

配置Microsoft 365的安全邮件

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置Microsoft 365的安全邮件](#)

[在 Microsoft 365 中配置来自 Cisco Secure Email 的传入邮件](#)

[绕过垃圾邮件过滤规则](#)

[接收连接器](#)

[配置从 Cisco Secure Email 发送到 Microsoft 365 的邮件](#)

[目的控制](#)

[收件人访问表](#)

[SMTP 路由](#)

[DNS \(MX 记录 \) 配置](#)

[测试入站邮件](#)

[配置从 Microsoft 365 发送到 Cisco Secure Email 的传出邮件](#)

[在 Cisco Secure Email 网关上配置 RELAYLIST](#)

[启用 TLS](#)

[配置从 Microsoft 365 发送到 CES 的邮件](#)

[创建邮件流规则](#)

[测试出站邮件](#)

[相关信息](#)

[思科安全电邮网关文档](#)

[安全电邮云网关文档](#)

[Cisco Secure Email and Web Manager文档](#)

[Cisco Secure产品文档](#)

简介

本文档介绍将Microsoft 365与思科安全邮件集成以进行入站和出站邮件传送的配置步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Secure Email 网关或云网关
- 对思科安全邮件云网关环境的命令行界面(CLI)访问：
[思科安全邮件云网关\(Cisco Secure Email Cloud Gateway\) >命令行界面\(CLI\)访问](#)

- Microsoft 365
- 简单邮件传输协议 (SMTP)
- 域名服务器或域名系统(DNS)

使用的组件

本文档不限于特定的软件和硬件版本。

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。

背景信息

本文档可用于本地网关或思科云网关。

如果您是思科安全电邮管理员，欢迎信将包含您的云网关IP地址和其他相关信息。除了您在此处看到的信以外，还会向您发送一封加密邮件，提供有关为分配调配的云网关（也称为ESA）以及云邮件和网络管理器（也称为SMA）数量的其他详细信息。如果您尚未收到或没有收到该信件的副本，请联系ces-activations@cisco.com，提供您的联系信息和服务域名。

Your Cisco Cloud Email Security (CES) service is ready!

Organization Name: ██████████

Start Date: 2022-09-09 05:09:04 America/Los_Angeles

Below you will find information about your login credentials and other important information regarding your CES. Please retain this email for future reference

MX Records for inbound email from Internet

- mx1.██████.iphmx.com
- mx2.██████.iphmx.com

Your Cisco CES portals:

Email Security

https://dh██████-esa1.iphmx.com

Security Management

https://dh██████-sma1.iphmx.com

End User Quarantine

https://dh██████-euq1.iphmx.com

Please sign in the portals with this user ID:

Username: ██████████

Password: ██████████

Note: We recommend changing your password after the initial login.

Hostname and IP addresses to be whitelisted(for Microsoft/Office365 and G-Suite users):

Email Security:

██████.140.105

██████.150.143

██████.143.186

██████.32.98

Security Management:

██████.157.91

If you are using a Cloud service such as Office365, G-Suite, etc., you should direct your outbound emails to the address below to have them scanned by Cisco Cloud Email Security:


Host and IP address used for outbound relay from Office365 and G-Suite:


ob1.hc██████.iphmx.com

Include CES host and IP address in your SPF record:

v=spf1 exists:%{i}.spf.hc██████.iphmx.com ~all

每个客户端都有专用IP。您可以在 Microsoft 365 配置中使用已分配给您的 IP 或主机名。

 **注意：**强烈建议您在计划的生产邮件切换之前进行测试，因为在Microsoft 365 Exchange控制台中复制配置需要时间。至少等待一小时以使所有更改生效。

 **注意：**屏幕捕获中的IP地址与分配给您的分配的云网关数量成比例。例如，xxx.yy.140.105 是网关1的数据1接口IP地址，xxx.yy.150.1143 是网关2的数据1接口IP地址。网关1的数据2接口IP地址是xxx.yy.143.186，网关2的数据2接口IP地址是xxx.yy.32.98。如果您的欢迎信不包括Data 2 (传出接口IP) 的信息，请与Cisco TAC联系以将Data 2接口添加到您的分配中。

