补救邮箱中的邮件

本章包含以下部分：

概述

邮件网关提供对已传送到用户邮箱的恶意邮件进行补救的功能。您可以将邮件网关配置为通过以下方式来补救邮件：

- 当 AMP 向您的邮件网关发送追溯性警报时自动修复邮件
- 使用邮件跟踪过滤器来手动搜索和修复邮件

文件在任何时候都可以变成恶意的，即使它已经到达用户的邮箱。AMP 可以识别这一点，新的信息涌现，并推动追溯警报到您的邮件网关。您可以将邮件网关配置为在威胁判定更改时对用户邮箱中的邮件执行自动补救操作。例如，当附件的判决从“清除”更改为“恶意”时，您可以将邮件网关配置为从收件人邮箱中删除邮件。

您还可以使用“邮件跟踪”(Message Tracking) 页面来搜索和补救已传送到用户邮箱的邮件。“邮件跟踪”(Message Tracking) 页面是一个统一位置，可用于搜索已传送到邮箱的所有邮件。从搜索结果中，您可以选择要补救的邮件，并应用要对邮件执行的操作。

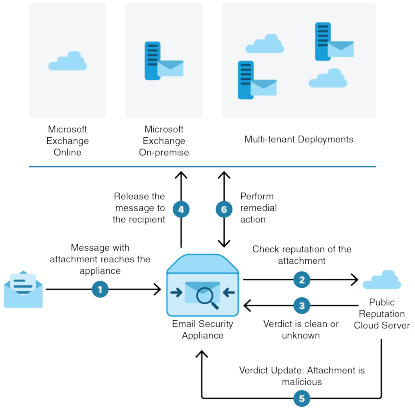
邮件网关可以对以下邮箱部署中的邮件执行补救操作（手动或自动）：

- Microsoft Exchange 在线 – 在 Microsoft Office 365 上托管的邮箱
- Microsoft Exchange 内部部署 – 本地 Microsoft Exchange server

- 混合/多租户配置 – 在 Microsoft Exchange 在线和 Microsoft Exchange 内部部署中配置的邮箱的组合

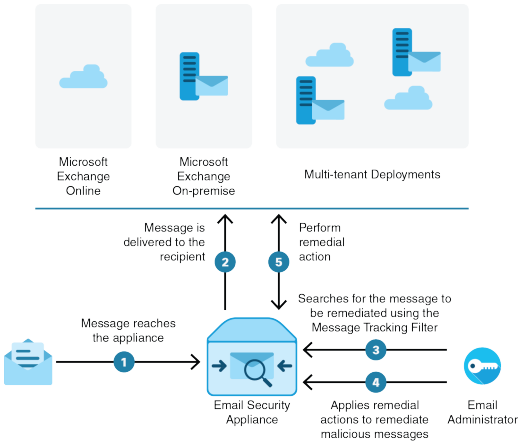
工作流程

邮箱自动修复工作流



1. 包含附件的邮件将发送至邮件网关。
2. 邮件网关将查询公共文件信誉云服务器以评估附件的信誉。
3. 公共文件信誉云服务器将判定发送到邮件网关。判定为安全或未知。
4. 邮件网关将邮件释放发给收件人。
5. 经过一段时间后，邮件网关将从公共文件信誉云服务器收到判定更新。新判定为恶意。
6. 邮件网关对驻留在收件人邮箱中的邮件（带有恶意附件）执行配置的修复操作。

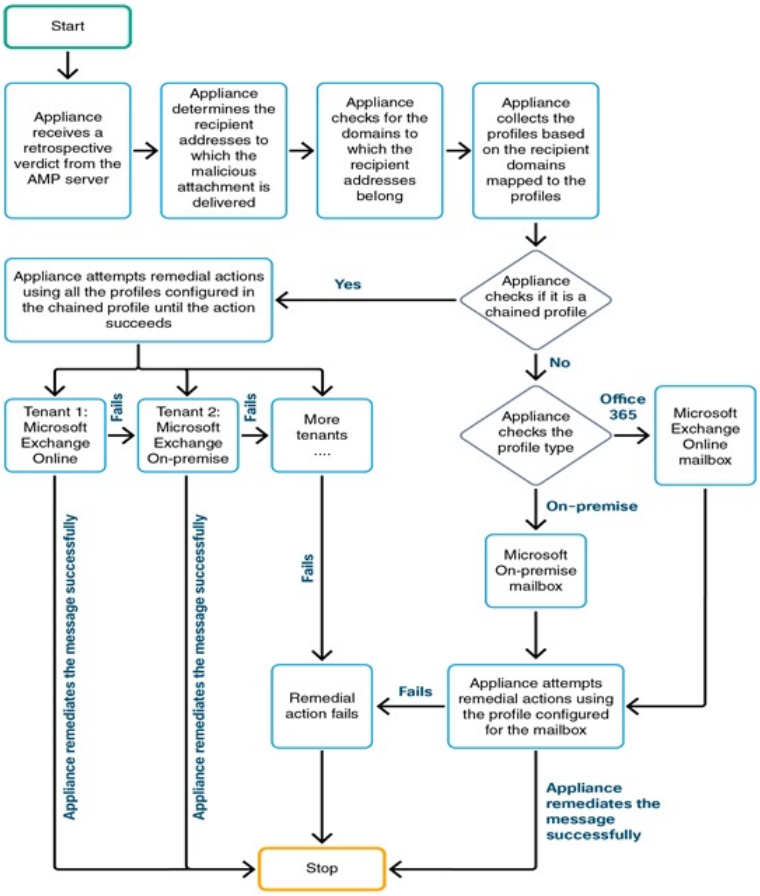
搜索和补救邮件工作流程



1. 邮件到达邮件网关。
2. 邮件被送达给收件人。
3. 管理员使用邮件跟踪过滤器来搜索传送给收件人的邮件。
4. 用户从收件人的邮箱中选择要补救的邮件，并对邮件采取补救操作。

