在ISE中配置基于OAuth的SMTP身份验证并排除故障

目录

简介

本文档介绍ISE中的OAuth 2.0配置，以通过Microsoft Exchange Online Mail SMTP服务器启用邮件通信。

先决条件

要求

思科建议您了解思科身份服务引擎(ISE)、简单邮件传输协议(SMTP)服务器功能和OAuth授权的基本知识。

使用的组件

ISE版本3.5 P1（3.2补丁8、3.3补丁8、3.4补丁4也支持此功能）

访问Microsoft EntraID和Microsoft 365管理中心

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

本节介绍Microsoft Entra ID和ISE上的配置，以支持用于以下目的的邮件通知：

- 向任何内部管理员用户发送电子邮件警报通知，同时启用邮件中包含系统警报选项。要配置发

件人邮件地址，请单击“管理”>“系统”>“设”>“设置”>“警报设置”>“警报通知”，然后键入在Microsoft 365管理中心下配置的邮件地址

- 发起人向访客发送电子邮件通知及其登录凭证和密码重置说明。对于访客和发起人流，发件人邮件在工作中心 > 访客接入 > 设置 > 访客邮件设置 > >默认“发件人”邮件地址下配置为在Microsoft 365管理中心下配置的邮件地址
- 使访客在成功注册自身后自动接收其登录凭证，并在访客帐户过期之前执行操作。
- 在密码到期日期之前，向ISE上配置的ISE管理员用户/内部网络用户发送提醒电子邮件。

发送邮件的ISE节点

电子邮件的目的	发送电子邮件的节点
访客访问过期	主策略管理节点(PAN)
警报	主动监控和故障排除节点(PMnT)
访客门户和发起人门户的发起人和访客通知	策略服务节点(PSN)
密码过期	主PAN

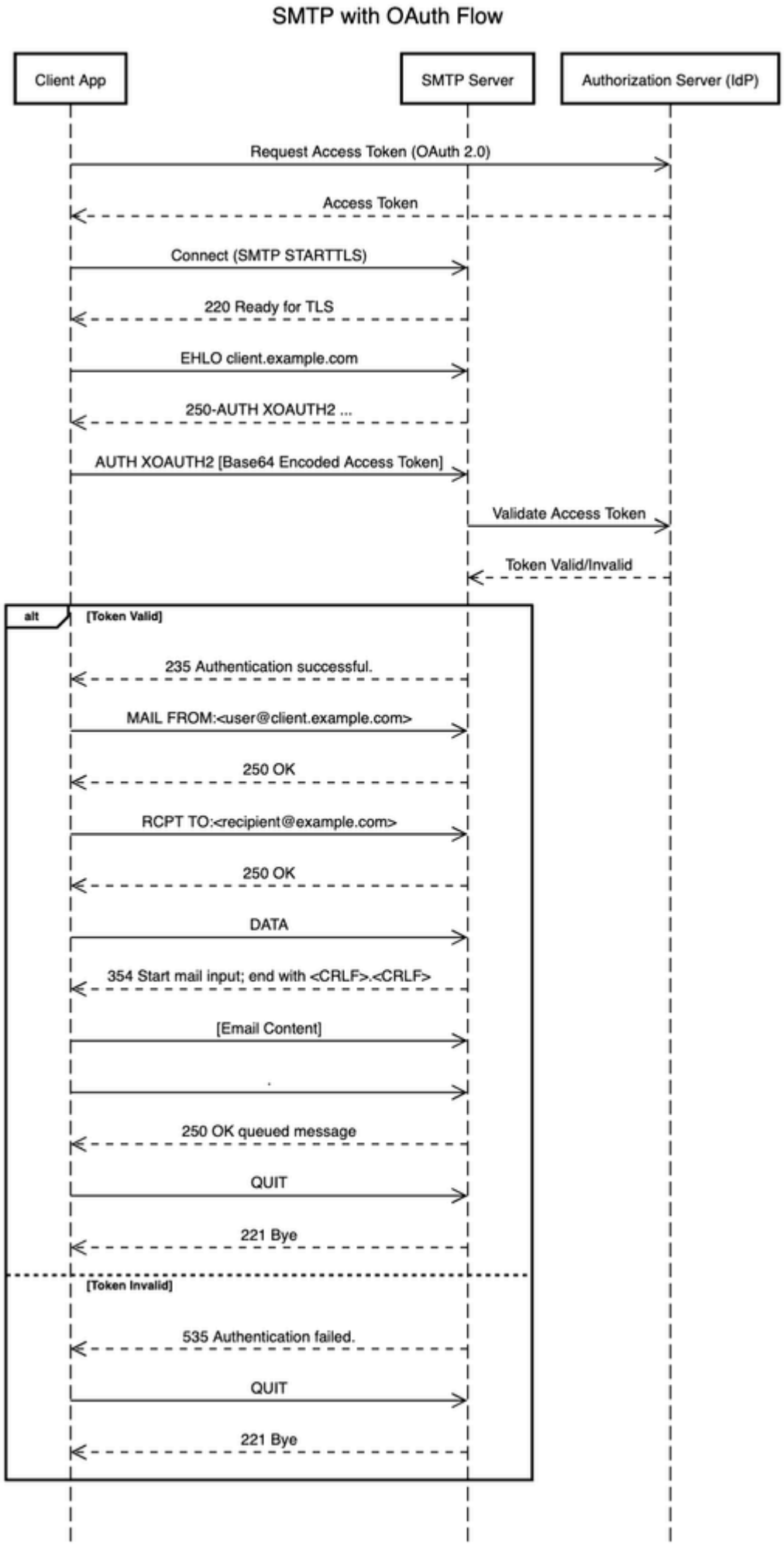
网络图

要将OAuth与ISE配合使用，需要3个步骤：

1.使用Microsoft Entra ID注册ISE应用

2.从令牌服务器(IDP)获取访问令牌

3.使用访问令牌验证与SMTP服务器的连接请求。


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

配置

```
abc@abc-M-5O6L ~ % sh
sh-3.2$ brew update
sh-3.2$ brew upgrade powershell
```

```
[PS /Users/[redacted]> 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
```

