CLI 用户

托管设备中有一个用于 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 CLI 用户，第 1 页
- CLI 用户准则，第 2 页
- 在 CLI 中添加内部用户，第 3 页
- 配置 FTD 的外部身份验证，第 5 页
- LDAP 身份验证连接故障排除，第 17 页
- CLI 用户的历史记录，第 19 页

关于 CLI 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 防火墙管理中心时，该用户只能访问防火墙管理中心；您不能使用该用户名直接登录托管设备。您必须单独在托管设备上添加用户。

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。

CLI 访问

Firepower 设备包括一个在 Linux 上运行的 Firepower CLI。您可以使用 CLI 在设备上创建内部用户。您可以使用 防火墙管理中心在 Firewall Threat Defense 设备上建立外部用户。

⚠

注意 拥有 CLI 配置级别访问权的用户可以使用 **expert** 命令来访问 Linux 外壳，并在 Linux 外壳中获得 `sudoers` 权限，这可能会带来安全风险。出于系统安全原因，我们强烈建议：

- 仅在 TAC 监督下或在 Firepower 用户文档明确指示时使用 Linux 外壳。
- 请确保相应地限制具有 CLI 访问权限的用户列表。
- 在授予 CLI 访问权限时，请显示具有“配置”级别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。
- 除非思科 TAC 指示或 Firepower 用户文档中有明确说明，否则请不要使用 CLI 专家模式来访问 Firepower 设备。

CLI 用户角色

在托管设备上，用户在 CLI 中的命令访问权限取决于您所分配的角色。

无

用户无法在命令行上登录设备。

配置

用户可以访问所有命令，包括配置命令。请谨慎将此访问级别分配给用户。

基本

用户只能访问非配置命令。允许的命令包括 dig、ping 和 traceroute。只有内部用户和 Firewall Threat Defense 外部 RADIUS 用户支持基本角色。

CLI 用户准则

用户名

- 不能为内部和外部用户添加相同的用户名。如果外部服务器使用重复的用户名，则部署到设备会失败。
- 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 (/)

默认值

所有设备都包括一个 **admin** 用户作为本地用户帐户；您不能删除 **admin** 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。代理将修改后的凭证存储在 Windows 注册表中，并使用与防火墙管理中心相同的加密方式，即密码块链(CBC)。有关系统初始化的详细信息，请参阅您的型号的入门指南 。

用户账户数量

您最多可以为 Firepower 1100系列设备创建 43 个用户账户。

在 CLI 中添加内部用户

使用 CLI 可在 Firewall Threat Defense上创建内部用户。

过程

步骤 1 使用具有配置权限的帐户登录设备 CLI。

管理员用户账号具有所需的权限，但具有配置权限的任何帐户都可以执行操作。您可以使用 SSH 会话或控制台端口。

对于某些 Firewall Threat Defense型号，控制台端口会带您进入 FXOS CLI。使用 **connect ftd** 命令进入 Firewall Threat Defense CLI。

步骤 2 创建用户账号。

configure user add *username* {**basic** | **config**}

- 用户名-设置用户名。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 (/)
- **basic**- 提供用户基本访问权限。此角色不允许用户输入配置命令。允许的命令包括 dig、ping 和 traceroute。
- **config**- 提供用户配置访问权限。此角色将赋予用户完整管理员权限，让其可以输入所有配置命令。

示例：

以下示例将添加一个名为 johncrichton 且具有配置访问权限的用户账号。在您键入密码时，密码不会显示。

```
> configure user add johncrichton config
```

```
Enter new password for user johncrichton: newpassword
Confirm new password for user johncrichton: newpassword
> show user
Login              UID   Auth Access  Enabled Reset    Exp Warn  Str Lock Max
admin             1000  Local Config  Enabled    No  Never  N/A  Dis   No N/A
johncrichton      1001  Local Config  Enabled    No  Never  N/A  Dis   No   5
```

