分配管理任务

本章包含以下部分：

处理用户帐户

邮件网关提供两种添加用户账号的方法：在邮件网关上创建用户账号；使用您自己的集中身份验证系统（可以是 LDAP 或 RADIUS 目录）启用用户身份验证。可以在 GUI 中的**系统管理 (System Administration) > 用户 (Users)** 页面上（或使用 CLI 中的 **`userconfig`** 命令）管理用户和指向外部身份验证源的连接。有关使用外部目录对用户进行身份验证的信息，请参阅外部身份验证, on page 23。

admin 是系统的默认用户账户，具有所有管理权限。不能删除 admin 用户账户，但可以更改密码以及锁定该账户。

在创建新用户帐户时，可将该用户分配给某一预定义或自定义用户角色。每个角色包含系统之内不同级别的权限。

虽然对可在该邮件网关上创建的用户账号数量并无限制，但不能使用系统保留的名称来创建用户账号。例如，不能创建名为“operator”或“root”的用户账户。

用户角色

Table 1: 用户角色列表

用户角色	说明
admin	admin 用户是系统的默认用户帐户，并且拥有完全管理权限。此处列出 admin 用户账户是出于方便考虑，但该账户不能通过用户角色分配，也不能编辑或删除，只能更改密码。 只有 admin 用户可以发出 **resetconfig** 和 revert 命令。
管理员 (Administrator)	具有“管理员 (Administrator)”角色的用户账户具有系统的所有配置设置的完全访问权限。不过，只有“管理员”(admin) 用户有权访问 **resetconfig** 和 **revert** 命令。 **Note** AsyncOS 不支持多个管理员同时通过 GUI 配置邮件网关。
技术人员 (Technician)	具有“技术人员”(Technician) 角色的用户账号可以执行系统升级、重新引导邮件网关，以及管理功能密钥。为对邮件网关进行升级，“技术人员”(Technician) 还可以执行以下操作： • 暂停邮件传送和接收。 • 查看工作队列和侦听程序的状态。 • 保存及通过邮件发送配置文件。 • 备份安全列表和阻止列表。“技术人员”(Technician) 不能恢复这些列表。 • 断开邮件网关与集群的连接。 • 启用或禁用对思科技术支持的远程服务访问权限。 • 提交支持请求。
操作员 (Operator)	具有“操作员”(Operator) 角色的用户账户限制执行以下操作： • 创建或编辑用户账户。 • 发出 **resetconfig** 命令。 • 升级邮件网关。 • 发出 **systemsetup** 命令或运行“系统设置”(System Setup) 向导。 • 发出 **adminaccessconfig** 命令。 • 执行某些隔离区功能（包括创建、编辑、删除和集中隔离区）。 • 在启用 LDAP 进行外部身份验证的情况下，修改除用户名和密码以外的 LDAP 服务器配置文件设置。 除上述情况外，他们所拥有的权限与管理员角色相同。
访客 (Guest)	具有“访客”(Guest) 角色的用户账户只能查看状态信息和报告。如果在隔离区中启用了访问权限，则具有“访客”(Guest) 角色的用户还可管理隔离区中的邮件。具有“访客 (Guest)”角色的用户不能访问邮件跟踪。

用户角色	说明
只读操作员 (Read-Only Operator)	具有“只读操作员”(Read-Only Operator) 角色的用户账户才有查看配置信息的访问权限。具有“只读操作员”(Read-Only Operator) 角色的用户可以执行和提交更改，以了解如何配置功能，但不能确认更改。如果在隔离区中启用了访问权限，则具有此角色的用户可以管理隔离区中的邮件。 具有此角色的用户不能访问以下内容： • 文件系统、FTP 或 SCP。 • 用于创建、编辑、删除或集中隔离区的设置。
服务中心用户 (Help Desk User)	具有“服务中心用户”(Help Desk User) 角色的用户账户限制执行以下操作： • 邮件跟踪。 • 管理隔离区中的邮件。 具有此角色的用户不能访问系统的其余部分，包括CLI。需要启用每个隔离区中的访问权限，然后具有此角色的用户才能管理它们。
自定义用户角色 (Custom user role)	具有“自定义用户角色”(Custom user role) 的用户账户只能访问分配给该角色的邮件安全功能。这些功能可以是 DLP 策略、邮件策略、报告、隔离区、本地邮件跟踪、加密配置文件跟踪调试工具以及访问日志订用、日志记录API和日志文件的任意组合。此类用户不能访问系统配置功能，包括全局启用功能。只有管理员可以定义自定义用户角色。有关详细信息，请参阅管理授权管理的自定义用户角色, on page 9。 **Note** 分配了自定义角色的用户不能访问 CLI。
云角色	云邮件安全设备使用一组专为云环境设计的用户角色。有关为云用户定义的角色的信息，请参阅管理思科安全云邮件网关 , on page 6。

除“服务中心用户”角色和自定义用户角色（他们只能访问 GUI）以外，上表中定义的所有角色均可访问 GUI 和 CLI。

如果使用 LDAP 目录验证用户，可以将目录组分配给用户角色（而不是单个用户）。为目录组分配用户角色时，该组中的每个用户都会收到为该用户角色定义的权限。有关详细信息，请参阅外部身份验证, on page 23。

相关主题

- 管理用户, on page 3

管理用户

“用户”(Users) 页面列出系统的现有用户，包括用户名、完整名称和用户类型或组。

从“用户”(Users) 页面，可以执行以下操作：

- 添加新用户。有关详细信息，请参阅添加用户 , on page 4。
- 删除用户。有关详细信息，请参阅删除用户, on page 5。
- 编辑用户，如更改用户的密码，以及锁定和解锁用户账户。有关详细信息，请参阅编辑用户, on page 5。
- 强制用户更改密码。请参阅强制用户更改其密码, on page 5。
- 配置本地账户的用户账户和密码设置。有关详细信息，请参阅配置受限制的用户帐户和密码设置, on page 20。
- 使邮件网关能够使用 LDAP 或 RADIUS 目录对用户进行身份验证。有关详细信息，请参阅外部身份验证, on page 23。
- 启用非管理员对“邮件跟踪”(Message Tracking) 中的“DLP 匹配内容”(DLP Matched Content) 的访问权限。有关详细信息，请参阅控制对“邮件跟踪”中敏感信息的访问权限, on page 5。

相关主题

管理思科安全云邮件网关 , on page 6

添加用户

准备工作

- 确定要使用的用户角色。
  - 有关预定义用户角色的说明，请参阅用户角色 , on page 2。
  - 要创建自定义角色，请参阅管理授权管理的自定义用户角色, on page 9。
- 指定密码要求。请参阅配置受限制的用户帐户和密码设置, on page 20。

Procedure

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 点击**添加用户 (Add User)**。

步骤 3 为用户输入登录名。某些词语是保留词语（如“operator”或“root”）。

步骤 4 输入用户的完整名称。

步骤 5 选择预定义或自定义用户角色。

步骤 6 输入密码。

Note 除了手动创建登录密码之外，您还可以创建系统生成的密码以登录邮件网关。

步骤 7 提交并确认更改。

编辑用户

使用以下过程执行更改密码等操作。

Procedure

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。
步骤 2 在“用户 (Users)”列表中点击用户名。
步骤 3 对用户进行更改。
步骤 4 提交并确认更改。

强制用户更改其密码

Procedure

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。
步骤 2 从“用户”(Users) 列表中选择用户。
步骤 3 点击**强制密码更改 (Enforce Passphrase Change)**。
步骤 4 选择用户是必须在下次登录时更改密码，还是必须在指定持续时间（以天为单位）之后更改密码。
步骤 5 （可选）如果在指定持续时间后强制更改密码，请设置在密码到期后重置密码的宽限期（以天为单位）。
步骤 6 点击**确定 (OK)**。
步骤 7 提交并确认更改。

删除用户

Procedure

步骤 1 点击对应“用户”(Users) 列表中用户名的垃圾桶图标。
步骤 2 在出现的警告对话框中点击**删除 (Delete)**，确认删除。
步骤 3 确认您的更改。

控制对“邮件跟踪”中敏感信息的访问权限

您可能希望限制对可能包含敏感信息的邮件详细信息的管理访问：

- 违反防数据丢失 (DLP) 策略的邮件可能包含公司机密信息或个人信息（包括信用卡号和健康记录）等信息。默认情况下，对邮件网关具有访问权限的所有用户都可以看到此内容。
- 由爆发过滤器或基于 URL 信誉或类别的内容过滤器捕获的 URL 也可能被视为是敏感的。默认情况下，只有具有管理员权限的用户才能查看此内容。

