Cómo configurar Cisco Secure Email Account Settings para la API de Microsoft Azure (Microsoft 365)

Contenido

Introducción

Este documento proporciona un "procedimiento" paso a paso para registrar una nueva aplicación en Microsoft Azure (Azure Active Directory) para generar la ID de cliente, la ID de arrendatario y las credenciales de cliente necesarias y, a continuación, la configuración de la configuración de cuenta en un Cisco Secure Email Gateway o Cloud Gateway. Se requiere la configuración de la configuración de la cuenta y del perfil de cuenta asociado cuando un administrador de correo configura la remediación automática de buzón (MAR) para la protección frente a malware avanzado (AMP) o el filtrado de URL, o bien utiliza la acción Remediar del rastreo de mensajes en Cisco Secure Email and Web Manager o Cisco Secure Gateway/Cloud Gateway.

Flujo del proceso de remediación automática del buzón

Un archivo adjunto (archivo) en el correo electrónico o una URL puede calificarse de malicioso en cualquier momento, incluso después de que haya llegado al buzón de un usuario. AMP en Cisco Secure Email (a través de Cisco Secure Malware Analytics) puede identificar este desarrollo a medida que surgen nuevas informaciones y envía alertas retrospectivas a Cisco Secure Email. Cisco Talos proporciona lo mismo con el análisis de URL, que con AsyncOS 14.2 para Cisco Secure Email Cloud Gateway. Si su organización utiliza Microsoft 365 para administrar buzones de correo, puede configurar Cisco Secure Email para realizar acciones de remediación automática en los mensajes del buzón de correo de un usuario cuando cambien estos veredictos de amenaza.

Cisco Secure Email se comunica de forma segura y directa con Microsoft Azure Active Directory para obtener acceso a los buzones de correo de Microsoft 365. Por ejemplo, si un correo electrónico con un archivo adjunto se procesa a través del gateway y AMP lo analiza, el archivo adjunto (SHA256) se proporciona a AMP para la reputación del archivo. La disposición de AMP se puede marcar como Limpia (paso 5, figura 1) y luego entregarse al buzón de correo Microsoft 365 del destinatario final. Más adelante, la disposición de AMP se cambia a Malintencionada, Cisco Malware Analytics envía una actualización de veredicto retrospectiva (paso 8, figura 1) a *cualquier* gateway que haya procesado ese SHA256 específico. Una vez que la puerta de enlace recibe la actualización de veredicto retrospectivo de Malicious (si está configurada), la puerta de enlace realizará una de las siguientes acciones de Remediación automática de buzón (MAR): Reenviar, Eliminar o Reenviar y Eliminar.

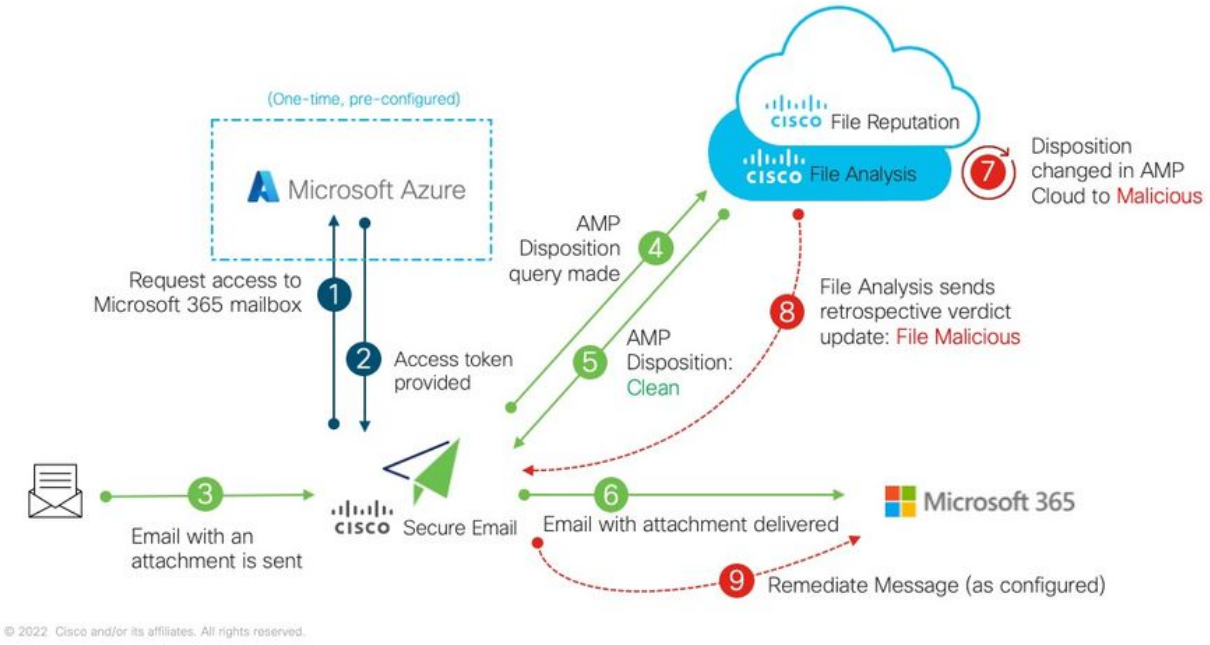


Figura 1: MAR (para AMP) en correo electrónico seguro de Cisco

En esta guía se explica cómo configurar Cisco Secure Email con Microsoft 365 sólo para la remediación automática del buzón de correo. AMP (Reputación de archivos y análisis de archivos) y/o filtrado de URL en el gateway ya deben configurarse. Para obtener más detalles sobre Reputación de archivos y Análisis de archivos, consulte la guía del usuario para la versión de AsyncOS que ha implementado.

Prerequisites

1. Suscripción a la cuenta de Microsoft 365 (asegúrese de que la suscripción a la cuenta de Microsoft 365 incluye acceso a Exchange, como una cuenta Enterprise E3 o Enterprise E5.)

2. Cuenta de administrador de Microsoft Azure y acceso a http://portal.azure.com

3. Tanto las cuentas de Microsoft 365 como las de Microsoft Azure AD están vinculadas correctamente a una dirección de correo electrónico "user@domain.com" activa, y usted puede enviar y recibir correos electrónicos a través de esa dirección de correo electrónico.

Estará creando los siguientes valores para configurar la comunicación de la API de gateway de correo electrónico seguro de Cisco a Microsoft Azure AD:

- **ID del cliente**
- **ID del arrendatario**
- **Secreto de cliente**

  Nota: A partir de AsyncOS 14.0, **Account Settings** permite la configuración mediante un secreto de cliente al crear el Registro de aplicaciones de Microsoft Azure. Este es el método más fácil y preferido.

Opcional: si NO utiliza el secreto de cliente, deberá crear y tener listo:

- **Huella digital**
- **La clave privada (archivo PEM)**

La creación de la huella digital y la clave privada se tratan en el Apéndice de esta guía:

1. Un certificado público (o privado) activo y la clave privada utilizada para firmar el certificado (PEM), o la posibilidad de crear un certificado público (CER) y la capacidad de guardar la clave privada utilizada para firmar el certificado (PEM). Cisco proporciona dos métodos en este documento para hacerlo en función de sus preferencias de administración: Certificado: Unix/Linux/OS X (con OpenSSL)Certificado: Windows (con PowerShell)

2. Acceso a Windows PowerShell, normalmente administrado desde un host o servidor de Windows o acceso a la aplicación Terminal a través de Unix/Linux

Para generar estos valores requeridos, deberá completar los pasos proporcionados en este documento.

