How-to configure Cisco Secure Email Account Settings for Microsoft Azure (Microsoft 365) API

Contents

Introduction

This document provides a step-by-step "how-to" for registering a new application in Microsoft Azure (Azure Active Directory) to generate the needed Client ID, Tenant ID, and Client credentials, and then the configuration for Account Settings on a Cisco Secure Email Gateway or Cloud Gateway. Configuration of the Account Settings and associated Account Profile are required when a mail administrator configures Mailbox Auto Remediation (MAR) for Advanced Malware Protection (AMP) or URL Filtering or utilizes the Remediate action from Message Tracking on the Cisco Secure Email and Web Manager or Cisco Secure Gateway/Cloud Gateway.

Mailbox Auto Remediation Process Flow

An attachment (file) in your email or a URL may be scored as malicious at any time, even after it has reached a user's mailbox. AMP on Cisco Secure Email (via Cisco Secure Malware Analytics) can identify this development as new information emerges and will push retrospective alerts to Cisco Secure Email. Cisco Talos provides the same with URL analysis, as of AsyncOS 14.2 for Cisco Secure Email Cloud Gateway. If your organization is using Microsoft 365 to manage mailboxes, you can configure Cisco Secure Email to perform auto-remediation actions on the messages in a user's mailbox when these threat verdicts change.

Cisco Secure Email communicates securely and directly to Microsoft Azure Active Directory to gain access to Microsoft 365 mailboxes. For example, if an email with an attachment is processed through your gateway and scanned by AMP, the file attachment (SHA256) is provided to AMP for file reputation. The AMP disposition can be marked as Clean (step 5, Figure 1), and then delivered to the end recipient's Microsoft 365 mailbox. At a later time, the AMP disposition is changed to Malicious, Cisco Malware Analytics sends a retrospective verdict update (step 8, Figure 1) to *any* gateway that has processed that specific SHA256. Once the gateway receives the retrospective verdict update of Malicious (if configured), the gateway will then take one of the following Mailbox Auto Remediation (MAR) actions: Forward, Delete, or Forward and Delete.

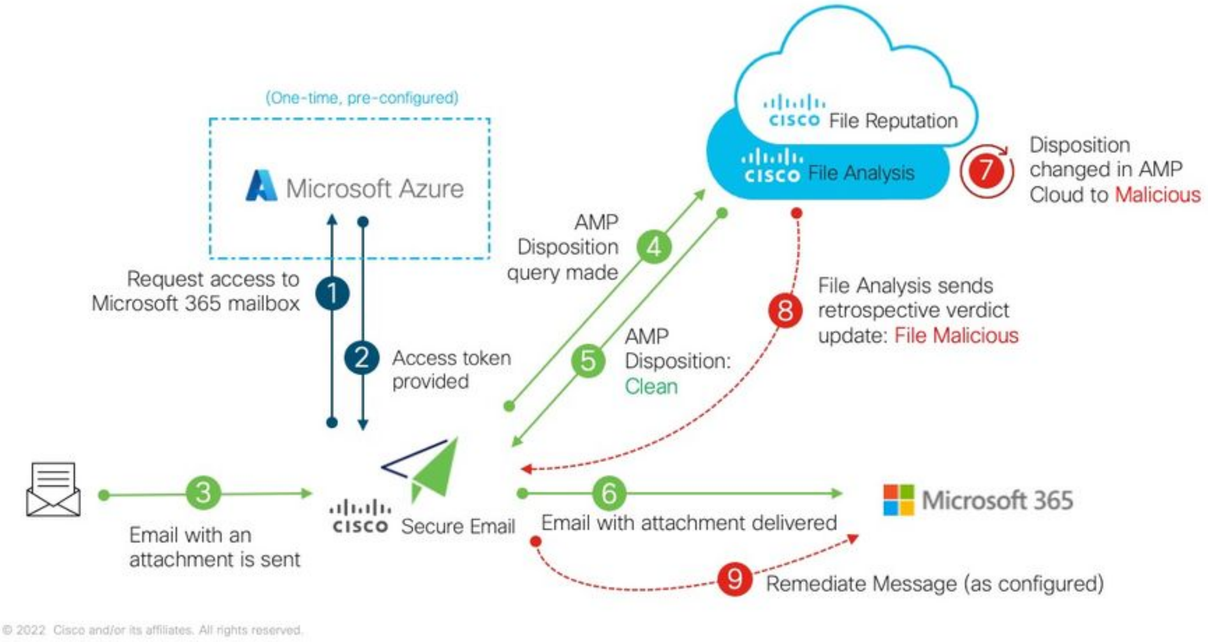

(One-time, pre-configured)
Microsoft Azure
CISCO File Reputation
CISCO File Analysis
7
Disposition changed in AMP Cloud to Malicious
AMP Disposition query made
4
Request access to Microsoft 365 mailbox
1
2
Access token provided
5
AMP Disposition: Clean
8
File Analysis sends retrospective verdict update: File Malicious
3
Email with an attachment is sent
CISCO Secure Email
6
Email with attachment delivered
Microsoft 365
9
Remediate Message (as configured)
© 2022 Cisco and/or its affiliates. All rights reserved.

Figure 1: MAR (for AMP) on Cisco Secure Email

This guide is on how-to configure Cisco Secure Email with Microsoft 365 for Mailbox Auto Remediation only. AMP (File Reputation and File Analysis) and/or URL Filtering on the gateway should already be configured. For further details on File Reputation and File Analysis, please consult the User Guide for the version of AsyncOS you have deployed.

Prerequisites

1. Microsoft 365 account subscription (Please make sure that your Microsoft 365 account subscription includes access to Exchange, such as an Enterprise E3 or Enterprise E5 account.)

2. Microsoft Azure administrator account and access to http://portal.azure.com

3. Both the Microsoft 365 and Microsoft Azure AD accounts are tied properly to an active "user@domain.com" email address, and you are able to send and receive emails via that email address.

You will be creating the following values in order to configure the Cisco Secure Email gateway API communication to Microsoft Azure AD:

- **Client ID**
- **Tenant ID**
- **Client secret**

> **Note**: Starting with AsyncOS 14.0, **Account Settings** allows configuration using a Client secret when creating the Microsoft Azure App Registration. This is the easier and preferred method.

Optional - If you are NOT utilizing the Client secret, you will need to create and have ready:

- **Thumbprint**
- **The private key (PEM file)**

Creating the thumbprint and private key are covered in the Appendix of this guide:

1. An active public (or private) certificate (CER) and the private key used to sign the certificate (PEM), or the ability to create a public certificate (CER) and the ability to save the private key used to sign the certificate (PEM). Cisco provides two methods in this document to get this done based on your administration preference: Certificate: Unix/Linux/OS X (utilizing OpenSSL)Certificate: Windows (utilizing PowerShell)

2. Access to Windows PowerShell, usually administered from a Windows Host or Server -or- access to Terminal application via Unix/Linux

In order to build these required values, you will need to complete the steps provided in this document.

Register an Azure app for use with Cisco Secure Email

Application Registration

Login to your Microsoft Azure Portal
1. Click on **Azure Active Directory** (Figure 2)
2. Click on **App registrations**
3. Click on **+ New registration**
4. On the "Register an application" page:
    a. Name: **Cisco Secure Email MAR** (or the name of your choice)
    b. Supported account types: **Accounts in this**

organizational directory only (Account Name)
c. Redirect URI: (optional)
[Note: You may leave this blank, or feel free to use https://www.cisco.com/sign-on for fill-in]
d. At the bottom of the page, click on **Register**

