

Cómo configurar el Microsoft Azure AD y la oficina 365 para el uso en el ESA

Contenido

[Introducción](#)

[prerrequisitos](#)

[Valores del certificado de la configuración](#)

[Microsoft Azure AD de la configuración](#)

[Cree la aplicación de Web de encargo](#)

[Configure la aplicación de Web de encargo](#)

[Cree el evidente](#)

[Encontrar al arrendatario ID](#)

[Revisión final de los valores que se guardarán](#)

[Configuraciones del buzón de la configuración en el ESA](#)

Introducción

Este documento describe cómo poner y configurar el Microsoft Azure AD y la oficina 365 para trabajar con el dispositivo de seguridad del correo electrónico de Cisco (ESA).

Prerrequisitos

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- AsyncOS para la Seguridad 9.9.5-039 (Bellagio) del correo electrónico, o más nuevo.

Este documento también requiere el siguiente:

- Suscripción de la cuenta de la [oficina 365](#) (asegurese por favor que su [suscripción de la cuenta de la oficina 365](#) incluye el acceso para enviar por correo electrónico, por ejemplo una cuenta de la empresa E3 o de la empresa E5.)
- Cuenta del [Microsoft Azure](#)
- Las cuentas de la oficina 365 y del Microsoft Azure AD se atan correctamente a una dirección de correo electrónico activa de *user@domain.com*, y usted puede enviar y recibir los correos electrónicos vía ese dominio y cuenta.
- Acceso a Windows PowerShell, administrado generalmente de un Servidor Windows.
- Público activo del dominio/certificado privado y la clave privada usada para firmar el certificado, o la capacidad de crear un certificado público/privado y capacidad de salvar la clave privada usada para firmar el certificado.

Valores del certificado de la configuración

Inicie sesión a Windows, y con PowerShell complete los siguientes comandos de asociar y de

obtener *\$keyid*, *\$base64Thumbprint*, y *\$base64Value*:

1. **\$cer = Nuevo-objeto System.Security.Cryptography.X509Certificates.X509Certificate2**
2. **\$cer. Importación ("_to_cert \ PEM_certificate.crt de C:\path ")**
3. **\$bin = \$cer.GetRawCertData()**
4. **\$base64Value = [System.Convert]::ToBase64String(\$bin)**
5. **\$bin = \$cer.GetCertHash()**
6. **\$base64Thumbprint = [System.Convert]::ToBase64String(\$bin)**
7. **\$keyid = [System.Guid]::NewGuid().ToString()**
8. **generación de eco \$base64Value**
9. **generación de eco \$base64Thumbprint**
10. **generación de eco \$keyid**

Con el fin de este documento, el ejemplo de configuración será basado en "esatest.onmicrosoft.com." Los comandos según lo ejecutado vía PowerShell deben ser similares al siguiente ejemplo:

Windows PowerShell

Copyright (C) 2014 Microsoft Corporation. All rights reserved.

```
PS C:\Users\Administrator> cd .\Desktop
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> $cer = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2
PS C:\Users\Administrator\Desktop>
$cer.Import('C:\Users\Administrator\Desktop\esatest.onmicrosoft.com_PEM.crt')
PS C:\Users\Administrator\Desktop> $bin = $cer.GetRawCertData()
PS C:\Users\Administrator\Desktop> $base64Value = [System.Convert]::ToBase64String($bin)
PS C:\Users\Administrator\Desktop> $bin = $cer.GetCertHash()
PS C:\Users\Administrator\Desktop> $base64Thumbprint = [System.Convert]::ToBase64String($bin)
PS C:\Users\Administrator\Desktop> $keyid = [System.Guid]::NewGuid().ToString()
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> echo $base64Value
MIIEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwZCcxZCZAJBgNVBAYTAlVTMRcwFQYDVQQLIEw5OOb3J0aCBDYXJv
bGluYTEEMMAoGA1UEBxMDU1RQM04wDAYDVQQKEwVDAxNjBzEMMAoGA1UECxMDVEF
DMSAwHgYDVQQDExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcnAY2lzY28uY29tMB4
XDTE2MDMyODE0NTYwMFoXDTE2MDMyODE0NTYwMFowZCcxZCZAJBgNVBAYTAlVTMR
cwFQYDVQQLIEw5OOb3J0aCBDYXJvY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzB6r/MtfKwG+86eHzdYk1CdyT+
j/j/+5yM6W9K8rqhW0FFT8et0vjp402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
axulraQeZgY/dkyHkTE26vt6rpy5g611TLloTZG1F0nkzT5Gs+zLOuhPHAT1DMU70LCXh8CHS2cLsczpdWfb20sHxTVLISVJ
qjdhYHYM7vC6VNFfMYIYXAE90ZE19QH0dU5n7spPyxUP0fp8z8gHsQ7HhRTsCNG
WbFyYb0Ib1RTOznzmXaSONRKYaIpkLkOSwZurT0wyGJd+TZSw+RgsXlvKJNmKih/iilYlVMKyyq+T7PjBPdWuU8uAGQIDAQA
Bo4HWMiHTMAwGAlUdEwQFMAMBAf8wCwYDVR0PBAQDAGWgMHAGA1UdJQRpMGcGCC
sGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAWQCisGAQQBgjcCARUGCisGAQQBgjcCARYGCisGAQQBgjcKAwEGCisGAQQBgj
cKAwMGcIsGAQQBgjcKAwQCysGAQQBgjcKAwQBMEQGA1UdEQQ9MDUwCF2VzYXRlc
3Qub25taWNyb3NvZnQuY29tSByb2JzaGVyZ0Blc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTANBgkqhkiG9w0BAQUFAAOCAQEAR
/F2tqxBriYK8fEt0swLZQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625
f31olkADPcK3ml0UarT35hH6f9abZSXm3mj3zMnuK5nW2ypDCVUiuA2C5l+woEubSmvn980GHuSXOqfLMPtniUMTubp+SICD
rtCse2l2Gke1OCrmxFlwtwgrCatwyoRxnDA5U4VyWQnyd7dL8eBOIhZMg1sFU6Z
xg8NKtiyEzV99OJ6+DokMnlfQOXDBPkgHIlmzFmVQogUGDcVbvpsdlroT4JcsUebmAdGvCek49HtHtlo6+aBLHQH+pX6pUqj
l+guS0X0FmMhkDJOTyZWnAQ==
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> echo $base64Thumbprint
3DLH9EqnuMPdkMrUj/Faljxa+XU=
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> echo $keyid
89ed56fc-7fae-4d10-ad63-7ddaeaf8e737
```

Salve la salida que usted recibe para *\$keyid*, *\$base64Thumbprint*, y *\$base64Value*, pues estos

valores serán utilizados más adelante en el *crear la sección evidente* de este documento. El `$base64Thumbprint` será utilizado durante la configuración ESA.

Nota: El `$base64Value` se requiere ser editado para ser una sola línea.

Salve el certificado de la clave pública (.crt) y la clave privada usada para firmar el certificado (.pem) localmente. La clave privada será necesaria durante la configuración ESA.

Microsoft Azure AD de la configuración

Cree la aplicación de Web de encargo

1. Inicie sesión al [Microsoft Azure](#).
2. Navegue a **TODOS LOS ELEMENTOS**.
3. Haga clic en el nombre del recurso para su dominio.
4. De las lengüetas de la herramienta para el nombre del recurso, seleccione las **APLICACIONES**.

Microsoft Azure | Check out the new port | CREDIT STATUS | @esatest.onmicrosoft.com

cisco tac (content security)

USERS | GROUPS | APPLICATIONS | DOMAINS | DIRECTORY INTEGRATION | CONFIGURE | REPORTS

LICENSES

Show Applications my company uses Search Application name or Client ID

NAME	PUBLISHER	TYPE	APP URL
Microsoft Intune	Microsoft Corporation	Web application	http://www.microsoft.com/en-us...
Office 365 Exchange Online	Microsoft Corporation	Web application	http://office.microsoft.com/outlo..
Office 365 Management APIs	Microsoft Corporation	Web application	
Office 365 SharePoint Online	Microsoft Corporation	Web application	http://office.microsoft.com/share..
Office 365 Yammer	Microsoft Corporation	Web application	https://products.office.com/yam..
Skype for Business Online (prev...	Microsoft Corporation	Web application	

+ NEW | ADD | VIEW ENDPOINTS | 1 ! ?

5. De la barra de herramientas inferior, selecta **AGREGUE**:

+ NEW |  ADD | VIEW ENDPOINTS | 1 ! ?

6. ¿Cuando está presentado “*qué usted quiere hacer?*”, selecto **agregue una aplicación que mi organización está desarrollando**.

