the tool assesses your system, it shows the results. For future configuration, write down the recommended quantities for G711 and combo codecs. Click **OK**, and then click **Exit**.



- 5 You can now restart the MaxACD installation. Return to *Step 5: Install MaxACD 6.5.8* on page 35 and begin the installation process again.

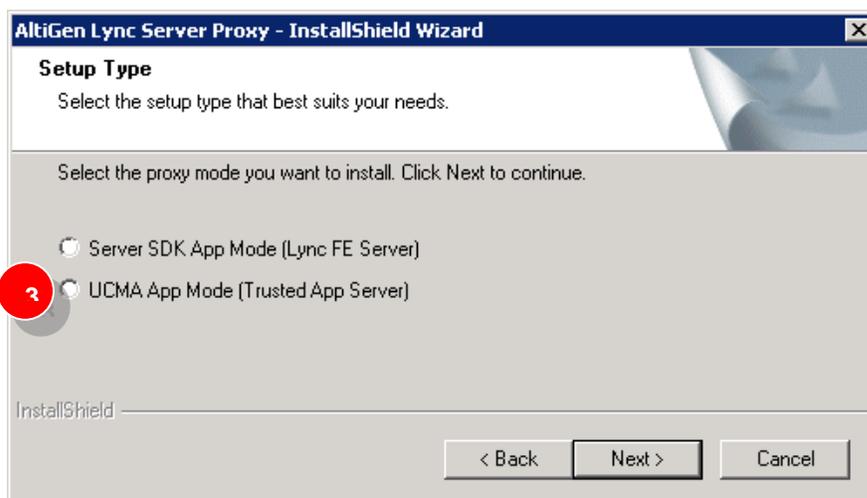
Step 6: Install the UCMA Application Service on the MaxACD System

The next step is to install the UCMA Application Service on the new system where you installed MaxACD.

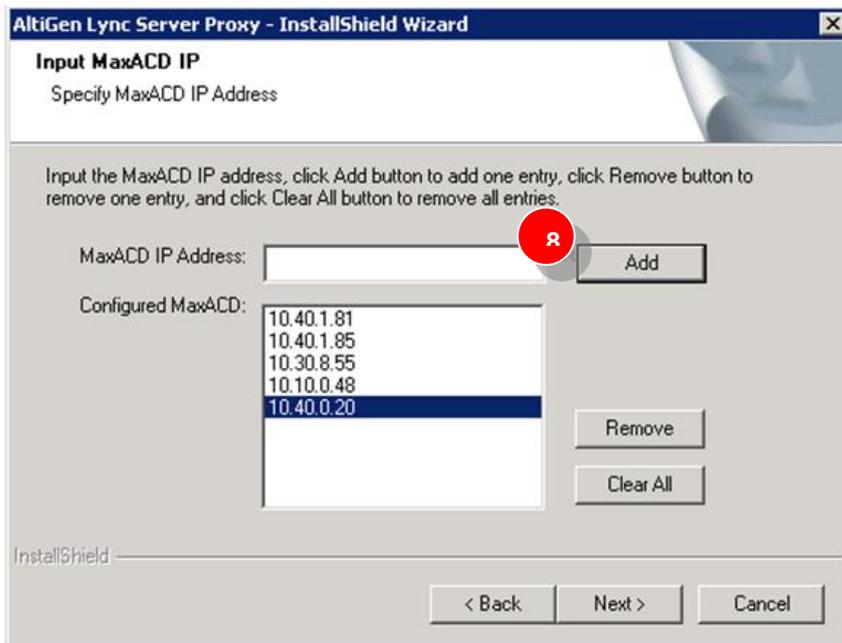
Note: The UCMA Application Proxy can be installed on a different server than the MaxACD server.

The only system that must be added to the Lync Trusted Application Pool and must have Lync/Skype for Business deployed to it is the system that is running the UCMA Application Proxy. Therefore, if the UCMA Application Proxy will be installed on a different server than the MaxACD server, then the MaxACD server does not need to be added to the Trusted Application Pool.

