Fehlerbehebung bei ECE OAUTH2-Authentifizierung mit Office 365

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Fehlerbehebung bei Enterprise Chat und E-Mail (ECE)-Integration mit Microsoft Office 365 (O365) E-Mail beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Enterprise Chat und E-Mail (ECE) 12.6
- Microsoft Office 365 (OS 365)
- Microsoft Azure Active Directory (Azure AD)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- ECE 12.6(1)
- Azure AD
- O365

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrund

Microsoft hat die grundlegende Authentifizierung mit O365-E-Mail-Konten offiziell verworfen. Dies wurde im Jahr 2019 angekündigt, dann wurde bis Oktober 2022 wegen COVID-19 verschoben. Selbst nach Ablauf der Frist im Oktober 2022 hat Microsoft die erneute Aktivierung der grundlegenden Authentifizierung ein letztes Mal zugelassen. Diese letzte Ausnahme endete am 31. Dezember 2022. Nach diesem Datum aktiviert Microsoft keine Standardauthentifizierung mehr für Kunden.

Die Elemente in dieser Checkliste stammen aus Serviceanfragen, bei denen das TAC mit Kunden zusammengearbeitet hat, um diese Funktion zu konfigurieren. Aufgrund der Lizenzierung von O365 und Azure AD kann das TAC diese Elemente in einer Übung nicht neu erstellen oder überprüfen. Wenn Sie Hilfe bei einem dieser Probleme benötigen, wenden Sie sich an den Microsoft-Support oder Ihr internes IT-Supportteam.

Elemente überprüfen

Mindestversion

Die OAuth-Unterstützung für ECE mit O365 wurde in Engineering Specials für ECE als Reaktion auf den Cisco Bug CSCvr86493 eingeführt. . Sie müssen sicherstellen, dass bei ECE das richtige ES installiert ist und die richtige Dokumentation verwendet wird.

- ECE 11.6(1) - Erfordert ES12 UND ES12_ET1
- ECE 12.0(1) - erfordert ES6
- ECE 12.5(1) - erfordert ES3
- ECE 12.6(1) - Erfordert ES1

Als Best Practice sollten Sie die neueste Version von ES installieren, die für Ihre Version verfügbar ist.

Systemkonfiguration

Die Web-URL muss korrekt konfiguriert sein. Die spezifischen Einstellungen ändern sich je nach ECE-Version. Diese muss so konfiguriert werden, dass sie mit der URL übereinstimmt, die Agenten und Administratoren für die Anmeldung bei ECE verwenden. Sie hat das Format https://ece.example.com.

Name für jede Version:

11.5 - 12.5: Einstellung auf Partitionsebene, "Webserver-URL oder Load Balancer-URL"

12.6 + : Partition > Apps > Allgemeine Einstellungen > "Externe URL der Anwendung"

Diese Einstellung wird auch für die einmalige Anmeldung (Single Sign-On, SSO) und für den Standard-HTML-Code für den Chat-Einstiegspunkt verwendet. In Versionen vor der Veröffentlichung von OAuth für O365 war diese Einstellung nicht obligatorisch, es sei denn, der Agent SSO wurde verwendet. Bei allen Bereitstellungen, die OAuth verwenden, muss dies konfiguriert werden. Darüber hinaus muss dies mit dem FQDN übereinstimmen, der für die Anmeldung bei der Admin-Konsole verwendet wird.

Azure AD-Anwendung

Befolgen Sie die Dokumentation genau, wenn Sie die Azure AD-Anwendung konfigurieren.

Spezifische Hinweise:

1. Umleitungs-URL: Der FQDN muss mit der Einstellung für die externe URL der Anwendung in ECE übereinstimmen und beim Zugriff auf die Admin-Konsole verwendet werden.
2. Zugriffstoken: Das Aktualisierungstoken muss eine Dauer von 60 Minuten haben.

Tokenerstellung

Die Tokenerstellung ist einer der wichtigsten Schritte im Konfigurationsprozess. Als Best Practice sollten Sie sicherstellen, dass der Browser im Inkognito- oder privaten Modus geöffnet wurde, bevor Sie versuchen, das Token auszugeben. Der Benutzer wird zur Eingabe der Anmeldeinformationen aufgefordert. Stellen Sie sicher, dass der Benutzer, für den das Token erstellt wird, die vollständige Kontrolle über das Postfach hat.

Die Erklärung hierfür ist, dass die meisten Kunden Azure AD auch für die Benutzerauthentifizierung verwenden. Wenn ein Benutzer einen Browser öffnet, werden seine Anmeldeinformationen über Kerberos an die Websites login.microsoft.com weitergeleitet. Dies wiederum führt dazu, dass das Token für den Benutzer ausgestellt wird, der an der Workstation oder dem Server angemeldet ist, und nicht für ein Konto, das auf die Mailbox zugreifen kann.

