设备管理

TACACS+ 设备管理

Cisco ISE 支持设备管理通过使用终端访问控制器访问控制系统 (TACACS+) 安全协议控制，来控制和审计网络设备的配置。网络设备可以配置为向Cisco ISE 查询对设备管理员操作所进行的身份验证和授权，并发送Cisco ISE 的记账信息以记录操作。它可以促进对谁可以访问哪个网络及更改关联网络设置进行精细控制。Cisco ISE 管理员可以创建策略集，允许在设备管理访问服务的授权策略规则中选择 TACACS 结果（如命令集和外壳配置文件）。Cisco ISE 监控节点可提供与设备管理相关的增强型报告。“工作中心”(Work Center) 菜单中包含所有设备管理页面，可作为 ISE 管理员的单一入手点。

Cisco ISE 需要设备管理许可证才能使用 TACACS+。

设备管理中存在两种类型的管理员

- 设备管理员
- Cisco ISE 管理员

设备管理员是指登录到交换机、无线接入点、路由器和网关（一般通过 SSH）等网络设备以执行对所管理设备进行配置和维护的用户。Cisco ISE 管理员可登录Cisco ISE，配置并协调设备管理员所登录的设备。

Cisco ISE 管理员是本文档的目标读者，他们可登录Cisco ISE 以配置相应的设置，控制设备管理员的操作。Cisco ISE 管理员使用设备管理功能（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**工作中心 (Work Centers) > 设备管理 (Device Administration)**）来控制和审核网络设备的配置。设备可配置为使用终端访问控制器访问控制系统 (TACACS) 安全协议来查询Cisco ISE 服务器。Cisco ISE 监控节点可提供与设备管理相关的增强型报告。Cisco ISE 管理员可以执行以下任务：

- 配置带有 TACACS+ 详细信息（共享密钥）的网络设备。
- 添加设备管理员为内部用户，并根据需要为其设置启用密码。
- 创建策略集，这些策略集可使得 TACACS 结果（例如，命令集和 shell 配置文件）被选中到设备管理访问服务中的的授权策略规则中。
- 在Cisco ISE 中配置 TACACS 服务器，允许设备管理员基于策略集来访问设备。

设备管理员负责设置设备以与Cisco ISE 服务器进行通信。当设备管理员登录到设备时，设备将查询Cisco ISE 服务器，后者进而查询内部或外部身份存储区，以验证设备管理员的详细信息。当Cisco ISE 服务器完成验证后，设备将通知Cisco ISE 服务器每个会话或用于记账和审核的命令授权操作的最终结果。

Cisco ISE 管理员可以使用 TACACS 和Cisco ISE 2.0 及更高版本来进行设备管理。与设备管理相关的配置也可以从Cisco安全访问控制系统 (ACS) 服务器5.5、5.6、5.7 和 5.8 中迁移。更早期的版本需在迁移之前升级到版本 5.5 或 5.6。

注释 您应选中**管理 (Administration)** > **系统 (System)** > **部署 (Deployment)** > **常规设置 (General Settings)** 页面中的**启用设备管理服务 (Enable Device Admin Service)**，以便启用 TACACS+ 操作。确保部署中每个 PSN 都启用了此选项。

由于已知会限制 TACACS+ 协议在交换机或路由器与思科 ISE 之间创建安全连接，因此，请确保在双方之间部署 IPsec 协议。

ISE 社区资源

有关设备管理属性的信息，请参阅 ISE 设备管理属性。

有关无线局域网控制器、IOS 网络设备、Cisco NX-OS 网络设备和网络设备的 TACACS+ 配置信息，请参阅 ISE 设备管理 (TACACS +)。

设备管理工作中心

“工作中心”(Work Center) 菜单中包含所有设备管理页面，可以作为Cisco ISE 管理员的单一入手点。然而，未指定用于设备管理的页面（例如，“用户”(Users)、“用户身份组”(User Identity Groups)、“网络设备”(Network Devices)、“默认网络设备”(Default Network Devices)、“网络设备组”(Network Device Groups)、“身份验证”(Authentication) 和“授权条件”(Authorization Conditions)）依然可从其原始菜单选项（例如，“管理”(Administration)）访问。仅在获得并安装了正确的 TACACS+ 许可证后，“工作中心”(Work Centers) 选项才可用。