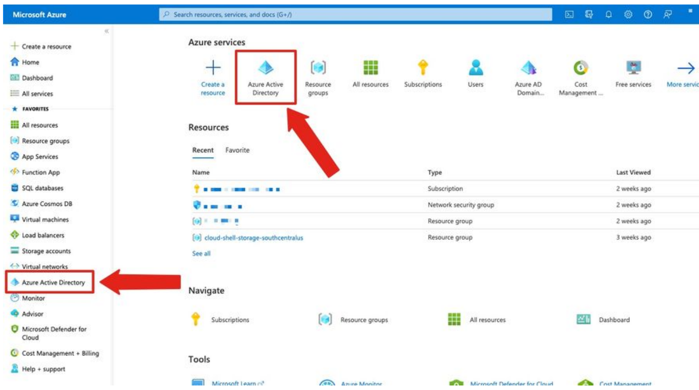
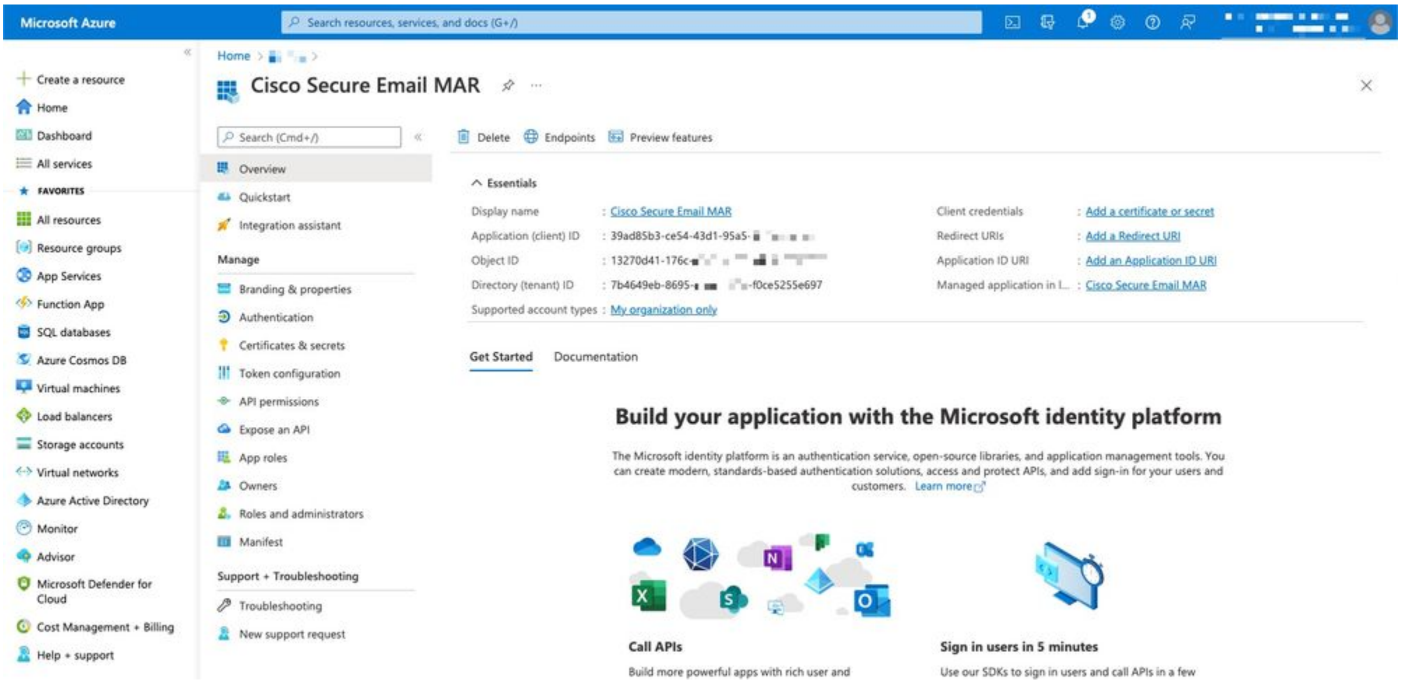


Figure 2: Microsoft Azure Portal example

Once completed with the above steps you will be presented with your application:



Display name : Cisco Secure Email MAR
Application (client) ID : 39ad85b3-ce54-43d1-95a5-[redacted]
Object ID : 13270d41-176c-[redacted]
Directory (tenant) ID : 7b4649eb-8695-[redacted]-f0ce5255e697
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : Cisco Secure Email MAR

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. Learn more

Build more powerful apps with rich user and

Use our SDKs to sign in users and call APIs in a few

Figure 3: Microsoft Azure Active Directory application page

Certificates and Secrets

If you are running AsyncOS 14.0 or newer, Cisco recommends configuring your Azure app to utilize a client secret. On your application pane, in the Manage options:

1. Select **Certificates & secrets**

2. In the ***Client secrets*** section, click **+ New client secret**

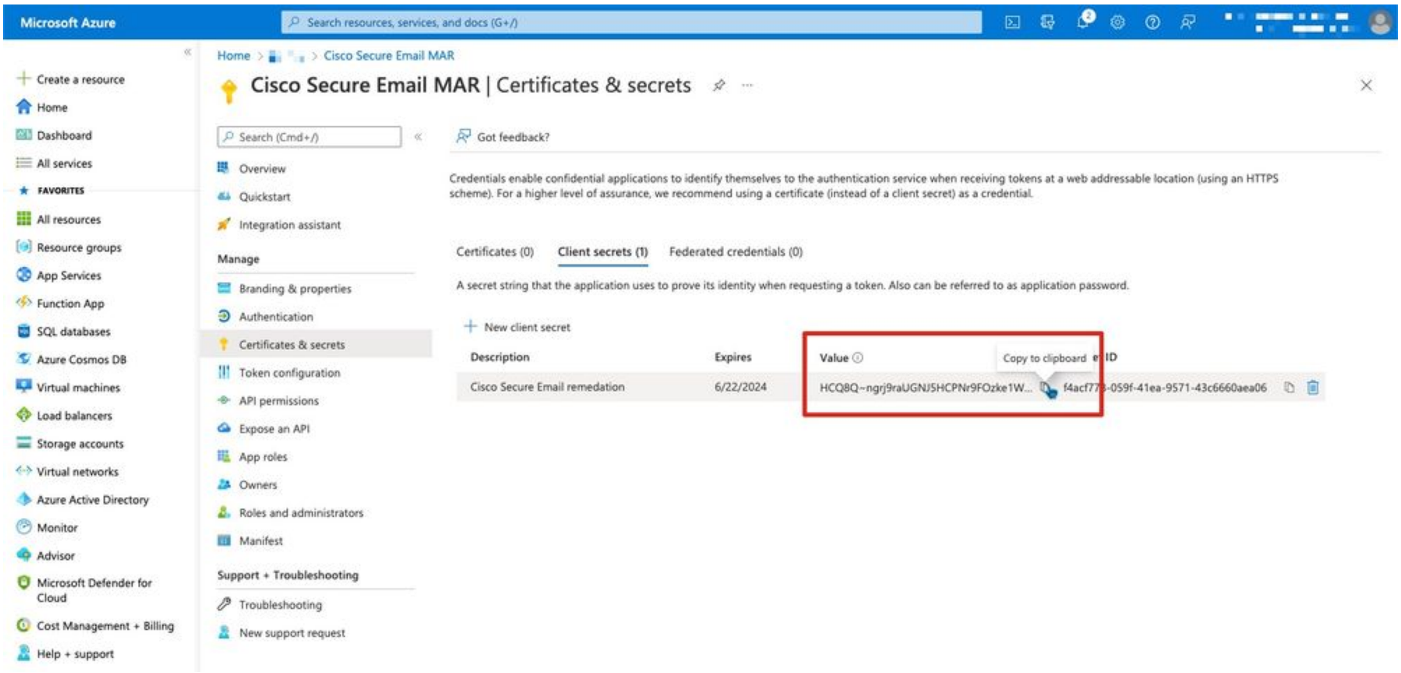
3. Add a description to help identify what this client secret is for, e.g. "Cisco Secure Email remediation"

4. Select an expiration period

5. Click **Add**

6. Mouse over to the right of the value that is generated, and click the **Copy to Clipboard** icon

7. Save this value to your notes, note this as "Client secret”



Cisco Secure Email MAR | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	ID
Cisco Secure Email remedation	6/22/2024	HCQ8Q~ngrj9raUGNJ5HCPNr9FOzke1W...	f4acf773-059f-41ea-9571-43c6660aea06

Figure 4: Microsoft Azure create client secret example

> **Note**: Once you exit your active Microsoft Azure session, the value of the client secret you just generated will *** out the value. If you do not record and safeguard the value before exiting, you will need to recreate the client secret in order to see the clear text output.

Optional **-** If you are not configuring your Azure application with a Client secret, please configure your Azure app to use your certificate. On your application pane, in the Manage options:

1. Select **Certificates & secrets**
2. Click **Upload certificate**
3. Select the CRT file (as created earlier)
4. Click **Add**

API Permissions

Note: Starting in AsyncOS 13.0 for Email Security, the API permissions for Microsoft Azure to Cisco Secure Email communication required changed from using Microsoft Exchange to Microsoft Graph. If you have already configured MAR and you are upgrading your existing Cisco Secure Email gateway to AsyncOS 13.0, you may simply update/add the new API permissions. (If you are running an older version of AsyncOS, 11.x or 12.x, please see Appendix B before you continue.)