Registre una aplicación de Azure para usarla con Cisco Secure Email

Registro de aplicaciones

Inicie sesión en su [Portal de Microsoft Azure](#)

1. Haga clic en **Azure Active Directory** (Figura 2)
2. Haga clic en **Registros de aplicaciones**
3. Haga clic en **+ Nuevo registro**
4. En la página "Registrar una aplicación":
    a. Nombre: **Cisco Secure Email MAR** (o el nombre que elija)
    b. Tipos de cuenta admitidos: **Solo cuentas en este directorio organizativo (Nombre de cuenta)**
    c. Redirigir URI: (opcional)
    [Nota: Puede dejar esto en blanco o no dude en utilizar https://www.cisco.com/sign-on para rellenar]
    d. En la parte inferior de la página, haga clic en **Registro**

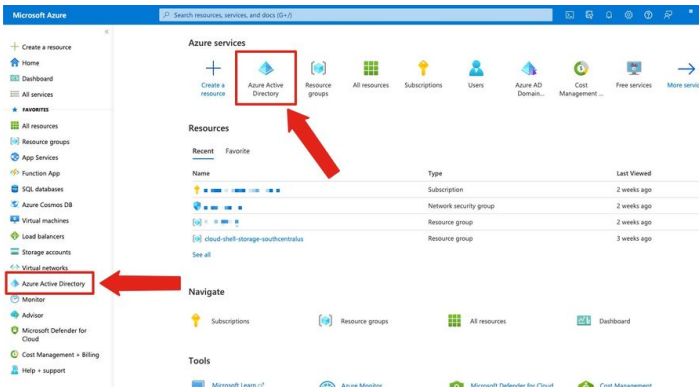


Figura 2: ejemplo de Microsoft Azure Portal

Una vez completados los pasos anteriores, se le presentará la solicitud:

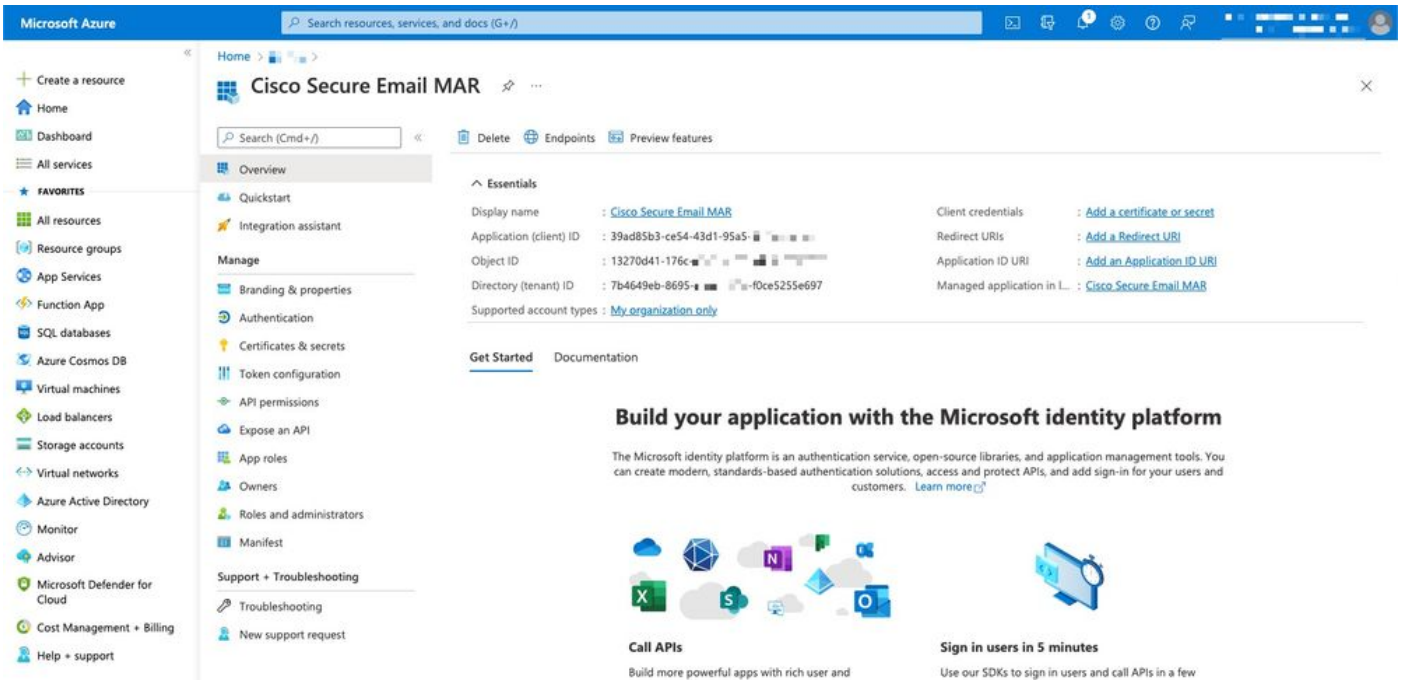


Figura 3: página de la aplicación Microsoft Azure Active Directory

Certificados y secretos

Si ejecuta AsyncOS 14.0 o posterior, Cisco recomienda configurar su aplicación de Azure para utilizar un secreto de cliente. En el panel de la aplicación, en las opciones Administrar:

1. Seleccionar **certificados y secretos**

2. En la sección ***Secretos de cliente***, haga clic en **+ Nuevo secreto de cliente**

3. Agregue una descripción para ayudar a identificar para qué sirve este secreto de cliente, por ejemplo, "Solución de correo electrónico seguro de Cisco"

