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

Contenido

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](#) (aseegurese 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
MIIEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwgZcxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJv
bGluYTEMMAoGA1UEBxMDUlRQMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEF
DMSAwHgYDVQQDExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcndAY2lzY28uY29tMB4
XDTE2MDMyODE0NTYwMFoXDTE3MDMyODE0NTYwMFowgZcxCzAJBgNVBAYTAlVTMR
cwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEMMAoGA1UEBxMDUlRQMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMSAwHg
YDVQQDExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYSc
m9ic2hlcndAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzB6r/MtfKwG+86eHzdhYklCdyyT+j
/j/+5yM6W9K8rqhW0FFT8et0vjp402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
axu1raQeZgY/dkyHkTE26vt6rpy5g611TLloTZGlF0nkzT5Gs+zLOuhPHaT1DMU70LCXh8CHs2cLsczpDWfb2OsHxTVlISVJ
qjdhYHYM7vC6VNffMYIYxAE90ZEl9QHOdU5n7spPyxUP0fp8z8gHsQ7HhRTsCNg
WbFyYb0Ib1RTOznmzMXaSOnRKYaIpkLkOSwZurT0wyGJd+TZSw+RgsX1vKJNmKih/ii1YLvMKyq+T7PJbPDwhU8uAGQIDAQA
Bo4HWMIHTMAwGA1UdEwQFMAMBAf8wCwYDVR0PBAQDAgWgMHAGA1UdJQRpMGcGCC
sGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwQGCisGAQQBgjcCARUGCisGAQQBgjcCARYGCisGAQQBgjcKAwEGCisGAQQBgj
cKAwMGCisGAQQBgjcKAwQGCysGAQQBgjcKAwQBMEQGA1UdEQQ9MDuCF2VzYXRlc
3Qub25taWNyb3NvZnQuY29tgSByb2JzaGVyd0Blc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbTANBgkqhkiG9w0BAQUFAAOCAQEAR
/F2tqxBriYK8fEt0swLZQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625
f31o1kADPcK3ml0UarT35hH6f9abZSXm3mj3zMnuK5nW2ypDCVUiuA2C5l+woEubSmvn980GHuSXOqfLMPtniUMTubp+SICD
rtCse2l2GkE1OCRmxF1wtwgrCatwyoRxnDA5U4VyWQnyd7dL8eBOIhZMg1sFU6Z
xg8NKtiyEzV99OJ6+DOkMn1fQOXDBPkgHI1mzFmVQogUGDcVbvpsd1roT4JcsUebmAdGvCek49HtHtlo6+aBLHQH+pX6pUqj
1+guS0X0FMmhkDJOTyZWnAQ==
PS C:\Users\Administrator\Desktop>
PS C:\Users\Administrator\Desktop> echo $base64Thumbprint
3DLH9EqnuMPdkMrUj/Fa1jxa+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.

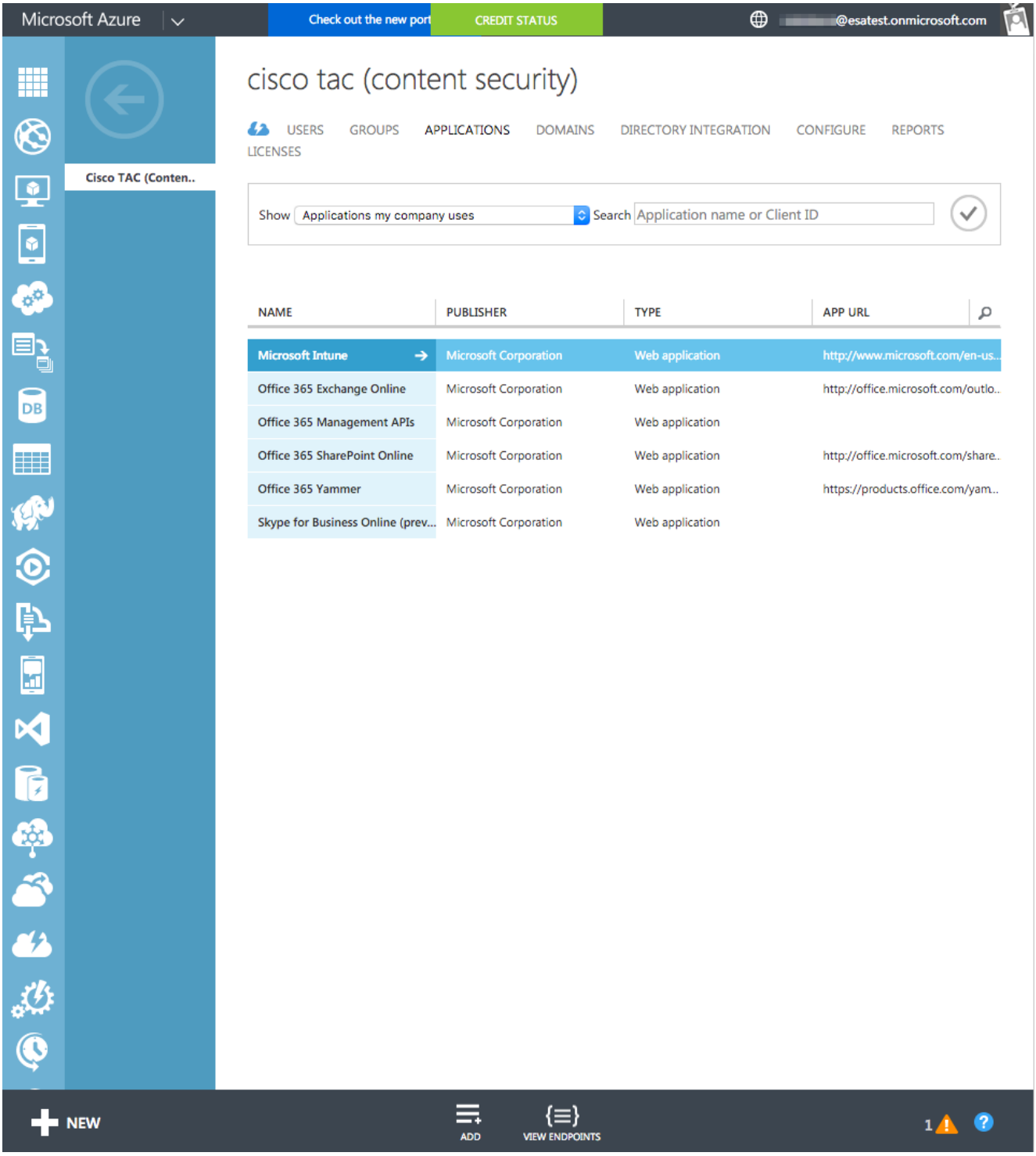
> Nota: *El $base64Value* se requiere ser editado para ser una sola línea.

