如何为Microsoft Azure(Microsoft 365)API配置思科安全电子邮件帐户设置

目录

简介

本文档提供在Microsoft Azure(Azure Active Directory)中注册新应用以生成所需的客户端ID、租户ID和客户端凭证的分步“操作”，然后在思科安全电子邮件网关或云网关上配置帐户设置。当邮件管理员配置邮箱自动修复(MAR)以进行高级恶意软件防护(AMP)或URL过滤，或在思科安全邮件和Web管理器或思科安全网关/云网关上使用邮件跟踪中的补救操作时，需要配置帐户设置和关联的帐户配置文件。

邮箱自动补救流程

您的电子邮件或URL中的附件（文件）随时可能被评为恶意，即使它已到达用户的邮箱。思科安全电邮上的AMP（通过思科安全恶意软件分析）可在新信息出现时识别此发展，并将追溯性警报推送至思科安全电邮。Cisco Talos提供URL分析，与AsyncOS 14.2 for Cisco Secure E-mail Cloud Gateway相同。 如果您的组织使用Microsoft 365管理邮箱，则可以配置思科安全邮件，以在这些威胁判定发生更改时对用户邮箱中的邮件执行自动补救操作。

思科安全电子邮件可安全直接与Microsoft Azure Active Directory通信，以访问Microsoft 365邮箱。例如，如果包含附件的电子邮件通过您的网关进行处理并由AMP扫描，则文件附件(SHA256)将提供给AMP以获得文件信誉。 AMP处置情况可标记为Clean（第5步，图1），然后传送到最终收件人的Microsoft 365邮箱。 稍后，AMP处置被更改为恶意，思科恶意软件分析将追溯性判定更新（第8步，图1）发送到已处理该特定SHA256的任何网关。 网关收到恶意的追溯性判定更新（如果已配置）后，网关将执行以下邮箱自动补救(MAR)操作之一：转发、删除或转发和删除。

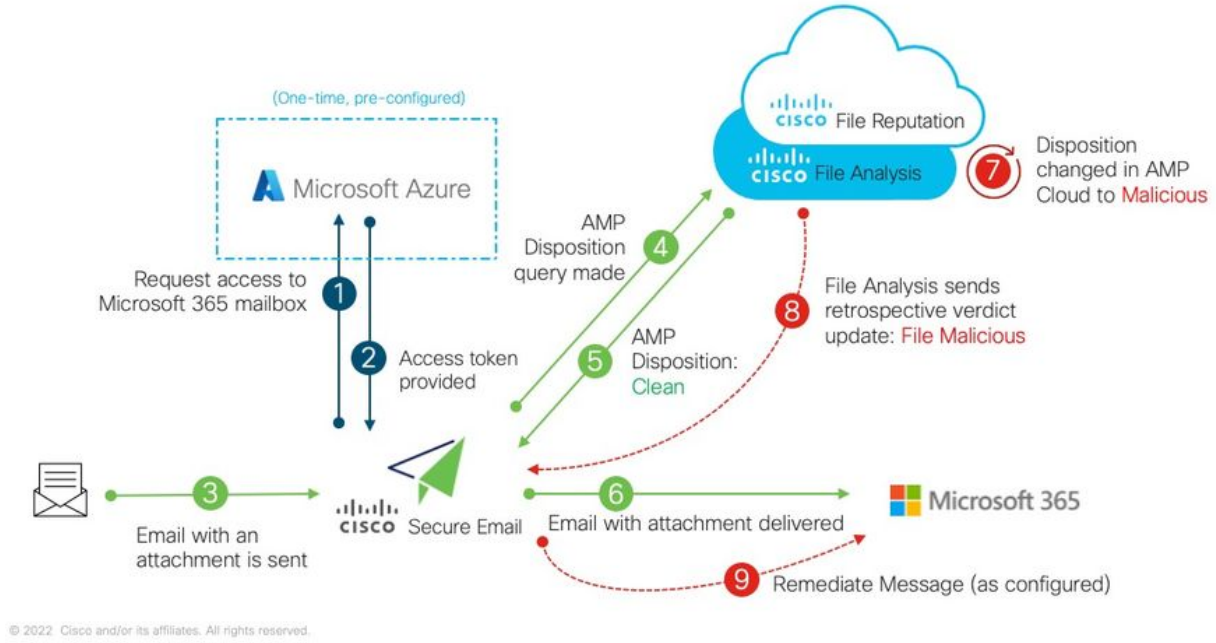


图 1：思科安全电邮上的MAR（用于AMP）

本指南介绍如何使用Microsoft 365配置思科安全电邮，仅用于邮箱自动补救。 网关上的AMP（文件信誉和文件分析）和/或URL过滤应已配置。 有关文件信誉和文件分析的更多详细信息，请参阅《用户指南》，了解您部署的AsyncOS版本。

先决条件

1. Microsoft 365帐户订用（请确保您的Microsoft 365帐户订用包括对Exchange的访问，如企业E3或企业E5帐户。）

2. Microsoft Azure管理员帐户和http://portal.azure.com访问

3. Microsoft 365和Microsoft Azure AD帐户均正确绑定到活动的“user@domain.com”电子邮件地址，并且您可以通过该电子邮件地址发送和接收电子邮件。

您将创建以下值以配置与Microsoft Azure AD的思科安全邮件网关API通信：

- **客户端ID**
- **租户ID**

- **客户端密钥**

  注意： 从AsyncOS 14.0开始，“帐户设**置”允**许在创建Microsoft Azure App注册时使用客户端密钥进行配置。这是更简单、首选的方法。

可选 — 如果您未使用客户端密钥，则需要创建并准备好：

- **指纹**
- **私钥（PEM文件）**

本指南的附录中介绍了如何创建指纹和私钥：

1. 活动公共（或专用）证书(CER)和用于签署证书(PEM)的私钥，或创建公共证书(CER)的能力，以及保存用于签署证书(PEM)的私钥的能力。思科在本文档中提供了两种方法，以根据您的管理首选项完成此操作： 证书:Unix/Linux/OS X（使用OpenSSL）证书:Windows（使用PowerShell）

2. 对Windows PowerShell的访问，通常从Windows主机或服务器进行管理 — 或通过Unix/Linux访问终端应用程序

要构建这些所需值，您需要完成本文档中提供的步骤。

注册Azure应用以与思科安全电子邮件配合使用

申请注册

登录到你的Microsoft Azure门户
1.单击**Azure Active Directory**（图2）
2.单击“应用**程序注册”**
3.单击+新**注册**
4.在“注册申请”页：
a.名称：**Cisco Secure Email MAR**（或您选择的名称）
b.支持的帐户类型：**仅此组织目录中的帐户（帐户名称）**
c.重定向URI:（可选）
[注意：您可以留空，也可以随意使用 https://www.cisco.com/sign-on进行填充]
d.在页面底部，单击“Register（注册）”