On your application pane, in the Manage options:

1. Select **API permissions**
2. Click **+ Add a permission**
3. Select **Microsoft Graph**
4. Select the below permissions on ***Application permissions***: Mail > "Mail.Read" (Read mail in all mailboxes)Mail > "Mail.ReadWrite" (Read and write mail in all mailboxes)Mail > "Mail.Send" (Send mail as any user)Directory > "Directory.Read.All" (Read directory data) [*Optional: If you are using LDAP Connector/LDAP synchronization, enable. If not, this is not required.]
5. *Optional*: You will see that Microsoft Graph by default is enabled for “User.Read” permissions; you may leave this as configured or click **Read** and click **Remove permission** to remove this from your API permissions associated with your application.
6. Click **Add permissions** (or **Update permissions**, if Microsoft Graph was already listed)
7. Finally, click on **Grant admin consent for...** to ensure that your new permissions are applied to the application
8. There will be an in-pane pop-up that asks:

   "*Do you want to grant consent for the requested permissions for all accounts in <Azure Name>? This will update any existing admin consent records this application already has to match what is listed below.*"

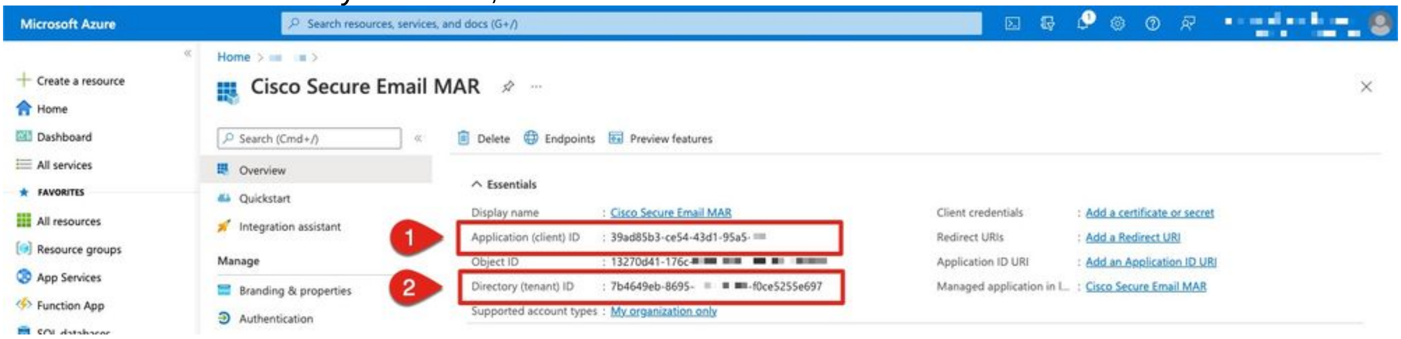
   Click **Yes**

At this point, you should see a green success message and the "Admin Consent Required" column display Granted.

Getting Your Client ID and Tenant ID

On your application pane, in the Manage options:

1. Click **Overview**
2. Mouse over to the right of your Application (Client) ID and click the **Copy to Clipboard** icon
3. Save this value to your notes, note this as "Client ID”
4. Mouse over to the right of your Directory (tenant) ID and click the **Copy to Clipboard** icon
5. Save this value to your notes, note this as "Tenant ID"



Cisco Secure Email MAR

Essentials

Display name : Cisco Secure Email MAR
Application (client) ID : 39ad85b3-ce54-43d1-95a5-[redacted]
Object ID : 13270d41-176c[redacted]
Directory (tenant) ID : 7b4649eb-8695-[redacted]-f0ce5255e697
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : Cisco Secure Email MAR

Figure 5: Microsoft Azure... Client ID, Tenant ID example

Configuring Your Cisco Secure Email Gateway/Cloud Gateway

At this time, you should have the following values prepared and saved to your notes:

- **Client ID**
- **Tenant ID**
- **Client secret**

Optional, if not using Client secret:

- **Thumbprint**
- **The private key (PEM file)**

You are ready to use the created values from your notes and configure the Account Settings on the Cisco Secure Email gateway!

Create Account Profile

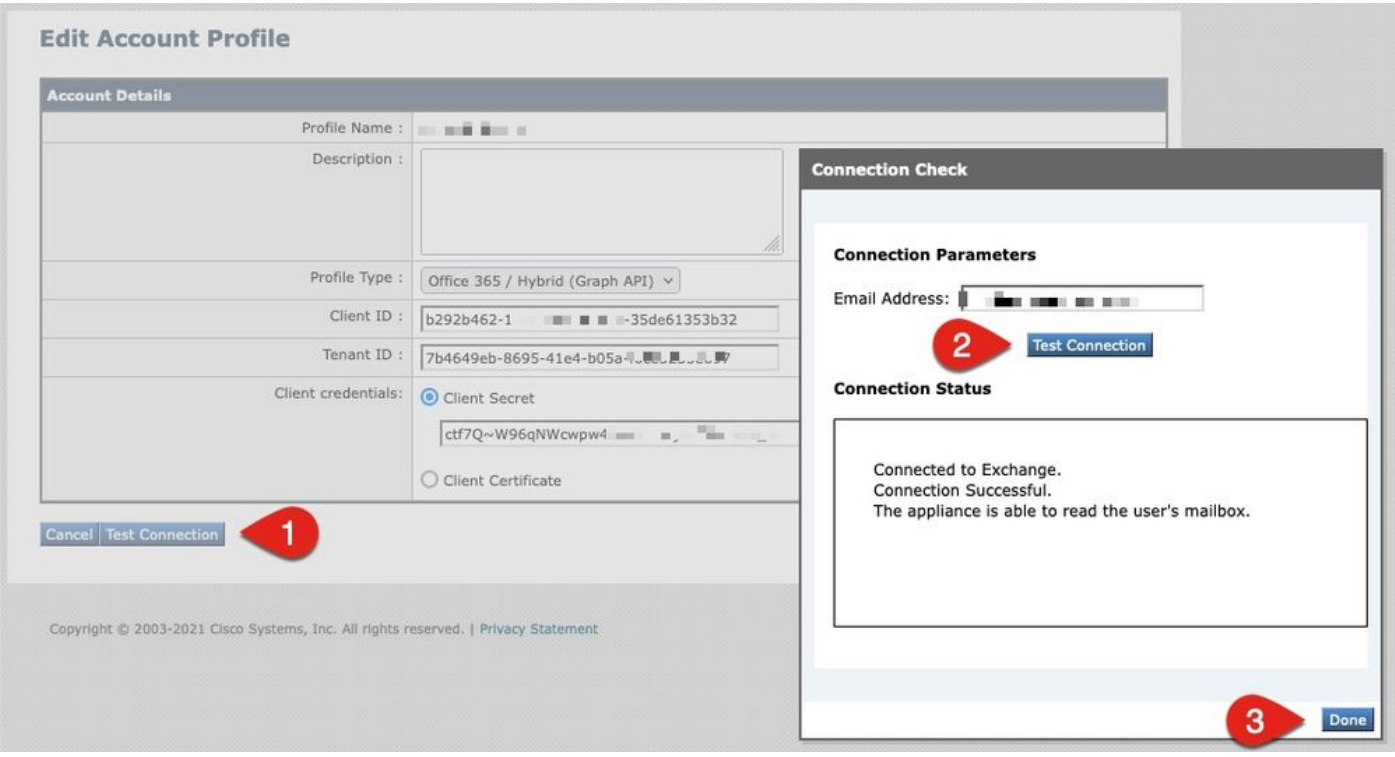
1. Log in to your gateway
2. Navigate to **System Administration > Account Settings** Note: If you are running a version prior to AsyncOS 13.x, this will be **System Administration > Mailbox Settings**
3. Click **Enable**
4. Click the checkbox for Enable Account Settings and click **Submit**
5. Click **Create Account Profile**
6. Provide a profile name and description (something that will uniquely describe your account if you have multiple domains)
7. As you are defining a Microsoft 365 connection, leave the profile type as **Office 365 / Hybrid (Graph API)**
8. Enter your **Client ID**
9. Enter your **Tenant ID**
10. For Client credentials do one of the following, as you have configured in Azure: Click **Client Secret** and paste in your configured client secret, or...Click **Client Certificate** and enter in your Thumbprint and also provide your PEM by clicking "Choose File"
11. Click **Submit**
12. Click **Commit Changes** in the upper right-hand of the UI
13. Enter in any comments and complete the configuration changes by clicking **Commit Changes**

Check Connection

The next step is only to verify the API connection from your Cisco Secure Email gateway to

Microsoft Azure:

1. From the same Account Details page, click **Test Connection**
2. Enter in a valid email address for the domain that is managed in your Microsoft 365 account
3. Click **Test Connection**
4. You should receive a success message (Figure 6)
5. Click **Done** to finish



Edit Account Profile

Account Details

Profile Name : [redacted]

Description :

Profile Type : Office 365 / Hybrid (Graph API)

Client ID : b292b462-1[redacted]-35de61353b32

Tenant ID : 7b4649eb-8695-41e4-b05a[redacted]

Client credentials: ● Client Secret

ctf7Q~W96qNWcwpw4[redacted]

○ Client Certificate

Copyright © 2003-2021 Cisco Systems, Inc. All rights reserved. | Privacy Statement

Connection Check

Connection Parameters

Email Address: [redacted]

Connection Status

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

Figure 6: Account Profile/Connection Check example

6. In the *Domain Mapping* section, click **Create Domain Mapping**

7. Enter in your domain name(s) that are associated with the Microsoft 365 account you have just validated the API connection for

The following is a list of valid domain formats that can be used to map a Mailbox Profile:

- The domain can be the special keyword 'ALL' to match all domains in order to create a default domain mapping.

- Domain names such as 'example.com' - Matches any address with this domain.

- Partial domain names such as '@.partial.example.com' - Matches any address ending with this domain

- Multiple domains can be entered by using a comma-separated list of domains.