- 1 Log into the system as a Domain user with local Administrator privileges.
- 2 Insert the MaxACD Installation CD, and in the **MaxACD Server > AltiGen Lync Proxy** folder, run *setup.exe*.
- 3 When prompted, choose **UCMA App Mode (Trusted App Server)** and click **Next**.



- 4 Choose **Microsoft Lync 2013** and click **Next**.
- 5 When prompted, enter your user name and company name and click **Next**.
- 6 The setup wizard creates a user account and suggests a random password. If you choose not to use this password, enter a different one (up to 20 characters). Click **Next**.
- 7 We recommend that you accept the default installation location. Click **Next**.



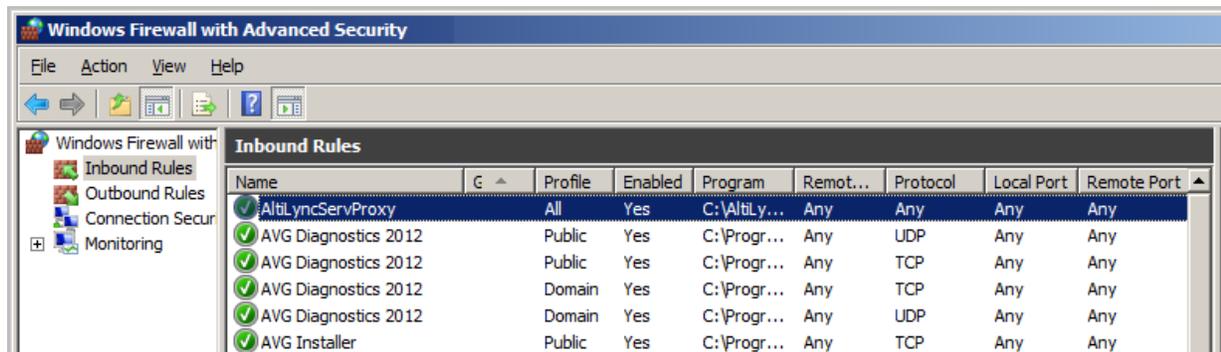
- 8 Enter the new MaxACD server's IP address and click **Add**. To connect to multiple MaxACD servers, enter the IP address of each server. Click **Next** when you are done.
- 9 Enter the FQDN of the Trusted Application Pool. Click **Next**.
- 10 Click **Install**. After the process has finished, click **Finish**.

Note: If you need to change the IP addresses in the future, log in as a user with Administrative privileges and run this wizard again. To do this, in Windows, click **Start > All Programs**, then right-click *AltiGen Lync Server Proxy Configuration* and select **Run as Admin**.

Step 7: Check the MaxACD System's Firewall Exception List

The installation program is designed to update the list of firewall exceptions on the MaxACD system. You should confirm this list. The steps may vary from one version of Windows to another.

- 1 On the server where you installed MaxACD, open Windows Firewall (found in the Windows Control Panel, in **System and Security**).
- 2 Click **Advanced Settings**.
- 3 Select **Inbound Rules**.
- 4 Check that the MaxACD system Components list has inbound routing rules established. If not, manually add a new rule.



Step 8: Perform a Restore on the New MaxACD System

Perform a Restore operation on the new MaxACD system, using the backup that you created in the section *Step 2: Make a Backup* on page 29.

Step 9: Register Your System Key in MaxACD

Make sure that your AltiGen representative has reset your system key before you begin this step.

IMPORTANT: Once you register the key on the new system, you cannot register the key on the original MaxACD 6.5.8 system again. If you try to do so, the original system will immediately be deactivated and all of its licenses will become invalid.

To register the key,

- 1 Open MaxAdministrator and select **License > License Information**.
- 2 Click **Registration**.
- 3 Select the checkbox **Use Soft System Key**.
- 4 Click **Enter the System Key** and type the key into the System Key field.
- 5 After the key is validated, close MaxAdministrator and restart the system.

Step 10: Change the System ID on the new MaxACD System

Change the System ID in the new MaxACD 6.5.8 system to a different ID number from the original 6.5.8 installation.

You do this in MaxAdministrator in **System > System Configuration**, on the **General** tab.

Refer to Chapter 4 of the *MaxACD Administrator Manual* as needed.