4. Seleccione un período de vencimiento

5. Haga clic en Add (Agregar)

6. Desplácese a la derecha del valor generado y haga clic en el icono **Copiar al portapapeles**

7. Guarde este valor en sus notas, anótelo como "secreto de cliente"

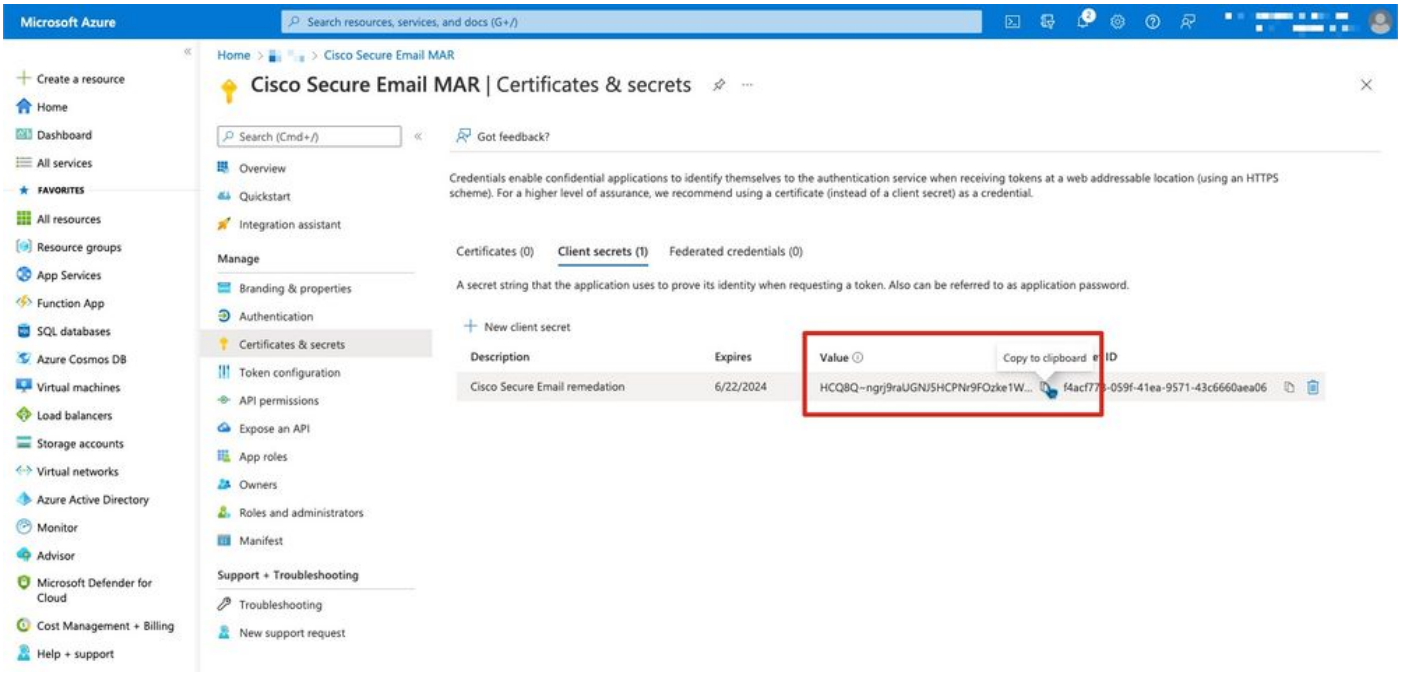


Figura 4: ejemplo de secreto de cliente de creación de Microsoft Azure

> **Nota:** Una vez que haya salido de la sesión activa de Microsoft Azure, el valor del secreto de cliente que acaba de generar será ***. Si no registra y protege el valor antes de salir, deberá volver a crear el secreto del cliente para ver el resultado del texto sin cifrar.

Opcional: si no está configurando su aplicación de Azure con un secreto de cliente, configure su aplicación de Azure para utilizar su certificado. En el panel de la aplicación, en las opciones Administrar:

1. Seleccionar **certificados y secretos**
2. Haga clic en **Cargar certificado**
3. Seleccione el archivo CRT (tal y como se creó anteriormente)
4. Haga clic en Add (Agregar)

Permisos de API

Nota: A partir de AsyncOS 13.0 para Email Security, los permisos de la API para Microsoft Azure

para la comunicación de correo electrónico seguro de Cisco han cambiado de utilizar Microsoft Exchange a Microsoft Graph. Si ya ha configurado MAR y está actualizando su gateway Cisco Secure Email existente a AsyncOS 13.0, puede simplemente actualizar/agregar los nuevos permisos de API. (Si ejecuta una versión anterior de AsyncOS, 11.x o 12.x, consulte el Apéndice B antes de continuar.)

En el panel de la aplicación, en las opciones Administrar:

1. Seleccionar **permisos de API**
2. Haga clic **+ Agregar un permiso**
3. Seleccionar **Microsoft Graph**
4. Seleccione los permisos siguientes en ***Permisos de aplicación***: Correo > "Correo.Lectura" (Leer correo en todos los buzones de correo)Mail > "Mail.ReadWrite" (Leer y escribir correo en todos los buzones)Mail > "Mail.Send" (Enviar correo como cualquier usuario)Directorio > "Directorio.Leer.Todos" (Leer datos del directorio) [*Opcional: Si utiliza la sincronización LDAP Connector/LDAP, active. Si no es así, esto no es obligatorio.]
5. *Opcional:* Verá que Microsoft Graph está habilitado de forma predeterminada para los permisos "User.Read"; puede dejar esto tal como está configurado o hacer clic en **Leer** y haga clic en **Quitar permiso** para quitar esto de los permisos de API asociados a su aplicación.
6. Haga clic en **Agregar permisos** (o en **Actualizar permisos**, si Microsoft Graph ya estaba en la lista)
7. Por último, haga clic en **Conceder consentimiento administrativo para...** para asegurarse de que los nuevos permisos se aplican a la aplicación
8. Habrá una ventana emergente en el panel que preguntará:
   "*¿Desea conceder el consentimiento para los permisos solicitados para todas las cuentas de <Azure Name>? Esto actualizará cualquier registro de consentimiento de administrador existente que esta aplicación ya tenga para coincidir con lo que se enumera a continuación*".

   Haga clic en **Sí**

En este punto, debería ver un mensaje de confirmación de color verde y la columna "Admin Consent Required" (Consentimiento administrativo requerido) aparece Granted (Concedido).

Obtención de ID de cliente e ID de arrendatario

En el panel de la aplicación, en las opciones Administrar:

1. Haga clic en **Descripción general**
2. Sitúe el ratón sobre la derecha de la ID de la aplicación (Cliente) y haga clic en el icono **Copiar al Portapapeles**
3. Guarde este valor en sus notas, anótelo como "ID de cliente"
4. Desplácese a la derecha de la ID de directorio (arrendatario) y haga clic en el icono **Copiar al portapapeles**
5. Guarde este valor en sus notas, anótelo como "ID de arrendatario"

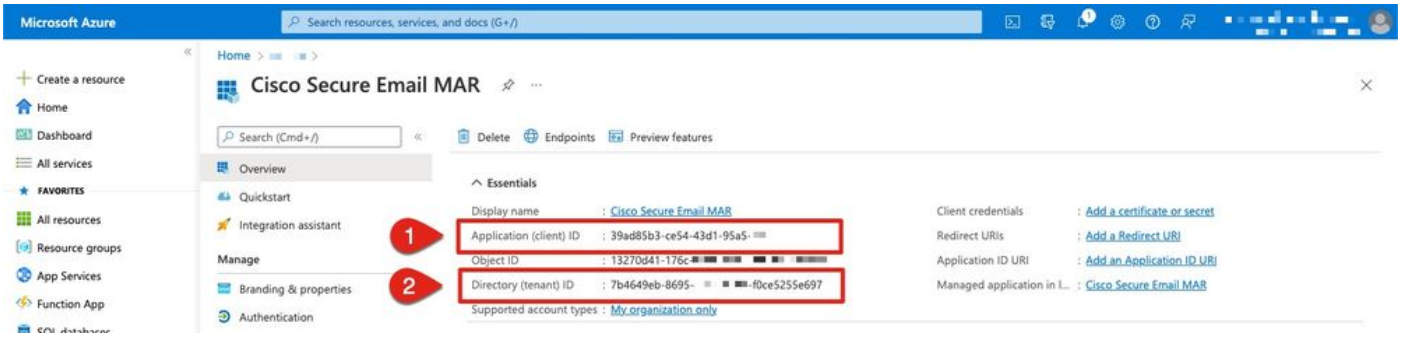


Figura 5: Microsoft Azure... Ejemplo de ID de cliente, ID de arrendatario

Configuración de Cisco Secure Email Gateway/Cloud Gateway

En este momento, debe preparar y guardar los siguientes valores en sus notas:

- **ID del cliente**
- **ID del arrendatario**
- **Secreto de cliente**

Opcional, si no utiliza Client secret:

- **Huella digital**
- **La clave privada (archivo PEM)**

Está preparado para utilizar los valores creados a partir de las notas y configurar la configuración de la cuenta en el gateway de correo electrónico seguro de Cisco.

