Configure and Troubleshoot OAuth Based SMTP Authentication in ISE

Contents

Introduction

This document describes the OAuth 2.0 configuration in ISE to enable email communication through Microsoft Exchange Online Mail SMTP servers.

Prerequisites

Requirements

Cisco recommends that you have a basic knowledge of the Cisco Identity Services Engine (ISE) and Simple Mail Transfer Protocol (SMTP) Server functionality and OAuth Authorization.

Components Used

ISE version 3.5 P1 (3.2 Patch 8, 3.3 Patch 8, 3.4 Patch 4 also supports this functionality)

Access to Microsoft EntraID and Microsoft 365 admin center

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.

Configure

This section describes the configuration on Microsoft Entra ID and ISE in order to support email notifications used to:

- Send email alarm notifications to any internal admin users with the inclusion of system alarms in emails option enabled. To configure the sender email address, click on **Administration** > **System** > **Settings** > **Alarm Settings** > **Alarm Notification** and type in the

email address to the one configured under Microsoft 365 admin center

- Sponsors to send an email notification to guests with their log in credentials and password reset instructions. For Guest and Sponsor flow, sender email is configured under **Work Centers** > **Guest Access** > **Settings** > **Guest email settings** > Default 'From' email address to the one configured under Microsoft 365 admin center
- Enable guests to automatically receive their log in credentials after they successfully register themselves and with actions to take before their guest accounts expire.
- Send reminder emails to ISE admin users/Internal network users configured on the ISE prior to their password expiration date.

ISE Nodes that Send Emails

Purpose of Email	**Node That Sends Email**
Guest access expiration	Primary Policy Administration Node (PAN)
Alarms	Active Monitoring and Troubleshooting node (PMnT)
Sponsor and guest notifications from guest and sponsor portals	Policy Service node (PSN)
Password expiration	Primary PAN

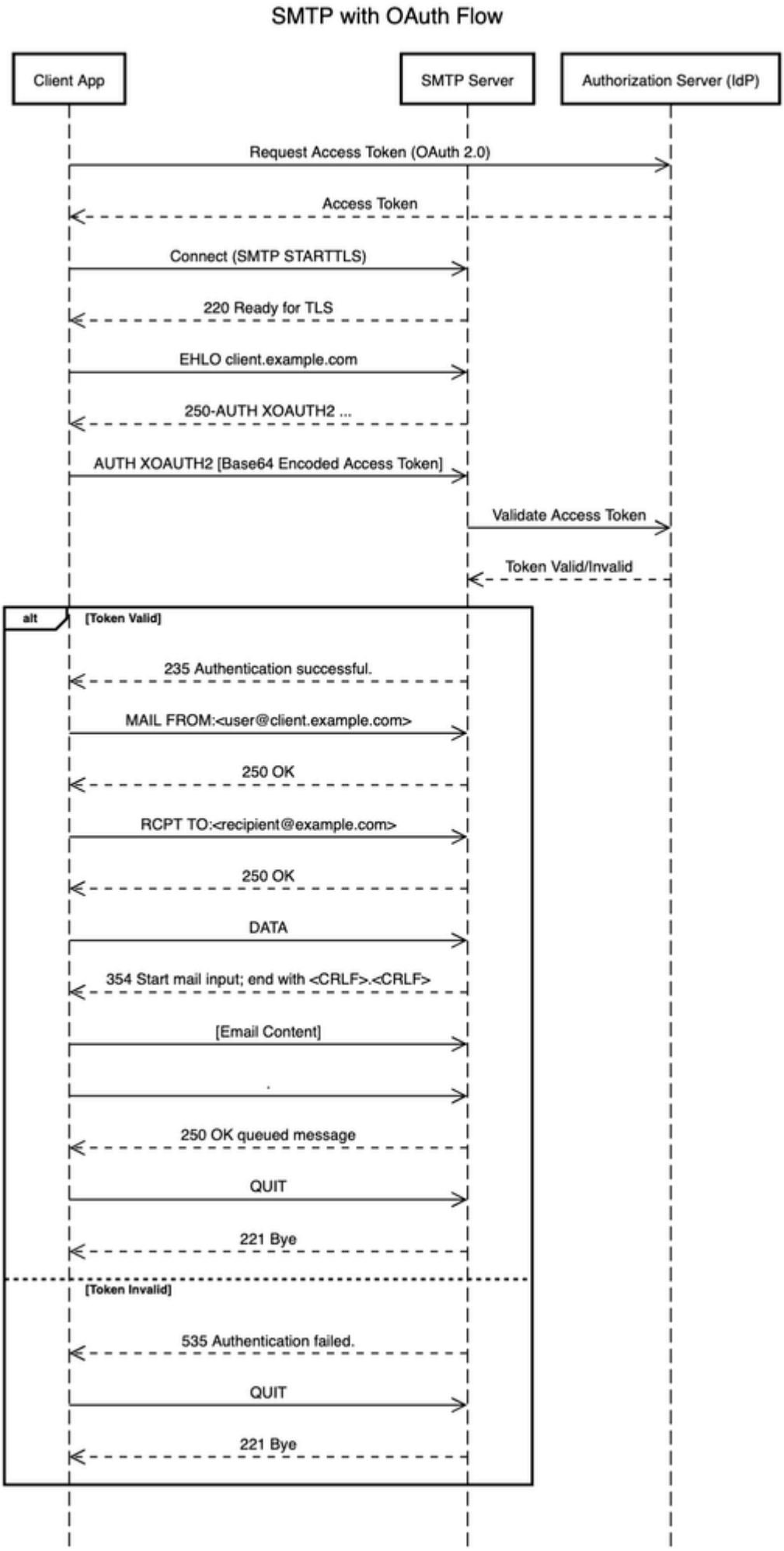
Network Diagram

To use OAuth with ISE, 3 steps are needed:

1. Register ISE application with Microsoft Entra ID

2. Get an access token from the token server (IDP)

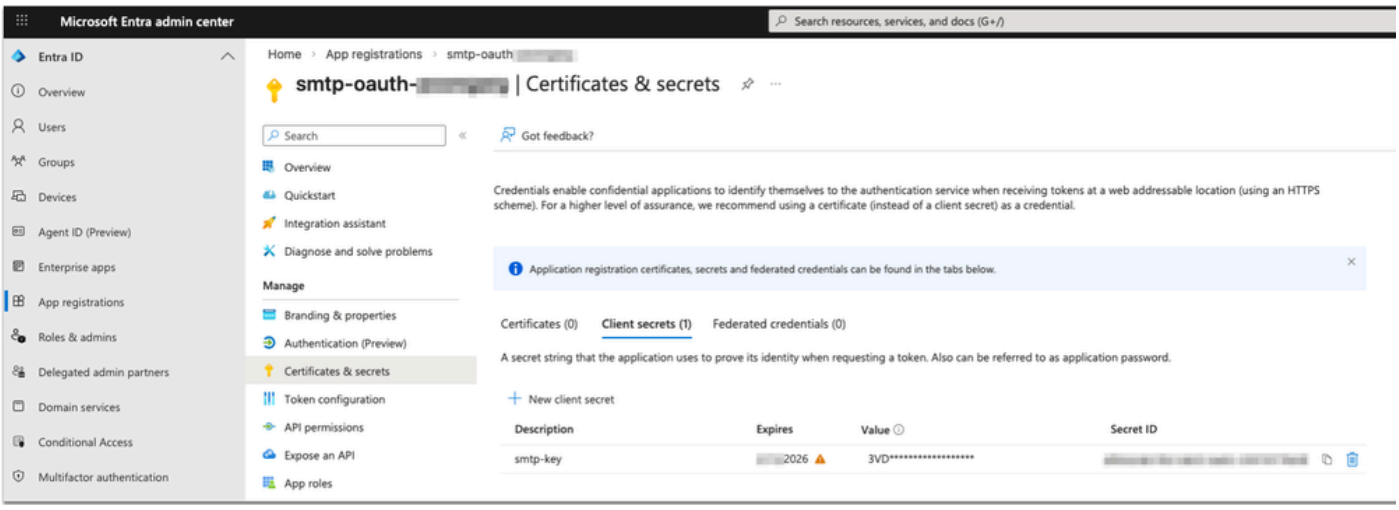
3. Authenticate connection requests to SMTP Server with an access token.



Configurations

as Client secret values cannot be viewed, except for immediately after creation. Be sure to save the secret when created before leaving the page.

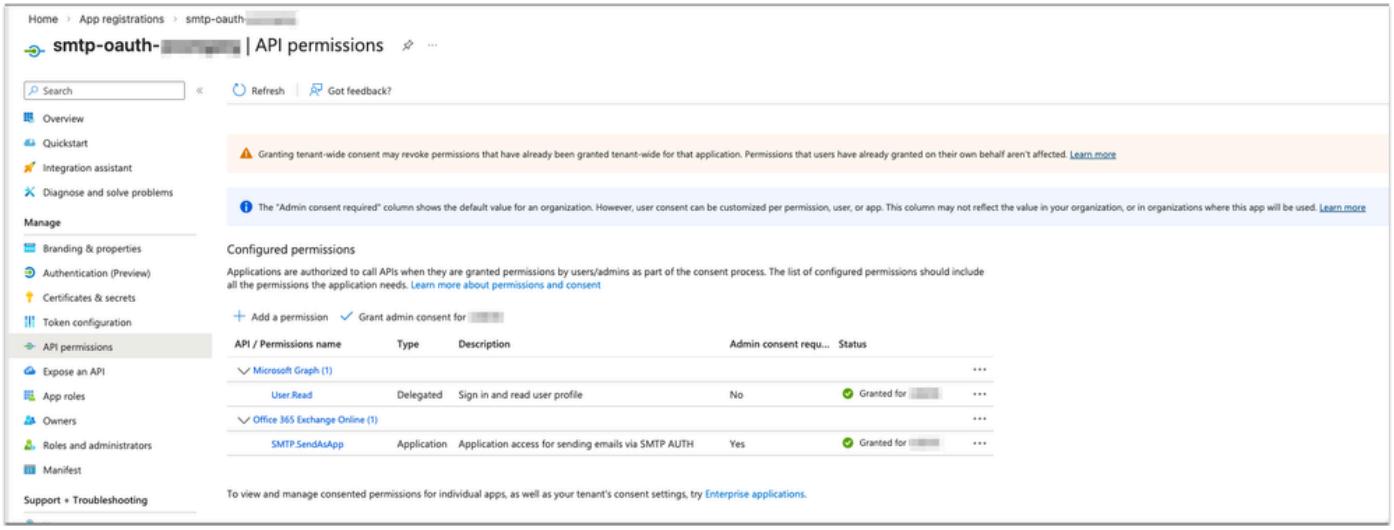
3. Also note down the key expiry date.



Application Client Secret configuration

6. Applications are authorized to call APIs when they are granted permissions by users/admins. Now add SMTP permissions to the MS Entra Application.

1. In the newly registered application, browse to **Manage > API permissions.** Select **Add a permission.**
2. Select the **APIs my organization uses** tab and search for "*Office 365 Exchange Online*".
3. Click **Application permissions**.
4. For SMTP access, choose the **SMTP.SendAsApp** permission.
5. Tenant Admin consent is required for this permission. Click on **Grant admin consent for <tenant name>**



Assign API permission to application

<#root>

Note:

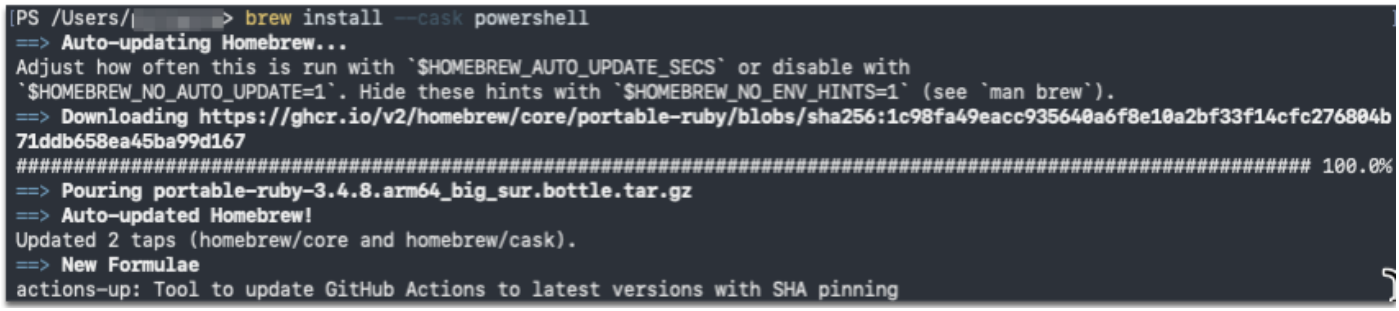
User.Read Permission for Microsoft Graph is added by default (No Admin consent for the tenant)

7. **Service principals** in Exchange are used to enable applications to access Exchange mailboxes via client credentials flow with the SMTP, POP, and IMAP protocols.