Step 11: Check the External Logger Service

Confirm that the External Logger Service shows as “Connected.”

You do this in MaxAdministrator, in **System > System Configuration**, on the **Call Report** tab.



Step 12: Verify MaxACD Interaction with Lync 2013/Skype for Business

When you restored the configuration from the old MaxACD system, your settings should have been applied to the new MaxACD system. It is a good idea at this point to check these settings, to make sure that they apply to the new system. Adjust settings as needed.

Especially important to confirm are the settings for the Mediation server pool, the outcall routing, and the mediation server entry in Enterprise Manager.

- 1 In MaxACD Administrator, click **System Configuration > General**. Confirm the FQDN for the Mediation pool. Do not use an alias. Confirm the MaxACD *Dial Tone Pilot Number*.
Note: If you are using a hardware load balancer, you should enter the FQDN of the hardware load balancer instead of the FQDN of the Mediation pool.
- 2 Click the *Number Plan* tab. Check the digit assigned as “IP Trunk Access.”
- 3 Open the Trunk Configuration page and select a SIP-Tie trunk. Confirm that the Trunk Access Code matches the IP Trunk Access digit from the previous step.
- 4 Click **VoIP > Enterprise Network Manager** and click the *Server* tab. Check the Mediation server and Front-end server entries; update these as needed.
- 5 Restart the system.

Step 13: Install the Server SDK Proxy on Each Lync/Skype Front-end Server

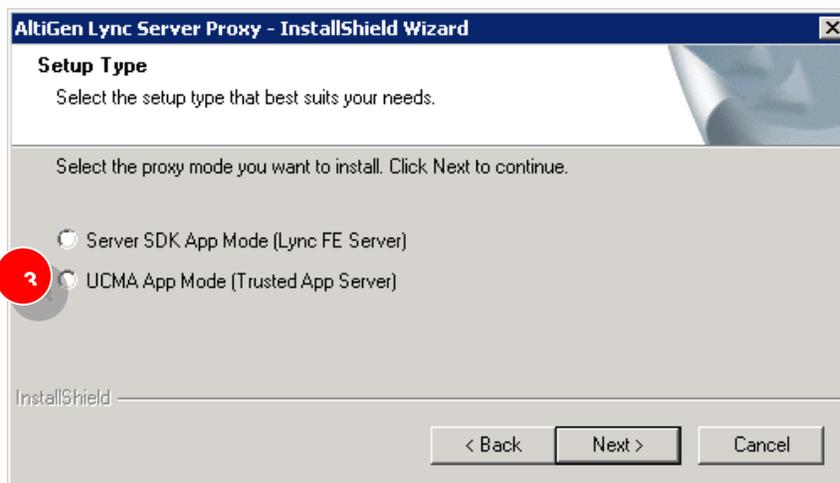
If you have multiple Lync/Skype Front-end servers, then the Server SDK Application Proxy must be installed on each one.

The installation account must be a member of the following groups:

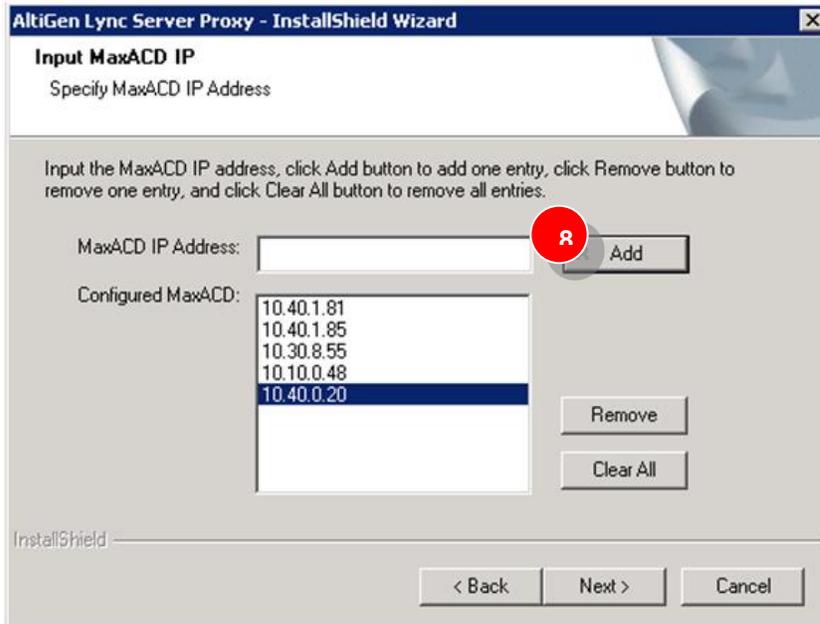
- *RTCUniversalServerAdmins*
- *Account Operator*