Crear perfil de cuenta

1. Inicie sesión en su gateway
2. Vaya a **Administración del sistema > Configuración de la cuenta** Nota: Si está ejecutando una versión anterior a AsyncOS 13.x, esto será **Administración del sistema > Configuración del buzón**
3. Haga clic en **Enable (Activar)**
4. Haga clic en la casilla de verificación Enable Account Settings (Activar configuración de cuenta) y haga clic en **Submit (Enviar)**
5. Haga clic en **Crear perfil de cuenta**
6. Proporcione un nombre de perfil y una descripción (algo que describirá de forma única su cuenta si tiene varios dominios)
7. Al definir una conexión de Microsoft 365, deje el tipo de perfil como **Office 365 / Hybrid (API de gráficos)**
8. Introduzca su **ID de cliente**
9. Introduzca su **ID de arrendatario**
10. Para las credenciales del cliente, realice una de las siguientes acciones, como se ha

configurado en Azure: Haga clic en **Secreto de cliente** y pegue en su secreto de cliente configurado, o...Haga clic en **Certificado de cliente** e introduzca su huella digital y proporcione su PEM haciendo clic en "Elegir archivo"

11. Haga clic en Submit (Enviar)
12. Haga clic en **Registrar cambios** en la parte superior derecha de la interfaz de usuario
13. Introduzca en cualquier comentario y complete los cambios de configuración haciendo clic en **Registrar cambios**

Comprobar conexión

El siguiente paso es solamente verificar la conexión API de su gateway de Cisco Secure Email a Microsoft Azure:

1. En la misma página Detalles de la cuenta, haga clic en **Probar conexión**
2. Introduzca una dirección de correo electrónico válida para el dominio administrado en su cuenta Microsoft 365
3. Haga clic en **Probar conexión**
4. Debe recibir un mensaje de confirmación (figura 6)
5. Haga clic en **Finalizado** para finalizar

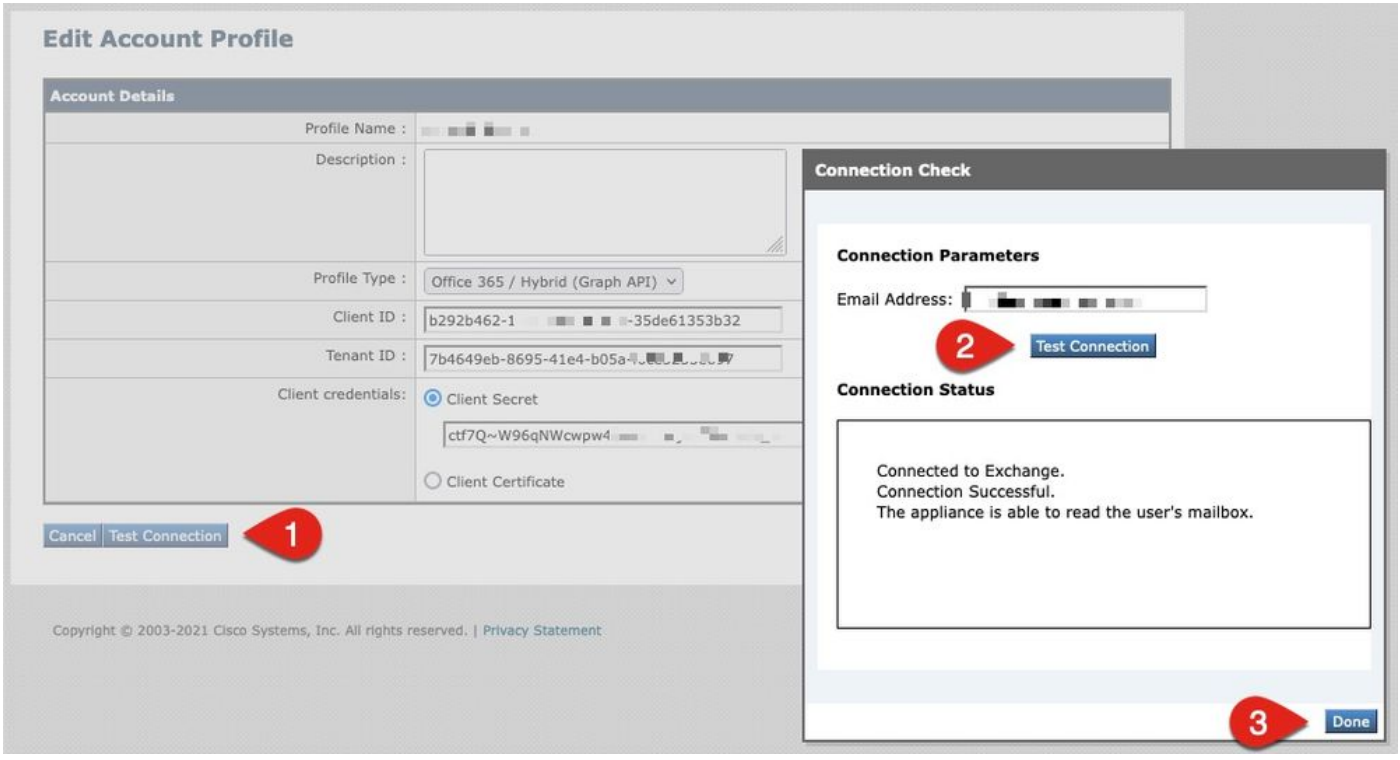


Figura 6: Ejemplo de verificación de conexión/perfil de cuenta

6. En la sección *Asignación de dominio*, haga clic en **Crear asignación de dominio**

7. Introduzca los nombres de dominio asociados a la cuenta de Microsoft 365 para la que acaba de validar la conexión de la API

A continuación se muestra una lista de formatos de dominio válidos que se pueden utilizar para asignar un perfil de buzón de correo:

- El dominio puede ser la palabra clave especial 'ALL' para que coincida con todos los dominios para crear una asignación de dominio predeterminada.

- Nombres de dominio como 'example.com' - Coincide con cualquier dirección con este dominio.

- Nombres de dominio parciales como '@.parcial.example.com' - Coincide con cualquier dirección que termine con este dominio

- Se pueden ingresar varios dominios mediante una lista de dominios separada por comas.

8. Haga clic en Submit (Enviar)

9. Haga clic en **Registrar cambios** en la parte superior derecha de la interfaz de usuario

10. Introduzca en cualquier comentario y complete los cambios de configuración haciendo clic en **Registrar cambios**

Habilitar la solución automática de correo (MAR) para la protección frente a malware avanzado en la política de correo

Complete este paso para habilitar MAR en la configuración de AMP para las políticas de correo.

