防数据丢失

本章包含以下部分：

防数据丢失概述

防数据丢失 (DLP) 功能可以防止用户恶意或无意中通过邮件将您网络中的敏感数据发送出去，从而保护您的组织的专有信息和知识产权，同时强制遵守政府法规。您可通过创建DLP策略来定义不允许员工通过邮件发送的数据类型，这些策略用于扫描外发邮件，确定其中是否包含任何可能违反法律或公司政策的数据。

相关主题

DLP 扫描过程概述

	操作	详细信息
1.	在您的组织中，某位用户给组织外部的收件人发送了一封邮件。	邮件网关会处理进入或离开您的网络的邮件。 发送给您的网络内其他用户的邮件不会受到扫描。
2.	邮件网关将在邮件到达 DLP 扫描阶段之前，在其邮件“工作队列”的各个阶段对邮件进行处理。	例如，DLP 扫描前的过程可确保邮件不包含垃圾邮件或恶意软件。 要了解工作队列中发生 DLP 处理的位置，请参阅邮件管道流中的工作队列流程图。
3.	邮件网关将扫描邮件正文、信头和附件，确定其中是否包含 DLP 策略中标识的敏感内容。	请参阅防数据丢失的工作原理 , on page 2。
4.	如果找到敏感内容，则邮件网关将采取相应措施来保护该数据，例如隔离邮件、将其丢弃或在进行限制的情况下传送该邮件。 否则，该邮件将在邮件网关的工作队列中继续传送，如果未发现任何问题，邮件网关便会将其传送给收件人。	要采取的操作由您定义。请参阅邮件操作, on page 22。

防数据丢失的工作原理

当您的组织中的某人向组织外的收件人发送邮件时，此邮件网关将根据您定义的规则，确定要应用于该邮件的发件人或收件人的外发邮件策略。此邮件网关将使用该外发邮件策略中指定的 DLP 策略来评估邮件内容。

具体而言，此邮件网关将扫描邮件内容（包括信头和附件），确定其中是否包含与您在适用的 DLP 策略中标识为敏感内容的字词、短语、预定义模式（例如社会保险号）或正则表达式匹配的文本。

此邮件网关还将评估禁止内容的上下文，以尽量减少误报匹配。例如，某个数字与信用卡号模式相匹配，如果还随该数字一起提供了到期日期、信用卡公司名称（Visa、AMEX 等）或者某人的姓名和地址，则只能认定该数字违规。

如果邮件内容与多个 DLP 策略相匹配，则根据您指定的顺序，列表中第一个匹配的 DLP 策略适用。如果外发邮件策略有多个使用同一条件来确定内容是否违规的 DLP 策略，则所有这些策略都将使用单一内容扫描所产生的结果。

当邮件中存在可能属于敏感数据的内容时，此邮件网关将对这个潜在的违规指定介于 0 与 100 之间的风险系数得分。此得分指示该邮件发生 DLP 违规的可能性。

随后，此邮件网关将分配您为该风险因素得分定义的严重性级别（如“关键”(Critical) 或“低”(Low)），并执行您在适用的 DLP 策略中为该严重性级别指定的邮件操作。

防数据丢失的系统需求

除使用 D-模式许可证的设备以外，所有受支持的 C 系列和 X 系列设备都支持防数据丢失。

防数据丢失的设置方式

请按顺序执行下列步骤：

Procedure

	Command or Action	Purpose
步骤 1	启用 DLP 功能。	启用防数据丢失 (DLP) , on page 4
步骤 2	定义对于在其中发现或怀疑其中存在违规的邮件可以采取的可能操作。例如，您可隔离此类邮件。	邮件操作, on page 22
步骤 3	创建 DLP 策略，这些策略将： • 标识不得从您的组织通过邮件发送的内容，并且 • 指定对于每一项违规将采取的操作。	选择一种方法： • 使用向导来设置 DLP 防护 , on page 5 • 使用预定义模板创建 DLP 策略 , on page 7 • 创建自定义 DLP 策略（高级） , on page 8
步骤 4	设置 DLP 策略的顺序，以确定当内容可能与多个 DLP 策略匹配时，使用哪个 DLP 策略来评估邮件是否发生 DLP 违规。	排列邮件 DLP 策略用于违规匹配的顺序 , on page 21
步骤 5	对于要扫描其邮件是否发生 DLP 违规的每一组发件人和收件人，确保您已创建相应的外发邮件策略。	请参阅邮件策略 要在各个 DLP 策略中进一步优化允许的及限制的邮件发件人和收件人，请参阅根据 DLP 策略过滤邮件, on page 19。
步骤 6	通过将 DLP 策略分配给外发邮件策略，指定哪些 DLP 策略应用于哪些发件人和收件人。	将 DLP 策略与传出邮件策略关联, on page 21
步骤 7	配置敏感 DLP 信息的存储设置及访问设置。	• 在邮件跟踪中显示敏感 DLP 数据 , on page 27 • 控制对“邮件跟踪”中敏感信息的访问权限

启用防数据丢失 (DLP)

Procedure

步骤 1 选择**安全服务 (Security Services) > 防数据丢失 (Data Loss Prevention)**。

步骤 2 单击**启用 (Enable)**。

步骤 3 滚动到许可协议页面底部，并单击**接受 (Accept)** 以接受该协议。

Note 如果您不接受许可协议，则不会在邮件网关上启用 DLP。

步骤 4 在**防数据丢失全局设置**下，选择**启用防数据丢失**。

步骤 5 （建议）目前，请取消选择此页面上的其他选项。

您稍后可根据本章中其他部分提供的说明来更改这些设置。

步骤 6 提交并确认更改。

What to do next

请参阅防数据丢失的设置方式 , on page 3。

相关主题

- 在邮件跟踪中显示敏感 DLP 数据 , on page 27
- 使用向导来设置 DLP 防护 , on page 5
- 关于更新 DLP 引擎和内容匹配分类器, on page 28

防数据丢失策略

相关主题

- DLP 策略说明 , on page 5
- 预定义的 DLP 策略模板, on page 5
- 使用向导来设置 DLP 防护 , on page 5
- 使用预定义模板创建 DLP 策略 , on page 7
- 创建自定义 DLP 策略（高级） , on page 8
- 关于使用内容匹配分类器来定义不允许的内容 , on page 9
- 根据 DLP 策略过滤邮件, on page 19
- 关于评估违规严重性 , on page 20
- 排列邮件 DLP 策略用于违规匹配的顺序 , on page 21
- 将 DLP 策略与默认的传出邮件策略关联 , on page 21
- 关于编辑或删除 DLP 策略的重要信息 , on page 22