8. Click **Submit**

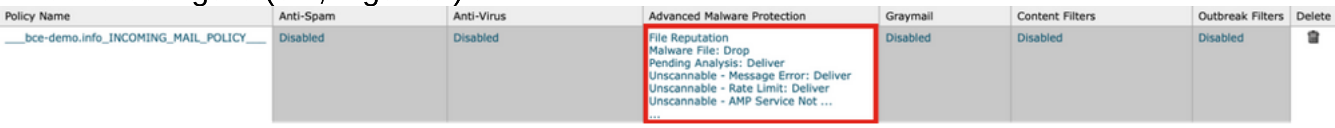
9. Click **Commit Changes** in the upper right-hand of the UI

10. Enter in any comments and complete the configuration changes by clicking **Commit Changes**

Enable Mailbox Auto Remediation (MAR) for Advanced Malware Protection in Mail Policy

Complete this step to enable MAR in the AMP configuration for mail policies.

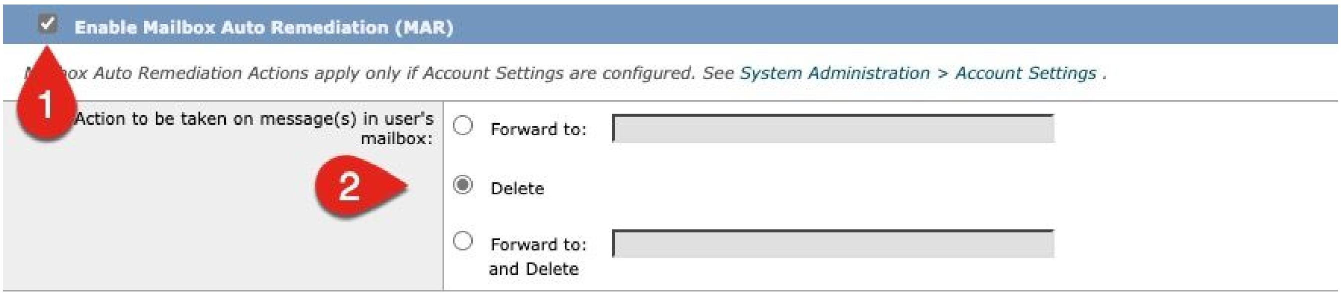
1. Navigate to **Mail Policies > Incoming Mail Policies**
2. Click on the settings in the Advanced Malware Protection column for the policy name you wish to configure (ex., Figure 7):



Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
___bce-demo.info_INCOMING_MAIL_POLICY___	Disabled	Disabled	File Reputation Malware File: Drop Pending Analysis: Deliver Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Disabled	Disabled	Disabled	🗑

Figure 7: Enable MAR (incoming mail policies)

3. Scroll to the bottom of the page
4. Click the checkbox for Enable Mailbox Auto Remediation (MAR)
5. Select one of the following actions you wish to take for MAR (ex., Figure 8): Forward to: <*enter in email address*>DeleteForward to: <*enter in email address*> and Delete



☑ Enable Mailbox Auto Remediation (MAR)

Mailbox Auto Remediation Actions apply only if Account Settings are configured. See System Administration > Account Settings .

Action to be taken on message(s) in user's mailbox:

○ Forward to:

● Delete

○ Forward to: and Delete

Figure 8: Enable MAR for AMP configuration example

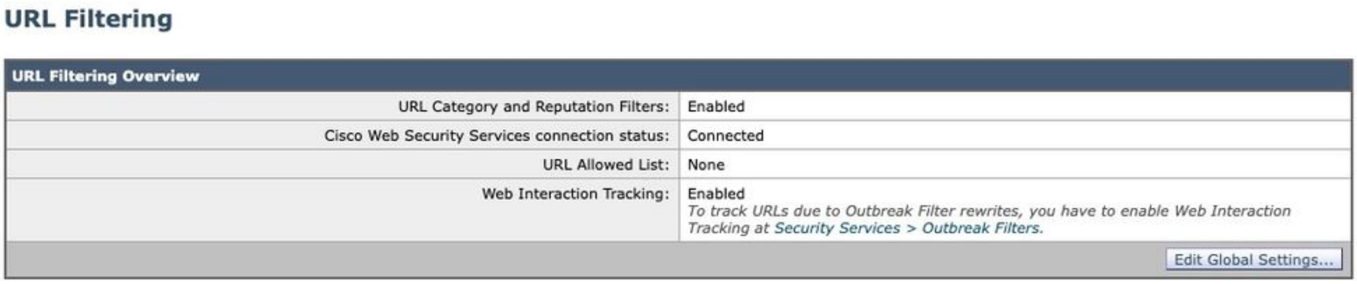
6. Click **Submit**
7. Click **Commit Changes** in the upper right-hand of the UI
8. Enter in any comments and complete the configuration changes by clicking **Commit Changes**

Enable Mailbox Auto Remediation (MAR) for URL Filtering

Starting with AsyncOS 14.2 for Cisco Secure Email Cloud Gateway, URL Filtering now includes URL Retrospective Verdict and URL Remediation.

1. Navigate to **Security Services > URL Filtering**
2. If you do not already have URL Filtering configured, click **Enable**
3. Click the checkbox for "Enable URL Category and Reputation Filters"
4. The *Advanced Settings* with the default settings
5. Click **Submit**

Your URL Filtering should look similar to the following:



URL Filtering

URL Filtering Overview	
URL Category and Reputation Filters:	Enabled
Cisco Web Security Services connection status:	Connected
URL Allowed List:	None
Web Interaction Tracking:	Enabled *To track URLs due to Outbreak Filter rewrites, you have to enable Web Interaction Tracking at Security Services > Outbreak Filters.*

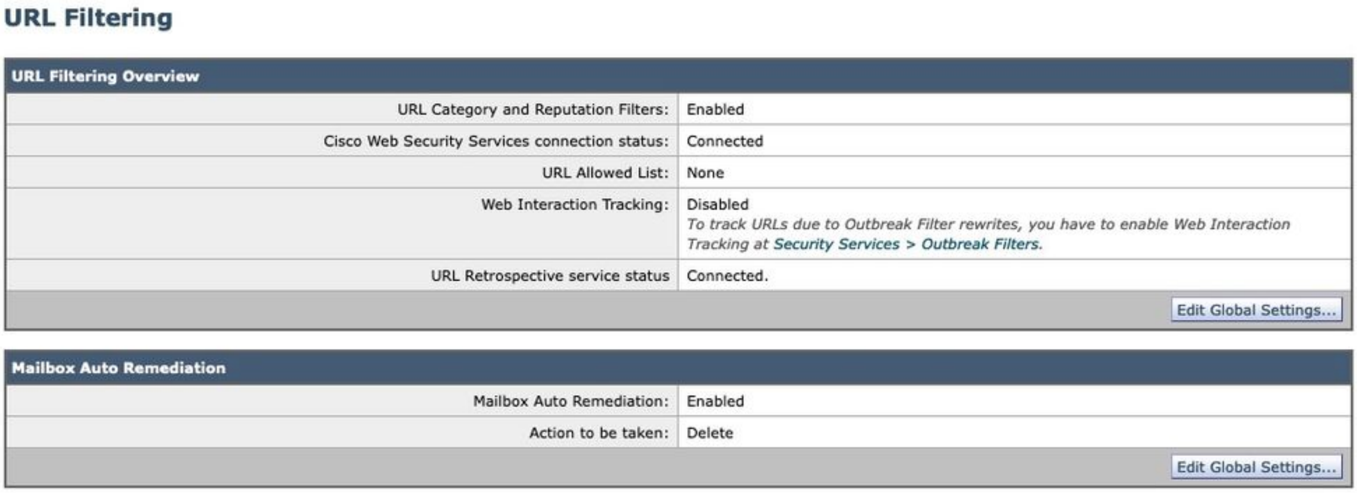
Figure 9: URL Filtering post-enable example

In order to see URL Retrospection with-in URL Filtering, perform the following, or have a support case opened for Cisco to perform:

```
esa1.hcxxyy-zz.iphmx.com> urlretroservice enable

URL Retro Service is enabled.

esa1.hcxxyy-zz.iphmx.com> websecurityconfig

URL Filtering is enabled.
No URL list used.
Web Interaction Tracking is enabled.
URL Retrospective service based Mail Auto Remediation is disabled.
URL Retrospective service status - Unavailable

Disable URL Filtering? [N]>

Do you wish to disable Web Interaction Tracking? [N]>

Do you wish to add URLs to the allowed list using a URL list? [N]>


Enable URL Retrospective service based Mail Auto Remediation to configure remediation actions.

Do you wish to enable Mailbox Auto Remediation action? [N]> y

URL Retrospective service based Mail Auto Remediation is enabled.

Please select a Mailbox Auto Remediation action:
1. Delete
2. Forward and Delete
3. Forward
[1]> 1

esa1.hcxxyy-zz.iphmx.com> commit

Please enter some comments describing your changes:
[]>

Do you want to save the current configuration for rollback? [Y]>
```

```
Changes committed: Tue Mar 29 19:43:48 2022 EDT
```

Once complete, refresh your UI on the URL Filtering page and you should now see similar to the following:



URL Filtering

URL Filtering Overview	
URL Category and Reputation Filters:	Enabled
Cisco Web Security Services connection status:	Connected
URL Allowed List:	None
Web Interaction Tracking:	Disabled *To track URLs due to Outbreak Filter rewrites, you have to enable Web Interaction Tracking at Security Services > Outbreak Filters.*
URL Retrospective service status	Connected.

