Remediating Messages in Mailboxes

This chapter contains the following sections:

Overview

The appliance provides the capability to remediate the malicious messages that are already delivered to the user mailbox. You can configure your appliance to remediate the messages in the following ways:

- automatically remediate the messages when the AMP sends the retrospective alert to your appliance
- manually search and remediate the messages using the Message Tracking filter

A file can turn malicious anytime, even after it has reached user's mailbox. AMP can identify this as new information emerges and push retrospective alerts to your appliance . You can configure your appliance to perform auto-remedial actions on the messages in user mailbox when the threat verdict changes. For example, you can configure your appliance to delete the message from the recipient's mailbox when the verdict of the attachment changes from clean to malicious.

You can also use the Message Tracking page to search and remediate the messages that are delivered to the user mailbox. The Message Tracking page is a unified place to search for all messages delivered to the mailboxes. From the search result, you can choose the messages you want to remediate and apply the action you want to perform on the messages.

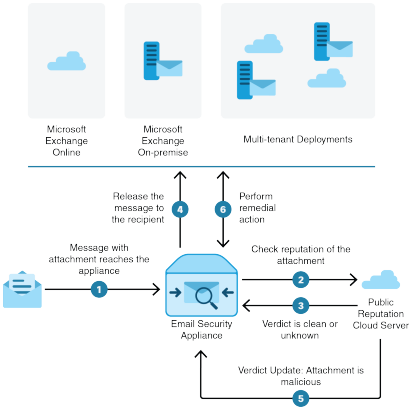
The appliance can perform remedial actions(manually or automatically) on the messages in the following mailbox deployments:

- Microsoft Exchange online – mailbox hosted on Microsoft Office 365
- Microsoft Exchange on-premise – a local Microsoft Exchange server

- Hybrid/Multiple tenant configuration – a combination of mailboxes configured across Microsoft Exchange online and Microsoft Exchange on-premise deployments

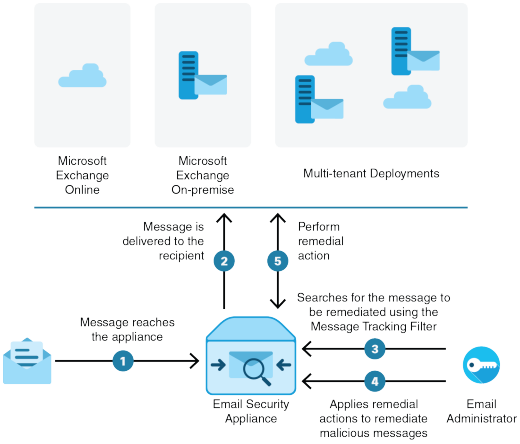
Workflow

Mailbox Auto Remediation Workflow



1. Message with an attachment reaches the appliance .
2. The appliance queries the public file reputation cloud server to evaluate the reputation of the attachment.
3. The public file reputation cloud server sends the verdict to the appliance . The verdict is clean or unknown.
4. The appliance releases the message to the recipient.
5. After a certain period, the appliance receives a verdict update from the public file reputation cloud server. The new verdict is malicious.
6. The appliance performs the configured remedial action on the message (with malicious attachment) residing in the recipient's mailbox.