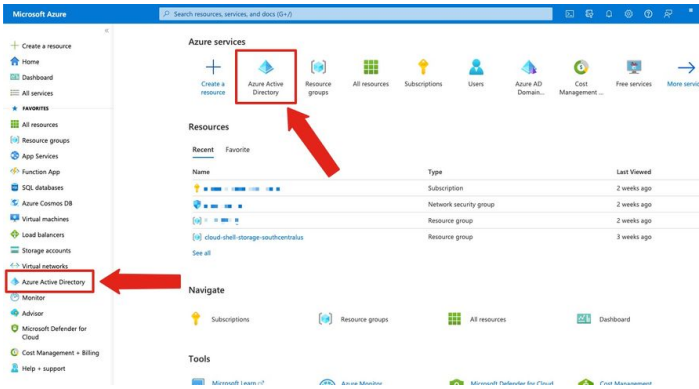


图 2：Microsoft Azure门户示例

完成上述步骤后，您将看到您的应用：

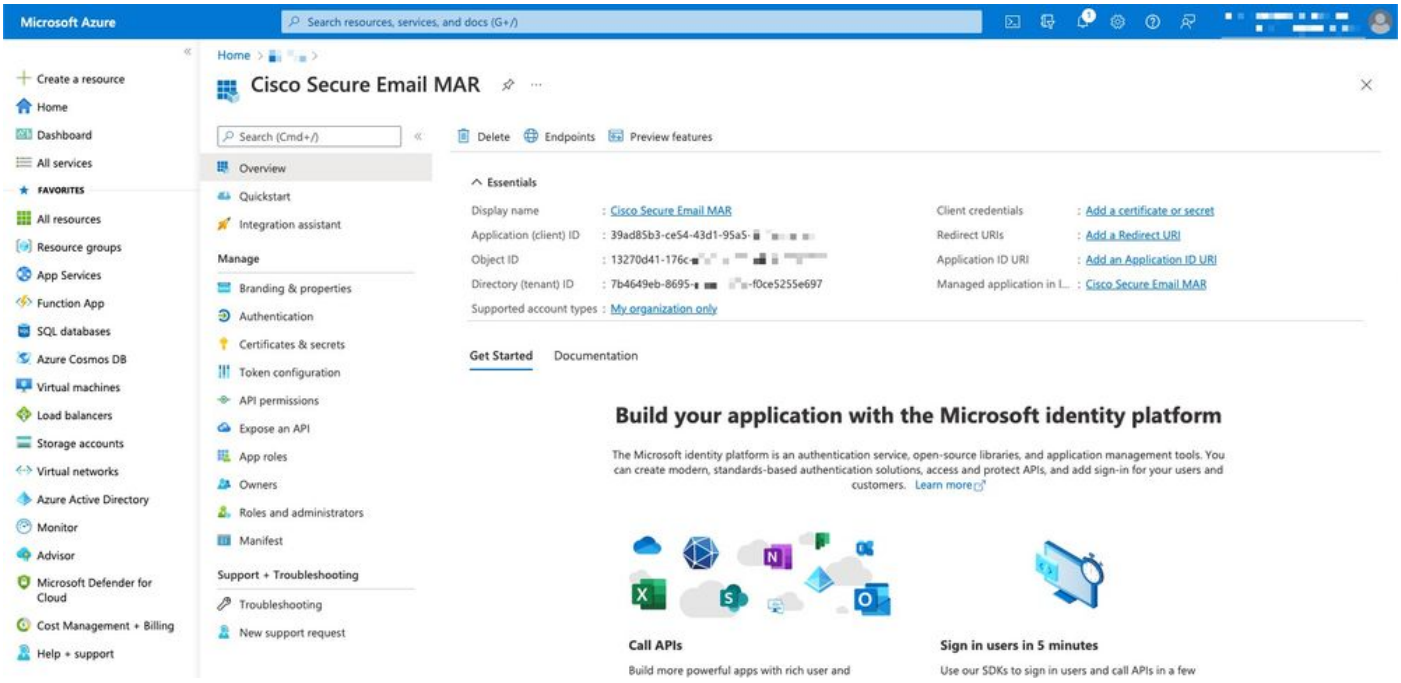


图 3：Microsoft Azure Active Directory应用程序页

证书和机密

如果您运行的是AsyncOS 14.0或更高版本，思科建议配置Azure应用以使用客户端密钥。 在应用程序窗格的管理选项中：

1.选择“证**书和机密”**

2.在“客户机***密钥”***部分，单击**+“新客户机密钥”**

3.添加说明以帮助确定此客户机密钥的用途，例如“思科安全电邮补救”

4.选择到期期

5.单击“添**加”**

6.将鼠标悬停在所生成值的右侧，然后单击“复制到剪贴**板”图**标

7.将此值保存到您的备注中，请注意“客户机密码”

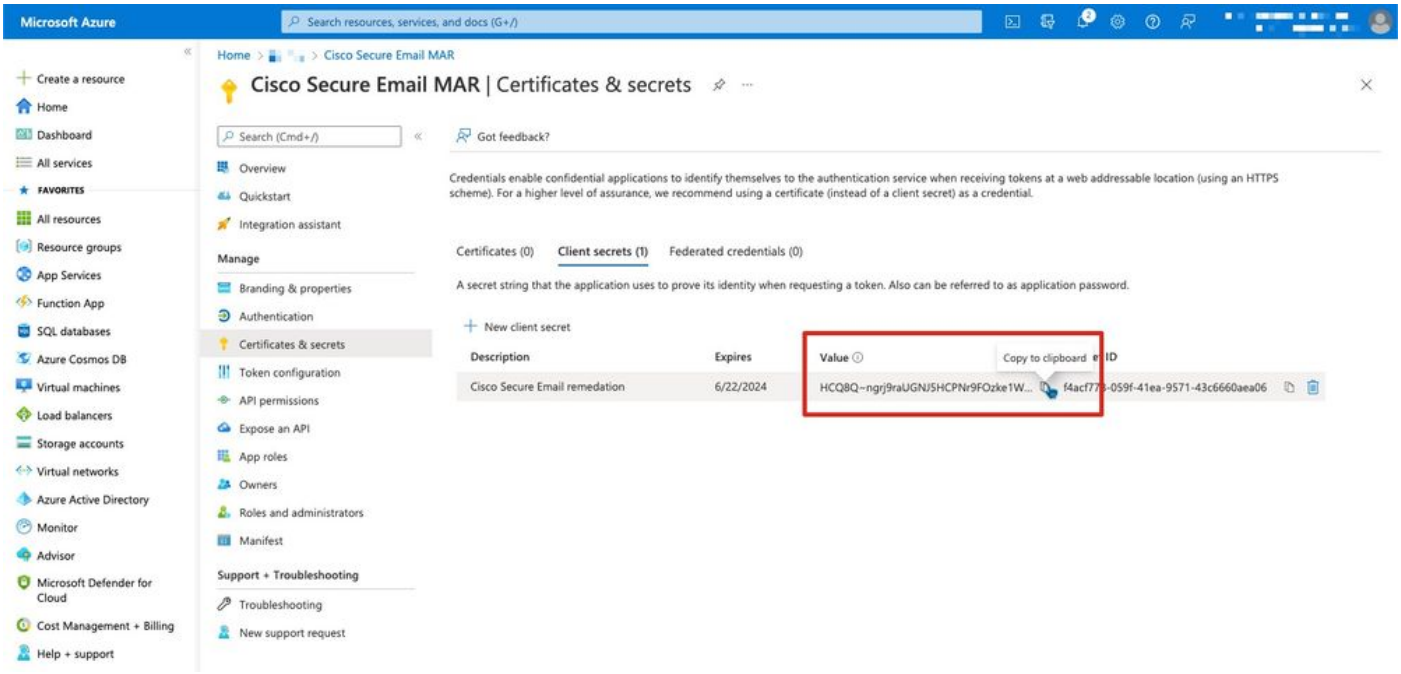


图 4：Microsoft Azure创建客户端密钥示例

注意：退出活动的Microsoft Azure会话后，您刚生成的客户端密钥的值将***超出该值。 如果在退出之前未记录并保护该值，则需要重新创建客户端密钥以查看明文输出。