注释
告知用户他们可以使用 **configure password** 命令更改自己的密码。

步骤 3 （可选） 根据安全要求调整该帐户的特性。

您可以使用以下命令更改默认帐户行为。

- **configure user aging** *username max_days warn_days*

  设置用户密码的到期日。指定密码最大有效天数，以及密码到期前向用户发出密码即将到期警告的天数。两个值均介于 1 到 9999 之间，但是警告天数必须小于最大天数。当您创建帐户时，密码没有到期日。

- **configure user forcereset** *username*

  强制用户下次登录时更改密码。

- **configure user maxfailedlogins** *username number*

  设置在锁定帐户之前您允许的最大连续失败登录次数，该值介于 1 至 9999 之间。使用 **configure user unlock** 命令解锁帐户。新帐户的默认值为 5 次连续失败登录。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。

- **configure user minpasswdlen** *username number*

  设置最小密码长度，此值介于 1 至 127 之间。

- **configure user strengthcheck** *username* {**enable** | **disable**}

  启用或禁用密码强度检查，此检查要求用户在更改密码时要满足特定的密码条件。如果用户密码到期或使用了 **configure user forcereset** 命令，则此要求会在用户下次登录时自动启用。

步骤 4 根据需要管理用户账号。

用户可能被锁定在帐户之外了，也可能您需要删除帐户或解决其他问题。使用以下命令管理系统中的用户账号。

- **configure user access** *username* {**basic** | **config**}

  更改用户账号的权限。

- **configure user delete** *username*

  删除指定的帐户。

- **configure user disable** *username*

  禁用指定的帐户，而不将其删除。用户无法登录，直到您启用该帐户为止。

- **configure user enable** *username*

  启用指定的帐户。

- **configure user password** *username*

  更改指定用户的密码。通常情况下，用户应使用 **configure password** 命令更改自己的密码。

  注意
  请不要在专家模式下使用 Linux **passwd** 命令更改管理员用户密码。此命令可能会导致文件系统损坏。仅使用常规的 Firewall Threat Defense CLI **configure user password admin** 命令（如果您不是管理员）或 **configure password** 命令（如果您是管理员）。如果您不知道密码并且根本无法登录，请参阅 密码恢复 程序。

- **configure user unlock** *username*

  解锁因超出最大连续失败登录尝试次数而被锁定的用户账号。

注释
Firewall Threat Defense使用可插拔身份验证模块 (PAM) 框架进行用户身份验证。在此框架中，pam_unix.so 模块使用 SHA-512 算法处理密码散列和验证。

密码使用 SHA-512 算法进行散列处理。

配置 FTD 的外部身份验证

要启用 FTD 设备的外部身份验证，您需要添加一个或多个外部身份验证对象。

关于Firewall Threat Defense外部身份验证

在为 Firewall Threat Defense 用户启用外部身份验证时，Firewall Threat Defense 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。

防火墙管理中心 和 Firewall Threat Defense 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。对于 Firewall Threat Defense，您智能在部署到设备的平台设置中激活一个外部身份验证对象。

注释 Firewall Threat Defense 和 防火墙管理中心 的超时范围不同，因此，如果共享对象，请确保不要超过 Firewall Threat Defense 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 Firewall Threat Defense 外部身份验证配置将不起作用。

只有外部身份验证对象中一个子集的字段可用于 Firewall Threat Defense SSH 访问。如果填入其他字段，它们将被忽略。如果对于其他设备类型也使用此对象，系统将使用这些字段。

LDAP 用户始终具有“配置”权限。RADIUS 用户可定义为“配置”或“基本”用户。

您可以在 RADIUS 服务器上（通过 Service-Type 属性）定义用户，也可以预定义外部身份验证对象中的用户列表。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 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。

Secure Firewall 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 Secure Firewall 设备上无需配置任何其他信息来支持 SecurID。

准则

- 默认 RADIUS 身份验证端口为 1812。
- 默认 RADIUS 记账端口为 1813（比 RADIUS 身份验证端口大 1）。

如果更改RADIUS身份验证端口，RADIUS 记账端口会相应更改。确保 防火墙管理中心 可以连接到新 RADIUS 服务器；否则，可能会出现认证延迟。

为 Firewall Threat Defense 添加 LDAP 外部身份验证对象

添加 LDAP 服务器以支持外部用户执行 Firewall Threat Defense 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。