5. 邮件网关对驻留在收件人邮箱中的邮件执行配置的修复操作。

邮件网关如何执行自动补救操作



1. [仅用于搜索和补救邮件] 用户使用邮件跟踪过滤器来搜索传送到用户邮箱的邮件。
2. [仅用于搜索和补救邮件] 用户选择要补救的邮件并对邮件应用补救操作。
3. [仅用于自动补救邮件] 当邮件网关收到来自公共文件信誉云服务器的追溯性判定时，邮件网关会启动邮箱补救过程。
4. [仅用于自动补救邮件] 邮件网关将确定恶意邮件传送到的邮件地址。
5. 设备将标识邮件地址所属的收件人域。
6. 根据收件人域，邮件网关将收集映射到域的帐户配置文件。

帐户配置文件定义设备用于连接到邮箱并执行自动补救操作的邮箱设置。您必须创建帐户配置文件并将其映射到收件人域，才能成功补救邮箱中的邮件。

7. 邮件网关将检查映射到域的配置文件：
   - [仅适用于混合或多租户部署] 如果是链式配置文件，邮件网关会尝试使用链式配置文件中的所有帐户配置文件执行补救操作。

     链式配置文件是多个帐户配置文件的组合。如果混合或多租户部署在多个部署中存在邮箱，则必须创建链式配置文件，以组合在部署中为邮箱定义的所有配置文件。邮件网关尝试根据在链式配置文件中添加帐户配置文件的顺序来执行补救操作。
   - 如果不是链式配置文件，邮件网关会检查配置文件类型，了解它是 Microsoft Exchange Online 配置文件还是 Microsoft Exchange On-Premise 配置文件。
8. 邮件网关使用已识别的配置文件执行补救操作并补救邮件。

Note 由于各种原因，邮箱补救可能会失败。有关详细信息，请参阅邮箱补救故障排除, on page 19。

相关主题

- 对 Microsoft Exchange Online 邮箱中的邮件执行补救操作, on page 4
- 对 Microsoft Exchange On-Premise 邮箱中的邮件执行补救操作 , on page 6
- 对混合部署上的邮箱中的邮件执行补救操作, on page 7

对邮箱中的邮件执行补救操作

您可以对以下邮箱部署中的邮件执行补救操作：

- Microsoft Exchange Online (Office 365) - #unique_1030
- Microsoft Exchange On-Premise - #unique_1031
- 混合/多租户部署 - #unique_1032

对 Microsoft Exchange Online 邮箱中的邮件执行补救操作

您可以将邮件网关配置为对用户邮箱中的邮件执行补救。

如果您的组织使用 Microsoft Exchange Online 管理邮箱, 则可以将邮件网关配置为在威胁判决更改时对用户邮箱中的邮件执行自动补救操作。例如, 当附件的判决从“清除”更改为“恶意”时，您可以将邮件网关配置为从收件人邮箱中删除邮件。

您可以对已传送到用户邮箱的邮件手动执行补救操作。例如，监控传入邮件的管理员可以使用邮件跟踪过滤器来对用户邮箱中的邮件执行补救操作。

目录

如何对 Microsoft Exchange Online 邮箱中的邮件配置补救操作

	相应操作	更多信息
第 1 步	查看前提条件。	在 Microsoft Exchange Online 邮箱中补救邮件的前提条件, on page 9
第 2 步	将邮件网关注册为 Azure AD（Azure 管理门户）上的应用。	在 Azure AD 上将您的邮件网关注册为应用, on page 11
第 3 步	在邮件网关上启用帐户设置。	在邮件网关上启用邮箱补救。 在邮件网关上启用帐户设置 , on page 13

第 4 步	在邮件网关上创建 Office 365/混合 (Graph API) 类型的帐户配置文件。	为用户邮箱创建 Office 365 配置文件，并在邮件网关上定义邮箱设置。
		在开始之前，请确保您已拥有：
		• 以下参数的值 - 在 Azure 管理门户上注册的应用的客户端 ID 和租户 ID。请参阅在 Azure AD 上将您的邮件网关注册为应用, on page 11的步骤 9。
		• 对于基于客户端证书的通信，请获取以下参数值：
		  • .pem 格式的证书私钥。查看用于安全通信的证书
		  • 证书指纹 ($base64Thumbprint)。请参阅在 Azure AD 上将您的邮件网关注册为应用, on page 11的步骤 8。
		• 对于基于客户端密钥的通信，请获取您在 Azure 管理门户上创建的应用生成的客户端密钥值。请参阅在 Azure AD 上将您的邮件网关注册为应用, on page 11的步骤 8。
		请参阅创建账户配置文件 , on page 14。

