

Configure Mailbox Auto Remediation for AsyncOS 13.0+

Contents

Issue

This document describes how to configure Mailbox Auto Remediation (MAR) features in AsyncOS 13.0 and later for Exchange Online, Exchange on-premises, hybrid, and multi-tenant deployments.

MAR was introduced in AsyncOS 10.0 and only supported Microsoft Office 365 Online.

AsyncOS 13.0 and newer capabilities include:

- Microsoft Exchange Online – mailbox hosted on Microsoft Office 365
- Microsoft Exchange on-premises – a local Microsoft Exchange server
- Hybrid and multi-tenant configurations – a combination of mailboxes configured across Microsoft Exchange Online and Microsoft Exchange on-premises deployments

Initial setup steps are available in the original MAR setup guide for Microsoft Office 365, along with an addendum that describes changes in AsyncOS 13.0 and newer.

The original article remains valid and covers an explanation of the feature, as well as steps to generate certificates for the Microsoft Office 365 Azure implementation, ESA settings, and general troubleshooting.

[How to Configure Azure AD and Office 365 Mailbox Settings for ESA](#)

New changes to Azure API permissions for 13.0

The current [User Guide](#) provides more detailed information about the Auto Remediation feature.

See the chapter titled, Automatically Remediating Messages in Mailboxes.

Environment

- AsyncOS 13.0 or newer for ESA
- License keys for File Reputation and File Analysis
- Microsoft Office 365 or Microsoft Exchange on-premises deployment

Resolution

1. For Exchange Online account profiles, use these Azure configuration articles first to create the Azure application, certificates, and API permissions required by AsyncOS 13.0 and newer:
 - [How to Configure Azure AD and Office 365 Mailbox Settings for ESA](#)
2. Create the required account profiles in the ESA.
3. Configure domain mapping for each profile.
4. If the deployment is hybrid or multi-tenant, configure chained profiles.
5. Test each account profile.

ESA 13.0 and newer support multiple account profiles created with Exchange Online, Exchange on-premises, or both:

- Organizations with complex setups can use multiple account profiles when domains are segregated and reside on different deployments.
- Organizations that absorb a new acquisition can include the acquired domain in the MAR feature.
 - Creating multiple account profiles provides more flexibility than previous ESA capabilities.

Configure Exchange Online Microsoft Office 365 Profile

Instructions to create an account profile for Microsoft Office 365 in Azure are included in the referenced articles in the Issue section.

Select **Office 365 Hybrid Graph API** to configure a mailbox deployed on Exchange Online and enter these details:

- Client ID and Tenant ID for the application registered in the Azure Management Portal.
- The certificate thumbprint (the value of \$base64Thumbprint).
- Click **Choose File** and select the **.pem file** to upload the private key for the certificate.

Create Account Profile

Account Details	
Profile Name :	azure-rcdntac
Description :	MAR-Charella
Profile Type :	Office 365 / Hybrid (Graph API)
Client ID :	7355f8d1-1fc-accfdde889b5
Tenant ID :	045542f0-1d7d251805f
Thumbprint :	Zy028wn-1IG+1Wc4azaA
Certificate Private Key :	Browse... charella_mar.pem .PEM format is required.

Cancel Test Connection Submit

Sample Profile connecting to O365

Exchange Online account profile example

Configure Exchange On-premises Profile

Creating an account profile for an Exchange on-premises instance requires a user account with the ApplicationImpersonation role and a valid host value.

This method requires the designated Exchange on-premises service account with the ApplicationImpersonation role.

1. In a browser, open the **Exchange Admin Center** URL for your Exchange on-premises environment.
For example: <https://mail.example.com/ecp/>.
2. After you log in, navigate to **Permissions > Admin Roles**.
3. Click **Add** to create a new role group.
4. If a role group already exists, add the **designated user account** as a member.
5. Enter the **role group name** and **description**.
6. Under **Roles**, click **Add**.
7. Select **ApplicationImpersonation**, and then click **Add**.
8. Click **OK**.
9. Return to the newly created role group, click **Members: +**, locate the designated user account, and add it for use on the ESA.
10. Commit all **changes** in Exchange. For more details, refer to the Microsoft Support documentation.
11. In the ESA web interface, navigate to **System Administration > Account Settings**.
12. Create the **account profile**, and then enter the **profile name** and **description**.
13. From the **Profile Type** drop-down list, select **Exchange On-Premise**.
14. Enter the **username**, **password**, and **Host** value.
15. Enter a valid **Exchange server host name** for the **Host** value.
16. Click **Submit**, then **Commit Changes**.

Create Account Profile

Error — Errors have occurred. Please see below for details.

Account Details

Profile Name :

exchange-mar

Description :

Exchange on premise profile

Profile Type :

Exchange On Premise

Username :

MARimpersonator

Password :

...