7. Cree con un nombre apropiado, y deje el *tipo* como la **aplicación de Web y/o red API**, y haga clic la flecha para continuar:

Tell us about your application

NAME

Type

- WEB APPLICATION AND/OR WEB API [?]
- NATIVE CLIENT APPLICATION [?]



8. Para acabar de agregar la aplicación de Web de encargo, ingresar los valores siguientes para su dominio, y hacer clic el control para acabar: MUESTRA-EN EL URL: **https://<your.domain.com>/ManualRegistration** IDENTIFICACIÓN APP URI: **https://<your.domain.com>**

App properties

SIGN-ON URL ?

APP ID URI ?



9. De Microsoft, mirando [identificación App URI](#): “Porque identificación App URI es un identificador lógico, no necesita resolver a una dirección de Internet. Es presentado por su app al enviar un solo muestra-en la petición al azul AD. El azul AD identifica su app y envía muestra-en la respuesta (un token de SAML) a la contestación URL que fue proporcionada durante el registro del app. Utilice identificación App el valor de URI para fijar la propiedad del wtrealm (para la WS-federación) o la propiedad del emisor (para SAML-P) al hacer una petición del ingresar. **Identificación App URI** debe ser un valor único en el azul AD de su organización.”

Nota: “Al habilitar un app para los usuarios externos, el valor identificación App de URI del app debe ser un direccionamiento en uno de los dominios verificados de su directorio. Como consecuencia, no puede ser una URNA. Esta salvaguarda evita que otras organizaciones especificar (y tomen) la propiedad única que pertenece a su organización. Durante el desarrollo, usted puede cambiar su identificación App URI a una ubicación en el dominio inicial de su organización (si usted no ha verificado un dominio de encargo/de la vanidad), y pone al día su app para utilizar este nuevo valor. El dominio inicial es el dominio 3-level durante el cual usted crea firma para arriba, por ejemplo contoso.onmicrosoft.com.”

Aplicación de Web de la aduana de la configuración

1. Una vez que se ha creado la aplicación de Web de encargo, le navegan automáticamente en la aplicación de Web de encargo sí mismo. De aquí, en las lengüetas de la herramienta, seleccione la **CONFIGURACIÓN**:

Microsoft Azure | Check out the new port | CREDIT STATUS | @esatest.onmicrosoft.com

esa_beta

DASHBOARD USERS **CONFIGURE** OWNERS

Your app has been added!
Enable your app to integrate with Microsoft Azure AD
 Skip Quick Start the next time I visit

GET STARTED

- ▶ ENABLE USERS TO SIGN ON
- ▶ LEARN: MICROSOFT AZURE AD FEATURES FOR DEVELOPERS

CONFIGURE

- ▶ ACCESS WEB APIS IN OTHER APPLICATIONS
- ▶ EXPOSE WEB APIS TO OTHER APPLICATIONS
- ▶ CONFIGURE MULTI-TENANT APPLICATION

2. De esta pantalla, usted puede ver Muestra-en el URL y otros detalles de la configuración según lo creado. Nota: **El ID de cliente** se enumera en esta pantalla. Este valor será necesario durante la configuración ESA.

Microsoft Azure | Check out the new port | CREDIT STATUS | @esatest.onmicrosoft.com


esa_beta

DASHBOARD | USERS | CONFIGURE | OWNERS

properties

NAME: ESA_Beta

SIGN-ON URL: https://esatest.onmicrosoft.com/ManualRegistration

LOGO: 