“设备管理菜单”(Device Administration Menu) 包含了以下菜单选项：“概述”(Overview)、“身份”(Identitie)、“用户身份组”(User Identity Groups)，“外部 ID 存储”(Ext ID Stores)、“网络资源”(Network Resources)，“网络设备组”(Network Device Groups)，“策略元素”(Policy Elements)、“设备管理策略集”(Device Admin Policy Sets)、“报告”(Reports) 和“设置”(Settings)。

设备管理部署设置

“设备管理部署”(Device Administration Deployment) 页面（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **概述 (Overview)** > **部署 (Deployment)**）可供Cisco ISE 管理员集中查看设备管理系统，而无需参考部署部分中的每个节点。

“设备管理部署”(Device Administration Deployment) 页面列出了部署中的 PSN。这简化了在部署中的每个节点中单独启用设备管理服务的任务。您可以通过选择以下任一选项为多个 PSN 集中启用设备管理服务：

选项	说明
无	默认情况下，所有节点的设备管理服务为禁用状态。
所有策略服务节点 (All Policy Service Nodes)	启用所有节点的设备管理服务。通过该选项，在添加新 PSN 时，其设备管理将自动启用。
指定节点 (Specific Nodes)	显示“ISE 节点”(ISE Nodes) 部分，其中列出了部署中的所有节点。您可以选择需要启用设备管理服务的节点。

注释 如果部署未许可用于 TACACS+，以上选项均为禁用状态。

通过“TACACS 端口”(TACACS Ports) 字段，您可以输入最多 4 个 TCP 端口，它们使用逗号隔开，并且端口值范围为 1 至 65535。Cisco ISE 节点及其接口通过指定端口侦听 TACACS+ 请求，而且您需要确保其他服务未使用该指定端口。默认 TACACS+ 端口值为 49。

当您点击**保存 (Save)** 时，所做更改同步到以下位置中指定的节点： **管理 (Administration)** > **系统 (System)** > **部署列表 (Deployment Listing)** 窗口。

设备管理策略集

“设备管理策略集”(Device Admin Policy Sets) 窗口（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **“设备管理”(Device Administration)** > **“设备管理策略集”(Device Admin Policy Sets)**）包含了Cisco ISE 管理员用于控制 TACACS+ 设备管理员的身份验证和授权的策略集列表。每个策略可以为两种模式中的一种：常规和代理顺序模式。

常规策略集包括一个身份验证规则表和一个授权规则表。身份验证规则表包含一组规则，用于选择对网络设备进行身份验证所需的操作。

这些授权规则表由一组规则组成，这些规则用于选择要实施授权业务模式所需的特定授权结果。每个授权规则都包含一个或多个条件（匹配时才能使用该规则）、一组命令集和/或一个外壳配置文件，选中后即可控制授权过程。每个规则表有一个可在特定条件下覆盖这些规则的例外策略，通常在临时情况下使用。

注释 不支持 TACACS + CHAP 出站身份验证。

一个代理策略集包含单个的所选代理顺序。如果策略集处于此模式，则使用一个或多个远程代理服务器处理请求（虽然本地计费可由代理顺序进行配置）。

创建设备管理策略集

创建设置的设备管理策略集：

开始之前

- 确保为 TACACS+ 操作启用**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **概述 (Overview)** > **部署 (Deployment)** 窗口中的“设备管理”(Device Administration)。
- 确保创建策略所需的用户身份组（例如，System_Admin、帮助台）。（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **用户身份组 (User Identity Groups)** 页面）。确保将成员用户（例如，ABC、XYZ）分配给其对应的组。（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **身份 (Identities)** > **用户 (Users)** 窗口）。
- 确保在需要管理的设备上配置 TACACS 设置。（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add)** > **TACACS 身份验证设置 (TACACS Authentication Settings)** 复选框已启用，并且用于 TACACS 和设备的共享密钥相同，以便于设备查询Cisco ISE。）
- 确保网络设备组已根据设备类型和位置创建。（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络设备组 (Network Device Groups)** 窗口）

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)**。

步骤 2 从任意行对应的**操作 (Actions)** 列中，点击齿轮图标，然后从下拉菜单中，根据需要通过选择任何插入或重复选项来插入新策略集。
“策略集”(Policy Sets) 表中会显示一个新行。