这些敏感内容显示在“邮件跟踪”(Message Tracking) 结果中所列邮件的“邮件详细信息”(Message Details) 页面上的专用选项卡中。

您可以根据管理用户的用户角色将这些选项卡及其内容向管理用户隐藏。虽然有一个选项可以向具有管理员角色的用户隐藏此敏感内容，但具有管理员角色的任何用户（包括云管理员用户）都可以更改这些权限，从而可以随时查看这些敏感信息。

准备工作

确保您已满足这些功能的前提条件。请参阅在邮件跟踪中显示 URL 详细信息。

Procedure

步骤 1 依次转到**系统管理 (System Administration) > 用户 (Users)** 页面。

步骤 2 在**对邮件跟踪中敏感信息的访问 (Access to Sensitive Information in Message Tracking)**下，点击**编辑设置 (Edit Settings)**。

步骤 3 选择要为其授予每种敏感信息的访问权限的角色。

无权访问“邮件跟踪”(Message Tracking) 的自定义角色永远不能查看此信息，因此不会列出。

步骤 4 提交并确认更改。

What to do next

相关主题

- 邮件跟踪详细信息
- 在邮件跟踪中显示敏感 DLP 数据
- 在邮件跟踪中显示 URL 详细信息

管理思科安全云邮件网关

在管理思科安全云邮件网关服务时，有一些管理任务是由思科安全专家执行的，还有一些管理任务可由组织的成员执行。为了满足组织中思科安全云邮件网关用户的需要，思科安全云邮件网关服务包括以下基于云的角色：

Table 2: 云用户角色列表

云用户角色	说明
云管理员 (Cloud Administrator)	“云管理员”(Cloud Administrator) 角色是为思科安全云邮件网关创建的特殊管理员角色，旨在允许访问特定于云管理员角色的特定管理任务。该角色具有很多与内部管理员相同的权限，但不能执行可能干扰思科安全云邮件网关服务正常运行的活动，如关闭设备、运行安装或更新设备。 可为多个用户分配“云管理员”(Cloud Administrator) 角色。默认情况下，在调配时为至少一个用户分配此角色。 **Note** “云管理员”(Cloud Administrator) 是可以访问 CLI 的唯一云用户角色。其他云用户只有 GUI 访问权限。 有关详细信息，请参阅云管理员 (Cloud Administrator), on page 8。
云操作员 (Cloud Operator)	“云操作员”(Cloud Operator) 的用户账户具有有限的管理权限。此用户具有对邮件策略、DLP 策略、报告、邮件跟踪、调试跟踪功能，以及垃圾邮件和系统隔离区的完全访问权限。 必须启用对 IronPort 垃圾邮件隔离区和系统隔离区的访问权限，具有此角色的用户才能管理它们。 有关详细信息，请参阅云操作员 (Cloud Operator), on page 9。
云 DLP 管理员 (Cloud DLP Admin)	此用户账户用于履行管理 DLP 策略职能的云用户。此用户具有对 DLP 策略管理的完全访问权限。 有关详细信息，请参阅云 DLP 管理员 (Cloud DLP Admin), on page 9。
云服务中心 (Cloud Help Desk)	此用户账户用于“云服务中心用户”(Cloud Help Desk User)。此用户具有对邮件跟踪以及垃圾邮件和系统隔离区的完全访问权限。 必须启用对 IronPort 垃圾邮件隔离区和系统隔离区的访问权限，具有此角色的用户才能管理它们。 有关详细信息，请参阅云服务中心 (Cloud Help Desk), on page 9。
云访客 (Cloud Guest)	此用户账户用于可能希望运行报告或访问 IronPort 垃圾邮件隔离区和系统隔离区的云访客。此用户具有对报告和隔离区的完全访问权限。 必须启用对 IronPort 垃圾邮件隔离区和系统隔离区的访问权限，具有此角色的用户才能管理它们。 有关详细信息，请参阅云访客 (Cloud Guest), on page 9。
自定义用户角色 (Custom user role)	具有“自定义用户角色”(Custom user role) 的用户账户只能访问分配给该角色的邮件安全功能。这些功能可以是 DLP 策略、邮件策略、报告、隔离区、本地邮件跟踪、加密配置文件和跟踪调试工具的任意组合。用户不能访问系统配置功能。只有云管理员可以定义自定义用户角色。有关详细信息，请参阅管理授权管理的自定义用户角色, on page 9。

云管理员 (Cloud Administrator)

“云管理员”(Cloud Administrator) 角色旨在允许组织的成员执行思科安全云邮件网关服务的一些管理功能，但其管理权限受到限制，以防干扰由思科邮件安全专家处理的任务。

思科邮件安全专家负责更改网络接口、更改安全服务更新设置、启动和关闭设备、管理集群，以及维护和更新配置。

具有“云管理员”(Cloud Administrator) 角色的用户账户可以执行以下管理任务：

- 创建或修改属于“云管理员”(Cloud Administrator) 角色的用户
- 创建和修改自定义用户角色（具有有限权限）
- 创建和重置密码（但不能修改密码策略）
- 用户管理，如创建新用户，以及锁定和解锁账户
- 访问和运行报告，以及跟踪邮件
- 创建邮件策略和内容过滤器
- 创建和修改 DLP 策略
- 运行跟踪调试工具
- 配置和修改加密配置文件
- 访问系统隔离区和 IronPort 垃圾邮件隔离区
- 保存、修改和加载安全列表/阻止列表文件

“云管理员”(Cloud Administrator) 角色不能执行下面这组选定的管理任务：

- 修改网络接口设置（包括路由和证书）
- 关闭和重新引导设备
- 将软件升级应用于设备
- 禁用集群化，以及将设备添加到集群或从集群中删除设备
- 创建或删除管理员
- 更改安全服务更新设置
- 加载配置文件或重置配置
- 修改“外部身份验证”(External Authentication) 设置
- 修改计划报告设置
- 修改警报设置
- 修改密码账户策略，如密码强度设置
- 运行“系统安装”(System Setup) 向导

在使用外部身份验证时，如果某一用户所属的组映射到“云管理员”(Cloud Administrator) 角色，将为该用户分配“云管理员”(Cloud Administrator) 的权限。

云操作员 (Cloud Operator)

“云操作员”(Cloud Operator) 角色具有对邮件策略、DLP 策略、报告、邮件跟踪、调试跟踪功能，以及垃圾邮件和系统隔离区的完全访问权限。

“操作员”(Operator) 角色具有很多与“云管理员”(Cloud Administrator) 角色相同的权限，但不能执行以下活动：

- 创建或编辑用户账户。
- 执行一些隔离区功能（包括创建和删除隔离区）。

云 DLP 管理员 (Cloud DLP Admin)

“云 DLP 管理员”角色旨在允许用户具有对 DLP 策略的完全访问权限。此用户具有对邮件网关上的所有 DLP 策略的完全访问权限，包括能够创建新策略。DLP 管理器还可以对 DLP 策略管理器中的 DLP 策略重新排序。

有关防数据丢失的详细信息，请参阅防数据丢失

云服务中心 (Cloud Help Desk)

“云服务中心”(Cloud Help Desk) 角色旨在允许用户具有对邮件跟踪以及垃圾邮件和系统隔离区的完全访问权限，以便为最终用户提供支持。“云服务中心”(Cloud Help Desk) 用户可以查看已分配的隔离区，并对它们进行操作，如放行或删除邮件，但不能更改隔离区的配置，如隔离区的大小、保留时间，并且他们不能创建或删除隔离区。

云访客 (Cloud Guest)

此账户专为希望跟踪信息、但不一定需要修改基础设施配置的用户而设计。“云访客”(Cloud Guest) 账户具有对报告以及系统和垃圾邮件隔离区的完全访问权限。“云访客”(Cloud Guest) 用户可以查看已分配的隔离区，并对它们进行操作，如放行或删除邮件，但不能更改隔离区的配置，如隔离区的大小、保留时间，并且他们不能创建或删除隔离区。

必须启用对 IronPort 垃圾邮件隔离区和系统隔离区的访问权限，具有此角色的用户才能管理它们。

管理授权管理的自定义用户角色

可以设计自定义用户角色，以及向用户授权与其在组织内的角色一致的特定职责，允许这些授权的管理员仅访问他们负责的邮件安全功能，而不能访问与其角色无关的系统配置功能。通过授权管理，用户可以比预定义的管理员、操作员和服务中心用户角色更灵活地控制对邮件网关上的邮件安全功能的访问。