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.

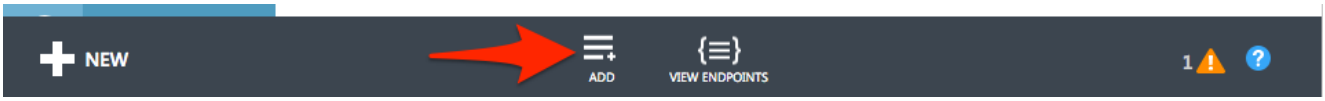
Microsoft Azure AD de la configuración

Cree la aplicación de Web de encargo

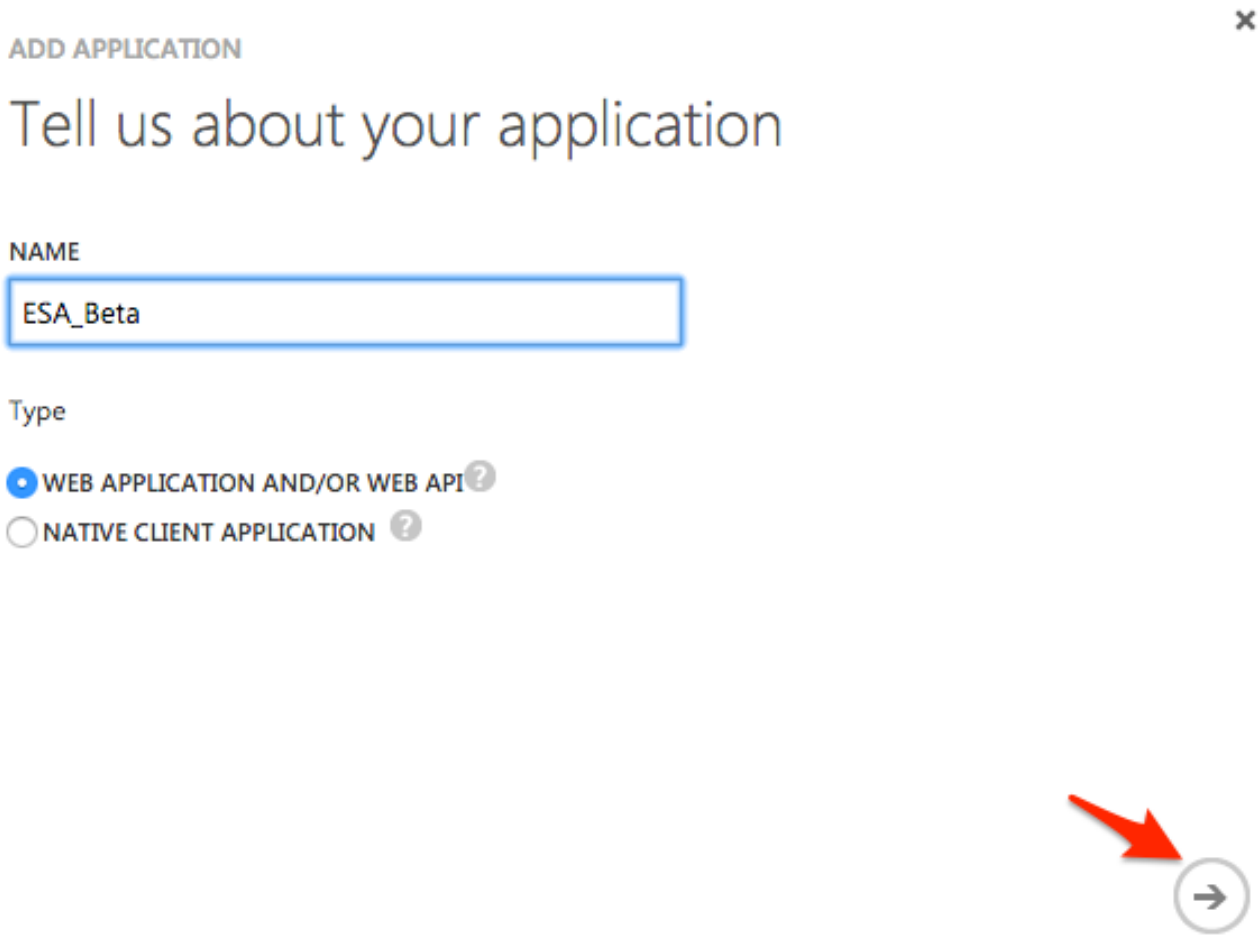
1. Inicie sesión al Microsoft Azure.
2. Navegue a **TODOS LOS ELEMENTOS**.
3. Haga clic en el nombre del recurso para su dominio.
4. De las lenguetas de la herramienta para el nombre del recurso, seleccione las **APLICACIONES**.