步骤 3 输入策略集的名称和说明。

步骤 4 如果需要，请从“允许的协议/服务器序列”(Allowed Protocols/Server Sequence) 列中，点击 (+) 符号并选择以下选项之一：

a) 创建新的允许的协议
b) 创建 TACACS+ 服务器序列

步骤 5 在**条件 (Conditions)** 列中，点击 (+) 符号。

步骤 6 在**Conditions Studio 页面**中创建所需的条件。在**编辑器 (Editor)**部分中，点击**点击以添加属性 (Click To Add an Attribute)** 文本框，然后选择所需的字典和属性（例如，Device-Location Equals Europe）。

您可以将库条件拖放到**点击以添加属性 (Click To Add an Attribute)** 文本框。

步骤 7 点击**使用 (Use)**。

步骤 8 从“视图”(View) 列中，点击 ›以访问所有策略集详细信息，并创建身份验证和授权策略以及策略例外。

步骤 9 创建所需的身份验证策略（例如，规则名称：ATN_Internal_Users，条件：DEVICE： DEVICE:Location EQUALS Location #All Locations#Europe - 该策略仅匹配位于欧洲的设备）。

步骤 10 点击**保存 (Save)**。

步骤 11 创建所需的授权策略。

示例 1：规则名称：Sys_Admin_rule, Conditions: if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8 - 该策略匹配用户名为 ABC 的系统管理员，支持要执行的指定命令，并分配权限级别 8。

示例 2：规则名称：HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1 - 该策略匹配用户名为 XYZ 系统管理员，支持要执行的指定命令，并分配权限级别 1。

在上述示例中：

- cmd_Sys_Admin 和 cmd_HDesk 命令集是在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 命令集 (TACACS Command Sets)** > **添加 (Add)** 窗口中创建的。
- TACACS 配置文件 Profile_Priv_1 和 Profile_priv_8 是在**工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 配置文件 (TACACS Profiles)** > **添加 (Add)** 窗口中创建的。

注释 您可以在身份验证和授权策略中使用的条件中为设备 IP 地址属性添加 IPv4 或 IPv6 单一地址。

步骤 12 点击**保存 (Save)**。

TACACS+ 身份验证设置和共享密钥

下表介绍“网络设备”(Network Device) 窗口中的字段，您可以使用这些字段为网络设备配置 TACACS+ 身份验证设置。导航路径为：

- （适用于网络设备）在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add)** > **TACACS 身份验证设置 (TACACS Authentication Settings)**。
- （适用于默认设备）在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **网络资源 (Network Resources)** > **默认设备 (Default Devices)** > **TACACS 身份验证设置 (TACACS Authentication Settings)**。有关详细信息，请参阅默认网络设备定义。

字段名称	使用指南
共享密钥	当 TACACS+ 协议启用时，将文本字符串分配给网络设备。在网络设备验证用户名和密码之前，用户必须输入文本。在用户提供共享密钥之前，连接始终被拒绝。此字段为必填字段。
停用的共享密钥处于启用状态	当停用期处于启用状态时显示。
淘汰 (Retire)	停用现有的共享密钥而不是结束它。当您点击“停用”(Retire) 时，系统会显示一个消息框。您可以点击**是**或**否**。
剩余停用期	（仅当在上述消息框中选择**是 (Yes)** 时可用）显示在以下导航路径中指定的默认值： 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)** > **连接设置 (Connection Settings)** > **默认共享密钥停用期 (Default Shared Secret Retirement Period)**。 您可以更改默认值。 这允许您输入新的共享密钥，而且旧共享密钥将在指定天数中保持启用状态。
结束	（只有当您在上述消息框中选择**是**时才可用）结束停用期并终止旧共享密钥。
启用单连接模式	选中该选项以将单一 TCP 连接用于与网络设备之间的所有 TACACS+通信。选择以下其中一个选项： • 传统Cisco设备 (Legacy Cisco Devices) • 或“TACACS+ 草案合规性单连接支持 (TACACS+ Draft Compliance Single Connect Support)。如果禁用单连接模式，ISE 使用新的 TCP 连接以用于每个 TACACS+ 请求。

总而言之，您可以

- 通过指定停用期的天数（范围为 1 至 99）停用旧的共享密钥，同时设置新的共享密钥。
- 在停用期间，使用旧的共享密钥和新的共享密钥。
- 在停用期到期之前，延长停用期。
- 仅在停用期间结束之前使用旧的共享密钥。
- 在停用期到期之前，终止停用期（点击 结束[End] 然后 提交[Submit]）。

注释 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备 (Network Devices)** > **添加 (Add)** 窗口，访问“TACACS+ 身份验证设置”(TACACS+ Authentication Settings) 选项。

设备管理 - 授权策略结果

Cisco ISE 管理员可以使用 TACACS+ 命令集和 TACACS+ 配置文件（策略结果）对授予给设备管理员的权限和命令进行控制。策略与网络设备协同工作，从而防止可能发生的意外或恶意配置更改。如果发生此种更改，您可以使用设备管理审计报告对执行特定命令的设备管理员进行跟踪。

FIPS 和非 FIPS 模式支持的 TACACS+ 设备管理协议

Cisco ISE 提供众多可用于创建策略结果的身份认证协议服务。但是，当用于 RADIUS 的Cisco ISE 设备启用 FIPS 模式时，设备会禁用适用于 TACACS+ 协议的身份验证协议服务，例如 PAP/ASCII、CHAP 和 MS-CHAPv1。因此，无法在 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **允许的协议 (Allowed Protocols)** 窗口中启用这些协议来管理设备（当使用启用 FIPS 的 (**管理 (Administration)** > **系统设置 (System Settings)** > **FIPS 模式 (FIPS Mode)**) Cisco ISE 设备时）。

因此，要在设备管理策略结果中为 FIPS 和非 FIPS 模式配置 PAP/ASCII、CHAP 和 MS-CHAPv1 协议，您必须导航至 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **允许的协议 (Allowed Protocols)** 窗口。在启用 FIPS 模式时只会使用默认设备管理支持的协议设置。RADIUS 不支持该选项。

TACACS+ 命令集

命令集实施可由设备管理员执行的指定命令列表。当设备管理员在网络设备上发出操作命令时，查询Cisco ISE 确定管理员是否被授权发出这些命令。这也称为命令授权。

命令集中的通配符和正则表达式

命令行包括命令和零个或多个参数。当Cisco ISE 收到命令行（请求）时，它可以以不同的方式处理命令及其参数：

- 使用通配符匹配模式将请求中的命令与命令集列表中指定的命令进行匹配。

示例：Sh?? or S*

- 使用正则表达式 (regex) 匹配模式将请求中的参数与命令集列表中指定的参数进行匹配。

  示例：Show interface[1-4] port[1-9]:tty*

命令行和命令集列表匹配

将请求的命令行与包含通配符和 Regrex 的命令集列表进行匹配：

1. 循环访问命令集列表以检测匹配的命令。

   通配符匹配允许：

   - 不区分大小写
   - 命令集的命令中的任意字符都可以为“?”，它与请求的命令中必须存在的任意单个字符匹配
   - 命令集的命令中的任意字符都可以为“*”，它与请求的命令中的 0 或多个字符匹配

     示例：

请求	命令集	匹配	备注
show	show	支持	—
show	SHOW	支持	不区分大小写
show	Sh??	支持	匹配任意字符
show	Sho??	N	第二个“?”与不存在的字符相交
show	S*	支持	“*”匹配任意字符
show	S*w	支持	“*”匹配字符“ho”
show	S*p	N	请求中没有字符与字符“p”对应

2. 对于每个匹配的命令，Cisco ISE 会验证参数。

   对于每个命令，命令集列表将包含一组以空格隔开的参数。

   示例：Show interface[1-4] port[1-9]:tty.*

   该命令含有两个参数。

   1. 参数 1：interface[1-4]
   2. 参数 2：port[1-9]:tty.*

对于请求中的命令参数，按照它们在数据包中的位置重要性顺序进行匹配。如果命令定义中的所有参数与请求中的参数匹配，那么该命令/参数可认为是匹配的。注意：请求中的任何外来参数都会被忽略。

