在ISE中配置基於OAuth的SMTP身份驗證並對其進行故障排除

目錄

簡介

必要條件

- 需求
- 採用元件

設定

- 網路圖表
- 組態

驗證

疑難排解

排除連線故障

簡介

本文檔介紹ISE中的OAuth 2.0配置，以便通過Microsoft Exchange Online Mail SMTP伺服器啟用電子郵件通訊。

必要條件

需求

思科建議您瞭解思科身份服務引擎(ISE)和簡單郵件傳輸協定(SMTP)伺服器功能和OAuth授權的基本知識。

採用元件

ISE版本3.5 P1（3.2補丁8、3.3補丁8、3.4補丁4也支援此功能）

訪問Microsoft EntraID和Microsoft 365管理中心

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

本節介紹Microsoft Entra ID和ISE上的配置，以支援用於以下操作的電子郵件通知：

- 向任何內部管理員使用者傳送電子郵件警報通知，同時啟用郵件中包含系統警報選項。若要配

置發件人電子郵件地址，請按一下「管理」>「系統」>「設定」>「警報設定」>「警報通知」，然後鍵入在Microsoft 365管理中心下配置的電子郵件地址

- 發起人向訪客傳送電子郵件通知，告知其登入憑證和密碼重置說明。對於訪客和發起人流，發件人郵件在Work Centers > Guest Access > Settings > Guest email settings > Default 'From'郵件地址下配置為Microsoft 365管理中心下配置的郵件地址
- 使訪客能夠在成功註冊自身後自動接收其登入憑證，並在訪客帳戶過期之前執行操作。
- 在密碼到期日期之前，向ISE管理員使用者/在ISE上配置的內部網路使用者傳送提醒電子郵件。

傳送電子郵件的ISE節點

電子郵件的目的	傳送電子郵件的節點
訪客訪問過期	主要原則管理節點(PAN)
警報	主動監控和故障排除節點(PMnT)
來自訪客和發起人門戶的發起人和訪客通知	原則服務節點(PSN)
密碼過期	主要PAN

