如何在思科安全访问(SA)和思科邮件威胁防御(ETD)中配置邮件DLP策略

目录

简介

电子邮件仍是无意或未经授权的数据暴露最常见的渠道之一。为帮助组织保护通过邮件共享的敏感

信息，思科通过集成思科安全访问(SA)和思科邮件威胁防御(ETD)，提供邮件数据丢失防护(DLP)功能。

在此架构中，所有邮件DLP策略的创建、配置和实施操作都在思科安全访问中执行。思科电邮威胁防御提供电邮可视性和邮件跟踪，而思科安全访问则充当用于定义DLP规则和实施行为的策略引擎。

本文解释如何使用预定义的DLP模板或自定义DLP模板，在思科安全访问中创建邮件DLP策略。

先决条件

开始配置过程之前，请确保满足以下要求：

- 管理访问：您必须对思科邮件威胁防御内联控制台和思科安全访问控制台具有“完全管理员”权限。
- 活动订用：确保您的邮件威胁防御和安全访问租户均处于活动状态且已调配。
- 连接：必须成功建立邮件威胁防御和安全访问之间的API集成。
- 邮件流配置：邮件威胁防御必须正确部署在内联模式中，以确保它主动检查邮件流量。

重要信息：虽然此解决方案同时使用思科安全访问和思科邮件威胁防御，但本文中介绍的所有邮件DLP规则配置步骤都仅在思科安全访问中执行。

要求和使用的组件

要成功实施邮件DLP策略，需要使用以下组件：

- 思科邮件威胁防御(ETD):充当邮件检查点。它捕获出站邮件流量并促进DLP引擎执行分析所需的通信流。
- 思科安全访问(SA)- DLP引擎：这是所有DLP配置驻留的主要组件。您将使用Secure Access控制台定义：
  - 数据标识符：系统应监控的特定模式或敏感数据类型（例如PII、信用卡号或内部项目代码）。
  - DLP策略：规定系统在检测到敏感数据（例如阻止、加密或通知）时如何反应的规则。
  - 策略操作：由DLP引擎触发的自动响应，例如阻止发送邮件或应用强制加密。
- 集成框架：允许ETD将邮件元数据移交给安全访问DLP引擎以进行策略评估和后续实施的后端连接。