第 5 步	添加收件人域并将该域映射到 Office 365 配置文件。	添加收件人邮箱所属的域，并将该域映射到 Office 365 帐户配置文件。 请参阅将域映射到帐户配置文件 , on page 16。

	相应操作	更多信息
第 6 步	[仅用于自动补救邮件]将您的邮件网关配置为在威胁判定变为恶意时，对传递给最终用户的邮件执行补救操作。	在邮箱中配置邮件的自动补救操作, on page 16
第 7 步	[仅用于搜索和补救邮件]将邮件网关配置为对传送给最终用户的邮件手动执行补救操作。	在邮箱中搜索和补救邮件, on page 17

对 Microsoft Exchange On-Premise 邮箱中的邮件执行补救操作

您可以将邮件网关配置为对 Exchange 内部部署服务器上的邮箱中的邮件执行补救。邮件可以由邮件网关自动补救，也可以由用户使用邮件跟踪过滤器手动补救。

邮件网关使用具有 impersonator 权限的用户账号访问 Exchange 内部部署邮箱，并对邮件执行补救操作。您必须在邮件网关要连接到的邮件交换服务器上创建具有 impersonator 权限的此用户账号，并对邮件进行补救。

Note 思科已验证仅可在 Microsoft Exchange 2013、2016 和 2019 上执行邮箱自动补救。

目录

如何对 Microsoft Exchange On-Premise 邮箱中的邮件配置补救操作

	相应操作	更多信息
第 1 步	查看前提条件。	在 On-Premise 账户中补救邮件的前提条件, on page 10
第 2 步	在邮件网关上启用帐户设置。	在邮件网关上启用邮箱补救。 在邮件网关上启用帐户设置 , on page 13
第 3 步	在邮件网关上创建现场类型的帐户配置文件。	为用户邮箱创建 On-Premise 配置文件，并在邮件网关上定义邮箱设置。 在开始之前，请确保您已拥有： • impersonator 用户帐户详细信息 • 本地邮件交换服务器的主机名 创建账户配置文件 , on page 14。

	相应操作	更多信息
第 4 步	添加收件人域并将该域映射到On-Premise帐户配置文件。	添加收件人邮箱所属的域，并将该域映射到内部帐户配置文件。 请参阅将域映射到帐户配置文件 , on page 16。
第 5 步	[仅用于自动补救邮件]将您的邮件网关配置为在威胁判定变为恶意时，对传递给最终用户的邮件执行补救操作。	在邮箱中配置邮件的自动补救操作, on page 16
第 6 步	[仅用于搜索和补救邮件]为现场邮箱中的邮件配置补救操作。	在邮箱中搜索和补救邮件, on page 17

对混合部署上的邮箱中的邮件执行补救操作

您可以配置单个邮件网关来对混合交换部署或多个交换租户中的邮件进行补救。例如，如果贵组织正在将邮箱从 Microsoft Exchange On-Premise 迁移到 Microsoft Exchange 在线，则会在 Microsoft Exchange Online 和 Microsoft Exchange On-Premise 中部署邮箱，直到迁移完成为止。邮件可以由邮件网关自动补救，也可以由用户使用邮件跟踪过滤器手动补救。

要自动补救在不同部署中配置的多个邮箱的邮件，请创建链式配置文件。链式配置文件结合了混合或多租户部署的所有账户配置文件。配置文件添加到链式配置文件的顺序定义了邮件网关检查配置文件以补救邮件的优先级。

当邮件网关收到来自 AMP 服务器的追溯性判定时，设备将尝试按照链式配置文件中定义的优先级顺序，使用链式配置文件中存在的每个配置文件执行补救操作。

要手动搜索和补救已传送到用户邮箱的邮件，可使用“邮件跟踪”(Message Tracking) 过滤器。您可以使用此过滤器来选择要补救的邮件，配置补救操作，并对邮件应用补救操作。

目录

如何对混合部署上的邮箱中的邮件执行自动补救操作

	相应操作	更多信息
第 1 步	查看前提条件。	确保在混合或多租户部署中满足对 Microsoft Exchange Online 和 Microsoft Exchange On-Premise 邮箱执行自动补救操作的所有前提条件。 请参阅 前提条件, on page 9。

	相应操作	更多信息
第 2 步	将邮件网关注册为 Azure AD（Azure 管理门户）上的应用。	在 Azure AD 上将您的邮件网关注册为应用, on page 11
第 3 步	在邮件网关上启用帐户设置。	在邮件网关上启用邮箱补救。 请参阅在邮件网关上启用帐户设置 , on page 13。

第 4 步	为混合/多租户部署中的所有邮箱创建帐户配置文件。	为用户邮箱创建帐户配置文件，并在邮件网关上定义邮箱设置。
		在开始之前，请确保您已拥有：
		• 以下参数的值 - 在 Azure 管理门户上注册的应用的客户端 ID 和租户 ID。请参阅在 Azure AD 上将您的邮件网关注册为应用, on page 11的步骤 9。
		• 对于基于客户端证书的通信，请获取以下参数值：
		  • .pem 格式的证书私钥。查看用于安全通信的证书
		  • 证书指纹 ($base64Thumbprint)。请参阅在 Azure AD 上将您的邮件网关注册为应用, on page 11的步骤 8。
		• 对于基于客户端密钥的通信，请获取您在 Azure 管理门户上创建的应用生成的客户端密钥值。请参阅在 Azure AD 上将您的邮件网关注册为应用, on page 11的步骤 8。
		• impersonator 用户账号详细信息。
		• 本地邮件交换服务器的主机名。
		请参阅创建账户配置文件 , on page 14。

