思科邮件安全应用 - Office 365 威胁分析器工具 v1

最后更新日期：2017 年 11 月 10 日

关于本演示

本预配置演示指南包括以下内容：

要求

下表列出了本预配置演示的要求。

表 1. 要求

必需	可选
• 笔记本电脑	• 思科 AnyConnect®

关于此解决方案

随着越来越多客户从传统的本地 Microsoft Exchange 迁移到基于云的 Office 365 作为其邮件策略的一部分，对于更严格的邮件安全解决方案的需求也越来越普遍。

本演示介绍如何展示无成本、低影响地使用思科 Office 365 威胁分析器工具的价值。此工具配合云邮件安全设备使用，通过应用编程接口 (API) 扫描 Microsoft Office 365 邮箱并提供报告，报告中包含对 Office 365 邮件环境中存在的垃圾邮件、病毒、灰色邮件和恶意软件等威胁的重要见解。

思科邮件安全设备具有业界领先的入站和出站邮件清理和控制功能，针对当今影响邮件且不断迅速变化的动态威胁提供高可用性邮件保护，并以各种外形满足客户的不同需求。

有关思科邮件安全设备的特性和优势、可以提供的外形、思科的竞争优势等，请阅读邮件安全设备概述了解详细信息。

有关思科云邮件安全设备的其他信息，请访问 http://www.cisco.com/go/cloudemail

拓扑

本部分内容包括用于说明解决方案脚本化场景和功能的预配置用户和组件。大多数组件完全可以使用预定义的管理用户帐户进行配置。通过点击活动会话的**拓扑**菜单中的组件图标，您可以查看用于访问组件的 IP 地址和用户帐户凭证，在需要用到 IP 地址和用户帐户凭证的场景步骤中也同样如此。

图 1. dCloud 拓扑

开始演示

演示前的准备

思科 dCloud 强烈建议您事先使用活动会话执行本文档中的任务，然后再给现场观众演示。这样您将熟悉文档和内容的结构。

遵循本指南后，有必要安排一个新会话，以将环境重置为其原始配置。

细致的准备对于一场成功的演示至关重要。

按照步骤安排内容会话并配置演示环境。

1. 启动 dCloud 会话。[查看具体操作]

注意：激活会话可能需要 10 分钟的时间。

2. 为了获得最佳性能，请通过**思科 AnyConnect VPN** [查看具体操作] 和**笔记本电脑上的本地 RDP 客户端** [查看具体操作] 连接到工作站。
   - 工作站 1：**198.18.133.36**，用户名：**administrator**，密码：**C1sco12345**

注意：您也可以使用思科 dCloud 远程桌面客户端 [查看具体操作] 连接到工作站。dCloud 远程桌面客户端非常适合于访问极少交互的活动会话。但是，许多用户在使用此方法时会遇到连接和性能问题。

场景 1： Office 365 概述

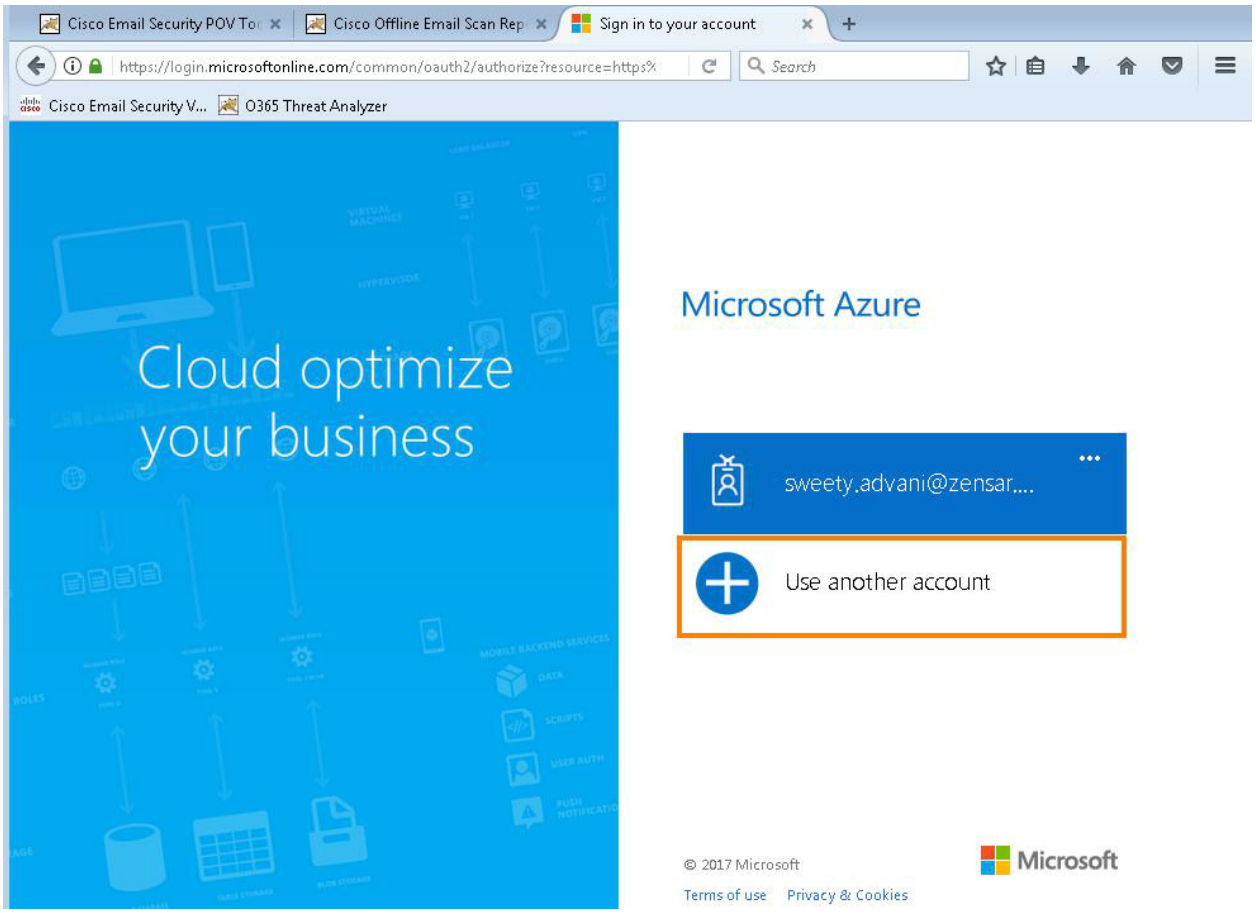
步骤

创建 API 注册

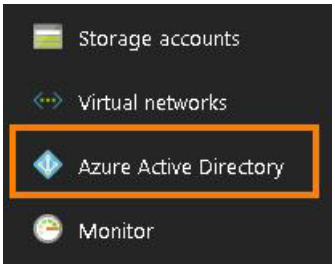
1. 在工作站上打开 Firefox。打开新的选项卡并导航至 **https://portal.azure.com**。