可选 — 如果您没有使用客户端密钥配置Azure应用，请将Azure应用配置为使用您的证书。 在应用程序窗格的管理选项中：

1. 选择证**书和机密**
2. 单击上**传证书**
3. 选择CRT文件（如之前创建的）
4. 单击“添**加”**

API权限

注意：从AsyncOS 13.0 for Email Security开始，需要将Microsoft Azure到Cisco Secure Email通信的API权限从使用Microsoft Exchange更改为Microsoft Graph。如果已配置MAR，并且您正在将现有Cisco Secure Email网关升级到AsyncOS 13.0，则只需更新/添加新API权限。 （如果您运行的是AsyncOS的旧版本11.x或12.x，请参阅附录B，然后继续。）

在应用程序窗格的管理选项中：

1. 选择**API权限**
2. 单击**+添加权限**
3. 选择**Microsoft Graph**
4. 选择以下应用程序权***限权限***: Mail > "Mail.Read"（在所有邮箱中读取邮件）Mail > "Mail.ReadWrite"（在所有邮箱中读写邮件）Mail > "Mail.Send"（以任何用户身份发送邮件）目录>“目录。读取。所有”（读取目录数据）[*可选：如果使用LDAP连接器/LDAP同步，请

启用。 如果不是，则不需要。]

5. *可选：*您将看到Microsoft Graph默认为“User.Read”权限启用；您可以保留此配置，或者单击“**读取”**并单击“**删除权限”**，以从与应用程序关联的API权限中删除此权限。
6. 单击**添加权**限(或**更新权**限，如果Microsoft Graph已列出)
7. 最后，单击“Grant admin consent for...(授**予管理员同意……)”** 确保将新权限应用到应用程序
8. 会出现一个窗格内弹出窗口，询问：

"*是否要授予<Azure Name>中所有帐户的请求权限的同意？这将更新此应用程序已经必须与下面列出的内容匹配的任何现有管理员同意记录。”*

单击**是**

此时，您应看到绿色的成功消息，并且“Admin Consent Required”（需要管理员同意）列显示Granted（已授权）。

获取您的客户端ID和租户ID

在应用程序窗格的管理选项中：

1. 单击Overview
2. 将鼠标悬停在应用（客户端）ID的右侧，然后单击“复制到剪**贴板”图**标
3. 将此值保存到您的备注中，请注意“客户端ID”
4. 将鼠标悬停在目录（租户）ID的右侧，然后单击“复制到剪**贴板”图**标
5. 将此值保存到您的备注中，请注意“租户ID”

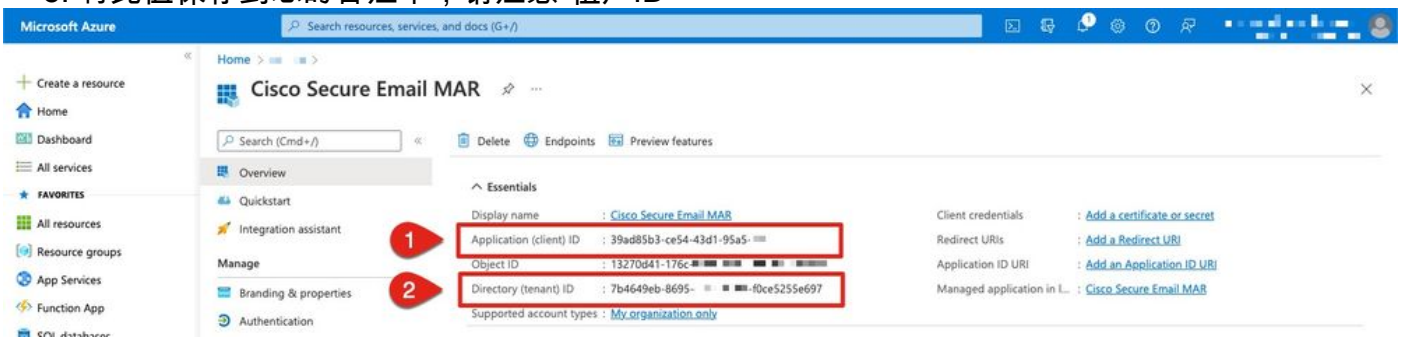


图 5：Microsoft Azure...客户端ID，租户ID示例

配置思科安全电邮网关/云网关

此时，您应准备好以下值并将其保存到您的备注中：

- **客户端ID**
- **租户ID**
- **客户端密钥**

可选，如果不使用客户端密钥：

- **指纹**
- **私钥（PEM文件）**

您已准备好使用注释中创建的值并在思科安全电邮网关上配置帐户设置！

创建帐户配置文件

1. 登录您的网关
2. 导航至“系**统管理”>“帐户设置”** 注意：如果运行的版本早于AsyncOS 13.x，则这将是“系统管理”**>“邮箱设置”**
3. 单击“**启用”**
4. 单击启用帐户设置复选框，然后单击提**交**
5. 单击创**建帐户配置文件**
6. 提供配置文件名称和说明（如果您有多个域，将唯一描述您的帐户）
7. 在定义Microsoft 365连接时，请将配置文件类型保**留为Office 365 /混合（图形API）**
8. 输入您的**客户端ID**
9. 输入您的**租户ID**
10. 对于客户端凭据，请执行以下操作之一，如您在Azure中配置的： 单击**Client Secret**并粘贴到已配置的客户端密钥中，或……单击**Client Certificate**并输入您的指纹，并通过单击“Choose File”提供PEM
11. 单击 **Submit**
12. 单击UI右上角的**Commit Changes**
13. 输入任何注释，并通过点击提交更改完成**配置更改**

检查连接

下一步只是验证从您的思科安全电子邮件网关到Microsoft Azure的API连接：

1. 在同一“帐户详细信息”页中，单击“测试**连接”**
2. 输入在Microsoft 365帐户中管理的域的有效电子邮件地址
3. 单击“**测试连接”**
4. 您应收到成功消息（图6）
5. 单击“**完成**”完成

