ISEでのOAuthベースのSMTP認証の設定およびトラブルシューティング

内容

はじめに

このドキュメントでは、Microsoft Exchange Online Mail(SMTP)サーバを介した電子メール通信を可能にするISEでのOAuth 2.0の設定について説明します。

前提条件

要 件

Cisco Identity Services Engine(ISE)、シンプルメール転送プロトコル(SMTP)サーバ機能、およびOAuth認証に関する基本的な知識があることが推奨されます。

使用するコンポーネント

ISEバージョン3.5 P1（3.2パッチ8、3.3パッチ8、3.4パッチ4もこの機能をサポート）

Microsoft EntraIDおよびMicrosoft 365管理センターへのアクセス

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

このセクションでは、次の目的で使用される電子メール通知をサポートするためのMicrosoft

Entra IDおよびISEの設定について説明します。

- Eメールオプションにシステムアラームを含めることを有効にした状態で、すべての内部管理ユーザにEメールアラーム通知を送信します。 送信者の電子メールアドレスを設定するには、Administration > System > Settings > Alarm Settings > Alarm Notificationの順にクリックし、Microsoft 365 admin centerで設定されている電子メールアドレスを入力します

- スポンサーは、ログイン資格情報とパスワードのリセット手順を記載した電子メール通知をゲストに送信します。ゲストおよびスポンサーフローでは、送信者の電子メールはWork Centers > Guest Access > Settings > Guest email settings > Default 'From' email addressで、Microsoft 365 admin centerで設定されたアドレスに設定されます
- ゲストが正常に登録した後、ゲストアカウントの有効期限が切れる前に実行するアクションを使用して、ログイン資格情報をゲストが自動的に受け取れるようにします。
- パスワードの有効期限が切れる前に、ISEで設定されたISE管理ユーザ/内部ネットワークユーザにリマインダメールを送信します。

電子メールを送信するISEノード

電子メールの目的	電子メールを送信するノード
ゲストアクセスの有効期限	プライマリポリシー管理ノード(PAN)
アラーム	アクティブモニタリングおよびトラブルシューティングノード(PMnT)
ゲストおよびスポンサーポータルからのスポンサーおよびゲスト通知	ポリシーサービスノード(PSN)
パスワードの有効期限	プライマリPAN

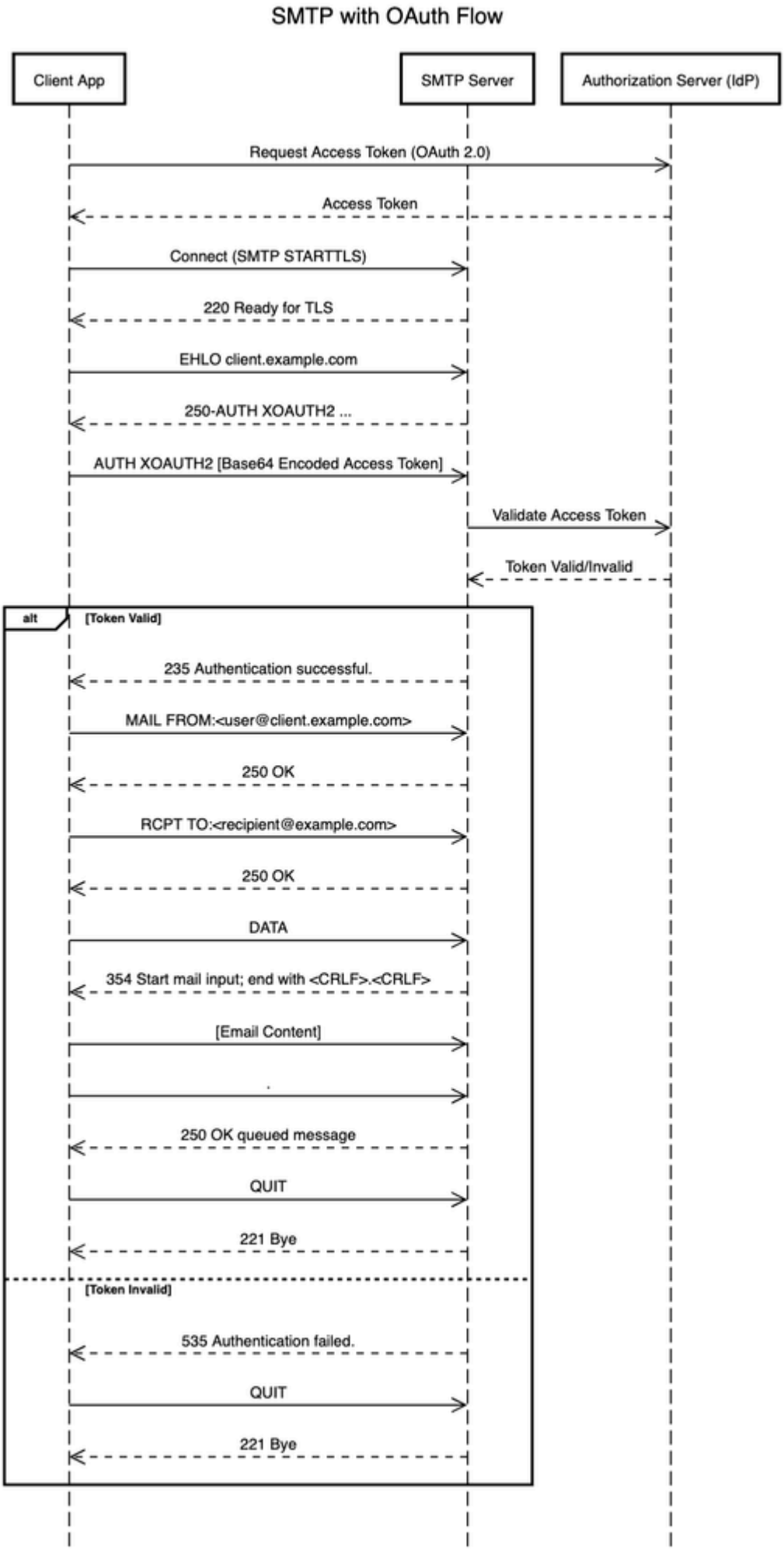
ネットワーク図

ISEでOAuthを使用するには、次の3つの手順を実行する必要があります。

1. ISEアプリケーションをMicrosoft Entra IDに登録する

2. トークンサーバー(IDP)からアクセストークンを取得する

3. アクセストークンを使用して、SMTPサーバーへの接続要求を認証します。



コンフィギュレーション

```
abc@abc-M-506L ~ % sh
sh-3.2$ brew update
sh-3.2$ brew upgrade powershell
```

```
[PS /Users/      > brew install --cask powershell
==> Auto-updating Homebrew...
Adjust how often this is run with `$HOMEBREW_AUTO_UPDATE_SECS` or disable with
`$HOMEBREW_NO_AUTO_UPDATE=1`. Hide these hints with `$HOMEBREW_NO_ENV_HINTS=1` (see `man brew`).
==> Downloading https://ghcr.io/v2/homebrew/core/portable-ruby/blobs/sha256:1c98fa49eacc935640a6f8e10a2bf33f14cfc276804b
71ddb658ea45ba99d167
######################################################################################################################## 100.0%
==> Pouring portable-ruby-3.4.8.arm64_big_sur.bottle.tar.gz
==> Auto-updated Homebrew!
Updated 2 taps (homebrew/core and homebrew/cask).
==> New Formulae
actions-up: Tool to update GitHub Actions to latest versions with SHA pinning
```