第 5 步	创建链式配置文件。	创建链式配置文件并添加混合/多租户部署的所有配置文件。 请参阅创建链式配置文件 , on page 15。
第 6 步	添加收件人的域并将其映射到链式配置文件。	添加收件人邮箱所属的域，并将该域映射到链式配置文件。 请参阅将域映射到帐户配置文件 , on page 16。

	相应操作	更多信息
步骤 7	[仅用于自动补救邮件]将您的邮件网关配置为在威胁判定变为恶意时，对传递给最终用户的邮件执行补救操作。	在邮箱中配置邮件的自动补救操作, on page 16
第 8 步	[仅用于搜索和补救邮件]对邮件应用补救操作。	在邮箱中搜索和补救邮件, on page 17

在邮件网关上配置邮箱补救

前提条件

在 Microsoft Exchange Online 邮箱中补救邮件的前提条件

文件信誉服务和文件分析服务的功能密钥

Note 在对用户邮箱中的邮件执行搜索和补救操作时，不需要文件信誉服务和文件分析服务功能密钥。

要为用户邮箱中的邮件配置邮箱自动补救的补救操作，请确保您拥有：

- 向邮件网关添加文件信誉服务和文件分析服务的功能密钥。
- 在邮件网关上启用了文件信誉和分析功能。请参阅文件信誉过滤和文件分析：。

Office 365 帐户

确保您拥有将邮件网关注册到 Azure AD 所需的以下帐户：

- Office 365 企业账户
- 与您的 Office 365 企业账户关联的 Azure AD 订用

有关详情，请联系您的 Office 365 管理员。

安全通信客户端密钥证书或

要保护 Office 365 服务与邮件网关之间的通信，您必须执行以下任务之一：

- 为在 Azure 管理门户上创建的应用生成客户端密钥。
- 以下列方式之一设置证书：创建自签名证书或从受信任的 CA 获取证书。

  您必须具有：

  - 采用 .crt 或 .p12 格式的公钥。请确保 emailAddress 设置为 Office 365 管理员的邮件地址 (<admin_username>@<domain>.com)
  - 采用 .pem 格式的关联私钥，密钥大小至少为 2048 位。

Note 此版本不支持带密码的私钥。

有关详细信息，请参阅 https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/211404-How-to-configure-Azure-AD-and-Office-365.html。

在 On-Premise 账户中补救邮件的前提条件

- [仅限邮箱自动补救] - 文件信誉服务和文件分析服务的功能密钥, on page 9
- （可选）导入 Microsoft Exchange Web 服务 (EWS) 证书, on page 11
- 将用户添加到 Impersonator 角色, on page 11

文件信誉服务和文件分析服务的功能密钥

Note 在对用户邮箱中的邮件执行搜索和补救操作时，不需要文件信誉服务和文件分析服务功能密钥。

要为用户邮箱中的邮件配置邮箱自动补救的补救操作，请确保您拥有：

- 向邮件网关添加文件信誉服务和文件分析服务的功能密钥。
- 在邮件网关上启用了文件信誉和分析功能。请参阅文件信誉过滤和文件分析：。

（可选）导入 Microsoft Exchange Web 服务 (EWS) 证书

如果您在用于 EWS 服务的 Microsoft Exchange On-Premise 服务器上使用自签证书，则必须将证书从 Microsoft Exchange On-Premise 服务器导入到邮件网关中。要导入证书，请参阅导入证书。

将用户添加到 Impersonator 角色

邮件网关使用具有 impersonator 特权的用户账号来访问 Microsoft Exchange On-Premise 邮箱。邮件交换管理员必须在本地 Exchange 服务器上创建一个具有 impersonator 特权的用户帐户。邮件网关使用此用户账号来补救邮箱中的邮件。

Procedure

步骤 1 创建必须为其分配 impersonator 特权的用户帐户。邮件网关使用此用户账号访问和操作邮箱以补救邮件。

步骤 2 使用管理员凭证登录到 Microsoft Exchange 控制面板界面。

步骤 3 导航至**权限 -> 管理员角色**。

步骤 4 创建角色并为该角色分配 "ApplicationImpersonation" 权限。

步骤 5 将必须为其分配 impersonator 权限的用户帐户添加为此新角色的成员。

在 Azure AD 上将您的邮件网关注册为应用

Office 365 服务使用 Azure Active Directory (Azure AD) 提供对用户邮箱的安全访问。要使您的邮件网关能够访问 Office 365 邮箱，您必须使用 Azure AD 注册您的邮件网关设备。以下是使用 Azure AD 注册邮件网关需要执行的概要步骤。有关详细说明，请参阅 Microsoft 文档（https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app）。

准备工作

执行 在 Microsoft Exchange Online 邮箱中补救邮件的前提条件, on page 9 中描述的任务。

Procedure

步骤 1 使用 Office 365 业务账户凭证登录到 Azure 管理门户。

步骤 2 将新应用添加到链接到 Office 365 订用的目录中。

步骤 3 导航至**应用注册 > 新注册**以添加新应用。

步骤 4 添加新应用时，请确保：

- 指定应用名称以及应用必须支持的帐户类型。
- （可选）选择 Web 应用类型，提供用户可用来登录并使用您邮件网关的 URL。

步骤 5 分配应用所需的权限。点击导航窗格上的 **API 权限 (API permissions)**，然后点击**添加权限 (Add a permission)**。

