



MaxACD Release 7.1

All-in-One Deployment Guide for Enterprise Environments

April 24, 2019



NOTICE: While every effort has been made to ensure accuracy, Altigen Communications, Inc., will not be liable for technical or editorial errors or omissions contained within the documentation. The information contained in this documentation is subject to change without notice.

This documentation may be used only in accordance with the terms of the Altigen Communications, Inc., License Agreement.

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

All product and company names herein may be trademarks of their registered owners. Copyright © Altigen Communications, Inc. 2019. All rights reserved.



Contents

Introduction	5
Important Hardware Considerations	5
Components of MaxACD 7.1	5
Component Requirements	5
Client Requirements	6
Cumulative Updates	9
MaxServer Licenses	9
System Architecture	10
MaxACD Installation	10
Step 1: Plan and Prepare	10
Step 2: Create a Trusted Application Pool on the Microsoft Unified Communication Server	13
Step 3: Make the System an Application Server	14
Step 4: Install MaxACD	20
Step 5: Log into the Service Hub and MaxAdmin	24
Step 6: Register the System Key and Load the License File	26
Step 7: Configure Exchange UM for Workgroup Voicemail	28
Step 8: Configure the System	28
Step 9: Configure the MaxACD External Logger Service	29
Step 10: Turn off SIP Refer	33
Enable Windows Authentication for External Logger	33
Federated Deployments	35
dbConnect Service Configuration Deployment Steps	35
Additional Configuration Steps for Federated Users	36
MaxACD Redundancy Installation	36
Redundancy Architecture	37
Switchover Considerations	38
Deploy a Redundant System	38
Configure the Database for Redundancy	42
Change IP Addresses to FQDNs	50
Microsoft UC Paired Pools Deployment	51
Overview of MaxACD Paired Pools Deployment	51
Configuration Procedures	51
How to Fail Over to the Backup Server	53



- Deploying a Stand-alone Web Portal.....55
- Exchange UM Integration Utility.....55
- SQL Authentication of External Logger Service.....56
- Operational Notes.....59
- Uninstalling MaxACD.....60
- Altigen Technical Support.....60



Introduction

This guide details the hardware and software requirements and basic configuration steps that are necessary to connect Altigen MaxACD to a Microsoft® Lync™ or a Skype for Business Server.

If you are upgrading from an earlier version of MaxACD, follow the steps in the *MaxACD 7.1 Upgrade Guide* instead of the procedures in this guide.

This guide does not cover the process of configuring the Web IM Chat feature; refer to the *MaxACD 7.1 Web IM Deployment Guide* for those instructions.

Important Hardware Considerations



Before you deploy MaxACD 7.1 or migrate from an earlier release, make sure that your Skype for Business servers (including the front-end servers, mediation servers, and SQL servers) all meet the requirements as published by Microsoft. Most critical are the CPU, SSD, and memory requirements.

For those organizations who may be upgrading from MaxACD Release 6.5.8, be aware that Release 6.5.8 uses media resources directly from the HMCP engine that is built in MaxACD. MaxACD 7.1, however, utilizes voice media and conference resources on the Skype front-end and back-end servers. In other words, MaxACD 7.1 may have performance issues if your Skype4Business Servers' hardware does not meet Microsoft's requirements, **even though MaxACD Release 6.5.8 performed fine on the same hardware.**

For more information, you can search for "Lync 2013 hardware requirement" or "Skype for business hardware requirement" on the web. The following articles may also help clarify Microsoft requirements:

[https://technet.microsoft.com/en-us/library/gg398835\(v=ocs.15\).aspx](https://technet.microsoft.com/en-us/library/gg398835(v=ocs.15).aspx)

<https://technet.microsoft.com/en-us/library/dn951388.aspx>

Components of MaxACD 7.1

In this version of MaxACD, all of the components are installed on a single machine.

- **MaxACD AS** – The MaxACD Application server, which provides IVR and ACD feature services.
- **MaxACD Proxy** – A UCMA-based application service residing in a *Trusted Application Pool*. MaxACD Proxy provides SIP signaling and media codecs through UCMA. The MaxACD Proxy handles calls using the UCMA API, and it interacts with MaxACD AS for Workgroup and IVR call processing.
- **Service Hub** – This component is new in Release 7.1; the Service Hub provides a single sign-on for customer who have deployed MaxACD and various add-on applications.
- **MaxAdmin** – A web-based program, MaxAdmin, is used for feature provisioning and is used by IT administrators and workgroup /MaxGroup supervisors. This application obtains company and Skype user information from Active Directory (AD).

Make sure that your browser has JavaScript enabled, so that you can see all of the information in the portal, including the license information.

- **Service Hub DB** – A configuration database hosted by a MS SQL Server or SQL Server Express. MaxACD Proxy, MaxACD AS, and MaxAdmin all read configuration settings from the Service Hub database.

Component Requirements

Minimum requirements for the MaxACD server are as follows:

- Quad-core CPU
- 4GB memory



- 100GB available hard drive disk space
- SSD or similar performance

The following tables list the requirements for the components of MaxACD 7.1.

Component Requirements	
MaxACD Server	<ul style="list-style-type: none"> • Windows Server 2012 R2 with SP1 or later • .Net 4.6 • IIS 8.5 • Chrome, Internet Explorer 11, or Edge • A monitor with at least 1024 x 768 resolution
Service Hub	<ul style="list-style-type: none"> • Windows Server 2012 R2 with SP1 or Windows Server 2016 • .Net 4.6 • IIS 8.5
Service Hub Database Internal	<ul style="list-style-type: none"> • Microsoft SQL Express Server 2014 SP1
Service Hub Database External	<ul style="list-style-type: none"> • Microsoft SQL Express Server 2014 SP1
MaxACD Proxy/Redirector	<ul style="list-style-type: none"> • Windows Server 2012 R2 with SP1 • .Net 4.6 • IIS 8.5
MaxAdmin	<ul style="list-style-type: none"> • Windows Server 2012 R2 with SP1 or Windows Server 2016 • .Net 4.6 • IIS 8.5 • Internet Explorer 11 and Edge, or Chrome
MaxACD CWS DB Internal	<ul style="list-style-type: none"> • Microsoft SQL Express 2014 SP1 (32-bit)
MaxACD CWS DB External	<ul style="list-style-type: none"> • Microsoft SQL Server 2014 SP1
External CDR Database	<ul style="list-style-type: none"> • Microsoft SQL Server 2014 SP1
Email Integration	<ul style="list-style-type: none"> • Microsoft Exchange Server 2013, 2016, and Exchange Online
Microsoft Lync/Skype for Business	<ul style="list-style-type: none"> • Lync Server 2013, plus the latest CU that has been approved by Altigen • Skype for Business 2015, plus the latest CU that has been approved by Altigen
Web Chat Server	<p>Note: The Web Chat server is not supported on Windows 10.</p>

Client Requirements

The following table lists the requirements for the MaxACD client applications.

Note: For client systems that are not already running .NET 4.6, you must install .NET 4.6 before you upgrade or install MaxAgent and/or MaxSupervisor on those systems.



Client Requirements	
MaxAgent	<p>Supported operating systems</p> <ul style="list-style-type: none"> • Windows 8.1 (64-bit) • Windows 10 • .NET Framework 4.6 • Outlook 2010 <p>Hardware minimum requirements</p> <ul style="list-style-type: none"> • 2GHz CPU • 5GB available disk space • 1GB RAM • SVGA monitor 1024 x 768 with 256-color display • Keyboard and mouse <p>Lync/Skype requirements</p> <ul style="list-style-type: none"> • Lync 2013 desktop client • Skype for Business 2015/2016 desktop client
MaxSupervisor	<p>Supported operating systems</p> <ul style="list-style-type: none"> • Windows 8.1 (64-bit) • Windows 10 • .NET Framework 4.6 <p>Hardware minimum requirements</p> <ul style="list-style-type: none"> • 2GHz CPU • 5GB available disk space • 1GB RAM • SVGA monitor 1024 x 768 with 256-color display • Keyboard and mouse <p>Lync/Skype requirements</p> <ul style="list-style-type: none"> • Lync 2013 desktop client • Skype for Business 2015 desktop client
MaxInSight	<p>Supported operating systems</p> <ul style="list-style-type: none"> • Windows 8.1 (64-bit) • Windows 10 <p>Minimum hardware requirements</p> <ul style="list-style-type: none"> • 1GHz CPU • 5GB disk space • 1GB RAM • SVGA monitor 1024 x 768 with 256-color display or better • Keyboard and mouse



Client Requirements	
<p>VR Manager</p> <p>A VR Manager license must be installed in MaxAdmin</p>	<p>Supported operating system for the VRM Server</p> <ul style="list-style-type: none"> Windows Server 2012 R2 SP1 The installation program will automatically install JAVA JRE 1.8.0.171 VRM Server should be installed on a standalone server, not on the MaxACD server. <p>During a new installation of VRM, SQL Express 2014 will automatically be installed.</p> <p>Minimum hardware requirements for the VRM Server</p> <ul style="list-style-type: none"> 2GHz Quad-core CPU For installation: 10GB disk space (more space is required for storing voice files) 3GB RAM <p>Supported operating systems for the VRM Client</p> <ul style="list-style-type: none"> Windows 8.1 64-bit or Windows 10 .Net 4.5 <p>Minimum hardware requirements for the VRM Client</p> <ul style="list-style-type: none"> Intel 2GHz Pentium 4 or equivalent 40GB available disk space and 2GB RAM
<p>Advanced Call Router (must be installed on the same machine as MaxACD Admin)</p>	<p>Supported operating system</p> <ul style="list-style-type: none"> Windows Server 2012 R2 SP1 <p>Minimum hardware requirements</p> <ul style="list-style-type: none"> Intel 2GHz Pentium 4 or equivalent 40GB available disk space 2GB RAM
<p>MaxReports</p>	<p>Supported operating systems</p> <ul style="list-style-type: none"> Windows Server 2012 R2 with SP1 JAVA JRE 1.8.0.171 Tomcat 8.5 will be automatically installed Database with ODBC/JDBC Driver SQL Server <p>Minimum hardware requirements</p> <ul style="list-style-type: none"> 2GHz CPU 60GB available disk space 3GB RAM <p>Client system requirements</p> <ul style="list-style-type: none"> Chrome or Internet Explorer 11 or Edge
<p>AltiSDK</p>	<p>Supported operating systems</p> <ul style="list-style-type: none"> Windows Server 2012 R2 with SP1 Windows 8.1 64-bit Windows 10
<p>AltiControl</p>	<p>Supported operating systems</p> <ul style="list-style-type: none"> Windows 8.1 64-bit Windows 10



Cumulative Updates

MaxACD is a component of Microsoft UCMA server roles for Skype for Business Server.

Important! It is important that you check with Altigen **before** applying a Cumulative Update, to make sure that the CU is supported by Altigen. Contact your Altigen representative for a list of approved CU updates.

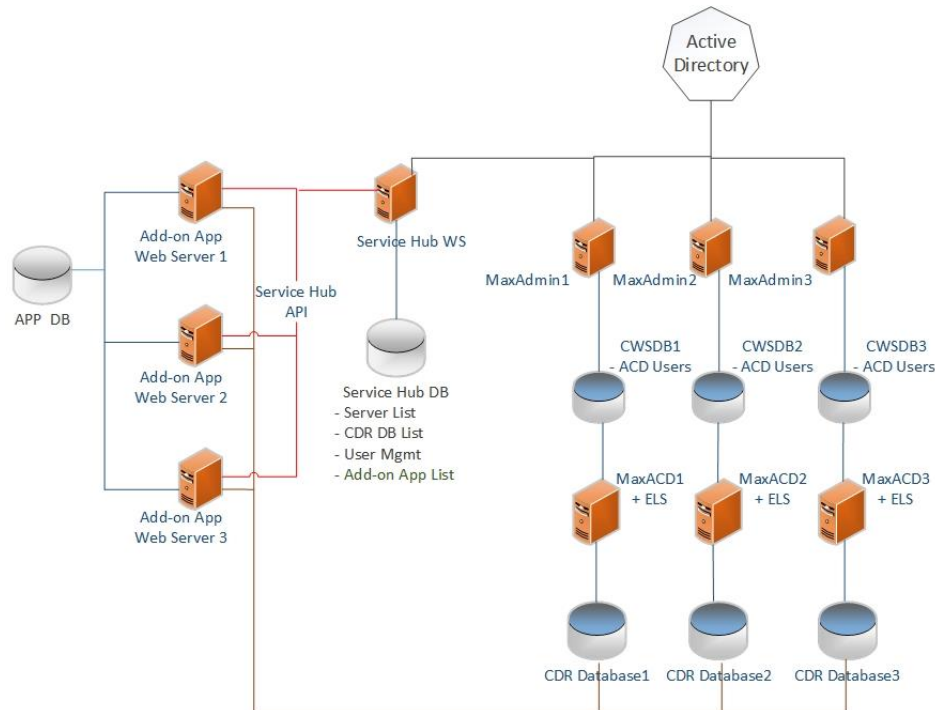
MaxServer Licenses

The following table lists the licenses available for new MaxServer customers.

Licenses for MaxACD	
MaxServer Base Server License (9Unn0)	This base license enables basic functions for MaxServer. This license does not include MaxGroup or ACD functionality; therefore, customers must also order one of the following licenses: <ul style="list-style-type: none"> • MaxGroups Feature License • MaxACD Feature License
MaxGroup Feature License (6MG00)	This license enables MaxGroups and AA/IVR features; the MaxServer Base Server License is required.
MaxGroups Seat License (RYnn0)	
MaxACD Feature License (6CC00)	This license enables workgroup, chat, and AA/IVR features; the MaxServer Base Server License is required
Advanced Call Router License (6CR01)	
MaxAgent Seat Combo License (9Knn0)	This license supports both voice and chat media. This license requires a MaxACD Feature License
MaxSupervisor License (RBnn0)	This license requires a MaxACD Feature License
Workgroup Recording License (R9nn0)	This license requires a MaxACD Feature License
Redundancy License (6RD00)	This license requires a MaxACD Feature License
VR Manager (6VM02)	This license requires a MaxACD Feature License
Salesforce Integration Seat License (RNnn0)	This license requires a MaxACD Feature License
Client SDK Seat License (ACD-CLTSDK)	

System Architecture

The following figure illustrates the typical configuration for MaxACD 7.1 in an Enterprise (on-premise) deployment.



The Application server can reside in a different location, as long as it is in the same Windows Domain. A VPN is required.

MaxACD Installation

Follow these instructions to install MaxACD 7.1.

Note: To deploy a redundant system, review the section, [MaxACD Redundancy Installation](#) on page 35.

Step 1: Plan and Prepare

First, plan your MaxACD deployment and make sure that the server has all of the required components.

Plan your Deployment

Before you begin, carefully plan the following four elements:

- A. **A Fully Qualified Domain Name (FQDN) for the Trusted Application Pool** for each MaxACD server

This FQDN should **not** be the same as the MaxCS server's FQDN, even if it points to the same IP address.

Note that in large call center environments (larger than 300 concurrent agents) you may need multiple MaxACD servers. In this case, you will need a separate (unique) Trusted Application Pool for each MaxACD server.

- B. **A Lync Trusted Application ID** that will be assigned to each MaxACD server



Create a unique Application ID for each MaxACD server. These are names that you come up with yourself. Each name should be a descriptive name that will be used by Skype for Business to create an URN (Uniform Resource Name). The URN is used to authenticate the MaxACD server role. You will use these names in Step 2, as *Your_ApplicationID*.

C. A Trusted Application Endpoint Prefix for each MaxACD Server

You will need these names during the installation of MaxACD, on page 23. In that example, we use *Corp* as the Application Endpoint Prefix. These names must be unique for each MaxACD server installed against the same Microsoft Unified Communications (MSUC) instance.

D. A MaxACD System ID for each MaxACD Server

Each MaxACD server needs a unique MaxACD System ID number for the MaxACD installation. (The reason for the unique MaxACD System ID is that if two or more systems share the same CDR or VR Manager database, then having the same System ID may cause conflicts.)

Redundant pairs must have the same ID.

This is not the same as the Microsoft Unified Communications Trusted Application ID. We mention this System ID here for planning purposes; you will enter this ID in the MaxACD installation procedures later in this guide.

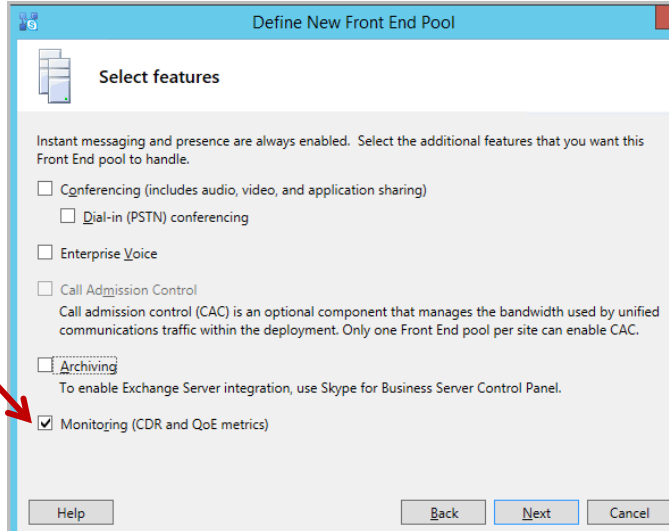
For convenience, you can use the space below to note the Application Pool FQDN, Application ID, and Endpoint Prefix for each MaxACD server planned for your environment.

Server	Redundant? Y/N	A. FQDN for Trusted Application Pool	B. Lync Trusted Application ID	C. Trusted Application Endpoint Prefix	D. MaxACD System ID

Prepare the MaxACD Server

The next step is to prepare the server for installation. It is important that all of the services and components are installed before you begin your Skype for Business configuration.

1. Collect the following:
 - **MaxACD 7.1 installation media:** The CD (or other media) that contains the MaxACD 7.1 installation program.
 - **Software license key:** A 20-digit key located on the front of the End User License Agreement.
2. When you install the Skype for Business Front-end Pool, make sure that you install the monitoring feature. If you did not install this tool, open Topology Builder, right-click on the Front-end Pool, choose **Edit Properties > General** and check the option **Monitoring (CDR and QoE metrics)**.

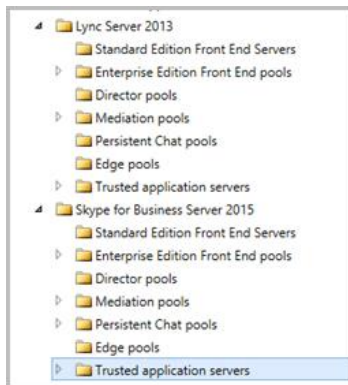


3. On the server where you will install MaxACD 7.1, install Windows Server 2012 R2 or Windows Server 2016.
4. Join the system to the same domain as your Skype for Business server.
5. Perform the following steps (Windows will prompt you if any reboots are required):
 - a) In Windows 2012 R2, search for "Server Manager" and open it.
 - b) In *Server Manager*, click **Add Roles and Features**.
 - c) In the *Features* section, check **.NET Framework 3.5 Features**.
Windows will prompt you to add other related features; accept all of the related features.
 - d) In *.NET Framework 4.5 Features*, check **ASP.NET 4.5**. In *WCF Services*, check **TCP Port Sharing**.
 - e) Make sure that **Windows PowerShell** is selected.
 - f) In *User Interfaces and Infrastructure*, make sure that **Desktop Experience** is checked (this applies only for Windows Server 2012 R2).
 - g) In *Message Queuing*, make sure that **Message Queuing Server is checked**.
 - h) Check **Windows Identity Foundation 3.5**.
6. Click **Next**, and then click **Install** to install the features you selected. Do not close the *Add Roles and Features* wizard until the installation progress bar shows 100%.
7. Reboot Windows to finish all pending tasks related to the installation.
8. Install Unified Communications Managed API Runtime (UCMARuntimeSetup.exe). You can download this from the Microsoft web site.
 - Install version UCMA 4.0 for Lync 2013, version 5.0.8308.0:
<https://www.microsoft.com/en-us/download/details.aspx?id=34992>
 - Install version UCMA 5.0 for Skype for Business 2015, version 6.0.9319.0:
<https://www.microsoft.com/en-us/download/details.aspx?id=47344>

Step 2: Create a Trusted Application Pool on the Microsoft Unified Communication Server

Next, you will create a Trusted Application Pool on the front-end server.

- If the Microsoft Unified Communications Server role on the front-end server is Lync 2013, create a 2013 Trusted Application Pool.
- If the role on the front-end server is Skype, create a Skype for Business Trusted Application Pool.
- If there are multiple Server roles on the front-end server, you must add the Trusted Application Pool to the Skype server role.