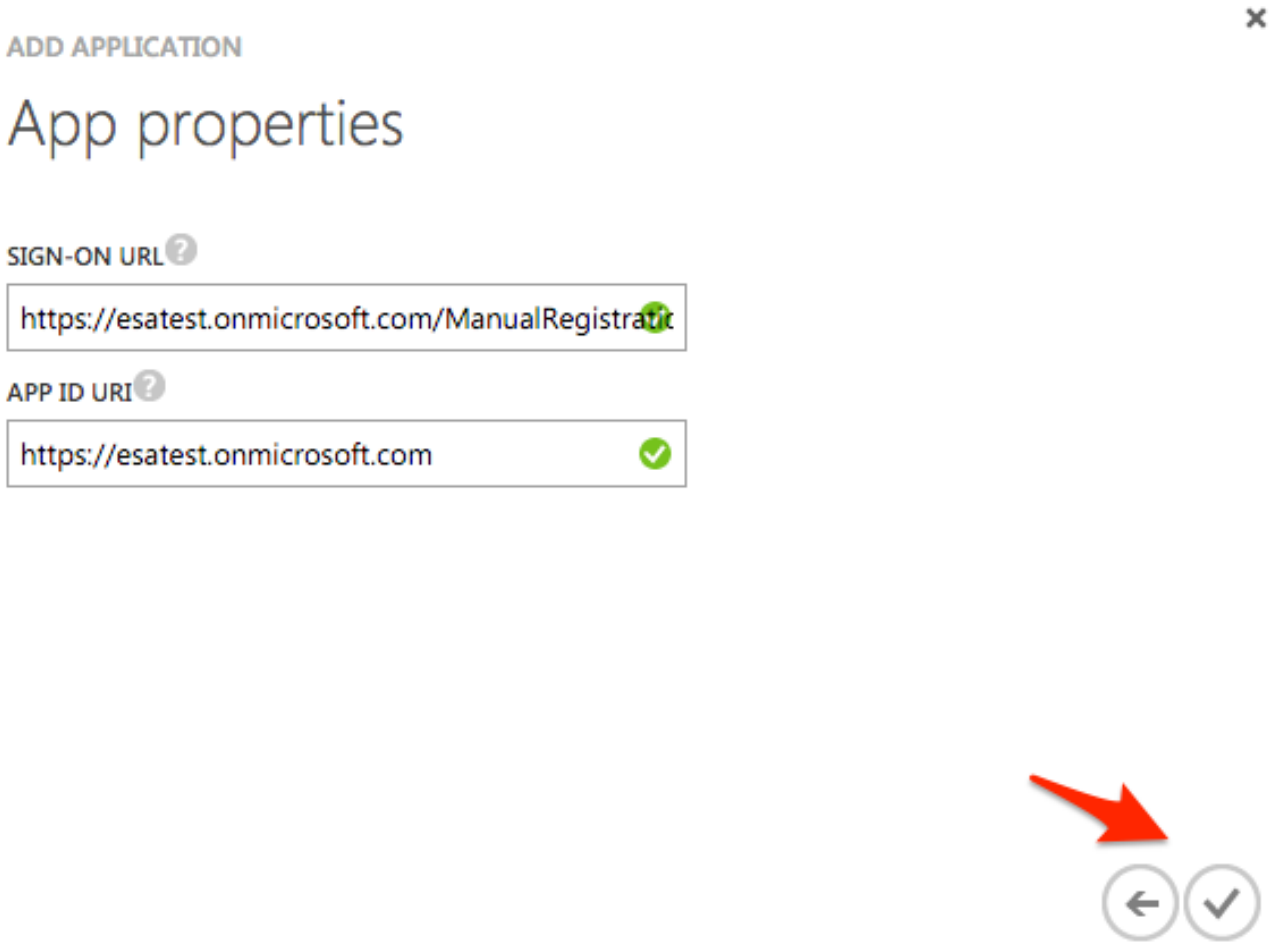
5. De la barra de herramientas inferior, selecta **AGREGUE**:



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:



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>***

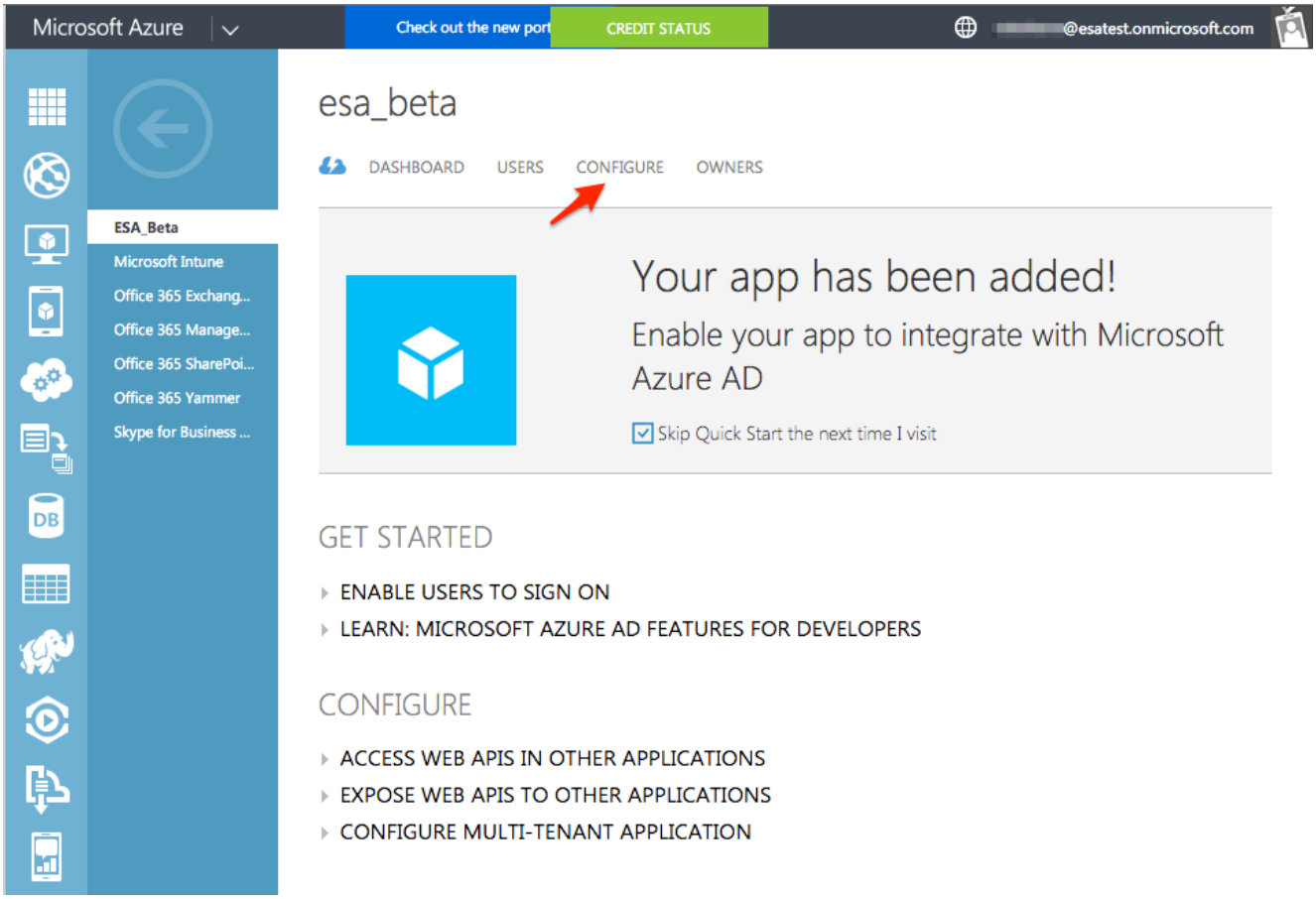


9. De Microsoft, mirando identificación App URI: “Porque identificación App URI es un identificador lógico, no necesita resolver a una dirección de Internet. Es presentado por su app al enviar un solo muestra-en la petición al azul AD. El azul AD identifica su app y envía muestra-en la respuesta (un 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.”

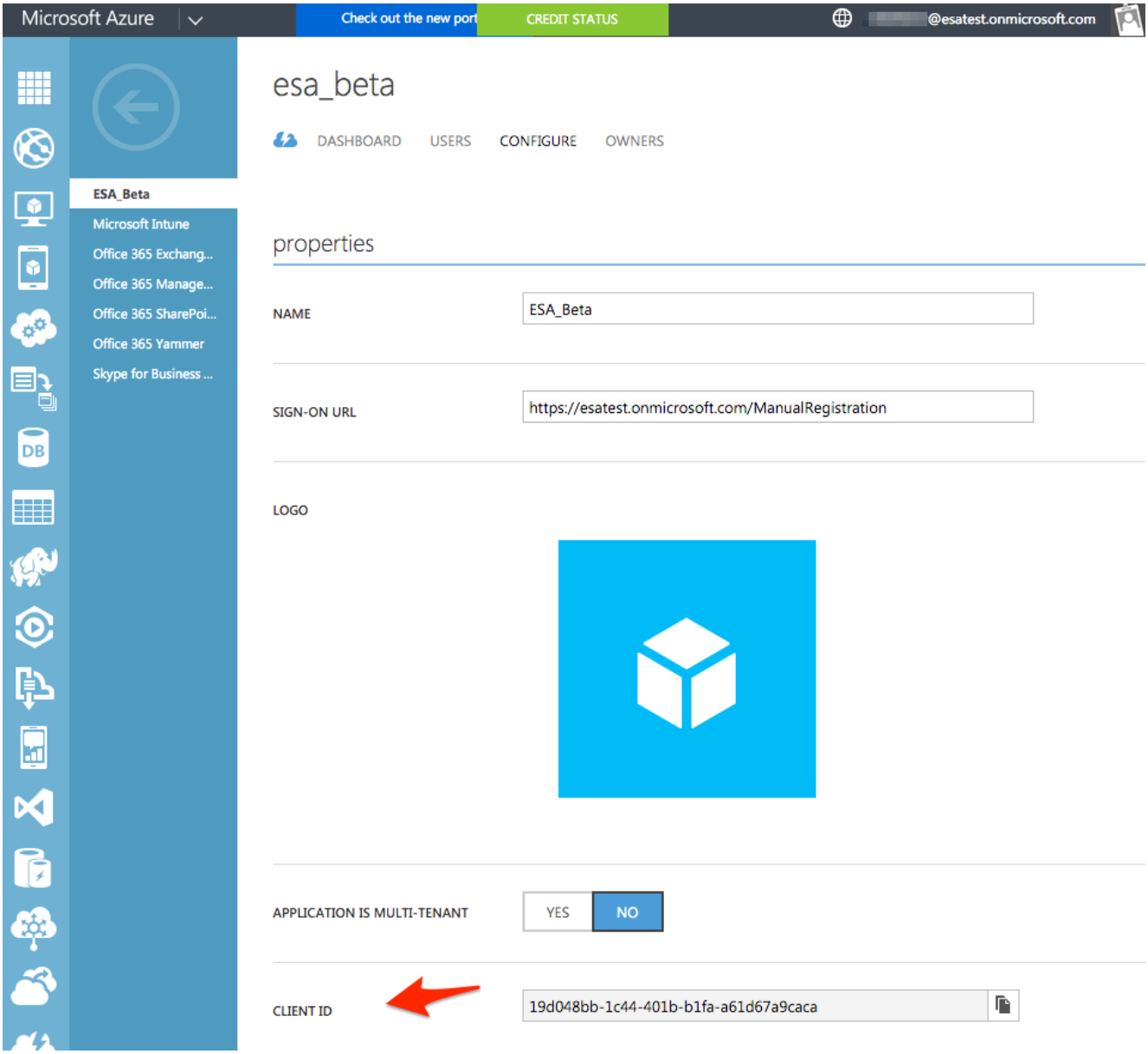
   Nota: “Al habilitar un app para los usuarios externos, el valor identificación App de URI del app debe ser un direccionamiento en uno de los dominios verificados de su directorio. Como consecuencia, no puede ser una URNA. Esta salvaguardia evita que otras organizaciones especificar (y tomen) la propiedad 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