DLP 策略说明

DLP 策略包含以下内容：

- 一组条件，用于确定外发邮件是否包含敏感数据，以及
- 当邮件包含敏感数据时要采取的操作。

您可指定如何根据以下条件来评估邮件内容：

- 不允许的特定内容或信息模式。根据策略，您可能需要创建正则表达式以搜索标识号。请参阅关于使用内容匹配分类器来定义不允许的内容 , on page 9。
- 特定发件人和收件人的列表，用于过滤邮件。请参阅根据 DLP 策略过滤邮件, on page 19。
- 附件文件类型的列表，用于过滤邮件。请参阅根据 DLP 策略过滤邮件, on page 19。
- 允许根据违规的严重性来采取不同操作的设置。请参阅关于评估违规严重性 , on page 20。

您在外发邮件策略中启用 DLP 策略时，应确定应用每个策略的邮件发件人及收件人。

预定义的 DLP 策略模板

为了简化 DLP 策略的创建，邮件网关包括大量预定义策略模板。

模板类别包括：

- **合规性**。这些模板用于识别包含个人身份信息、信用信息或者其他受保护或非公共信息的邮件及附件。
- **使用规定**。这些模板用于识别发送给竞争对手或受限收件人的包含组织敏感信息的邮件。
- **隐私保护**。这些模板用于识别包含财务账户识别号、报税记录或身份证号码的邮件及附件。
- **知识产权保护**。这些模板用于识别可能包含组织想要保护的知识产权的常用发布和设计文档文件类型。
- **公司机密**。这些模板用于识别包含公司会计信息及即将进行的合并和收购的相关信息的文档及邮件。
- **自定义策略**。这个“模板”允许您使用预定的内容匹配分类器或者组织所指定的违规识别条件，从头创建您自己的策略。这是一个高级选项，只应该在预定义策略模板无法满足网络环境的独特要求的极少数情况下使用。

这其中的一些模板需要自定义。

使用向导来设置 DLP 防护

DLP 评估向导可帮助您配置常用的 DLP 策略，并在邮件网关的默认外发邮件策略中启用这些策略。

Note 默认情况下，使用 DLP 评估向导添加的 DLP 策略将传送所有邮件，而不考虑所检测到的 DLP 违规的严重性。您需要对使用此向导创建的策略进行编辑。

准备工作

- 从邮件网关中删除所有的现有 DLP 策略。仅当邮件网关上不存在现有的 DLP 策略时，才能使用 DLP 评估向导。
- 如果您需要检测包含除信用卡号、美国社会保险号和美国驾驶执照号码以外的学生标识号或帐号的邮件，请创建识别这些号码的正则表达式。有关详细信息，请参阅用于识别标识号的正则表达式 , on page 13。

Procedure

步骤 1 选择**安全服务 (Security Services) > 防数据丢失 (Data Loss Prevention)**。

步骤 2 单击**编辑设置 (Edit Settings)**。

步骤 3 选中**使用 DLP 评估向导启用并配置 DLP (Enable and configure DLP using the DLP Assessment Wizard)** 复选框。

步骤 4 单击**提交 (Submit)**。

步骤 5 完成向导。

记住以下几点：

- 任何在美国加利福尼亚州开展业务并且拥有或许可使用加利福尼亚州居民的计算机化个人身份信息 (PII) 数据的企业，无论其实体位置在哪，均需遵守**美国国家法规（加利福尼亚州 SB-1386 号法案）**。此法案是向导的其中一个策略选项。
- 如果您不输入用于接收自动生成的计划内 DLP 事件摘要报告的邮件地址，则不会生成该报告。
- 在审核已配置的设置时，如果您返回到某个步骤进行更改，则必须继续完成余下的步骤，直至再次到达审核页面为止。系统将记住您先前输入的所有设置。
- 完成此向导时，将显示“外发邮件策略”(Outgoing Mail Policies) 页面，并且已在默认外发邮件策略中启用您的 DLP 策略。您的 DLP 策略配置摘要将显示在该页面顶部。

步骤 6 确认更改。

What to do next

- （可选）要编辑这些 DLP 策略、创建其他策略、更改对邮件执行的总体操作，或更改严重性级别设置，请依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。有关信息，请参阅使用预定义模板创建 DLP 策略 , on page 7、创建自定义 DLP 策略（高级） , on page 8和调整严重性刻度 , on page 20。
- （可选）要为其他外发邮件策略启用现有的 DLP 策略，请参阅使用传出邮件策略向发件人和收件人指定 DLP 策略 , on page 22。

相关主题

- 使用预定义模板创建 DLP 策略 , on page 7
- 创建自定义 DLP 策略（高级） , on page 8

使用预定义模板创建 DLP 策略

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 单击**添加 DLP 策略 (Add DLP Policy)**。

步骤 3 单击类别名称，以显示可用的 DLP 策略模板的列表。

Note 要查看每个模板的说明，请单击**显示策略说明 (Display Policy Descriptions)**。

步骤 4 对于您想要使用的 DLP 策略模板，单击**添加 (Add)**。

步骤 5 （可选）更改该模板的预定义名称和说明。

步骤 6 如果策略要求或建议自定义一个或多个内容匹配分类器，请输入一个正则表达式以定义您的组织的标识编号系统模式，并输入一系列与标识号相关的字词或短语，这些字词或短语将它们标识为标识号或者通常与其相关联。

有关信息，请参阅：

关于使用内容匹配分类器来定义不允许的内容 , on page 9和用于识别标识号的正则表达式 , on page 13。

Note 无法为基于预定义模板的策略添加或删除内容匹配分类器。

步骤 7 （可选）将该 DLP 策略仅应用于具有特定收件人、发件人、附件类型或先前添加的邮件标记的邮件。

有关详细信息，请参阅根据 DLP 策略过滤邮件, on page 19。

您可使用换行符或逗号来分隔多个条目。

步骤 8 在“严重性设置”(Severity Settings) 部分：

- 选择针对每个违规严重性级别要采取的操作。有关详细信息，请参阅关于评估违规严重性 , on page 20。
- （可选）单击**编辑刻度 (Edit Scale)**，以调整该策略的违规严重性刻度。有关详细信息，请参阅调整严重性刻度 , on page 20。

步骤 9 提交并确认更改。

What to do next

相关主题

- 使用向导来设置 DLP 防护 , on page 5
- 创建自定义 DLP 策略（高级） , on page 8

创建自定义 DLP 策略（高级）

Note 创建自定义策略非常复杂；仅当预定义 DLP 策略模板无法满足您的组织需求时，才应创建自定义策略。

您可使用自定义策略模板从头开始创建自定义 DLP 策略，然后向该策略添加预定义内容匹配分类器或自定义分类器。

当内容与单个分类器或所有分类器（具体取决于策略的定义）匹配时，自定义策略可返回 DLP 违规。

准备工作

建议：定义可识别内容违规的条件。请参阅为自定义 DLP 策略创建内容匹配分类器 , on page 11。您也可以在此过程中定义这些条件。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 单击**添加 DLP 策略 (Add DLP Policy)**。

