Automatically Remediating Messages in Mailboxes

This chapter contains the following sections:

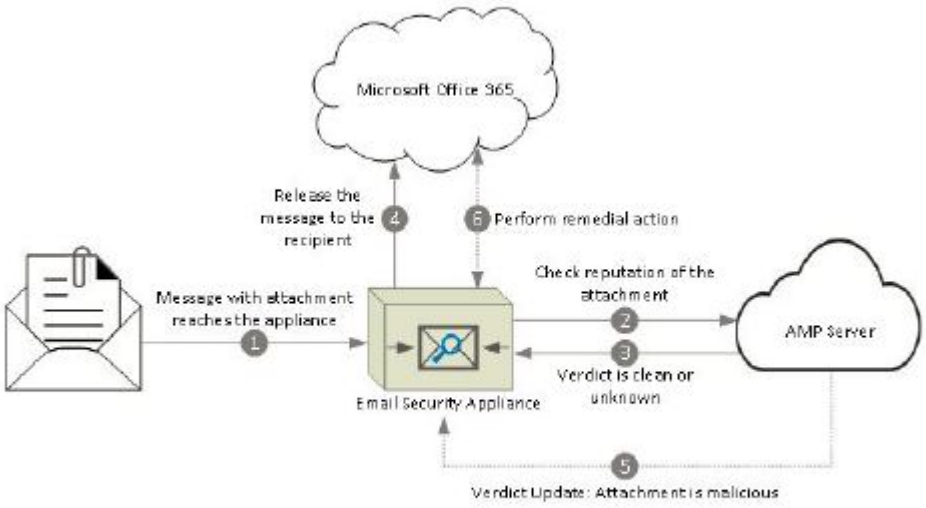
Performing Remedial Actions on Messages Delivered to End Users When the Threat Verdict Changes to Malicious

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. With this release you get more than just alerting. If your organization is using Office 365 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.

Contents

Workflow

Figure 1: Mailbox Auto Remediation Workflow



1. Message with an attachment reaches the appliance.
2. The appliance queries the AMP server to evaluate the reputation of the attachment.
3. The AMP 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 AMP 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.

How to Perform Remedial Actions on Messages Delivered to End Users When the Threat Verdict Changes to Malicious

	Do This	More Info
Step 1	Review the prerequisites.	Prerequisites, on page 3
Step 2	Register Email Security appliance as an application on Azure AD (Azure Management Portal).	Registering Your Cisco Secure Email Cloud Gateway as an Application on Azure AD, on page 4

	Do This	More Info
Step 3	Configure Office 365 mailbox settings on your appliance.	Configure Office 365 Mailbox Settings on Cisco Email Security Appliance, on page 5.
Step 4	Configure your appliance to perform remedial actions on messages delivered to end users when the threat verdict changes to malicious.	Configure Automatic Remedial Actions on Messages in the Mailboxes, on page 6

Prerequisites

Feature Keys for File Reputation Service and the File Analysis Service

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.

Registering Your Cisco Secure Email Cloud Gateway as an Application on Azure AD

Office 365 services use Azure Active Directory (Azure AD) to provide secure access to users' mailboxes. For your Cisco Secure Email Cloud Gateway to access the Office 365 mailboxes, you must register your Cisco Secure Email Cloud Gateway with Azure AD. The following are the high level steps you need to perform to register your Cisco Secure Email Cloud Gateway 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, on page 3.

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**.

- Application Permissions
  - Read mail in all mailboxes
  - Read and write mail in all mailboxes
  - Send mail as any user
  - Use Exchange Web Services with full access to all mailboxes
- Delegated Permissions
  - Send mail as a user
  - Read and write user mail
  - Read user mail
  - Access mailboxes as the signed-in user via Exchange Web Services

Step 6 Grant admin consent for all the requested permissions for all accounts in the organization.

