

MaxACD Release 7.0 Update 1 Exchange Integration Guide

June 4, 2018



Contents

About This Guide	3
Requirements	3
Integration Procedures	3
Option 1: Set the Exchange Administrator as the MaxACD Exchange Integration Service Administrator	3
MaxACD Configuration	3
Exchange Configuration	4
Option 2: Set a Different User as the MaxACD Exchange Integration Service Administrator	7
MaxACD Configuration	7
Exchange Configuration	8
Optional: Restrict the Scope of the Impersonation Service Account	10
AltiGen Technical Support	10

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. 2018. All rights reserved.



About This Guide

This guide describes how to configure MaxACD to integrate with Microsoft Exchange, to enable two-way synchronization between user MaxACD voicemail messages and user Outlook mailboxes.

Requirements

MaxACD supports the following versions of Exchange:

- Exchange Server 2013
- Exchange Online

Integration Procedures

You can specify the Exchange Administrator as the MaxACD Exchange Integration Service Administrator, or you can select another Exchange user as the MaxACD Exchange Integration Service Administrator. Whichever you chose, this user account will be used to log in to Exchange through Exchange Web Services (EWS).

Option 1: Set the Exchange Administrator as the MaxACD Exchange Integration Service Administrator

MaxACD Configuration

- 1. Within MaxACD, select **System > Server**.
- 2. In the Exchange Integration section, check the *Enable* option.
- 3. Complete the fields and click **OK**.
 - UPN Enter the Exchange Administrator account's UPN
 - Password Enter the password for the Exchange Administrator account
 - Email Enter the Exchange Administrator account's email address
 - UM Subscriber Access Enter or select the SIP address of the Exchange UM Subscriber Access account.

Note: You must configure and test this SIP URI in your SFB environment first.

Exchange Integ	ration					
Add Exchange Inte	gration					
	Enable	UPN	Password	Email	UM Subscriber Access	

4. If you have multiple Exchange servers for different domains, click the **Add Exchange Integration** button and add more entries as needed.

Exchange Configuration

During these procedures, you will configure Application Impersonation.

- 1. Log into the Exchange portal as the Exchange Administrator.
- 2. Click **permissions** in the left panel.

	Office 365	Admin
Exc	hange admin c	enter
dasht	board	admin
recipi	ents	
perm	issions	+ 🖉 i
comp	liance management	NAME
orgar	nization	Discovery
prote	ction	Help Des Helpdesk

3. In the middle panel, click the *admin roles* tab, select **Organization Management**, and then click the Pencil (edit) icon.



admin roles	user roles	Outlook Web App polic			
+ 🖍 🖮 🖻 🔎 😅					
NAME					
Compliance Manage	ment				
Discovery Managem	ent				
Help Desk					
HelpdeskAdmins_46	8077634				
Hygiene Managemei	nt	1			
MaxACDImpersonati	on				
Organization Manag	ement				
Recipient Manageme	ent				
Records Managemer	nt				
RIM-MailboxAdmins	cdeb67ae454d4	433682e2f48ed2fdc06b			
Security Administrate	or				
Security Reader					
TenantAdmins_80820	05019				
UM Management					
View-Only Organizat	ion Manageme	nt			

4. In the Role Group popup window, click the add button (the Plus sign) under *Roles*.

ঝ Role Group - Google Chrome	_	×
Organization Management		
*Name:		
Organization Management		- 1
Description:		- 1
Members of this management role group have permissions to manage Exchange objects and their properties in the Exchange organization. Members can also delegate role groups and management roles in the organization. This role group shouldn't be deleted.		
Write scope:		
Default 🔻		
Roles:		- 8
+ -		- 1
· · · · · · · · · · · · · · · · · · ·		

5. In the *Select a Role* popup window, select *ApplicationImpersonation* and click the **add** -> button. Then click **OK** to return to the previous window.



DISPLAY NAME	A
Address Lists	
ApplicationImpersonation	Applicationimpersonation
ArchiveApplication	This role enables applications to imperso
Audit Logs	tasks on behalf of the user.
Compliance Admin	
Data Loss Prevention	Default recipient scope
Distribution Groups	Organization
E-Mail Address Policies	
Federated Sharing	Default configuration scope
Information Rights Management	None
Journaling	-
1 selected of 53 total	
add -> ApplicationImpersonation[remove];	

6. In the Role Group window, you should now see *ApplicationImpersonation* in the Roles list. Click **Save** to save your changes.



🕞 Role Group - Google Chrome	—		×
Organization Management			
*Namo			
Organization Management			
Description:			
Members of this management role group have permissions to manage Exchange objects and their properties in the Exchange organization. Members can also delegate role groups and management roles in the organization. This role group shouldn't be deleted.			l
Write scope:			ł
Default 🔻			
Roles:			
+ -			۱I
NAME S	elect the admin oles that corres he Exchange fea	istrator pond to atures and	
ApplicationImpersonation	ervices that me	mbers of	
Audit Logs	his role group s	hould have	
Compliance Admin	ermissions to n	ianage.	
Data Loss Prevention	earn more		
Distribution Groups			
Members:			
+ -			

Option 2: Set a Different User as the MaxACD Exchange Integration Service Administrator

Perform these steps if you want to assign a user other than the Exchange Administrator as the MaxACD Exchange Integration Service Administrator.