Mailbox Auto Remediation	
Mailbox Auto Remediation:	Enabled
Action to be taken:	Delete

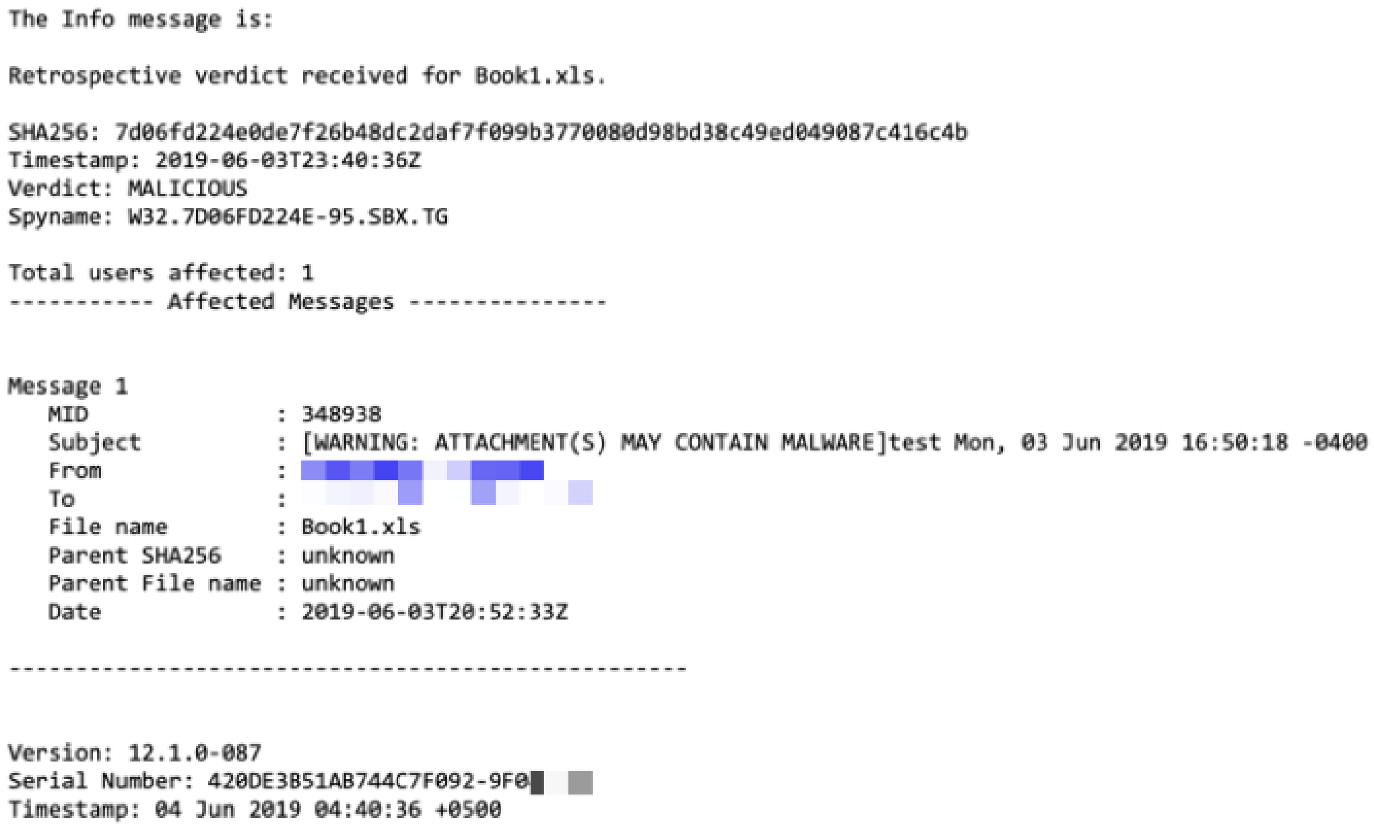
Figure 10: URL Filtering (AsyncOS 14.2 for Cisco Secure Email Cloud Gateway)

URL protection is now ready to perform remedial actions when a verdict changes score. For more information, please see Protecting Against Malicious or Undesirable URLs in the User Guide for AsyncOS 14.2 for Cisco Secure Email Cloud Gateway.

Configuration complete!

At this time Cisco Secure Email is ready to continuously evaluate emerging threats as new information becomes available and notify you about files that are determined to be threats after they have entered your network.

When a retrospective verdict is produced from File Analysis (Cisco Secure Malware Analytics), an info message is sent to the Email Security administrator (if configured). Example:

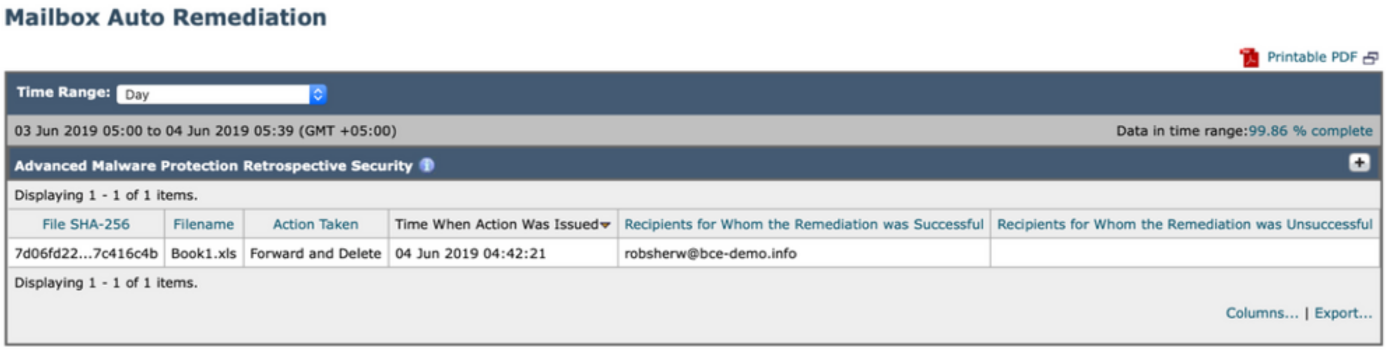


```
The Info message is:

Retrospective verdict received for Book1.xls.

SHA256: 7d06fd224e0de7f26b48dc2daf7f099b3770080d98bd38c49ed049087c416c4b
Timestamp: 2019-06-03T23:40:36Z
Verdict: MALICIOUS
Spyname: W32.7D06FD224E-95.SBX.TG

Total users affected: 1
----------- Affected Messages --------------


Message 1
   MID              : 348938
   Subject          : [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]test Mon, 03 Jun 2019 16:50:18 -0400
   From             : [redacted]
   To               : [redacted]
   File name        : Book1.xls
   Parent SHA256    : unknown
   Parent File name : unknown
   Date             : 2019-06-03T20:52:33Z

---------------------------------------------------


Version: 12.1.0-087
Serial Number: 420DE3B51AB744C7F092-9F0[redacted]
Timestamp: 04 Jun 2019 04:40:36 +0500
```

Mailbox Auto Remediation will be taken as configured if configured against the mail policy.

Mailbox Auto Remediation Report Examples

Reporting for any SHA256 that has been remediated will be in the Mailbox Auto Remediation report available both on the Cisco Secure Email gateway and Cisco Secure Email and Web Manager.



Mailbox Auto Remediation

Time Range: Day

03 Jun 2019 05:00 to 04 Jun 2019 05:39 (GMT +05:00)

Data in time range:99.86 % complete

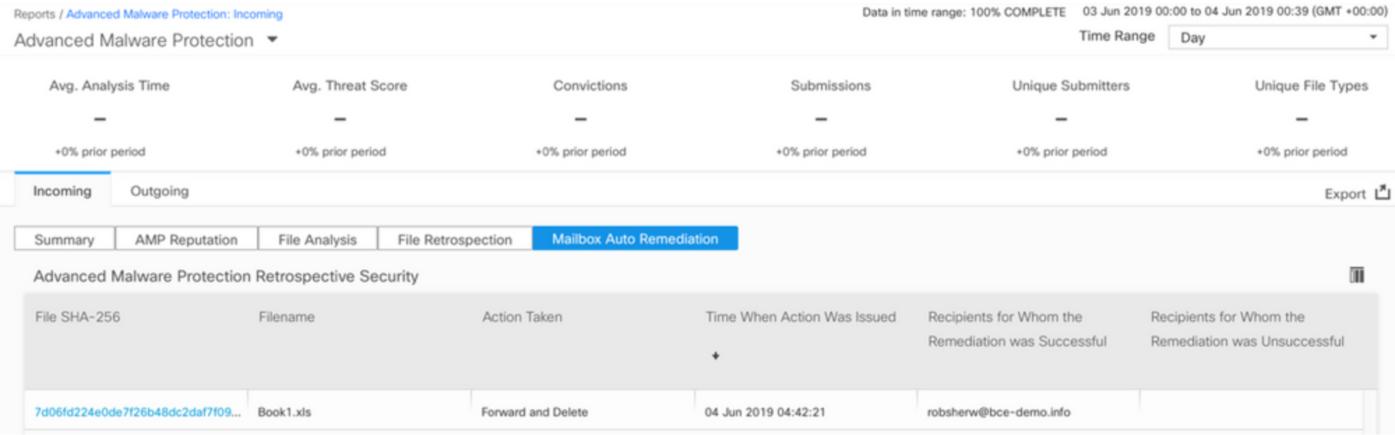
Advanced Malware Protection Retrospective Security

Displaying 1 - 1 of 1 items.