Powershellのインストール

II. New-ServicePrincipalコマンドレットを使用するには、ExchangeOnlineManagementをインストールし、スニペットに示されているようにテナントに接続します。

```
sh-3.2$ pwsh
PowerShell 7.5.4

PS/Users/abc> Install-Module -Name ExchangeOnlineManagement
PS/Users/abc> Import-module ExchangeOnlineManagement
PS/Users/abc> Connect-ExchangeOnline -Organization xxxxxxxx-xxxx-xxxx-xxxx-xxxxx999be76 ---->Directory
```

```
[PS /Users/      > Connect-ExchangeOnline -Organization f1108d3c                    9be76

------------------------------------------------------------------------------
This V3 EXO PowerShell module contains new REST API backed Exchange Online cmdlets which doesn't require WinRM for Clien
t-Server communication. You can now run these cmdlets after turning off WinRM Basic Auth in your client machine thus mak
ing it more secure.

Unlike the EXO* prefixed cmdlets, the cmdlets in this module support full functional parity with the RPS (V1) cmdlets.

V3 cmdlets in the downloaded module are resilient to transient failures, handling retries and throttling errors inherent
ly.

REST backed EOP and SCC cmdlets are also available in the V3 module. Similar to EXO, the cmdlets can be run without WinR
M basic auth enabled.

For more information check https://aka.ms/exov3-module

Starting with EXO V3.7, use the LoadCmdletHelp parameter alongside Connect-ExchangeOnline to access the Get-Help cmdlet,
 as it will not be loaded by default
------------------------------------------------------------------------------
```

Exchange Onlineテナントへの接続

III. ExchangeでのMicrosoft Entraアプリケーションサービスプリンシパルの登録。AppIDとObjectID [OBJECT_IDは、アプリケーション登録のエンタープライズアプリケーションノード(Azure Portal)の[概要]ページのオブジェクトIDです。これは、「アプリケーション登録」ノードの「概要」ページにあるオブジェクトIDではありません。誤ったオブジェクトIDを使用すると、認証が失敗します]。

```
PS/Users/abc> New-ServicePrincipal -AppId xxxxxxxx-xxxx-xxxx-xxxx-xxxxxx6a953e -ObjectId b10axxxx-xxxx-
```

```
PS /Users/[redacted]> New-ServicePrincipal -AppId efc0713[redacted]6a953e -ObjectId b10aa0d[redacted]e189bb
```

ExchangeにEntraアプリケーションサービスプリンシパルを登録する

IV. [Get-ServicePrincipalコマンドレット](#)を使用して、登録済みのサービスプリンシパル識別子を確認します

```
PS/Users/abc> Get-ServicePrincipal | fl
```

```
PS /Users/[redacted]> Get-ServicePrincipal | fl

DisplayName                              :
AppId                                    : efc0713[redacted]6a953e
ObjectId                                 : b10aa0d[redacted]e189bb
Sid                                      : S-1-5-21-1250255160-1655375293-4198951263-24390743
SidHistory                               : {}
OverrideEnforceExoAppRbacPermissions     : False
Identity                                 : b10aa0d[redacted]e189bb
Id                                       : b10aa0d[redacted]189bb
IsValid                                  : True
ExchangeVersion                          : 1.1 (15.0.0.0)
Name                                     : b10aa0d[redacted]e189bb
DistinguishedName                        : CN=b10aa0d[redacted]e189bb,OU=[redacted].onmicrosoft.com,OU=Micro
                                           soft Exchange Hosted Organizations,DC=[redacted]05,DC=PROD,DC=OUTLOOK,DC=COM
ObjectCategory                           : [redacted]005.PROD.OUTLOOK.COM/Configuration/Schema/Person
ObjectClass                              : {top, person, organizationalPerson, user}
WhenChanged                              : 16/12/2025 12:53:16 PM
WhenCreated                              : 16/12/2025 12:53:06 PM
WhenChangedUTC                           : 16/12/2025 7:23:16 AM
WhenCreatedUTC                           : 16/12/2025 7:23:06 AM
ExchangeObjectId                         : fb005f[redacted]a32c10
OrganizationalUnitRoot                   : [redacted].onmicrosoft.com
OrganizationId                           : [redacted]05.PROD.OUTLOOK.COM/Microsoft Exchange Hosted
                                           Organizations/[redacted].onmicrosoft.com - [redacted]05.PROD.OUTLOOK.COM/Config
                                           urationUnits/[redacted].onmicrosoft.com/Configuration
Guid                                     : fb005f2[redacted]a32c10
OriginatingServer                        : [redacted]5DC004.[redacted]A005.PROD.OUTLOOK.COM
ObjectState                              : Changed
```

登録済みサービスプリンシパルIDの確認

V.テナント管理者は、アプリケーションがアクセスを許可する特定のメールボックスをテナントに追加できるようになりました。この構成は、[Add-MailboxPermissionコマンドレット](#)を使用して行います。

```
PS/Users/abc> Add-MailboxPermission -Identity "no-reply@abcdef.onmicrosoft.com" -User b10aa0dx-xxxx-xxx
```

```
PS /Users/[redacted]> Add-MailboxPermission -Identity "no-reply@[redacted].onmicrosoft.com" -User b10aa0d[redacted]
[redacted]e189bb -AccessRights FullAccess

Identity             User                     AccessRights     IsInherited Deny
--------             ----                     ------------     ----------- ----
964d0d41-a43f-4257-… S-1-5-21-1250255160…     {FullAccess}     False       False
```

Microsoft Entraアプリケーションは、OAuth 2.0クライアント資格情報の許可フローを使用して、SMTP、POP、またはIMAPプロトコル経由で許可されたメールボックスにアクセスできるようになりました。

ステップ3:MS Exchange Online OAuth経由でISE SMTPユーザ認証を設定します。

Simple Mail Transfer Protocol(SMTP)サーバを設定するには、メニューアイコン(☰)Administration > System > Settings > SMTP Serverの順に選択します。 フィールドを設定します。

- SMTP Server Settings領域で、次の操作を行います。
  - SMTPサーバ:smtp.office365.com
  - SMTPポート:587
  - 接続タイムアウト:60秒
- Authentication Settings領域で、トグルスイッチを使用してUse Authentication Settingsオプションを有効にします。