1. Vaya a **Políticas de correo > Políticas de correo entrante**
2. Haga clic en los parámetros de la columna Protección frente a malware avanzado para el nombre de política que desea configurar (por ejemplo, Figura 7):

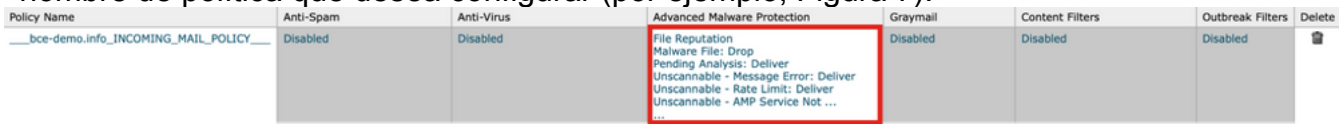


Figura 7: Habilitar MAR (políticas de correo entrante)

3. Desplácese hasta la parte inferior de la página
4. Haga clic en la casilla de verificación Enable Mailbox Auto Remediation (MAR)
5. Seleccione una de las siguientes acciones que desea realizar para MAR (por ejemplo, figura 8): Reenviar a: <*introduzca una dirección de correo electrónico*>EliminarReenviar a: <*ingrese en dirección de correo electrónico*> y Delete

Figura 8: Ejemplo de configuración Enable MAR for AMP

6. Haga clic en Submit (Enviar)
7. Haga clic en **Registrar cambios** en la parte superior derecha de la interfaz de usuario
8. Introduzca en cualquier comentario y complete los cambios de configuración haciendo clic en **Registrar cambios**

Habilitar la remediación automática del buzón de correo (MAR) para el filtrado de URL

A partir de AsyncOS 14.2 para Cisco Secure Email Cloud Gateway, el filtrado de URL ahora incluye veredicto retrospectivo de URL y remediación de URL.

1. Vaya a **Servicios de seguridad > Filtrado de URL**
2. Si aún no ha configurado el filtrado de URL, haga clic en **Enable (Activar)**
3. Haga clic en la casilla de verificación "Habilitar categoría de URL y filtros de reputación".
4. *Parámetros avanzados* con la configuración predeterminada
5. Haga clic en Submit (Enviar)

El filtrado de URL debe tener un aspecto similar al siguiente:

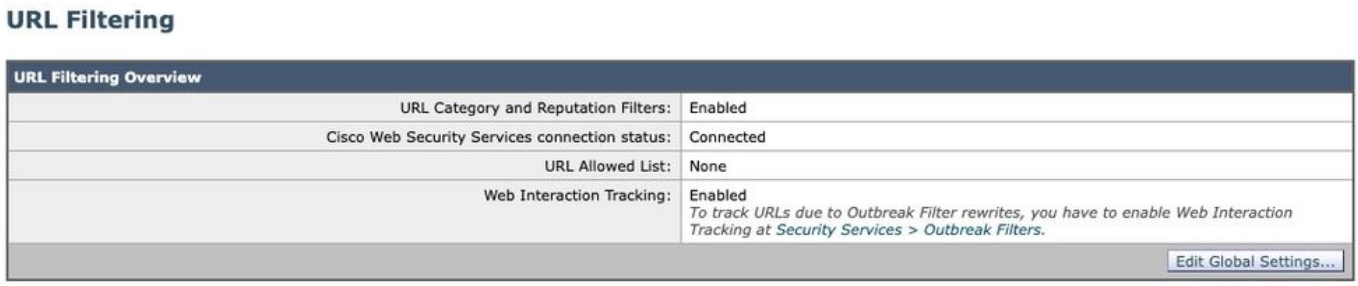


Figura 9: Ejemplo de Filtrado de URL después de habilitar

Para ver la retrospección de URL con filtrado de URL, realice lo siguiente o tenga abierto un caso de soporte para que Cisco lo realice:

```
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
```

Una vez completada, actualice la interfaz de usuario en la página Filtrado de URL y ahora debería ver algo similar a lo siguiente:

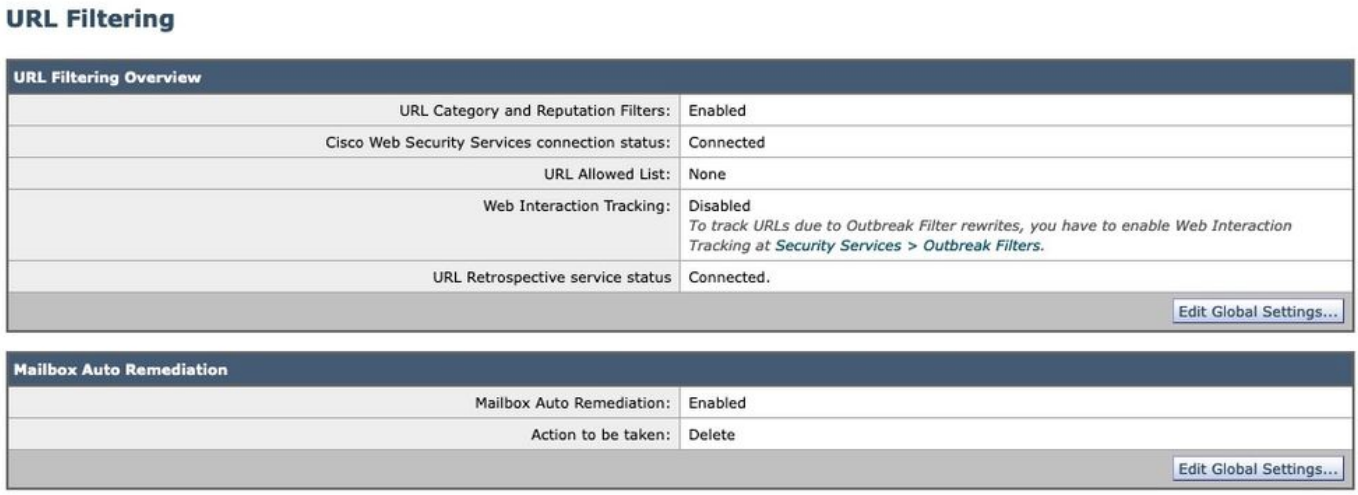


Figura 10: Filtrado de URL (AsyncOS 14.2 para Cisco Secure Email Cloud Gateway)

La protección de URL ya está lista para realizar acciones correctivas cuando un veredicto cambia la puntuación. Para obtener más información, consulte Protección contra URL malintencionadas

o no deseadas en la Guía del usuario para AsyncOS 14.2 para Cisco Secure Email Cloud Gateway.

Configuración completada

En este momento, Cisco Secure Email está preparado para evaluar continuamente las amenazas emergentes a medida que se dispone de nueva información y le notifica los archivos que se consideran amenazas después de que hayan entrado en la red.

Cuando se produce un veredicto retrospectivo a partir de Análisis de archivos (Cisco Secure Malware Analytics), se envía un mensaje de información al administrador de Email Security (si está configurado). Ejemplo:

```
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
```

La Remediación automática del buzón se tomará como se configuró si se comparó con la política de correo.

Ejemplos de informe de reparación automática de buzón

Los informes de cualquier SHA256 que se haya solucionado se incluirán en el informe de remediación automática de buzón de correo disponible tanto en el gateway de correo electrónico seguro de Cisco como en Cisco Secure Email and Web Manager.

