

# 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: <u>info@altigen.com</u> Web site: <u>www.altigen.com</u>

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<sup>™</sup> 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 Skype4Busness 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/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> <li>Windows Server 2012 R2 with SP1 or later</li> <li>.Net 4.6</li> <li>IIS 8.5</li> <li>Chrome, Internet Explorer 11, or Edge</li> <li>A monitor with at least 1024 x 768 resolution</li> </ul>	
Service Hub	<ul> <li>Windows Server 2012 R2 with SP1 or Windows Server 2016</li> <li>.Net 4.6</li> <li>IIS 8.5</li> </ul>	
Service Hub Database Internal	Microsoft SQL Express Server 2014 SP1	
Service Hub Database External	Microsoft SQL Express Server 2014 SP1	
MaxACD Proxy/Redirector	<ul> <li>Windows Server 2012 R2 with SP1</li> <li>.Net 4.6</li> <li>IIS 8.5</li> </ul>	
MaxAdmin	<ul> <li>Windows Server 2012 R2 with SP1 or Windows Server 2016</li> <li>.Net 4.6</li> <li>IIS 8.5</li> <li>Internet Explorer 11 and Edge, or Chrome</li> </ul>	
MaxACD CWS DB Internal	Microsoft SQL Express 2014 SP1 (32-bit)	
MaxACD CWS DB External	Microsoft SQL Server 2014 SP1	
External CDR Database	Microsoft SQL Server 2014 SP1	
Email Integration	Microsoft Exchange Server 2013, 2016, and Exchange Online	
Microsoft Lync/Skype for Business	<ul> <li>Lync Server 2013, plus the latest CU that has been approved by Altigen</li> <li>Skype for Business 2015, plus the latest CU that has been approved by Altigen</li> </ul>	
Web Chat Server	<b>Note:</b> The Web Chat server is not supported on Windows 10.	

# **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	Supported operating systems <ul> <li>Windows 8.1 (64-bit)</li> <li>Windows 10</li> <li>.NET Framework 4.6</li> <li>Outlook 2010</li> </ul>	
	<ul> <li>Hardware minimum requirements</li> <li>2GHz CPU</li> <li>5GB available disk space</li> <li>1GB RAM</li> <li>SVGA monitor 1024 x 768 with 256-color display</li> <li>Keyboard and mouse</li> </ul>	
	<ul> <li>Lync/Skype requirements</li> <li>Lync 2013 desktop client</li> <li>Skype for Business 2015/2016 desktop client</li> </ul>	
MaxSupervisor	<ul> <li>Supported operating systems</li> <li>Windows 8.1 (64-bit)</li> <li>Windows 10</li> <li>.NET Framework 4.6</li> <li>Hardware minimum requirements</li> <li>2GHz CPU</li> <li>5GB available disk space</li> <li>1GB RAM</li> <li>SVGA monitor 1024 x 768 with 256-color display</li> <li>Keyboard and mouse</li> <li>Lync/Skype requirements</li> <li>Lync 2013 desktop client</li> <li>Skype for Business 2015 desktop client</li> </ul>	
MaxInSight	<ul> <li>Supported operating systems</li> <li>Windows 8.1 (64-bit)</li> <li>Windows 10</li> <li>Minimum hardware requirements</li> <li>1GHz CPU</li> <li>5GB disk space</li> <li>1GB RAM</li> <li>SVGA monitor 1024 x 768 with 256-color display or better</li> <li>Keyboard and mouse</li> </ul>	



Client Requirements		
VR Manager A VR Manager license must be installed in MaxAdmin	<ul> <li>Supported operating system for the VRM Server</li> <li>Windows Server 2012 R2 SP1</li> <li>The installation program will automatically install JAVA JRE 1.8.0.171</li> <li>VRM Server should be installed on a standalone server, not on the MaxACD server.</li> <li>During a new installation of VRM, SQL Express 2014 will automatically be installed.</li> <li>Minimum hardware requirements for the VRM Server</li> <li>2GHz Quad-core CPU</li> <li>For installation: 10GB disk space (more space is required for storing voice files)</li> <li>3GB RAM</li> <li>Supported operating systems for the VRM Client</li> <li>Windows 8.1 64-bit or Windows 10</li> <li>.Net 4.5</li> <li>Minimum hardware requirements for the VRM Client</li> <li>Intel 2GHz Pentium 4 or equivalent</li> <li>40GB available disk space and 2GB RAM</li> </ul>	
Advanced Call Router (must be installed on the same machine as MaxACD Admin)	<ul> <li>Supported operating system</li> <li>Windows Server 2012 R2 SP1</li> <li>Minimum hardware requirements</li> <li>Intel 2GHz Pentium 4 or equivalent</li> <li>40GB available disk space</li> <li>2GB RAM</li> </ul>	
MaxReports	Supported operating systems • 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 Minimum hardware requirements • 2GHz CPU • 60GB available disk space • 3GB RAM Client system requirements • Chrome or Internet Explorer 11 or Edge	
AltiSDK	Supported operating systems <ul> <li>Windows Server 2012 R2 with SP1</li> <li>Windows 8.1 64-bit</li> <li>Windows 10</li> </ul>	
AltiControl	Supported operating systems <ul> <li>Windows 8.1 64-bit</li> <li>Windows 10</li> </ul>	



# **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**

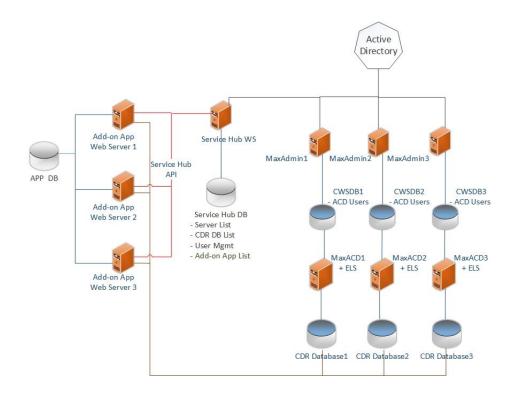
The following table lists the licenses available for new MaxServer customers.

Licenses for MaxACD				
MaxServer Base Server License (9Unn0)	<ul> <li>This base license enables basic functions for MaxServer.</li> <li>This license does not include MaxGroup or ACD functionality; therefore, customers must also order one of the following licenses: <ul> <li>MaxGroups Feature License</li> <li>MaxACD Feature License</li> </ul> </li> </ul>			
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, <u>MaxACD Redundancy Installation</u> 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.
- 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).