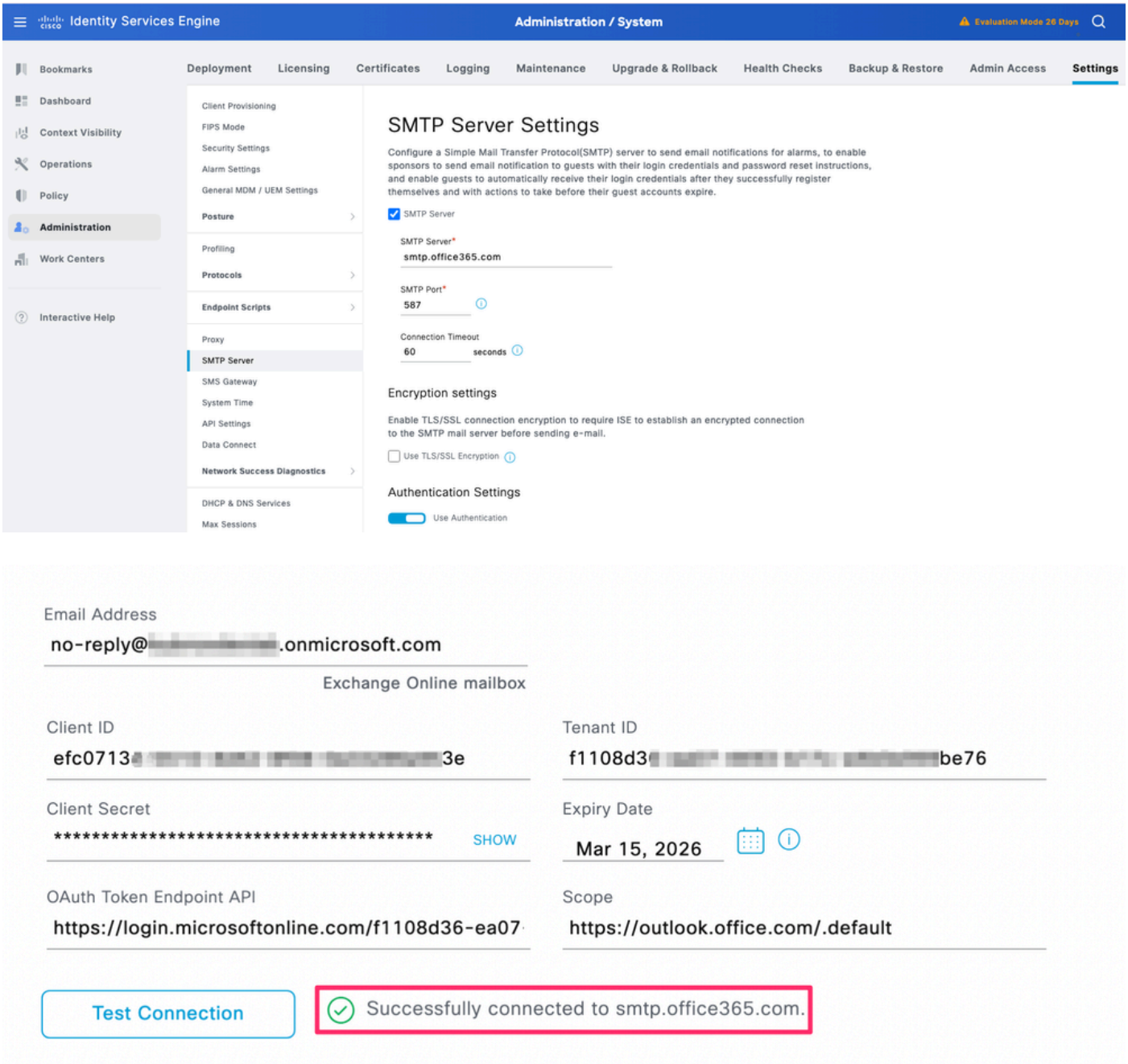
MS Exchange Online OAuthを選択します。次の値を入力して、Microsoft Exchange Online OAuthを設定します。

- Usernameフィールドに、Exchange Onlineユーザ名の完全な電子メールアドレスを入力します。
- クライアントIDフィールドに、Azure Entra IDアプリケーションのクライアントIDを入力します。
- テナントIDフィールドに、Azure Entra IDアプリケーションのテナントIDを入力します。
- Client Secretフィールドに、Azure Entra IDアプリケーションのクライアントシークレットを入力します。
- Expiry Dateフィールドに、クライアントシークレットの有効期限を入力します。

クライアントシークレット期限切れアラームは、この設定に基づいてトリガーされます。

- OAuth Token Endpoint API およびScopeファイルには、値が自動的に入力されます。

構成は、接続テスト操作が正常に完了した後にのみ保存できます。



SMTPサーバへのテスト接続に成功しました。

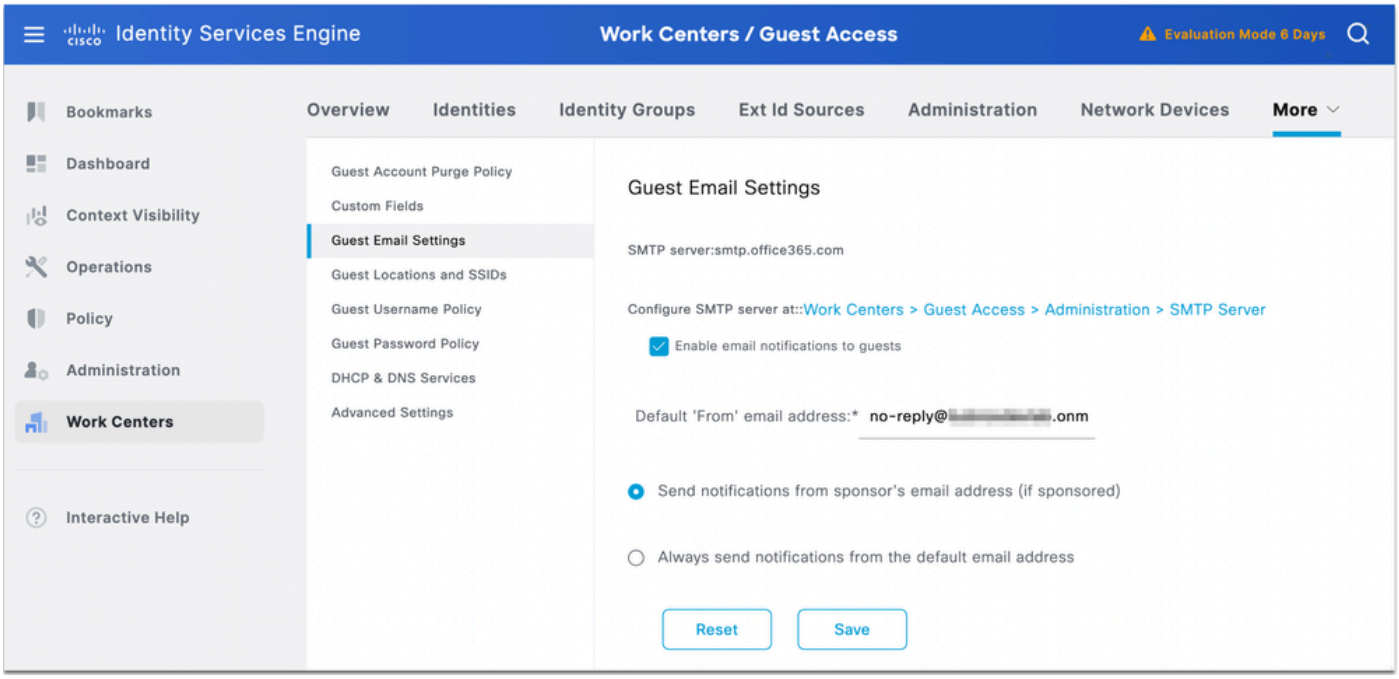
<#root>

Note:

```
 To protect sensitive customer data, these configurations are excluded from Backup and Restore operatio
```