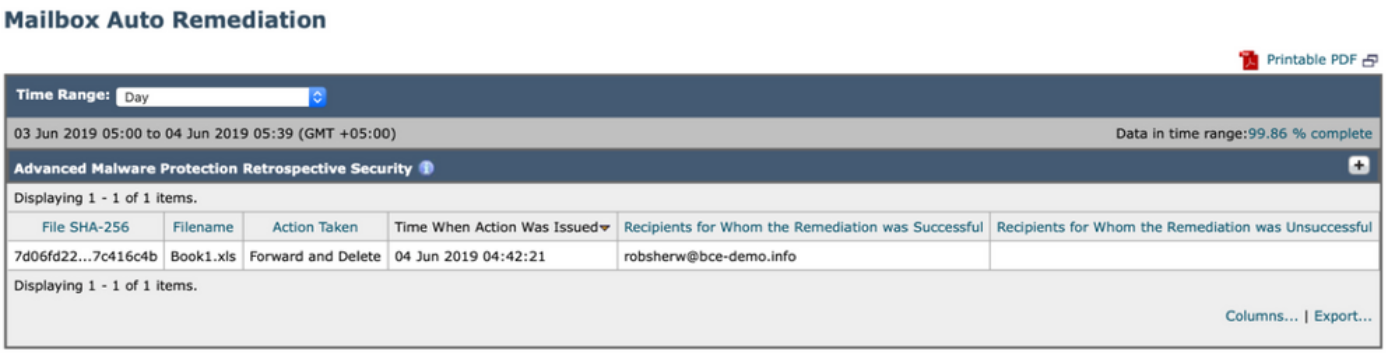


Figura 11: Informe de remediación automática de buzón (interfaz de usuario antigua)

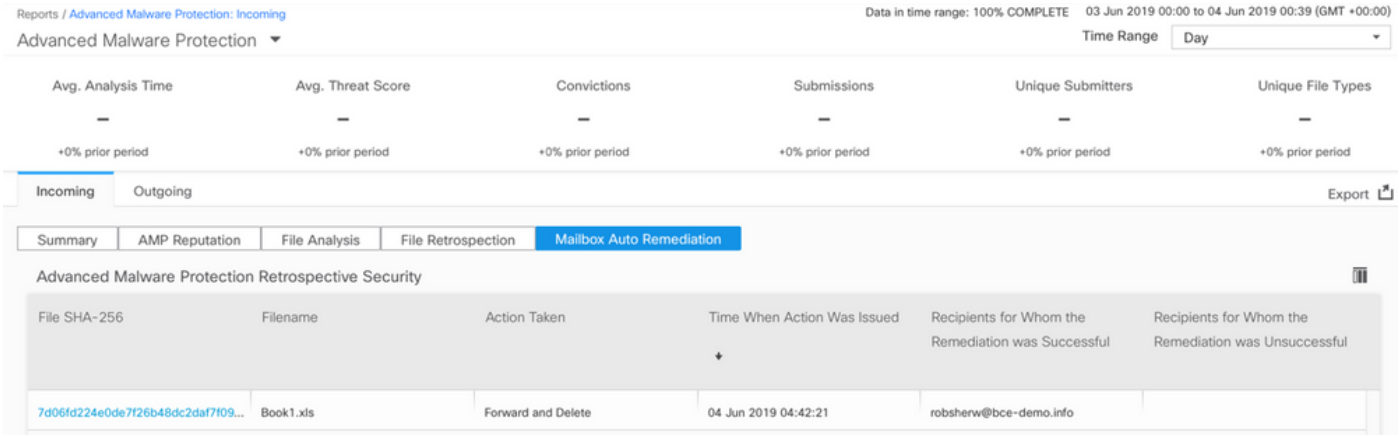


Figura 12: Informe de remediación automática de buzón de correo (NG UI)

Registro de Remediación Automática de Buzón

La Remediación automática del buzón tiene un registro individual, "mar". Los registros de Remediación automática del buzón contendrán toda la actividad de comunicación entre el gateway de correo electrónico seguro de Cisco y Microsoft Azure, Microsoft 365.

Un ejemplo de los registros de mar:

```
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.
```

Resolución de problemas de Cisco Secure Email Gateway

Si no ve resultados satisfactorios para la prueba de estado de la conexión, es posible que desee revisar el registro de la aplicación realizado desde Microsoft Azure AD.

Desde el gateway de correo electrónico seguro de Cisco, configure los registros de MAR en el nivel de 'seguimiento' y vuelva a probar la conexión.

Para conexiones fallidas, los registros pueden mostrar similares a:

```
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
```

Confirme la ID de la aplicación, la ID del directorio (que es la misma que la ID del arrendatario) u otros identificadores asociados del registro con su aplicación en Azure AD. Si no está seguro de los valores, elimine la aplicación del portal de Azure AD y vuelva a iniciarla.

Para una conexión correcta, los registros deben ser similares a:

```
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.
```

Solución de problemas de Azure AD

Nota: Cisco TAC y Cisco Support no tienen derecho a resolver problemas del lado del cliente con Microsoft Exchange, Microsoft Azure AD o Office 365.

Para los problemas del lado del cliente con Microsoft Azure AD, deberá ponerse en contacto con el soporte técnico de Microsoft. Consulte la opción "Ayuda + soporte" desde su panel de Microsoft Azure. Es posible que pueda abrir solicitudes de soporte directo al soporte técnico de Microsoft desde el panel.

Apéndice A

Nota: Esto SOLO es necesario si NO utiliza el secreto de cliente para configurar su aplicación de Azure.

Creación de un par de claves y un certificado público y privado

Sugerencia: Por favor, tenga el resultado guardado localmente para *$base64Value*, *$base64Thumbprint* y *$keyid*, **ya que se necesitarán más adelante en los pasos de configuración.** Tenga el .crt y el .pem asociado del certificado en una carpeta local disponible del equipo.

Nota: Si ya tiene un certificado (formato x509/estándar) y una clave privada, omita esta sección. Asegúrese de que tiene los archivos CRT y PEM, ya que los necesitará en las secciones siguientes.

Certificado: Unix/Linux (utilizando openssl)

Valores a crear:
Thumbprint
Certificado público (archivo CRT)
Clave privada (archivo PEM)

Los administradores que utilizan Unix/Linux/OS X, para el propósito y la ejecución de la secuencia de comandos proporcionada, se asume que tiene instalado OpenSSL.

> **Nota:** Ejecute los comandos 'what openssl' y 'openssl version' para verificar la instalación de OpenSSL. Instale OpenSSL si no está presente.

Consulte el siguiente documento para obtener asistencia: Azure AD Configuration Script para Cisco Secure Email

Desde su host (UNIX/Linux/OS X):