The examples in this section use the following placeholder names:

- **Lyncdomain.com** is used as your Lync/Skype domain.
- **MaxAcdPool.lyncdomain.com** is used as the name for the Trusted Application Pool.
- **Pool01.lyncdomain.com** is used as your front-end pool.
- **MaxACDA.lyncdomain.com** is used as a stand-alone or first redundant MaxACD server's FQDN (fully qualified domain name).

1. Log into the Skype Front-end server as a Domain user with Administrative privileges.

(If this is a redundant system and you are installing the second system, the trusted application pool and ID should have already been created; you can skip this step and go to step 3. If this is a stand-alone, or the first redundant system, continue with step 2.)

2. Open the Skype for Business Server Management shell.

You will enter four commands in Skype for Business Server Management Shell on the front-end server. The commands in red are single-line commands. When you enter them, do not separate them into multiple lines. Confirm the Microsoft UC-dependent attributes, such as *Site ID*, with your MSUC system administrator.

As mentioned on page 10, you should create a unique name for the Application ID. This name will be used by Skype for Business to create a Uniform Resource Name.

```
New-CsTrustedApplicationPool -Identity MaxAcdPool.lyncdomain.com -Registrar
pool01.lyncdomain.com -Site <Site ID> -ComputerFqdn MaxACDA.lyncdomain.com
```

```
Enable-CsTopology
```

```
New-CsTrustedApplication -ApplicationId Your_ApplicationID -TrustedApplicationPoolFqdn
MaxAcdPool.lyncdomain.com -Port 7000
```

```
Enable-CsTopology
```

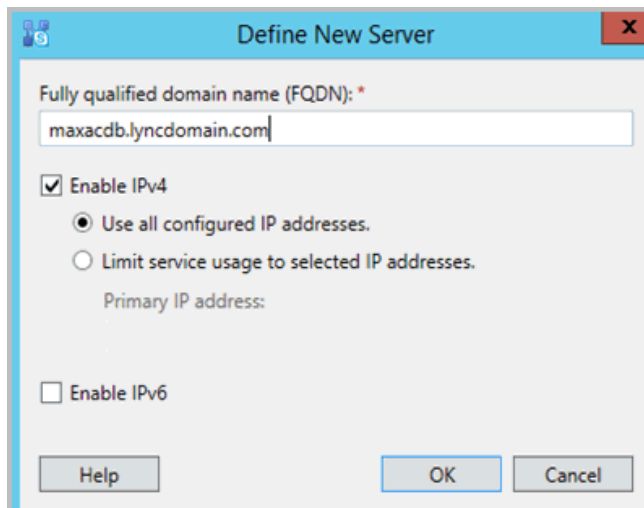
Note: **YOU MUST USE PORT 7000** for each MaxACD instance. Do not use a different port or the deployment may fail.

3. This step is required if you are adding a second server to configure redundancy. If you are not configuring redundancy, skip this step and proceed to *Step 3: Make the System an Application Server* beginning on page 14.

To add the second server,

- a) In the front-end server, open the Topology Builder and download the current topology.
- b) Go to the trusted application pool and add the redundant server to the trusted application pool.

In this example, *maxacda.lyncdomain.com* is the first MaxACD server, and *maxacdb.lyncdomain.com* is the second MaxACD server.



4. Publish the topology. Proceed to the next section.

Step 3: Make the System an Application Server

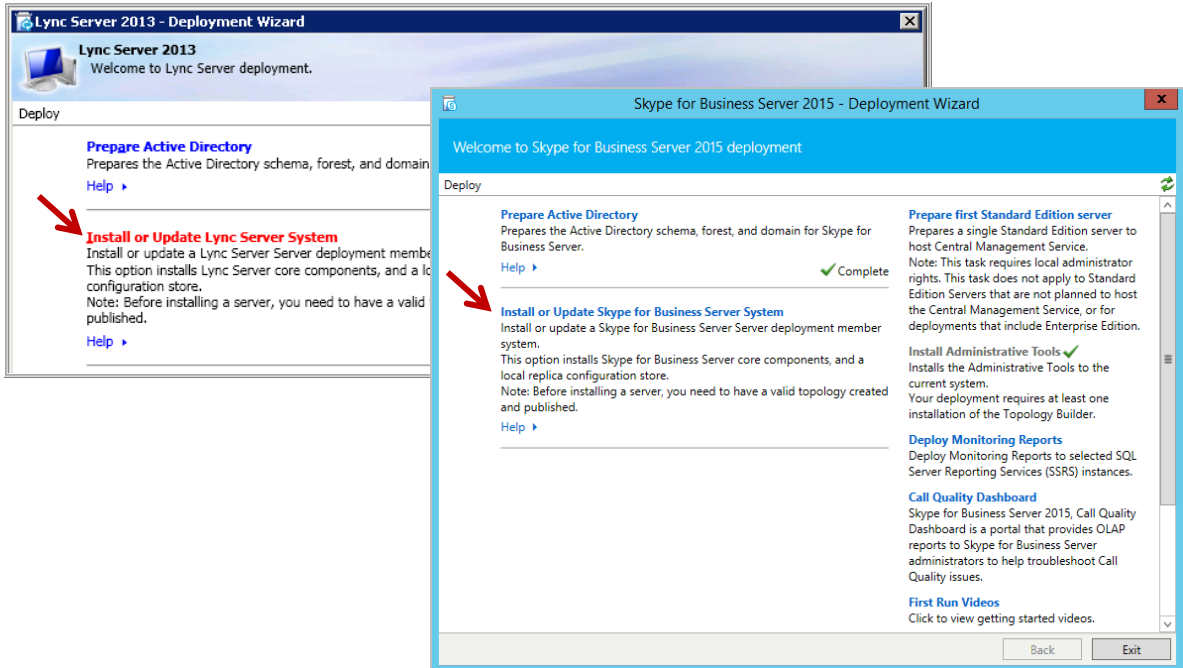
Next, you will deploy Skype core components on the system where you will be installing MaxACD 7.1.

3A: Install Local Configuration Store

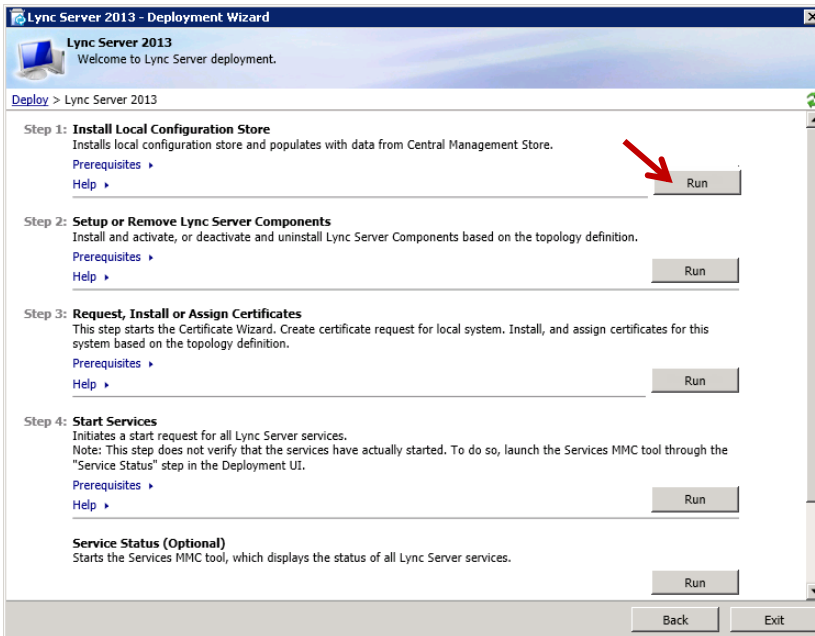
The processes for installing Lync 2013 and Skype for Business are very similar.

1. Log in as a user in RTC Universal Server Admins AD group. Use your Lync Server or Skype Installation media and run *the Lync Server Deployment Wizard*.

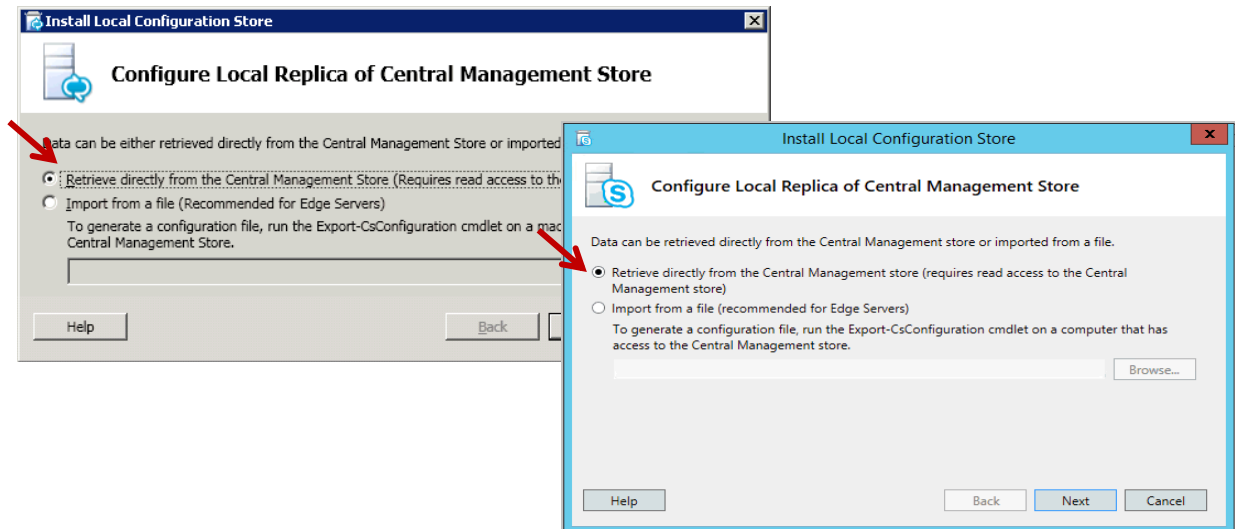
2. On the main page of the wizard, choose **Install or Update Lync Server System**.



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



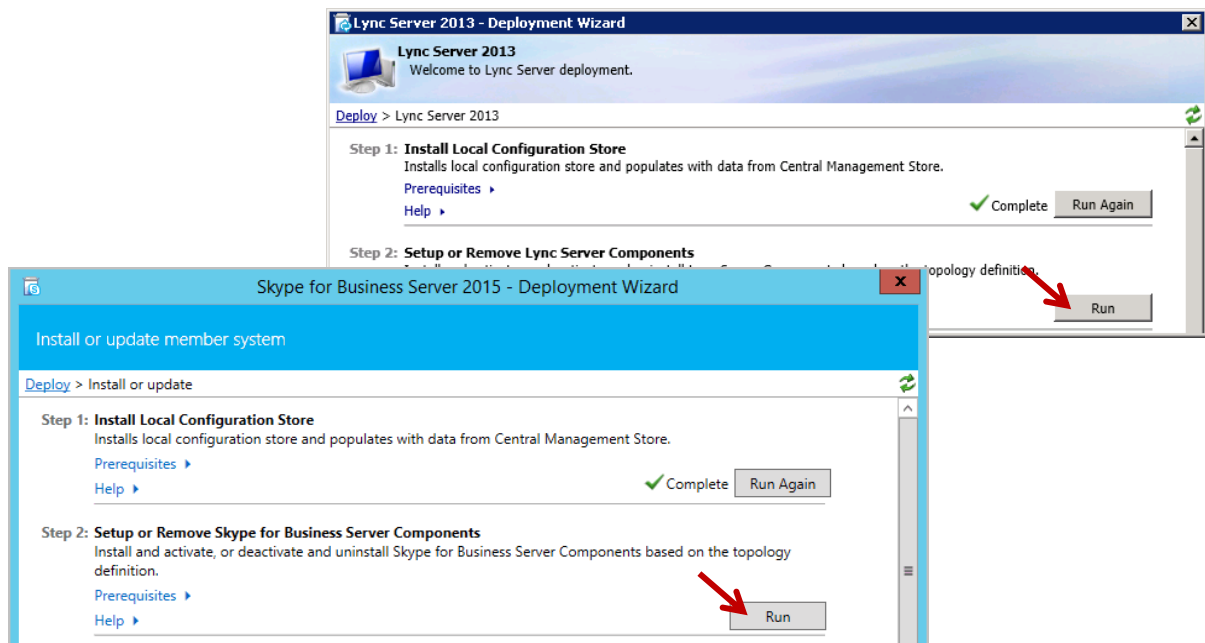
- In the next panel, choose **Retrieve directly from the Central Management Store**, and then click **Next**. When processing has completed, click **Finish**. You return to the main page of the Deployment wizard.



3B: Set Up Lync Server Components

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

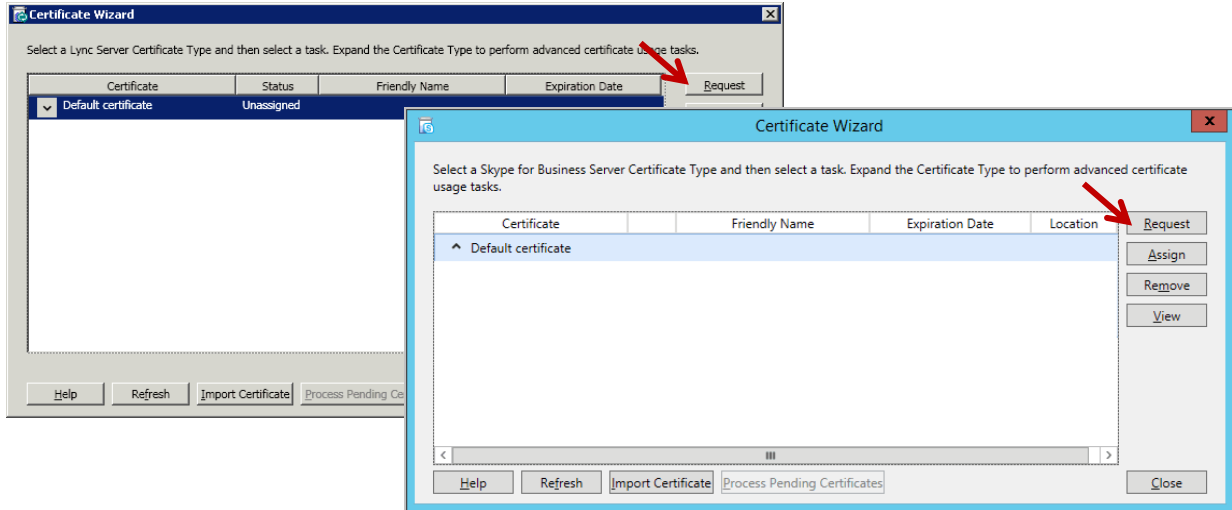
Note: In Lync Server 2013, you may not see the green checkmark when Step 2 is complete.



3C: Install and Assign Certificate

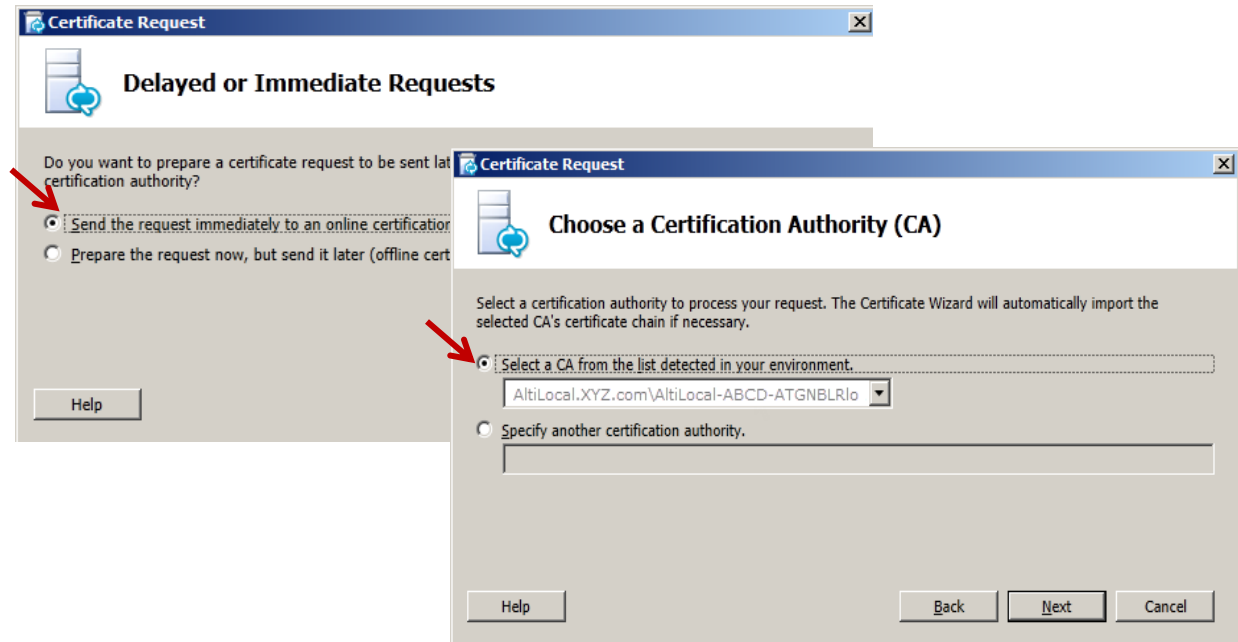
Next, you will install and assign a certificate.

1. For “Step 3, Request, Install, or Assign Certificates,” click **Run**.
2. Select the default certificate, click **Request**, and then click **Next**.

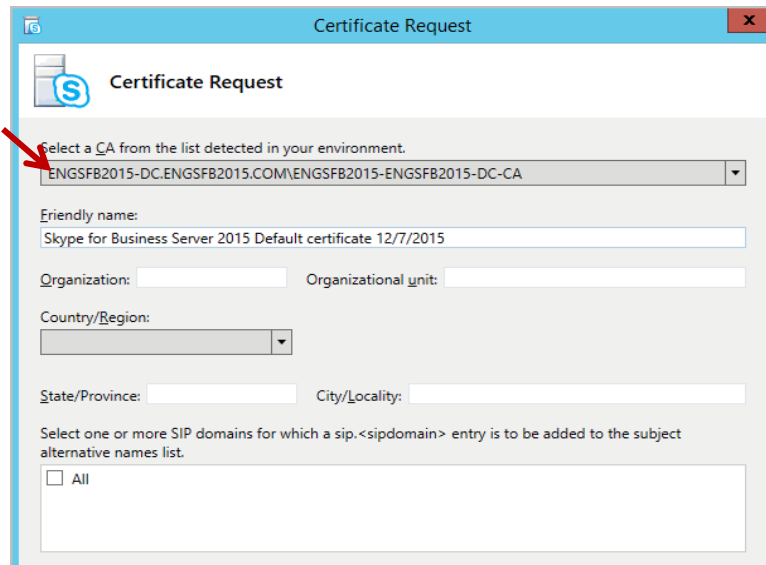


3. In the *Certificate Request* panel, the Lync steps are slightly different from the Skype for Business steps.

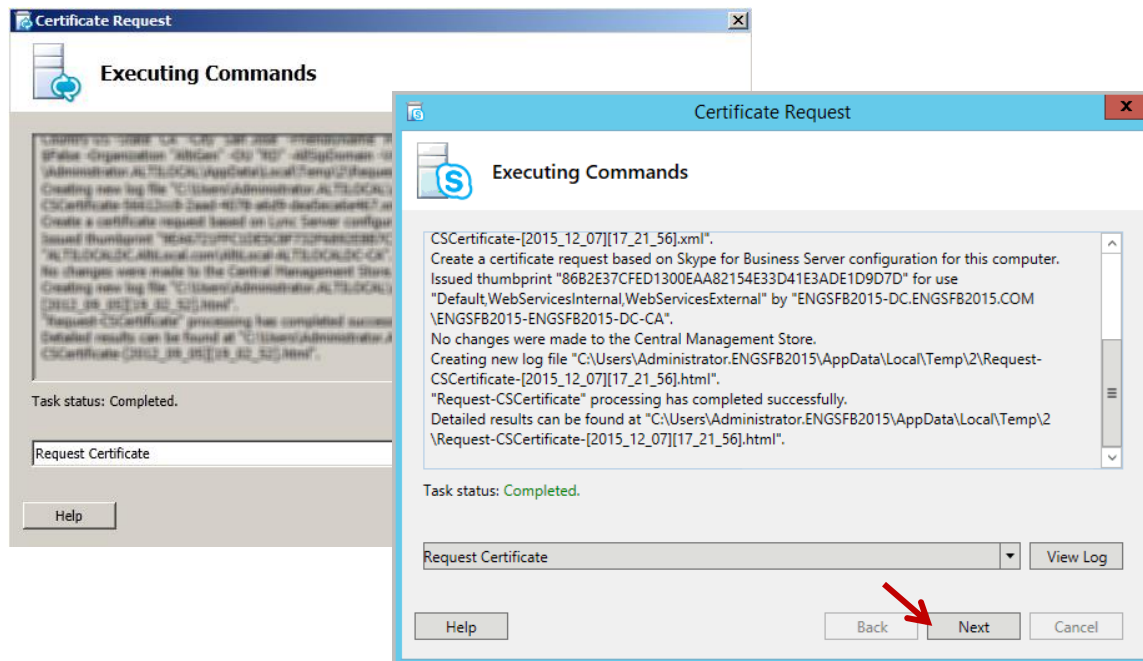
For Lync 2013, select **Send the request immediately to an online certification authority** and click **Next**. Then, choose the Certificate Authority (CA) from the list and click **Next**. Continue through the wizard, providing the information requested for the next few panels.



