

# Office 365로 ECE OAUTH2 인증 문제 해결

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경](#)

[항목 확인](#)

[최소 버전](#)

[시스템 컨피그레이션](#)

[Azure AD 응용 프로그램](#)

[토큰 생성](#)

[사서함 구성](#)

[Exchange 라이선스](#)

[사서함 권한](#)

[네트워크 연결](#)

[URL](#)

[포트](#)

[연결 테스트](#)

[문서 링크](#)

[11.6\(1\)](#)

[12.0\(1\)](#)

[12.5\(1\)](#)

[12.6\(1\)](#)

## 소개

이 문서에서는 ECE(Enterprise Chat and Email)와 Microsoft Office 365(O365) 이메일의 통합 문제를 해결하는 단계를 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- ECE 12.6(1)
- Azure AD
- O365

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경

Microsoft는 O365 전자 메일 계정을 통한 기본 인증을 공식적으로 중단했습니다. 이는 2019년 발표됐다가 코로나19로 인해 2022년 10월까지 연기됐다. 2022년 10월 기한 이후에도 Microsoft는 기본 인증을 마지막으로 한 번 다시 활성화할 수 있도록 허용했습니다. 이 최종 예외는 2022년 12월 31일에 종료되었다. 이 날짜가 지나면 Microsoft는 더 이상 모든 고객에게 기본 인증을 사용하지 않습니다.

이 검사 목록의 항목은 TAC이 이 기능을 구성하기 위해 고객과 협력한 서비스 요청에서 가져옵니다. O365 및 Azure AD의 라이선스 방식으로 인해 TAC에서는 이러한 항목을 랩에서 다시 만들거나 확인할 수 없습니다. 이 중 하나에 대한 도움이 필요한 경우 Microsoft 지원 또는 내부 IT 지원 팀에 문의하십시오.

## 항목 확인

### 최소 버전

Cisco 버그 ID CSCvr에 대한 응답으로 ECE의 엔지니어링 스페셜에서 O365를 통한 ECE에 대한 OAuth 지원이 [도입되었습니다86493](#). ECE에 올바른 ES가 설치되어 있고 올바른 문서가 사용되었는지 확인해야 합니다.

- ECE 11.6(1) - [ES12](#) 및 [ES12 ET1 필요](#)
- ECE 12.0(1) - [ES6 필요](#)
- ECE 12.5(1) - [ES3 필요](#)
- ECE 12.6(1) - [ES1 필요](#)

사용 중인 버전에 사용할 수 있는 최신 ES를 설치하는 것이 좋습니다.

### 시스템 컨피그레이션

웹 URL을 올바르게 구성해야 합니다. ECE 버전에 따라 특정 설정이 변경됩니다. 상담원 및 관리자가 ECE에 로그인하기 위해 사용하는 URL과 일치하도록 구성되어야 하며, 형식은 <https://ece.example.com>입니다.

각 버전의 이름 설정:

11.5 - 12.5: 파티션 수준 설정, "웹 서버 URL 또는 로드 밸런서 URL"

12.6 + : 파티션 > 앱 > 일반 설정 > "애플리케이션의 외부 URL"

이 설정은 SSO(Single Sign-On) 및 채팅 진입점의 기본 HTML에도 사용됩니다. O365에 대한

OAuth 릴리스 이전 버전에서는 에이전트 SSO를 사용하지 않는 한 이 설정이 필수 사항이 아닙니다. OAuth를 사용하는 모든 구축에서 이 컨피그레이션을 수행해야 합니다. 또한 이는 관리 콘솔에 로그인하는 데 사용되는 FQDN과 일치해야 합니다.

## Azure AD 응용 프로그램

Azure AD 응용 프로그램을 구성할 때 설명서를 정확히 따라야 합니다.

특정 참고 사항:

1. Redirect URL(리디렉션 URL) - FQDN은 ECE의 External URL of Application(애플리케이션 외부 URL) 설정과 일치해야 하며 관리 콘솔에 액세스할 때 사용해야 합니다.
2. Access Token(액세스 토큰) - 새로 고침 토큰은 60분 동안이어야 합니다.

## 토큰 생성

토큰 생성 프로세스는 구성 프로세스에서 가장 중요한 단계 중 하나입니다. 가장 좋은 방법은 토큰을 발급하기 전에 브라우저가 익명 또는 개인 모드로 열려 있는지 확인하는 것입니다. 사용자에게 자격 증명을 묻는 프롬프트가 표시됩니다. 토큰을 만든 사용자에게 사서함에 대한 모든 권한이 있는지 확인합니다.

이에 대한 설명은 대부분의 고객이 사용자 인증에 Azure AD도 사용한다는 것이다. 사용자가 브라우저를 열면 자격 증명이 Kerberos를 통해 login.microsoft.com 사이트로 전달됩니다. 이렇게 하면 사용자가 사서함에 액세스할 수 있는 계정이 아닌 워크스테이션 또는 서버에 로그인한 사용자에 대해 토큰이 발급됩니다.