配置Microsoft 365的安全邮件

在 Microsoft 365 中配置来自 Cisco Secure Email 的传入邮件

绕过垃圾邮件过滤规则

- 登录到Microsoft 365管理中心(<https://portal.microsoft.com>)。
- 在左侧菜单中，展开 **Admin Centers**.
- 点击 **Exchange**.
- 从左侧菜单中导航至 **Mail flow > Rules**.
- 点击 [+] 以创建新规则。
- 从下拉列表中选择 **Bypass spam filtering...** 。
- 输入新规则的名称：**Bypass spam filtering - inbound email from Cisco CES**.
- 对于*Apply this rule if...，选择 **The sender - IP address is in any of these ranges or exactly matches**.
 1. 对于“指定IP地址范围”(specify IP address ranges)弹出窗口，请添加思科安全邮件欢迎信中提供的IP地址。
 2. 点击 **OK**.
- 对于*执行以下操作.....，新规则已预先选择：**Set the spam confidence level (SCL) to... - Bypass spam filtering**.
- 点击 **Save**.

规则显示方式的一个示例：

Bypass spam filtering - inbound email from Cisco CES

Name:

Bypass spam filtering - inbound email from Cisco CES

*Apply this rule if...

Sender's IP address is in the range...

add condition

*Do the following...

Set the spam confidence level (SCL) to...

add action

Except if...

add exception

Properties of this rule:

Priority:

3

Enter in the IP address(es)
associated with your Cisco
Secure Email Gateway/
Cloud Gateway



Bypass spam filtering

Mark specific messages with an SCL before they're even scanned by spam filtering. Use mail flow rules to set the spam confidence level (SCL) in messages in EOP.

Save

Cancel

接收连接器

- 保留在 Exchange 管理中心。
- 从左侧菜单中导航至 **Mail flow > Connectors**。
- 点击 [+] 以创建新连接器。
- 在“选择您的邮件流方案”弹出窗口中，选择：

1. From (发件人) : Partner organization

- 更改为 : **Office365**
- 点击 **Next**。

- 输入新连接器的名称：**Inbound from Cisco CES**.
- 您可以添加说明.
- 点击 **Next**.
- 点击 **Use the sender's IP address**.
- 点击 **Next**.
- 单击 **[+]** 并输入您的Cisco安全电子邮件欢迎信中指示的IP地址。
- 点击 **Next**.
- 选择 **Reject email messages if they aren't sent over Transport Layer Security (TLS)**.
- 点击 **Next**.
- 点击 **Save**.

连接器配置的示例如下：

Inbound from Cisco CES



Mail flow scenario

From: Partner organization

To: Office 365

Name


Inbound from Cisco CES

Status

On

[Edit name or status](#)

How to identify your partner organization

Identify the partner organization by verifying that messages are coming from these IP address ranges: 

[Edit sent email identity](#)

Security restrictions

Reject messages if they aren't encrypted using Transport Layer Security (TLS)

[Edit restrictions](#)

配置从 Cisco Secure Email 发送到 Microsoft 365 的邮件

目的控制

对目标控制中的传输域执行自我限制。当然，您可以稍后删除限制，但这些都是Microsoft 365的新IP，并且由于未知信誉，您不希望Microsoft进行任何限制。

- 登录到您的网关。
- 导航至 **Mail Policies > Destination Controls**.
- 点击 **Add Destination**.

- 使用:

1. 目标 : 输入您的域名

2. Concurrent Connections (并发连接数) : 10

- Maximum Messages Per Connection (每个连接的最大邮件数) : 20
- TLS Support (TLS 支持) : Preferred

- 点击 **Submit**.
- 点击用户界面(UI)右上角的 **Commit Changes** 以保存您的配置更改。

目标控制表的外观示例 :

Destination Control Table							Items per page 20
Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All <input type="checkbox"/> Delete
your_domain_here.com	Default	10 concurrent connections, 20 messages per connection, Default recipient limit	Preferred	Default	Default	Default	<input type="checkbox"/>
Default	IPv6 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	None	None	Off	Default	

* Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.
 ^ DANE will not be enforced for domains that have SMTP Routes configured.

收件人访问表

接下来，设置收件人访问表 (RAT) 以接受发往您的域的邮件：

- 导航至 **Mail Policies > Recipient Access Table (RAT)**.