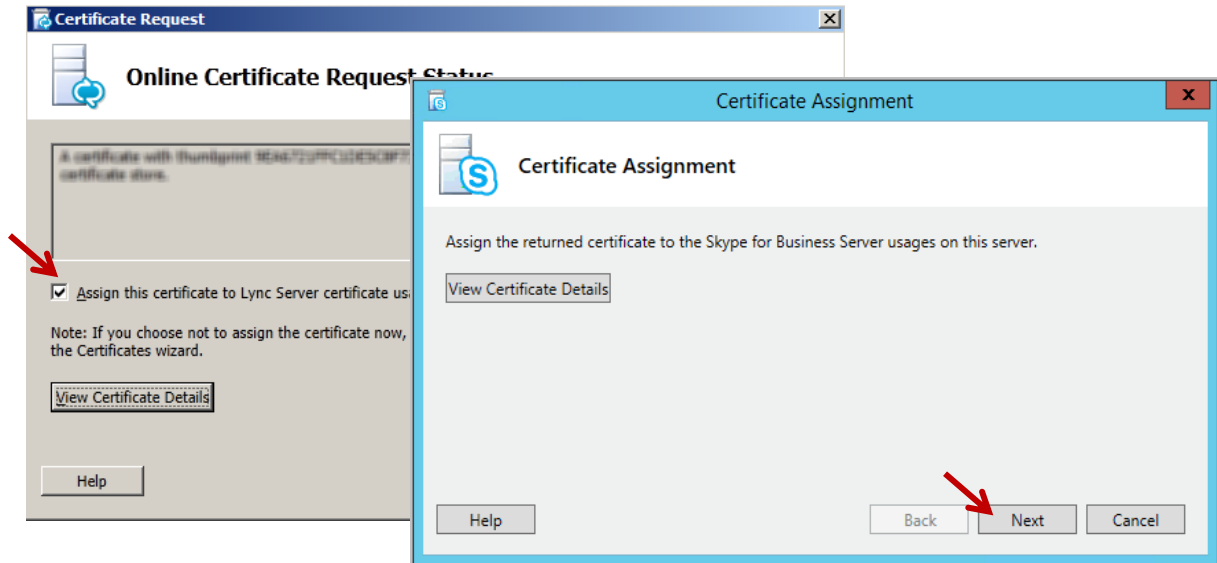
For Skype for Business, select the certificate from the list and provide the information as appropriate. Click **Next**.



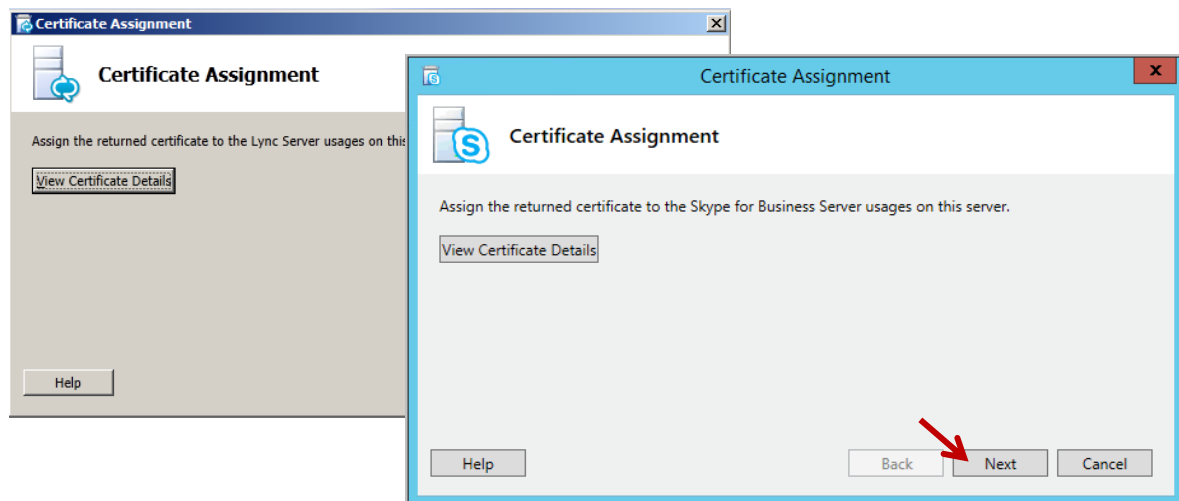
4. When you reach the *Certificate Request Summary* panel, verify that the information on the page is correct. If it is incorrect, click **Back** to correct the details. Otherwise, click **Next**.
5. When the process has finished, click **Next**.



6. Check the box **Assign this certificate to Lync Server/Skype for Business certificate usages** and click **Finish**.

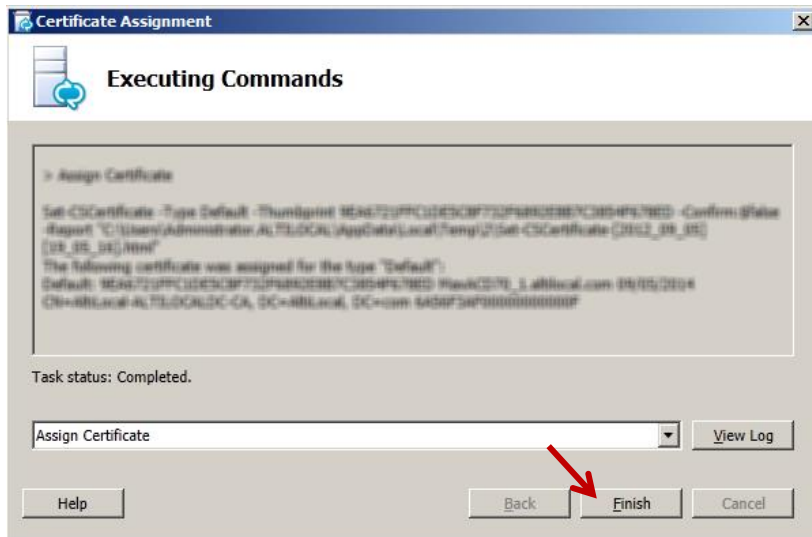


7. Click **Next** to assign this certificate.



8. In the Summary, review the assignment details. If there are no changes, click **Next**.

- When the certificate assignment has finished, click **Finish**. Click **Close** to return to the main page of the Deployment wizard.



Step 4: Install MaxACD

Next, you will install MaxACD 7.1.

Environment Checklist

Check the following conditions before you begin:

- Make sure that your current login Windows user account either has Domain Admin privileges or has all of the following privileges:
 - RTC Universal Server Admins membership
 - Domain Users membership
 - Is an Administrator on the local system
- Confirm that the system has already been joined to the domain where your Skype Server is installed.
- If you are upgrading or re-installing MaxACD 7.0, make sure that you perform the installation under the same Windows user account as during the initial installation. If you do not install under the same user account, SQL may fail to install due to insufficient SQL account rights.

Note: If you are deploying an all-in-one configuration, then a SQL 2014 Express server will be automatically installed to the same MaxACD system. If you are deploying a redundant configuration, then you must install the SQL 2014 Express Server or another version of SQL server in a stand-alone machine. This SQL system cannot be on the same server as the two MaxACD systems. That system cannot be on the same server as the two MaxACD systems, or else it will defeat the purpose of having a redundant configuration. After the SQL server has been set up, make sure that you have the database instance name, SQL SA account and password, because they will be used during procedures in this guide.

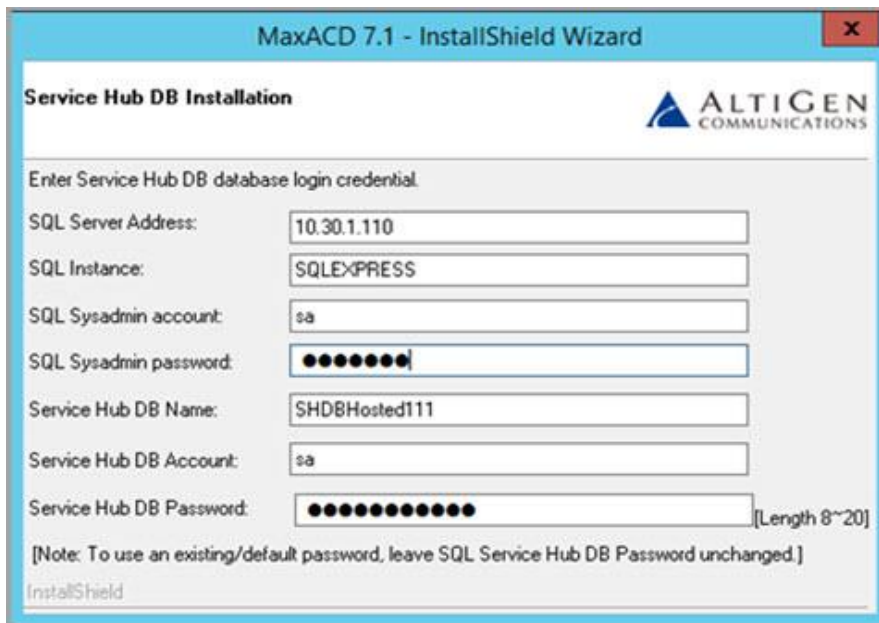
Installation Procedures

- Check with your Altigen representative to determine which CU (cumulative updates) and other updates may need to be applied to the Skype Server on the system where you are installing MaxACD. Make all required updates before you proceed.

2. Close any open Windows applications. Log onto the system as a Domain user with Administrative privileges. From your installation media, run the *setup* file in the *MaxACD* folder.
3. On the introductory screen, click **Next**.
4. Enter a System ID number. This ID number will be used to identify this server and distinguish it from any other servers in your MaxACD deployment. This ID was mentioned earlier, in *Plan your Deployment* on page 10.

Observe the following guidelines:

- **You cannot change the System ID number later.** The only way to change a System ID afterwards is to uninstall MaxACD and then reinstall it.
 - Each MaxACD system **MUST** have a unique ID number **except two systems that are a pair in a redundant configuration.**
 - If you are deploying a pair of servers in a redundant configuration, those two systems **must have the same System ID.**
5. Choose either **Single Server** or **Redundancy**. Click **Next**. (Note: You can convert a single server system to a redundant system later. Refer to the instructions in the separate document, *MaxACD Conversion to a Redundant System*.)
 6. If you chose **Single Server**, skip ahead to step 7.
If you chose **Redundancy**, indicate whether you have already deployed the database.
 - a. If you chose **No**, enter the database login credentials. For a default installation, leave the SQL Instance field blank.



- **SQL Server Address** – The IP Address of your SQL server (use the AlwaysOn Availability Group’s listener IP address, or hostname that resolves to that address).
- **SQL Instance** – SQL Instance name (leave this field blank for a default installation)
- **SQL Sysadmin Account** – SQL Login account name; this is required for creating the database and table for MaxACD Admin
- **SQL Sysadmin Password** – The password for the SQL account
- **Service Hub DB Name** – Enter a name for the Service Hub
- **Service Hub DB Account** – The user name for MaxACD modules to access the Service Hub database



- **Service Hub DB Password** – When the database is created, this password is created for CWSDBServerUser1. If you don't change the password, a hardcoded default password will be used. You can create your own password by changing this password. If you do so, you must remember this password for future installations.
- b. If you chose **Yes** (for a redundant system), enter the details for your SQL server installation.
- **SQL Server Address** – The IP Address of your SQL server
 - **SQL Instance** – SQL Instance name
 - **Service Hub DB Name** – The name for the Service Hub
 - **Service HUB DB Password** – The password for the Service Hub DB account. If the password is incorrect, or if the database is not running, then the installation process will not continue.
7. Choose either Lync 2013 or Skype for Business.
You must choose the Lync/Skype version that matches the version of the application pool where your MaxACD server resides. If you choose a version that does not match, the installation wizard will proceed; however, the MaxACD system will not work.
8. Accept the license agreement. Click **Next**.
9. Enter your name and the name of your company. Click **Next**.

Customer Information
Please enter your information.

Please enter your name and the name of the company for which you work.

User Name:
Windows User

Company Name:
Altigen

InstallShield

< Back Next > Cancel

10. Accept the random password that was generated for you, recording it for future use. Click **Next**.
11. Enter a MaxACD system name. Click **Next**.

Input the system name

Enter ACD System Name with length from 1 to 24 characters. Only alphanumeric characters and "_" are allowed.

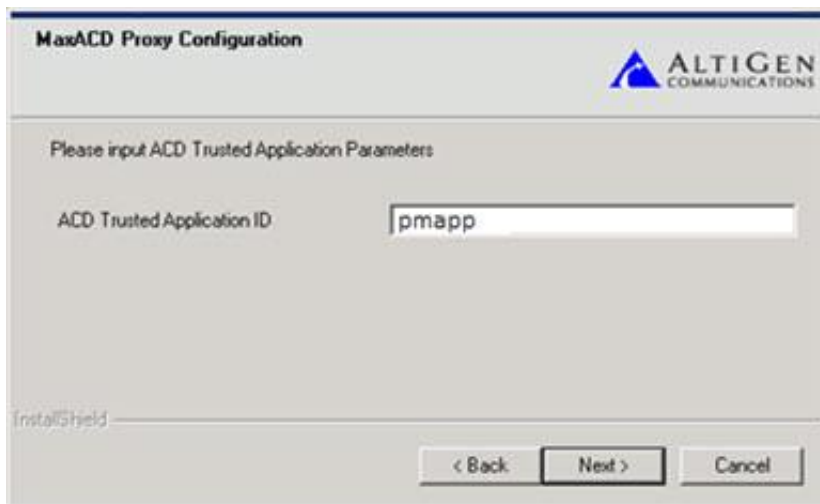
System Name: ACD1

InstallShield

< Back Next > Cancel

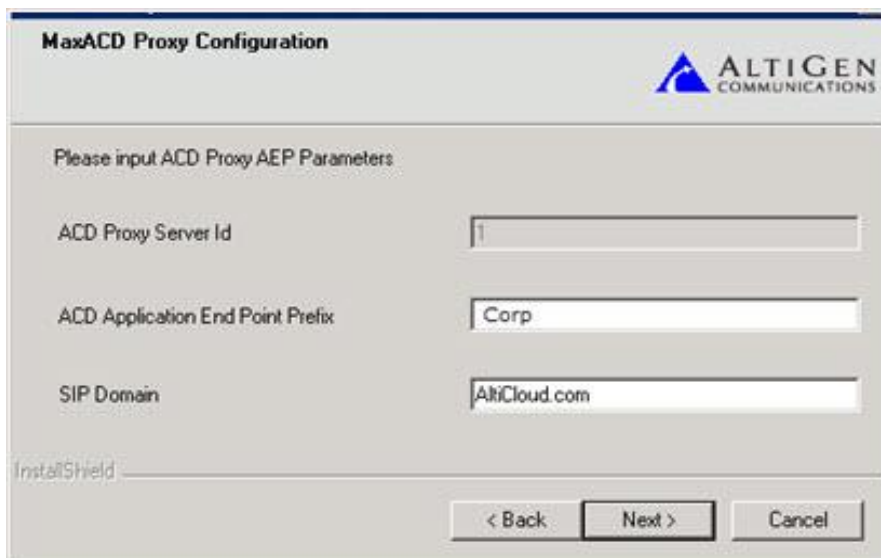
12. Specify a drive and folder destination for MaxACD. Click **Next**.
13. Choose whether to provide the license file now or register later; we recommend that you do this step later. Click **Next**. (If you choose to provide the file now, enter the path to that file.)
14. Enter the FQDN (Fully Qualified Domain Name) of the Trusted Application Pool that you created in *Step 2: Create a Trusted Application Pool on the Microsoft Unified Communication Server*. Click **Next**. The program will take a moment to validate that the pool name you entered is valid.
15. Enter the MaxACD Trusted Application ID that you created in *Step 2: Create a Trusted Application Pool on the Microsoft Unified Communication Server* on page 13. Click **Next**. (For redundancy deployment, enter the same ACD Trusted Application ID for the primary server and the secondary server.)

The program again validates that the ID you enter is valid.



The screenshot shows a dialog box titled "MaxACD Proxy Configuration" with the Altigen Communications logo in the top right corner. Below the title bar, it says "Please input ACD Trusted Application Parameters". There is a text input field labeled "ACD Trusted Application ID" containing the text "pmapp". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

16. Specify an Application End Point (AEP) prefix (which will be used to precede a portal name, viewer name, and dialer name), and enter your SIP domain (SIP domain is the domain where your MaxACD server resides for on-premise deployments). You planned this prefix back in the section *Plan your Deployment* on page 10. (For redundancy deployment, enter a different MaxACD Application End Point Prefix name for the primary server and the secondary server.) Click **Next**.



The screenshot shows a dialog box titled "MaxACD Proxy Configuration" with the Altigen Communications logo in the top right corner. Below the title bar, it says "Please input ACD Proxy AEP Parameters". There are three text input fields: "ACD Proxy Server Id" with the value "1", "ACD Application End Point Prefix" with the value "Corp", and "SIP Domain" with the value "AltCloud.com". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".



17. To begin the installation process, click **Install**. During installation, a window provides the default password.
18. Once the installation process has finished, select **Yes, I want to restart my computer now** and then click **Finish**. Your system will restart.

Note: MaxACD Administrator is installed with HTTP as the default connection. You may want to configure IIS to support an HTTPS connection for this web-based application.

19. After your system reboots, open the Windows Services page.

A new service account was created for MaxACD services.

In following example, SYMPHONY\Alt_i_COBALT200103 is created as the service account. Make sure the account has domain administrator rights, so that Exchange can be synchronized. If you don't want to assign domain admin rights to that service account, then you can change the "Altigen VM Exchange Integration Service" login account to an account with domain administrator right.

In following example, AltIServAdmin@Altigen.com has domain administrator rights. If this is a redundant system, make sure to apply this setting on both the primary and secondary MaxACD servers.

Altigen Lync Proxy Service	Altigen Lyn...	Running	Automatic (D...	SYMPHONY\Alt_i_COBALT200103
Altigen Lync Redirector Ser...	Altigen Lyn...	Running	Automatic (D...	SYMPHONY\Alt_i_COBALT200103
Altigen Switch Gateway Ser...	Altigen Swit...	Running	Automatic	SYMPHONY\Alt_i_COBALT200103
Altigen Switching Service C...	Altigen Serv...	Running	Automatic	SYMPHONY\Alt_i_COBALT200103
Altigen VM AltView Service	Altigen VM ...	Running	Manual	SYMPHONY\Alt_i_COBALT200103
Altigen VM Exchange Integr...	COM Server...	Running	Automatic	AltIServAdmin@altigen.com
Altigen VM Message Service	Altigen VM ...	Running	Manual	SYMPHONY\Alt_i_COBALT200103
Altigen VM POP3 Service	COM Server...	Running	Manual	SYMPHONY\Alt_i_COBALT200103
Altigen VM Postman Service	Altigen VM ...	Running	Automatic	SYMPHONY\Alt_i_COBALT200103

20. After you assign those rights, start the Altigen VM Exchange Integration Service. Wait two minutes and then refresh the Windows Services page, confirm that the Altigen VM Exchange Integration Service is running.
21. Add the FQDN for the Trusted Application Pool and the FQDN for the Trusted Application Server to the domain DNS server. Confirm that you can ping both of them within the same domain.

Step 5: Log into the Service Hub and MaxAdmin

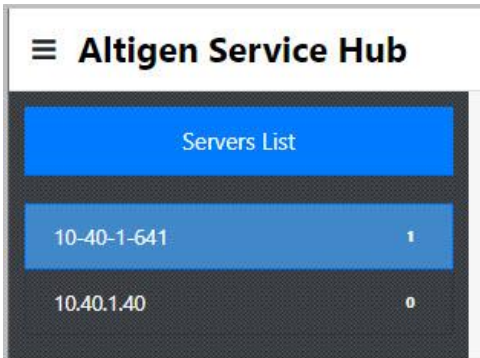
The Service Hub is your starting point; you log into the Service Hub and then open your applications and services from there.