注释 在参数中使用标准 Unix 正则表达式。

含多个命令集的处理规则

1. 如果命令集包含命令及其参数的匹配项，并且匹配项具有“始终拒绝”(Deny Always)，则Cisco ISE 会指定该命令集为 Commandset-DenyAlways。
2. 如果命令集中的命令匹配项没有“始终拒绝”(Deny Always)，则Cisco ISE 会依次检查命令集中的所有命令直到找到第一个匹配项。
    1. 如果第一个匹配项具有“允许”(Permit)，则Cisco ISE 会指定命令集为 Commandset-Permit。
    2. 如果第一个匹配项具有“拒绝”(Deny)，则Cisco ISE 会指定命令集为 Commandset-Deny。
3. 在Cisco ISE 分析所有命令集后，它会授权以下命令：
    1. 如果Cisco ISE 指定任何命令集为 Commandset-DenyAlways，则Cisco ISE 拒绝该命令。
    2. 如果没有 Commandset-DenyAlways，且任意命令集为 Commandset-Permit，则Cisco ISE 允许该命令；否则，Cisco ISE 将拒绝该命令。唯一的例外情况是**不匹配 (Unmatched)** 复选框已选中。

创建 TACACS+ 命令集

要使用 TACACS+ 命令集策略结果创建策略集，请按照以下步骤操作：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 命令集 (TACACS Command Sets)**。

您还可以在以下位置配置 TACACS 命令集： **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)** 页面。

步骤 2 点击**添加 (Add)**。

步骤 3 输入名称和说明。

步骤 4 点击**添加 (Add)** 指定授予权限、命令和参数。

步骤 5 在**授予 (Grant)** 下拉列表，您可以选择以下选项之一：

- **允许 (Permit)** ：允许指定的命令（例如，permit show, permit con* Argument terminal）。
- **拒绝 (Deny)** ：拒绝指定的命令（例如，deny mtrace）。

- **始终拒绝 (Deny Always)** ：覆盖在其他命令集中允许的命令（例如，clear auditlogs）

注释　点击操作图标以增加或减少“Grant”(授予)、“Command”(命令) 和“参数”(Argument) 字段的列宽。

步骤 6 选中**允许以下未列出的任何命令 (Permit any command that is not listed below)** 复选框允许未在“授予”列中指定为允许、拒绝或始终拒绝的命令和参数。

TACACS+ 配置文件

TACACS+ 配置文件控制设备管理员的初始登录会话。会话是指每个单独的身份验证、授权或记帐请求。对网络设备的会话授权请求会引发Cisco ISE 响应。响应包括由网络设备解释的令牌，限制可能在会话期限执行的命令。用于设备管理访问服务的授权策略可以包含单个外壳配置文件和多个命令集。TACACS+ 配置文件定义分为两个组件：

- 常见任务
- 自定义用户属性

“TACACS+ Profiles (TACACS+ 配置文件)”窗口中有两个视图（在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 配置文件 (TACACS Profiles)**）：**任务属性视图 (Task Attribute View)** 和**原始视图 (Raw View)**。可以使用**任务属性视图 (Task Attribute View)** 输入常见任务，且自定义属性可在**任务属性视图 (Task Attribute View)** 和**原始视图 (Raw View)** 中创建。

您可通过**常见任务 (Common Tasks)** 部分为配置文件选择并配置最常用的属性。这里包含的属性为 TACACS+ 协议草案说明定义的那些属性。但是值可用于来自其他服务的请求授权。在**任务属性视图 (Task Attribute View)** 中，Cisco ISE 管理员可以设置分配给设备管理员的权限。常见任务类型如下：

- 外壳
- WLC
- Nexus
- 通用

您可通过**自定义属性 (Custom Attributes)** 部分配置其他属性。它提供不被**常见任务 (Common Tasks)** 部分识别的属性列表。每个定义包括属性名称、该属性是强制还是可选的说明和属性值。

注释　您可以为启用 TACACS 的网络设备定义总共 24 个任务属性。如果定义的任务属性超过 24 个，则不会将这些属性发送到启用 TACACS 的网络设备。

在**原始视图 (Raw View)** 中，可以在属性名称及其值之间使用等号 (=) 输入强制属性，在属性名称及其值之间使用一个星号 (*) 可输入可选属性。**原始视图 (Raw View)** 中输入的属性反映在**任务属性视图 (Task Attribute View)** 中的**自定义属性 (Custom Attributes)** 部分，反之亦然。**原始视图 (Raw View)**