步骤 3 单击**自定义策略 (Custom Policy)**。

步骤 4 对于自定义策略模板，单击**添加 (Add)**。

步骤 5 输入该策略的名称和描述。

步骤 6 标识构成 DLP 违规的内容和上下文：

a) 选择内容匹配分类器。

b) 单击**添加 (Add)**。

- 如果您已选择**创建分类器**，请参阅为自定义 DLP 策略创建内容匹配分类器 , on page 11。
- 否则，选择的分类器将添加到表中。

c) （可选）向该策略添加其他分类器。

例如，您可以通过添加另一个分类器并选择“否”(NOT)，消除已知可能发生的误报匹配。

d) 如果您已添加多个分类器：请在表格标题中选择一个选项，以指定是匹配**任何**分类器即可使实例计作违规，还是必须匹配**全部**分类器才会计作违规。

步骤 7 （可选）将该 DLP 策略仅应用于具有特定收件人、发件人、附件类型或先前添加的邮件标记的邮件。

有关详细信息，请参阅根据 DLP 策略过滤邮件, on page 19。

您可使用换行符或逗号来分隔多个条目。

步骤 8 在“严重性设置”(Severity Settings) 部分：

- 选择针对每个违规严重性级别要采取的操作。有关详细信息，请参阅关于评估违规严重性 , on page 20。
- （可选）单击**编辑刻度 (Edit Scale)**，以调整该策略的违规严重性刻度。有关详细信息，请参阅调整严重性刻度 , on page 20

步骤 9 提交并确认更改。

What to do next

相关主题

- 使用向导来设置 DLP 防护 , on page 5
- 使用预定义模板创建 DLP 策略 , on page 7

关于使用内容匹配分类器来定义不允许的内容

内容匹配分类器定义不能通过邮件发送的内容，还可（可选）定义内容必须处于何种上下文才会被视为防数据丢失违规。

假设您希望防止通过邮件将患者标识号从您的组织中发送出去。

要让邮件网关识别这些号码，您必须使用一个或多个正则表达式指定您的组织所使用的记录编号系统的模式。您还可以添加一系列可能作为支持信息伴随记录号一起出现的字词和短语。如果该分类器在外发邮件中检测到该数字模式，则会搜索这些支持信息，以确认该模式是标识号，而不是随机数字符串。包括上下文匹配信息可以减少误报匹配。

对于此示例，您可以创建一项使用 HIPAA 和 HITECH 模板的 DLP 策略。此模板包含“患者标识号”内容匹配分类器，您可自定义该分类器，以检测患者标识号。要检测 123-CL456789 模式的号码，请为分类器输入正则表达式 [0-9]{3}\-[A-Z]{2}[0-9]{6}。输入“患者 ID”，作为相关短语。完成创建该策略，并在外发邮件策略中将其启用。提交并确认更改。现在，如果该策略在外发邮件中检测到此数字模式旁边出现短语“患者 ID”，则 DLP 策略会返回 DLP 违规。

关于在 DLP 策略中使用内容匹配分类器

许多预定义的 DLP 策略模板包含内容匹配分类器。其中的一些分类器要求进行自定义，才能识别您组织中的数据所使用的模式。

如果创建自定义 DLP 策略，可以选择自定义分类器，或者创建自己的分类器。

相关主题

- 内容匹配分类器示例, on page 10
- 为自定义 DLP 策略创建内容匹配分类器 , on page 11
- 用于识别敏感内容的分类器检测规则（仅适用于自定义 DLP 策略） , on page 12
- 用于识别标识号的正则表达式 , on page 13
- 使用敏感 DLP 术语的自定义词典（仅适用于自定义 DLP 策略） , on page 14

- 可疑违规的风险系数的决定因素 , on page 16
- 查看使用了自定义内容分类器的策略 , on page 19

内容匹配分类器示例

以下示例显示分类器如何匹配邮件内容：

- 信用卡号, on page 10
- 美国社会保险号, on page 10
- ABA 路由编号, on page 10
- 驾驶执照编号（美国） , on page 10
- 国家运营商 ID（美国）, on page 11
- 学术记录（英文）, on page 11
- 财务声明（英文）, on page 11

信用卡号

多个 DLP 策略模板包含“信用卡号”分类器。信用卡号本身受各种约束制约，例如数字和标点的模式、发卡行专用前缀以及最终校验位。分类器需要额外的支持信息才能做出匹配决策，例如，到期日期、发卡行名称。这将减少误报的数量。

示例：

- `378734493671000`（因为没有支持信息，所以不匹配）
- `378734493671000 VISA`（匹配）
- `378734493671000 exp: 12/2019`（匹配）

美国社会保险号

“美国社会保险号”分类器需要格式正确的号码以及支持数据（例如出生日期、姓名或字符串 SSN）。

示例：

- `321-02-3456`（因为没有支持信息，所以不匹配）
- `SSN: 132-45-6788`（匹配）

ABA 路由编号

“美国银联转帐号”分类器与“信用卡号”分类器类似。

示例：

- `119999992`（因为没有支持信息，所以不匹配）
- `ABA No. 800000080`（匹配）

驾驶执照编号（美国）

许多策略使用“美国驾驶执照”分类器。默认情况下，此分类器将搜索在美国颁发的驾驶执照。美国政府特定的策略（如加利福尼亚 AB-1298 和蒙大拿 HB-732）仅搜索其各自的州的美国驾照。

各个州分类器根据相应州的模式进行匹配，并需要相应的州名或缩写以及额外的支持数据。

示例：

- CA DL# C3452362（因为具有正确的号码模式以及支持数据，所以匹配）
- California DL# C3452362（匹配）
- DL: C3452362（因为没有足够的支持数据，所以不匹配）
- California C3452362（因为没有足够的支持数据，所以不匹配）
- OR DL# C3452362（匹配）
- OR DL# 3452362（因为是俄勒冈州的正确模式，所以匹配）
- WV DL# D654321（因为是西弗吉尼亚州的正确模式，所以匹配）
- WV DL# G654321（匹配）

国家运营商 ID（美国）

“美国国内供应商标识”分类器用于扫描“美国国内供应商标识”(NPI) 号码，后者是带有校验位的 10 位数号码。

示例：

- NPI No. 1245319599（与 NPI 匹配）
- NPI No. 1235678996（与 NPI 匹配）
- 3459872347（因为没有支持信息，所以不匹配）
- NPI: 3459872342（因为校验位不正确，所以不匹配）

学术记录（英文）

预定义的FERPA（《家庭教育权和隐私权法案》）DLP 策略模板使用“学生记录”分类器。将其与自定义“学生标识号”分类器组合可检测特定的学生 ID 模式，以提高准确度。

示例：

- Fall Semester Course Numbers: CHEM101, ECON102, MATH103（匹配）

财务声明（英文）

预定义的“沙宾法案”(SOX) 策略模板使用“公司财务”分类器来搜索非公共公司财务信息。

示例：

Gross Profits, Current Assets, and Cash Flow Statement for the Quarter ended June 30, 2016.（匹配）