Mailbox-Konfiguration

Stellen Sie sicher, dass für die Mailbox die erforderlichen Protokolle aktiviert sind. SMTP muss mindestens aktiviert sein, damit E-Mails versendet werden können. Sie müssen je nach Design auch IMAP oder POP3 aktivieren.

Exchange-Lizenz

Stellen Sie sicher, dass dem Postfach in Exchange Online mindestens eine E3-Lizenz zugewiesen wurde.

Postfachrechte

ECE unterstützt zwei Arten von Benutzerkonten für den Postfachzugriff.

1. Postfachkonto: Für diese Methode müssen Sie ein Konto und ein Zugriffstoken für jedes Postfach erstellen, für das Sie eine ECE-Prüfung wünschen. Wenn Sie beispielsweise zwei Mailboxen haben, sales@example.com und support@example.com, müssen Sie zwei E-Mail-Konten in der Abteilung erstellen. Für ein Konto müssen Sie das Token erstellen und sich mit dem Benutzernamen und dem Kennwort sales@example.com anmelden. Das zweite Konto-Token muss mit dem Benutzernamen und dem Kennwort support@example.com erstellt werden.

2. Freigegebenes Konto - Mit dieser Methode können Sie ein einzelnes E-Mail-Konto verwenden, das auf mehrere Postfächer zugreifen kann. Um die Vertriebs- und Support-Mailboxen weiter zu verwenden, erstellen Sie hier ein einzelnes Konto, erstellen jedoch das Token mit einem Benutzernamen und Kennwort für ein Azure AD-Konto, das die volle Kontrolle über die Mailboxen erhält.

Beide Zugriffsmethoden haben Vor- und Nachteile, Sie können jedoch selbst entscheiden, welche für Ihre spezifische Umgebung am besten geeignet ist.

Netzwerkverbindungen

ECE setzt voraus, dass der Dienstserver und alle Anwendungsserver auf die O365-Domänen sowie die login.microsoft.com-Domänen zugreifen können. Die erste Tokenerstellung erfolgt vom Anwendungsserver, während alle nachfolgenden Tokenaktualisierungen auf dem Dienstserver erfolgen. Da der Retriever- und der Dispatcher-Prozess auf dem Dienstserver ausgeführt werden, müssen die IMAP-/POP3- und SMTP-Ports für diesen Server offen sein. Darüber hinaus muss der Anwendungsserver in der Lage sein, E-Mails zu senden, damit Alarmmeldungen funktionieren. Überprüfen Sie, ob alle im Installationshandbuch genannten Ports geöffnet wurden, bevor Sie versuchen, O365-Integrationen einzurichten oder zu verwenden.

URL

Sowohl der Dienstserver als auch der Anwendungsserver müssen mindestens auf diese URLs zugreifen können.

- *.office365.com

-login.microsoftonline.com

Für Ihre spezifische Implementierung können weitere URLs erforderlich sein.

Ports

Sowohl der Dienstserver als auch der Anwendungsserver müssen mindestens auf diese Ports zugreifen können.

- TCP 443 - (HTTPS) Wird zum Generieren und Aktualisieren von Zugriffs- und Aktualisierungstoken verwendet

- TCP 587 - (SMTP über STARTTLS) Wird vom Dispatcher-Prozess und vom Alarmbenachrichtigungsprozess verwendet

- TCP 993 - (IMAP über SSL/TLS) Wird vom Retriever-Prozess verwendet

- TCP 995 - (POP3 über SSL/TLS) Wird vom Retriever-Prozess verwendet

Referenz: POP-, IMAP- und SMTP-Einstellungen

Verbindungstest

Microsoft hat eine Website erstellt, mit der die Konnektivität getestet werden kann. Es handelt sich nicht um ein von Cisco oder von eGain bereitgestelltes Tool, und das TAC kann bei seiner Verwendung keinen Support bereitstellen. Sie können diese Funktion auf dem Anwendungs- und Dienstserver verwenden, um Ihre Konfiguration und Konnektivität zu testen. ECE unterstützt nur SMTP für ausgehenden und entweder IMAP oder POP3 für eingehenden Datenverkehr. Verwenden Sie den Test für ausgehende SMTP-E-Mails zusammen mit den POP-E-Mail- und IMAP-E-Mail-Tests der Microsoft-Website.

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

Dokumentations-Links

11.6(1)

- **UCCE/PCCE** - Administratorhandbuch für E-Mail-Ressourcen

12.0(1)

- **UCCE** - Administratorhandbuch für E-Mail-Ressourcen (UCCE)
- **PCCE** - Administratorhandbuch für Chat- und E-Mail-Ressourcen (PCCE)

12.5(1)

- **UCCE** - Administratorhandbuch für E-Mail-Ressourcen (UCCE)
- **PCCE** - Administratorhandbuch für Chat- und E-Mail-Ressourcen (PCCE)

12.6(1)

- **UCCE/PCCE** - Administratorhandbuch für E-Mail- und Routing-Ressourcen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.