Troubleshoot ECE OAUTH2 Authentication with Office 365

Contents

Introduction

This document describes the steps to troubleshoot Enterprise Chat and Email (ECE) integration with Microsoft Office 365 (O365) email.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Enterprise Chat and Email (ECE) 12.6
- Microsoft Office 365 (O365)
- Microsoft Azure Active Directory (Azure AD)

Components used

The information in this document is based on these software versions:

- ECE 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. If your network is live, ensure that you understand the potential impact of any command.

Background

Microsoft has formally deprecated basic authentication with O365 email accounts. This was announced in 2019, then was delayed until October 2022 due to COVID-19. Even after the October 2022 deadline, Microsoft allowed basic authentication to be re-enabled one last time. This final exception ended on December 31, 2022. After this date, Microsoft no longer enables basic authentication for any customers.

The items in this check list come from service requests where TAC have worked with customers to get this feature configured. Due to how O365 and Azure AD is licensed, TAC does not have the ability to recreate or check these items in a lab. If you require help with any of these, please contact Microsoft support or your internal IT support team.

Check Items

Minimum Version

OAuth support for ECE with O365 was introduced in engineering specials for ECE as a response to Cisco bug ID CSCvr86493 . You must ensure that ECE has the correct ES installed and that the correct documentation is used.

- ECE 11.6(1) – Requires ES12 AND ES12_ET1
- ECE 12.0(1) – Requires ES6
- ECE 12.5(1) – Requires ES3
- ECE 12.6(1) – Requires ES1

Best practice is to install the latest ES available for your version.

System Configuration

The Web URL must be configured correctly. The specific setting changes based on the version of ECE. This must be configured to match the URL that agents and administrators use to login to ECE and is in the the format of, https://ece.example.com.

Setting name in each version:

11.5 - 12.5: Partition level setting, "Web server URL or Load Balancer URL"

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

This setting is also used for Single Sign-On (SSO) and for the default HTML for chat entry point. In versions prior to the release of OAuth for O365, this setting was not mandatory unless agent SSO was used. In all deployments that use OAuth, this must be configured. In addition, this must match the FQDN used to login to the admin console.

Azure AD Application

Ensure that you follow the documentation exactly when you configure the Azure AD application.

Specific notes:

1. Redirect URL – The FQDN must match the External URL of Application setting in ECE and must be used when you access the admin console.
2. Access Token – The refresh token must last 60 minutes.

Token Generation

The token generation process is one of the most important steps in the configuration process. The best practice is to ensure that the browser has been opened in incognito or private mode before you attempt to issue the token. This prompts the user for credentials. Ensure that the user for whom the token is created has full control of the mailbox.

The explanation for this is that most customers also use Azure AD for user authentication. When a user opens a browser, their credentials are passed through Kerberos to the login.microsoft.com sites. This, in turn, causes the token to be issued for the user logged into the workstation or server rather than an account which can access the mailbox.

Mailbox Configuration

Ensure that the mailbox has the required protocols enabled. At a minimum, SMTP must be enabled to allow mail to be dispatched. You must also enable either IMAP or POP3 based on design.

Exchange License

Ensure that at least an E3 license has been assigned to the mailbox in Exchange Online.

Mailbox Rights

ECE supports two types of user accounts for mailbox access.

1. Mailbox Account – This method requires that you create an account and access token for each mailbox you wish to have ECE check. For example, if you have two mailboxes, sales@example.com and support@example.com, then you must create two email accounts in the department. For one account, you must create the token and login with the sales@example.com username and password. The second account token must be created with the support@example.com username and password.

2. Shared Account – This method allows you to use a single mail account that can access multiple mailboxes. To continue the use of the sales and support mailboxes, here, you create a

single account but create the token with a username and password for an Azure AD account that has been given full control of the mailboxes.

Both access methods have pros and cons, but it is up to you to decide which is best for your specific environment.

Network Connectivity

ECE requires that the services server and all application servers can access the O365 domains as well as the login.microsoft.com domains. The initial token creation occurs from the application server while all subsequent token updates occur on the services server. The services server has the retriever and dispatcher processes on it, so the IMAP/POP3 and SMTP ports must be open to this server. In addition, the application server must be able to send emails for alarm notifications to work. Verify all ports called out in the Installation Guide have been opened before you attempt to setup or use O365 integrations.

URLs

Both the services server and application server must be able to access these URLs at a minimum.

- *.office365.com

- login.microsoftonline.com

There can be additional URLs which are required for your specific implementation.

Ports

Both the services server and application server must be able to access these ports at a minimum.

- TCP 443 – (HTTPS) Used to generate and update the access and refresh tokens

- TCP 587 – (SMTP over STARTTLS) Used by dispatcher process and alarm notification process

- TCP 993 – (IMAP over SSL/TLS) Used by retriever process

- TCP 995 – (POP3 over SSL/TLS) Used by retriever process

Reference: POP, IMAP, and SMTP settings

Connectivity Test

Microsoft has created a website that can be used to test connectivity. This is not a Cisco or eGain provided tool and TAC cannot provide any support on its use. You can use this from the application and services server to test your configuration and connectivity. ECE supports only SMTP for outbound and either IMAP or POP3 for inbound. Use the Outbound SMTP email test along with the POP Email and IMAP Email tests from the Microsoft website.

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

Documentation Links

11.6(1)

- **UCCE/PCCE** – Administrator's Guide to Email Resources

12.0(1)

- **UCCE** – Administrator's Guide to Email Resources (UCCE)
- **PCCE** – Administrator's Guide to Chat and Email Resources (PCCE)

12.5(1)

- **UCCE** – Administrator's Guide to Email Resources (UCCE)
- **PCCE** – Administrator's Guide to Chat and Email Resources (PCCE)

12.6(1)

- **UCCE/PCCE** – Administrator's Guide to Email and Routing Resources