確認

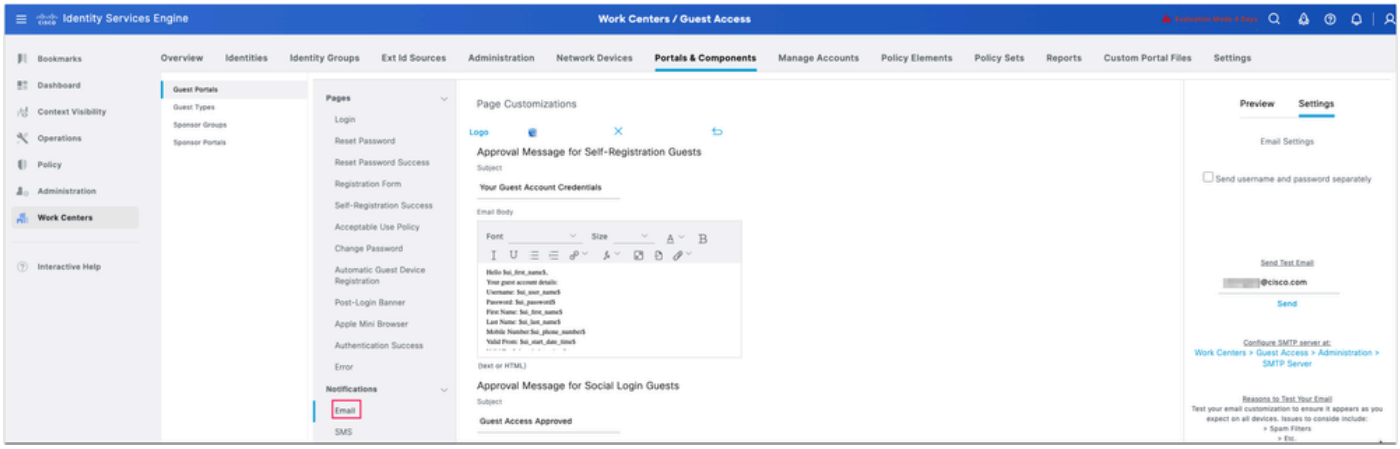
確認するには、ゲスト電子メールの設定を構成します。Work Centers > Guest Access > Guest Email Settingsに移動します。Enable email notifications to guestsを選択し、設定と保存のステップ1で設定した無応答アカウントのデフォルトの「送信元」電子メールアドレスを設定します。



ゲストの電子メール設定の変更

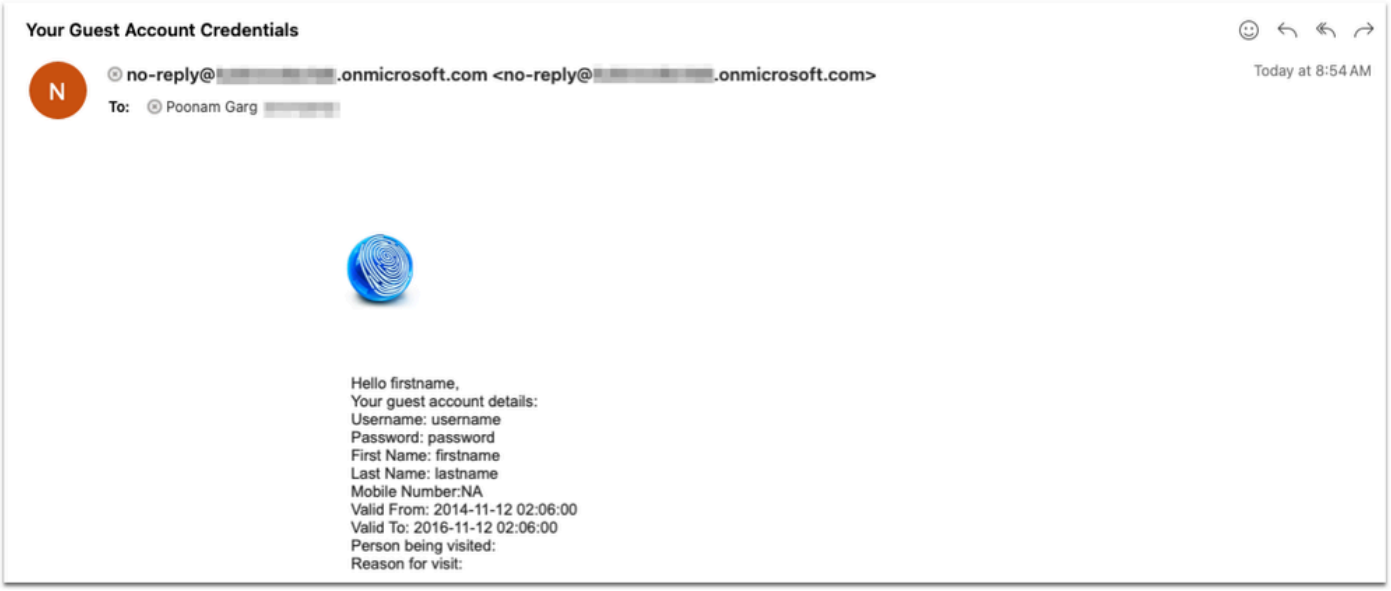
Work Centers > Guest Access > Portal & Components > Guest Portals > Self-Registered Guest Portal (default) > Portal Page Customization > Notifications > Emailの順に移動して、テスト電子メールを送信します。

