

使用ISE配置Catalyst Center外部身份验证TACACS

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[思科身份服务引擎\(ISE\)](#)

[许可并启用TACACS+服务](#)

[创建管理员用户并添加网络设备](#)

[配置TACACS+配置文件](#)

[配置TACACS+策略](#)

[思科Catalyst中心](#)

[配置ISE/AAA服务器](#)

[启用并配置外部身份验证。](#)

[验证](#)

[故障排除](#)

[1.属性配置错误](#)

[2.共享密钥不匹配](#)

简介

本文档介绍将思科身份服务引擎与Catalyst Center集成以启用TACACS+身份验证所需的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 对Cisco ISE和Cisco Catalyst Center的管理员访问权限。
- 基本了解AAA（身份验证、授权和记帐）概念。
- 有关TACACS+协议的工作知识。
- Catalyst Center和ISE服务器之间的网络连接。

使用的组件

本文档中的信息基于以下硬件和软件版本：

- Cisco Catalyst Center版本2.3.7.x
- 思科身份服务引擎(ISE)3.x(或更高版本)
- 用于外部用户身份验证的TACACS+协议

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

此集成允许外部用户登录Catalyst Center进行管理访问和管理。

配置

思科身份服务引擎(ISE)

许可并启用TACACS+服务

开始使用ISE中的TACACS+配置之前，必须确认安装了正确的许可证并启用了功能。

1. 验证您在[Cisco Smart Software Manage](#)或[Cisco License Central](#)门户中有PID许可证L-ISE-TACACS-ND=。

在ISE许可门户中启用设备管理。

- Device Admin许可证(PID:L-ISE-TACACS-ND=)在策略服务节点(PSN)上启用TACACS+服务。
- 导航至：

管理>System >许可

- 选中Tier选项下的Device Admin复选框。

Tier ☒ Essential ☒ Advantage ☒ Premier ☒ Device Admin

Virtual Appliance ☒ ISE VM License

This enables the ISE features for the purchased licenses to be tracked by Cisco Smart Licensing.

By clicking Register you will agree to the Terms&Conditions. You can download Terms&Conditions on [Smart Licensing Resources](#).