为自定义 DLP 策略创建内容匹配分类器

您创建的自定义分类器将添加到创建自定义 DLP 策略时可使用的分类器列表中。

Procedure

	Command or Action	Purpose
步骤 1	了解内容匹配分类器如何用于识别潜在的DLP违规。	请参阅：

	Command or Action	Purpose
		• 关于使用内容匹配分类器来定义不允许的内容 , on page 9 • 内容匹配分类器示例, on page 10
步骤 2	选择**邮件策略 (Mail Policies) > DLP 策略自定义 (DLP Policy Customizations)**，然后单击**添加自定义分类器 (Add Custom Classifier)**。输入分类器名称及说明。	-
步骤 3	输入接近度和最低总分。	请参阅可疑违规的风险系数的决定因素 , on page 16
步骤 4	选择以下检测规则类型之一，并定义相关联的内容匹配条件： • 词汇或短语 • 词典中的文本 • 正则表达式，或 • 现有的防数据丢失实体	请参阅： • 用于识别敏感内容的分类器检测规则（仅适用于自定义 DLP 策略） , on page 12 • 使用敏感 DLP 术语的自定义词典（仅适用于自定义 DLP 策略） , on page 14 • 用于识别标识号的正则表达式 , on page 13
步骤 5	（可选）通过单击**添加规则 (Add Rule)**，添加其他规则。	有关权重和最高得分的信息，请参阅可疑违规的风险系数的决定因素 , on page 16。
步骤 6	如果包括多条规则，请指定是必须匹配**全部 (All)** 规则，还是匹配**任何 (Any)** 规则即可。	此设置位于“规则”(Rules) 部分顶部。
步骤 7	提交并确认更改。	-

What to do next

在自定义 DLP 策略中使用自定义内容分类器。请参阅创建自定义 DLP 策略（高级） , on page 8。

相关主题

- 查看使用了自定义内容分类器的策略 , on page 19

用于识别敏感内容的分类器检测规则（仅适用于自定义 DLP 策略）

内容匹配分类器需要用于在邮件或文档中检测 DLP 违规的规则。分类器可以使用以下一条或多条检测规则：

- **字词或短语**。分类器应检测的一系列字词或短语。请使用逗号或换行符来分隔多个条目。
- **正则表达式**。用于为邮件或附件定义搜索模式的正则表达式。您也可定义要从匹配中排除的模式，以避免误报。有关详细信息，请参阅用于识别标识号的正则表达式 , on page 13和用于识别标识号的正则表达式的示例 , on page 14。
- **词典**。相关字词和短语的词典。邮件网关包含预定义的词典，您也可创建自己的词典。请参阅使用敏感 DLP 术语的自定义词典（仅适用于自定义 DLP 策略） , on page 14。

- **实体**。这是用于识别常见敏感数据类型（例如信用卡号、地址、社会保险号或美国银联转帐号）的预定义模式。有关实体的说明，请依次转至**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**，然后依次单击**添加 DLP 策略 (Add DLP Policy)**、**隐私保护 (Privacy Protection)**、**显示策略说明 (Display Policy Descriptions)**。

用于识别标识号的正则表达式

一些策略模板要求对一个或多个内容匹配分类器进行自定义，这涉及创建正则表达式以搜索可能链接到机密信息（例如自定义帐号、患者标识号或学生ID）的标识号。您可以使用**Perl 兼容正则表达式 (PCRE2)** 语法为内容匹配分类器或DLP策略模板添加正则表达式。只有在邮件网关上启用了 DLP 功能时才会验证正则表达式的 PCRE2 兼容性。

Note 正则表达式区分大小写，因此它们应包含大写和小写字符，例如 `[a-zA-Z]`。如果仅使用特定的字母，您可相应地定义正则表达式。

模式越不具体（例如 8 位数的号码），您就越有可能希望策略搜索额外的字词和短语，以区分随机的 8 位数号码与实际客户号码。

在为分类器创建正则表达式时，请使用下表作为指南：

元素	说明
正则表达式 (abc)	对于分类器的正则表达式，如果其中的指令序列与一个字符串的任何部分匹配，则该正则表达式与该字符串匹配。 例如，正则表达式 **ACC** 与字符串 **ACCOUNT** 以及 **ACCT** 匹配。
[ ]	使用方括号可指示一组字符。可以逐个定义字符，也可使用范围来定义字符。 例如，**[a-z]** 与 a 到 z 的所有小写字母匹配，而 **[a-zA-Z]** 与 A 到 Z 的所有大写及小写字母匹配。**[xyz]** 仅与字母 x、y 或 z 匹配。
反斜线特殊字符 (\)	反斜线字符对特殊字符进行转义。因此，序列\仅与句点的字母表达匹配，序列\$ 仅与美元符号的字母表达匹配，序列 \^ 仅与克拉符号的字母表达匹配。 反斜线字符也作为标记的开头，例如 \d。 **重要说明**：反斜线也是解析器的特殊转义字符。因此，如果您想在正则表达式中包括一个反斜线，则必须使用两个反斜线。这样，在解析后，将仅保留一个“真正的”反斜线，这个反斜线将传递到正则表达式系统。

元素	说明
\d	与一个数字 (0-9) 匹配的标记。要与多个数字匹配，请输入一个括在 {} 中的整数以定义数值长度。 例如，\d 仅与 5 之类的单个数字匹配，而与 55 不匹配。使用 \d{2} 表示与 55 等包含两个数字的数值匹配，但与 5 不匹配。
\D	与任何非数字字符匹配的标记。要与多个非数字字符匹配，请输入一个括在 {} 中的整数以定义长度。
\w	与任何字母数字字符和下划线（a-z、A-Z、0-9 以及 _）匹配的标记。
重复次数 {min,max}	此正则表达式记法指示前一个标记可以重复的次数。 例如，表达式“\d{8}”与 12345678 和 11223344 匹配，但与 8 不匹配。
Or (|)	替换或“或”运算符。如果 A 和 B 是正则表达式，则表达式“A|B”将与任何与“A”或“B”匹配的字符串匹配。这可用来在正则表达式中组合数字模式。 例如，表达式“foo|bar”将与 foo 或 bar 匹配，但与 foobar 不匹配。

相关主题

- 用于识别标识号的正则表达式的示例 , on page 14

用于识别标识号的正则表达式的示例

用于说明标识号或帐号中的数字及字母模式的简单正则表达式可能如下所示：

- 一个 8 位数：`\d{8}`
- 在各组数值之间以连字符分隔的标识代码：`\d{3}-\d{4}-\d`
- 以单个大写或小写字母开头的标识代码：`[a-zA-Z]\d{7}`
- 以 3 个数字开头并且后跟 9 个大写字母的标识代码：`\d{3}[A-Z]{9}`
- 使用 | 定义两种不同的号码模式用于搜索：`\d{3}[A-Z]{9}|\d{2}[A-Z]{9}-\d`