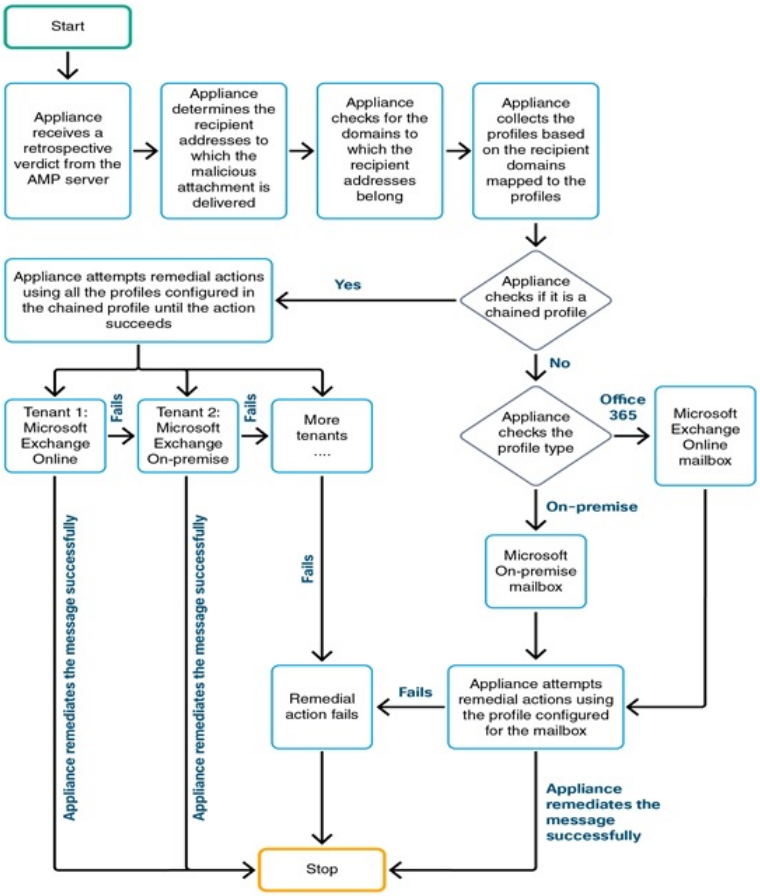
Search and Remediate Messages Workflow



1. Message reaches the appliance .
2. Message is delivered to the recipient.
3. The administrator searches for the message delivered to the recipient using the Message Tracking filter.

4. The user selects the message to be remediated from the recipient's mailbox and applies the remedial action on the message.
5. The appliance performs the configured remedial action on the message residing in the recipient's mailbox.

How the Appliance Performs Auto-Remedial Actions



1. [Only to search and remediate messages] The user searches for the messages delivered to the user mailbox using the Message Tracking filter.
2. [Only to search and remediate messages] The user selects the messages to be remediated and applies remedial action on the messages.
3. [Only to automatically remediate messages] When the appliance receives a retrospective verdict from the public file reputation cloud server, the appliance initiates the mailbox remediation process.
4. [Only to automatically remediate messages] The appliance determines the email addresses to which the malicious message was delivered.

5. The appliance identifies the recipient domains to which the email addresses belong.
6. Based on the recipient domains, the appliance collects the account profile that is mapped to the domains.

   An account profile defines the mailbox settings that are used by the appliance to connect to the mailbox and perform the auto-remedial actions. You must create an account profile and map it to the recipient domains to successfully remediate the message from the mailbox.
7. The appliance checks for the profile mapped to the domains:
   - [Only for hybrid or multi-tenant deployment] If it is a chained profile, the appliance attempts to perform remedial actions using all the account profiles in the chained profile.

     A chained profile is a combination of multiple account profiles. In case of a hybrid or multi-tenant deployment, where there are mailboxes present across multiple deployments, you must create a chained profile to combine all the profiles defined for mailboxes in the deployment. The appliance attempts to perform remedial actions based on the order in which the account profiles are added in the chained profile.
   - If it is not a chained profile, the appliance checks the profile type to know if it is an Microsoft Exchange online profile or an Microsoft Exchange on-premise profile.
8. The appliance performs remedial actions using the identified profile and remediates the message.

Note Mailbox remediation may fail for various reasons. For more information, see Troubleshooting Mailbox Remediation, on page 20.

Contents

Performing Remedial Actions on Messages in Mailboxes

You can perform remedial actions on messages in the following mailbox deployments:

- Microsoft Exchange Online (Office 365) - Performing Remedial Actions on Messages in Microsoft Exchange Online Mailboxes, on page 5
- Microsoft Exchange On-Premise - Performing Remedial Actions on Messages in Microsoft Exchange On-Premise Mailboxes , on page 6
- Hybrid/Multi-tenant Deployment - Performing Remedial Actions on Messages in Mailboxes on Hybrid Deployment, on page 8

Performing Remedial Actions on Messages in Microsoft Exchange Online Mailboxes

You can configure your appliance to perform remediation of messages from user mailbox.

If your organization is using Microsoft Exchange online to manage mailboxes, you can configure your appliance to perform auto-remedial actions on the messages in user mailbox when the threat verdict changes. For example, you can configure your appliance to delete the message from the recipient's mailbox when the verdict of the attachment changes from clean to malicious.

You can perform remedial actions manually on messages that are already delivered to the user mailbox. For example, an administrator monitoring the incoming messages can perform remedial actions on messages in the user mailbox using the Message Tracking filter.

Contents

How to Configure Remedial Action on Messages in Microsoft Exchange Online Mailboxes

	Do This	More Info
Step 1	Review the prerequisites.	Prerequisites for Remediating Messages in Microsoft Exchange Online Mailboxes, on page 10
Step 2	Register appliance as an application on Azure AD (Azure Management Portal).	Registering Your Appliance as an Application on Azure AD, on page 12
Step 3	Enable the account settings on your appliance .	Enable mailbox remediation on your appliance . Enabling Account Settings on Cisco Email Security Appliance , on page 14

	Do This	More Info

Step 4	Create an account profile of type Office 365/Hybrid (Graph API) on your appliance .	Create an Office 365 profile for the user mailbox and define the mailbox settings on the appliance .
		Before you Begin, make sure that you have:
		• Acquired the private key of the certificate in .pem format. See Certificate for Secure Communication.
		• The values of the following parameters:
		  • Client ID and Tenant ID of the application that you registered on the Azure Management Portal.
		  • See Step 9 of Registering Your Appliance as an Application on Azure AD.
		  • Certificate thumbprint ($base64Thumbprint). See Step 8 of Registering Your Appliance as an Application on Azure AD.
		See Creating an Account Profile , on page 15.