注意：登录此门户需要使用管理员帐户。

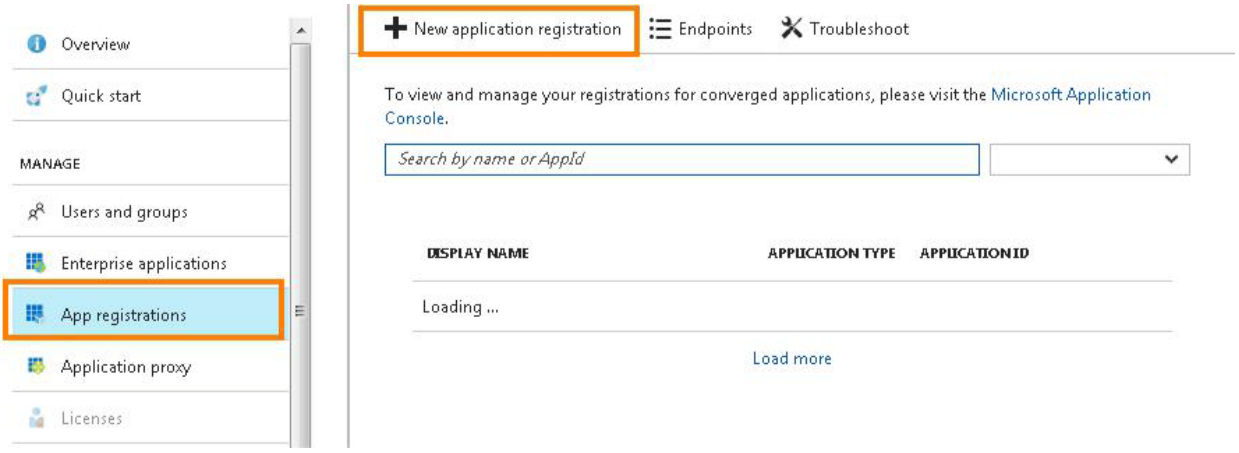
2. 选择**使用其他帐户**并使用公司的邮件信息**登录 Azure**。



3. 从菜单中选择 Azure Active Directory。



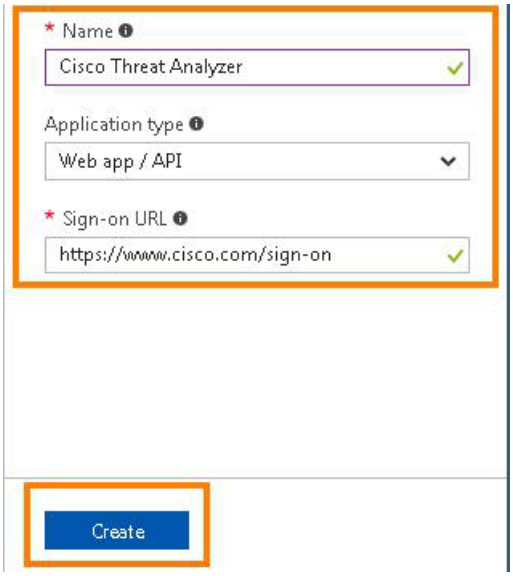
4. 从菜单中选择**应用注册**，然后点击**新应用注册**。



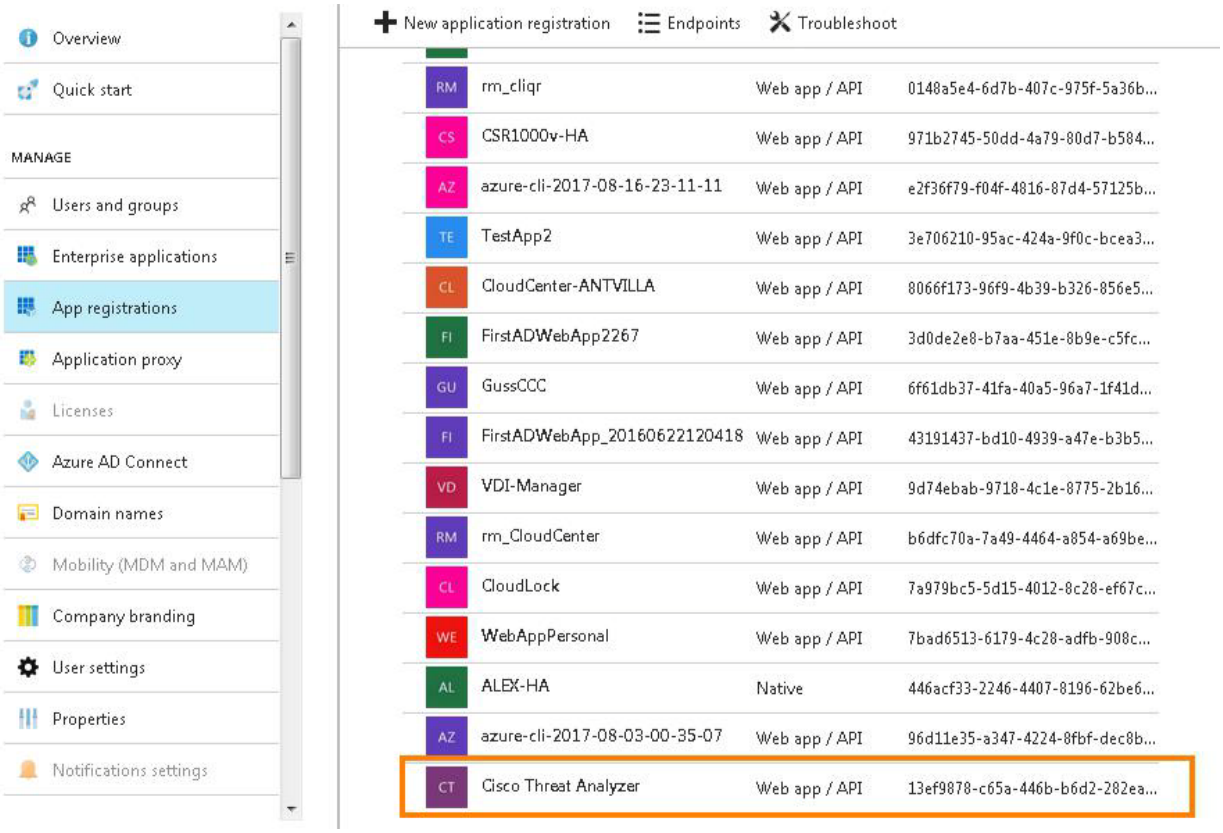
5. 为新应用输入以下信息：

   - **名称**：思科威胁分析器
   - **应用类型**：Web 应用/API
   - **登录 URL**：https:<yourcompanydomain/sign-on>，例如 https://www.cisco.com/sign-on

