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。

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。

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

思科防御协调器 (CDO) 中有多种用户角色：只读、仅编辑、仅部署、管理员和超级管理员。为每个租户上的每个用户配置用户角色。如果 CDO 用户可以访问多个租户，则他们可能具有相同的用户

ID，但在不同的租户中具有不同的角色。用户可能在一个租户上具有只读角色，在另一个租户上具有超级管理员角色。当界面或文档提及只读用户、仅部署、仅编辑、管理员用户或超级管理员用户时，我们描述的是该用户对特定租户的权限级别。

只读

只读用户无法编辑策略和对象，也无法将更改部署到设备，只能查看它们。

仅部署

仅部署用户可以查看所有策略和对象。将暂存更改部署到一个或多个设备。

仅编辑

“仅编辑”用户可以修改并保存策略和对象，但不能将其部署到设备。

超级管理员和管理员

超级管理员和管理员用户可以访问产品中的所有内容。此用户可以创建、读取、修改和删除任何策略和对象，并将其部署到设备。

使用您的 CDO 用户名创建 CDO 用户记录

只有具有“超级管理员”权限的 CDO 用户才能创建 CDO 用户记录。超级管理员应使用上述 **创建您的 CDO 用户名** 任务中指定的相同邮箱地址创建用户记录。

使用以下程序创建具有适当用户角色的用户记录：

Procedure

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单栏中，选择 **设置** > **用户管理**。

步骤 3 点击蓝色加号按钮  ，将新用户添加到租户。

步骤 4 提供用户的邮件地址。

Note 用户的邮箱地址必须与 Cisco Secure Log-On 账户的邮箱地址相对应。

步骤 5 从下拉菜单中选择用户的 角色 。

步骤 6 点击**确定 (OK)**。

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。

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。

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 CDO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。

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。

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。
- 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 输入**名称**和可选**说明**。

步骤 6 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 7 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 8 （可选） 更改**端口**使用的默认值。

步骤 9 （可选） 输入**备份服务器**参数。

步骤 10 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**，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** - 点击**无**、**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** - 对于 SSL 或 TLS 加密，必须通过点击**选择文件**选择一个证书。

  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 (Timeout)** - 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 11 （可选） 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。

- 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 12 （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`。

步骤 13 （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，请选择**与基本过滤器相同 (Same as Base Filter)**。
- 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；不能包含句点 (.)、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 14 （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 16 页。

步骤 15 （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 16 点击**保存 (Save)**。

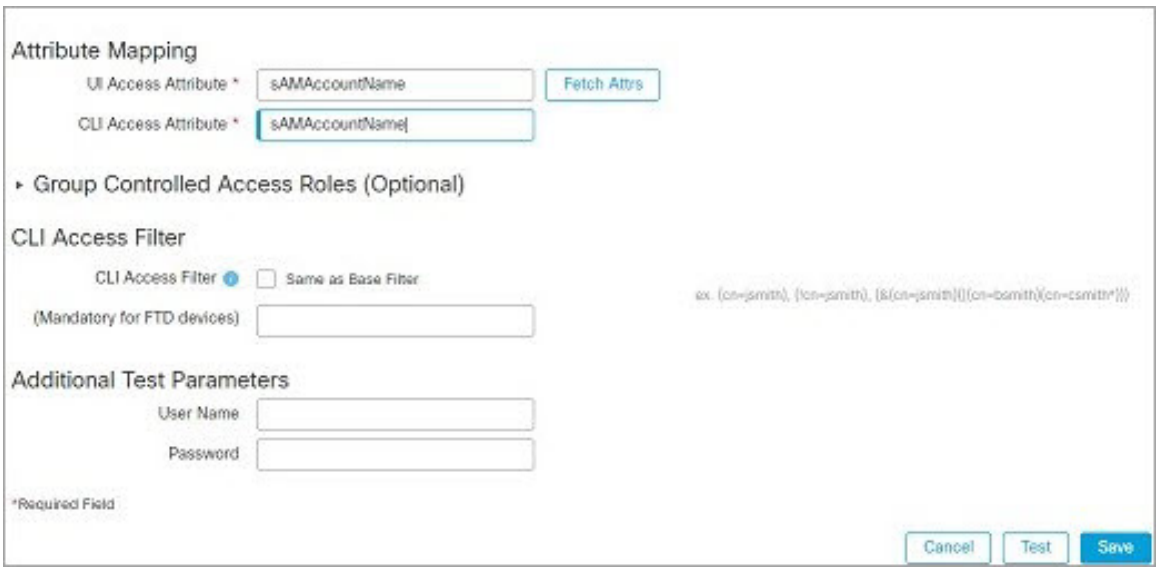
步骤 17 启用此服务器。请参阅为 CDO上的用户启用外部身份验证，第 15 页。