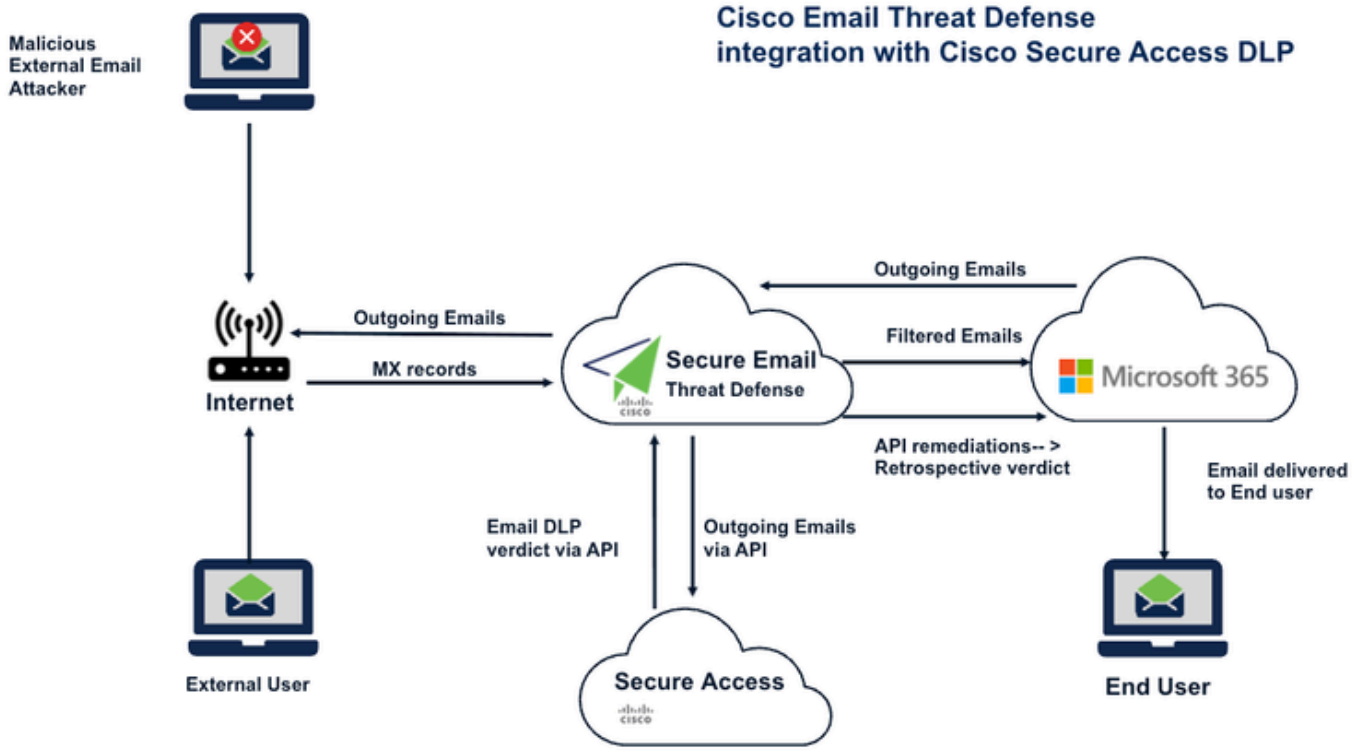
邮件DLP策略功能

在思科安全访问中创建邮件DLP策略时，可以配置：

- 规则名称和说明
- 严重级别
- 数据分类
- 检查范围，包括：
    - 电子邮件主题
    - 邮件正文
    - 附件名称
    - 附件内容
- 文件控制，包括：
    - MIP标签
    - Titus标签
- 发件人条件
- 收件人条件
- 策略操作：
    - 监控
    - 阻止
- 可选的用户通知

网络图

找到以下网络图，说明思科安全邮件威胁防御与思科安全访问的集成，以及流量流程图。



NOTE:在上图中，交换服务器是O365，但此DLP配置可以在支持SMTP的任何Exchange服务器上完成。

NOTE:请参阅文章“Steps to integrate Cisco Email Threat Defense(ETD)with Cisco Secure Access:(将思科电邮威胁防御(ETD)与思科安全访问集成的步骤：)”以通过API集成思科电邮威胁防御和思科安全访问。

配置

在思科安全访问中配置邮件DLP策略

步骤 1：登录思科安全访问

使用具有所需权限的管理员帐户登录到Cisco Secure Access(SA)控制台。

步骤 2：导航到Email DLP Rule Creation

从Secure Access控制面板导航至：

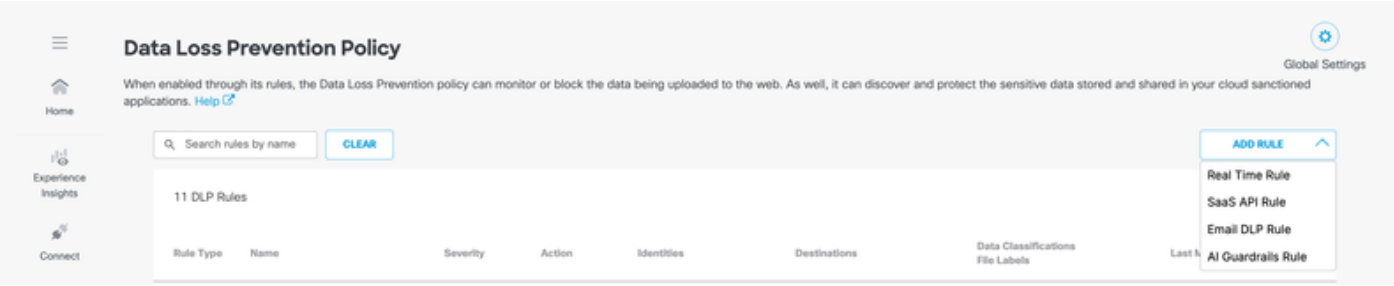
Secure > Policy > Data Loss Prevention Policy > Add Rule > Email DLP Rule