6. 点击**创建**。

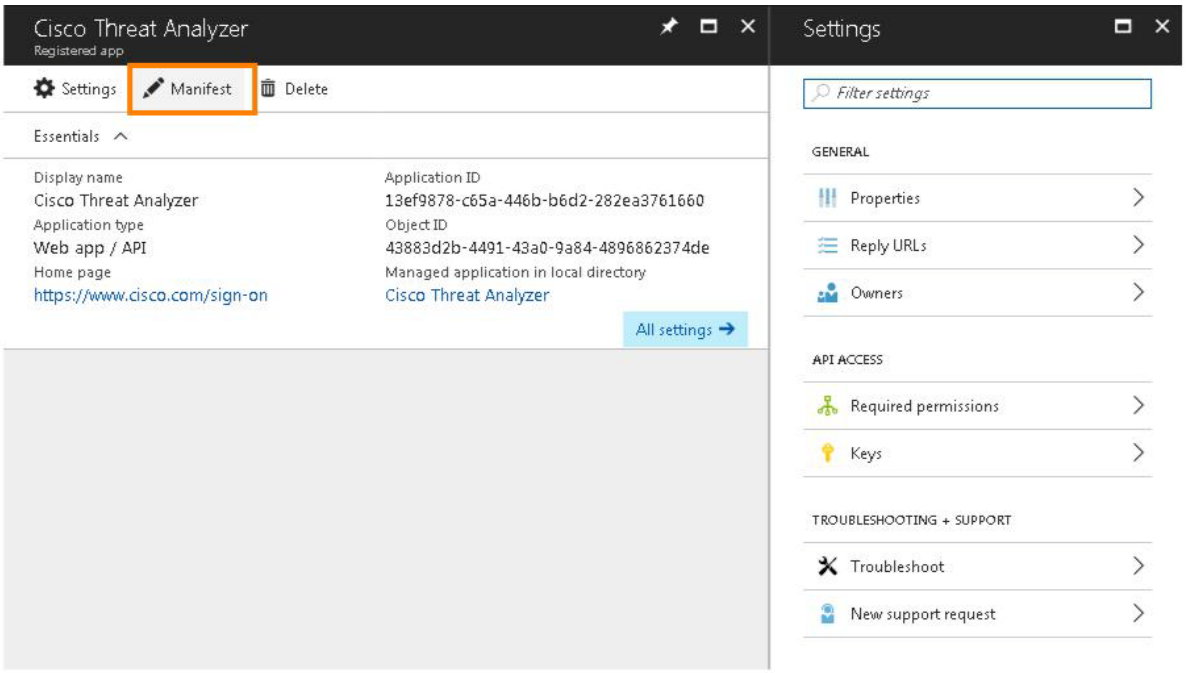


7. 系统会将该应用注册到列表中。



编辑清单

1. 从列表中选择已注册应用的名称，然后点击**清单**。



2. 将光标置于 keyCredentials 一节的**方括号之间**。

3. 粘贴以下文本字符串。（请参阅此处的说明。）

注意：如果是从笔记本电脑复制后粘贴到 WKST1 中，请使用文本编辑器（例如记事本）保存该 ID，直到需要使用时为止。如果是在 WKST1 中打开并配置 Azure 门户，请使用 <Ctrl>+<Alt>+<Shift> 复制并粘贴该 ID。

```
{
"customKeyIdentifier": "B2ybFYpimVk+etGYPZX9QvIAgw8=",
"keyId": "169acc09-1d17-4235-8eb1-22a387b494c4",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value":
"MIIDiTCCAnGgAwIBAgIBATANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExCzAJBgNVBAcTAkNBMQ4wDAY
DVQQKEwVDaXNjbzEMMAoGA1UECxMDRVNBMQwwCgYDVQQDEwNFU0ExIDAeBgkqhkiG9w0BCQEWEWVzYS10bWVAY2lzY28uY29tMB4XDTE
3MDcxODAwMDAwMFoXDTI3MDcxNzIzNTk1OVowdTELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMQswCQYDVQQHEwJDQTEOMAwGA1UEChM
FQ2lzY28xDDAKBgNVBAsTA0VTQTEMMAoGA1UEAxMDRVNBMSAwHgYJKoZIhvcNAQkBFhFlc2EtdG1lQGNpc2NvLmNvbTCCASIwDQYJKoZ
IhvcNAQEBBQADggEPADCCAQoCggEBAKEpwf9e/Fyh2tc4r+9+J59SXOKwWx9ODu7K5P7I2KTa2QwPyahp+ehvOGvbknAnwhnJ+d1mwy5
NsoQ9MQtcAmrZQXaeqJGmf2Nke/AwQXkth8uDrIWo9D5FCuU35W0+C4Hv2Gn1BBt38mvItReaye5Iqe8Nr2shI8k8kCYa3Gk5jWnp02L
llcRETo9/CwWAfhaE6T9XlARXevB6M9Y6Ua0zu2sM4MIdeR74+1D3ZIK57yElGubuymZ7AsrYWVrQ1iM5rJpemS/kNsSrULsZl4PX63/
eRw9lvY1HK9+yOYdI6J4aSaQl8jRh1hEHdzZowPq82dCsNptGEaCUsGZuYdcCAwEAAaMkMCIwCwYDVR0PBAQDAgWgMBMGA1UdJQQMMAo
GCCsGAQUFBwMEMA0GCSqGSIb3DQEBBQUAA4IBAQAK6H5v3mq+nglgqnQ3pX+K6PjMTYrDTKrkM+6slaV1jv9TRHfM5xrQjInkO+evQrC
nnn/Pg6AhkfYbivFsMZiN0yTUind9lNgIOx/ZJqcsnZrr3M8Y8xLa7zrM6sxV5fNzpun2Ly0fKHN90eNpTyixp31rgINLCmsm9w9UqV5
+VVkubt0c9fS2BQOSsJzR613kfvCPjI4h7ppYypcERnNgXxlJrJGcu4F6Hzsf2QJVhlYgKN8+VoBhtlmlX7EqaoTloH53f7/b4lB2pG9
DT7raE9IkGJ3Hw2AtoQQwLIjYivYKwd6JO3+pO3w2KzDpJ7GQPNW6UzN4waITfDMevcRz"
}
```