Reset

Update

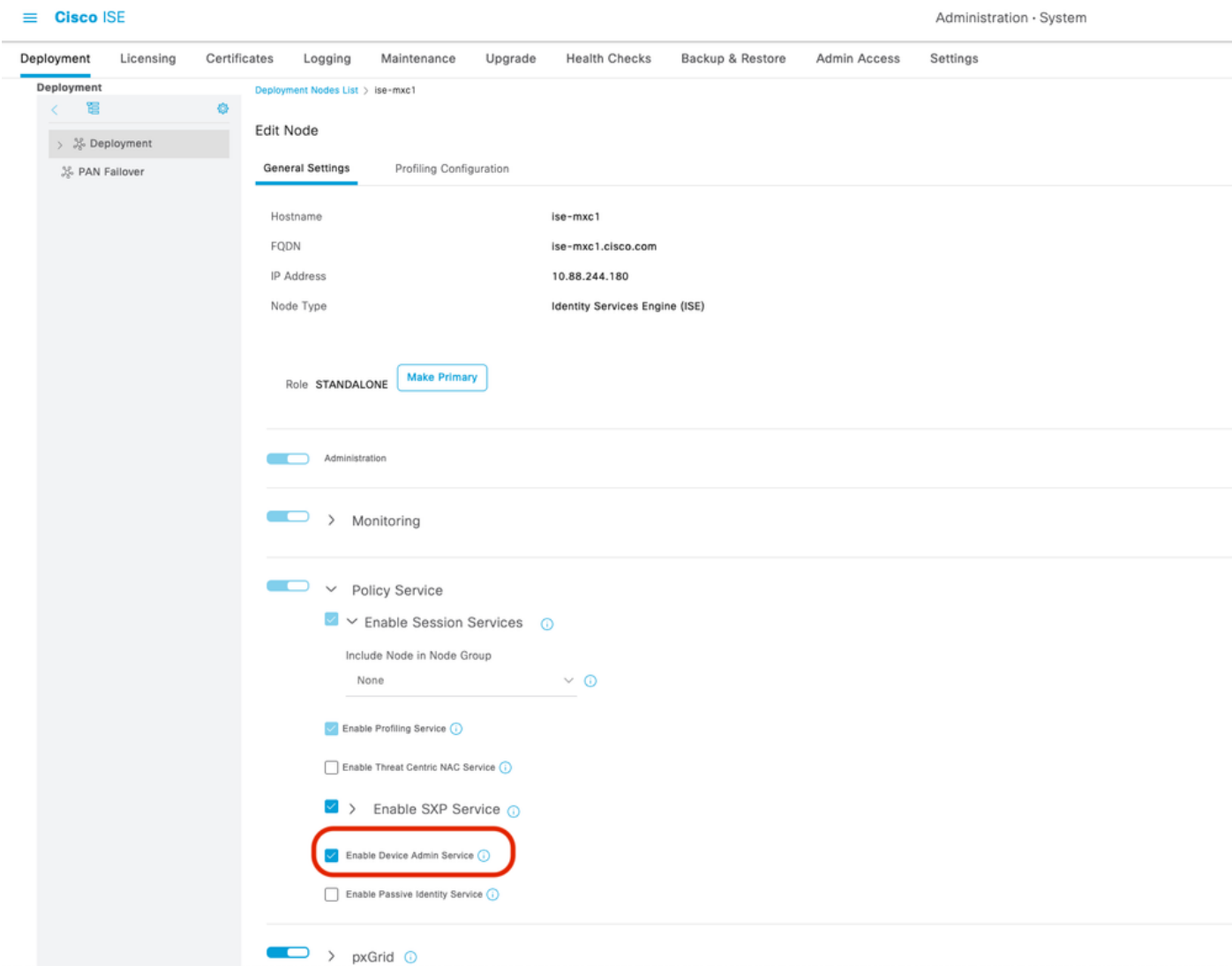
☐	Premier	Enabled	Released Entitlement	0	-	Dec 27,2024 18:16:00 PM
☐	Device Admin	Enabled	In Compliance	1	-	Sep 11,2025 20:53:12 PM
Virtual Appliance						
	ISE VM License	Enabled	In Compliance	1	-	Sep 11,2025 20:53:12 PM

许可证设备管理

3.在运行TACACS+服务的ISE节点上启用设备管理服务。

- 导航至：

管理>System >部署>选择节点
- 选中选项Enable Device Admin Service。



启用设备管理服务

创建管理员用户并添加网络设备

1.创建管理员用户。

- 此用户帐户用于通过ISE身份验证登录Catalyst Center UI。

- 导航至：

工作中心(Work Centers)>网络访问(Network Access)>身份(Identities)>网络访问用户(Network Access User)

- 添加新用户(例如catc-user)。
- 如果用户已存在，请继续执行下一步。

2.创建网络设备。

- 导航至：

工作中心(Work Centers)>网络访问(Network Access)>身份(Identities)>网络资源(Network Resource)

- 添加Catalyst Center的IP地址，或定义Catalyst Center IP所在的子网。
- 如果设备已存在，请验证它是否包含参数：
 - TACACS身份验证设置已启用。
 - Shared Secret已配置且已知（请保存此值，因为稍后在Catalyst Center中需要使用此值）。

The screenshot displays the Cisco ISE configuration interface for a Network Resource named 'Catalyst-Center_6'. The left sidebar shows the navigation menu with 'Network Devices' selected. The main content area is titled 'Network Devices List > Catalyst-Center_6'. Below this, the 'Network Devices' section contains several configuration fields: Name (Catalyst-Center_6), Description, IP Address (10.88.244.160 / 32), Device Profile (Cisco), Model Name, Software Version, Network Device Group (All Locations), Location (All Locations), IPSEC (No), Device Type (All Device Types), and DNAC (DNAC Devices). The 'RADIUS Authentication Settings' section is collapsed, while the 'TACACS Authentication Settings' section is expanded and highlighted with a red box. This section includes a 'Shared Secret' field with a 'Show' button and a 'Retire' button. Below this, there are checkboxes for 'Enable Single Connect Mode', 'Legacy Cisco Device' (selected), and 'TACACS Draft Compliance Single Connect Support'.