这将打开Add New Email Rule页。

思科安全访问提供两种创建邮件DLP规则的方法：

- 使用预定义的DLP模板创建邮件DLP规则
- 使用自定义DLP模板创建邮件DLP规则

图1.导航至邮件DLP规则创建



选项 1：使用预定义的DLP模板创建邮件DLP规则

步骤 3：配置基本规则信息

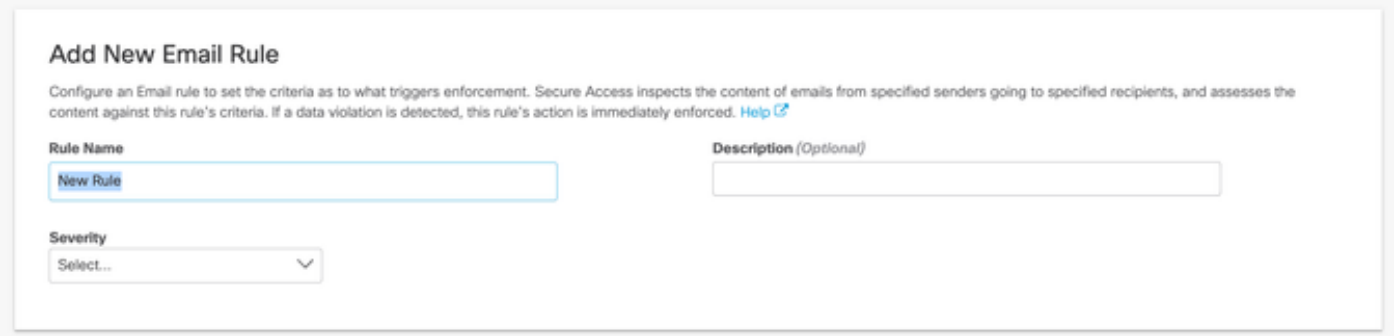
导航至ADD RULE > Email DLP Rule窗口，

在Add New Email Rule窗口中，输入以下详细信息：

- 规则名称
  输入邮件DLP规则的描述性名称。
- 描述
  简要总结规则的用途。
- 严重级别
  为策略选择相应的严重性级别：
  - 低

- 中
- 高
- 关键

这些字段有助于对规则进行分类，以实现管理、报告和操作可视性。



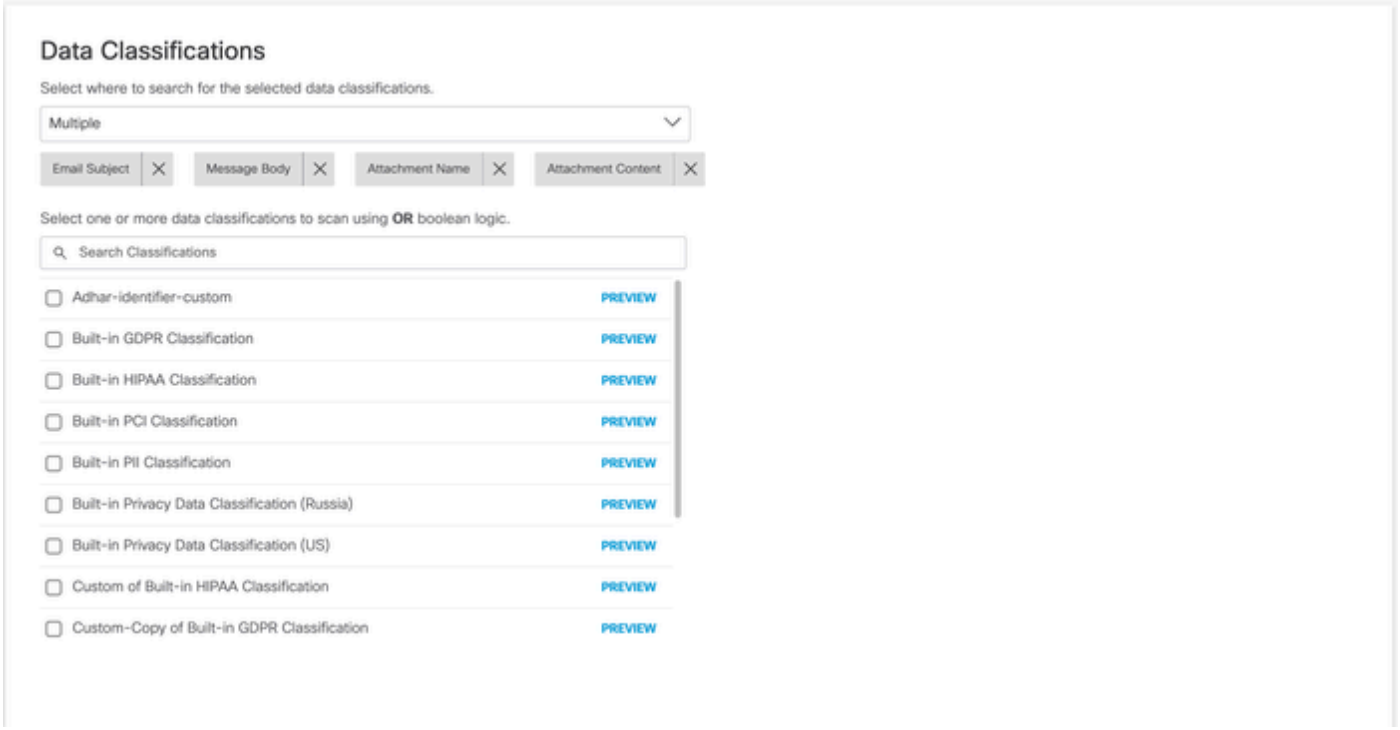
步骤 4：选择数据分类

