Solucionar problemas de autenticación ECE OAUTH2 con Office 365

Contenido

Introducción

Este documento describe los pasos para resolver problemas de la integración de Enterprise Chat and Email (ECE) con el correo electrónico de Microsoft Office 365 (O365).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Chat y correo electrónico empresarial (ECE) 12.6
- Microsoft Office 365 (O365)
- Microsoft Azure Active Directory (Azure AD)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- CEPE 12.6(1)
- Azure AD
- O365

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Background

Microsoft ha desaprobado formalmente la autenticación básica con las cuentas de correo electrónico O365. Esto se anunció en 2019 y se retrasó hasta octubre de 2022 debido a la COVID-19. Incluso después de la fecha límite de octubre de 2022, Microsoft permitió que se volviera a habilitar la autenticación básica por última vez. Esta excepción final finalizó el 31 de diciembre de 2022. Después de esta fecha, Microsoft ya no permite la autenticación básica para ningún cliente.

Los elementos de esta lista de comprobación provienen de solicitudes de servicio en las que el TAC ha colaborado con los clientes para configurar esta función. Debido a cómo se otorga la licencia de O365 y Azure AD, TAC no tiene la capacidad de recrear o verificar estos elementos en un laboratorio. Si necesita ayuda con alguno de estos procedimientos, póngase en contacto con el servicio de asistencia de Microsoft o con su equipo de asistencia de TI interno.

Comprobar elementos

Versión mínima

El soporte de OAuth para ECE con O365 se introdujo en las ofertas especiales de ingeniería para ECE como respuesta a la identificación de error de Cisco CSCvr86493 . Debe asegurarse de que ECE tiene instalado el ES correcto y de que se utiliza la documentación correcta.

- ECE 11.6(1) - Requiere ES12 Y ES12_ET1

- ECE 12.0(1): requiere ES6
- ECE 12.5(1): requiere ES3
- ECE 12.6(1): requiere ES1

Se recomienda instalar el ES más reciente disponible para su versión.

Configuración del sistema

La URL web debe estar configurada correctamente. El entorno específico cambia en función de la versión de ECE. Debe configurarse para que coincida con la URL que utilizan los agentes y los administradores para iniciar sesión en ECE y tiene el formato de, https://ece.example.com.

Configuración del nombre en cada versión:

11.5 - 12.5: Configuración del nivel de partición, "URL del servidor web o URL del equilibrador de carga"

12.6 + : Partición > Aplicaciones > Configuración general > "URL externo de la aplicación"

Esta configuración también se utiliza para el inicio de sesión único (SSO) y para el HTML predeterminado para el punto de entrada del chat. En las versiones anteriores al lanzamiento de OAuth para O365, esta configuración no era obligatoria a menos que se usara el SSO del agente. En todas las implementaciones que utilizan OAuth, se debe configurar. Además, debe coincidir con el FQDN utilizado para iniciar sesión en la consola de administración.

Aplicación de Azure AD

Asegúrese de seguir exactamente la documentación al configurar la aplicación de Azure AD.

Notas específicas:

1. URL de redirección: el FQDN debe coincidir con la configuración de URL externa de la aplicación en ECE y debe utilizarse al acceder a la consola de administración.
2. Token de acceso: el token de actualización debe durar 60 minutos.

Generación de tokens

El proceso de generación de tokens es uno de los pasos más importantes en el proceso de configuración. La práctica recomendada es asegurarse de que el explorador se ha abierto en modo incógnito o privado antes de intentar emitir el token. Esto solicita al usuario las credenciales. Asegúrese de que el usuario para el que se crea el token tiene control total del buzón.

La explicación de esto es que la mayoría de los clientes también utilizan Azure AD para la autenticación de usuarios. Cuando un usuario abre un explorador, sus credenciales se pasan a través de Kerberos a los sitios login.microsoft.com. Esto, a su vez, hace que se emita el token para el usuario que inició sesión en la estación de trabajo o el servidor en lugar de una cuenta que pueda acceder al buzón.