S	Define New Front End Pool
Ē.	Select features
	t messaging and presence are always enabled. Select the additional features that you want this End pool to handle.
<u>ء</u> ک	2nferencing (includes audio, video, and application sharing) ]Dial-in (PSTN) conferencing
🗆 En	terprise ⊻oice
Ca	all Ad <u>m</u> ission Control III admission control (CAC) is an optional component that manages the bandwidth used by unified mmunications traffic within the deployment. Only one Front End pool per site can enable CAC.
	chiving enable Exchange Server integration, use Skype for Business Server Control Panel.
М № М	onito <u>r</u> ing (CDR and QoE metrics)
He	lp <u>B</u> ack <u>N</u> ext Cancel

- 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.
- 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: <u>https://www.microsoft.com/en-us/download/details.aspx?id=34992</u>
  - 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.

16	Define Ne	ew Server	x
Fully qua	lified domain name (FQDN	l): *	
maxacd	b.lyncdomain.com		
🖌 Enabl	e IPv4		
• U	se all configured IP addres	ses.	
O Li	mit service usage to select	ed IP addresses.	
Pi	rimary IP address:		
🗌 Enabl	е ІРνб		
Help		OK	Cancel

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.

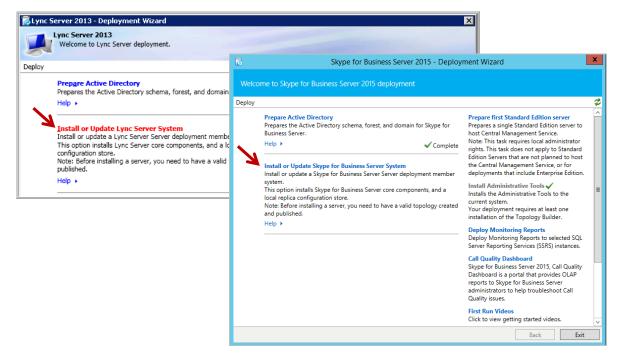
#### 3A: Install Local Configuration Store

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

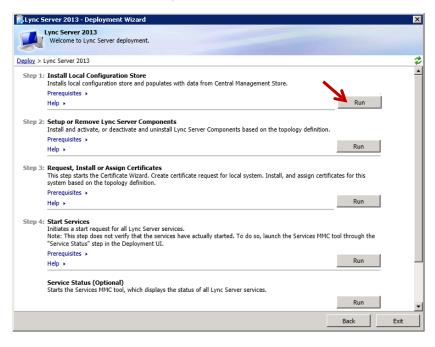
1. Log in as a user in RTC Universal Server Admins AD group. Use your Lync Server or Skype Installation media and run *the Lync Server Deployment Wizard*.



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

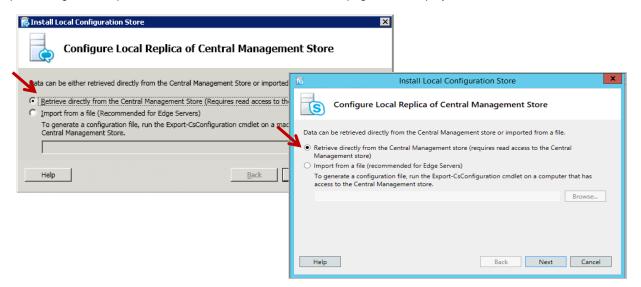


3. For "Step 1, Install Local Configuration Store," click Run.





4. 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

- 1. For "Step 2, Setup or Remove Lync Server Components," click Run and then click Next.
- 2. 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.

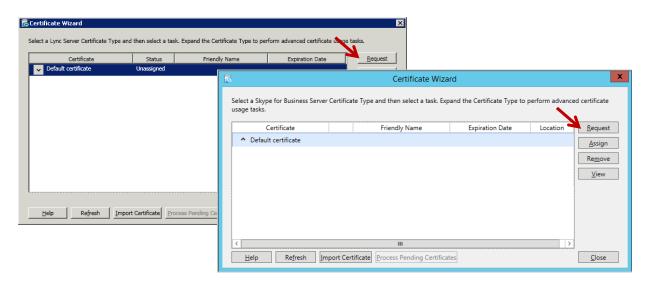
	🔂 Lync Server 2013 - Deployment Wizard	×
	Velcome to Lync Server deployment.	
	Deploy > Lync Server 2013	\$
	Step 1: Install Local Configuration Store Installs local configuration store and populates with data from Central Management Prerequisites  Help  Help	t Store.
	Step 2: Setup or Remove Lync Server Components	
🐻 Skype fo	r Business Server 2015 - Deployment Wizard	opology definition.
Install or update member system		Run
Deploy > Install or update		2
Step 1: Install Local Configuration Store Installs local configuration store and	populates with data from Central Management Store.	
Prerequisites 🕨		
Help 🕨	✓ Complete Run Again	
	ess Server Components d uninstall Skype for Business Server Components based on the topology	
definition.		=
Prerequisites >	Run	
Help 🕨	Kun	



#### 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.

🐻 Certificate Request	×
Delayed or Immediate Reque	ests
Do you want to prepare a certificate request to be sent lat certification authority? © I send the request immediately to an online certification © Prepare the request now, but send it later (offline cert	Choose a Certification Authority (CA)
Help	Select a certification authority to process your request. The Certificate Wizard will automatically import the selected CA's certificate chain if necessary.  Select a CA from the list detected in your environment.  AltiLocal.XYZ.com\AltiLocal-ABCD-ATGNBLRIo  Specify another certification authority.
	Help Back Next Cancel
	Help <u>B</u> ack <u>N</u> ext Cancel



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

ธี	Certificate Request	x
Cer	tificate Request	
Select a <u>C</u> A from	n the list detected in your environment.	
ENGSFB2015-	DC.ENGSFB2015.COM\ENGSFB2015-ENGSFB2015-DC-CA	-
<u>Friendly name:</u>		
Skype for Busir	ness Server 2015 Default certificate 12/7/2015	
Organization:	Organizational <u>u</u> nit:	
Country/ <u>R</u> egior	N:	
State/Province:	City/ <u>L</u> ocality:	
Select one or m alternative nam	ore SIP domains for which a sip. <sipdomain> entry is to be added to the subject es list.</sipdomain>	
🗆 All		

- 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.