Step 5	Add the recipient domain and map the domain to the Office 365 profile.	Add the domain that the recipient mailbox belongs and map the domain to the Office 365 account profile. See Mapping Domains to the Account Profile , on page 17.
Step 6	[Only to automatically remediate messages] Configure your appliance to perform remedial actions on messages delivered to end users when the threat verdict changes to malicious.	Configure Auto-Remedial Actions on Messages in the Mailboxes, on page 17
Step 7	[Only to search and remediate messages] Configure your appliance to perform remedial actions manually on messages delivered to end users.	Search and Remediate Messages in the Mailboxes, on page 18

Performing Remedial Actions on Messages in Microsoft Exchange On-Premise Mailboxes

You can configure the appliance to remediate messages from a mailbox on an Exchange on-premise server. The messages can be remediated automatically by the appliance or manually by the user using the Message Tracking filter.

The appliance uses a user account with impersonator privileges to access the Exchange on-premise mailbox and perform remedial actions on the message. You must create this user account with impersonator privileges on the mail exchange server to which the appliance has to connect and remediate the message.

Note Cisco has validated Mailbox Auto Remediation only on Microsoft Exchange 2013, 2016, and 2019.

Contents

How to Configure Remedial Actions on Messages in Microsoft Exchange On-Premise Mailboxes

	Do This	More Info
Step 1	Review the prerequisites.	Prerequisites for Remediating Messages in an On-Premise Account, on page 11
Step 2	Enable the account settings on your appliance .	Enable mailbox remediation on your appliance . Enabling Account Settings on Cisco Email Security Appliance , on page 14
Step 3	Create an account profile of type On-Premise on your appliance .	Create an On-Premise profile for the user mailbox and define the mailbox settings on your appliance . Before you begin, make sure that you have: • The impersonator user account details • The host name of the local mail exchange server Creating an Account Profile , on page 15.
Step 4	Add the recipient domain and map the domain to the On-premise account profile.	Add the domain that the recipient mailbox belongs and map the domain to the On-premise account profile. See Mapping Domains to the Account Profile , on page 17.
Step 5	[Only to automatically remediate messages] Configure your appliance to perform remedial actions on messages delivered to end users when the threat verdict changes to malicious.	Configure Auto-Remedial Actions on Messages in the Mailboxes, on page 17
Step 6	[Only to search and remediate messages] Configure remedial actions on messages in the on premise mailbox.	Search and Remediate Messages in the Mailboxes, on page 18

Performing Remedial Actions on Messages in Mailboxes on Hybrid Deployment

You can configure a single appliance to remediate messages from a hybrid exchange deployment or multiple exchange tenants. For example, if your organization is in a process of moving the mailbox from Microsoft Exchange on-premise to Microsoft Exchange online, there will be mailboxes deployed on Microsoft Exchange online and Microsoft Exchange on-premise until the migration is complete. The messages can be remediated automatically by the appliance or manually by the user using the Message Tracking filter.

To automatically remediate messages from multiple mailboxes configured across different deployments, create a chained profile. A chained profile combines all the account profiles of a hybrid or multi-tenant deployment. The order in which the profiles are added to the chained profile defines the priority in which the appliance checks the profile to remediate messages.

When the appliance receives a retrospective verdict from the AMP server, the appliance attempts to perform the remediation action using each profile present in the chained profile in the order of priority defined in the chained profile.

To manually search and remediate the messages that are delivered to the user mailbox, use the Message Tracking filter. You can use this filter to select the messages you want to remediate, configure the remedial action, and apply the remedial action on the messages.

Contents

How to Perform Remedial Actions on Messages in Mailboxes on Hybrid Deployment

	Do This	More Info
Step 1	Review the prerequisites.	Ensure that all the prerequisites for performing auto-remedial actions on Microsoft Exchange online and Microsoft Exchange on-premise mailboxes are met for a hybrid or multi-tenant deployment. See Prerequisites, on page 10.
Step 2	Register appliance as an application on Azure AD (Azure Management Portal).	Registering Your Appliance as an Application on Azure AD, on page 12
Step 3	Enable the account settings on your appliance .	Enable mailbox remediation on your appliance . See Enabling Account Settings on Cisco Email Security Appliance , on page 14.