Once a tenant admin consents your Microsoft Entra application, admin must register your Entra application service principal in Exchange via Exchange Online PowerShell. This registration is enabled by the New-ServicePrincipal cmdlet.

1. Install Powershell, if not already installed on your laptop

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



Install Powershell

II. To use the ***New-ServicePrincipal*** **cmdlet,** install ExchangeOnlineManagement and connect to your tenant as shown in the snippet:

```
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/[redacted]> Connect-ExchangeOnline -Organization f1108d3[redacted]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
```

Connect to Exchange Online Tenant

III. **Registration of an Microsoft Entra application service principal in Exchange**. Use the AppID and ObjectID [The OBJECT_ID is the Object ID from the Overview page of the Enterprise Application node (Azure Portal) for the application registration. It is **NOT** the Object ID from the Overview page of the App Registrations node. Using the incorrect Object ID results in authentication failure].

```
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
```

Register Entra application service principal in Exchange

IV. Verify your registered service principal identifier using the Get-ServicePrincipal cmdlet

```
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]005,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]005.PROD.OUTLOOK.COM/Config
                                       urationUnits/[redacted].onmicrosoft.com/Configuration
Guid                                 : fb005f2[redacted]a32c10
OriginatingServer                    : [redacted]5DC004.[redacted]A005.PROD.OUTLOOK.COM
ObjectState                          : Changed
```

Verify registered service principal identifier

V. Tenant admin can now add the specific mailboxes in the tenant that is be allowed to be accessed by your application. This configuration is done with the [Add-MailboxPermission cmdlet](#).

```
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
```

Add mailbox permission to access application

Your Microsoft Entra application can now access the allowed mailboxes via the SMTP, POP, or IMAP protocols using the OAuth 2.0 client credentials grant flow.

STEP 3: Configure ISE SMTP User authentication via MS Exchange Online OAuth

To configure an Simple Mail Transfer Protocol (SMTP) server, click the **Menu** icon (☰) and choose **Administration** > **System** > **Settings** > **SMTP Server**. Configure the fields.

- In the **SMTP Server Settings** area:
  - **SMTP Server**: smtp.office365.com
  - **SMTP Port**: 587
  - **Connection Timeout**: 60 seconds
- In the **Authentication Settings** area, Use the toggle switch to enable the **Use Authentication Settings** option.

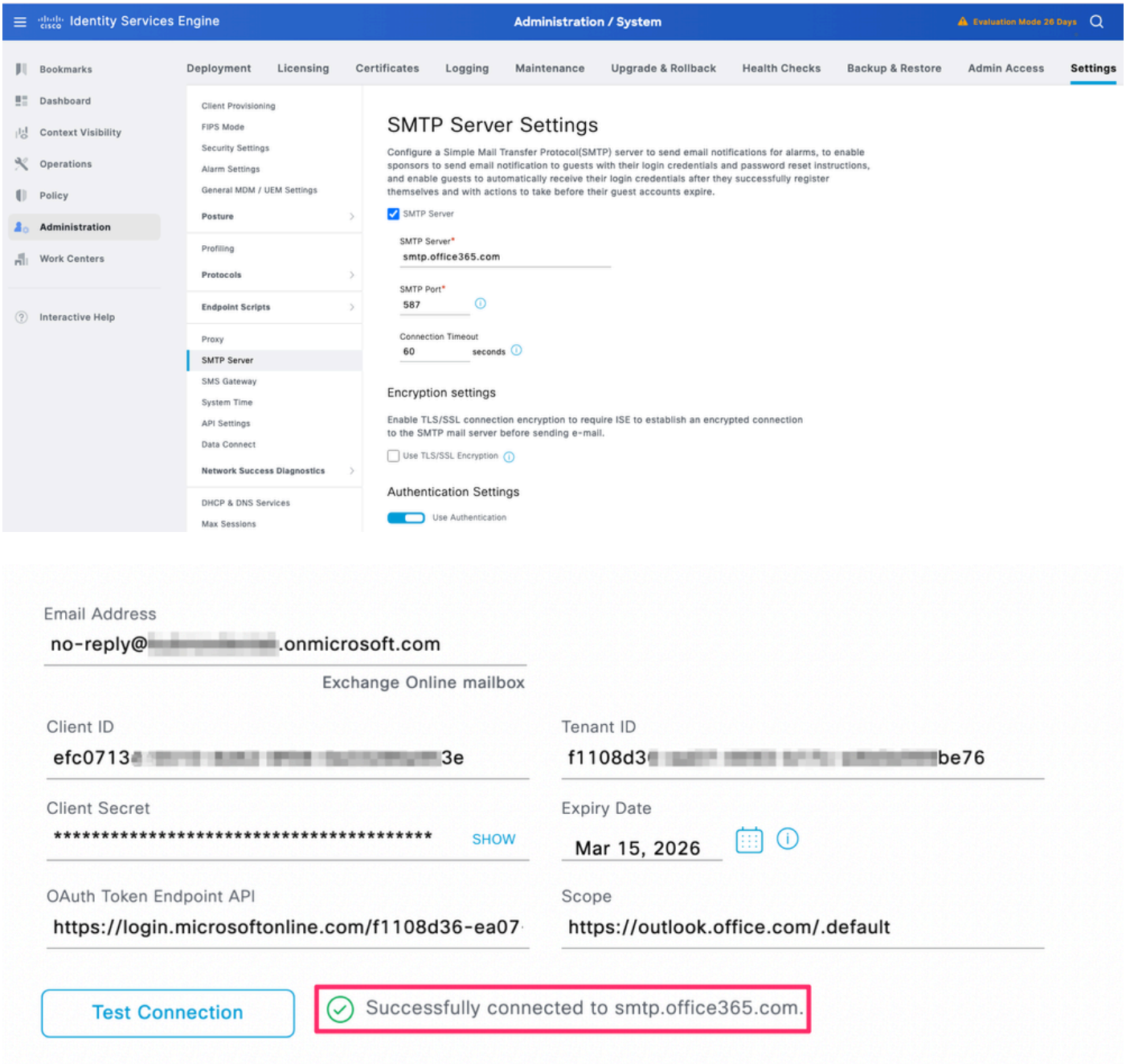
Choose **MS Exchange Online OAuth**: Enter these values to configure Microsoft Exchange Online OAuth.