Certificate Request	×	
	Certificate Request	x
Country us some CA. SUID said and internationalitie in State Organization "Altrictics" (3) "80" adSigContain (0 Valuentister AL TELECK UpgContrictics(C)Telegian Creating new log file "Cliters/idenmetrator AL TELECK) CSCentrate Statistics Suid (00% add) deallocatient(C) in	Executing Commands	
Search a certificate request leased on Love Sance compar- based from one "HEAL" of the Control of Table Control of the "A Table Control of the Control of the Control of Table Control to the Control of the Control of the Control of Table Control Control one log file "Citizent information at Table Control Control on 1913 is 12 - 23 (Mini)". Tagued Control of the Control of the Comparison Social Control of the Control of the Control of the Control Control on 1913 is 12 - 20 (Mini)". Task status: Completed.	CSCertificate-[2015_12_07][17_21_56].xml". Create a certificate request based on Skype for Business Server configuration for this computer. Issued thumbprint "86B2E37CFED1300EAA82154E33D41E3ADE1D9D7D" for use "Default,WebServicesInternal,WebServicesExternal" by "ENGSFB2015-DC.ENGSFB2015.COM \ENGSFB2015-ENGSFB2015-DC-CA". No changes were made to the Central Management Store. Creating new log file "C:\Users\Administrator.ENGSFB2015\AppData\Local\Temp\2\Request- CSCertificate-[2015_12_07][17_21_56].html". "Request-CSCertificate" processing has completed successfully. Detailed results can be found at "C:\Users\Administrator.ENGSFB2015\AppData\Local\Temp\2 \Request-CSCertificate-[2015_12_07][17_21_56].html".	
Request Certificate	Task status: Completed.	~
	Request Certificate	og
	Help Back Next Cance	2



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

🔂 Certificate Request	X	
Online Certificate Request	Ctatue	X
	Certificate Assignment	
A certificate with thumburnt 9636.725PPC328562977 certificate store.	Certificate Assignment	
	Assign the returned certificate to the Skype for Business Server usages on this server.	
Assign this certificate to Lync Server certificate us	View Certificate Details	
Note: If you choose not to assign the certificate now, the Certificates wizard.		
View Certificate Details		
Help	Help Back Next Ca	ncel

7. Click Next to assign this certificate.

🔞 Certificate Assignment		
Certificate Assignment	Certificate Assignment	×
Assign the returned certificate to the Lync Server usages on this	Certificate Assignment	
View Certificate Details	Assign the returned certificate to the Skype for Business Server usages on this server. View Certificate Details	
Help		
	Help Back Next	Cancel

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



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

Certificate Assignment		
Executing Commands	3	
> Awage Cattificate Set CSCattificate - Tops Default -Thumburiet rilagost C: USaevickimmistratur, ALTECCAL (92, 92, 93, 94) Amerikaning cattificate was assigned for the Default Statistication Construction Con- Relation (Statistication) Chi-rithEarch ALTECORDC CA, DC-ABLaco	AppCatal).acal(Neng)2566-CSC e tupe "Definit": NC3854967880 ManACDIN_5.alt	Sertificate (2012_09_05) Nacal.com 05/05/2014
Task status: Completed.		
Assign Certificate		▼

# 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
  - o 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. That system cannot be on the same server as the two MaxACD systems 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**

1. 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. <u>Make all required updates before you proceed</u>.



- 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.

N	AaxACD 7.1 - InstallShield Wiza	ard 🗶
Service Hub DB Installati	on	
Enter Service Hub DB databa	se login credential.	
SQL Server Address:	10.30.1.110	
SQL Instance:	SQLEXPRESS	
SQL Sysadmin account:	sa	
SQL Sysadmin password:	******	
Service Hub DB Name:	SHDBHosted111	
Service Hub DB Account:	sa	
Service Hub DB Password:	********	[Length 8~20]
[Note: To use an existing/def InstallShield	ault password, leave SQL Service Hub DB	

- **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.

Please enter your information.		
Please enter your name and the name of the com	any for which you	work.
User Name:		
Windows User		
Company Name:		
Company Name: [AltiGen]		
The second second		

- 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 and "_" are allowed.	n from 1 to 24 characters. Only alphanumeric characters
System Name: ACD1	
stallShield	
	<back next=""> Cancel</back>



- 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.

MaxACD Proxy Configuration		۸	
Please input ACD Trusted Applicatio	n Parameters		
ACD Trusted Application ID	pmapp		
installShield			
	< Back	Next >	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**.

MaxACD Proxy Configuration	
Please input ACD Proxy AEP Parameters	
ACD Proxy Server Id	1
ACD Application End Point Prefix	Corp
SIP Domain	ARCloud.com
InstalShield	
	< Back Next > 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\Alti\_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\Alti_COBALT200103
🔍 AltiGen Lync Redirector Ser	AltiGen Lyn	Running	Automatic (D	SYMPHONY\Alti_COBALT200103
🎑 AltiGen Switch Gateway Ser	AltiGen Swit	Running	Automatic	SYMPHONY\Alti_COBALT200103
🔍 AltiGen Switching Service C	AltiGen Serv	Running	Automatic	SYMPHONY\Alti_COBALT200103
🎑 AltiGen VM AltiView Service	AltiGen VM	Running	Manual	SYMPHONY\Alti_COBALT200103
🔍 AltiGen VM Exchange Integr	COM Server	Running	Automatic	AltiServAdmin@altigen.com
🔍 AltiGen VM Message Service	AltiGen VM	Running	Manual	SYMPHONY\Alti_COBALT200103
🎑 AltiGen VM POP3 Service	COM Server	Running	Manual	SYMPHONY\Alti_COBALT200103
🔍 AltiGen VM Postman Service	AltiGen VM	Running	Automatic	SYMPHONY\Alti 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 the 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.

■ Altigen Service	
Servers List	
10-40-1-641	1
10.40.1.40	0

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.

≡ Altigen Servie	ce Hub			admin 🛔	Internet
Servers List		Administration Applications			
10-40-1-641					
10.40.1.40	0	Service Hub Configuration 10.40.1.40 MaxServer Admin MaxReports Pro for A	.CD		

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**.)