共享外部身份验证对象

防火墙管理中心 和 Firewall Threat Defense 设备可使用外部 LDAP 对象。防火墙管理中心 和设备可共享同一个对象，也可以为它们创建不同的对象。确保即使您未共享对象，Firewall Threat Defense 和 防火墙管理中心 也都可以访问 LDAP 服务器。防火墙管理中心 对于检索用户列表并将其下载到设备至关重要。

注释 对于 LDAP，Firewall Threat Defense 和 防火墙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 Firewall Threat Defense的较小超时范围（1-30 秒）。如果将超时设置为更高的值，则到 Firewall Threat Defense 的部署将失败。

Firewall Threat Defense 支持的字段

只有 LDAP 对象中一个子集的字段可用于 Firewall Threat Defense SSH 访问。如果填入其他字段，它们将被忽略。如果您也将此对象用于 防火墙管理中心，则将使用这些字段。此程序仅涵盖 Firewall Threat Defense 支持的字段。有关其他字段，请参阅《*Cisco Secure Firewall Management Center* 管理指南》中的“为 防火墙管理中心 添加 LDAP 外部身份验证对象’ ”。

用户名

用户名必须是 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 (/)

不能为外部身份验证添加 **admin** 或 **sshd** 用户。

只能在防火墙管理中心添加外部用户（作为外部身份验证对象的一部分）；不能在CLI中添加他们。请注意，内部用户只能在 CLI 中添加，不能在防火墙管理中心添加。

如果您之前使用 **configure user add** 命令为内部用户配置过相同的用户名，则 Firewall Threat Defense 首先对照此内部用户检查密码，如果失败，再检查 LDAP 服务器。请注意，此后不能再将具有相同名称的内部用户添加为外部用户；仅支持以前存在的内部用户。

特权等级

LDAP 用户始终具有“配置”权限。

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。请参阅在 CLI 中修改 Firewall Threat Defense 管理接口来添加 DNS 服务器。

过程

步骤 1 选择**管理** > **用户**。

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**。

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 (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)`。

要检索所有 cn 名称（禁止的用户 admin 和 sshd 除外），请输入 `(&(cn=*)(!(|(cn=sshd)(cn=admin)))`。

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。

  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。对于 SSL，Firewall Threat Defense 同样要求有证书。对于其他平台，SSL 不要求有证书。但我们建议您始终上传 SSL 证书以防中间人攻击。

- （未使用）**用户名模板** - Firewall Threat Defense 未使用。
- **超时（秒）**-输入滚动到备份连接之前等待的秒数（1-30 秒）。默认值为 30。

  注释
  Firewall Threat Defense 和 防火墙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 Firewall Threat Defense的较小超时范围（1-30 秒）。如果将超时设置为更高的值，则 Firewall Threat Defense LDAP 配置将不起作用。

步骤 11 配置**属性映射 (Attribute Mapping)** 以基于属性检索用户。

- 输入 **UI 访问属性 (UI Access Attribute)**。**注意**：此字段不用于设备 CLI 访问；但是，它是必填字段，因此您需要输入一个值。您可以输入与为 **CLI 访问属性**输入的值相同的值。
- 如果要使用用户可分辨类型之外的 CLI 访问属性，请设置 **CLI 访问属性**。例如，在 Microsoft 活动目录服务器上，通过键入 `sAMAccountName`可使用 `sAMAccountName` 外壳 CLI 访问属性来检索外壳访问用户。

  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。请确保限制具有 CLI 或 Linux 外壳访问的用户列表。

