ılıılı cısco

Configuring Microsoft Active Directory for Cisco WAAS Encrypted MAPI Acceleration



Abstract

The most current versions of Exchange-based email solutions from Microsoft (MAPI) contain data encryption at the Remote Procedure Call (RPC) level as a default configuration. Customers that wish to enable Cisco WAAS acceleration for these encrypted email services need to grant Cisco WAAS the permission to participate in this communication. This document will guide users through the configuration of Microsoft Active Directory (AD) to allow Cisco WAAS to accelerate encrypted RPC and MAPI traffic.

Figure 1. Cisco WAAS Encrypted Exchange Architecture



Considerations

Active Directory

This document assumes that the user has familiarity with Windows Active Directory, and has the appropriate Active Directory domain rights to make these changes.

User or Workstation Account

Granting Cisco WAAS permission to accelerate Exchange encrypted email can be done via a User account, or a Workstation (Computer) account.

Method	Benefits	Considerations
User Account	 One User account can be used for all Core WAAS devices. 	 User account should have a password that does not expire.
	 One or multiple User accounts can be used for multiple Exchange email domains. 	 If password is entered or changed incorrectly, the account could become locked out due to incorrect log
	• In test environments, the Administrator account can be used. Administrator already has the needed rights.	attempts.
	WAAS devices do not need to perform a Domain Join when only User Accounts are used.	
Workstation account	Each Core WAAS device will use its own Workstation account.	All Core WAAS devices must be joined to Active Directory.
	 Account is created and password is changed and maintained automatically by WAAS and Active Directory. 	 Only one Workstation account can be used per WAAS device.
	• User and Workstation accounts can be used at the same time for multiple Exchange email domains.	

Table 1. WAAS individual User account versus WAAS Workstation accounts

It is highly recommended to grant the required WAAS permissions to an Active Directory Group, and then add Workstation or User accounts as required above to that group. This guide will follow this Group-based process.

WAAS Configuration

Once the steps outlined in this document are completed, the next step is to configure WAAS to accelerate encrypted Exchange email (RPC and MAPI). Directions and steps for this configuration are located in the <u>Cisco</u> <u>WAAS 5.0.1 Configuration Guide</u>, located on Cisco.com. These steps are beyond the scope of this document

Configuration Steps

To grant Cisco WAAS permission to accelerate Exchange encrypted email sessions, do the following:

Note: This group is for accounts that WAAS will use to optimize Exchange traffic. Normal users and computers should not be added to this group.

- Step 1. Using an account with "Domain Administrator" privileges, launch the Active Directory Users and Computers application.
- Step 2. A new group is needed. Right-click the Organizational Unit (OU) where you wish to place this group, and

choose new > Group.				
Active Directory Users and Computers				_ 🗆 ×
File Action View Help				
♦ ♦ 2 🖬 ¾ 🗎 🗙 🗒 4 :	🛓 🛛 🖬 🗏 🐮 🐨 🏹 🗕	38.		
Active Directory Users and Computers [ADC-1	MAIL.adb Name	Туре	Description	
🛨 🧮 Saved Queries	& Administrator	User	Built-in account for admini	
🖃 🏭 adbu-exch.local	Allowed RODC Passwor	rd Security Group	. Members in this group can	
🗉 🚞 Builtin	& Cert Publishers	Security Group	. Members of this group are	
Computers	& Denied RODC Password	d R Security Group	. Members in this group can	
🛨 💼 Domain Controllers	📕 DiscoverySearchMailbo	x { User		
ForeignSecurityPrincipals	& DnsAdmins	Security Group	. DNS Administrators Group	
Managed Service Accounts	& DnsUpdateProxy	Security Group	DNS clients who are permi	
E Microsoft Exchange Security Groups	& Domain Admins	Security Group	. Designated administrators	
Delegate Control	& Domain Computers	Security Group	. All workstations and serve	
Find	& Domain Controllers	Security Group	. All domain controllers in th	
	1 da	Security Group	. All domain quests	
	puter	Security Group	. All domain users	
All Tasks Cont	ns	Security Group	. Designated administrators	
View Grou	-only D	o Security Group	. Members of this group are	
	OrgPerson 4c1f4d	18b User	5 1	
	kchDynamicDistributionList	wn Security Group	. Members in this group can	
	naging-PSPs	User	Built-in account for guest	
Properties	Q Queue Alias	Security Group	-	
Print	hin Con			
Help User		Security Group		
Shar	ed Folder 1f05a9		· · · · , · · · · · · · · · · · · · · · · · · ·	
	SystemMailbox{e0dc1d	29 User		
	L Test1 Tester	User		
	Test2 Tester	User		
	Tant? Tantor	User		•
Create a new object				