- In the **Username** field, enter the full email address of the Exchange Online Username.
- In the **Client ID** field, enter the client ID of the Azure Entra ID application.
- In the **Tenant ID** field, enter the tenant ID of the Azure Entra ID application.
- In the **Client Secret** field, enter the client secret of the Azure Entra ID application.
- In the **Expiry Date** field, enter the expiry date of the client secret.

Client secret expiry alarms are triggered based on this configuration.

- The **OAuth Token Endpoint API** and **Scope** files are automatically populated.

Configuration can be saved only after successful Test Connection operation.



Successful test connection to SMTP sever

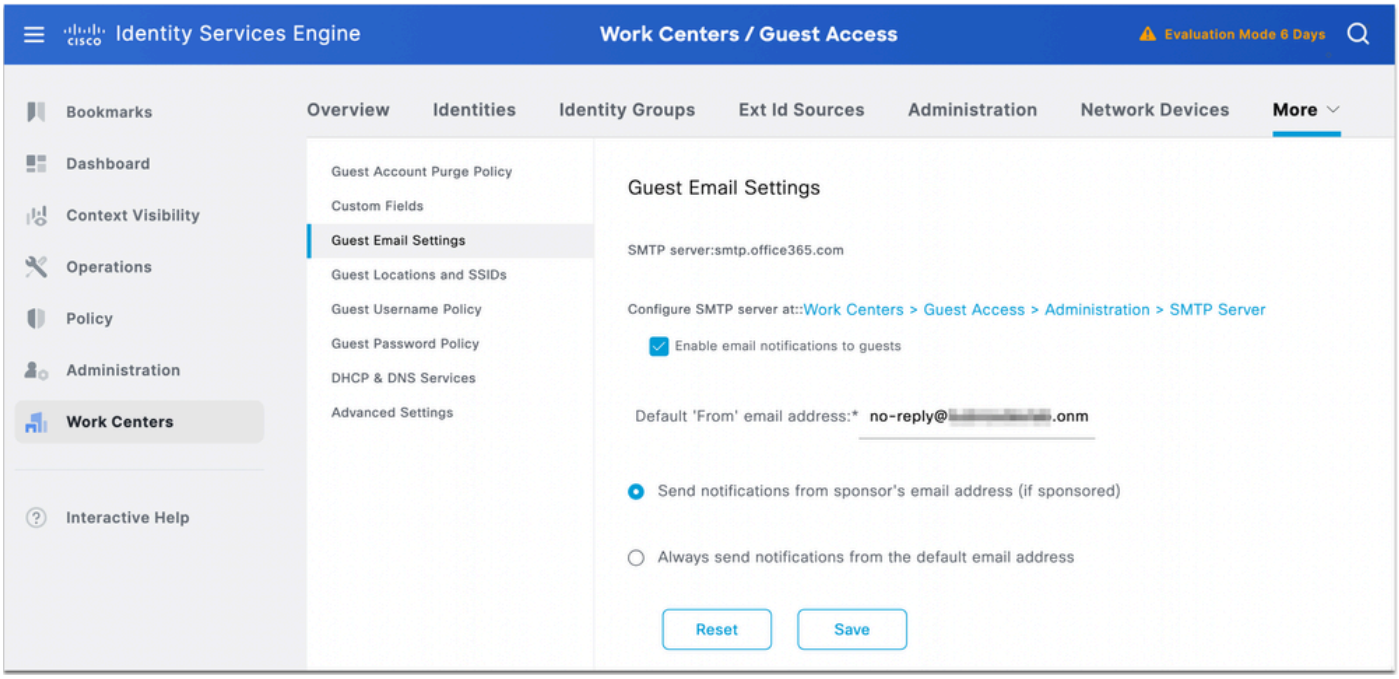
<#root>

Note:

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

Verify

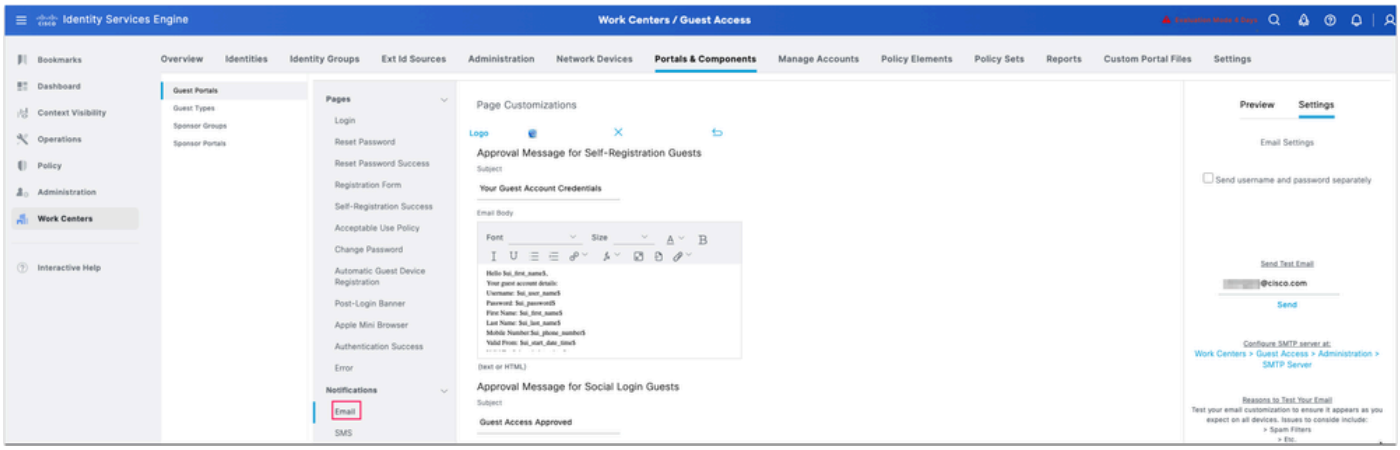
To verify, configure the Guest Email Settings. Navigate to **Work Centers** > **Guest Access** > **Guest Email** Settings. Select the **Enable email notifications to guests** and configure the **Default 'From' email Address** of no-reply account configured during Step1 of configuration and **Save**.