部分也用于将属性列表（例如，另一产品的属性列表）从剪贴板复制并粘贴到Cisco ISE 上。可为非外壳服务定义自定义属性。

创建 TACACS+ 配置文件

要创建 TACACS+ 配置文件：

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 配置文件 (TACACS Profiles)**。

还可以在以下位置配置 TACACS 命令集 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设备管理策略集 (Device Admin Policy Sets)** 页面。

步骤 2 点击**添加 (Add)**。

步骤 3 在 **TACACS 配置文件 (TACACS Profile)** 部分中，请输入名称和说明。

步骤 4 在**任务属性视图 (Task Attribute View)** 选项卡中，请选中所需的**常见任务 (Common Tasks)**。请参阅常见任务设置，第 11 页页面。

步骤 5 在**任务属性视图 (Task Attribute View)** 选项卡**自定义属性 (Custom Attributes)** 部分中，点击**添加 (Add)** 输入必要的属性。

常见任务设置

在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **TACACS 配置文件 (TACACS Profiles)** > **添加 (Add)** 以查看常见任务设置窗口。常见任务类型为：外壳、WLC、Nexus 和通用。

Shell

Cisco ISE 管理员可使用以下选项设置设备管理员的权限。

选项	说明
默认权限 (Default Privilege)	为设备管理员启用默认（初始）权限级别，以供其进行外壳授权。请选择以下任意一个选项： • 选择 0 - 15 之间的值。 • 选择所需的“身份存储属性”(Identity Store Attribute)。
最大权限 (Maximum Privilege)	启用“启用身份验证”(Enable authentication) 所需的最大权限级别。您可以选择 0 - 15 之间的值。
访问控制列表 (Access Control List)	选择一个 ASCII 字符串 (1-251*) 或所需的“身份数据库属性”(Identity Store Attribute)。

选项	说明
自动命令 (Auto Command)	选择一个 ASCII 字符串 (1-248*) 或所需的“身份存储属性”(Identity Store Attribute)。
禁用转义 (No Escape)	对于转义字符，选择以下任一选项： • True：说明转义预防已启用。 • False：说明转义预防未启用。 • 选择所需的“身份存储属性”(Identity Store Attribute)。
超时 (Timeout)	选择 0 - 9999 之间的值或所需的“身份存储属性”(Identity Store Attribute)。
空闲时间 (Idle Time)	选择 0 - 9999 之间的值或所需的“身份存储属性”(Identity Store Attribute)。

WLC

Cisco ISE 管理员可使用以下选项控制设备管理员对 WLC 应用选项卡的访问权限。WLC 应用包含以下选项卡：WLAN、“控制器”(Controller)、“无线”(Wireless)、“安全”(Security)、“管理”(Management) 和“命令”(Commands)。

选项	说明
所有 (All)	设备管理员对所有 WLC 应用选项卡均具有完全访问权限。
监控器 (Monitor)	设备管理员对 WLC 应用选项卡仅有只读访问权限。
大厅 (Lobby)	设备管理员仅有部分配置权限。
选中 (Selected)	设备管理员可以访问Cisco ISE管理员从以下复选框中选中的选项卡：WLAN、控制器(Controller)、无线 (Wireless)、安全 (Security)、管理 (Management) 和命令 (Commands)。

Nexus

Cisco ISE 管理员可使用以下选项控制设备管理员对Cisco Nexus 交换机的访问权限。

选项	说明
将属性设置为 (Set Attribute As)	Cisco ISE 管理员可以将常见任务生成的 Nexus 属性指定为“可选”(Optional) 或“必选”(Mandatory)。
网络角色 (Network Role)	将 Nexus 配置为使用Cisco ISE 进行身份验证时，默认情况下，设备管理员拥有只读访问权限。可将设备管理员分配至其中一个角色。每个角色定义允许的操作： • 无 (None)：无权限。 • 操作者（只读）(Operator (Read Only))：对整个 NX-OS 设备有完全的读取访问权限。 • 管理员（读/写）(Administrator (Read/Write))：对整个 NX-OS 设备有完全的读写访问权限。
虚拟设备环境 (VDC) (Virtual Device Context [VDC])	无 (None)：无权限。 操作者（只读）(Operator (Read Only))：仅对 VDC 有读取访问权限 管理员（读/写）(Administrator (Read/Write))：仅对 VDC 有读写访问权限。