注：根据主要邮件流的监听程序的实际名称，确保监听程序适用于传入监听程序、IncomingMail或MailFlow。

- 点击 **Add Recipient**.
- 在“Recipient Address” (收件人地址) 字段中添加您的域.
- 选择默认操作 **Accept**.

- 点击 **Submit**.
- 点击UI右上角的**Commit Changes** 以保存您的配置更改。

RAT条目显示的一个示例：

Recipient Details				
Order:	<input type="text" value="1"/>			
Recipient Address: ?	<input type="text" value="your_domain_here.com"/>			
Action:	<input type="button" value="Accept"/> <input type="checkbox"/> Bypass LDAP Accept Queries for this Recipient			
Custom SMTP Response:	<input checked="" type="radio"/> No			
	<input type="radio"/> Yes			
	<table border="1"> <tr> <td>Response Code:</td> <td><input type="text" value="250"/></td> </tr> <tr> <td>Response Text:</td> <td><div style="background-color: #cccccc; height: 100px; width: 100%;"></div></td> </tr> </table>	Response Code:	<input type="text" value="250"/>	Response Text:
Response Code:	<input type="text" value="250"/>			
Response Text:	<div style="background-color: #cccccc; height: 100px; width: 100%;"></div>			
Bypass Receiving Control: ?	<input checked="" type="radio"/> No <input type="radio"/> Yes			

SMTP 路由

设置SMTP路由以将邮件从Cisco Secure邮件传送到您的Microsoft 365域：

- 导航至 **Network > SMTP Routes**.
- 点击 **Add Route...**
- 接收域(Receiving Domain)：输入域名。
- 目标主机：添加您的原始Microsoft 365 MX记录。
- 点击 **Submit**.
- 点击UI右上角的**Commit Changes** 以保存您的配置更改。

SMTP路由设置的示例如下：

SMTP Route Settings			
Receiving Domain: ?	<input type="text" value="your_domain_here.com"/>		
Destination Hosts:	Priority ?	Destination ?	Port
	<input type="text" value="0"/>	<input type="text" value="your_domain.mail.prot"/> <small>(Hostname, IPv4 or IPv6 address.)</small>	<input type="text" value="25"/>
			<input type="button" value="Add Row"/>
			<input type="button" value="🗑"/>
Outgoing SMTP Authentication:	No outgoing SMTP authentication profiles are configured. See Network > SMTP Authentication		
<small>Note: DANE will not be enforced for domains that have SMTP Routes configured.</small>			

DNS (MX 记录) 配置

您已准备好通过邮件交换(MX)记录更改来切换域。请与DNS管理员合作，按照思科安全邮件欢迎信中的规定，将您的MX记录解析为思科安全邮件云实例的IP地址。


从Microsoft 365控制台验证对MX记录的更改：

- 登录到Microsoft 365管理控制台(<https://admin.microsoft.com>)。
- 导航至 **Home > Settings > Domains**。
- 选择您的默认域名。
- 点击Check Health。

这提供了Microsoft 365如何查找与域关联的DNS和MX记录的当前MX记录：

The screenshot shows the Microsoft 365 admin center interface. The main content area displays the 'Domains' section for a specific domain. A notification banner at the top states: 'We didn't detect that you added new records to bce-demo.com. Make sure the records you created at your host exactly match the records shown here. If they do, please wait for our system to detect the changes. This usually takes around 10 minutes, although some DNS hosting providers require up to 48 hours.' Below this, there is a link to 'Amazon Web Services (AWS)' for managing DNS records. A table titled 'Microsoft Exchange' lists DNS records:

Type	Status	Name	Value	TTL
MX	Error	@	0 mail.protection.outlook.com	1 Hour
TXT	Error	@	v=spf1 include:spf.protection.outlook.com -all	1 Hour
CNAME	OK	autodiscover	autodiscover.outlook.com	1 Hour

 **注意：**在本示例中，DNS由Amazon Web Services (AWS)托管和管理。作为管理员，如果您的DNS托管在Microsoft 365帐户以外的任何位置，您会看到一条警告。您可以忽略如下警告：“我们没有检测到您向your_domain_here.com添加了新记录。请确保在主机上创建的记录与此处所示的记录匹配...” 分步说明将MX记录重置为最初配置为重定向到您的Microsoft 365帐户的内容。这会从传入流量中删除思科安全邮件网关。