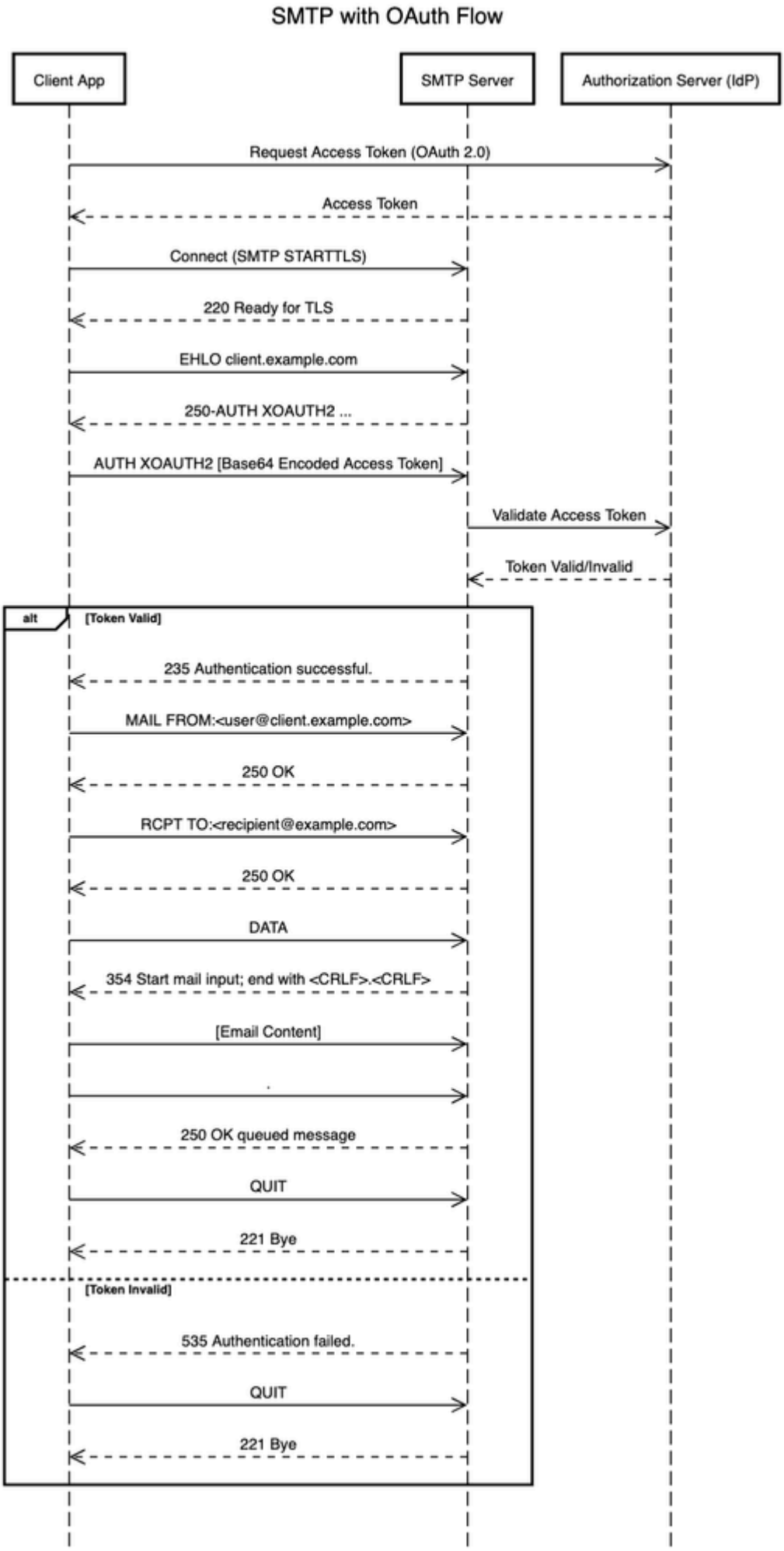
網路圖表

要將OAuth與ISE配合使用，需要3個步驟：

1.使用Microsoft Entra ID註冊ISE應用程式

2.從令牌伺服器(IDP)獲取訪問令牌

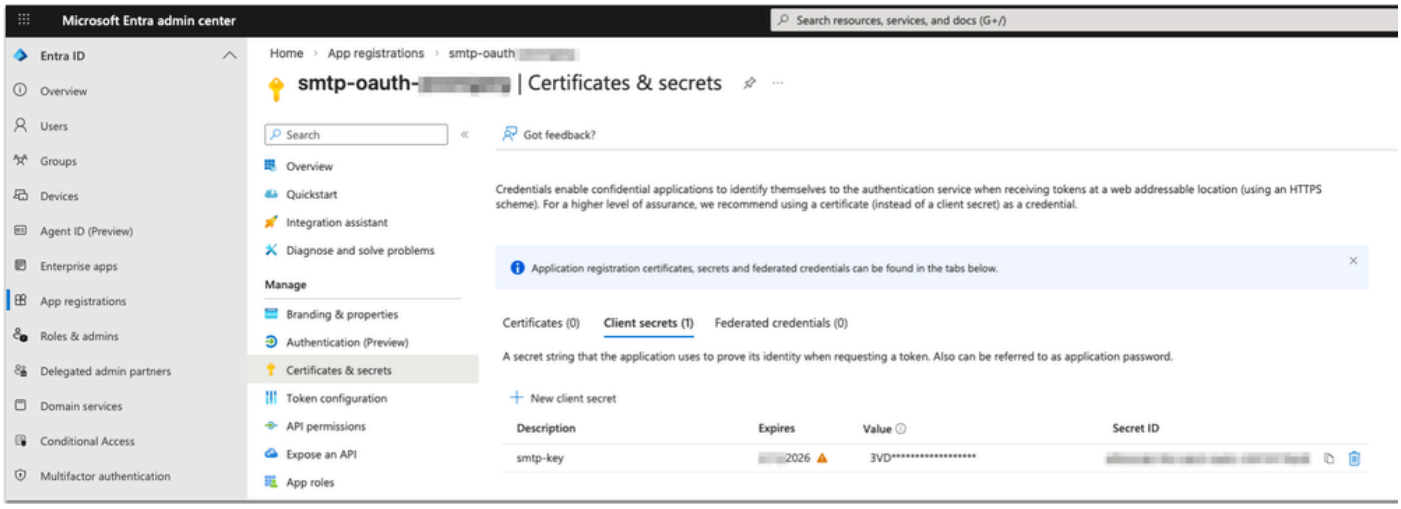
3.使用訪問令牌驗證與SMTP伺服器的連線請求。


SMTP with OAuth Flow
Client App
SMTP Server
Authorization Server (IdP)
Request Access Token (OAuth 2.0)
Access Token
Connect (SMTP STARTTLS)
220 Ready for TLS
EHLO client.example.com
250-AUTH XOAUTH2 ...
AUTH XOAUTH2 [Base64 Encoded Access Token]
Validate Access Token
Token Valid/Invalid
alt
[Token Valid]
235 Authentication successful.
MAIL FROM:<user@client.example.com>
250 OK
RCPT TO:<recipient@example.com>
250 OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
[Email Content]
.
250 OK queued message
QUIT
221 Bye
[Token Invalid]
535 Authentication failed.
QUIT
221 Bye

組態

，因為除了在建立後立即檢視外，不能檢視客戶機加密值。請在離開頁面之前確保建立時儲存密碼。

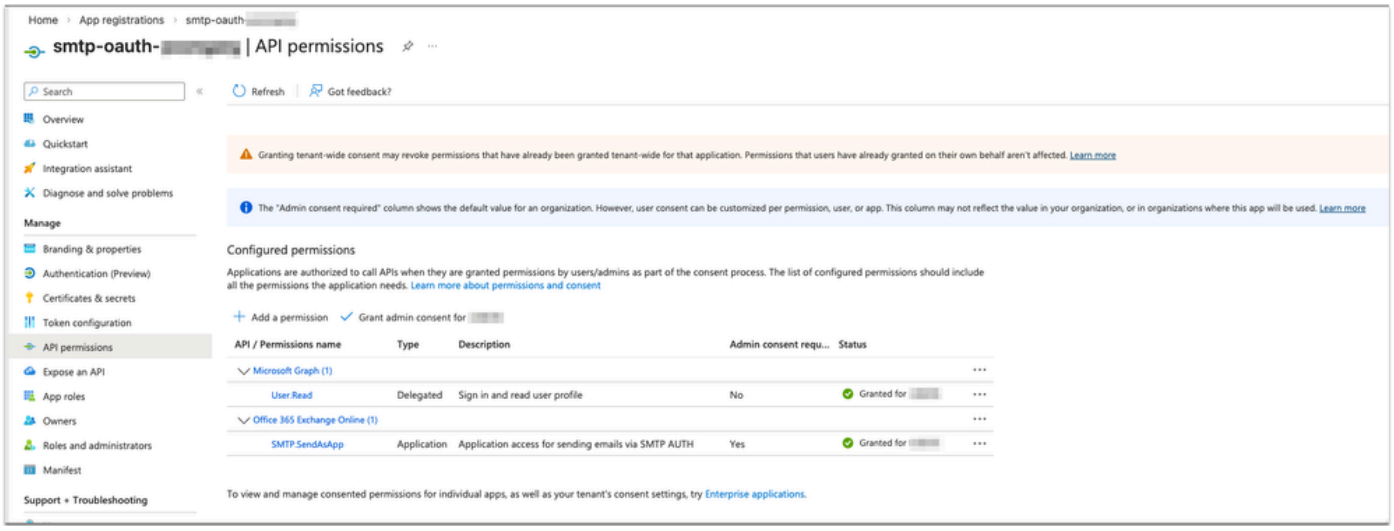
3. 同時記下重要的到期日。



應用程式客戶端加密配置

6.應用程式在使用者/管理員授予其許可權時有權呼叫API。現在向MS Entra應用程式新增SMTP許可權。

1. 在新註冊的應用程式中，瀏覽到管理> API許可權。選擇「新增許可權」。
2. 選擇我組織使用的API頁籤，並搜尋「Office 365 Exchange Online」。
3. 按一下Application permissions。
4. 對於SMTP訪問，請選擇SMTP.SendAsApp許可權。
5. 此許可權需要租戶管理員同意。按一下Grant admin agree for <tenant name>



向應用程式分配API許可權

<#root>

Note:

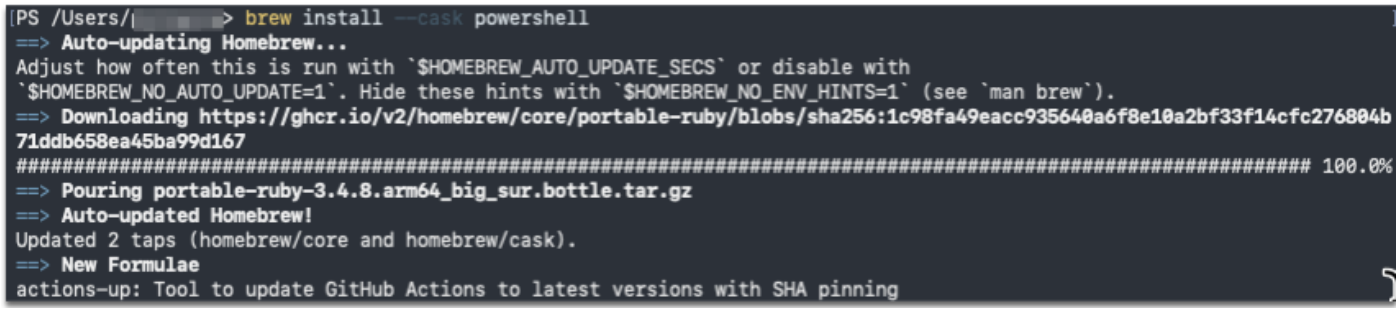
User.Read Permission for Microsoft Graph is added by default (No Admin consent for the tenant)

7. Exchange中的服務主體用於使應用程式能夠通過使用SMTP、POP和IMAP協定的客戶端憑據流訪問Exchange郵箱。

一旦租戶管理員同意您的Microsoft Entra應用程式，管理員必須通過Exchange Online PowerShell在Exchange中註冊您的Entra應用程式服務主體。此註冊由New-ServicePrincipal cmdlet啟用。

1. 安裝Powershell（如果尚未安裝在筆記型電腦上）

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



安裝Powershell

II.要使用New-ServicePrincipal cmdlet，請安裝ExchangeOnlineManagement並連線到您的租戶，如代碼片斷所示：

```
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
------------------------------------------------------------------------------------
```