In addition, the installation account must be added to *RTC Server Applications* group on the Lync/Skype Front-end server.

1. Log in as a Domain user with Administrator privileges.
2. Insert the MaxACD Installation CD, and in the **MaxACD Server > AltiGen Lync Proxy** folder, run *setup.exe*.
3. When prompted, choose **Server SDK App Mode (Lync FE Server)** and click **Next**.



4. Choose **Microsoft Lync 2013** and click **Next**.
5. When prompted, enter your user name and company name and click **Next**.
6. The setup wizard creates a user account and suggests a random password. If you choose not to use this password, enter a different one (up to 20 characters). Click **Next**.
7. We recommend that you accept the default installation location. Click **Next**.



8. Enter the new MaxACD server's IP address and click **Add**. To connect to multiple MaxACD servers, enter the IP address of each server. Click **Next** when you are done.
9. Enter the FQDN of the Lync/Skype Front-end Pool. Click **Next**.

Note: You can run `Get-CsSite` from the Lync Server Management Shell on this system to obtain this information.

10. Click **Install**.
11. For Skype for Business deployments, you must apply a patch after the installation process has finished:

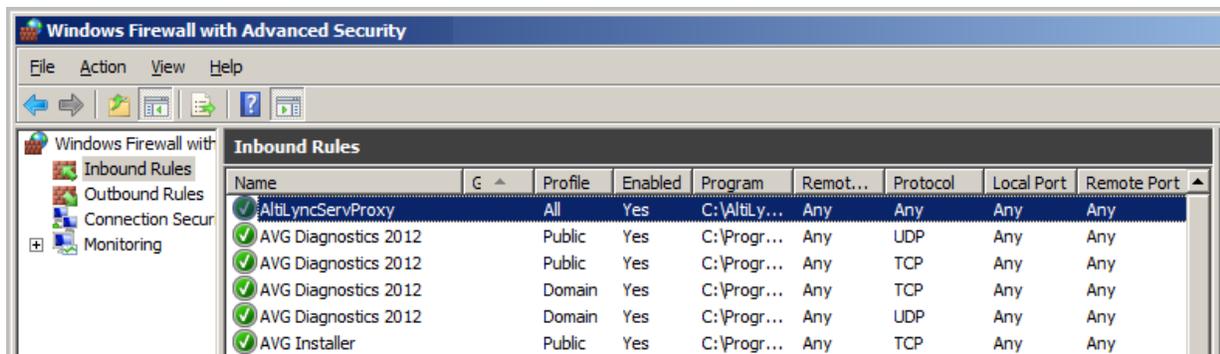
- a. Download the Proxy_S4B patch from this site:
https://tsfiles.altigen.com/main.html?download&weblink=453058e519a341c9ca835b159d91f1a0&realfilename=Proxy_S4B.zip
- b. From the Windows Services panel, stop the AltiGen Lync/Skype proxy service on the MaxACD server.
- c. Unzip the update file. Copy the new files to this folder on the MaxACD server:
 \AltLyncServProxy folder.
- d. From the Windows Services panel, restart the AltiGen Lync proxy service.

These updated files are needed only on the proxy on the MaxACD server; you do not need to update the files on the Skype Front-end server.

Step 14: Check Each Lync/Skype Front-end Server's Firewall Exception List

The installation program is designed to update the list of firewall exceptions on each Front-end server. You should confirm this list on each server. The steps may vary from one version of Windows to another.

