管理中心 的

管理中心 包括用于 Web 和 CLI 访问的默认 **管理员** 账户。本章介绍如何创建自定义用户帐户。有关使用用户帐户登录 管理中心 的详细信息，请参阅登录到管理中心。

关于用户

您可以在托管设备上作为内部用户添加自定义用户账号，也可以作为 LDAP 或 RADIUS 服务器上的外部用户添加自定义用户账号。每个托管设备单独维护用户账号。例如，将某个用户添加到 管理中心时，该用户只能访问管理中心；您不能使用该用户名直接登录受管设备。您必须单独在受管设备上添加用户。

内部和外部用户

托管设备支持两种用户类型：

- 内部用户 - 设备在本地数据库中检查用户。
- 外部用户 - 如果本地数据库中没有用户，则系统会查询外部 LDAP 或 RADIUS 身份验证服务器。

Web 接口和 CLI 访问

管理中心 具有 Web 接口、CLI（可从控制台（串行端口或键盘和显示器）访问或使用 SSH 访问管理界面）和 Linux 外壳。有关管理 UI 的详细信息，请参阅系统用户界面。

请参阅以下有关 FMC 用户类型及其可以访问的 UI 的信息：

- 管理员用户- 管理中心 支持两种不同的内部 **管理员** 用户：一种用于 Web 接口，另一种用于 CLI 访问。系统初始化过程会同步这两个 **管理员** 账户的密码，因此它们开始时相同，但由不同的内部机制跟踪，并且在初始配置后可能会出现分歧。有关系统初始化的详细信息，请参阅您的型号的 入门指南 。（要更改 Web 接口 **管理员**密码，请使用 **系统**（⚙） > **用户 (Users)** > **用户**。要更改 CLI **管理员**密码，请使用 管理中心 CLI 命令 **configure password**。）
- 内部用户 - 在 Web 界面中添加的内部用户仅具有 Web 接口访问权限。
- 外部用户 - 外部用户具有 Web 接口访问权限，您可以选择配置 CLI 访问权限。
- SSO 用户 - SSO 用户仅具有 Web 接口访问权限。

注意 CLI 用户可以使用 **expert** 命令访问 Linux 外壳。强烈建议您不要使用 Linux 外壳，除非 Cisco TAC 或 管理中心 文档明确说明需要这样做。CLI 用户可以获得 Linux 外壳中的 `sudoers` 权限，带来安全风险。出于系统安全原因，我们强烈建议：

- 限制具有 CLI 访问权限的用户列表。
- 请勿在 Linux 外壳中直接添加用户；请仅使用本章中的这些程序。

用户角色

CLI 用户角色

管理中心 上的 CLI 外部用户没有用户角色；他们可以使用所有可用命令。

Web 界面用户角色

用户权限以分配的用户角色为基础。例如，可以授予分析师预定义角色（如“安全分析师”和“发现管理员”），并为管理设备的安全管理员保留“管理员”角色。也可以创建具有根据贵组织需求定制的访问权限的自定义用户角色。

管理中心包括以下预定义的用户角色：

注释 出于并发会话限制的目的，系统将其视为只读的预定义用户角色在 **系统**（⚙） > **用户** > **用户** 和 **系统**（⚙） > **用户** > **用户角色**下的角色名称中标记为 （**只读**） 。如果用户角色的角色名称中不包含（**只读**）**(Read Only)**，则系统认为该角色为读/写。有关并发会话限制的详细信息，请参阅 用户配置。

访问管理员

提供对**策略 (Policies)** 菜单中访问控制策略和关联功能的访问权限。“访问管理员”(Access Admin) 无法部署策略。

管理员

“管理员”有权访问所有产品信息；其会话如果受攻击会有更高安全风险，因此不能使其免于登录会话超时。

出于安全原因，应限制“管理员”(Administrator) 角色的使用。

发现管理员

提供对**策略 (Policies)** 菜单中网络发现、应用检测和关联功能的访问权限。“发现管理员”(Discovery Admin) 无法部署策略。

外部数据库用户（只有读取权限）

使用支持 JDBC SSL 连接的应用对数据库提供只读访问权限。如果第三方应用要向应用进行身份验证，必须在系统设置中启用数据库访问权限。在Web界面上，“外部数据库用户”(External Database User) 仅有权访问**帮助 (Help)** 菜单中与联机帮助相关的选项。由于此角色的功能不涉及 Web 界面，因此提供访问只是为便于支持和密码更改。

入侵管理员 **(Intrusion Admin)**

提供对**策略 (Policies)** 和**对象 (Objects)** 中所有入侵策略、入侵规则和网络分析策略功能的访问权限。“入侵管理员”(Intrusion Admin) 无法部署策略。

维护用户

提供对监控和维护功能的访问权限。“维护用户”(Maintenance User) 有权访问**运行状况 (Health)** 和**系统 (System)** 菜单中与维护相关的选项。

网络管理员

提供对**策略 (Policies)** 菜单中访问控制、SSL 检查、DNS 策略和身份策略功能以及**设备 (Devices)** 菜单中设备配置功能的访问权限。“网络管理员”(Network Admin) 可对设备部署配置更改。

安全分析师

提供对**概述 (Overview)**、**分析 (Analysis)**、**运行状况 (Health)** 和**系统 (System)** 菜单中安全事件分析功能的访问权限，以及对其中运行状况事件的只读访问权限。

Security Analyst (Read Only)

提供对**概述 (Overview)**、**分析 (Analysis)**、**运行状况 (Health)** 和**系统 (System)** 菜单中安全事件分析功能和运行状况事件的只读访问权限。

具有此角色的用户还可以：

- 从特定设备的运行状况监控页面，生成并下载故障排除文件。
- 在用户首选项下，设置文件下载首选项。
- 在用户首选项下，设置事件视图的默认时间段（**审核日志时间窗口**除外）。

安全审批人

提供对**策略 (Policies)** 菜单中访问控制和关联策略以及网络发现策略的访问权限。“安全审批人”(Security Approver) 可以查看和部署这些策略，但不能进行策略更改。

威胁情报导向器 (TID) 用户

提供对**情报**菜单中威胁情报导向器配置的访问。威胁情报导向器 (TID) 用户可以查看和配置 TID。

用户密码

以下规则适用于管理中心上启用或禁用无人值守管理(LOM)的内部用户账户的密码。不同的密码要求适用于外部身份验证的账户或启用了安全认证合规性的系统。有关详细信息，请参阅为管理中心配置外部身份验证，第 8 页和安全认证合规性。

在管理中心初始配置期间，系统要求**管理员**用户设置账户密码，以满足下表中所述的强密码要求。对于物理 管理中心，使用启用 LOM 的强密码要求；对于虚拟管理中心，使用未启用 LOM 的强密码要求。此时，系统会同步 Web 界面**管理员** 和 CLI 访问 **管理员**的密码。初始配置后，Web 界面**管理员**可以删除强密码要求，但 CLI 访问**管理员**必须始终遵守强密码要求，且未启用 LOM。

	未启用 LOM	已启用 LOM
密码强度检查开启	密码必须包含： • 至少八个字符，或管理员为用户配置的字符数，以较大者为准。 • 连续的重复字符数不超过两个 • 至少一个小写字母 • 至少一个大写字母 • 至少一位 • 至少一个特殊字符，例如 ！ @ # * - _ + 系统会将您的密码与密码破解词典进行比较，该词典不仅会检查许多英语词典单词，还会检查其他容易被常用密码破解技术破解的字符串。	密码必须包含： • 介于 8 到 20 个字符之间 （在 MC 1000、MC 2500 和 MC 4500 上，上限为 14 个字符，而不是 20 个字符。） • 连续的重复字符数不超过两个 • 至少一个小写字母 • 至少一个大写字母 • 至少一位 • 至少一个特殊字符，例如 ！ @ # * - _ + 不同系列的物理 管理中心 之间的特殊字符规则有所不同。我们建议您只选择上面最后一项中列出的特殊字符。 请勿在密码中包含用户名。 系统会将您的密码与密码破解词典进行比较，该词典不仅会检查许多英语词典单词，还会检查其他容易被常用密码破解技术破解的字符串。

	未启用 LOM	已启用 LOM

密码强度检查关闭	密码必须包含管理员为用户配置的最小字符数。（有关详细信息，请参阅 添加或编辑内部用户，第 6 页 。）	密码必须包含：
		• 介于 8 到 20 个字符之间 （在 MC 1000、MC 2500 和 MC 4500 上，上限为 14 个字符，而不是 20 个字符。）
		• 至少包含四种以下类别的字符：
		  • 大写字母
		  • 小写字母
		  • 数字
		  • 特殊字符，例如！@ # * - _ +
		不同系列的物理 管理中心 之间的特殊字符规则有所不同。我们建议您只选择上面最后一项中列出的特殊字符。
		请勿在密码中包含用户名。

管理中心用户帐户的指南和限制

- 管理中心 包括一个 **管理员** 用户用于所有形式的访问；您无法删除 **管理员** 用户。默认初始密码为 **Admin123**；系统会强制您在初始化过程中更改此设置。有关系统初始化的详细信息，请参阅您的型号的 入门指南 。
- 默认情况下，以下设置适用于 管理中心上的所有用户账户：
  - 重复使用密码方面没有限制。
  - 系统不会跟踪成功登录。
  - 系统不会为输入错误登录凭证的用户强制执行定时临时锁定。
  - 对可以同时打开的只读和读/写会话的数量没有用户定义的限制。

  您可以将所有用户的这些设置更改为系统配置。**(系统**（⚙）> **配置** > **用户配置)** 请参阅 用户配置。
- 在初始设置时向用户分配默认访问角色时，请确保遵循最小权限原则。当用户首次使用其凭证登录系统时，他们的账户将被分配此默认访问角色。我们建议将默认访问角色设置为任何人登录系统所需的最低权限。例如，可以为常见用户提供“安全分析师（只读）”角色作为默认访问角色，并且可以将管理员添加到单独的管理员组以授予他们完全管理员权限。如果在分配默认访问角色时不遵循最小权限原则，则在后续登录时可能会为用户分配意外的权限级别。这可

能会导致用户拥有超出其所需访问角色的权限。请注意，此准则适用于所有用户 - 内部、外部或 CAC 用户。

如果使用默认访问角色登录的用户需要临时提升其权限，则具有管理权限的用户可以通过为其分配具有更高权限的角色来临时为其提供所需的更高级别的访问权限。此权限将在24小时不活动后撤销，并且用户将返回其默认访问角色。

如果用户需要将永久访问角色重新分配到更高权限级别（例如系统管理员），请使用“组控制访问角色”方法为用户提供管理员访问权限。此方法可确保提供的访问角色持续超过24小时，并且用户将根据组分配具有正确的权限级别。有关配置组控制访问角色的详细信息，请参阅为管理中心 步骤 15 部分。

FMC 用户帐户的前提条件和要求

型号支持

管理中心

支持的域

- SSO 配置 - 仅全局。
- 所有其他功能 - 任意。

用户角色

- SSO 配置 - 只有通过内部或通过 LDAP 或 RADIUS 进行身份验证的具有管理员角色的用户才能配置 SSO。
- 所有其他功能-具有管理员角色的任何用户。
- 使用 LDAP 配置通用访问卡身份验证 ， 第 23 页 还支持 网络管理员 角色。

添加或编辑内部用户

此程序介绍如何为 管理中心的 Web 界面中添加自定义内部用户账号。

系统 (System) > **用户 (Users)** > **用户 (Users)** 显示您手动添加的内部用户，以及用户使用 LDAP 或 RADIUS 身份验证登录时自动添加的外部用户。对于外部用户，如果分配具有较高权限的角色，可以在此屏幕上修改用户角色；不能修改密码设置。

在 管理中心上的多域部署中，用户仅在创建它们的域中可见。如果您在全局域中添加了一个用户并为其分配了分叶域的用户角色，则该用户仍显示在添加其的全局**用户**页面，尽管该用户属于分叶域。

如果在设备上启用安全认证合规性或无人值守管理 (LOM)，则适用不同的密码限制。有关安全认证合规性的详细信息，请参阅安全认证合规性。

当您在分叶域中添加用户时，该用户在全局域中不可见。

注释 避免让多个管理员用户同时在 管理中心上创建新用户，因为这可能会因用户数据库访问冲突而导致错误。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 要创建新用户：

a) 点击**创建用户**。

b) 输入**用户名 (User Name)**。

用户名必须符合以下限制：

- 最多 32 个字母数字字符，外加连字符 (-) 和下划线 (_)。
- 字母可以是大写或小写。
- 不能包含除句号 (.) 、连字符 (-)和下划线 (_)和以外的任何标点或特殊字符。

步骤 3 要编辑现有用户，请点击要编辑的用户旁边的 **编辑**（✎） 图标。

步骤 4 **真实名称 (Real Name)**：输入描述性信息，以标识账户所属的用户或部门。

步骤 5 对于使用 LDAP 或 RADIUS 登录时自动添加的用户，**使用外部身份验证方法 (Use External Authentication Method)** 复选框已选中 。无需预配置外部用户，因此您可以忽略此字段。对于外部用户，通过取消选中此复选框，可以将此用户恢复为内部用户。

步骤 6 在**密码**和**确认密码**字段中输入值。

这些值必须符合您为此用户设置的密码选项。

步骤 7 设置**最大失败登录次数**。

输入不含空格的整数，用于指定每个用户在登录尝试失败后且帐户锁定之前可以尝试的最大次数。默认设置为五次尝试；使用 **0** 可允许无限次的登录失败。除非已启用安全认证合规性，否则**管理员**账户不会在达到最大失败登录次数后被锁定。

步骤 8 设置**最大密码长度**。

输入不含空格的整数，用于指定用户密码的最小所需长度（以字符数为单位）。默认设置为 **8**。值为 **0** 指示无需最小长度。

步骤 9 设置**密码到期前天数**。

输入用户密码到期之前经过的天数。默认设置为 **0**，指示密码永不过期。如果更改默认值，则**用户**列表的**密码生存期**列指示每个用户密码的剩余有效天数。

步骤 10 设置**密码过期前警告天数**。

输入在用户密码实际到期之前警告用户必须更改其密码的警告天数。默认设置为 0 天。

步骤 11 设置以下**选项**：

- **登录时强制密码重置 (Force Password Reset on Login)**：强制用户在下次登录时更改密码。
- **检查密码强度 (Check Password Strength)**：需要强密码。启用密码强度检查时，密码必须符合用户密码，第 4 页中所述的强密码要求。
- **免除浏览器会话超时 (Exempt from Browser Session Timeout)**：免除用户的登录会话因不活动而终止。具有管理员角色的用户无法获得豁免。

步骤 12 在**用户角色配置 (User Role Configuration)** 区域中分配用户角色。有关用户角色的详细信息，请参阅自定义 Web 界面的用户角色，第 73 页。

对于外部用户，如果通过组或列表成员身份用户角色，则无法删除最低访问权限。但是，可以分配其他权限。如果用户角色是您在设备上设置的默认用户角色，则可以在用户帐户中不受限制地修改角色。修改用户角色时，**用户**选项卡上的**身份验证方法**列提供**外部 - 本地修改**的状态。

显示的选项取决于设备是在单域还是多域部署中。

- 单域：查看要为用户分配的用户角色。
- 多域：在多域部署中，可以在已为您分配管理员访问权限的任何域中创建用户账号。用户在每个域中可拥有不同的权限。可以同时分配祖先域和后代域中的用户角色。例如，可以在全局域中为用户分配只读权限，但在后代域中分配管理员权限。请参阅以下步骤：

  1. 点击**添加域**。
  2. 从**域 (Domain)** 下拉列表中选择域。
  3. 选中要分配用户的用户角色。
  4. 点击**保存 (Save)**。

步骤 13 （可选，仅用于物理 管理中心）如果您为用户分配了管理员角色，系统将显示**管理员选项 (Administrator Options)**。您可以选择**允许无人值守管理访问 (Allow Lights-Out Management Access)** 以向用户授予无人值守管理访问权限。有关无人值守管理的详细信息，请参阅无人值守管理概述。

步骤 14 点击**保存 (Save)**。

为管理中心配置外部身份验证

要启用外部身份验证，您需要添加一个或多个外部身份验证对象。

关于管理中心外部身份验证

在为管理用户启用外部身份验证时，管理中心 会使用 外部身份验证对象中指定的 LDAP 或 RADIUS 服务器验证用户凭证。

您可以为 Web 界面访问配置多个外部身份验证对象。例如，如果您有 5 个外部身份验证对象，则其中任意对象的用户均可通过身份验证来访问 Web 界面。对于 CLI 访问，仅可使用一个外部身份验证对象。如果您启用了多个外部身份验证对象，用户仅可使用列表中的第一个对象进行身份验证。

管理中心 和 威胁防御 设备可使用外部身份验证对象。不同应用/设备可共享同一个对象，也可以为它们创建不同的对象。

注释 威胁防御 和 管理中心 的超时范围不同，因此，如果共享对象，请确保不要超过 威胁防御 的较小超时范围（对于 LDAP 为 1-30 秒，对于 RADIUS 为 1-300 秒）。如果将超时设置为更高的值，则 威胁防御 外部身份验证配置将不起作用。

对于管理中心，请直接在 **系统** > **用户** > **外部身份验证** 选项卡上启用外部身份验证对象；此设置仅会影响 管理中心 的使用情况，无需在此选项卡上为了受管设备的使用而启用此设置。对于 威胁防御 设备，必须在部署到设备的平台设置中启用外部身份验证对象。

Web 界面用户由外部身份验证对象中的 CLI 用户单独定义。对于 RADIUS 上的 CLI 用户，您必须预配置外部身份验证对象中的 RADIUS 用户名列表。对于 LDAP，您可以指定过滤器来匹配 LDAP 服务器上的 CLI 用户。

您无法将同时配置用于 CAC 身份验证的 LDAP 对象用于 CLI 访问。

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。确保：

- 限制具有 CLI 或 Linux 外壳访问权限的用户列表。
- 请勿创建 Linux 外壳用户。

关于 LDAP

通过轻量级目录访问协议 (LDAP)，可以在网络上设置一个目录，用于在一个集中位置组织对象，如用户凭证。然后，多个应用可以访问这些凭证和用于描述凭证的信息。如果需要更改用户凭证，则可以在一个位置进行更改。

Microsoft 已宣布 Active Directory 服务器将在 2020 年开始实施 LDAP 绑定和 LDAP 签名。Microsoft 将这些作为一项要求，因为在使用默认设置时，Microsoft Windows 中存在一个权限提升漏洞，该漏洞可能允许中间人攻击者将身份验证请求成功转发到 Windows LDAP 服务器。有关详细信息，请参阅 Microsoft 支持站点上的 Windows 2020 LDAP 通道绑定和 LDAP 签名要求 。

如果您尚未执行此操作，我们建议您开始使用 TLS / SSL 加密对 Active Directory 服务器进行身份验证。

关于 RADIUS

远程身份验证拨入用户服务 (RADIUS) 是用于验证/授权和说明用户对网络资源的访问的一种身份验证协议。可以为符合 RFC 2865 的任何 RADIUS 服务器创建身份验证对象。

Firepower 设备支持使用 SecurID 令牌。使用 SecurID 通过服务器来配置身份验证时，利用该服务器进行身份验证的用户会将 SecurID 令牌追加到其 SecurID PIN 的末尾，并使用此代码作为其登录密码。在 Firepower 设备上无需配置任何其他信息来支持 SecurID。

添加 管理中心的 LDAP 外部身份验证对象

添加 LDAP 服务器以支持外部用户执行设备管理。

开始之前

- 您必须在设备上指定 DNS 服务器用于域名查找。即使您在此程序中为 LDAP 服务器指定了 IP 地址而非主机名，LDAP 服务器也可能返回可能包括主机名的身份验证 URI。解析主机名需要进行 DNS 查询。请参阅 修改 管理中心 管理接口 来添加 DNS 服务器。
- 如果是配置用于 CAC 身份验证的 LDAP 身份验证对象，请勿移除在计算机中插入的 CAC。启用用户证书后，必须一直插入 CAC。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击 **External Authentication** 选项卡。

步骤 3 点击添加图标 （+）**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 4 将**身份验证方法**设置为 **LDAP** 。

步骤 5 （可选） 如果计划将此身份验证对象用于 CAC 身份验证和授权，请勾选 **CAC** 的对应复选框。

此外，还必须遵循使用 LDAP 配置通用访问卡身份验证，第 23 页中的程序，才能完全配置 CAC 身份验证和授权。不能将此对象用于 CLI 用户。

步骤 6 在 **CAC 环境变量** 字段中，输入包含用于登录的用户名的环境变量。选中 **CAC** 复选框时，将显示此字段。启用 CAC 并使用浏览器访问设备后，可以使用包含 CAC 信息的环境变量进行登录。示例，

```
SSL_CLIENT_S_DN_CN = last.first.1234567890
```

步骤 7 在**CAC 用户名模板**字段中，输入模板以从CAC环境变量中提取用户名部分。例如，输入`\.(\d{10})$`以提取 CAC 环境变量字符串的最后 10 位数字。

步骤 8 输入**名称**和可选**说明**。

步骤 9 从下拉列表中选择**服务器类型**。

提示 如果点击**设置默认值 (Set Defaults)**，设备将使用服务器类型的默认值填充**用户名模板 (User Name Template)**、**UI 访问属性 (UI Access Attribute)**、**CLI 访问属性 (CLI Access Attribute)**、**组成员属性 (Group Member Attribute)** 和**组成员 URL 属性 (Group Member URL Attribute)** 字段。

步骤 10 对于**主服务器**，输入**主机名/IP 地址**。

如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与此字段中使用的主机名匹配。此外，加密连接不支持 IPv6 地址。

步骤 11 （可选） 更改**端口**使用的默认值。

步骤 12 （可选） 输入**备份服务器**参数。

步骤 13 输入 **LDAP 特定参数**。

a) 在**基础 DN** 中为要访问的 LDAP 目录输入基础 DN。例如，要对 Example 公司的 Security 组织中的名称进行身份验证，请输入 `ou=security,dc=example,dc=com`。或者，点击**获取 DN (Fetch DNs)**，然后从下拉列表中选择相应的基本可分辨名称。

b) （可选） 输入**基本过滤器**。例如，如果目录树中的用户对象具有 `physicalDeliveryOfficeName` 属性，并且 New York 办公室中的用户对于该属性具有属性值 `NewYork`，要仅检索 New York 办公室中的用户，请输入 `(physicalDeliveryOfficeName=NewYork)`。

如果使用 CAC 身份验证，要仅过滤活动用户账号（禁用的用户账号除外），请输入 `(!(userAccountControl:1.2.840.113556.1.4.803:=2))`。此条件检索 AD 中属于 `ldpgrp` 组且 `userAccountControl` 属性值不为 `2` （已禁用）的用户账户。

c) 为有足够凭证浏览 LDAP 服务器的用户输入**用户名**。例如，如果是连接到 OpenLDAP 服务器，其中用户对象具有 `uid` 属性，并且 Example 公司 Security 部门的管理员对象的 `uid` 值为 `NetworkAdmin`，则您可以输入 `uid=NetworkAdmin,ou=security,dc=example,dc=com`。

d) 在**密码**和**确认密码**字段中输入用户密码。

e) （可选） 点击**显示高级选项**配置以下高级选项。

- **加密 (Encryption)** - 点击**无 (None)**、**TLS** 或 **SSL**。

  如果在指定端口后更改加密方法，则会将端口重置为该方法的默认值。对于**无**或 **TLS**，端口将重置为默认值 389。如果选择 SSL 加密，端口将重置为 636。

- **SSL 证书上传路径 (SSL Certificate Upload Path)** - 对于 SSL 或 TLS 加密，必须通过点击**选择文件 (Choose File)** 选择一个证书。

  要删除上传的证书，请选中**清除已加载证书 (Clear loaded certificate)** 复选框。此选项只有在上传了证书并处于外部身份验证对象的编辑模式时才会出现。

  如果之前已上传证书并要将其替换，请上传新证书并将该配置重新部署到设备，以复制转移新证书。

  注释 TLS 加密要求所有平台上均有证书。但我们建议您始终上传 SSL 证书以防中间人攻击。

- **用户名模板** - 提供与您的 **UI 访问属性**对应的模板。例如，要通过连接到 UI 访问属性为 `uid` 的 OpenLDAP 服务器来对 Example 公司的 Security 组织中工作的所有用户进行身份验证，可在**用户名模板**字段中输入 `uid=%s,ou=security,dc=example,dc=com`。对于 Microsoft Active Directory Server，可以输入 `%s@security.example.com`。

  CAC 身份验证需要使用此字段。

- **外壳用户名模板 (Shell User Name Template)** - 提供与您的 **CLI 访问属性 (CLI Access Attribute)** 对应的模板以进行 CLI 用户身份验证。例如，要通过连接到 CLI 访问属性为 `sAMAccountName` 的 OpenLDAP 服务器来对 Security 组织中工作的所有用户进行身份验证，可在**外壳用户名模板 (Shell User Name Template)** 字段中输入 `%s` 。
- **超时（秒）**-输入滚动到备份连接之前等待的秒数（1-1024 秒）。默认值为 30。

  注释 威胁防御 和 管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 威胁防御的较小超时范围（1-30 秒）。如果将超时设置为更高的值，则 威胁防御 LDAP 配置将不起作用。

步骤 14 配置**属性映射 (Attribute Mapping)** 以基于属性检索用户。

- 输入 **UI 访问属性**或点击**获取属性**，以检索可用属性的列表。例如，在 Microsoft 活动目录服务器上，可能要使用 UI 访问属性检索用户，因为在 Active 目录服务器用户对象上可能没有 `uid` 属性。相反，可以通过在 **UI 访问属性 (UI Access Attribute)** 字段中输入 `userPrincipalName` 来搜索 `userPrincipalName` 属性。

  CAC 身份验证需要使用此字段。
- 如果要使用用户可分辨类型之外的外壳访问属性，请设置 **CLI 访问属性 (CLI Access Attribute)** 。例如，在 Microsoft 活动目录服务器上，通过键入 `sAMAccountName` 可使用 `sAMAccountName` CLI 访问属性来检索外壳访问用户。

步骤 15 （可选） 配置**组控制的访问角色**。

如果不使用组控制的访问角色配置用户权限，则用户仅具有外部身份验证策略默认授予的权限。

a) （可选） 在与用户角色对应的字段中，输入包含应向其分配这些角色的用户的 LDAP 组的可分辨名称。

   引用的任何组都必须存在于 LDAP 服务器上。可以引用静态 LDAP 组或动态 LDAP 组。静态 LDAP 组是成员身份由指向特定用户的组对象属性确定的组，动态 LDAP 组是通过创建根据用户对象属性检索组用户的 LDAP 搜索来确定成员身份的组。角色的组访问权限仅影响身为组成员的用户。

   如果使用动态组，则完全按照 LDAP 查询在 LDAP 服务器上的配置来使用 LDAP 查询。因此，Firepower 设备将搜索的递归数限制为 4，以防搜索语法错误导致无限循环。

   示例：

   在**管理员**字段中输入以下内容，以便对 Example 公司信息技术部门中的名称进行身份验证：

   ```
   cn=itgroup,ou=groups, dc=example,dc=com
   ```

b) 对于不属于任何指定组的用户，选择**默认用户角色**。
c) 如果使用静态组，请输入**组成员属性 (Group Member Attribute)**。

   示例：

   如果使用 `member` 属性指示默认“安全分析师”访问权限静态组中的成员身份，请输入 `member`。

d) 如果使用动态组，请输入**组成员 URL 属性 (Group Member URL Attribute)**。

示例：

如果 `memberURL` 属性包含用于检索为默认“管理员”访问权限指定的动态组成员的 LDAP 搜索，请输入 `memberURL`。

如果更改用户的角色，必须保存/部署更改的外部身份验证对象，并从**用户**屏幕中移除该用户。该用户下次登录时会自动被重新添加。

步骤 16 （可选） 设置 **CLI 访问过滤器 (Shell Access Attribute)** 以允许 CLI 用户。

为防止对 CLI 访问进行 LDAP 身份验证，请将此字段留空。要指定 CLI 用户，请选择以下方法之一：

- 要使用配置身份验证设置时指定的同一过滤器，请选中 **与基本过滤器相同**复选框。
- 要根据属性值检索管理用户条目，请输入要用作过滤器的属性名、比较运算符和属性值（用括号括起来）。例如，如果所有网络管理员都具有属性值为 `shell` 的 `manager` 属性，则可以设置基本过滤器 `(manager=shell)`。

用户名必须对 Linux 有效：

- 最多 32 个字母数字字符，外加句号 (.)、 连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含 at 符号 (@) 或斜线 (/)