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。



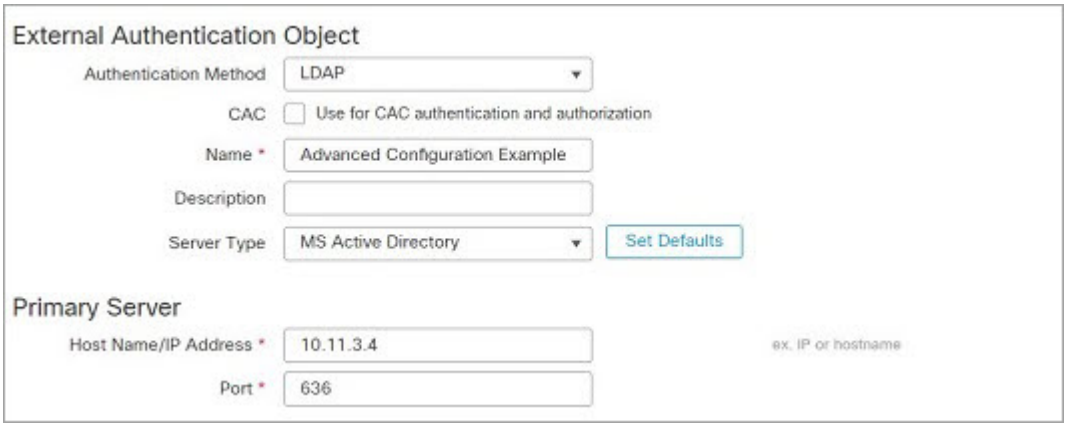
但是，由于此服务器是 Microsoft Active Directory 服务器，因此其使用 `sAMAccountName` 属性存储用户名而不是 `uid` 属性。选择 MS Active Directory 服务器类型并点击**设置默认值 (Set Defaults)** 会将“UI 访问属性”(UI Access Attribute) 设置为 `sAMAccountName`。因此，当用户尝试登录系统时，系统会检查各对象的 `sAMAccountName` 属性以查找匹配的用户名。

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。

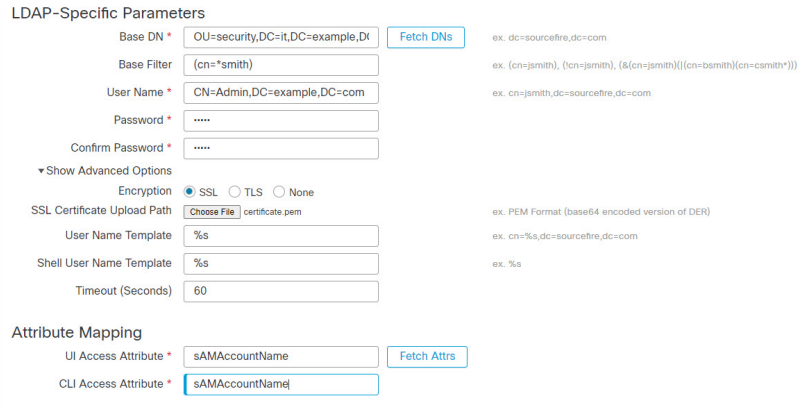
请注意，由于未对此服务器应用基本过滤器，因此系统会检查目录中基本可分辨名称所指示的所有对象的属性。经过默认时间段（或 LDAP 服务器上设置的超时期）后，与服务器的连接将超时。