1. Desde una aplicación terminal, el editor de texto (o como sea que se sienta cómodo creando un script de shell), cree un script copiando lo siguiente: https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.sh
2. Pegar el script
3. ¡Asegúrese de que el script sea ejecutable! Ejecute el siguiente comando: **chmod u+x my_azure.sh**
4. Ejecute el 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): MARforO365.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: MARforO365.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
```

Figura 13: salida de pantalla de my_azure.sh

Como puede ver en la Figura 2, el script genera y llama al **Certificado Público (archivo CER)** necesario para el registro de la aplicación Azure. La secuencia de comandos también indica el***Huella digital*** y ***Clave privada de certificado (archivo PEM)*** se utilizará en la sección Configuración de Cisco Secure Email.

tiene los valores necesarios para registrar nuestra aplicación en Microsoft Azure.

[Omita la siguiente sección. Proceda a "Registrar una aplicación de Azure para utilizarla con Cisco

Secure Email"]

Certificado: Windows (con PowerShell)

Para los administradores que utilizan Windows, deberá utilizar una aplicación o disponer de los conocimientos necesarios para crear un certificado autofirmado. Este certificado se utiliza para crear la aplicación de Microsoft Azure y asociar la comunicación API.

Valores a crear:
Thumbprint
Certificado público (archivo CRT)
Clave privada (archivo PEM)

Nuestro ejemplo para que este documento cree un certificado autofirmado es el uso de XCA (https://hohnstaedt.de/xca/, https://sourceforge.net/projects/xca/).

Nota: XCA se puede descargar para Mac, Linux o Windows.

1. Cree una base de datos para el certificado y las claves:
   a. Seleccione **Archivo** de la barra de herramientas
   b. Seleccionar **nueva base de datos**
   c. Crear una contraseña para la base de datos (lo necesitará en pasos posteriores, ¡recuérdelo!)
2. Haga clic en la ficha Certificados y, a continuación, haga clic en **Nuevo certificado**
3. Haga clic en la ficha Asunto y rellene los siguientes campos:
   a. Nombre interno
   b. countryName
   c. stateOrOwnerName
   d. localityName
   e. organizationName
   f. OrganizationUnitName (OU)
   g CommonName (CN)
   h. emailAddress
4. Haga clic en **Generar una nueva clave**
5. En la ventana emergente, verifique la información proporcionada (cambio según lo deseado):
   a. Nombre
   b. Tipo de clave: RSA
   c. Tamaño de la clave: 2048 bit

d. Haga clic en Create (Crear)
e. Confirme la ventana emergente "Creado correctamente la clave privada RSA 'Name'" haciendo clic en **Aceptar**

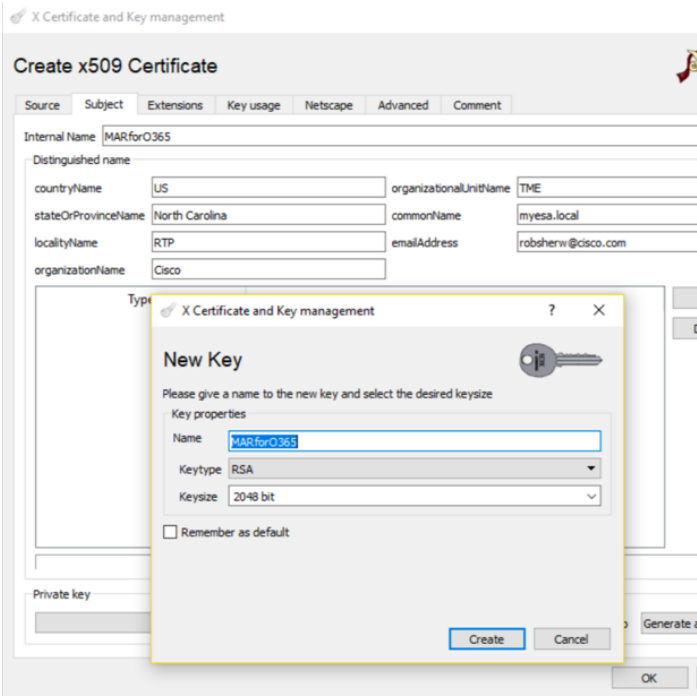


Figura 14: Uso de XCA (pasos 3-5)

6. Haga clic en la ficha Key usage (Uso de claves) y seleccione lo siguiente:
   a. En Uso de claves X509v3:
      Firma digital, inscripción clave
   b. En Uso de clave ampliada X509v3:
      Protección de correo electrónico
7. Haga clic en **Aceptar** para aplicar cambios a su certificado
8. Acepte la ventana emergente "Creado correctamente el certificado '*Nombre*'" haciendo clic en **Aceptar**

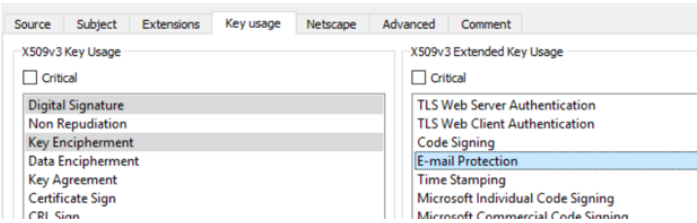
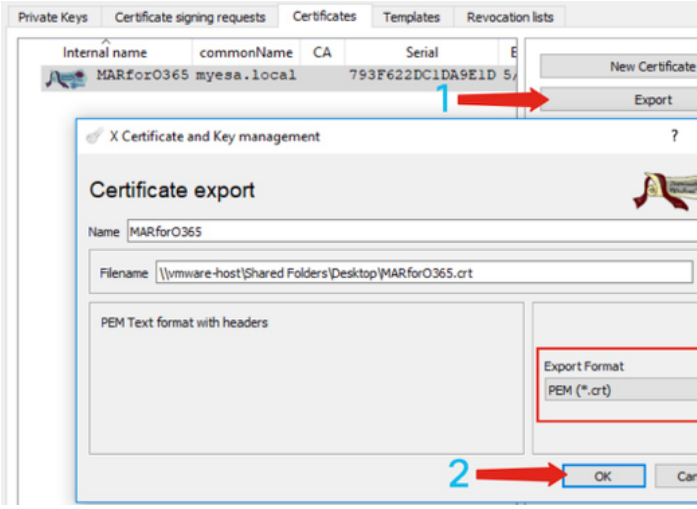


Figura 15: Uso de XCA (paso 6)

A continuación, desea exportar tanto el **Certificado Público (archivo CER)** como la ***Clave Privada de Certificado (archivo PEM)*** para su uso en los comandos de PowerShell hacia arriba y para su uso en los pasos de Configuración de Cisco Secure Email:

1. Haga clic y resalte el nombre interno del certificado recién creado.
2. Haga clic en **Exportar**
   a. Configure el directorio de almacenamiento para facilitar el acceso (cambiando según lo desee)
   b. Asegúrese de que el formato de exportación esté establecido en **PEM (.crt)**
   c. Haga clic en OK (Aceptar).



3. Haga clic en la pestaña **Private Keys**
4. Haga clic y resalte el nombre interno del certificado recién creado.
5. Haga clic en **Exportar**
    a. Configure el directorio de almacenamiento para facilitar el acceso (cambiando según lo desee)
    b. Asegúrese de que el formato de exportación esté configurado en **PEM private (.pem)**
    c. Haga clic en OK (Aceptar).
6. Salir y cerrar XCA

Figura 16: Uso de XCA (exportar CRT)(pasos 1-2)

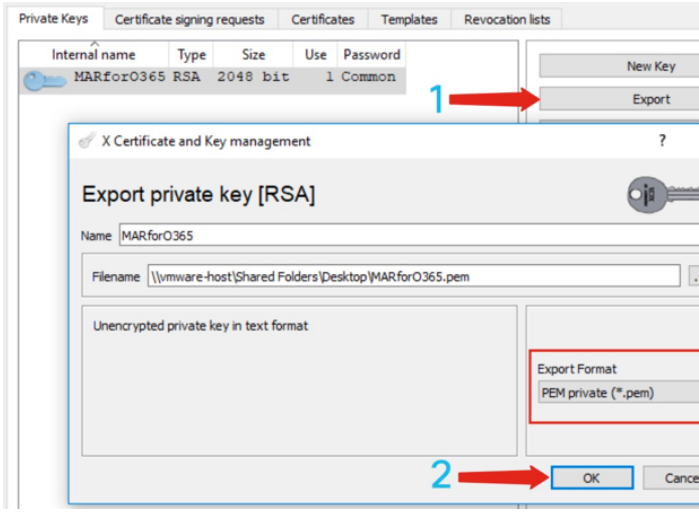


Figura 17: Uso de XCA (exportar PEM) (pasos 3-5)

Por último, tomará el certificado creado y extraerá la **huella digital**, que es necesaria para configurar Cisco Secure Email.

1. Con Windows PowerShell, ejecute lo siguiente:

```
$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. Para obtener valores para los próximos pasos, guarde en un archivo o copie en el portapapeles:

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

Nota: “c:\Users\joe\Desktop..." es la ubicación del PC en la que se guarda la salida.