使用敏感 DLP 术语的自定义词典（仅适用于自定义 DLP 策略）

AsyncOS 附带一组预定义词典，但您也可创建自定义 DLP 词典，以指定要让 DLP 扫描功能匹配的术语。

可以通过多种方式创建自定义 DLP 词典：

- 直接添加自定义 DLP 词典 , on page 15
- 以文本文件的形式创建 DLP 词典 , on page 15，然后导入 DLP 词典 , on page 16。
- 从另一个邮件网关导出 DLP 词典 , on page 15，然后导入 DLP 词典 , on page 16。

直接添加自定义 DLP 词典

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 在**高级设置 (Advanced Settings)** 部分，单击**自定义词典 (Custom DLP Dictionaries)** 旁的链接。

步骤 3 单击**添加词典 (Add Dictionary)**。

步骤 4 为自定义词典输入一个名称。

步骤 5 将新词典条目（字词和短语）输入到词条列表中。

词典词条区分大小写，并可包含非 ASCII 字符。

输入多个条目时，请使用换行符来分隔各个条目。

步骤 6 单击**添加 (Add)**。

步骤 7 提交并确认更改。

以文本文件的形式创建 DLP 词典

您可以采用文本文件形式在本地计算机上创建自己的词典，然后将其导入到邮件网关上。对于词典文本文件中的每个词条，请使用换行符。词典词条区分大小写，并可包含非 ASCII 字符。

导出 DLP 词典

Note 预定义的 DLP 词典不可导出。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 单击“高级设置”(Advanced Settings) 下的**自定义 DLP 词典 (Custom DLP Dictionaries)** 部分的链接。

步骤 3 单击**导出词典 (Export Dictionary)**。

步骤 4 选择要导出的词典。

步骤 5 为该词典输入一个文件名。

步骤 6 选择将导出的词典保存到什么位置，可以保存在本地计算机上，也可以保存在邮件网关上的配置目录中。

步骤 7 为该文件选择一种编码方式。

步骤 8 单击**提交 (Submit)** 并保存该文件。

导入 DLP 词典

准备工作

如果您要导入一个文件，而该文件使您从邮件网关上的非 DLP 词典中导出的，必须首先从文本文件中拆分出权重值，并将所有正则表达式转换为词汇或短语。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 在**高级设置 (Advanced Settings)** 部分，单击**自定义词典 (Custom DLP Dictionaries)** 旁的链接。

步骤 3 单击**导入词典 (Import Dictionary)**。

步骤 4 从本地计算机或者邮件网关上的配置目录中选择要导入的文件。

步骤 5 选择一种编码方式。

步骤 6 单击**下一步 (Next)**。

系统将显示“导入成功”(Success) 的消息，并且导入的词典将显示在“添加词典”(Add Dictionary) 页面中。但是，操作过程尚未完成。

步骤 7 命名并编辑词典。

步骤 8 单击**提交 (Submit)**。

可疑违规的风险系数的决定因素

当邮件网关扫描邮件以确定是否包含 DLP 违规时，会对邮件指定风险系数得分。此得分指示该邮件发生 DLP 违规的可能性。得分为 0 表示邮件几乎肯定不包含违规。得分为 100 表示邮件几乎肯定包含违规。

对于基于预定义模板的 DLP 策略

您无法查看或修改根据预定义模板创建的 DLP 策略的风险系数得分参数。但是，如果对于某一特定 DLP 策略存在过多误报匹配，则可调整该策略的严重性标度。请参阅关于评估违规严重性 , on page 20。对于基于没有内容匹配分类器的模板的策略（如 SOX（萨班斯 - 奥克斯利法案 (Sarbanes-Oxley)）模板），当某一邮件违反该策略时，扫描引擎将始终返回一个值为“75”的风险因素。

对于自定义 DLP 策略

在为自定义 DLP 策略创建内容匹配分类器时，您需指定用来确定风险系数得分的值：

- **接近度**。规则匹配项在邮件或附件中必须达到何种接近度才算作违规。例如，如果在一封较长邮件的开头附近出现类似于社会保险号的数字模式，并且末尾的发件人签名中出现地址，则假设它们不相关，且此数据不算匹配项。
- **最低总分**。将敏感内容标记为 DLP 违规所需达到的最小风险系数得分。如果邮件的匹配项得分未达到最低总分，则将其数据视为不敏感。

- **权重**。对于您创建的每个自定义规则，您可指定“权重”以指示该规则的重要性。得分是通过将检测规则匹配项数与规则权重相乘计算而得。如果某一规则有两个实例，其权重为 10，则得分结果为 20。如果某条规则对于分类器而言比其他规则更重要，则应为其指定较大的权重。
- **最大得分**。规则的最大得分用于防止低权重规则的大量匹配项导致扫描的最终得分出现偏差。
- **最低分数**。您可以使用建议的最低分数，也可以选择根据“DLP 策略自定义”页面的“自定义分类器设置”部分中选择的**使用基于实体规则的建议最低分数**复选框来使用权重。有关详细信息，请参阅使用基于实体的规则的最低分数（仅限自定义 DLP 策略）, on page 18

为了计算风险因素，分类器会将某一检测规则的匹配数量与该规则的权重相乘。如果这个值超过该检测规则的最大得分，则分类器将使用最大得分值。如果分类器有多条检测规则，则它会将其所有检测规则的得分累加为一个值。分类器会使用下表所示的对数刻度将检测规则得分 (10 - 10000) 映射到刻度 10 - 100，以创建风险系数：

Table 1: 根据检测规则得分计算风险系数得分的方式

规则得分	风险系数
0	0
1	1
2	2
3	3
5	6
6	7
7	8
8	9
9	10
10	11
15	16
20	20
25	24
30	26
40	32
50	36
75	44
100	50

规则得分	风险系数
125	54
150	58
257	67
300	70
400	75
500	78
750	84
1000	87
5000	98
8000	99
10000	99
20000	100

使用基于实体的规则的最低分数（仅限自定义 DLP 策略）

过程

步骤 1 转到**邮件策略 (Mail Policies) > DLP 策略自定义 (DLP Policy Customizations)**。

步骤 2 在**自定义分类器设置**部分中，选中**使用基于实体规则的建议最低分数**复选框。

如果选中此选项，系统将使用所配置的最低分数（而不是权重）为基于实体的规则计算分数。

例如，当您禁用此选项且邮件的某一特定实体有五个规则匹配的权重配置为10时，则该规则将分数计算为 5 个匹配项乘以 10 次出现，即 50。如果针对某一最低分数为 10 的实体启用此选项，则系统将根据配置的最低分数以及部分和完全匹配数来计算分数。

注释　当您选择“使用基于实体规则的建议最低分数”选项时，必须使用基于实体的规则查看所有分类器的最低总分。

步骤 3 单击**提交 (Submit)** 并确认更改。

启用此选项后，您必须查看自定义分类器的基于实体规则的最低分数。有关详细信息，请参阅为自定义 DLP 策略创建内容匹配分类器 ， 第 11 页。

查看使用了自定义内容分类器的策略

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略自定义 (DLP Policy Customizations)**。

步骤 2 在**自定义分类器 (Custom Classifiers)** 部分中，单击“自定义分类器”(Custom Classifiers) 表的标题中的**策略 (Policies)** 链接。