- 导航至：

- 添加配置文件名称。

- 按如下方式添加自定义属性：

- type : 必需
- 名称 : cisco-av-pair
- 值 : Role=SUPER-ADMIN-ROLE

- 保存配置文件。

Cisco ISE

Work Centers · Device Administration

OverviewIdentitiesUser Identity GroupsExt Id SourcesNetwork ResourcesPolicy ElementsDevice Admin Policy SetsReportsSettings

Conditions>

Network Conditions>

Results▼

Allowed Protocols

TACACS Command Sets

TACACS Profiles

TACACS Profiles > CatC_TACACS_Profile

TACACS Profile

Name

CatC_TACACS_Profile

Description

Catalyst Center External Authentication

Task Attribute ViewRaw View

Common Tasks

Common Task TypeShell▼

☐ Default Privilege

▼

(Select 0 to 15)

☐ Maximum Privilege

▼

(Select 0 to 15)

☐ Access Control List

▼

☐ Auto Command

▼

☐ No Escape

▼

(Select true or false)

☐ Timeout

▼

Minutes (0-9999)

☐ Idle Time

▼

Minutes (0-9999)

Custom Attributes

AddTrash▼Edit

☐ Type

Name

Value

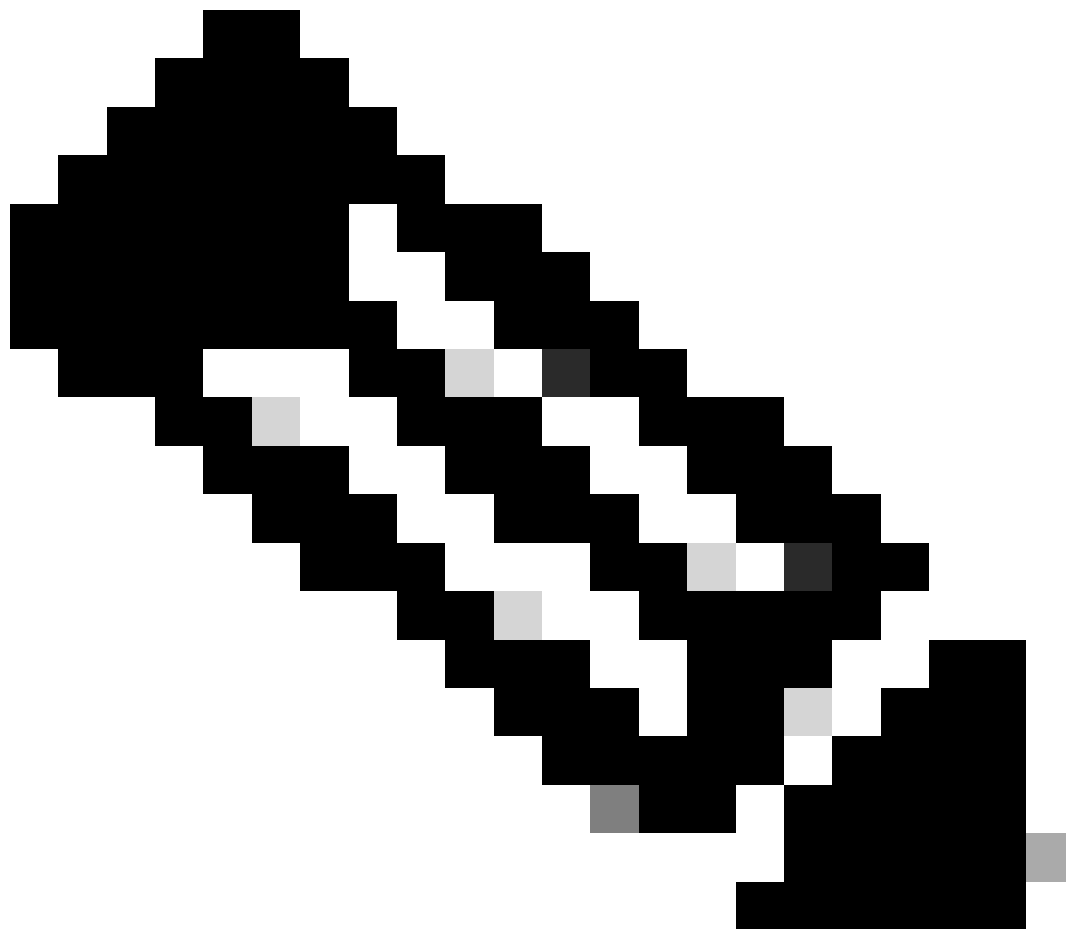
☐ MANDATORY

cisco-av-pair

Role=SUPER-ADMIN-ROLE

Cancel

Save



注意：Cisco Catalyst Center支持用于访问控制的外部身份验证、授权和记帐(AAA)服务器。如果您使用外部服务器对外部用户进行身份验证和授权，则可以在Cisco Catalyst Center中启用外部身份验证。默认AAA属性设置与默认用户配置文件属性匹配。

TACACS协议的默认AAA属性值为cisco-av-pair。

RADIUS协议的默认AAA属性值为Cisco-AVPair。