  注释
  部署允许大量具有 CLI 访问权限的用户的外部身份验证对象可能会导致部署超时并在等待创建用户时失败。

步骤 12 设置 **CLI 访问过滤器**。

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)`。

有关用户名准则，请参阅此程序之前的用户名。

步骤 13 点击**保存**。

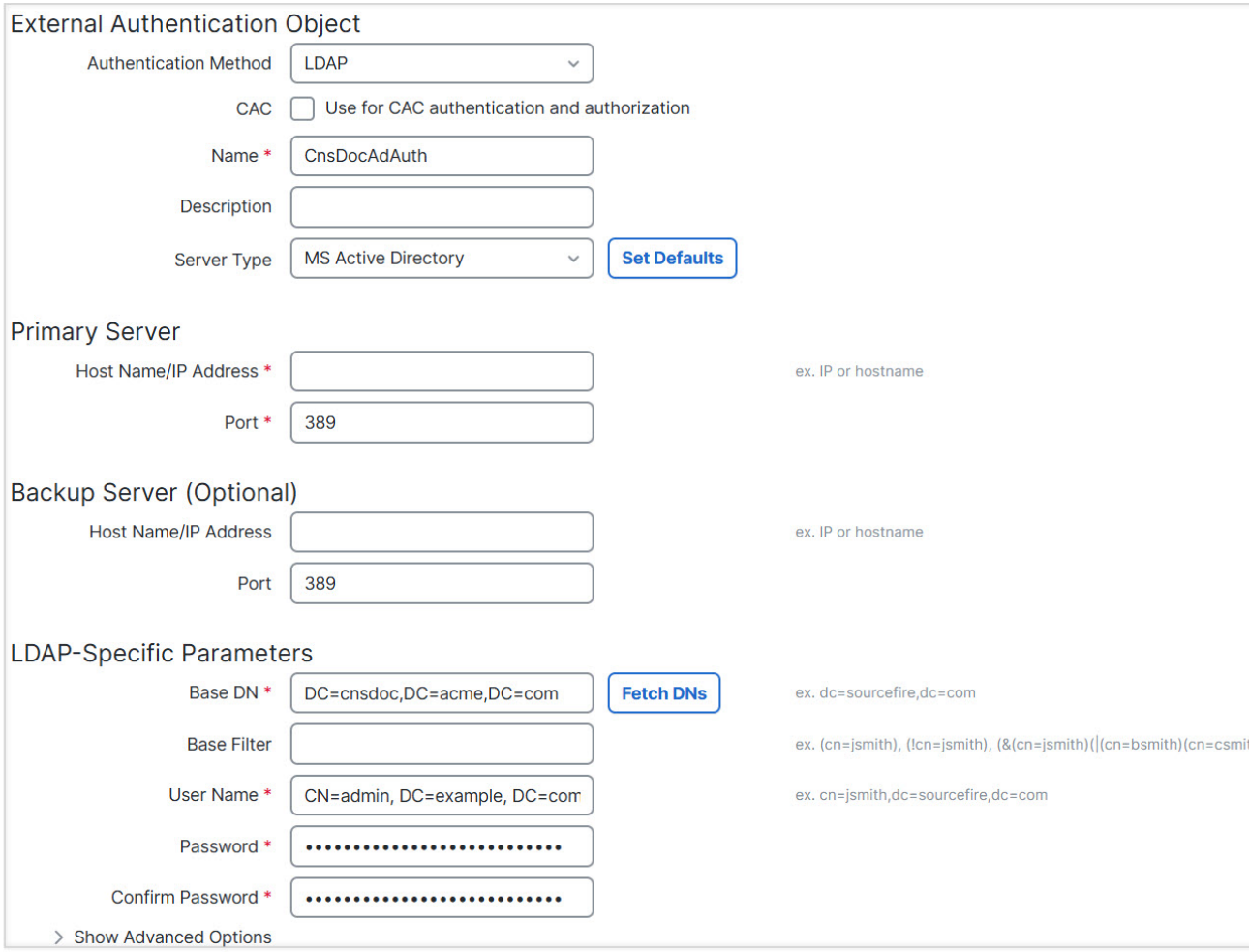
步骤 14 启用此服务器。请参阅外部身份验证。

步骤 15 如果以后在 LDAP 服务器上添加或删除用户，必须在托管设备上重新部署“平台设置”。防火墙管理中心 会重新下载用户列表并将其部署到设备。请参阅部署配置更改。