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

注释 请勿创建与包括在 **CLI 访问过滤器 (CLI Access Filter)** 中的用户具有相同用户名的任何内部用户。唯一的内部 管理中心 用户应为 **admin**；请勿在 **CLI 访问过滤器 (CLI Access Filter)** 中包含**管理员**用户。

步骤 17 （可选） 点击**测试**以测试与 LDAP 服务器的连接状况。

测试输出列出有效和无效的用户名。有效用户名是唯一的，并且可以包含下划线 (_)、句号 (.)、连字符 (-) 和字母数字字符。请注意，受 UI 页面大小限制，测试与具有 1000 个以上用户的服务器的连接仅会返回 1000 个用户。如果测试失败，请参阅LDAP 身份验证连接故障排除 ，第 78 页。

步骤 18 （可选） 此外，还可以输入**其他测试参数**来测试应可以执行身份验证的用户的用户凭证：输入**用户名** `uid` 和**密码**，然后点击**测试**。

如果是连接到 Microsoft Active Directory Server 并提供 UI 访问属性来代替 `uid`，请使用该属性的值作为用户名。还可以为用户指定完全限定的可分辨名称。

提示 如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。要验证服务器配置是否正确，请点击**测试**，而无需首先在**其他测试参数**字段中输入用户信息。如果成功，请提供要通过特定用户进行测试的用户名和密码。

示例：

要测试是否可以在 Example 公司检索到 `JSmith` 用户凭证，请输入 `JSmith` 和正确的密码。

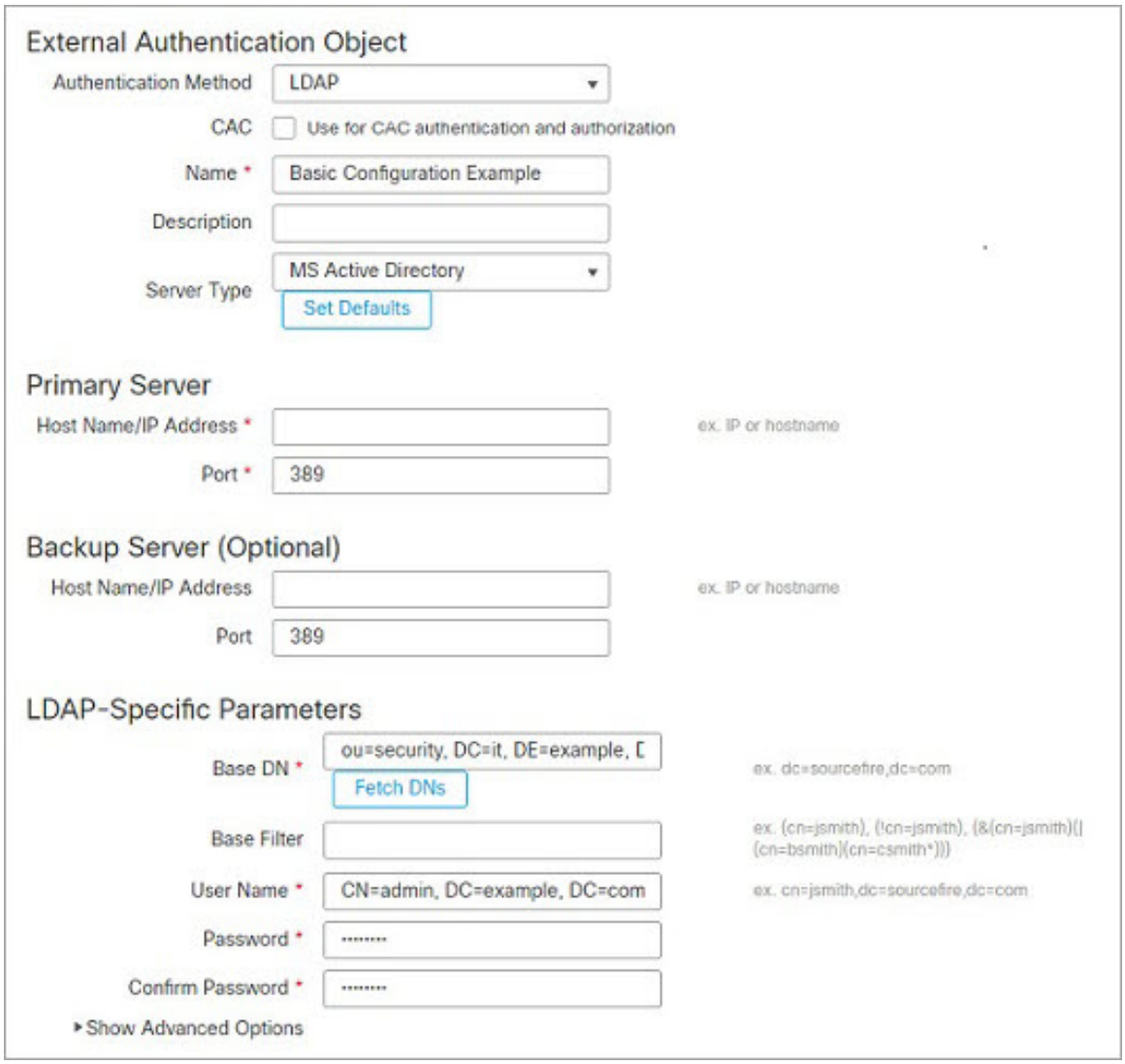
步骤 19 点击**保存 (Save)**。

步骤 20 启用此服务器。请参阅为管理中心上的用户启用外部身份验证 ，第 22 页。

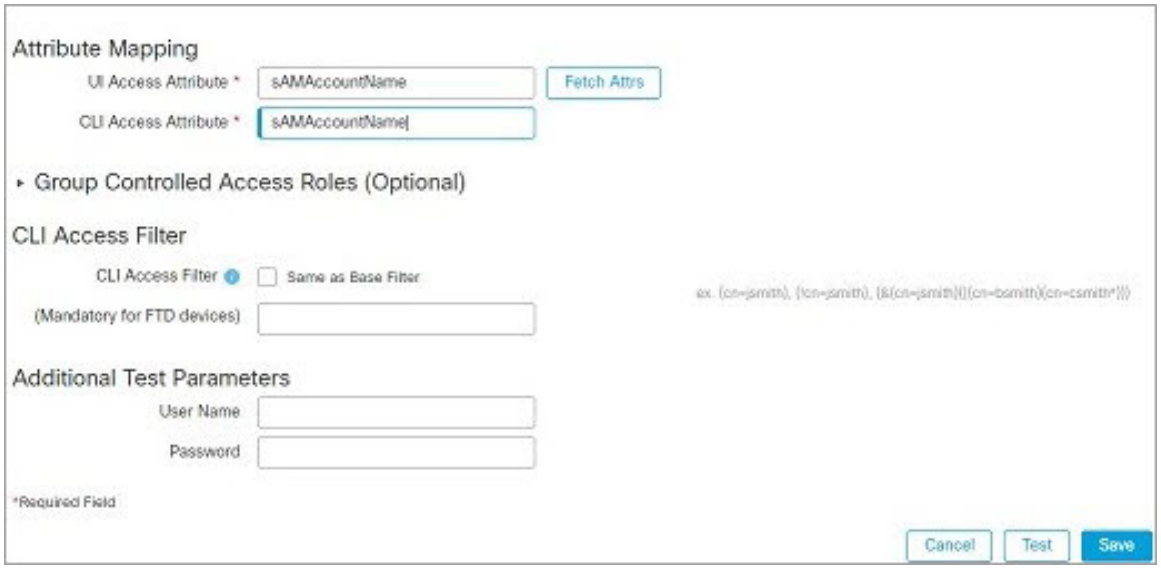
示例

基本示例

下图说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的基本配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 389 进行访问。



此示例显示对于示例公司的信息技术领域中的安全组织使用基本可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。



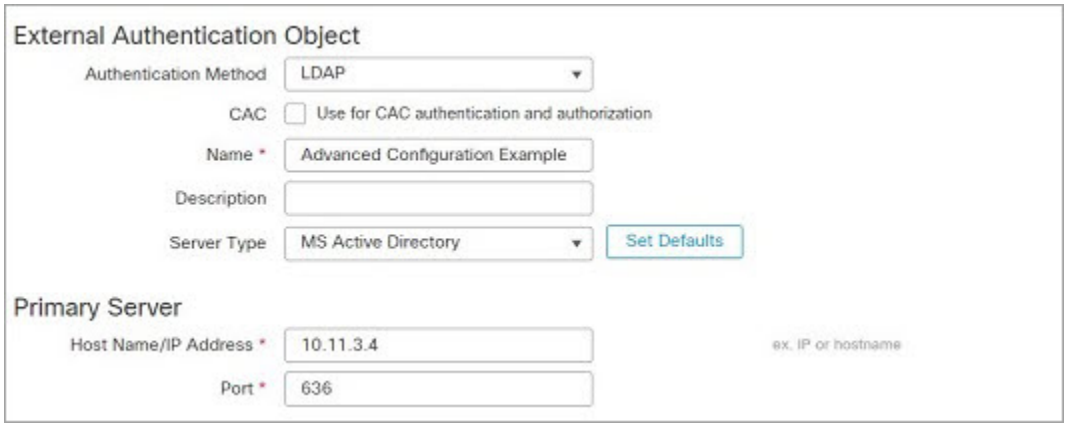
但是，由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。选择 MS Active Directory 服务器类型并点击**设置默认值 (Set Defaults)** 会将“UI 访问属性”(UI Access Attribute) 设置为 `sAMAccountName`。因此，当用户尝试登录系统时，系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

此外，当用户登录到设备上的 CLI 账户中时， `sAMAccountName` 的 CLI会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

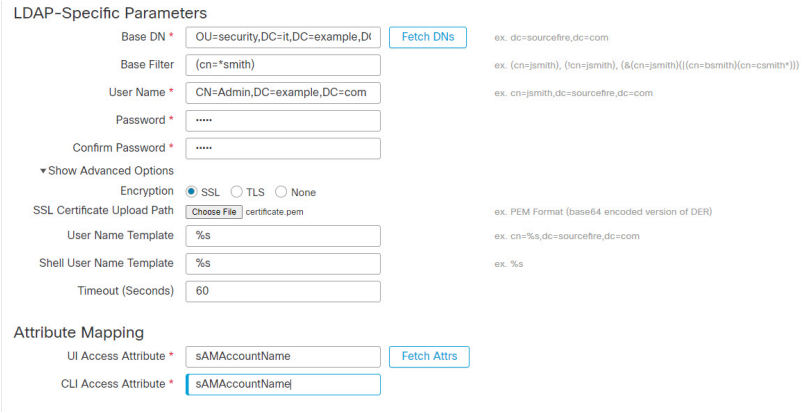
请注意，由于未对此服务器应用基本过滤器，因此系统会检查目录中基本可分辨名称所指示的所有对象的属性。经过默认时间段（或 LDAP 服务器上设置的超时期）后，与服务器的连接将超时。

高级示例

此示例说明 Microsoft Active Directory Server 的 LDAP 登录身份验证对象的高级配置。此示例中的 LDAP 服务器的 IP 地址为 10.11.3.4。此连接使用端口 636 进行访问。



此示例显示对于示例公司的信息技术领域中的安全组织使用基本可分辨名称 `OU=security,DC=it,DC=example,DC=com` 的连接。但请注意，此服务器具有基本过滤器 `(cn=*smith)`。该过滤器将从服务器检索到的用户限制为公用名称以 `smith` 结尾的用户。

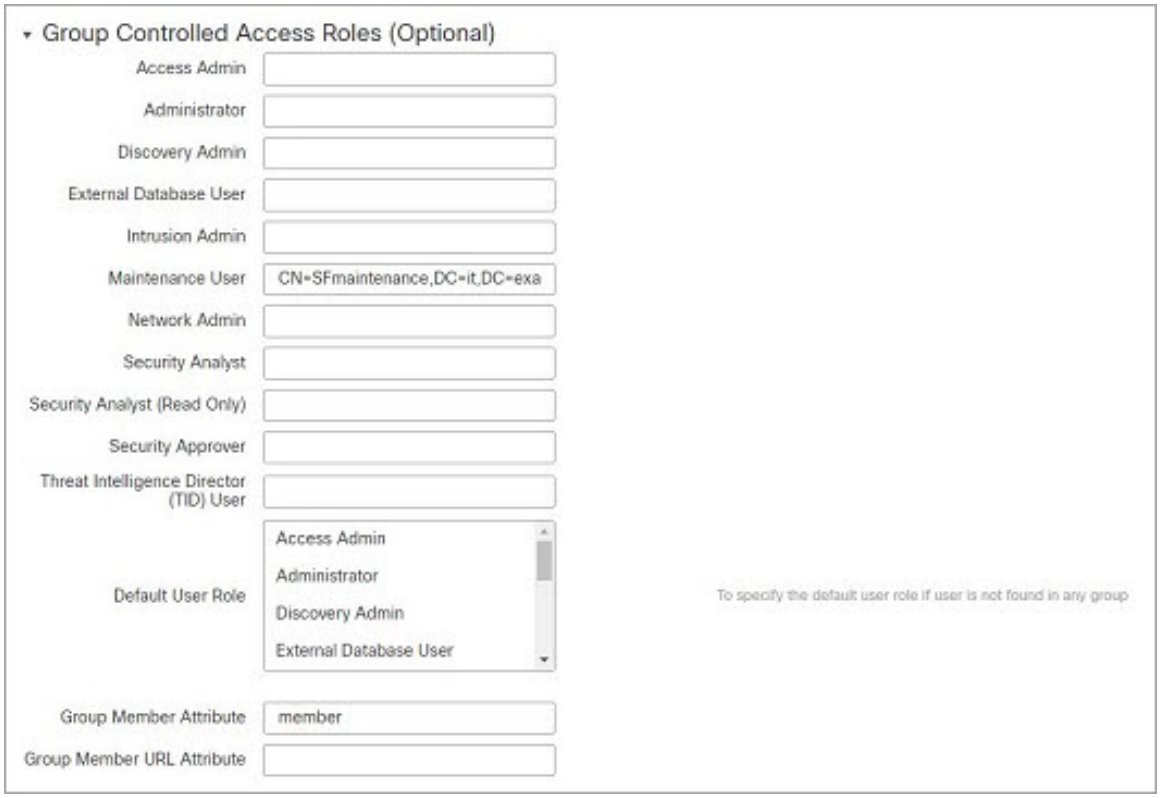


与服务器的连接使用 SSL 进行加密，并且会为该连接使用一个名为 `certificate.pem` 的证书。此外，由于 **超时（秒）** 设置，与服务器的连接在 60 秒后将超时。

由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。请注意，配置包括 `sAMAccountName`的 **UI 访问属性 (UI Access Attribute)**。因此，当用户尝试登录系统时，系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

此外，当用户登录到设备上的 CLI 账户中时， `sAMAccountName` 的 **CLI 访问属性** 会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

此示例还具有相应的组设置。“维护用户”角色将被自动分配给具有成员组属性且基本域名为 `CN=SFmaintenance,DC=it,DC=example,DC=com` 的组的所有成员。



CLI 访问过滤器 设置为与基本过滤器相同，因此相同用户可以通过 CLI 访问设备，如同通过 web 接口进行访问一样。

添加管理中心的 RADIUS 外部身份验证对象

添加 RADIUS 服务器以支持外部用户执行设备管理。

在多域部署中，外部身份验证对象仅在创建对象的域中可用。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击**外部身份验证 (External Authentication)**。

步骤 3 点击 添加图标 （➕） **添加外部身份验证对象**。

步骤 4 将**身份验证方法**设置为 **RADIUS**。

步骤 5 输入**名称**和可选**说明**。

步骤 6 对于**主服务器**，输入**主机名/IP 地址**。

步骤 7 （可选） 更改**端口**使用的默认值。

步骤 8 输入 **RADIUS 服务器密钥**。

步骤 9 （可选） 输入**备份服务器**参数。

步骤 10 （可选） 输入 **RADIUS 特定参数**。

a) 在 **超时** 中输入重试主服务器之前允许的秒数（介于 1 和 1024 之间）。默认值为 30。

注释 威胁防御 和 管理中心的超时范围不同，因此，如果共享对象，请确保不要超过 威胁防御 的较小超时范围（1-300 秒）。如果将超时设置为更高的值，则 威胁防御 RADIUS 配置将不起作用。

b) 输入滚动到备份服务器之前允许的**重试次数**。默认值为 3。

c) 在与用户角色对应的字段中，输入各用户的名称或确定应分配给这些角色的属性-值对。

将用户名和属性-值对以逗号分隔。

示例：

如果您知道所有本应为“安全分析师”的用户的 `User-Category` 属性值为 `Analyst`，则可以在**安全分析师**字段中输入 `User-Category=Analyst`，以将该角色授予这些用户。

示例：

要将“管理员”角色授予用户 `jsmith` 和 `jdoe`，请在**管理员**字段中输入 `jsmith, jdoe`。

示例：

要将“维护用户”角色授予 `User-Category` 值为 `Maintenance` 的所有用户，请在**维护用户**字段中输入 `User-Category=Maintenance`。

d) 对于不属于任何指定组的用户，请选择**默认用户角色**。

如果更改用户的角色，必须保存/部署更改的外部身份验证对象，并从**用户**屏幕中移除该用户。该用户下次登录时会自动被重新添加。

步骤 11 （可选） **定义自定义 RADIUS 属性**。

如果 RADIUS 服务器返回 `/etc/radiusclient/` 中 `dictionary` 文件内不包含的属性值，并且您计划使用这些属性来设置具有这些属性的用户的角色，则需要定义这些属性。可以通过查看 RADIUS 服务器上的用户配置文件来查找为用户返回的属性。

a) 输入**属性名称**。

定义属性时，请提供属性的名称，其中包含字母数字字符。请注意，属性名称中的单词应以破折号而不是空格进行分隔。

b) 以整数形式输入**属性 ID**。

属性 ID 应为整数且不应与 `etc/radiusclient/dictionary` 文件中的任何现有属性 ID 冲突。

c) 从下拉列表中选择**属性类型**。

还请指定属性的类型：字符串、IP 地址、整数或日期。

d) 点击**添加**以添加自定义属性。

在创建 RADIUS 身份验证对象时，系统会在设备上的 `/var/sf/userauth` 目录中创建该对象的新目录文件。添加的所有自定义属性都会添加到字典文件。

示例：

如果在含有思科路由器的网络上使用 RADIUS 服务器，则可能要使用 `Ascend-Assign-IP-Pool` 属性向从特定 IP 地址池登录的所有用户授予特定角色。`Ascend-Assign-IP-Pool` 是一个整数属性，用于定义允许用户登录的地址池，其中整数指示已分配的 IP 地址池的编号。

要声明自定义属性，请创建一个自定义属性，使其属性名称为 `Ascend-IP-Pool-Definition`，属性 ID 为 `218`，并且属性类型为 `integer`。

然后，可以在**安全分析（只读）(Security Analyst [Read Only])** 字段中输入 `Ascend-Assign-IP-Pool=2`，将只读安全分析师权限授予 `Ascend-IP-Pool-Definition` 属性值为 `2` 的所有用户。

步骤 12 （可选） 在 **CLI 访问过滤器** 区域**管理员 CLI 用户列表** 字段中，输入应具有外壳访问权限的用户名并以逗号分隔。

请确保这些用户名匹配 RADIUS 服务器上的用户名。名称必须是 Linux 有效的用户名：

- 最多 32 个字母数字字符，外加句号 (.)、连字符 (-) 和下划线 (_)
- 全部小写
- 不能以连字符 (-) 开头；不能全部是数字；不能包含 at 符号 (@) 或斜线 (/)

为防止对 CLI 访问进行 RADIUS 身份验证，请将此字段留空。

注释 具有配置层级访问权限的用户可以使用 CLI **expert** 命令访问 Linux 外壳程序。Linux 外壳用户可以获得 root 权限，带来安全风险。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

注释 删除与包括在外壳访问过滤器中的用户具有相同用户名的任何内部用户。对于 管理中心，唯一的内部 CLI 用户是 **管理员**，因此请勿同时创建 **管理员** 外部用户。

步骤 13 （可选） 点击 **测试** 以测试与 RADIUS 服务器的 管理中心 连接。

步骤 14 （可选） 此外，还可以输入**其他测试参数**来测试应可以执行身份验证的用户的用户凭证：输入**用户名**和**密码**，然后点击**测试**。

提示 如果测试用户的名称或密码键入不正确，即使服务器配置正确，测试也会失败。要验证服务器配置是否正确，请点击**测试**，而无需首先在**其他测试参数**字段中输入用户信息。如果成功，请提供要通过特定用户进行测试的用户名和密码。

示例：

要测试是否可以在 Example 公司检索到 `JSmith` 用户凭证，请输入 `JSmith` 和正确的密码。

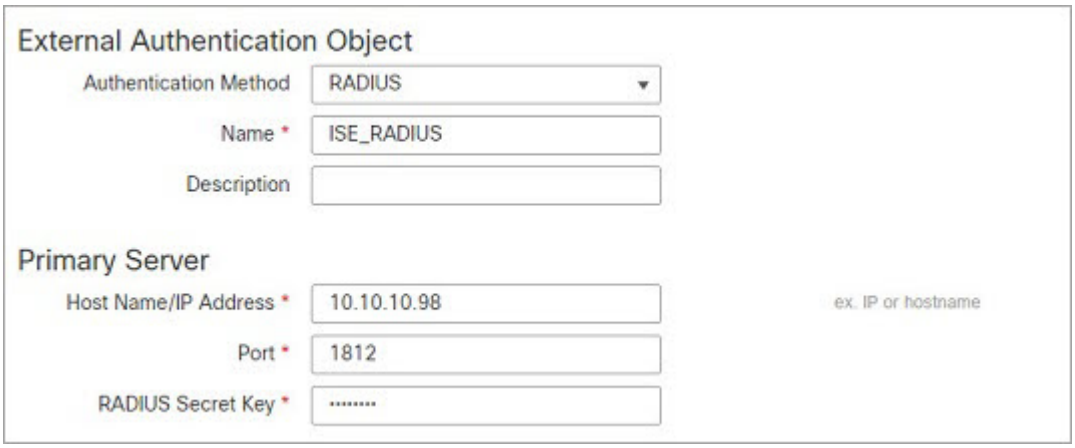
步骤 15 点击**保存 (Save)**。

步骤 16 启用此服务器。请参阅为管理中心上的用户启用外部身份验证，第 22 页。

示例

简单的用户角色指定

下图说明端口 1812 上 IP 地址为 10.10.10.98 的运行 Cisco Identity Services Engine (ISE) 的服务器的示例 RADIUS 登录身份验证对象。未定义备份服务器。



以下示例显示 RADIUS 特定参数，包括超时（30 秒）和 Firepower 系统尝试联系备份服务器（如有）之前的失败重试次数。

此示例说明 RADIUS 用户角色配置的重要方面：

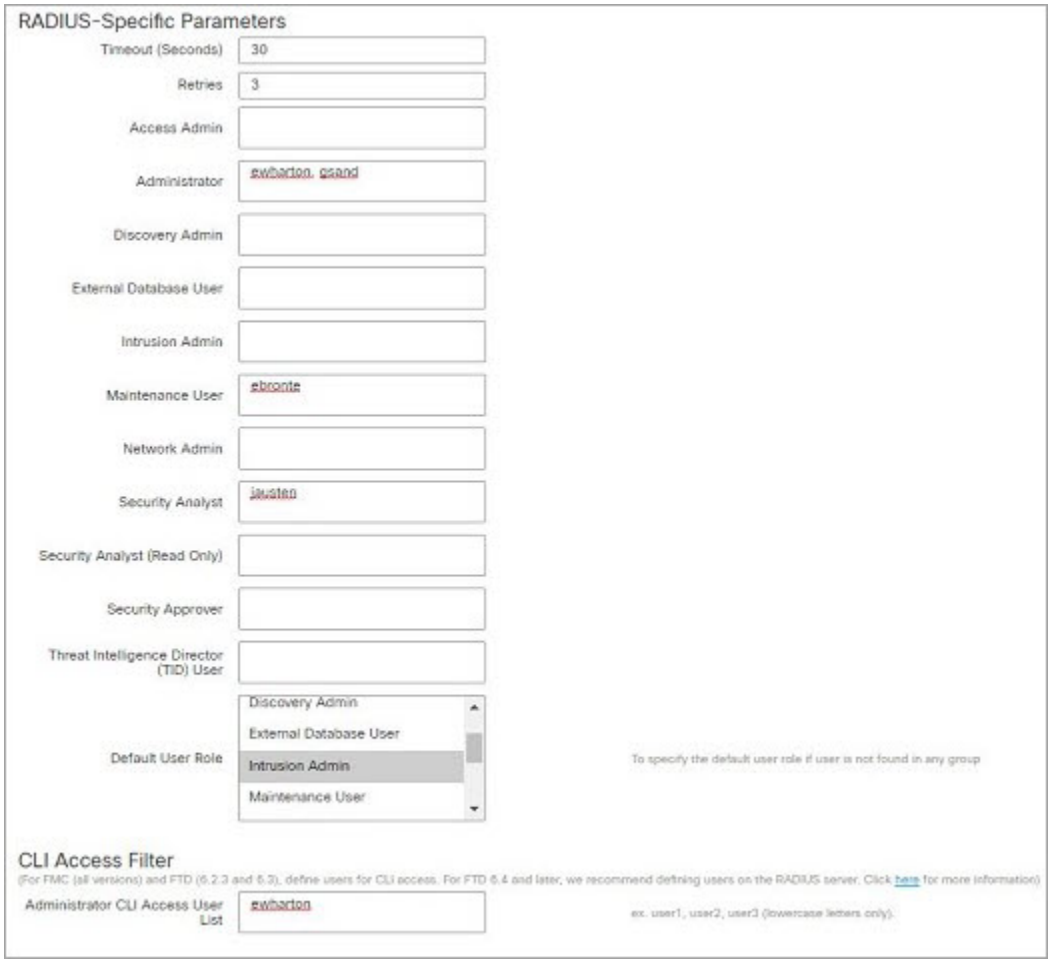
授予用户 `ewharton` 和 `gsand` Web 界面管理权限。

授予用户 `cbronte` Web 界面“维护用户”权限。

授予用户 `jausten` Web 界面“安全分析师”权限。

用户 `ewharton` 可以使用 CLI 帐户登录到设备中。

下图说明示例的角色配置：

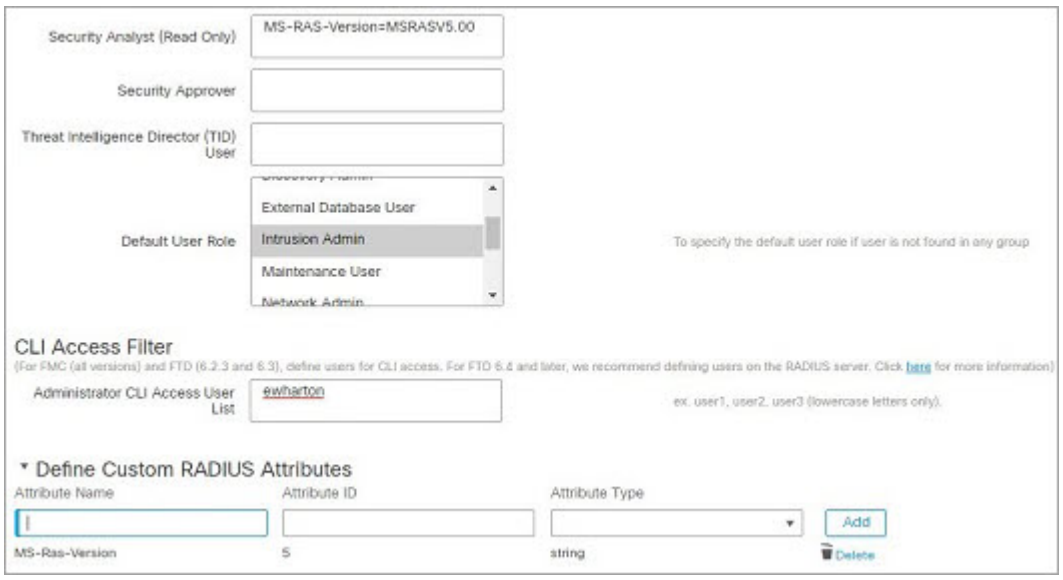


匹配属性-值对的用户角色

可以使用属性-值对识别应接收特定用户角色的用户。如果使用的属性是自定义属性，必须定义该自定义属性。

下图说明与前一示例中相同的 ISE 服务器的示例 RADIUS 登录身份验证对象中的角色配置和自定义属性定义。

但是，在此示例中，由于正在使用 Microsoft 远程访问服务器，因此为一个或多个用户返回了 `MS-RAS-Version` 自定义属性。请注意，`MS-RAS-Version` 自定义属性为字符串。在此示例中，通过 Microsoft v. 5.00 远程访问服务器登录 RADIUS 的所有用户都应得到“安全分析师（只读）”(Security Analyst [Read Only]) 角色，因此请在**安全分析师（只读）(Security Analyst [Read Only]** 字段中输入属性-值对 `MS-RAS-Version=MSRASV5.00`。