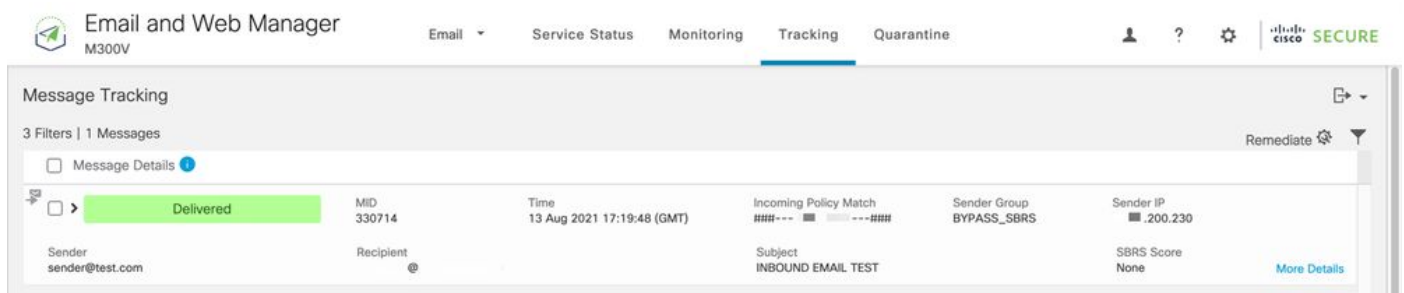
测试进站邮件

测试发送到您的Microsoft 365电子邮件地址的进站邮件。然后，检查它是否到达Microsoft 365电子邮件收件箱中。

验证实例随附的Cisco Secure Email and Web Manager（也称为SMA）的“邮件跟踪”(Message Tracking)中的邮件日志。

在 SMA 执行以下操作以查看邮件日志：

- 登录您的SMA(<https://sma.ipmx.com/ng-login>)。
- 点击 **Tracking**.
- 输入所需的搜索条件并单击 **Search**；然后希望看到以下结果：



The screenshot displays the 'Message Tracking' section of the Cisco Secure Email and Web Manager interface. It shows a table with the following columns: Message Details (with a 'Delivered' status), MID (330714), Time (13 Aug 2021 17:19:48 (GMT)), Incoming Policy Match (###- - - - -###), Sender Group (BYPASS_SBRS), and Sender IP (.200.230). Below the table, there are fields for Sender (sender@test.com) and Recipient (@). The subject of the message is 'INBOUND EMAIL TEST' and the SBRS Score is 'None'. A 'More Details' link is visible at the bottom right of the message entry.

若要在 Microsoft 365 中查看邮件日志，请执行以下操作：

- 登录到Microsoft 365管理中心(<https://admin.microsoft.com>)。
- 扩大采购 **Admin Centers**.
- 点击 **Exchange**.
- 导航至 **Mail flow > Message trace**.
- Microsoft提供了用于搜索的默认条件。例如，选择 **Messages received by my primary domain in the last day**以开始搜索查询。
- 为收件人输入所需的搜索条件，然后点击 **Search** 并期望看到类似以下内容的结果：

Message trace > Message trace search results

Export results Edit message trace Refresh 2 items Search


Date (UTC-05:00) ↓	Sender	Recipient	Subject	Status
8/13/2021, 1:20 PM	sender@test.com		INBOUND EMAIL TEST	Delivered

配置从 Microsoft 365 发送到 Cisco Secure Email 的传出邮件

在 Cisco Secure Email 网关上配置 RELAYLIST

请参阅您的思科安全电邮欢迎函。此外，为通过网关的出站消息指定辅助接口。

- 登录到您的网关。
- 导航至 **Mail Policies > HAT Overview**。

 **注意：**根据外部/出站邮件流的侦听程序的实际名称，确保侦听程序用于出站侦听程序、OutgoingMail或MailFlow-Ext。

- 点击 **Add Sender Group...**
- 将发件人组配置为：


1. 名称：RELAY_O365

2. 注释：<<如果您希望通知发件人组，请输入注释>>

3. 策略：已中继

4. 点击 **Submit and Add Senders**。

- 发件人：.protection.outlook.com

 **注意：**。号需要放在发件人域名开头。

- 点击 **Submit**.
- 点击UI右上角的 **Commit Changes** 以保存您的配置更改。

“发件人组设置”(Sender Group Settings)的示例如下：

Sender Group Settings	
Name:	RELAY_O365
Order:	1
Comment:	From Microsoft 365 mail to Cisco Secure Email
Policy:	RELAYED
SBRS (Optional):	Not in use
External Threat Feed (Optional): <i>For IP lookups only</i>	None
DNS Lists (Optional):	None
Connecting Host DNS Verification:	None Included
<< Back to HAT Overview Edit Settings...	