連線到Exchange Online租戶

三、在Exchange中註冊Microsoft Entra應用程式服務主體。使用AppID和ObjectID [OBJECT_ID是企業應用程式節點（Azure門戶）的「概述」頁中的對象ID以進行應用程式註冊。它不是App Registrations節點的Overview頁中的Object ID。使用不正確的對象ID會導致身份驗證失敗]。

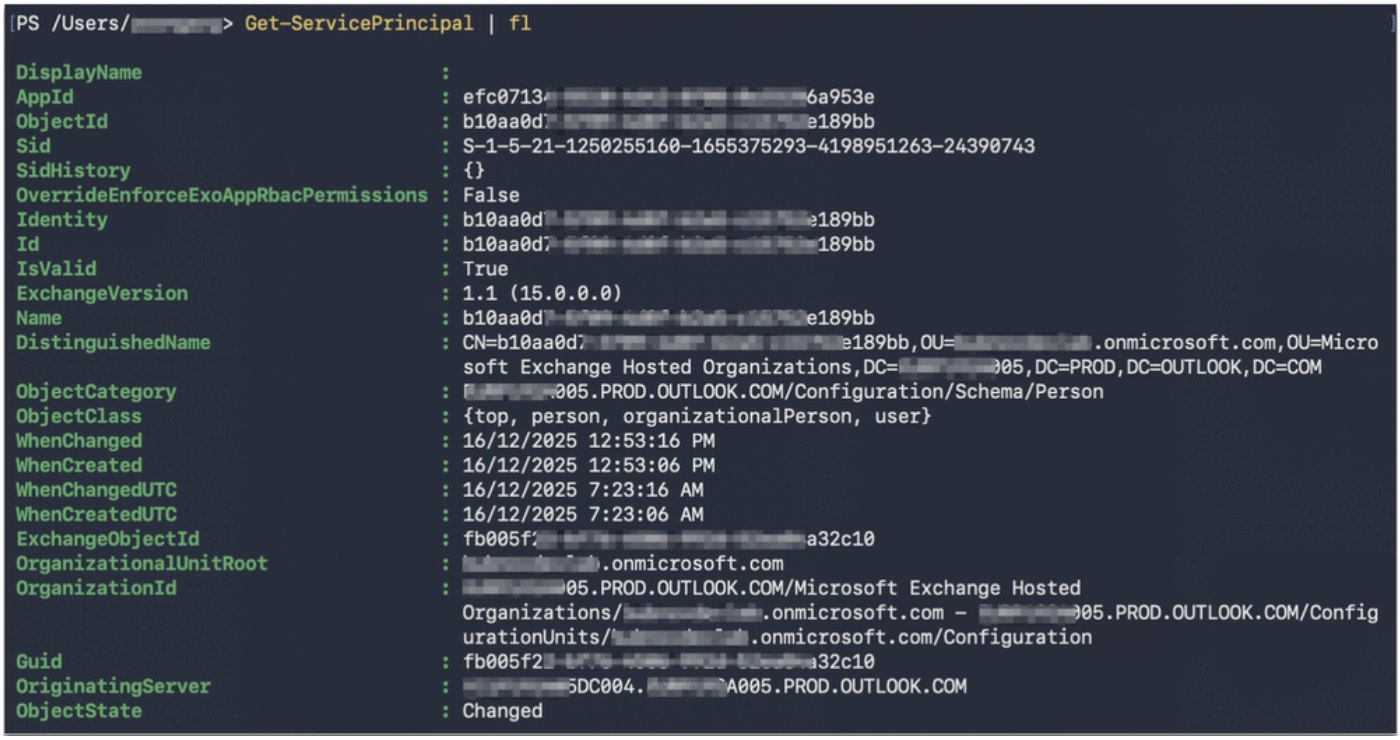
```
PS/Users/abc> New-ServicePrincipal -AppId xxxxxxxx-xxxx-xxxx-xxxx-xxxxxx6a953e -ObjectId b10axxxx-xxxx-
```

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

在Exchange中註冊Entra應用程式服務主體

四。 使用Get-ServicePrincipal cmdlet驗證您的註冊服務主體識別符號

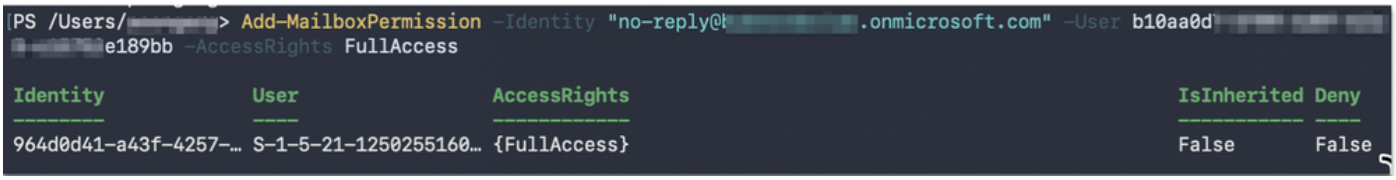
```
PS/Users/abc> Get-ServicePrincipal | fl
```



驗證註冊的服務主體識別符號

五。 租戶管理員現在可以在租戶中新增允許您的應用程式訪問的特定郵箱。此配置是使用Add-MailboxPermission cmdlet完成的。

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



新增訪問應用程式的郵箱許可權

Microsoft Entra應用程式現在可以使用OAuth 2.0客戶端憑據授予流，通過SMTP、POP或IMAP協定訪問允許的郵箱。

步驟 3:通過MS Exchange Online OAuth配置ISE SMTP使用者身份驗證

要配置簡單郵件傳輸協定(SMTP)伺服器，請按一下選單圖示(☰)，然後選擇Administration > System > Settings > SMTP Server.配置欄位。

- 在「SMTP Server Settings(SMTP伺服器設定)」區域中：
  - SMTP伺服器:smtp.office365.com
  - SMTP埠:587
  - 連線超時:60秒
- 在Authentication Settings區域中，使用切換開關啟用Use Authentication Settings選項。