To log into the Service Hub,

1. In your browser, using either the IP address or the FQDN, navigate to the directory where the Service Hub is installed:
`http://[localhost]/ServiceHub/`
For example, `http://10.20.3.40/ServiceHub`
2. The first time you log in, use the default user name "admin" and the default password, which is 22222. For security purposes, change the password as soon as possible. You can do this by clicking your profile button in the top right toolbar.

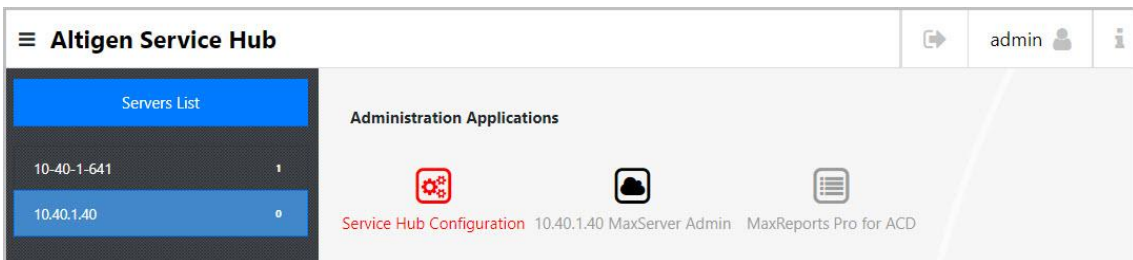
If the login attempt fails, you will need to enter the domain and user ID in the User Name field.

The Service Hub has a list in the left panel. This is a list of your MaxServers, in alphabetical order. The example in the next figure shows an environment with two MaxServers.



In the main panel, you see several icons:

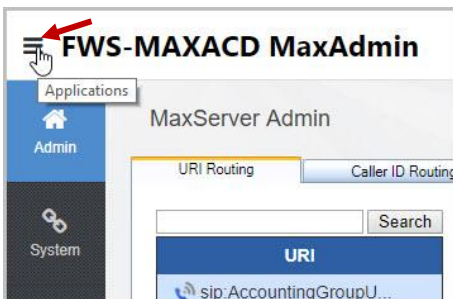
- One icon is “Service Hub Configuration.” You click this to configure options for the Service Hub itself.
- One icon will be for the server that is selected in the left panel. When you click a MaxServer icon, MaxAdmin opens, allowing you to make configuration changes to that server.
- Other icons in that panel represent other services that you have purchased. You click one of those icons to configure that service.



3. Log into the administrator portal (MaxAdmin) for your portal, by clicking its icon in the right panel. It will look something like this, with the server’s name.



MaxAdmin should open at this point. (For future reference, to return to the Service Hub configuration panel, click the *Applications* icon in the top left corner and choosing **Settings**.)



Continue with the next step; you will return to MaxAdmin later.

Step 6: Register the System Key and Load the License File

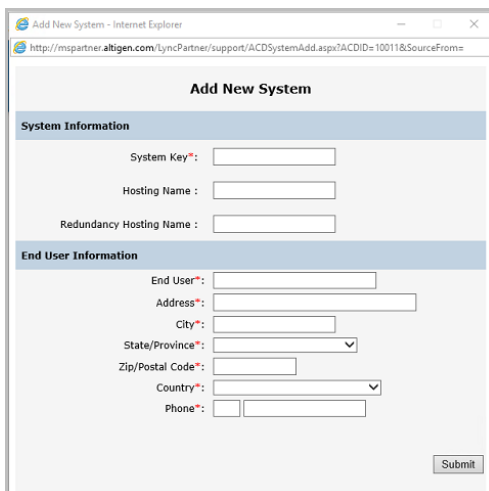
Next, download and register the license files.

1. Log into your partner account in the Altigen Partner portal (<https://mspartner.altigen.com>).
If you do not have login permissions on this site, please contact your VAR or your Altigen representative to obtain a license file, then skip ahead to step 7 on page 27.
2. On the **Support** menu, click **MaxACD**.
3. You can click **List View** to view any existing MaxACD systems in your account.



End User	System Key	Address	City	State	Zip Code	Start Date	Configure	License File
Singapore Office		123 A St	San Jose	CA	94567	02/02/10	Activate Lic	License File
Shanghai Office		456 B St	Fremont	CA	94536	02/02/10	Activate Lic	License File
VOIP Lab Office		fgh	fgh	AL	2424	02/22/10	Activate Lic	License File

4. Click **Add New System**. Enter all of the details of this new system and click **Submit**.



5. Click **Activate License**. Enter the appropriate quantities to activate and then click **Generate License File**.
6. After the license file has been generated, click **Download License File**. Choose whether to email the EXCTL.DAT file or save it. You will need this file in the next step.

Software License Activation

End User:
 System Key:
 Current Registration Version: MAXACD for Lync 7.0
 Target Registration Version: MAXACD for Lync 7.0

License	Activated	Available	Additional Qty
MaxACD Redundancy (6RD00)	1	984	<input checked="" type="checkbox"/>
MaxACD for Lync Server License (9Lnn0)	1	3271	<input type="checkbox"/>
MaxAgent for Lync License (9Anno)	36	1319	<input type="text"/>
MaxSupervisor for Lync License (9Bnn0)	501	1964	<input type="text"/>
MaxACD CRM Integration (RNnn0)	202	176	<input type="text"/>
MAXACD MaxAgent Seat Combo - Voice and Chat (9Knn0)	5	35	<input type="text"/>
Recording Seat (R9nn0)	501	1289	<input type="text"/>

The license activation file was generated successfully. [Download License File](#)

Email License File to:

- On the MaxACD server, open the \Altiserv\exe folder and run the executable *RegLicense.exe*.

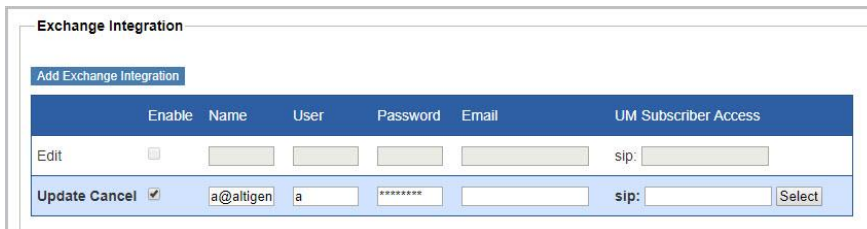
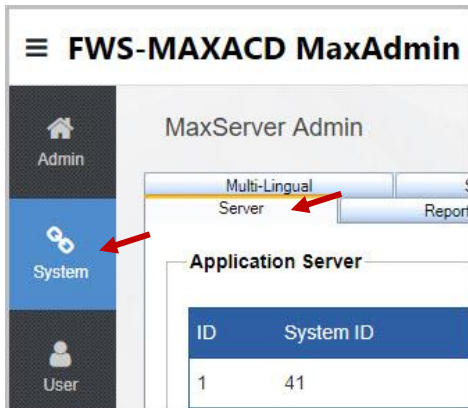
- Check the box **Use Soft System Key**.
- Click **Enter the System Key**.
- Type the system key into the **System Key** field.
- Click **Load**, navigate to the EXCTL.DAT file you downloaded from the Altigen Partner portal, and then click **Open**.
- The licenses should now appear in the window. The licenses are now loaded. You can see these licenses in MaxAdmin, on the *License* tab.

Note: If you accidentally load a license file with insufficient licenses for those already assigned to users, you will need to restart the MaxACD services to recover the license assignments.

Step 7: Configure Exchange UM for Workgroup Voicemail

MaxACD uses Exchange Server for voicemail message storage. You will add a user account for each workgroup voicemail.

1. Within MaxAdmin, configure the client access server address and the Exchange UM subscriber access by selecting **System** on the Sidebar, then selecting the **Server** tab.



2. Complete the fields and click **Update**. For more about the Exchange UM subscriber, refer to page 55.
3. If you plan to configure workgroup voicemail, add a user account in Skype for Business Server and in the Exchange server for each workgroup voicemail. This can be configured in MaxAdmin by selecting **Workgroup > General**. In the next example, `tso-maxacd@altigen.com` is the email / SIP URI that you created for the workgroup.



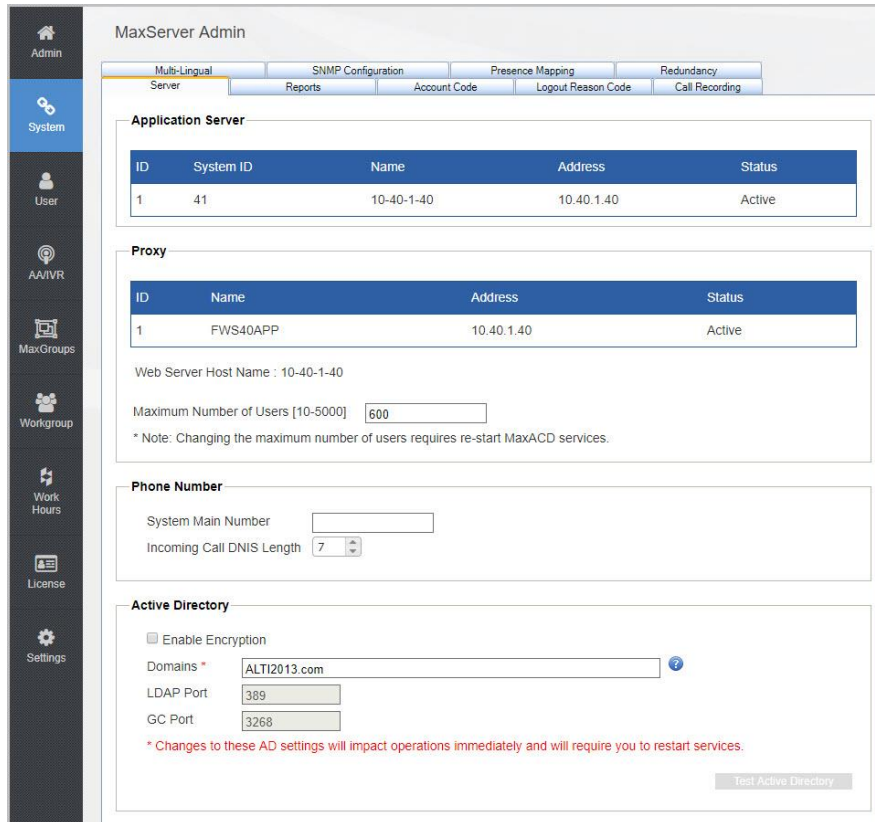
Note: Use a unique email address for each workgroup. Do not use the same email address as another workgroup on a different MaxACD server. The Skype account requires a Skype for Business Enterprise voice feature license.

Step 8: Configure the System

At this point, we suggest that you configure system settings and routing rules, and then set up users and workgroups. For instructions, refer to the *MaxACD 7.1 Administration Manual*.

Make sure that your browser has JavaScript enabled, so that you can see all of the information in the portal. If JavaScript is not enabled, you may not be able to view license information.

See the chapter *Getting Started* in the *MaxACD Administration Manual* for an overview of the MaxAdmin Portal interface and descriptions of the types of configuration you can perform on each tab.



The screenshot shows the MaxServer Admin interface with a sidebar on the left containing navigation icons for Admin, System, User, AA/IVR, MaxGroups, Workgroup, Work Hours, License, and Settings. The main content area is titled 'MaxServer Admin' and features several configuration tabs: Multi-Lingual, SNMP Configuration, Presence Mapping, Redundancy, Server, Reports, Account Code, Logout Reason Code, and Call Recording. The 'Server' tab is active, displaying four sections:

- Application Server:** A table with columns ID, System ID, Name, Address, and Status. It contains one entry: ID 1, System ID 41, Name 10-40-1-40, Address 10.40.1.40, and Status Active.
- Proxy:** A table with columns ID, Name, Address, and Status. It contains one entry: ID 1, Name FWS40APP, Address 10.40.1.40, and Status Active. Below the table, there is a text field for 'Web Server Host Name' with the value '10-40-1-40' and a text field for 'Maximum Number of Users [10-5000]' with the value '600'. A note states: '* Note: Changing the maximum number of users requires re-start MaxACD services.'
- Phone Number:** Text input fields for 'System Main Number' and a dropdown menu for 'Incoming Call DNIS Length' set to '7'.
- Active Directory:** A checkbox for 'Enable Encryption' is unchecked. A text field for 'Domains *' contains 'ALTI2013.com'. Text input fields for 'LDAP Port' (389) and 'GC Port' (3268) are present. A red note states: '* Changes to these AD settings will impact operations immediately and will require you to restart services.' A 'Test Active Directory' button is at the bottom right.

Step 9: Configure the MaxACD External Logger Service

Follow these steps to set up the external logger service, create an external CDR database, and configure MaxReports.

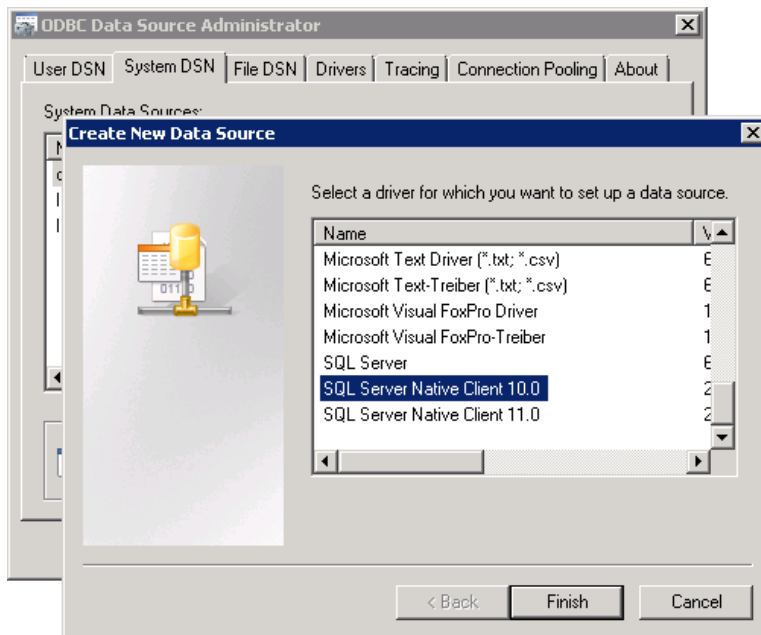
Notes

- We recommend that you configure these steps on a system other than the MaxACD 7.1 server
- If you have already created a new database, you can skip the first two steps

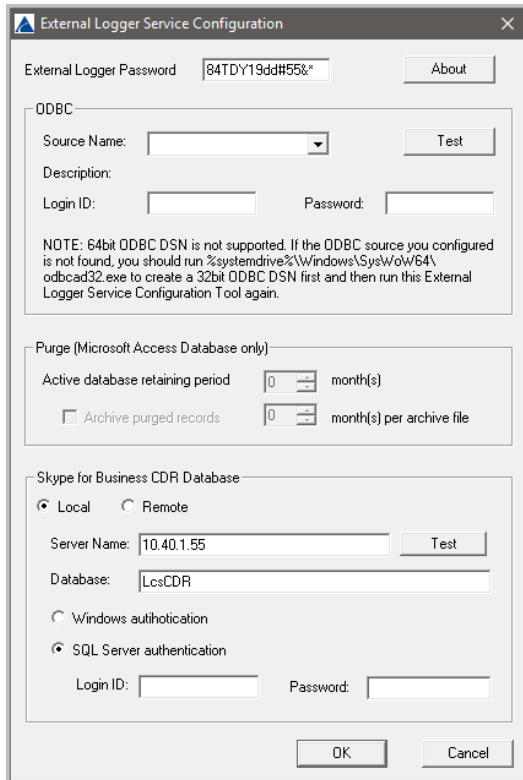
These instructions assume that you have a working knowledge of SQL Server Management Studio.

1. Create a new DB SQL 2014 on the SQL server to host the external CDR database. To do this,
 - a. Open SQL Server Management Studio.
 - b. Create a new database; you will need to provide the name of this database later, in step 3.
 - c. Create a new SQL login user; you will need to provide the name of this database later, in step 3.
2. Create a new ODBC entry. To do this,
 - a. Run `odbc.exe` (The default location for this executable file should be in `%systemdrive%\Windows\SysWOW64` – the exact location was provided when you installed the External Logger Service.) **This must be the 32-bit version; the 64-bit version is not supported.**
 - b. Switch to the **System DSN** tab and add a new ODBC Data Source.

- c. Choose either the SQL Server Native Client 10.0 or 11.0 driver.



- d. Give the new Data Source a name and choose the instance (the one you created during step 2).
- e. Set up log in with SQL Server authentication you created at step 1c.
- f. Change the default database to the one you created at step 1b.
3. Insert the MaxACD 7.1 media and run *Setup.exe* in the External Logger Service folder. Complete the installation process.
4. After you finish installing External Logger, you must run the ELS Configuration tool from the folder where you installed it in the preceding step. By default, this is `\Program Files (x86)\Altigen\External Logger Service`. The program is *ELSCfg.exe*.



- a. Create a password for the External Logger service.
- b. For **Source Name**, choose the ODBC Data Source you created in step 3 from the dropdown list.
- c. Enter its Login ID and password.
- d. Click **Test**. Click **Create Tables** in the pop-up window.
- e. Click **OK** to return to the previous window.
- f. Enter the Skype for Business CDR Database information.
 - If you are deploying a Federated system, check the option **Remote** and complete the fields (the password to the Skype database and the open port that MaxACD listens on). Then, after you have completed the initial deployment, follow the steps in the section [Federated Deployments](#) to configure the dbConnect Service.

Note: If you want to enable Windows authentication, follow the steps in the section [Enable Windows Authentication](#) starting on page 33 **after you complete the steps in this section.**

5. Add external logger in MaxACD Administrator. To do this,
 - a. Log into MaxAdmin (if you did not remain logged in earlier).
 - b. Select **System > Reports**.

Log Service

[Add Log Service](#)

	Enable	Name	Server	Port	Status	Password
	<input checked="" type="checkbox"/>	Internal Log Service	127.0.0.1	10029	Connected	Default
Edit Delete	<input type="checkbox"/>	External Logger	10.40.1.123	10027	Disable	Default

Internal Database Configuration

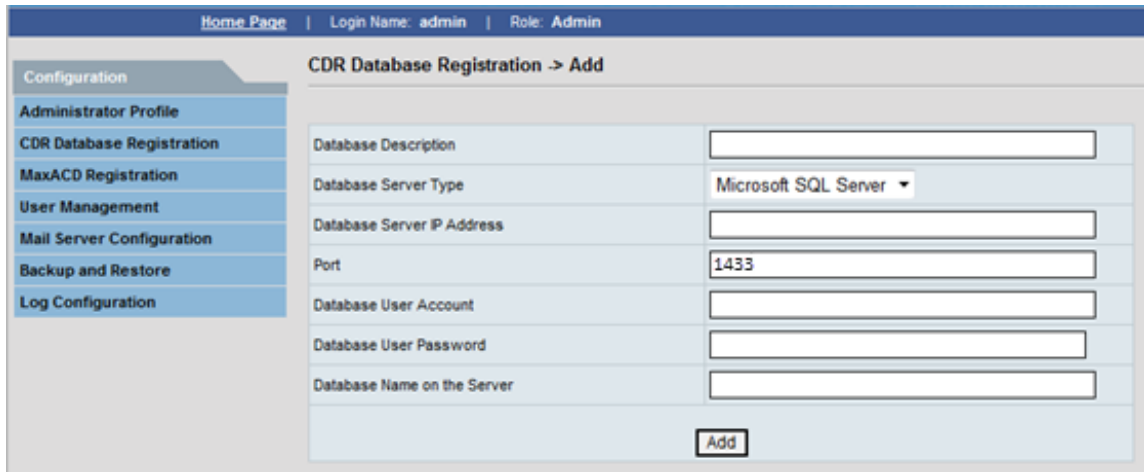
Active database retaining period months

Archive purged records

month(s) per archive file

- c. Click **Add Log Service**.
 - d. Give the new entry a name and set the *Server* field to the IP Address of the external logger service.
 - e. Set the port to **10027** and enter the password that you created for the External Logger service in step 4.a on page 31.
6. To configure SQL Server, follow these steps:
 - a. Open Microsoft SQL Server 2014. Choose **Configuration Tools > SQL Server Configuration Manager**.
 - b. Expand **SQL Server Network Configuration (32-bit)**
 - c. Click **Protocols** for SQLCWSDB1. (This is for the CWS database instance name; it should not be the same name as the external logger database. If you use the default instance, the instance name should be "MSSQLSERVER.")
 - d. Double click **TCP/IP**.
 - e. On the Protocol tab, make sure that *Enabled* is set to **Yes**.
 - f. On the IP Addresses tab, expand **IP All** and enter **1433** for **TCP Port**.
 - g. Click **Apply** and close SQL Server Configuration Manager.
 7. Restart the SQL Server service.
 8. Install MaxReports
 - a. From the MaxACD 7.1 installation media, run the Setup.exe program in the MaxReports folder and install the application.
 - b. Go to the MaxReports web site ([http://\[machinename\]:8080/MaxReports](http://[machinename]:8080/MaxReports)).
 - c. Log in as the admin (default password is '22222').