右側のプレビューペインで、Settings > Send Test Emailの順にクリックし、電子メールIDをAddして、Sendをクリックします。



自己登録ポータルからのテスト電子メール

Outlookは、確認の手順1で設定した返信なしのアカウントから電子メールを受信する必要があります。スクリーンショットのサンプル電子メール。

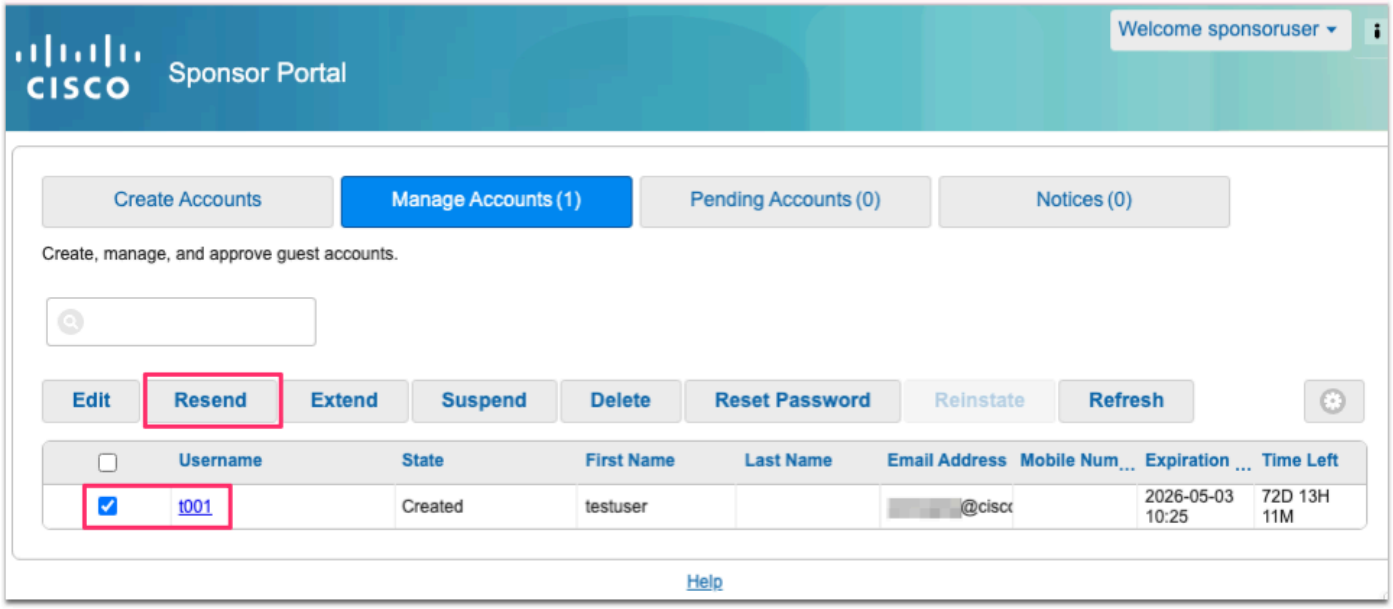


Outlookで受信した電子メールのサンプル

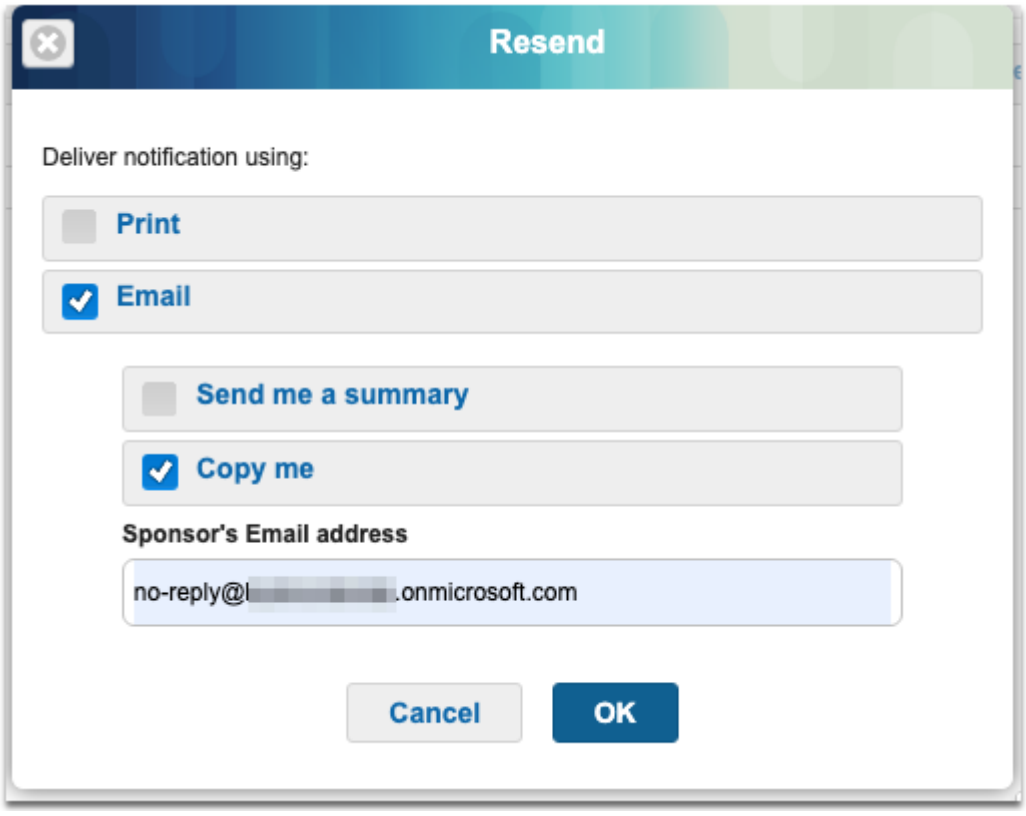
<#root>

```
Guest.log at debug level:
2026-02-02 05:17:34,608 INFO   [admin-http-pool139][[]] cpm.guestaccess.apiservices.util.SmtpMsgRetryTh

sendMailMessage: Submitting Mail Job

.............
2026-02-02 05:17:34,608 INFO   [admin-http-pool139][[]] cpm.guestaccess.apiservices.util.SmtpMsgRetryTh

smtp.office365.com


2026-02-02 05:17:34,609 INFO   [admin-http-pool139][[]] cpm.guestaccess.apiservices.util.SmtpMsgRetryTh
2026-02-02 05:17:34,609 INFO   [admin-http-pool139][[]] cpm.guestaccess.apiservices.util.SmtpMsgRetryTh
2026-02-02 05:17:34,609 INFO   [GUEST_ACCESS_SMTP_RETRY_THREAD][[]] cpm.guestaccess.apiservices.util.Sm
2026-02-02 05:17:39,365 INFO   [GUEST_ACCESS_SMTP_RETRY_THREAD][[]] cpm.guestaccess.apiservices.util.Sm
2026-02-02 05:17:39,365 INFO   [admin-http-pool139][[]] cpm.guestaccess.apiservices.util.SmtpMsgRetryTh

sendMailMessage: Future.get status: success

 Time taken for Future.get method call is 4756 Milliseconds.
```