	Do This	More Info

Step 4	Create account profiles for all the mailboxes in the hybrid/multi-tenant deployment.	Create account profiles for the user mailboxes and define mailbox settings on the appliance .
		Before you Begin, make sure that you have:
		• Acquired the private key of the certificate in .pem format. See Certificate for Secure Communication.
		• The values of the following parameters:
		  • Client ID and Tenant ID of the application that you registered on the Azure Management Portal.
		  • See Step 9 of Registering Your Appliance as an Application on Azure AD.
		  • Certificate thumbprint ($base64Thumbprint). See Step 8 of Registering Your Appliance as an Application on Azure AD.
		• The impersonator user account details
		• The host name of the local mail exchange server
		See Creating an Account Profile , on page 15.

Step 5	Create a chained profile.	Create a chained profile and add all the profiles of a hybrid/multi- tenant deployment. See Creating a Chained Profile , on page 16.
Step 6	Add the recipients' domains and map them to the chained profile.	Add the domains that the recipients' mailboxes belong and map the domains to the chained profile. See Mapping Domains to the Account Profile , on page 17.
Step 7	[Only to automatically remediate messages] Configure your appliance to perform remedial actions on messages delivered to end users when the threat verdict changes to malicious.	Configure Auto-Remedial Actions on Messages in the Mailboxes, on page 17
Step 8	[Only to search and remediate messages] Apply the remedial actions on the messages.	Search and Remediate Messages in the Mailboxes, on page 18

Configuring Mailbox Remediation on Cisco Email Security Appliance

Prerequisites

Prerequisites for Remediating Messages in Microsoft Exchange Online Mailboxes

Feature Keys for File Reputation Service and the File Analysis Service

Note The File Reputation Service and the File Analysis Service feature keys are not required for performing Search and Remediate actions on messages in the user mailbox.

To configure remedial actions for Mailbox Auto Remediation on messages in the user mailbox, make sure that you have:

- Added the feature keys for the file reputation service and the file analysis service to you appliance .
- Enabled File Reputation and Analysis feature on your appliance . See File Reputation Filtering and File Analysis.

Office 365 Accounts

Make sure that you have the following accounts that are required to register your appliance with Azure AD:

- An Office 365 business account
- An Azure AD subscription associated with your Office 365 business account

For more information, contact your Office 365 administrator.

Certificate for Secure Communication

To secure the communication between Office 365 services and your appliance , you must set up a certificate in one of the following ways: create a self-signed certificate or obtain a certificate from a trusted CA.

You must have:

- A public key in .crt or .p12 format. Make sure that the emailAddress is set to the email address of the Office 365 administrator (<admin_username>@<domain>.com).
- An associated private key in .pem format, with keysize at least 2048 bit.

For more information, see https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/211404-How-to-configure-Azure-AD-and-Office-365.html.

Note Private keys with passphrase are not supported in this release.

To secure the communication between Office 365 services and your email gateway, you must perform any one of the following tasks:

- Generate a Client Secret of the application that you created on the Azure Management Portal.
- Set up a certificate in one of the following ways: create a self-signed certificate or obtain a certificate from a trusted CA.

  You must have:

  - A public key in .crt or .p12 format. Make sure that the emailAddress is set to the email address of the Office 365 administrator (<admin_username>@<domain>.com)
  - An associated private key in .pem format, with keysize at least 2048 bit.

Prerequisites for Remediating Messages in an On-Premise Account

- [Only for Mailbox Auto Remediation] - Feature Keys for File Reputation Service and the File Analysis Service, on page 10
- (Optional) Import Microsoft Exchange Web Service (EWS) Certificate, on page 12
- Add a User to the Impersonator Role, on page 12

Feature Keys for File Reputation Service and the File Analysis Service

Note The File Reputation Service and the File Analysis Service feature keys are not required for performing Search and Remediate actions on messages in the user mailbox.

To configure remedial actions for Mailbox Auto Remediation on messages in the user mailbox, make sure that you have:

- Added the feature keys for the file reputation service and the file analysis service to you appliance .
- Enabled File Reputation and Analysis feature on your appliance . See File Reputation Filtering and File Analysis.

(Optional) Import Microsoft Exchange Web Service (EWS) Certificate

If you are using a self-signed certificate on an Microsoft Exchange on-premise server for the EWS service, you must import the certificate from the Microsoft Exchange on-premise server into the appliance . To import a certificate, see Importing a Certificate.

Add a User to the Impersonator Role

The appliance uses a user account that has impersonator privileges to access the Microsoft Exchange on-premise mailbox. The mail exchange administrator must create a user account with impersonator privileges on the local exchange server. The appliance used this user account to remediate messages from the mailbox.

Procedure

Step 1 Create a user account for which impersonator privileges must be assigned. This user account is used by the appliance to access and operate the mailbox to remediate the messages.

Step 2 Log in to the Microsoft Exchange Control Panel interface using administrator credentials.