只有当AAA服务器在用户配置文件中具有自定义属性时，才需要进行更改。在AAA服务器上，AAA属性值的格式为Role=role1。在Cisco身份服务引擎(Cisco ISE)服务器上，在配置RADIUS或TACACS配置文件时，用户可以选择或输入cisco av-pair作为AAA属性。

例如，您可以手动选择和配置AAA属性为cisco-av-pair=Role=SUPER-ADMIN-ROLE或Cisco-AVPair=Role=SUPER-ADMIN-ROLE。

2.创建TACACS+命令集。

- 导航至：

Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets

- 添加名称。
- 选中选项Permit any command that is not listed below。
- 保存命令集。

The screenshot shows the Cisco ISE web interface for configuring TACACS Command Sets. The breadcrumb trail is: Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets. The left sidebar shows the navigation menu with 'Results' expanded and 'TACACS Command Sets' selected. The main content area shows the configuration for a specific Command Set named 'PermitAllCommands'. The 'Name' field is filled with 'PermitAllCommands'. The 'Description' field is empty. Under the 'Commands' section, the checkbox 'Permit any command that is not listed below' is checked. Below this, there are buttons for 'Add', 'Trash', 'Edit', 'Move Up', and 'Move Down'. A table with columns 'Grant', 'Command', and 'Arguments' is shown, but it is empty with the message 'No data found.' at the bottom. 'Cancel' and 'Save' buttons are at the bottom right.

