Configuraciones del buzón del Azure AD y de la oficina 365 de la configuración del Cómo para el ESA

Contenido

Introducción

Este documento proporciona un gradual “cómo-a” para registrar una nueva aplicación en Windows Azure y obtener los valores necesarios, para completar la configuración para las configuraciones del buzón de la oficina 365 en un dispositivo de seguridad del correo electrónico de Cisco (ESA). Se requiere esto cuando un administrador ESA configura la corrección auto del buzón (MARCHA) para la protección avanzada de Malware (AMP) en las configuraciones de la directiva del correo ESA.

Prerequisites

Productos Relacionados

Este documento se aplica al siguiente:

- Todo el ESA, hardware y funcionamiento virtual 10.x y más nuevo
- Toda la Seguridad del correo electrónico de la nube (CES) ESA, 10.x y más nuevo corrientes

Requisitos

Este documento 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 intercambiar, 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 host o de un servidor de 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.

Usted creará los cuatro valores siguientes para configurar el conector del buzón ESA de nuevo al Azure AD:

1. ID de cliente
2. Arrendatario ID
3. Thumbprint
4. Clave privada del certificado en el formato del .pem

Para construir estos valores requeridos, usted necesitará completar los pasos en este documento. Antes de comenzar, usted necesitará ejecutar el siguiente vía Windows Powershell:

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**

Note: Para #2, substituya el **"_to_cert \ PEM_certificate.crt de C:\path" por la** trayectoria a su certificado.

$base64Thumbprint = *Thumbprint*. Agregue este valor a su lista de los requisitos previos de valores requeridos.

Tip: Por favor tenga la salida guardada localmente para *$base64Value*, *$base64Thumbprint*, y *$keyid*, pues serán requeridos más adelante en los pasos para la configuración. Ahora, le hacen con el .crt del certificado. Tenga por favor el .pem asociado de su certificado en un disponible, carpeta local en su ordenador.

Antecedentes

Microsoft permite el acceso a dos versiones del portal azul:

- https://manage.windowsazure.com (portal clásico)
- https://portal.azure.com (nuevo portal)

Usted puede acceder el "portal clásico" del nuevo portal por la barra de herramientas de la mano izquierda, "Active Directory azul selecto" > portal clásico

Con el propósito de este documento, el registro y la configuración de la aplicación se hacen en el nuevo portal. Los pasos a usar el "portal clásico" son incluidos en el extremo de este documento. (Microsoft puede elegir en alguna vez inhabilitar el portal azul clásico.)

Configuraciones del buzón del Azure AD y de la oficina 365 de la configuración del Cómo para el ESA

Registre una nueva aplicación en Azure

1. Acceda la interfaz de usuario azul: https://portal.azure.com/
2. La barra de menú izquierda, hace clic **más > SECURITY (SEGURIDAD) de los servicios + IDENTIDAD: Registros del App**
3. Del cristal de los registros del App, tecleo **+Add**
4. Cree un nombre para su app
5. Para Application type (Tipo de aplicación), váyase como **red app/API**
6. Para Muestra-en el URL, utilice el formato siguiente: https://*<company_domain.com>/ManualRegistration***Note**: *<company_domain.com> es el* dominio de su O365 donde los Domain User pueden ingresar y acceder su dominio O365.
7. El tecleo **crea**

Fije los permisos requeridos para la aplicación

1. Haga clic en el "nombre de la visualización" asociado para el app que usted acaba de registrarse
2. En el cristal de las configuraciones, para el acceso API, el tecleo **requirió los permisos**
3. Tecleo **+Add**
4. En "agregue el cristal del acceso API", tecleo **seleccionan un API**
5. En el cristal "seleccione y API", **Online del intercambio de la oficina 365 del** tecleo **(el Microsoft Exchange)**
6. En la parte inferior del tecleo de la página **seleccione**
7. Para los permisos de la aplicación seleccione:
   • Utilice los servicios web del intercambio con el acceso total a todos los buzones

- Envíe el correo como cualquier usuario
- Lea y escriba el correo en todos los buzones

8. Para los permisos Delegated seleccione:
   - Envíe el correo como usuario
   - Lea y escriba el correo del usuario
   - Lea el correo del usuario
   - Acceda los buzones como el usuario ingresado vía los servicios web del intercambio
9. Haga clic **selecto** en la parte inferior de la página, esto cerrará “seleccionan el cristal API”
10. Haga clic **hecho** en la parte inferior de la página, esto cerrará “agregan el cristal del acceso API”
11. Haga clic los **permisos de Grant**
12. ¿Cuando se le pregunte “usted quiere conceder los permisos abajo para el myESA para todas las cuentas en el directorio actual? Esta acción pondrá al día cualquier permisos existente que esta aplicación tenga que hacer juego ya cuál es mencionado abajo. ”, haga clic **sí**

Usted ahora debe hacer dos API enumerar, “Active Directory de Windows Azure” y “Online del intercambio de la oficina 365”.

