消息

“邮件”(Messages) 页面会显示您的邮件和搜索结果，并允许您查找可能的威胁。每页最多可以显示 100 封邮件。

邮件页面图标

下表显示了“邮件”(Messages) 页面上使用的图标及其含义。

表 1　　邮件页面图标

图标	名称	说明
	链接	邮件包含链接。
	附件	邮件包含附件。
	手动补救或手动重新分类	邮件已手动补救或重新分类。如果邮件经过了补救，则会在“操作”(Action) 旁边显示图标；如果对邮件进行了重新分类，则会在“判定”(Verdict) 旁边显示图标。
	追溯性判定	“追溯性判定”已被应用。“追溯性判定”是在 Secure Email Threat Defense 首次扫描邮件后应用的判定。
	允许	根据指示的项目允许邮件：允许列表、MS 允许列表或安全发件人。
	判定覆盖	判定已根据“判定覆盖”邮件规则被覆盖。
	绕过分析	由于存在绕过分析邮件规则，邮件未经过分析。指明规则的类型，即“安全发件人”或“网络钓鱼测试”。
	BEC	邮件已被手动或通过自动补救标记为“商业电子邮件泄露 (BEC)”。
	诈骗	邮件已被手动或通过自动补救标记为“诈骗”。
	网络钓鱼	邮件已被手动或通过自动补救标记为“网络钓鱼”。
	恶意	邮件已被手动或通过自动补救标记为“恶意”。
	垃圾邮件	邮件已被手动或通过自动补救标记为“垃圾邮件”。
	灰色邮件	邮件已被标记为“灰色邮件”。灰色邮件是指已被确定为营销邮件、社交邮件或垃圾邮件。
	一般	邮件已标记为“中性”。

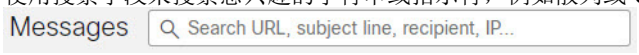
表 1　　邮件页面图标

图标	名称	说明
	传入	从 O365 租户之外收到的邮件。
	内部	发送给您的 O365 租户的邮件。
	混合	内部和外部收件人的邮件。
	传出	发送给 O365 租户之外的收件人的邮件。

搜索和过滤

使用日历控件来显示定义的时间段（最近的日、周或月）或过去 90 天内某个自定义时间范围内的数据。

使用搜索字段来搜索感兴趣的字符串或指示符，例如散列或 URL。

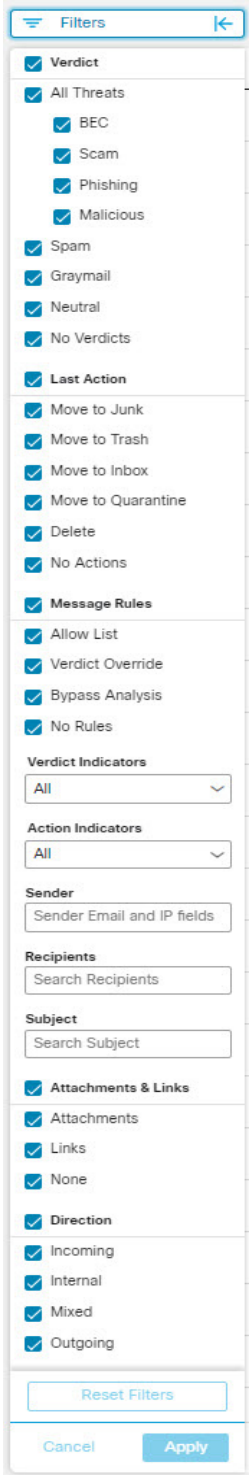


过滤器面板

使用以下过滤器来缩小搜索结果范围：例如，您可能希望查看从特定发件人发送的所有邮件、具有特定判定的邮件、包含附件或链接的邮件、已重新分类的邮件或已移至“垃圾邮件”的邮件。