为管理中心上的用户启用外部身份验证

在为管理用户启用外部身份验证时，管理中心会使用外部身份验证对象中指定的 LDAP 或 RADIUS 服务器验证用户凭证。

开始之前

根据 添加 管理中心的 LDAP 外部身份验证对象，第 10 页 和 添加管理中心的 RADIUS 外部身份验证对象，第 17 页中所述，添加一个或多个外部身份验证对象。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击**外部身份验证 (External Authentication)**。

步骤 3 为外部 Web 界面用户设置默认用户角色。

没有角色的用户无法执行任何操作。外部身份验证对象中定义的任何用户角色将覆盖此默认用户角色。

a) 点击 **默认用户角色** 值（默认为未选定）。

a) 在**默认用户角色配置**对话框中，选中要使用的角色。

b) 点击**保存 (Save)**。

步骤 4 点击要使用的每个外部身份验证对象旁边的**滑块已启用**（🔵）。如果启用多个对象，系统会按指定顺序参照服务器比较用户。请参阅后续步骤对服务器重新排序。

如果启用外壳身份验证，则必须启用包括**CLI 访问过滤器 (CLI Access Filter)** 的外部身份验证对象。另外，CLI 访问用户只能参照其身份验证对象在列表中排在第一位的服务器进行身份验证。

步骤 5 （可选） 拖放服务器可更改出现身份验证请求时访问身份验证的顺序。

步骤 6 如果要允许外部用户执行 CLI 访问，请选择**外壳身份验证 (Shell Authentication)** > **已启用 (Enabled)**。

注释 CLI 中不支持多域功能。因此， **外壳身份验证** 选项仅在全局域中可用，在子域中不可用。

第一个外部身份验证对象名称显示在**已启用 (Enabled)** 选项旁边，提醒您只有第一个对象用于 CLI。

步骤 7 点击**保存并应用**。

使用 LDAP 配置通用访问卡身份验证

如果您的组织使用通用访问卡 (CAC)，您可以配置 LDAP 身份验证来验证登录 Web 接口的 管理中心 用户。使用 CAC 身份验证，用户可以选择直接登录，而不用为设备提供单独的用户名和密码。

CAC 身份验证用户通过其电子数据交换个人标识符 (EDIPI) 号码进行识别。

在非活动状态持续 24 小时之后，设备会删除**用户**选项卡中的 CAC 身份验证用户。每次后续登录后系统会重新添加用户，但必须重新配置对其用户角色的任何手动更改。

⚠

注意 使用 LDAP 配置 CAC 身份验证时，请确保在向用户分配默认访问角色时遵循最小权限原则。当用户首次使用其 CAC 凭证登录系统时，将为其账户分配此默认访问角色。

如果在分配默认访问角色时不遵循最小权限原则，则在后续登录时可能会为用户分配意外的权限级别。这可能会导致用户拥有超出其所需访问角色的权限。

如果使用默认访问角色登录的用户需要临时提升其权限，则具有管理权限的用户可以通过为其分配具有更高权限的角色来临时为其提供所需的更高级别的访问权限。此权限将在 24 小时不活动后撤销，并且用户将返回其默认访问角色。

如果用户需要将永久访问角色重新分配到更高权限级别（例如系统管理员），请使用 **组控制访问角色** 方法为用户提供管理员访问权限。此方法可确保提供的访问角色持续超过 24 小时，并且用户将根据组分配具有正确的权限级别。有关配置组控制访问角色的详细信息，请参阅为管理中心步骤 15部分。

开始之前

您必须在浏览器中具有有效的用户证书（在这种情况下，即通过您的 CAC 传递至您的浏览器的证书），才能在 CAC 配置流程中启用用户证书。配置 CAC 身份验证和授权之后，网络上的用户必须在其浏览会话的持续时间内维持 CAC 连接。如果在会话期间移除或替换 CAC，则网络浏览器会终止该会话，并且系统会注销网络界面。

过程

步骤 1 按照您的组织的指示插入 CAC。

步骤 2 将浏览器定向到 **https://***ipaddress_or_hostname/*，其中 *ipaddress* 或 *hostname* 对应您的设备。

步骤 3 如有提示，请输入与步骤 1 中插入的 CAC 关联的 PIN。

步骤 4 如有提示，请从下拉列表中选择相应的证书。

步骤 5 在“登录”(Login) 页面的**用户名 (Username)** 和**密码 (Password)** 字段中，以具备管理员权限的用户身份登录。您还**不能**使用 CAC 凭证登录。

步骤 6 依次选择**系统** > **用户** > **外部身份验证**。

步骤 7 遵循添加 管理中心的 LDAP 外部身份验证对象 ， 第 10 页中的程序，专门为 CAC 创建一个 LDAP 身份验证对象。必须配置以下内容：

- **CAC** 复选框。
- **LDAP 特定参数** > **显示高级选项** > **用户名模板**。
- **属性映射** > **UI 访问属性**。

步骤 8 点击**保存 (Save)**。

步骤 9 启用外部身份验证和 CAC 身份验证，如为管理中心上的用户启用外部身份验证 ， 第 22 页所述。

步骤 10 选择**系统**（⚙） > **配置**，然后点击 **HTTPS 证书**。

步骤 11 如有必要，请遵循导入 HTTPS 服务器证书中概括的过程导入 HTTPS 服务器证书。

您计划使用的 HTTPS 服务器证书和 CAC 用户证书必须由同一个证书颁发机构 (CA) 签发。

步骤 12 在 **HTTPS 客户端证书设置 (HTTPS Client Certificate Settings)** 下，选择**启用客户端证书 (Enable Client Certificates)**。有关详细信息，请参阅需要有效的 HTTPS 客户端证书。

步骤 13 根据 使用 CAC 凭证登录 Cisco Secure Firewall Management Center登录设备。

配置 SAML 单点登录

您可以将 管理中心 配置为使用单点登录，即中央身份提供程序 (IdP) 为登录 管理中心 的用户以及组织内的其他应用提供身份验证和授权的系统。配置为参与此类 SSO 安排的应用称为联合服务提供商应用。SSO 用户只需登录一次即可访问属于同一联盟的所有服务提供商应用。

关于 SAML 单点登录

为 SSO 配置的 管理中心 在登录页面上显示单点登录链接。配置为进行 SSO 访问的用户点击此链接，将被重定向到 IdP 进行身份验证和授权，而不是在 管理中心 登录页面上提供用户名和密码。IdP 成功通过身份验证后，SSO 用户将被重定向回 管理中心 Web 界面并登录。 管理中心 与 IdP 之间的所有通信都是通过浏览器作为中介来完成的；因此， 管理中心 不需要网络连接即可直接访问身份提供程序。

管理中心 支持使用符合用于身份验证和授权的安全断言标记语言 (SAML) 2.0 开放标准的任何 SSO 提供程序。

Note 管理中心无法签署 SAML 身份验证请求消息。因此，如果 IdP 要求服务提供商对身份验证请求进行签名，则管理中心上的 SSO 将失败。

管理中心 Web 界面为以下 SSO 提供程序提供配置选项：

- Okta
- OneLogin
- Azure
- 面向客户云解决方案的 PingID 的 PingOne
- 其他

Note Cisco Secure Sign On SSO 产品不会将 管理中心 识别为预先集成的服务提供商。

管理中心的 SSO 指南

将 管理中心 配置为 SSO 联合的成员时，请记住以下几点：

- 管理中心 一次只能支持一个 SSO 提供程序，例如，您不能将 管理中心 配置为同时使用 Okta 和 OneLogin 进行 SSO。
- 高可用性配置中的管理中心可以支持 SSO，但必须牢记以下注意事项：
  - 高可用性对的成员之间未同步 SSO 配置；您必须在 SSO 对的每个成员上单独配置 SSO。
  - 高可用性对中的两个 管理中心必须使用相同的 IdP 进行 SSO。您必须在 IdP 上为每个 管理中心 配置的 SSO 配置服务提供商应用。
  - 在均配置为支持 SSO 的 管理中心高可用性对中，在用户首次使用 SSO 访问辅助 管理中心之前，该用户必须首先使用 SSO 至少登录一次主 管理中心。
  - 为高可用性对中的 管理中心配置 SSO 时：
    - 如果在主 管理中心上配置 SSO，则不需要在辅助 管理中心上配置 SSO。
    - 如果在辅助 管理中心上配置 SSO，则还需要在主 管理中心 上配置 SSO。（这是因为 SSO 用户必须在登录辅助 管理中心 之前至少登录一次主 管理中心。）
- 在使用多租户的 管理中心 中，SSO 配置只能在全局域级别应用，并且适用于全局域和所有子域。
- 只有通过内部或通过 LDAP 或 RADIUS 进行身份验证的具有管理员角色的用户才能配置 SSO。
- 管理中心 不支持从 IdP 发起的 SSO。

- 管理中心 不支持使用 SSO 账户的 CAC 凭证登录。
- 请勿使用 CC 模式在部署中配置 SSO。
- SSO 活动记录在 管理中心 审核日志中，并在子系统字段中指定登录或注销。

Related Topics

高可用性
域
使用 CAC 凭证登录 Cisco Secure Firewall Management Center
安全认证合规性
审核记录

SSO 用户账户

身份提供程序可以直接支持用户和组配置，也可以从其他用户管理应用（例如 Active Directory、RADIUS 或 LDAP）导入用户和组。本文档重点介绍如何配置 管理中心 与 IdP 配合使用，以支持 SSO（假设已建立 IdP 用户和组）；要配置 IdP 以支持来自其他用户管理应用的用户和组，请参阅 IdP 供应商文档。

SSO 用户的大多数账户特征（包括用户名和密码）都是在 IdP 上建立的。在这些账户首次登录之前，这些账户不会显示在 管理中心 Web 接口用户页面上。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

可以从 管理中心 Web 接口的 **系统**（⚙）> **系统** > **编辑用户** 下配置 SSO 用户的以下账户特征：

- 实际名称
- 豁免浏览器会话超时

SSO 用户的用户角色映射

默认情况下，系统会为所有被授予 SSO 访问 管理中心 权限的用户分配安全分析师（只读）角色。您可以更改此默认值，也可以为具有用户角色映射的特定 SSO 用户或组覆盖此默认值。建立并成功测试 管理中心 SSO 配置后，您可以配置用户角色映射，以建立 SSO 用户在登录时分配的 管理中心 用户角色。

用户角色映射需要将 管理中心 上的配置设置与 SSO IdP 应用上的设置进行协调。可以将用户角色分配给 IdP 应用中定义的用户或组。用户可能是组的成员，也可能不是，并且用户或组定义可能会或可能不会从组织内的其他用户管理系统（例如 Active Directory）导入到 IdP。因此，要有效配置 管理中心 SSO 用户角色映射，您必须熟悉 SSO 联合的组织方式，以及如何在 SSO IdP 应用中分配用

户、组及其角色。本文档重点介绍如何配置 管理中心 与 IdP 配合使用的用户角色映射；要在 IdP 中创建用户或组，或者从用户管理应用将用户或组导入 IdP，请参阅 IdP 供应商文档。

在用户角色映射中，IdP 维护 管理中心 服务提供商应用的角色属性，并且每个用户或组都配置 管理中心 有角色属性的字符串或表达式（每个 IdP 的属性值要求不同）。在 管理中心 该角色属性的名称是 SSO 配置的一部分。 管理中心 SSO 配置还包含分配给 管理中心 用户角色列表的表达式列表。当用户使用 SSO 登录 管理中心 时， 管理中心 会将该用户（或该用户的组，具体取决于配置）的角色属性值与每个 管理中心 用户角色的表达式进行比较。 管理中心 为用户分配表达式与用户提供的属性值匹配的所有角色。

Note 您可以根据个人用户权限或组权限配置要映射的 管理中心 角色，但单个 管理中心 应用不能同时支持组和个人用户的角色映射。

在 管理中心启用单点登录

Before you begin

- 在 SAML SSO 管理应用中，为 管理中心 配置服务提供商应用，并将用户或组分配给服务提供商应用：
  - 要为 Okta 配置 管理中心 服务提供商应用，请参阅为 Okta 配置管理中心服务提供商应用, on page 29。
  - 要为 OneLogin 配置管理中心服务提供商应用，请参阅为 OneLogin 配置管理中心服务提供商应用, on page 40。
  - 要为 Azure 配置管理中心服务提供商应用，请参阅为 Azure 配置管理中心服务提供商应用, on page 52。
  - 要为 PingID 的 PingOne 客户云解决方案配置 管理中心 服务提供商应用，请参阅为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 64。
  - 要为任何符合 SAML 2.0 的 SSO 提供程序配置 管理中心 服务提供程序应用，请参阅为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用, on page 68。

Procedure

步骤 1 选择**系统**（⚙）> **用户** > **单点登录**。

步骤 2 点击 **单点登录 (SSO) 配置** 滑块以启用 SSO。

步骤 3 点击 **配置 SSO (Configure SSO)** 按钮。

步骤 4 在 **选择防火墙管理中心 SAML 提供程序** 对话框中，点击所选 SSO IdP 的单选按钮，然后点击 **下一步**。

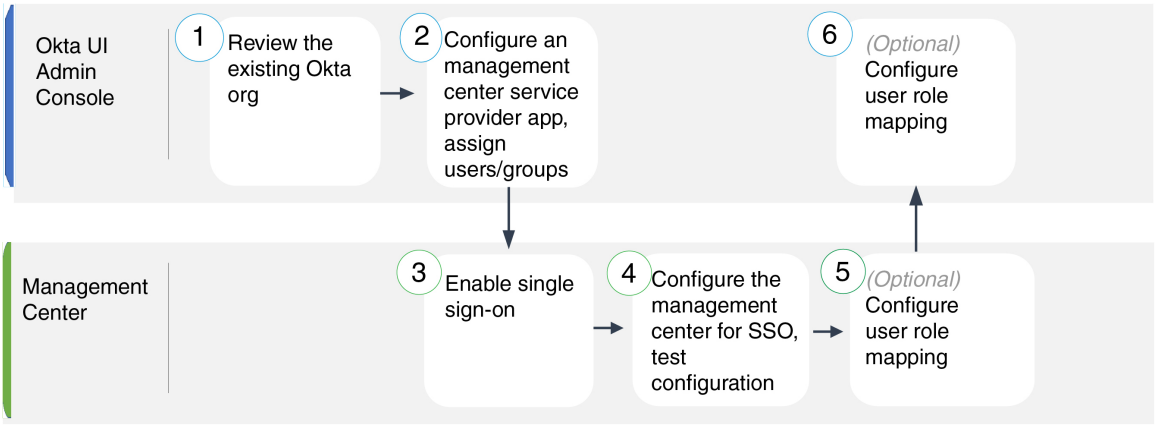
What to do next

继续执行适合您选择的 SSO 提供商的说明：

- 为 Okta SSO 配置管理中心；请参阅为 Okta SSO 配置管理中心 , on page 31。
- 使用 PingID 的 PingOne 客户云解决方案为 SSO 配置管理中心；请参阅为客户使用 PingID PingOne 为 SSO 配置管理中心 , on page 66。
- 为 Azure SSO 配置管理中心；请参阅为 Azure SSO 配置管理中心 , on page 54。
- 为 OneLogin SSO 配置管理中心；请参阅为 OneLogin SSO 配置 管理中心 , on page 42。
- 使用任何符合 SAML 2.0 的提供程序为 SSO 配置管理中心；请参阅为使用任何 SAML 2.0 兼容 SSO 提供程序的 SSO 配置 管理中心 , on page 70。

通过 Okta 配置单点登录

请参阅以下任务以使用 Okta 配置 SSO：



1	Okta UI 管理控制台	查看 Okta 组织, on page 29
2	Okta UI 管理控制台	为 Okta 配置管理中心服务提供商应用, on page 29
3	管理中心	在 管理中心启用单点登录, on page 27
4	管理中心	为 Okta SSO 配置管理中心 , on page 31
5	管理中心	在管理中心上为 Okta 配置用户角色映射, on page 32
6	Okta UI 管理控制台	在 Okta IdP 上配置用户角色映射, on page 32

查看 Okta 组织

在 Okta 中，包含用户可以使用同一 SSO 账户访问的所有联合设备和应用的实体称为 组织。在将 管理中心 添加到 Okta 组织之前，请熟悉其配置；思考以下问题：

- 有多少用户可以访问 管理中心？
- Okta 组织中的用户是否是组的成员？
- 用户和组定义是 Okta 本地的还是从用户管理应用（例如 Active Directory、RADIUS 或 LDAP）导入的？
- 您是否需要将更多用户或组添加到 Okta 组织以支持 管理中心上的 SSO？
- 您要分配哪种类型的用户角色？（如果您选择不分配用户角色， 管理中心 会自动为所有 SSO 用户分配可配置的默认用户角色。）
- 必须如何组织 Okta 组织内的用户和组，以支持所需的用户角色映射？

请记住，您可以根据个人用户权限或组权限配置要映射的 管理中心 角色，但单个 管理中心 应用不能同时支持组和个人用户的角色映射。

本文档假设您已经熟悉 Okta 经典 UI 管理控制台，并且拥有可以执行需要超级管理员权限的配置功能的账户。如果您需要更多信息，请参阅 Okta 的在线文档。

为 Okta 配置管理中心服务提供商应用

使用 Okta 经典 UI 管理控制台中的这些说明在 Okta 中创建 管理中心 服务提供商应用，并将用户或组分配给该应用。您应该熟悉 SAML SSO 概念和 Okta 管理控制台。本文档并未介绍建立功能齐全的 SSO 组织所需的所有 Okta 功能；例如，要创建用户和组，或从其他用户管理应用导入用户和组定义，请参阅 Okta 文档。

Note 如果您计划将用户组分配给 管理中心 应用，则不要将这些组中的用户作为个人进行分配。

Note 管理中心 不能支持使用多个 SSO 属性的角色映射；您必须选择用户角色映射或组角色映射，并配置单个属性以将用户角色信息从 OneLogin 传送到 管理中心。

Before you begin

- 熟悉 SSO 联合及其用户和组；请参阅 查看 Okta 组织, on page 29。
- 如有必要，在 Okta 组织中创建用户账户和/或组。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

- 确认目标 管理中心 的登录 URL (`https://ipaddress_or_hostname`)。

Note 如果可以使用多个 URL（例如，完全限定域名和 IP 地址）访问 管理中心 Web 界面，则 SSO 用户必须使用您在此任务中配置的登录 URL 一致地访问 管理中心 。

Procedure

步骤 1 在 Okta 经典 UI 管理控制台中，为 管理中心创建服务提供商应用。使用以下选项配置 管理中心 应用：

- 为 **平台**选择 `Web` 。
- 选择 `SAML 2.0` 作为 **登录方法**。
- 提供 **单点登录 URL**。

  这是浏览器代表 IdP 向其发送信息的 管理中心 URL。

  将字符串 `saml/acs` 附加到 管理中心 登录 URL。例如： `https://ExampleFMC/saml/acs`。
- 启用 **将此用于收件人 URL**”和“**目标 URL**”。
- 输入 **受众 URI**（**SP 实体 ID**）。

  这是服务提供商的全局唯一名称 (管理中心)，通常采用 URL 格式。

  将字符串 `/saml/metadata` 附加到 管理中心 登录 URL。例如：
  `https://ExampleFMC/saml/metadata`。
- 对于 **名称 ID 格式** ，选择 `未指定`。

步骤 2 （如果要向应用分配组，则可选。）将单个 Okta 用户分配给 管理中心 应用。（如果您计划将组分配给 管理中心 应用，请勿将属于这些组的成员的用户作为个人进行分配。）

步骤 3 （如果要将单个用户分配给应用，则可选。）将 Okta 组分配给 管理中心 应用。

步骤 4 （可选）为了简化 管理中心 上的 SSO 设置，您可以将 管理中心 服务提供商应用的 SAML XML 元数据文件从 Okta 下载到本地计算机。

What to do next

启用单点登录；请参阅 在 管理中心启用单点登录, on page 27。

为 Okta SSO 配置管理中心

在 管理中心 web 接口上使用这些说明。

准备工作

- 在 Okta 经典 UI 管理控制台中创建 管理中心 服务提供商应用；请参阅为 Okta 配置管理中心服务提供商应用, on page 29。
- 启用单点登录；请参阅 在 管理中心启用单点登录, on page 27。

Procedure

步骤 1 （此步骤直接从 在 管理中心启用单点登录, on page 27开始。）在 **配置 Okta 元数据** 对话框中，您有两个选择：

- 要手动输入 SSO 配置信息，请执行以下操作：
  a. 点击 **手动配置** 单选按钮。
  b. 从 Okta SSO 服务提供程序应用中输入以下值。（从 Okta 经典 UI 管理控制台检索这些值。）
     - **身份提供程序单点登录 (SSO) URL**
     - **身份提供程序颁发机构**
     - **X.509 证书**
- 如果已将 Okta 生成的 XML 元数据文件保存到本地计算机（ 为 Okta 配置管理中心服务提供商应用, on page 29中的步骤 4），则可以将文件上传到 管理中心：
  a. 点击 **上传文件** 单选按钮。
  b. 按照屏幕上的说明导航到本地计算机上的 XML 元数据文件并选择该文件。

步骤 2 点击**下一步**。

步骤 3 在 **验证元数据** 对话框中，查看配置参数，然后点击 **保存**。

步骤 4 点击 **测试配置**。如果系统显示错误消息，请查看 管理中心 的 SSO 配置以及 Okta 服务提供商应用配置，更正所有错误，然后重试。

步骤 5 当系统报告配置测试成功时，点击 **应用**。

What to do next

您可以选择为 SSO 用户配置用户角色映射；请参阅 在管理中心上为 Okta 配置用户角色映射, on page 32。如果您选择不配置角色映射，则默认情况下会为登录 管理中心 的所有 SSO 用户分配您在 在管理中心上为 Okta 配置用户角色映射, on page 32的步骤 4 中配置的用户角色。

在管理中心上为 Okta 配置用户角色映射

无论您选择哪种 SSO 提供商，在管理中心 Web 接口上为用户角色映射配置的字段都是相同的。但是，您配置的值必须考虑您使用的 SAML SSO 提供程序实施用户角色映射的方式。

Before you begin

- 查看 Okta 用户组映射信息；请参阅查看 Okta 组织, on page 29。
- 为管理中心配置 SSO 服务提供商应用；请参阅为 Okta 配置管理中心服务提供商应用, on page 29。
- 在管理中心上启用并配置单点登录；请参阅在 管理中心启用单点登录, on page 27和为 Okta SSO 配置管理中心 , on page 31。

Procedure

步骤 1 选择 **系统**（⚙）> **用户**。

步骤 2 点击 **单点登录 (SSO)** 选项卡。

步骤 3 展开 **高级配置**（**角色映射**）。

步骤 4 从**默认用户角色 (Default User Role)** 下拉列表中选择要分配用户的 管理中心 用户角色作为默认值。

步骤 5 输入 **组成员属性**。此字符串必须与在 Okta 管理中心 提供程序应用中为用户或组的用户角色映射配置的属性名称匹配。（请参阅 在 Okta IdP 上配置角色映射的用户属性, on page 33 中的第 1 步或 在 Okta IdP 上配置角色映射的组属性, on page 34 中的第 1 步。）

步骤 6 在要分配给 SSO 用户的每个 管理中心 用户角色旁边，输入正则表达式。（ 管理中心 使用 Golang 和 Perl 支持的 Google RE2 正则表达式标准的受限版本。） 管理中心 将这些值与 IdP 发送到 管理中心的用户角色映射属性值和 SSO 用户信息进行比较。 管理中心 授予用户找到匹配项的所有角色的并集。

What to do next

- 在服务提供商应用中配置用户角色映射；请参阅 在 Okta IdP 上配置用户角色映射, on page 32。

在 Okta IdP 上配置用户角色映射

您可以在 Okta 经典 UI 管理控制台中根据个人用户权限或组权限配置 SSO 用户角色映射。

- 要基于单个用户权限进行映射，请参阅 在 Okta IdP 上配置角色映射的用户属性, on page 33。

- 要基于组权限进行映射，请参阅 在 Okta IdP 上配置角色映射的组属性, on page 34。

当 SSO 用户登录到 管理中心时，Okta 会向 管理中心 提供在 Okta IdP 配置的用户或组角色属性值。管理中心 将该属性值与分配给 SSO 配置中每个 管理中心 用户角色的正则表达式进行比较，并向用户授予找到匹配项的所有角色。（如果未找到匹配项， 管理中心 将授予用户可配置的默认用户角色。）分配给每个 管理中心 用户角色的表达式必须符合 Golang 和 Perl 支持的 受限版本的 Google RE2 正则表达式标准。 管理中心 将从 Okta 接收的属性值视为使用相同标准的正则表达式，以便与管理中心 用户角色表达式进行比较。

Note 单个 管理中心 不能同时支持组和单个用户的角色映射；您必须为 管理中心 服务提供商应用选择一种映射方法，并一致地使用它。此外， 管理中心 可以仅使用 Okta 中配置的每个 管理中心 服务提供商应用的一个组属性语句来支持组角色映射。通常，对于具有许多用户的管理中心，基于组的滚动映射更有效。您应考虑在您的 Okta 组织中建立的用户和组定义。

在 Okta IdP 上配置角色映射的用户属性

使用 Okta 经典 UI 管理控制台中的这些说明将自定义角色映射属性添加到 Okta 默认用户配置文件。

Okta 服务提供商应用可以使用两种类型的用户配置文件之一：

- Okta 用户配置文件，可以使用任何自定义属性进行扩展。
- 应用用户配置文件，只能使用 Okta 通过查询第三方应用或目录（例如 Active Directory、LDAP 或 Radius）生成的预定义列表中的属性进行扩展。

您可以在 Okta 组织中使用任一类型的用户配置文件；有关如何配置它们的信息，请参阅 Okta 文档。无论使用哪种类型的用户配置文件，要支持与管理中心的用户角色映射，都必须在配置文件中配置自定义属性，以将每个用户的角色映射表达式传达给 管理中心。

本文档介绍如何使用 Okta 用户配置文件进行角色映射；使用应用配置文件进行映射需要熟悉您的组织中使用的第三方用户管理应用来设置自定义属性。有关详细信息，请参阅 Okta 文档。

Before you begin

- 在 Okta IdP 上配置 管理中心 服务提供商应用，如为 Okta 配置管理中心服务提供商应用, on page 29中所述。
- 配置 SSO 用户角色映射 管理中心 ，如 在管理中心上为 Okta 配置用户角色映射, on page 32中所述。

Procedure

步骤 1 向默认 Okta 用户配置文件添加新属性：

- 对于 **数据类型** ，请选择 字符串。

- 提供 Okta IdP 将发送到 管理中心的 **变量名称**，其中包含要匹配用户角色映射的表达式。此变量名称必须与您在 管理中心 SSO 配置中为 **组成员属性**输入的字符串匹配。（请参阅中 在管理中心上为 Okta 配置用户角色映射, on page 32的步骤 5。）

步骤 2 对于使用此配置文件分配给 管理中心 服务提供商应用的每个用户，请为您刚刚创建的用户角色属性分配一个值。

使用表达式表示 管理中心 将分配给用户的一个或多个角色。 管理中心 将此字符串与您在 在管理中心上为 Okta 配置用户角色映射, on page 32的步骤 6 中分配给每个 管理中心 用户角色的表达式进行比较。（为了与 管理中心 用户角色表达式进行比较， 管理中心 将从 Okta 接收的属性值视为符合 Golang 和 Perl 支持的受限版本的 Google RE2 正则表达式标准。）

在 Okta IdP 上配置角色映射的组属性

使用 Okta 经典 UI 管理控制台中的这些说明将自定义角色映射组属性添加到 管理中心 服务提供商应用。每个 Okta 管理中心 服务提供商应用仅使用一个组属性语句 管理中心 即可支持组角色映射。

Okta 服务提供商应用可以使用以下两种类型的组之一：

- Okta 组，可以使用任何自定义属性进行扩展。
- 应用组，只能使用 Okta 通过查询第三方应用或目录（例如 Active Directory、LDAP 或 Radius）以获取受支持属性而生成的预定义列表中的属性。

您可以在 Okta 组织中使用任一类型的组；有关如何配置它们的信息，请参阅 Okta 文档。无论使用哪种类型的组，要支持与管理中心的用户角色映射，都必须为该组配置自定义属性，以将其角色映射表达式传达给 管理中心。