- 1 On each Lync/Skype Front-end server, open Windows Firewall (found in the Windows Control Panel, in **System and Security**).
- 2 Click **Advanced Settings**.
- 3 Select **Inbound Rules**.
- 4 Check that the MaxACD system Components list has inbound routing rules established. If not, manually add a new rule.



Step 15: Configure Call Routing from Lync/Skype Server to MaxACD

Determine targets in MaxACD that should be available to all Lync Users

Although not all Lync users will be MaxACD agents, Lync/Skype for Business users may still want to be able to place calls to the MaxACD workgroups, or transfer calls into these workgroups. For this reason, it is recommended that these workgroups be added to the Lync Global Dial Plan.

In the following example, workgroups 500-509 are MaxACD workgroups that all Lync/Skype users should be able to call.

Create a Normalization Rule that Performs No Translation

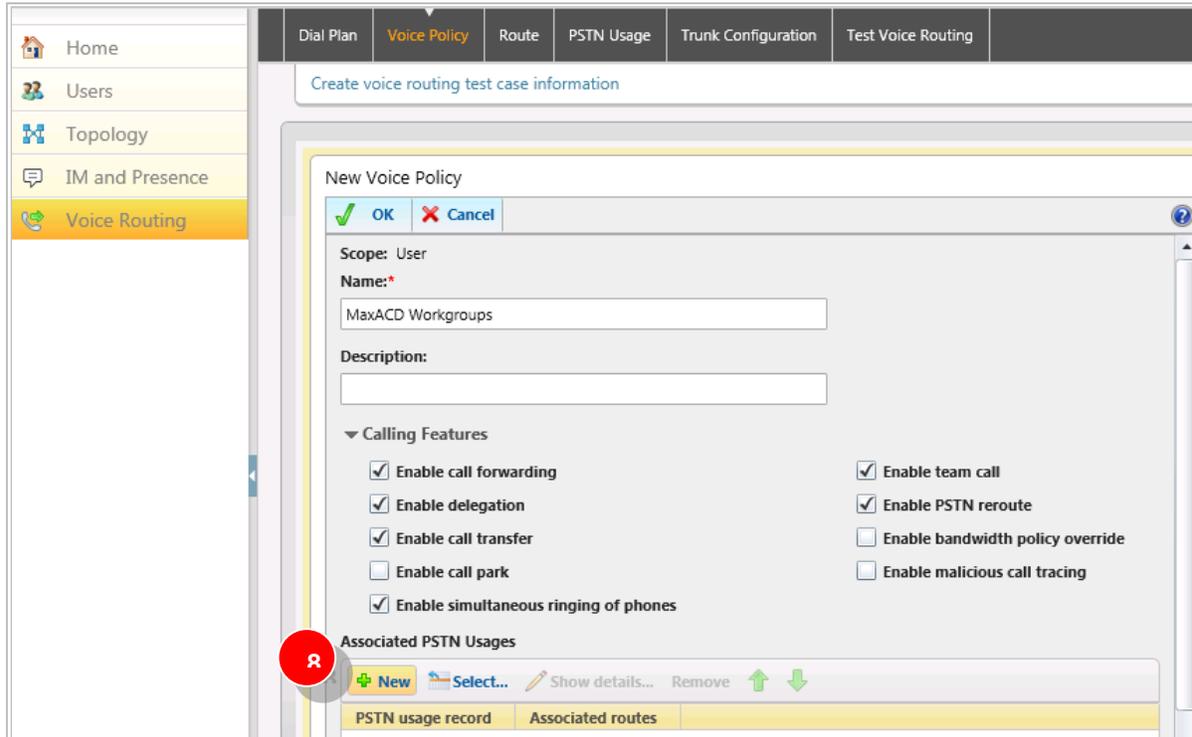
Under **Lync/Skype Server Control Panel > Voice Routing > Dial Plan**, create a new entry that performs no translation for these workgroup numbers:

- 1 Double click the **Global** dial plan to begin editing.
- 2 Select **New** under Associated normalization rules to add the new rule. Name this rule "MaxACD Workgroup Normalization."
- 3 Create a rule that begins with "50" (by adding the digits 50 in the starting digits field) and is exactly 3 digits long.
- 4 Remove 0 digits from this rule, and add no digits to this rule.
- 5 Because of this rule, any numbers between 500 and 509 will be normalized exactly as dialed.
- 6 Create a similar rule for the MaxACD Dial tone (e.g. 222), so that a pattern beginning with 222 that is exactly 3 digits long will have no digit translation performed on it.
- 7 **Commit** these changes to the dial plan. Lync should display a message indicating that the changes were successfully published.
- 8 Double-click the Global dial plan again, and verify that your entry has been added.