Step 3 Navigate to **Permissions -> Admin Roles**.

Step 4 Create a role and assign the 'ApplicationImpersonation' privileges for the role.

Step 5 Add the user account for which the impersonator privileges must be assigned as a member of this new role.

Registering Your Appliance as an Application on Azure AD

Office 365 services use Azure Active Directory (Azure AD) to provide secure access to users' mailboxes. For your appliance to access the Office 365 mailboxes, you must register your appliance with Azure AD. The following are the high level steps you need to perform to register your appliance with Azure AD. For detailed instructions, see Microsoft documentation (https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app).

Before You Begin

Perform the tasks described in Prerequisites for Remediating Messages in Microsoft Exchange Online Mailboxes, on page 10.

Procedure

Step 1 Sign into the Azure Management Portal using your Office 365 business account credentials.

Step 2 Add a new application to the directory linked to your Office 365 subscription.

Step 3 Navigate to **App Registrations** > **New Registration** to add a new application.

Step 4 While adding a new application, make sure that you:

- Specify the application name and the account types the application must support.
- (Optional) Select the application type as Web and provide the URL where users can sign-in and use your appliance .

Step 5 Assign the permissions that the application requires. Click **API permissions** on the navigation pane and click **Add a permission**.

Step 6 Select **Microsoft Graph >Application permissions** and assign the following permissions:

- Mail.Read – Read mail in all mailboxes
- Mail. ReadWrite - Read and write mail in all mailboxes
- Mail.Send - Send mail as any user
- Directory.Read.All - Read user or group information from Azure Active Directory to store them on an LDAP server configured on the Cisco Cloud environment.

Step 7 Grant admin consent for all the requested permissions for all accounts in the organization.

Step 8 Secure the communication between the Office 365 services and the appliance by updating the application manifest with the key credentials from the public key certificate. Perform the following steps:

a) Using a Windows PowerShell prompt, get the values for `$base64Thumbprint` , `$base64Value` , and `$keyid` from the public key certificate. See the example below. From the Windows PowerShell prompt, navigate to the directory containing the public key certificate and run the following:

Example:

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import(".\mycer.cer")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()
```

After running the above commands, run the following commands to extract their values:

```
$keyid
$base64Value
$base64Thumbprint
```

b) Click **Manifest** on left pane of the registered application pane to open the manifest of the application.

c) In the manifest text editor, replace the empty KeyCredentials property with the following JSON:

Example:

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint_from_step_1",
"keyId": "$keyid_from_step1",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value_from_step1"
}
],
```

Example:

In the above JSON snippet, make sure that you replace the values of `$base64Thumbprint` , `$base64Value`, and `$keyid` with the values you obtained in step a. Each value must be entered in a single line

Step 9 After registering your appliance with Azure AD, note down the following details from the Azure Management Portal from the Overview pane of the registered application:

- Client ID
- Tenant ID. The Tenant ID is the unique value that will available on all the URLs listed on this page. For instance, the URLs listed on this page are:
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/federationmetadata/2007-06/federationmetadata.xml
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/wsfed
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/saml2

In this case, the Tenant ID is abcd1234-bcdd-469d-8545-a0662708cbc3 .

What to do next

Enabling Account Settings on Cisco Email Security Appliance , on page 14

Enabling Account Settings on Cisco Email Security Appliance

Before You Begin

Make sure that you have:

- [Required only for Mailbox Auto Remediation] Enabled File Reputation and Analysis feature on your appliance . See File Reputation Filtering and File Analysis.

Procedure

Step 1 Log in to the appliance .

Step 2 Click **System Administration** > **Account Settings**.

Step 3 Click **Enable**.

Step 4 Select **Enable Account Settings**.

Step 5 (Optional) Enter the maximum number of attempts the appliance makes to connect to the mailbox to remediate the message. The value must be an integer from 1 to 5.

Step 6 (Optional) Enter the number of seconds the appliance must wait before the connection times out to the hybrid mail exchange server. The value must be an integer from 15 to 90.

Step 7 (Optional) Enter the number of seconds the appliance must wait before the connection times out to the local mail exchange server. The value must be an integer from 15 to 90.

Step 8 Submit and commit your changes.

What to do next

Creating an Account Profile , on page 15

Creating an Account Profile

An account profile defines the mailbox parameters that are required for the appliance to connect to the mailbox and perform remedial actions when the threat verdict of the message in the mailbox turns malicious.

Each profile credentials are related to one single tenant. If you want to perform remediation across multiple tenants, then you have to configure one profile for each tenant and chain them together using a chained profile. However, if you are using a load balancer for a multi-tenant deployment, you can still configure a single profile and use the hostname of the load balancer while creating a profile.