Change Guest Email Settings

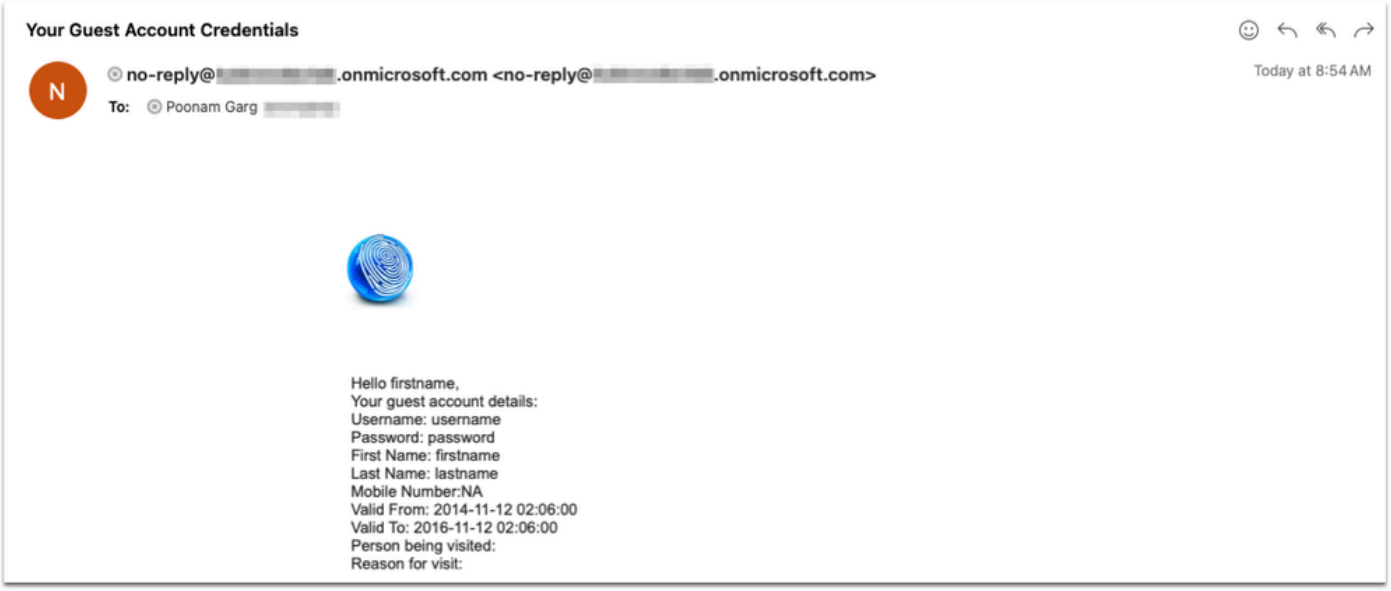
Send a test email by navigating to **Work Centers** > **Guest Access** > **Portal & Components** > **Guest Portals** > **Self-Registered Guest Portal (default)** > **Portal Page Customization** > **Notifications** > **Email**.

Under preview pane right hand side, click **Settings** > **Send Test Email**, **Add** your email ID and click **Send**.



Test Email from Self-Registration Portal

Your Outlook must receive an email from no-reply account configured in step 1 of verification. Sample email in the screenshot.