在Data Classifications下，选择用于检查邮件内容是否存在潜在DLP违规的预定义DLP模板。

接下来，选择应匹配所选分类的位置。支持的检测位置包括：

- 电子邮件主题
- 邮件正文
- 附件名称
- 附件内容

这样，策略可以检查邮件内容和附件中的敏感信息。



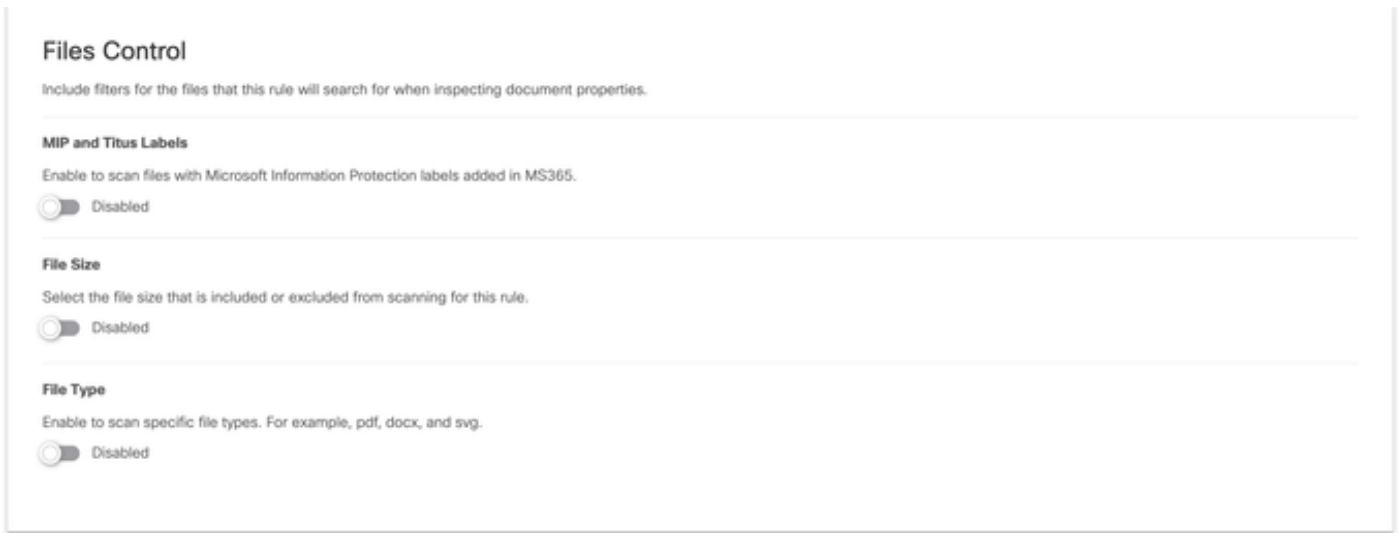
步骤 5：配置文件控制

在Files Control下，配置规则的基于文件的检查条件。

其中包括以下支持：

- MIP标签
- Titus标签

当DLP实施必须考虑与附加文件关联的敏感度标签或元数据时，这些设置非常有用。



步骤 6：定义发件人范围

在发件人部分中，指定策略应用于哪些发件人。

可用选项包括：

- 所有发件人
- 特定发件人
- 排除特定发件人

这样，您就可以广泛应用规则，或者将规则限制为选定用户或组。

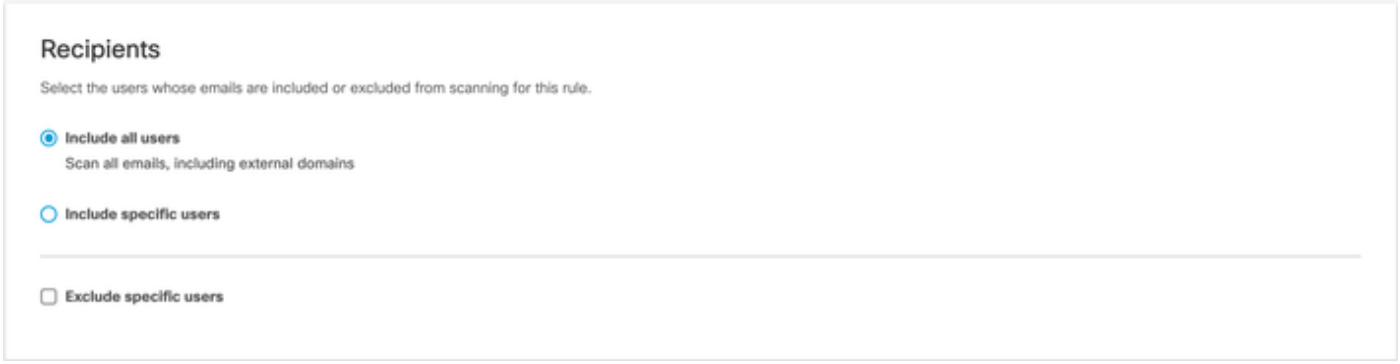
步骤 7：定义收件人范围

在Recipients部分中，选择应包括在策略评估中或从策略评估中排除的用户或组。

可用选项包括：

- 包括所有用户
- 包括特定用户
- 排除特定用户

这有助于根据预期收件人定制策略实施。



步骤 8::选择策略操作

在操作部分中，选择思科安全访问应如何处理被明确标识为违反DLP规则的邮件。

可用操作包括：

- 监控
  允许使用电子邮件，并记录事件以进行可视性和报告。
- 阻止
  邮件被丢弃，以防止传输敏感数据。

注意：目前，可以允许已确认的电子邮件通过Monitor操作或通过Block操作删除。

重要信息：邮件DLP操作仅在Cisco Secure Access中配置。如果邮件被安全访问阻止，则此事件也可在思科ETD邮件跟踪中看到。

步骤 9：配置用户通知

通知选项仅适用于“Recipients”。

在User Notifications下，配置当邮件与DLP策略匹配时是否应通知用户。
可以选择通知“参与者经理”或“自定义收件人”。“自定义收件人”可以是任何人。