また、スポンサー管理者がゲストユーザにユーザクレデンシャルを再送信することで、スポンサーポータルからテストします。

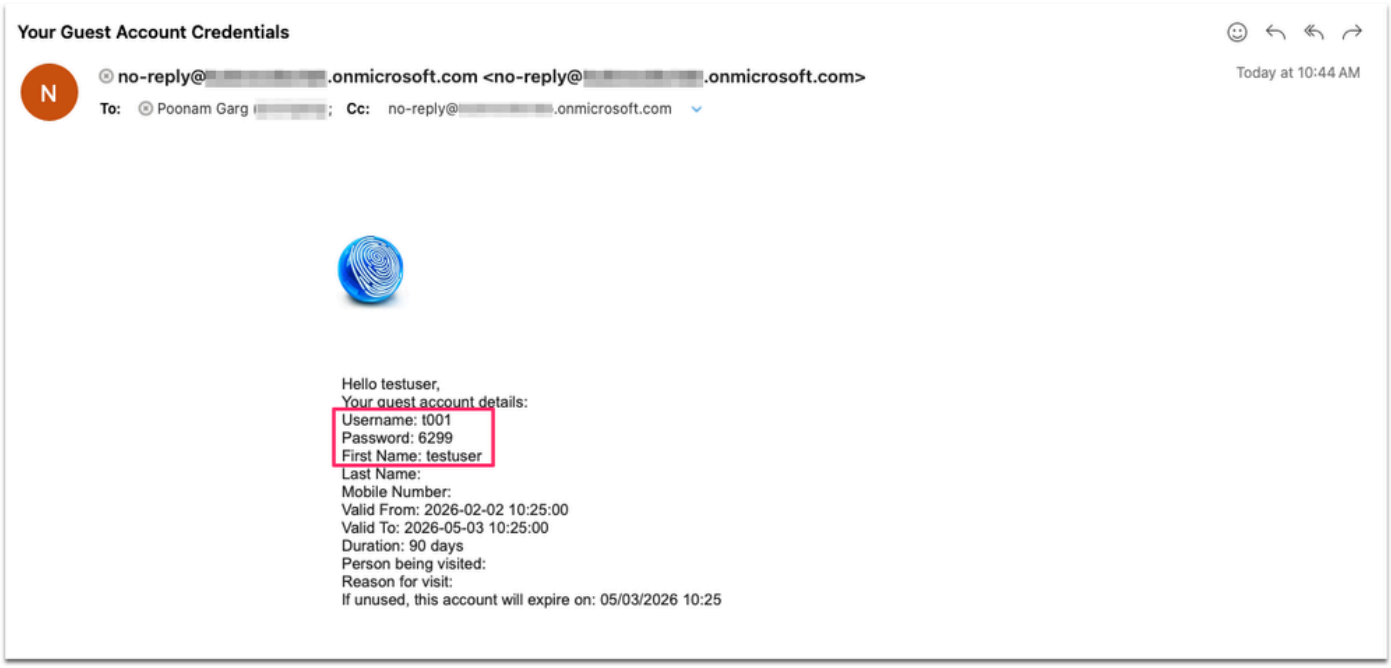


スポンサーポータルからのテスト



ゲストユーザへのクレデンシャルの送信

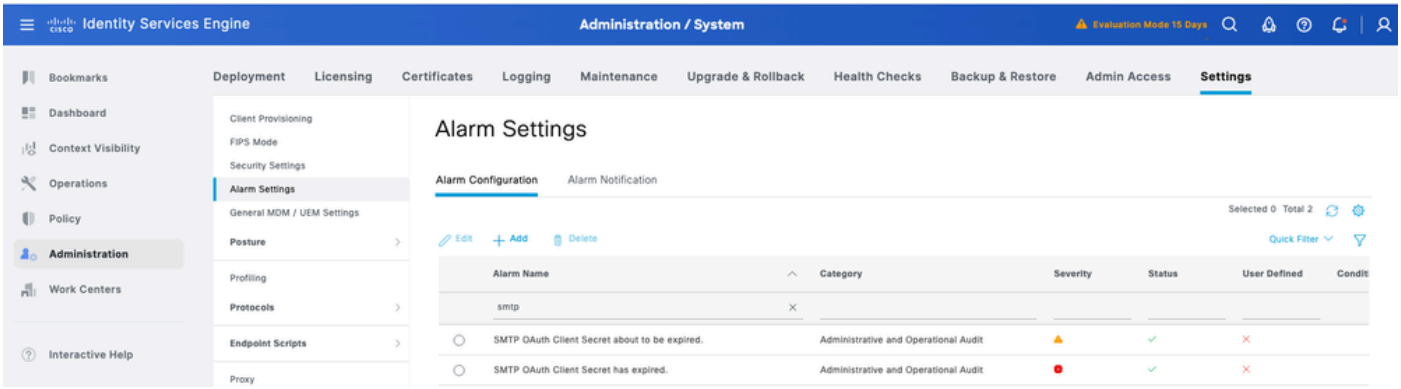
ゲストユーザが受信した電子メールのサンプル：



ゲストユーザへの電子メール通知

トラブルシュート

クライアントシークレットの有効期限に関するアラームの確認から始めます。SMTP OAuth Client Secretに関連する新しいアラームがISEに追加されました。



さらにトラブルシューティングを進めるには、トラブルシューティングする問題に応じて、PAN、PSN、またはPMnTノードでデバッグログを有効にします。

- ロギングコンポーネント：guest-access-admin、guestaccess
- ログファイル：guest.log

接続操作のテスト

```
2026-02-02 05:58:21,501 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.S
2026-02-02 05:58:21,501 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.S
2026-02-02 05:58:21,501 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.S
2026-02-02 05:58:21,513 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.S
2026-02-02 05:58:21,513 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.S
2026-02-02 05:58:21,513 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.S
```

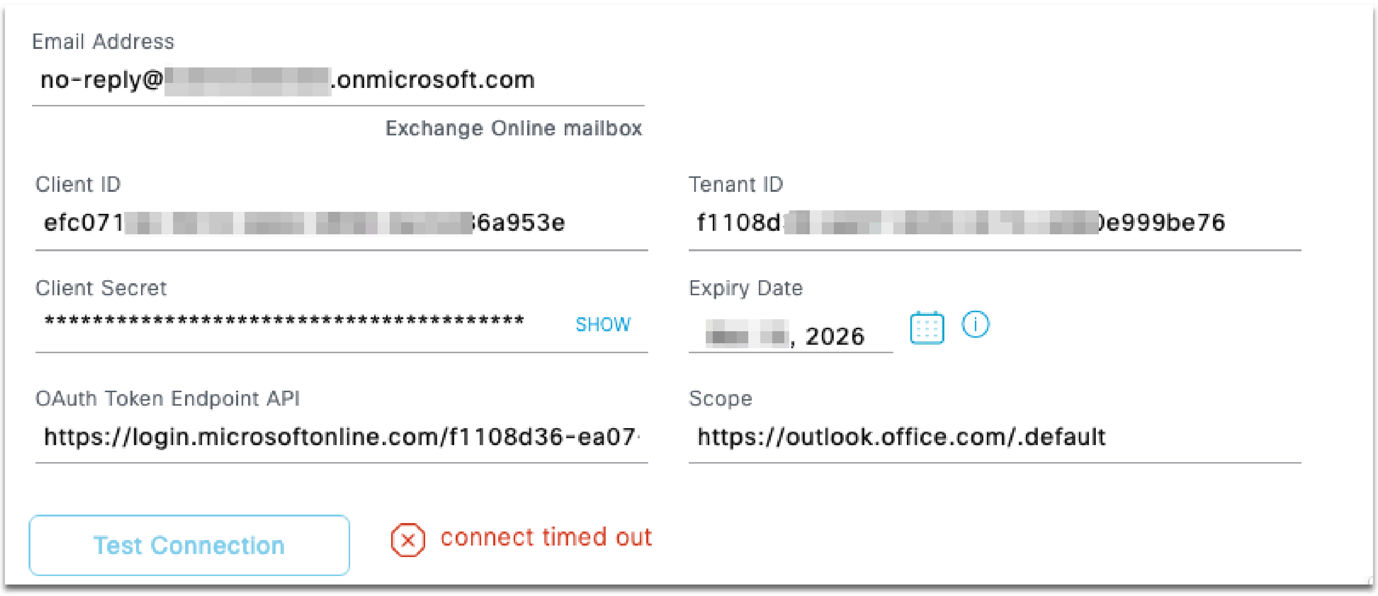
```
2026-02-02 05:59:14,872 DEBUG [admin-http-pool136][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
2026-02-02 05:59:14,872 DEBUG [admin-http-pool136][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
2026-02-02 05:59:15,630 DEBUG [admin-http-pool136][[]] cpm.guestaccess.apiservices.oauth.OauthTokenCach
2026-02-02 05:59:15,630 DEBUG [admin-http-pool136][[]] cpm.guestaccess.apiservices.oauth.ExchangeOnline
2026-02-02 05:59:15,630 DEBUG [admin-http-pool136][[]] cpm.guestaccess.apiservices.oauth.OauthTokenCach
2026-02-02 05:59:20,146 DEBUG [admin-http-pool136][[]] cpm.guestaccess.apiservices.util.SmtpSession -::
2026-02-02 05:59:20,146 DEBUG [admin-http-pool136][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
```

