Dépannage de l'authentification ECE OAUTH2 avec Office 365

Table des matières

Introduction

Ce document décrit les étapes de dépannage de l'intégration de la messagerie instantanée et de la messagerie électronique d'entreprise (ECE) avec la messagerie électronique Microsoft Office 365 (O365).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Chat et e-mail d'entreprise (ECE) 12.6
- Microsoft Office 365 (O365)

- Microsoft Azure Active Directory (Azure AD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- CEE 12.6 1)
- Azure AD
- O365

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Fond

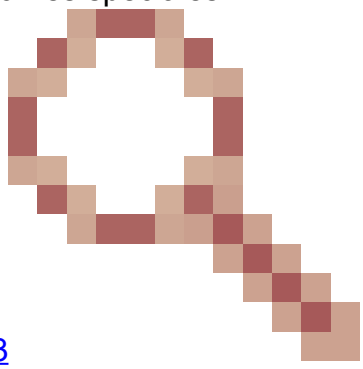
Microsoft a officiellement déconseillé l'authentification de base avec les comptes de messagerie O365. Cette décision a été annoncée en 2019, puis a été reportée à octobre 2022 en raison de la COVID-19. Même après la date limite d'octobre 2022, Microsoft a autorisé une dernière réactivation de l'authentification de base. Cette dernière exception a pris fin le 31 décembre 2022. Après cette date, Microsoft n'active plus l'authentification de base pour les clients.

Les éléments de cette liste de contrôle proviennent de demandes de service pour lesquelles le centre d'assistance technique a travaillé avec des clients pour configurer cette fonctionnalité. En raison de la manière dont O365 et Azure AD sont concédés sous licence, le centre d'assistance technique ne peut pas recréer ou vérifier ces éléments dans un TP. Si vous avez besoin d'aide sur l'un de ces points, contactez le support technique de Microsoft ou votre équipe d'assistance informatique interne.

Vérifier les éléments

Version minimale

La prise en charge OAuth pour ECE avec O365 a été introduite dans les offres spéciales



d'ingénierie pour ECE en réponse au bogue Cisco ayant l'ID CSCvr86493
. Vous devez vous assurer que l'ECE est correctement installé et que la documentation appropriée est utilisée.

- ECE 11.6(1) - Requiert ES12 ET ES12_ET1

- ECE 12.0(1) - Requiert ES6
- ECE 12.5(1) - Requiert ES3
- ECE 12.6(1) - Requiert ES1

La meilleure pratique consiste à installer la dernière version d'ES disponible pour votre version.

Configuration système

L'URL Web doit être configurée correctement. Le réglage spécifique change en fonction de la version de la CEE. Cette adresse doit être configurée de manière à correspondre à l'URL que les agents et les administrateurs utilisent pour se connecter à l'ECE. Elle est au format suivant : https://ece.example.com.

Nom du paramètre dans chaque version :

11.5 - 12.5 : Paramètre de niveau de partition, "URL de serveur Web ou URL d'équilibrage de charge"

12.6 + : Partition > Apps > General Settings > "External URL of Application"

Ce paramètre est également utilisé pour l'authentification unique (SSO) et pour le code HTML par défaut du point d'entrée de conversation. Dans les versions antérieures à la version d'OAuth pour O365, ce paramètre n'était pas obligatoire, sauf si l'agent SSO était utilisé. Dans tous les déploiements qui utilisent OAuth, ce paramètre doit être configuré. En outre, il doit correspondre au nom de domaine complet utilisé pour se connecter à la console d'administration.

Application Azure AD

Assurez-vous de suivre la documentation exactement lorsque vous configurez l'application Azure AD.

Remarques spécifiques :

1. URL de redirection : le nom de domaine complet doit correspondre au paramètre URL externe de l'application dans ECE et doit être utilisé lorsque vous accédez à la console d'administration.
2. Jeton d'accès : le jeton d'actualisation doit durer 60 minutes.

Génération de jeton

Le processus de génération de jeton est l'une des étapes les plus importantes du processus de configuration. La meilleure pratique consiste à vous assurer que le navigateur a été ouvert en mode incognito ou privé avant de tenter d'émettre le jeton. L'utilisateur est invité à saisir ses informations d'identification. Assurez-vous que l'utilisateur pour lequel le jeton est créé a le contrôle total de la boîte aux lettres.

La plupart des clients utilisent également Azure AD pour l'authentification des utilisateurs. Lorsqu'un utilisateur ouvre un navigateur, ses informations d'identification sont transmises via

Kerberos aux sites login.microsoft.com. Ceci, à son tour, provoque l'émission du jeton pour l'utilisateur connecté à la station de travail ou au serveur plutôt qu'un compte qui peut accéder à la boîte aux lettres.