File SHA-256	Filename	Action Taken	Time When Action Was Issued	Recipients for Whom the Remediation was Successful	Recipients for Whom the Remediation was Unsuccessful
7d06fd22...7c416c4b	Book1.xls	Forward and Delete	04 Jun 2019 04:42:21	robsherw@bce-demo.info	

Displaying 1 - 1 of 1 items.

Figure 11: (Legacy UI) Mailbox Auto Remediation Report



Data in time range: 100% COMPLETE 03 Jun 2019 00:00 to 04 Jun 2019 00:39 (GMT +00:00)

Time Range: Day

Avg. Analysis Time	Avg. Threat Score	Convictions	Submissions	Unique Submitters	Unique File Types
–	–	–	–	–	–
+0% prior period	+0% prior period	+0% prior period	+0% prior period	+0% prior period	+0% prior period

Advanced Malware Protection Retrospective Security

File SHA-256	Filename	Action Taken	Time When Action Was Issued	Recipients for Whom the Remediation was Successful	Recipients for Whom the Remediation was Unsuccessful
7d06fd224e0de7f26b48dc2daf7f09...	Book1.xls	Forward and Delete	04 Jun 2019 04:42:21	robsherw@bce-demo.info	

Figure 12: (NG UI) Mailbox Auto Remediation Report

Mailbox Auto Remediation Logging

Mailbox Auto Remediation has an individual log, “mar”. The Mailbox Auto Remediation logs will contain all communication activity between your Cisco Secure Email gateway and Microsoft Azure, Microsoft 365.

An example of the mar logs:

```
Mon May 27 02:24:28 2019 Info: Version: 12.1.0-087 SN: 420DE3B51AB744C7F092-9F0000000000
Mon May 27 02:24:28 2019 Info: Time offset from UTC: 18000 seconds
Fri May 31 01:11:53 2019 Info: Process ready for Mailbox Auto Remediation
Fri May 31 01:17:57 2019 Info: Trying to connect to Azure AD.
Fri May 31 01:17:57 2019 Info: Requesting token from Azure AD.
Fri May 31 01:17:58 2019 Info: Token request successful.
Fri May 31 01:17:58 2019 Info: The appliance is able to read the user's(robsherw@bce-demo.info)
mailbox.
Fri May 31 04:41:54 2019 Info: Trying to perform the configured action on MID:312391
SHA256:de4dd03acda0a24d0f7e375875320538952f1fa30228d1f031ec00870ed39f62 Recipient:robsherw@bce-
demo.info.
Fri May 31 04:41:55 2019 Info: Message containing attachment(s) for which verdict update
was(were) available was not found in the recipient's (robsherw@bce-demo.info) mailbox.
Tue Jun  4 04:42:20 2019 Info: Trying to perform the configured action on MID:348938
SHA256:7d06fd224e0de7f26b48dc2daf7f099b3770080d98bd38c49ed049087c416c4b Recipient:robsherw@bce-
demo.info.
Tue Jun  4 04:42:21 2019 Info: Message containing attachment(s) for which verdict update
was(were) available was not found in the recipient's (robsherw@bce-demo.info) mailbox.
```

Troubleshooting Cisco Secure Email Gateway

If you are not seeing successful results for the connection status test, you may wish to review the application registration performed from Microsoft Azure AD.

From the Cisco Secure Email gateway, set your MAR logs to the 'trace' level and re-test the connection.

For unsuccessful connections, logs may show similar to:

```
Thu Mar 30 16:08:49 2017 Info: Trying to connect to Azure AD.
Thu Mar 30 16:08:49 2017 Info: Requesting token from Azure AD.
Thu Mar 30 16:08:50 2017 Info: Error in requesting token: AADSTS70001: Application with
identifier '445796d4-8e72-4d06-a72c-02eb47a4c59a' was not found in the directory ed437e13-ba50-
479e-b40d-8affa4f7e1d7
Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
Timestamp: 2017-03-30 20:08:50Z
Thu Mar 30 16:08:50 2017 Info: Error while requesting token AADSTS70001: Application with
identifier '445796d4-8e72-4d06-a72c-02eb47a4c59a' was not found in the directory ed437e13-ba50-
479e-b40d-8affa4f7e1d7
Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
Timestamp: 2017-03-30 20:08:50Z
```

Confirm the Application ID, Directory ID (which is the same as the Tenant ID), or other associated identifiers from the log with your application in Azure AD. If you are unsure of the values, delete the application from the Azure AD portal and start over.

For a successful connection, logs should be similar to:

```
Thu Mar 30 15:51:58 2017 Info: Trying to connect to Azure AD.
Thu Mar 30 15:51:58 2017 Info: Requesting token from Azure AD.
Thu Mar 30 15:51:58 2017 Trace: command session starting
Thu Mar 30 15:52:00 2017 Info: Token request successful.
Thu Mar 30 15:52:00 2017 Info: The appliance is able to read the
user's(myuser@mydomain.onmicrosoft.com) mailbox.
```

Troubleshooting Azure AD

> **Note**: Cisco TAC and Cisco Support are not entitled to troubleshoot customer-side issues with Microsoft Exchange, Microsoft Azure AD, or Office 365.

For customer-side issues with Microsoft Azure AD, you will need to engage Microsoft Support. Please see the "Help + support" option from your Microsoft Azure Dashboard. You may be able to open direct support requests to Microsoft Support from the dashboard.

Appendix A

> **Note**: This is ONLY required if you are NOT utilizing the Client secret for setting up your Azure application.

Building a Public and Private Certificate and Key Pair

> **Tip**: Please have the output saved locally for *$base64Value*, *$base64Thumbprint*, and *$keyid*, as they will be required later in the configuration steps. Please have the .crt and associated .pem of your certificate in an available, local folder on your computer.

> **Note**: If you already have a certificate (x509 format/standard) and private key, skip this section. Be sure you have both CRT and PEM files, as you will need them in the coming sections!

Certificate: Unix/Linux (utilizing openssl)

Values to be created:

Thumbprint
Public Certificate (CRT file)
Private Key (PEM file)

Administrators using Unix/Linux/OS X, for the purpose and execution of the provided script, it is under the assumption that you have OpenSSL installed.

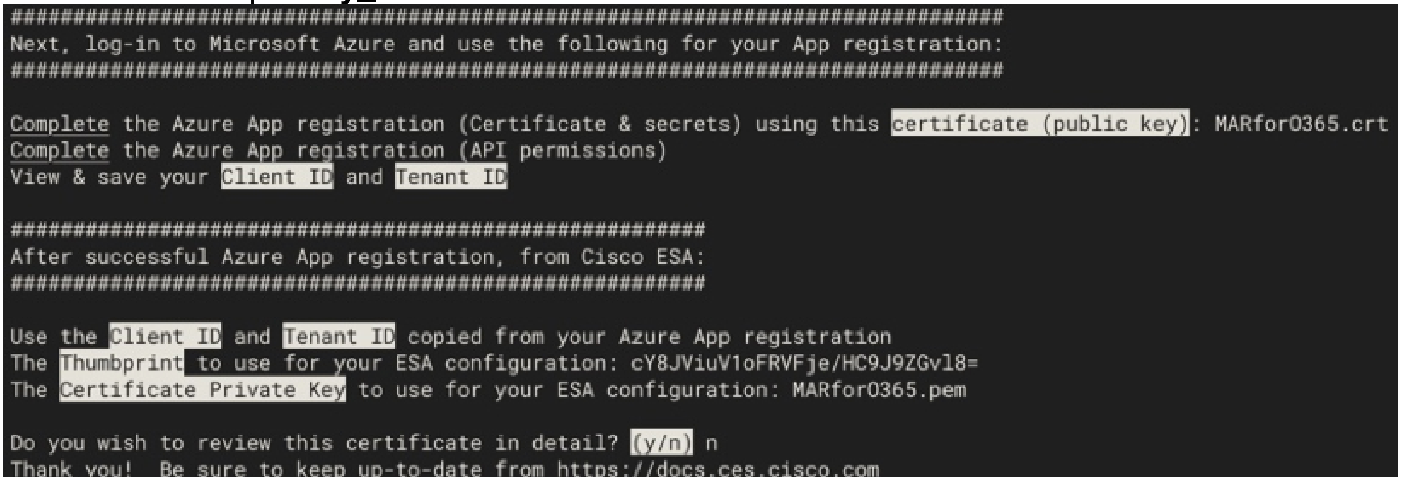
> **Note**: Run the commands 'which openssl' and 'openssl version' in order to verify OpenSSL installation. Install OpenSSL if it is not present!