- d. Click **CDR Database Registration** and then click **Register New CDR Database**.



- e. Enter a database description.
- f. Choose **Microsoft SQL Server** as the Database Server Type.
- g. Enter the IP address of SQL server.
- h. Set the Port to **1433**.
- i. Enter the user name and password that you created in step 1c.
- j. Enter the database name that you created in step 1b (the default name will be EXTERNAL_CDR).
9. Restart the External logger service.

Step 10: Turn off SIP Refer

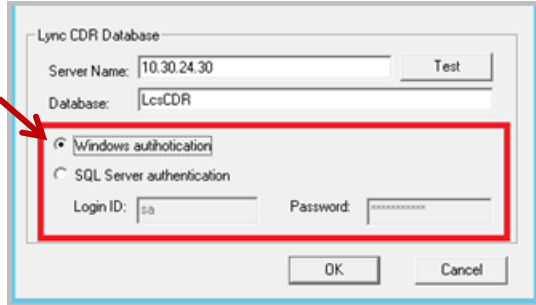
In order to avoid various call forward or transfer issues, Altigen recommends that you set the Skype for Business **Refer Support** option (**Voice Routing > Trunk Configuration**) to **None**.

Important: If you are running both MaxACD 6.5.8 and MaxACD 7.1 in your environment while you upgrade, be careful with the Skype SIP Refer Support option. Release 6.5.8 trunk configuration needs SIP Refer Support to be enabled. However, Release 7.1 needs SIP Refer Support to be disabled. If you disable the SIP Refer Support option for Release 6.5.8, then that service may stop working.

Enable Windows Authentication for External Logger

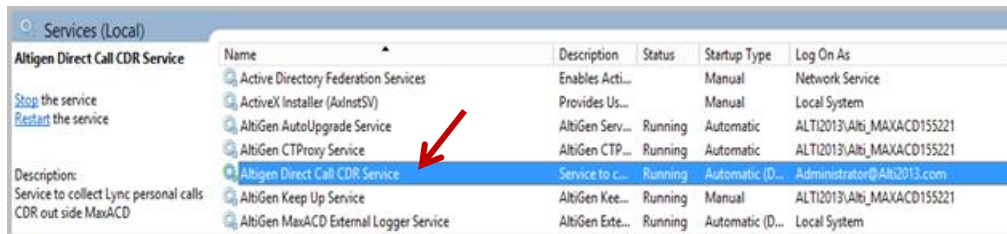
Follow these steps to enable Windows authentication for External Logger.

1. Run the External Logger Configuration tool (ELSCfg.exe) from the folder where you installed it (by default, this is stored in \Program Files (x86)\Altigen\External Logger Service).
2. Near the bottom of the dialog box, check the **Windows authentication** option. Click **OK**.

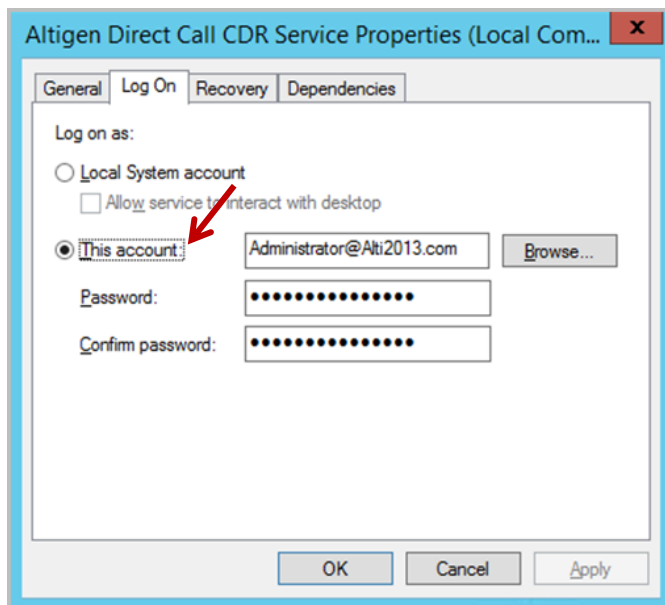


You will see a message, stating that a Windows login account must be assigned to the Lync CDR database and to the Altigen Direct Call CDR Service. You will configure these next. Click **OK**.

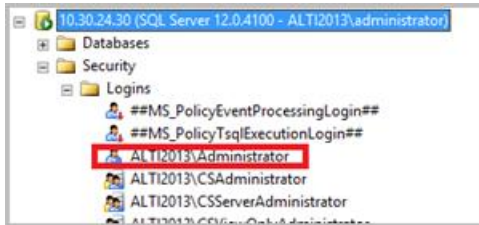
3. Create a Windows login account that will be used specifically for Windows authentication. This account does not need to be an administrator account, but the account must have permission to run services.
4. Open the Windows *Services* panel. Right-click the **Altigen Direct Call CDR Service** and choose **Properties**.



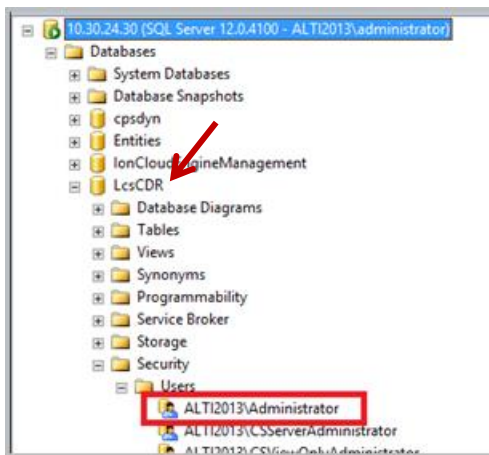
5. On the *General* tab, set *Startup Type* to **Manual**.
6. Switch to the *Log On* tab. Select **This account** and enter the username and password for the Windows login account that you created in step 3. Click **OK**.



- Open SQL Management Studio for Lync SQL database. Add this Windows user account to the Lync SQL Server **Security > Logins**.



- Select the *LcsCDR* database. Add this Windows user account to **Security > Users**.



Federated Deployments

For Federated deployments where MaxACD is stored in the Cloud but Skype for Business is deployed on your local servers, Altigen is providing a new component.

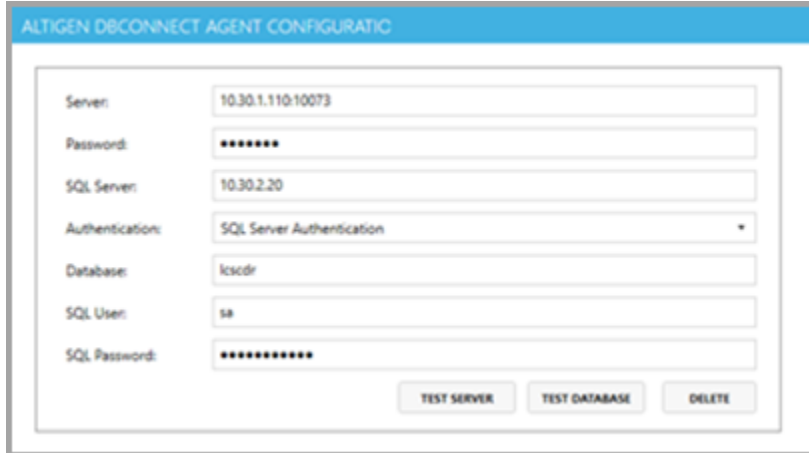
This component, *dbConnect Service*, runs on your local server. Its sole function is to accept SQL commands from the MaxACD system's direct call service and return queried data. This allows the service to synchronize CDR data in your Skype for Business system with the MaxACD system.

dbConnect Service Configuration Deployment Steps

In order to configure the dbConnect service, during your initial deployment you must have chosen **Remote** in the procedure in the section, [Step 9: Configure the MaxACD External Logger Service](#). Otherwise, this configuration will not properly connect your Skype for Business data with MaxACD systems data.

To configure this service, so that CDR records are accurate,

- On your local Windows server, navigate to the Altigen folder dbConnect. This folder was stored there during your initial deployment.
- In that folder, run the executable file *RemoteDatabaseAgent.Configurator.exe*.



3. In the configuration tool, you can create connections to multiple servers (or multiple databases) as needed. Complete the following information for each connection.
 - **Server** – Enter the URL and port for the MaxACD Server.
 - **Password** – Enter a two-way authentication password.
 - **SQL Server** – Enter the IP address for the SQL server.
 - **Authentication** – Choose an authentication method (SQL Server or Windows). Windows authentication will use the service account for the dbConnect service.
 - **Database** – Enter the database instance.
 - **SQL User** – Enter the user account. This does not have to be the sa account; it must have SQL read-only privileges.
 - **SQL Password** – Enter the password for the SQL User account.
4. Click the **Test** buttons to verify the connection. If each test completes successfully, your configuration is complete. If a test does not pass, check the IP Addresses in the External Logger configuration and the fields that you completed in the dbConnect configuration tool, and try again.\

Additional Configuration Steps for Federated Users

Perform the following one-time steps to prevent Federated users from getting popups when they are in a call or conference.

1. On the MaxACD server, open the LyncProxyMain.txt file that is stored under C:\AcdRoot\AcdProxy\log\.
2. Search for "Viewer@" in that file. You should find a SIP URI xxxViewer@xxx.
3. Copy that SIP URI.
4. For each Federated user, add that SIP URI as a contact to the user's Skype for Business client. Right click that contact and select *Change Privacy Relationship*. Change it to *Workgroup*.

MaxACD Redundancy Installation

MaxACD supports system redundancy (a Redundancy license is required).

Two Softswitch servers must be configured. When the active server goes down, the standby server takes control. The change is transparent to direct connected calls.

After you configure redundancy, the second server will get the license information from the first server.



If you did not choose Redundancy during your initial deployment, run the MaxACD installation program on the system again, and choose **Redundancy** instead of Single Server.

After deployment, within MaxACD Administrator, you must enable redundancy. You do this on the *Redundancy* tab of the System menu.

Redundancy Architecture

For a redundant system, two MaxACD servers must be installed. Each server will have its own Proxy.

The two servers connect to a single CWS DB. If one server is down, an administrator can use the other server to make any configuration changes.

The external SQL Server hosts a single CWS DB to store phrases and configuration settings, which allows concurrent access by both active and standby MaxACD servers.

Here is an overview of the automatic switchover process:

The "active" server is the server that is currently in control of operations. The active server sends a "heartbeat" to the CWS DB every few seconds.

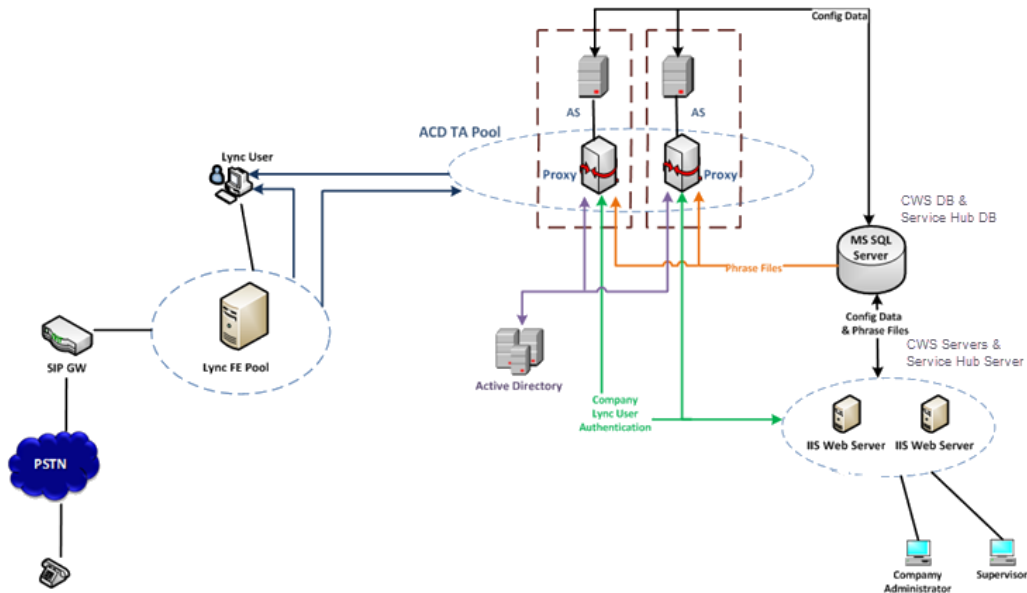
The standby server's Skype proxy AEP is registered as the "will not take call" state in the trusted application pool, so that Skype will not route calls to it. The standby server keeps a connection with the CWS DB and checks for the active server's heartbeat.

If the standby server does not detect the active server's heartbeat for 10 seconds, the standby server promotes itself, registers Proxy to the ACD Trusted Application Pool, and routes AEPs to its own Proxy. It will take over control within approximately 10 seconds. When switchover occurs, the standby server's Skype proxy becomes the active server, and it will register as the "take call" state. After that, all calls can be routed to it.

New calls are routed to the newly promoted MaxACD server. Active calls, which were connected to the failing server, are dropped.

The MaxACD client applications use FQDN to get the Application server's IP address list, then try to connect to an application server one by one. Only the active server will accept the connection request. Once the connection to the active server is made, the clients save this server's IP address. The clients will try to connect to this server first the next time they need to reconnect.

Administrators can manually switch from the active server to the standby server by clicking the Manual Switchover button within MaxACD Admin.



Note: If the SQL server goes down, MaxACD will continue to function normally, receiving inbound calls and sending outbound calls. However, while the SQL server is unresponsive, administrators cannot make MaxACD configuration changes.

Switchover Considerations

When system control switches from the active to the standby server, it affects calls in the following ways:

- Current calls will be disconnected. Within a few minutes, new calls will go through.
- CDRs will be dropped for all calls, including connected calls.
- Voicemail recording will stop.
- Daily RTM statistics will be reset.

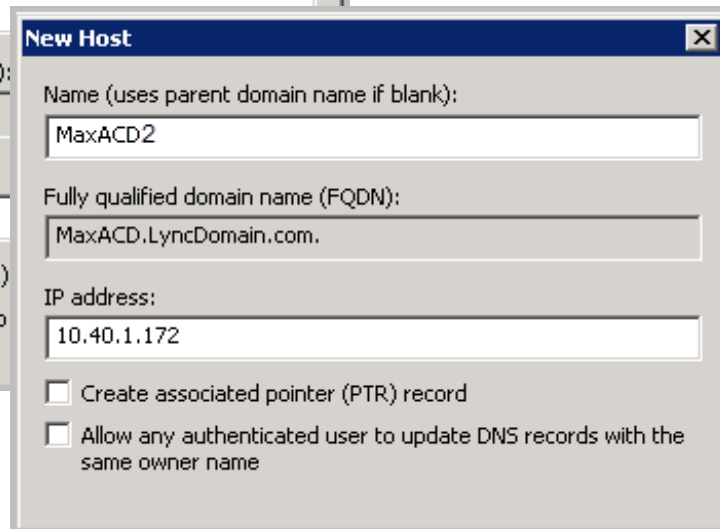
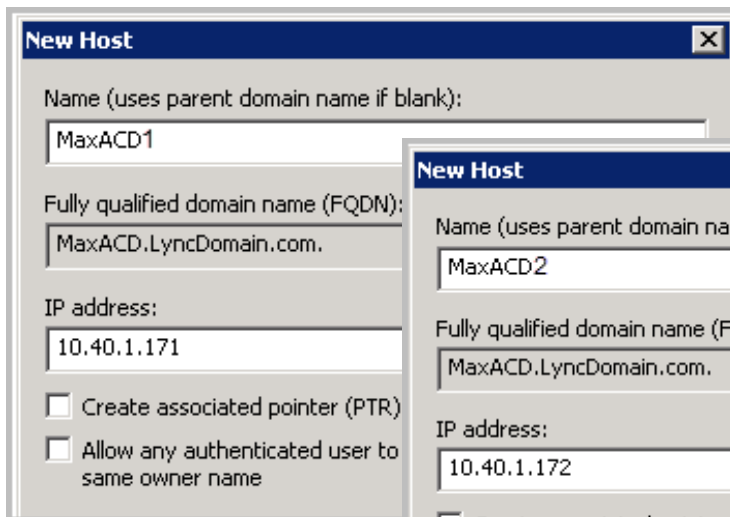
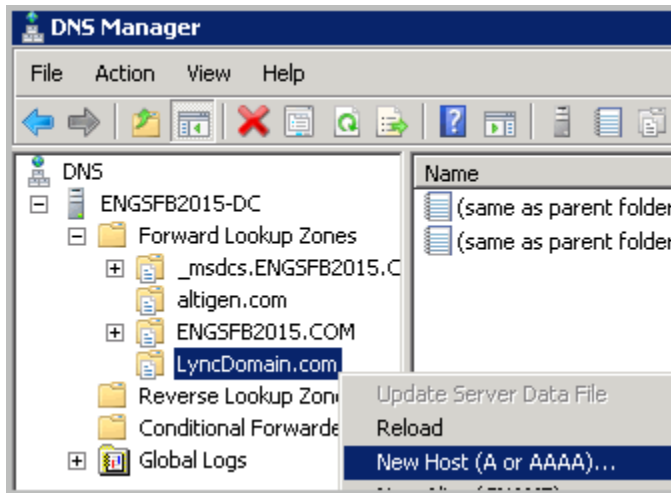
In addition, after the service switches to the standby server, users who are running client applications will need to log in again.

Note: For a redundant system, the time among the redundant MaxACD servers and the SQL server that hosts the database **must be synchronized**. If the time is off by as much as 10 seconds, unwanted automatic switchovers can occur.

Deploy a Redundant System

For a redundant system, there will be two MaxACD servers and one Service Hub database. For example, say that the first server's computer FQDN is *MaxACD1.lyncdomain.com* and the second one is *MaxACD2.lyncdomain.com*. In DNS server, add a new FQDN (for example, *MaxACD.lyncdomain.com*) that has the IP address for both MaxACD1 and MaxACD2.

In DNS Manager of the domain, create two entries for *MaxACD.lyncdomain*.

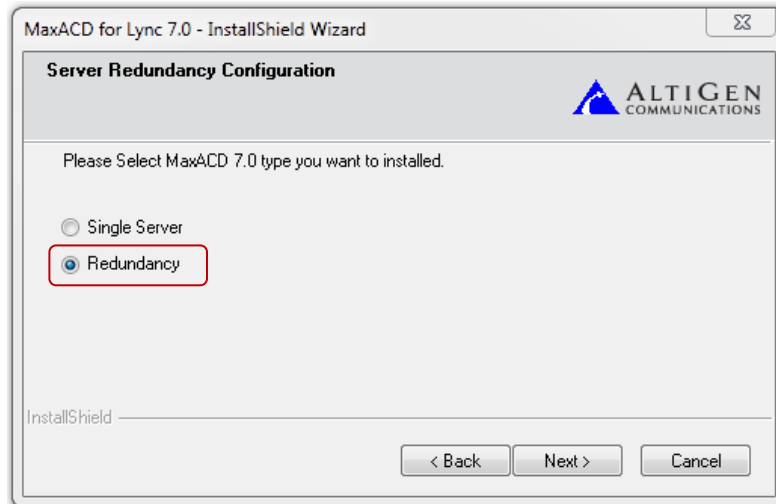


If access from the Internet is required, work with your ISP to obtain and register both public IP address for *MaxACD.lyncdomain.com*. Certain port-forwarding and network configurations are required to provide access from the Internet.

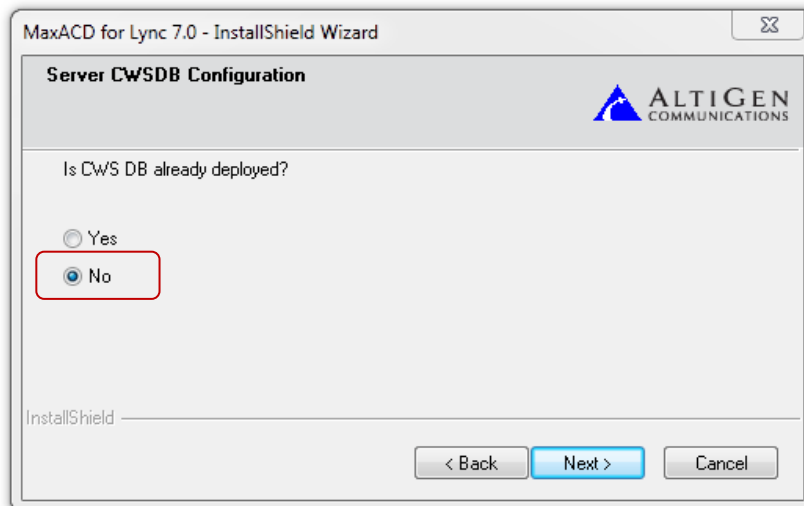
Later, when you log into the MaxAdmin, MaxAgent, and MaxSupervisor, use *MaxACD.lyncdomain.com* instead.