Before You Begin

Make sure that you have:

- Enabled the account settings. See Enabling Account Settings on Cisco Email Security Appliance , on page 14.
- A valid email address in the Microsoft Exchange online or Microsoft Exchange on-premise server.
- The parameters required to configure the Microsoft Exchange online or Microsoft Exchange on-premise account.

Procedure

Step 1 Log in to the appliance .

Step 2 Click **System Administration** > **Account Settings**.

Step 3 Click **Create Account Profile**.

Step 4 Enter a name and description for the profile.

Step 5 Select the profile type based on the mailbox deployment:

- **Office 365/Hybrid (Graph API)** – Select this to configure a mailbox deployed on Microsoft Exchange online and enter the following details:Client ID and Tenant ID of the application that you registered on the Azure Management Portal.
  - Client ID and Tenant ID of the application that you registered on the Azure Management Portal.
  - Thumbprint of the certificate (value of $base64Thumbprint).
  - Upload the private key of the certificate. Click **Choose File** and select the .pem file.
  - (Optional) If you want the credentials configured in this profile to be used by the Office 365 LDAP connector, select **Use for LDAP synchronization**. LDAP connector uses this credentials to synchronize LDAP entries from Azure Active Directory to the local LDAP server.
- **Exchange On-premise** - Select this to configure a mailbox deployed on Microsoft Exchange on-premise and enter the following details:
  - Enter the username and password of the user account with impersonator privileges. For more information, see Add a User to the Impersonator Role, on page 12.
  - Enter the hostname of the Microsoft Exchange on-premise server.

    Note If you are using a load balancer for a multi-tenant deployment, you must configure the hostname of your load balancer.

Step 6 Verify whether the appliance can connect to the Microsoft Exchange online or Exchange on-premsie server.

a) Click **Test Connection**.
b) Enter an email address. This must be a valid email address in the Microsoft Exchange online or Microsoft Exchange on-premise.
c) Click **Test Connection**.
The status is displayed confirming whether your appliappliance ance can connect to the mailbox server.
d) 4. Click **Done**. For troubleshooting the errors, see Troubleshooting Mailbox Remediation, on page 20.

Step 7 Submit and commit your changes.

What to do next

- Creating a Chained Profile , on page 16
- Mapping Domains to the Account Profile , on page 17

Creating a Chained Profile

This task is mandatory only if you want to remediate messages in a mailbox on a hybrid or multi-tenant deployments.

Before You Begin

Make sure that you have at least one account profile added on your appliance :

Procedure

Step 1 Log in to the appliance .

Step 2 Click **System Administration** > **Account Settings**.

Step 3 Click **Create Chained Profile**.

Step 4 Enter a name and description for the chained profile.

Step 5 Select the account profile you want to add to the chained profile from the drop-down menu. To add more profiles, click **Add Account Profile**.

Note
- You must add the profiles in the order of priority in which you want the appliance to check the profile for remediating the message.
- You can create a maximum of five chained profiles at a time on your appliance .
- You can add a maximum of 10 account profiles per chained profile.

Step 6 Submit and commit your changes.

What to do next

Mapping Domains to the Account Profile , on page 17

Mapping Domains to the Account Profile

You must define the domain to which the recipient's mailbox belongs. The domain is then mapped to the account profile which is used by the appliance to remediate message in the mailbox.

Note

- You can edit the domain mapping to add new domains to the existing domain mapped to the profile.
- The domain mapping is unique to a profile. Domains mapped to one profile cannot be mapped to another.

Before You Begin

Make sure that you have at least one account profile added on your appliance .

Procedure

Step 1 Log in to the appliance .

Step 2 Click **System Administration** > **Account Settings**.

Step 3 Click **Create Domain Mapping**.

Step 4 Enter the domain names separated my commas. If you want to map the profile to all the domains, type the string 'ALL'.

Step 5 Select the profile to be mapped to the domain(s). You can also map a chained profile to the domain(s).

Step 6 Submit and commit your changes.

What to do next

- Configure Auto-Remedial Actions on Messages in the Mailboxes, on page 17
- Search and Remediate Messages in the Mailboxes, on page 18

Configure Auto-Remedial Actions on Messages in the Mailboxes

Note Perform the following steps if you want to configure remedial actions for Mailbox Auto Remediation on messages in the mailboxes.

Before You Begin

Make sure that you have enabled Mailbox Auto Remediation and configured the account settings on your appliance. See Enabling Account Settings on Cisco Email Security Appliance , on page 14.

Procedure

Step 1 Select **Mail Policies** > **Incoming Mail Policies**.

Step 2 Click the link in the **Advanced Malware Protection** column of the mail policy to modify.

Step 3 Select **Enable Mailbox Auto Remediation**.