例如，您可能有负责管理邮件网关上特定域的邮件策略的用户，但您不希望这些用户访问系统管理和安全服务配置功能，这些功能是由预定义的管理员和操作员角色授权的。您可以为邮件策略管理员创建自定义用户角色，这些邮件策略管理员可向这些用户授予对其所管理的邮件策略的访问权限，以及对其他邮件安全功能（他们可以使用这些功能管理由这些策略处理的邮件）的访问权限，如“邮件跟踪”(Message Tracking) 和策略隔离区。

使用 GUI 中的**系统管理 (System Administration) > 用户角色 (User Roles)** 页面（或 CLI 中的 **`userconfig -> role`** 命令）定义自定义用户角色，以及管理他们负责的邮件安全功能，如邮件策略、DLP 策略、邮件报告和隔离区。有关授权的管理员可以管理的邮件安全功能的完整列表，请参阅分配访问权限, on page 11。还可以在使用**系统管理 (System Administration) > 用户 (Users)** 页面添加或删除本地用户帐户时创建自定义角色。有关详细信息，请参阅在添加用户帐户时定义自定义用户角色, on page 17。

您应确保在创建自定义用户角色时，该角色的职责不会与其他授权的管理员的职责重叠过多。例如，如果多个授权的管理员负责同一内容过滤器，并在不同的邮件策略中使用该内容过滤器，则由一个授权的管理员对该过滤器所做的更改，可能会对由其他授权的管理员管理的邮件策略造成意想不到的副作用。

如果您已创建了自定义用户角色，则可以像任何其他用户角色一样，向他们分配本地用户和外部身份验证组。有关详细信息，请参阅处理用户帐户, on page 1。请注意，分配给自定义角色的用户不能访问 CLI。

相关主题

- “帐户权限”(Account Privileges) 页面, on page 10
- 分配访问权限, on page 11
- 定义自定义用户角色, on page 16
- 在添加用户帐户时定义自定义用户角色, on page 17
- 更新自定义用户角色的职责 , on page 17
- 编辑自定义用户角色, on page 18
- 复制自定义用户角色, on page 18
- 删除自定义用户角色, on page 18

“帐户权限”(Account Privileges) 页面

在某一授权的管理员登录到邮件网关时，“帐户权限”(Account Privileges) 页面将显示指向该授权的管理员所负责的安全功能的链接，及其访问权限的简短说明。授权的管理员可以通过选择“选项”(Options) 菜单中的“账户权限”(Account Privileges) 返回到此页面。授权的管理员还可以使用位于网页顶部的菜单访问其所管理的功能。

下图显示了具有对邮件策略、邮件报告、邮件跟踪和隔离区的访问权限的授权的管理员“帐户权限”(Account Privileges) 页面。

Figure 1: 授权的管理员的“帐户权限”***(Account Privileges)*** 页面

下图显示了具有对邮件策略、高级恶意软件保护、邮件报告、消息跟踪和隔离的访问权限的授权的管理员“帐户权限”(Account Privileges) 页面。

Figure 2: 授权的管理员的“帐户权限”***(Account Privileges)*** 页面

分配访问权限

在创建自定义用户角色时，您应定义对授权的管理员所负责的安全功能的访问权限的级别。

可供授权的管理员管理的安全功能包括：

- 传入和传出邮件策略，以及内容过滤器
- 防数据丢失 (DLP) 策略
- AMP 配置
- 邮件报告
- 邮件跟踪
- 跟踪调试工具
- 垃圾邮件、策略、病毒和爆发隔离
- 思科邮件加密配置文件
- 日志订用

在定义自定义用户角色的访问权限级别之后，您需要分配授权的管理员将要负责的特定邮件策略、内容过滤器、DLP 策略、隔离区或加密配置文件。

例如，您可以创建两个负责不同 DLP 策略的不同 DLP 策略管理员角色。其中一个角色仅负责与公司保密性和可接受的使用有关的 DLP 违规，而另一个角色则负责与隐私保护有关的 DLP 违规。除了 DLP 策略访问权限以外，还可以为这些自定义用户角色分配跟踪邮件数据以及查看隔离区和报告的权限。他们可以使用邮件跟踪搜索与他们所负责的策略相关的 DLP 违规。

可以通过点击“用户角色”(User Roles) 页面上“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 表中已分配权限的链接，查看可将哪些职责分配给自定义用户角色。请参阅更新自定义用户角色的职责 , on page 17。

相关主题

- 邮件策略和内容过滤器, on page 12
- DLP 策略, on page 13
- AMP 配置, on page 14
- 邮件报告, on page 15
- 邮件跟踪, on page 15
- 跟踪, on page 16
- 隔离区, on page 16
- 加密配置文件：, on page 16
- 日志订用, on page 16

邮件策略和内容过滤器

邮件策略和内容过滤器访问权限定义授权的管理员对邮件网关上的传入和传出邮件策略及内容过滤器的访问权限级别。可将特定的邮件策略和内容过滤器分配给自定义用户角色，仅允许属于此角色的授权的管理员，与操作员和管理员一起，管理邮件策略和内容过滤器。

具有此访问权限的所有授权的管理员可以查看默认传入和传出邮件策略，但如果他们具有完全访问权限，只能编辑这些策略。

具有访问权限的所有授权的管理员可以创建新内容过滤器，以与其邮件策略一起使用。由某一授权的管理员创建的内容过滤器可供分配到该自定义用户角色的其他授权的管理员使用。未分配给任何自定义用户角色的内容过滤器都是公共的，并且可由所有具有邮件策略访问权限的授权的管理员查看。默认情况下，由操作员或管理员创建的内容过滤器是公共的。授权的管理员可以启用或禁用针对已分配给其自定义用户角色的所有现有的内容过滤器，但不能修改或删除公共内容过滤器。

如果某一授权的管理员删除了由他们自己的邮件策略以外的其他邮件策略使用的某一内容过滤器，或者如果该内容过滤器已分配给其他自定义用户角色，则 AsyncOS 不会从系统中删除该内容过滤器。相反，AsyncOS 将会取消内容过滤器与自定义角色的链接，并将其从该授权的管理员的邮件策略中删除。内容过滤器仍可用于其他自定义用户角色和邮件策略。

授权的管理员可在其内容过滤器中使用任何文本资源或词典，但他们不能访问 GUI 中的“文本资源”(Text Resources) 或“词典”(Dictionaries) 页面来查看或修改它们。授权的管理员也不能创建新文本资源或词典。

对于传出邮件策略，授权的管理员可以启用或禁用 DLP 策略，但他们不能自定义 DLP 设置，除非他们还具有 DLP 策略权限。

可为自定义用户角色分配对邮件策略和内容过滤器的以下访问权限级别之一：

- **无访问权限 (No access)**：授权的管理员不能查看或编辑邮件网关上的邮件策略和内容过滤器。
- **查看已分配，编辑已分配 (View assigned, edit assigned)**：授权的管理员可以查看和编辑分配给自定义用户角色的邮件策略及内容过滤器，还可创建新内容过滤器。授权的管理员可以编辑策略的“反垃圾邮件”(Anti-Spam)、“防病毒”(Anti-Virus) 和“爆发过滤器”(Outbreak Filters) 设置。他们可为策略启用其内容过滤器，以及禁用分配给策略的所有现有内容过滤器，而无论他们是否负责该策略。授权的管理员不能修改邮件策略的名称或其发件人、收件人或组。授权的管理员可以修改分配给其自定义用户角色的邮件策略的内容过滤器的顺序。
- **查看全部，编辑已分配 (View all, edit assigned)**：授权的管理员可以查看邮件网关上的所有邮件策略和内容过滤器，但他们只能编辑分配给该自定义用户角色的邮件策略和内容过滤器。

查看全部，编辑全部（完全访问权限）(View all, edit all [full access])：授权的管理员具有对邮件网关上所有邮件策略和内容过滤器的完全访问权限，包括默认邮件策略，并能创建新邮件策略。授权的管理员可以修改所有邮件策略的发件人、收件人和组。他们还可以对邮件策略重新排序。

可以使用“邮件安全管理器”(Email Security Manager) 或“用户角色”(User Roles) 页面上的“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 表，将单个邮件策略和内容过滤器分配给自定义用户角色。

有关使用“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 表分配邮件策略和内容过滤器的信息，请参阅更新自定义用户角色的职责 , on page 17。

DLP 策略

DLP 策略访问权限通过邮件网关上的 DLP 策略管理器定义授权的管理员对 DLP 策略的访问权限级别。可将 DLP 策略分配给特定的自定义用户角色，除了操作员和管理员以外，还允许授权的管理员管理这些策略。具有 DLP 访问权限的授权的管理员还可以从“防数据丢失全局设置”(Data Loss Prevention Global Settings) 页面导出 DLP 配置文件。