0	-MAXACD Ma	axAdmin
Application Admin	MaxServer Adr	nin
	URI Routing	Caller ID Routing
<b>%</b>		Search
System	U	રા
	🔊 sip:Accountir	ngGroupU

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 (<u>https://mspartner.altigen.com</u>).

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.

			System Lis	t				
			(Total 3)					
		A	dd New Syste	m				
End User	System Key	Address	City	State	Zip Code	Start Date	Configure	
Singapore Office	the contract of the second states	123 A St	San Jose	CA	94567	02/02/10	Activate Lic	License File
ondohare ouree			C	CA	94536	02/02/10	Activate Lic	License File
Shanghai Office	same of the second second	456 B St	Fremont	CA.	04000	02002010	A ARREST PRESE PRESE	

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

🥖 Add New System - Internet Explorer	- 0	×
http://mspartner.altigen.com/LyncPartner/	/support/ACDSystemAdd.aspx?ACDID=10011&SourceFr	om=
Ad	d New System	
System Information		
System Key*:		
Hosting Name :		
Redundancy Hosting Name :		
End User Information		
End User*: Address*: City*: State/Province*: Zip/Postal Code*: County*: Phone*:		
	5	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: MAXACI Target Registration Version: MAXACI		,		
icense	Activated	Available	Additional Qty	
axACD Redundancy (6RD00)	1	984	V	
laxACD for Lync Server License (9Lnn0)	1	3271		
taxAgent for Lync License (9Ann0)	36	1319		
axSupervisor for Lync License (9Bnn0)	501	1964		
axACD CRM Integration (RNnn0)	202	176		
IAXACD MaxAgent Seat Combo - Voice and Chat 9Knn0)	5	35		
ecording Seat (R9nn0)	501	1289		
The license activation file	e was generated Email License		Generate License Download License	

7. On the MaxACD server, open the \AltiServ\exe folder and run the executable RegLicense.exe.

uration	
Use Soft System Key	
Expiration Date	~
	=
	_
	_
	~
	Enter the System Key

- 8. Check the box **Use Soft System Key.**
- 9. Click Enter the System Key.
- 10. Type the system key into the **System Key** field.
- 11. Click **Load**, navigate to the EXCTL.DAT file you downloaded from the Altigen Partner portal, and then click **Open**.
- 12. 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.



Enable Name User Password Email UM Subscriber A	ccess
Edit sip:	

- 2. Complete the fields and click **Update**. For more about the Exchange UM subscriber, refer to page 55.
- 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.

Voicemail			
Enable (	Group V	/oicemail	
V Engl		nt to Access Group Voicemail	
L Cliar	ne Agei	it to Access Group voicemail	
SIP URI	sip:	tso-maxacd@altigen.com	

**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.

Multi-Lingual	SNMP Configuration	Presence Mapping	Redundancy
Server	Reports Account Code	Logout Reason Code	Call Recording
Application Server			
ID System ID	Name	Address	Status
1 41	10-40-1-40	10.40.1.40	Active
Proxy			
ID Name	Ad	dress	Status
1 FWS40APP	10.	40.1.40	Active
Maximum Number of Users * Note: Changing the maxin		art MaxACD services.	
Web Server Host Name : 1 Maximum Number of Users * Note: Changing the maxim Phone Number System Main Number Incoming Call DNIS Leng	s [10-5000] 600 mum number of users requires re-sta	art MaxACD services.	
Maximum Number of Users * Note: Changing the maxii Phone Number System Main Number	s [10-5000] 600 mum number of users requires re-sta	art MaxACD services.	
Maximum Number of Users * Note: Changing the maxin Phone Number System Main Number Incoming Call DNIS Len	s [10-5000] 600 mum number of users requires re-sta	art MaxACD services.	
Maximum Number of Users * Note: Changing the maxii Phone Number System Main Number Incoming Call DNIS Len Active Directory	s [10-5000] 600 num number of users requires re-sta gth 7 \$	art MaxACD services.	] 0
Maximum Number of Users * Note: Changing the maxii Phone Number System Main Number Incoming Call DNIS Len Active Directory Enable Encryption	s [10-5000] 600 num number of users requires re-sta gth 7 \$	art MaxACD services.	] 0
Maximum Number of Users * Note: Changing the maxii Phone Number System Main Number Incoming Call DNIS Len Active Directory Enable Encryption Domains * ALTI20	s [10-5000] 600 num number of users requires re-sta gth 7 \$	art MaxACD services.	@

# 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,
  - 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.

🚟 ODBC Da	ta Source Administra	tor	×
User DSN	System DSN File DSN	Drivers Tracing Connection Pooling Ab	out
- 2	ata Sources:		
Creat	e New Data Source		×
с 		Select a driver for which you want to set up a	data source.
		Name	\▲
		Microsoft Text Driver (*.txt; *.csv)	E
	011 0	Microsoft Text-Treiber (*.txt; *.csv)	E
		Microsoft Visual FoxPro Driver	1
		Microsoft Visual FoxPro-Treiber	1
		SQL Server	E
		SQL Server Native Client 10.0	2
		SQL Server Native Client 11.0	2
t		•	Þ
		< Back Finish	Cancel

- 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*.



External Logger Service Configuration
External Logger Password 84TDY19dd#55&* About
CODBC
Source Name: Test
Description:
Login ID: Password:
NOTE: 64bit DDBC DSN is not supported. If the DDBC source you configured is not found, you should run %systemdrive%\Windows\Sys\WoW64\ odbcad32.exe to create a 32bit DDBC DSN first and then run this External Logger Service Configuration Tool again.
Purge (Microsoft Access Database only)
Active database retaining period 0 month(s)
Archive purged records
Skype for Business CDR Database
Server Name: 10.40.1.55 Test
Database: LcsCDR
C Windows autihotication
SQL Server authentication
Login ID: Password:
OK Cancel

- 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 <u>Federated</u> <u>Deployments</u> to configure the dbConnect Service.
- **Note:** If you want to enable Windows authentication, follow the steps in the section <u>Enable Windows</u> <u>Authentication</u> 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.



	Enable	Name	Server	Port	Status	Password
	$\checkmark$	Internal Log Service	127.0.0.1	10029	Connected	Default
Edit Delete		External Logger	10.40.1.123	10027	Disable	Default

- 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 (<u>http://[machinename]:8080/MaxReports</u>).
  - c. Log in as the admin (default password is '22222').