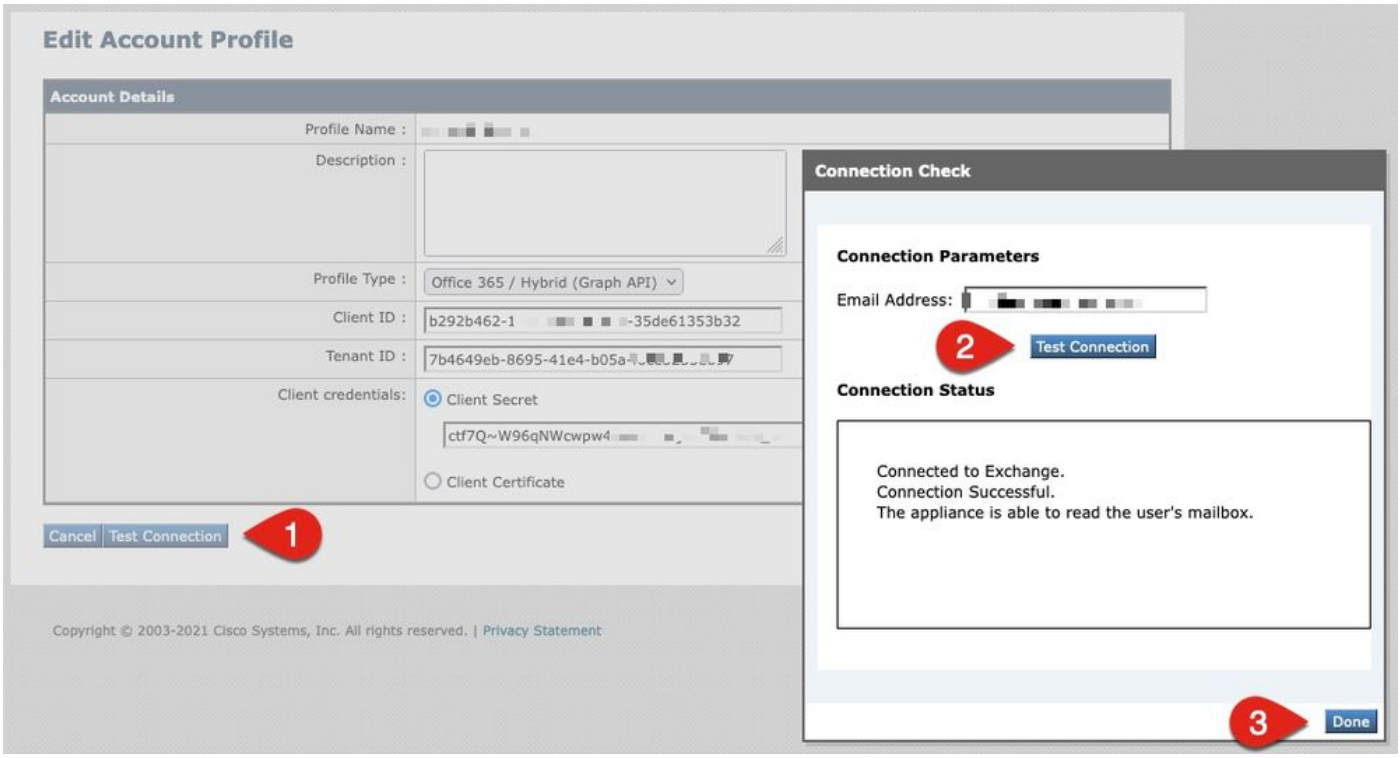


图 6：帐户配置文件/连接检查示例

6.在“域映*射”部分*，单击**创建域映射**

7.输入与您刚验证API连接的Microsoft 365帐户关联的域名

以下是可用于映射邮箱配置文件的有效域格式列表：

— 域可以是特殊关键字“ALL”，以匹配所有域以创建默认域映射。

— 域名，如“example.com” — 将任何地址与此域匹配。

— 部分域名（如“@.partial.example.com”）— 匹配以此域结尾的任何地址

— 可以使用逗号分隔的域列表输入多个域。

8.单击“提**交”**

9.单击**UI**右上角的“提交更改”

10.输入任何注释，并通过单击“提交更改”完**成配置更改**

在邮件策略中为高级恶意软件防护启用邮箱自动补救(MAR)

完成此步骤，在邮件策略的AMP配置中启用MAR。

1. 导航至“邮**件策略”>“传入邮件策略”**
2. 点击“高级恶意软件防护”(Advanced Malware Protection)列中要配置的策略名称的设置（例如，图7）：

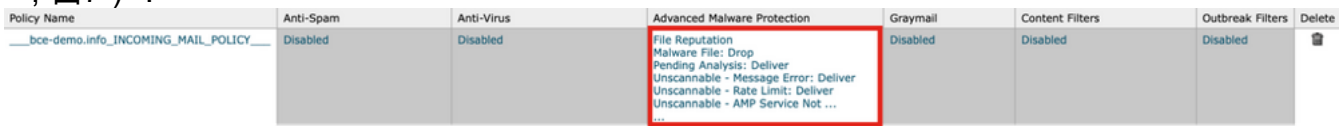


图 7：启用MAR（传入邮件策略）

3. 滚动到页面底部
4. 点击启用邮箱自动补救(MAR)复选框
5. 选择您希望对MAR采取的以下操作之一（例如，图8）： 前转到:<*输入电子邮件地址*>DELETE前转到:<*输入电子邮件地址*>并删除

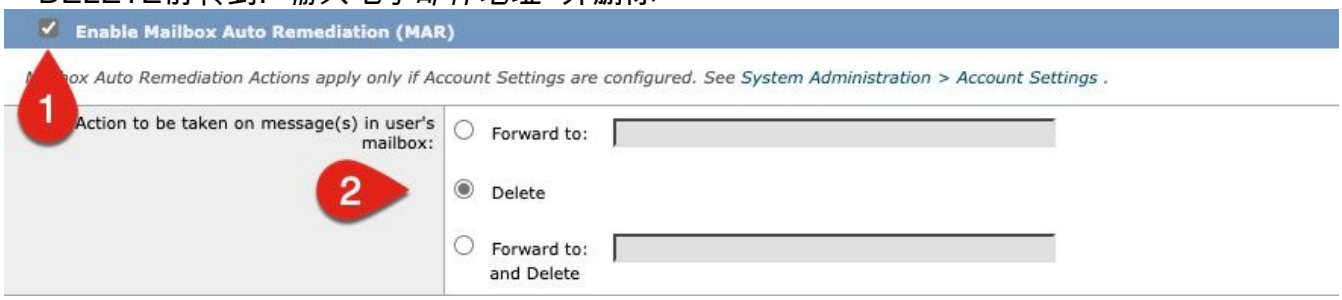


图 8：为AMP启用MAR配置示例

6. 单击 **Submit**
7. 单击UI右上角的**Commit Changes**
8. 输入任何注释，并通过点击提交更改完成**配置更改**

为URL过滤启用邮箱自动补救(MAR)

从AsyncOS 14.2 for Cisco Secure Email Cloud Gateway开始，URL过滤现在包括URL追溯性判定和URL补救。

1. 导航至安**全服务> URL过滤**
2. 如果尚未配置URL过滤，请单击启**用**
3. 点击“启用URL类别和信誉过滤器”复选框
4. 使用*默认设置*的高级设置
5. 单击 Submit