APPLICATION IS MULTI-TENANT: YES NO

CLIENT ID: 19d048bb-1c44-401b-b1fa-a61d67a9caca

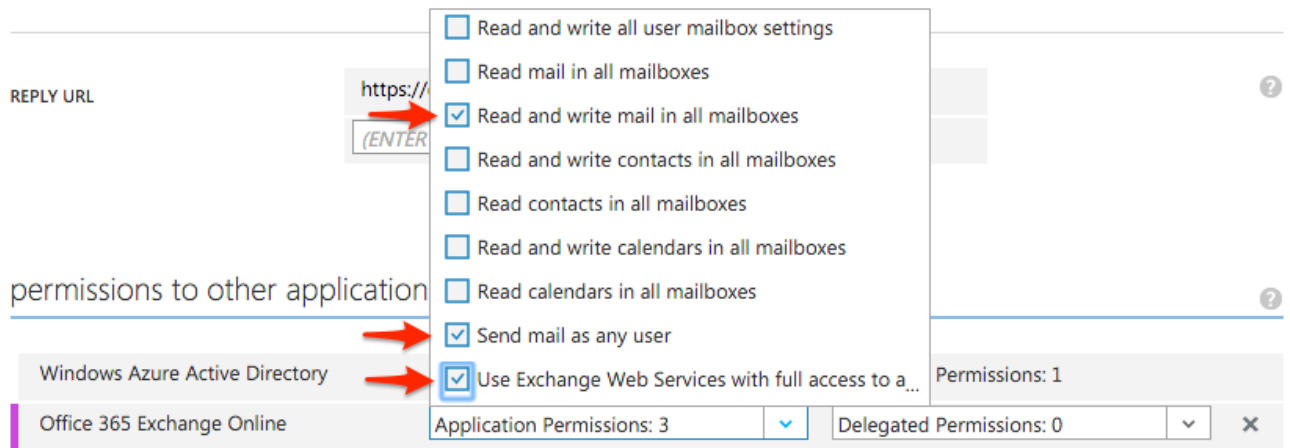
- De esta misma pantalla para la configuración de aplicación de Web de encargo, navegue a la parte inferior y el tecleo **agrega la aplicación**:

permissions to other applications

Windows Azure Active Directory	Application Permissions: 0	Delegated Permissions: 1
--------------------------------	----------------------------	--------------------------

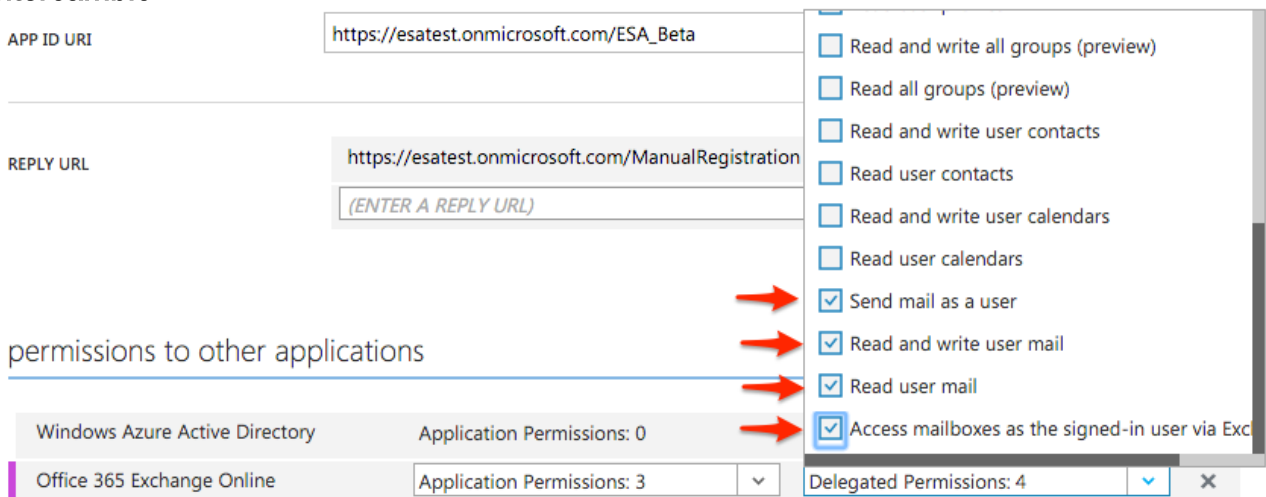
Add application

- El Online selecto del intercambio de la oficina 365 y hace clic el control para continuar.
- Para los *permisos de OnlineApplication del intercambio de la oficina 365*, seleccione **leído** y escriba el correo en todos los buzones, envíe el correo como cualquier usuario, y utilice los servicios web del intercambio con el acceso **total...**:



Add application

6. Para los *permisos de OnlineDelegated del intercambio de la oficina 365*, selecto envíe el correo como un usuario, leyó y escribe el correo del usuario, leyó el correo del usuario, y accede los buzones como el usuario ingresado vía el intercambio:



Add application

7. Haga clic la **salvaguardia de la** barra de herramientas inferior para salvar todo el trabajo y configuración para la aplicación de Web de encargo:



Cree el evidente

1. Una vez que la aplicación de Web de encargo ha completado el ahorro y la puesta al día, el tecleo **MANEJA EVIDENTE > descarga evidente de la barra de herramientas inferior:**



