登录到管理中心

以下主题介绍如何登录 Firepower 系统：

用户账户

您必须提供用户名和密码才能访问 防火墙管理中心 或托管设备的 Web 接口或 CLI。在托管设备上，具有配置层级访问权限的 CLI 用户可以使用 专家 命令访问 Linux 外壳程序。在 防火墙管理中心 上，所有 CLI 用户都可以使用 专家 命令。 和 防火墙管理中心 可配置为使用外部身份验证，将用户凭证存储在外部 LDAP 或 RADIUS 服务器上；您可以保留或向外部用户提供 CLI 访问权限。 防火墙管理中心 可以配置为使用符合安全断言标记语言 (SAML) 2.0 开放式身份验证和授权标准的任何 SSO 提供程序支持单点登录 (SSO)。

防火墙管理中心CLI 提供一个有权访问所有命令的 **admin** 用户。 用户可以访问的 防火墙管理中心 Web 接口功能由管理员授予用户账户的权限控制。在托管设备上，用户可以访问 CLI 和 Web 接口的功能由管理员授予用户账号的权限控制。

注释 系统根据用户账号审核用户活动；请确保用户使用正确的账户登录系统。

注意 在托管设备上，所有 防火墙管理中心 CLI 用户和具有配置层 CLI 访问权限的用户可以在外壳程序中获取 root 权限，这可能构成安全风险。出于系统安全原因，我们强烈建议：

- 如果您建立外部身份验证，请确保对具有 CLI 访问权限的用户列表进行适当的限制。
- 在托管设备上授予 CLI 访问权限时，请显示具有配置层 CLI 访问权限的内部用户列表。
- 不建立 Linux 外壳用户；仅使用预定义的 **管理员** 用户和 **管理员** 用户在 CLI 中创建的用户。

注意 强烈建议您不要使用 Linux Shell，除非 Cisco TAC 或 Cisco Secure Firewall 用户文档明确说明需要这样做。

不同的设备支持不同类型的用户帐户，每个帐户都具有不同的功能。

Cisco Secure Firewall Management Centers

Cisco Secure Firewall Management Center 支持以下用户帐户类型：

- 用于 Web 界面访问的预定义 **admin** 帐户具有管理员角色，可以通过 Web 界面进行管理。
- 自定义用户账户，**admin** 用户和具有管理员权限的用户可以创建和管理此类账户。
- 预先定义 CLI 访问的 **admin** 账户。使用此账户登录的用户可以使用 专家 命令以获得访问 Linux 外壳的权限。

  在初始配置期间，CLI **admin** 账户和 Web 接口 **admin** 账户的密码会同步，但此后您可以为两个 **admin** 账户配置单独的密码。

注意 出于系统安全原因，思科强烈建议您不要在任何设备上建立其他 Linux 外壳用户。

Cisco Secure Firewall Threat Defense 和 Cisco Secure Firewall Threat Defense Virtual 设备

Cisco Secure Firewall Threat Defense 和 Cisco Secure Firewall Threat Defense Virtual 设备支持以下用户帐户类型：

- 预先定义的 **admin** 帐户，可用于对设备进行任何形式的访问。
- 自定义用户账户，**admin** 用户和具有“配置”访问权限的用户可以创建和管理此类账户。

Cisco Secure Firewall Threat Defense支持对 SSH 用户进行外部身份验证。

系统用户界面

根据设备类型，可以使用基于 Web 的 GUI、辅助 CLI 或 Linux 外壳与设备交互。在 Cisco Secure Firewall Management Center 部署中，可从 防火墙管理中心的 GUI 执行从大多数配置任务。只有少数任务需要使用 CLI 或 Linux 外壳直接访问设备。我们强烈不鼓励您使用 Linux 外壳，除非 Cisco TAC 或用户文档明确说明需要这样做。