La salida esperada al ejecutar el comando PowerShell debe ser similar a la siguiente:

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

Como puede ver, el comando de PowerShell llama a la *huella digital base64Thumbprint*, que es la **huella digital** necesaria para la configuración del gateway de correo electrónico seguro de Cisco.

También ha terminado de crear el **Certificado público (archivo CER)** necesario para el registro de la aplicación de Azure. Y ha creado la ***clave privada de certificado (archivo PEM)*** que utilizará en la sección Configuración de Cisco Secure Email.

Tiene los valores necesarios para registrar su aplicación en Microsoft Azure.

[Proceda a "Registrar una aplicación de Azure para usarla con Cisco Secure Email"]

Apéndice B

> **Nota**: Esto SOLO es necesario si ejecuta AsyncOS 11.x o 12.x para el correo electrónico en su gateway.

Permisos de API (AsyncOS 11.x, 12.x)

En el panel de aplicaciones, en las opciones Administrar...

1. Seleccionar **permisos de API**
2. Haga clic **+ Agregar un permiso**
3. Desplácese hacia abajo hasta **API antiguas admitidas** y seleccione **Exchange**
4. Seleccione los permisos siguientes en Permisos delegados: EWS > "EWS.AccessAsUser.All" (Acceda a los buzones de correo como usuario que ha iniciado sesión a través de Exchange Web Services)Mail > "Mail.Read" (Leer correo de usuario)Mail > "Mail.ReadWrite" (correo de usuario de lectura y escritura)Mail > "Mail.Send" (Enviar correo como usuario)
5. Desplácese hasta la parte superior del panel...
6. Seleccione los permisos siguientes en Permisos de aplicación: "full_access_as_app" (utilice Exchange Web Services con acceso completo a todos los buzones de correo)Mail > "Mail.Read" (Leer correo de usuario)Mail > "Mail.ReadWrite" (correo de usuario de lectura y escritura)Mail > "Mail.Send" (Enviar correo como usuario)
7. *Opcional:* Verá que Microsoft Graph está habilitado de forma predeterminada para los permisos "User.Read"; puede dejar esto tal como está configurado o hacer clic en **Leer** y haga clic en **Quitar permiso** para quitar esto de los permisos de API asociados a su aplicación.
8. Haga clic en **Agregar permisos** (o en **Actualizar permisos**, si Microsoft Graph ya estaba en la lista)
9. Por último, haga clic en **Conceder consentimiento administrativo para...** para asegurarse de

que los nuevos permisos se aplican a la aplicación

10. Habrá una ventana emergente en el panel que preguntará:

"*¿Desea conceder el consentimiento para los permisos solicitados para todas las cuentas de <Azure Name>? Esto actualizará cualquier registro de consentimiento de administrador existente que esta aplicación ya tenga para coincidir con lo que se enumera a continuación*".

Haga clic en **Sí**

En este punto, debería ver un mensaje de confirmación de color verde y la columna "Consentimiento de administrador requerido" aparece Granted, similar a la que se muestra:

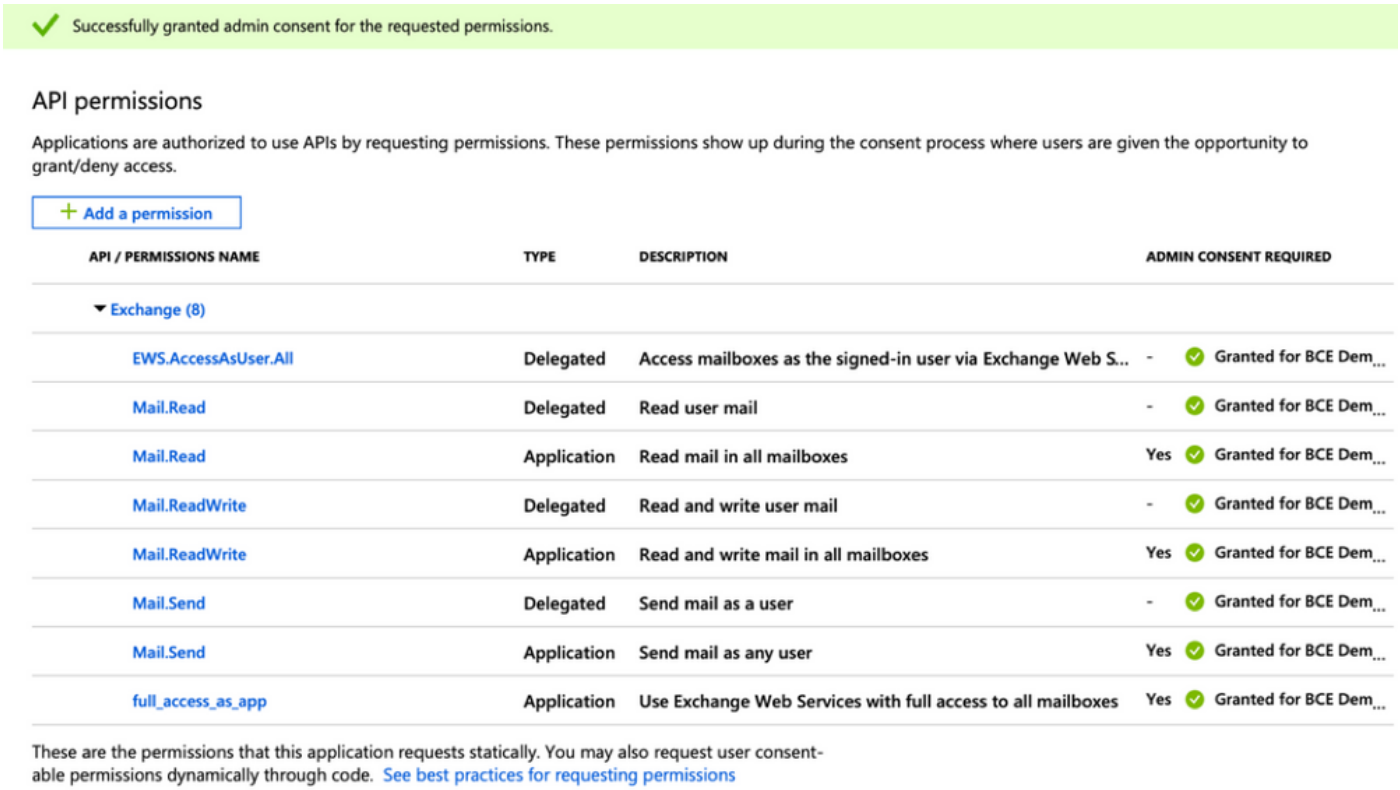


Figura 18: Registro de aplicaciones de Microsoft Azure (se requieren permisos de API)

[Proceda a "Registrar una aplicación de Azure para usarla con Cisco Secure Email"]

Información Relacionada

- Dispositivo de seguridad Cisco Email Security Appliance - Asistencia para productos
- Cisco Email Security Appliance - Notas de la versión
- Dispositivo de seguridad Cisco Email Security Appliance - Guía del usuario final