Find Senders	
Find Senders that Contain this Text: ?	<input type="text"/> Find

Sender List: Display All Items in List		Items per page 20 ▼
Add Sender...		
Sender	Comment	All <input type="checkbox"/> Delete
.protection.outlook.com	From Microsoft 365 mail to Cis...	<input type="checkbox"/>
<< Back to HAT Overview		Delete

启用 TLS

- 点击 [<<Back to HAT Overview](#).
- 点击邮件流策略：**RELAYED**.
- 向下滚动，在 **Security Features** 部分中查找 **Encryption and Authentication**.
- 对于 TLS，请选择：**Preferred**.
- 点击 **Submit**.
-

点击UI右上角的Commit Changes 以保存您的配置更改。

邮件流策略配置示例如下：

Encryption and Authentication:	TLS:	<input type="radio"/> Use Default (Off) <input type="radio"/> Off <input checked="" type="radio"/> Preferred <input type="radio"/> Required
	TLS is Mandatory for Address List:	None ▾
	<input type="checkbox"/> Verify Client Certificate	
	SMTP Authentication:	<input checked="" type="radio"/> Use Default (Off) <input type="radio"/> Off <input type="radio"/> Preferred <input type="radio"/> Required
	If Both TLS and SMTP Authentication are enabled:	<input type="checkbox"/> Require TLS To Offer SMTP Authentication

配置从 Microsoft 365 发送到 CES 的邮件

- 登录到Microsoft 365管理中心(<https://admin.microsoft.com>)。
- 扩大采购 Admin Centers.
- 点击 Exchange.
- 导航至 Mail flow > Connectors.
- 单击[+]创建新连接器。
- 在“选择您的邮件流方案”弹出窗口中，选择：

1. From (发件人) : Office365

- 更改为 : Partner organization

- 点击 Next.
- 输入新连接器的名称 : Outbound to Cisco CES.
- 您可以添加说明.
- 点击 Next.
- 对于何时要使用此连接器？ :

1. 选择 : Only when I have a transport rule set up that redirects messages to this connector.

- 点击 Next.

- 点击 **Route email through these smart hosts**.
- 点击 [+] 并输入CES欢迎信中提供的出站IP地址或主机名。
- 点击 **Save**.
- 点击 **Next**.
- Office 365应如何连接到合作伙伴组织的电子邮件服务器？

1. 选择：**Always use TLS to secure the connection (recommended)**.

- 选择 **Always use TLS to secure the connection (recommended)**。Any digital certificate, including self-signed certificates
- 点击 **Next**.
- 系统将显示确认屏幕。
- 点击 **Next**.
- 使用 [+] 输入有效的电子邮件地址，然后单击 **OK**.
- 点击 **Validate** 并允许运行验证。
- 完成后，点击 **Close**.
- 点击 **Save**.

Outbound Connector的外观示例：

Outbound to Cisco CES



Mail flow scenario

From: Office 365

To: Partner organization

Name

Outbound to Cisco CES

Status

On

[Edit name or status](#)

Use of connector

Use only when I have a transport rule set up that redirects messages to this connector.

[Edit use](#)

Routing

Route email messages through these smart hosts:   .iphmx.com

[Edit routing](#)

Security restrictions

Always use Transport Layer Security (TLS) and connect only if the recipient's email server has a digital certificate.