See the following document for assistance: Azure AD Configuration Script for Cisco Secure Email

From your host (UNIX/Linux/OS X):

1. From a terminal application, text editor (or however you are comfortable creating a shell script), create a script by copying the following: https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.sh

2. Paste the script
3. Be sure that you make the script executable! Run the following command: **chmod u+x my_azure.sh**
4. Run the script: **./my_azure.sh**



```
#################################################################################
Next, log-in to Microsoft Azure and use the following for your App registration:
#################################################################################

Complete the Azure App registration (Certificate & secrets) using this certificate (public key): MARfor0365.crt
Complete the Azure App registration (API permissions)
View & save your Client ID and Tenant ID

########################################################
After successful Azure App registration, from Cisco ESA:
########################################################

Use the Client ID and Tenant ID copied from your Azure App registration
The Thumbprint to use for your ESA configuration: cY8JViuV1oFRVFje/HC9J9ZGvl8=
The Certificate Private Key to use for your ESA configuration: MARfor0365.pem

Do you wish to review this certificate in detail? (y/n) n
Thank you!  Be sure to keep up-to-date from https://docs.ces.cisco.com
```

Figure 13: screen output from my_azure.sh

As you see in Figure 2, the script builds and calls out the **Public Certificate (CER file)**needed for the Azure App registration. The script also calls out the***Thumbprint***and***Certificate Private Key (PEM file)***you will use in the Configuring Cisco Secure Email section.

youhave the needed values to register our application in Microsoft Azure!

[Skip the next section! Please proceed to "Register an Azure app for use with Cisco Secure Email"]

Certificate: Windows (utilizing PowerShell)

For administrators using Windows, you will need to utilize an application or have the knowledge to create a self-signed certificate. This certificate is used in order to create the Microsoft Azure application and associate API communication.

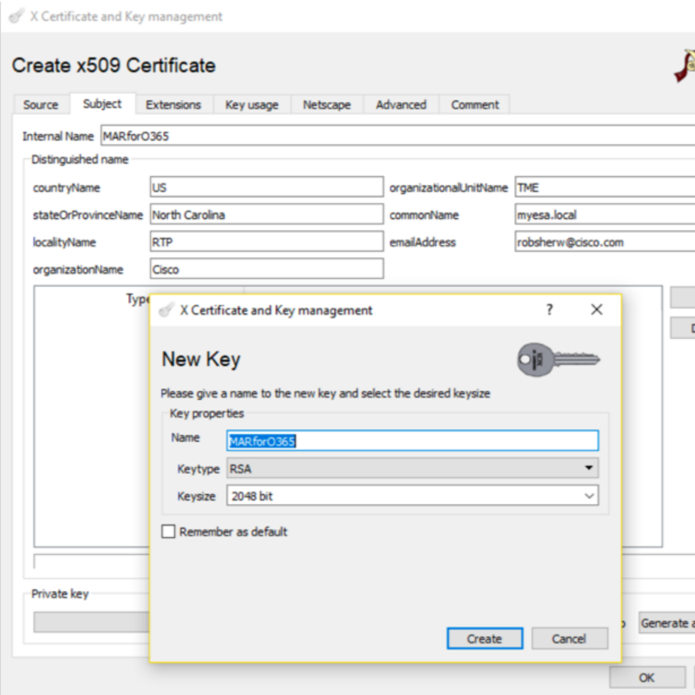
Values to be created:

Thumbprint
Public Certificate (CRT file)
Private Key (PEM file)

Our example for this document to create a self-signed certificate is using XCA (https://hohnstaedt.de/xca/,https://sourceforge.net/projects/xca/).

Note: XCA can be downloaded for Mac, Linux, or Windows.

1. Create a database for your certificate and keys:
   a. Select **File** from the toolbar
   b. Select **New Database**
   c. Create a password for your database
   (you will need it in later steps, so remember it!)
2. Click on the Certificates tab, then click **New Certificate**
3. Click on the Subject tab and fill in the following:
   a. Internal Name
   b. countryName
   c. stateOrProvinceName
   d. localityName
   e. organizationName
   f. organizationalUnitName (OU)
   g. commonName (CN)
   h. emailAddress
4. Click on **Generate a New Key**
5. At the pop-up, verify the provided information (changing as desired):
   a. Name
   b. Keytype: RSA
   c. Keysize: 2048 bit
   d. Click on Create
   e. Acknowledge the "Successfully created the RSA private key 'Name' " pop-up by clicking on **OK**



Internal Name: MARforO365

Distinguished name

countryName: US

stateOrProvinceName: North Carolina

localityName: RTP

organizationName: Cisco

organizationalUnitName: TME

commonName: myesa.local

emailAddress: robsherw@cisco.com

New Key

Please give a name to the new key and select the desired keysize

Key properties

Name: MARforO365

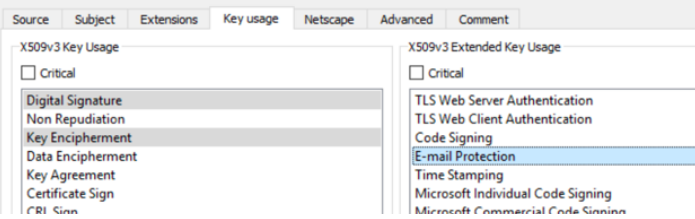
Keytype: RSA

Keysize: 2048 bit

☐ Remember as default

Figure 14: Using XCA (steps 3-5)

6. Click on the Key usage tab and select the following:
   a. Under X509v3 Key Usage:
      Digital Signature, Key Encipherment
   b. Under X509v3 Extended Key Usage:
      E-Mail Protection



X509v3 Key Usage

☐ Critical

Digital Signature
Non Repudiation
Key Encipherment
Data Encipherment
Key Agreement
Certificate Sign
CRL Sign

X509v3 Extended Key Usage

☐ Critical

TLS Web Server Authentication
TLS Web Client Authentication
Code Signing
E-mail Protection
Time Stamping
Microsoft Individual Code Signing
Microsoft Commercial Code Signing

Figure 15: Using XCA (step 6)

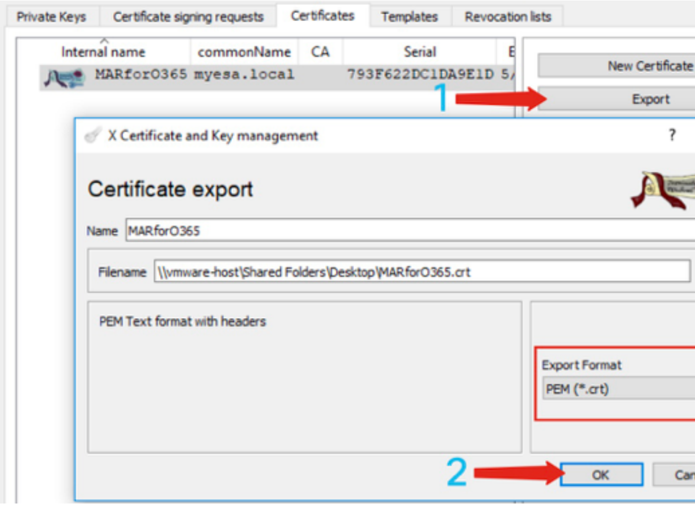
7. Click on **OK** to apply changes to your certificate
8. Acknowledge the "Successfully created the certificate '*Name*' " pop-up by clicking on **OK**

Next, you will want to export both the **Public Certificate (CER file)** and ***Certificate Private Key (PEM file)*** for use in the PowerShell commands up next, and for use in the Configuring Cisco Secure Email steps:

1. Click and highlight the Internal Name of your newly

created certificate.

2. Click **Export**
    a. Set the save directory for ease of access (changing as desired)
    b. Assure the Export Format is set to **PEM (.crt)**
    c. Click **OK**



Internal name	commonName	CA	Serial	E
MARfor0365	myesa.local		793F622DC1DA9E1D	5/

X Certificate and Key management ?

Certificate export

Name: MARfor0365

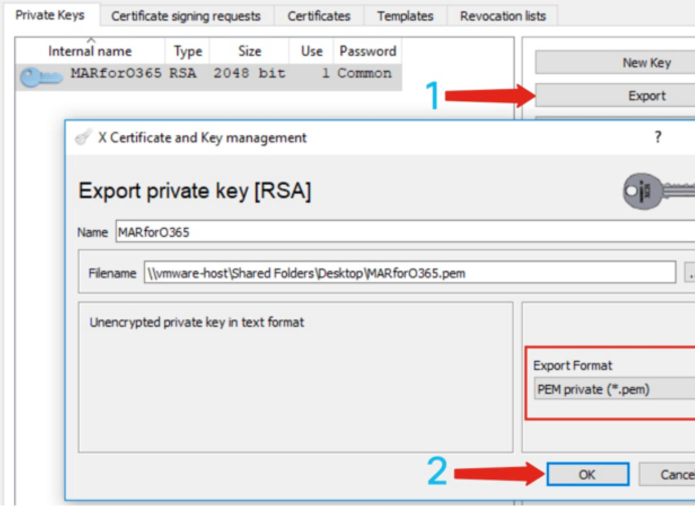
Filename: \\vmware-host\Shared Folders\Desktop\MARfor0365.crt

PEM Text format with headers

Export Format: PEM (*.crt)

Figure 16: Using XCA (export CRT)(steps 1-2)

3. Click on the **Private Keys** tab
4. Click and highlight the Internal Name of your newly created certificate.
5. Click **Export**
    a. Set the save directory for ease of access (changing as desired)
    b. Assure the Export Format is set to **PEM private (.pem)**
    c. Click **OK**
6. Exit and close XCA



Internal name	Type	Size	Use	Password
MARfor0365	RSA	2048 bit	1	Common

X Certificate and Key management ?