您的URL过滤应类似于以下内容：

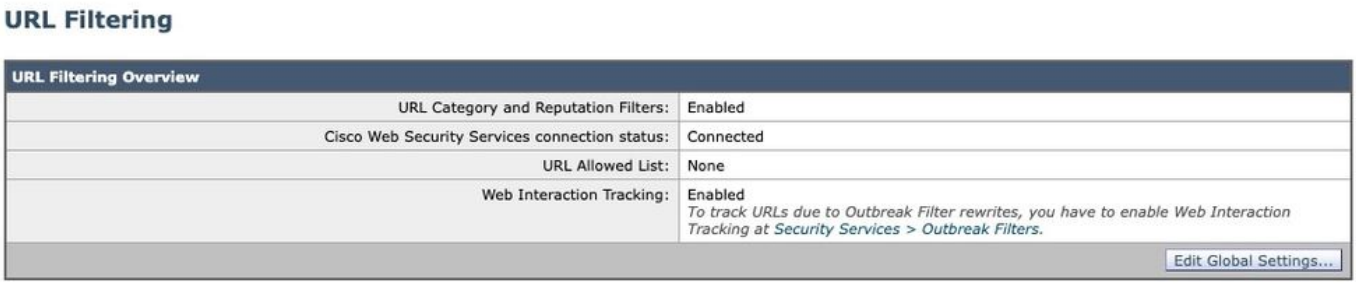


图 9：URL过滤后启用示例

要查看URL追溯和内置URL过滤，请执行以下操作，或为思科打开支持案例以执行：

```
esa1.hcxxyy-zz.iphmx.com> urlretroservice enable

URL Retro Service is enabled.

esa1.hcxxyy-zz.iphmx.com> websecurityconfig

URL Filtering is enabled.
No URL list used.
Web Interaction Tracking is enabled.
URL Retrospective service based Mail Auto Remediation is disabled.
URL Retrospective service status - Unavailable

Disable URL Filtering? [N]>

Do you wish to disable Web Interaction Tracking? [N]>

Do you wish to add URLs to the allowed list using a URL list? [N]>


Enable URL Retrospective service based Mail Auto Remediation to configure remediation actions.

Do you wish to enable Mailbox Auto Remediation action? [N]> y

URL Retrospective service based Mail Auto Remediation is enabled.

Please select a Mailbox Auto Remediation action:
1. Delete
2. Forward and Delete
3. Forward
[1]> 1

esa1.hcxxyy-zz.iphmx.com> commit

Please enter some comments describing your changes:
[]>

Do you want to save the current configuration for rollback? [Y]>

Changes committed: Tue Mar 29 19:43:48 2022 EDT
```

完成后，在URL过滤页面上刷新您的UI，您现在应会看到类似以下内容：

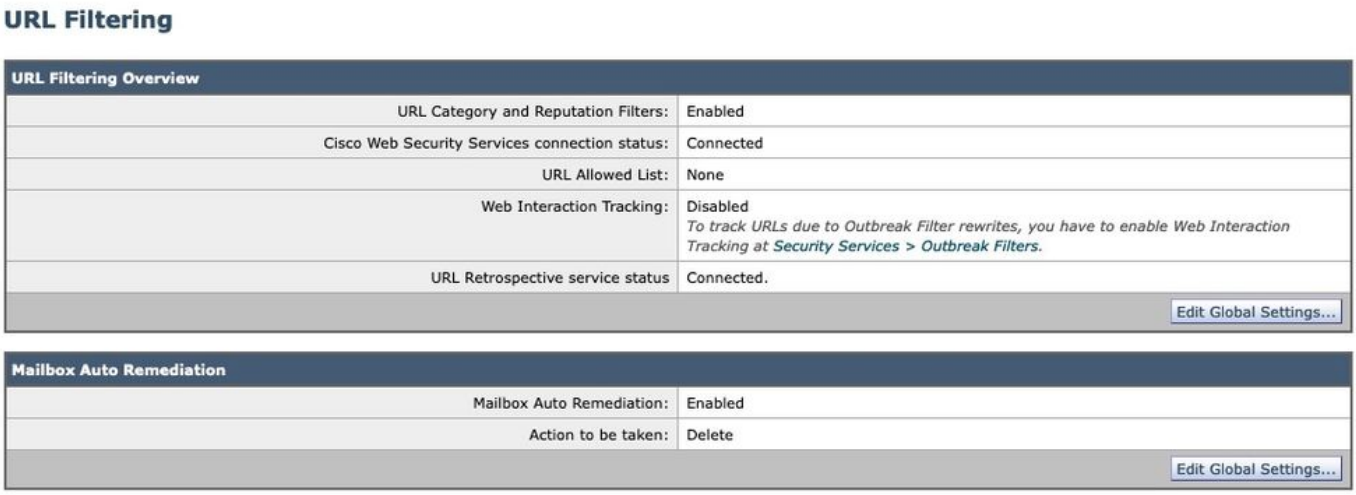


图 10：URL过滤（思科安全邮件云网关的AsyncOS 14.2）

URL保护现已准备就绪，可以在判定更改分数时执行补救操作。 有关详细信息，请参阅AsyncOS 14.2 for Cisco Secure Email Cloud Gateway 的用户指南中的“防止恶意或不需要的URL”。

配置完成!

此时，思科安全电邮已准备好在新信息可用时持续评估新出现的威胁，并在它们进入网络后通知您确定为威胁的文件。

当从文件分析（思科安全恶意软件分析）生成追溯性判定时，会向邮件安全管理员发送信息消息（如果已配置）。 示例：

```
The Info message is:

Retrospective verdict received for Book1.xls.

SHA256: 7d06fd224e0de7f26b48dc2daf7f099b3770080d98bd38c49ed049087c416c4b
Timestamp: 2019-06-03T23:40:36Z
Verdict: MALICIOUS
Spyname: W32.7D06FD224E-95.SBX.TG

Total users affected: 1
---------- Affected Messages ---------------


Message 1
   MID              : 348938
   Subject          : [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]test Mon, 03 Jun 2019 16:50:18 -0400
   From             :
   To               :
   File name        : Book1.xls
   Parent SHA256    : unknown
   Parent File name : unknown
   Date             : 2019-06-03T20:52:33Z

------------------------------------------------


Version: 12.1.0-087
Serial Number: 420DE3B51AB744C7F092-9F0
Timestamp: 04 Jun 2019 04:40:36 +0500
```

如果根据邮件策略配置了邮箱自动补救，则将采用配置的方式。

邮箱自动补救报告示例

任何已修复的SHA256的报告都将显示在思科安全电邮网关和思科安全电邮和Web管理器上提供的邮箱自动修复报告中。

Mailbox Auto Remediation

Printable PDF

Time Range: Day

03 Jun 2019 05:00 to 04 Jun 2019 05:39 (GMT +05:00) — Data in time range:99.86 % complete

Advanced Malware Protection Retrospective Security

Displaying 1 - 1 of 1 items.

File SHA-256	Filename	Action Taken	Time When Action Was Issued	Recipients for Whom the Remediation was Successful	Recipients for Whom the Remediation was Unsuccessful
7d06fd22...7c416c4b	Book1.xls	Forward and Delete	04 Jun 2019 04:42:21	robsherw@bce-demo.info	

Displaying 1 - 1 of 1 items.

Columns... | Export...