本文档介绍如何使用Okta组进行角色映射；与应用组进行映射需要熟悉您的组织中使用的第三方用户管理应用来设置自定义属性。有关详细信息，请参阅 Okta 文档。

Before you begin

- 在 Okta IdP 上配置 管理中心 服务提供商应用；请参阅为 Okta 配置管理中心服务提供商应用, on page 29。
- 在 管理中心配置用户角色映射； 在管理中心上为 Okta 配置用户角色映射, on page 32。

Procedure

为 管理中心 服务提供商应用创建新的 SAML 组属性：

- 对于 **名称**，请使用您在 管理中心 SSO 配置中为 **组成员属性**输入的相同字符串。（请参阅中 在管理中心上为 Okta 配置用户角色映射, on page 32的步骤 5。）
- 对于 **过滤器**，请指定一个表达式来表示 管理中心 将分配给组成员的一个或多个角色。Okta 将此值与用户所属的组的名称进行比较，然后发送匹配的组名称至 管理中心 。 管理中心 依次将

这些组名称与您 在管理中心上为 Okta 配置用户角色映射, on page 32在步骤 6 中分配给每个 管理中心 用户角色的正则表达式进行比较。

Okta 用户角色映射示例

如以下示例所示，用于支持用户角色映射的管理中心SSO配置对于单个用户和组是相同的。区别在于 Okta 中 管理中心 服务提供商应用的设置。

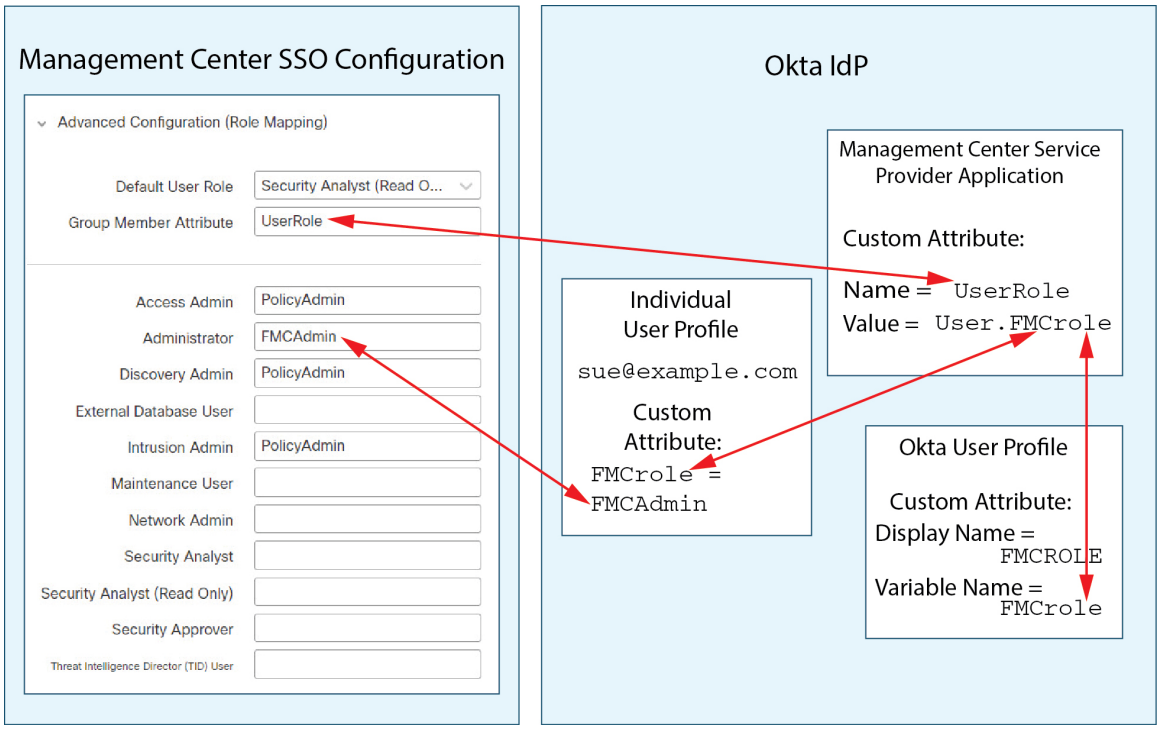
Note 您可以根据个人用户权限或组权限配置要映射的 管理中心 角色，但单个 管理中心 应用不能同时支持组和个人用户的角色映射。此外， 管理中心 可以仅使用 Okta 中配置的每个 管理中心 服务提供商应用的一个组属性语句来支持组角色映射。

个人用户账户的 Okta 角色映射示例

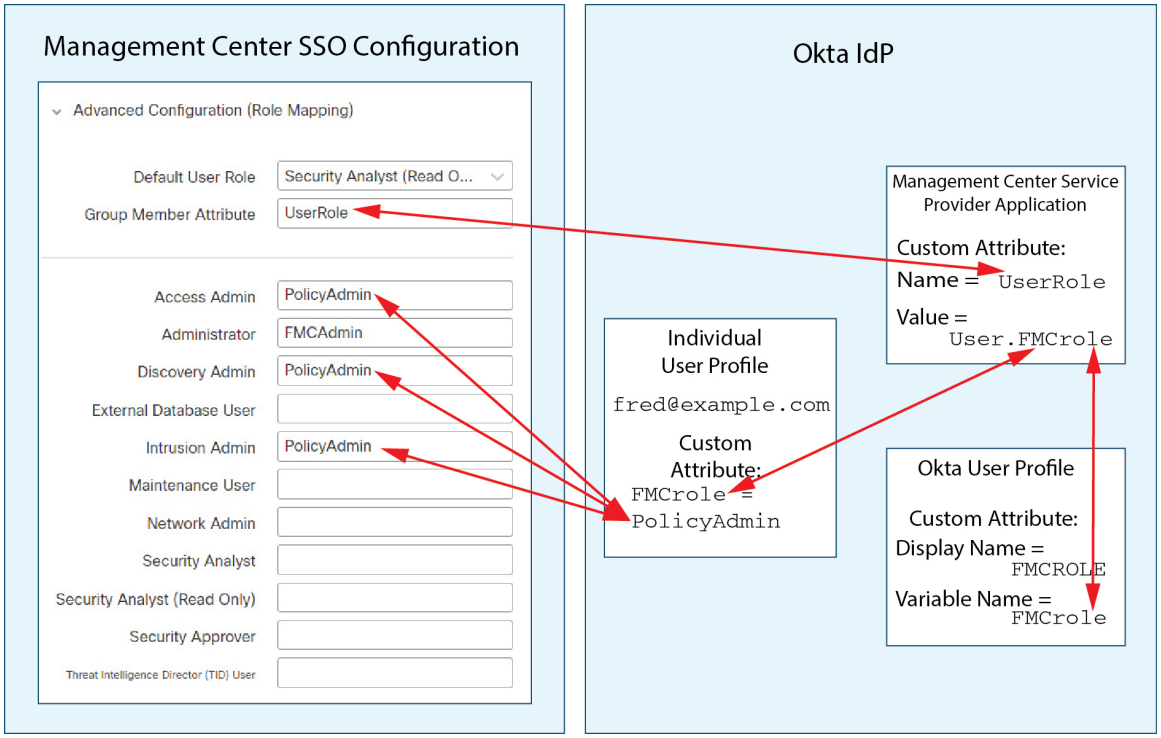
在单个用户的角色映射中，Okta管理中心服务应用具有一个自定义属性，其名称与管理中心上的组成员属性的名称匹配。（在本例中为 `UserRole`）。Okta 中的用户配置文件也有一个自定义属性（在本例中为名为 `FMCrole`的变量）。应用自定义属性 `UserRole` 的定义规定，当 Okta 将用户角色映射信息传递到 管理中心时，它将使用为相关用户分配的自定义属性值。

下图说明了 管理中心 和 Okta 配置中的相关字段和值在各个账户的用户角色映射中如何相互对应。每个图表在 管理中心 和 Okta UI 管理控制台上使用相同的 SSO 配置，但在 Okta UI 管理控制台上为每个用户分配的配置不同，以在 管理中心上为每个用户分配不同的角色。

- 在此图中，sue@example.com 使用 `FMCrole` 值 `FMCAdmin`，并且 管理中心 为她分配管理员角色。



- 在此图中，fred@example.com 使用 `FMCrole` 值 `PolicyAdmin`，并且 管理中心 分配给他角色访问管理员、发现管理员和入侵管理员。



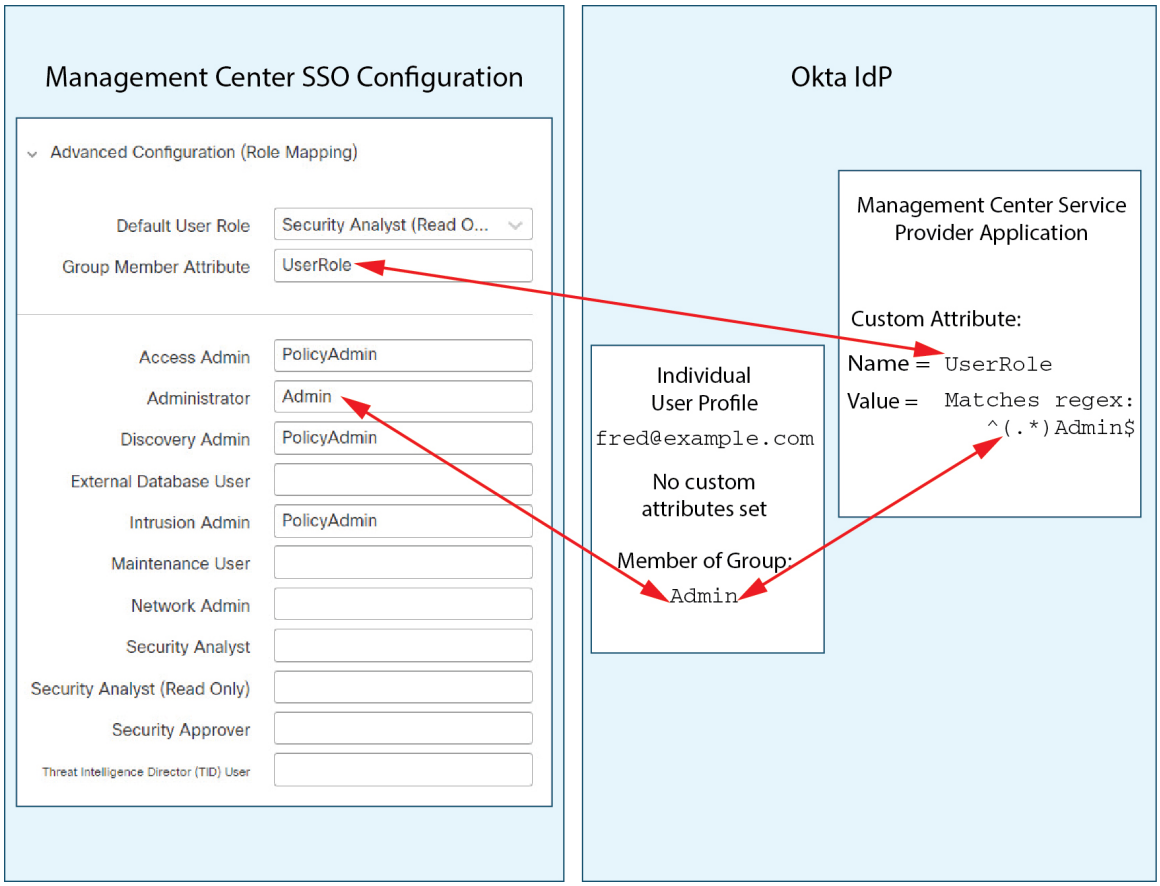
- 出于以下原因之一，为此 管理中心 分配到Okta服务应用的其他用户会被分配默认用户角色“安全分析师（只读）”：
  - 他们没有为 Okta 用户配置文件中的 `FMCole` 变量分配值。
  - 分配给其 Okta 用户配置文件中的 `FMCrole` 变量的值与为 SSO 配置 管理中心中的用户角色配置的任何表达式都不匹配。

组的 Okta 角色映射示例

在组的角色映射中，Okta服务应用具有一个自定义组属性，其名称与上的组成员属性的名称匹配（在本例中为 UserRole）。管理中心管理中心当 Okta 处理 SSO 登录请求时，它会将用户的组成员身份与分配给服务应用组属性的表达式（在本例中为^(.*)Admin$）进行比较。管理中心管理中心Okta将与组属性匹配的用户组成员身份发送给 管理中心 。 管理中心 将其接收的组名称与为每个用户角色配置的正则表达式进行比较，并相应地分配用户角色。

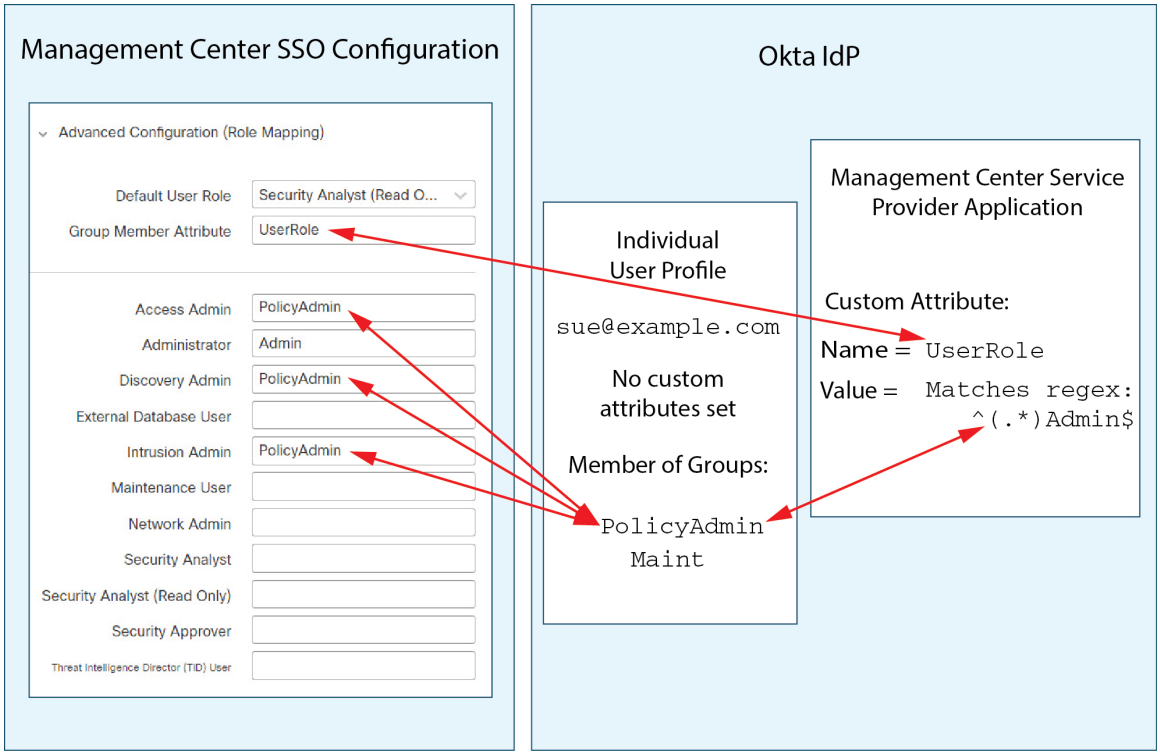
下图说明了 管理中心 和 Okta 配置中的相关字段和值在组的用户角色映射中如何相互对应。每个图表在 管理中心 和 Okta UI 管理控制台上使用相同的 SSO 配置，但在 Okta UI 管理控制台上为每个用户分配的配置不同，以在 管理中心上为每个用户分配不同的角色。

- 在此图中，fred@example.com 是 Okta IdP 组 `管理员` 的成员，与表达 `^(.*)Admin$`匹配。Okta 向管理中心 Fred 的 `管理员` 组成员发送邮件，并且 管理中心 为他分配管理员角色。

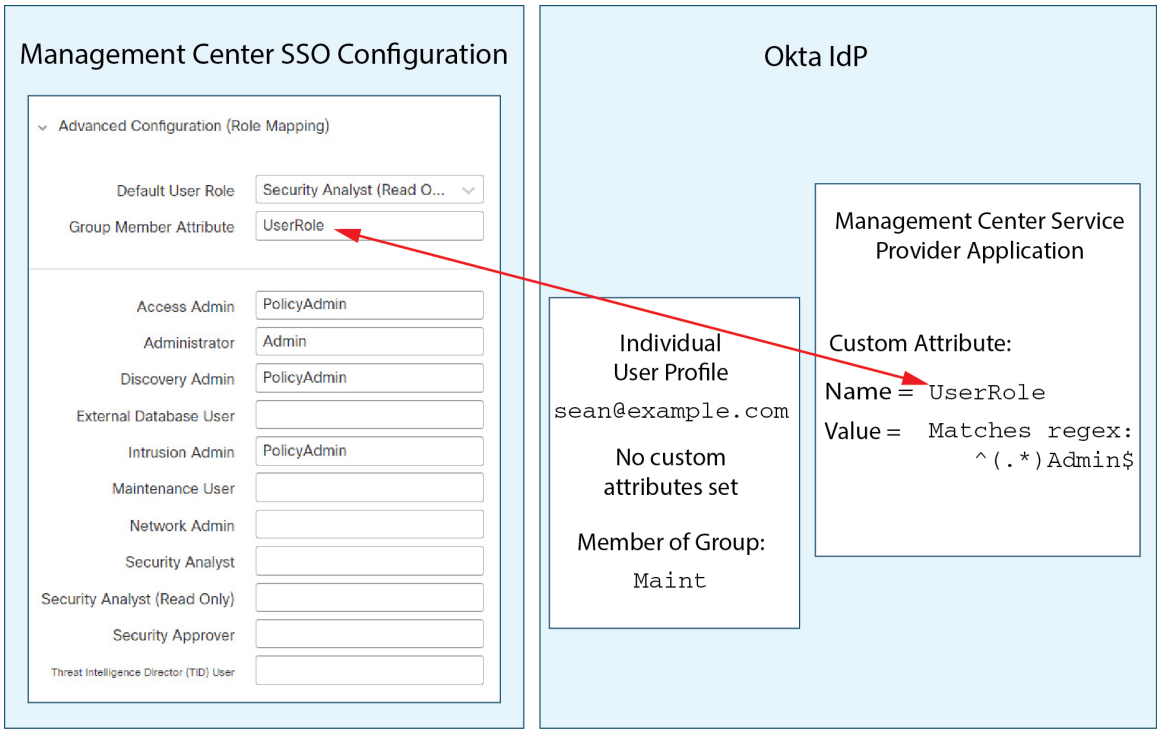


- 在此图中，sue@example.com 是 Okta IdP 组 `PolicyAdmin`的成员，它与表达式`^(.*)Admin$`匹配。Okta 发送 管理中心 Sue 的 `PolicyAdmin` 组成员身份，并且 管理中心 为她分配访问管理员、发现管理员和入侵管理员角色。

  Sue 也是 Okta 组 `Maint` 的成员，但由于此组名称与分配给 Okta 管理中心 服务应用中的组成员身份属性的表达式不匹配，因此 Okta 不会向 管理中心发送有关 Sue 的 `Maint` 组成员身份的信息，并且她在`Maint` 组不参与 管理中心 分配给她的角色。



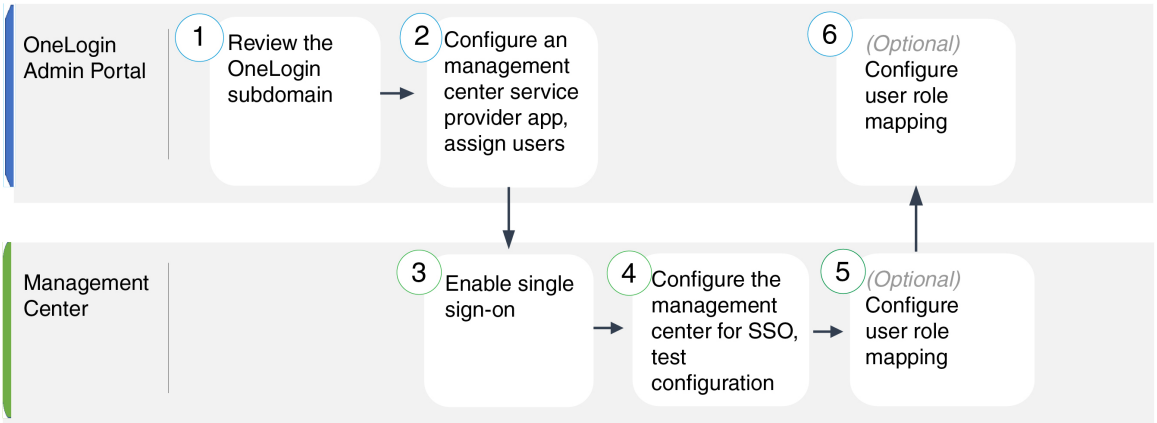
- 在此图中，sean@example.com 是 Okta IdP 组 `Maint` 的成员。此组名称与表达 `^(.*)Admin$` 不匹配，因此，当 sean@example.com 登录 管理中心时，Okta 不会将有关 Sean 的 `Maint` 组成员身份的信息发送到 管理中心 ，并且会为 Sean 分配默认用户角色（安全分析师（只读）），而不是“维护用户”角色。



这些图说明了在建立角色映射策略时提前规划的重要性。在本示例中，任何具有访问管理中心权限的 Okta 用户（仅为 `Maint` 组的成员）只能被分配默认用户角色。 管理中心 支持在其 Okta 服务应用配置中仅使用一个自定义组属性。分配给该属性的表达式以及建立与之匹配的组名称必须精心设计。通过在 管理中心 SSO 配置中的用户角色分配字符串中使用正则表达式，可以提高角色映射的灵活性。（分配给每个 管理中心 用户角色的表达式必须符合 Golang 和 Perl 支持的受限版本的 Google RE2 正则表达式标准。）

通过 OneLogin 配置单点登录

请参阅以下任务以使用 OneLogin 配置 SSO：



1	管理中心	查看 OneLogin 子域, on page 40
2	管理中心	为 OneLogin 配置管理中心服务提供商应用, on page 40
3	OneLogin 管理员门户	在 管理中心启用单点登录, on page 27
4	OneLogin 管理员门户	为 OneLogin SSO 配置 管理中心 , on page 42
5	OneLogin 管理员门户	在管理中心为 OneLogin 配置用户角色映射, on page 43
6	管理中心	在 OneLogin IdP 上配置用户角色映射, on page 44

查看 OneLogin 子域

在 OneLogin 中，包含用户可以使用同一 SSO 账户访问的所有联合设备和应用的实体称为子域。在将 管理中心 添加到 OneLogin 子域之前，请熟悉其配置；思考以下问题：

- 有多少用户可以访问 管理中心？
- OneLogin 子域中的用户是否是组的成员？
- 第三方目录（例如 Active Directory、Google Apps 或 LDAP）中的用户和组是否与 OneLogin 子域同步？
- 是否需要将更多用户或组添加到 OneLogin 子域以支持 管理中心上的 SSO？
- 您要分配哪种类型的 管理中心 用户角色？（如果您选择不分配用户角色， 管理中心 会自动为所有 SSO 用户分配可配置的默认用户角色。）
- 如何组织 OneLogin 子域中的用户和组，以支持所需的用户角色映射？

请记住，您可以将 管理中心 角色配置为基于单个用户或基于组进行映射，但单个 管理中心 应用不能同时支持组和单个用户的角色映射。

本文档假设您已经熟悉OneLogin管理员门户，并且拥有具有超级用户权限的账户。要配置用户角色映射，您还需要订用支持自定义用户字段的 OneLogin Unlimited 计划。如果您需要更多信息，请参阅在线提供的 OneLogin 文档。

为 OneLogin 配置管理中心服务提供商应用

使用 OneLogin 管理门户中的这些说明在 OneLogin 中创建 管理中心 服务提供商应用，并将用户或组分配给该应用。您应该熟悉 SAML SSO 概念和 OneLogin 管理员门户。本文档并未介绍建立功能齐全的 SSO 组织所需的所有 OneLogin 功能；例如，要创建用户和组，或从其他用户管理应用导入用户和组定义，请参阅 OneLogin 文档。

Note 如果您计划将用户组分配给 管理中心 应用，则不要将这些组中的用户作为个人进行分配。

Note 管理中心 不能支持使用多个 SSO 属性的角色映射；您必须选择用户角色映射或组角色映射，并配置单个属性以将用户角色信息从 OneLogin 传送到 管理中心。

Before you begin

- 熟悉 OneLogin 子域及其用户和组；请参阅 查看 OneLogin 子域, on page 40。
- 如有必要，在 OneLogin 子域中创建用户账户。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

- 确认目标 管理中心 的登录 URL (`https://ipaddress_or_hostname/`)。

Note 如果可以使用多个 URL 访问您的 管理中心 Web 接口。（例如，完全限定域名和 IP 地址），SSO 用户必须使用您在此任务中配置的登录 URL 一致地访问 管理中心 。

Procedure

步骤 1 使用 **SAML 测试连接器（高级）** 作为基础创建 管理中心 服务提供商应用。

步骤 2 使用以下设置配置应用：

- 对于 **受众（实体 ID）**，将字符串 `/saml/metadata` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/metadata`。
- 对于 **接收方**，将字符串 `/saml/acs` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/acs`。
- 对于 **ACS (消费者) URL 验证方**，输入 OneLogin 用于确认其使用的是正确 管理中心 URL 的表达式。您可以通过使用 ACS URL 并按如下方式修改来创建简单的验证程序：
  - 将 ^ 附加到 ACS URL 的开头。

- 在 ACS URL 末尾附加 `$`。
- 在每个 `/` 和 `?` 前面插入 `\`，在 ACS URL 中。

例如，对于 ACS URL `https://ExampleFMC/saml/acs`，适当的 URL 验证程序为 `^https:\/\/ExampleFMC\/saml\/acs$`。

- 对于 **ACS（使用者）URL**，请将字符串 `/saml/acs` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/acs`。
- 对于 **登录 URL**，请将字符串 `/saml/acs` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/acs`。
- 对于 **SAML 发起方**，请选择 服务提供商。

步骤 3 将 OneLogin 用户分配给 管理中心 服务提供商应用。

步骤 4 （可选）为了简化 管理中心 上的 SSO 设置，您可以将 管理中心 服务提供商应用的 SAML XML 元数据从 OneLogin 下载到本地计算机。

What to do next

启用单点登录；请参阅 在 管理中心启用单点登录, on page 27。

为 OneLogin SSO 配置 管理中心

在 管理中心 web 接口上使用这些说明。

Before you begin

- 在 OneLogin 管理门户上创建 管理中心 服务提供商应用；请参阅为 OneLogin 配置管理中心服务提供商应用, on page 40。
- 启用单点登录；请参阅 在 管理中心启用单点登录, on page 27。

Procedure

步骤 1 （此步骤直接从 在 管理中心启用单点登录, on page 27开始。）在 **配置 OneLogin 元数据** 对话框中，您有两个选择：

- 要手动输入 SSO 配置信息，请执行以下操作：
  - **a.** 点击 **手动配置** 单选按钮。
  - **b.** 从 OneLogin 服务提供应用输入以下 SSO 配置值：
    - **身份提供程序单点登录 URL**：从 OneLogin 输入 **SAML 2.0 终端 (HTTP)**。
    - **身份提供程序颁发者**：输入 OneLogin 中的 **颁发者 URL**。

- **X.509 证书**：输入 OneLogin 中的 **X.509 证书** 。

- 如果已将 OneLogin 生成的 XML 元数据文件保存到本地计算机（ 为 OneLogin 配置管理中心服务提供商应用, on page 40中的步骤 4），则可以将该文件上传到 管理中心：

  a. 点击 **上传文件** 单选按钮。

  b. 按照屏幕上的说明导航到本地计算机上的 XML 元数据文件并选择该文件。

步骤 2 点击**下一步**。

步骤 3 在 **验证元数据** 对话框中，查看配置参数，然后点击 **保存**。

步骤 4 点击 **测试配置**。如果系统显示错误消息，请查看 管理中心 的 SSO 配置以及 OneLogin 服务提供程序应用配置，更正所有错误，然后重试。

步骤 5 当系统报告配置测试成功时，点击 **应用**。

What to do next

您可以选择为 SSO 用户配置用户角色映射；请参阅 在管理中心为 OneLogin 配置用户角色映射, on page 43。如果您选择不配置角色映射，则默认情况下会为登录 管理中心 的所有 SSO 用户分配您在 在管理中心为 OneLogin 配置用户角色映射, on page 43的步骤 4 中配置的用户角色。

在管理中心为 OneLogin 配置用户角色映射

无论您选择哪种 SSO 提供商，在 管理中心 web 接口上为用户角色映射配置的字段都是相同的。但是，您配置的值必须考虑您使用的 SAML SSO 提供程序实施用户角色映射的方式。