Next, follow the procedures listed earlier in this guide for to install MaxACD on both servers. During the steps in the section *MaxACD Installation* beginning on page 10, choose the following options:

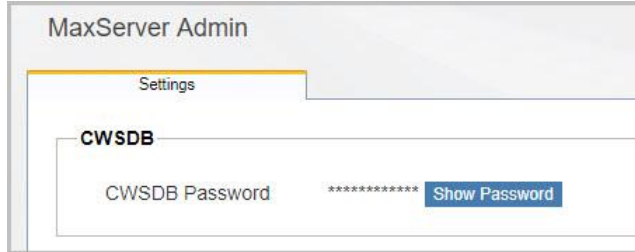
1. Install MaxACD **on the first server**:
 - a. For step 5 on page 21, choose **Redundancy**.



- b. For step 6 on page 21, choose **No**. Then enter the details for your SQL server instance. For a default installation, leave the *SQL Instance* field blank.



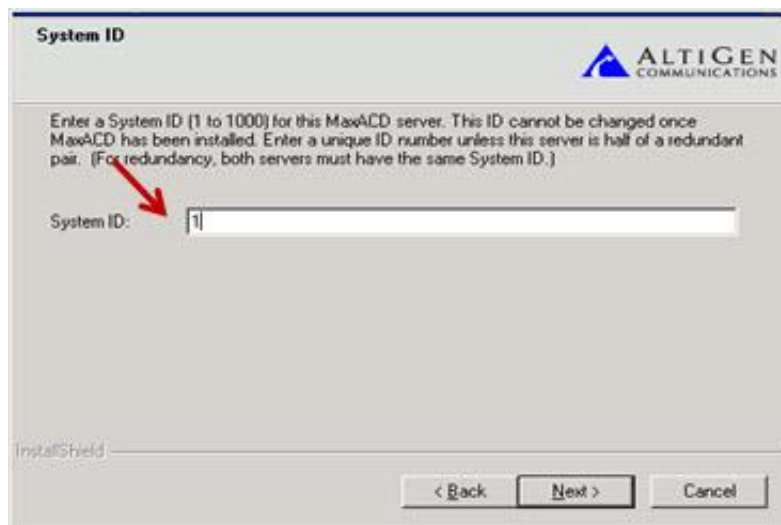
Note: The installation program may remember this password and populate it for you (from your entry on page 21). If you forget this password, you can log into MaxAdmin and retrieve it from the *Settings* tab.




- c. After you have installed MaxACD on the first system, restart it.
- d. Register the system key and load the license file; perform the steps in the section *Step 6: Register the System Key and Load the License File* starting on page 26.

2. Install MaxACD **on the second server**:

- a. For step 4 on page 21, **you must enter the same System ID** as you entered when you installed MaxACD on the first system.



- b. For step 5 on page 21, choose **Redundancy**.
- c. For step 6 on page 21, choose **Yes**. Then enter the same SQL instance details as you entered for the first system.
- d. Restart the system.
- e. Register the system key on the second server by following the steps in *Step 6: Register the System Key and Load the License File* starting on page 26.

 **This step is critical. You MUST register the system key on the second server in order to enable redundancy.**

You should not need to load the license file; it should automatically be applied.

- 3. After you have set up both servers, enable redundancy within MaxACD Admin. To do this, log into MaxAdmin, and on the **System** menu switch to the **Redundancy** tab. Select the option **Enable Redundancy**.

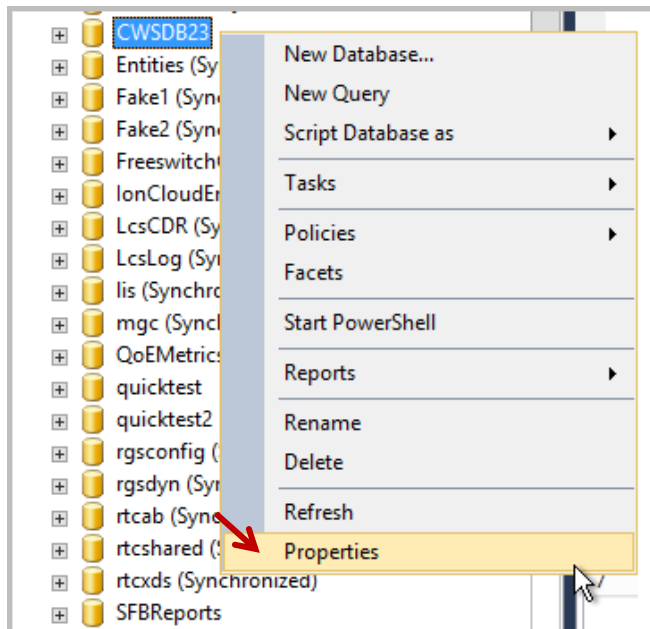
This tab shows the current state of both servers. It also shows the date and time of the most recent switchover, and the reason for that switchover. For further details, see the *MaxACD 7.1 Administration Manual*.



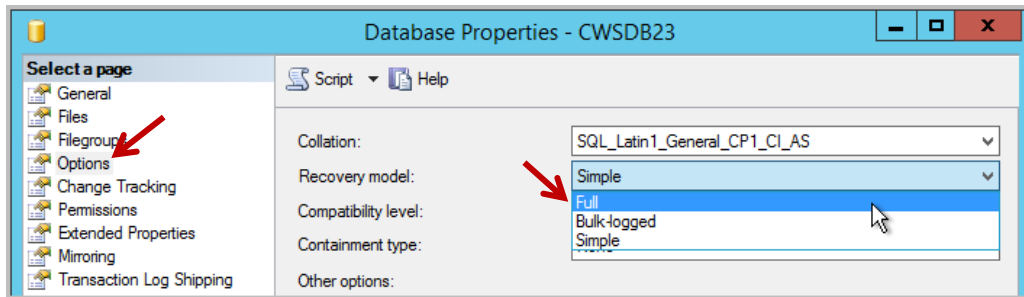
Configure the Database for Redundancy

This section describes how to configure the database for redundancy.

1. First, change the database backup model from *Simple* to *Full*. Databases cannot be added to the recovery group when the recovery model is *Simple*, which is how the MaxACD installation wizard creates it.
 - A. In *Microsoft SQL Server Management Studio*, right click the database, and select **Properties**.

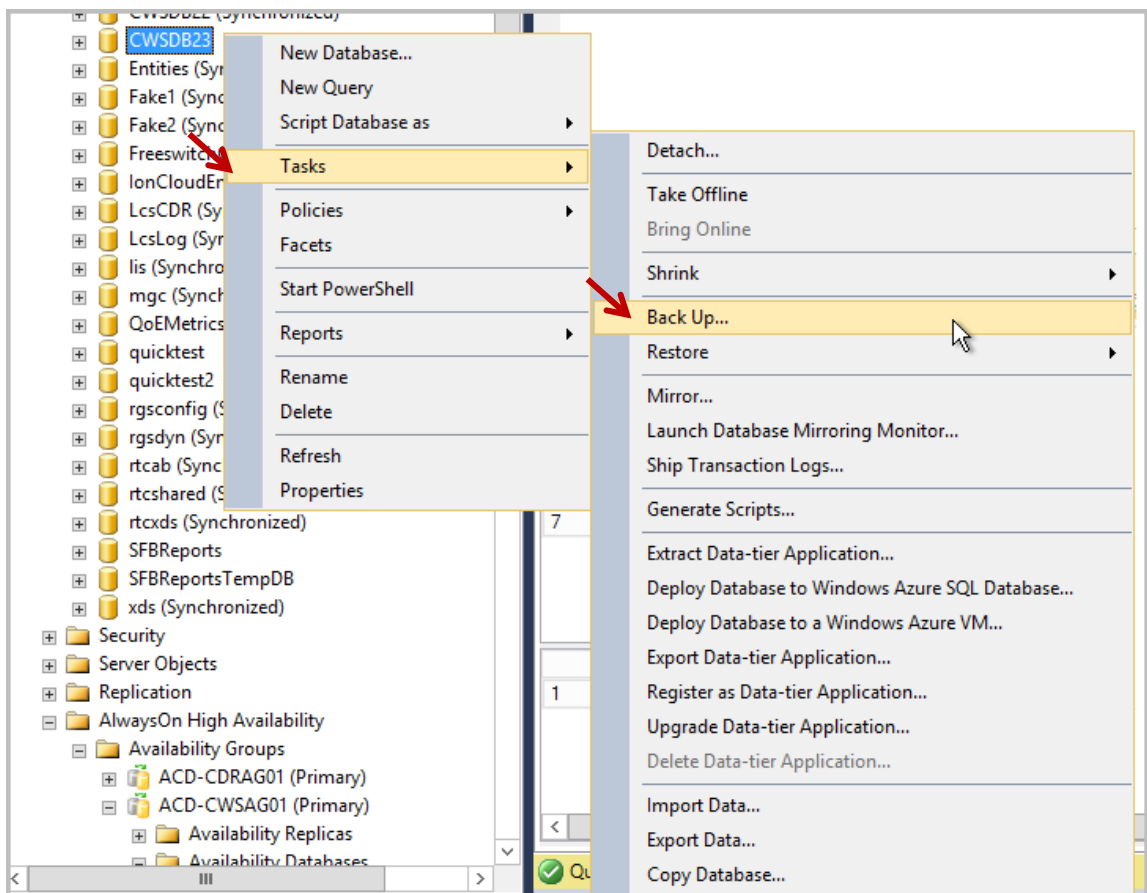


- B. Select the *Options* page and change the *Recovery Model* setting to **Full**. Click **OK**.

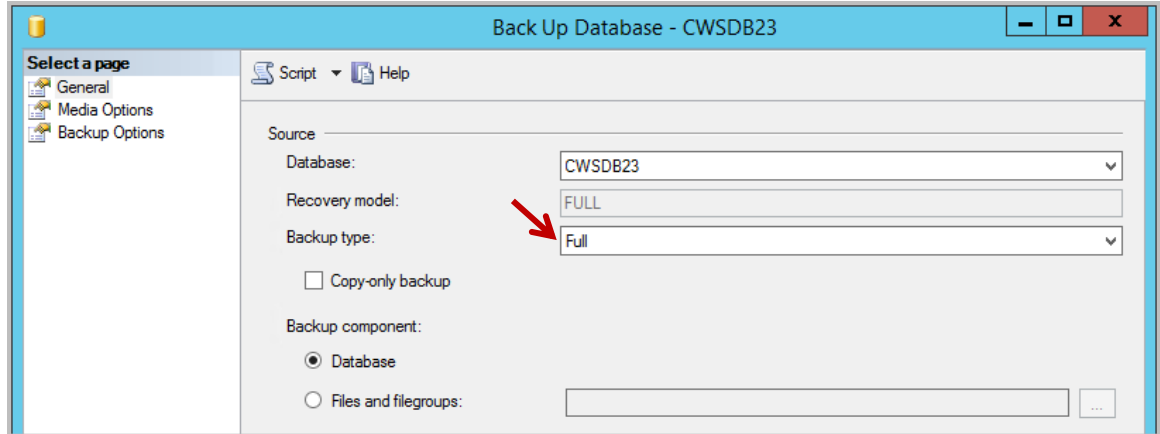


2. Back up the database. The database must be backed up prior to adding to the availability group. Perform a full backup.

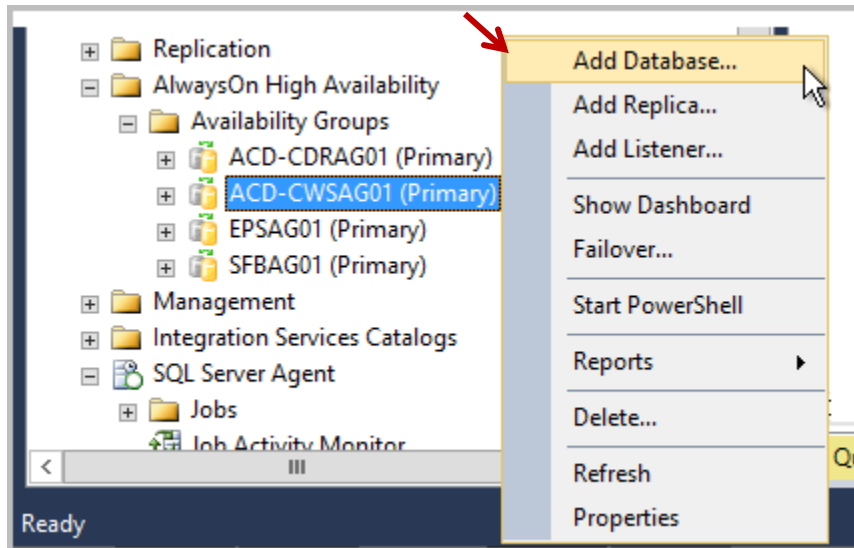
- A. Right-click the database name on the left and select **Tasks > Backup**.



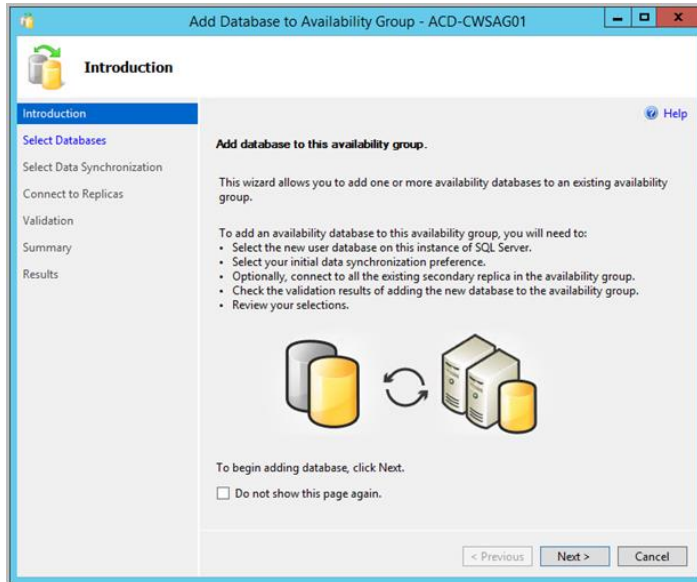
- B. Perform a full backup. The location should be a network drive that all of the AlwaysOn Availability Group replication servers can access.



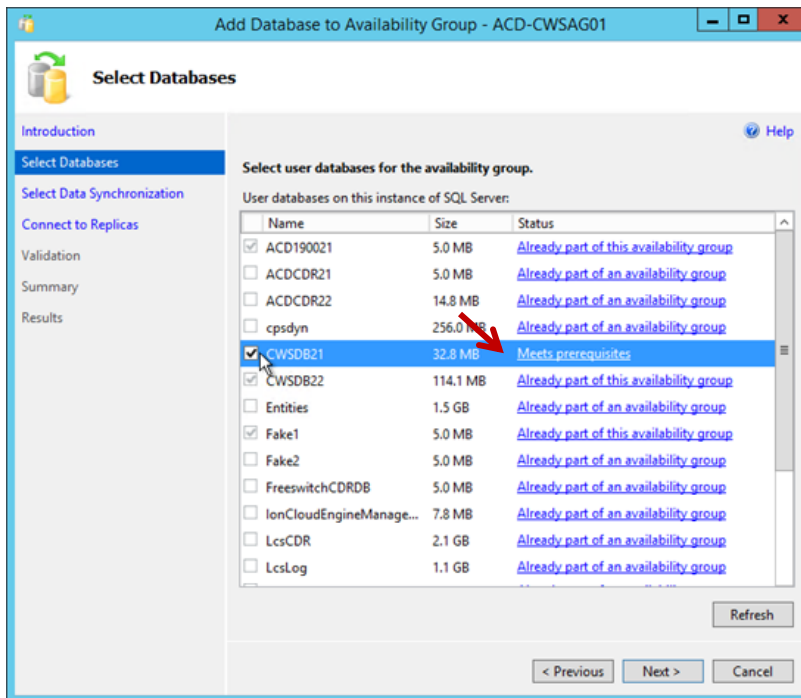
3. Once this is done, add the server to the availability group.
 - A. Right-click the AlwaysOn Availability group and select **Add Database**.



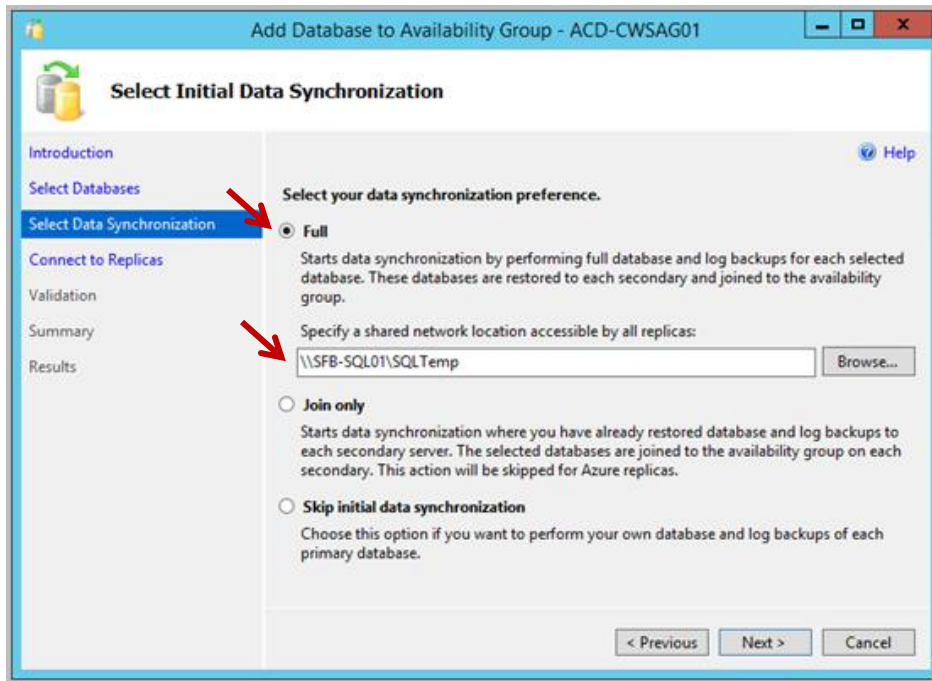
B. On the Introduction page, click **Next**.



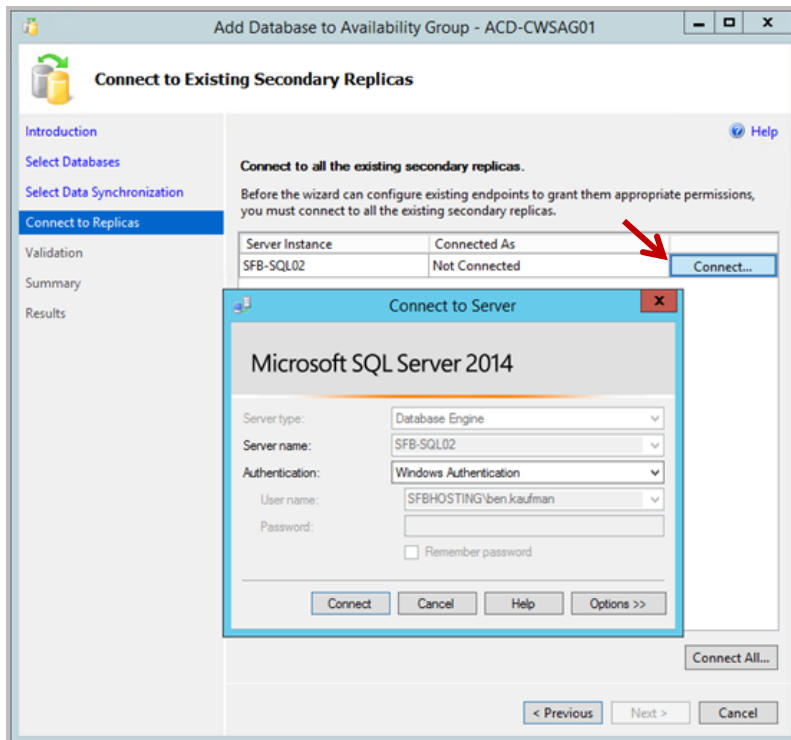
C. Select the database to be added to the group. If there are any unmet pre-requisites, you must resolve them before you proceed.