如果某一授权的管理员还具有邮件策略权限，则他们可以自定义 DLP 策略。授权的管理员可以使用其 DLP 策略的任何自定义 DLP 词典，但他们无法查看或修改自定义 DLP 词典。

可为自定义用户角色分配对 DLP 策略的以下访问权限级别之一：

- **无访问权限**：授权的管理员不能查看或编辑邮件网关上的 DLP 策略。
- **查看已分配，编辑已分配**：授权的管理员可以使用 DLP 策略管理器查看和编辑分配给自定义用户角色的 DLP 策略。授权的管理员不能对 DLP 策略管理器中的 DLP 策略进行重命名或重新排序。授权的管理员可以导出 DLP 配置。
- **查看所有，编辑已分配**：授权的管理员可以查看和编辑分配给自定义用户角色的 DLP 策略。他们可以导出 DLP 配置。他们还可以查看未分配给自定义用户角色的所有 DLP 策略，但他们不能编辑这些策略。授权的管理员不能对 DLP 策略管理器中的 DLP 策略重新排序，也不能重命名策略。
- **查看全部，编辑全部（完全访问权限）(View all, edit all [full access])**：授权的管理员具有对邮件网关上的所有 RSA 邮件 DLP 策略的完全访问权限，包括能够创建新策略。授权的管理员可对 DLP 策略管理器中的 DLP 策略重新排序。他们不能更改邮件网关所使用的 DLP 模式。

可以使用 DLP 策略管理器或“用户角色”(User Roles) 页面上的“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 表，将各个 DLP 策略分配给自定义用户角色。

有关 DLP 策略和 DLP 策略管理器的详细信息，请参阅防数据丢失。

有关使用“授权管理的自定义用户角色”列表分配 DLP 策略的详细信息，请参阅更新自定义用户角色的职责 , on page 17。

AMP 配置

AMP 配置访问权限定义授权的管理员对以下权限的访问级别：

- “安全服务”下的“文件信誉和分析”
- AMP 报告 - 高级恶意软件防护（AMP 信誉）、文件分析、AMP 判定更新（文件追溯）和邮箱自动补救
- 文件分析隔离
- 邮件跟踪

您（管理员）可为自定义用户角色分配对 AMP 配置的以下访问权限级别之一：

- 无访问权限 - 授权的管理员无权访问 AMP 配置。
- 完全访问权限 - 授权的管理员具有对 AMP 配置的完全访问权限。授权的管理员可以访问 AMP 配置、AMP 报告、文件分析隔离区和邮件跟踪。

有关文件信誉和分析的详细信息，请参阅 文件信誉过滤和文件分析： 。

有关使用授权管理的自定义用户角色列表来提供访问 AMP 配置的权限的信息，请参阅 更新自定义用户角色的职责 ， 第 17 页 。

邮件报告

邮件报告访问权限根据自定义用户角色对邮件策略、内容过滤器和 DLP 策略的访问权限，定义授权的管理员可以查看哪些报告和“邮件安全监控”(Email Security Monitor) 页面。这些报告没有针对已分配的策略进行过滤；授权的管理员可以查看不属于负责的邮件和 DLP 策略的报告。

可为自定义用户角色分配对邮件报告的以下访问权限级别之一：

- **无访问权限 (No access)**：授权的管理员不能查看邮件网关上的报告。
- **查看相关报告 (View relevant reports)**：授权的管理员可以查看“邮件安全监控”(Email Security Monitor) 页面上与其邮件策略、内容过滤器和 DLP 策略访问权限相关的报告。具有邮件策略和内容过滤器访问权限的授权的管理员可以查看以下“邮件安全监控”(Email Security Monitor) 页面：
  - 概述 (Overview)
  - 传入邮件 (Overview)
  - 外发目标
  - 传出邮件发件人
  - 内部用户
  - 内容过滤器 (Content Filters)
  - 病毒爆发 (Virus Outbreaks)
  - 病毒类型 (Virus Types)
  - 存档的报告 (Archived Reports)

  具有 DLP 策略访问权限的授权的管理员可以查看以下“邮件安全监控”(Email Security Monitor) 页面：
  - 概述 (Overview)
  - DLP 事件
  - 存档的报告 (Archived Reports)
- **查看所有报告 (View all reports)**：授权的管理员可以查看邮件网关上的所有报告和“邮件安全监控”(Email Security Monitor) 页面。

有关邮件报告和邮件安全监控的详细信息，请参阅使用邮件安全监控一章。

邮件跟踪

邮件跟踪访问权限定义分配给自定义用户角色的授权的管理员是否有权访问邮件跟踪；如果已在**系统管理 (System Administration) > 用户 (Users)** 页面上启用了“DLP 追踪策略”(DLP Tracking Policies) 选项，并且自定义用户角色也具有 DLP 策略访问权限，则还包括可能违反组织的 DLP 策略的邮件内容。

授权的管理员只能搜索分配给他们的 DLP 策略的 DLP 违规。

有关邮件跟踪的详细信息，请参阅邮件跟踪。

有关允许授权的管理员访问查看“邮件跟踪”(Message Tracking) 中匹配的 DLP 内容的信息，请参阅控制对“邮件跟踪”中敏感信息的访问权限, on page 5。

跟踪

跟踪访问权限定义分配给自定义用户角色的授权的管理员是否可以使用“跟踪”(Trace) 调试通过系统的邮件流。具有访问权限的授权的管理员可以运行“跟踪”(Trace) 和查看所有生成的输出。跟踪结果不会根据授权的管理员的邮件或 DLP 策略权限进行过滤。

有关使用跟踪的详细信息，请参阅使用测试邮件调试邮件流：追踪。

隔离区

隔离区访问权限定义授权的管理员是否可以管理已分配的隔离区。授权的管理员可以查看已分配的隔离区中的所有邮件，并对它们进行操作，如放行或删除邮件，但不能更改隔离区的配置（例如大小、保留时间等）。或创建或删除隔离区。

可以使用“监控”(Monitor) > “隔离区”(Quarantines) 页面或“用户角色”(User Roles) 页面上的“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 表，将任何隔离区分配给自定义用户角色。

有关将隔离区管理任务分配给管理用户的详细信息，请参阅关于向其他用户分配邮件处理任务和配置对垃圾邮件隔离区的管理用户访问权限。

有关使用“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 列表分配隔离区的信息，请参阅更新自定义用户角色的职责 , on page 17。

加密配置文件：

加密配置文件访问权限定义授权的管理员是否可在编辑内容过滤器或 DLP 策略时，使用分配给自己的自定义用户角色的加密配置文件。加密配置文件只能分配给具有邮件或 DLP 策略访问权限的自定义用户角色。未分配给自定义角色的加密配置文件可供具有邮件或 DLP 策略权限的所有授权的管理员使用。授权的管理员不能查看或修改任何加密配置文件。

在使用“安全服务”(Security Services) > “IronPort 邮件加密”(IronPort Email Encryption) 页面创建或编辑加密配置文件时，可以分配加密配置文件。

日志订用

“日志订用”(Log Subscription) 访问权限定义分配给自定义用户角色的授权管理员是否可以访问日志订用或日志 API，以便查看或下载日志文件。

定义自定义用户角色

可以使用 GUI 中的“用户角色”页（或 CLI 中的 userconfig -> role 命令）定义新用户角色和分配其访问权限。“用户角色”(User Roles) 页面显示在邮件网关上的所有现有自定义用户角色，以及每个角色的访问权限。

Procedure

步骤 1 依次选择**系统管理 (System Administration) > 用户角色 (User Roles)**。

步骤 2 点击**添加用户角色 (Add User Role)**。

步骤 3 为用户角色输入一个名称。

步骤 4 为用户角色及其权限输入一段说明。

步骤 5 选择用户角色的访问权限。（有关各种类型访问权限的详细信息，请参阅分配访问权限, on page 11。）

步骤 6 提交并确认更改。

在添加用户帐户时定义自定义用户角色

在邮件网关上添加或编辑本地用户账号时，可以创建新自定义用户角色。

有关添加用户账户的详细信息，请参阅管理用户, on page 3。

Procedure

步骤 1 依次转到**系统管理 (System Administration) > 用户 (Users)** 页面。

步骤 2 点击 **Add User**（添加用户）。

步骤 3 在创建用户账户时，选择“自定义角色”(Custom Roles)。

步骤 4 选择**添加角色 (Add Role)**。

步骤 5 为新角色输入名称。

步骤 6 提交新用户账户。

AsyncOS 显示一条通知，表示已添加新用户账户和自定义用户角色。

步骤 7 依次转到**系统管理 (System Administration) > 用户角色 (User Roles)** 页面。

步骤 8 在“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 表中，点击自定义用户角色的名称。

步骤 9 为用户角色及其权限输入一段说明。

步骤 10 选择用户角色的访问权限。（有关各种类型访问权限的详细信息，请参阅分配访问权限, on page 11。）

步骤 11 提交并确认更改。

更新自定义用户角色的职责

Procedure

步骤 1 依次转到**系统管理 (System Administration) > 用户角色 (User Roles)** 页面。

步骤 2 点击您要更新的自定义用户角色的访问权限的名称。

AsyncOS 将显示一个列表，其中包括邮件网关上可用的所有邮件策略、内容过滤器、DLP 策略或隔离区，以及任何其他已分配的自定义用户角色的名称。

步骤 3 选择您希望已分配的授权的管理员负责的邮件策略、内容过滤器、DLP 策略或隔离区。

步骤 4 提交并确认更改。

编辑自定义用户角色

Procedure

步骤 1 依次转到**系统管理 (System Administration) > 用户角色 (User Roles)** 页面。

步骤 2 在“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 列表中，点击用户角色的名称。

步骤 3 对该用户角色进行更改。

步骤 4 提交并确认更改。

复制自定义用户角色

您可能希望创建多个具有相似访问权限的自定义用户角色，但为不同的用户组分配不同的职责。例如，如果邮件网关处理多个域的邮件，您可能希望创建多个具有相似访问权限、但适用于基于该域的不同邮件策略的自定义用户角色。这样可使授权的管理员能够管理自己的域的邮件策略，而不干扰其他授权的管理员的职责。

Procedure

步骤 1 依次转到**系统管理 (System Administration) > 用户角色 (User Roles)** 页面。

步骤 2 点击与您希望在“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 列表中复制的用户角色相对应的复制图标。

步骤 3 更改自定义用户角色的名称。

步骤 4 进行新自定义用户角色所需的所有访问权限更改。

步骤 5 提交并确认更改。

删除自定义用户角色

在删除某一自定义角色后，用户将变为未分配状态，并且没有对邮件网关的访问权限。如果删除分配给一个或多个用户的自定义用户角色，则您不会收到警告消息。您应重新分配先前分配给已删除的自定义用户角色的所有用户。

Procedure

步骤 1 依次转到**系统管理 (System Administration) > 用户角色 (User Roles)** 页面。

步骤 2 点击与您希望在“授权管理的自定义用户角色”(Custom User Roles for Delegated Administration) 列表中删除的用户角色相对应的垃圾桶图标。

步骤 3 在出现的警告对话框中点击**删除 (Delete)**，确认删除。

步骤 4 确认您的更改。

密码

更改密码

管理用户可以通过位于 GUI 顶部的“选项”>“更改密码”链接更改他们自己的密码。

提交新密码后，系统会立即将您注销并转到登录屏幕。

在 CLI 中，使用 passphrase 或 passwd 命令更改密码。如果忘记了管理员用户账户的密码，请联系您的客户支持提供商重置密码。

Note 除了手动创建登录密码之外，您还可以创建系统生成的密码以登录邮件网关。

为了安全起见，passphrase 命令要求输入旧密码。

Note 密码更改会立即生效，并且不会要求您确认更改。

锁定和解锁用户帐户

锁定用户账号防止本地用户登录邮件网关。可以通过以下方式之一锁定用户账户：

- 如果某一用户超过了“本地用户账户和密码设置”部分中定义的最大尝试登录失败次数，AsyncOS 将锁定该用户账户。

- 管理员可以为了安全目的，使用“系统管理”(System Administration) > “用户”(Users) 页面手动锁定用户账户。

在查看“编辑用户”(Edit User) 页面上的用户帐户时，AsyncOS 将显示用户帐户被锁定的原因。

要解锁用户账户，请通过点击“用户”(Users) 列表中的用户名打开用户账户，然后点击**解锁账户 (Unlock Account)**。

要手动锁定本地用户账户，请通过点击“用户”(Users) 列表中的用户名打开用户账户，然后点击**锁定账户 (Lock Account)**。AsyncOS 将显示一条消息，表示用户无法登录到邮件网关，并询问是否要继续。

如果用户在已配置的尝试次数后未能成功登录，您还可以将所有本地用户账户配置为锁定。有关详细信息，请参阅配置受限制的用户帐户和密码设置, on page 20。

Note 如果锁定“admin”账户，您仅能通过到串行控制台端口的串行通信连接，以管理员身份登录后，才能解锁该管理账户。即使在 admin 帐户被锁定时，admin 用户也可以使用串行控制台端口访问邮件网关。有关使用串行控制台端口访问邮件网关的详细信息，请参阅连接到邮件网关。

配置受限制的用户帐户和密码设置

可以通过定义用户帐户和密码限制来实施组织密码策略。用户账号和密码限制适用于在邮件网关上定义的本地用户。您可以配置以下设置：

- **用户账户锁定 (User account locking)**。可以定义导致用户账户被锁定的失败登录尝试次数。
- **密码有效期规则**。可以定义密码的有效期，在该期限之后，用户登录后需要更改密码。
- **密码规则**。可以定义用户可选择的密码类型，例如哪些字符是可选的或必需的。

可以在“本地用户账户和密码设置”部分的“系统管理”(System Administration) > “用户”(Users) 页面上定义用户账户和密码限制。

云用户帐户

云用户帐户已预配置密码设置，不能由云管理员更改。以下密码设置是为云用户配置的：

- 用户必须在首次登录时更改其密码。
- 用户必须每 6 个月更改一次密码。
- 密码必须包含至少八个字符；并且密码必须包含一个大写字符 (A-Z)、一个小写字符 (a-z)、一个数字字符 (1-9) 和一个特殊字符（如 @#$%）。

Procedure

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 滚动到**本地用户账户和密码设置**部分。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 按以下说明配置设置。

设置	说明
用户账户锁定 (User Account Lock)	选择用户登录失败后是否锁定用户账户。指定导致账户锁定的失败登录尝试次数。您可以输入一 (1) 到 60 之间的任一数值。默认值为五 (5)。 配置账户锁定时，请输入要向尝试登录的用户显示的消息。使用 7 位 ASCII 字符组成的文本。仅在用户为被管理员锁定的账户输入正确的密码时，才会显示此消息。对于因尝试登录失败而被锁定的账户，不会显示此消息。 用户帐户被锁定后，管理员可以在 GUI 中的“编辑用户”(Edit User) 页面中或使用 userconfig 命令解锁帐户。 无论用户连接的计算机或连接类型（例如 SSH 或 HTTP）如何，用户都会跟踪失败的登录尝试。一旦用户成功登录，失败登录尝试次数就会被重置为零 (0)。 当用户账户由于达到最大失败登录尝试次数而被注销时，系统会向管理员发送警报。警报的严重级别设置为“参考 (Info)”。 **Note** 此外，还可以手动锁定各个用户账户。有关详细信息，请参阅锁定和解锁用户帐户, on page 19。

密码重置	可以选择是否：
	
	• 应在管理员更改用户的密码后，强制用户更改其密码。
	• 应在指定期限后，强制用户更改其密码。输入过多少天后用户必须更改密码。您可以输入一 (1) 到 366 之间的任一数值。默认值为 90。在这种情况下，可以选择性地选择：
	  • 显示关于即将到来的密码过期的通知。输入在到期前多少天通知用户。
	  • 留出在密码到期后重置密码的宽限期（指定天数）。输入天数。
	
	如果您设置了宽限期，则如果未在指定期限内更改密码，用户账户将被锁定。如果您未设置宽限期，则用户可在密码到期后任何时候更改其密码。
	
	Note 当用户账户使用 SSH 密钥（而不是密码质询）时，密码重置规则仍然适用。当使用 SSH 密钥的用户账户到期时，用户必须输入其旧密码或请管理员手动更改密码，才能更改与该账户相关的密钥。有关详细信息，请参阅管理安全外壳 (SSH) 密钥, on page 32。

设置	说明
密码规则： 至少需要 <数字> 个字符。	输入密码可以包含字符的最小数量。 输入 0 和 128 之间的任何数字。 默认为 8 个字符。 密码可以具有比您在此处指定的数字更多的字符。
密码规则： 至少需要一个数字 (0-9)。(Password Rules: Require at least one number (0-9).)	选择密码是否必须至少包含一个数字。
密码规则： 至少需要一个特殊字符。(Password Rules: Require at least one special character.)	选择密码是否必须包含至少一个特殊字符。密码可以包含以下特殊字符： ~ ? ! @ # $ % ^ & * - _ + = \ | / [ ] ( ) < > { } ` ' " ; : , .