Configuration des boîtes aux lettres

Assurez-vous que les protocoles requis sont activés pour la boîte aux lettres. SMTP doit au minimum être activé pour permettre l'envoi de messages. Vous devez également activer IMAP ou POP3 en fonction de la conception.

Licence Exchange

Assurez-vous qu'au moins une licence E3 a été attribuée à la boîte aux lettres dans Exchange Online.

Droits de boîte aux lettres

ECE prend en charge deux types de comptes utilisateur pour l'accès aux boîtes aux lettres.

1. Compte de boîte aux lettres : cette méthode nécessite la création d'un compte et d'un jeton d'accès pour chaque boîte aux lettres que vous souhaitez faire vérifier par ECE. Par exemple, si vous avez deux boîtes de messagerie, sales@example.com et support@example.com, alors vous devez créer deux comptes de messagerie dans le service. Pour un compte, vous devez créer le jeton et la connexion avec le nom d'utilisateur et le mot de passe sales@example.com. Le deuxième jeton de compte doit être créé avec le nom d'utilisateur et le mot de passe support@example.com.

2. Compte partagé : cette méthode vous permet d'utiliser un compte de messagerie unique pouvant accéder à plusieurs boîtes aux lettres. Pour continuer à utiliser les boîtes aux lettres de vente et d'assistance, créez ici un compte unique, mais créez le jeton avec un nom d'utilisateur et un mot de passe pour un compte Azure AD qui a reçu le contrôle total des boîtes aux lettres.

Les deux méthodes d'accès ont des avantages et des inconvénients, mais c'est à vous de décider laquelle est la meilleure pour votre environnement spécifique.

Connectivité réseau

L'ECE exige que le serveur de services et tous les serveurs d'applications puissent accéder aux domaines O365 ainsi qu'aux domaines login.microsoft.com. La création initiale du jeton se produit à partir du serveur d'applications, tandis que toutes les mises à jour de jeton suivantes se produisent sur le serveur de services. Le serveur de services dispose des processus de récupérateur et de répartiteur, de sorte que les ports IMAP/POP3 et SMTP doivent être ouverts sur ce serveur. En outre, le serveur d'applications doit être en mesure d'envoyer des e-mails pour que les notifications d'alarme fonctionnent. Vérifiez que tous les ports indiqués dans le Guide d'installation ont été ouverts avant de tenter de configurer ou d'utiliser les intégrations O365.

URL

Le serveur de services et le serveur d'applications doivent pouvoir accéder à ces URL au minimum.

- *.office365.com

-login.microsoftonline.com

Il peut y avoir des URL supplémentaires qui sont nécessaires pour votre implémentation spécifique.

Ports

Le serveur de services et le serveur d'applications doivent pouvoir accéder à ces ports au minimum.

- TCP 443 - (HTTPS) Utilisé pour générer et mettre à jour les jetons d'accès et d'actualisation

- TCP 587 - (SMTP sur STARTTLS) Utilisé par le processus du répartiteur et le processus de notification d'alarme

- TCP 993 - (IMAP sur SSL/TLS) Utilisé par le processus de récupération

- TCP 995 - (POP3 sur SSL/TLS) Utilisé par le processus de récupération

Référence : paramètres POP, IMAP et SMTP

Test de connectivité

Microsoft a créé un site Web qui peut être utilisé pour tester la connectivité. Il ne s'agit pas d'un outil fourni par Cisco ou eGain et le TAC ne peut fournir aucune assistance sur son utilisation. Vous pouvez l'utiliser à partir du serveur d'applications et de services pour tester votre configuration et votre connectivité. ECE prend uniquement en charge SMTP pour les appels sortants et IMAP ou POP3 pour les appels entrants. Utilisez le test E-mail SMTP sortant avec les tests E-mail POP et E-mail IMAP du site Web Microsoft.

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

Liens de documentation

11.6(1)

- UCCE/PCCE - Guide de l'administrateur des ressources de messagerie

12.0(1)

- UCCE - Guide de l'administrateur des ressources de messagerie (UCCE)
- PCCE - Guide de l'administrateur des ressources de conversation et de messagerie (PCCE)

12.5(1)

- UCCE - Guide de l'administrateur des ressources de messagerie (UCCE)
- PCCE - Guide de l'administrateur des ressources de conversation et de messagerie (PCCE)

12.6(1)

- UCCE/PCCE - Guide de l'administrateur des ressources de messagerie et de routage

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.