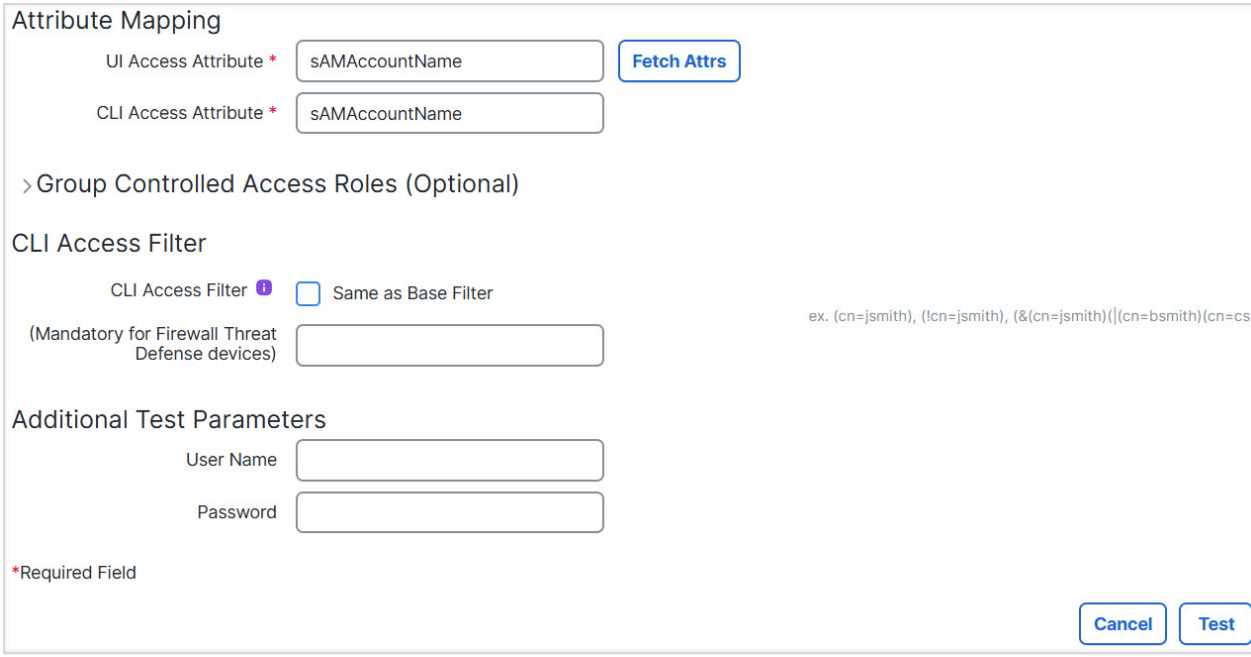
示例

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。

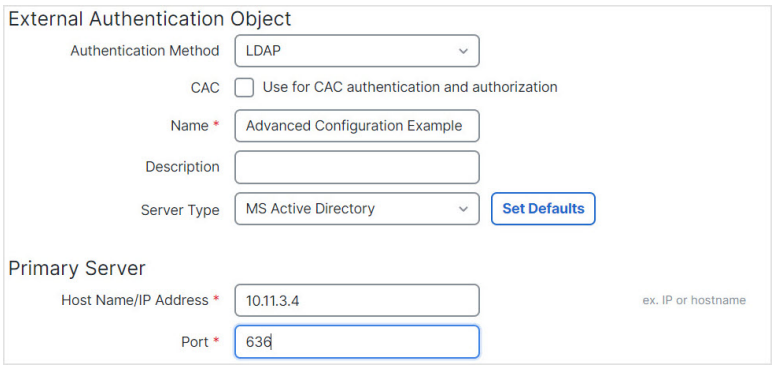


当用户登录 Firewall Threat Defense 时，`sAMAccountName` 的 **CLI 访问属性**会导致检查目录中所有对象的 `sAMAccountName` 属性以查找匹配项。