[Edit restrictions](#)

Validation

Last validation result: Validation successful

Last validation time: 10/5/2020, 9:08 AM

[Validate this connector](#)

1. 对于“选择发件人位置”弹出窗口，选择：**Inside the organization.**

- 点击 **OK.**

- 点击 **More options...**

- 点击 **add condition** 按钮并插入第二个条件：

1. 选择 **The recipient...**

- 选择：**Is external/internal.**
- 对于“选择发件人位置”弹出窗口，选择：**Outside the organization .**
- 点击 **OK.**

- 对于*执行以下操作.....，选择：**Redirect the message to...**

1. 选择：**以下连接器。**

2. 并选择**Outbound to Cisco CES**连接器。

3. Click **OK.**

- 返回“*请执行以下操作.....”并插入第二个操作：

1. 选择：**Modify the message properties...**

- 选择：**set the message header**
- 设置邮件信头：**X-OUTBOUND-AUTH.**
- 点击 **OK.**
- 设置值：**mysecretkey.**

- 点击 **OK**.

- 点击 **Save**.

 **注意：**为防止来自Microsoft的未授权邮件，当邮件离开Microsoft 365域时，可以对x信头加密签名；在将信头传送到互联网之前，系统会评估和删除此信头。

Microsoft 365路由配置的示例如下：

Outbound to Cisco CES

Name:

Outbound to Cisco CES

*Apply this rule if...

The sender is located... ▼

[Inside the organization](#)

and

The recipient is located... ▼

[Outside the organization](#)

add condition

*Do the following...

Set the message header to this value... ▼

Set the message header '[X-OUTBOUND-AUTH](#)' to the value '[mysecretkey](#)'.

and

Use the following connector... ▼

[Outbound to Cisco CES](#)

add action

Except if...

add exception

Properties of this rule:

Priority:

0

Audit this rule with severity level:

Not specified ▼

Choose a mode for this rule:

Enforce

Test with Policy Tips

Test without Policy Tips

Activate this rule on the following date:

Fri 8/13/2021 ▼

1:30 PM ▼

Deactivate this rule on the following date:

Fri 8/13/2021 ▼

1:30 PM ▼

Stop processing more rules

Defer the message if rule processing doesn't complete

Match sender address in message:

Header ▼

Add to DLP policy

PCI ▼

Comments:

```
office365_outbound: if sendergroup == "RELAYLIST" {  
  if header("X-OUTBOUND-AUTH") == "^mysecretkey$" {  
    strip-header("X-OUTBOUND-AUTH");  
  } else {  
    drop();  
  }  
}
```

- 按回车键一次以创建新的空白行。
- 在新行中输入 [.] 以结束新邮件过滤器。
- 单击 **return** 一次退出“过滤器”菜单。
- 运行 **Commit** 命令以保存对配置所做的更改。



注意：避免使用密钥的特殊字符。邮件过滤器中显示的^和\$为正则表达式字符，如示例中所示。



注意：请复习如何配置RELAYLIST的名称。可以使用备用名称进行配置，也可以使用基于中继策略或邮件提供商的特定名称。

测试出站邮件

测试从您的Microsoft 365电子邮件地址发送到外部域收件人的出站邮件。您可以查看Cisco Secure Email and Web Manager中的邮件跟踪，以确保将其正确路由到出站。