Usted necesitará volver al cristal registrado del app para proceder con la siguiente sección:

1. Haga clic “X” para cerrar “requirió el cristal de los permisos”
2. Haga clic el “X para cerrar “cristal de las configuraciones el”

Usted ahora está detrás en el cristal registrado del app.

Prepare el evidente para la aplicación

Edite evidente

1. Del cristal registrado del app, haga clic evidente en la barra de herramienta
2. Le presentan el completo manifiesta en el editor. Encuentre la línea exisiting de los “keyCredentials”. Usted substituirá SOLAMENTE los “keyCredentials” por el siguiente:

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

3. Usted necesitará substituir $base64Thumbprint, $keyid, y $base64Value por sus valores Deje las citas ("") alrededor de TODOS LOS valores, como se muestraPreste la especial atención que cada valor es SOLAMENTE 1 línea, incluyendo el $base64Thumbprint
4. Haga clic la **salvaguardia** para poner al día su aplicación. Usted debe ver el aviso “de la aplicación con éxito actualizada” en el área de la barra de herramientas.

Usted necesitará volver al cristal registrado del app para proceder con la siguiente sección:

El tecleo “X” para cerrar “edita” el cristal evidente.

(Opcional) descargue el evidente

> **Tip**: Usted puede saltar la descarga evidente y cargar evidente si usted podía con éxito utilizar el editor de en-Azure para el evidente. Si no, y usted necesita editar manualmente el evidente, proceda por favor.

1. Del cristal registrado del app, tecleo evidente en la barra de herramienta
2. En la **descarga** evidente del tecleo del menú del editar
3. Salve el evidente al directorio que contiene su certificado. Esto salvará el evidente en el formato .json localmente a su ordenador.
4. Usando un editor local (Wordpad++, átomo, etc.), los pasos completos 2 y 3 del “editan” la sección evidente de este documento
5. Salve el archivo evidente .json localmente

(Opcional) cargue el evidente

Si usted eligió descargar y editó el evidente manualmente, usted necesitará cargar el evidente editada:

1. Vuelva a su navegador y al portal de Azure
2. **La carga del** tecleo del “edita” el cristal evidente

Usted necesitará volver al cristal registrado del app para proceder con la siguiente sección:

El tecleo “X” para cerrar “edita” el cristal evidente.

Consiga el ID de cliente para la aplicación

1. Del app registrado encuentre el “ID de la aplicación”
2. Copie el ID de la aplicación (ID de la aplicación = el *ID de cliente*)
3. Agregue este valor a su lista de los requisitos previos de valores requeridos.

Consiga el valor del arrendatario ID para la aplicación

1. “Del cristal de los registros del App”, haga clic en los “puntos finales” y seleccione la primera línea para el DOCUMENTO de los META DATOS de la FEDERACIÓN
2. La copia y pega la línea a un editor externo
3. Usted querrá extraer al *arrendatario ID*, que es la cadena de ID después de “https://login.windows.net/”
4. Agregue este valor a su lista de los requisitos previos de valores requeridos.

Ejemplo:

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
```

```
}
],
```

Por este ejemplo, el arrendatario ID será el "ed437e13-ba50-479e-b40d-8affa4f7e1d7".

Verifique los valores requeridos

Sus valores ahora se completan. Usted debe poder completar los valores siguientes:

- ID de cliente
- Arrendatario ID
- Thumbprint (véase los requisitos previos)
- Certifique la clave privada en el formato del .pem (véase los requisitos previos)

Usted está listo para completar las configuraciones del buzón de la oficina 365 configurando estos valores en el ESA.

Configure el ESA

1. En el ESA GUI: **Las configuraciones de la administración del sistema > del buzón > editan las configuraciones…**
2. Ingrese en sus valores de la sección anterior (ID de cliente, arrendatario ID, Thumbprint)
3. Cargue el certificado guardado (el .pem)
4. El tecleo **somete**
5. Usted verá que “las configuraciones fueron configuradas con éxito. Usted debe confiar los cambios y probar la conexión.”
6. De la esquina derecha superior, el **cometer del** tecleo **cambia** antes de cualquier prueba
7. Tecleo “conexión del control…” y ingrese en una dirección email buena, de trabajo sabida asociada a su dominio O365
8. Haga clic la “conexión de prueba”

Usted debe recibir los resultados del éxito en el estado de la conexión:

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

Resolver problemas el ESA

Si usted no está viendo que los resultados acertados para el estado de la conexión prueban, usted puede desear revisar el registro de la aplicación realizado del Azure AD.

Del ESA, fije los registros de MARCHA al nivel de traza y reexamine la conexión.

Para las conexiones fracasadas, los registros pueden mostrar similar a:

```
"keyCredentials": [
```

```
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value": "$base64Value"
}
],
```

Confirme el ID de la aplicación, el directorio ID (que es lo mismo que el arrendatario ID), u otros identificadores asociados del registro con su aplicación en el Azure AD. Si usted es inseguro de los valores, borre la aplicación del Azure AD porta y comience encima.

Para la conexión satisfactoria, los registros deben ser similares a:

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

Resolver problemas el Azure AD

> **Note**: El TAC de Cisco y el soporte de Cisco no se dan derecho a resolver problemas los problemas de lado del cliente con el Microsoft Exchange, el Microsoft Azure AD, o la oficina 365.

Para los problemas de lado del cliente con el Microsoft Azure AD, usted necesitará dedicar el soporte de Microsoft. Vea por favor la opción de la “ayuda + del soporte” de su panel del Microsoft Azure. Usted puede poder abrir las peticiones del soporte directo en el soporte de Microsoft del panel.

(Opcional) cómo crear y configurar una aplicación en Azure usando el portal clásico

> **Note**: Usted no necesita completar esto si usted podía con éxito utilizar el portal de Azure accediendo https://portal.azure.com (nuevo portal). Esto se refiere solamente para el administrador azul que elige todavía utilizar el “portal clásico”. Si usted desea utilizar esta versión del portal del Azure AD, encuentre por favor las instrucciones paso a paso siguientes para completar los valores requeridos:

Agregue una aplicación

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

APLICACIONES

5. Del área inferior de la barra de herramientas, el tecleo **AGREGA**
6. *¿*Cuando está presentado *"qué usted quiere hacer? "*, selecto **agregue una aplicación que mi organización está desarrollando**
7. Complete "*nos hablan la* información de *su aplicación*": Cree un nombre para su appPara Application type (Tipo de aplicación), váyase como la **aplicación de Web y/o red API**Haga clic en la flecha para continuar
8. Complete las propiedades del App: Para MUESTRA-EN EL URL, utilice el formato siguiente: https:// *<Office365_assigned_company_domain.com>/ManualRegistration***Note**: *<company_domain.com> es el* dominio de su O365 donde los Domain User pueden ingresar y acceder su dominio O365.Para IDENTIFICACIÓN APP URI, utilice el formato siguiente: https:// < *Office365_assigend_company_domain.com* >Haga clic la marca de cotejo para completar

Configure su aplicación

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. **El ID de cliente se enumera en esta pantalla. Copie y agregue** este valor a su lista de los requisitos previos de valores requeridos.
3. Navegue a la parte inferior de la pantalla para ver los "permisos a otras aplicaciones".
4. El tecleo **agrega la aplicación El Online** selecto del **intercambio de la oficina 365** y hace clic el control para continuarPara los **permisos de la aplicación**, selecto: **Lea y escriba el correo en todos los buzonesEnvíe el correo como cualquier usuarioUtilice los servicios web del intercambio con el acceso total…**Para los permisos Delegated, selecto: **Envíe el correo como usuarioLea y escriba el correo del usuarioLea el correo del usuarioAcceda los buzones como el usuario ingresado vía el intercambio**
5. Haga clic la **salvaguardia de la** barra de herramientas inferior para salvar todo el trabajo y configuración para la aplicación de Web de encargo

Maneje 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. Localmente, encuentre el archivo .json y ábrase con un editor de textos. (Notepad++ preferible, átomo, etc.)
4. Busque y encuentre la línea de los "keyCredentials"
5. Reemplazo de esta sola línea con las líneas múltiples siguientes, personalizando usando el *$base64Thumbprint*, el *$keyid*, y el *$base64Value*:

```
"keyCredentials": [
{
"customKeyIdentifier": "$base64Thumbprint",
"keyId": "$keyid",
"type": "AsymmetricX509Cert",
"usage": "Verify",
```

```
"value": "$base64Value"
}
],
```

6. Al ingresar el *$base64Value*, esto se requiere ser editada a un valor de la sola línea
7. Salve el archivo .json localmente
8. Vuelva a su navegador y al portal del Microsoft Azure
9. El tecleo **MANEJA EVIDENTE > carga evidente**
10. Hojee y encuentre el archivo editado .json
11. Seleccione la marca de tilde para completar la carga

Encontrar al arrendatario ID

1. De la barra de herramientas inferior, haga clic en los **PUNTOS FINALES de la VISIÓN** para ver los puntos finales integrados en el Azure AD de Microsoft
2. Seleccione la primera línea para el DOCUMENTO de los META DATOS de la FEDERACIÓN
3. La copia y pega la línea a un editor externo
4. Usted querrá extraer al *arrendatario ID*, que es la cadena de ID después de "https://login.windows.net/"
5. Agregue este valor a su lista de los requisitos previos de valores requeridos

Ejemplo:

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

Por este ejemplo, el arrendatario ID será el "ed437e13-ba50-479e-b40d-8affa4f7e1d7".

Información Relacionada

- Dispositivo de seguridad del correo electrónico de Cisco - Soporte de productos
- Dispositivo de seguridad del correo electrónico de Cisco - Release Note
- Dispositivo de seguridad del correo electrónico de Cisco - Guías del usuario final