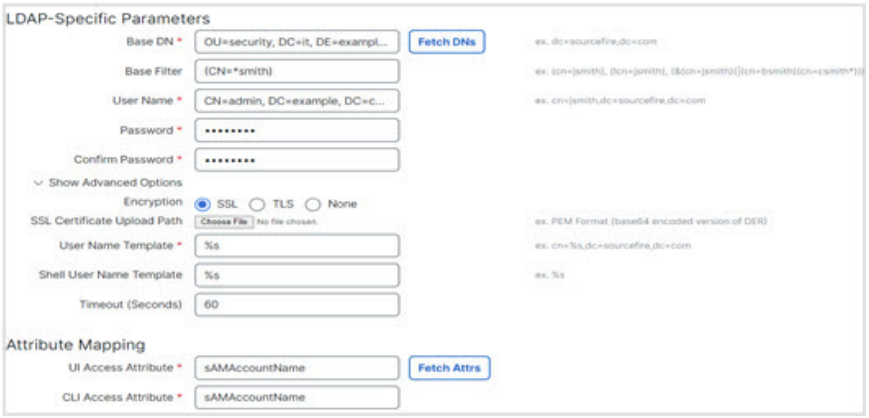
请注意，由于未对此服务器应用基本过滤器，因此 Firewall Threat Defense 会检查目录中基本可分辨名称所指示的所有对象的属性。经过默认时间段（或 LDAP 服务器上设置的超时期）后，与服务器的连接将超时。

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。

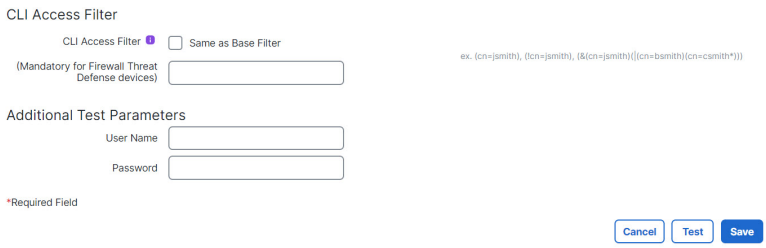


与服务器的连接使用 SSL 进行加密，并且会为该连接使用一个名为 `certificate.pem` 的证书。此外，由于 **超时（秒）** 设置，与服务器的连接在 60 秒后将超时。

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。

当用户登录 Firewall Threat Defense 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。

在以下示例中，CLI 访问过滤器设置为与基本过滤器相同。



为 Firewall Threat Defense 添加 RADIUS 外部身份验证对象

添加 RADIUS 服务器以支持外部用户进行Firewall Threat Defense。

共享外部身份验证对象

防火墙管理中心 和设备可共享同一个对象，也可以为它们创建不同的对象。请注意，Firewall Threat Defense 支持在 RADIUS 服务器上定义用户，而 防火墙管理中心 要求您在外部身份验证对象中预定义用户列表。您可以选择针对 Firewall Threat Defense使用预定义列表方法，但如果要在 RADIUS 服务器上定义用户，则必须为 Firewall Threat Defense 和 防火墙管理中心创建单独的对象。

注释 Firewall Threat Defense 和 防火墙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 Firewall Threat Defense 的较小超时范围（1-300 秒）。如果将超时设置为更高的值，则 Firewall Threat Defense RADIUS 配置将不起作用。

Firewall Threat Defense 支持的字段

只有 RADIUS 对象中一个子集的字段可用于 Firewall Threat Defense SSH 访问。如果填入其他字段，它们将被忽略。如果您也将此对象用于防火墙管理中心，则将使用这些字段。此程序仅涵盖 Firewall Threat Defense 支持的字段。有关其他字段，请参阅*Cisco Secure Firewall Management Center* 管理指南中的为 防火墙管理中心 添加 RADIUS 外部身份验证对象。

用户名

不能为外部身份验证添加**管理员**用户。只能在防火墙管理中心添加外部用户（作为外部身份验证对象的一部分）；不能在 CLI 中添加他们。请注意，内部用户只能在 CLI 中添加，不能在防火墙管理中心添加。