Create a Route for These Numbers to the MaxACD Server

Under **Lync/Skype Server Control Panel > Voice Routing > Route**, create a new route:

- 1 Click **New** to create a new Voice Route. Name this route "MaxACD Workgroups."
- 2 Click **Edit** and use the following pattern to match for workgroups 500-509: **^(50\d)\$**
- 3 Scroll down the Route page and click **Add...** next to *Associated Trunks*.
- 4 Add the gateway record that corresponds to the MaxACD server.
- 5 Click OK to return to the Route configuration window.
- 6 Create a similar Route entry for the MaxACD Dial Tone Pilot Number. Pattern match: **^(222)\$**
- 7 Under **Server Control Panel > Voice Routing > Voice Policy**, create a new PSTN Usage Record that associates with the Route(s) that you just created.



- 8 Select **New**, then select **User Policy** under the *Voice Policy* section, and create a PSTN usage record for MaxACD targets. Name this record “MaxACD Workgroup Policy.”
- 9 Click **Select...** in the *Associated Routes* section, and add the routes that were created in the steps above.
- 10 Click **OK** to return to the Global Voice Policy record, and click **OK** again to return to the **Voice Policy** menu.
- 11 **Commit** these changes.

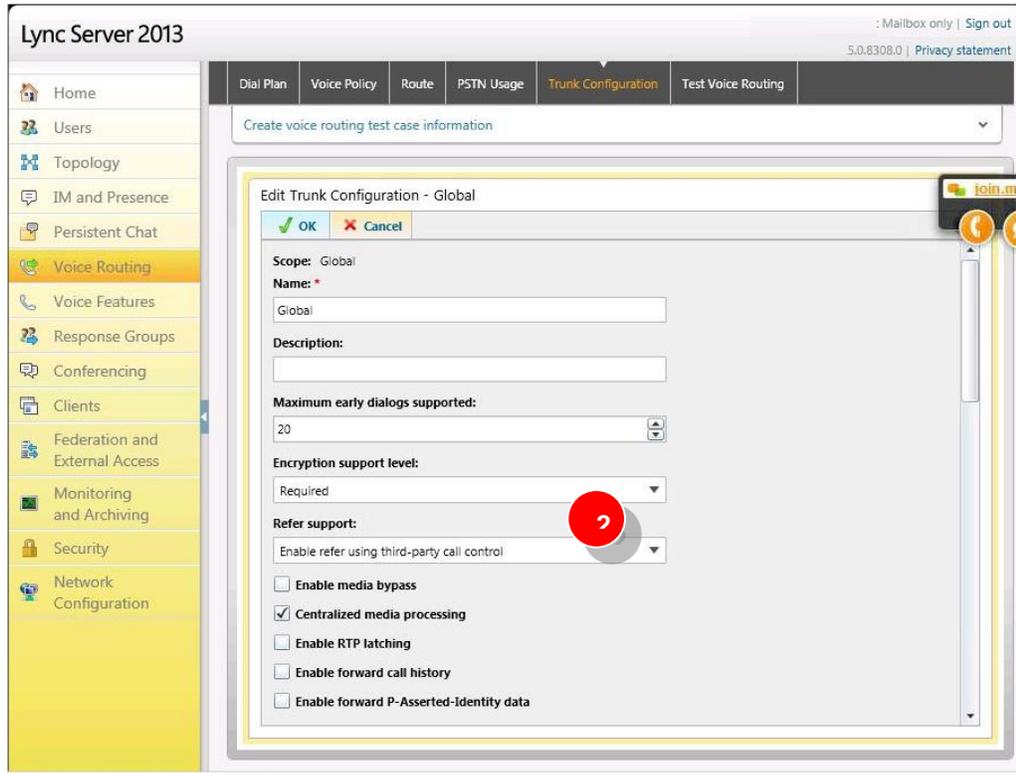
All users assigned to the Global Dial Plan, and Global Voice Policy, should now be able to place calls to MaxACD workgroups.