安装Powershell

II.要使用New-ServicePrincipal cmdlet，请安装ExchangeOnlineManagement并连接到您的租户，如片断所示：

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

连接到Exchange Online租户

三、在Exchange中注册Microsoft Entra应用服务主体。使用AppID和ObjectID [OBJECT_ID是来自企业应用程序节点（Azure门户）的“概述”(Overview)页面的“对象ID”(Object ID)进行应用程序注册。它不是App Registrations节点的Overview页面中的Object ID。使用错误的对象ID会导致身份验证失败]。

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

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

在Exchange中注册Entra应用程序服务主体

四。 使用Get-ServicePrincipal cmdlet验证已注册的服务主体标识符

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

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

DisplayName                          :
AppId                                : efc0713 6a953e
ObjectId                             : b10aa0d e189bb
Sid                                  : S-1-5-21-1250255160-1655375293-4198951263-24390743
SidHistory                           : {}
OverrideEnforceExoAppRbacPermissions : False
Identity                             : b10aa0d e189bb
Id                                   : b10aa0d 189bb
IsValid                              : True
ExchangeVersion                      : 1.1 (15.0.0.0)
Name                                 : b10aa0d e189bb
DistinguishedName                    : CN=b10aa0d e189bb,OU= .onmicrosoft.com,OU=Micro
                                       soft Exchange Hosted Organizations,DC= 005,DC=PROD,DC=OUTLOOK,DC=COM
ObjectCategory                       : 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 a32c10
OrganizationalUnitRoot               : .onmicrosoft.com
OrganizationId                       : 05.PROD.OUTLOOK.COM/Microsoft Exchange Hosted
                                       Organizations/ .onmicrosoft.com - 05.PROD.OUTLOOK.COM/Config
                                       urationUnits/ .onmicrosoft.com/Configuration
Guid                                 : fb005f2 a32c10
OriginatingServer                    : 5DC004. A005.PROD.OUTLOOK.COM
ObjectState                          : Changed
```

验证注册的服务主体标识符

五。 租户管理员现在可以在租户中添加允许您的应用程序访问的特定邮箱。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
```

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

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

添加邮箱权限以访问应用程序

现在，Microsoft Entra应用程序可以使用OAuth 2.0客户端凭证授权流程，通过SMTP、POP或IMAP协议访问允许的邮箱。

步骤 3：通过MS Exchange Online OAuth配置ISE SMTP用户身份验证

要配置简单邮件传输协议(SMTP)服务器，请点击菜单图标(☰)并选择Administration > System > Settings > SMTP Server。配置字段。

- 在SMTP Server Settings区域中：
  - SMTP服务器:smtp.office365.com
  - SMTP端口:587
  - 连接超时:60 秒
- 在Authentication Settings区域中，使用切换开关启用Use Authentication Settings选项。

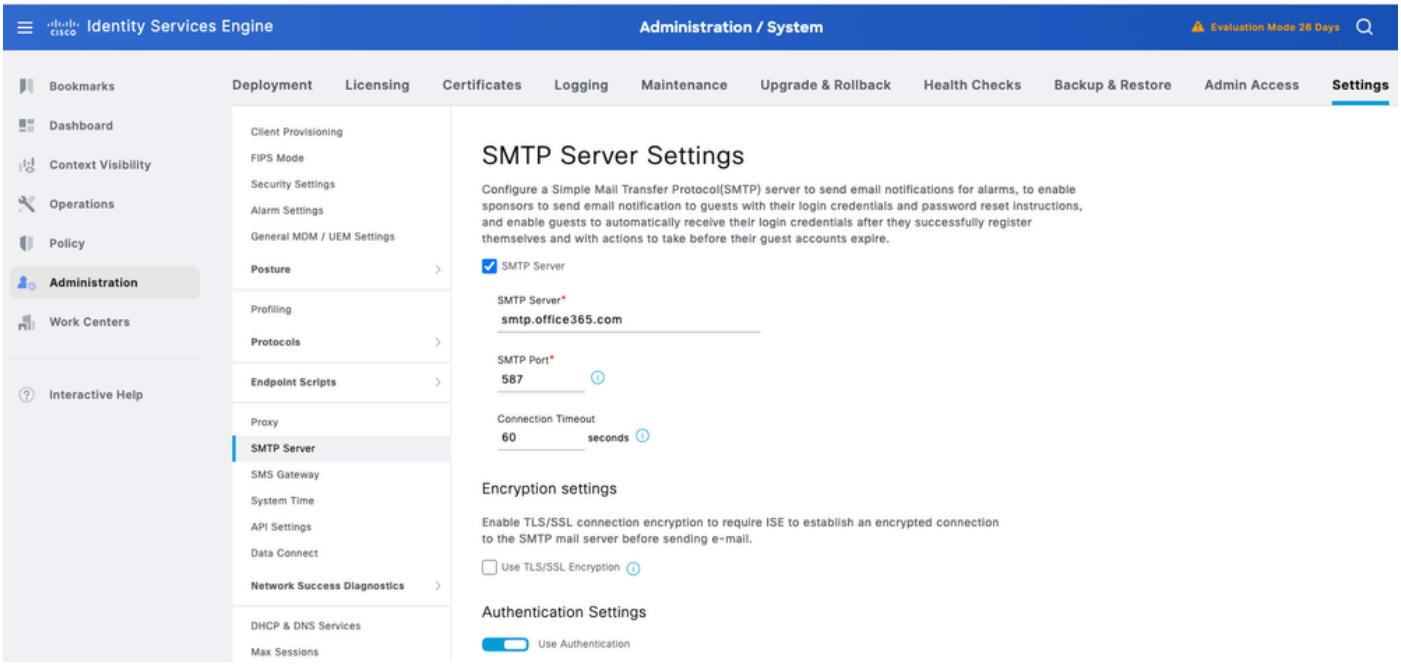
选择MS Exchange Online OAuth:输入这些值以配置Microsoft Exchange Online OAuth。