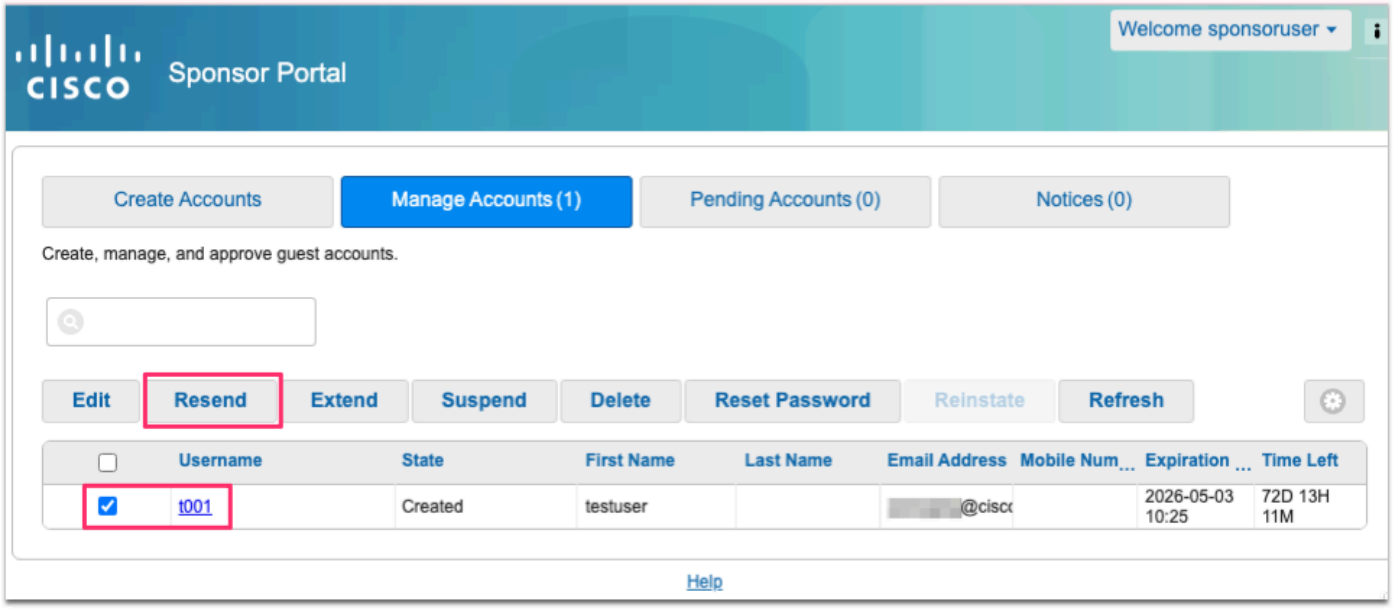


Sample Email received in Outlook

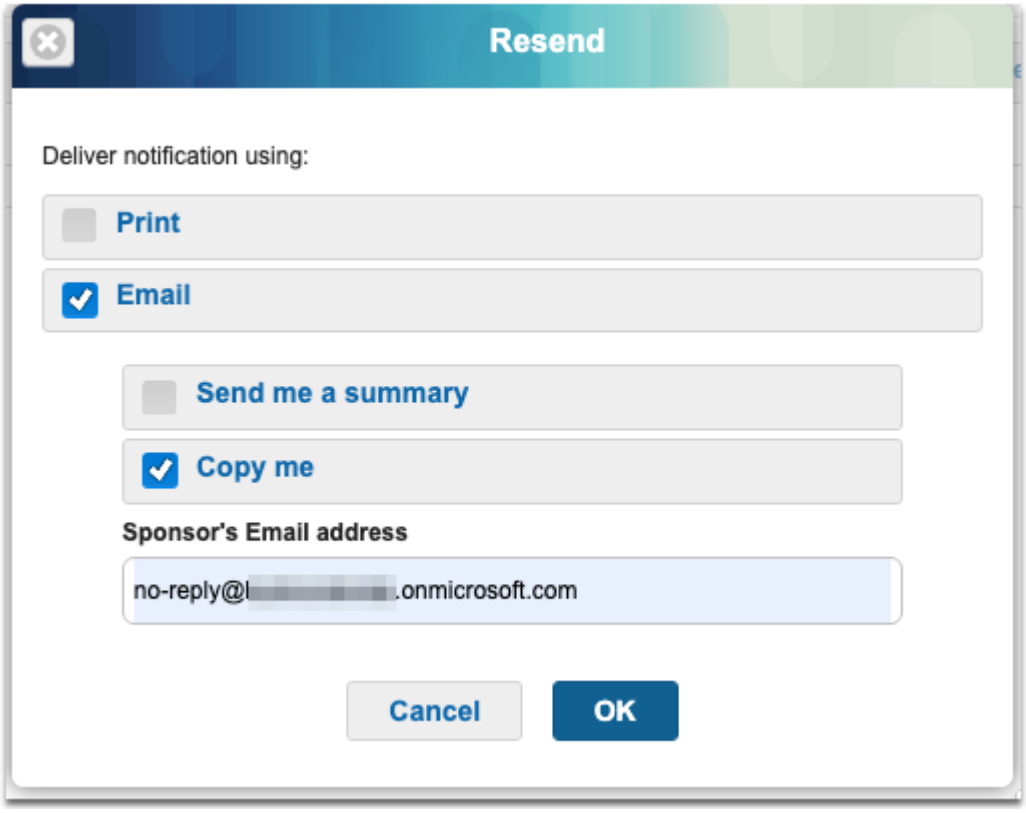
<#root>

```
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.
```

Also test from sponsor portal by resending the user credentials to the guest user by sponsor admin.

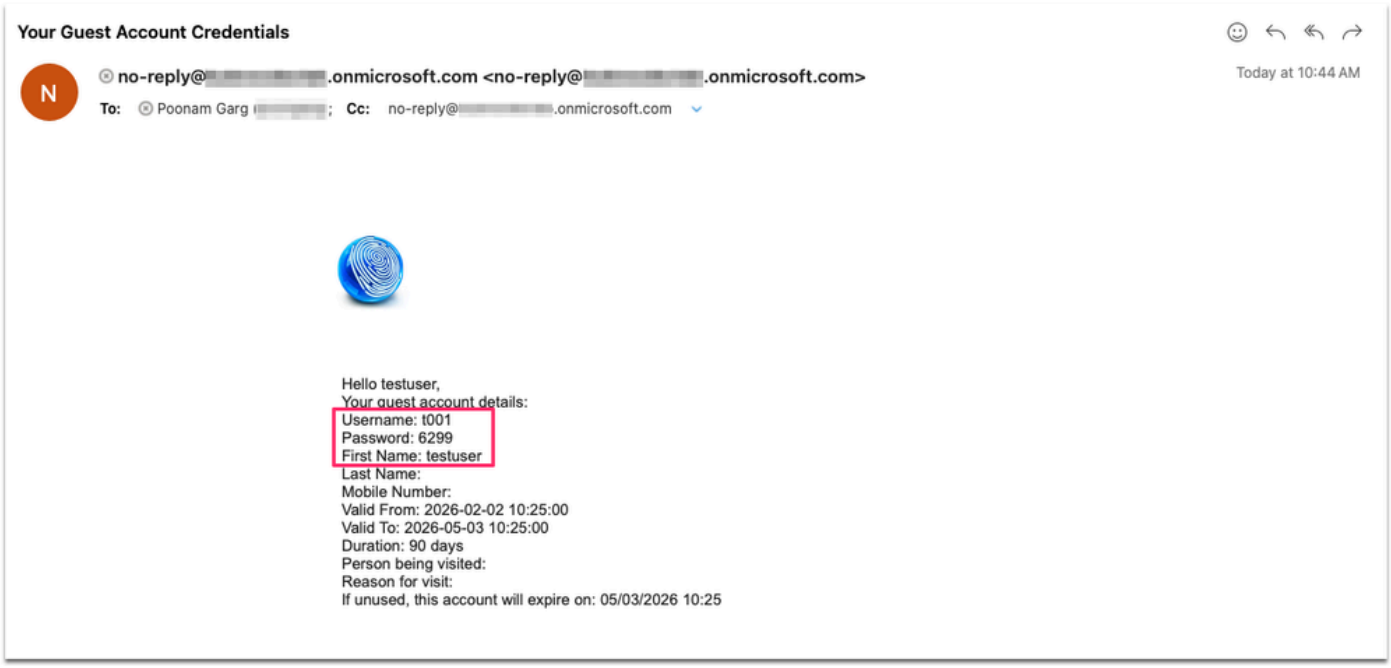


Test from Sponsor Portal



Send credentials to Guest user

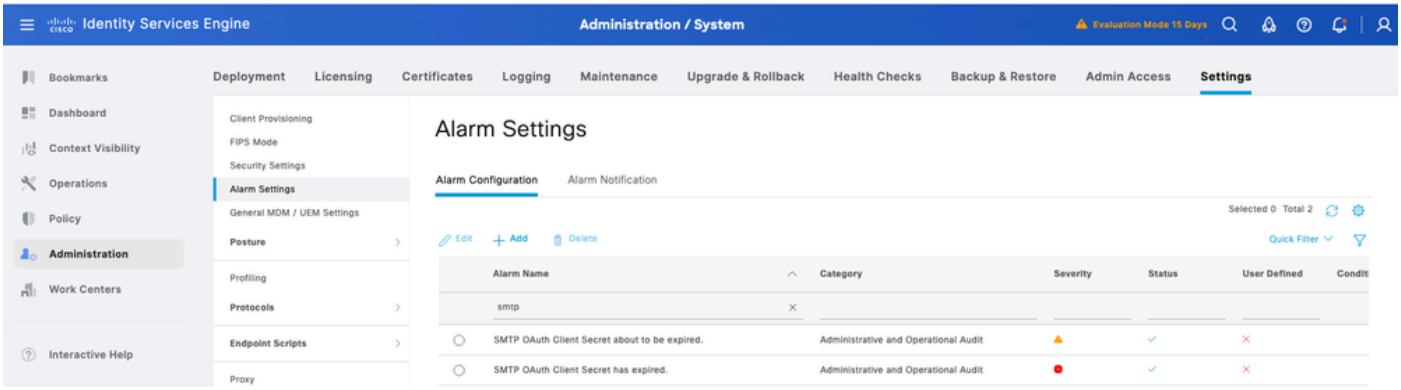
Sample email received by guest user:



Email notification to guest user

Troubleshoot

Start with checking alarms for Client Secret expiry. New alarms related to SMTP OAuth Client Secret are added in ISE.