- Navegue con las respuestas, y salve la aplicación de Web evidente en el formato .json a su computadora local.
- Encuentre este archivo .json y abra este archivo .json con un editor de textos. (Notepad++ preferible, átomo, etc.)
- Busque y encuentre la línea de los "keyCredentials".
- Usted substituirá esta sola línea con las líneas múltiples siguientes, y personaliza usando las credenciales identificadas anteriores de la sección de los valores del *certificado de la configuración* (*\$base64Thumbprint*, *\$keyid*, y *\$base64Value*):
- ```

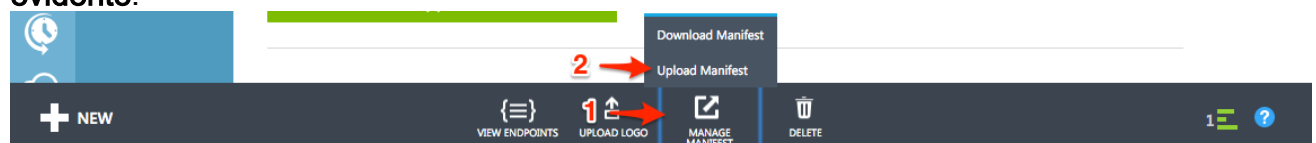
6. "keyCredentials": [
 {
 "customKeyIdentifier": "$base64Thumbprint",
 "keyId": "$keyid",
 "type": "AsymmetricX509Cert",
 "usage": "Verify",
 "value": "$base64Value"
 }
],

```
- Según lo observado anterior, al ingresar el *\$base64Value*, esto se requiere ser editada para ser un valor de la sola línea.
- Continuando con el ejemplo según lo creado desde el principio de este documento, los *keyCredentials* modificados serán como sigue:
- ```

9. "keyCredentials": [
  {
    "customKeyIdentifier": "3DLH9EqnuMPdkMrUj/Faljxa+XU=",
    "keyId": "89ed56fc-7fae-4d10-ad63-7ddaeaf8e737",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value":
"MIIEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwZcxzCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aC
BDYXJvbGluYTEEMMAoGALUEBxMDU1RQM04wDAYDVQQKEwVDaXNjbzEMMAoGALUECzMDVEFDMSAwHgYDVQQDEXd1c2F0Z
XN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcnRAY2l2Y28uY29tMB4XDTE2MDMyODE0NTYw
MFoXDTE3MDMyODE0NTYwMFowZcxzCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw50b3J0aCBBYXJvbGluYTEEMMAoGALUEBxM
DU1RQM04wDAYDVQQKEwVDaXNjbzEMMAoGALUECzMDVEFDMSAwHgYDVQQDEXd1c2F0ZXXN0Lm9ubWljcm9zb2Z0LmNvbT
EhMB8GCSqGSIb3DQEJARYScm9ic2hlcnRAY2l2Y28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz
B6r/MtFkKg+86eHzdYk1CdyT+j/j/+5yM6W9K8rqhW0FFT8et0vj402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
axulraQeZgY/dkyHkTE26vt6rpy5g611TLLoTZG1F0nkzT5Gs+zL0uhPHaT1DMU70LCXh8CHs2cLsczPDWfb20sHXTV
lISVJqjdhYHYM7vC6VNfMYIYxAE90ZEL9QH0dU5n7spPyUP0fp8z8gHsQ7HhRTsCNgWbFyYb0Ib1RTOznmzMXaSon
RKYaIpkLkOSwZurT0wyGJd+TZSw+RgsXlvKJNmKih/iilYLvMKYq+T7PJbPDwhU8uAGQIDAQABo4HWMHTMAwGALUdE
wQFMAMBAF8wCwYDVR0PBAQDAgWgMHAGA1UdJQRpMGcGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAWQCisGAQQB
gjcCARUGCisGAQQBgjcCARYGCisGAQQBgjcKAwEGCisGAQQBgjcKAwMGCisGAQQBgjcKAwQGCysGAQQBgjcKAwQBMEQ
GALUdEQQ9MDuCF2VzYXRlc3Qub25taWNyb3NvZnQuY29tSByb2JzaGVyY29tY29tY29tY29tY29tY29tY29tY29tY29t
ANBgkqhkiG9w0BAQUFAAOCAQEAR/F2tqxBrIYK8fEt0swLZQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625f
31o1kADPcK3ml0UarT35hH6f9abZSxm3mj3zMnuK5nW2ypDCVUiuA2C5l+woEubSsmvn980GHuSXOqfLMPtniUMTubp+
SICDrtCse2l2GkE1OCRmxFlwtwgrCatwyoRxnDA5U4VYwQnyd7dL8eBOIhZMg1sFU6Zxg8NKtiyEzV99OJ6+DokMnlf
QOXDBPkgHI1mzFmVQogUGDcVbvpsdlroT4JcsUebmAdGvCek49HtHtlo6+aBLHQH+pX6pUqjl+guS0X0FMmhkDJOTyZ
WnAQ== "
  }
],