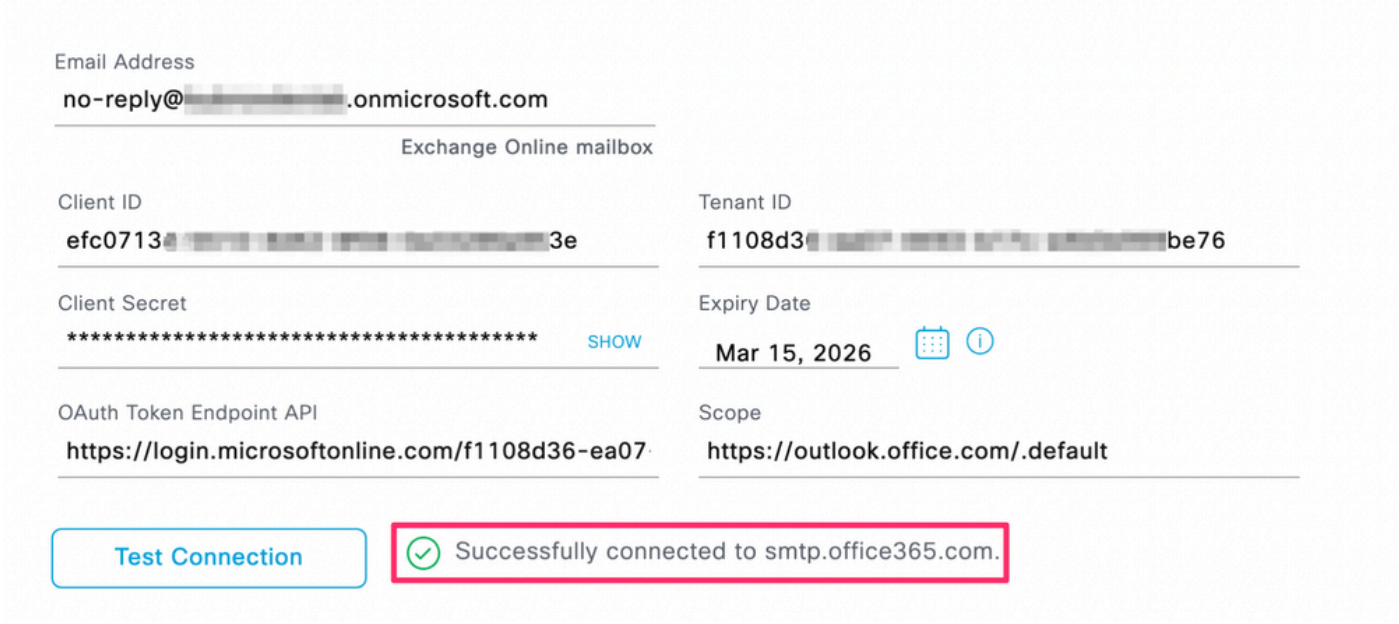
- 在用户名字段中，输入Exchange Online用户名的完整电子邮件地址。
- 在客户端ID字段中，输入Azure Entra ID应用程序的客户端ID。
- 在租户ID字段中，输入Azure Entra ID应用程序的租户ID。
- 在Client Secret字段中，输入Azure Entra ID应用程序的客户端密码。
- 在Expiry Date字段中，输入客户端密钥的到期日期。

根据此配置触发客户端密钥到期警报。

- 将自动填充OAuth令牌终端API 和作用域文件。

只有在测试连接操作成功后才能保存配置。





成功测试与SMTP服务器的连接

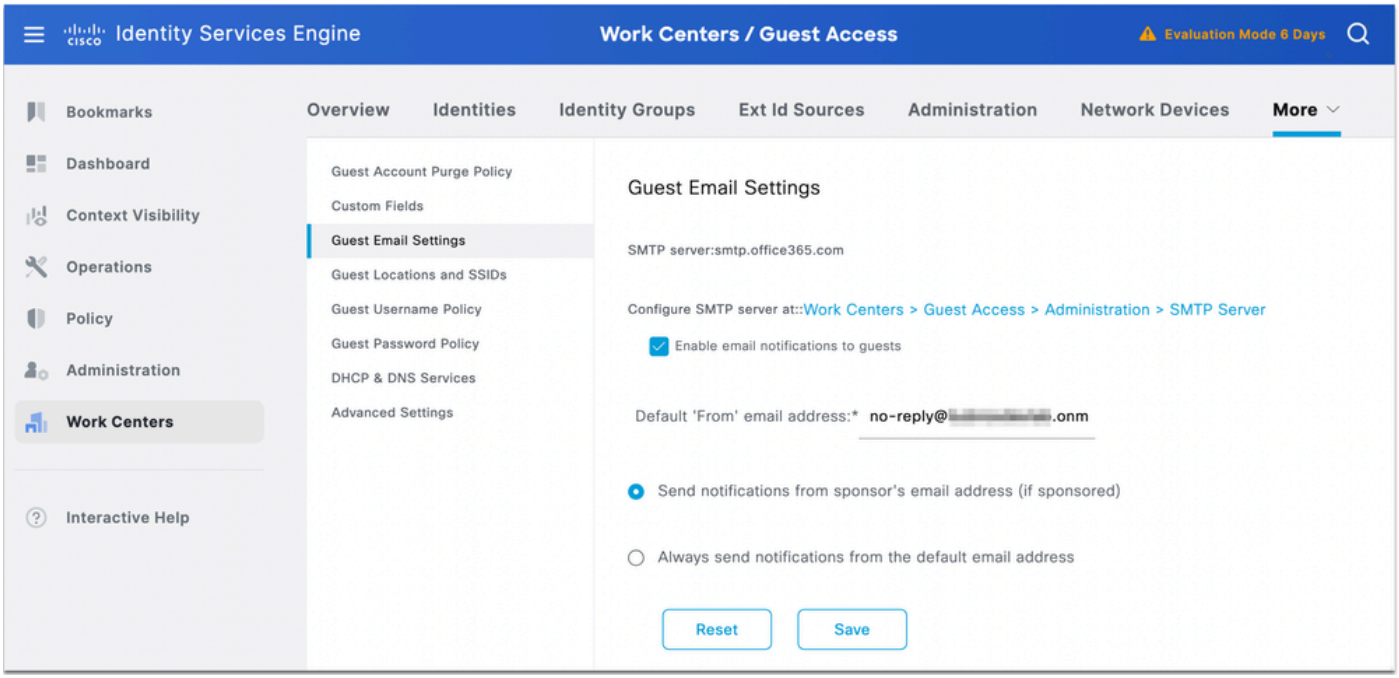
<#root>

Note:

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

验证

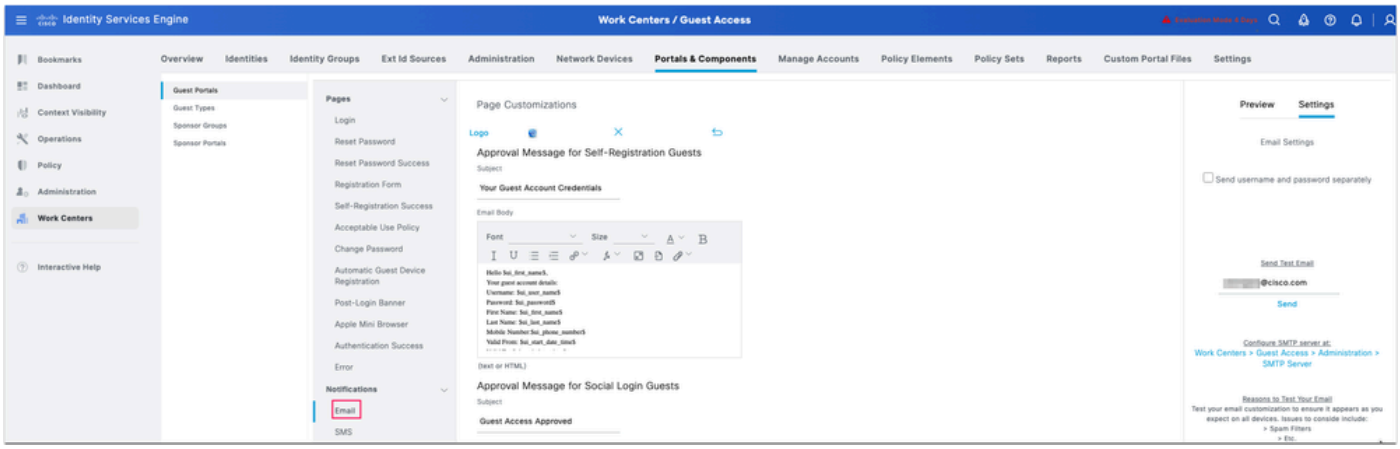
要验证，请配置访客邮件设置。导航到工作中心 > 访客接入 > 访客邮件设置。选择Enable email notifications to guests，并配置和Save的第1步中配置的无应答帐户的Default 'From'邮件地址。



更改访客邮件设置

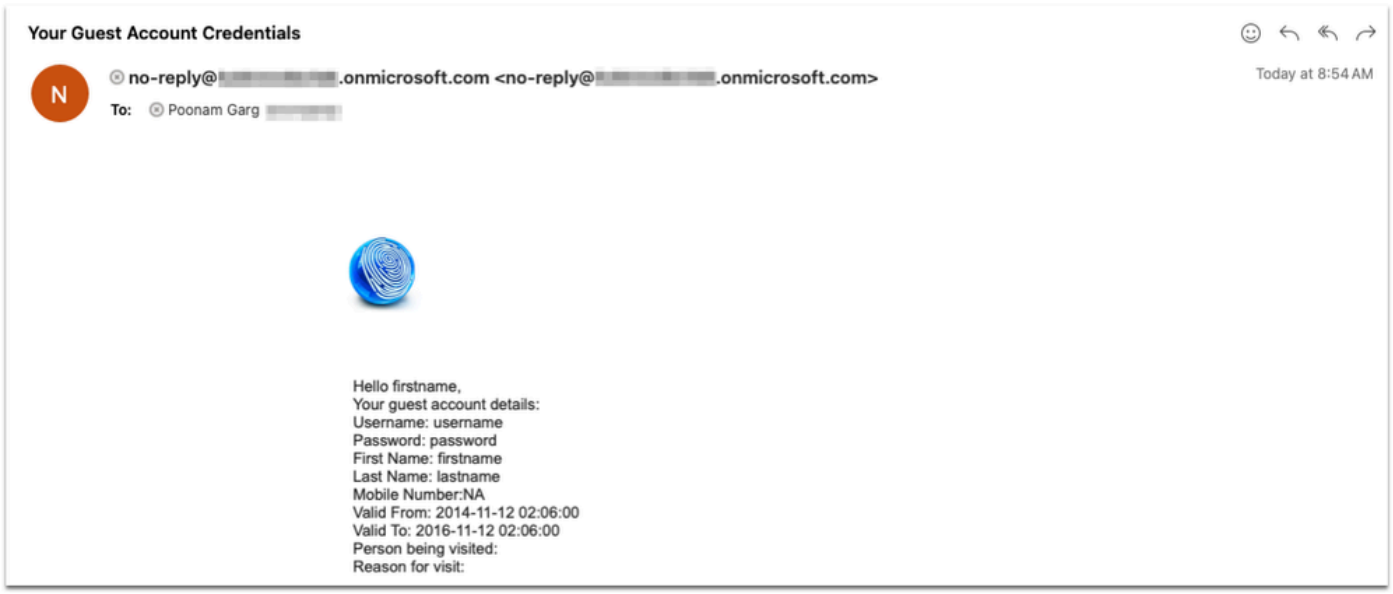
通过导航到工作中心(Work Centers)>访客接入(Guest Access)>门户和组件(Portal & Components)>访客门户(Guest Portals)>自注册访客门户(Self-Registered Guest Portal)（默认）>门户页面定制(Portal Page Customization)>通知(Notifications)>邮件(Email)来发送测试电子邮件。