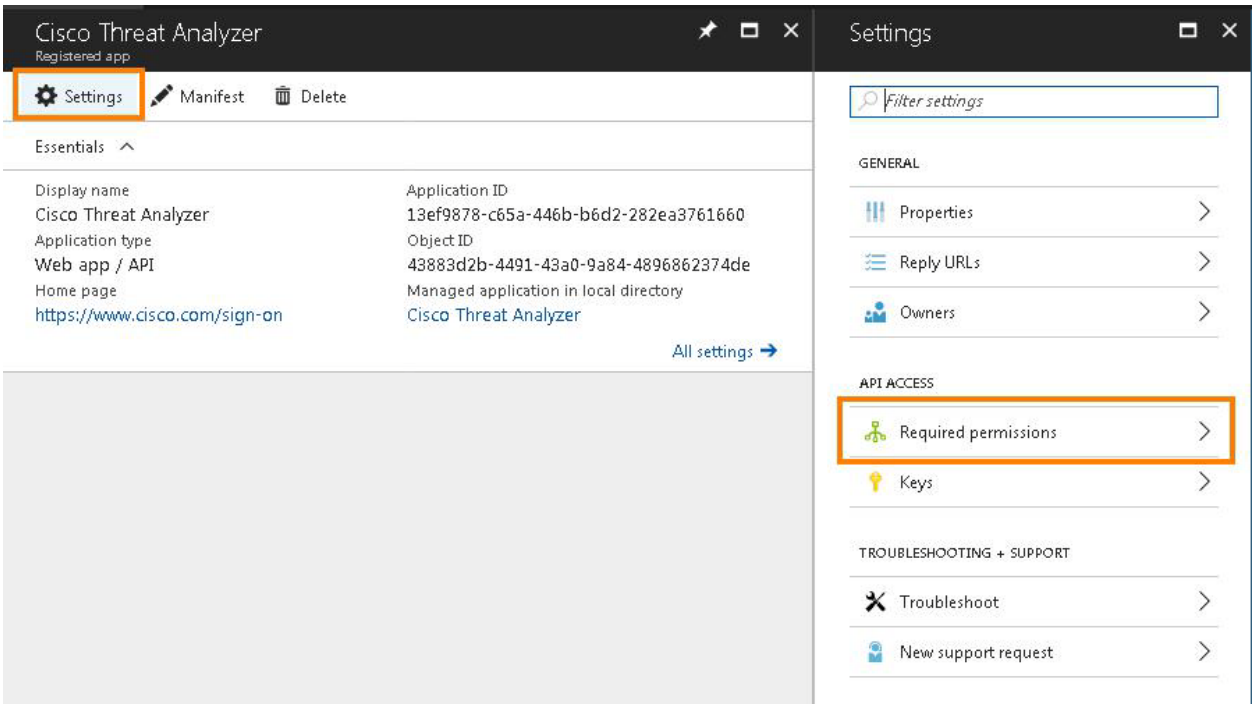
注意：以 MIIDiTCC 开头且以 DMevcRz 结尾的值字符串必须在一行上。建议使用记事本文本编辑器来编辑字符串。

```
  "homepage": "https://www.cisco.com/sign-on",
  "identifierUris": [
    "https://ciscoit.onmicrosoft.com/d4f0a16a-7a64-4947-b479-731802d5538d"
  ],
  "keyCredentials": [{
"customKeyIdentifier": "B2ybFYpimVk+etGYPZX9QvIAgw8=",
"keyId": "169acc09-1d17-4235-8eb1-22a387b494c4",
"type": "AsymmetricX509Cert",
"usage": "Verify",
"value":
"MIIDiTCCAnGgAwIBAgIBATANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExCzAJBgNVBAcTA
OMAwGA1UEChMFQ2lzY28xDDAKBgNVBAsTA0VTQTEMMAoGA1UEAxMDRVNBMSAwHgYJKoZIhvcNAQkBFhFlc2EtdG1lQGNpc
+C4Hv2Gn1BBt38mvItReaye5Iqe8Nr2shI8k8kCYa3Gk5jWnp02LllcRETo9/CwWAfhaE6T9XlARXevB6M9Y6Ua0zu2sM4
+yOYdI6J4aSaQl8jRh1hEHdzZowPq82dCsNptGEaCUsGZuYdcCAwEAAaMkMCIwCwYDVR0PBAQDAgWgMBMGA1UdJQQMMAoG
+evQrCnnn/Pg6AhkfYbivFsMZiN0yTUind9lNgIOx/ZJqcsnZrr3M8Y8xLa7zrM6sxV5fNzpun2Ly0fKHN90eNpTyixp31
}
],
  "knownClientApplications": [],
```