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

Home Page		
Configuration	CDR Database Registration -> Add	
Administrator Profile		
CDR Database Registration	Database Description	
MaxACD Registration	Database Server Type	Microsoft SQL Server -
User Management		
Mail Server Configuration	Database Server IP Address	
Backup and Restore	Port	1433
Log Configuration	Database User Account	
	Database User Password	
	Database Name on the Server	
		Add

- 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<br/>careful with the Skype SIP Refer Support option. Release 6.5.8 trunk configuration needs SIP<br/>Refer Support to be enabled. However, Release 7.1 needs SIP Refer Support to be disabled. If you<br/>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.



Server Name: 10.30.24		Test
Database: LcsCDR		
<ul> <li>Windows autihotica</li> </ul>		
C SQL Server authen	ication	
Login ID: sa	Passwo	rd:

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**.

Altigen Direct Call CDR Service	Name	Description Stat	tus Startup Type	Log On As
	G Active Directory Federation Services	Enables Acti	Manual	Network Service
Stop the service Restart the service	G ActiveX Installer (AxInstSV)	Provides Us	Manual	Local System
	AltiGen AutoUpgrade Service	AltiGen Serv Run	nning Automatic	ALTI2013\Alti_MAXACD155221
	G AltiGen CTProxy Service	AltiGen CTP Run	nning Automatic	ALTI2013\Alti_MAXACD155221
Description: Service to collect Lync personal calls CDR out side MaxACD	Q Altigen Direct Call CDR Service	Service to c Run	nning Automatic (D	Administrator@Alti2013.com
	🕼 AltiGen Keep Up Service	AltiGen Kee Run	nning Manual	ALTI2013\Alki_MAXACD155221
	AltiGen MaxACD External Logger Service	AltiGen Exte Run	nning Automatic (D	Local System

- 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**.

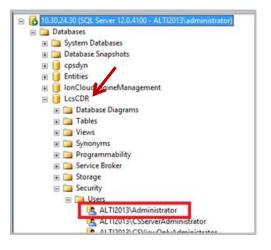
Altigen Direct Call C	DR Service Properties (Local Com 💌
General Log On Reco	very Dependencies
Log on as:	
Local System accour     Allo <u>w</u> service to in	nt iteract with desktop
This account:	Administrator@Alti2013.com
Password:	•••••
Confirm password:	•••••
L	OK Cancel Apply



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

æ 📮	Databases
8	Security
E	🔁 Logins
	2 ##MS_PolicyEventProcessingLogin##
	##MS_PolicyTsqlExecutionLogin##
	ALTI2013\Administrator
	ALTI2013\CSAdministrator
	ALTI2013\CSServerAdministrator
	ALTIDOTOLOGICA

8. 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, <u>Step 9: Configure the MaxACD External Logger Service</u>. 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,

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



Serveri	10.30.1.110:10073	
Password		
SQL Server	10.30.2.20	
Authentication:	SQL Server Authentication •	
Database:	lesedr	
SQL User:	5 <b>3</b>	
SQL Password:		

- 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 readonly 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.

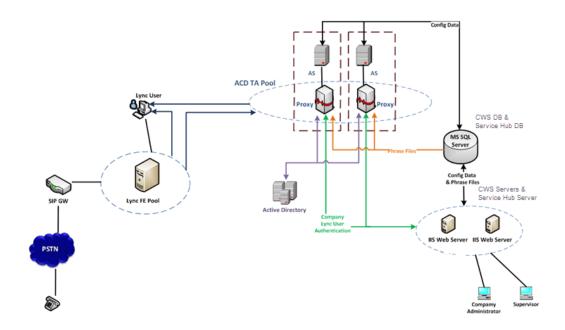
If the standby server does not detect the active server's heartbeat for 10 seconds, the standby server promotes itself, registers Proxy to the ACD Trusted Application Pool, and routes AEPs to its own Proxy. It will take over control within approximately 10 seconds. When switchover occurs, the standby 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.

🛔 DNS Manager	
File Action View Help	
🗢 🔿 🖄 🖬 🗙 🖬 🧟 📾	
Conditional Forwarde Rel	Name (same as parent folder (same as parent folder (same as parent folder date Server Data File oad Host (A or AAAA)
New Host Name (uses parent domain name if b	ank):
MaxACD1 Fully qualified domain name (FQDN): MaxACD.LyncDomain.com.	New Host
IP address: 10.40.1.171	Fully qualified domain name (FQDN): MaxACD.LyncDomain.com.
<ul> <li>Create associated pointer (PTR)</li> <li>Allow any authenticated user to same owner name</li> </ul>	IP address: 10.40.1.172
	<ul> <li>Create associated pointer (PTR) record</li> <li>Allow any authenticated user to update DNS records with the same owner name</li> </ul>

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.

MaxACD for Lync 7.0 - InstallShield Wizard	23
Server Redundancy Configuration	
Please Select MaxACD 7.0 type you want to installed. Single Server Redundancy	
InstallShield	Next > Cancel

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.

MaxACD for Lync 7.0 - InstallShield Wizard	x
Server CWSDB Configuration	
Is CWS DB already deployed?	
InstallShield	< Back Next > Cancel

**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.



Settings	
CWSDB	
CWSDB Password	*********** Show Password

- 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.

System ID	
MaxACD has been installed. Ente	this MaxACD server. This ID cannot be changed once r a unique ID number unless this server is half of a redundant rs must have the same System ID.}
nstafföhleid	< Back Next > Cancel

- 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.

 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*.

ast Switch O	ver Time		
ast Switch O	ver Reason		
First Serve	r	Second Server	5
Server	10-40-1-40.ALTI2013.com	Server	
In Control	None	in Control N	one
Status	None	Status N	one

## **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.

E CWSDB23	
	New Database
🗄 📔 Fake1 (Syn	New Query
🗉 🧻 Fake2 (Syn	Script Database as
🗉 📔 Freeswitch	
🗉 🧻 IonCloudEr	Tasks •
🗉 📋 LcsCDR (Sy	Policies
🕀 📔 LcsLog (Syı	Facets
표 📔 lis (Synchro	
🗉 🧻 mgc (Syncl	Start PowerShell
🗉 间 QoEMetric	
🗉 🧻 quicktest	Reports •
🗉 🧻 quicktest2	Rename
🗉 🧻 rgsconfig (	Delete
표 间 rgsdyn (Syr	
🕀 📔 rtcab (Sync	Refresh
🗉 🧻 rtcshared (	Properties
🗉 间 rtcxds (Synchr	onized)
🕀 间 SFBReports	×.