1. 点击箭头以展开过滤器面板。

2. 进行选择，然后点击**应用 (Apply)**。请注意，您必须在“判定”(Verdict) 下至少选择一个项目。



使用**重置过滤器 (Reset Filters)** 按钮将过滤器重置为其默认设置。

邮件图形和快速过滤器

“邮件”(Messages) 页面顶部的邮件图形和快速过滤器可提供邮件流量的图形视图。使用该图形可快速过滤邮件。该图形包括：

- 威胁和类别分组，用于查看威胁总数并轻松过滤威胁
- 隔离区总数，可用于过滤隔离的项目
- 邮件方向总计，可用于按方向快速进行过滤

判定结果

安全邮件威胁防御会将以下威胁判定应用于邮件：

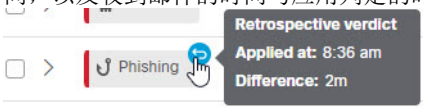
- **BEC：**商业邮件感染 (BEC) 是一种复杂的骗局，它利用社交工程和入侵技术对组织造成经济损失。
- **诈骗：**诈骗的重点是利用彩票或勒索欺诈等手段对个人造成经济损失。
- **网络钓鱼：**这些邮件被判定为欺诈性复制或模仿合法服务，试图获取用户名、密码、信用卡号等敏感信息。
- **恶意：**这些邮件会被判定为包含、提供或支持恶意软件的传送或传播。

追溯性判定

追溯性判定是在 Secure Email Threat Defense 首次扫描邮件后的某个时间应用于邮件的判定。

Secure Email Threat Defense 中的追溯性判定与其他思科安全产品中的判定略有不同。虽然 Secure Email Threat Defense 并非内联邮件处理器，但它具有完成邮件初始分析的固定时间范围。分析时间较长的较新内容引擎（例如 Talos 的深度 URL 分析）会被视为追溯性判定。由于判定被延迟，补救也会随之延迟。因此，Secure Email Threat Defense 可以清楚地标记这些判定。

追溯性判定在判定旁边的“邮件”(Messages) 页面上用蓝色图标表示。将光标悬停在图标上即可查看应用追溯性判定的时间，以及收到邮件的时间与应用判定的时间之间的差异。



追溯性判定邮件通知

要打开或关闭追溯性判定的邮件通知，请执行以下操作：

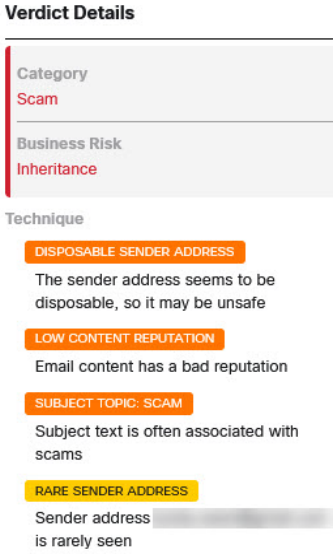
1. 选择**设置**（齿轮图标）> **管理 (Administration)** > **企业 (Business)**。
2. 在**通知邮件地址 (Notification Email Address)** 下，选择或取消选择**发送追溯性判定通知 (Send Notifications for Retrospective Verdicts)**。

如果选中此复选框，则追溯性判定邮件通知将被发送到指定的通知邮件地址。这些通知会默认处于关闭状态。

展开的邮件视图

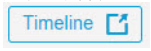
要对“邮件”(Messages) 页面搜索结果中的邮件进行调查，请选择 **>** 图标以展开邮件并查看更多详细信息，包括判定详细信息、发件人 IP、Microsoft 邮件 ID、附件、链接等。通过该视图还可以访问“时间表”(Timeline)、“对话视图”(Conversation View) 和“EML 下载”(EML Downloads)。

“判定详细信息”(Verdict Details) 列将显示判定、业务风险和使用的技术的直观表示。技术采用了颜色编码，以表明其严重性。 恶意文件名/SHA256 和 URL 会在可用时动态显示。如果无法使用动态文本，则会显示静态说明。



时间表

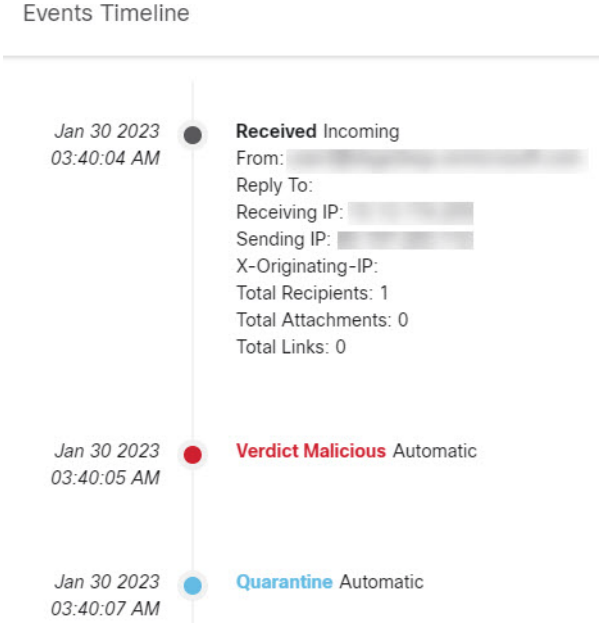
展开邮件后，点击右上角的**时间表 (Timeline)** 按钮即可查看特定邮件的事件时间表。