图 11：（旧版UI）邮箱自动补救报告

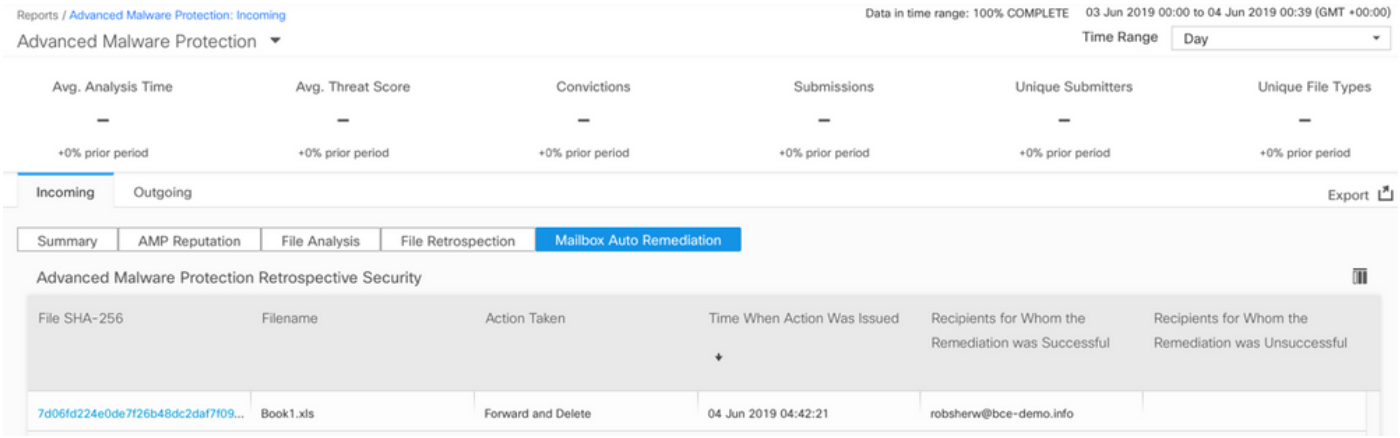


图 12：(NG UI)邮箱自动补救报告

邮箱自动补救日志记录

邮箱自动修复具有单个日志“mar”。 邮箱自动补救日志将包含您的思科安全电子邮件网关与Microsoft Azure， Microsoft 365之间的所有通信活动。

mar日志的示例：

```
Mon May 27 02:24:28 2019 Info: Version: 12.1.0-087 SN: 420DE3B51AB744C7F092-9F0000000000
Mon May 27 02:24:28 2019 Info: Time offset from UTC: 18000 seconds
Fri May 31 01:11:53 2019 Info: Process ready for Mailbox Auto Remediation
Fri May 31 01:17:57 2019 Info: Trying to connect to Azure AD.
Fri May 31 01:17:57 2019 Info: Requesting token from Azure AD.
Fri May 31 01:17:58 2019 Info: Token request successful.
Fri May 31 01:17:58 2019 Info: The appliance is able to read the user's(robsherw@bce-demo.info)
mailbox.
Fri May 31 04:41:54 2019 Info: Trying to perform the configured action on MID:312391
SHA256:de4dd03acda0a24d0f7e375875320538952f1fa30228d1f031ec00870ed39f62 Recipient:robsherw@bce-
demo.info.
Fri May 31 04:41:55 2019 Info: Message containing attachment(s) for which verdict update
was(were) available was not found in the recipient's (robsherw@bce-demo.info) mailbox.
Tue Jun  4 04:42:20 2019 Info: Trying to perform the configured action on MID:348938
SHA256:7d06fd224e0de7f26b48dc2daf7f099b3770080d98bd38c49ed049087c416c4b Recipient:robsherw@bce-
demo.info.
Tue Jun  4 04:42:21 2019 Info: Message containing attachment(s) for which verdict update
was(were) available was not found in the recipient's (robsherw@bce-demo.info) mailbox.
```

思科安全电邮网关故障排除

如果您未看到连接状态测试的成功结果，则可能希望查看从Microsoft Azure AD执行的应用程序注册。

从思科安全邮件网关，将MAR日志设置为“跟踪”级别并重新测试连接。

对于不成功的连接，日志可能显示类似于：

```
Thu Mar 30 16:08:49 2017 Info: Trying to connect to Azure AD.
Thu Mar 30 16:08:49 2017 Info: Requesting token from Azure AD.
Thu Mar 30 16:08:50 2017 Info: Error in requesting token: AADSTS70001: Application with
identifier '445796d4-8e72-4d06-a72c-02eb47a4c59a' was not found in the directory ed437e13-ba50-
479e-b40d-8affa4f7e1d7
Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
Timestamp: 2017-03-30 20:08:50Z
Thu Mar 30 16:08:50 2017 Info: Error while requesting token AADSTS70001: Application with
identifier '445796d4-8e72-4d06-a72c-02eb47a4c59a' was not found in the directory ed437e13-ba50-
479e-b40d-8affa4f7e1d7
Trace ID: 4afd14f4-ca97-4b15-bba4-e9be19f30d00
Correlation ID: f38e3388-729b-4068-b013-a08a5492f190
Timestamp: 2017-03-30 20:08:50Z
```

确认应用程序ID、目录ID（与租户ID相同）或日志中与Azure AD中的应用程序关联的其他标识符。如果不确定这些值，请从Azure AD门户删除应用程序，然后重新开始。

要成功连接，日志应类似于：

```
Thu Mar 30 15:51:58 2017 Info: Trying to connect to Azure AD.
Thu Mar 30 15:51:58 2017 Info: Requesting token from Azure AD.
Thu Mar 30 15:51:58 2017 Trace: command session starting
Thu Mar 30 15:52:00 2017 Info: Token request successful.
Thu Mar 30 15:52:00 2017 Info: The appliance is able to read the
user's(myuser@mydomain.onmicrosoft.com) mailbox.
```

Azure AD故障排除

> **注意**：思科TAC和思科支持部门无权对Microsoft Exchange、Microsoft Azure AD或Office 365的客户端问题进行故障排除。

对于Microsoft Azure AD的客户端问题，您需要与Microsoft支持部门接洽。 请从您的Microsoft Azure仪表板查看“帮助+支持”选项。 您可以从控制面板向Microsoft支持部门提交直接支持请求。

附录 A

注意：仅当您未使用客户端密钥设置Azure应用程序时，才需要此设置。

构建公共证书和私有证书及密钥对

提示：请将输出保存为本地$base64Value、*$base64Thumbprint*和*$keyid*，**因为在稍后的配置步骤中将需要这些输出。** 请将证书的.crt和关联的.pem放在计算机上的可用本地文件夹中。

注意：如果您已经拥有证书（x509格式/标准）和私钥，请跳过此部分。 确保您同时拥有CRT和PEM文件，因为在接下来的章节中您需要它们！

证书:Unix/Linux（利用openssl）

要创建的值：
- **指纹**
- **公共证书（CRT文件）**
- **私钥（PEM文件）**

使用Unix/Linux/OS X的管理员为了执行提供的脚本，假设您安装了OpenSSL。

注意：运行命令“which openssl”和“openssl version”以验证OpenSSL安装。如果OpenSSL不存在，请安装它！

请参阅以下文档以获得帮助：Azure AD思科安全电子邮件配置脚本

从主机(UNIX/Linux/OS X):

1. 从终端应用程序、文本编辑器（或者，您可以轻松创建外壳脚本），通过复制以下内容创建脚本：https://raw.githubusercontent.com/robsherw/my_azure/master/my_azure.sh
2. 粘贴脚本
3. 确保脚本可执行！运行以下命令：**chmod u+x my_azure.sh**

4. 运行脚本：**./my_azure.sh**

```
################################################################################
Next, log-in to Microsoft Azure and use the following for your App registration:
################################################################################

Complete the Azure App registration (Certificate & secrets) using this certificate (public key): MARforO365.crt
Complete the Azure App registration (API permissions)
View & save your Client ID and Tenant ID

########################################################
After successful Azure App registration, from Cisco ESA:
########################################################

Use the Client ID and Tenant ID copied from your Azure App registration
The Thumbprint to use for your ESA configuration: cY8JViuV1oFRVFje/HC9J9ZGvl8=
The Certificate Private Key to use for your ESA configuration: MARforO365.pem

Do you wish to review this certificate in detail? (y/n) n
Thank you!  Be sure to keep up-to-date from https://docs.ces.cisco.com
```