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

0	Database Properti	es - CWSDB23	- 🗆 X
Select a page	🔄 Script 🔻 📑 Help		
Files Filegroup Options Change Tracking Fermissions Extended Properties Mirroring Transaction Log Shipping	Collation: Recovery model: Compatibility level: Containment type: Other options:	SQL_Latin1_General_CP1_CI_AS Simple Full Bulk-logged Simple	~

- 2. Back up the database. The database must be backed up prior to adding to the availability group. Perform a full backup.
  - T CHODDLE (Synchronized) 🕀 间 CWSDB23 New Database... 🗉 📋 Entities (Syr New Query 🕀 📋 Fake1 (Sync Script Database as 표 间 Fake2 (Şync ۲ Detach... 🕀 📔 Freeswitc Tasks ۲ 🗉 间 IonCloudEr Take Offline Policies 🗄 📔 LcsCDR (Sy Þ **Bring Online** 표 间 LcsLog (Syr Facets 🗉 间 lis (Synchro Shrink Start PowerShell 표 间 mgc (Synck Back Up... 🗉 间 QoEMetrics Reports ۲ R 🗉 🧻 quicktest Restore Rename 🗉 间 quicktest2 Mirror... 🗉 间 rgsconfig ( Delete Launch Database Mirroring Monitor... 표 间 rgsdyn (Syr Refresh Ship Transaction Logs... 표 📔 rtcab (Sync Properties 🕀 📔 rtcshared (S Generate Scripts... It is in the second Extract Data-tier Application... SFBReportsTempDB Deploy Database to Windows Azure SQL Database... 🗉 间 xds (Synchronized) Deploy Database to a Windows Azure VM... 🗉 🚞 Security Export Data-tier Application ... 🗉 🚞 Server Objects Register as Data-tier Application... 🚞 Replication 1 🖃 🚞 AlwaysOn High Availability Upgrade Data-tier Application... 🖃 🚞 Availability Groups Delete Data-tier Application... ACD-CDRAG01 (Primary) ACD-CWSAG01 (Primary) Import Data... < 🗉 🚞 Availability Replicas Export Data... 📼 🚞 Availability Databases 🕗 Οι Copy Database... >
  - 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.

۲

۲



Ū	В	ack Up Database - CWSDB23	_ <b>D</b> X
Select a page General	Script 🔻 📑 Help		
Media Options	Source		
	Database:	CWSDB23	×
	Recovery model:	FULL	
	Backup type:	Full	۷
	Copy-only backup		
	Backup component:		
	<ul> <li>Database</li> </ul>		
	○ Files and filegroups:		

- 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**.

tê -	Add Database to Availability Group - ACD-CWSAG01
Introduction	
Introduction	😨 Help
Select Databases Select Data Synchronization Connect to Replicas Validation Summary Results	Add database to this availability group. This wizard allows you to add one or more availability databases to an existing availability croup. The new user database on this instance of SQL Server. Select your initial data synchronization preference. Select your initial data synchronization preference. Check the validation results of adding the new database to the availability group. Review your selections. The proference of the synchronization of the synchronization of the synchronization of the synchronization preference. Review your selections. The proference of the synchronization of the synchronizatio
	To begin adding database, click Next.
	< Previous Net> Cancel

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

ñ	Add Database to Availability	y Group - A	CD-CWSAG01 - 🗆 🗙
Select Databas	ses		
Introduction			😥 Help
Select Databases	Select user databases for the	availability gr	roup.
Select Data Synchronization	User databases on this instance	of SQL Server	r.
Connect to Replicas	Name	Size	Status ^
Validation	ACD190021	5.0 MB	Already part of this availability group
Summary	ACDCDR21	5.0 MB	Already part of an availability group
	ACDCDR22	14.8 MB	Already part of an availability group
Results	cpsdyn	256.0 NB	Already part of an availability group
	CWSDB21	32.8 MB	Meets prerequisites
	CWSDB22	114.1 MB	Already part of this availability group
	Entities	1.5 GB	Already part of an availability group
	Fake1	5.0 MB	Already part of this availability group
	Fake2	5.0 MB	Already part of an availability group
	FreeswitchCDRDB	5.0 MB	Already part of an availability group
	IonCloudEngineManage	7.8 MB	Already part of an availability group
	LcsCDR	2.1 GB	Already part of an availability group
	LcsLog	1.1 GB	Already part of an availability group
			Refresh
			< Previous Next > Cancel



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

<u>()</u>	Add Database to Availability Group - ACD-CWSAG01	×
Select Initial	l Data Synchronization	
Introduction		😧 Help
Select Databases	Select your data synchronization preference.	
Select Data Synchronization	• Full	
Connect to Replicas	Starts data synchronization by performing full database and log backups for each s database. These databases are restored to each secondary and joined to the availab group.	
Summary	Specify a shared network location accessible by all replicas:	
Results	V\SFB-SQL01\SQLTemp Bro	owse
	<ul> <li>Join only         Starts data synchronization where you have already restored database and log back each secondary server. The selected databases are joined to the availability group o secondary. This action will be skipped for Azure replicas.     </li> <li>Skip initial data synchronization         Choose this option if you want to perform your own database and log backups of e primary database.     </li> </ul>	on each
	< Previous Next > C	ancel

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).