步骤 6 选择 **Microsoft Graph > 应用权限**，并分配以下权限：

- Mail.Read – 读取所有邮箱中的邮件
- 邮件。ReadWrite - 读取并写入所有邮箱中的邮件
- Mail.Send - 以任何用户的方式发送邮件
- Directory.Read.All - 从 Azure Active Directory 中读取用户或组信息，以将其存储在思科云环境中配置的 LDAP 服务器上。

步骤 7 授予管理员同意组织中所有帐户请求的所有权限。

步骤 8 通过执行以下任一任务来保护 Office 365 服务与邮件网关之间的通信安全：

- 为在 Azure 管理门户上创建的应用生成客户端密钥。

  Note 确保您复制客户端密钥值，因为在后续登录 Azure 管理门户期间不会再显示该值。

- 使用公钥证书中的密钥凭证来更新应用清单。执行以下步骤：

  a. 使用 Windows PowerShell 提示符，从公钥证书中获取 `$base64Thumbprint`、`$base64Value` 和 `$keyid` 的值。请参阅以下示例。在 Windows PowerShell 提示符下，导航到包含公钥证书的目录，然后运行以下内容：

  示例

  ```
  $cer = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2
  $cer.Import(".\mycer.cer")
  $bin = $cer.GetRawCertData()
  $base64Value = [System.Convert]::ToBase64String($bin)
  $bin = $cer.GetCertHash()
  $base64Thumbprint = [System.Convert]::ToBase64String($bin)
  $keyid = [System.Guid]::NewGuid().ToString()
  ```

  运行上述命令后，运行以下命令以提取它们的值：

  ```
  $keyid
  $base64Value
  $base64Thumbprint
  ```

  b. 点击“已注册应用”窗格左侧窗格中的**清单**，打开应用的清单。

  c. 在清单文本编辑器中，用以下 JSON 替换空的 KeyCredentials 属性：

  示例

  ```
  "keyCredentials": [
  {
  "customKeyIdentifier": "$base64Thumbprint_from_step_1",
  "keyId": "$keyid_from_step1",
  "type": "AsymmetricX509Cert",
  "usage": "Verify",
  "value": "$base64Value_from_step1"
  }
  ],
  ```

示例：

在上面的 JSON 代码片段中，确保用步骤 a 中获得的值替换 `$base64Thumbprint`、`$base64Value` 和 `$keyid` 的值。必须在单行中输入每个值

步骤 9 在使用 Azure AD 注册您的设备后，请通过注册应用的“概述”窗格记下 Azure 管理门户中的以下详细信息：

- 客户端 ID
- 租户 ID。租户 ID 是此页上列出的所有 URL 上都可用的唯一值。例如，此页上列出的 URL 为：
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/federationmetadata/2007-06/federationmetadata.xml
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/wsfed
  - https://login.microsoftonline.com/abcd1234-bcdd-469d-8545-a0662708cbc3/saml2

在这种情况下，租户 ID 为 abcd1234-bcdd-469d-8545-a0662708cbc3。

What to do next

在邮件网关上启用帐户设置 , on page 13

在邮件网关上启用帐户设置

准备工作

确保：

- [仅邮箱自动补救需要] 在邮件网关上启用文件信誉和分析功能。请参阅文件信誉过滤和文件分析：。

Procedure

步骤 1 登录到邮件网关。

步骤 2 点击**系统管理 (System Administration)** > **帐户设置 (Account Settings)**。

步骤 3 点击**启用 (Enable)**。

步骤 4 选择**启用帐户设置 (Enable Account Settings)**。

步骤 5 （可选）输入邮件网关连接邮箱以对邮件进行补救的最大尝试次数。值必须为 1 到 5 之间的整数。

步骤 6 （可选）输入连接到混合邮件交换服务器超时之前邮件网关必须等待的秒数。值必须为 15 到 90 之间的整数。

步骤 7 （可选）输入连接到本地邮件交换服务器超时之前邮件网关必须等待的秒数。值必须为 15 到 90 之间的整数。

步骤 8 提交并确认更改。

What to do next

创建账户配置文件 , on page 14

创建账户配置文件

账户配置文件定义邮件网关连接到邮箱所需的邮箱参数，并在邮箱中邮件的威胁判定为恶意时执行补救操作。

每个配置文件凭证与单一租户相关。如果要在多个租户之间执行补救，则必须为每个租户配置一个配置文件，并使用链式配置文件将它们关联起来。但是，如果您使用的是多租户部署负载均衡器，则仍可配置单个配置文件，并在创建配置文件时使用负载均衡器的主机名。

准备工作

确保：

- 已启用账户设置。请参阅在邮件网关上启用帐户设置 , on page 13。
- Microsoft Exchange Online 服务器或 Microsoft Exchange On-Premise 服务器中的有效邮件地址。
- 配置 Microsoft Exchange Online 账户或 Microsoft Exchange On-Premise 账户所需的参数。