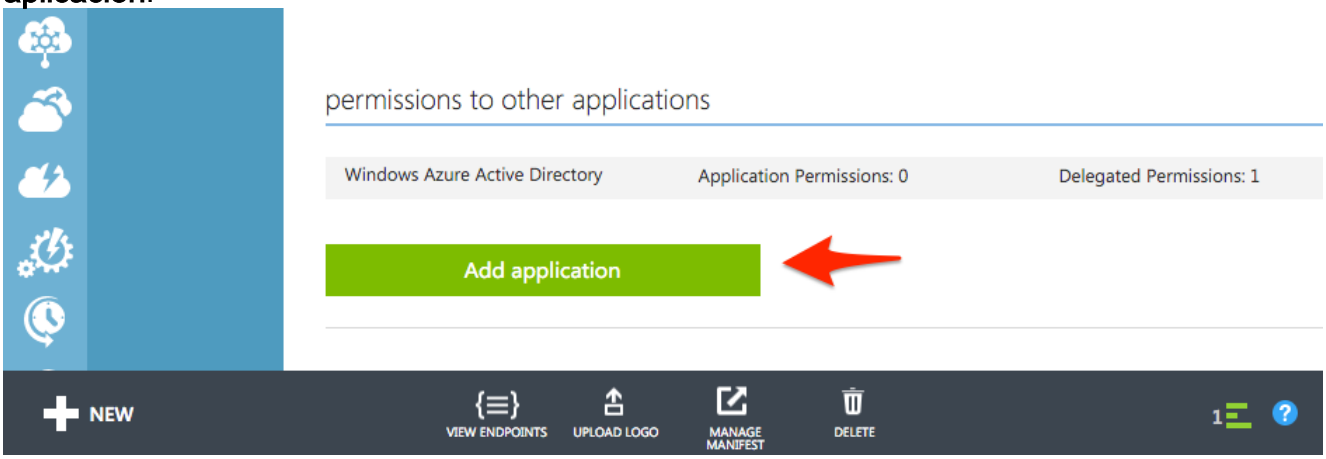
1. Una vez que se ha creado la aplicación de Web de encargo, le navegan automáticamente en la aplicación de Web de encargo sí mismo. De aquí, en las lenguetas de la herramienta, seleccione la
   CONFIGURACIÓN:



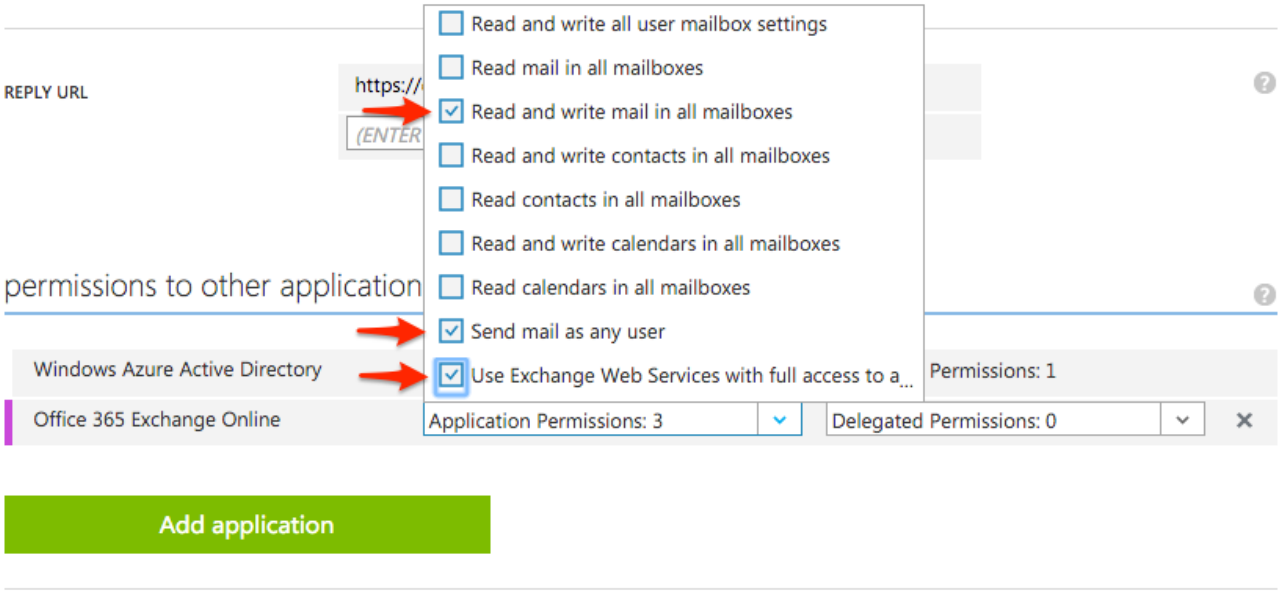
2. De esta pantalla, usted puede ver Muestra-en el URL y otros detalles de la configuración según lo creado. Nota: ***El ID de cliente*** se enumera en esta pantalla. Este valor será necesario durante la configuración
ESA.