For further troubleshooting, enable debug logs on PAN, PSN or PMnT node as per the issue you are troubleshooting.

- **Logging Component:** guest-access-admin, guestaccess
- **Log File:** guest.log

Test Connection Operation

```
2026-02-02 05:58:21,501 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.Sm
2026-02-02 05:58:21,501 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.Sm
2026-02-02 05:58:21,501 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.Sm
2026-02-02 05:58:21,513 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.Sm
2026-02-02 05:58:21,513 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.Sm
2026-02-02 05:58:21,513 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.Sm
2026-02-02 05:59:14,872 DEBUG [admin-http-pool136][[]] cpm.admin.guestaccess.action.SmtpServerSettingsAc
2026-02-02 05:59:14,872 DEBUG [admin-http-pool136][[]] cpm.admin.guestaccess.action.SmtpServerSettingsAc
```

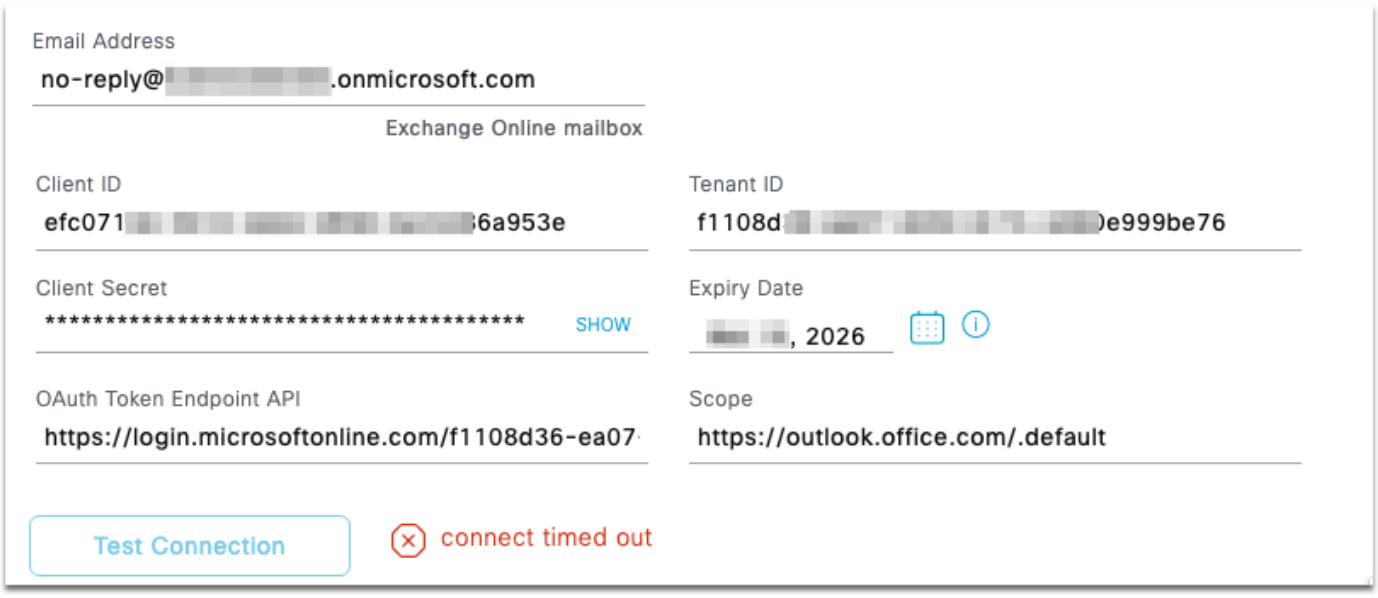
```
2026-02-02 05:59:15,630 DEBUG [admin-http-pool136][[]] cpm.guestaccess.apiservices.oauth.OauthTokenCach
2026-02-02 05:59:15,630 DEBUG [admin-http-pool136][[]] cpm.guestaccess.apiservices.oauth.ExchangeOnline
2026-02-02 05:59:15,630 DEBUG [admin-http-pool136][[]] cpm.guestaccess.apiservices.oauth.OauthTokenCach
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
```