Configuración del buzón

Asegúrese de que el buzón tiene habilitados los protocolos necesarios. Como mínimo, SMTP debe estar habilitado para permitir que se envíe correo. También debe activar IMAP o POP3 en función del diseño.

Licencia de Exchange

Asegúrese de que se haya asignado al menos una licencia E3 al buzón de Exchange Online.

Derechos de buzón

ECE admite dos tipos de cuentas de usuario para el acceso al buzón de correo.

1. Cuenta de buzón: este método requiere que cree una cuenta y un token de acceso para cada buzón que desee que se compruebe ECE. Por ejemplo, si tiene dos buzones, sales@example.com y support@example.com, debe crear dos cuentas de correo electrónico en el departamento. Para una cuenta, debe crear el token e iniciar sesión con el nombre de usuario y la contraseña sales@example.com. El segundo token de cuenta se debe crear con el nombre de usuario y la contraseña support@example.com.

2. Cuenta compartida: este método permite utilizar una única cuenta de correo que puede acceder a varios buzones. Para continuar usando los buzones de ventas y de soporte, aquí debe crear una cuenta única, pero debe crear el token con un nombre de usuario y una contraseña para una cuenta de Azure AD a la que se haya otorgado control total de los buzones.

Ambos métodos de acceso tienen pros y contras, pero depende de usted decidir cuál es la mejor para su entorno específico.

Conectividad de red

ECE requiere que el servidor de servicios y todos los servidores de aplicaciones puedan acceder a los dominios O365, así como a los dominios login.microsoft.com. La creación inicial de tokens se produce desde el servidor de aplicaciones, mientras que todas las actualizaciones de tokens posteriores se producen en el servidor de servicios. El servidor de servicios tiene los procesos de recuperador y despachador, por lo que los puertos IMAP/POP3 y SMTP deben estar abiertos para este servidor. Además, el servidor de aplicaciones debe poder enviar correos electrónicos para que funcionen las notificaciones de alarma. Verifique que todos los puertos indicados en la Guía de instalación se hayan abierto antes de intentar configurar o utilizar las integraciones O365.

URL

Tanto el servidor de servicios como el de aplicaciones deben poder acceder a estas URL como mínimo.

- *.office365.com

-login.microsoftonline.com

Puede haber direcciones URL adicionales necesarias para su implementación específica.

Puertos

Tanto el servidor de servicios como el de aplicaciones deben poder acceder a estos puertos como mínimo.

- TCP 443: (HTTPS) se utiliza para generar y actualizar los tokens de acceso y actualización

- TCP 587 - (SMTP sobre STARTTLS) Utilizado por el proceso del despachador y el proceso de notificación de alarma

- TCP 993 - (IMAP sobre SSL/TLS) Utilizado por el proceso de recuperación

- TCP 995 - (POP3 sobre SSL/TLS) Utilizado por el proceso de recuperación

Referencia: configuración de POP, IMAP y SMTP

Prueba de conectividad

Microsoft ha creado un sitio web que se puede utilizar para probar la conectividad. Esta no es una herramienta proporcionada por Cisco o eGain y TAC no puede proporcionar ningún soporte sobre su uso. Puede utilizarla desde el servidor de aplicaciones y servicios para probar la configuración y la conectividad. ECE sólo admite SMTP para tráfico saliente y IMAP o POP3 para tráfico entrante. Utilice la prueba de correo electrónico SMTP saliente junto con las pruebas de correo electrónico POP e IMAP del sitio web de Microsoft.

https://testconnectivity.microsoft.com/tests/o365

Enlaces de documentación

11.6(1)

- UCCE/PCCE: Guía del administrador para recursos de correo electrónico

12.0(1)

- UCCE: Guía del administrador para recursos de correo electrónico (UCCE)
- PCCE: Guía del administrador para recursos de chat y correo electrónico (PCCE)

12.5(1)

- UCCE: Guía del administrador para recursos de correo electrónico (UCCE)
- PCCE: Guía del administrador para recursos de chat y correo electrónico (PCCE)

12.6(1)

- UCCE/PCCE: Guía del administrador para recursos de correo electrónico y routing

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).