Before you begin

- 查看 OneLogin 用户和组，请参阅 查看 OneLogin 子域, on page 40。
- 为 管理中心配置 SSO 服务提供商应用；请参阅 为 OneLogin 配置管理中心服务提供商应用, on page 40。
- 在 管理中心上启用并配置单点登录；请参阅 在 管理中心启用单点登录, on page 27和 为 OneLogin 配置管理中心服务提供商应用, on page 40。

Procedure

步骤 1 选择 **系统**（⚙） > **用户** > **单点登录系统** > **用户**。

步骤 2 展开 **高级配置**（**角色映射**）。

步骤 3 从**默认用户角色 (Default User Role)** 下拉列表中选择要分配给用户的 管理中心 用户角色作为默认值。

步骤 4 输入 **组成员属性**。此字符串必须与您在 OneLogin 中为 管理中心 服务提供商应用中的角色映射定义的自定义参数的字段名称匹配。（请参阅 在 OneLogin IdP 上配置单个用户的用户角色映射, on page 44 的步骤 1 或 在 OneLogin IdP 上配置组的用户角色映射, on page 45的步骤 1。）

步骤 5 在要分配给 SSO 用户的每个 管理中心 用户名旁边，输入正则表达式。 管理中心 将这些值与 IdP 发送到 管理中心 的用户角色映射属性和 SSO 用户信息进行比较。 管理中心 授予用户找到匹配项的所有角色的并集。

What to do next

在服务提供商应用中配置用户角色映射；请参阅 在 OneLogin IdP 上配置用户角色映射, on page 44。

在 OneLogin IdP 上配置用户角色映射

您可以在 Onelogin 管理员门户上根据个人权限或组权限配置 SSO 用户角色映射。

- 要基于单个用户权限进行映射，请参阅 在 OneLogin IdP 上配置单个用户的用户角色映射, on page 44。
- 要基于组权限进行映射，请参阅 在 OneLogin IdP 上配置组的用户角色映射, on page 45。

当 SSO 用户登录 管理中心时，OneLogin 会向 管理中心 提供从 OneLogin IdP 配置的自定义用户字段获取其值的用户或组角色属性值。 管理中心 将该属性值与分配给 SSO 配置中每个 管理中心 用户角色的正则表达式进行比较，并向用户授予找到匹配项的所有角色。（如果未找到匹配项， 管理中心 将授予用户可配置的默认用户角色。）分配给每个 管理中心 用户角色的表达式必须符合 Golang 和 Perl 支持的受限版本的 Google RE2 正则表达式标准。 管理中心 将从 OneLogin 接收的属性值视为使用相同标准的正则表达式，以便与 管理中心 用户角色表达式进行比较。

Note 单个 管理中心 不能同时支持组和单个用户的角色映射；您必须为 管理中心 服务提供商应用选择一种映射方法，并一致地使用它。 管理中心 只能使用 OneLogin 中配置的一个自定义用户字段来支持角色映射。通常，对于具有许多用户的 管理中心 ，基于组的角色映射更有效。您应该考虑在您的 OneLogin 子域中建立的用户和组定义。

在 OneLogin IdP 上配置单个用户的用户角色映射

使用 OneLogin 管理门户为 管理中心 服务提供商应用创建自定义参数和自定义用户字段。这些为 OneLogin 提供了在 SSO 登录过程中将用户角色信息传递到 管理中心 的方法。

Before you begin

- 查看 OneLogin 子域及其用户和组；请参阅 查看 OneLogin 子域, on page 40。
- 在 OneLogin 中创建和配置 管理中心 服务提供商应用；请参阅为 OneLogin 配置管理中心服务提供商应用, on page 40。
- 配置 SSO 用户角色映射 ， 如 在管理中心为 OneLogin 配置用户角色映射, on page 43中所述。

Procedure

步骤 1 为 管理中心 服务提供商应用创建自定义参数。

- 对于 **字段名称**，请使用您在 管理中心 SSO 配置中用于 **组成员属性** 的相同名称。（请参阅 在管理中心为 OneLogin 配置用户角色映射, on page 43中的步骤 4。）
- 对于 **值**，请提供助记符名称，例如 `FMCUserRole`。这必须与您将在此程序的步骤 2 中配置的客户用户字段的名称匹配。

步骤 2 创建自定义用户字段，以包含具有访问 管理中心权限的每个 OneLogin 用户的用户角色信息。

- 对于 **名称**字段，请提供助记符名称，例如 `FMCUserRole`。这必须与为此程序步骤 1 中所述的应用自定义参数提供的值匹配。
- 对于 **短名称**，请提供该字段的缩写备用名称。（这用于 OneLogin 编程接口。）

步骤 3 对于有权访问 管理中心 服务提供商应用的每个用户，请为此程序的步骤 2 中创建的自定义用户字段分配一个值。

当用户使用 SSO 登录 管理中心 时，您为该用户分配给此字段的值是 管理中心 与您在 SSO 配置中分配给 管理中心 用户角色的表达式进行比较的值。（请参阅中 在管理中心为 OneLogin 配置用户角色映射, on page 43的步骤 5。）

What to do next

- 通过使用 SSO 从各种账户登录 管理中心 并确认用户已按预期分配 管理中心 用户角色，测试您的角色映射方案。

在 OneLogin IdP 上配置组的用户角色映射

使用 OneLogin 管理门户为 管理中心 服务提供商应用创建自定义参数和自定义用户字段。将 OneLogin 用户分配到组。然后，在自定义用户字段和用户组之间创建一个或多个映射，以便 OneLogin 根据用户的组成员身份为自定义用户字段分配一个值。这些为 OneLogin 提供了在 SSO 登录过程中将基于组的用户角色信息传递到 管理中心 的方法。

OneLogin 服务提供程序应用可以使用以下两种组之一：

- OneLogin 的本地组。
- 从第三方应用（例如 Active Directory、Google Apps 或 LDAP）同步的组。

您可以使用任一类型的 管理中心 组进行组角色映射。本文档介绍使用 OneLogin 组进行角色映射；使用第三方应用组需要熟悉您的组织中使用的第三方用户管理应用。有关详细信息，请参阅 OneLogin 文档。

Before you begin

- 查看 OneLogin 子域及其用户和组；请参阅 查看 OneLogin 子域, on page 40。
- 在 OneLogin 中创建和配置 管理中心 服务提供商应用；请参阅为 OneLogin 配置管理中心服务提供商应用, on page 40。
- 配置 SSO 用户角色映射 ， 如 在管理中心为 OneLogin 配置用户角色映射, on page 43中所述。

Procedure

步骤 1 为 管理中心 服务提供商应用创建自定义参数。

- 对于 **字段名称**，请使用您在 管理中心 SSO 配置中用于 **组成员属性** 的相同名称。（请参阅 在管理中心为 OneLogin 配置用户角色映射, on page 43中的步骤 4。）
- 对于 **值**，请提供助记符名称，例如 `FMCUserRole`。这必须与您将在此程序的步骤 2 中配置的客户用户字段的名称匹配。

步骤 2 创建自定义用户字段，以包含具有访问 管理中心权限的每个 OneLogin 用户的用户角色信息。

- 对于 **名称**字段，请提供助记符名称，例如 `FMCUserRole`。这必须与为此程序步骤 1 中所述的应用自定义参数提供的值匹配。
- 对于 **短名称**，请提供该字段的缩写备用名称。（这用于 OneLogin 编程接口。）

步骤 3 创建一个或多个用户字段映射，以将基于组的值分配给您在此程序的步骤 2 中创建的自定义用户字段。创建任意数量的映射，以便为每个 OneLogin 用户组分配正确的 管理中心 用户角色。

- 为映射创建一个或多个 **条件** ，将用户 **组** 字段与组名称进行比较。
- 如果创建多个 **条件**，请选择用户的组是否必须匹配 任何 或 所有 条件才能进行映射。
- 为映射创建 **操作** ，以将值分配给您在此程序的步骤 2 中创建的自定义用户字段。提供字段 **名称**，以及 OneLogin 为满足指定 **条件** 的所有用户分配给此自定义用户字段的字符串。

  管理中心 将此字符串与您在 在管理中心为 OneLogin 配置用户角色映射, on page 43的步骤 5 中分配给每个 管理中心 用户角色的表达式进行比较。
- 完成更改后，请 **重新应用所有映射** 。

What to do next

- 通过使用 SSO 从各种账户登录 管理中心 并确认用户已按预期分配 管理中心 用户角色，测试您的角色映射方案。

OneLogin 用户角色映射示例

如以下示例所示，用于支持用户角色映射的管理中心SSO配置对于单个用户和组是相同的。不同之处在于 OneLogin 中 管理中心 服务提供商应用的设置。

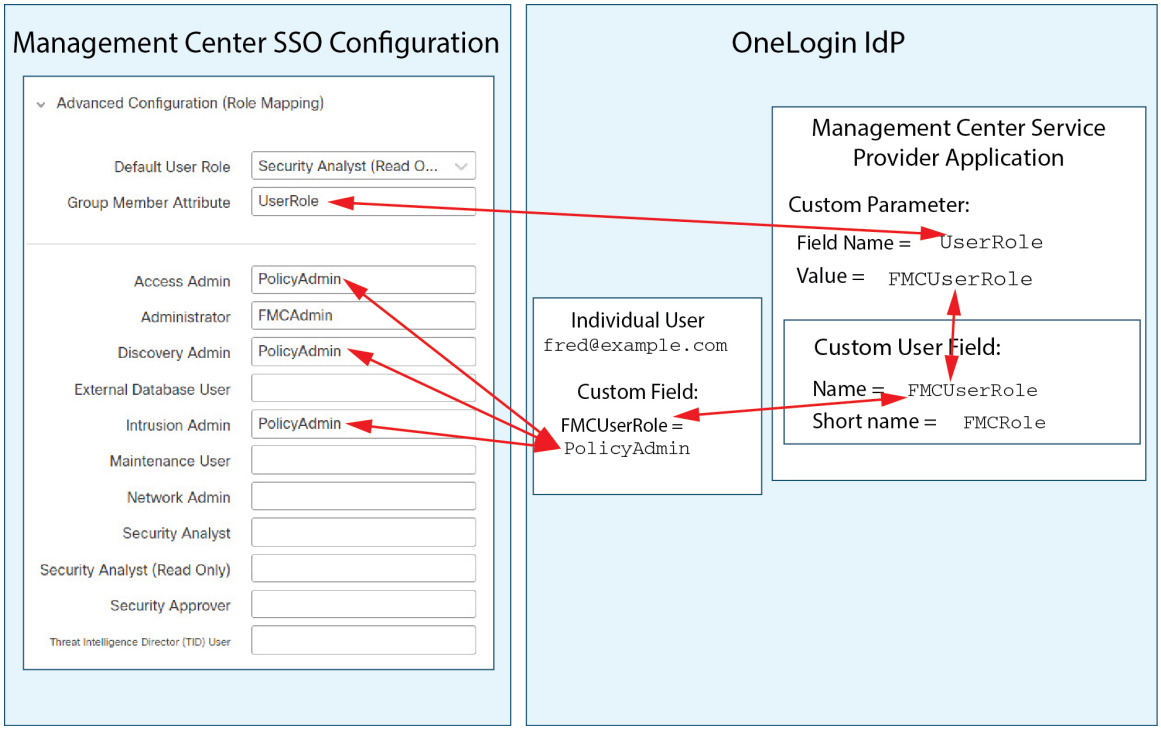
Note 单个 管理中心 不能同时支持组和单个用户的角色映射；您必须为 管理中心 服务提供商应用选择一种映射方法，并一致地使用它。 管理中心 只能使用 OneLogin 中配置的一个自定义用户字段来支持角色映射。通常，对于具有许多用户的 管理中心 ，基于组的角色映射更有效。您应该考虑在您的 OneLogin 子域中建立的用户和组定义。

单个用户账户的 OneLogin 角色映射示例

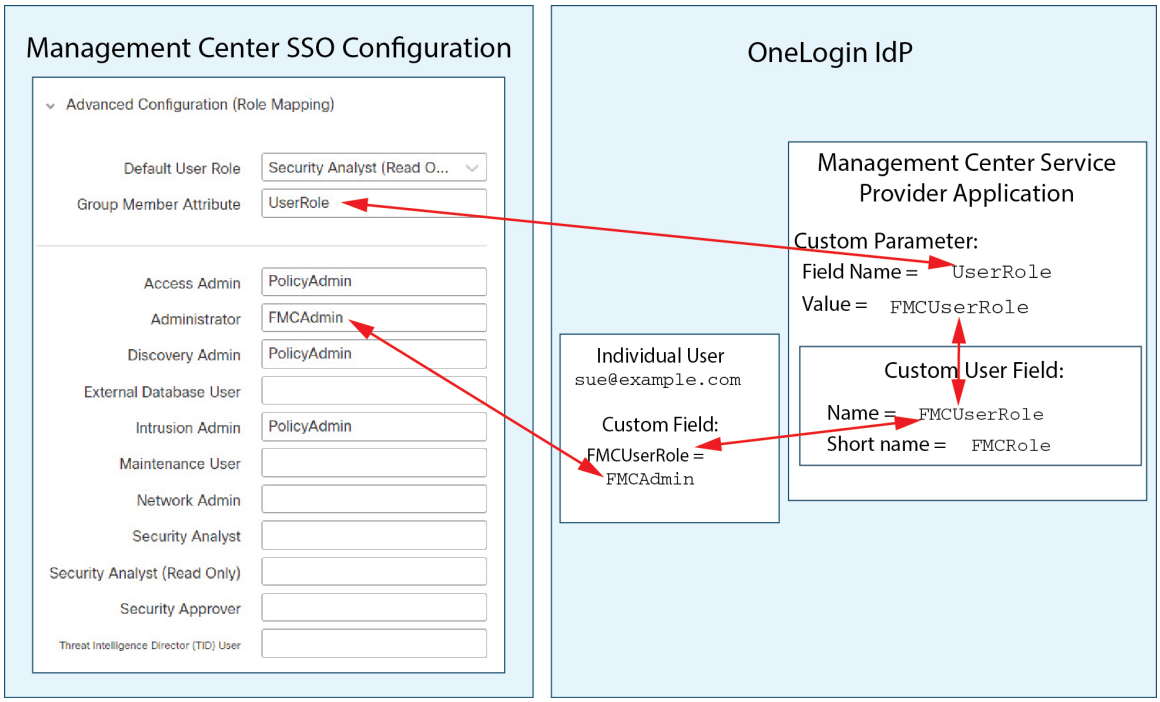
在个人用户的角色映射中，OneLogin 管理中心 服务应用具有一个自定义参数，其名称与 管理中心 上的“组成员”属性的名称匹配（在本例中为 `UserRole`）。OneLogin 还定义了一个自定义用户字段（在本例中为 `FMCUserRole`）。应用自定义参数 `UserRole` 的定义规定，当 OneLogin 将用户角色映射信息传递到 管理中心 时，它将使用相关用户的自定义用户字段 `FMCUserRole` 的值。

下图说明了 管理中心 和 OneLogin 配置中的相关字段和值在各个账户的用户角色映射中如何相互对应。每个图在 管理中心 和 OneLogin Admin 门户使用相同的 SSO 配置，但 OneLogin Admin 门户上每个用户的配置不同，在 管理中心 上为每个用户分配不同的角色。

- 在此图中，fred@example.com 使用 `FMCUserRole` 值 `PolicyAdmin` ，并且 管理中心 分配给他角色访问管理员、发现管理员和入侵管理员。



- 在此图中，sue@example.com 使用 `FMCUserRole` 值 `FMCAdmin`，并且 管理中心 为她分配管理员角色。



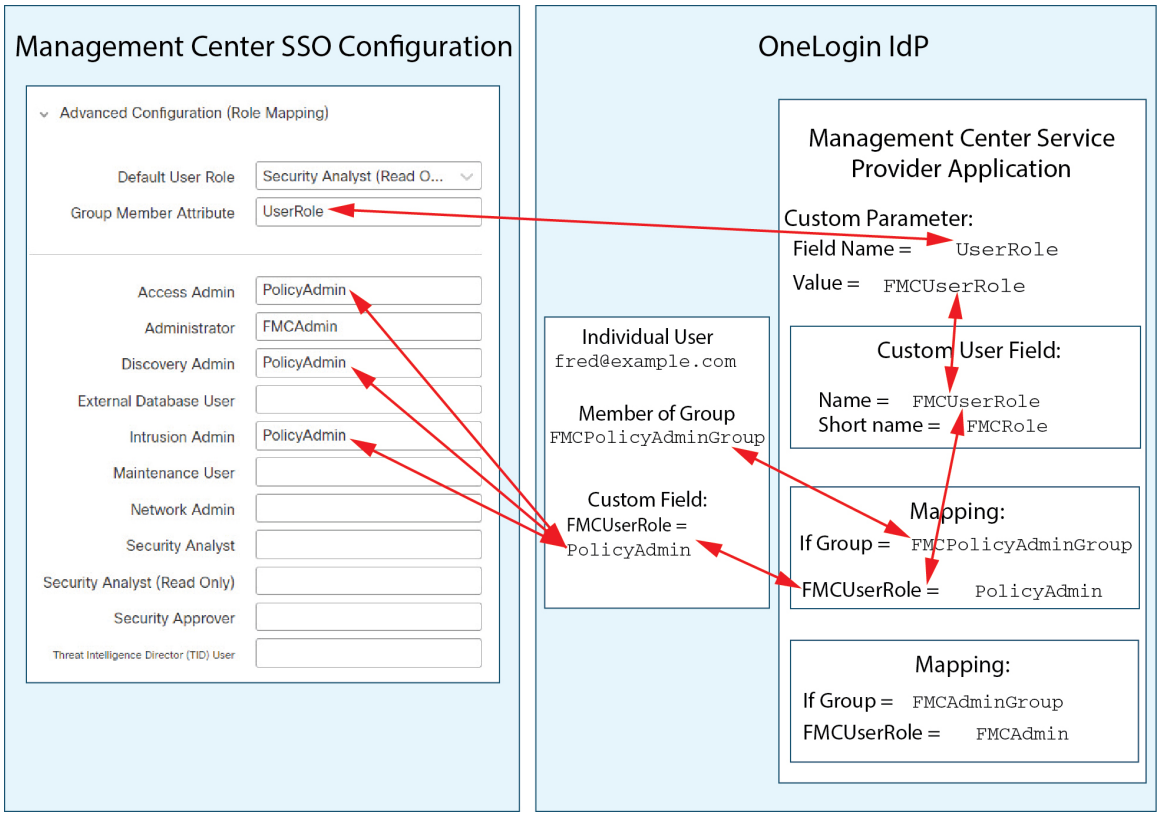
- 出于以下原因之一，为此 管理中心 分配到 OneLogin 服务应用的其他用户会被分配默认用户角色“安全分析师（只读）”：
  - 它们没有分配给 `FMCUserRole` 自定义用户字段的值。
  - 分配给 `FMCUserRole` 自定义用户字段的值与 SSO 配置 管理中心中为用户角色配置的任何表达式都不匹配。

组的 OneLogin 角色映射示例

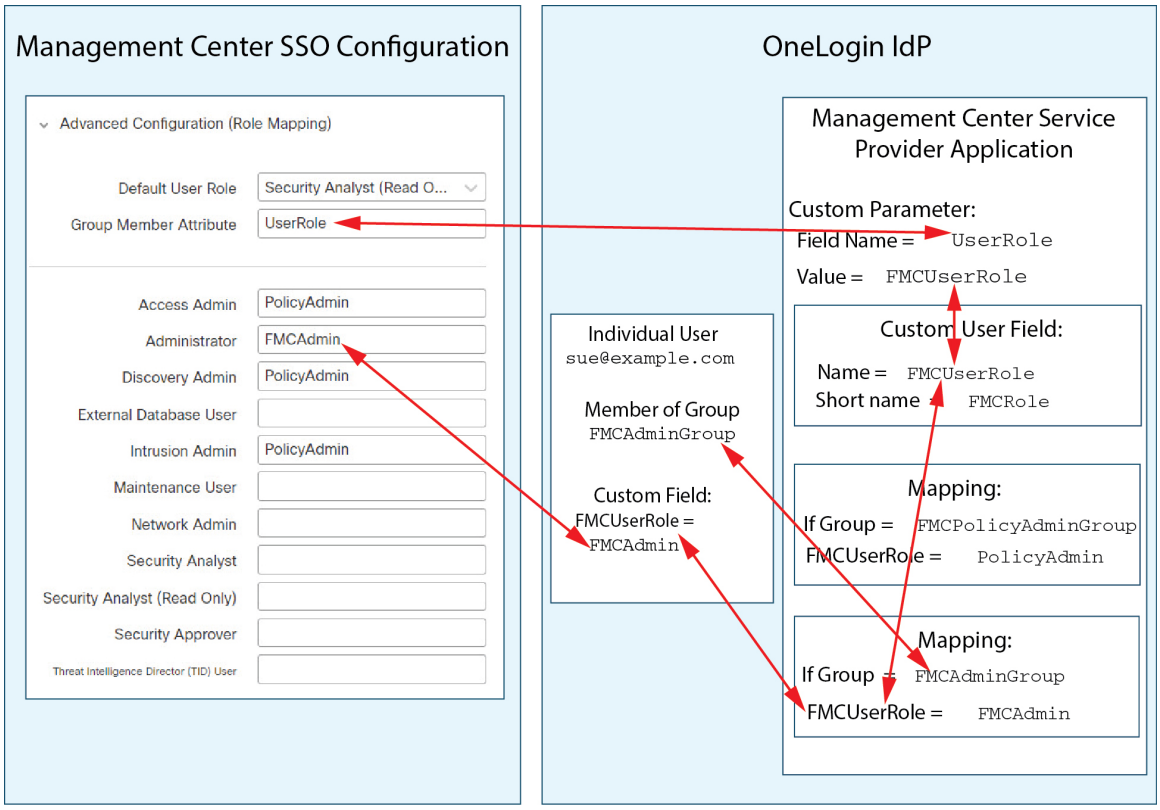
在组的角色映射中，OneLogin管理中心 服务应用具有一个自定义参数，其名称与管理中心 上的“组成员”属性的名称匹配（在本例中为 `UserRole`）。OneLogin还定义了一个自定义用户字段（在本例中为 `FMCUserRole`）。应用自定义参数 `UserRole` 的定义规定，当 OneLogin 将用户角色映射信息传递到 管理中心时，它将使用相关用户的自定义用户字段 `FMCUserRole` 的值。要支持用户组映射，必须在 OneLogin 中建立映射，以根据该用户的 OneLogin 组成员身份为每个用户的 `FMCUserRole` 字段分配值。

下图说明 管理中心 和 OneLogin 配置中的相关字段和值在组的用户角色映射中如何相互对应。每个图在 管理中心 和 OneLogin Admin 门户使用相同的 SSO 配置，但 OneLogin Admin 门户上每个用户的配置不同，在 管理中心上为每个用户分配不同的角色。

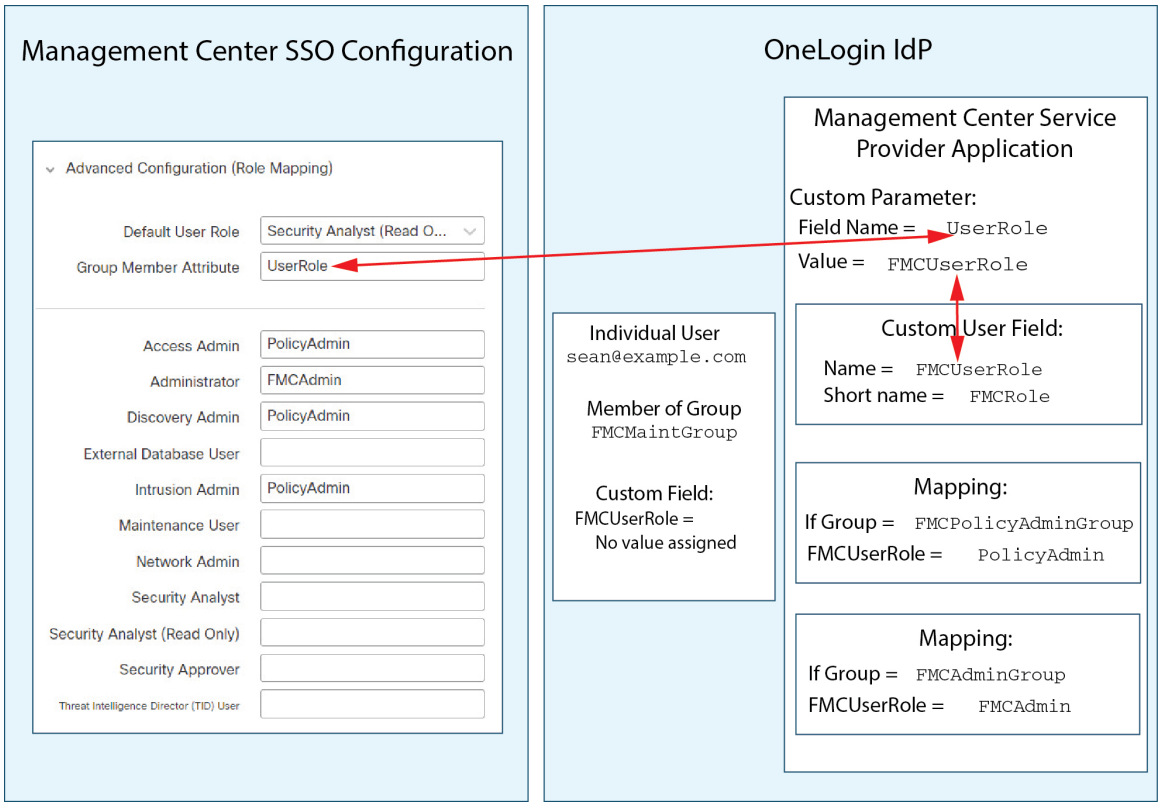
- 在此图中，fred@example.com 是 OneLogin IdP 组 `FMCPolicyAdminGroup`的成员。OneLogin 映射将值 `PolicyAdmin` 分配给 `FMCPolicyAdminGroup` 成员的自定义用户字段 `FMCUserRole` 。 管理中心为Fred 和 `FMCPolicyAdminGroup` 的其他成员分配角色访问管理员、发现管理员和入侵管理员。



- 在此图中，sue@example.com 是 OneLogin IdP 组 `FMCAdminGroup`的成员。OneLogin 映射将值 FMCAdmin 分配给 `FMCAdminGroup`成员的自定义用户字段 `FMCUserRole` 。 管理中心 为 Sue 和 `FMCAdminGroup` 的其他成员分配管理员角色。

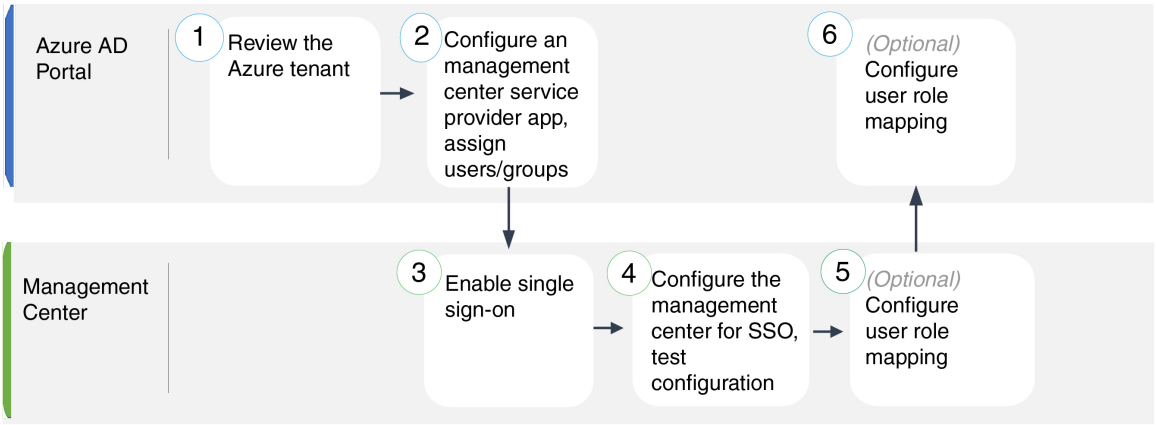


- 在此图中，sean@example.com 是 Idp 组 `FMCMaintGroup`的成员。没有与此组关联的 OneLogin 映射，因此 OneLogin 不会为 Sean 的自定义用户字段 `FMCUserRole` 分配值。 管理中心 为 Sean 分配默认用户角色（安全分析师（只读）），而不是“维护用户”角色。



通过 Azure AD 配置单点登录

请参阅以下任务以使用 Azure 配置 SSO：



1	Azure AD 门户	查看 Azure 租户, on page 52
2	Azure AD 门户	为 Azure 配置管理中心服务提供商应用, on page 52

3	管理中心	在 管理中心启用单点登录, on page 27
4	管理中心	为 Azure SSO 配置管理中心 , on page 54
5	管理中心	在管理中心上为 Azure 配置用户角色映射, on page 55
6	Azure AD 门户	在 Azure IdP 上配置用户角色映射, on page 56