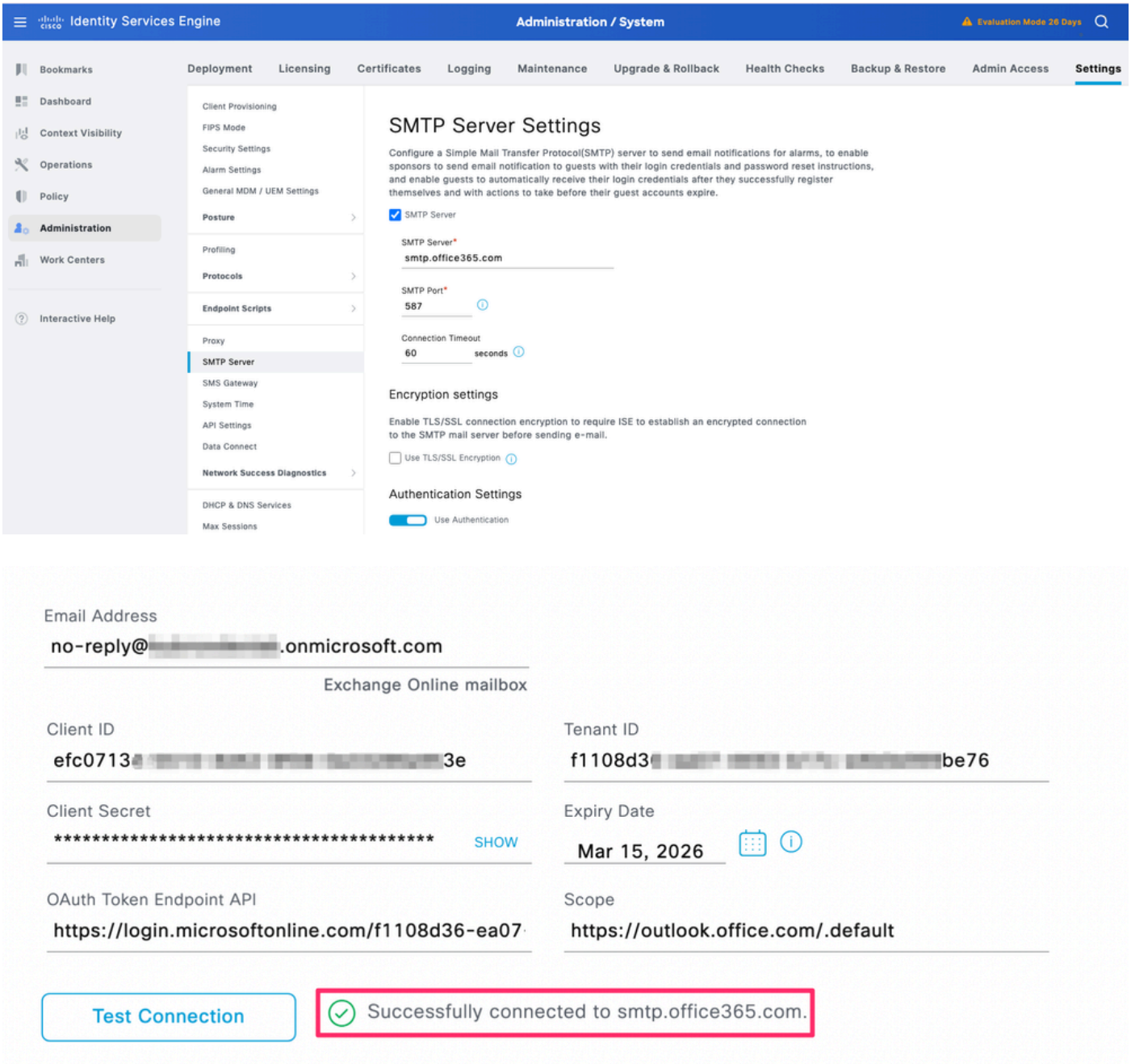
選擇MS Exchange Online OAuth:輸入這些值以配置Microsoft Exchange Online OAuth。

- 在「Username」欄位中，輸入Exchange Online使用者名稱的完整電子郵件地址。
- 在「客戶端ID」欄位中，輸入Azure Entra ID應用程式的客戶端ID。
- 在「租戶ID」欄位中，輸入Azure Entra ID應用程式的租戶ID。
- 在「Client Secret」欄位中，輸入Azure Entra ID應用程式的客戶端密碼。
- 在「Expiry Date」欄位中，輸入客戶端密碼的到期日期。

根據此配置觸發客戶端密碼到期警報。

- OAuth令牌終結點API 和Scope檔案將自動填充。

只能在測試連線操作成功後儲存配置。



成功測試與SMTP伺服器的連線

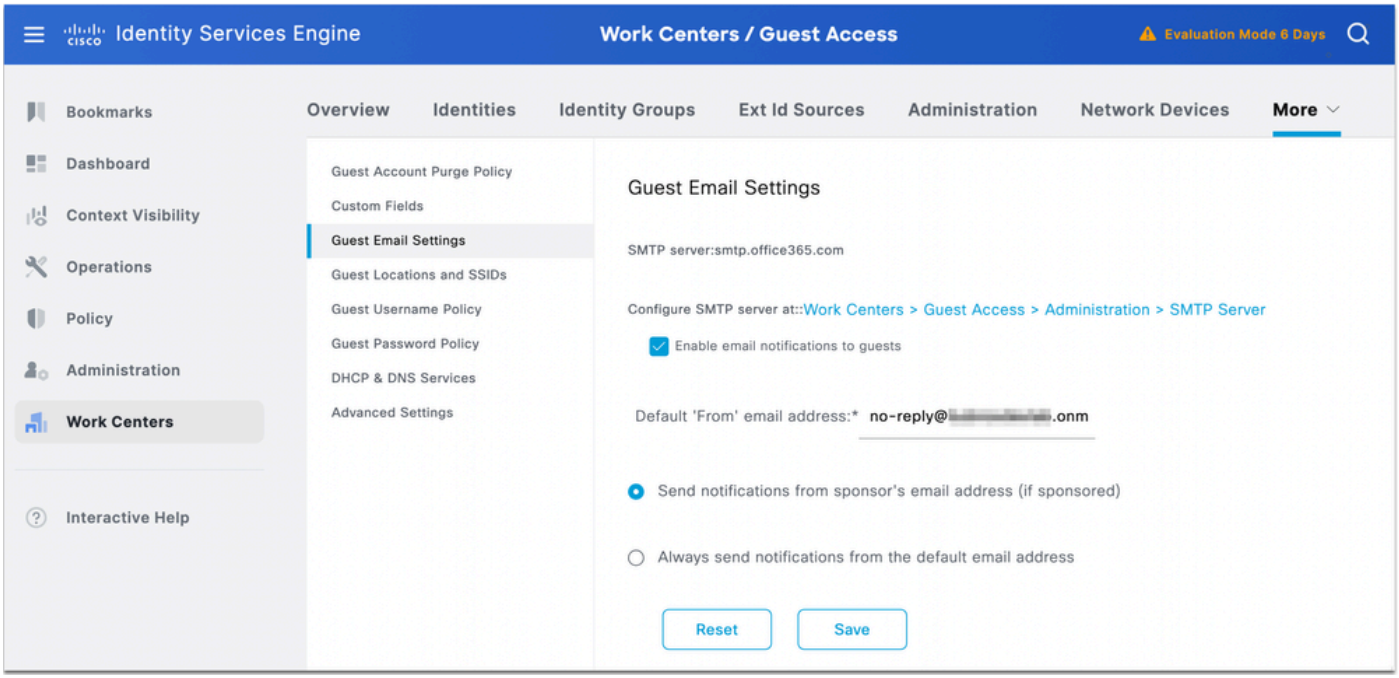
<#root>

Note:

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

驗證

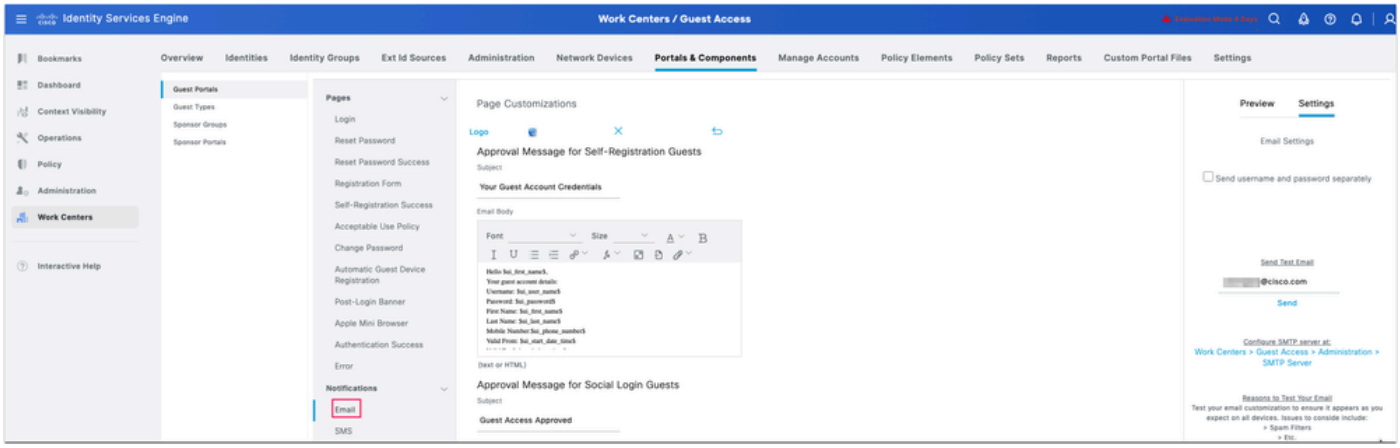
要驗證，請配置訪客電子郵件設定。導覽至工作中心 > Guest Access > Guest Email Settings。選擇Enable email notifications to guests，並配置在配置和Save的步驟1中配置的無回覆帳戶的預設「From」電子郵件地址。



更改訪客電子郵件設定

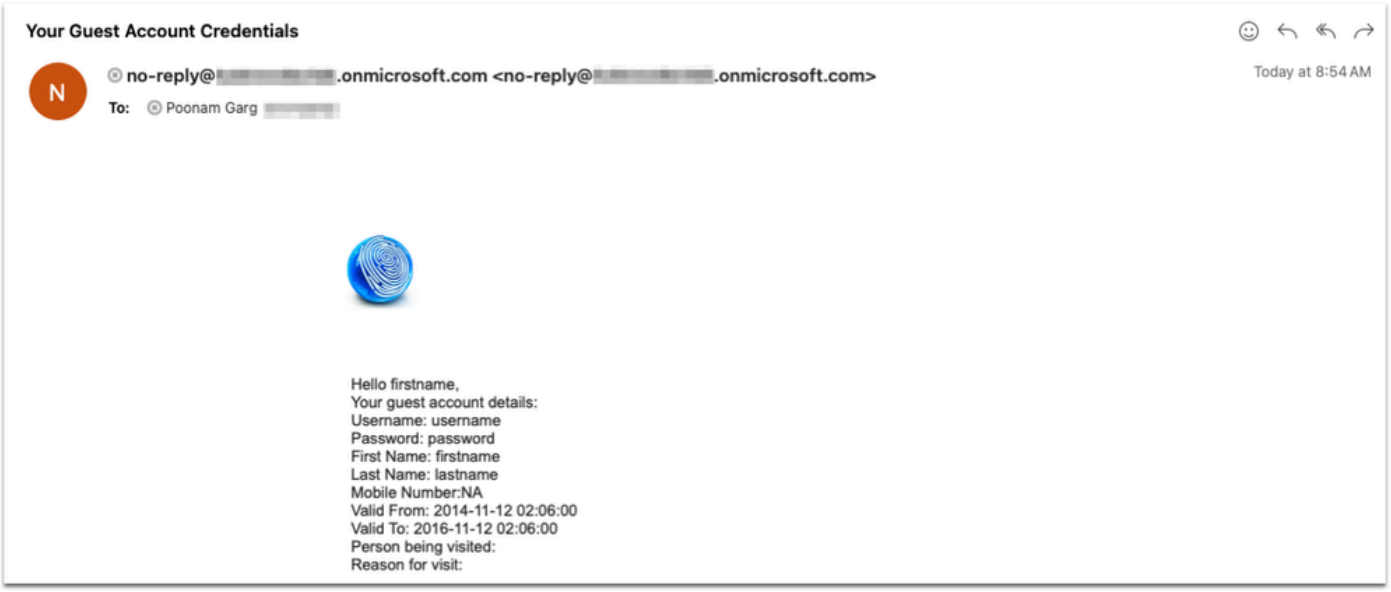
通過導航到工作中心(Work Centers)>訪客接入(Guest Access)>門戶和元件(Portal & Components)>訪客門戶(Guest Portals)>自註冊訪客門戶(Self-Registered Guest Portal)（預設）>門戶頁面定製(Portal Page Customization)>通知(Notifications)> Email來傳送測試電子郵件。