Procedure

步骤 1 登录到邮件网关。

步骤 2 点击**系统管理 (System Administration)** > **账户设置 (Account Settings)**。

步骤 3 点击**创建账户配置文件 (Create Account Profile)**。

步骤 4 输入配置文件的名称和描述。

步骤 5 根据邮箱部署选择配置文件类型：

- **Office 365/Hybrid (Graph API)** - 选择此选项以配置在 Microsoft Exchange 在线部署的邮箱，并输入以下详细信息：
  - 在 Azure 管理门户上注册的应用的客户端 ID 和租户 ID。
  - 选择以下任一方法来验证客户端凭证：
    - **客户端密钥**：选择此选项并输入在 Azure 管理门户上生成的应用的客户端密钥。
    - **客户端证书**：选择此选项，输入证书的指纹（值 $base64Thumbprint），然后点击**选择文件 (Choose File)** 以 .pem 格式上传证书的私钥。

- **Exchange On-premise** - 选择此选项以配置在 Microsoft Exchange On-Premise 部署的邮箱，并输入以下详细信息：
  - 输入具有 impersonator 特权的用户账户的用户名和密码。有关详细信息，请参阅将用户添加到 Impersonator 角色, on page 11。
  - 输入 Microsoft Exchange On-Premise 服务器的主机名。

Note 如果您使用的是多租户部署负载均衡器，则必须配置负载均衡器的主机名。

步骤 6 验证邮件网关是否可以连接到 Microsoft Exchange Online 或 Exchange On-Premise 服务器。

a) 点击**测试连接 (Test Connection)**。

b) 输入邮箱地址。这必须是 Microsoft Exchange Online 或 Microsoft Exchange On-Premise 中的有效邮件地址。

c) 点击**测试连接 (Test Connection)**。
显示状态，确认您的邮件网关是否可以连接到邮箱服务器。

d) 4. 点击**完成 (Done)**。有关错误的故障排除， 请参阅邮箱补救故障排除, on page 19。

步骤 7 提交并确认更改。

What to do next

- 创建链式配置文件 , on page 15
- 将域映射到帐户配置文件 , on page 16

创建链式配置文件

仅当您要对混合或多租户部署中邮箱中的邮件进行补救时，才需要此任务。

准备工作

请确保您的邮件网关上至少添加了一个帐户配置文件：

Procedure

步骤 1 登录到邮件网关。

步骤 2 点击**系统管理 (System Administration)** > **帐户设置 (Account Settings)**。

步骤 3 点击**创建链式配置文件 (Create Chained Profile)**。

步骤 4 输入链式配置文件的名称和描述。

步骤 5 从下拉菜单中选择要添加到链式配置文件的帐户配置文件。要添加更多配置文件，请点击**添加帐户配置文件 (Add Account Profile)**。

Note
- 您必须按照希望邮件网关检查配置文件以对邮件进行补救的优先级顺序添加配置文件。
- 您可以在邮件网关上一次最多创建五个链式配置文件。
- 每个链式配置文件最多可以添加 10 个帐户配置文件。

步骤 6 提交并确认更改。

What to do next

将域映射到帐户配置文件 , on page 16

将域映射到帐户配置文件

您必须定义收件人邮箱所属的域。然后，该域将映射到邮件网关用于补救邮箱中邮件的帐户配置文件。

Note

- 您可以编辑域映射，以将新域添加到已映射到该配置文件的现有域。
- 配置文件的域映射具有唯一性。映射到某一配置文件的域不能映射到另一个配置文件。

准备工作

请确保您的邮件网关上至少添加了一个帐户配置文件。

Procedure

步骤 1 登录到邮件网关。

步骤 2 点击**系统管理 (System Administration)** > **帐户设置 (Account Settings)**。

步骤 3 点击**创建域映射 (Create Domain Mapping)**。

步骤 4 输入逗号分隔的域名。如果要将配置文件映射到所有域，请键入字符串 ' ALL '。

步骤 5 选择要映射到域的配置文件。您还可以将链式配置文件映射到域。

步骤 6 提交并确认更改。

What to do next

- 在邮箱中配置邮件的自动补救操作, on page 16
- 在邮箱中搜索和补救邮件, on page 17

在邮箱中配置邮件的自动补救操作

Note 如果要为邮箱中的邮件配置邮箱自动补救的补救操作，请执行以下步骤。

准备工作

请确保已启用邮箱自动补救并在设备上配置帐户设置。请参阅在邮件网关上启用帐户设置 , on page 13。

Procedure

步骤 1 选择**邮件策略 (Mail Policies)** > **传入邮件策略 (Incoming Mail Policies)**。

步骤 2 点击邮件策略的**高级恶意软件防护 (Advanced Malware Protection)** 列中的链接进行修改。

步骤 3 选择**启用邮箱自动补救 (Enable Mailbox Auto Remediation)**。

步骤 4 指定当威胁判定更改为恶意时，对发送给最终用户的邮件将执行的操作。根据您的要求，选择下列补救操作之一：

- 转发到某个邮件地址。选择此选项可将包含恶意附件的邮件转发给指定用户，例如邮件管理员。
- 删除邮件。选择此选项可从最终用户的邮箱中永久删除包含恶意附件的邮件。
- 转发到邮件地址并删除该邮件。选择此选项可将包含恶意附件的邮件转发给指定用户（例如邮件管理员），并从最终用户的邮箱中永久删除该邮件。