Enable Third-Party Call Control

Next, enable refer support. The option varies from one version of Lync/Skype to another.

- 1 In the **Lync/Skype Server Control Panel**, select **Voice Routing > Trunk Configuration**, and then double-click the Global entry.

- 2 Under *Refer support*, select **Enable refer using third-party call control**. This specifies that the third-party control protocol can be used to allow transferred calls to bypass the hosted site.



- 3 Click **OK**. Return to the Voice Policy menu and click **Commit** to save these changes.

Step 16: Configure Outbound Workgroup Call Rules

In an outbound call center, the agent should be able to place ‘workgroup’ calls so that those call details will be logged to the workgroup for call accounting purposes. Additionally, call recording will be controlled by workgroup settings, and supervisors may be able to barge/coach/monitor these calls.

In order to allow for this, all of the agent’s outbound calls **MUST** route through the MaxACD server. If an agent is ever to participate in any outbound workgroup calling, then **ALL** of that agent’s calls must follow this route.

Make a User Voice Policy for Lync/Skype Users Who Will Make Outbound Workgroup Calls

In order to apply the new rules to **ONLY** Lync users that will utilize features of outbound calling, a new User Voice Policy must be created:

- 1 Under **Server Control Panel > Voice Routing > Voice Policy**, select **New > User policy**.
- 2 Name this policy “MaxACD Agent Policy” to indicate that it will apply to MaxACD agents for outbound workgroup calling.
- 3 Select **New** under *Associated PSTN Usages* to create the PSTN Usage Record to be used by this policy.
- 4 Name this PSTN Usage Record “MaxACD Agent Usage.”
- 5 Click **New** in the *Associated Routes* section, to create a new route to be used by this policy.
- 6 Because all calls in this policy will route to the MaxACD server, only a catch-all route is needed. Name this new Route, “Route All to MaxACD”.
- 7 The wild-card pattern to match (.*) can be left as is.
- 8 In the *Associated Trunks* section, click **Add...**, and associate the PSTN Gateway record for the MaxACD server.
- 9 Click **OK** to return to the PSTN Usage rule, then **OK** again to return to the Voice Policy configuration, and **OK** once more to return to the general Voice Policy window.
- 10 Commit the new Voice Policy rules.

Configure Trunks for PSTN Calls that Route Through MaxACD Server

Outbound calls that will route *through* the MaxACD server must have the leading digit translated in order to access trunks through MaxACD’s route access table (typically set to 9 on the MaxACD server). Because the outbound numbers are currently in e.164 format, they will all have a leading “+” (plus) symbol. A new Pool Trunk rule will be used to change the leading + to a 9 as follows:

- 1 Under **Server Control Panel > Voice Routing > Trunk Configuration**, click **New > Pool trunk**.
- 2 Chose the PSTN Record for the MaxACD server, and then click **OK**.
- 3 Under *Associated Translation Rules*, click **New** to create a new translation rule.
- 4 Name this rule “Replace + with 9”.
- 5 Use “9” as the Digits to add. Keep all other settings at default.
- 6 Click **OK** to save this rule, Click **OK** again to return to the main Trunk Configuration window.
- 7 Commit the new Pool trunk configuration.



Assign the New Voice Policy to Users Who Make Outbound Workgroup Calls

Only Lync/Skype users that are assigned to this new voice policy will have their outbound calls route *through* the MaxACD server. Note that these Lync/Skype users must also be configured as MaxACD agents as well in order to get any of the benefits of outbound workgroup calling. In order to assign this policy to the users, do the following:

- 1 Go to **Server Control Panel > Users**, and search for the user(s) that need to have this policy applied to.
- 2 Double-click the user to edit the user's configuration.
- 3 Change the user's assigned Voice Policy to "MaxACD Agent Policy" (The policy name assigned in step 2 of the section titled "**Create a new User Voice Policy for Lync users that will participate in Outbound Workgroup calling**" of this document.
- 4 Click **Commit** to save these changes.