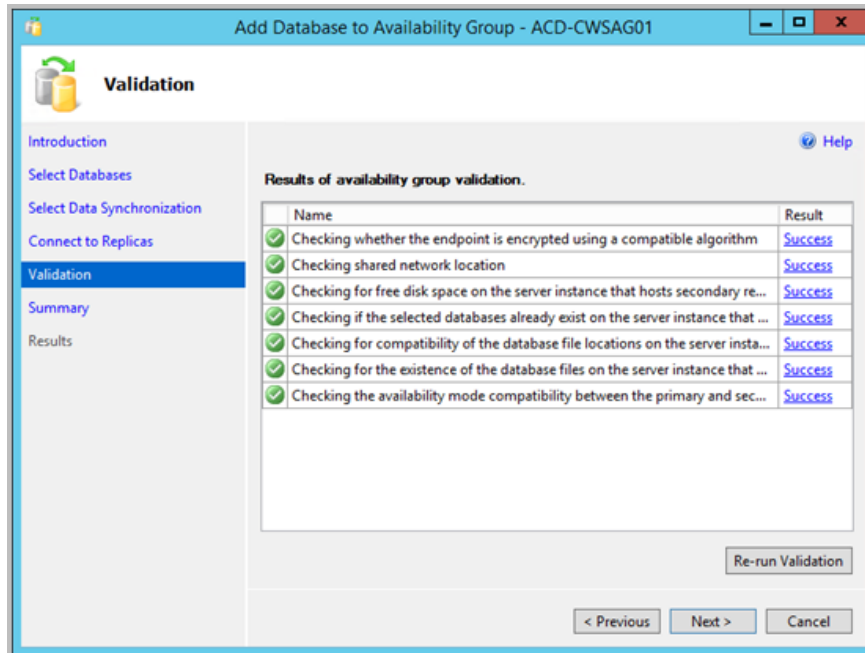
- D. For the data synchronization options, select **Full** and specify a network location.



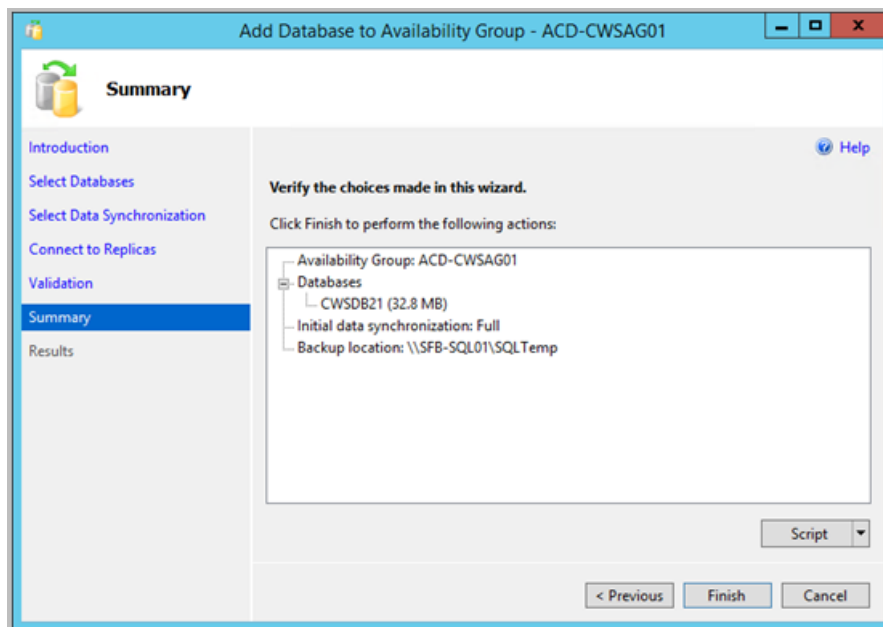
- E. You are logged into the primary server to do this configuration. To allow the replication, log into the secondary servers as well. Click **Connect...** then connect to the server (the account with sysadmin privileges).



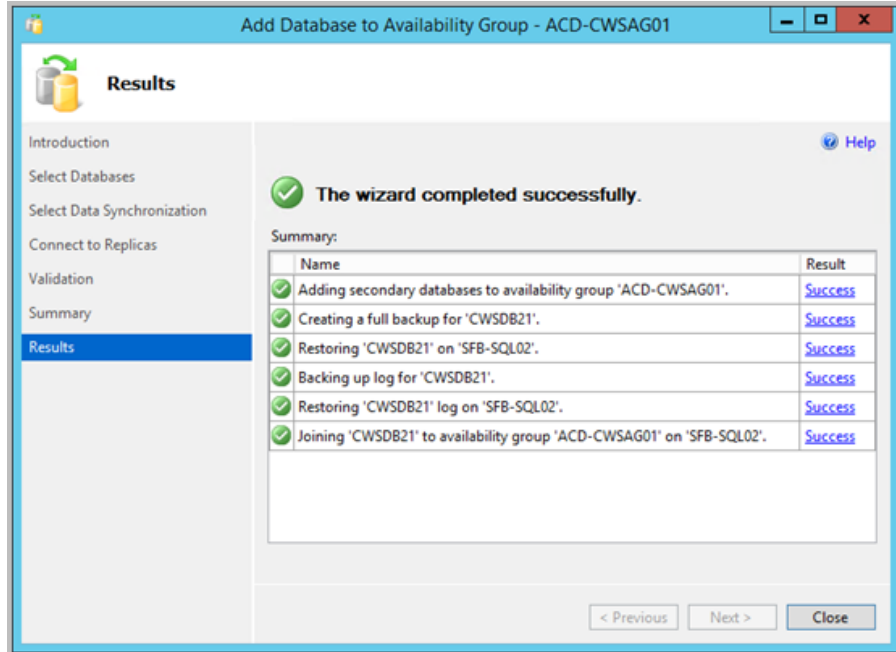
- F. Click **Next** once the connection is complete.
- G. Let the validation checks run. Click **Next**.



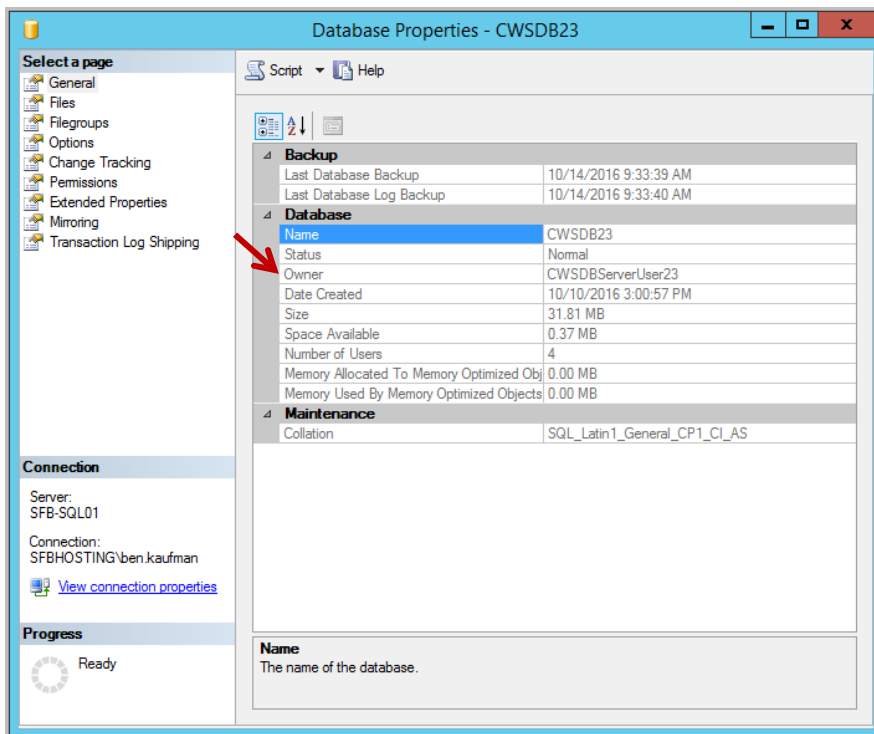
- H. On the Summary page, click **Finish**.



- I. On the Results page, all results should say *Success*.

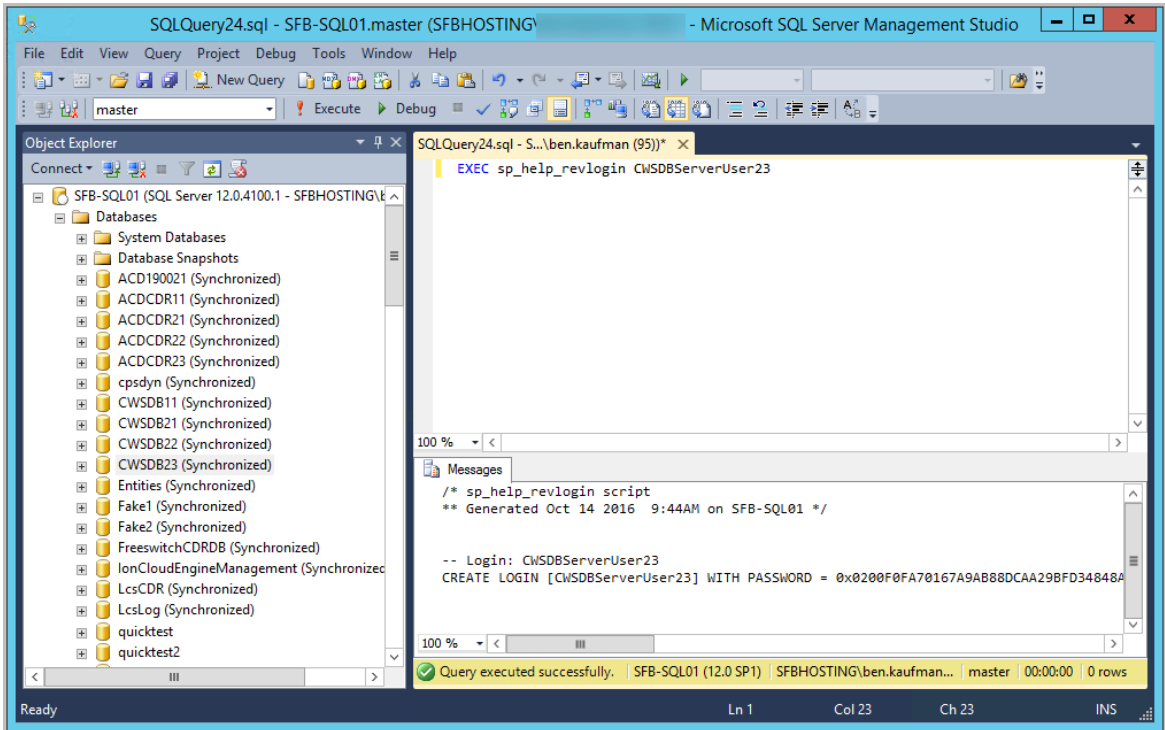


- Identify the database owner (the account that MaxACD uses to connect to the database). To find this, on the Database Properties “General” page, look at the *Owner* field. Make a note of this, because you will need it in step

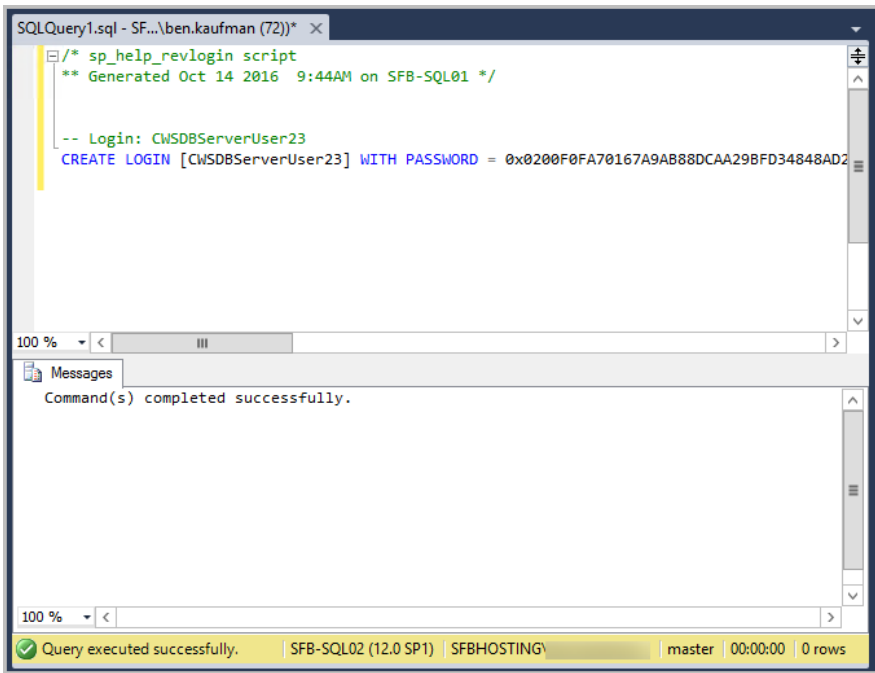


- Create a stored procedure for `sp_help_revlogin`, based on this Microsoft article: <https://support.microsoft.com/en-us/kb/918992>

- Run `sp_help_revlogin` on the PRIMARY replication server. Use the database owner you identified in step 4.



- Copy the command that is returned, and run it on all secondary replication servers in the availability group:



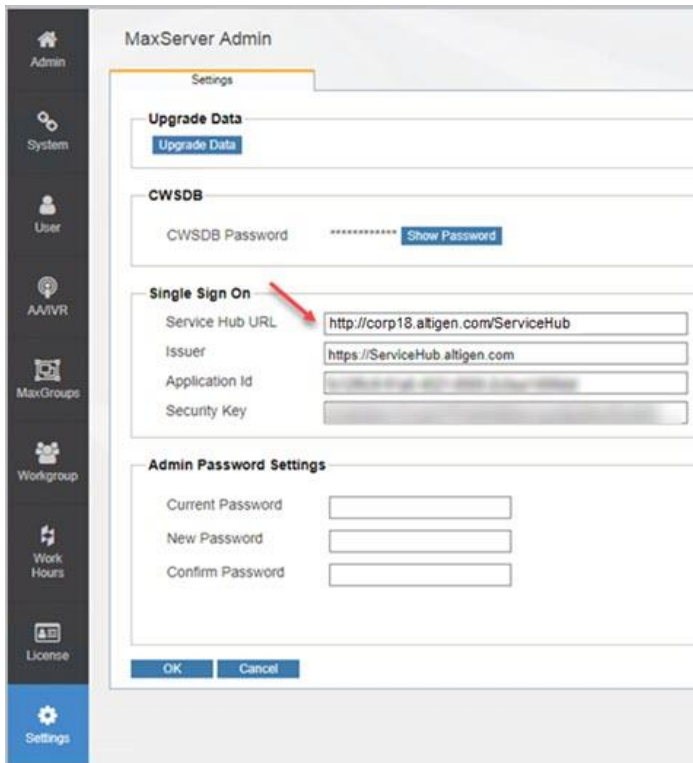
Change IP Addresses to FQDNs

Perform these additional steps for a redundant system:

1. Log into the Service Hub. On the *MaxServers* tab, in the *MaxServer Admin* section, check the entry for the *Landing Page* field. If this entry is an IP address, then you must change it to a Fully Qualified Domain Name (FQDN.)



2. Log into MaxAdmin. On the *Settings* tab, in the *Single Sign On* section, check the entry for the *Service Hub URL* field. If this entry is an IP address, then you must change it to an FQDN.





Microsoft UC Paired Pools Deployment

This section provides guidelines for setting up a disaster recovery environment for MaxACD. Deploying paired pools will help you to recover quickly in the event of a physical disaster at one location and to retain as much data as possible.

Microsoft recommends deploying pairs of Front End pools across two geographically distant sites. Each site has a Front-End pool. Each Front-End pool is paired with a corresponding Front End pool at the other site. Both sites are active, and the Backup Service keeps the pools synchronized.

This guide assumes that you have already configured Skype disaster recovery at your sites. Configuration steps for deploying Skype disaster recovery are beyond the scope of this guide; refer to the detailed instructions in <https://technet.microsoft.com> for those guidelines. You may find the following articles useful:

- Deploying paired Front-End pools for disaster recovery in Lync Server 2013” - [https://technet.microsoft.com/en-us/library/jj204773\(v=ocs.15\).aspx](https://technet.microsoft.com/en-us/library/jj204773(v=ocs.15).aspx)
- Front End pool disaster recovery in Skype for Business Server 2015” - <https://technet.microsoft.com/en-us/library/jj204697.aspx>

Following is a list of files you will be using to configure paired pools and set up the recovery process: These files can be found in the Altigen Partner Knowledgebase, attached to this article.

- *copyCWS.bat* – a batch file that copies the backup file to a shared remote folder
- *moveaep.ps1* – a PowerShell script that helps update the Application Endpoints for recovery
- *moveCWSDB.sql* – a SQL script that you can use to update the MaxACD FQDN and address in the DB to the backup ones

Overview of MaxACD Paired Pools Deployment

Altigen recommends that you configure two MaxACD servers at each site and one SQL server at each site.

During configuration, you will put in place various batch files, tasks, and processes. With these items in place, you can quickly execute a failover if a disaster brings down a site.

When disaster incapacitates one site, during the recovery process, the CWS (Administrator Portal) will be restored to the most recent MaxACD system backup. Assuming that daily backups are being made, as recommended, then you will lose only those configuration changes that have been made since the most recent backup (which would be less than one day).

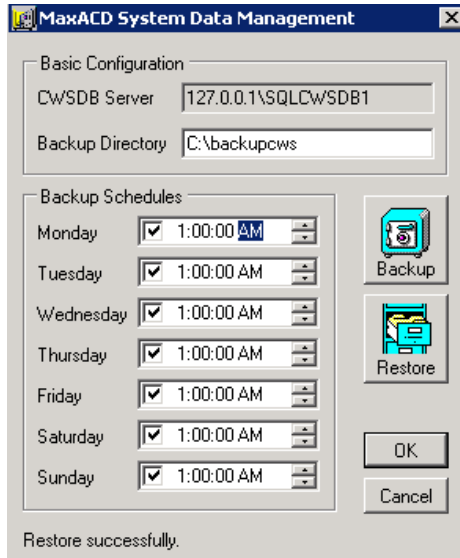
After data from the daily backup has been restored to the backup site, the backup MaxACD server will continue processing activities. Agents who are using any client applications will need to use the backup server FQDN in order to log back in.

Configuration Procedures

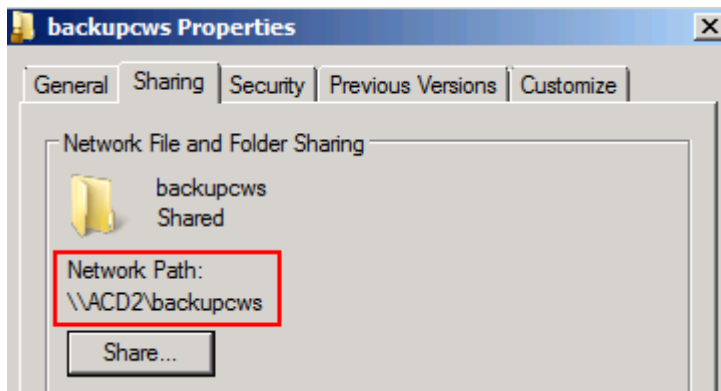
These instructions refer to a main MaxACD deployment, which is the active one, and a backup site.

1. Deploy the same structure of the main MaxACD system on the backup site server. Use the same configuration as the main MaxACD deployment, but use the **backup** Trusted Application pool.

- On the main MaxACD server, configure a recurring backup. Altigen suggests that you schedule the backup to occur once daily. Please note the location of the backup directory – you will need that location in a later step.



- On the main MaxACD server, create a backup user in the domain (for example: *FailOverUser*). This user should be the member of the *Domain Admins* group.
- Set up a sharing folder on the backup CWS DB system (for example: *c:\backupcws*). Grant write/modify privileges to the backup user that you created in the preceding step. Note this sharing path; it is needed in the next step.



- Altigen has provided a template batch file for you to modify, *copyCWS.bat*, which we have copied here for your convenience.

```
rem This script is used to copy the CWS DB backup file to a remote sharing folder.
rem Please edit it before using.
rem Replace the "[Source]" string in the script with source path. Example: "C:\cwsbackup"
rem Replace the "[Dest]" string in the script with destination path. Example:
"\\192.168.1.231\backupcws"
```



```
rem Logs can be found at [Source]\log.txt

date /t >> [Source]\log.txt 2>&1

time /t >> [Source]\log.txt 2>&1

xcopy [Source]\cws*.* [Dest] /Y >> [Source]\log.txt 2>&1

echo ----- >> [Source]\log.txt 2>&1

exit
```

Edit this file as follows:

- Replace [Source] tag with the backup directory path in step 2.
- Replace the [Dest] tag with the network sharing path in step 4.