事件时间表会显示：

- **已接收 (Received)**：收到邮件的时间以及邮件相关详细信息
- **判定 (Verdict)**：有关所呈现的任何判定的信息
- **操作 (Action)**：有关对邮件执行的任何操作的信息

- **规则 (Rule)**：有关已应用的任何邮件规则的信息



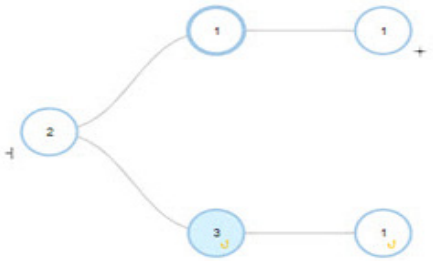
对话视图

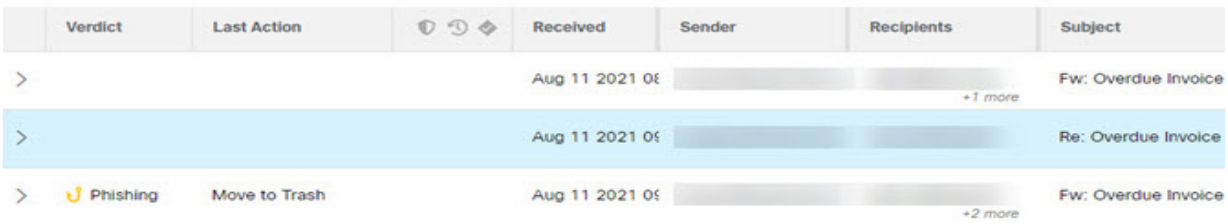
对话视图提供对话的整体视图。使用对话视图可跟踪对话中的邮件，同时全面了解邮件流。这在确定威胁的来源及其在组织内的传播方式时非常有用。

展开邮件后，点击**对话视图 (Conversation View)** 按钮即可查看与特定邮件相关的邮件。

点击 **+** 图标可展开对话的节点，以便您查看对话中更早或更晚的邮件。展开的节点将被添加到节点下方显示的邮件网格中。节点和邮件采用了颜色编码，以表示传入、传出、混合或内部。

节点圆圈内的数字表示邮件被发送到的地址数量。节点中的图标表示是否检测到威胁。在选择节点时，网格中的相应邮件会被突出显示。





SecureX Pivot 菜单

如果您的思科安全邮件威胁防御业务与SecureX集成，则可以从展开的邮件视图中访问SecureX透视菜单。有关与SecureX集成的信息，请参阅SecureX，第 49 页。

移动和重新分类邮件

如果您认为邮件分类不正确，请使用“邮件”(Messages) 页面来移动或重新分类邮件。通过更改每页显示的邮件数，一次最多可以移动或重新分类 100 封邮件。

注意：重新分类只会影响对所选邮件的判定。它不会指明来自所选发件人的未来邮件或基于邮件内容的任何更改。邮件将排队等待思科 Talos 审核。Talos 可能会使用反馈来影响未来的分类。对于误报的垃圾邮件或灰色邮件，请考虑添加判定覆盖规则，第 46 页。

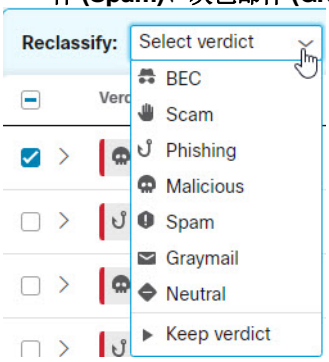
关于混合 Exchange 帐户

Secure Email Threat Defense 只能对 Exchange Online (O365) 中的邮箱执行。如果您正在将邮箱从现场 Exchange 迁移到ExchangeOnline(O365)，则补救（移动或删除）将仅适用于ExchangeOnline(O365)中的邮箱。您不会收到现场Exchange邮箱补救失败的通知。