图 13：my_azure.sh的屏幕输出

如图2所示，脚本构建并调用Azure应用注**册所需的公**共证书（CER文件）。脚本还将***指纹***和***证书私钥（PEM文件）***您将在配置思科安全电邮部分中使用。

您具有在Microsoft Azure中注册我们的应用程序所需的值！

[跳过下一节！ 请继续"注册Azure应用以与思科安全电子邮件配合使用"]

证书:Windows（使用PowerShell）

对于使用Windows的管理员，您需要利用应用程序或具备创建自签名证书的知识。 此证书用于创建Microsoft Azure应用并关联API通信。

要创建的值：
- **指纹**
- **公共证书（CRT文件）**
- **私钥（PEM文件）**

本文档创建自签名证书的示例是使用XCA(https://hohnstaedt.de/xca/、https://sourceforge.net/projects/xca/)。

注意：XCA可以下载到Mac、Linux或Windows。

1.为证书和密钥创建数据库：
   a.从工**具栏**中选择文件

b.选择新**建数据库**
c.为数据库创建密码
（您需要在后续步骤中使用它，所以请记住它！）

2.单击“证书”选项卡，然后单击“新建**证书”**

3.单击“主题”选项卡并填写以下内容：
a.内部名称
b.countryName
c.stateOrProvinceName
d.localityName
e.organizationName
f. 组织单位名称(OU)
g.commonName(CN)
h.emailAddress

4.单击“生**成新密钥”**

5.在弹出窗口中，验证提供的信息（根据需要更改）：
a.名称
b.密钥类型：RSA
c.密钥大小：2048 位
d.点击创建
e.单击确定确认“已成功创建RSA私钥‘Name’”弹**出**

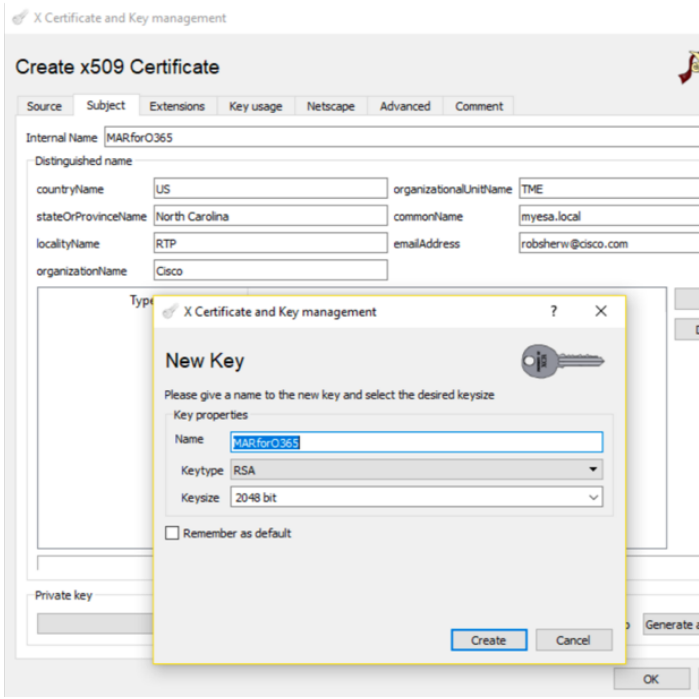


图 14：使用XCA（步骤3-5）

6.单击“密钥用法”选项卡并选择以下选项：
a.在“X509v3密钥用法：
数字签名、密钥加密
b.在X509v3扩展密钥使用下：
电子邮件保护

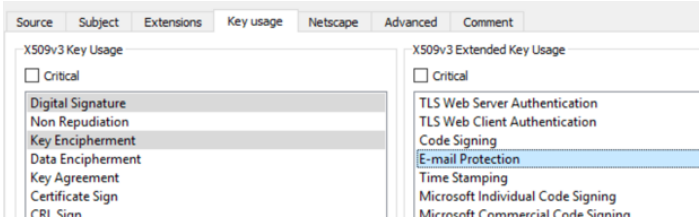
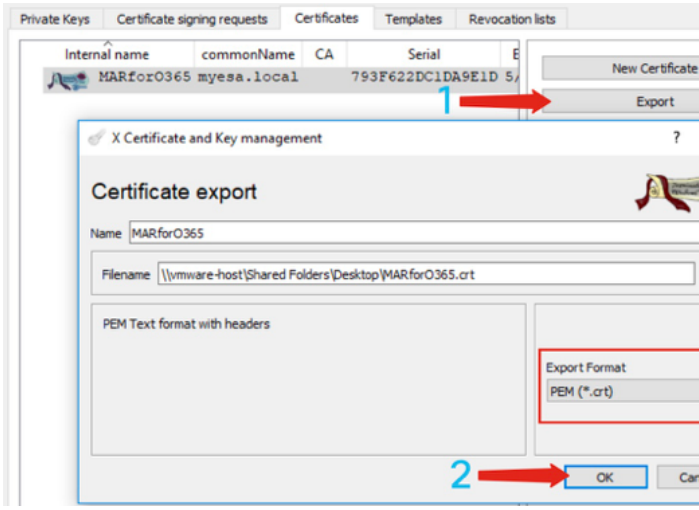


图 15：使用XCA（第6步）

7.单击“**确定”**将更改应用到证书
8.单击“确定”确认“已成功创*建证*书‘名称’”弹出窗**口**

接下来，您将要导出公共证书（CER文件）和***证书私钥（PEM文件）***，以便在下一步的PowerShell命令中使用，并在“配置思科安全邮件”步骤中使用：

1.单击并突出显示新创建的证书的内部名称。
2.单击“导**出”**
a.设置保存目录以便于访问（根据需要更改）
b.确保导出格式设置为**PEM(.crt)**
c.单击“**确定”**



3.单击“私钥”**选项**卡
4.单击并突出显示新创建的证书的内部名称。
5.单击“导**出**”
    a.设置保存目录以便于访问（根据需要更改）
    b.确保导出格式设置为**PEM专用(.pem)**
    c.单击“**确定**”
6.退出并关闭XCA

图 16：使用XCA（导出CRT）（步骤1-2）

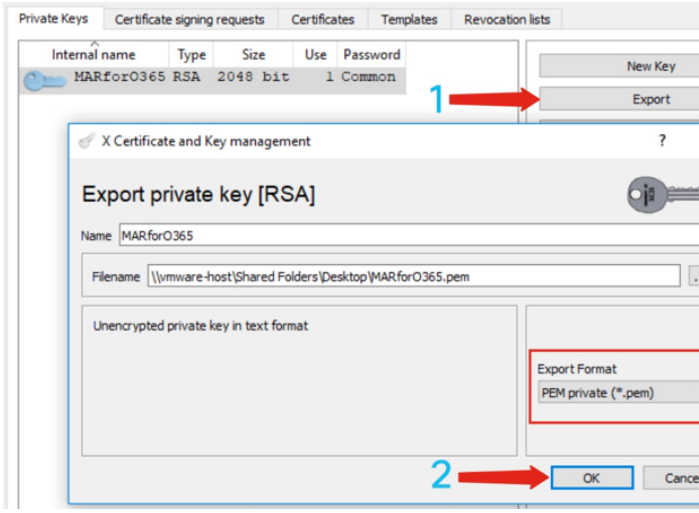


图 17：使用XCA（导出PEM）（步骤3-5）

最后，您将获取已创建的证书并解压**指纹**，这是配置思科安全邮件所需的。

1. 使用Windows PowerShell，运行以下命令：

```
$cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
$cer.Import("c:\Users\joe\Desktop\myCert.crt")
$bin = $cer.GetRawCertData()
$base64Value = [System.Convert]::ToBase64String($bin)
$bin = $cer.GetCertHash()
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()[Note: “c:\Users\joe\Desktop...” is the location on
your PC where your CRT file is saved.]
```