步骤 5 提交并确认更改。

What to do next

相关主题

- 监控邮箱补救结果, on page 19
- 查看邮件跟踪中的邮箱修复详细信息, on page 19
- 邮箱补救故障排除, on page 19

在邮箱中搜索和补救邮件

准备工作

- 请确保已启用邮箱自动补救并在邮件网关上配置账户设置。请参阅在邮件网关上启用帐户设置，第 13 页。
- 在邮件网关上启用邮件跟踪。请参阅启用邮件跟踪。
- 如果您使用的是集中邮件跟踪服务，请确保已在托管邮件网关上启用了 trailblazer 端口和 AsyncOS API HTTP 端口，并且思科安全邮件和 Web 管理器可以访问该 trailblazer 端口。如果禁用 trailblazer 端口，请确保思科安全邮件和 Web 管理器可以访问托管的邮件网关上的 AsyncOS API HTTP 端口。

注释 您只能在邮件网关的新 Web 界面中执行以下步骤。

过程

步骤 1 点击邮件安全设备以获得新的外观。旧 Web 界面上的“试试！！”(Try it!!) 链接。请参阅访问基于 Web 的图形用户界面 (GUI)。

步骤 2 点击**跟踪 (Tracking)** 选项卡。

步骤 3 点击**邮件 (Messages)** 选项卡以缩小搜索结果范围。有关详细信息，请参阅 在新 Web 界面上搜索邮件。

步骤 4 选择要补救的邮件。您一次最多可以选择 1000 封邮件。您只能补救处于已传送状态的邮件。

步骤 5 点击**补救 (Remediate)**。

步骤 6 输入下列详细信息：

- 输入补救的批处理名称。
- 选择以下任一补救操作：
  - 删除邮件。选择此选项可从最终用户的邮箱中永久删除恶意邮件。
  - 转发到一个或多个以分号 (;) 分隔的邮件地址。选择此选项可将恶意邮件转发给指定用户，例如邮件管理员。
  - 转发到一个邮件地址或多个以分号 (;) 分隔的邮件地址，然后删除该邮件。选择此选项可将恶意邮件转发给指定用户（例如邮件管理员），并从最终用户的邮箱中永久删除该邮件。

步骤 7 点击**应用 (Apply)**。

点击“应用”(Apply) 后，您可以在“邮件跟踪”(Message Tracking) 页面的右下角查看**补救报告状态 (Remediation Report Status)** 小组件。可使用此小组件来检查补救报告生成的状态。生成补救报告后，点击小组件上的**查看详细信息 (View Details)** 转至补救报告，以便查看补救结果。

注释 您还可以通过导航至“报告”(Reports) > “用户报告”(User Reports) > “补救报告”(Remediation Report) 并点击**邮箱搜索和补救 (Mailbox Search And Remediate)** 选项卡来直接查看补救报告。

下一步做什么

相关主题

- 监控邮箱补救结果， 第 19 页
- 查看邮件跟踪中的邮箱修复详细信息， 第 19 页
- 邮箱补救故障排除， 第 19 页

升级到 AsyncOS 13.0 及更高版本

在上一个 AsyncOS 版本中定义的邮箱设置在升级期间无缝迁移。此邮箱创建时，配置文件名称为 "默认"，并映射到 "所有" 域。在升级后，可以根据需要编辑此配置文件。确保您的应用可以访问

Azure Active Directory 上的 Microsoft 图 API，以从 Microsoft Exchange Online 邮箱补救消息。有关详细信息，请参阅 在 Azure AD 上将您的邮件网关注册为应用, on page 11。

监控邮箱补救结果

您可以使用“补救”(Remediation) 报告页查看邮箱补救结果的详细信息。要查看报告，请执行以下操作：

1. 点击**邮件安全设备以获得新的外观。旧 Web 界面上的“试试！！”(Try it!!)** 链接。
2. 点击**监控 (Monitoring)** 选项卡。
3. 点击**报告 (Reports)**下拉菜单并选择**补救报告 (Remediation Report)**。

使用此报告查看以下详细信息：

- 使用邮箱自动补救以及邮箱搜索和补救进行补救的邮件总数。
- 为已配置的补救操作成功补救的邮件数。
- 补救失败的邮件数。
- 有关尝试进行补救的邮件的详细信息。

有关详细信息，请参阅“补救报告”(Remediation Report) 页面一节。

查看邮件跟踪中的邮箱修复详细信息

您可以使用“邮件跟踪”(Mail Tracking) 页面中的“邮箱搜索”(Mailbox Search) 和“补救”(Remediate) 查看邮件补救的详细信息。在开始补救之前，请确保已启用邮件跟踪。

Note 尝试使用邮箱自动补救进行补救的邮件不会包含在跟踪搜索结果中。

有关所显示数据的详细信息，请参阅邮件跟踪详细信息。

邮箱补救故障排除

连接错误

问题

尝试在“帐户设置”(Account Settings) 页面（**系统管理 (System Administration)** > **帐户设置 (Account Settings)**）上检查邮件网关与收件人邮箱之间的连接时，您会收到一条错误消息：`连接不成功 (Connection Unsuccessful)`。