What to do next

相关主题

- 为自定义 DLP 策略创建内容匹配分类器 , on page 11

根据 DLP 策略过滤邮件

为了改善性能或准确度，您可根据以下条件对 DLP 策略进行限制，使其仅应用于特定的邮件：

选项	说明
按发件人和收件人过滤 (Filtering by Senders and Recipients)	您可对 DLP 策略进行限制，使其应用于包含或不包含您使用下列其中一项指定的收件人或发件人的邮件： • 完整的邮件地址：`user@example.com` • 不完整邮件地址：`user@` • 域中的所有用户：`@example.com` • 不完整域中的所有用户：`@.example.com` 请使用换行符或逗号来分隔多个条目。 AsyncOS 首先会将外发邮件的收件人或发件人与外发邮件策略匹配，然后将发件人或收件人与您为该邮件策略启用的 DLP 策略中指定的发件人和收件人过滤器匹配。 例如，您可能希望不允许所有发件人向合作伙伴域中的收件人以外的收件人发送特定类型的信息。您应为该信息创建一个 DLP 策略，包括一个用于免除合作伙伴域中所有用户的过滤器，然后将这个 DLP 策略包括在应用于所有发件人的外发邮件策略中。
按附件类型过滤 (Filtering by Attachment Types)	您可对 DLP 策略进行限制，以便仅扫描包含或不包含特定附件类型的邮件。请选择附件类别，然后选择预定义的文件类型，或指定未列出的文件类型。如果指定非预定义文件类型，则 AsyncOS 会根据附件的扩展名来搜索该文件类型。 您还可将 DLP 扫描限制为扫描文件大小最小的附件。

选项	说明
按邮件标记过滤 (Filtering by Message Tag)	如果要将 DLP 策略限制为仅应用于包含特定短语的邮件，可使用邮件或内容过滤器在外发邮件中搜索该短语，并在该邮件中插入自定义邮件标记。有关详细信息，请参阅内容过滤器操作和使用邮件过滤器实施邮件策略

关于评估违规严重性

当DLP扫描引擎检测到潜在的DLP违规时，它将计算风险系数得分，该得分表示该实例确实为DLP违规的可能性。策略将对该风险因素得分与该策略中定义的严重性标度进行比较，以确定严重性级别（例如，“低”[Low]或“关键”[Critical]）。您可指定对于每个严重性级别的违规要采取的操作（“忽略”级别除外，此级别无需采取任何操作）。可以调整达到各个严重性级别所需的风险因素得分。

相关主题

- 调整严重性刻度 , on page 20

调整严重性刻度

所有策略都具有默认的严重性刻度。您可以为每个策略调整此刻度。

例如，在默认情况下，如果一项违规的风险系数得分介于 90 与 100 之间，则其严重性级别为“严重”。但是，对于与特定策略匹配的违规，您可能想提高潜在数据丢失的敏感度。对于此 DLP 策略，可将严重性级别“严重”更改为风险系数得分介于 75 与 100 之间的所有违规。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略管理器 (DLP Policy Manager)**。

步骤 2 单击策略名称进行编辑。

步骤 3 在**严重性设置 (Severity Settings)** 部分，单击**编辑刻度 (Edit Scale)**。

步骤 4 使用刻度的箭头来调整严重性级别的得分。

步骤 5 单击**完成 (Done)**。

步骤 6 在“严重性刻度”(Severity Scale) 表中，确认得分与您的期望相符。

步骤 7 单击**提交 (Submit)**。

What to do next

相关主题

- 关于评估违规严重性 , on page 20

排列邮件 DLP 策略用于违规匹配的顺序

如果某个 DLP 违规与外发邮件策略中启用的多个 DLP 策略匹配，则将仅使用列表中的第一个匹配 DLP 策略。

Procedure

步骤 1 在“DLP 策略管理器”(DLP Policy Manager) 页面上，单击**编辑策略顺序 (Edit Policy Order)**。

步骤 2 单击您想要移动的策略所对应的行，并将其拖动到顺序中的新位置。

步骤 3 当您完成重新排列策略顺序后，请提交并确认更改。

将 DLP 策略与传出邮件策略关联

相关主题

- 将 DLP 策略与默认的传出邮件策略关联 , on page 21
- 使用传出邮件策略向发件人和收件人指定 DLP 策略 , on page 22

将 DLP 策略与默认的传出邮件策略关联

当没有任何外发邮件策略与发件人或收件人匹配时，将使用默认的外发邮件策略。

准备工作

完成防数据丢失的设置方式 , on page 3的表中此项活动之前的所有活动。例如，请确保已创建要包括在默认的外发邮件策略中的 DLP 策略。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **外发邮件策略 (Outgoing Mail Policies)**。

步骤 2 在表的**默认策略 (Default Policy)** 行中，单击 **DLP** 列中的**禁用 (Disabled)** 链接。

步骤 3 选中**启用 DLP（自定义设置）(Enable DLP [Customize Settings])**。

步骤 4 选择要为默认外发邮件策略启用的 DLP 策略。

步骤 5 提交并确认更改。

What to do next

为其他外发邮件策略选择 DLP 策略。请参阅使用传出邮件策略向发件人和收件人指定 DLP 策略 , on page 22。

使用传出邮件策略向发件人和收件人指定 DLP 策略

通过在外发邮件策略中启用 DLP 策略，指定将哪些 DLP 策略应用于哪些发件人和收件人。只能在外发邮件策略中使用 DLP 策略。

准备工作

为默认的外发邮件策略配置 DLP 策略设置。请参阅将 DLP 策略与默认的传出邮件策略关联 , on page 21。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies)** > **外发邮件策略 (Outgoing Mail Policies)**。

步骤 2 单击表中任何一行的 DLP 列中的链接。

步骤 3 选择要与此外发邮件策略相关联的 DLP 策略。

步骤 4 提交更改。

步骤 5 根据需要，为其他外发邮件策略重复上述步骤。

步骤 6 确认更改。

What to do next

请参阅防数据丢失的设置方式 , on page 3。

关于编辑或删除 DLP 策略的重要信息

操作	信息
编辑 DLP 策略	如果重命名一个策略，则必须在外发邮件策略中重新启用该策略。
删除 DLP 策略	如果删除一个策略，并且该 DLP 策略已用于一个或多个外发邮件策略，则您会收到通知。删除 DLP 策略会将其从这些邮件策略中移除。