读取补救模式

如果处于“读取”模式，则可以对邮件重新分类（应用不同的判定）。

1. 选择要重新分类的邮件。
2. 从下拉菜单中选择判定。您可以将邮件重新分类为**BEC**、**诈骗 (Scam)**、**网络钓鱼 (Phishing)**、**恶意 (Malicious)**、**垃圾邮件 (Spam)**、**灰色邮件 (Graymail)** 或**中性 (Neutral)**，或者也可以选择**保留判定 (Keep verdict)**。



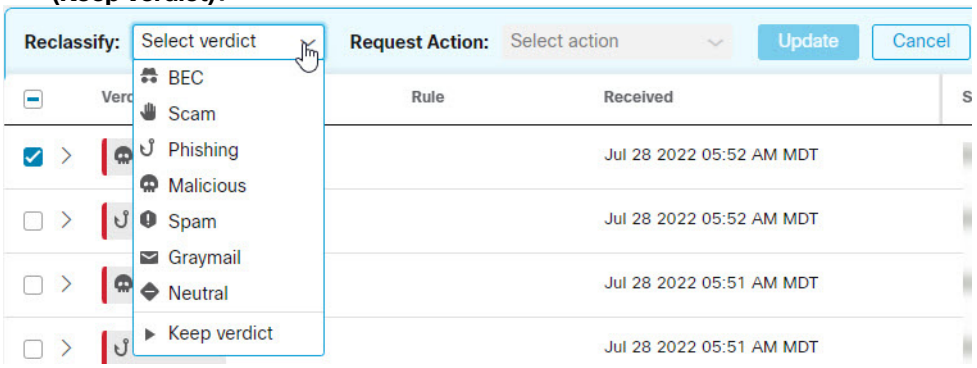
3. 点击**更新 (Update)** 以应用新分类。

读/写补救模式

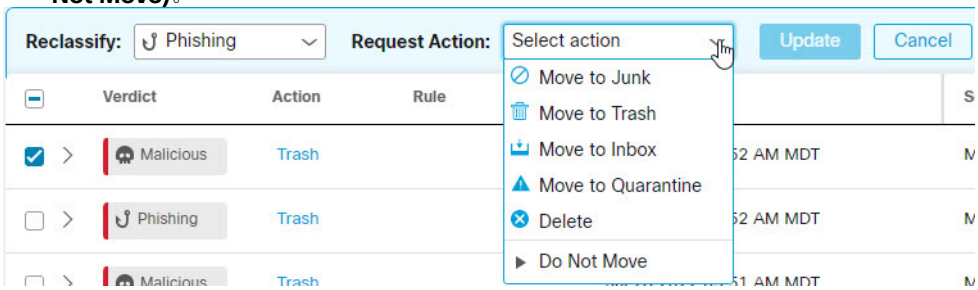
如果处于读/写补救模式，则可以将可疑邮件从用户收件箱移至其垃圾邮件或垃圾桶，或移至其无法访问的隔离区文件夹。同样，如果您确定被移至垃圾邮件、垃圾桶或隔离区的邮件并无可疑之处，则可以将其移回用户的收件箱。您也可以彻底删除邮件。该过程还允许您对邮件重新分类（应用不同的判定）。

1. 选择要移动或重新分类的邮件。

2. 从“重新分类”(Reclassify) 下拉菜单中选择判定。您可以将邮件重新分类为 **BEC**、**诈骗 (Scam)**、**网络钓鱼 (Phishing)**、**恶意 (Malicious)**、**垃圾邮件 (Spam)**、**灰色邮件 (Graymail)** 或**中性 (Neutral)**，或者也可以选择**保留判定 (Keep verdict)**。



3. 从“请求操作”(Request Action) 下拉菜单中选择操作。您可以选择**移至垃圾邮件 (Move to Junk)**、**移至垃圾桶 (Move to Trash)**、**移至收件箱 (Move to Inbox)**、**移至隔离区 (Move to Quarantine)**、**删除 (Delete)**，或者也可以选择**不移动 (Do Not Move)**。