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。

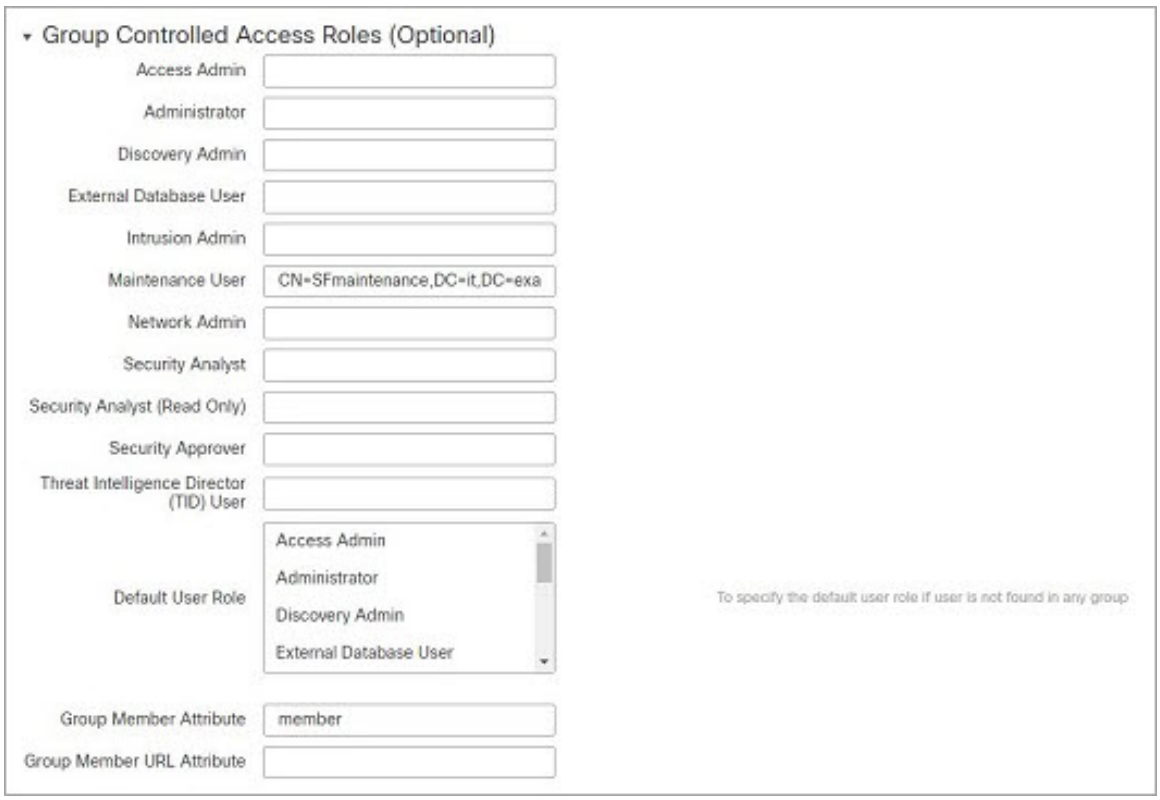


与服务器的连接使用 SSL 进行加密，并且会为该连接使用一个名为 `certificate.pem` 的证书。此外，由于**超时 (Timeout)** 设置，与服务器的连接在 60 秒后将超时。

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 CDO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。

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 **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。

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；不能包含句点 (.)、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。

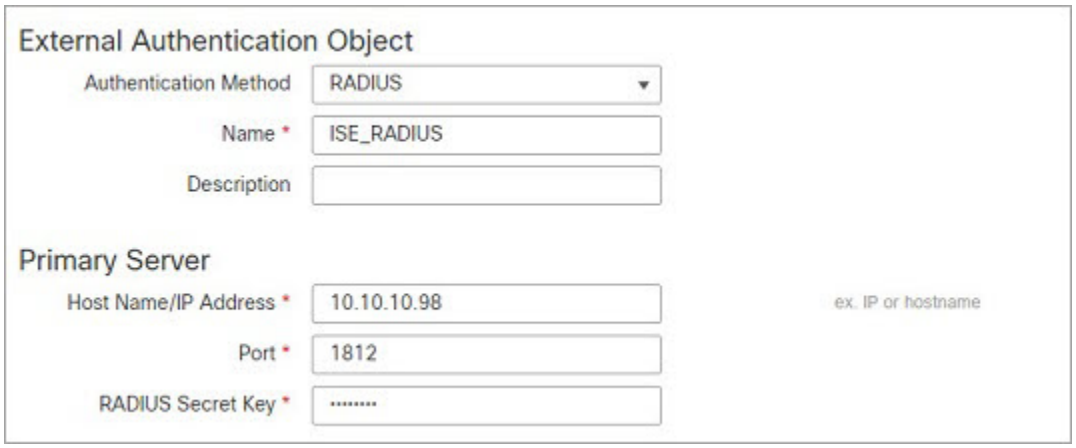
步骤 15 点击**保存 (Save)**。

步骤 16 启用此服务器。请参阅为 CDO上的用户启用外部身份验证 ， 第 15 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：

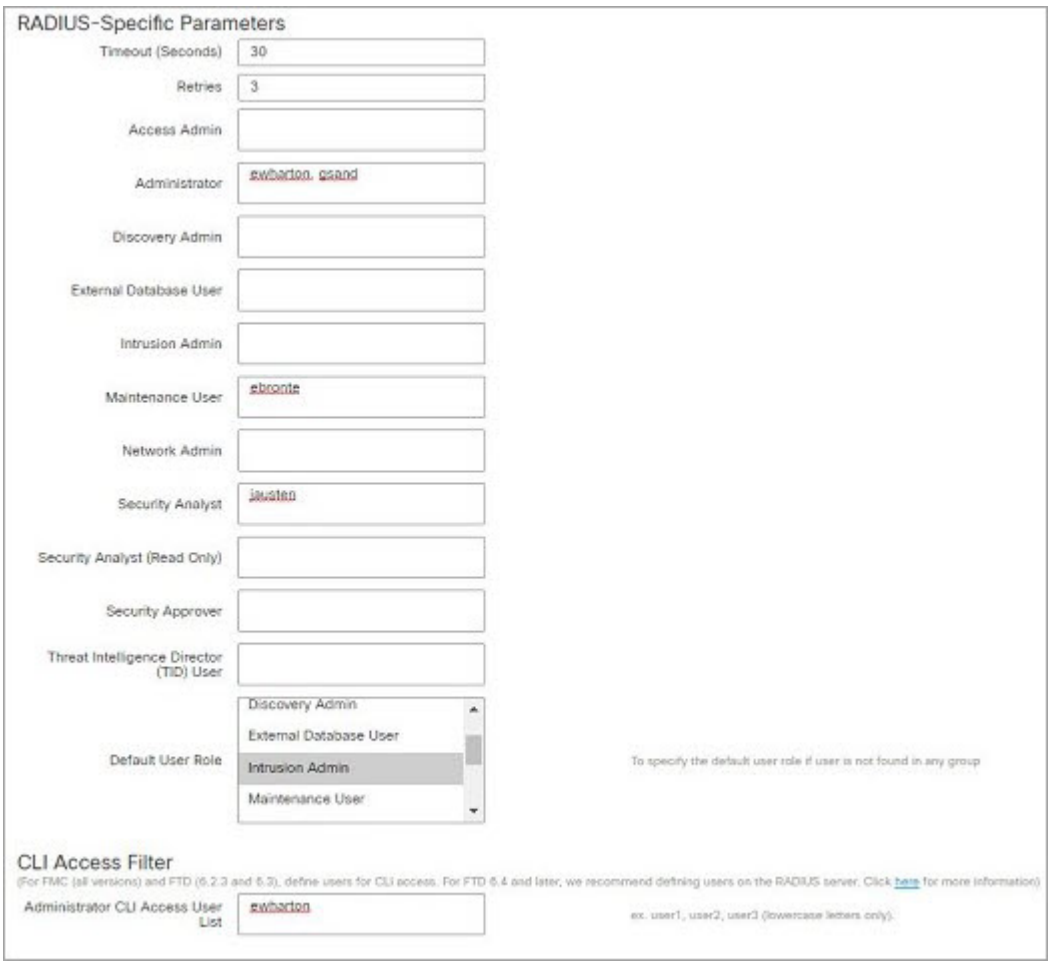
授予用户 `ewharton` 和 `gsand` Web 界面管理权限。

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：

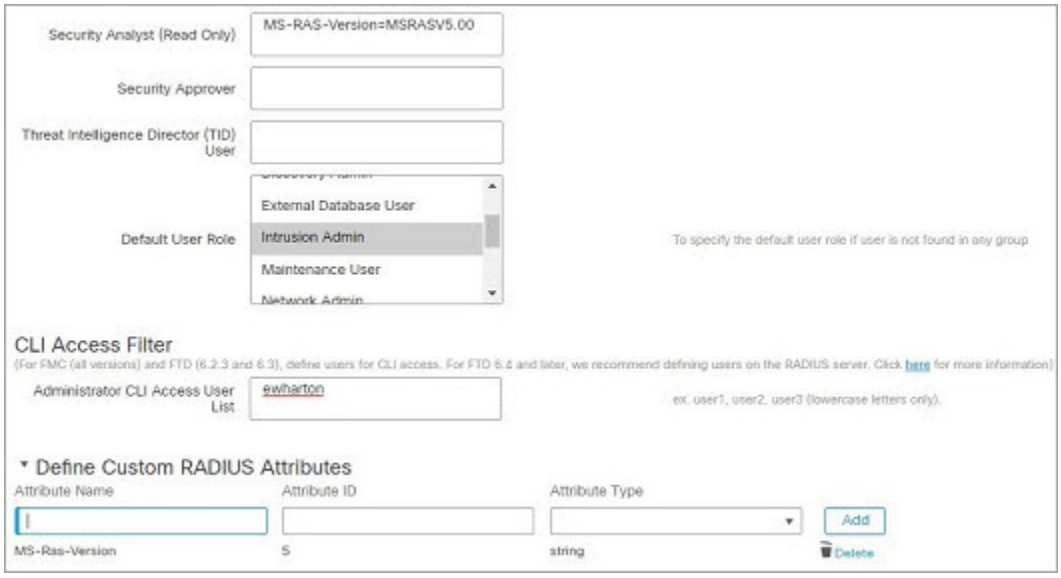


匹配属性-值对的用户角色

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 CDO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 CDO的 LDAP 外部身份验证对象，第 4 页 和 添加 CDO的 RADIUS 外部身份验证对象，第 10 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)**。

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**。

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。

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。