邮件操作

您应指定当邮件网关检测到传出邮件中存在可能的 DLP 违规时，它应采取的主要和次要操作。对于不同的违规类型和严重性，可指定不同的操作。

主要操作包括：

- 传送
- 删除
- 隔离

辅助操作包括：

- 如果您选择传送邮件，则向策略隔离区发送一个副本。该副本与原始邮件完全一样，其中包含邮件 ID。隔离副本不仅提供了另一种监控 DLP 违规的方法，还允许在部署前测试 DLP 系统。从隔离区释放该副本时，邮件网关会将该副本传送给收件人，而该收件人已接收了原始邮件。
- 对邮件进行加密。邮件网关仅对邮件正文进行加密。不会对邮件信头进行加密。
- 改动包含 DLP 违规的邮件的主题信头。
- 向邮件添加免责声明文本。
- 将邮件发送到备用目标邮件主机。
- 将邮件副本发送（密件抄送）给其他收件人。（例如，您可以将包含严重 DLP 违规的邮件复制到合规官的邮箱以供检查。）
- 将 DLP 违规通知邮件发送给发件人或其他联系人（例如经理或 DLP 合规官）。请参阅创建 DLP 通知 , on page 25。

Note 这些操作并不互相排斥：您可以在不同的 DLP 策略中组合这些操作，以满足不同用户组的各种处理需求。您也可以在同一个策略中基于不同严重性级别配置不同的处理操作。例如，您可能希望隔离包含严重 DLP 违规的邮件并向合规官发送通知，但您希望传送严重性级别较低的邮件。

相关主题

- 定义要针对 DLP 违规采取的操作（邮件操作） , on page 23
- 查看和编辑邮件操作 , on page 24
- 创建 DLP 通知 , on page 25

定义要针对 DLP 违规采取的操作（邮件操作）

准备工作

- 至少创建一个专用的隔离区，用于存放违反 DLP 策略的邮件（或邮件副本）。

  这可以是邮件网关上的本地隔离区，也可以是思科安全邮件和网路隔离区上的集中隔离区。

  有关信息，请参阅策略、病毒和病毒爆发隔离区

- 如果您希望在传送邮件前对其进行加密，请确保已设置加密配置文件。请参阅思科邮件加密
- 要在传送包含 DLP 违规或疑似违规的邮件时包括免责声明文本，请在**邮件策略 (Mail Policies) > 文本资源 (Text Resources)** 中指定免责声明文本。有关信息，请参阅免责声明模板
- 要向 DLP 违规的发件人或其他人员（例如合规官）发送通知，请先创建 DLP 通知模板。请参阅创建 DLP 通知 , on page 25。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略自定义 (DLP Policy Customizations)**。

步骤 2 在**邮件操作 (Message Actions)** 部分，单击**添加邮件操作 (Add Message Action)**。

步骤 3 为该邮件操作输入一个名称。

步骤 4 输入对该邮件操作的说明。

步骤 5 选择是丢弃、传送还是隔离包含 DLP 违规的邮件。

Note 如果您选择“传送”(Deliver)，则可选择将该邮件的副本发送到策略隔离区。该邮件副本与原始邮件完全一样，其中包含邮件 ID。

步骤 6 如果要在传送后或者从隔离区释放时对邮件进行加密，请选中**启用加密 (Enable Encryption)** 复选框，并选择下列选项：

- **加密规则 (Encryption Rule)**。始终对邮件进行加密，或者仅在首先尝试通过 TLS 连接发送邮件失败时对其进行加密。
- **加密配置文件 (Encryption Profile)**。使用指定的加密配置文件对邮件进行加密，并传送该邮件（如果您使用的是思科 IronPort 加密装置或托管密钥服务）。
- **加密邮件主题 (Encrypted Message Subject)**。加密邮件的主题。使用值 **`$Subject`** 可保留现有的邮件主题。

步骤 7 如果您选择“隔离”(Quarantine) 操作，请选择要用于包含 DLP 违规的邮件的策略隔离区。

步骤 8 如果您想要使用下列任何选项来修改邮件，请单击**高级 (Advanced)**：

- 添加自定义信头
- 修改邮件主题
- 将其传送到备用主机
- 将副本发送（密件抄送）给其他收件人
- 发送 DLP 通知邮件

步骤 9 提交并确认更改。

查看和编辑邮件操作

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > DLP 策略自定义 (DLP Policy Customizations)**。

步骤 2 在**邮件操作 (Message Actions)** 部分，选择操作：

收件人	相应操作
查看每一项操作所分配到的邮件策略	单击“邮件操作”(Message Actions) 表的标题中的**策略 (Policies)** 链接。
查看您为每一项操作输入的说明	单击“邮件操作”(Message Actions) 表的标题中的**说明 (Description)** 链接。

收件人	相应操作
查看或编辑邮件操作的详细信息	单击邮件操作的名称。
删除邮件操作	单击您要删除的邮件操作旁边的垃圾桶图标。 如果该邮件操作已用于一个或多个 DLP 策略，您会收到一条确认消息通知。
复制邮件操作 您可使用此功能在更改邮件操作前创建备份副本，或用作相似的新邮件操作的起点。	单击您要复制的邮件操作旁边的**复制 (Duplicate)** 图标。

步骤 3 提交并确认所有更改。

创建 DLP 通知

使用此过程可创建通知模板，用于在邮件中包含违反组织防数据丢失策略的信息时发送相应通知。您可将此通知发送给违反 DLP 策略的邮件的发件人，或发送到其他地址（例如经理或 DLP 合规官的邮箱）。

准备工作

- 熟悉 DLP 通知模板变量定义, on page 26。您可借助这些变量，以每项违规的特定详细信息来自定义通知。

Procedure

步骤 1 依次选择**邮件策略 (Mail Policies) > 文本资源 (Text Resources)**。

步骤 2 单击**添加文本资源 (Add Text Resource)**。

步骤 3 对于**类型 (Type)**，请选择 **DLP 通知模板 (DLP Notification Template)**。

DLP 变量不可用于纯文本通知模板。

步骤 4 请输入通知文本和变量。

此通知应该向其收件人指出，外发邮件可能包含违反组织防数据丢失策略的敏感数据。

What to do next

在 DLP 策略管理器上，在 DLP 策略的邮件操作中，指定此 DLP 通知模板。

相关主题

- DLP 通知模板变量定义, on page 26

DLP 通知模板变量定义

使用下列变量可在通知中包括有关每项 DLP 违规的特定信息。

变量	替换内容
$DLPPolicy	替换为违反的邮件 DLP 策略的名称。
$DLPSeverity	替换为违规严重性。可以是“低”(Low)、“中”(Medium)、“高”(High) 或“严重”(Critical)。
$DLPRiskFactor	替换为邮件敏感资料的风险系数（得分 0 - 100）。
$To	替换为邮件“收件人:”(To:) 信头（不是“信封收件人”[Envelope Recipient]）。
$From	替换为邮件“发件人:”(From:) 信头（不是“信封收件人”[Envelope Recipient]）。
$Subject	替换为原始邮件的主题。
$Date	替换为当前日期，采用 MM/DD/YYYY 格式。
$Time	替换为本地时区中的当前时间。
$GMTimestamp	替换为当前时间和日期，即电子邮件的“接收时间：”(Received:) 行中的时间，采用 GMT 时间。
$MID	替换为邮件 ID，或内部用来标识邮件的“MID”。请勿与 RFC822 的“Message-Id”值（使用 $Header 检索该值）混淆。
$Group	替换为注入邮件时发件人匹配的发件人组的名称。如果发件人组没有名称，则会插入字符串“>Unknown<”。
$Reputation	替换为发件人的 IP 信誉得分。如果没有信誉得分，会替换为“None”。
$filenames	替换为邮件附件文件名的逗号分隔列表。
$filetypes	替换为邮件附件文件类型的逗号分隔列表。
$filesizes	替换为邮件附件文件大小的逗号分隔列表。
$remotehost	替换为将邮件发送到思科设备的系统的主机名。
$AllHeaders	替换为邮件信头。
$EnvelopeFrom	替换为邮件的信封发件人（即，<MAIL FROM>）。
$Hostname	替换为邮件网关的主机名。
$bodysize	替换为邮件的大小（以字节为单位）。