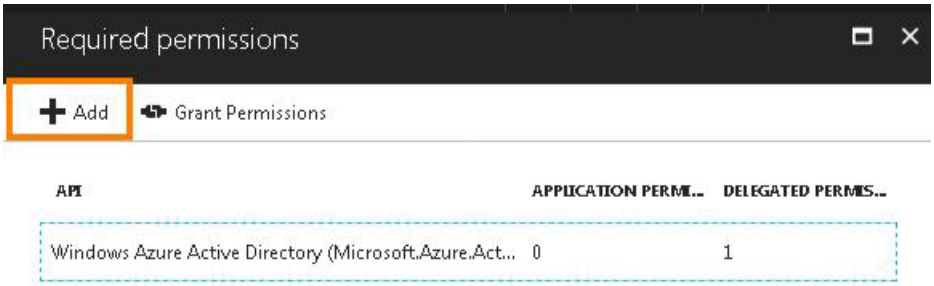

4. 点击**保存**。该应用已成功更新。

配置权限

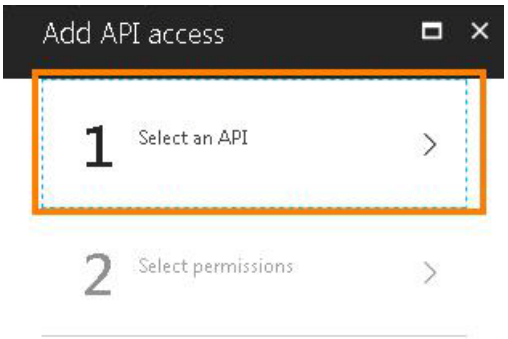
1. 在应用页面上，依次选择**设置 > 所需权限**。



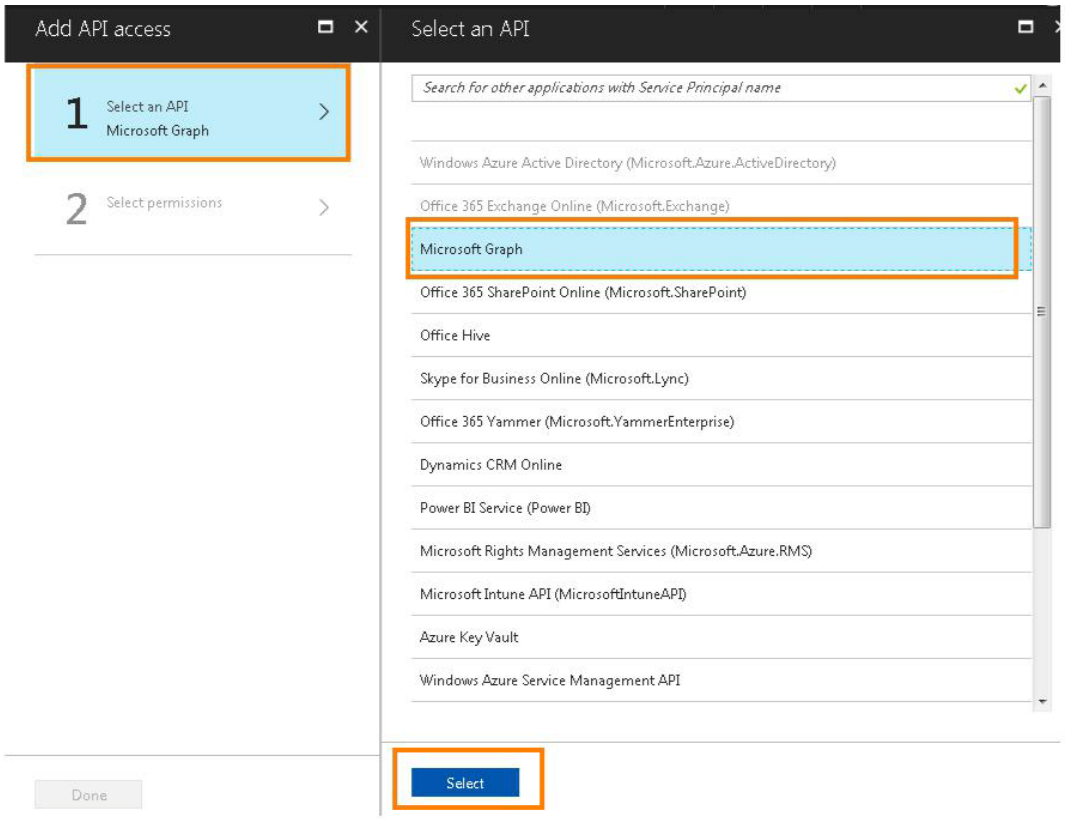
2. 点击**添加**。



3. 点击 **1 选择 API**。



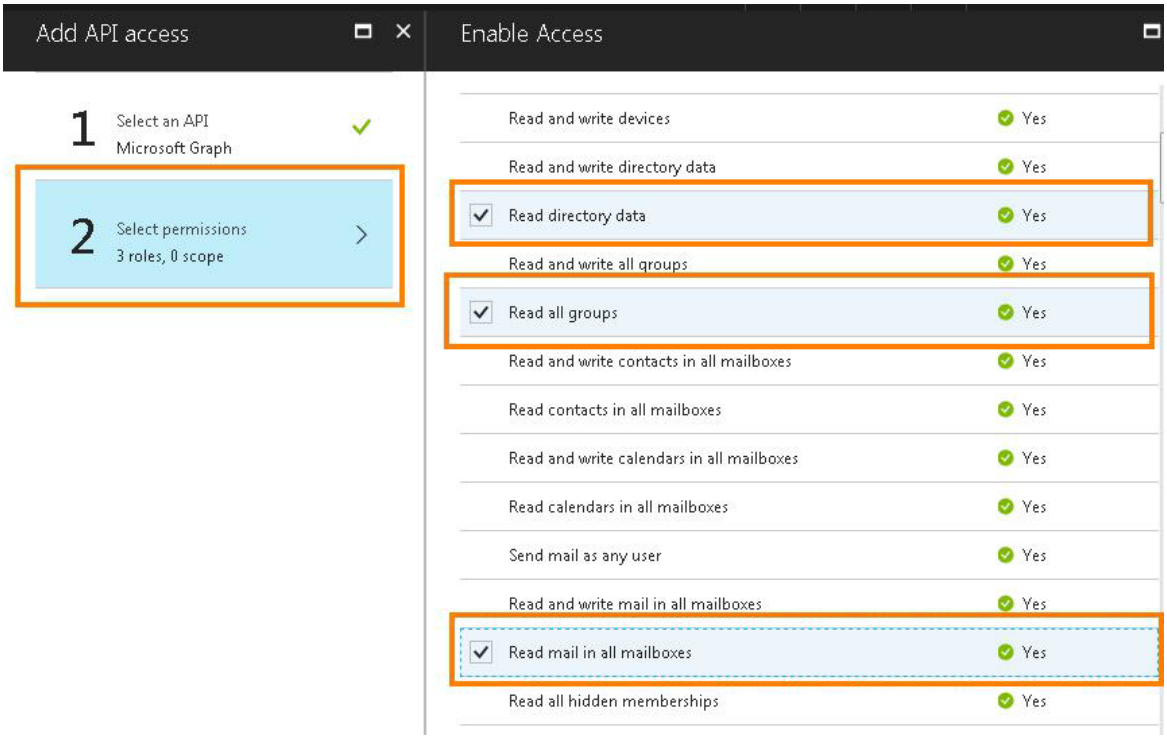
4. 选择 **Microsoft Graph**，然后点击**选择**。



5. 系统将突出显示 **2 选择权限**。从列表中选择以下选项：

应用权限

- 读取目录数据
- 读取所有组
- 读取所有邮箱中的邮件



6. 向下滚动列表并选择以下选项：

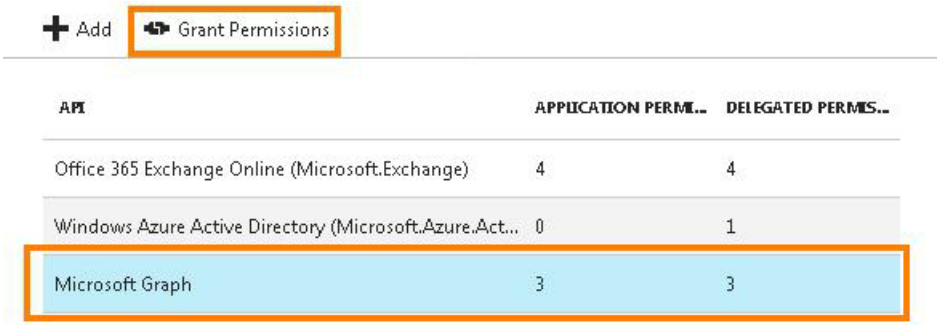