MaxACD Configuration

Note the following requirements for this configuration:

- This user's email address must be the same as the user's UPN
- This UPN must be able to log into the Office 365 Outlook or Exchange Web Access (OWA) account
- Use this UPN and its password for Exchange Integration service login

To configure the MaxACD fields,

- 1. Within MaxACD, select **System > Server**.
- 2. In the Exchange Integration section, check the *Enable* option.



- 3. Complete the fields and click **OK**.
 - UPN Enter the Exchange Administrator account's UPN
 - Password Enter the password for the Exchange Administrator account
 - Email Enter the Exchange Administrator account's email address
 - UM Subscriber Access Enter or select the SIP address of the Exchange UM Subscriber Access account.

Note: You must configure and test this SIP URI in your SFB environment first.

Add Exchange Inte	gration					
	Enable	UPN	Password	Email	UM Subscriber Access	
Indate Cancel		kstrattenberg@altigu.net	23a5iids2	kstrattenberg@altigu.net	sip: sa@altiquinet	Select

4. If you have multiple Exchange servers for different domains, click the **Add Exchange Integration** button and add more entries as needed.

Exchange Configuration

During these procedures, you will configure Application Impersonation and will add the user whom you want to assign as the MaxACD Exchange Integration Service Administrator to the *Members* list.

- 1. Log into the Exchange portal as the Exchange Administrator.
- 2. Click **permissions** in the left panel.



3. In the middle panel, click the *admin role* tab. Click the Add (Plus sign) button to add a new role.



admin roles user roles	Outlook Web App poli
1	
▶ ★ / 前 師 2 ♂	
NAME	
Compliance Management	
Discovery Management	
Help Desk	

- 4. In the Role Group window, provide a meaningful name and enter a brief description.
- 5. In the same window, click the Add (Plus sign) button under *Roles* again, to add another new role. In the *Select a Role* popup window, select *ApplicationImpersonation* and click the **add** -> button. Click **OK** return to the previous window.

DISPLAY NAME	▲
Address Lists	Application
ApplicationImpersonation	Applicationimpersonation
ArchiveApplication	This role enables applications to imperson
Audit Logs	tasks on behalf of the user.
Compliance Admin	
Data Loss Prevention	Default recipient scope
Distribution Groups	Organization
E-Mail Address Policies	
Federated Sharing	Default configuration scope
Information Rights Management	None
Journaling	
1 selected of 53 total	
add -> ApplicationImpersonation[remove];	

- 6. In the Role Group window, click the Add (Plus sign) button below Members.
- 7. In the *Select Members* window, select the user whom you want to use as the MaxACD Exchange Integration Service Administrator and click the **add** -> button. Click **OK** to return to the previous window.



- 8. Make sure that *ApplicationImpersonation* appears in the *Roles* list. Confirm that the MaxACD Exchange Integration Administrator appears in the *Members* list.
- 9. Click Save.

Optional: Restrict the Scope of the Impersonation Service Account

The steps in this section are optional.

You can restrict the scope of the impersonation service account if desired.

If you are unfamiliar with this concept or process, we recommend that you review the following web page for details before you create a new scope:

https://technet.microsoft.com/en-us/library/dd351083(v=exchg.150).aspx

Procedures:

- 1. Create a group in AD, for example *ExSync*.
- 2. Add users that will be impersonated to this new group *ExSync*.
- 3. Open Exchange PowerShell and execute the command to create a new scope. In our example we use the name *AcdMailSyncScope*, with *alti2013.com* is a domain example.

```
New-ManagementScope -Name:AcdMailSyncScope -RecipientRestrictionFilter:
"MemberOfGroup -eq 'CN=ExSync,CN=Users,DC=alti2013,DC=com'"
```

4. In Exchange PowerShell, execute the command to assign the impersonation to an email account. In our example, we use the email account *john@alti2013.com*.

```
New-ManagementRoleAssignment -Name: AcdMailSyncAssign
-Role:ApplicationImpersonation -User:john@alti2013.com
-CustomRecipientWriteScope:AcdMailSyncScope
```

5. Use the email account from step 4 for MaxACD Exchange Voicemail synchronization.

AltiGen Technical Support

Authorized AltiGen Partners and distributors may contact AltiGen technical support by the following methods:

- You may request technical support on AltiGen's Partner web site, at https://mspartner.altigen.com. Open a case on this site; a Technical Support representative will respond within one business day.
- 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 Tech ID.



- Product serial number.
- MaxACD version number.
- Server model.
- Number and types of boards in the system.
- Indicate whether this is a virtual or standalone server installation.
 - If this is a virtual installation, be prepared to identify whether you're using VMware or Hyper-V, and which version of the virtual software is installed.
- The amount of memory and the number of CPUs that are reserved for MaxACD Server use. Be aware that memory and CPU cores should always be dedicated and reserved for MaxACD Server use exclusively.
- Indicate whether SSD drives are installed. If they are not, be prepared to describe what NAS devices are installed, and whether they are shared or dedicated to MaxACD Server.
- The telephone number where you can be reached.