Step 4 Specify the action to be taken on messages delivered to end users when the threat verdict changes to malicious. Depending on your requirements, choose one of the following remedial actions:

- Forward to an email address. Select this option to forward the message with malicious attachment to a specified user, for example, an email administrator.
- Delete the message. Select this option to permanently delete the message with malicious attachment from the end user's mailbox.
- Forward to an email address and delete the message. Select this option to forward the message with malicious attachment to a specified user, for example, an email administrator and permanently delete that message from the end user's mailbox.

Step 5 Submit and commit your changes.

What to do next

Related Topics

- Monitoring Mailbox Remediation Results, on page 19
- Viewing Mailbox Remediation Details in Message Tracking, on page 20
- Troubleshooting Mailbox Remediation, on page 20

Search and Remediate Messages in the Mailboxes

Before You Begin

- Make sure that you have enabled mailbox remediation and configured the account settings on your appliance . See Enabling Account Settings on Cisco Email Security Appliance , on page 14.
- Enable Message Tracking on your appliance . See Enabling Message Tracking.
- If you are using the Centralized Message Tracking service, make sure that you have enabled the trailblazer port and AsyncOS API HTTP port on the managed Cisco Email Security Gateway and the Cisco Content Security Management appliance can access the trailblazer port. If the trailblazer port is disabled, ensure that the Cisco Content Security Management appliance can access the AsyncOS API HTTP port on the managed Cisco Email Security Gateway .

Note You can perform the following steps only in the new web interface of the appliance .

Procedure

Step 1 Click the Email Security Appliance is getting a new look. Try it!! link on the legacy web interface. See Accessing the Web-Based Graphical User Interface (GUI).

Step 2 Click the **Tracking** tab.

Step 3 Click the **Messages** tab to narrow your search results. For more information, see Searching for Email Messages on the New Web Interface.

Step 4 Select the messages you want to remediate. You can select a maximum of 1000 messages at a time. You can remediate the messages that are only in the delivered state.

Step 5 Click **Remediate**.

Step 6 Enter the following details:

- Enter a batch name for the remediation.
- Select anyone of the following remediation action:
  - Delete the messages. Select this option to permanently delete the malicious messages from the end user's mailbox.
  - Forward to an email address or multiple email addresses separated by a semicolon(;). Select this option to forward the malicious messages to a specified user, for example, an email administrator.
  - Forward to an email address or multiple email addresses separated by a semicolon(;) and delete the messages. Select this option to forward the malicious messages to a specified user, for example, an email administrator and permanently delete that messages from the end user's mailbox.

Step 7 Click **Apply**.

What to do next

Related Topics

- Monitoring Mailbox Remediation Results, on page 19
- Viewing Mailbox Remediation Details in Message Tracking, on page 20
- Troubleshooting Mailbox Remediation, on page 20

Upgrading to AsyncOS 13.0 and Later Releases

The mailbox settings defined in the previous AsyncOS versions are migrated seamlessly during the upgrade. This mailbox is created with the profile name as 'Default' and mapped to 'ALL' domains. This profile can be edited as required after the upgrade. Ensure that your application has access to Microsoft Graph API on Azure Active Directory to remediate messages from Microsoft Exchange online mailboxes. For more information, see Registering Your Appliance as an Application on Azure AD, on page 12.

Monitoring Mailbox Remediation Results

You can view the details of the mailbox remediation results using the Remediation report page. To view the report:

1. Click the **Email Security Appliance is getting a new look. Try it!!** link on the legacy web interface.
2. Click the **Monitoring** tab.
3. Click the **Reports** drop-down menu and select **Remediation Report**.

Use this report to view the following details:

- Total number of messages attempted for remediation using Mailbox Auto Remediation and Mailbox Search and Remediate.

- Number of messages successfully remediated for a configured remedial action.
- Number of messages for which the remediation failed.
- Details about the messages for which the remediation was attempted.

For more information, refer to the section Remediation Report Page.

Viewing Mailbox Remediation Details in Message Tracking

You can view the details of messages remediated using Mailbox Search and Remediate in Message Tracking page. Before you begin the remediation, ensure that the Message Tracking is enabled.

Note Messages attempted for remediation using Mailbox Auto Remediation are not included in the tracking search results.

For more information about the data displayed, see Message Tracking Details.

Troubleshooting Mailbox Remediation

Connection Errors

Problem

While trying to check the connection between your appliance and recipent mailbox on the Account Settings page (**System Administration** > **Account Settings**), you receive an error message: `Connection Unsuccessful`.

Solution

Depending on the response from the server, do one of the following:

Error Message	Reason and Solution
`The SMTP address has no mailbox associated with it`	You have entered an email address that is not part of the associated mail domain. Enter a valid email address and check the connection again.