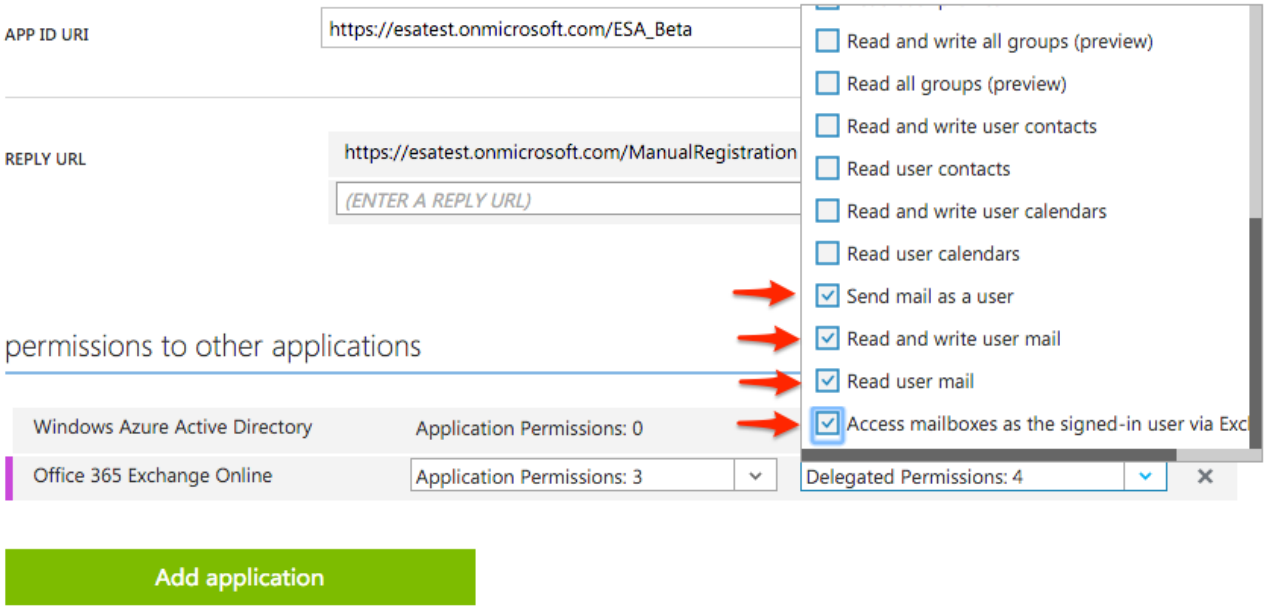
3. De esta misma pantalla para la configuración de aplicación de Web de encargo, navegue a la parte inferior y el tecleo **agrega la aplicación**:



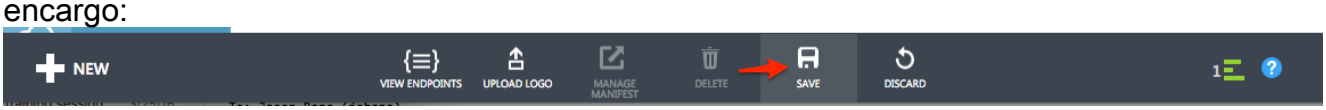
4. **El Online** selecto del **intercambio de la oficina 365** y hace clic el control para continuar.
5. Para los *permisos de OnlineApplication del intercambio de la oficina 365*, seleccione **leído y escriba el correo en todos los buzones**, **envíe el correo como cualquier usuario**, y **utilice los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



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**:



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:

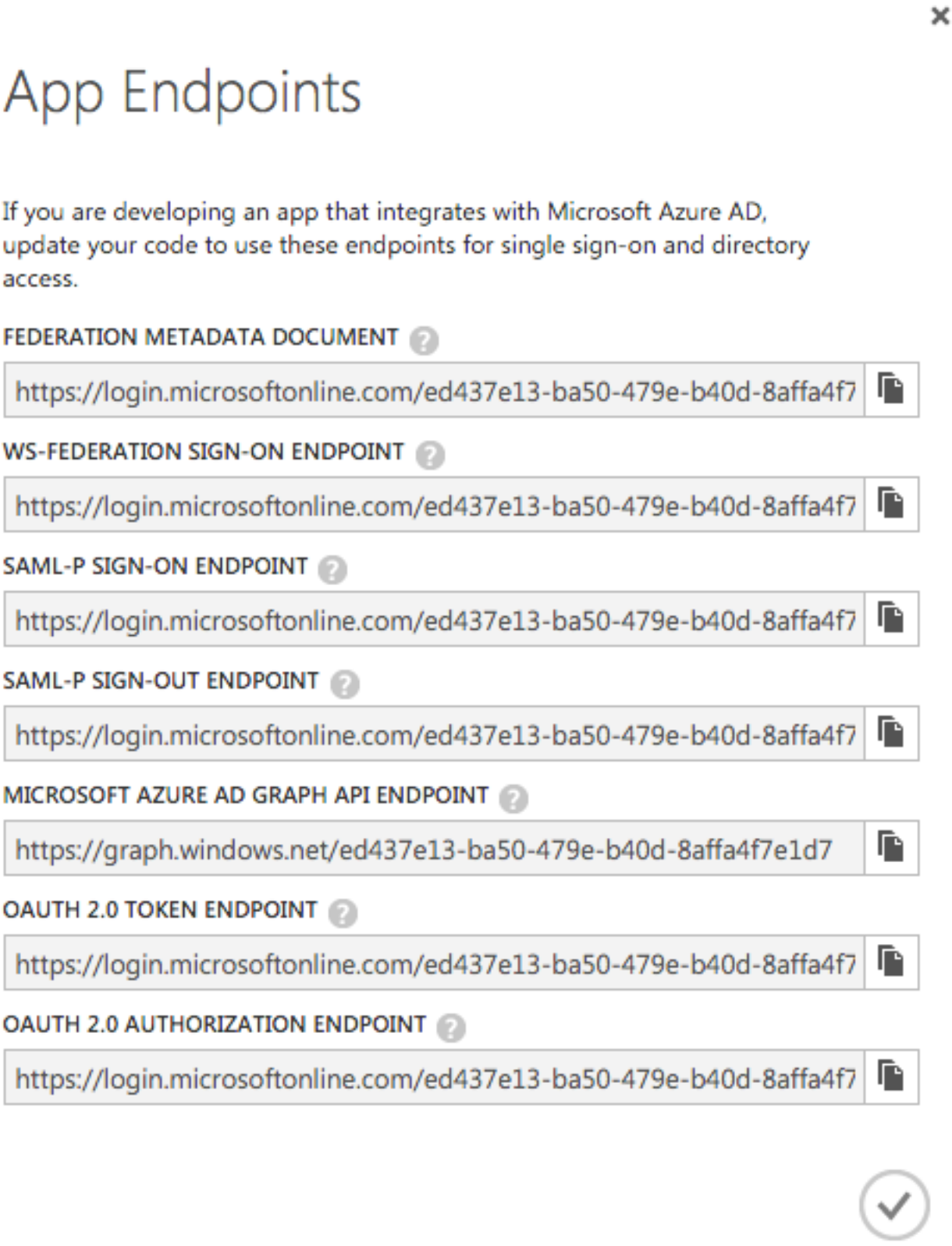
2. Navegue con las respuestas, y salve la aplicación de Web evidente en el formato .json a su computadora local.
3. Encuentre este archivo .json y abra este archivo .json con un editor de textos. (Notepad++ preferible, átomo, etc.)
4. Busque y encuentre la línea de los “keyCredentials”.
5. Usted substituirá 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"
}
],
```
7. Según lo observado anterior, al ingresar el *$base64Value*, esto se requiere ser editada para ser un valor de la sola línea.
8. Continuando con el ejemplo según lo creado desde el principio de este documento, los *keyCredentials* modificados serán como sigue:
9.
```
"keyCredentials": [
{
"customKeyIdentifier": "3DLH9EqnuMPdkMrUj/Fa1jxa+XU=",
"keyId": "89ed56fc-7fae-4d10-ad63-7ddaeaf8e737",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value":
"MIIEhjCCA26gAwIBAgIFIBYDKAEwDQYJKoZIhvcNAQEFBQAwgZcxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aC
BDYXJvbGluYTEMMAoGA1UEBxMDUlRQMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMSAwHgYDVQQDExdlc2F0Z
XN0Lm9ubWljcm9zb2Z0LmNvbTEhMB8GCSqGSIb3DQEJARYScm9ic2hlcndAY2lzY28uY29tMB4XDTE2MDMyODE0NTYw
MFoXDTE3MDMyODE0NTYwMFowgZcxCzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEMMAoGA1UEBxM
DUlRQMQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDVEFDMSAwHgYDVQQDExdlc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbT
EhMB8GCSqGSIb3DQEJARYScm9ic2hlcndAY2lzY28uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAz
B6r/MtfKwG+86eHzdhYklCdyyT+j/j/+5yM6W9K8rqhW0FFT8et0vjp402sI8wg34m0LckFkvbakP6w3mam1hfsocj5