<i>4</i>	Add Database to Av	vailability Group - ACD-CWSAG01	_ 🗆 X
Connect to Exis	sting Secondary R	eplicas	
Introduction			😧 Help
Select Databases	Connect to all the	existing secondary replicas.	
Select Data Synchronization		n configure existing endpoints to grant them	appropriate permissions,
Connect to Replicas	you must connect to	o all the existing secondary replicas.	<b>\</b>
Validation	Server Instance	Connected As	7
Summary	SFB-SQL02	Not Connected	Connect
Results	e.	Connect to Server	×
	Server type: Server name:	Database Engine SFB-SQL02	~
	Authentication:	Windows Authentication	~
	User name:	SFBHOSTING\ben.kaufman	~
	Password:		
		Remember password	
	Conn	ect Cancel Help Opti	ons >>
			Connect All
		< Previous	Next > Cancel



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

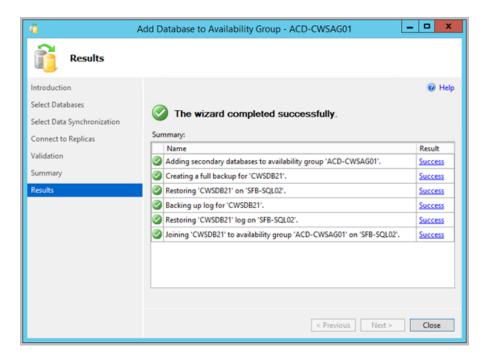
- ñ	Add Database to Availability Group - ACD-CWSAG01	D X
Validation		
Introduction		😧 Help
Select Databases	Results of availability group validation.	
Select Data Synchronization	Name	Result
Connect to Replicas	Checking whether the endpoint is encrypted using a compatible algorithm	Success
Validation	Checking shared network location	Success
Summary	Checking for free disk space on the server instance that hosts secondary re	Success
Summary	Checking if the selected databases already exist on the server instance that	Success
Results	Checking for compatibility of the database file locations on the server insta	Success
	Checking for the existence of the database files on the server instance that	Success
	Checking the availability mode compatibility between the primary and sec	Success
	Re-run	Validation
	< Previous Next >	Cancel

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

ñ	Add Database to Availability Group - ACD-CWSAG01	_ <b>D</b> X
Summary		
Introduction Select Databases Select Data Synchronization	Verify the choices made in this wizard. Click Finish to perform the following actions:	😧 Help
Connect to Replicas Validation Summary Results	Availability Group: ACD-CWSAG01 Databases CWSDB21 (32.8 MB) Initial data synchronization: Full Backup location: \\SFB-SQL01\SQLTemp	
	< Previous Fini	Script 💌

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





4. 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

Ũ		Database Properties - CWSD	DB23
Select a page	🛒 So	cript 🔻 📑 Help	
Files     Filegroups     Options     Change Tracking     Pemissions     Fetneded Properties			10/14/2016 9:33:39 AM 10/14/2016 9:33:40 AM
Transaction Log Shipping		Database Name Status Owner Date Created Size Space Available Number of Users Memory Allocated To Memory Optimized Objects Memory Used By Memory Optimized Objects	
	⊿	Maintenance Collation	SQL_Latin1_General_CP1_CI_AS
Connection			
Server: SFB-SQL01 Connection: SFBHOSTING/ben.kaufman P View connection properties			
Progress Ready	Na The	<b>ne</b> name of the database.	

5. Create a stored procedure for sp\_help\_revlogin, based on this Microsoft article: https://support.microsoft.com/en-us/kb/918992



6. Run sp\_help\_revlogin on the PRIMARY replication server. Use the database owner you identified in step 4.

sQLQuery24.sql - SFB-SQL01.master (SFBHOSTING) - Microsoft SQL Server Management Studio - 🗖 🗙
File Edit View Query Project Debug Tools Window Help
: 🛐 🕶 📨 💕 🛃 🥥 🔔 New Query 🕞 🤧 🚱 🕉 🕉 🦓 🖘 🛍 🍂 🦿 🕫 🖓 🕫 🖓 👘 🖓 👘 🖓 👘
1 말 값 master 🔹 🧜 Execute 🕨 Debug 💻 🗸 🎲 🕘 🔒 🎬 🍓 🎒 🔚 🗄 😫 🐺 👘 🕼 📮
Object Explorer
Connect * 🛂 👷 = 🍸 😰 😹 🕴 EXEC sp_help_revlogin CWSDBServerUser23
🔤 🔁 SFB-SQL01 (SQL Server 12.0.4100.1 - SFBHOSTING\tag
🖃 🧰 Databases
🛞 🧰 System Databases
🕑 🧰 Database Snapshots 🛛 🗏
ACDCDR11 (Synchronized)     ACDCDR21 (Synchronized)     ACDCDR21 (Synchronized)
■ ACDCR23 (synchronized)
CWSDB11 (Synchronized)
🗉 🧻 CWSDB21 (Synchronized)
🗑 📔 CWSDB22 (Synchronized)
🗄 📔 CWSDB23 (Synchronized)
Entities (Synchronized)
⊮ Generated Oct 14 2016 9:44AM on SFB-SQL01 */     ** Generated Oct 14 2016 9:44AM on SFB-SQL01 */
■ Fake2 (Synchronized)
H      FreeswitchCDRDB (Synchronized)     Login: CWSDBServerUser23     Torrest control of the second seco
B Conclosultiginetwiningement (Synchronized)     CREATE LOGIN [CWSDBServerUser23] WITH PASSWORD = 0x0200F0FA70167A9AB88DCAA29BFD34848A     CREATE LOGIN [CWSDBServerUser23] WITH PASSWORD = 0x0200F0FA70167A9AB88DCAA29BFD34848A
C III COLORIDA CUERT CONTRACTOR C
Ready Ln 1 Col 23 Ch 23 INS

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

SQLQuery1.sql - SF\ben.kaufman (72))* 🗙
□/* sp_help_revlogin script ** Generated Oct 14 2016 9:44AM on SFB-SQL01 */ Login: CWSDBServerUser23
CREATE LOGIN [CWSDBServerUser23] WITH PASSWORD = 0x0200F0FA70167A9AB88DCAA29BFD34848AD2
100 % × < III >
100 % V III
Command(s) completed successfully.
=
~
100 % • < >
Query executed successfully. SFB-SQL02 (12.0 SP1) SFBHOSTING master 00:00:00 0 rows



#### **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.)

MaxServer Adm	lin		
Version	7.1		
Landing Page	https://	cws.sfbhosting.com/avb94	
Security Key			5

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.

Admin	MaxServer Admin	
Streets G	Settings	
<b>%</b> System	Upgrade Data Upgrade Data	
a User	CWSDB Password Show Password	
	Single Sign On Service Hub URL http://corp18.atigen.com/ServiceHub	]
MaxGroups	Issuer https://ServiceHub.altigen.com Application.ld Security Key	
Workgroup	Admin Password Settings	-
t Work Hours	Current Password New Password Confirm Password	
License	OK Cancel	-
¢ Settings		



# **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 are 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
- Front End pool disaster recovery in Skype for Business Server 2015" <u>https://technet.microsoft.com/en-us/library/ij204697.aspx</u>

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.