在预览窗格右侧下，单击Settings > Send Test Email，然后单击Send。



来自自助注册门户的测试电子邮件

您的Outlook必须收到来自验证步骤1中配置的无应答帐户的邮件。屏幕截图中的示例电子邮件。



Outlook中接收的示例电子邮件

<#root>

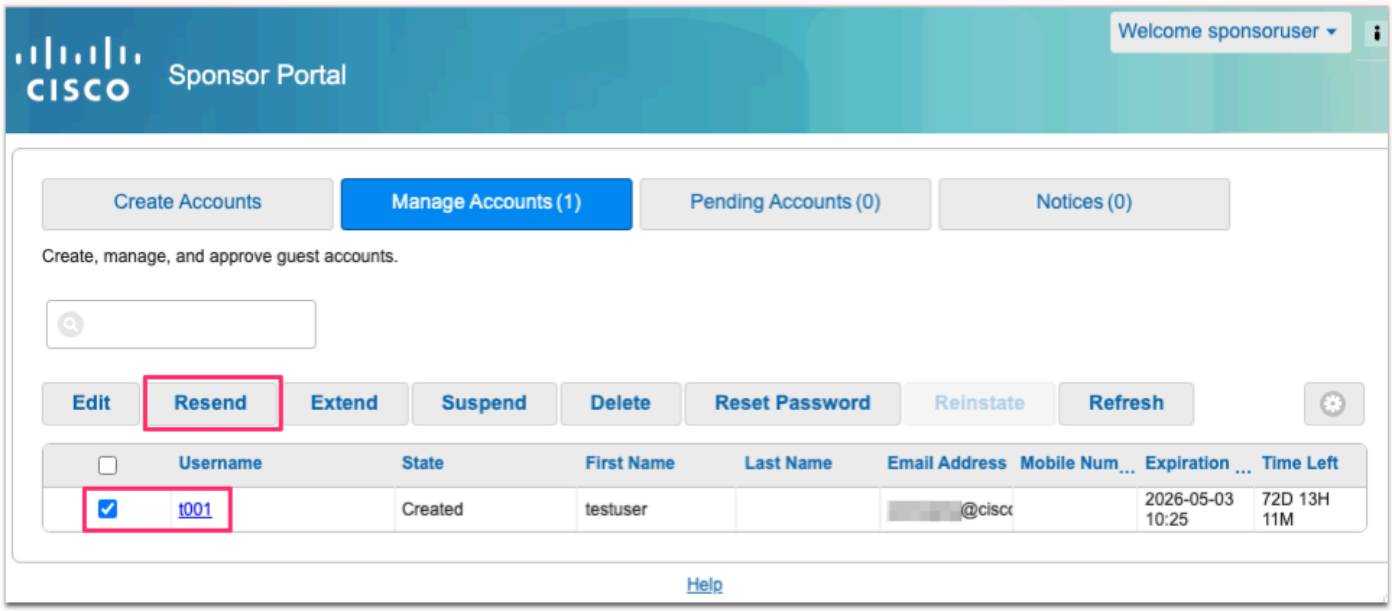
```
Guest.log at debug level:
2026-02-02 05:17:34,608 INFO    [admin-http-pool139][[]] cpm.guestaccess.apiservices.util.SmtpMsgRetryTh

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
```

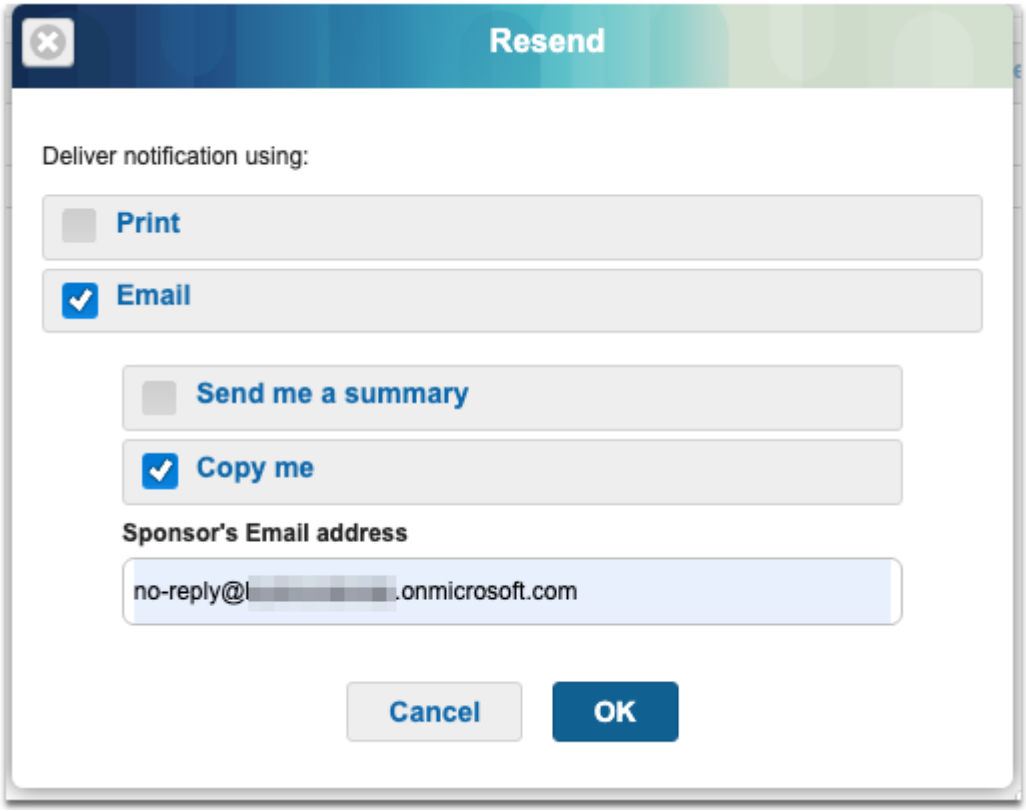
sendMailMessage: Future.get status: success