axu1raQeZgY/dkyHkTE26vt6rpy5g611TLloTZGlF0nkzT5Gs+zLOuhPHaT1DMU70LCXh8CHs2cLsczpDWfb2OsHxTV
lISVJqjdhYHYM7vC6VNffMYIYxAE90ZEl9QHOdU5n7spPyxUP0fp8z8gHsQ7HhRTsCNgWbFyYb0Ib1RTOznmzMXaSOn
RKYaIpkLkOSwZurT0wyGJd+TZSw+RgsX1vKJNmKih/ii1YLvMKyq+T7PJbPDwhU8uAGQIDAQABo4HWMIHTMAwGA1UdE
wQFMAMBAf8wCwYDVR0PBAQDAgWgMHAGA1UdJQRpMGcGCCsGAQUFBwMBBggrBgEFBQcDAgYIKwYBBQUHAwQGCisGAQQB
gjcCARUGCisGAQQBgjcCARYGCisGAQQBgjcKAwEGCisGAQQBgjcKAwMGCisGAQQBgjcKAwQGCysGAQQBgjcKAwQBMEQ
GA1UdEQQ9MDuCF2VzYXRlc3Qub25taWNyb3NvZnQuY29tgSByb2JzaGVyd0Blc2F0ZXN0Lm9ubWljcm9zb2Z0LmNvbT
ANBgkqhkiG9w0BAQUFAAOCAQEAR/F2tqxBriYK8fEt0swLZQYYq+JWma6MxNjODXoSj4SWKxFv8Vb5LwE7goxi9625f
31o1kADPcK3ml0UarT35hH6f9abZSXm3mj3zMnuK5nW2ypDCVUiuA2C5l+woEubSmvn980GHuSXOqfLMPtniUMTubp+
SICDrtCse2l2GkE1OCRmxF1wtwgrCatwyoRxnDA5U4VyWQnyd7dL8eBOIhZMg1sFU6Zxg8NKtiyEzV99OJ6+DOkMn1f
QOXDBPkgHI1mzFmVQogUGDcVbvpsd1roT4JcsUebmAdGvCek49HtHtlo6+aBLHQH+pX6pUqj1+guS0X0FMmhkDJOTyZ
WnAQ=="
}
],
```
10. Salve el archivo .json localmente.
11. Vuelva a su navegador y al portal del Microsoft Azure.
12. El tecleo **MANEJA EVIDENTE > carga evidente**:

13. 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***.



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

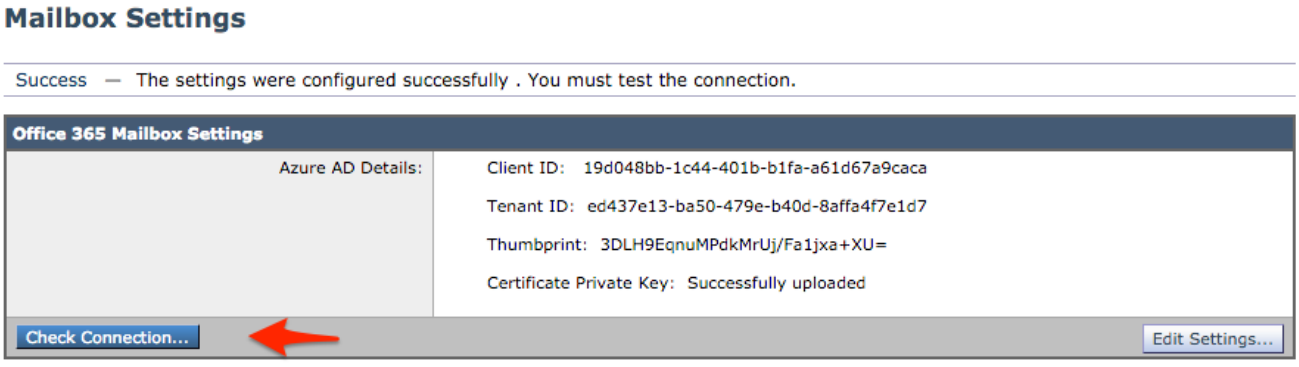
De encontrar al arrendatario ID:

- Arrendatario ID

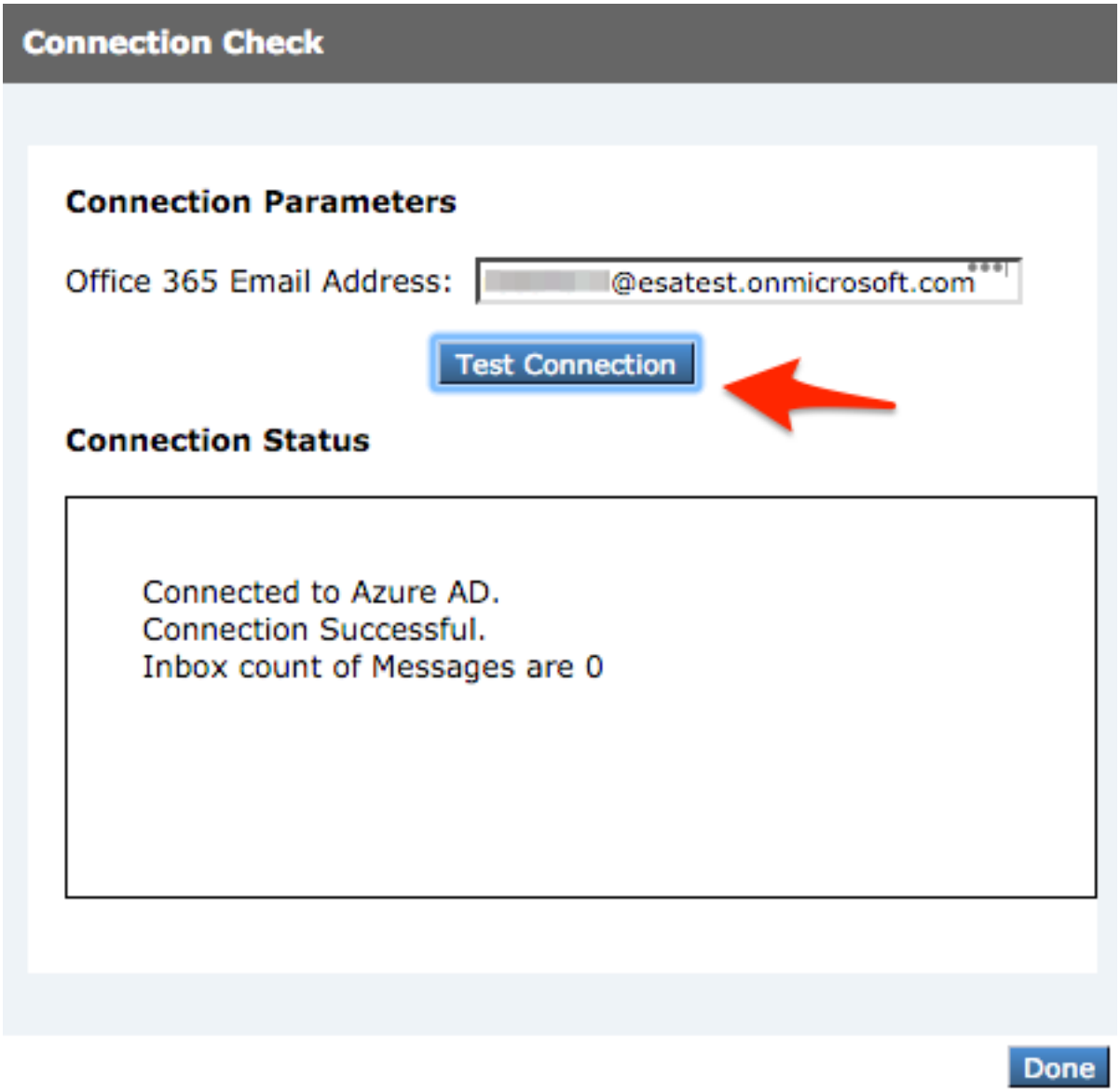
Configuraciones del buzón de la configuración en el ESA

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:



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



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** tecleo para salvar todos los cambios de configuración en el ESA.