代理权限

- 阅读用户邮件
- 读取目录数据
- 读取所有组

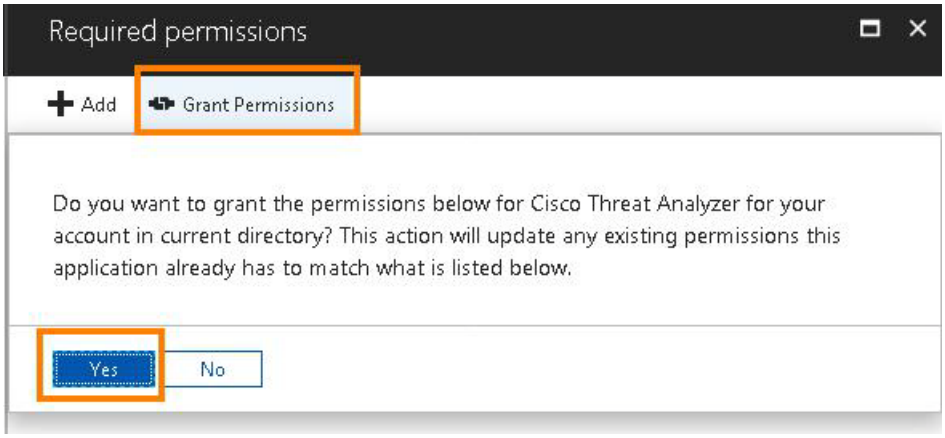
7. 点击**选择**，然后点击**完成**。

授予权限

1. 从 API 列表中选择 **Microsoft Graph**。
2. 选择**授予权限**。



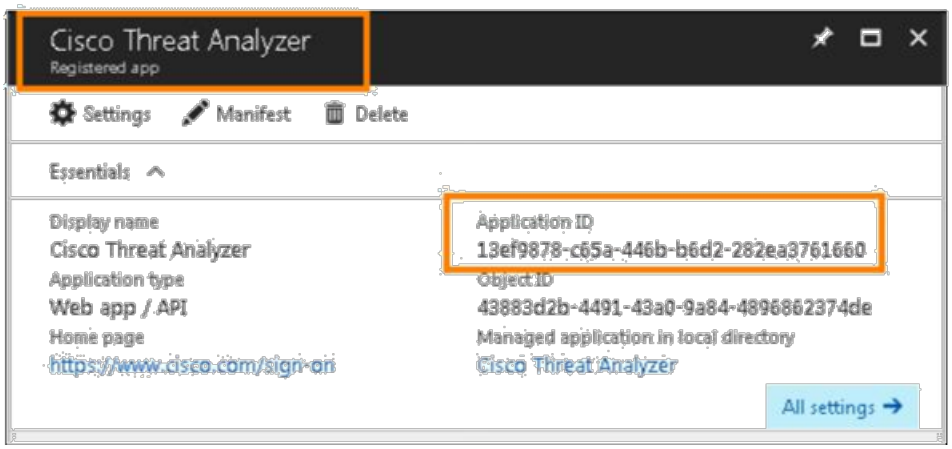
3. 点击**是**继续完成授予权限请求。



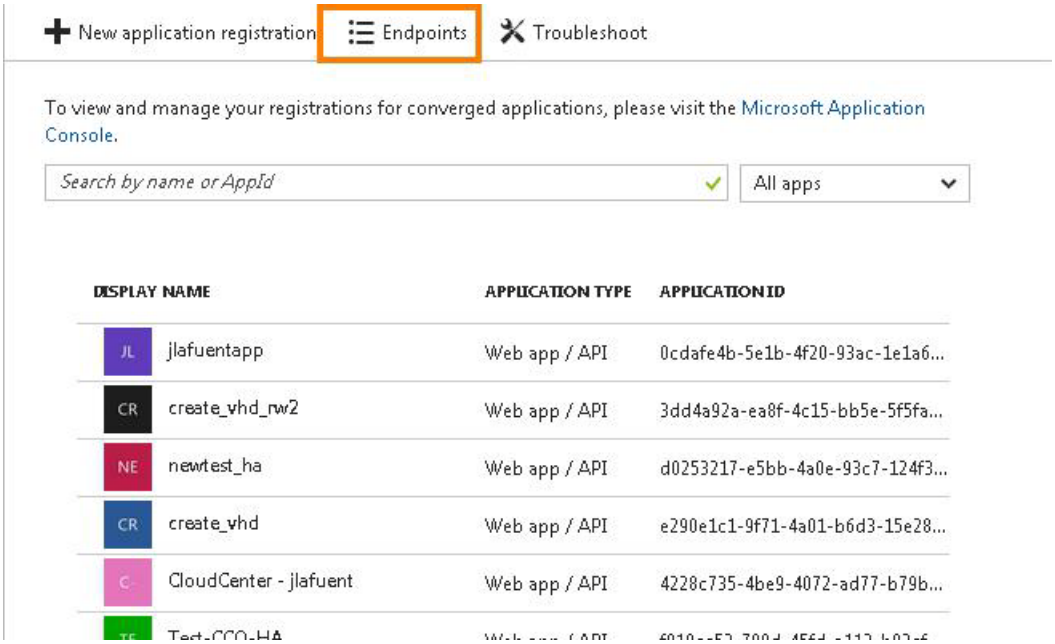
查找应用（客户端）ID 和租户 ID

1. 返回思科威胁分析器的已注册应用屏幕，并复制**应用 ID**。

注意：如果是从笔记本电脑复制后粘贴到 WKST1 中，请使用文本编辑器（例如记事本）保存该 ID，直到需要使用时为止。如果是在 WKST1 中打开并配置 Azure 门户，请使用 <Ctrl>+<Alt>+<Shift> 复制并粘贴该 ID。