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

此外，通过保证人管理员将用户凭证重新发送给访客用户，从保证人门户进行测试。

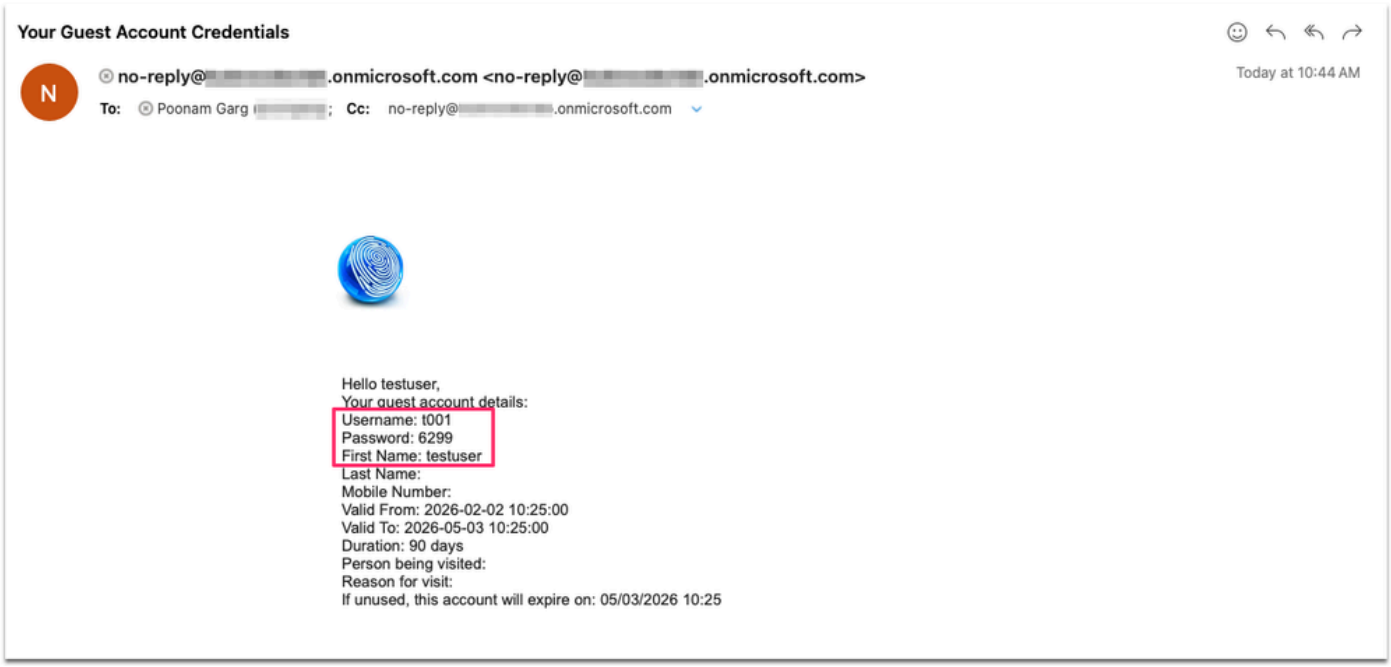


从发起人门户进行测试



向访客用户发送凭证

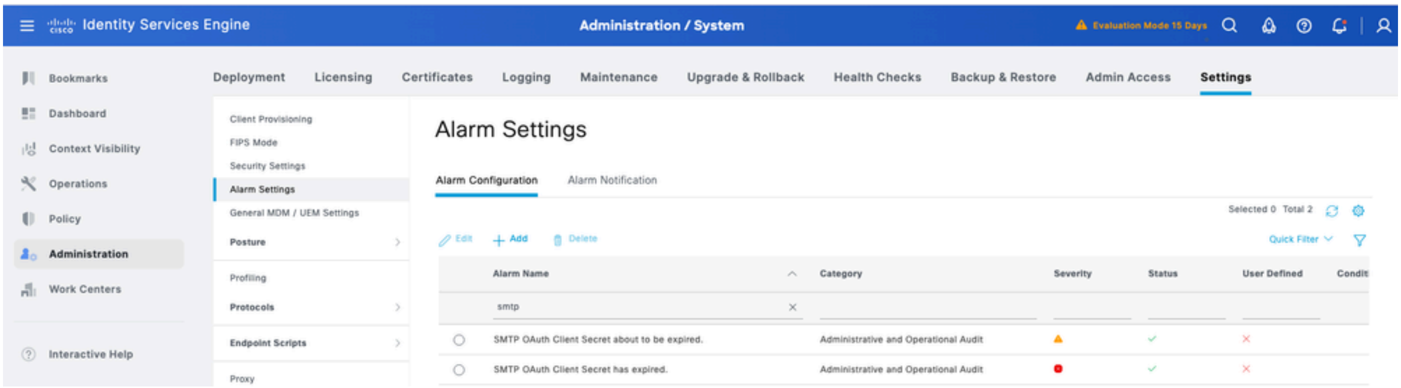
访客用户接收的示例电子邮件：



向访客用户发送电子邮件通知

故障排除

首先检查客户端密钥到期的警报。与SMTP OAuth客户端密钥相关的新警报将在ISE中添加。



要进一步排除故障，请根据您正在排除的问题在PAN、PSN或PMnT节点上启用调试日志。

- 日志记录组件：guest-access-admin， guestaccess
- 日志文件:guest.log

测试连接操作

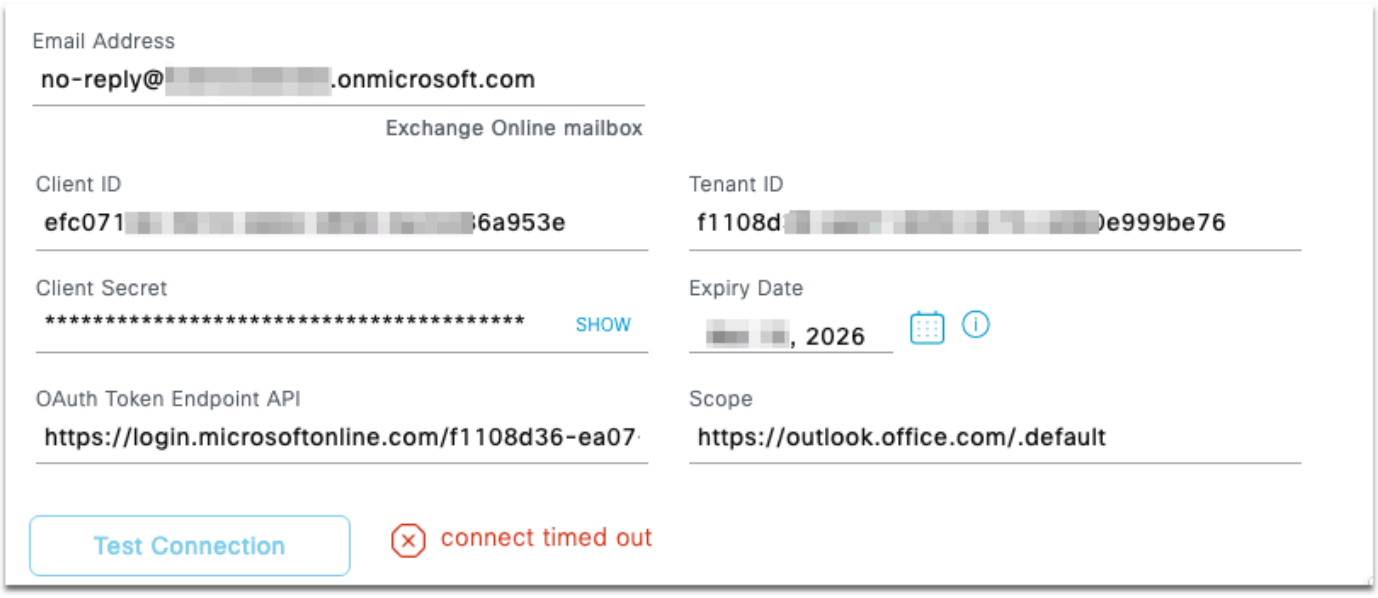
```