Error Message	Reason and Solution
`The mailbox cannot be accessed using this profile or the required permissions may be missing`	Verify that: • You have the required permission to access the user mailbox. The Micrsoft Exchange online account can be accessed only using the Microsoft Graph API and the Microsoft Exchange on-premise account using an user account with impersonator privileges. • You have selected the incorrect profile type. Modify the profile details on the Edit Account Profile page and check the connection again.
`Access is denied. Check credentials and try again`	The Office 365 application configured in Microsoft Azure does not have the required permission to access the Microsoft Exchange online mailbox.
`Application with identifier '<client_id>' was not found in the directory <tenant_id>`	You have entered an invalid Client ID. Modify the Client ID on the Account Profile page and check the connection again.
`No service namespace named '<tenant_id>' was found in the data store.`	You have entered an invalid Tenant ID. Modify the Tenant ID on the Account Profile page and check the connection again.
`Error validating credentials. Credential validation failed`	You have entered an invalid certificate thumbprint. Modify the certificate thumbprint on the Account Profile page and check the connection again.
`Error validating credentials. Client assertion contains an invalid signature.`	You have entered an incorrect certificate thumbprint or you have uploaded an invalid or incorrect certificate private key. Verify that: • You have entered the correct thumbprint. • You have uploaded the correct certificate private key. • The certificate private key is not expired. • The time zone of your appliance matches the time zone in the certificate private key.
`The requested user <email address> is invalid`	The email address entered does not match with the profile type of the account profile. Enter a valid email address or modify the account profile on the Account Profile page and check the connection again.

Error Message	Reason and Solution
`Failed to verify exchange server('<host name>') certificate. If self-signed certificate is used on exchange server install its custom CA certificate`	• You have entered an invalid CA or self-signed certificate on the Microsoft Exchange on-premise server. Verify the certificate and check the connection again. **Note** Ensure that the certificate you are using corresponds to the hostname provided in the profile. For example, if you have provided the IP address of the exchange server in your profile setting and the certificate is based on the hostname, then the connection will fail. • You have not imported the self-signed certificate from the Microsoft Exchange on-premise server to your appliance . For more information, see Importing a Certificate.
`Invalid username or password entered for exchange server ('<email address>')`	You have entered an invalid user name or password for the impersonator user account that is used to connect to the Microsoft Exchange on-premise mailbox.)
`The account does not have permission to impersonate the requested user`	The user account used to connect to the Microsoft Exchange on-premise mailbox is not a member of the impersonator role (does not have impersonator privileges).
`Please check host <hostname> is valid exchange server address.`	You have entered an incorrect hostname of the Microsoft Exchange on-premise server. Modify the hostname on the Account Profile page and check the connection again.

Viewing Logs

Mailbox remediation information is posted to the following logs:

- Mail Logs (mail_logs). The time at which the mailbox remediation process started is posted to this log. Information about Mailbox Auto Remediation or Mailbox Search and Remediate action:
  - The time at which the mailbox remediation process started is posted to this log.
  - The remediation status.
  - The reason for the unsuccessful remediation.
  - The recipients for whom the remediation was successful and unsuccessful.
  - The source from which the Search and Remediate action is initiated.
  - The user who initiated the Search and Remediate action.
  - The remedial action attempted on the messages.
- Remediation Logs. Information related to remediation status, actions performed, errors and so on are posted to this log.

Alerts

Alert: Connectivity Issues Between Appliance and Microsoft Exchange Services Detected

Problem

You receive an info-level alert indicating that there are connectivity issues between your appliance and Microsoft Exchange online or Microsoft Exchange on-premise services and the appliance is unable to perform the configured remedial action.

Solution

Do the following:

- Check for network issues that might prevent the communication between your appliance and Microsoft Exchange online or Microsoft Exchange on-premise services.

  Review the network settings of your appliance . See Changing Network Settings.

- Ensure that your application has access to Microsoft Graph API on Azure Active Directory.
- Ensure that the user account used to access the Exchange on-premise mailbox has impersonator privileges.
- Verify that the parameters configured in the corresponding profiles are valid and test the connection.
- Check for firewall issues. See Firewall Information.
- Check whether the Microsoft Exchange online or Microsoft Exchange on-premise services are operational.

Configured Remedial Actions Are Not Performed

Problem

After receiving a retrospective alert from the AMP server, configured remedial actions are not performed on the malicious messages in Exchange online and Exchange on-premise mailboxes.

Or

The user is unable to remediate the messages manually using the Remediate option on the Message Tracking page.

Solution

Do the following:

- Test the connection between your appliance and Exchange online and Exchange on-premise services. See Creating an Account Profile , on page 15.
- [Only for Mailbox Auto Remediation] Check whether you have received the following alert: Connectivity Issues Between Appliance and Exchange online and Exchange on-premise Services Detected. See Alerts, on page 22.