```
- Salve el archivo .json localmente.
- Vuelva a su navegador y al portal del Microsoft Azure.
- El tecleo **MANEJA EVIDENTE > carga**

evidente:



- Hojee y encuentre el archivo editado .json, y seleccione la marca de tilde para completar la

carga.

Encontrar al arrendatario ID

1. Haga clic en los **PUNTOS FINALES de la VISIÓN** para ver los puntos finales integrados en el azul AD de Microsoft.
2. Con en los URL, note el valor similar para cada línea, el "ed437e13-ba50-479e-b40d-8affa4f7e1d7," que éste es el **arrendatario ID**.



App Endpoints

If you are developing an app that integrates with Microsoft Azure AD, update your code to use these endpoints for single sign-on and directory access.

FEDERATION METADATA DOCUMENT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



WS-FEDERATION SIGN-ON ENDPOINT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



SAML-P SIGN-ON ENDPOINT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



SAML-P SIGN-OUT ENDPOINT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



MICROSOFT AZURE AD GRAPH API ENDPOINT

<https://graph.windows.net/ed437e13-ba50-479e-b40d-8affa4f7e1d7>



OAuth 2.0 TOKEN ENDPOINT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



OAuth 2.0 AUTHORIZATION ENDPOINT

<https://login.microsoftonline.com/ed437e13-ba50-479e-b40d-8affa4f7>



Esto será único a su aplicación y configuración. Registre este valor para configuración más posterior en el ESA.

Revisión final de los valores que se guardarán

Los valores siguientes se deben haber registrado durante la configuración del Microsoft Azure AD para el uso al configurar las configuraciones del buzón en el ESA:

De los valores del certificado de la configuración:

- Certificado de la clave privada (.pem)
- \$base64Thumbprint

De la aplicación de Web de encargo de la configuración:

- ID de cliente

De encontrar al arrendatario ID:

- Arrendatario ID

Configuraciones del buzón de la configuración en el ESA


Con la configuración del Microsoft Azure AD completa, usted está listo para hacer que el ESA comunique y valide.

1. Login al dispositivo ESA vía el GUI.
2. Configuraciones del buzón de la oficina 365 del **permiso** bajo **configuraciones de la administración del sistema > del buzón**.
3. “La casilla de verificación selecta de las **configuraciones del buzón de la oficina 365 del permiso**” y proporciona sus detalles del Microsoft Azure AD (*ID de cliente y el arrendatario ID*) obtenidos mientras que registra la aplicación ESA con el Microsoft Azure AD junto con Thumbprint y la clave privada del certificado.
4. El tecleo **somete** para salvar los cambios a las configuraciones del buzón.
5. Usted necesitará probar la conexión al Microsoft Azure AD ahora para su dominio de la oficina 365 según lo configurado:

Mailbox Settings

Success — The settings were configured successfully . You must test the connection.

Office 365 Mailbox Settings	
Azure AD Details:	Client ID: 19d048bb-1c44-401b-b1fa-a61d67a9caca
	Tenant ID: ed437e13-ba50-479e-b40d-8affa4f7e1d7
	Thumbprint: 3DLH9EqnuMPdkMrUj/Fa1jxa+XU=
	Certificate Private Key: Successfully uploaded

Check Connection...  Edit Settings...

6. Utilice una dirección de correo electrónico activa y válida en la cuenta, Haga clic en Probar conexión:

Connection Check

Connection Parameters

Office 365 Email Address:

[Test Connection](#)



Connection Status

Connected to Azure AD.
Connection Successful.
Inbox count of Messages are 0

[Done](#)

7. Una vez que el estado de la conexión es acertado, haga clic **hecho** para completar el control de la conexión.
8. Finalmente, **cometer del** teclado para salvar todos los cambios de configuración en el ESA.