根据需要将邮件模板从“默认”配置为“自定义”通知。

如果启用，通知可以帮助提高用户感知并减少重复违反策略的情况。根据您组织的运行和合规性要求配置此设置。

步骤 9：配置用户通知

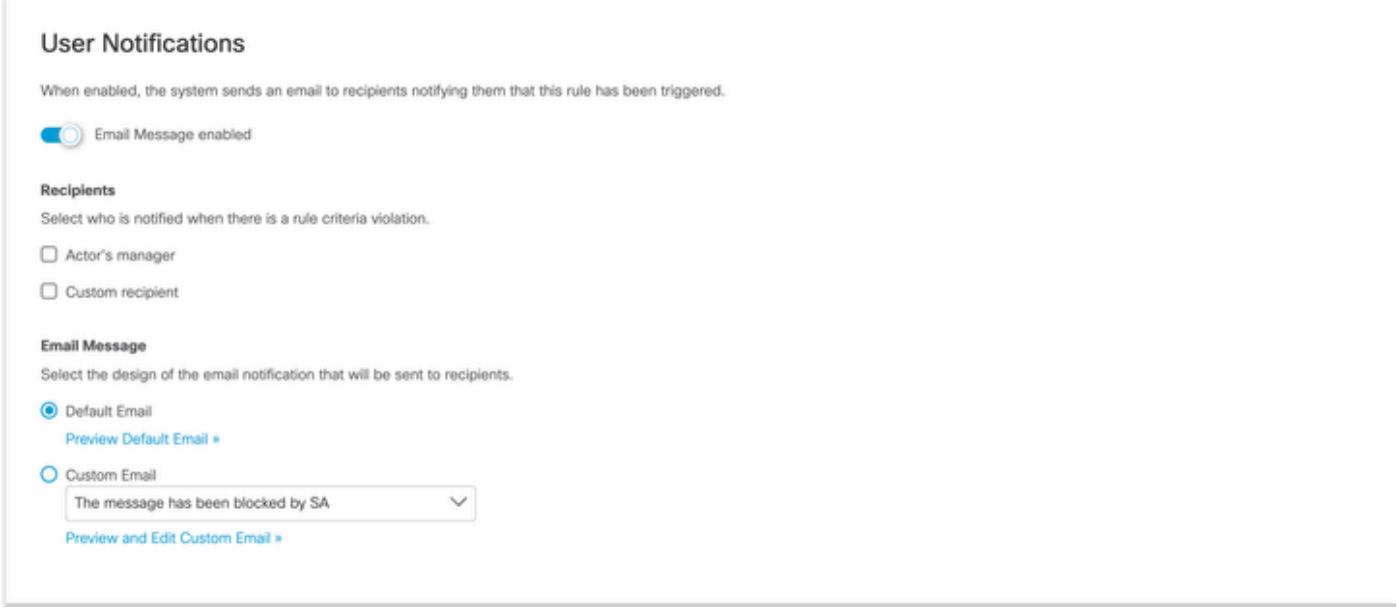
用户通知是促进安全意识和确保合规性的强大工具。通过在邮件触发DLP策略时提醒用户或管理员，您可以立即提供有关违规的反馈和情景。

注意：通知设置主要面向邮件收件人和指定的利益相关者。

要配置通知，请执行以下操作：

1. 定义通知接收人:在User Notificationssection下，指定接收警报的人员。您有两个主要选项：
    - 演员经理:将通知直接发送给触发策略违规的用户的管理员。
    - 自定义收件人：允许您指定任何邮件地址（例如，安全运营中心或特定部门负责人）。
2. 选择消息模板:您可以在Defaultnotification模板或aCustomnotification之间进行选择。
    - 建议:如果您的组织有特定的合规性消息或内部品牌要求，请使用Customoption定制邮件正文，向收件人提供明确且可行的说明。
3. 查看并保存:配置后，请确保设置与组织的运营和合规性策略一致。