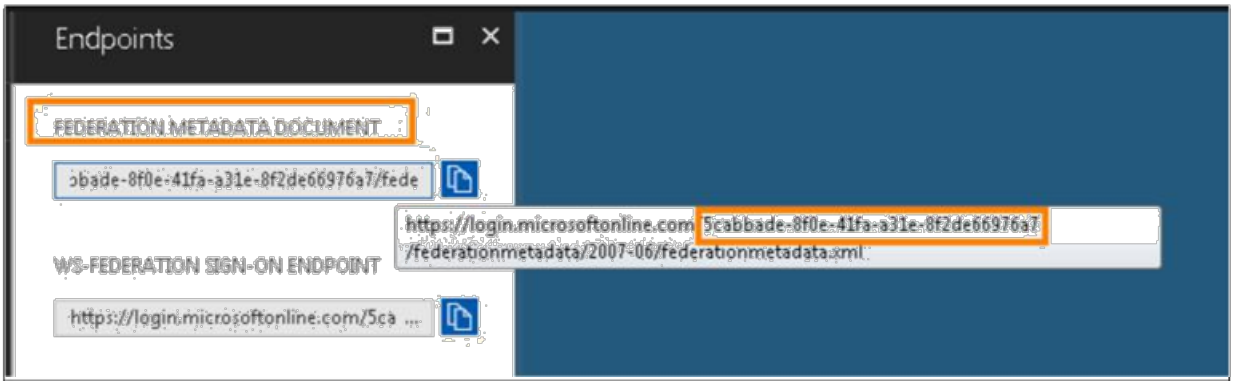


2. 点击打开的窗口右上角的 **X** 返回到“应用注册”页面。
3. 点击**终端**。



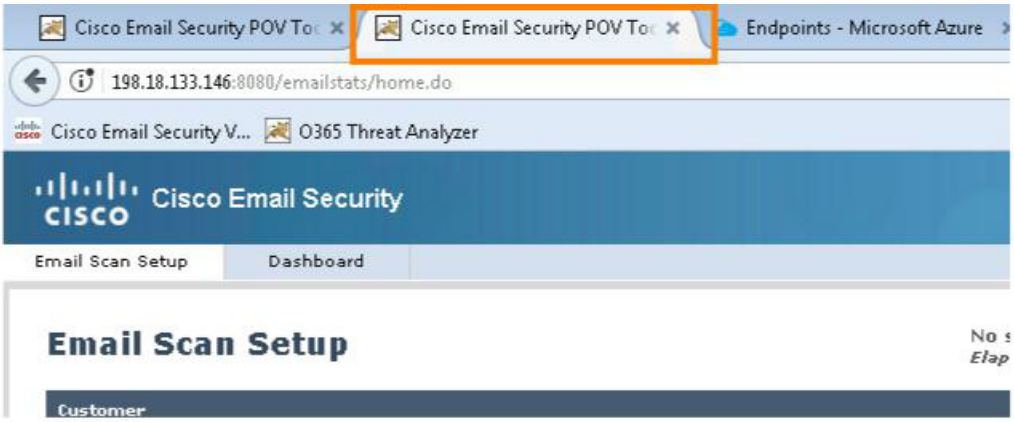
4. 从“联合身份验证元数据文档”中，复制 URL 字符串内的**租户 ID**。

注意：如果是从笔记本电脑复制后粘贴到 WKST1 中，请使用文本编辑器（例如记事本）保存该 ID，直到需要使用时为止。如果是在 WKST1 中打开并配置 Azure 门户，请使用 <Ctrl>+<Alt>+<Shift> 复制并粘贴该 ID。



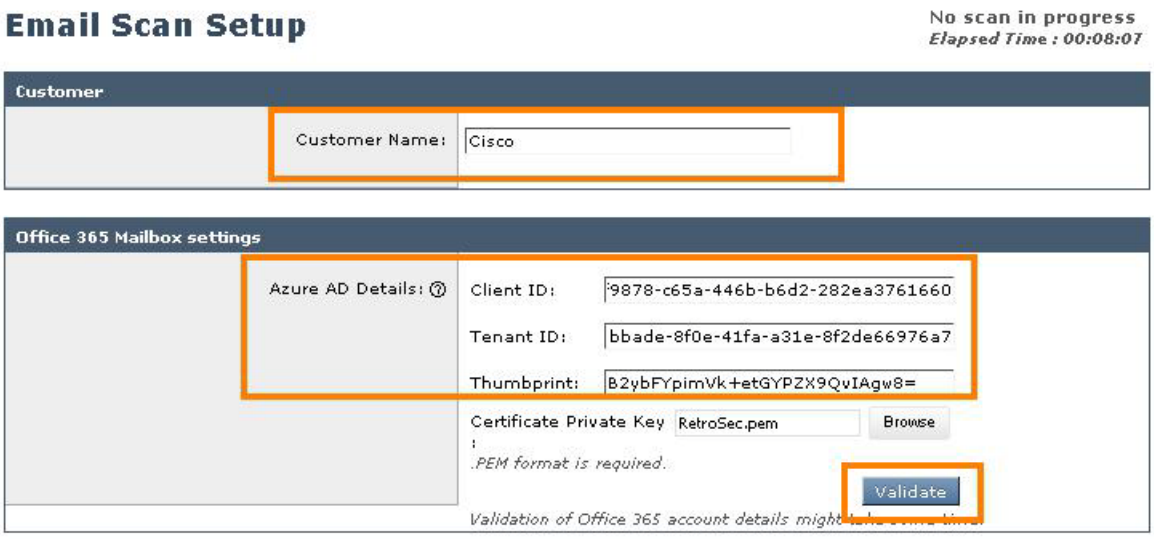
启动威胁分析器

1. 选择标题为**思科邮件安全 POV 工具** (http://198.18.133.146:8080/emailstats) 的已打开选项卡。



注意：如果 POV 工具用户界面 (UI) 无法显示，请在 ESA 的命令行界面 (CLI) 中使用 PuTTy 执行命令“**startofflinescan 198.18.133.146**”以重新启动分析器服务。

2. 如果尚未选择，请点击**邮件扫描设置**选项卡。
3. 输入以下信息：
   - **客户名称**：您的公司名称，例如思科
   - 前面的步骤中的**客户端 ID**
   - 前面的步骤中的**租户 ID**
   - **指纹**：B2ybFYpimVk+etGYPZX9QvIAgw8=（请参阅此处的说明。）