X

Step 3. Name the new group, and ensure the group is a Universal, Security Group.

New Object - Group	×
Create in: adbu-exch.local/Users	
Group name:	
WAAS-AD-Readers	
Group name (pre-Windows 2000):	
WAAS-AD-Readers	
Group scope C Domain local C Global C Universal Group type Security C Distribution	
ОК Са	ncel

Step 4. After the group is created, return to the **Active Directory Users and Computers** window. Select **View** >



Step 5. Right-click the root of the domain, and choose Properties.



Step 6. Click the Security tab, and then press the Add button under Group or User Names.

General Managed By Object Security Attrib	ute Editor		
Group or user names:			
& Everyone			
& SELF			
Authenticated Users			
& NETWORK SERVICE			
Representation Management (ADBU-EXCH\Or	ganization N	lanage	•
Ac	на П	Remove	. 1
		Homove	<u> </u>
Permissions for Everyone	Allow	Deny	
Full control			4
Read			
Write			
Create all child objects	님		
Delete all child objects	<u> </u>		•
For special permissions or advanced settings, clic	k j	Advanced	1
Advanced.			
Leam about access control and permissions			
OK Cancel	Apply	Ηe	ip.

Step 7. Enter the name of the group that was entered in **Step 3**, and press **OK**.

Select Users, Computers, Service Accounts, or Groups	? X
Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
adbu-exch.local	Locations
Enter the object names to select (<u>examples</u>):	
WAAS-AD-Readers	Check Names
Advanced OK	Cancel
	/

Step 8. The group entered in **Step 3** should now show in the **Group or User Names** list. Click on the group to select it. Then, scroll down in the **Permissions for *Group Name*** pane, until the permissions **Replicating Directory Changes** and **Replicating Directory Changes All** are visible. Check **Allow** to allow both of these permissions, and press **OK**.

dbu-exch.local Properties
General Managed By Object Security Attribute Editor
Group or user names:
Administrators (ADBU-EXCH\Administrators) Access (ADBU-EXCH\Pre-Wind Access (ADBU-EXCH\Pre-Wind Contract Furst Builders (ADBU-EXCH\Incoming Forest Tr Contract Furst Builders (ADBU-EXCH\WAAS-AD-Readers)
Add Remove Permissions for WAAS-AD-Readers Allow Deny
Read only replication secret synchronization
Reanimate tombstones Replicating Directory Changes Replicating Directory Changes All
Replicating Directory Changes In Filtered Set Image: Change of the set of t
OK Cancel Apply Help

Step 9. User or Workstation (Computer) accounts now need to be added to this group for WAAS to use to optimize Exchange encrypted email. To add an account, right click on the account you wish to add, and select the **Member Of** tab. Click the add button, and pick the group used above in **Step 3**. Press **OK**.

Step 10. After adding the User or Workstation (Computer) accounts to the group, the Active Directory configuration is now complete. All remaining configuration for Encrypted Exchange acceleration is performed on the WAAS Central Manager and/or devices themselves.

For More Information

For Cisco WAAS Exchange encrypted email configuration steps, see the <u>Cisco WAAS 5.0.1 Configuration Guide</u> on Cisco.com.

For more information Cisco WAAS, see http://www.cisco.com/go/waas



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA