分配管理任务

本章包含以下部分：

关于分配管理任务

您可以根据自己分配给其他人员的用户账户的用户角色，将思科内容安全管理设备上的管理任务分配给其他人员。

要进行设置以分配管理任务，您应该确定预定义的用户角色是否满足您的需求，创建任何需要的自定义用户角色，并设置设备以在安全设备上对管理用户进行本地身份验证，并且/或者使用您自己的集中 LDAP 或 RADIUS 系统进行外部身份验证。

此外，您可以对访问设备和设备上的某些信息指定额外的控制。

分配用户角色

要获得隔离区访问权限，需要进行其他配置。请参阅对隔离区的访问权限 , on page 11。

预定义用户角色

除非另有说明，否则您可以为每个用户分配具有下表所述权限的预定义用户角色，或者为用户分配自定义用户角色。

Table 1: 用户角色的说明

用户角色名称	说明	**Web** 报告/计划报告功能
admin	**admin** 用户是系统的默认用户账户，并且拥有完全管理权限。为方便起见，此处列出了管理员用户账户，但此账户无法通过用户角色进行分配，也无法编辑或删除，只能更改口令。 只有**管理员**用户可以发出 **resetconfig** 和 **revert** 命令。	是/是
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。	是/是
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 • 升级设备 • 发出 `resetconfig` 命令 • 运行系统设置向导 • 在启用LDAP进行外部身份验证的情况下，修改除用户名和口令以外的LDAP服务器配置文件设置。 • 配置、编辑、删除或集中隔离区。 除上述情况外，他们所拥有的权限与管理员角色相同。	是/是
技术人员 (Technician)	具有“技术人员”(Technician) 角色的用户账户可以执行系统管理活动，例如升级和重新启动、从设备保存配置文件、管理功能密钥等。	访问网络和邮件选项卡下的“系统容量”(System Capacity) 报告

用户角色名称	说明	Web 报告/计划报告功能
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) 角色的用户可以进行和提交大多数更改以了解如何配置功能，但是不能够确认更改或进行任何不需要确认的更改。如果启用了访问权限，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。 • 创建、编辑、删除或集中隔离区的设置。	是/否
访客 (Guest)	具有“访客”(Guest) 角色的用户账户可以查看状态信息（包括报告和 Web 跟踪），如果启用了访问权限，还可以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。	是/否
网络管理员 (Web Administrator)	具有“网络管理员”角色的用户账户可以访问**网络** 选项卡下的所有配置设置。	是/是
网络策略管理员 (Web Policy Administrator)	具有“网络策略管理员”(Web Policy Administrator) 角色的用户账户可以访问“网络”(Web) 选项卡下的所有配置设置。“网络策略管理员”(Web Policy Administrator) 可以配置身份、访问策略、解密策略、路由策略、代理绕行、自定义 URL 类别和时间范围。“网络策略管理员”(Web Policy Administrator) 无法发布配置。	否/否
邮件管理员 (Email Administrator)	具有“邮件管理员”(Email Administrator) 角色的用户账户只能访问“邮件”(Email) 菜单内的所有配置设置，包括隔离区。	否/否
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。在为用户分配此角色后，您还必须配置隔离区以允许此用户访问。	否/否

用户角色名称	说明	Web 报告/计划报告功能
自定义角色 (Custom Roles)	被分配自定义用户角色的用户账户只能查看和配置策略、功能或者专门委派给该角色的特定策略或功能实例。 这些功能可以是访问日志订用、日志记录 API 和日志文件。 您可以从“添加本地用户”(Add Local User) 页面创建新的自定义邮件用户角色或新的自定义网络用户角色。但是，您必须先将权限分配给此自定义用户角色，然后才能使用该角色。要分配权限，请转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户角色 (User Roles)**，然后点击用户名。 **Note** 分配给自定义邮件用户角色的用户无法访问 CLI。 有关详细信息，请参阅自定义用户角色 , on page 4。	否/否

自定义用户角色

安全管理设备允许拥有管理权限的用户为自定义角色授权管理功能。与预定义用户角色相比，自定义角色可以更灵活地控制用户的访问权限。

您为其分配自定义用户角色的用户可以管理设备、功能或最终用户子集的策略或访问报告。例如，您可能允许网络服务的一个委派管理员管理组织在某个不同国家/地区的分支机构的策略，该分支机构的可接受使用策略可能与组织总部的可接受使用策略不同。您通过创建自定义用户角色并将访问权限分配给这些角色来委派管理职责。您确定委派的管理员可以查看和编辑哪些策略、功能、报告、自定义 URL 类别等。

管理员可以为隔离区邮件创建具有只读选项的自定义角色。只读选项可防止用户删除或释放邮件，并且仅对隔离区具有只读访问权限。

有关详情，请参阅：

- 关于自定义邮件用户角色 , on page 4
- 删除自定义用户角色 , on page 10

关于自定义邮件用户角色

可以分配自定义角色，以允许授权的管理员在安全管理设备上访问下列信息：

- 所有报告（可选择通过报告组限制）
- 邮件策略报告（可根据需要按报告组限制）
- DLP 报告（可根据需要按报告组限制）

- AMP 报告（可根据需要按报告组限制）
- 邮件跟踪
- 隔离区
- 日志订用

有关以上各项的详细信息，请参阅此部分之后的内容。此外，所有被授予上述任一权限的用户均可以在“管理设备”(Management Appliance) >“集中服务”(Centralized Services) 菜单下查看系统状态。分配了自定义邮件用户角色的用户无法访问 CLI。

Note 与安全管理设备中的用户角色相比，邮件安全设备中的自定义用户角色可提供更精细的访问权限。例如，可以向邮件和 DLP 策略及内容过滤器授予访问权限。有关详细信息，请参阅邮件安全设备文档或在线帮助“通用管理”一章中的“管理授权管理的自定义用户角色”部分。

对邮件报告的访问权限

可以按以下部分所述授予自定义用户角色访问邮件报告的权限。

有关安全管理设备中“邮件安全监控”(Email Security Monitor) 页面的完整信息，请参阅使用集中邮件安全报告一章。

所有报告

如果授予自定义角色访问所有报告的权限，则分配了此角色的用户可以查看所有邮件安全设备或所选的“报告组”(Reporting Group) 的“邮件安全监控”(Email Security Monitor) 页面：

- 邮件流摘要
- 邮件流详细信息
- 外发目标
- 用户邮件摘要
- DLP 事件 (DLP Incidents)
- 内容过滤器
- 病毒过滤
- TLS 加密
- 计划的报告 (Scheduled Reports)
- 存档的报告 (Archived Reports)

邮件策略报告

如果授予自定义角色访问邮件策略报告的权限，则分配了此角色的用户可以查看所有邮件安全设备或所选的“报告组”(Reporting Group) 的“邮件安全监控”(Email Security Monitor) 页面：

- 邮件流摘要
- 邮件流详细信息
- 外发目标
- 用户邮件摘要
- 内容过滤器
- 病毒过滤
- 存档的报告

DLP 报告

如果授予自定义角色访问 DLP 报告的权限，则分配了此角色的用户可以查看所有邮件安全设备或所选的“报告组”(Reporting Group) 的“邮件安全监控”(Email Security Monitor) 页面：

- DLP 事件
- 存档的报告

AMP 报告

如果授予自定义角色访问 AMP 报告的权限，则分配给该角色的用户可以查看所有邮件网关或所选报告组的以下 AMP 相关报告：

- 高级恶意软件保护（AMP 信誉）
- 文件分析
- AMP 判定更新（文件追溯）
- 邮箱自动补救

对邮件跟踪数据的访问权限

如果授予自定义角色访问邮件跟踪的权限，则分配了此角色的用户可以找到安全管理设备跟踪的所有邮件的状态。

要控制对违反 DLP 策略的邮件中敏感信息的访问，请参阅控制对“邮件跟踪”中敏感信息的访问权限 , on page 28。

有关邮件跟踪的详细信息（包括设置设备以便在安全管理设备中启用邮件跟踪访问权限的说明），请参阅跟踪。

自定义用户角色的隔离区访问权限

如果授予自定义角色访问隔离区的权限，则分配了此角色的用户可以搜索、查看、发布或删除此安全管理设备中所有隔离区的邮件。

您必须启用此访问权限，用户才能访问隔离区。请参阅对隔离区的访问权限 , on page 11。

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。

创建自定义邮件用户角色

您可以创建自定义邮件用户角色以访问邮件报告、邮件跟踪和隔离区。

有关以上每个选项允许的访问权限的说明，请参阅关于自定义邮件用户角色 , on page 4及其子部分。

Note 要授予对其他功能、报告或策略的更为精细的访问，请在每个邮件安全设备定义用户角色。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户角色 (User Roles)**。

步骤 3 点击**添加邮件用户角色 (Add Email User Role)**。

Tip 或者，您可以通过复制现有的邮件用户角色创建新角色：点击适用的表行中的“复制”(Duplicate) 图标，然后修改生成的副本。

步骤 4 为用户角色输入唯一的名称（例如“dlp-auditor”）和说明。

- 不能复制邮件和网络自定义用户角色名称。
- 名称必须仅包含小写字母、数字和短划线。不能以短划线或数字开头。
- 如果授予具有此角色的用户访问集中策略隔离区的权限，并且还希望具有此角色的用户能够在邮件安全设备上的邮件及内容过滤器中指定这些集中隔离区以及 DLP 邮件操作，则两种设备上的自定义角色的名称必须相同。

步骤 5 选择要为此角色启用的访问权限。

管理员可以为隔离区邮件创建具有只读选项的自定义角色。只读选项可防止用户删除或释放邮件，并且仅对隔离区具有只读访问权限。

步骤 6 点击**提交 (Submit)** 以返回到“用户角色”(User Roles) 页面，其中列出了新的用户角色。

步骤 7 如果您按报告组限制了访问权限，请点击用户角色的“邮件报告”(Email Reporting) 列中的**未选择组 (no groups selected)** 链接，然后选择至少一个报告组。

步骤 8 确认您的更改。

步骤 9 如果您向此角色授予了对隔离区的访问权限，请为此角色启用访问权限：

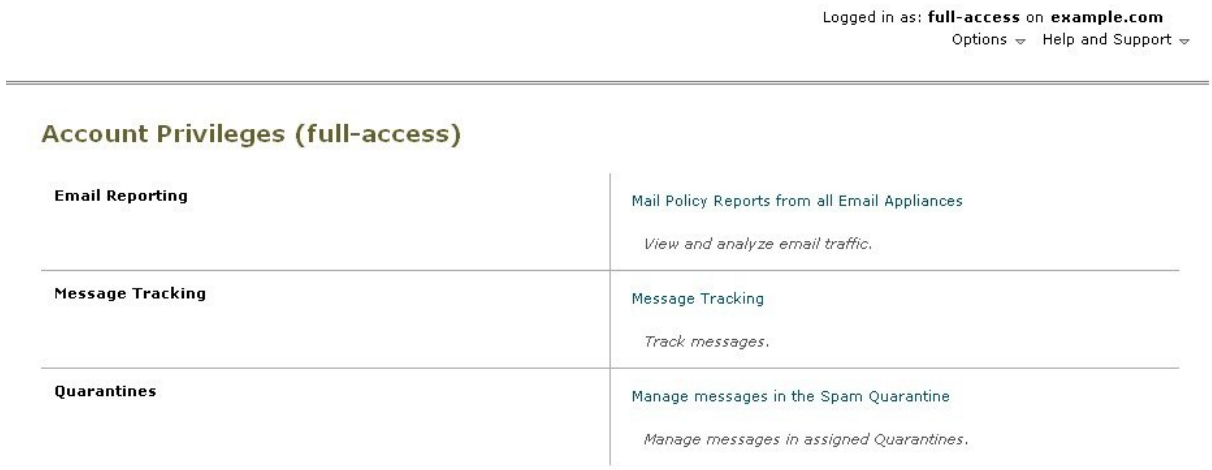
请参阅：

- 配置对垃圾邮件隔离区的管理用户访问权限
- 配置策略、病毒和爆发隔离区

使用自定义邮件用户角色

当分配了自定义邮件用户角色的用户登录到设备时，该用户只能看到其有权访问的安全功能的链接。该用户可以通过选择“选项”(Options) 菜单中的“账户权限”(Account Privileges) 随时返回到该主页。这些用户还可以通过网页顶部的菜单访问其有权访问的功能。在以下示例中，用户可通过自定义邮件用户角色访问安全管理设备中可用的所有功能。

Figure 1: 分配了自定义邮件用户角色的授权管理员的“账户权限”***(Account Privileges)*** 页面



关于自定义网络用户角色

自定义网络用户角色允许用户向不同的网络安全设备发布策略，并赋予他们针对不同设备编辑或发布自定义配置的权限。

在安全管理设备中的**网络 (Web) > 主配置 (Configuration Master) > 自定义 URL 类别 (Custom URL Categories)** 页面，可以查看允许您管理和发布的 URL 类别与策略。此外，您可以转到**网络 (Web) > 实用程序 (Utilities) > 立即发布配置 (Publish Configuration Now)** 页面并查看可能的配置。

Note 请注意，如果您创建具有“发布权限”(Publish Privilege) 功能的自定义角色，则用户在登录时将不具有任何可用的菜单。他们不具有发布菜单，并且将登录在一个不可编辑的登录屏幕上，因为 URL 和策略选项卡不具有任何功能。实际上，您具有无法发布或管理任何类别或策略的用户。此问题的解决办法：如果您希望用户能够发布，但无法管理任何类别或策略，则**必须**创建不用于任何策略的自定义类别，并使该用户能够管理该自定义类别和发布。这样，如果用户从该类别中添加或删除 URL，不会产生任何影响。

您可以通过创建和编辑自定义用户角色委派网络管理。

- 创建自定义网络用户角色, on page 9
- 编辑自定义网络用户角色, on page 10
- 删除自定义用户角色 , on page 10

创建自定义网络用户角色

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **用户角色 (User Roles)**。

步骤 3 点击**添加网络用户角色 (Add Web User Role)**。

Tip 或者，您可以通过复制现有的网络用户角色创建新角色：点击适用的表行中的“复制”(Duplicate) 图标，然后修改生成的副本。

步骤 4 输入用户角色的唯一名称（例如“canadian-admins”）和说明。

Note 名称只能包含小写字母、数字和破折号。它不能以破折号开头。

步骤 5 选择您希望在默认情况下显示还是隐藏策略和自定义 URL 类别。

步骤 6 选择您希望开启还是关闭发布权限。

此权限允许用户发布该用户可以编辑其访问策略或 URL类别的任何主配置。

步骤 7 选择是要从新的（空的）设置开始还是复制现有的自定义用户角色。如果您选择复制现有的用户角色，请从列表中选择要复制的角色。

步骤 8 点击**提交 (Submit)** 以返回到“用户角色”(User Roles) 页面，其中列出新的用户角色。

Note 如果您在 Web 报告内启用了匿名功能，则有权访问 Web 报告的所有用户角色将在交互式报告页面中具有无法识别的用户名和角色。请参阅使用集中 Web 报告和跟踪一章中的计划 Web 报告部分。但“管理员”角色例外，该角色可以在计划的报告中查看实际用户名。如果启用了匿名功能，“操作员”和“网络管理员”生成的计划报告将采用匿名。

如果您使用**网络 (Web) > 实用程序 (Utilities) > 安全 (Security) > 服务显示 (Services Display) > 编辑安全服务显示 (Edit Security Services Display)** 页面隐藏其中一个主配置，则“用户角色”(User Roles) 页面还会隐藏相应的主配置列；但是，会保留已隐藏的主配置的权限设置。

编辑自定义网络用户角色

步骤 1 在“用户角色”(User Roles) 页面上，点击角色名称以显示“编辑用户角色”(Edit User Role) 页面。

步骤 2 编辑任何设置：名称、说明以及策略和自定义 URL 类别的可视性。

步骤 3 点击**提交 (Submit)**。

要编辑自定义用户角色的权限，请执行以下操作：

导航到“用户角色”(User Roles) 页面。

- 要编辑访问策略权限，请点击“访问策略”(Access policies) 以显示主配置中配置的访问策略列表。在“包括”(Include) 列中，选中您要向用户授予编辑权限的策略的复选框。点击**提交 (Submit)** 返回到“用户角色”(User Roles) 页面。

-或者-

- 要编辑自定义 URL 类别权限，请点击“自定义 URL 类别”(Custom URL Categories) 以显示“主配置”(Configuration Master) 上定义的自定义 URL 类别列表。在“包括”(Include) 列中，选中您要向用户授予编辑权限的自定义 URL 类别的复选框。点击**提交 (Submit)** 返回到“用户角色”(User Roles) 页面。

删除自定义用户角色

如果删除已分配给一个或多个用户的自定义用户角色，系统不会报错。

可访问 CLI 的用户角色

某些角色可以访问 GUI 和 CLI：“管理员”(Administrator)、“操作员”(Operator)、“访客”(Guest)、“技术人员”(Technician) 和“只读操作员”(Read-Only Operator)。其他角色只能访问 GUI：“服务中心用户”(Help Desk User)、“邮件管理员”(Email Administrator)、“网络管理员”(Web Administrator)、“网络策略管理员”(Web Policy Administrator)、“URL 过滤管理员”(URL Filtering Administrator)（适用于网络安全）和自定义用户。

使用 LDAP

如果您使用 LDAP 目录对用户进行身份验证，您将目录组分配给用户角色而不是各个用户。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，请参阅外部用户身份验证 , on page 19。

对隔离区的访问权限

您必须先启用该访问权限，然后用户才可以访问隔离区。请参阅以下信息：

- 配置对垃圾邮件隔离区的管理用户访问权限
- 关于向其他用户分配邮件处理任务（适用于策略隔离区）和配置策略、病毒和爆发隔离区
- 为自定义用户角色配置集中隔离区访问权限

“用户”(User) 页面

有关此部分的信息	请参阅
用户 重置口令按钮	关于分配管理任务 , on page 1 管理本地定义的管理用户 , on page 12 要求用户按要求更改口令 , on page 17
本地用户账户与口令设置	设置口令和登录要求 , on page 14
外部身份验证	外部用户身份验证 , on page 19
DLP 跟踪权限	控制对“邮件跟踪”中敏感信息的访问权限 , on page 28

关于对管理用户进行身份验证

您可以控制对设备的访问权限，方法是在设备上本地定义授权用户，并/或使用外部身份验证或双因素身份验证。

- 更改管理员用户的口令, on page 12
- 到期后更改用户的口令, on page 12
- 管理本地定义的管理用户 , on page 12
- 外部用户身份验证 , on page 19
- 双因素身份验证, on page 22

更改管理员用户的口令

所有管理员级别的用户均可通过 GUI 或 CLI 更改“管理员”用户的口令。

Note 思科建议您在首次登录设备或将配置重置为出厂默认设置时更改密码。

要通过 GUI 更改口令，请执行以下操作：

- [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。
- 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **用户 (Users)** 页面，然后选择管理员用户。

要在 CLI 中更改管理员用户的口令，请使用 `passphrase` 命令。为了安全起见，`passphrase` 命令要求输入旧口令。

如果忘记了“管理员”用户账户的口令，请联系客户支持提供商重置口令。

Note 对口令所做的更改会立即生效，不要求确认更改。

到期后更改用户的口令

如果账户已过期，系统则会向您显示以下消息“您的口令已过期。请点击此处更改口令。”进行提示。

点击链接，然后输入登录详细信息以及过期的口令，转到“更改口令”(Change PasswordPassphrase) 页面。有关设置口令的详细信息，请参阅设置口令和登录要求 ， 第 14 页。

注释 对口令所做的更改会立即生效，不要求确认更改。

管理本地定义的管理用户

添加本地定义的用户

如果不使用外部身份验证，请按照以下程序直接将用户添加到安全管理设备。或者在 CLI 中使用 **userconfig** 命令。

Note 如果还启用了外部身份验证，请确保本地用户名与经过外部身份验证的用户名不相同。

对您可以在设备上使用的用户账户数量没有限制。

步骤 1 如果您将分配自定义用户角色，我们建议您首先定义这些角色。请参阅自定义用户角色 , on page 4。

步骤 2 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 3 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。

步骤 4 点击**添加用户 (Add User)**。

步骤 5 输入用户的唯一名称。不能输入系统保留的词（例如，“operator”和“root”）。

如果您还使用外部身份验证，则用户名不能与经过外部身份验证的用户名相同。

步骤 6 输入用户的全称。

步骤 7 选择预定义的角色或自定义角色。有关用户角色的详细信息，请参阅预定义用户角色 , on page 2部分中的用户角色说明表。

如果您在此处添加新的邮件角色或网络角色，请为该角色输入名称。有关命名限制的信息，请参阅创建自定义邮件用户角色 , on page 7或创建自定义网络用户角色, on page 9。

步骤 8 确认当前密码以进行安全验证。

步骤 9 您可以生成或输入密码并重新输入相同的密码进行确认。

步骤 10 提交并确认更改。

步骤 11 如果您在此页面上添加了自定义用户角色，现在请为该角色分配权限。请参阅自定义用户角色 , on page 4。

编辑本地定义的用户

例如，使用此程序更改口令。

步骤 1 在“用户 (Users)”列表中点击用户名。

步骤 2 对用户进行更改。

步骤 3 确认当前密码以进行安全验证。

步骤 4 提交并确认更改。

删除本地定义的用户

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 点击**确认 (Commit)** 确认更改。

查看本地定义的用户列表

要查看本地定义的用户列表，请执行以下操作：

- 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **用户 (Users)**。

Note 星号表示被分配委派管理的自定义用户角色的用户。如果用户的自定义角色已被删除，则“未分配”(Unassigned) 会以红色出现。有关自定义用户角色的详细信息，请参阅自定义用户角色 , on page 4。

设置和更改口令

- 添加用户时，需要为该用户指定初始口令。
- 要更改系统中配置的用户的口令，请使用 GUI 中的“编辑用户”(Edit User) 页面（有关详细信息，请参阅编辑本地定义的用户, on page 13）。

Note 思科建议您在首次登录设备时或完成系统设置向导后更改密码。

- 要更改系统的默认管理员用户账户的口令，请参阅更改管理员用户的口令, on page 12。
- 要强制用户更改其口令，请参阅要求用户按要求更改口令 , on page 17。
- 用户可以更改自己的口令，方法是点击 GUI 右上角的“选项”(Options) 菜单并选择“更改口令”(Change PasswordPassphrase) 选项。

设置口令和登录要求

可以通过定义用户账户和口令限制来实施组织口令策略。用户账户和口令限制适用于安全管理设备上定义的本地用户。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。
- **口令有效期规则**。可以定义口令的有效期，在该期限之后，用户登录后需要更改口令。
- **口令规则**。可以定义用户可选择的口令类型，例如哪些字符是可选的或必需的。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 2 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。

步骤 3 向下滚动到**本地用户账户和口令设置**部分。

步骤 4 点击**编辑设置 (Edit Settings)**。

步骤 5 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。仅当用户输入已锁定账户的正确口令时，才会显示此消息。 用户账户被锁定后，管理员可以在 GUI 中的“编辑用户”(Edit User) 页面中或使用 `userconfig` 命令解锁账户。 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。请参阅手动锁定用户账户, on page 18。
口令重置	选择是否应在管理员更改用户的口令后强制用户更改其口令。 您还可以选择是否应强制用户在其口令到期后更改。输入在用户必须更改口令之前可以持续使用密码的天数。您可以输入一 (1) 到 366 之间的任一数值。默认值为 90。要强制用户在非计划的时间更改其口令，请参阅要求用户按要求更改口令 , on page 17。 如果强制用户在其口令到期后更改，可以显示关于口令即将到期的通知。选择在到期之前通知用户的天数。 **Note** 当用户账户使用 SSH 密钥（而不是口令质询）时，口令重置规则仍然适用。当使用 SSH 密钥的用户账户到期时，用户必须输入其旧口令或请管理员手动更改口令，才能更改与该账户相关的密钥。
口令规则： 至少需要 <数字> 个字符。	输入口令可以包含的最小字符数。 输入一 (1) 和 128 之间的任何数字。 默认值为 8。 口令可以具有比您在此处指定的数字更多的字符。

设置	说明
口令规则： 至少需要一个数字 (0-9)。(Password Rules: Require at least one number (0-9).)	选择口令是否必须至少包含一个数字。
口令规则： 至少需要一个特殊字符。(Password Rules: Require at least one special character.)	选择口令是否必须包含至少一个特殊字符。口令可以包含以下特殊字符： ~ ? ! @ # $ % ^ & * - _ + = \ | / [ ] ( ) < > { } ` ' " ; : , .
口令规则： 禁止将用户名及其变体用作口令。	选择是否允许口令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，以下规则适用于口令： • 口令不能与用户名相同，不区分大小写。 • 口令不能与反写的用户名相同，不区分大小写。 • 口令不能在使用以下字符替代的情况下与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”
口令规则： 禁止再次使用最近 <数字> 次用过的口令。	选择强制用户更改口令时，是否允许用户选择最近使用的口令。如果不允许再次使用最近的口令，请输入禁止再次使用的最近口令次数。 您可以输入一 (1) 到 15 之间的任一数值。默认值为三 (3)。
口令规则： 不允许在口令中使用的单词列表	您可以创建口令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_口令_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口令时，可以显示口令强度指示器。 此设置不强制创建强口令，只显示猜测所输入的口令的难易程度。 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，意味着注册为强口令的密码口令越难破解。此设置无最大值。 示例： • 如果输入 30，则注册为强口令的 8 位字符的口令至少包含 1 个大写和小写字母、数字和特殊字符。 • 如果输入 18，则注册为强密码口令的 8 位字符口令全部为小写字母、不含数字或特殊字符。 口令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，高强度口令具有以下特征： • 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口令，请使用此页面中的其他设置。
密码规则	您的邮件和 Web 管理器中添加了新的密码规则，用于定义您的登录密码： 避免使用包含三个或更多重复或连续字符的密码（例如，“AAA@124”、“Abc@123”等）。
密码规则	新的密码规则会添加到您的邮件和 Web 管理器，以定义您的登录密码： 避免在密码中使用用户名子字符串。不允许包含用户名中的三个或更多字符以及数字和特殊字符。

步骤 6 提交并确认更改。

What to do next

要求用户将其口令更改为符合新要求的新口令。请参阅要求用户按要求更改口令 , on page 17

要求用户按要求更改口令

如果需要所有或选定的用户在任何时间临时更改其口令，请执行此程序中的步骤。这是一次性的操作。

要自动执行更改口令的定期要求，请使用设置口令和登录要求 , on page 14所述的“口令重置”选项。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 2 依次选择**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。

步骤 3 在“用户”部分中，选中需要更改口令的用户旁边的复选框。

步骤 4 选择**强制口令更改**。

步骤 5 选择选项。

在“本地用户账户和口令设置”中配置宽限期的全局设置。

步骤 6 点击**确定 (OK)**。

锁定和解除锁定本地用户账户

锁定用户账户防止本地用户登录设备。可以通过以下方式之一锁定用户账户：

- 您可以将所有本地用户账户配置为在用户经过配置的尝试次数后未能成功登录时锁定：请参阅设置口令和登录要求 , on page 14。
- 管理员可以手动锁定用户账户。请参阅手动锁定用户账户, on page 18。

AsyncOS 会显示您在“编辑用户”(Edit User) 页面上查看用户账户时，用户账户被锁定的原因。

手动锁定用户账户

步骤 1 仅第一次：设置设备以启用用户账户锁定：

步骤 2 请执行以下操作：

a) [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。
b) 依次转到**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**。
c) 在**本地用户账户和口令设置 (Local User Account & PasswordPassphrase Settings)** 部分中，点击**编辑设置 (Edit Settings)**。
d) 选中**在管理员已手动锁定用户账户时显示已锁定账户消息 (Display Locked Account Message if Administrator has manually locked a user account)** 复选框，然后输入消息。
e) 提交更改。

步骤 3 转至**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)**，然后点击用户名。

Note 在锁定管理员账户之前，确保您可以将其解除锁定。请参阅将用户账户解除锁定 , on page 19中的注释。

步骤 4 点击**锁定账户 (Lock Account)**。

AsyncOS 会显示一则消息，说明用户将不能登录设备，并询问您是否要继续操作。

将用户账户解除锁定

要将用户账户解除锁定，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“解除锁定账户”(Unlock Account)。

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账户被锁定时，admin用户也可以使用串行控制台端口访问设备。有关使用串行控制台端口访问设备的详细信息，请参阅邮件安全设备文档或在线帮助中的“设置和安装”章节。

外部用户身份验证

如果在网络中将用户信息存储在 LDAP 或 RADIUS 目录，则可以将安全管理设备配置为使用外部目录对登录到设备的用户进行身份验证。

Note 经过外部身份验证的用户无法使用自定义视图所述的某些功能。

- 如果您的部署使用本地和外部身份验证，则本地用户名不能与经过外部身份验证的用户名相同。
- 如果设备无法与外部目录进行通信，则具有外部和本地账户的用户可以设备上的本地用户账户登录。

请参阅：

- 使用 LDAP 配置管理用户的外部身份验证
- 启用 RADIUS 身份验证, on page 19

配置 LDAP 身份验证

要配置 LDAP 身份验证，请参阅使用 LDAP 配置管理用户的外部身份验证。

启用 RADIUS 身份验证

您可以使用 RADIUS 目录对用户进行身份验证，并将用户组分配给用户角色以便管理您的设备。RADIUS 服务器应支持 CLASS 属性，AsyncOS 使用该属性将 RADIUS 目录中的用户分配给用户角色。

Note 如果外部用户更改其 RADIUS 组的用户角色，则该用户应注销设备，然后再次登录。用户将具有新角色的权限。

Before you begin

访问 RADIUS 服务器的共享密钥长度不能超过 48 个字符。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 依次选择**管理设备 (Management Appliance)** > **系统管理 (System Administration)** > **用户 (Users)** 页面，然后点击**启用 (Enable)**。

步骤 3 选中**启用外部身份验证 (Enable External Authentication)** 复选框。

步骤 4 为身份验证类型选择“RADIUS”。

步骤 5 输入 RADIUS 服务器的主机名。

步骤 6 输入 RADIUS 服务器的端口号。默认端口号为 `1812`。

步骤 7 输入 RADIUS 服务器的共享密钥。

Note 为邮件安全设备的集群启用外部身份验证时，请在集群中的所有设备上输入相同的共享密钥。

步骤 8 输入设备在超时前等待服务器响应的秒数。

步骤 9 选择要将口令身份验证协议 (PAP) 还是质询握手身份验证协议 (CHAP) 用作身份验证协议。

步骤 10 （可选）点击**添加行 (Add Row)** 添加另一台 RADIUS 服务器。为您的设备用于身份验证的每台 RADIUS 服务器重复步骤 6 和 7。

在定义多台外部服务器时，设备按设备上定义的顺序连接到服务器。您可能希望定义多台外部服务器，以允许在一台服务器暂时不可用时进行故障转移。

步骤 11 输入在网络用户界面上存储外部身份验证凭证的所花费的时间。

Note 如果 RADIUS 服务器使用一次性口令（例如基于令牌创建的口令），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。

步骤 12 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（推荐）	AsyncOS 将基于 RADIUS“类 (CLASS)”属性向设备角色分配 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）。 下面是设备角色限制性由低到高的顺序： • 管理员 • 电子邮件管理员 • Web 管理员 • Web策略管理员 • URL 过滤管理员（用于网络安全） • 自定义用户角色（邮件或 Web） 如果为用户分配了多个映射到自定义用户角色的“类(Class)”属性，将使用 RADIUS 服务器上列表中的最后一个“类 (Class)”属性。 • 技术人员 • 操作员 • 只读操作员 • 网络管理员用户 • 访客
将所有通过外部身份验证的用户映射到“管理员”角色	AsyncOS 会为 RADIUS 用户分配“管理员”(Administrator) 角色。

步骤 13 （可选）点击**添加行 (Add Row)** 添加另一个组。为设备进行身份验证的每个用户组重复步骤 11。

步骤 14 提交并确认更改。

双因素身份验证

可以使用 RADIUS 目录为特定用户角色配置双因素身份验证。设备支持以下与 RADIUS 服务器通信的身份验证协议：

- 口令身份验证协议 (PAP)
- 质询握手身份验证协议 (CHAP)

可以为以下用户角色启用双因素身份验证：

- 预定义
- custom

该功能已在以下设备上进行了测试：

- RSA 身份验证管理器 v8.2
- FreeRADIUS v1.1.7 及更高版本
- ISE v1.4 及更高版本

相关主题

- 启用双因素身份验证， 第 22 页
- 禁用双因素身份验证， 第 23 页
- 使用预共享密钥通过 SSH 添加邮件或网络安全设备， 第 23 页

启用双因素身份验证

请确保从 IT 管理员那里获得了双因素身份验证所需的 RADIUS 服务器详细信息。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 选择**系统管理** > **用户**页面，然后点击“双因素身份验证”下的**启用**。

步骤 3 输入 RADIUS 服务器的主机名或 IP 地址。

步骤 4 输入 RADIUS 服务器的端口号。

步骤 5 输入 RADIUS 服务器的共享密钥口令。

步骤 6 输入超时之前等待服务器响应的秒数。

步骤 7 选择相应的身份验证协议。

步骤 8 （可选）点击**添加行 (Add Row)** 添加另一台 RADIUS 服务器。对每个 RADIUS 服务器重复步骤 2 到 6。

注释 最多可以添加十个 DNS 服务器。

步骤 9 选择要为其启用双因素身份验证的所需用户角色。

步骤 10 提交并确认更改。

启用双因素身份验证后，当用户输入用户名和密码后，系统会提示输入密码，以便登录到该设备。

禁用双因素身份验证

开始之前

确保设备已启用双因素身份验证。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 加载旧 Web 界面。

步骤 2 选择**系统管理 > 用户**页面，然后点击“双因素身份验证”下的**编辑全局设置**

步骤 3 取消选择**启用双因素身份验证 (Enable Two-Factor Authentication)**。

步骤 4 提交并确认更改。

使用预共享密钥通过 SSH 添加邮件或网络安全设备

以下示例展示如何使用预共享密钥通过 SSH 将邮件安全设备 (testesa.example.com) 添加到安全管理设备 (testsma.example.com)。

要添加网络安全设备，当系统提示输入思科设备类型时，请选择 **WSA**。

```
testsma.example.com> applianceconfig

Choose the operation you want to perform.

ADD - Add SMA Connection Parameters and Keys.
EDIT - Edit an appliance.
DELETE - Remove an appliance.
TEST - Test that an appliance is properly configured.
SERVICES - Configure the centralized services for an appliance.
STATUS - Display the status of centralized services.
PORT - Configure which port is used to communicate with remote appliances.

[]> add

Please enter the type of Cisco appliance that this device is
1. ESA
2. WSA

[1]> 1

Enter the IP address or hostname of an appliance to transfer data with.
(A hostname may be entered in this field, however it will be immediately
resolved to an IP address when the form is submitted.)
[]> IP address entered

Enter a name to identify this appliance

[]> name of appliance
```

```
File transfer access via SSH is required to transfer reporting data, message logs,
and quarantine safelist/blocklist data from appliances

Would you like to configure file transfer access for this appliance? [Y]>

Would you like to use a custom ssh port to connect to this appliance? [N]>

Would you like to connect an Email Security appliance using pre-shared keys?
Use this option if you have enabled two-factor authentication on the Email
Security appliance. [N]> yes

To add an Email Security appliance to the Content Security Management appliance
using pre-shared keys, log in to the Email Security appliance,
run the smaconfig > add command, enter the following details.

Host: vm10sma0006.qa

User Key:
AAAAB3NzaC1yc2EAAAADAQABAAABAQDgm3kG9RHc4gVZxRe0orh5DW5Yje5UB9BpJqcTRQJoxUIAv2Xig
8q5geyaWHZcFoUxH61YQbPX3R8CVMYgJ8/QB/iunjkr3jowV/SCuBBikEFgj1zuxlsFhL0L487epEgby1gH0rfJ
gwSa2/6dhfyUayst6pT87CZGOQltgx7s51wc+ve770X3SqlQD5bdYC4x9+gCX0wdwfhTH1+4/82jwYjK1lAEXc
O4k4TuZJEJnyBQ3YyCyVwXuDkXpI6xJDemxcc36e7Wwtpn3mn2VLaTG2/I38XwSvlYB6TcqmWnO10gL+aD
wkKAKcuhYpz4NFr9myej1mhMk7ZAFXmRNxvT
```

注释 在继续下一步之前，确保已将**主机**和**用户密钥**详细信息添加到邮件或网络安全设备。继续在安全管理设备中添加连接参数的过程之前，确认在邮件或网络安全设备中所做的更改。

```
Do you want to continue connecting using pre-shared keys? [Y]> yes
```

对访问安全管理设备指定额外的控制

配置基于 IP 的网络访问

通过为直接连接到设备的用户和通过反向代理连接的用户（如果组织对于远程用户使用反向代理）创建访问列表，可以控制用户从哪些 IP 地址访问安全管理设备。

直接连接

可以为可连接到安全管理设备的计算机指定 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设备。如果用户尝试从不包含在列表中的地址连接设备，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安全管理设备之间使用反向代理服务器，AsyncOS 允许您使用可以连接到设备的代理的 IP 地址创建访问列表。

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 地址发送到邮件安全设备，代理需要在其连接设备的请求中包括 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。）安全管理设备对照访问列表中允许的用户和代理 IP 地址，匹配信头中的远程用户 IP 地址和连接代理的 IP 地址。

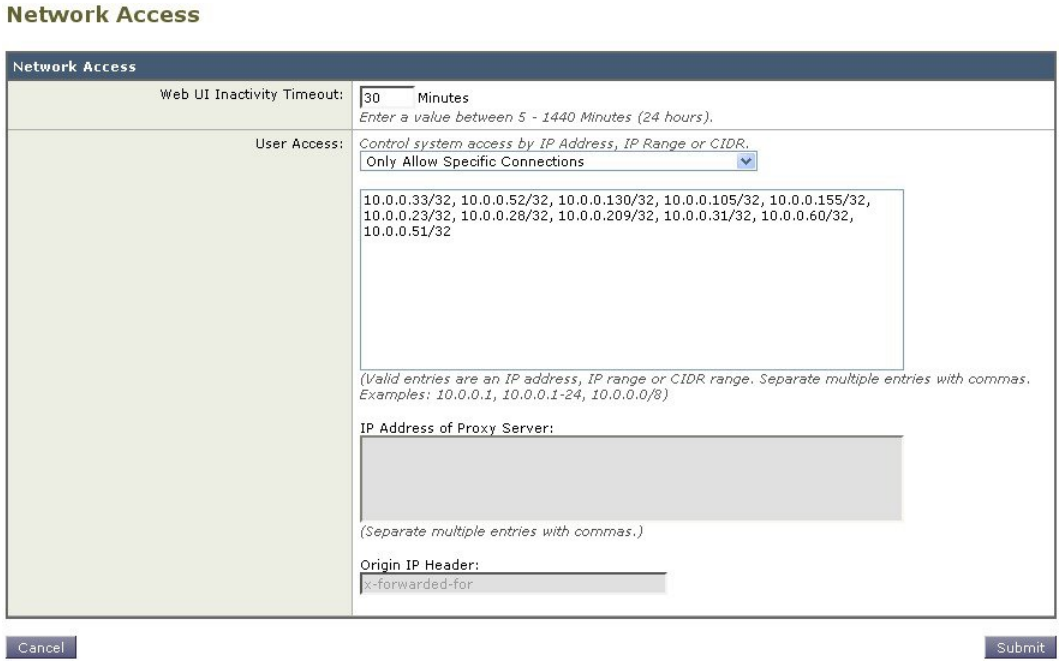
Note AsyncOS 仅支持 x-forwarded-for 信头中的 IPv4 地址。

创建访问列表

您可以通过 GUI 上的“网络访问”(Network Access) 页面或 **adminaccessconfig > ipaccess** CLI 命令创建网络访问列表。下图显示了“网络访问”(Network Access) 页面，其中包含允许直接连接到安全管理设备的用户 IP 地址列表。

以下设置适用于设备的旧 Web 界面和新 Web 界面。

Figure 2: 网络访问设置示例



AsyncOS 为访问列表提供四种不同的控制模式：

- **允许全部 (Allow All)**。此模式允许到设备的所有连接。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 地址匹配访问列表中包含的 IP 地址、IP 范围或 CIDR 范围，则此模式允许用户连接到设备。
- **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设备：
  - 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。
- **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设备。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。

请注意，在您提交并确认更改后，如果以下条件之一为真，则您可能会失去对设备的访问权限：

- 如果选择**仅允许特定连接 (Only Allow Specific Connections)**，并且在列表中不包含当前计算机的 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)**，并且当前连接到设备的代理的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，并且连接到设备的代理的 IP 地址不在允许的代理列表中。

如果您选择继续而不更正访问列表，当您确认更改时，AsyncOS 将断开您的计算机或代理与设备的连接。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 依次选择**系统管理 (System Administration) > 网络访问 (Network Access)**。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 选择访问列表的控制模式。

步骤 5 输入将允许用户从其连接设备的 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 6 如果允许通过代理连接，请输入以下信息：

- 允许连接设备的代理的 IP 地址。使用逗号分隔多个条目。
- 代理发送给设备（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 7 提交并确认更改。

配置 Web UI 会话超时

可以指定用户因不活动而被 AsyncOS 注销前可登录安全管理设备 Web UI 的时间。此 Web UI 会话超时适用于所有用户（包括 admin），而且将用于 HTTP 和 HTTPS 会话。

一旦 AsyncOS 注销用户，设备会将用户的网络浏览器重定向到登录页面。

Note 网络 UI 会话超时不适用于垃圾邮件隔离区会话，这些会话具有无法配置的 30 分钟超时。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 使用**系统管理 (System Administration) > 网络访问 (Network Access)** 页面。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 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 5 提交并确认更改。

配置 CLI 会话超时

可以指定用户因不活动而被 AsyncOS 注销前可登录安全管理设备 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。

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 使用**系统管理 (System Administration) > 网络访问 (Network Access)** 页面。

步骤 3 点击**编辑设置 (Edit Settings)**。

步骤 4 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 5 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《用于思科邮件安全设备的 *AsyncOS CLI* 参考指南》。

控制对“邮件跟踪”中敏感信息的访问权限

步骤 1 [仅限新 Web 界面] 在安全管理设备中，点击 ⚙ 加载旧 Web 界面。

步骤 2 转到**管理设备 (Management Appliance) > 系统管理 (System Administration) > 用户 (Users)** 页面。

步骤 3 在**跟踪权限 (Tracking Privileges)** 部分，点击**编辑设置 (Edit Settings)**。

步骤 4 选择要为其授予邮件跟踪中敏感信息访问权限的角色。

系统只会列出有权访问邮件跟踪的自定义角色。

步骤 5 提交并确认更改。

只有在“管理设备 (Management Appliance)”>“集中服务 (Centralized Services)”下启用“集中邮件跟踪”功能，此设置才能生效。

为管理用户显示消息

可以显示管理用户登录到设备时将看到的消息。

要设置或清除消息，请执行以下操作：

步骤 1 如果您打算使用文本文件，请将其上传到设备上的 `/data/pub/configuration` 目录。

步骤 2 访问命令行界面 (CLI)。

步骤 3 运行 `adminaccessconfig > BANNER` 命令。

步骤 4 加载横幅消息。

步骤 5 确认更改。

启用和禁用管理用户的邮件横幅

您可以启用和禁用带有链接的横幅，以便从设备的旧 Web 界面导航到设备的新 Web 界面。

步骤 1 访问命令行界面 (CLI)。

步骤 2 运行 `adminaccessconfig > NGUIBANNER` 命令。

步骤 3 启用或禁用横幅消息。

步骤 4 确认更改。

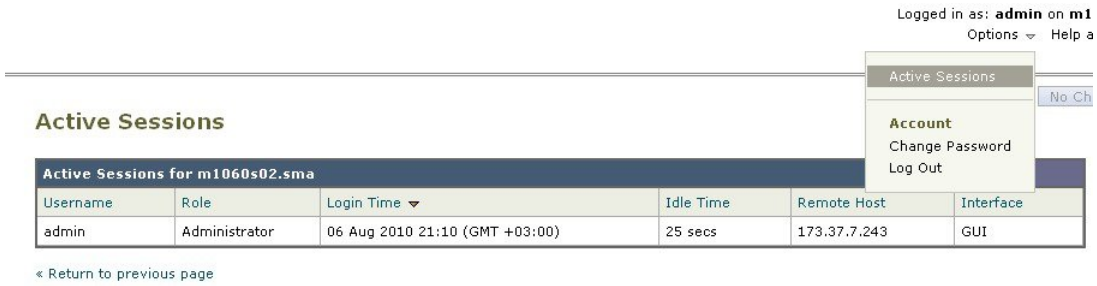
查看管理用户活动

使用网络查看活动会话

在安全管理设备中，可以查看所有活动的会话和登录到设备的用户。

在窗口的右上角，依次选择**选项 (Options) > 活动会话 (Active Sessions)**。

Figure 3: *“活动会话”(Active Sessions)* 菜单



在“活动会话”(Active Sessions) 页面，可以查看用户名、用户角色、用户登录时间、空闲时间以及用户从命令行还是 GUI 登录。

查看您最近的登录尝试

要查看最近几次通过Web界面、SSH和/或FTP进行的登录尝试（失败或成功），请执行以下操作：

步骤 1 请登录。

步骤 2 点击屏幕右上角附近的“登录身份”(Logged in as) 旁边的图图标。

通过命令行界面查看管理用户活动

以下命令支持多用户访问设备。

- **who** 命令列出了通过 CLI 或 Web 用户界面登录到系统的所有用户、用户角色、登录时间、空闲时间和用户登录的远程主机。
- whoami 命令显示当前已登录的用户的用户名和全称，以及用户所属的组：

```
mail3.example.com>
whoami
Username: admin
Full Name: Administrator
Groups: admin, operators, config, log, guest
```

- last 命令会显示哪些用户最近登录到设备。远程主机的 IP 地址以及登录时间、注销时间和总时间也会出现。

```
mail3.example.com> last
Username  Remote Host  Login Time        Logout Time       Total Time
========  ===========  ================  ================  ==========
admin     10.1.3.67    Sat May 15 23:42  still logged in   15m
admin     10.1.3.67    Sat May 15 22:52  Sat May 15 23:42  50m
admin     10.1.3.67    Sat May 15 11:02  Sat May 15 14:14  3h 12m
admin     10.1.3.67    Fri May 14 16:29  Fri May 14 17:43  1h 13m
shutdown                                 Fri May 14 16:22
shutdown                                 Fri May 14 16:15
admin     10.1.3.67    Fri May 14 16:05  Fri May 14 16:15  9m
admin     10.1.3.103   Fri May 14 16:12  Fri May 14 16:15  2m
admin     10.1.3.103   Thu May 13 09:31  Fri May 14 14:11  1d 4h 39m
admin     10.1.3.135   Fri May 14 10:57  Fri May 14 10:58  0m
admin     10.1.3.67    Thu May 13 17:00  Thu May 13 19:24  2h 24m
```

管理用户访问故障排除

错误：没有为用户分配访问权限

问题

已获得管理授权的用户可以登录到安全管理设备，但会看到未被分配访问权限的消息。

解决方案

确保已向此用户分配的自定义角色分配权限。查看“管理设备”(Management Appliance) >“系统管理”(System Administration) >“用户”(Users) 以确定已分配的用户角色，然后转到“管理设备”(Management Appliance) >“系统管理”(System Administration) >“用户角色”(User Roles)，点击用户角色的名称，并将权限分配给该角色。

如果您已根据报告组分配访问权限，请确保您在“管理设备”(Management Appliance) >“系统管理”(System Administration) >“用户角色”(User Roles) 页面上为该用户选择了报告组。要分配组，请点击“委派管理的用户角色”(User Roles for Delegated Administration) 表的“邮件报告”(Email Reporting) 列中的**未选择组 (no groups selected)** 链接。

用户没有活动的菜单

问题

您向其授予“发布”(Publish) 权限的用户在登录后没有活动的菜单。

解决方案

确保您已为至少一个访问策略或自定义URL类别授予访问权限。如果您不希望向此用户授予编辑任一内容的权限，请创建不用于任何策略的自定义类别，并在“自定义用户角色”(Custom User Role) 页面上向此用户角色授予对此类别的权限。

经过外部身份验证的用户看到“首选项”(Preferences) 选项

问题

通过外部身份验证的用户会看到“首选项”选项。

解决方案

确保直接在安全管理设备中添加的用户具有外部身份验证数据库中还未使用的唯一用户名。

经过外部身份验证的用户看到“首选项”**(Preferences)** 选项

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。