如果您之前使用 **configure user add** 命令为内部用户配置过相同的用户名，则 Firewall Threat Defense 首先对照此内部用户检查密码，如果失败，再检查 RADIUS 服务器。请注意，此后不能再将具有相同名称的内部用户添加为外部用户；仅支持以前存在的内部用户。对于 RADIUS 服务器上定义的用户，请务必将权限级别设置为与任何内部用户相同的权限级别；否则您无法使用外部用户密码登录。

过程

步骤 1 使用 Service-Type 属性在 RADIUS 服务器上定义用户。

以下是受支持的 Service-Type 属性值：

- 管理员 (6) - 提供 CLI 的配置访问授权。这些用户可以在 CLI 中使用所有命令。
- NAS 提示 (7) 或除级别 6 以外的任何级别 - 提供 CLI 的基本访问授权。这些用户可以使用只读命令，例如**show**命令，用于监控和故障排除。

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；不能包含符号 (@) 或斜线 (/)

或者，您可以在外部身份验证对象中预定义用户（参见步骤 12，第 14 页）。要在为 Firewall Threat Defense使用 Service-Type 属性的同时对 Firewall Threat Defense 和 防火墙管理中心 使用相同的 RADIUS 服务器，请创建可识别相同 RADIUS 服务器的两个外部身份验证对象：其中一个对象包括预定义的 **CLI 访问过滤器** 用户（用于 防火墙管理中心），另一个对象则将 **CLI 访问过滤器** 留空（用于 Firewall Threat Defense）。

步骤 2 在 防火墙管理中心上，选择 **管理** > **用户**。

步骤 3 点击**外部身份验证 (External Authentication)**。

步骤 4 点击 (+)**添加外部身份验证对象 (Add External Authentication Object)**。

步骤 5 将**身份验证方法**设置为 **RADIUS**。

步骤 6 输入**名称**和可选**说明**。

步骤 7 对于**主服务器**，输入**主机名/IP 地址**。

仅支持 IPv4。

注释
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。

步骤 8 （可选） 更改**端口**使用的默认值。

步骤 9 输入 **RADIUS 服务器密钥**。

步骤 10 （可选） 输入**备份服务器**参数。

步骤 11 （可选） 输入 **RADIUS 特定参数**。

a) 在**超时（秒）** 中输入重试主服务器之前允许的秒数（介于 1 和 300 之间）。默认值为 30。

注释
Firewall Threat Defense 和 防火墙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 Firewall Threat Defense 的较小超时范围（1-300 秒）。如果将超时设置为更高的值，则 Firewall Threat Defense 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。

步骤 12 （可选） 不要使用 RADIUS 定义的用户（请参阅 步骤 1，第 13 页），在 **CLI 访问过滤器 (CLI Access Filter)** 区域**管理员 CLI 访问用户列表 (Administrator CLI Access User List)** 字段中，输入应具有 CLI 访问权限的用户名并以逗号分隔。例如，输入 **`jchrichton`**、**`aerynsun`**、**`rygel`**。

您可能想要使用 Firewall Threat Defense 的 **CLI 访问过滤器** 方法以便对 Firewall Threat Defense 和其他平台类型使用相同的外部身份验证对象。

注释
如果想要使用 RADIUS 定义的用户，则必须将 **CLI 访问过滤器 (CLI Access Filter)** 留空。

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 (/)

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
部署允许大量具有 CLI 访问权限的用户的外部身份验证对象可能会导致部署超时并在等待创建用户时失败。