在預覽窗格右側下，按一下Settings > Send Test Email, Add您的電子郵件ID，然後按一下Send。



測試來自自助註冊門戶的電子郵件

您的Outlook必須收到來自驗證步驟1中配置的無回覆帳戶的電子郵件。螢幕截圖中的示例電子郵件
。

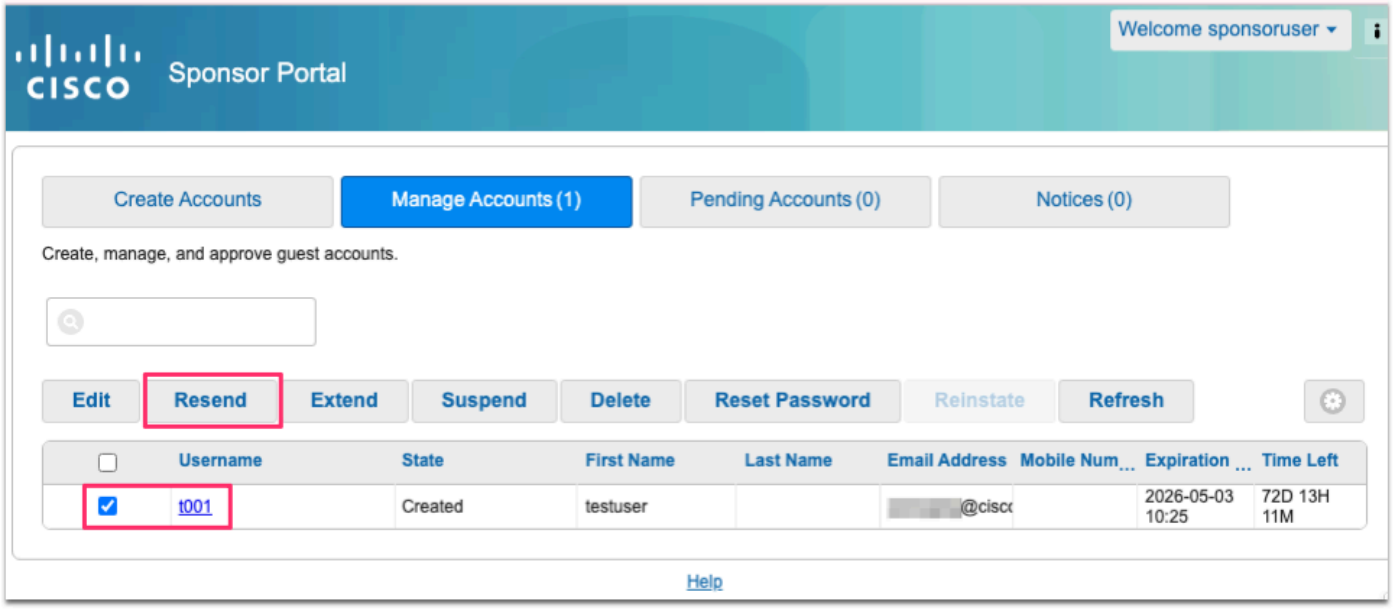


Outlook中接收的示例電子郵件

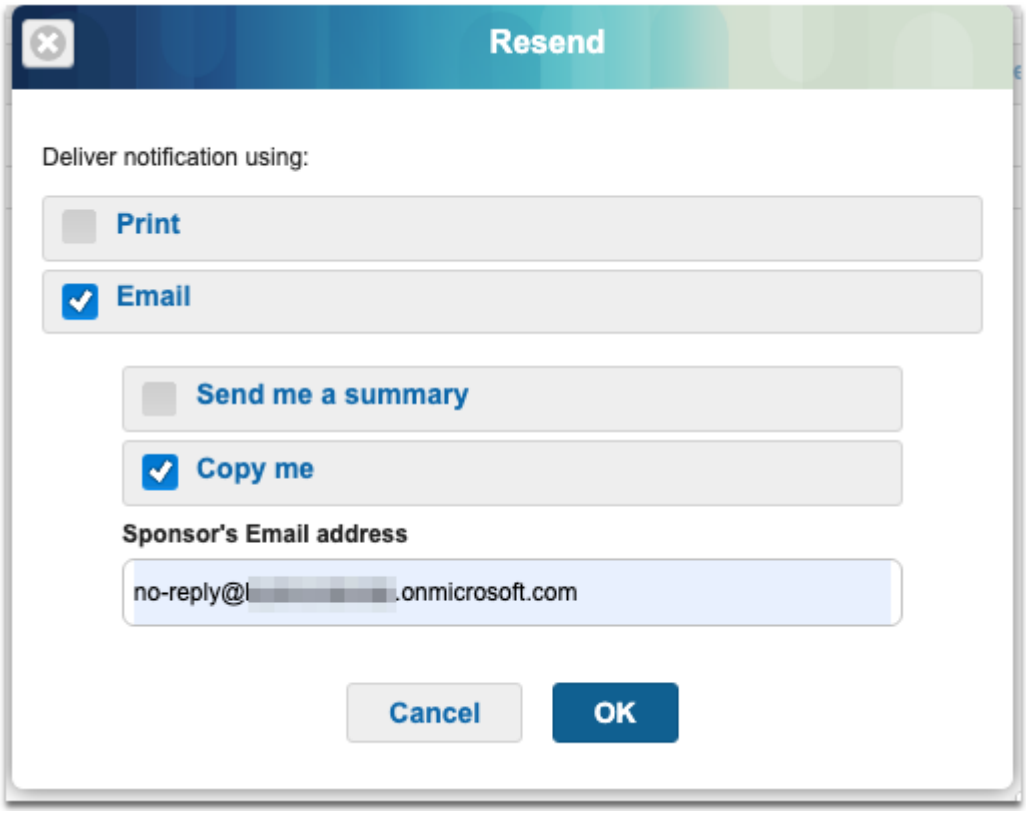
<#root>

```
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.
```