最佳实践:启用这些通知是减少重复策略违规的有效方法，可以实时培训用户有关敏感数据处理过程的信息。



注意：通知选项可能因租户配置和策略设置而异。

步骤 10：查看并保存规则

完成规则配置后：

1. 检查所有配置的设置。
2. 验证所选的数据分类、检测范围、发件人和收件人条件以及操作是否与您的预期策略行为匹配。
3. 点击保存(Save)创建邮件DLP规则。

邮件DLP策略现在在思科安全访问中处于活动状态。

选项 2：使用自定义DLP模板创建邮件DLP规则

创建自定义DLP模板涉及两个主要阶段：定义自定义标识符并配置数据分类。

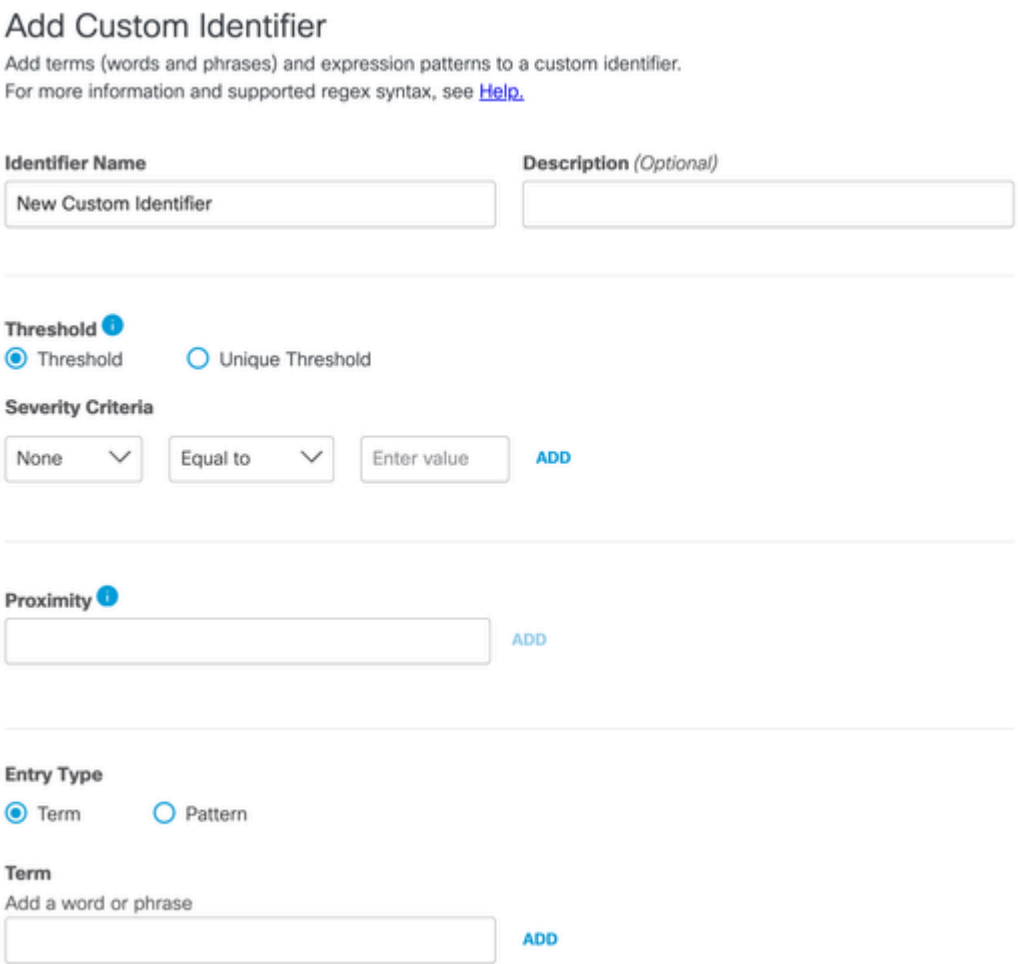
注意：数据分类引擎高度灵活，允许您使用单个自定义标识符或由AND/OR布尔运算符链接的自定义标识符和预定义标识符的组合来构建策略。