有关浏览器要求的信息，请参阅Cisco Secure Firewall 版本说明。

注释 在所有设备上，当用户连续三次尝试通过 SSH 登录 CLI 失败时，系统会终止 SSH 连接。

设备	基于 Web 的 GUI	辅助 CLI	Linux Shell
Cisco Secure Firewall Management Center	• 支持预定义的 **管理员** 用户和自定义用户账号。 • 可用于管理和分析任务。	• 支持预定义的 **管理员** 用户和自定义外部用户账号。 • 可通过 SSH、串行或键盘和显示器连接进行访问。 • 仅应用于思科 TAC 指导的管理和故障排除。	• 支持预定义的 **admin** 用户。 • 必须通过 Cisco Secure Firewall Management Center CLI 中的 `expert` 命令进行访问。 • 可通过 SSH、串行或键盘和显示器连接进行访问。 • 仅应用于思科 TAC 指导的管理和故障排除，或防火墙管理中心 文档中的详细指导。
Cisco Secure Firewall Threat Defense Cisco Secure Firewall Threat Defense Virtual	—	• 支持预定义的 **管理员** 用户和自定义用户账号。 • 可通过 SSH、串行或键盘和显示器连接在物理设备中进行访问。可通过 SSH 或虚拟机控制台进行访问。 • 可用于思科 TAC 指导的安装和故障排除。	• 支持预定义的 **管理员** 用户和自定义用户账号。 • 具有“配置”权限的CLI用户可使用 `expert` 命令访问。 • 仅应用于思科 TAC 指导的管理和故障排除，或防火墙管理中心 文档中的详细指导。

相关主题

添加或编辑内部用户

Web 界面注意事项

- 如果您的组织使用通用访问卡 (CAC) 进行身份验证，通过 LDAP 进行身份验证的外部用户可以使用 CAC 凭证获得对设备 Web 接口的访问权限。
- 在默认主页顶部显示的菜单和菜单选项取决于用户帐户的权限。但是，默认主页上的链接包括适用于各种用户帐户权限范围的选项。如果点击的链接所需的权限与已授予帐户的权限不同，系统将显示警告消息并记录相关活动。
- 某些进程耗时较长，这可能会导致网络浏览器显示指明脚本无响应的消息。如果出现这种情况，请确保允许脚本继续运行，直至完成。

相关主题

指定主页

会话超时

默认情况下，除非您以其他方式配置为免除会话超时，否则在不活动达 1 小时之后系统会自动将您从会话中注销。

注释 对于 SSO 用户，当 防火墙管理中心 会话超时时，显示内容会短暂重定向到 IdP 接口，然后是 防火墙管理中心 登录页面。除非已从其他位置终止 SSO 会话，否则任何人只需点击登录页面上的 **单点登录** 链接即可访问 防火墙管理中心，而无需提供登录凭证。为确保 防火墙管理中心 安全并防止其他人使用您的 SSO 账户访问 防火墙管理中心，我们建议您在注销 防火墙管理中心时不要让 防火墙管理中心 登录会话处于无人参与状态，并在 IdP 上注销 SSO 联合。

具有“管理员”(Administrator) 角色的用户可以通过以下设置更改设备的会话超时间隔：

系统 > 配置 > 外壳超时

相关主题

配置会话超时
配置 SAML 单点登录

登录到 Cisco Secure Firewall Management Center Web 界面

注释 此任务适用于通过 LDAP 或 RADIUS 服务器进行身份验证的内部用户和外部用户。有关 SSO 登录，请参阅 使用 SSO 登录防火墙管理中心 Web 接口，第 5 页。

用户受限于单个活动会话。如果您尝试通过已具有活动会话的用户账号登录，则系统会提示您终止另一会话或以另一个用户的身份登录。

在多个防火墙管理中心共享同一 IP 地址的 NAT 环境中：

- 每个防火墙管理中心只能支持一个登录会话。
- 要访问不同的防火墙管理中心，请为每次登录使用不同的浏览器（例如 Firefox 和 Chrome），或将浏览器设置为隐身或隐私模式。

开始之前

- 如果您无法访问网络界面，请联系系统管理员修改您的帐户权限，或者用具有管理员访问权限的用户身份登录并修改帐户的权限。
- 按照添加或编辑内部用户所述创建用户帐户。

过程

步骤 1 将浏览器定向到 **https://***ipaddress_or_hostname***/**，其中 *ipaddress* 或 *hostname* 对应您的防火墙管理中心。