Because of the steps above, if this user dials 1-888-258-4436, the Dial Plan should normalize the number to +18882584436. The Voice Policy will be used to select the "Route All to MaxACD" route, directing the call to the MaxACD server. The Trunk Configuration will then change the number sent to MaxACD from +18882584439 to 918882584436.



Step 17: Move Users to the New Platform and Adjust User Voice Policies

Follow your company's procedures to move selected Lync/Skype users to the new platform, and adjust user voice policies accordingly.

You can move Lync users from your original pool to your new platform pool using Lync/Skype Control Panel or Lync/Skype Management Shell. Refer to your Lync/Skype documentation or the various topics on the Lync/Skype website.

For those users whom you move to the new platform, you will need to adjust user policies accordingly.

Step 18: Reconfigure AltiGen Applications

- 1 Add the new MaxACD 6.5.8 system to MaxReports. Refer to Chapter 2 of the *MaxReports Manual* for instructions.
- 2 Add the new MaxACD system to VRManager. Refer to the *VRManager Manual* for details.
- 3 Install Advanced Call Router to the new MaxACD 6.5.8 system, if needed.
- 4 Inform users that they should point their client applications (MaxAgent, MaxSupervisor, and MaxInSight) to the new MaxACD system's IP address or FQDN.

Step 19: Remove Connections to the Original MaxACD System

After you have migrated all users to the new platform, you can remove any connections to the original Lync platform.

Troubleshooting

This section provides some tips for troubleshooting various issues with MaxACD.

- For MaxACD issues, in addition to gathering a complete set of traces, please provide all log files in this folder on the Lync Front-end server:
C:\AltilyncServProxy\Log
- For MaxAgent issues, provide traces from the client log files from this folder:
C:\Users\- For reproducible connection or routing issue, please provide Wireshark (www.wireshark.org) packet capture from the MaxACD system and possibly the Lync Server trace.
- If the issue is related to a call transfer, make sure that the *Enable refer support* option in Lync Trunk Configuration is enabled. MaxACD needs a referral from the Lync server to finish transferring calls.

To check this option, log into Lync Server and choose **Voice Routing > Trunk Configuration**. Double-click **Global** to see that option.

For further tips, log into the AltiGen Partner Knowledgebase (<http://thinklync.altigen.com>) and search for the article, “MaxACD Troubleshooting.” This article contains a list of common problem areas and configuration settings that you should check before you contact AltiGen Support. It also explains how to run traces and gather MaxAgent logs.



Performance

The following table illustrates feature capabilities based upon the type and speed of your processor, the amount of memory available, and the size of the hard drive.

Performance: MaxACD 6.5 for Lync		
System Configuration (Windows 2008 R2 SP1)	Vmware All-in-one	Installed on 2008 Telecom Server All-in-one
Virtualization software version	Vmware version (7)	
CPU	Intel Xeon E5620 2.4GHZ	Intel Core2 6600 2.4G HZ
Memory	4G	2G
Hard Drive	50G Allocated	150G
Maximum HMCP Resources		
Max G.711 Voice Processing Resources	600	600
Max G.723/G.729 Processing Resources	60	60
Max Recording Sessions	256	256
Max Number of Lync Extensions	512	512
Max Number of Virtual Extensions	2000	2000
Max number SIP Trunks	300	300
Maximum Group/Agent Configuration		
Max Number of Workgroups	128	128
Max Number of Agents Configured per Workgroup	512	512
Max Number of Logon Agents per System	256	256
Max Total Number of Agents Configured in all Workgroups	640	640
Maximum CT Sessions		
Max Number of MaxAgent Sessions	256	256
Max Number of MaxSupervisor Sessions	20	20
Max Number of Agent Appearances in MaxSupervisor	512	512
Max Number of Workgroups Monitor in MaxSupervisor	10	10
Max Number of MaxAdmin Sessions	5	5
Maximum Call Volume		
Max Hourly Call Volume	5000	5000