变量	替换内容
$header[‘*string*’]	如果原始邮件包含匹配的信头，则替换为被引用信头的值。请注意，也可以使用双引号。
$remoteip	替换为将邮件发送给邮件网关的系统的 IP 地址。
$recvlistener	替换为接收邮件的侦听程序的昵称。
$dropped_filenames	与 $filenames 相同，但显示已丢弃的文件的列表。
$dropped_filename	仅返回最近丢弃的文件名。
$recvint	替换为接收邮件的接口的昵称。
$timestamp	替换为当前时间和日期，即电子邮件的“接收时间：”(Received:)行中的时间，采用本地时区时间。
$Time	替换为本地时区中的当前时间。
$orgid	替换为 SenderBase 组织 ID（整数值）。
$enveloperecipients	替换为邮件的所有信封收件人（信封目标，<RCPT TO>）。
$dropped_filetypes	与 $filetypes 相同，但显示已丢弃的文件类型的列表。
$dropped_filetype	仅返回最近丢弃的文件的文件类型。

在邮件跟踪中显示敏感 DLP 数据

DLP 部署可以记录违反 DLP 策略的内容及其周围的内容，您可以随后在“邮件跟踪”中查看这些内容。此内容可能包含敏感数据（例如信用卡号和社会保险号）。

准备工作

启用“邮件跟踪”(Message Tracking)。请参阅启用邮件跟踪

Procedure

步骤 1 选择**安全服务 (Security Services) > 防数据丢失 (Data Loss Prevention)**。

步骤 2 单击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用匹配内容日志记录 (Enable Matched Content Logging)** 复选框。

步骤 4 提交并确认更改。

What to do next

指定哪些管理用户可以查看此信息。请参阅控制对“邮件跟踪”中敏感信息的访问权限。

相关主题

- 邮件跟踪详细信息

关于更新 DLP 引擎和内容匹配分类器

邮件网关上思科 DLP 引擎和预定义内容匹配分类器的更新与其他安全服务的更新无关。

相关主题

- 确定 DLP 引擎的当前版本 , on page 28
- 手动更新 DLP 引擎和内容匹配分类器 , on page 28
- 启用自动更新（不建议） , on page 29
- 集中（集群式）邮件网关上的 DLP 更新 , on page 29

确定 DLP 引擎的当前版本

Procedure

步骤 1 依次选择**安全服务 (Security Services) > 防数据丢失 (Data Loss Prevention)**。

步骤 2 查看**当前 DLP 版本文件 (Current DLP Version Files)** 部分。

Note 还可以使用 `dlpstatus` CLI 命令查看 DLP 引擎的当前版本。有关详细信息，请参阅《适用于思科安全邮件网关的 *AsyncOS CLI* 参考指南》。

手动更新 DLP 引擎和内容匹配分类器

准备工作

请参阅以下内容：

- （如果适用）集中（集群式）邮件网关上的 DLP 更新 , on page 29

Procedure

步骤 1 选择 **安全服务 (Security Services) > 数据丢失预防 (Data Loss Prevention)**。

步骤 2 在**当前 DLP 版本文件 (Current DLP Version Files)** 部分中，单击**立即更新 (Update Now)**。

仅当有可供下载的新更新时，此按钮才可用。

Note 还可以使用 `dlpupdate` CLI 命令更新 DLP 引擎。有关详细信息，请参阅《适用于思科安全邮件网关的 *AsyncOS CLI* 参考指南》。

启用自动更新（不建议）

使用此过程可使邮件网关能够定期查找并下载更新。

Note 思科建议您不要启用自动更新。这些更新可能会更改DLP策略中使用的内容匹配分类器。而是先手动下载 DLP 更新并在实验室环境中测试这些更新，然后再更新生产环境中使用的邮件网关。

准备工作

- 在**安全设置 (Security Settings) > 服务更新 (Service Updates)** 页面上，确保已针对所有服务更新启用自动更新并指定更新间隔。
- 请参阅 集中（集群式）邮件网关上的 DLP 更新 , on page 29。

Procedure

步骤 1 选择**安全服务 (Security Services) > 防数据丢失 (Data Loss Prevention)**。

步骤 2 单击**编辑设置 (Edit Settings)**。

步骤 3 选中**启用自动更新 (Enable automatic updates)** 复选框。

步骤 4 提交并确认更改。

集中（集群式）邮件网关上的 DLP 更新

请注意以下提示：

- 无法为集群式部署中的邮件网关启用自动 DLP 更新。
- DLP 更新始终在计算机级别执行，与在集群、计算机或组级别配置的 DLP 无关。
- 只能在计算机级别使用 **`dlpstatus`** CLI 命令检查邮件网关 DLP 引擎的状态。

处理 DLP 事件邮件及数据

Note 根据适用于您的部署的情况，另请参阅思科安全邮件和 Web 管理器的文档。

收件人	相应操作
使用条件（例如DLP策略名称、违规严重性以及采取的操作）来搜索包含DLP违规的邮件，并查看所找到的邮件的详细信息	请参阅邮件跟踪。
查看或管理已隔离为疑似 DLP 违规的邮件	请参阅处理策略、病毒或爆发隔离区中的邮件。
查看 DLP 事件摘要	请参阅使用邮件安全监控中有关 DLP 事件摘要报告的信息。
查看关于在外发邮件中发现的 DLP 违规的信息	请参阅使用邮件安全监控中有关 DLP 事件报告的信息。

相关主题

- 在邮件跟踪中显示敏感 DLP 数据 , on page 27
- 控制对“邮件跟踪”中敏感信息的访问权限

防数据丢失故障排除

DLP 无法在邮件附件中检测违规

问题

使用预定义的 DLP 策略时，DLP 无法在邮件附件中检测违规。这可能是由以下原因引起的：

- 预定义 DLP 策略中接近度参数的值较小

Note 您无法更改预定义 DLP 策略的接近度。

- 预定义 DLP 策略中定义的高严重性标度参数

解决方案

- 创建自定义策略，并根据需要调整接近度。请参阅 创建自定义 DLP 策略（高级） , on page 8
- 降低预定义 DLP 策略的严重性标度参数。请参阅 调整严重性刻度 , on page 20