 **注意：**检查网关上的TLS配置(系统管理(System Administration) > SSL配置)和用于出站SMTP的密码。思科最佳实践建议：



HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSL

成功传送的跟踪示例：

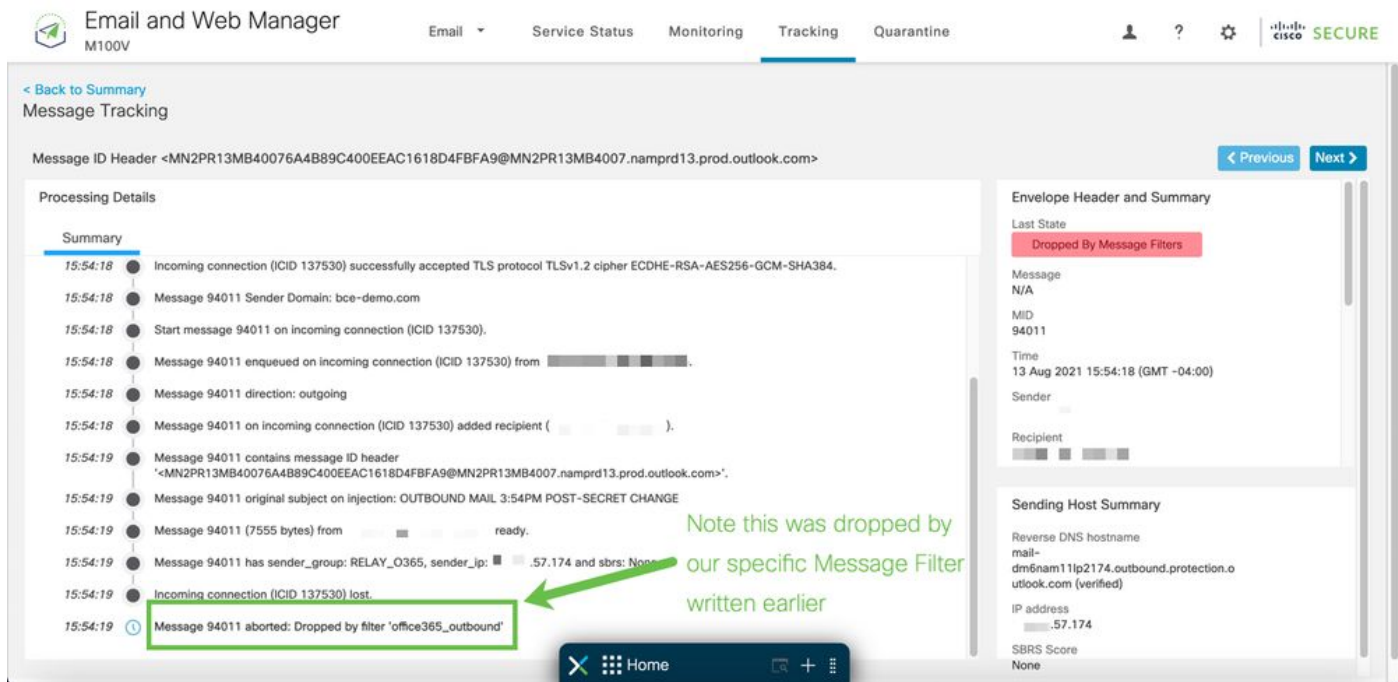
The screenshot shows the 'Tracking' tab in the Email and Web Manager interface. A message with MID 186371, 186372 is shown as 'Delivered'. The time is 13 Aug 2021 14:14:59 (GMT -04:00). The outgoing policy match is '>>_<<<'. The sender group is 'RELAY_O365' and the sender IP is '59.175'. The subject is 'OUTBOUND EMAIL TEST' and the SBRS score is 'None'. Annotations include a green arrow pointing to the 'Sender Group' and a blue arrow pointing to the 'Sender IP'.

点击More Details 可查看完整的消息详细信息：

The screenshot shows the 'More Details' view for the message tracking entry. It includes a 'Processing Details' section with a 'Summary' of events from 14:14:59 to 14:15:00. The events describe the incoming connection, SMTP interface data, policy match, TLS protocol acceptance, and message enqueueing. The 'Envelope Header and Summary' section shows the last state as 'Delivered', message type as 'Outgoing', and the sender IP as '59.175'. The 'Sending Host Summary' section shows the reverse DNS hostname as 'mail-dm6nam12lp2175.outbound.protection.outlook.com (verified)' and the IP address as '59.175'.

X 信头不匹配的邮件跟踪示例：

The screenshot shows the 'Tracking' tab in the Email and Web Manager interface. A message with MID 94011 is shown as 'Dropped By Message Filters'. The time is 13 Aug 2021 15:54:18 (GMT -04:00). The policy match is 'N/A'. The sender group is 'RELAY_O365' and the sender IP is '59.174'. The subject is 'OUTBOUND MAIL' and the SBRS score is 'None'.



相关信息

思科安全电邮网关文档

- [版本说明](#)
- [用户指南](#)
- [CLI参考指南](#)
- [思科安全邮件网关API编程指南](#)
- [思科安全邮件网关中使用的开源](#)
- [思科内容安全虚拟设备安装指南 \(包括vESA\)](#)

安全电邮云网关文档

- [版本说明](#)
- [用户指南](#)

Cisco Secure Email and Web Manager文档

- [版本说明和兼容性列表](#)

- [用户指南](#)
- [Cisco Secure Email and Web Manager API编程指南](#)
- [思科内容安全虚拟设备安装指南 \(包括vSMA \)](#)

Cisco Secure产品文档

- [思科安全产品组合命名架构](#)

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）。