步骤 2 在**用户名 (Username)** 和**密码 (Password)** 字段中，输入用户名和密码。请注意以下准则：

- 用户名不区分大小写。
- 在多域部署中，请在用户名前面附加在其中创建用户帐户的子域。您无需指定全局域。例如，如果您的用户账户是在 SubdomainA 中创建的，请按以下格式输入您的用户名：

  ```
  SubdomainA\username
  ```

  如果您的用户已添加到父域为 SubdomainA 的 SubdomainB，请按以下格式输入用户名：

  ```
  SubdomainA\SubdomainB\username
  ```

- 如果您的组织在登录时使用 SecurID® 令牌，请将令牌附加到 SecurID PIN，并将其用作密码进行登录。例如，如果 PIN 为 `1111` 且 SecurID 令牌为 `222222`，请输入 `1111222222`。必须生成 SecurID PIN 后才能登录系统。

步骤 3 点击**登录 (Login)**。

相关主题

会话超时，第 4 页

使用 SSO 登录防火墙管理中心 Web 接口

防火墙管理中心可以配置为参与符合安全断言标记语言 (SAML) 2.0 开放标准的 SSO 提供程序实施的任何单点登录 (SSO) 联合。SSO 用户账户必须在身份提供程序 (IdP) 上建立，并且必须使用邮件地址作为其账户名称。如果您的用户名不是邮件地址，或者 SSO 登录失败，请联系您的系统管理员。

注释 防火墙管理中心不支持使用 SSO 账户的 CAC 凭证登录。

用户受限于单个活动会话。如果您尝试通过已具有活动会话的用户账号登录，则系统会提示您终止另一会话或以另一个用户的身份登录。

在多个防火墙管理中心共享同一 IP 地址的 NAT 环境中：

- 每个防火墙管理中心只能支持一个登录会话。
- 要访问不同的防火墙管理中心，请为每次登录使用不同的浏览器（例如 Firefox 和 Chrome），或将浏览器设置为隐身或隐私模式。

开始之前

- 为 SSO 访问配置防火墙管理中心。请参阅配置 SAML 单点登录。
- 如果您无权访问 Web 界面，请联系系统管理员以在 SSO IdP 上配置您的账户。

过程

步骤 1 将浏览器定向到 **https://***ipaddress_or_hostname/*，其中 *ipaddress* 或 *hostname* 对应您的防火墙管理中心。

注释
SSO 用户必须使用专门为 SSO 访问配置的登录 URL 进行一致的访问防火墙管理中心；请向管理员咨询此信息。

步骤 2 点击**单点登录 (Single Sign-On)** 链接。

步骤 3 系统以以下两种方式之一进行响应：

- 如果您已登录 SSO 联合， 防火墙管理中心显示默认主页。
- 如果您尚未登录 SSO 联合， 防火墙管理中心 会将您的浏览器重定向到 IdP 的登录页面。在 IdP 完成登录过程后， 防火墙管理中心 显示默认主页。

相关主题

会话超时 ， 第 4 页
配置 SAML 单点登录

使用 CAC 凭证登录 Cisco Secure Firewall Management Center

用户受限于单个活动会话。如果您尝试通过已具有活动会话的用户账号登录，则系统会提示您终止另一会话或以另一个用户的身份登录。

在多个防火墙管理中心共享同一 IP 地址的 NAT 环境中：

- 每个防火墙管理中心只能支持一个登录会话。
- 要访问不同的防火墙管理中心，请为每次登录使用不同的浏览器（例如 Firefox 和 Chrome），或将浏览器设置为隐身或隐私模式。

注意 在浏览会话活动期间，**请勿**删除 CAC。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 Web 界面。

开始之前

- 如果您无法访问网络界面，请联系系统管理员修改您的帐户权限，或者用具有管理员访问权限的用户身份登录并修改帐户的权限。
- 创建用户账号，如 添加或编辑内部用户中所述。
- 配置 CAC 身份验证和授权，如 使用 LDAP 配置通用访问卡身份验证中所述。