2. 要获取后续步骤的值，请保存到文件或复制到剪贴板：

```
$base64Thumbprint | Out-File c:\Users\joe\Desktop\base64Thumbprint.txt
$base64Thumbprint
```

注意：“c:\Users\joe\Desktop..." 是PC上保存输出的位置。

运行PowerShell命令时的预期输出应类似于以下内容：

```
PS C:\Users\joe\Desktop> $base64Thumbprint
75fA1XJEJ4I1ZVFOB2xqkoCIh94=
```

如您所见，PowerShell命令调出*base64Thumbprint*，这是Cisco Secure E-mail网关配置**所需**的Thumbprint。

您还已完成创建Azure**应用注册所**需的公共证书（CER文件）。您已创建了将在***配置Cisco Secure Email***部分中使用的证书私钥（PEM文件）。

您具有在Microsoft Azure中注册应用程序所需的值！

[请继续"注册Azure应用以与思科安全电子邮件配合使用"]

附录 B

注意：仅在网关上运行AsyncOS 11.x或12.x for Email时，才需要此选项。

API权限(AsyncOS 11.x、12.x)

在应用程序窗格的管理选项……

1. 选择**API权限**
2. 单击**+添加权限**
3. 向下滚动到受支**持的旧版API并**选择**Exchange**
4. 选择以下授权权限： EWS > "EWS.AccessAsUser.All"（通过Exchange Web服务以登录用户身份访问邮箱）Mail > "Mail.Read"（读取用户邮件）Mail > "Mail.ReadWrite"（读写用户邮件）Mail > "Mail.Send"（以用户身份发送邮件）
5. 滚动到窗格顶部……
6. 选择以下对应用权限的权限： "full_access_as_app"（使用Exchange Web服务，可完全访问所有邮箱）Mail > "Mail.Read"（读取用户邮件）Mail > "Mail.ReadWrite"（读写用户邮件）Mail > "Mail.Send"（以用户身份发送邮件）
7. *可选：*您将看到Microsoft Graph默认为"User.Read"权限启用；您可以保留此配置，或者单击"**读取"**并单击"**删除权限"**，以从与应用程序关联的API权限中删除此权限。
8. 单击**添加权**限(或**更新权**限，如果Microsoft Graph已列出)
9. 最后，单击"Grant admin consent for...(授**予管理员同意……)"** 确保将新权限应用到应用程序
10. 会出现一个窗格内弹出窗口，询问：

"*是否要授予<Azure Name>中所有帐户的请求权限的同意？这将更新此应用程序已经必须与下面列出的内容匹配的任何现有管理员同意记录。*"

单击**是**

此时，您应看到绿色的成功消息，"Admin Consent Required"（需要管理员同意）列显示Granted（已授予），如下所示：

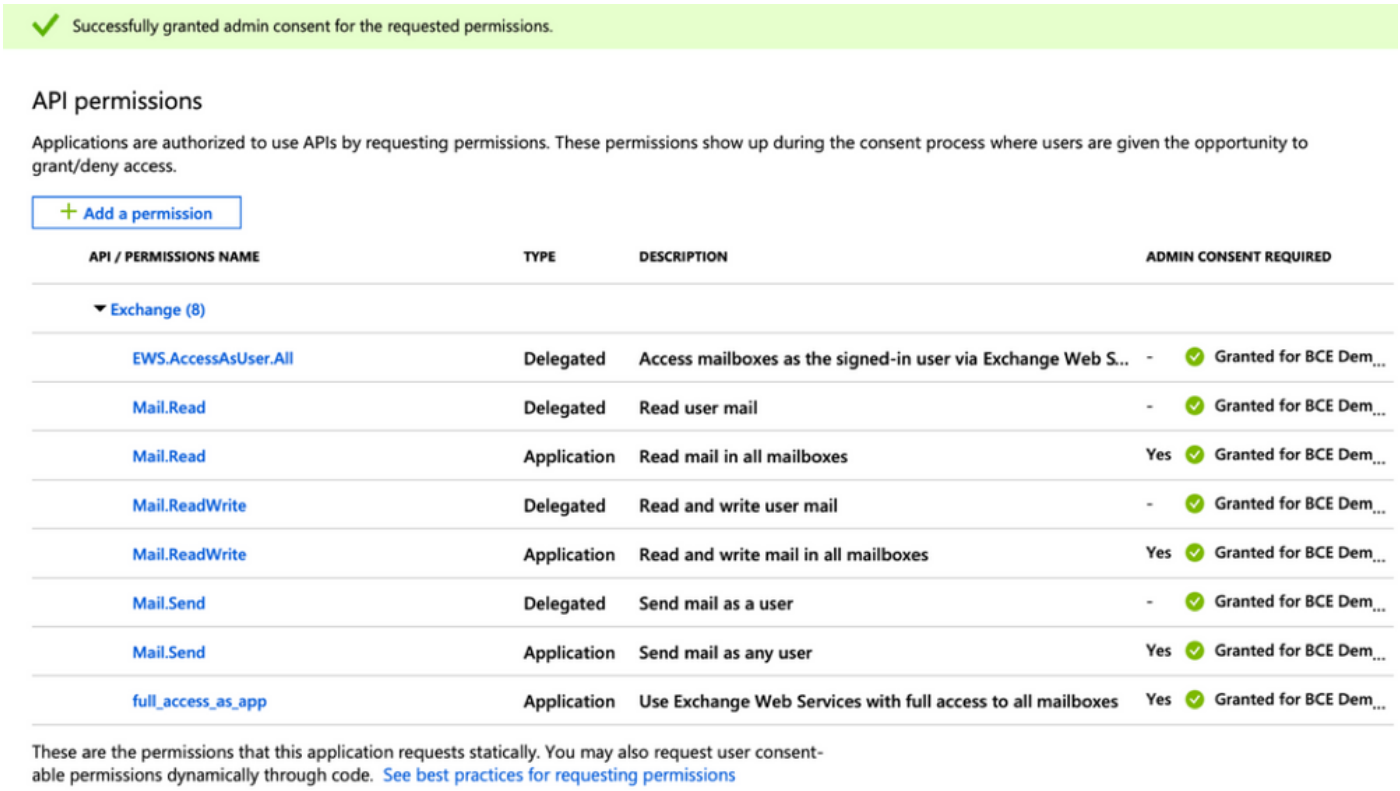


图 18：Microsoft Azure App注册（需要API权限）

[请继续“注册Azure应用以与思科安全电子邮件配合使用”]

相关信息

- 思科邮件安全设备 — 产品支持
- 思科邮件安全设备 — 版本说明
- 思科邮件安全设备 — 最终用户指南