密码规则：
禁止将用户名及其变体用作口令。
	选择是否允许密码与相关联的用户名或其变体形式相同。当禁止用户名变体形式时，以下规则适用于密码：
	• 密码无论如何都不能与用户名相同。
	• 密码无论如何都不能与反写的用户名相同。
	• 密码不能与替换以下字符的用户名或反写的用户名相同：
	  • “@”或“4”表示“a”
	  • “3”表示“e”
	  • “|”、“!”或“1”表示“i”
	  • “0”表示“o”
	  • “$”或“5”表示“s”
	  • “+”或“7”表示“t”

密码规则： 禁止再次使用最近<数字> 次用过的密码。	选择强制用户更改密码时，是否允许用户选择最近使用的密码。如果不允许再次使用最近的密码，请输入禁止再次使用的最近密码次数。 您可以输入一 (1) 到 15 之间的任一数值。默认值为三 (3)。
密码规则： 不允许在口令中使用的单词列表	可以创建密码中禁止使用的单词列表。 将此文件创建为文本文件，每个禁用单词单独为一行。以 forbidden_password_words.txt 为文件名保存文件并使用 SCP 或 FTP 将文件上传到设备中。 如果选择了此限制，但未上传单词表，将忽略此限制。

设置	说明
口令长度	当管理员或用户输入新密码时，可以显示密码强度指示器。 此设置不强制创建强密码，只显示猜测所输入的密码的难易程度。 选择要为其显示指标的角色。然后，为每个选定角色输入一个大于零的数值。数字越大，意味着注册为强密码的密码越难破解。此设置无最大值。 示例： • 如果输入 30，则注册为强密码的 8 位字符的密码至少包含 1 个大写和小写字母、数字和特殊字符。 • 如果输入 18，则注册为强密码的 8 位字符密码全部为小写字母，不含数字或特殊字符。 密码强度是按对数衡量的。根据美国国家标准与技术研究院在 NIST SP 800-63 中定义的熵值规则（附录 A）进行评估。 通常，高强度密码具有以下特征： • 较长 • 包含大写字母、小写字母、数字和特殊字符 • 不包含以任何语言表示的词典中的词语。 要实施具有上述这些特征的密码，请使用此页面中的其他设置。

步骤 5 提交并确认更改。

What to do next

如果您选择了**密码中不允许使用的单词列表 (List of words to disallow in passphrases)**，则请创建并上传所述的文本文件。

外部身份验证

如果您将用户信息存储在网络上的 LDAP 或 RADIUS 目录中，则可将邮件网关配置为使用外部目录对登录到该邮件网关的用户进行身份验证。要将邮件网关设置为使用外部目录进行身份验证，请使用 GUI 中的“系统管理”(System Administration) >“用户”(Users) 页面，或 CLI 中的 userconfig 命令和 external 子命令。

在启用外部身份验证后，并且用户登录到邮件网关时，该邮件网关会先确定该用户是否是系统定义的“admin”帐户。如果不是，则该邮件网关将检查配置的第一个外部服务器，以确定该用户是否是在那里定义的。如果该邮件网关无法连接到第一个外部服务器，则它将检查列表中的下一个外部服务器。

对于 LDAP 服务器，如果用户在任何外部服务器上的身份验证失败，则该邮件网关会尝试将该用户作为邮件网关上定义的本地用户进行身份验证。如果用户不存在于任何外部服务器或邮件网关上，或者如果用户输入错误的密码，则对该邮件网关的访问将被拒绝。

如果外部 RADIUS 服务器无法联系，将尝试列表中的下一个服务器。如果所有服务器都无法联系，则邮件网关会尝试将用户作为在邮件网关上定义的本地用户进行身份验证。但是，如果外部RADIUS服务器因故拒绝用户，如密码不正确或是用户缺习，则对该邮件网关的访问将被拒绝。

相关主题

- 启用 LDAP 身份验证, on page 24
- 启用 RADIUS 身份验证, on page 25
- 启用 SAML 身份验证, on page 26

启用 LDAP 身份验证

除了使用 LDAP 目录对用户进行身份验证以外，还可以将 LDAP 组分配给思科用户角色。例如，您可以将IT组中的用户分配给“管理员”(Administrator)用户角色，此外，您还可以将“支持”(Support)组中的用户分配给“服务中心用户”(Help Desk User)角色。如果用户属于具有不同用户角色的多个 LDAP 组，则 AsyncOS 会授予该用户访问最具限制性角色的权限。例如，如果用户属于具有“操作人员 (Operator)”权限的组和具有“服务中心用户 (Help Desk User)”权限的组，则 AsyncOS 会为该用户授予“服务中心用户 (Help Desk User)”角色的权限。

Note 如果外部用户更改其 LDAP 组的用户角色，则该用户应从邮件网关注销，然后重新登录。该用户将具有其新角色的权限。

准备工作

定义一个 LDAP 服务器配置文件和一个 LDAP 服务器的外部身份验证查询。有关详细信息，请参阅 LDAP 查询

Procedure

步骤 1 依次选择**系统管理 (System Administration) > 用户 (Users)**。

步骤 2 向下滚动到**外部身份验证 (External Authentication)** 部分。

步骤 3 点击**启用 (Enable)**。

步骤 4 选中**启用外部身份验证 (Enable External Authentication)** 复选框。

步骤 5 选择 **LDAP** 作为身份验证类型。

步骤 6 在网络用户界面中输入存储外部身份验证凭证的时间长度。

步骤 7 选择对用户进行身份验证的 LDAP 外部身份验证查询。

步骤 8 输入超时前邮件网关等待服务器响应的秒数。

步骤 9 输入希望邮件网关进行身份验证的 LDAP 目录中的组名称，然后选择该组中用户的角色。

步骤 10 （可选）点击**添加行 (Add Row)** 添加另一个目录组。为邮件网关进行身份验证的每个目录组重复执行步骤 9 和 10。

步骤 11 提交并确认更改。

启用 RADIUS 身份验证

您还可以使用 RADIUS 目录对用户进行身份验证，以及将用户组分配给角色。RADIUS 服务器应支持“类”(CLASS) 属性，AsyncOS 将使用该属性将 RADIUS 目录中的用户分配给用户角色。AsyncOS 支持两种用于与 RADIUS 服务器通信的身份验证协议：密码身份验证协议 (PAP) 和质询握手身份验证协议 (CHAP)。

要将 RADIUS 用户分配给思科用户角色，请先在包含字符串值 <radius-group> 的 RADIUS 服务器上设置 CLASS 属性，该字符串值将映射到思科用户角色。“类 (CLASS)”属性可以包含字母、数字和短划线，但不能以短划线开头。AsyncOS 不支持“类 (CLASS)”属性中的多个值。如果 RADIUS 用户属于某一个组，而该组不含“类”(CLASS) 属性，或者包含未映射的“类”(CLASS) 属性，则这些 RADIUS 用户不能登录到邮件网关。

如果邮件网关无法与 RADIUS 服务器通信，用户可以使用邮件网关上的本地用户账号登录。

Note 如果外部用户更改了其 RADIUS 组的用户角色，则该用户应注销设备，然后重新登录。该用户将获得新角色的权限。

Procedure

步骤 1 在**系统管理 (System Administration)** > **用户 (Users)** 页面中，点击**启用 (Enable)**。

步骤 2 如果尚未启用，请选中“启用外部身份验证”选项。

步骤 3 输入 RADIUS 服务器的主机名。

步骤 4 输入 RADIUS 服务器的端口号。默认端口号为 1812。

步骤 5 输入 RADIUS 服务器的共享密钥密码。

步骤 6 输入超时前邮件网关等待服务器响应的秒数。

步骤 7 （可选）点击**添加行 (Add Row)** 添加另一台 RADIUS 服务器。为每个 RADIUS 服务器重复步骤 3 - 6。

Note 最多可添加十个 RADIUS 服务器。

步骤 8 输入 AsyncOS 在再次与 RADIUS 服务器联系以在“外部身份验证缓存超时”(External Authentication Cache Timeout) 字段中再次进行身份验证之前，存储外部身份验证凭证的秒数。默认值为零 (0)。

Note 如果 RADIUS 服务器使用一次性密码（例如基于令牌创建的密码），请输入零 (0)。如果该值设置为零，在当前会话期间，AsyncOS 不会再次联系 RADIUS 服务器进行身份验证。