此外，通過由發起人管理員將使用者憑證重新傳送給訪客使用者來從發起人門戶進行測試。

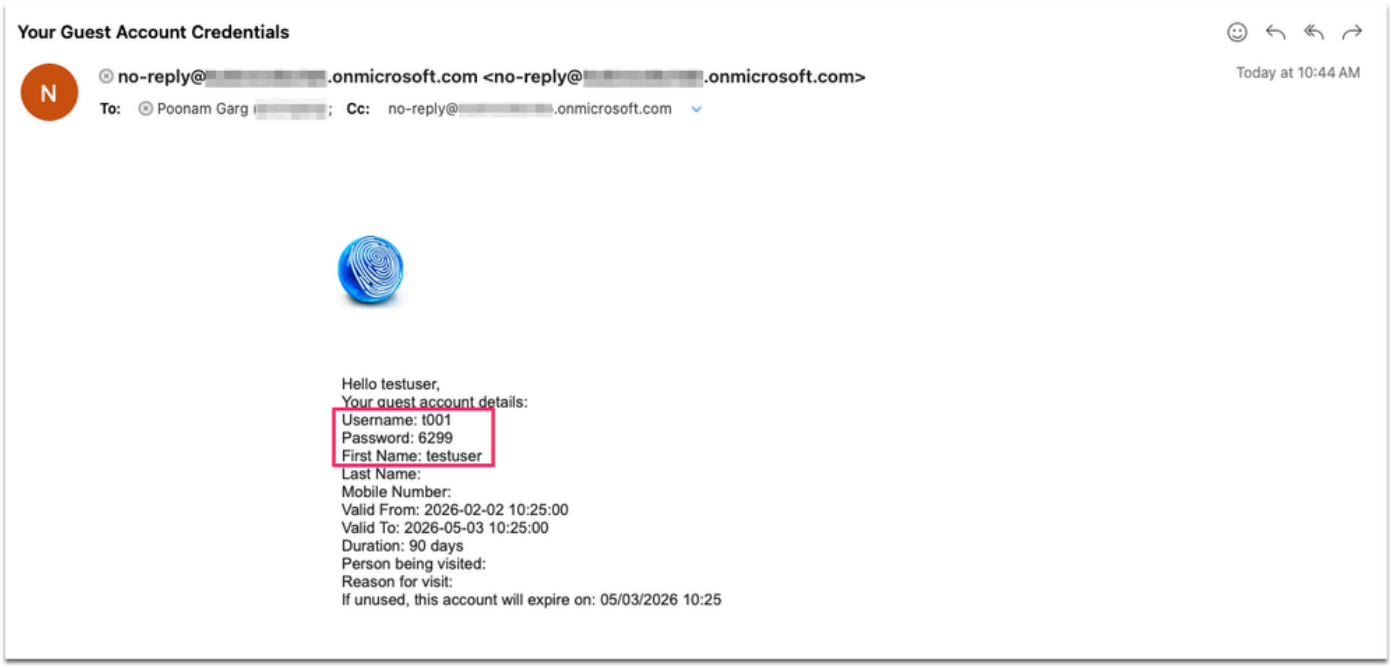


從發起人門戶測試



向訪客使用者傳送憑據

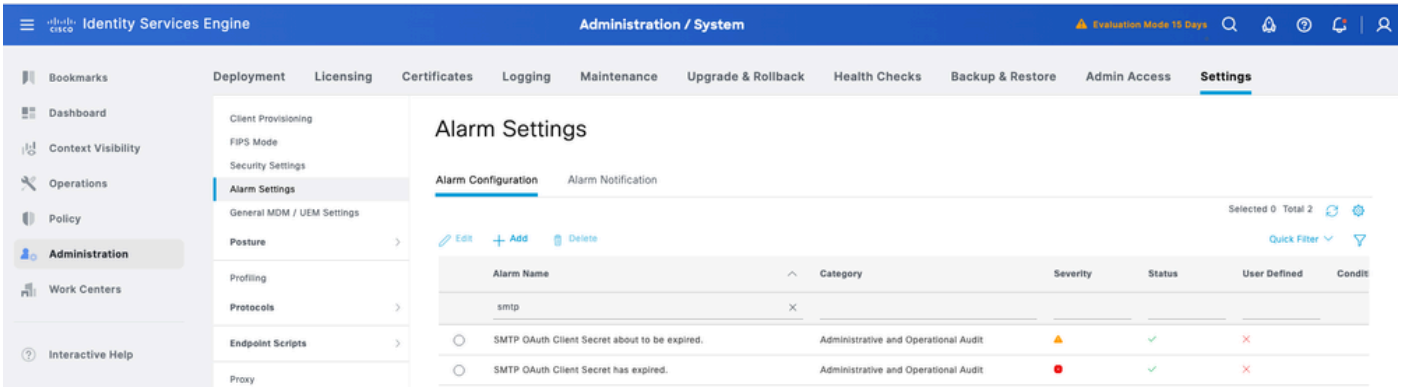
訪客使用者接收的示例電子郵件：



向訪客使用者傳送電子郵件通知

疑難排解

首先檢查客戶端金鑰到期的警報。與SMTP OAuth Client Secret相關的新警報將在ISE中新增。



要進一步排除故障，請根據您正在排除的問題在PAN、PSN或PMnT節點上啟用調試日誌。

- 日誌記錄元件：guest-access-admin， guestaccess
- 日誌檔案：guest.log

測試連線操作

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

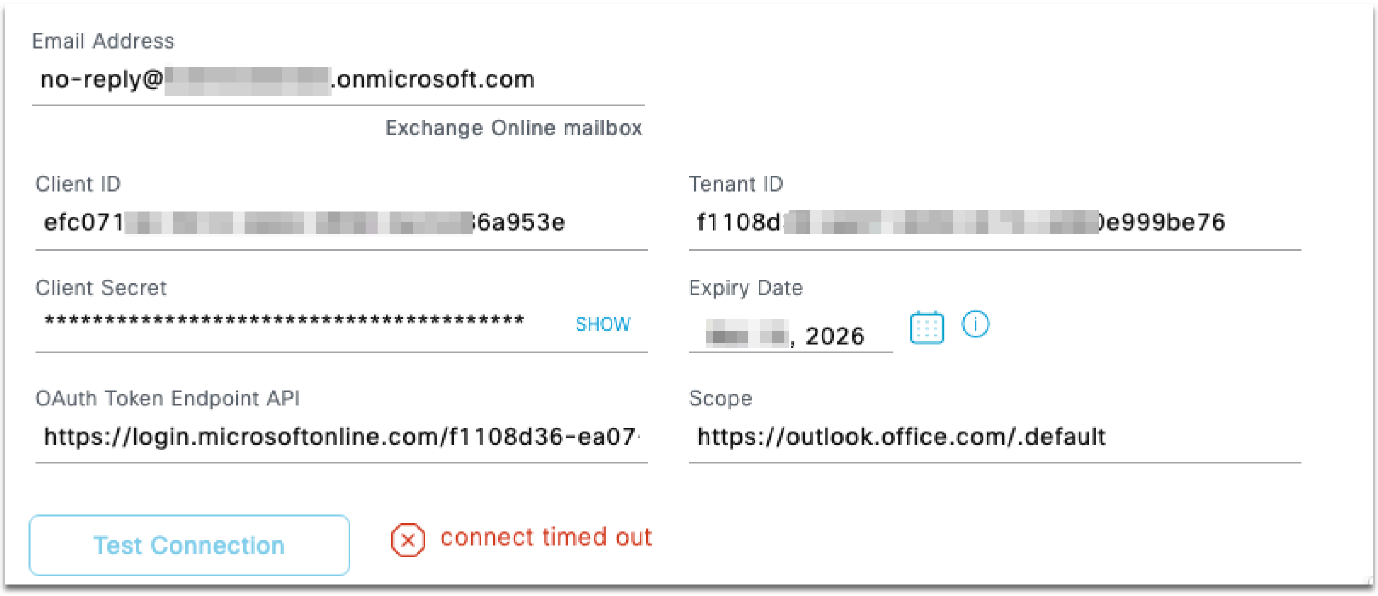
```
2026-02-02 05:59:15,630 DEBUG [admin-http-pool136][[]] cpm.guestaccess.apiservices.oauth.ExchangeOnline
2026-02-02 05:59:15,630 DEBUG [admin-http-pool136][[]] cpm.guestaccess.apiservices.oauth.OauthTokenCach
2026-02-02 05:59:20,146 DEBUG [admin-http-pool136][[]] cpm.guestaccess.apiservices.util.SmtpSession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

儲存操作

```
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
```

排除連線故障

1. GUI錯誤：連線到smtp.office365.con失敗。



連線超時錯誤

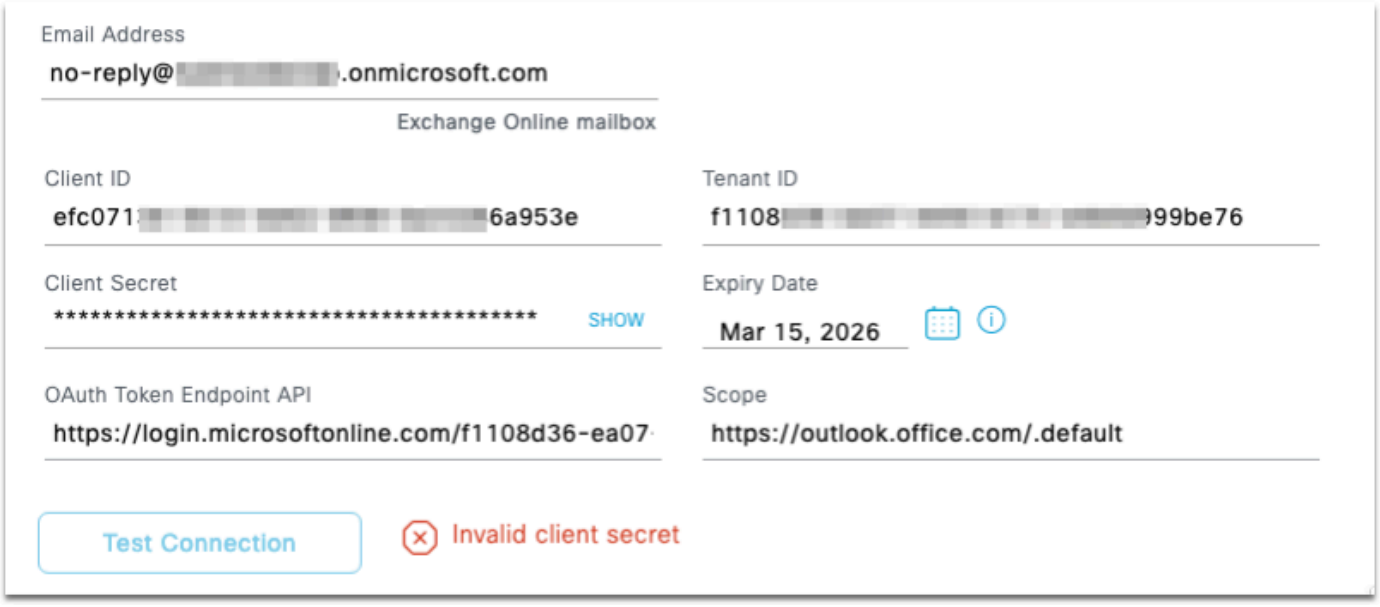
<#root>