查看 Azure 租户

Azure AD 是 Microsoft 基于多租户云的身份和访问管理服务。在 Azure 中，包含用户可以使用同一 SSO 账户访问的所有联合设备的实体称为 租户。在将 管理中心 添加到 Azure 租户之前，请熟悉其组织；思考以下问题：

- 有多少用户可以访问 管理中心？
- 用户是否属于组的 Azure 租户成员？
- 用户和组是否来自其他目录产品？
- 是否需要向 Azure 租户添加更多用户或组以支持 管理中心上的 SSO？
- 您要分配哪种类型的 管理中心 用户角色？（如果您选择不分配用户角色， 管理中心 会自动为所有 SSO 用户分配可配置的默认用户角色。）
- 必须如何组织 Azure 租户中的用户和组，以支持所需的用户角色映射？
- 请记住，您可以将 管理中心 角色配置为基于单个用户或基于组进行映射，但单个 管理中心 应用不能同时支持组和单个用户的角色映射。

本文档假定您已熟悉 Azure Active Directory 门户，并且拥有具有 Azure AD 租户应用管理员权限的账户。请记住， 管理中心 仅支持使用租户特定的单点登录和单点注销终端的 Azure SSO。您必须具有 Azure AD Premium P1 或更高版本的许可证和全局管理员权限；有关详细信息，请参阅 Azure 文档。

为 Azure 配置管理中心服务提供商应用

使用 Azure Active Directory 门户在 Azure Active Directory 租户中创建 管理中心 服务提供商应用并建立基本配置设置。

Note 如果您计划将用户组分配给 管理中心 应用，则不要将这些组中的用户作为个人进行分配。

Note 管理中心 不能支持使用多个 SSO 属性的角色映射；您必须选择用户角色映射或组角色映射，并配置单个属性以将用户角色信息从 OneLogin 传送到 管理中心。

Before you begin

- 熟悉 Azure 租户及其用户和组；请参阅 查看 Azure 租户, on page 52。
- 如有必要，在 Azure 租户中创建用户账号和/或组。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

- 确认目标 管理中心 的登录 URL (`https://ipaddress_or_hostname`)

Note 如果可以使用多个 URL（例如，完全限定域名和 IP 地址）访问 管理中心 Web 界面，则 SSO 用户必须使用您在此任务中配置的登录 URL 一致地访问 管理中心 。

Procedure

步骤 1 使用 Azure AD SAML 工具包作为基础创建 管理中心 服务提供商应用。

步骤 2 使用以下 **基本 SAML 配置设置**配置应用：

- 对于 **标识符（实体 ID）**，将字符串 `/saml/metadata` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/metadata`。
- 对于 **回复 URL（断言使用者服务 URL）**，将字符串 `/saml/acs` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/acs`。
- 对于 **登录 URL**，将字符串 `/saml/acs` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/acs`。

步骤 3 编辑应用的 **唯一用户标识符名称（名称 ID）**，以将登录 管理中心 的用户名强制为与用户账户关联的邮件地址：

- 对于 **源**，选择 属性。
- 对于 **源属性**：选择 `user.mail`。

步骤 4 生成证书以保护 管理中心上的 SSO。对证书使用以下选项：

- 为签名选项选择签名 SAML 响应和断言。
- 为签名算法选择 SHA-256。

步骤 5 将证书的 Base-64 版本下载到本地计算机；在 管理中心 Web 界面配置 Azure SSO 时需要用到它

步骤 6 在应用的基于 SAML 的登录信息中，请注意以下值：

- **登录 URL**
- **Azure AD 标识符**

在 管理中心 Web 界面配置 Azure SSO 时需要这些值。

步骤 7 （可选）为了简化 管理中心 的 SSO 设置，您可以将 管理中心 服务提供商应用的 SAML XML 元数据文件（在 Azure 门户中称为 **联合元数据 XML** ）下载到本地计算机。

步骤 8 将现有 Azure 用户和组分配给 管理中心 服务应用。

Note 如果您计划将用户组分配给 管理中心 应用，请勿将这些组中的用户作为个人进行分配。

Note 如果计划配置用户角色映射，则可以根据个人用户权限或组权限配置要映射的角色，但单个管理中心 应用不能同时支持组和个人用户的角色映射。

What to do next

启用单点登录；请参阅 在 管理中心启用单点登录, on page 27。

为 Azure SSO 配置管理中心

在 管理中心 web 接口上使用这些说明。

Before you begin

- 在 Azure AD 门户上创建 管理中心 服务提供商应用；请参阅为 Azure 配置管理中心服务提供商应用, on page 52。
- 启用单点登录；请参阅 在 管理中心启用单点登录, on page 27。

Procedure

步骤 1 （此步骤直接从 在 管理中心启用单点登录, on page 27开始。）在 **配置 Azure 元数据** 对话框中，您有两个选择：

- 要手动输入 SSO 配置信息，请执行以下操作：
  a. 点击 **手动配置** 单选按钮。
  b. 输入从 Azure SSO 服务提供程序应用检索的值：
  - 对于 **身份提供程序单点登录 URL** ，输入您在 为 Azure 配置管理中心服务提供商应用, on page 52步骤 6 中记下的 **登录 URL** 。

- 对于 **身份提供程序颁发者**，输入您在 为 Azure 配置管理中心服务提供商应用, on page 52 步骤 6 中记下的 **Azure AD 标识符**。
- 对于 **X.509 证书**，请使用您在 为 Azure 配置管理中心服务提供商应用, on page 52步骤 5 中从 Azure 下载的证书。（使用文本编辑器打开证书文件，复制内容并将其粘贴到 **X.509 证书** 字段中。）

- 如果已将 Azure 生成的 XML 元数据文件保存到本地计算机（ 为 Azure 配置管理中心服务提供商应用, on page 52的步骤 7），则可以将文件上传到 管理中心：

  a. 点击 **上传文件** 单选按钮。

  b. 按照屏幕上的说明导航到本地计算机上的 XML 元数据文件并选择该文件。

步骤 2 点击**下一步**。

步骤 3 在 **验证元数据** 对话框中，查看配置参数，然后点击 **保存**。

步骤 4 点击 **测试配置**。如果系统显示错误消息，请查看 管理中心 以及 Azure 服务提供商应用的 SSO 配置，更正所有错误，然后重试。

步骤 5 当系统报告配置测试成功时，点击 **应用**。

What to do next

您可以选择为 SSO 用户配置角色映射；请参阅 在管理中心上为 Azure 配置用户角色映射, on page 55。如果您选择不配置角色映射，则默认情况下会为登录 管理中心 的所有 SSO 用户分配您在 在管理中心上为 Azure 配置用户角色映射, on page 55的步骤 4 中配置的默认用户角色。

在管理中心上为 Azure 配置用户角色映射

无论您选择哪种 SSO 提供商，在 管理中心 web 接口上为用户角色映射配置的字段都是相同的。但是，您配置的值必须考虑您使用的 SAML SSO 提供程序实施用户角色映射的方式。

Before you begin

- 查看现有的 Azure 用户和组；请参阅 查看 Azure 租户, on page 52。
- 为 管理中心配置 SSO 服务提供商应用；请参阅 为 Azure 配置管理中心服务提供商应用, on page 52。
- 在 管理中心上启用并配置单点登录；请参阅 在 管理中心启用单点登录, on page 27和 为 Azure SSO 配置管理中心 , on page 54。

Procedure

步骤 1 选择 **系统** > **用户**。

步骤 2 点击 **单点登录** 选项卡。

步骤 3 展开 **高级配置（角色映射）**。

步骤 4 从**默认用户角色 (Default User Role)** 下拉列表中选择要分配用户的 管理中心 用户角色作为默认值。

步骤 5 输入 **组成员属性**。此字符串必须与您在 Azure 中为 管理中心 服务提供商应用创建的用户声明的名称相匹配；请参阅 在 Azure IdP 上配置个人用户的用户角色映射, on page 56 的步骤 1 或 在 Azure IdP 上配置组的用户角色映射, on page 57的步骤 1。

步骤 6 在要分配给 SSO 用户的每个 管理中心 用户角色旁边，输入正则表达式。（ 管理中心 使用 Golang 和 Perl 支持的 Google RE2 正则表达式标准的受限版本。） 管理中心 将这些值与 IdP 发送到 管理中心的用户角色映射属性值和 SSO 用户信息进行比较。 管理中心 授予用户找到匹配项的所有角色的并集。

What to do next

在服务提供商应用中配置用户角色映射；请参阅 在 Azure IdP 上配置用户角色映射, on page 56。

在 Azure IdP 上配置用户角色映射

您可以在 Azure AD 门户上根据个人用户权限或组权限配置 SSO 用户角色映射。

- 要根据个人用户权限进行映射，请参阅 在 Azure IdP 上配置个人用户的用户角色映射。
- 要基于组权限进行映射，请参阅 在 Azure IdP 上配置组的用户角色映射。

当 SSO 用户登录 管理中心时，Azure 会向 管理中心 提供用户或组角色属性值，该值从在 Azure AD 门户配置的应用角色获取。 管理中心 将该属性值与分配给 SSO 配置中每个 管理中心 用户角色的正则表达式进行比较，并向用户授予找到匹配项的所有角色。（如果未找到匹配项， 管理中心将授予用户可配置的默认用户角色。）分配给每个 管理中心 用户角色的表达式必须符合 Golang 和 Perl 支持的受限版本的 Google RE2 正则表达式标准。 管理中心 将从 Azure 接收的属性值视为使用相同标准的正则表达式，以便与 管理中心 用户角色表达式进行比较。

Note 单个 管理中心 不能同时支持组和单个用户的角色映射；您必须为 管理中心 服务提供商应用选择一种映射方法，并一致地使用它。 管理中心 只能使用 Azure 中配置的一个声明来支持角色映射。通常，对于具有许多用户的 管理中心，基于组的角色映射更有效。应考虑在整个 Azure 租户中建立的用户和组定义。

在 Azure IdP 上配置个人用户的用户角色映射

要在 Azure 中为 管理中心 服务应用的各个用户建立角色映射，请使用 Azure AD 门户向应用添加申领，将角色添加到应用的注册清单，并将角色分配给用户。

Before you begin

- 查看 Azure 租户；请参阅 查看 Azure 租户, on page 52。
- 在 Azure 中创建和配置 管理中心 服务提供商应用；请参阅为 Azure 配置管理中心服务提供商应用, on page 52。

- 配置 SSO 用户角色映射，如 在管理中心上为 Azure 配置用户角色映射, on page 55中所述。

Procedure

步骤 1 向 管理中心 服务应用的 SSO 配置添加具有以下特征的用户申领：

- **名称**：使用您在 管理中心 SSO 配置中为 **组成员属性** 输入的相同字符串。（请参阅中 在管理中心上为 Azure 配置用户角色映射, on page 55的步骤 5。）
- **名称标识符格式**：选择 持久性。
- **源**：选择 属性。
- **源属性**：选择 `user.assignedroles`。

步骤 2 编辑 管理中心 服务应用的清单（采用 JSON 格式）并添加应用角色以表示您希望分配给 SSO 用户的 管理中心 用户角色。最简单的方法是复制现有应用角色定义并更改以下属性：

- `displayName`：将显示在 AD Azure 门户中的角色的名称。
- `说明`：有关角色的简要说明。
- `Id`：一个字母数字字符串，在清单中的 ID 属性中必须是唯一的。
- `值`：表示一个或多个 管理中心 用户角色的字符串。（注意：Azure 不允许此字符串中包含空格。）

步骤 3 对于分配给管理中心服务应用的每个用户，请分配您已添加到该应用的清单中的一个应用角色。当用户使用 SSO 登录 管理中心 时，分配给该用户的应用角色是 Azure 在服务应用的申领中发送至 管理中心 的值。 管理中心 将申领与您在 SSO 配置中分配给 管理中心 用户角色的表达式进行比较（请参阅 在管理中心上为 Azure 配置用户角色映射, on page 55的第 6 步），并为用户分配匹配的所有 管理中心 用户角色。

What to do next

- 通过使用 SSO 从各种账户登录 管理中心 并确认用户已按预期分配 管理中心 用户角色，测试您的角色映射方案。

在 Azure IdP 上配置组的用户角色映射

要为 Azure 中的 管理中心 服务应用建立角色映射，请使用 Azure AD 门户向应用添加申领，向应用的注册清单添加角色，并将角色分配给组。

Before you begin

- 查看 Azure 租户；请参阅 查看 Azure 租户, on page 52。

- 在 Azure 中创建和配置 管理中心 服务提供商应用；请参阅为 Azure 配置管理中心服务提供商应用, on page 52。
- 配置 SSO 用户角色映射 ，如 在管理中心上为 Azure 配置用户角色映射, on page 55中所述。

Procedure

步骤 1 向 管理中心 服务应用的 SSO 配置添加具有以下特征的用户申领：

- **名称**：使用您在 管理中心 SSO 配置中为 **组成员属性** 输入的相同字符串。（请参阅中 在管理中心上为 Azure 配置用户角色映射, on page 55的步骤 5。）
- **名称标识符格式**：选择 持久性。
- **源**：选择 属性。
- **源属性**：选择 `user.assignedroles`。

步骤 2 编辑 管理中心 服务应用的清单（采用 JSON 格式）并添加应用角色以表示您希望分配给 SSO 用户的 管理中心 用户角色。最简单的方法是复制现有应用角色定义并更改以下属性：

- `displayName`：将在 Ad Azure 门户中显示的角色的名称。
- `说明`：有关角色的简要说明。
- `Id`：一个字母数字字符串，在清单中的 id 属性中必须是唯一的。
- `值`：表示一个或多个 管理中心 用户角色的字符串。（Azure 不允许此字符串中包含空格。）

步骤 3 对于分配给 管理中心 服务应用的每个组，请分配您已添加到该应用的清单中的一个应用角色。当用户使用 SSO 登录 管理中心 时，您分配给该用户的组的应用角色是 Azure 在服务应用的申领中发送至 管理中心 的值。 管理中心 将申领与您在 SSO 配置中分配给 管理中心 用户角色的表达式进行比较（请参阅 在管理中心上为 Azure 配置用户角色映射, on page 55的第 6 步），并为用户分配所有匹配的 管理中心 用户角色。

What to do next

通过使用 SSO 从各种账户登录 管理中心 并确认用户已按预期分配 管理中心 用户角色，测试您的角色映射方案。

Azure 用户角色映射示例

如以下示例所示，用于支持用户角色映射的管理中心SSO配置对于单个用户和组是相同的。区别在于 Azure 中 FMC 服务提供商应用的设置。

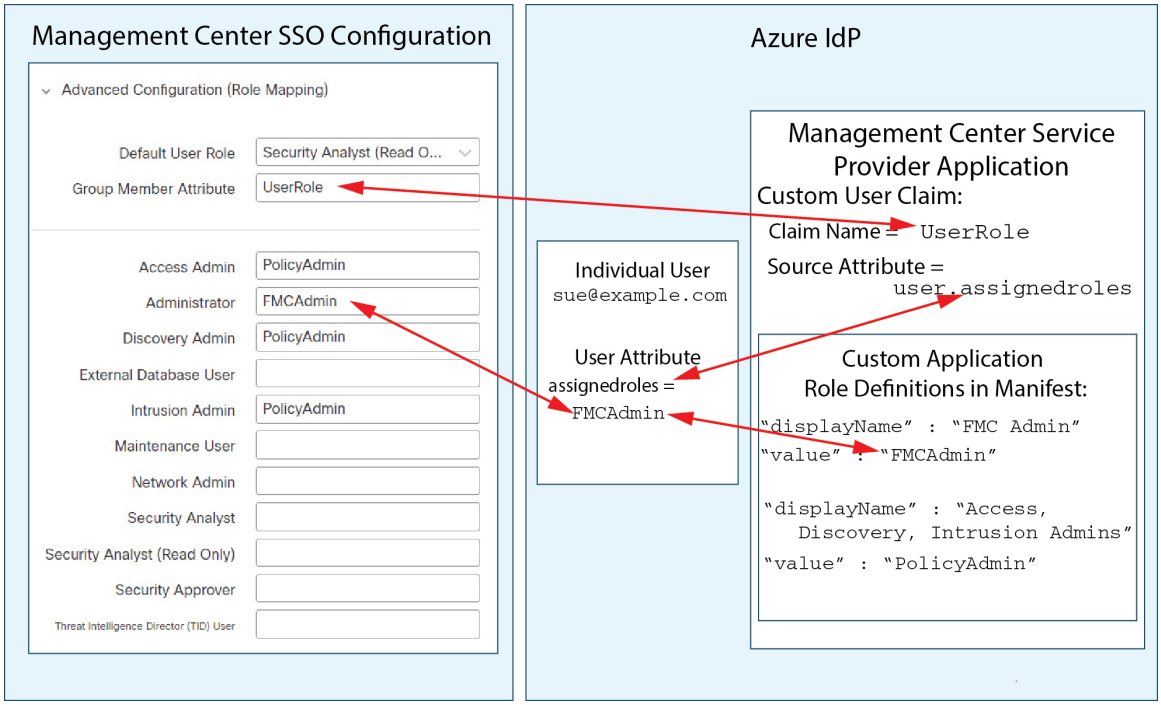
Note 您可以根据个人权限或组权限配置要映射的 管理中心 角色，但单个 FMC 应用不能同时支持组和个人用户的角色映射。 管理中心 只能使用 Azure 中配置的一个声明来支持角色映射。

个人用户账户的 Azure 角色映射示例

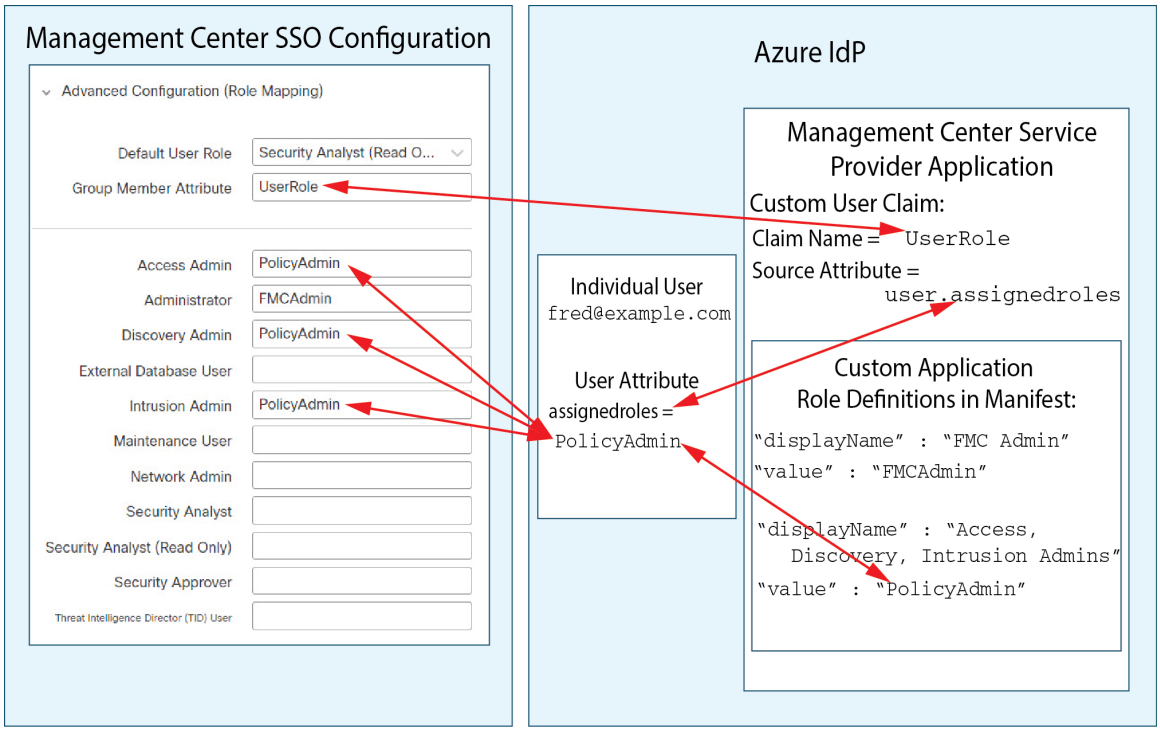
在单个用户的角色映射中，Azure 管理中心 服务应用在其清单中定义了自定义角色。（在本例中，为 FMCAdmin 和 PolicyAdmin。）这些角色可以分配给用户； Azure 将每个用户的角色分配存储在该用户的 assignedroles 属性中。该应用还定义了一个自定义用户声明，并且此声明配置为从使用 SSO 登录 FMC 的用户分配的用户角色获取其值。Azure 在 SSO 登录过程中将申领值传递给 管理中心，管理中心 将申领值与 管理中心 SSO 配置中分配给每个 管理中心 用户角色的字符串进行比较。

下图说明了 管理中心 和 Azure 配置中的相关字段和值在各个账户的用户角色映射中如何相互对应。每个图在 管理中心 和 Azure AD 门户上使用相同的 SSO 配置，但在 管理中心Azure AD 门户上为每个用户分配不同角色的配置有所不同。

- 在此图中，sue@example.com 使用 assignedroles 属性值 `FMCAdmin`，并且 管理中心 分配她的 管理中心 管理员角色。



- 在此图中，fred@example.com 使用 assignedroles 属性值 `PolicyAdmin`，并且 管理中心 分配给他角色访问管理员、发现管理员和入侵管理员。



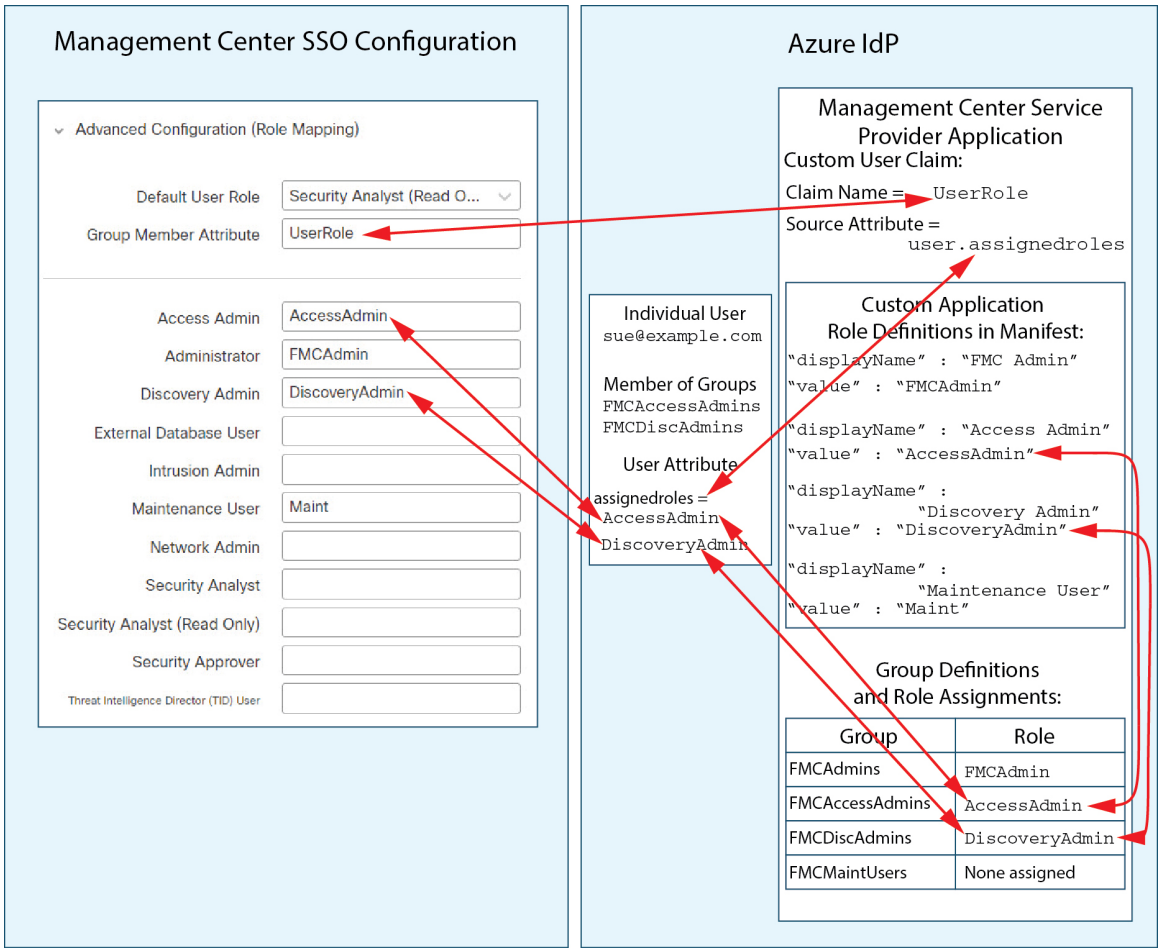
- 出于以下原因之一，为此 管理中心 分配到 Azure 服务应用的其他用户会被分配默认用户角色“安全分析师（只读）”：
  - 它们没有分配给其 assignedroles 属性的值。
  - 分配给其assignedroles 属性的值与 SSO 配置 管理中心中为用户角色配置的任何表达式都不匹配。

组的 Azure 角色映射示例

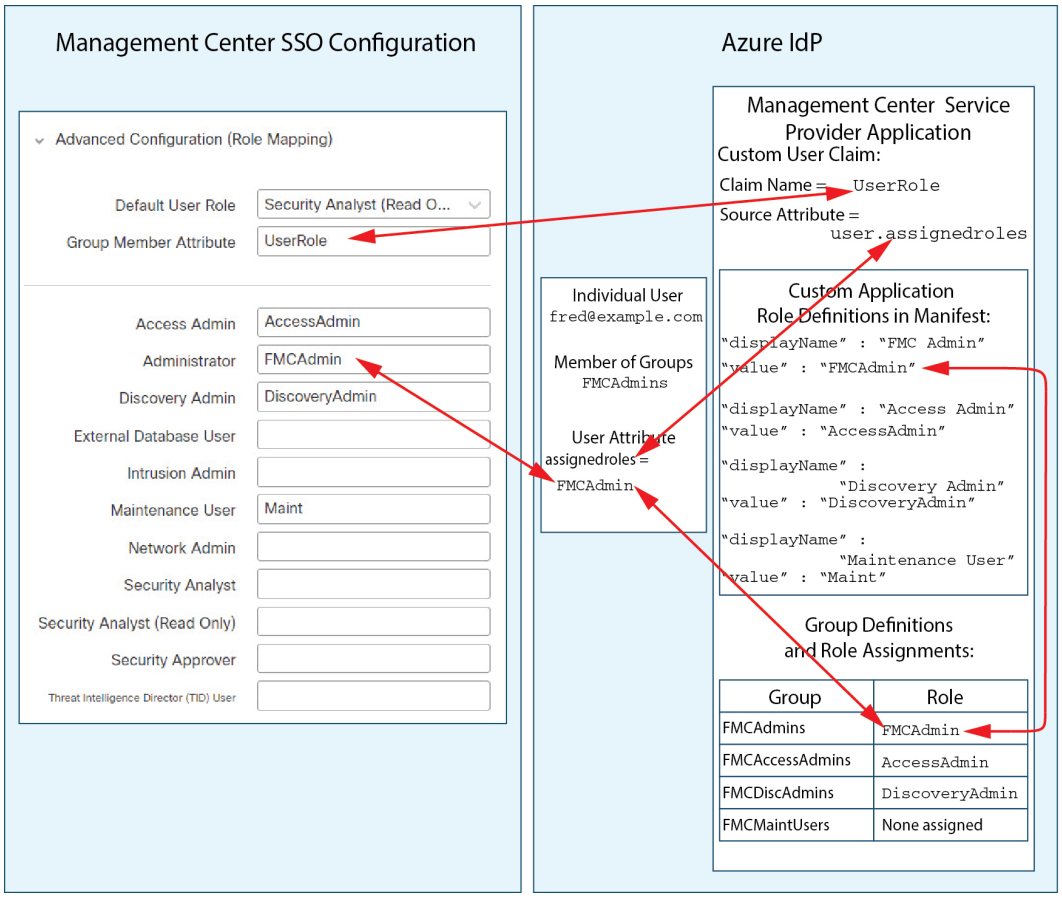
在组的角色映射中，Azure 管理中心 服务应用在其清单中定义了自定义角色。（在本例中，为 FMCAdmin、AccessAdmin、Discovery Admin 和 Maint。）这些角色可以分配给组； Azure 将每个组的角色分配传递给组成员的 assignedroles 属性。该应用还定义了一个自定义用户申领，此申领配置为从使用 SSO 登录 管理中心 的用户的已分配用户角色获取其值。Azure 在 SSO 登录过程中将申领值传递给 管理中心， 管理中心 将申领值与 管理中心 SSO 配置中分配给每个 管理中心 用户角色的字符串进行比较。

下图说明了 管理中心 和 Azure 配置中的相关字段和值在组的用户角色映射中如何相互对应。每个图在 管理中心 和 Azure AD 门户上使用相同的 SSO 配置，但在 管理中心Azure AD 门户上为每个用户分配不同角色的配置有所不同。

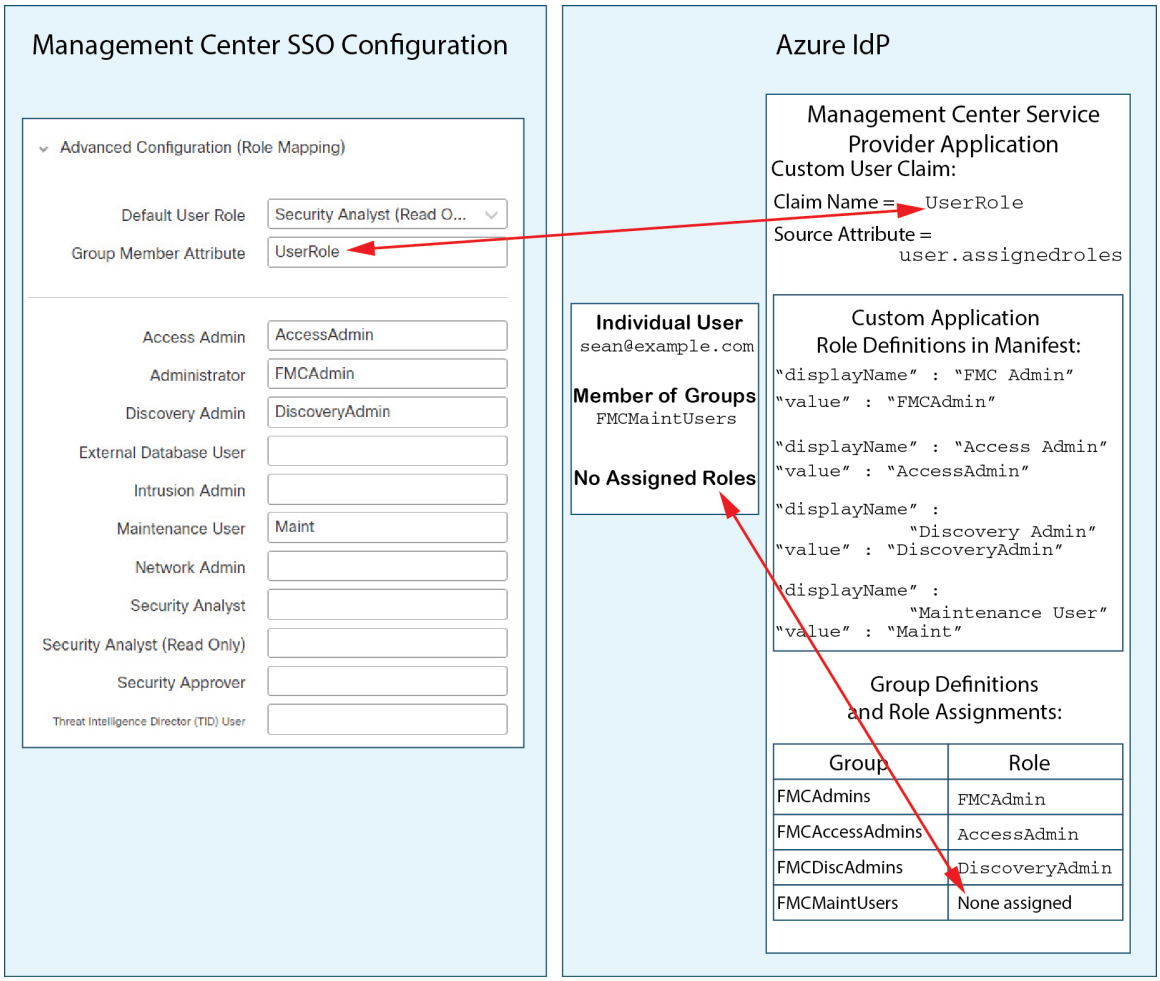
- 在此图中，sue@example.com 是组 `FMCAccessAdmins` 和 `FMCDiscoveryAdmins`的成员。她从这些组继承自定义角色 `AccessAdmin` 和 `DiscoveryAdmin`。当 Sue 使用 SSO 登录 管理中心 时， 管理中心 会为她分配访问管理员和发现管理员角色。



- 在此图中，fred@example.com 是 `FMCAdmins` 组的成员，从该组继承自定义角色 `FMCAdmin`。当Fred 使用 SSO 登录 管理中心 时， 管理中心 会为他分配管理员角色。

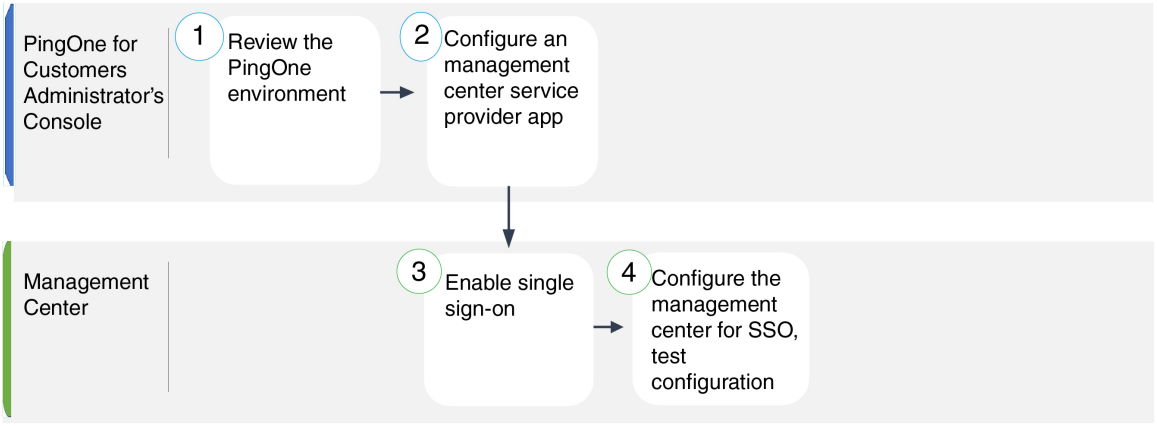


- 在此图中，sean@example.com 是 `FMCMaintUsers` 组的成员，但由于未在 Azure 管理中心 服务提供商应用中为 `FMCMaintUsers` 分配自定义角色，因此，Sean 未分配任何角色，当他使用 SSO 登录 管理中心 时， 管理中心 会为其分配默认角色“安全分析师（只读）”。



通过 PingID 配置单点登录

请参阅以下任务，以使用 PingID 的 PingOne 客户产品配置 SSO：



1	面向客户的 PingOne 管理员控制台	查看客户环境的 PingID PingOne, on page 64。
2	面向客户的 PingOne 管理员控制台	为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 64。
3	管理中心	在 管理中心启用单点登录, on page 27。
4	管理中心	为客户使用 PingID PingOne 为 SSO 配置管理中心 , on page 66。

查看客户环境的 PingID PingOne

面向客户的 PingOne 是 PingID 的云托管身份即服务 (IDaaS) 产品。在面向客户的 PingOne 中，包含用户可以使用同一 SSO 账户访问的所有联合设备的实体称为环境。在将 管理中心 添加到 PingOne 环境之前，请熟悉其组织；思考以下问题：

- 有多少用户可以访问 管理中心？
- 您是否需要添加更多用户来支持对 管理中心 的 SSO 访问？

本文档假定您已经熟悉 PingOne 客户管理员控制台，并且拥有具有组织管理员角色的账户。

为客户配置 PingID PingOne 的管理中心服务提供商应用

使用面向客户的 PingOne 管理员控制台在面向客户的 PingOne 环境中创建 管理中心 服务提供商应用，并建立基本配置设置。本文档并未介绍建立功能齐全的 SSO 环境所需的所有 PingOne 客户版功能；例如，要创建用户，请参阅 PingOne 客户文档。

Before you begin

- 熟悉面向客户的 PingOne 环境及其用户。
- 如有必要，创建更多用户。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

- 确认目标 管理中心 的登录 URL (`https://ipaddress_or_hostname`)

Note 如果可以使用多个 URL（例如，完全限定域名和 IP 地址）访问 管理中心 Web 界面，则 SSO 用户必须使用您在此任务中配置的登录 URL 一致地访问 管理中心 。

Procedure

步骤 1 使用 PingOne 客户管理员控制台使用以下设置在您的环境中创建应用：

- 选择 **Web App** 应用类型。
- 选择 **SAML** 连接类型。

步骤 2 使用 SAML 连接的以下设置配置应用：

- 对于 **ACS URL**，将字符串 `/sam/acs` 附加到登录 管理中心 URL。例如：`https://ExampleFMC/saml/acs`。
- 对于 **签名证书**，请选择签名断言和响应。
- 对于 **签名算法** ，请选择 RSA_SHA256。
- 对于 **实体 ID**，将字符串 `/saml/metadata` 附加到 管理中心 登录 URL。例如：`https://ExampleFMC/saml/metadata`。
- 对于 **SLO 绑定** ，选择 HTTP POST。
- 对于 **断言有效期** ，输入 300。

步骤 3 在应用的 SAML 连接信息中，请注意以下值：

- **单点登录服务**
- **颁发机构 ID**

在 管理中心 Web 界面上使用 PingID 的 PingOne 客户产品配置 SSO 时，需要这些值。

步骤 4 对于 **SAML 属性**，请为单个必需属性进行以下选择：

- **PINGONE 用户属性**： 邮箱地址
- **应用属性**： `saml_subject`

步骤 5 下载 X509 PEM (`.crt`) 格式的签名证书，并将其保存到本地计算机。

步骤 6 （可选）要简化 管理中心 的 SSO 设置，您可以将 管理中心 服务提供商应用的 SAML XML 元数据文件下载到本地计算机。

步骤 7 启用应用。

What to do next

启用单点登录；请参阅 在 管理中心启用单点登录, on page 27。

为客户使用 PingID PingOne 为 SSO 配置管理中心

在 管理中心 web 接口上使用这些说明。

Before you begin

- 在 PingOne 客户管理员控制台上创建 管理中心 服务提供商应用；请参阅为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 64。
- 启用单点登录；请参阅 在 管理中心启用单点登录, on page 27。

Procedure

步骤 1 （此步骤直接从 在 管理中心启用单点登录, on page 27开始。）在 **配置 PingID 元数据** 对话框中，您有两个选择：

- 要手动输入 SSO 配置信息，请执行以下操作：
  a. 点击 **手动配置** 单选按钮。
  b. 输入您从 PingOne 客户管理员控制台检索的值：
     - 对于 **身份提供程序单点登录 URL**，输入您在 为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 64步骤 3 中记下的 **单点登录服务** 。
     - 对于 **身份提供程序颁发者**，请输入您在 为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 64步骤 3 中记下的 **颁发者 ID** 。
     - 对于 **X.509 证书**，请使用您在 为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 64步骤 5 中从 PingOne for Customer 下载的证书。（使用文本编辑器打开证书文件，复制内容并将其粘贴到 **X.509 证书** 字段中。）
- 如果已将 PingOne for Customer 生成的 XML 元数据文件保存到本地计算机（为客户配置 PingID PingOne 的管理中心服务提供商应用, on page 64的步骤 6），则可以将文件上传到 管理中心：
  a. 点击 **上传文件** 单选按钮。
  b. 按照屏幕上的说明导航到本地计算机上的 XML 元数据文件并选择该文件。

步骤 2 点击**下一步**。

步骤 3 在 **验证元数据** 对话框中，查看配置参数，然后点击 **保存**。

步骤 4 展开 **高级配置**（**角色映射**）。

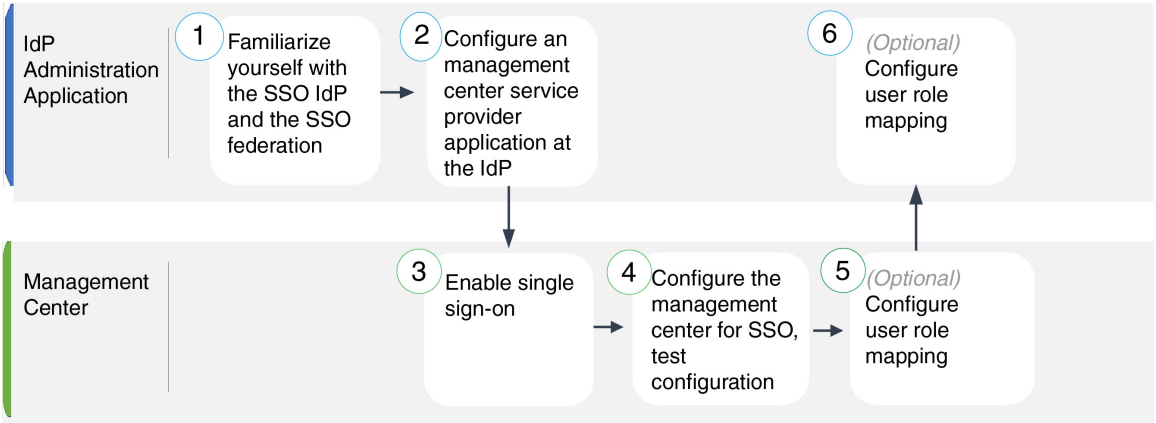
步骤 5 从**默认用户角色 (Default User Role)** 下拉列表中选择要分配用户的 管理中心 用户角色作为默认值。

步骤 6 点击 **测试配置**。如果系统显示错误消息，请查看 管理中心 的 SSO 配置以及面向客户的 PingOne 服务提供商应用，更正所有错误，然后重试。

步骤 7 当系统报告配置测试成功时，点击 **应用**。

使用任何符合 SAML 2.0 标准的 SSO 提供程序配置单点登录

管理中心 支持使用符合 SAML 2.0 SSO 协议的任何 SSO 身份提供程序 (IdP) 进行单点登录。使用各种 SSO 提供程序的通用说明必须解决要在较高级别执行的任务；使用本文档中未明确提及的提供商建立 SSO 要求您精通所选的 IdP。这些任务可帮助您确定使用任何符合 SAML 2.0 标准的 SSO 提供程序配置 管理中心 单点登录的步骤：



1	IdP 管理应用	熟悉 SSO 身份提供程序和 SSO 联合身份验证, on page 68。
2	IdP 管理应用	为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用, on page 68。
3	管理中心	在 管理中心启用单点登录, on page 27。
4	管理中心	为使用任何 SAML 2.0 兼容 SSO 提供程序的 SSO 配置 管理中心 , on page 70。
5	管理中心	在 管理中心上为符合 SAML 2.0 标准的 SSO 提供程序配置用户角色映射, on page 71。
6	IdP 管理应用	在 IdP 上为符合 SAML 2.0 标准的 SSO 提供程序配置 管理中心 用户角色映射, on page 72。

熟悉 SSO 身份提供程序和 SSO 联合身份验证

阅读 IdP 供应商文档时，请记住以下注意事项：

- SSO 提供商是否要求用户在使用 IdP 之前订用或注册任何服务？
- SSO 提供程序使用哪些术语来表示常见的 SSO 概念？例如，为了指代一组联合服务提供商应用，Okta 使用 “组织”，而 Azure 使用“租户”。
- SSO 提供程序是否仅支持 SSO 或一套功能（例如，多因素身份验证或域管理）？（这可能会影响功能之间共享的某些元素的配置，尤其是用户和组。）
- IdP 用户账户需要哪些权限才能配置 SSO？
- SSO 提供商要求您为服务提供商应用建立哪些配置？例如，Okta 会自动生成 X509 证书以保护其与 管理中心的通信，而 Azure 要求您使用 Azure 门户界面生成该证书。
- 如何创建和配置用户和组？如何将用户分配到组？如何授予用户和组访问服务提供商应用的权限？
- 在测试 SSO 连接之前，SSO 提供商是否要求将至少一个用户分配给服务提供商应用？
- SSO 提供程序是否支持用户组？如何配置用户和组属性？如何将属性映射到 SSO 配置中的 管理中心 用户角色？
- 是否需要向联盟添加更多用户或组以支持 管理中心上的 SSO？
- 联盟成员中的用户是否属于组？
- 用户和组定义是 IdP 本地的，还是从 Active Directory、RADIUS 或 LDAP 等用户管理应用导入的？
- 您要分配哪种类型的用户角色？（如果您选择不分配用户角色，管理中心会自动为用户分配一个可配置的默认用户角色给所有 SSO 用户。）
- 如何组织联盟中的用户和组，以支持您的用户角色映射计划？

为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用

通常，SSO 提供商要求您在 IdP 上为每个联合应用配置服务提供商应用。支持 SAML 2.0 SSO 的所有 IdP 都需要相同的服务提供商应用配置信息，但某些 IdP 会自动为您生成一些配置设置，而其他 IdP 则要求您自己配置所有设置。

Note 如果您计划将用户组分配给 管理中心 应用，请勿将这些组中的用户作为个人进行分配。

Note 管理中心 不能支持使用多个 SSO 属性的角色映射；您必须选择用户角色映射或组角色映射，并配置单个属性以将用户角色信息从 IdP 传送到 管理中心。

Before you begin

- 熟悉 SSO 联合及其用户和组；请参阅 熟悉 SSO 身份提供程序和 SSO 联合身份验证, on page 68。
- 确认您的 IdP 账户具有执行此任务所需的权限。
- 如有必要，在 SSO 联合中创建用户账户和/或组。

Note 系统要求 SSO 帐户的用户名以及 IdP 在 SAML 登录过程中发送给 管理中心 的 NameID 属性都必须是有效的邮箱地址。许多 IdP 会自动使用尝试登录的用户的用户名作为 NameID 属性，但您应确认您的 IdP 是否是这种情况。在 IdP 处配置服务提供商应用以及创建将被授予对 管理中心的 SSO 访问权限的 IdP 用户帐户时，请记住这一点。

- 确认目标 管理中心 的登录 URL (`https://ipaddress_or_hostname`)

Note 如果可以使用多个 URL 访问您的 管理中心 Web 接口。（例如，完全限定域名以及 IP 地址），SSO 用户必须使用您在此任务中配置的登录 URL 一致地访问 管理中心 。

Procedure

步骤 1 在 IdP 上创建新的服务提供商应用。

步骤 2 配置 IdP 所需的值。请务必添加下面列出的字段，以通过 管理中心支持 SAML 2.0 SSO 功能。（由于不同的SSO服务提供商对SAML概念使用不同的术语，此列表提供了这些字段的备用名称，以帮助您在 IdP 应用中找到正确的设置。）：

- 服务提供商实体 ID、服务提供商标识符、受众 URI：服务提供商的全局唯一名称 (管理中心)，格式为 URL。要创建它，请将字符串 `/saml/metadata` 附加到 管理中心 登录 URL，例如 `https://ExampleFMC/saml/metadata`。
- 单点登录 URL、收件人 URL、断言使用者服务 URL：浏览器代表 IdP 向其发送信息的服务提供商 (管理中心) 地址。要创建它，请将字符串 `saml/acs` 附加到 管理中心 登录 URL，例如 `https://ExampleFMC/saml/acs`。
- X.509 证书：用于保护 管理中心 与 IdP 之间的通信的证书。某些 IdP 可能会自动生成证书，而某些 IdP 可能要求您使用 IDP 接口明确生成证书。

步骤 3 （如果要向应用分配组，则可选）将单个用户分配到 管理中心 应用。（如果您计划将组分配给 管理中心 应用，请不要将这些组的成员作为个人进行分配。）

步骤 4 （如果要将单个用户分配给应用，则可选。）将用户组分配给 管理中心 应用。

步骤 5 （可选）某些 IdP 能够生成 SAML XML 元数据文件，其中包含您在此任务中配置的信息，格式为符合 SAML 2.0 标准。如果您的 IdP 提供此功能，您可以将文件下载到本地计算机，以简化 管理中心 上的 SSO 配置过程。

What to do next

启用单点登录；请参阅 在 管理中心启用单点登录, on page 27。

为使用任何 SAML 2.0 兼容 SSO 提供程序的 SSO 配置 管理中心

在 管理中心 web 接口上使用这些说明。要使用任何符合 SAML 2.0 的 SSO 提供程序为 SSO 配置 管理中心 ，您需要来自 IdP 的信息。

Before you begin

- 查看 SSO 联盟的组织及其用户和组。
- 在 IdP 上配置 管理中心 服务提供商应用；请参阅为使用任何 SAML 2.0 兼容 SSO 提供程序的 SSO 配置 管理中心 , on page 70。
- 从 IdP 收集服务提供商应用的以下 SSO 配置信息。由于不同的 SSO 服务提供商对 SAML 概念使用不同的术语，因此此列表提供了这些字段的备用名称，以帮助您在 IdP 应用中找到正确的值：
  - 身份提供程序单点登录 URL、登录 URL：浏览器代表 管理中心发送信息的 IdP URL。
  - 身份提供者颁发者、身份提供者颁发者 URL、颁发者 URL：IdP 的全局唯一名称，通常格式为 URL。
  - 用于保护 管理中心 和 IdP 之间通信的 X.509 数字证书。
- 启用单点登录；请参阅 在 管理中心启用单点登录, on page 27。

Procedure

步骤 1 （此步骤直接从 在 管理中心启用单点登录, on page 27开始。）在 **配置 SAML 元数据** 对话框中，您有两个选择：

- 要手动输入 SSO 配置信息，请执行以下操作：
  a. 点击 **手动配置** 单选按钮。
  b. 输入之前从 SSO 服务提供程序应用获取的以下值：
    - **身份提供程序单点登录 URL**
    - **身份提供程序颁发机构**
    - **X.509 证书**

- 如果您保存了 IdP 生成的 XML 元数据文件（ 为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用, on page 68中的步骤 5），则可以将该文件上传到 管理中心：
  a. 点击 **上传文件** 单选按钮。
  b. 按照屏幕上的说明导航到本地计算机上的 XML 元数据文件并选择该文件。

步骤 2 点击**下一步**。

步骤 3 在 **验证元数据** 对话框中，查看配置参数，然后点击 **保存**。

步骤 4 点击 **测试配置**。如果系统显示错误消息，请查看 管理中心 的 SSO 配置以及 IdP 上的服务提供商应用配置，更正所有错误，然后重试。

步骤 5 当系统报告配置测试成功时，点击 **应用**。

What to do next

您可以选择为 SSO 用户配置用户角色映射；请参阅 在 管理中心上为符合 SAML 2.0 标准的 SSO 提供程序配置用户角色映射, on page 71。如果您选择不配置角色映射，则默认情况下会为登录 管理中心 的所有 SSO 用户分配您在 在 管理中心上为符合 SAML 2.0 标准的 SSO 提供程序配置用户角色映射, on page 71的步骤 4 中配置的默认用户角色。

在 管理中心上为符合 SAML 2.0 标准的 SSO 提供程序配置用户角色映射

要实施 SAML SSO 用户角色映射，您必须在 IdP 和 管理中心上建立协调配置。

- 在 IdP 上，建立用户或组属性以传达用户角色信息并为其分配值； IdP 在对 SSO 用户进行身份验证和授权后，会将这些信息发送到 管理中心。
- 在 管理中心上，将值与要分配给用户的每个 管理中心 用户角色相关联。

当 IdP 发送与授权用户关联的 管理中心 用户或组属性时， 管理中心 会将属性值与与每个 管理中心 用户角色关联的值进行比较，并为用户分配产生匹配项的所有角色。管理中心执行此比较，将两个值视为符合 Golang 和 Perl 支持的受限版本的 Google RE2 正则表达式的正则表达式。

无论您选择哪种 SSO 提供商，在 管理中心 web 接口上为用户角色映射配置的字段都是相同的。但是，您配置的值必须考虑您使用的 SAML SSO 提供程序实施用户角色映射的方式。您的 IdP 可能会对用户或组属性实施语法限制；如果是，则必须使用符合这些要求的角色名称和正则表达式设计用户角色映射方案。

Before you begin

- 为 管理中心配置 SSO 服务提供商应用；请参阅 为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用, on page 68。
- 在 管理中心上启用和配置单点登录，请参阅 在 管理中心启用单点登录, on page 27和 为使用任何 SAML 2.0 兼容 SSO 提供程序的 SSO 配置 管理中心 , on page 70。

Procedure

步骤 1 选择 **系统** > **用户**。

步骤 2 点击 **单点登录** 选项卡。

步骤 3 展开 **高级配置（角色映射）**。

步骤 4 从**默认用户角色 (Default User Role)** 下拉列表中选择要分配用户的 管理中心 用户角色作为默认值。

步骤 5 输入 **组成员属性**。此字符串必须与 IdP 管理中心 服务提供商应用中为使用用户或组的用户角色映射配置的属性名称匹配。（请参阅 在 IdP 上为符合 SAML 2.0 标准的 SSO 提供程序配置 管理中心 用户角色映射, on page 72的第 1 步。）

步骤 6 在要分配给 SSO 用户的每个 管理中心 用户角色旁边，输入正则表达式。（ 管理中心 使用 Golang 和 Perl 支持的 Google RE2 正则表达式标准的受限版本。） 管理中心 将这些值与 IdP 发送到 管理中心的用户角色映射属性值和 SSO 用户信息进行比较。 管理中心 授予用户找到匹配项的所有角色的并集。

What to do next

在服务提供商应用中配置用户角色映射；请参阅 在 IdP 上为符合 SAML 2.0 标准的 SSO 提供程序配置 管理中心 用户角色映射, on page 72。

在 IdP 上为符合 SAML 2.0 标准的 SSO 提供程序配置 管理中心 用户角色映射

每个 IdP 配置用户角色映射的详细步骤各不相同。您必须确定如何为服务提供商应用创建自定义用户或组属性，并在 IdP 为每个用户或组分配属性值，以将用户或组权限传达给 管理中心。请注意以下事项：

- 如果您的 IdP 从第三方用户管理应用（例如 Active Directory、LDAP 或 Radius）导入用户或组配置文件，这可能会影响您如何使用属性进行角色映射。
- 考虑整个 SSO 联合中的用户和组角色定义。
- 管理中心 不能支持使用多个SSO属性的角色映射；您必须选择用户角色映射或组角色映射，并配置单个属性以将用户角色信息从 IdP 传送到 管理中心。
- 对于具有许多用户的 管理中心 ，组角色映射通常更有效。
- 如果将用户组分配给 管理中心 应用，则不要将这些组中的用户作为个人进行分配。
- 为了确定与 管理中心 用户角色的匹配， 管理中心 将从 IdP 接收的用户和组角色属性值视为符合 Golang 和 Perl 支持的 Google RE2 正则表达式标准的受限版本。您的 IdP 可能会对用户或组属性实施某些语法限制。如果是，则必须使用符合这些要求的角色名称和正则表达式设计用户角色映射方案。

Before you begin

- 确认您的 IdP 账户具有执行此任务所需的权限。

- 在 IdP 上配置 管理中心 服务提供商应用（请参阅为任何 SAML 2.0 兼容的 SSO 提供程序配置 FMC 服务提供程序应用, on page 68）。

Procedure

步骤 1 在 IdP 上，创建或指定要发送到 管理中心 的属性，以包含每个用户登录的角色映射信息。这可能是用户属性、组属性或从源（例如 IdP 或第三方用户管理应用维护的用户或组定义）获取其值的其他属性。

步骤 2 配置属性获取其值的方式。将可能的值与 管理中心 SSO 配置中的用户角色关联的值进行协调。

自定义 Web 界面的用户角色

必须为每个用户帐户定义用户角色。本部分介绍如何管理用户角色，以及如何配置可进行 Web 界面访问的自定义用户角色。对于默认用户角色，请参阅用户角色，第 2 页。

创建自定义用户角色

自定义用户角色可以拥有任意一组基于菜单的权限和系统权限，它们可以是全新的用户角色，可以从预定义或其他用户角色复制而来，也可以从其他 管理中心导入。

注释 （需要版本 7.4.1+） 虽然您可以在不升级产品的情况下启用对内容更新的访问，但我们建议您采用相反的做法：没有内容的产品。也就是说，如果您在自定义用户角色中启用**产品升级**，请同时启用**内容更新**。否则，您可能无法手动上传升级包 以及升级较早的 ASA FirePOWER 和 NGIPSv 设备。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击 **User Roles**。

步骤 3 使用以下方法之一添加新用户角色：

- 点击 **Create User Role**。
- 点击要复制的用户角色旁边的 **复制**（）。
- 从其他 管理中心导入自定义用户角色：
  1. 在其他 管理中心上，点击 **导出**（）将角色保存到您的 PC。
  2. 在新 管理中心上，选择 **系统**（⚙）> **工具** > **导入/导出**。