通用

Cisco ISE 管理员可使用此选项指定常见任务中不可用的自定义属性。

访问命令行界面以更改启用密码

要更改启用密码，请执行以下步骤：

开始之前

某些命令会分配到特权模式。因此，只能在设备管理员经过身份验证进入此模式时执行它们。

当设备管理员尝试进入特权模式时，设备会发送特殊的启用身份验证类型。Cisco ISE 支持使用单独的启用密码来验证此特殊的启用身份验证类型。当使用内部身份库对设备管理员进行身份验证时，系统将使用单独的启用密码。对于使用外部身份库进行的身份验证，系统将使用相同的密码来进行常规登录。

步骤 1 登录到交换机。

步骤 2 按 Enter 键显示以下提示符：

```
Switch>
```

步骤 3 执行以下命令来配置启用密码。

```
Switch> enable Password:（按 Enter 键可留空密码。）Enter Old Password:（输入旧密码。）Enter New Password:（输入新密码。）Enter New Password Confirmation:（确认新密码。）
```

注释 如果为登录密码和启用密码配置了密码有效期，则在指定时段内未更改密码时，用户帐户将禁用。如果将Cisco ISE 配置为 TACACS+ 服务器，并在网络设备上配置了**启用旁路 (Enable Bypass)** 选项，则无法通过 CLI（通过 telnet）更改启用密码。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择**管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **用户 (Users)**，更改内部用户的启用密码。

配置全局 TACACS+ 设置

配置全局 TACACS+ 设置

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **设置 (Settings)**。

在**连接设置 (Connection Settings)** 选项卡，您可以更改所需字段的默认值。

- 在**授权缓存超时 (Authorization cache timeout)** 字段中，可以设置生存时间 (TTL) 值，首次授权请求时，系统将在该时间内缓存内部用户的某些属性。缓存的属性包括用户名和用户特定属性，如用户组。“系统管理”（System Administration）“配置”（Configuration）“字典”（Dictionary）“身份”（Identity）“内部用户”（Internal Users）以创建属性。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 默认值为 0，表示禁用授权缓存。
- **单连接支持 (Single Connect Support)**：如果禁用单连接模式，则 ISE 对每个 TACACS+ 请求使用新的 TCP 连接。

步骤 2 在**密码更改控制 (Password Change Control)** 选项卡，定义所需字段以控制是否通过 TACACS+ 允许密码更新。

只有选中此选项，才会启用**启用 Telnet 更改密码 (Enable Telnet Change Password)** 部分中的提示。否则，会启用**禁用 Telnet 更改密码 (Disable Telnet Change Password)** 提示。密码提示可完全自定义，并可根据需要进行修改。

在**密码策略违规消息 (Password Policy Violation Message)** 字段中，如果新密码与指定条件不符，您可以为内部用户设置的密码显示相应的错误消息。

步骤 3 在**会话密钥分配 (Session Key Assignment)** 选项卡，请选择所需的字段以将 TACACS+ 请求链接到会话。

监控节点使用会话密钥来链接来自客户端的AAA请求。默认设置为启用NAS地址、端口、远程地址和用户字段。

步骤 4 点击**保存 (Save)**。

相关主题

TACACS+ 身份验证设置和共享密钥，第 5 页
RADIUS 令牌服务器中的用户属性缓存

从思科安全 ACS 将数据迁移至思科 ISE

您可以使用迁移工具导入来自 ACS 5.5 及更高版本的数据，然后为所有网络设备设置默认 TACACS+ 密钥。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **概述 (Overview)**，在**准备 (Prepare)** 部分中，点击**下载软件网页**，下载迁移工具。将工具保存到您的 PC，然后在 migTool 文件夹中，运行 migration.bat 文件以开始迁移过程。有关迁移的完整信息，请参阅您的Cisco ISE 版本的迁移指南。

监控设备管理活动

Cisco ISE 提供各种报告和日志，通过这些报告和日志，您可以查看通过 TACACS+ 配置的设备计费、身份验证、授权和命令计费相关的信息。您可以按需或按计划运行这些报告。

步骤 1 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **工作中心 (Work Centers)** > **设备管理 (Device Administration)** > **报告 (Reports)** > **报告 (Reports)**。。