4. 点击**更新 (Update)** 以应用新分类并对邮件执行操作。

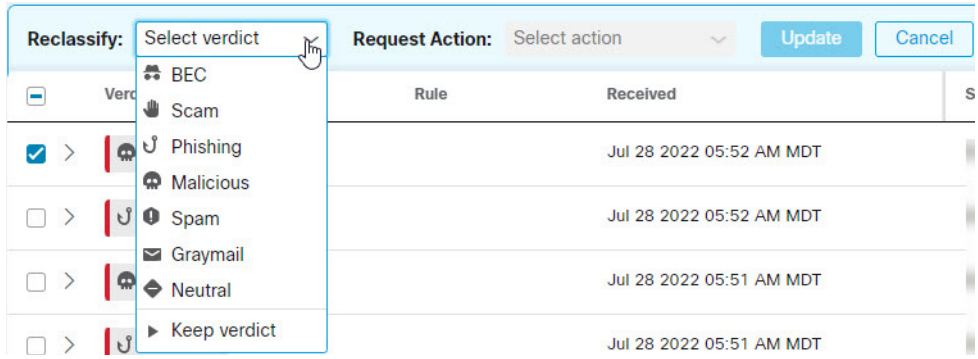
如果邮件已被移动，则会在**上次操作 (Last Action)** 列中指明。

删除邮件

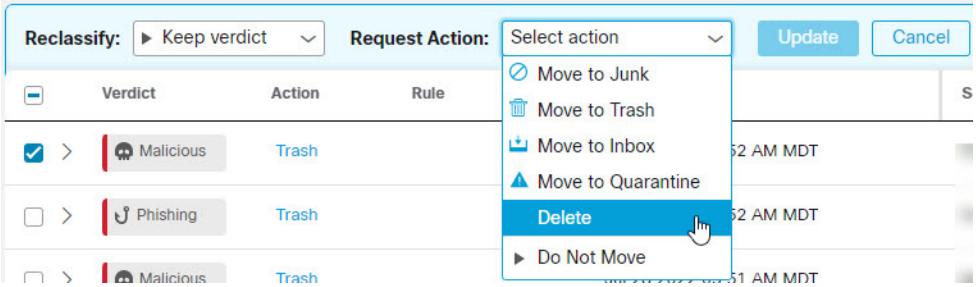
超级管理员和管理员用户可以使用“重新分类/补救”工作流程中的“删除”操作从邮箱中永久删除邮件。已删除的邮件会被移至 **recoverableitemspurges** 文件夹。用户无法访问此文件夹，并且 Secure Email Threat Defense 无法将已删除的邮件恢复到收件箱。

1. 选择要删除的邮件。

2. 从“重新分类”(Reclassify) 下拉菜单中选择判定。您可以将邮件重新分类为 **BEC**、**诈骗 (Scam)**、**网络钓鱼 (Phishing)**、**恶意 (Malicious)**、**垃圾邮件 (Spam)**、**灰色邮件 (Graymail)** 或**中性 (Neutral)**，或者也可以选择**保留判定 (Keep verdict)**。