```
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顯示連線超時。需要修復代理配置才能解決此問題。

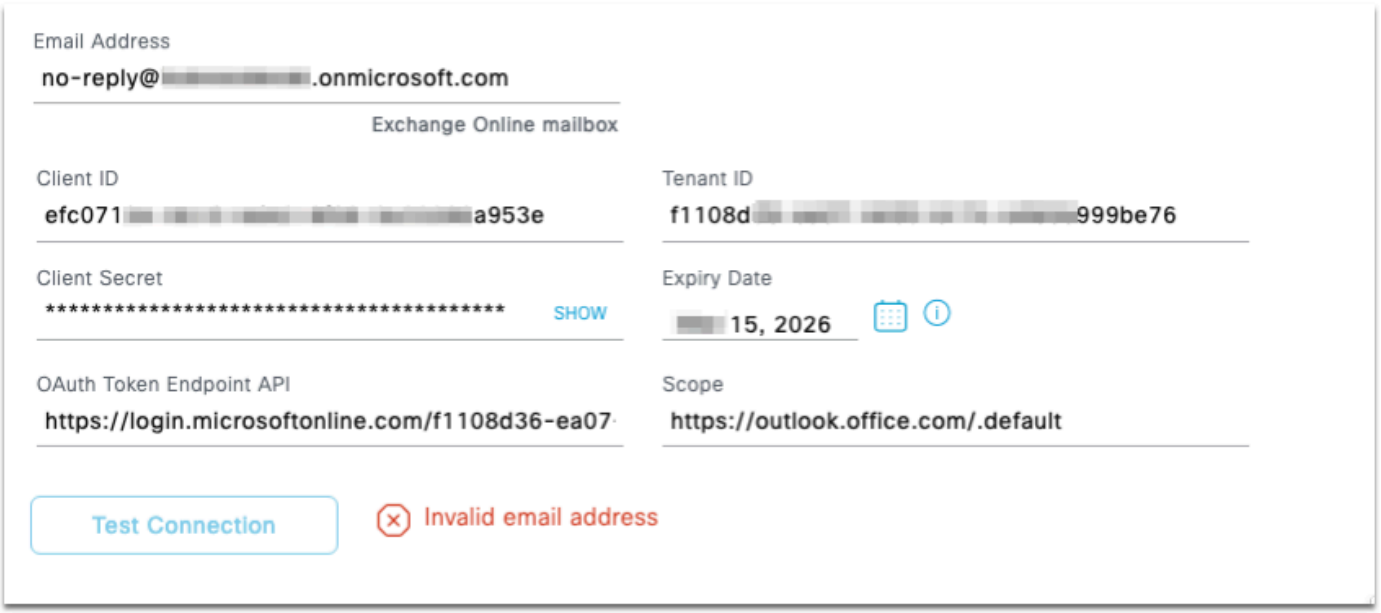
2. GUI錯誤：無效的OAuth終結點或租戶識別符號 — 自解釋。需要檢查租戶ID。

3.客戶端金鑰無效 — 相同，需要驗證客戶端金鑰值

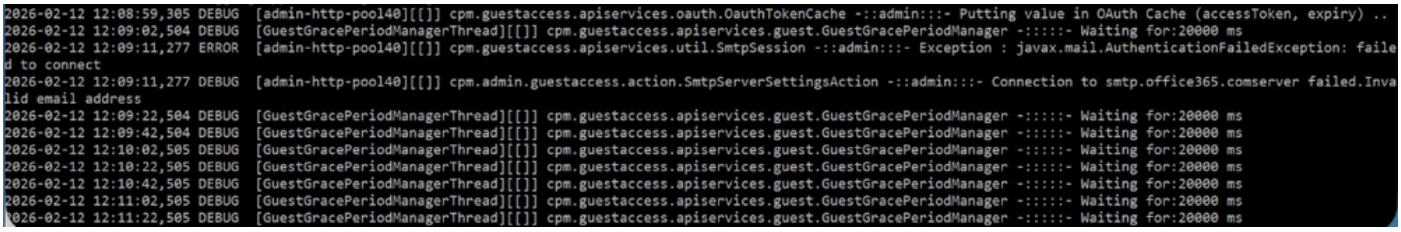


無效的客戶端加密錯誤

4.電子郵件地址無效 — 請確保服務原則配置正確。

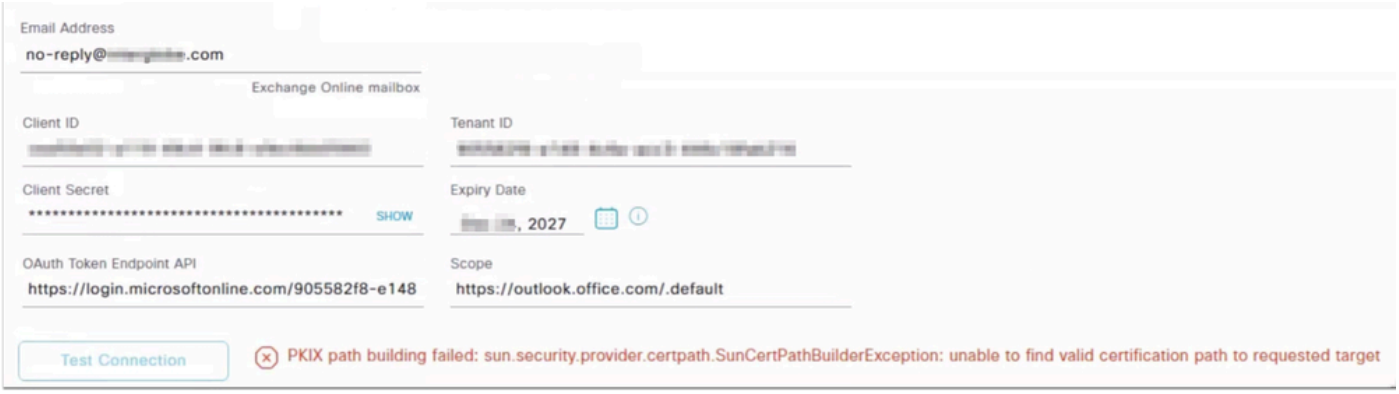


電子郵件地址無效錯誤



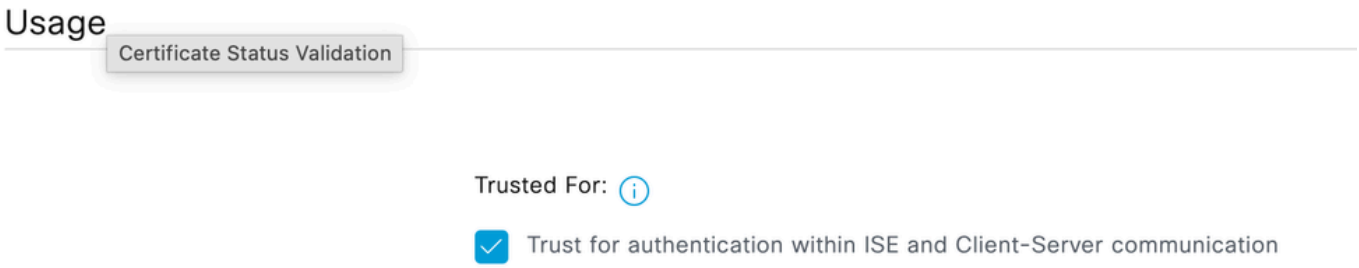
5.無法找到指向所請求目標的有效證書路徑:確保Entra ID證書鏈證書（根據pcap的Microsoft Azure RSA TLS頒發CA和DigiCert根CA等）存在於ISE的受信任證書儲存中，並且受信「信任ISE中的身份驗證和客戶端 — 伺服器通訊(基礎架構)」角色。

通過獲取pcap驗證EntraID傳送的所有證書。



證書驗證失敗

```
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
```



關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。