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 防火墙管理中心。

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 点击**继续**。

相关主题

使用 LDAP 配置通用访问卡身份验证
会话超时，第 4 页
防火墙管理中心的 SSO 指南

登录防火墙管理中心命令行接口

管理员 CLI 用户和某些自定义外部用户可以登录 防火墙管理中心 CLI。

注意 强烈建议您不要使用 Linux 外壳，除非 Cisco TAC 或 防火墙管理中心 文档明确说明需要这样做。

注释 对于所有设备上，当用户连续三次尝试通过 SSH 登录 CLI 失败时，系统会终止 SSH 连接。

开始之前

以 **管理员** 用户身份完成初始配置过程。请参阅首次登录。

过程

步骤 1 使用 **管理员** 用户名和密码通过 SSH 或控制台端口连接到 防火墙管理中心 。

如果您的组织在登录时使用 SecurID® 令牌，请将令牌附加到 SecurID PIN，并将其用作密码进行登录。例如，如果 PIN 为 `1111` 且 SecurID 令牌为 `222222`，请输入 `1111222222`。必须生成 SecurID PIN 后才能登录 。

步骤 2 使用任何可用的 CLI 命令。

查看您的上次登录

如果您怀疑未经授权的用户使用您的凭证登录 Cisco Secure Firewall Management Center，您可以查看上次使用您的凭证登录的日期、时间和 IP 地址：

过程

步骤 1 登录到 Cisco Secure Firewall Management Center。

步骤 2 在浏览器窗口的右上角，查找用于登录的用户 ID。

步骤 3 点击您的用户名。

步骤 4 有关上次登录的信息显示在所显示菜单的底部。

注销 Firepower 系统 Web 界面

不再使用 Firepower 系统 Web 界面时，思科建议您注销，即使只是暂时离开 Web 浏览器。注销会结束您的 Web 会话并确保没有人可以通过您的凭证使用界面。

注释 如果您要注销防火墙管理中心上的SSO会话，当您注销时，系统会将您的浏览器重定向到您的组织的 SSO IdP。为确保 防火墙管理中心 安全并防止其他人使用您的 SSO 账户访问 防火墙管理中心，我们建议您在 IdP 处注销 SSO 联合。

过程

步骤 1 从用户名下的下拉列表中，选择**注销 (Logout)**。

步骤 2 如果您要注销 防火墙管理中心上的 SSO 会话，系统会将您重定向到您的组织的 SSO IdP。在 IdP 上注销以确保 防火墙管理中心 安全。

相关主题

会话超时，第 4 页

登录管理中心的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
添加了对使用任何符合 SAML 2.0 的 SSO 提供程序的单点登录 (SSO) 的支持。	6.7	任意	为在任何第三方 SAML 2.0 兼容身份提供程序 (IdP) 上配置的用户添加了新功能，可以使用登录页面上的新 **单点登录** 链接登录 防火墙管理中心。 新的/修改后的屏幕： 登录屏幕
查看有关您上次登录 Cisco Secure Firewall Management Center的信息	6.5	任意	查看您上次登录的日期、时间和 IP 地址。 新增/修改的菜单： 窗口右上角的菜单，显示您用于登录的用户名。 支持的平台： 防火墙管理中心

功能	防火墙管理中心最低版本	最低版本	详细信息
自动CLI访问 防火墙管理中心	6.5	任意	使用 SSH 登录 防火墙管理中心时，会自动访问 CLI。虽然强烈建议不要这样做，但您可以使用 CLI 专家 命令访问 Linux 外壳程序。 **注释** 此功能弃用了为 防火墙管理中心启用和禁用CLI访问的版本6.3。由于弃用此选项，虚拟 防火墙管理中心 不再显示 **系统** > **配置** > **控制台配置** 页面，该页面仍显示在物理 防火墙管理中心上。
限制SSH登录失败次数	6.3	任意	当用户通过SSH访问任何设备并连续三次尝试登录失败时，设备会终止SSH 会话。
能启用和禁用CLI访问权限 防火墙管理中心	6.3	任意	新增/修改的屏幕： 防火墙管理中心 Web 界面中对管理员可用的新复选框：在**系统**> **配置**> **控制台配置**页面上**启用 CLI 访问**。 • 选中：使用 SSH 登录 防火墙管理中心可访问 CLI。 • 取消选中：使用 SSH 登录 防火墙管理中心可访问 Linux 外壳。此为全新的 6.3 版本以及以往版本至 6.3 版本升级的默认状态。 支持的平台： 防火墙管理中心

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。