Store this updated batch file on the main system.

6. On the main MaxACD CWS DB server, create a new task in the Task Scheduler to run the batch file *copyCWS.bat*.

- Set the Security options to use the backup user.
- Set the *Trigger* to **Daily** and set the start time to one hour later than the backup tool start time. For example, if the backup file is schedule to run at 12:01AM, set this task to begin at 1:01 AM.

Run the task and confirm that it works correctly. Consult the *log.txt* file in the main MaxACD backup directory if the batch file does not work properly.

How to Fail Over to the Backup Server

When an emergency takes the main MaxACD server out of production, follow these instructions on the backup MaxACD server to get back on track quickly.

Note that you should fail over (and back) Skype for Business **before** you fail over (and back) the MaxACD server.

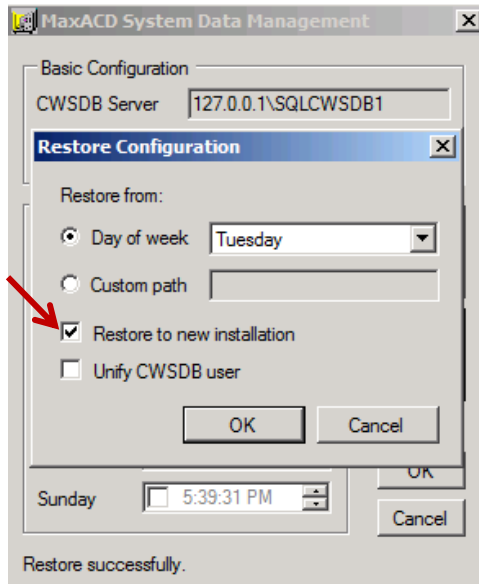
1. Stop all of the Altigen services on the backup MaxACD server.
2. In the Skype for Business Server Management Shell, delete the original AEP used by MaxACD. Re-create it with the backup trusted application pool. You can use the PowerShell script *moveaep.ps1* for this. Substitute the actual pool names for our placeholder variables.

```
moveaep.ps1 -appname [trusted application name] -apppool [backup trusted application pool]
```

Each time you run *moveaep.ps1*, a *.csv* file will be generated. It contains all the AEPs in the trusted application. If a problem occurred while moving AEPs, you can restore the AEPs with the following command:

```
restoreaep.ps1 -appname [trusted application name] -apppool [the pool you would like to restore back to] -restoreFile [the .csv file generated by running moveaep.ps1]
```

- Run the MaxACD Backup and Restore utility. Restore the latest backup file, selecting the **Restore to new installation** option.



- Open SQL Management Studio. Log into the backup CWS DB. Update the MaxACD FQDN and address in the DB to the backup one.

You can use the following SQL script with modified data: *moveCWSDB.sql*. Modify the values in the script before you run the script.

- replace **serverAddress** with the Backup MaxACD IP Address
- replace **ServerFQDN** with the Backup MaxACD FQDN
- replace **name** with the Backup MaxACD machine name
- replace **ACDTAPoolFQDN** with the Backup Trusted Application pool FQDN
- replace **LyncServerRegistrarFQDN** with the Backup FE Registrar FQDN
- replace **RedirectorTAPoolFQDN** with the Backup Redirector Trusted Application pool FQDN
- replace **CEMURL** with the Backup Service Hub URL. It should be:

`http://[Backup MaxACD IP]/Servicehub`

Open a new query in SQL Management Studio.

Replace the Backup MaxACD IP Address in the following script:

```
SELECT TOP 1000 [Id]
      ,[SecurityKey]
      ,[Link]
FROM [SHDB1].[dbo].[Applications]
Where [Link] should be '%[Backup MaxACD IP]%'
```

Execute this script in the new query window.



In `moveCWSDB.sql`, replace `applicationId` and `applicationSecurity` with the `Id` and `SecurityKey` just queried.

5. Reboot the MaxACD server. It may take 10-15 minutes for the URI routing to take effect.

The backup MaxACD server should now be online. Your agents should now log into their client applications using the backup MaxACD FQDN.

To switch back to the main server once the site has recovered, follow the same process.

Deploying a Stand-alone Web Portal

When you install MaxACD, a default MaxAdmin portal, is installed in the same machine.

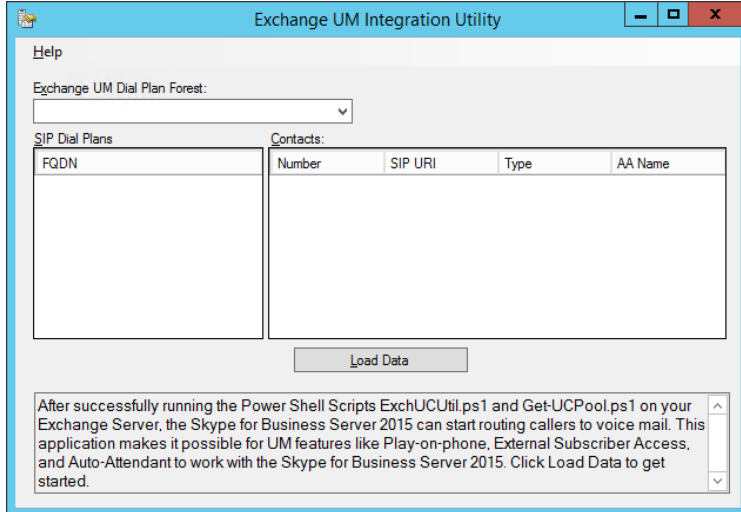
Altigen also provides a stand-alone installation package that you can use to install the MaxAdmin portal on a separate Windows 2012 R2 or Windows 2016 system.

To install a MaxAdmin Portal on a separate server,

1. On the installation media, open the `CWS` folder and run `setup.exe`.
2. For the `System ID` field, enter 1 unless you have multiple MaxACD systems.
3. Proceed through the wizard panels. When you reach the panel that requests database information, enter the CWSDB details:
 - **SQL Server Address** – The database's SQL IP address
 - **SQL Instance** – The database's SQL Instance name
 - **Service Hub DB Account** – This is an account user name (`CWSDBServerUser1`) that is used for MaxACD components to access SQL CWSDB; you cannot change this name
 - **Service Hub DB Account Password** – The password for the SQL CWSDB account user name. The installation program may remember this password and populate it for you. If the password is incorrect, or if the SQL CWSDB is not running, then the installation process will not continue. If you forget this password, you can log into MaxAdmin and retrieve it from the `Settings` tab.
4. Submit any additional information requested by the installation wizard. After the installation process has finished, confirm that you can log onto MaxAdmin from this system.

Exchange UM Integration Utility

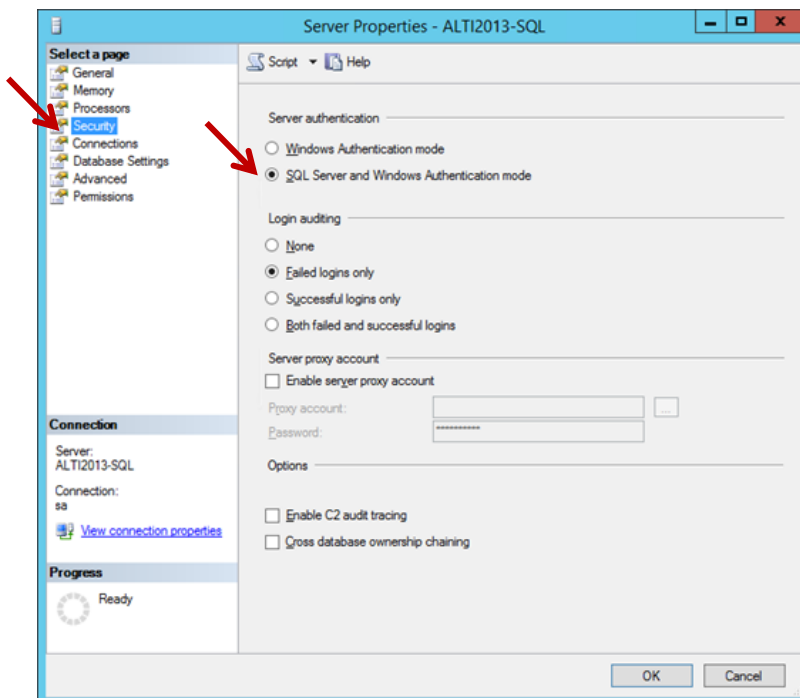
After successfully running the PowerShell Scripts `ExchUCUtil.ps1` and `Get-UCPool.ps1` on your Exchange Server, you should be able to run "OcsUmUtil.exe" on your Skype for Business server. The default location is `C:\Program Files\Common Files\Skype for Business Server 2015\Support`.



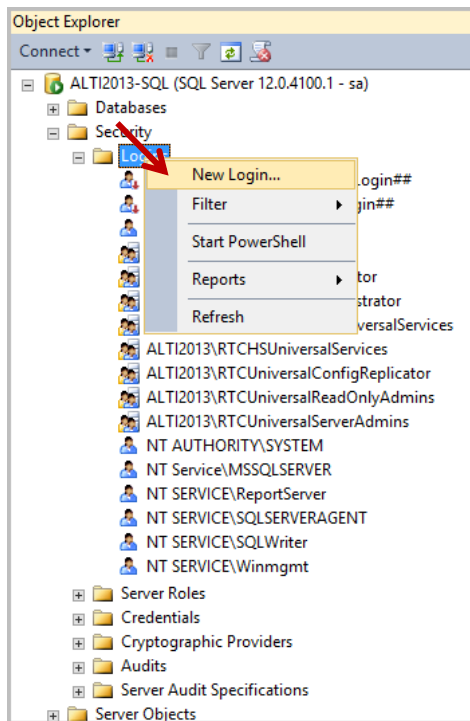
SQL Authentication of External Logger Service

On the SQL server side, follow these steps.

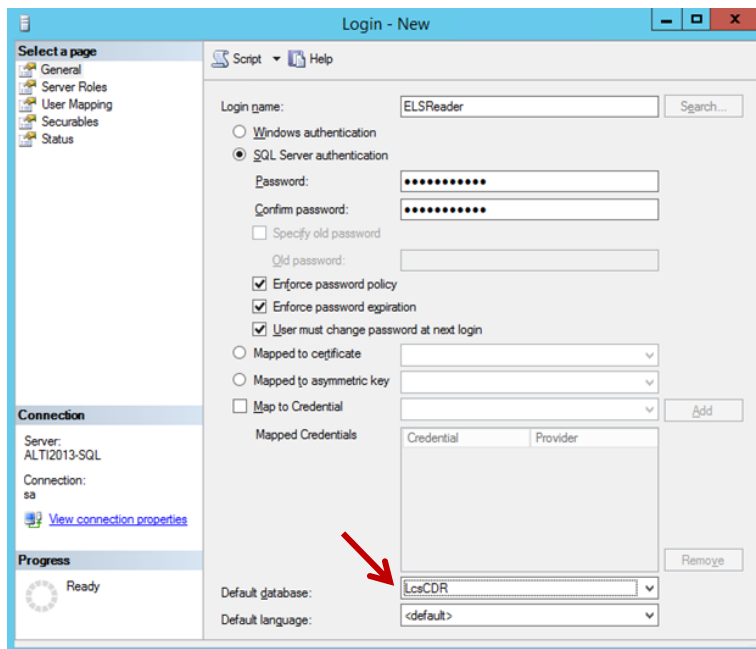
1. Select Server **Properties** > **Security**. Change the server authentication to **SQL Server and Windows Authentication mode**.



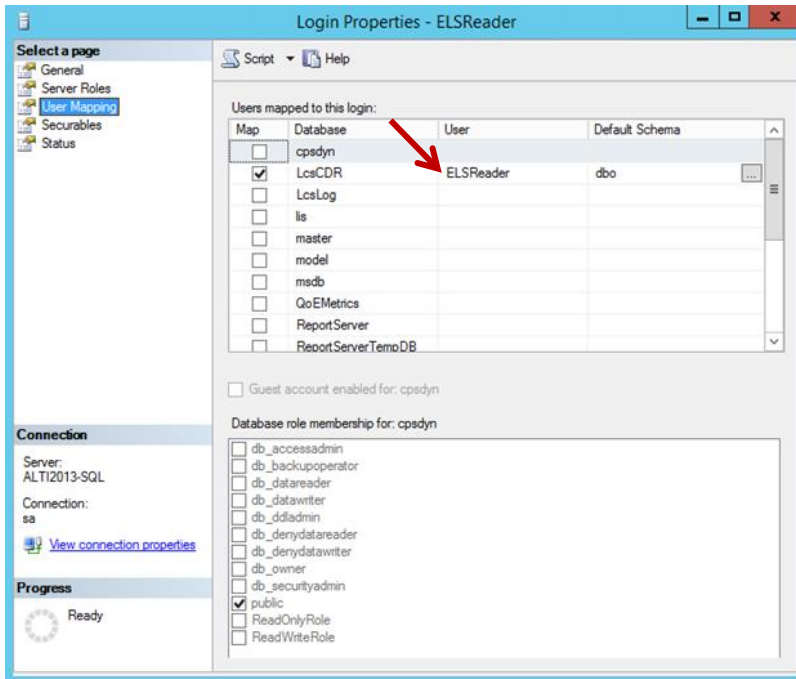
2. Create a new SQL user.



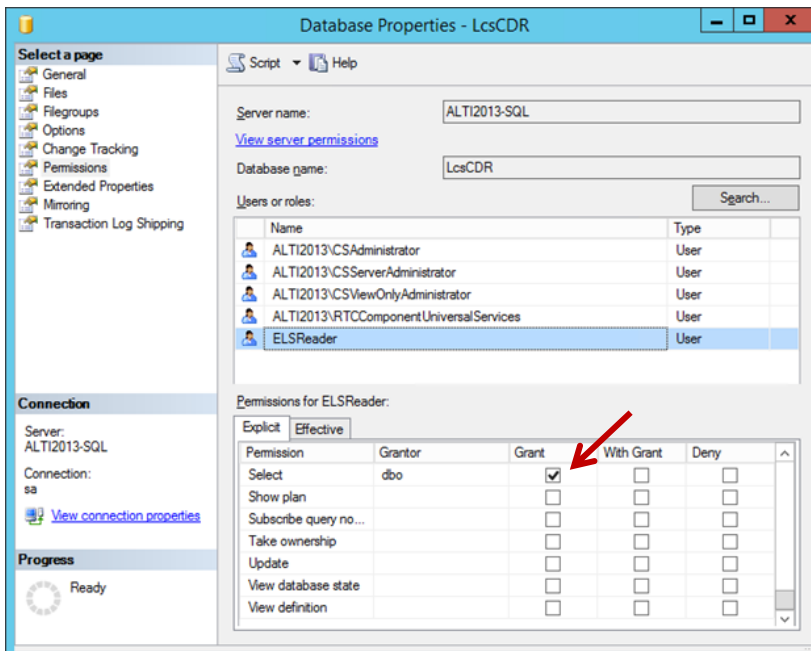
3. For this new user, assign a user name and a password. Change the user's default database to *LcsCDR*.



- Map *LcsCDR* to the new user.



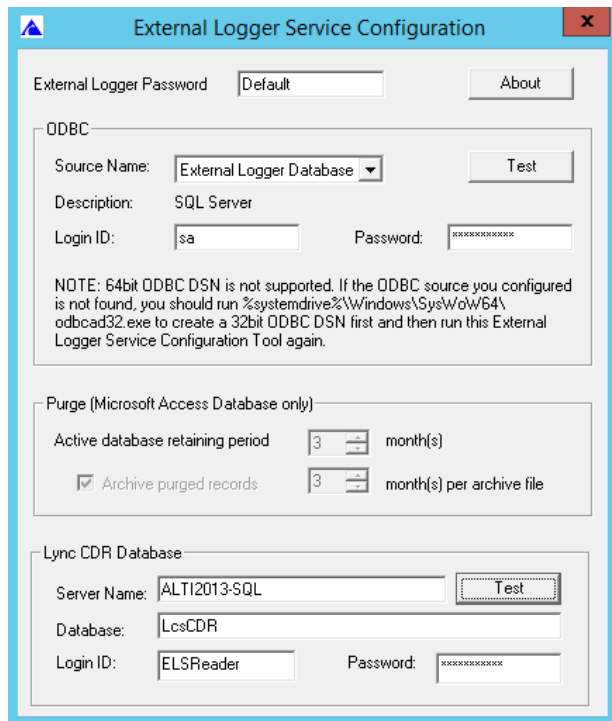
- Grant *Select* permission of *LcsCDR* to this user.



- Try to connect to the database as the user that you just created. Most SQL policies require users to change the password after the first login.

If the login attempt fails, check the user and instance properties.

- Configure External Logger service with the new user credentials and test the connection.



Operational Notes

- On some systems, closing and reopening your Skype for Business client may temporarily disable the Hang Up button. It may also temporarily disable the Attended Transfer feature. To resolve this issue, exit MaxAgent and restart it.
- When agents make an outbound workgroup call, conference a new member, or perform a consultative transfer, the target MUST be either a PSTN number or a Skype user. Other types of targets, such as a workgroup, IVR, voicemail, or AEP, are not supported.
- Make sure that Skype users set the following option in their Skype client: set **Options > Status** to: **I want everyone to be able to see my presence...** Otherwise, agents may not be able to log into their workgroups. This problem arises because the agent's Skype Presence cannot be detected by MaxACD.
- When a user first opens MaxSupervisor, it may take a minute to update an agent's status to Busy when the agent answers a call. This only occurs when MaxSupervisor is opened; subsequent agent calls update the agent's status within seconds.
- If you change to a new ODBC source, you must delete and re-enter the log service. You can do this, in MaxAdmin, by selecting **System > Reports > Log Service**.
- For FTP Server for VR Manager, make sure you unblock the firewall for the FTP Server.
- When the browser security is set to High, you may have difficulty working with the following MaxAdmin pages: Workgroup, User, and License pages. To avoid this issue, enable JavaScript in your browser.
- If you are running MaxAdmin in Internet Explorer 10, add the MaxAdmin URL to the browser's Compatibility View list (In IE, choose **Tools > Compatibility View Settings**).



- For a redundant system, the time among the redundant MaxACD servers and the SQL server that hosts the database must be synchronized.

Uninstalling MaxACD

To uninstall MaxACD 7.1, follow this process:

- Stop all MaxACD 7.1-related services. To do this, go to the MaxACD server, open Windows, and click **Start > Programs > All Programs > MaxACD 7.1 > Service Utility**.
This utility lets you stop the MaxACD system services, including the MaxACD Administrator application itself. Use this utility instead of stopping the service through the Windows Services panel (see Warning, below)
- Once the services have all been stopped, click **Start > Programs > Control Panel > Add / Remove Programs**, select **MaxACD 7.1** and click **Remove**.

Note: The process of uninstalling MaxACD 7.1 does not remove the AEPs that were created when URI routing rules were created. This is by design.

When performing an upgrade or when re-installing MaxACD 7.1, make sure you install under the same Windows login account as during the initial installation. If you do not install under the same account, SQL may fail to install due to insufficient SQL account rights.

Altigen Technical Support

Authorized Altigen Partners and distributors and Direct Customers on a Direct Support Plan may contact Altigen technical support by the following methods.

- You may request technical support on Altigen's Partner web site, at <https://mspartner.altigen.com>. Open a case on this site; a Technical Support representative will respond within one business day (Tier 1 Direct Customers must call to open a case).
- Call 888-ALTIGEN, choose option **5** from the IVR, or 408-597-9000, option **5** from IVR, and follow the prompts. Your call will be answered by one of Altigen's Technical Support Representatives or routed to the Technical Support Message Center if outside of normal business hours and no one is available to answer your call.

Technical support hours are 5:00 a.m. to 5:00 p.m., PST, Monday through Friday, except holidays.

If all representatives are busy, your call will be returned in the order it was received, within four hours under normal circumstances. Outside Altigen business hours, only urgent calls will be returned on the same day (within one hour). Non-urgent calls will be returned on the next business day.

Please be ready to supply the following **required** information when calling in for Support:

- Partner ID
- Altigen Certified Engineer Tech ID
- Serial numbers for any applicable hardware (chassis, boards, and so on)
- Number and types of boards in the system, if applicable
- MaxACD version number
- Server model
- The telephone number where you can be reached

Be prepared to answer the following questions:

- Is this a virtual or a standalone server installation?



- If this is a virtual installation, it is installed in VMware environment or Hyper-V? What is the version number of the virtual server?
- How much memory and how many CPU's are reserved for MaxACD Server use? Memory and CPU cores should always be dedicated and reserved for MaxACD Server use exclusively.
- Are SSD drives installed? If not, be prepared to describe what NAS devices are installed and whether they are shared or dedicated to the MaxACD server.