Note 缓存超时值必须是介于 0 和 86400 之间的整数（以秒为单位）。建议的最大缓存超时值为 3600。

步骤 9 配置群组映射：

设置	说明
将通过外部身份验证的用户映射到多个本地角色。	AsyncOS 将基于 RADIUS“类 (CLASS)”属性向邮件网关角色分配 RADIUS 用户。“类”(CLASS) 属性要求： • 最少 3 个字符 • 最多 253 个字符 • 无冒号、逗号或换行字符 • 每个 RADIUS 用户的一个或多个映射 CLASS 属性（通过此设置，AsyncOS 会拒绝访问不带映射 CLASS 属性的 RADIUS 用户。） 对于具有多个 CLASS 属性的 RADIUS 用户，AsyncOS 会分配最具限制性的角色。例如，如果 RADIUS 用户具有两个 CLASS 属性（映射到“操作员”[Operator] 和“只读操作员”[Read-Only Operator] 角色），则 AsyncOS 会为 RADIUS 用户分配“只读操作员”(Read-Only Operator) 角色（比“操作员”[Operator] 角色更严格）。 这些邮件网关角色按从最不严格到最严格的顺序排列。 • admin • 管理员 • 技术人员 • 操作员 cloudadmin • 只读操作员 (Read-only Operator) • 网络管理员用户 • 访客
将所有外部身份验证的用户映射为“管理员”(Administrator) 角色。	AsyncOS 将 RADIUS 用户分配到“管理员”角色。

步骤 10 选择是将所有外部身份验证的用户映射到“管理员”(Administrator) 角色，还是映射到不同的邮件网关用户角色类型。

步骤 11 如果将用户映射到不同的角色类型，请按照“组名称”(Group Name) 或“目录”(Directory) 字段中 RADIUS“类”(CLASS) 属性中的定义，输入组名称，并从“角色”(Role) 字段中选择邮件网关角色类型。可以通过点击**添加行 (Add Row)** 添加更多角色映射。

有关用户角色类型的详细信息，请参阅处理用户帐户, on page 1。

步骤 12 提交并确认更改。

启用 SAML 身份验证

您可以使用 SAML 来启用“单点登录”，以对用户进行身份验证，并将用户组分配给思科规则。

开始之前

请确保您已使用“服务提供商”和“身份提供程序”设置来配置 SAML 配置文件。请参阅如何在邮件网关上配置 SSO。

过程

步骤 1 导航至**系统管理 (System Administration)** > **用户 (Users)**。

步骤 2 向下滚动到**外部身份验证 (External Authentication)** 部分。

步骤 3 点击**启用 (Enable)**。

步骤 4 选中**启用外部身份验证 (Enable External Authentication)** 复选框。

步骤 5 从下拉列表中选择 **SAML** 作为身份验证类型。

步骤 6 （可选）在**外部身份验证属性名称映射**字段中，输入要从组映射中搜索的属性名称。

属性名称取决于为身份提供者配置以中继 SAML 响应的属性。邮件网关将从 SAML 响应中搜索与您在**组映射**字段中配置的属性匹配的属性名称条目。这是可选项。如果不配置此项，邮件网关将根据“组映射”字段中的配置搜索 SAML 响应中出现的所有属性的匹配条目。

步骤 7 在**组映射**字段中，根据预定义或自定义用户角色，输入 SAML 目录中定义的组名称属性。您可以点击**添加行 (Add Row)** 以添加多个角色映射。

组映射必须包含组属性。您可以添加“未指定组”属性以对 SAML 断言或响应进行身份验证。

有关用户角色类型的详细信息，请参阅处理用户帐户 ， 第 1 页。

注释 组映射属性区分大小写，必须完全一致才能返回正确的结果。

步骤 8 提交并确认更改。

下一步做什么

启用 SAML 外部身份验证后，您可以使用邮件网关设备登录页面上的**使用单点登录**链接，并输入用户名以登录到邮件网关。

配置对邮件网关的访问

AsyncOS 提供多种管理员控制措施，用于管理用户对邮件网关的访问，包括 Web UI 会话的超时，以及一个访问列表（它指定了用户和组织的代理服务器可通过其访问邮件网关的 IP 地址）。

相关主题

- 配置基于 IP 的网络访问, on page 28
- 配置会话超时, on page 30

配置基于 IP 的网络访问

可以通过为直接连接到设备的用户以及通过反向代理连接的用户（如果组织为远程用户使用反向代理）创建访问列表，控制用户通过哪些 IP 地址访问邮件网关。

相关主题

- 直接连接, on page 28
- 通过代理连接, on page 28
- 限制网络访问时的重要预防措施 , on page 28
- 创建访问列表 , on page 29

直接连接

可以为可连接到邮件网关的计算机指定 IP 地址、子网或 CIDR 地址。用户可以从使用访问列表中 IP 地址的任何计算机访问邮件网关。如果用户尝试从不包含在列表中的地址连接邮件网关，则用户访问会被拒绝。

通过代理连接

如果组织的网络在远程用户的计算机与邮件网关之间使用反向代理服务器，AsyncOS 将允许您创建访问列表，其中包含可连接到邮件网关的代理的 IP 地址。

即使使用反向代理，AsyncOS 仍会对照允许用户连接的 IP 地址列表验证远程用户计算机的 IP 地址。要将远程用户的 IP 地址发送到邮件网关，代理需要在邮件网关设备的连接请求中包括 x-forwarded-for HTTP 信头。

x-forwarded-for 信头是非 RFC 标准的 HTTP 信头，格式如下：

x-forwarded-for: client-ip, proxy1, proxy2,... CRLF。

此信头的值为逗号分隔的 IP 地址列表，最左边的地址为远程用户计算机的地址，之后是转发连接请求的每个后续代理的地址。（信头名称是可配置的。）邮件网关根据访问列表中允许的用户和代理 IP 地址，从信头和连接代理的 IP 地址开始匹配远程用户的 IP 地址。

Note AsyncOS 仅支持 x-forwarded-for 信头中的 IPv4 地址。

限制网络访问时的重要预防措施

警告！如果满足下列条件之一，在提交和确认网络访问更改后，可能会丧失对邮件网关的访问权限：

- 如果选择**仅允许特定连接 (Only Allow Specific Connections)**，并且不包括列表中当前计算机（PC、集群环境中的邮件网关或思科安全管理器邮件和网络网关等）的 IP 地址。
- 如果选择**仅允许通过代理的特定连接 (Only Allow Specific Connections Through Proxy)**，并且当前连接到邮件网关的代理的 IP 地址不在代理列表中，原始 IP 信头的值不在允许的 IP 地址列表中。

- 如果选择**仅允许直接或通过代理的特定连接 (Only Allow Specific Connections Directly or Through Proxy)**，并且
  - 原始 IP 信头的值不在允许的 IP 地址列表中

    或

  - 原始 IP 信头的值不在允许的 IP 地址列表中，并且连接到邮件网关的代理的 IP 地址不在允许的代理列表中。

创建访问列表

通过 GUI 或使用 **adminaccessconfig > ipaccess** CLI 命令，可创建网络访问列表。

准备工作

请确保更改网络访问设置不会导致您自己无法登录到邮件网关。请参阅限制网络访问时的重要预防措施 , on page 28。

Procedure

步骤 1 依次选择**系统管理 (System Administration) > 网络访问 (Network Access)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 选择访问列表的控制模式：

选项	说明
允许全部 (Allow All)	此模式允许到邮件网关的所有连接。 此模式为默认操作模式。
仅允许特定连接 (Only Allow Specific Connections)	如果用户的 IP 地址与访问列表中所含的 IP 地址、IP 范围或 CIDR 范围匹配，此模式则允许该用户连接到邮件网关。
仅允许通过代理的特定连接 (Only Allow Specific Connections Through Proxy)	如果满足以下条件，则此模式允许用户通过反向代理连接到邮件网关： • 连接代理的 IP 地址包含在访问列表的“代理服务器 IP 地址”(IP Address of Proxy Server) 字段中。 • 代理在其连接请求中包含 **x-forwarded-header** HTTP 信头。 • **x-forwarded-header** 的值不能为空。 • 远程用户的 IP 地址包含在 x-forwarded-header 中，并与访问列表中为用户定义的 IP 地址、IP 范围或 CIDR 范围匹配。

选项	说明
仅允许直接或通过代理的特定连接 (Only Allow Specific Connections Directly or Through Proxy)	如果用户的 IP 地址与访问列表中包含的 IP 地址、IP 范围或 CIDR 范围相匹配，则此模式会允许用户通过反向代理或直接连接到邮件网关。通过代理进行连接的条件与在“仅允许通过代理的特定连接”(Only Allow Specific Connections Through Proxy) 模式下的条件相同。

步骤 4 输入将允许用户从其连接邮件网关的 IP 地址。

您可以输入 IP 地址、IP 地址范围或 CIDR 范围。使用逗号分隔多个条目。

步骤 5 如果允许通过代理连接，请输入以下信息：

a. 允许连接邮件网关的代理的 IP 地址。使用逗号分隔多个条目。

b. 代理发送给邮件网关（其中包含远程用户计算机以及转发请求的代理服务器的 IP 地址）的原始 IP 信头的名称。默认情况下，该信头的名称为 x-forwarded-for。