步骤 11：创建自定义标识符

要定义用于检测的新数据模式，请执行以下步骤：

1. 登录到Secure Access(安全访问)控制面板。
2. 导航到安全>数据分类。
3. 点击Add Custom Identifier。
4. 在“添加自定义标识符”(Add Custom Identifier)窗口中配置以下参数：

- 名称和说明:提供要检测的数据类型的唯一名称和简短说明。
- 阈值:
  - 阈值:监视检测数据的总频率。
  - 唯一阈值:仅监控数据的重复出现次数，忽略重复项。
- 严重性标准：根据检测频率指定严重性级别(Very Low、Low、Medium、High)。可以使用比较运算符(如等于、大于、小于或范围)来定义它们。
- 接近度:设置接近阈值。这适用于在此标识符内共同定义的所有术语和模式，而不是单个术语。
- 条目类型:定义系统如何识别数据：
  - 期限:一个特定的词或短语。
  - 模式:正则表达式(regex)用于检测特定数据格式（例如，信用卡号或内部项目代码）。



步骤 12：配置数据分类

保存自定义标识符后，您可以将其集成到数据分类对象中：

1. 导航到安全>数据分类>添加（使用右上角的按钮）
2. 从可用列表中选择新创建的Custom Identifier。
3. （可选）使用AND/OR逻辑将自定义标识符与预定义标识符组合以细化检测范围。
4. 保存配置，使其可用于邮件DLP策略。
5. 有关详细信息，请参阅下面的屏幕截图。
6. 现在，请按照步骤4到步骤10中的相同步骤使用自定义数据分类创建策略。

此配置可确保您的组织能够检测专门针对您的内部数据结构和合规性要求而定制的敏感信息。

故障排除

如果邮件DLP规则未按预期运行，请查看以下内容：

规则与电子邮件不匹配

- 确认已选择correctdata classification templates。
- 验证相关检查位置是否已启用：
  - 电子邮件主题
  - 邮件正文
  - 附件名称
  - 附件内容
- 确保发件人和收件人过滤器不会无意中排除测试邮件。

电子邮件未被阻止

- 验证规则操作是否设置为Blockand notMonitor。
- 确认规则已保存并启用。
- 确保邮件内容与配置的DLP条件正确匹配。

DLP事件在ETD中不可见

- 确认Cisco ETD和Cisco Secure Access正确集成。
- 确认ETD正在积极处理相关电子邮件流量。
- 检查策略事件是否首先出现在思科安全访问中。

未检测到基于附件的匹配

- 确认Attachment Name和/或Attachment Contents已在检查范围中选定。
- 如果诸如MIPorTitusare等标签属于规则逻辑的一部分，请验证文件控制设置。

最佳实践

部署邮件DLP策略时，请考虑以下最佳实践：

- 从Monitormode开始，在实施Block之前验证策略行为。
- 使用清楚的描述性规则名称来简化管理。
- 仔细界定发件人和收件人条件，以减少意外匹配。
- 在广泛部署之前使用代表性数据进行测试。
- 定期检查ETD邮件跟踪，以验证受阻止或监控的邮件活动。
- 使用需要特定业务数据标识符的自定义模板。

摘要

思科安全访问是在集成的思科安全访问和思科邮件威胁防御部署中配置邮件DLP策略的中央平台。虽然ETD提供可视性和邮件跟踪，但所有DLP规则创建、分类选择、实施操作和通知均在安全访问中进行配置。

通过使用预定义或自定义DLP模板，管理员可以检查邮件内容和附件，定义发件人和收件人范围，并应用Monitor或Block操作来帮助防止通过邮件丢失敏感数据。

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）。