Save operation

```
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
```

Troubleshooting Connectivity Issue

1. GUI Error: Connection to smtp.office365.con failed.



Connect timed out error

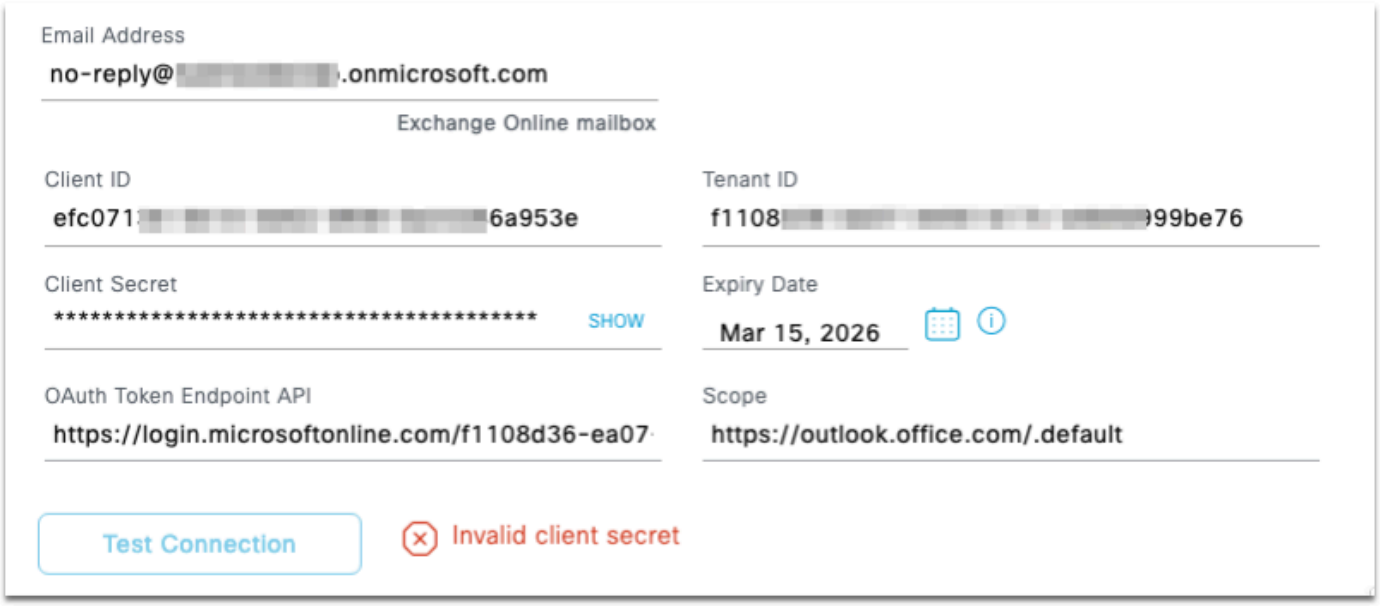
<#root>

```
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 shows connect timed out. Proxy configuration need to be fixed to resolve this issue.

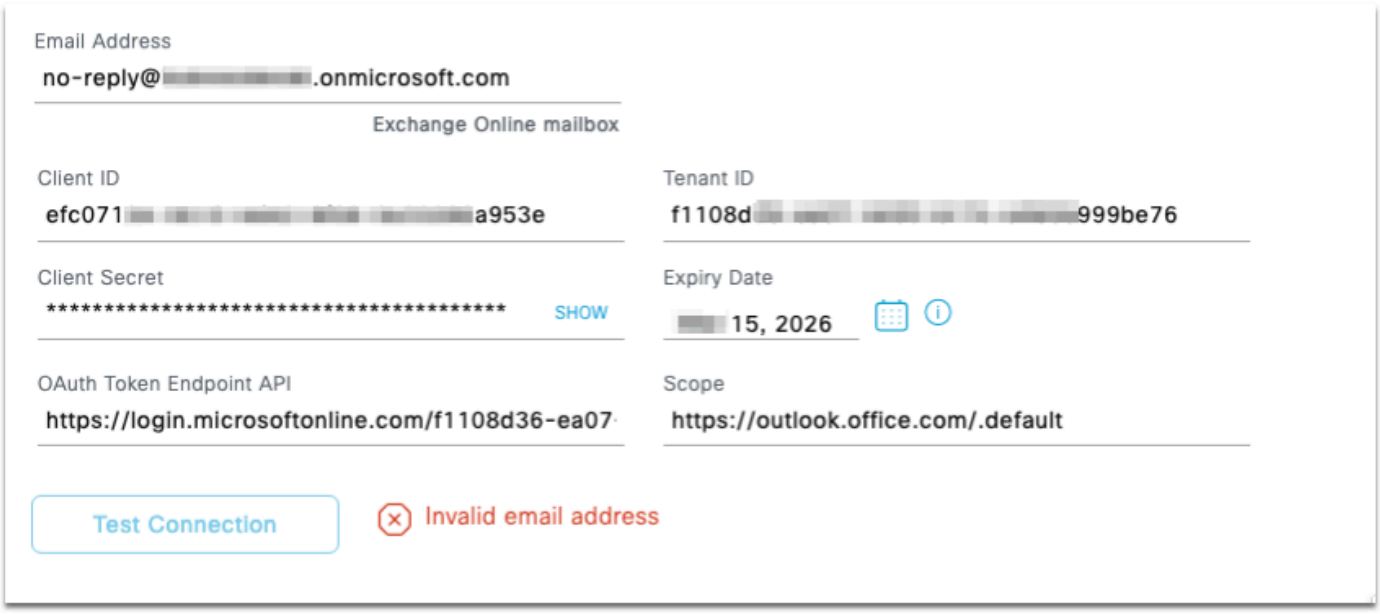
2. GUI Error: Invalid OAuth endpoint or tenant identifier - Self explanatory. Need to check the Tenant ID.

3. Invalid client secret - Same, need to verify client secret value



Invalid client secret error

4. Invalid Email Address- Make sure the Service Priciple configuration is correct.

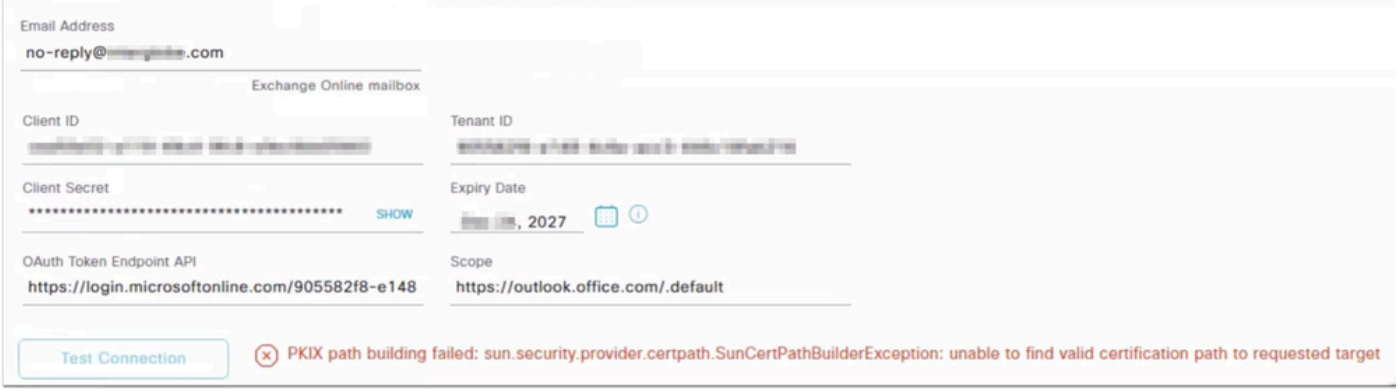


Invalid Email Address Error

```
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. Unable to find valid certification path to requested Target: Make sure the Entra ID certificate chain certificates (Microsoft Azure RSA TLS Issuing CA and DigiCert Root CA etc as per the pcap) are present in the Trusted certificate store of ISE and is Trusted for "Trust for authentication within ISE and Client-Server communication (Infrastructure)" role.

Verify all the certificates sent by EntraID by taking a pcap.



Certificate validation failure

```
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
```