您还可以在其他位置查看报告。 在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** 页面。

步骤 2 在**报告选择器 (Report Selector)** 中，展开**设备管理 (Device Administration)** 以查看**身份验证摘要 (Authentication Summary)**、**TACACS 记账 (TACACS Accounting)**、**TACACS 身份验证 (TACACS Authentication)**、**TACACS 授权 (TACACS Authorization)**、**TACACS 命令记账 (TACACS Command Accounting)**、**不同失败原因的前 N 个身份验证 (Top N Authentication by Failure Reason)**、**不同网络设备的前 N 个身份验证 (Top N Authentication by Network Device)**、**不同用户的前 N 个身份验证 (Top N Authentication by User)** 报告。

步骤 3 选择报告并选取您想要使用 **Filters** 下拉列表搜索的数据。

步骤 4 在 **Time Range** 中选择您想要查看的数据的时间范围。

步骤 5 点击**运行 (Run)**。

TACACS 实时日志

下表列出“TACACS+ 实时日志”(TACACS Live Logs) 页面的字段，此页面显示 TACACS+ AAA 详细信息。在思科 ISE GUI 中，点击**菜单 (Menu)** 图标 (☰)，然后选择 **操作 (Operations)** > **TACACS** > **实时日志 (Live Logs)**。您只能在主 PAN 中查看 TACACS 实时日志。

表 *1: TACACS* 实时日志

字段名称	使用指南
生成时间 **(Generated Time)**	根据特定事件触发时间显示系统日志生成时间。
日志记录时间 **(Logged Time)**	显示监控节点处理和存储系统日志的时间。此列为必选项，无法取消选择。
状态 **(Status)**	显示身份验证是否成功。此列为必选项，无法取消选择。绿色用于代表已通过的身份验证。红色用于代表失败的身份验证。
详细信息 **(Details)**	在点击放大镜图标时显示报告，使您能够深入查看有关所选身份验证方案的更多详细信息。此列为必选项，无法取消选择。
会话密钥 **(Session Key)**	显示由 ISE 返回到网络设备的会话密钥（在 EAP 成功或 EAP 失败消息中查找）。
用户名 **(Username)**	显示设备管理员的用户名。此列为必选项，无法取消选择。
类型 **(Type)**	包括两种类型 - 身份验证和授权。显示身份验证已通过和/或失败的用户名。此列为必选项，无法取消选择。
身份验证策略 **(Authentication Policy)**	显示为特定身份验证选择的策略的名称。
授权策略 **(Authorization Policy)**	显示为特定授权选择的策略的名称。
ISE 节点 **(ISE Node)**	显示处理访问请求的 ISE 节点的名称。
网络设备名称 **(Network Device Name)**	显示网络设备的名称。
网络设备 **IP (Network Device IP)**	显示访问请求已处理的网络设备的 IP 地址。
网络设备组 **(Network Device Groups)**	显示网络设备所属相应网络设备组的名称。
设备类型 **(Device Type)**	显示用于处理来自不同网络设备的访问请求的设备类型。
位置 **(Location)**	显示用于处理来自网络设备的访问请求的基于位置的策略。
设备端口 **(Device Port)**	显示发出访问请求的设备端口号。
故障原因 **(Failure Reason)**	显示拒绝网络设备发出的访问请求的原因。
远程地址 **(Remote Address)**	显示唯一标识终端站的 IP 地址、MAC 地址，或任何其他字符串。

字段名称	使用指南
匹配的命令集 (Matched Command Set)	如果 MatchedCommandSet 属性值存在，则显示该值，或如果 MatchedCommandSet 属性值为空或属性本身不存在于系统日志，则显示一个空值。
外壳配置文件 (Shell Profile)	显示已授予设备管理员用于在网络设备执行命令的权限。

您可以在 TACACS 实时日志页面执行以下操作：

- 将数据导出为 CSV 或 PDF 格式。
- 根据要求显示或隐藏列。
- 使用快速或自定义过滤器过滤数据。您也可以保存过滤器供以后使用。
- 重新排列列并调整列宽。
- 对列值排序。

注释 所有用户自定义将存储为用户首选项。

相关主题

TACACS+ 设备管理

配置全局 TACACS+ 设置，第 14 页