3. 从“请求操作”(Request Action) 下拉菜单中选择**删除 (Delete)**。



4. 点击**更新 (Update)** 以删除邮件。

5. “确认删除”(Confirm Deletion) 对话框指明邮件无法恢复，并确认是否要继续。点击**删除 (Delete)** 以继续。

上次操作 (Last Action) 列中会指明“删除”(Delete)。

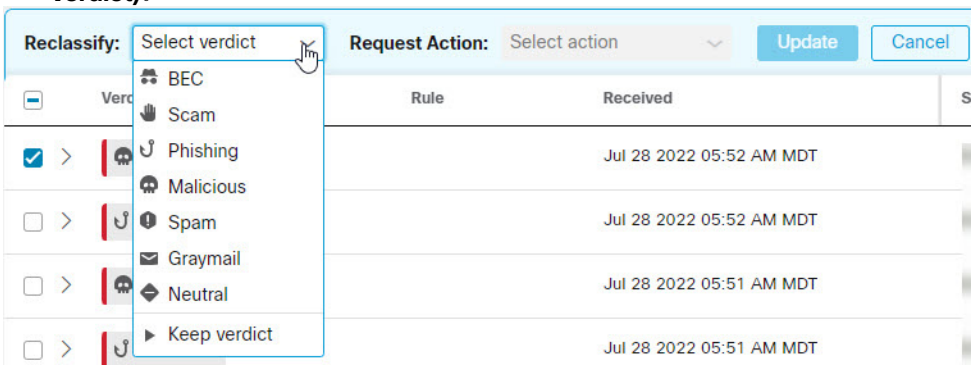
隔离邮件

隔离区文件夹是为每个邮箱自动创建的，并且 Outlook 用户不会看到该文件夹。超级管理员和管理员用户可以在**管理 (Administration) > 企业 (Business)** 页面中看到隐藏文件夹的名称。在 Outlook 中，隔离区文件夹中的邮件将根据您的“已删除邮件”(Deleted Items) 清除设置自动进行清除。Secure Email Threat Defense 当邮件从隔离区文件夹中清除后，其无法再被恢复到用户收件箱。

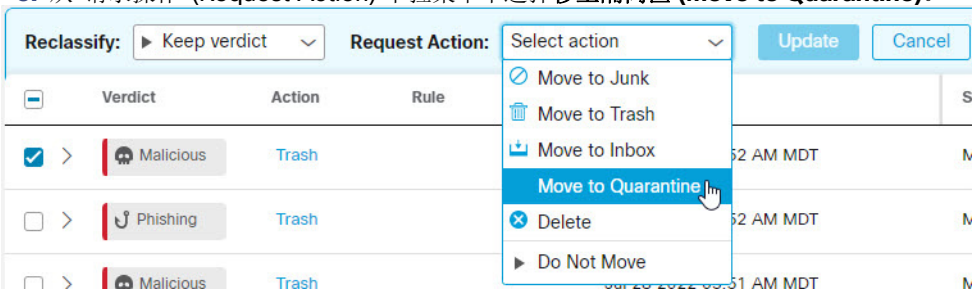
要将邮件手动移动至隔离区，请执行以下操作：

1. 选择要移至隔离区的邮件。

2. 从“重新分类”(Reclassify) 下拉菜单中选择判定。您可以将邮件重新分类为 **BEC**、**诈骗 (Scam)**、**网络钓鱼 (Phishing)**、**恶意 (Malicious)**、**垃圾邮件 (Spam)**、**灰色邮件 (Graymail)** 或**中性 (Neutral)**，或者也可以**保留判定 (Keep verdict)**。



3. 从“请求操作”(Request Action) 下拉菜单中选择**移至隔离区 (Move to Quarantine)**。



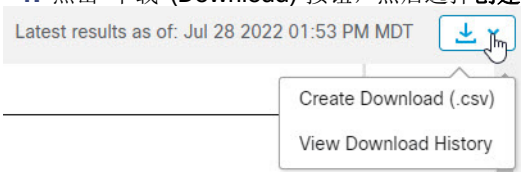
4. 点击**更新 (Update)** 以隔离邮件。

上次操作 (Last Action) 列中会指明“移至隔离区”(Move to Quarantine)。

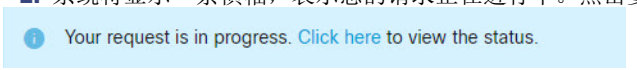
下载搜索结果

您可以将搜索结果中邮件数据作为 CSV 文件进行下载。下载限制为 10,000 封邮件。要下载数据，请完成以下步骤：

1. 点击“下载”(Download) 按钮，然后选择**创建下载 (.csv) (Create Download [.csv])**。



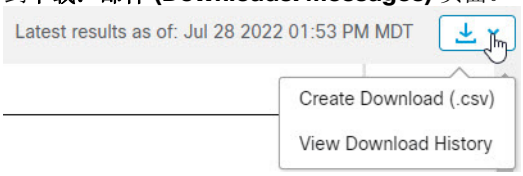
2. 系统将显示一条横幅，表示您的请求正在进行中。点击要转到**下载：邮件 (Downloads: Messages)** 页面的文本。



3. 当下载就绪时，点击“操作”(Actions) 列下的“下载”(Download) 图标以下载文件。

下载历史

您的下载历史记录将保留 90 天。点击“下载”(Download) 按钮，然后选择**查看下载历史记录 (View Download History)** 以转到**下载：邮件 (Downloads: Messages)** 页面。



该页面会显示日期范围、请求下载的用户、启动日期和状态。通过选择“操作”(Actions) 列下的“下载”(Download) 图标下载文件。

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。