解决方案

根据服务器的响应，执行以下操作之一：

错误消息	原因和解决方案
`The SMTP address has no mailbox associated with it`	输入的邮件地址不属关联的邮件域。 请输入有效的邮件地址，然后再次检查连接。
`The mailbox cannot be accessed using this profile or the required permissions may be missing`	核实： • 您拥有访问用户邮箱所需的权限。使用具有 impersonator 权限的用户帐户，只能使用 Microsoft Graphic API 和 Microsoft Exchange 的内部帐户访问 Micrsoft Exchange online 帐户。 • 您选择的配置文件类型不正确。修改 "编辑帐户配置文件" 页面上的配置文件详细信息，然后再次检查连接。
`Access is denied. Check credentials and try again`	Microsoft Azure 中配置的 Office 365 应用没有访问 Microsoft Exchange Online 邮箱所需的权限。
`Application with identifier '<client_id>' was not found in the directory <tenant_id>`	输入的客户端 ID 无效。 修改 "帐户配置文件" 页面上的“客户端 ID”，然后再次检查连接。
`No service namespace named '<tenant_id>' was found in the data store.`	输入的租户 ID 无效。 修改"帐户配置文件"页面上的“租户 ID”，然后再次检查连接。
`Error validating credentials. Credential validation failed`	输入的证书指纹无效。 修改 "帐户配置文件" 页面上的证书指纹，然后再次检查连接。
`Error validating credentials. Client assertion contains an invalid signature.`	输入了错误的证书指纹，或者上传了无效或不正确的证书私钥。 核实： • 输入了正确的指纹。 • 已上传了正确的证书私钥。 • 证书私钥未到期。 • 邮件网关的时区与证书私钥中的时区匹配。
`The requested user <email address> is invalid`	输入的电子邮件地址与帐户配置文件的配置文件类型不匹配。输入有效的电子邮件地址或修改“帐户配置文件”(Account Profile) 页面上的帐户配置文件，然后再次检查连接。

错误消息	原因和解决方案
`Failed to verify exchange server(‘<host name>’) certificate. If self-signed certificate is used on exchange server install its custom CA certificate`	• 您在 Microsoft Exchange On-Premise 服务器上输入了无效的 CA 或自签名证书。验证证书并再次检查连接。 **Note** 确保您使用的证书与配置文件中提供的主机名相对应。例如，如果您在配置文件设置中提供了 Exchange 服务器的 IP 地址，并且证书基于主机名，则连接将会失败。 • 您尚未将自签名证书从 Microsoft Exchange On-Premise 服务器导入到邮件网关。有关详细信息，请参阅导入证书。
`Invalid username or password entered for exchange server (‘<email address>’)`	您已为用于连接到 Microsoft Exchange On-Premise 邮箱的 impersonator 用户帐户输入了无效的用户名或密码。）
`The account does not have permission to impersonate the requested user`	用于连接到 Microsoft Exchange On-Premise 邮箱的用户帐户不是 impersonator 角色的成员（没有 impersonator 权限）。
`Please check host <hostname> is valid exchange server address.`	您输入的 Microsoft Exchange On-Premise 服务器的主机名不正确。修改“帐户配置文件”(Account Profile) 页面上的主机名，然后再次检查连接。

查看日志

邮箱补救信息发布到下列日志：

- 邮件日志 (mail_logs)。邮箱补救过程启动的时间发布到此日志。有关邮箱自动补救或邮箱搜索和补救操作的信息：
  - 邮箱补救过程启动的时间发布到此日志。
  - 补救状态。
  - 补救失败的原因。
  - 补救成功和不成功的收件人。
  - 发起“搜索和补救”操作的来源。
  - 发起“搜索和补救”操作的用户。
  - 尝试对邮件执行的补救操作。
- 补救日志。有关补救状态、执行的操作、错误等信息都将发布到此日志中。

警报

警报：检测到邮件网关和 Microsoft Exchange 服务之间的连接问题

问题

您收到一个信息级别警报，指示邮件网关和 Microsoft Exchange Online 服务或 Microsoft Exchange On-Premise 服务之间存在连接问题，而邮件网关无法执行配置的补救操作。

解决方案

执行以下操作：

- 检查是否存在可能阻止邮件网关之间的通信和 Microsoft Exchange Online 服务或内部部署服务 Microsoft Exchange 的网络问题。

  查看邮件网关的网络设置。请参阅更改网络设置。

- 确保您的应用可以访问 Azure Active Directory 上的 Microsoft Graph API。
- 确保用于访问 Exchange 内部部署邮箱的用户帐户具有 impersonator 特权。
- 验证相应配置文件中配置的参数是否有效并测试连接。
- 检查防火墙是否存在问题。请参阅防火墙信息。
- 检查 Microsoft Exchange Online 服务或 Microsoft Exchange On-Premise 服务是否运行正常。

未执行配置补救操作

问题

从 AMP 服务器收到追溯警报后，没有对 Exchange 在线邮箱和 Exchange 内部部署邮箱中的恶意邮件执行配置的补救操作。

或

用户无法使用“邮件跟踪”(Message Tracking) 页面上的“补救”(Remediate) 选项来手动补救邮件。

解决方案

执行以下操作：

- 测试邮件网关与 Exchange 在线服务和 Exchange 内部部署服务之间的连接。请参阅创建账户配置文件 , on page 14。
- [仅适用于邮箱自动补救] 检查是否收到以下警报：检测到邮件网关和 Exchange 在线服务和 Exchange 内部部署服务之间的连接问题。请参阅警报, on page 21。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。