保存操作

```
2026-02-02 05:54:07,337 DEBUG [admin-http-pool129][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
2026-02-02 05:54:07,337 DEBUG [admin-http-pool129][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
2026-02-02 05:54:07,339 DEBUG [admin-http-pool129][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
2026-02-02 05:54:07,339 DEBUG [admin-http-pool129][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
2026-02-02 05:54:07,339 DEBUG [admin-http-pool129][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
2026-02-02 05:54:07,339 DEBUG [admin-http-pool129][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
2026-02-02 05:54:07,339 DEBUG [admin-http-pool129][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
2026-02-02 05:54:07,357 DEBUG [admin-http-pool129][[]] cpm.admin.guestaccess.action.SmtpServerSettingsA
```

接続の問題のトラブルシューティング

1. GUIエラー： smtp.office365.conへの接続に失敗しました。



接続がタイムアウトしました

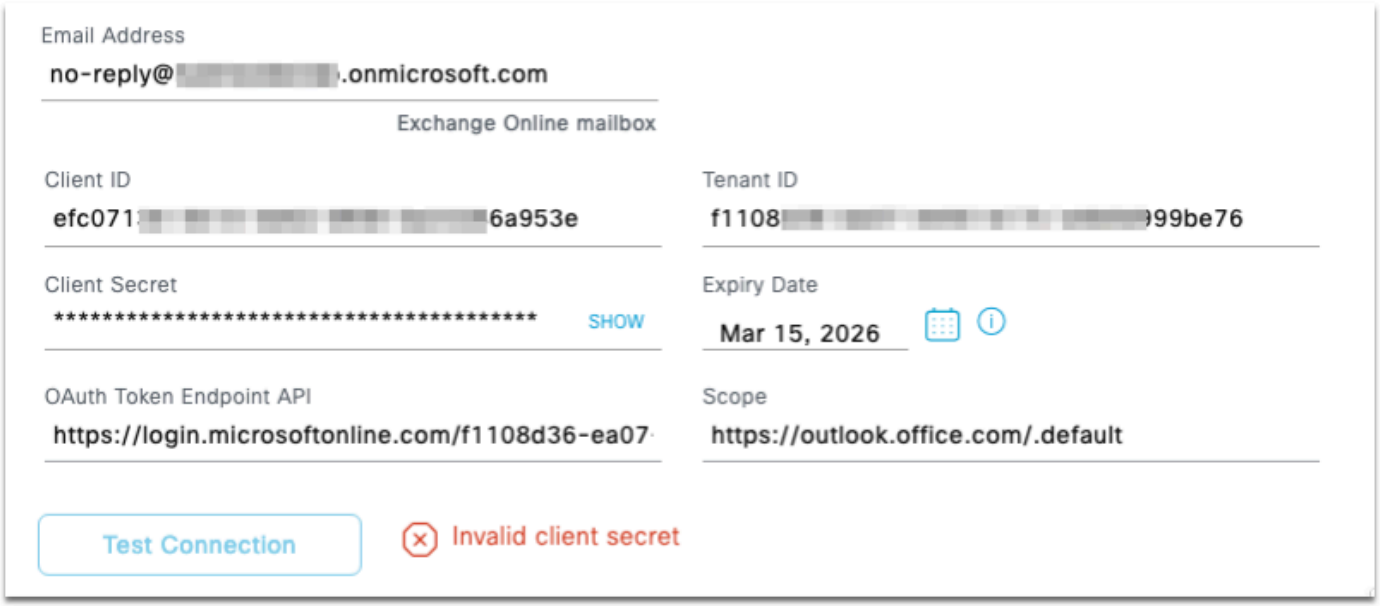
<#root>

```
2026-02-09 03:24:58,658 ERROR [admin-http-pool11][[]] cpm.guestaccess.apiservices.util.SmtpSession -::a
nested exception is:
java.net.SocketTimeoutException: connect timed out
```

Guest.logにconnect timed outと記録される。この問題を解決するには、プロキシ設定を修正する必要があります。

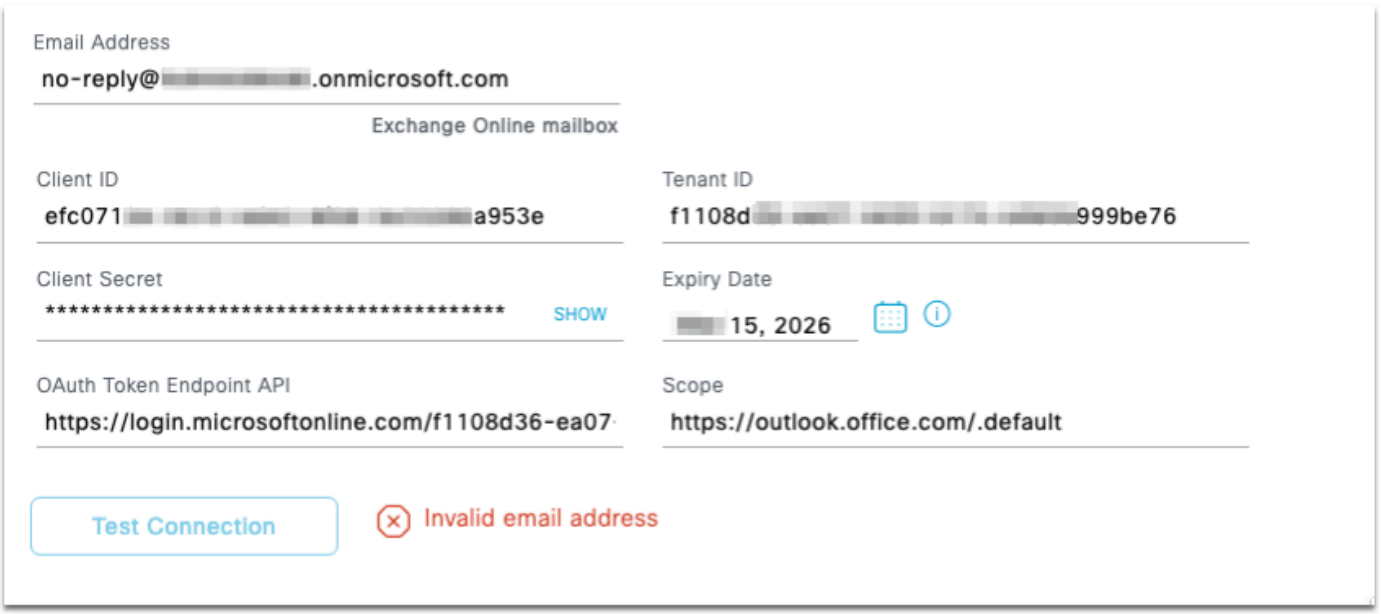
2. GUIエラー： OAuthエンドポイントまたはテナントIDが無効です – 説明を参照してください。テナントIDを確認する必要があります。