## 사서함 구성

사서함에 필요한 프로토콜이 활성화되어 있는지 확인합니다. 최소한 SMTP를 활성화하여 메일 발송을 허용해야 합니다. 또한 설계에 따라 IMAP 또는 POP3를 활성화해야 합니다.

## Exchange 라이선스

Exchange Online의 사서함에 E3 라이선스가 하나 이상 할당되었는지 확인하십시오.

## 사서함 권한

ECE는 사서함 액세스를 위해 두 가지 유형의 사용자 계정을 지원합니다.

1. 사서함 계정 - 이 방법을 사용하려면 ECE 확인을 받고자 하는 각 사서함에 대한 계정 및 액세스 토큰을 만들어야 합니다. 예를 들어, 두 개의 사서함(sales@example.com과 [support@example.com](#))이 있는 경우 부서에 두 개의 이메일 계정을 만들어야 합니다. 하나의 계정에 대해 토큰을 생성하고 sales@example.com 사용자 이름과 **비밀번호**로 로그인해야 합니다. 두 번째 계정 토큰은 support@example.com 사용자 이름과 **비밀번호**를 사용하여 생성해야 합니다.

2. 공유 계정 - 이 방법을 사용하면 여러 사서함에 액세스할 수 있는 단일 메일 계정을 사용할 수 있습니다. 여기서 판매 및 지원 사서함의 사용을 계속하려면 단일 계정을 만들되 사서함에 대한 모든 권한이 부여된 Azure AD 계정에 대한 사용자 이름 및 암호로 토큰을 만듭니다.

두 가지 액세스 방법 모두 장단점이 있지만 특정 환경에 가장 적합한 액세스 방법을 결정하는 것은

사용자의 책임입니다.

## 네트워크 연결

ECE에서는 서비스 서버 및 모든 애플리케이션 서버가 O365 도메인 및 login.microsoft.com 도메인에 액세스할 수 있어야 합니다. 모든 후속 토큰 업데이트가 서비스 서버에서 발생하는 동안 응용 프로그램 서버에서 초기 토큰 생성이 발생합니다. 서비스 서버에는 검색기 및 디스패처 프로세스가 있으므로 이 서버에 대해 IMAP/POP3 및 SMTP 포트가 열려 있어야 합니다. 또한 애플리케이션 서버는 경보 알림이 작동하도록 이메일을 보낼 수 있어야 합니다. O365 통합을 설정하거나 사용하기 전에 Installation Guide에서 호출된 모든 포트가 열려 있는지 확인합니다.

## URL

서비스 서버와 애플리케이션 서버 모두 최소한 이러한 URL에 액세스할 수 있어야 합니다.

- \*.office365.com

-login.microsoftonline.com

특정 구현에 필요한 추가 URL이 있을 수 있습니다.

## 포트

서비스 서버와 애플리케이션 서버 모두 최소한 이러한 포트에 액세스할 수 있어야 합니다.

- TCP 443 - (HTTPS) 액세스 및 새로 고침 토큰을 생성하고 업데이트하는 데 사용됩니다.

- TCP 587 - (SMTP over STARTTLS) 디스패처 프로세스 및 경보 알림 프로세스에서 사용

- TCP 993 - (SSL/TLS를 통한 IMAP) 검색기 프로세스에서 사용됨

- TCP 995 - (SSL/TLS를 통한 POP3) 검색기 프로세스에서 사용됨

참조: [POP, IMAP 및 SMTP 설정](#)

## 연결 테스트

Microsoft에서 연결을 테스트하는 데 사용할 수 있는 웹 사이트를 만들었습니다. 이는 Cisco 또는 eGain에서 제공한 툴이 아니며 TAC에서는 이 툴의 사용을 지원할 수 없습니다. 애플리케이션 및 서비스 서버에서 이를 사용하여 컨피그레이션 및 연결을 테스트할 수 있습니다. ECE는 아웃바운드에 대해서는 SMTP만, 인바운드에 대해서는 IMAP 또는 POP3만 지원합니다. Microsoft 웹 사이트의 POP 이메일 및 IMAP 이메일 테스트와 함께 아웃바운드 SMTP 이메일 테스트를 사용합니다.

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

## 문서 링크

11.6(1)

- UCCE/PCCE - [이메일 리소스에 대한 관리자 설명서](#)

## 12.0(1)

- UCCE - [UCCE\(Administrator's Guide to Email Resources\)](#)
- PCCE - [PCCE\(Administrator's Guide to Chat and Email Resources\)](#)

## 12.5(1)

- UCCE - [UCCE\(Administrator's Guide to Email Resources\)](#)
- PCCE - [PCCE\(Administrator's Guide to Chat and Email Resources\)](#)

## 12.6(1)

- UCCE/PCCE - [이메일 및 라우팅 리소스에 대한 관리자 설명서](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.