Host :

mytestexchangeserver.com

Parameters for the HOST: field

The address must be a hostname or an IP address. The IP address must be 4 numbers separated by a period. Each number must be a value from 0 to 255. (Example: 192.168.1.1) A hostname is a string that must match the following rules:

- A label is a set of characters, numbers and dashes.
- The first and last character of a label must be a letter or a number.
- The hostname must have at least 2 labels separated by a period.
- The last label cannot be all numbers.

Cancel

Test Connection

Submit

Sample Exchange On-Premise Profile

Exchange on-premises account profile example

Account Profiles ?			
Create Account Profile			
Account Profile Name	Profile Type	Description	Delete
azure-rtptac	Office 365 / Hybrid (Graph API)	rtp domains	
exchange-mar-2	Exchange On Premise	secondary on premise profile	
exchange-mar	Exchange On Premise	Exchange On-Premise	
azure-rcdntac	Office 365 / Hybrid (Graph API)	MAR-Charella	

Samples of MAR Account Profiles

Samples of MAR account profiles

Configure Domain Mapping

Domain mapping is the assignment of one or more domains to an account profile.

Every implementation requires at least one domain mapping:

1. In the ESA web interface, navigate to **System Administration > Account Settings > Create Domain Mapping**.
2. Enter the **domain names** separated by commas. Acceptable domain formats are shown in the image.
3. If there is only one account profile in the configuration, enter **ALL** in the **Domain Name** field.
4. A domain can only be used once.

Edit Domain Mapping

Domain Mapping	
Enter Domain Name(s): ?	rtptacsecondary.com
Mapped Profile:	azure_exch mar_chain_1 all-domains exchange-mar-2
Cancel Submit	

Domain Mapping Sample

Domain mapping example

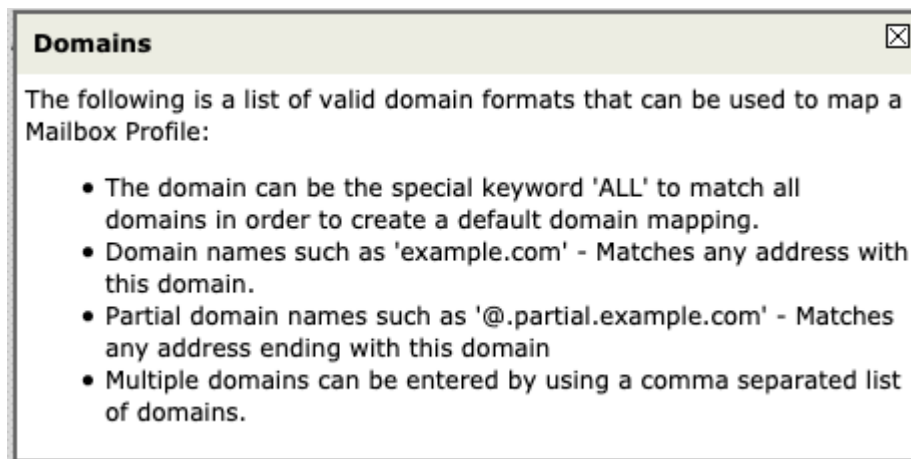


Image 1. Acceptable Domain Formats

Acceptable domain formats

Domain Mapping ?		
Create Domain Mapping		
Mailbox Profile/Chained Profile	Recipient Domain(s)	Delete
azure-rtptac	rtprocks.com	
exchange-mar-2	rtptacsecondary.com	
exchange-mar	charella1212.com,charees6868.com,@.home....	
azure-rcdntac	charella111.com	

Domain Mapping Sample

Domain mapping example

Configure Chained Profiles

Configure chained profiles only when you remediate messages in mailboxes that are part of a hybrid or multi-tenant deployment.

Add the profiles in priority order, with the most heavily used domain profile first.

1. In the ESA web interface, navigate to **System Administration > Account Settings > Create Chained Profiles**.
2. Enter the **Profile Name** and **Description**.
3. Select a **domain** from the **MAR Profile** drop-down list.
4. Click **Add Account Profile** to add another domain profile until all required profiles are added.
5. Click **Submit**, then **Commit Changes**.

Create Chained Profile

Chained Profile

Profile Name :

azure_exch1_exch2

Description :

List of account profiles

MAR Profile	Server Type	Description	Delete
azure-rtptac	Office 365 / Hybrid (Graph API)	rtp domains	
exchange-mar-2	Exchange On Premise	secondary on premise profile	
exchange-mar	Exchange On Premise	Exchange On-Premise	
✓ -- Select Profile --	N/A	N/A	

azure-rtptac

exchange-mar-2

exchange-mar

azure-rcdntac

Add Account Profile...

Submit

Chain Profile Creation.

Chained profile creation

Test each Account Profile

Confirm each account profile by clicking the **Test Connection** button in the individual profile.