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

此功能只能测试 防火墙管理中心 与 RADIUS 服务器的连接；没有用于托管设备与 RADIUS 服务器的连接的测试功能。

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**。

步骤 16 启用此服务器。请参阅 外部身份验证

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。

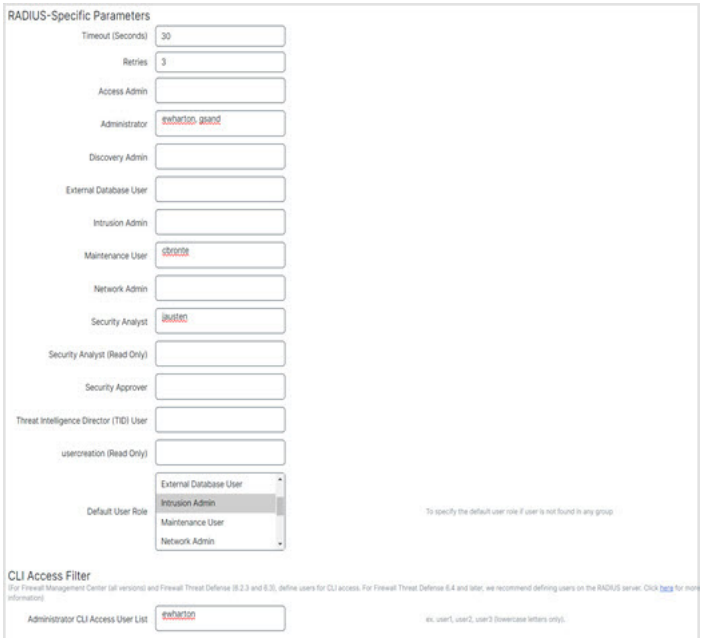
此示例说明 RADIUS 用户角色配置的重要方面：

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。



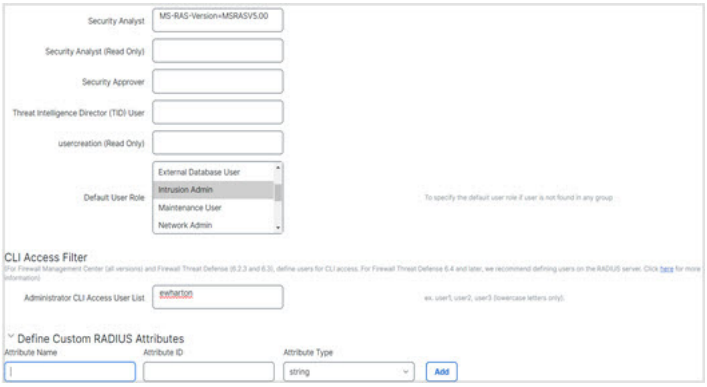
下图说明示例的角色配置：

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 FTD 设备上的用户启用外部身份验证

在 Firepower 威胁防御平台设置中启用“外部身份验证”(External Authentication)，然后将这些设置部署到托管设备。有关详细信息，请参阅外部身份验证。

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。
  - 配置 LDAP 身份验证时，请避免在绑定密码中使用反斜线（“\”）。密码中存在反斜线会导致 LDAP 绑定过程失败，从而导致外部身份验证失败。
- 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。防火墙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。

CLI 用户的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
威胁防御CLI基本用户的有限用户权限。	7.7.0	7.7.0	威胁防御 CLI 基本用户权限的范围现在仅限于以下命令：dig、ping、traceroute。如果创建的用户具有基本权限，请评估是否需要将其更改为配置权限。您可以使用 **configure user access** 命令来更改用户的权限级别。 请参阅： *Cisco Secure Firewall Threat Defense 命令参考*
对RADIUS服务器上定义的 Firewall Threat Defense用户的 Service-Type 属性的支持。	6.4.0	任意	对于 Firewall Threat Defense CLI 用户的 RADIUS 身份验证，以往，您须预定义RADIUS外部身份验证对象中的用户名，且须手动确保该列表匹配 RADIUS 服务器上定义的用户名。现在，您可以使用 Service-Type 属性在 RADIUS 服务器上定义 CLI 用户，亦可同时定义“基本”和“配置”用户角色。要使用此方法，请务必将外部身份验证对象中的外壳访问过滤器留空。 新增/修改的屏幕：**系统** > **用户** > **外部身份验证** > **添加外部身份验证对象** > **外壳访问筛选器**
用于 Firewall Threat Defense SSH 访问的外部身份验证。	6.2.3	任意	现在，您可以配置外部身份验证以便对使用 LDAP 或 RADIUS 的 Firewall Threat Defense进行 SSH 访问。 新增/修改的屏幕：**设备 (Devices)** > **平台设置 (Platform Settings)** > **外部身份验证 (External Authentication)**

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。

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。

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。