步骤 6 请确保您未配置在提交并落实更改后将会导致您自己无法登录到邮件网关的更改。

步骤 7 提交并确认更改。

配置会话超时

- 配置 Web UI 会话超时, on page 30
- 配置 CLI 会话超时, on page 31

配置 Web UI 会话超时

可以指定用户因不活动而被 AsyncOS 注销前可登录邮件网关的时长。此 Web UI 会话超时适用于：

- 所有用户，包括管理员
- HTTP 和 HTTPS 会话
- 思科垃圾邮件隔离区

AsyncOS 注销用户后，邮件网关会将用户的网络浏览器重定向到登录页。

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **网络访问 (Network Access)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 在 **Web UI 不活动超时时间 (Web UI Inactivity Timeout)** 字段中，输入用户可在注销之前保持不活动状态的分钟数。可以定义 5 到 1440 分钟之间的超时期限。

步骤 4 提交并确认更改。

What to do next

也可以使用 CLI 中的 adminaccessconfig 命令来配置 Web UI 会话超时。请参阅《适用于*Cisco Secure Email Gateway*的 *AsyncOS CLI* 参考指南》。

配置 CLI 会话超时

可以指定用户因不活动而被 AsyncOS 注销前可以登录邮件网关的 CLI 的时间。CLI 会话超时适用于：

- 所有用户，包括管理员
- 仅适用于使用安全外壳 (SSH)、SCP和直接串行连接的连接

Note 在 CLI 会话超时时的所有未提交的配置更改都将丢失。确保在进行配置更改后立即进行确认。

Procedure

步骤 1 依次选择**系统管理 (System Administration)** > **网络访问 (Network Access)**。

步骤 2 点击**编辑设置 (Edit Settings)**。

步骤 3 在 **CLI 不活动超时时间 (CLI Inactivity Timeout)** 字段中，输入用户可在注销之前保持不活动状态的分钟数。可以定义 5 到 1440 分钟之间的超时期限。

步骤 4 提交并确认更改。

What to do next

也可以使用 CLI 中的 adminaccessconfig 命令来配置 CLI 会话超时。请参阅《适用于*Cisco Secure Email Gateway*的 *AsyncOS CLI* 参考指南》。

向管理用户显示消息

在登录前显示消息

可将邮件网关配置为在用户尝试通过 SSH、FTP 或 Web UI 登录到该邮件网关设备前显示一条消息。登录横幅是可自定义的文本，显示在登录提示的上方。可以使用登录横幅显示邮件网关的内部安全

信息或最佳实践说明。例如，您可以创建一段简单说明，指出禁止未经授权使用该邮件网关，或者有关组织有权审核用户对该邮件网关所做更改的详细警告。

可以使用 CLI 中的 adminaccessconfig > banner 命令创建登录横幅。登录横幅的最大长度是 2000 个字符，以适合 80x25 的控制台。可从邮件网关上 /data/pub/configuration 目录中的文件导入登录横幅。在创建横幅之后，请确认您的更改。

在登录后显示消息

可将 AsyncOS 配置为在用户通过 SSH、FTP 或 Web UI 成功登录到邮件网关后显示一个欢迎横幅。可以使用欢迎横幅显示邮件网关的内部安全信息或最佳实践说明。

可以使用 CLI 中的 adminaccessconfig > welcome 命令创建欢迎横幅。欢迎横幅的最大长度为 1600 个字符。

可从邮件网关 /data/pub/configuration 目录中的文件导入欢迎横幅。在创建横幅之后，请确认您的更改。

有关详细信息，请参阅《适用于*Cisco Secure Email Gateway*的 *AsyncOS CLI* 参考指南》。

管理安全外壳 (SSH) 密钥

可将 sshconfig 命令用于：

- 向/从系统上已配置的用户帐户（包括 admin 帐户）的 authorized_keys 文件添加/删除安全外壳 (SSH) 公共用户密钥。这将允许使用 SSH 密钥而不是密码质询队用户账户进行身份验证。
- 编辑以下 SSH 服务器配置设置：
  - 公钥身份验证算法 (Public Key Authentication Algorithms)
  - 加密算法 (Cipher Algorithms)
  - KEX 算法 (KEX Algorithms)
  - MAC 方法 (MAC Methods)

Note 要配置主机密钥，以便在将日志文件从邮件网关 SCP 推送到其他主机时使用，请使用 **logconfig -> hostkeyconfig**。有关详细信息，请参阅 日志记录。

使用 **hostkeyconfig**，可以扫描远程主机的密钥，并将它们添加到邮件网关。

相关主题

- 示例：安装新公钥, on page 33
- 示例：编辑 SSH 服务器配置, on page 33

示例：安装新公钥

在下面的示例中，将为管理员账户安装一个新公钥：

```
mail.example.com> sshconfig
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]> userkey
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
[]> new
Please enter the public SSH key for authorization.
Press enter on a blank line to finish.
[-paste public key for user authentication here-]
Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
[]>
```

示例：编辑 SSH 服务器配置

下面的示例显示了如何编辑 SNMP 服务器配置。

```
mail1.example.com> sshconfig

Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
- ACCESS CONTROL - Edit SSH allowed list/blocked list
[]> sshd

ssh server config settings:
Public Key Authentication Algorithms:
        ssh-rsa
        rsa-sha2-256
        ssh-ed25519
        ecdsa-sha2-nistp256
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-cbc
        aes192-cbc
        aes256-cbc
        aes128-gcm@openssh.com
        chacha20-poly1305@openssh.com
MAC Methods:
        hmac-sha1
        hmac-sha2-256
KEX Algorithms:
        diffie-hellman-group14-sha1
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        curve25519-sha256
        diffie-hellman-group14-sha256
        curve25519-sha256@libssh.org
```

```
Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]> setup

Available Public Key Authentication Algorithms options :
        rsa-sha2-256
        ssh-rsa
        ssh-dss
        ssh-ed25519
        ecdsa-sha2-nistp256
Enter the Public Key Authentication Algorithms do you want to use
[ssh-rsa,rsa-sha2-256, ssh-ed25519,ecdsa-sha2-nistp256]>

Available Cipher Algorithms options :
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-cbc
        aes192-cbc
        aes256-cbc
        aes128-gcm@openssh.com
        chacha20-poly1305@openssh.com
Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc,
 aes128-gcm@openssh.com,chacha20-poly1305@openssh.com]>

Available MAC Methods options :
        hmac-sha1
        hmac-sha2-256

Enter the MAC Methods do you want to use
[hmac-sha1, hmac-sha2-256]>

Available KEX Algorithms options :
        diffie-hellman-group14-sha1
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        curve25519-sha256
        diffie-hellman-group14-sha256
        curve25519-sha256@libssh.org
Enter the KEX Algorithms do you want to use
[diffie-hellman-group14-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,
 curve25519-sha256,diffie-hellman-group14-sha256,curve25519-sha256@libssh.org]>

ssh server config settings:
Public Key Authentication Algorithms:
        ssh-rsa
        rsa-sha2-256
        ssh-ed25519
        ecdsa-sha2-nistp256
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-cbc
        aes192-cbc
        aes256-cbc
        aes128-gcm@openssh.com
        chacha20-poly1305@openssh.com
MAC Methods:
        hmac-sha1
        hmac-sha2-256
```

```
KEX Algorithms:
        diffie-hellman-group14-sha1
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        curve25519-sha256
        diffie-hellman-group14-sha256
        curve25519-sha256@libssh.org

Choose the operation you want to perform:
- SETUP - Setup SSH server configuration settings
[]>
```

远程 SSH 命令执行

CLI 允许通过远程执行 SSH 命令来运行命令。例如，如果已为邮件网关上的“admin”帐户配置 SSH 公钥，则可从未质询的远程主机运行以下命令：

```
# ssh admin@mail3.example.com status

Enter "status detail" for more information.

Status as of: Mon Jan 20 17:24:15 2003

Last counter reset: Mon Jan 20 17:08:21 2003

System status: online

[rest of command deleted]
```

监控管理用户访问权限

要想	相应操作
查看邮件网关的所有活动用户的会话详细信息	点击页面右上角的**选项 (Options) > 活动会话 (Active Sessions)** 在命令行界面中，使用 w、whoami 和 who 命令。
查看最近登录到邮件网关的用户。 还将显示远程主机的 IP 地址，以及登录、注销和总时间。	在命令行界面，使用 last 命令。

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。