3. 点击 **上传数据包**，然后按照说明将保存的用户角色导入到新 管理中心。

步骤 4 为新用户角色输入一个**名称**。用户角色名称区分大小写。

步骤 5 （可选） 添加**说明**。

步骤 6 为新角色选择**基于菜单的权限**。

选择权限时，会选择其所有子级，且多值权限使用第一个值。如果清除选择高级权限，则也会清除其所有子级。如果您选择权限但没有选择其所有子级，则权限以斜体文本显示。

复制要用作自定义角色基础的预定义用户角色将预先选择与该预定义角色关联的权限。

可以对自定义用户角色应用受限搜索。这些搜索将限制用户可在“分析”菜单下可用页面上的表中所看到的数据。可以配置受限搜索，方法是先创建专用的已保存搜索，然后在适当的基于菜单的权限下从**受限搜索**下拉菜单中选择该搜索。

步骤 7 （可选） 选中 **外部数据库访问（只读）** 复选框为新角色设置数据库访问权限。

此选项使用支持 JDBC SSL 连接的应用提供数据库的只读访问权限。如果第三方应用要向 管理中心进行身份验证，必须在系统设置中启用数据库访问权限。

步骤 8 （可选） 要为新用户角色设置升级权限，请参阅启用用户角色升级，第 76 页。

步骤 9 点击**保存 (Save)**。
自定义角色已保存。如果系统确定它是只读角色，则会将该角色标记为“（只读）”。这在为只读和读写用户配置并发会话数时非常重要。不能通过将“（只读）”添加到角色名称来将角色设置为只读。 有关并发会话限制的详细信息，请参阅 用户配置。

示例

您可以为与访问控制相关的功能创建自定义用户角色，以指定用户是否可以查看和修改访问控制和关联策略。

下表显示了如何区分应能配置访问控制策略的所有方面（入侵配置除外）的网络管理员，以及应仅能配置与入侵相关的功能的入侵管理员。 **修改威胁配置** 权限允许在规则中选择入侵策略、变量集和文件策略，配置网络分析和入侵策略的高级选项，配置安全智能策略访问控制策略，以及策略默认操作中的入侵操作。**修改剩余访问控制策略配置 (Modify Remaining Access Control Policy Configuration)** 权限涵盖策略和规则的所有其他方面，包括创建和删除策略和规则。在此示例中，策略审批人可以查看（但无法修改）访问控制和入侵策略。他们还可以将配置更改部署到设备。

表 *1:* 访问控制自定义角色示例

基于菜单的权限	示例角色		
	访问控制编辑器	**Intrusion & Network Analysis Editor**	策略审批人
访问控制	是	是	是

基于菜单的权限	示例角色		
	访问控制编辑器	**Intrusion & Network Analysis Editor**	策略审批人
访问控制策略	是	是	是
修改访问控制策略 (Modify Access Control Policy)	否	是	否
修改威胁配置	否	是	否
修改其余的访问控制策略配置	是	否	否
入侵策略	否	是	是
修改入侵策略	否	是	否
将配置部署到设备	否	否	是

停用用户角色

停用角色会从已分配有该角色的任何用户从移除该角色和所有相关权限。不能删除预定义用户角色，但是可以将其停用。

在多域部署中，系统会显示在当前域中创建的自定义用户角色，您可以对其进行编辑。系统还会显示在祖先域中创建的自定义用户角色，您不可以对其进行编辑。要查看和编辑较低域中的自定义用户角色，请切换至该域。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击 **User Roles**。

步骤 3 点击要激活或停用的用户角色旁边的滑块。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

如果在具有某个角色的用户已登录时通过远端控制管理停用，然后重新启用该角色，或者在该用户的登录会话期间从备份恢复用户或用户角色，则该用户必须重新登录到Web 界面中才能重新获取对 IPMItool 命令的访问。

启用用户角色升级

可以通过密码为自定义用户角色提供权限，以除基本角色的权限以外，暂时获取其他目标用户角色的权限。通过此功能，您可以在某一用户不在场时轻松替换用户，或更密切地跟踪高级用户权限的使用。默认的用户角色不支持升级。

例如，基本角色的权限非常有限的用户可升级到管理员角色来执行管理操作。可以配置此功能，以便用户可以使用其自己的密码，或者因此使用所指定的其他用户的密码。通过第二个选项，可以轻松管理所有适用用户的一个升级密码。

要配置用户角色升级，请参阅以下工作流程。

过程

步骤 1 设置升级目标角色，第 76 页。一次只能有一个用户角色作为升级目标角色。

步骤 2 为升级配置自定义用户角色，第 76 页。

步骤 3 （对于登录的用户）升级用户角色，第 77 页。

设置升级目标角色

可以分配任何用户角色（预定义或自定义）来充当系统范围的升级目标角色。这是自定义角色可升级到的角色（如果具备这个能力）。一次只能有一个用户角色作为升级目标角色。每次升级持续时长为登录会话的持续时间，并会记录在审计日志中。

过程

步骤 1 选择**系统**（⚙）> **用户 (Users)**。

步骤 2 点击 **User Roles**。

步骤 3 点击 **Configure Permission Escalation**。

步骤 4 从**升级目标**下拉列表中选择一个用户角色。

步骤 5 点击 **OK**，保存更改。

更改升级目标角色立即生效。已升级会话中的用户现在具有新升级目标的权限。

为升级配置自定义用户角色

要对其启用升级的用户必须属于已启用升级的自定义用户角色。以下步骤介绍如何为自定义用户角色启用升级。

为自定义角色配置升级密码时，请考虑贵组织的需求。如果要轻松管理多个升级用户，可能需要选择另一个使用密码充当升级密码的用户。如果更改该用户的密码或停用该用户，则需要该密码的所

有升级用户都会受影响。通过此操作，可以更加高效地管理用户角色升级，尤其是在选择可以集中管理的外部身份验证用户的情况下。

开始之前

根据设置升级目标角色，第 76 页设置目标用户角色。

过程

步骤 1 开始配置自定义用户角色，如创建自定义用户角色，第 73 页中所述。

步骤 2 在 **系统权限**中，选择 **设置此角色以升级至：维护用户** 复选框。

当前升级目标角色列于复选框旁边。

步骤 3 选择此角色用于升级的密码。此时您有两种选择：

- 如果希望具有此角色的用户在升级时使用其自己的密码，请选择**使用分配的用户密码进行身份验证**。
- 如果希望具有此角色的用户使用其他用户的密码，请选择**使用指定用户的密码进行身份验证**，并输入该用户名。

  注释 在使用其他用户的密码进行身份验证时，可以输入任何用户名，甚至是已停用或不存在的用户的用户名。停用其密码用于升级的用户会使具有需要该密码的角色的用户无法升级。如有必要，可以使用此功能快速移除升级能力。

步骤 4 点击**保存 (Save)**。

升级用户角色

当用户具有带升级权限的已分配自定义用户角色时，该用户可以随时升级到目标用户的权限。请注意，升级对用户首选项没有影响。

过程

步骤 1 从用户名下的下拉列表中，选择**升级权限 (Escalate Permissions)**。

如果您没有看到此选项，则您的管理员没有为您的用户角色启用升级。

步骤 2 输入身份验证密码。

步骤 3 点击**升级 (Escalate)**。除当前角色以外，您现在具有升级目标角色的所有权限。

升级持续至登录会话结束。要仅返回到基本角色的权限，必须注销，然后开始新会话。

LDAP 身份验证连接故障排除

如果创建 LDAP 身份验证对象，并且其无法成功连接到选择的服务器或无法检索所需的用户列表，则可以调整该对象中的设置。

如果在测试连接时该连接失败，请尝试以下建议对配置进行故障排除。

- 使用 Web 界面屏幕顶部和测试输出中显示的消息确定对象的哪些方面导致问题。
- 检查用于对象的用户名和密码是否有效：
  - 检查用户是否有权通过使用第三方 LDAP 浏览器连接到 LDAP 服务器来浏览至基本可分辨名称中指示的目录。
  - 检查用户名对于 LDAP 服务器的目录信息树是否唯一。
  - 如果在测试输出中显示 LDAP 绑定错误 49，则表明用户的用户绑定失败。请尝试通过第三方应用对服务器进行身份验证，以了解通过该连接进行的绑定是否也失败。
- 检查是否已正确识别服务器：
  - 检查服务器 IP 地址或主机名是否正确。
  - 检查是否有从本地设备到要连接的身份验证服务器的 TCP/IP 访问权限。
  - 检查对服务器的访问是否未被防火墙阻止，以及在对象中配置的端口是否已打开。
  - 如果是使用证书通过 TLS 或 SSL 进行连接，则证书中的主机名必须与用于服务器的主机名匹配。
  - 如果是对 CLI 访问进行身份验证，请检查是否未对服务器连接使用 IPv6 地址。
  - 如果使用了服务器类型默认值，请检查是否具有正确的服务器类型，并再次点击**设置默认值 (Set Defaults)** 以重置默认值。
- 如果键入了基本可分辨名称，请点击**获取 DN (Fetch DNs)** 以检索服务器上的所有可用基本可分辨名称，然后从列表中选择名称。
- 如果使用的是任意过滤器、访问属性或高级设置，请检查各项是否有效且正确键入。
- 如果使用的是任意过滤器、访问属性或高级设置，请尝试移除各设置并测试没有此设置的对象。
- 如果使用的是基本过滤器或 CLI 访问过滤器，请确保用括号将过滤器括起来，并且使用的是有效的比较运算符（包括括号在内，最大450个字符）。
- 要测试受限更多的基本过滤器，请尝试将其设置为基本可分辨名称，以使用户仅检索该用户。
- 如果使用的是加密连接：
  - 检查证书中 LDAP 服务器的名称是否与用于连接的主机名匹配。
  - 检查是否未对加密服务器连接使用 IPv6 地址。

- 如果使用的是测试用户，请确保正确键入用户名和密码。
- 如果使用的是测试用户，请移除用户凭证并测试对象。
- 通过连接到 LDAP 服务器并使用以下语法测试使用的查询：

```
ldapsearch -x -b 'base_distinguished_name'
-h LDAPserver_ip_address -p port -v -D
'user_distinguished_name' -W 'base_filter'
```

例如，如果是尝试使用 `domainadmin@myrtle.example.com` 用户和基本过滤器 (`cn=*`) 连接到 `myrtle.example.com` 上的安全域，则可以使用以下语句测试连接：

```
ldapsearch -x -b 'CN=security,DC=myrtle,DC=example,DC=com'
-h myrtle.example.com -p 389 -v -D
'domainadmin@myrtle.example.com' -W '(cn=*)'
```

如果可以成功测试连接，但在部署平台设置策略后身份验证不起作用，请检查在应用到设备的平台设置策略中是否已启用要使用的身份验证和对象。

如果成功连接，但要调整连接检索到的用户列表，则可以添加或更改基本过滤器或CLI访问过滤器，或者使用限制较多或较少的基本 DN。

在对与 Active Directory (AD) 服务器的连接进行身份验证时，尽管与 AD 服务器的连接成功，但连接事件日志很少指示受阻 LDAP 流量。当 AD 服务器发送重复的重置数据包时，会出现此不正确的连接日志。威胁防御 设备将第二个重置数据包识别为新连接请求的一部分，并使用“阻止”操作记录连接。

配置用户首选项

根据您的用户角色，您可以为您的用户账号指定某些首选项。

在多域部署中，用户首选项适用于您的帐户有权访问的所有域。当指定主页和控制面板首选项时，请记住某些页面和控制面板构件会受域限制。

更改密码

所有用户帐户均采用密码保护。可以随时更改密码，根据用户帐户设置，可能需要定期更改密码。

启用密码强度检查时，密码必须符合 管理中心用户帐户的指南和限制，第 5 页中所述的强密码要求。

如果是 LDAP 或 RADIUS 用户，则不能通过 Web 界面更改密码。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 点击**更改密码**。

步骤 3 （可选）选中 **显示密码** 复选框可在使用此对话时查看密码。

步骤 4 输入您的 **当前密码**。

步骤 5 此时您有两种选择：

- 输入您的新密码的 **新密码** 和 **确认密码**。
- 点击**生成密码**按钮，让系统为您创建符合所列条件的密码。（生成的密码是非助记密码；如果您选择此选项，请仔细记下密码。）

步骤 6 点击**应用 (Apply)**。

更改到期密码

根据用户帐户设置，密码可能已过期。在账户已创建时，将会设置密码到期时间段。如果密码已过期，系统会显示 Password Expiration Warning 页面。

过程

在“密码到期警告”(Password Expiration Warning) 页面上，您有两种选择：

- 点击**更改密码**，立即更改密码。如果剩余的警告天数为零，则**必须**更改密码。

  提示 启用密码强度检查时，密码必须符合 管理中心用户帐户的指南和限制，第 5 页中所述的强密码要求。

- 点击**跳过**，稍后更改密码。

更改 Web 接口外观

您可以更改 Web 接口的显示方式。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。默认情况下，系统会显示 **常规** 选项卡。

步骤 2 选择主题：

- **亮色**
- **Dusk**

- **经典** （6.6 之前版本的外观）

指定主页

可以将网络界面中的页面指定用作该设备的主页。默认主页为“默认控制面板”(**概述**>**控制面板**)，但对无权访问控制面板的用户例外，录入外部数据库用户。（请参阅 指定默认控制面板 ， 第 86 页以设置默认控制面板。）

在多域部署中，您选择的主页适用于您的用户帐户具有访问权限的所有域。为经常访问多个域的帐户选择主页时，请记住某些页面限制为全局域。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 点击 **Home Page**。

步骤 3 从下拉列表中选择要用作主页的页面。

下拉列表中的选项基于用户帐户的访问权限。有关详细信息，请参阅用户角色 ， 第 2 页。

步骤 4 点击**保存 (Save)**。

配置事件视图设置

使用“事件视图设置”页面配置 管理中心上事件视图的特征。请注意，一些事件视图配置仅对特定的用户角色可用。使用外部数据库用户角色的用户可以查看事件视图设置用户界面的某些部分，但是更改这些设置不会产生有意义的结果。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 点击 **Event View Settings**。

步骤 3 在 **事件首选项** 部分，配置事件视图的基本特征；请参阅 事件视图首选项 ， 第 82 页。

步骤 4 在 **文件首选项** 部分，配置文件下载首选项；请参阅 文件下载首选项 ， 第 83 页。

步骤 5 在 **默认时间窗口** 部分，配置默认时间窗口；请参阅 默认时间窗口 ， 第 83 页。

步骤 6 在 **默认工作流程** 部分，配置默认工作流程；请参阅 默认工作流程 ， 第 85 页。

步骤 7 点击**保存 (Save)**。

事件视图首选项

使用“事件视图设置”(Event View Settings) 页面的“事件首选项”(Event Preferences) 部分可在 Firepower 系统中配置事件视图的基本特征。尽管此区域对无法查看事件的用户不重要，但所有用户角色均可使用。

以下字段显示在“事件首选项”(Event Preferences) 部分：

- **确认“所有”操作**字段控制设备是否强制确认影响事件视图中所有事件的操作。

  例如，如果已启用此设置且点击事件查看上的**Delete All**，必须确认要删除的所有事件满足当前的限制条件（包括在当前页面未显示的活动），然后才可将其从数据库中删除。

- **解析 IP 地址**字段允许设备在事件视图中显示主机名（若可能）而非 IP 地址。

  请注意，如果事件查看包含大量 IP 地址，并且已启用该选项，则该视图可能缓慢显示。另请注意，为使此设置生效，必须使用管理接口配置在系统设置中建立 DNS 服务器。

- **Expand Packet View** 字段可供您配置入侵事件数据包视图的显示方式。默认情况下，设备以折叠方式显示数据包视图：
  - **None** - 折叠数据包视图的 Packet Information 部分的所有子部分
  - **Packet Text** - 仅展开 Packet Text 子部分
  - **Packet Bytes** - 仅展开 Packet Bytes 子部分
  - **All** - 展开所有部分

无论默认设置如何，您始终可以手动展开数据包视图中的部分查看有关已捕获数据包的详细信息。

- **每页行数 (Rows Per Page)** 字段控制要在向下页面和表视图中显示的每页事件行数。
- **刷新时间间隔 (Refresh Interval)** 字段设置事件查看的刷新时间间隔（以分钟为单位）。输入 0 可禁用刷新选项。请注意，此时间间隔不适用于控制面板。
- **统计信息刷新时间间隔 (Statistics Refresh Interval)** 控制事件摘要页面（例如，“入侵事件统计信息”[Intrusion Event Statistics] 和“发现统计信息”[Discovery Statistics] 页面）的刷新时间间隔。输入 0 可禁用刷新选项。请注意，此时间间隔不适用于控制面板。
- **Deactivate Rules** 字段控制哪些链接显示在标准文本规则生成的入侵事件的数据包视图上：
  - **All Policies** - 用于取消激活所有本地定义的自定义入侵规则中的标准文本规则的一个链接。
  - **当前策略 (Current Policy)** - 用于仅停用当前部署的入侵规则中的标准文本规则的一个链接。请注意，您不能停用默认策略中的规则。
  - **Ask** - 每一这些选项的链接

要在数据包视图上看到这些链接，您的用户帐户必须具有管理员或入侵管理员权限。

文件下载首选项

使用“事件视图设置”(Event View Settings) 页面的“文件首选项”(File Preferences) 部分配置本地文件下载的基本特征。此部分仅适用于具有管理员、安全分析师或安全分析师（只读）用户角色的用户。

请注意，如果设备不支持下载捕获的文件，则这些选项会被禁用。

以下字段显示在“文件首选项”(File Preferences) 部分：

- **确认“下载文件”操作 (Confirm ‘Download File’ Actions)** 复选框控制“文件下载”(File Download) 弹出窗口是否每次都显示下载文件，同时显示警告并提示继续或取消。

注意 思科强烈建议**不要**下载恶意软件，因为其可能造成不利后果。下载任何文件时请保持谨慎，这些文件可能包含恶意软件。确保您在下载文件前已采取各种必要预防措施保证下载目标安全。

请注意，在下载文件时，可随时禁用此选项。

- 当下载捕获的文件时，系统会创建一个包含该文件的有密码保护的 .zip 归档文件。**Zip 文件密码 (Zip File Password)** 字段定义要用于限制 .zip 文件的访问权限的密码。如果将此字段留空，系统会创建不需要密码的归档文件。
- **显示 Zip 文件密码 (Show Zip File Password)** 复选框会切换显示 **Zip 文件密码 (Zip File Password)** 字段中的纯文本或模糊字符。当清除此字段时，**Zip 文件密码 (Zip File Password)** 显示模糊字符。

默认时间窗口

时间段，有时称为时间范围，会对任何事件查看中的事件施加时间限制。使用“事件视图设置”页面的“默认时间段”区域控制时间段的默认行为。

此区域的用户角色访问权限列出如下：

- 管理员和维护人员可以访问完整的区域。
- 安全分析师和安全分析师（只读）可访问除**审核日志时间段**之外的所有选项。
- 访问管理员、发现管理员、外部数据库用户、入侵管理员、网络管理员和安全审批人只能访问**事件时间段**选项。

请注意，无论默认时间段设置如何，在事件分析期间，可以始终手动更改单个事件查看的时间段。另请注意，时间段设置仅对当前会话有效。在注销后重新登录时，时间段会重置为在此页面中配置的默认设置。

可为以下三种类型的事件设置默认时间段：

- **事件时间段**可为按时间限制的多数事件设置单个默认时间段。
- **审核日志时间段**可为审核日志设置默认时间段。

- **运行状况监控时间段**可为运行状况事件设置默认时间段。

仅可以为用户帐户可访问的事件类型设置时间段。所有用户类型都可设置事件时间段。管理员、维护人员和安全分析师可以设置运行状况监控时间段。管理员和维护人员可以设置审核日志时间段。

请注意，因为不是所有的事件查看都可以受时间限制，所以时间段设置对显示主机、主机属性、应用程序、客户端、漏洞、用户身份或合规 allow 名单违规的事件查看没有影响。

可以使用**多个**时间段，每种事件类型一个，也可以使用适用于所有事件的**一个**时间段。如果使用一个时间段，则不会显示三种时间段类型的设置，会显示新的**全局时间段**设置。

有以下三种类型的时间段：

- 静态，显示从特定开始时间到特定结束时间生成的所有事件。
- 扩展，显示从特定开始时间到目前生成的所有事件；随着时间的推进，时间段会进行扩展，并会有新事件添加到事件视图中。
- 滑动，显示从某个特定开始时间（例如，一天前）到当前时间生成的所有事件；随着时间向前推进，时间段会“滑动”，以便只可以查看所配置范围内的事件（在本示例中，为最后一天）

所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。

以下选项显示在**时间段设置**下拉列表：

- **显示最后时间 - 滑动式**选项允许配置指定长度的默认滑动时间窗。

  设备显示在某个特定开始时间（例如，1 小时前）和当前时间期间生成的所有事件。更改事件视图时，时间窗口会“滑动”，以便始终显示最后一小时的事件。

- 通过**显示最后时间 - 静态/扩展式**选项，可以配置指定长度的静态或扩展默认时间窗口。

  对于**静态**时间段，启用**使用结束时间**复选框。设备会显示在某个特定开始时间（例如，1 小时前）和第一次查看事件时的时间期间生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。

  对于**扩展**时间段，禁用**使用结束时间**复选框。设备显示在某个特定开始时间（例如，1 小时前）和当前时间期间生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。

- **当日 - 静态/扩展式**选项允许为当日配置静态或扩展默认时间段。当日从午夜开始，基于当前会话的时区设置。

  对于**静态**时间段，启用**使用结束时间**复选框。设备会显示从午夜到第一次查看事件时的时间期间生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。

  对于**扩展**时间段，禁用**使用结束时间**复选框。设备会显示在午夜到当前时间期间生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。请注意，如果在您注销之前，分析持续 24 小时以上，则此时间窗口可以超过 24 小时。

- **当周 - 静态/扩展式**选项允许为当周配置静态或扩展默认时间段。当周从上一周日的午夜开始，基于当前会话的时区设置。

对于**静态**时间段，启用**使用结束时间**复选框。设备会显示从午夜到第一次查看事件时的时间期间生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。

对于**扩展**时间段，禁用**使用结束时间**复选框。设备会显示在周日午夜到当前时间期间生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。请注意，如果在您注销之前，分析持续 1 周以上，则此时间窗口可以超过 1 周。

默认工作流程

工作流程是一组页面，显示分析师评估事件所使用的数据。对于每个事件类型，设备附带了至少一个预定义工作流程。例如，作为安全分析师，根据执行分析的类型，可以在十种入侵事件工作流程中选择，每种类型都会以不同的方式显示入侵事件数据。

设备会使用每种事件类型的默认工作流程进行配置。例如，按优先级和分类事件的工作流程是入侵事件的默认值。这意味着，只要查看入侵事件（包括已审阅的入侵事件），设备都会显示按优先级和分类事件的工作流程。

但是，您可以更改每种事件类型的默认工作流程。可配置的默认工作流程取决于用户角色。例如，入侵事件分析师无法设置默认发现事件工作流程。

设置默认时区

此设置仅确定您的用户账号在 Web 界面中显示的时间，例如任务计划和查看控制面板。此设置不会更改系统时间或影响任何其他用户，也不会影响系统中存储的数据（通常使用 UTC）。

警告 时区功能（在“用户首选项”中）假设系统时钟设置为UTC时间。请勿尝试更改系统时间。不支持从 UTC 更改系统，而执行此操作将需要您重新映像设备以从不支持的状态中恢复。

注释 此功能不影响用于基于时间的策略应用的时区。在 **设备 > 平台设置**中设置设备的时区。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 点击 **时区** 下拉列表。

步骤 3 选择包含要使用时区的大洲或区域。

步骤 4 选择与要使用的时区对应的国家/地区和省/自治区名称。

指定默认控制面板

当选择**概述** > **控制面板**时，系统将会显示默认控制面板。除非更改，否则所有用户的默认控制面板都是“摘要”(Summary) 控制面板。如果您的用户角色是管理员、维护人员或安全分析师，则可以更改默认控制面板。

在多域部署中，选择的默认控制面板适用于用户帐户具有访问权限的所有域。当选择频繁访问多个域的帐户的控制面板时，请记住，某些控制面板构件会受域限制。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 点击 **控制面板设置**。

步骤 3 从下拉列表中选择要用作默认的控制面板。

步骤 4 点击**保存 (Save)**。

配置操作方法设置

“操作方法”是一个构件，它提供导航管理中心上任务的逐步指导。逐步指导将引导您完成每个步骤，依次熟悉可能必须导航的各类陌生UI界面，引导您完成实现任务所需执行的步骤，最终完成任务。**操作方法**构件默认为启用。

有关 管理中心 中支持的功能逐步指导的列表，请参阅Cisco Secure Firewall Management Center 支持的功能逐步指导。

注释

- 通常情况下，逐步指导对所有 UI 页面可用，并且不区分用户角色。但是，根据用户权限的不同，某些菜单项将不会显示在 管理中心 界面上。因此，逐步指导将不会在此类页面上执行。
- 此功能在经典主题中不可用。

过程

步骤 1 从用户名下的下拉列表中，选择**用户首选项**。

步骤 2 **How-To 设置**。

步骤 3 选中 **启用 How-To** 复选框以启用 How-To。

步骤 4 点击**保存**。

下一步做什么

要打开“操作方法”构件，请选择**帮助 (Help)** > **操作方法 (How-Tos)**。您可以搜索解决相关任务的操作方法逐步指导。有关详细信息，请参阅 搜索如何逐步指导。

的用户帐户历史记录

功能	最低 管理中心	最低 威胁防御	详情
用于修改访问控制策略和规则的精细权限。	7.4	任意	您可以定义自定义用户角色，以区分访问控制策略和规则中的入侵配置以及访问控制策略和规则的其余部分。使用这些权限，您可以分离网络管理团队和入侵管理团队的职责。 定义用户角色时，可以选择 **策略** > **访问控制** > **访问控制策略** > **修改访问控制策略** > **修改威胁配置** 选项，以允许在规则中选择入侵策略、变量集和文件策略，以及配置网络分析的高级选项和入侵策略、访问控制策略的安全情报策略配置以及策略默认操作中的入侵操作。您可以使用 **修改其余访问控制策略配置** 来控制编辑策略的所有其他方面的能力。包含“修改访问控制策略”权限的现有预定义用户角色继续支持所有子权限；如果要应用精细权限，则需要创建自己的自定义角色。
添加了用于分配外壳用户名模板的新字段。	7.0	任意	调配以指定用于 LDAP 外部身份验证的 CLI 访问属性模板 - 引入了 **外壳用户名模板** 。因此，CLI 属性将有自己的模板来标识 LDAP CLI 用户。 新增/修改的屏幕： **系统**（⚙）> **用户** > **外部身份验证**
添加了对使用任何符合 SAML 2.0 的 SSO 提供程序的单点登录的支持。	6.7	任意	增加了对任何第三方 SAML 2.0 兼容身份供应程序 (IdP) 上配置的外部用户的单点登录支持。这包括将用户或组角色从 IdP 映射到管理中心用户角色的能力。 只有通过内部或通过 LDAP 或 RADIUS 进行身份验证的具有管理员角色的用户才能配置 SSO。 新增/修改的屏幕： **系统**（⚙）> **用户** > **单点登录**
Web 界面的主题。	6.6	任意	您可以选择 Web 界面的外观。 选择“浅色”(Light) 或“黄昏”(Dusk) 主题，或使用以前版本中出现的经典主题。 新增/修改的屏幕： 用户名 (User Name) > **用户首选项 (User Preferences)** > **常规 (General)** > **UI 主题 (UI Theme)** 支持的平台： 管理中心

功能	最低 管理中心	最低 威胁防御	详情
为用户帐户中的名称添加了一个新字段。	6.6	任意	添加了可标识负责内部用户帐户的用户或部门的字段。 新增/修改的屏幕： **系统**（⚙）> **用户** > **用户> 实际名称 (Real Name)** 字段
不再支持思科安全管理器单点登录。	6.5	任意	从 Firepower 6.5 开始，不再支持 管理中心 和思科安全管理器之间的单点登录。 新增/修改的屏幕： **系统**（⚙）> **用户 (Users)> CSM 单点登录 (CSM Single Sign-on)**
增强密码安全性。	6.5	任意	对强密码的新要求现在显示在本章中的某处，并从其他章节交叉引用。 更改密码界面中添加了新字段：**显示密码 (Show Password)** 和**生成密码 (Generate Password)**。 新增/修改的屏幕： 用户名 (User Name) > **用户首选项 (User Preferences)** > **常规 (General)** > **更改密码 (Change Password)**

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。