2026-02-02 05:58:21,501 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.Sm
2026-02-02 05:58:21,501 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.Sm
2026-02-02 05:58:21,501 DEBUG [MnT-AlarmWorkerMail-Threadpool-0][[]] cpm.guestaccess.apiservices.util.Sm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

保存操作

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

排除连接故障

1. GUI错误：连接到smtp.office365.con失败。



连接超时错误

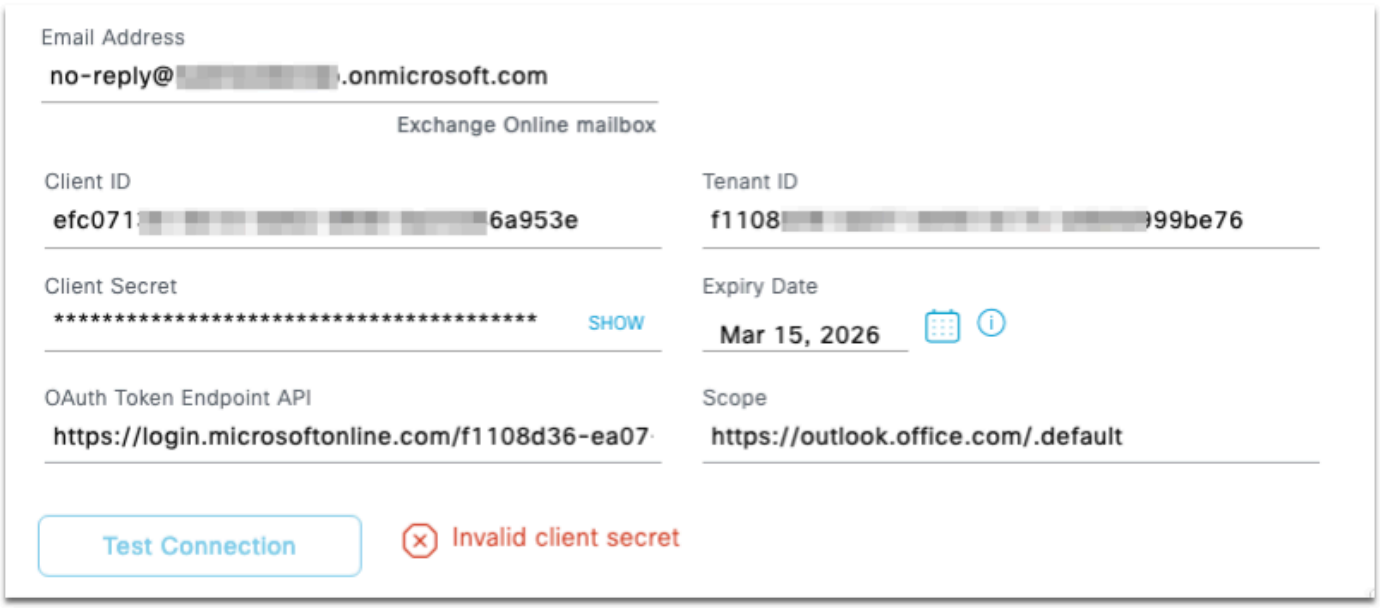
<#root>