4. 点击“证书私钥”对应的**浏览**。

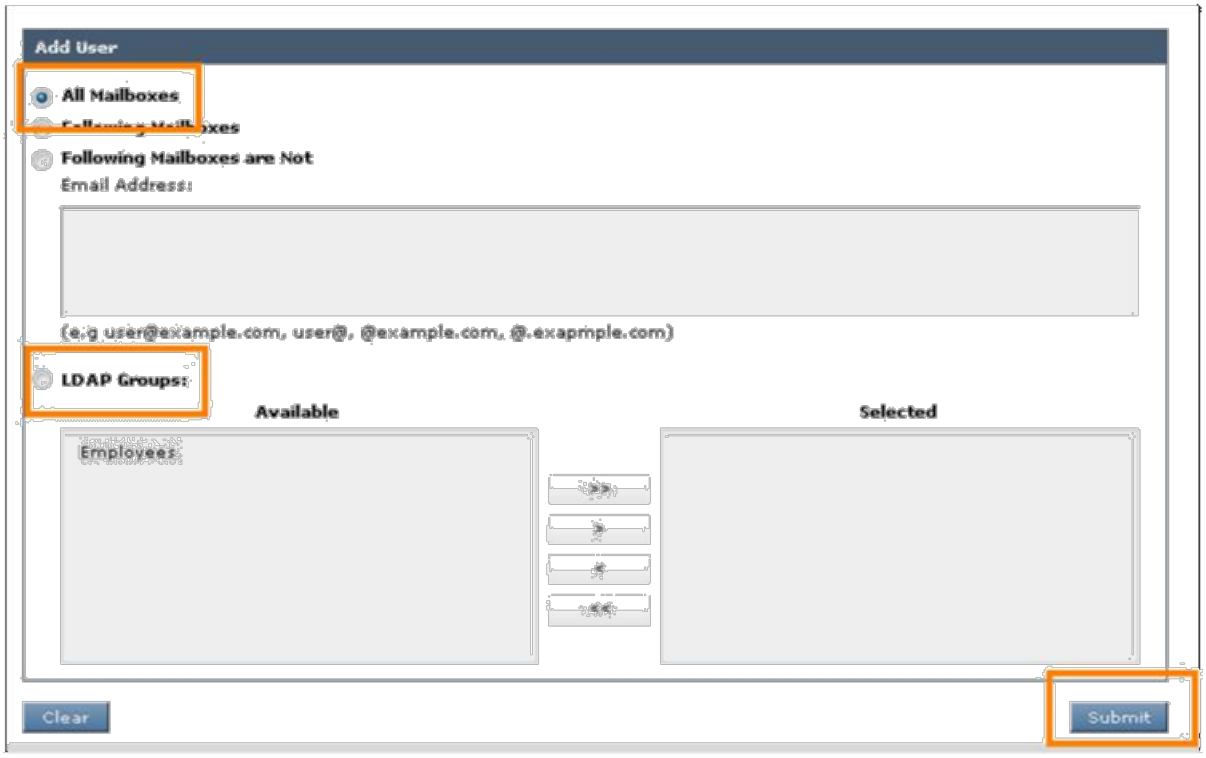
5. 在“文件上传”窗口中，选择 **C:\pov** 目录下的私钥 **demo.pem**。（请参阅此处的说明。）

注意：为简化扫描任务，自签证书和私钥已预先定义。如果客户对于使用此证书和私钥有顾虑，可以打开 Office 365 威胁分析器工具文档创建一组他们自己的证书和私钥，然后配置 Azure 注册应用。

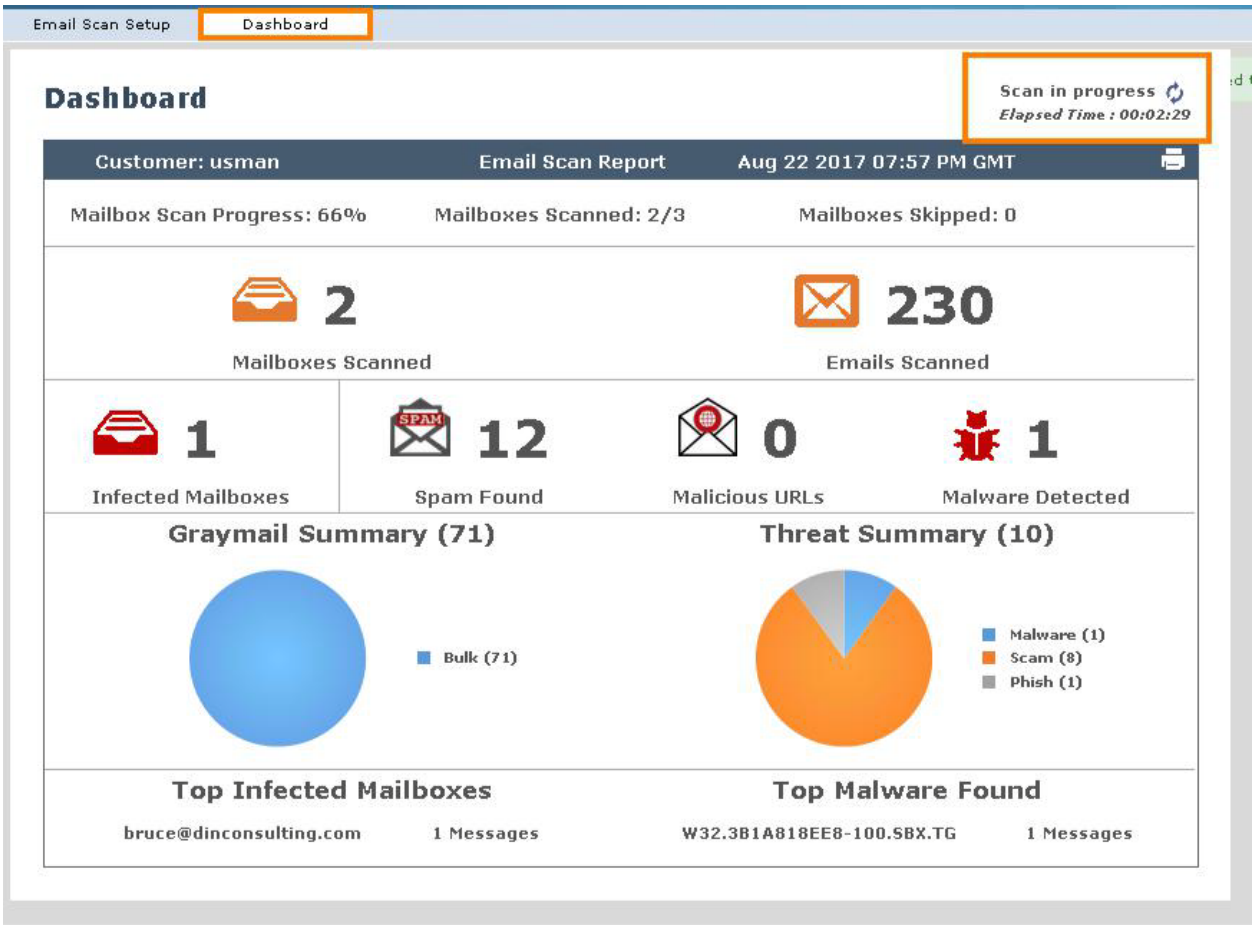
6. 点击**验证**。系统将显示一条消息，指出已成功验证 Office 365 凭证。

7. 关闭 **X** 提示消息。
8. 确保已选择**所有邮箱**。或者，选择**特定邮箱或 LDAP 组**缩小范围并缩短扫描时间。
9. 点击右下角的**提交**扫描所有邮箱。

注意：在进行邮箱提取和扫描操作之前，可能需要管理批准。



10. 点击**控制面板选项卡**查看报表填充扫描进度的统计信息。



11. 完成后，点击“打印”按钮**将报告保存为 PDF**。

12. 返回到**邮件扫描设置**页面

13. 点击**清除**删除 Office 365 邮箱设置。

注意：除控制面板报告的计数器数据外，威胁分析器中不会存储任何邮件内容。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。