Export private key [RSA]

Name: MARfor0365

Filename: \\vmware-host\Shared Folders\Desktop\MARfor0365.pem

Unencrypted private key in text format

Export Format: PEM private (*.pem)

Figure 17: Using XCA (export PEM) (steps 3-5)

Finally, you will take your created certificate and extract the **Thumbprint**, which is needed for Configuring Cisco Secure Email.

1. Using Windows PowerShell, run the following:

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import("c:\Users\joe\Desktop\myCert.crt")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()[Note: “c:\Users\joe\Desktop...” is the location on
your PC where your CRT file is saved.]
```

2. In order to get values for the upcoming steps, saving to a file or to copying to your clipboard:

```
$base64Thumbprint | Out-File c:\Users\joe\Desktop\base64Thumbprint.txt
$base64Thumbprint
```

> **Note**: “c:\Users\joe\Desktop...” is the location on your PC where you are saving the output.

The expected output when running the PowerShell command should like similar to the following:

```
PS C:\Users\joe\Desktop> $base64Thumbprint
75fA1XJEJ4I1ZVFOB2xqkoCIh94=
```

As you see, the PowerShell command calls out the *base64Thumbprint*, which is the **Thumbprint** needed for Cisco Secure Email gateway configuration.

You have also completed creating the **Public Certificate (CER file)** needed for the Azure App registration. And you have created the ***Certificate Private Key (PEM file)***you will use in the Configuring Cisco Secure Email section.

You have the needed values to register your application in Microsoft Azure!

[Please proceed to "Register an Azure app for use with Cisco Secure Email"]

Appendix B

> **Note**: This is ONLY required if you are running AsyncOS 11.x or 12.x for Email on your gateway.

API Permissions (AsyncOS 11.x, 12.x)

On your application pane, in the Manage options...

1. Select **API permissions**
2. Click **+ Add a permission**
3. Scroll down to **Supported legacy APIs** and select **Exchange**
4. Select the below permissions on Delegated permissions: EWS > “EWS.AccessAsUser.All” (Access mailboxes as the signed-in user via Exchange Web Services)Mail > "Mail.Read" (Read user mail)Mail > "Mail.ReadWrite" (Read and write user mail)Mail > "Mail.Send" (Send mail as a user)
5. Scroll to the top of the pane...
6. Select the below permissions on Application permissions: “full_access_as_app” (Use Exchange Web Services with full access to all mailboxes)Mail > "Mail.Read" (Read user

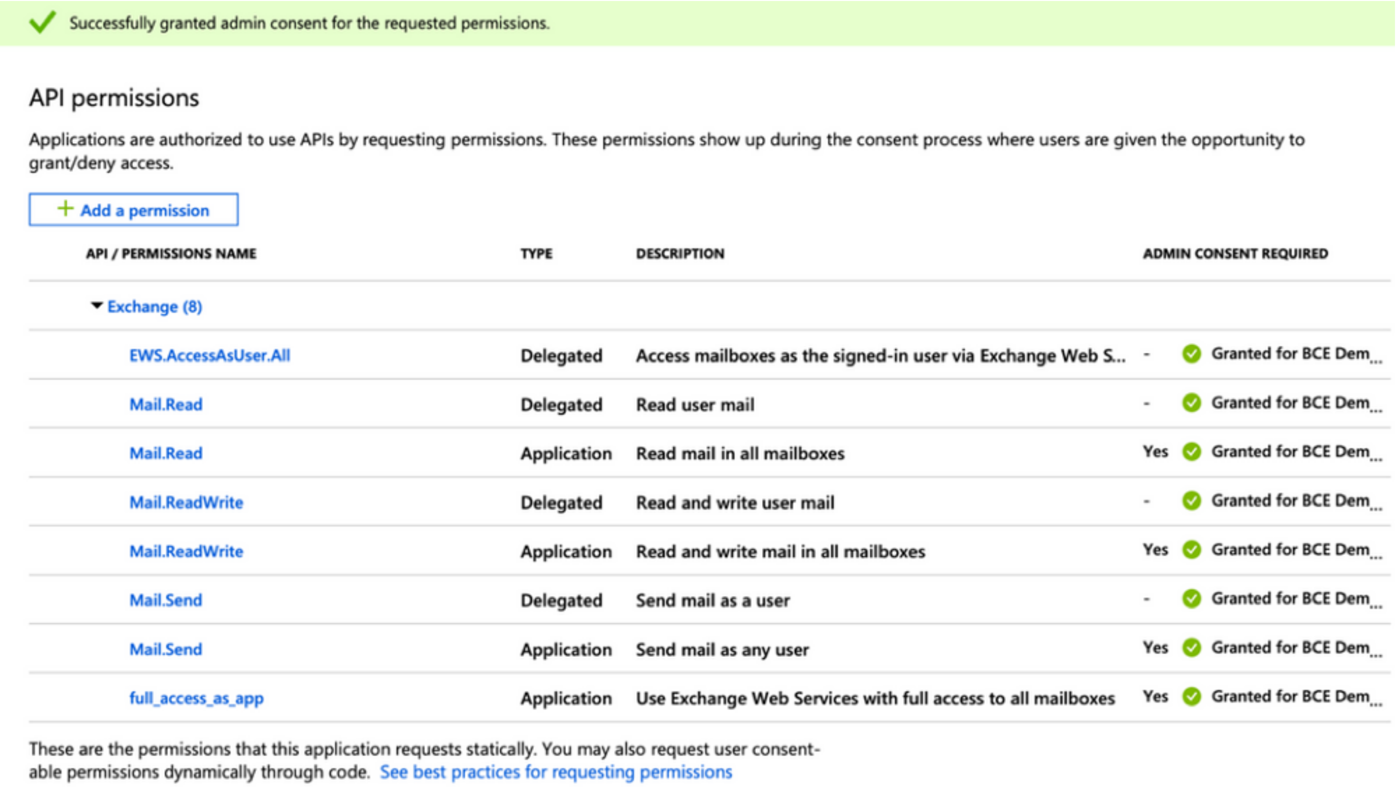
mail)Mail > "Mail.ReadWrite" (Read and write user mail)Mail > "Mail.Send" (Send mail as a user)

7. *Optional*: You will see that Microsoft Graph by default is enabled for “User.Read” permissions; you may leave this as configured or click **Read** and click **Remove permission** to remove this from your API permissions associated with your application.
8. Click **Add permissions** (or **Update permissions**, if Microsoft Graph was already listed)
9. Finally, click on **Grant admin consent for...** to ensure that your new permissions are applied to the application
10. There will be an in-pane pop-up that asks:

    "*Do you want to grant consent for the requested permissions for all accounts in <Azure Name>? This will update any existing admin consent records this application already has to match what is listed below.*"

    Click **Yes**

At this point, you should see a green success message and the "Admin Consent Required" column display Granted, similar to shown:



✓ Successfully granted admin consent for the requested permissions.

API permissions

Applications are authorized to use APIs by requesting permissions. These permissions show up during the consent process where users are given the opportunity to grant/deny access.

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT REQUIRED	
▾ Exchange (8)				
EWS.AccessAsUser.All	Delegated	Access mailboxes as the signed-in user via Exchange Web S...	-	✓ Granted for BCE Dem...
Mail.Read	Delegated	Read user mail	-	✓ Granted for BCE Dem...
Mail.Read	Application	Read mail in all mailboxes	Yes	✓ Granted for BCE Dem...
Mail.ReadWrite	Delegated	Read and write user mail	-	✓ Granted for BCE Dem...
Mail.ReadWrite	Application	Read and write mail in all mailboxes	Yes	✓ Granted for BCE Dem...
Mail.Send	Delegated	Send mail as a user	-	✓ Granted for BCE Dem...
Mail.Send	Application	Send mail as any user	Yes	✓ Granted for BCE Dem...
full_access_as_app	Application	Use Exchange Web Services with full access to all mailboxes	Yes	✓ Granted for BCE Dem...

These are the permissions that this application requests statically. You may also request user consent-able permissions dynamically through code. See best practices for requesting permissions

Figure 18: Microsoft Azure App registration (API permissions required)

[Please proceed to "Register an Azure app for use with Cisco Secure Email"]

Related Information

- Cisco Email Security Appliance - Product Support
- Cisco Email Security Appliance - Release Notes
- Cisco Email Security Appliance - End-User Guide