1. In the ESA web interface, navigate to **System Administration > Account Settings**, then choose one of the account profiles.
2. Click the **Test Connection** button in the lower-left corner.
3. Enter the **email address** in the **Email Address** field, then click **Test Connection**.

Connection Check

Connection Parameters

Email Address:

Test Connection

Connection Status

Connected to Exchange.
Connection Successful.
The appliance is able to read the user's mailbox.

Done

Test each Profile to verify successful connectivity

Test connection for an account profile

Troubleshooting

Logs contain:

- mail_logs: Final remediation action and summary
- mar_logs: The sequence in which remediation was performed
- Test Connection option in the UI: used to verify connectivity and permissions

A lot of information can be determined by the email test from Account Settings.

Troubleshooting using Test Connection

The SMTP address has no mailbox associated with it.

The user mailbox that is being used does not exist.

Access is denied. Check credentials and try again.

The application configured in Microsoft Azure does not have the required API permissions to access the Microsoft Office 365 mailbox.

Application with identifier <client_id> was not found in the directory <tenant_id>.

Client ID on the Account Profile Settings page is invalid.

No service namespace named <tenant_id> was found in the data store.

Tenant ID on the Account Profile Settings page is invalid.

Error validating credentials. Credential validation failed.

- Certificate Thumbprint on the Account Profile page is invalid.
- The profile type used to access the mailbox can be incorrect. For example, an on-premises mailbox is accessed by using a Microsoft Office 365 profile.
- The required permissions to access the mailbox can be missing.

Invalid username or password entered for the exchange server.

Impersonator Account Username and Password entered in the profile are not valid.

The account does not have permission to impersonate the requested user.

Impersonator Role privileges are not assigned to the user account configured in the profile.

Please check host <hostname> is a valid exchange server address.

The On-prem Exchange server Hostname entered in the profile is invalid.

The mailbox cannot be accessed using this profile or the required permissions can be missing.

A valid mailbox is being accessed by using the wrong type of profile. For example, an on-premises mailbox is accessed by using a Microsoft Office 365 profile.

Sample of successful remediation for a single profile:

<#root>

Fri Aug 30 11:57:30 2019 Info: Process ready for Mailbox Remediation

Fri Aug 30 12:29:54 2019 Info: MID: 782107 Attempting to remediate using `o365-profile-1` profile for re

Fri Aug 30 12:29:54 2019 Info: MID: 782107 Trying to perform the forward and delete action on Office 365 mailbox 1e6f324982d4eb71ad967e79261a6435aef928b57bc523dbb3e7de4ed65941ab recipient's (user@example.com) mailbox.
Fri Aug 30 12:29:58 2019 Info: MID: 782107 Message forwarded successfully to admin@example.com.
Fri Aug 30 12:29:58 2019 Info: MID: 782107 Message deleted successfully from user@example.com mailbox.
Fri Aug 30 12:29:58 2019 Info: MID: 782107 Remediation succeeded with 'o365-profile-1' profile for recipient.

Sample of successful remediation for a chained profile:

<#root>

Mon Oct 14 15:01:01 2019 Info: MID: 24 Attempting to remediate using 'o365-profile-1' profile for recipient.

Mon Oct 14 15:01:01 2019 Info: MID: 24 Trying to perform the delete action on Office 365 or Hybrid exchange mailbox recipient's (user@example.com) mailbox.
Mon Oct 14 15:01:09 2019 Info: MID: 24 Unable to read message(s) from the recipient's (user@example.com) mailbox. permissions can be missing

Mon Oct 14 15:01:09 2019 Info: MID: 24 Attempting to remediate using 'exchange-profile-1' profile for recipient.

Mon Oct 14 15:01:09 2019 Info: MID: 24 Trying to perform the delete action on Exchange on-premises for mailbox recipient's (user@example.com) mailbox.
Mon Oct 14 15:01:16 2019 Info: MID: 24 Message deleted successfully from user@example.com mailbox.
Mon Oct 14 15:01:16 2019 Info: MID: 24 Remediation succeeded with 'exchange-profile-1' profile for recipient.

Cause

AsyncOS 13.0 and newer introduce expanded MAR deployment support. This expanded support requires additional account profile, domain mapping, and chained profile configuration depending on whether the Exchange deployment is Exchange Online, Exchange on-premises, hybrid, or multi-tenant.

Related Content

- [How-to configure Azure AD and Office 365 mailbox settings for ESA](#)
- [Cisco Technical Support and Documentation](#)
- [Cisco Email Security Appliance - Product Support](#)
- [Cisco Email Security Appliance - Release Notes](#)
- [Cisco Email Security Appliance - End-User Guides](#)
- [Cisco Content Security Management Appliance - Product Support](#)
- [Cisco Content Security Management Appliance - Release Notes](#)
- [Cisco Content Security Management Appliance - End-User Guides](#)