Step 7 Secure the communication between the Office 365 services and the Cisco Secure Email Cloud Gateway 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 8 After registering your Cisco Secure Email Cloud Gateway with Azure AD, note down the following details from the Azure Management Portal from the Overview pane of the registered application:

- Cliend 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

Configure Office 365 Mailbox Settings on Cisco Email Security Appliance, on page 5

Configure Office 365 Mailbox Settings on Cisco Email Security Appliance

Before You Begin

Make sure that you have:

- Enabled File Reputation and Analysis feature on your appliance. See File Reputation Filtering and File Analysis.
- Acquired the private key of the certificate in .pem format. See Certificate for Secure Communication, on page 3.
- The values of the following parameters:
  - Client ID and Tenant ID of the application that you registered on the Azure Management Portal. See Registering Your Cisco Secure Email Cloud Gateway as an Application on Azure AD, on page 4
  - Certificate thumbprint ($base64Thumbprint). See Registering Your Cisco Secure Email Cloud Gateway as an Application on Azure AD, on page 4.

Step 1 Log in to the appliance.

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

Step 3 Click **Enable**.

Step 4 Select **Enable Office 365 Mailbox Settings**.

Step 5 Enter the following details:

- Client ID and Tenant ID of the application that you registered on the Azure Management Portal.
- Thumbprint of the certificate (value of $base64Thumbprint).

Step 6 Upload the private key of the certificate. Click **Choose File** and select the .pem file.

Step 7 Submit and commit your changes.

Step 8 Verify whether the appliance is able to connect to the Office 365 services.

a. Click **Check Connection**.

b. Enter an Office 365 email address. This must be a valid email address in the Office 365 domain.

c. Click **Test Connection**.

The popup will display whether your appliance is able to connect to the Office 365 services. If the connection fails, verify that:

- The values of Client ID, Tenant ID, and Thumbprint are correct.
- The private key that you have uploaded is correct and has not expired.

What to do next

Configure Automatic Remedial Actions on Messages in the Mailboxes, on page 6

Configure Automatic Remedial Actions on Messages in the Mailboxes

Before You Begin

Make sure that you have enabled mailbox remediation and configured the account settings on your Cisco Secure Email Cloud Gateway. See Configure Office 365 Mailbox Settings on Cisco Email Security Appliance, on page 5.

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

Step 2 Click the drop-down arrow next to the policy you want to edit.

Step 3 Click the edit icon next to **AMP** column.

Step 4 Select the **Enable Mailbox Auto Remediation** checkbox.

Step 5 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.

Note Messages from certain folders (for example, Deleted Items) cannot be deleted as Office exchange services do not support deletion of messages from these folders.

Step 6 Submit your changes.

What to do next

Related Topics

- Monitoring Mailbox Remediation Results, on page 7
- Viewing Mailbox Remediation Details in Message Tracking, on page 8
- Troubleshooting Mailbox Remediation, on page 8

Monitoring Mailbox Remediation Results

You can view the details of the mailbox remediation results using the Mailbox Auto Remediation report page (**Monitor** > **Mailbox Auto Remediation**). Use this report to view details such as:

- A list of recipients for whom the mailbox remediation was successful or unsuccessful
- Remedial actions taken on messages
- The filenames associated with a SHA-256 hash

The **Recipients for whom remediation was unsuccessful** field is updated in the following scenarios:

- The recipient is not a valid Office 365 user or the recipient does not belong to the Office 365 domain account configured on your appliance.
- The message containing the attachment is no longer available in the mailbox, for example, the end user deleted the message.
- There was a connectivity issue between your appliance and Office 365 services when the appliance was trying to perform the configured remedial action.

Click on a SHA-256 hash to view the related messages in Message Tracking.

Viewing Mailbox Remediation Details in Message Tracking

To display the details of mailbox remediation in message tracking,

- Message Tracking must be enabled. See Tracking Messages
- Mailbox remedial action (**Mail Policies** > **Incoming Mail Policies**> **Advanced Malware Protection**> **Enable Mailbox Auto Remediation**) must be configured. See Configure Automatic Remedial Actions on Messages in the Mailboxes, on page 6.

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** > **Mailbox SettingsAccount 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.
`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 Mailbox Settings 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 Mailbox Settings page and check the connection again.

Error Message	Reason and Solution
`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 is incorrect or does not match with the mailbox settings. Enter a valid email address or modify the Mailbox Settings 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.
- Mailbox Auto Remediation Logs (mar). 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 Office 365 mailboxes.

Solution

Do the following:

- Test the connection between your appliance and Office 365 services. See Configure Office 365 Mailbox Settings on Cisco Email Security Appliance, on page 5.
- Check whether you have received the following alert: Connectivity Issues Between Appliance Office 365 Services Detected. See Alerts, on page 9.