```
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显示连接超时。需要修复代理配置才能解决此问题。

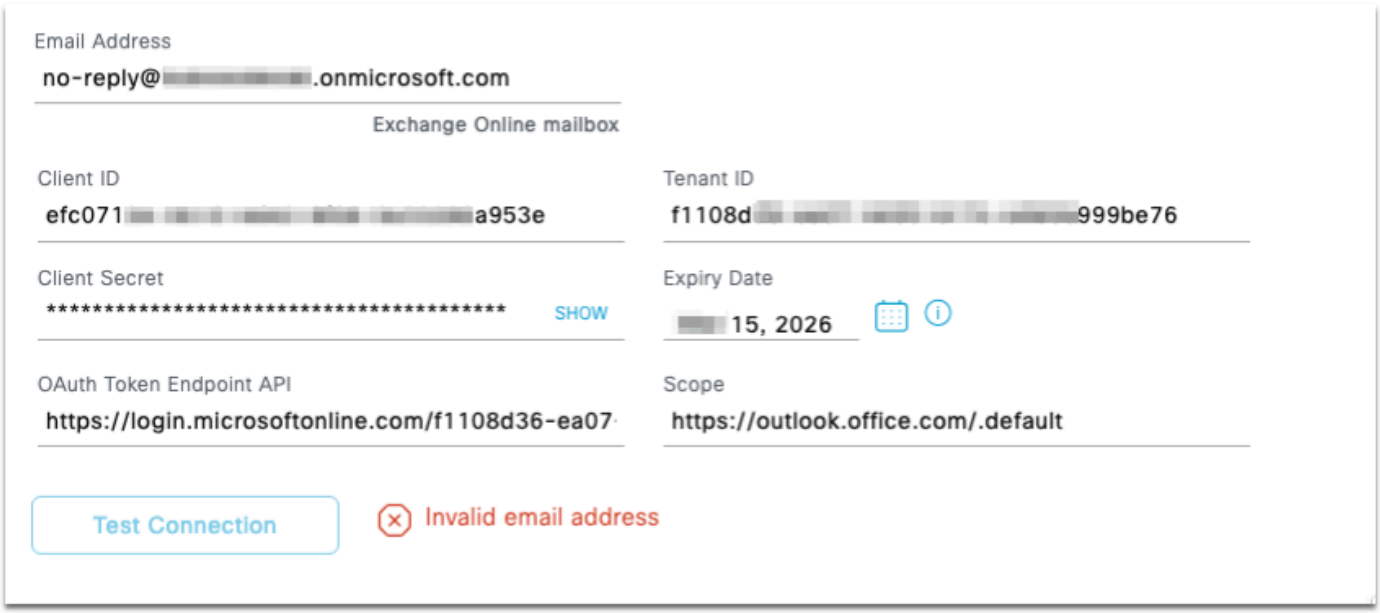
2. GUI错误：无效的OAuth终结点或租户标识符 — 自行解释。需要检查租户ID。

3.客户端密钥无效 — 相同，需要验证客户端密钥值

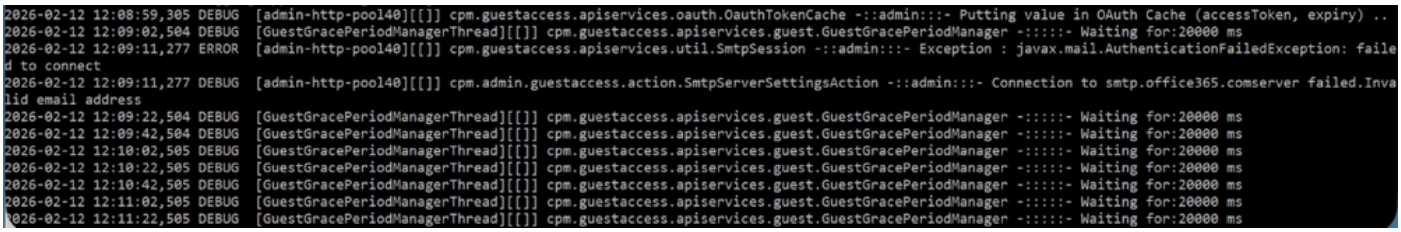


无效的客户端加密错误

4.电子邮件地址无效 — 请确保服务原则配置正确。

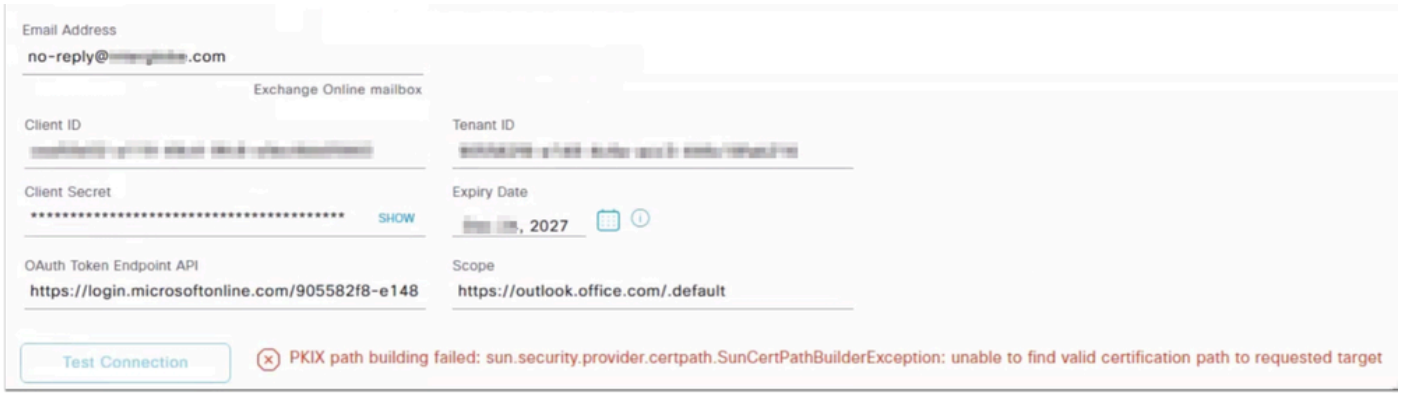


无效的电子邮件地址错误



5.无法找到到所请求目标的有效证书路径:确保Entra ID证书链证书（根据pcap的Microsoft Azure RSA TLS颁发CA和DigiCert Root CA等）存在于ISE的受信任证书存储中，并且为“Trust for authentication within ISE and Client-Server communication(Infrastructure)”角色受信任。

通过获取pcap验证EntraID发送的所有证书。



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
```

Usage

Certificate Status Validation

Trusted For: ⓘ

☑ Trust for authentication within ISE and Client-Server communication

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。