3. 無効なクライアントシークレット – 同じ。クライアントシークレット値を確認する必要があります



無効なクライアントシークレットエラー

4. 無効な電子メールアドレス – サービス価格の構成が正しいことを確認してください。

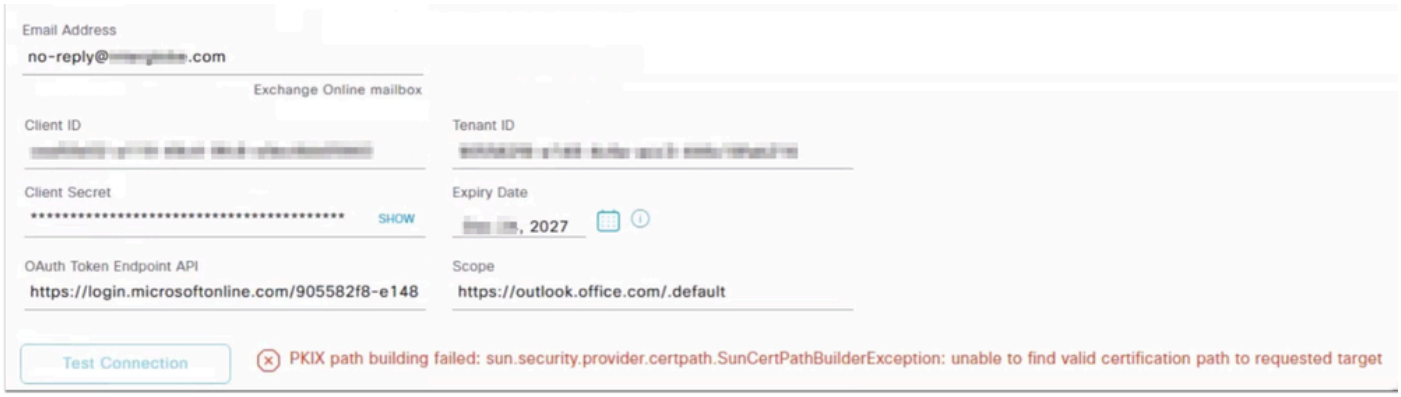


無効な電子メールアドレスのエラー

```
2026-02-12 12:08:59,305 DEBUG  [admin-http-pool40][[]] cpm.guestaccess.apiservices.oauth.OauthTokenCache -::admin:::- Putting value in OAuth Cache (accessToken, expiry) ..
2026-02-12 12:09:02,504 DEBUG  [GuestGracePeriodManagerThread][[]] cpm.guestaccess.apiservices.guest.GuestGracePeriodManager -::::- Waiting for:20000 ms
2026-02-12 12:09:11,277 ERROR  [admin-http-pool40][[]] cpm.guestaccess.apiservices.util.SmtpSession -::admin:::- Exception : javax.mail.AuthenticationFailedException: faile
d to connect
2026-02-12 12:09:11,277 DEBUG  [admin-http-pool40][[]] cpm.admin.guestaccess.action.SmtpServerSettingsAction -::admin:::- Connection to smtp.office365.comserver failed.Inva
lid email address
2026-02-12 12:09:22,504 DEBUG  [GuestGracePeriodManagerThread][[]] cpm.guestaccess.apiservices.guest.GuestGracePeriodManager -::::- Waiting for:20000 ms
2026-02-12 12:09:42,504 DEBUG  [GuestGracePeriodManagerThread][[]] cpm.guestaccess.apiservices.guest.GuestGracePeriodManager -::::- Waiting for:20000 ms
2026-02-12 12:10:02,505 DEBUG  [GuestGracePeriodManagerThread][[]] cpm.guestaccess.apiservices.guest.GuestGracePeriodManager -::::- Waiting for:20000 ms
2026-02-12 12:10:22,505 DEBUG  [GuestGracePeriodManagerThread][[]] cpm.guestaccess.apiservices.guest.GuestGracePeriodManager -::::- Waiting for:20000 ms
2026-02-12 12:10:42,505 DEBUG  [GuestGracePeriodManagerThread][[]] cpm.guestaccess.apiservices.guest.GuestGracePeriodManager -::::- Waiting for:20000 ms
2026-02-12 12:11:02,505 DEBUG  [GuestGracePeriodManagerThread][[]] cpm.guestaccess.apiservices.guest.GuestGracePeriodManager -::::- Waiting for:20000 ms
2026-02-12 12:11:22,505 DEBUG  [GuestGracePeriodManagerThread][[]] cpm.guestaccess.apiservices.guest.GuestGracePeriodManager -::::- Waiting for:20000 ms
```

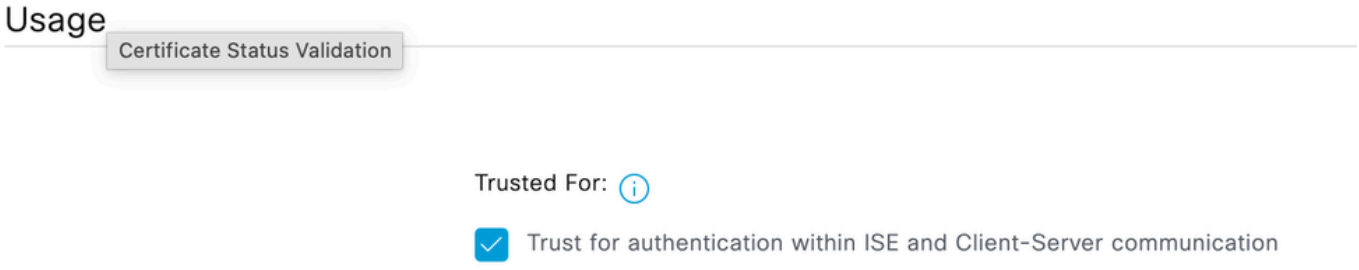
5. 要求されたターゲットへの有効な証明書パスが見つかりません：エントリID証明書チェーン証明書（pcapに従ってMicrosoft Azure RSA TLS発行側CAおよびDigiCertルートCAなど）がISEの信頼済み証明書ストアに存在し、「ISEおよびクライアントサーバ通信（インフラストラクチャ）での認証の信頼」ロールに対して信頼されていることを確認してください。

pcapを取得して、EntraIDから送信されたすべての証明書を確認します。



証明書の検証エラー

```
2026-02-10 14:32:47,528 ERROR  [admin-http-pool9][[]] cpm.guestaccess.apiservices.util.SmtpSession -::a
2026-02-10 14:34:06,549 ERROR  [admin-http-pool9][[]] cpm.guestaccess.apiservices.oauth.ExchangeOnlineP
2026-02-10 14:34:28,655 ERROR  [admin-http-pool27][[]] cpm.guestaccess.apiservices.oauth.ExchangeOnline
```



翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。