IJ	MaxACD S	yste	m Data Man	agemer	ıt 🚺	×
	Basic Config CWSDB Ser Backup Dire	ver	n 127.0.0.1\S C:\backupc		081	
	Backup Sch	nedule	es ———			1
	Monday		1:00:00 AM	÷	5	
	Tuesday		1:00:00 AM	÷	Backup	
	Wednesday		1:00:00 AM	÷		
	Thursday		1:00:00 AM	÷	Restore	
	Friday	~	1:00:00 AM	÷		
	Saturday	~	1:00:00 AM	÷	ОК	L
	Sunday		1:00:00 AM	÷	Cancel	
	Restore succe	ssfulļ	у.			1

- 3. 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.
- 4. 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.

🝶 backupcws Properties	×
General Sharing Security Previous Versions Customize	
Network File and Folder Sharing	
Shared	
Network Path: \\ACD2\backupcws	
Share	

5. 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"



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.
- 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]



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

MaxACD System Data Management
Basic Configuration
CWSDB Server 127.0.0.1\SQLCWSDB1
Restore Configuration
Restore from:
Day of week Tuesday
C Custom path
Restore to new installation
Unify CWSDB user
OK Cancel
Sunday 5:39:31 PM Cancel
Restore successfully.

4. 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.



<b>8</b>	Exchange UN	I Integration Ut	ility	_ 🗆 🗙
<u>H</u> elp				
Exchange UM Dial Plan Forest:				
	¥			
<u>SIP Dial Plans</u>	Contacts:			
FQDN	Number	SIP URI	Туре	AA Name
		oad Data		
After successfully running the F Exchange Server, the Skype for application makes it possible t and Auto-Attendant to work with started.	or Business Ser for UM features	ver 2015 can star like Play-on-phor	t routing callers ne, External Su	s to voice mail. This bscriber Access,

# **SQL** Authentication of External Logger Service

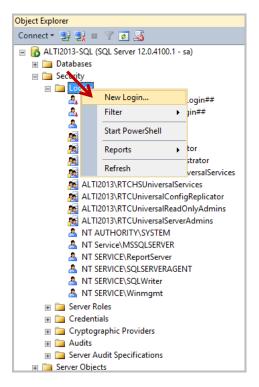
On the SQL server side, follow these steps.

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

8	Server Properties - ALTI2013-SQL		o x
Select a page	Sorpt  Kerver authentication  Windows Authentication mode  SQL Server and Windows Authentication mode  SQL Server and Windows Authentication mode  Login auditing  None  Ealied logins only  Successful logins only  Both failed and successful logins  Server proxy account  Enable server proxy account		
Connection	Proxy account:		
Server: ALTI2013-SQL Connection: sa <u>Wew connection properties</u>	Options		
Progress			
Ready			
	ОК	Ca	ncel



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.

8	Login - New			_ <b>D</b> X
Select a page	🔄 Script 🔻 🚺 Help			
Server Roles	Login game: 	tion		Sgarch
	O Mapped to certificate			~
Connection	Mapped to asymmetric key <u>Map</u> to Credential			✓ ✓ Add
Server: ALTI2013-SQL Connection: sa Jer View connection properties	Mapped Credentials	Credential	Provider	
Progress				Remo <u>v</u> e
Ready	Default <u>d</u> atabase: Default language:	iLcsCDR <default></default>		× ×



4. Map *LcsCDR* to the new user.

Select a page	(D	ER				
General	Script	🕶 🚺 Help				
Server Roles	Users mapped to this login:					
Securables	Мар	Database	User	Default Schema	^	
🚰 Status		cpsdyn				
		LcsCDR	ELSReader	dbo		
		LosLog			=	
		lis				
		master				
		model				
		msdb				
		QoEMetrics				
		ReportServer				
		Report Server Temp	DB		~	
	Databas	t account enabled for: e role membership for: o accessadmin				
Connection	db a					
Server:	_ db_b	ackupoperator				
Server: ALTI2013-SQL	db	backupoperator latareader				
Server: ALTI2013-SQL Connection:	db_b db_0 db_0	backupoperator latareader latawriter				
Server: ALTI2013-SQL Connection: sa	db_d db db db	backupoperator latareader				
Server: ALTI2013-SQL Connection:	4_40 0_40 0_40 0_40 0_40 0_40 0_40 0_40	backupoperator datareader datawriter ddladmin denydatareader denydatareader denydatawriter				
Server: ALT/2013-SQL Connection: sa Wew connection properties	1_40 0_40 0_40 0_40 0_40 0_40 0_40 0_40	backupoperator Jatareader Jatawriter Jdladmin Jernydatareader Jernydatawriter bernydatawriter				
Server: ALT2013-SQL Connection: sa View connection properties Progress	1_40 0_40 0_40 0_40 0_40 0_40 0_40 0_40	backupoperator latareader latawriter Idladmin denydatareader lenydatawriter wmer uecurityadmin				
Server: ALTI2013-SQL Connection: sa Wew connection properties		backupoperator latareader latawriter Idladmin denydatareader lenydatawriter wmer uecurityadmin				

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

U	Database Pro	perties - LcsCDR	t .			I X	
Select a page	🖾 Script 🔻 🚺 Help						
<ul> <li>Files</li> <li>Files</li> <li>Cptions</li> <li>Options</li> <li>Permissions</li> <li>Extended Properties</li> <li>Mirroring</li> <li>Transaction Log Shipping</li> </ul>	Server name: <u>View server permissions</u> Database <u>n</u> ame:	ALTI2013-SQL					
	Users or roles:					Search	
	Name       ALTI2013\CSAdministrator       ALTI2013\CSServerAdministrator       ALTI2013\CSSNewOnlyAdministrator       ALTI2013\RTCComponentUniversalServices       ELSReader				Type User User User User User		
Connection	Permissions for ELSReader:						
Server: ALTI2013-SQL	Explicit Effective	lor Gr	and and	With Grant	Deov		
Server:	Permission Gran Select dbo Show plan Subscribe query no	tor Gr	rant	With Grant	Deny	<u>^</u>	
Server: ALTI2013-SQL Connection: sa	Pemission Gran Select dbo Show plan	tor Gr		With Grant	Deny	^	

6. 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.



7. 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 <a href="https://mspartner.altigen.com">https://mspartner.altigen.com</a>. 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.