TACACS命令集

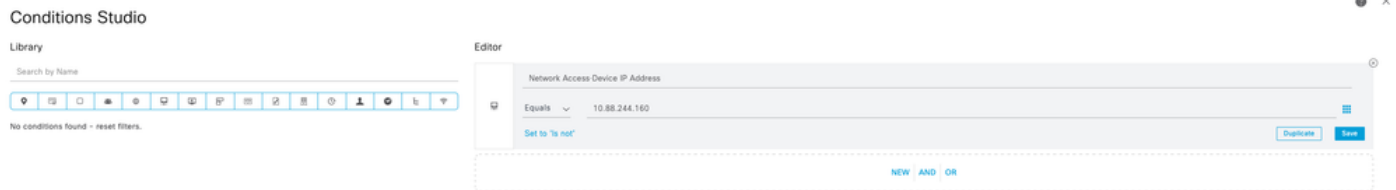
配置TACACS+策略

1.创建新的TACACS+策略集。

- 导航至：

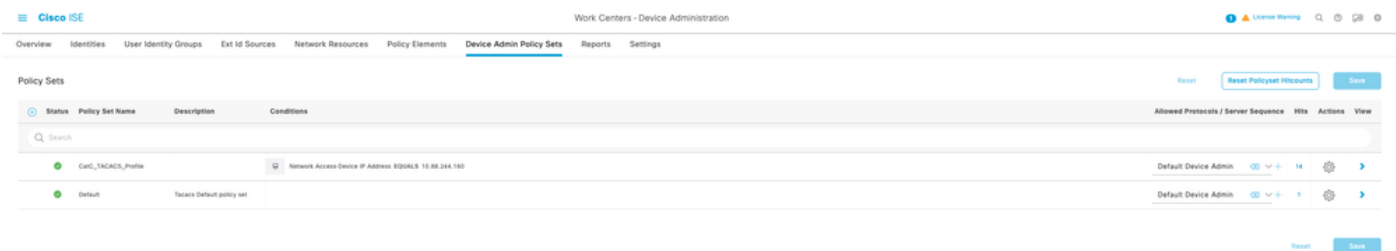
工作中心(Work Centers)>设备管理(Device Administration)>设备管理策略设置(Device Admin Policy Set)

- 为策略集添加名称。
- 配置条件。
 - 在本示例中，条件与Catalyst Center IP地址匹配。



Catalyst中心IP地址

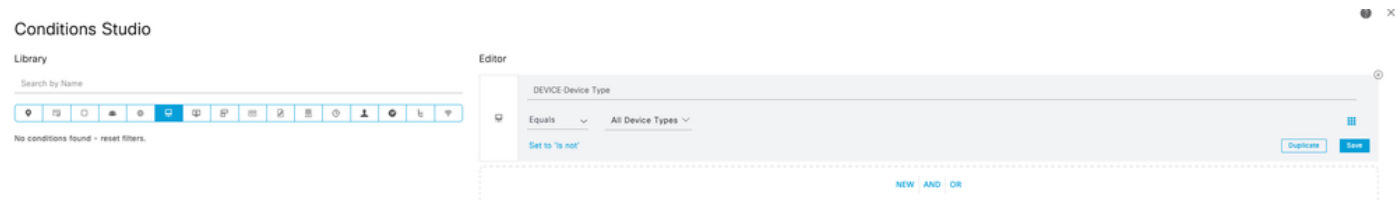
1.3在Allowed Protocols / Server Sequence上，选择Default Device Admin。



选择Default Device Admin

2.配置策略集。

- 点击右侧的箭头(>)展开并配置策略集。
- 在Authorization Policy下添加新规则。
- 按如下方式配置新规则：
 - 名称：输入描述性规则名称。
 - 条件：在本示例中，条件与All Device Types匹配。



所有设备类型

- 命令集：选择之前创建的TACACS+命令集。
- 外壳配置文件：选择之前创建的TACACS+配置文件。

Cisco ISE Work Centers - Device Administration

Overview Identities User Identity Groups Ext ID Sources Network Resources Policy Elements **Device Admin Policy Sets** Reports Settings

Policy Sets - CatC_TACACS_Profile

Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
●	CatC_TACACS_Profile		Network Access Device IP Address EQ 94.15.10.88 244.150	Default Device Admin	14

> Authentication Policy (1)
> Authorization Policy - Local Exceptions
> Authorization Policy - Global Exceptions
v Authorization Policy (2)

Status	Rule Name	Conditions	Results	Command Sets	Shell Profiles	Hits	Actions
●	Authorization Rule 1	DEVICE Device Type EQ 94.15. All Device Types		PermitAllCommands	CatC_TACACS_Profile	14	
●	Default			DenyAllCommands	Deny All Shell Profile	0	

Reset [Save](#)

TACACS+命令集

思科Catalyst中心

配置ISE/AAA服务器

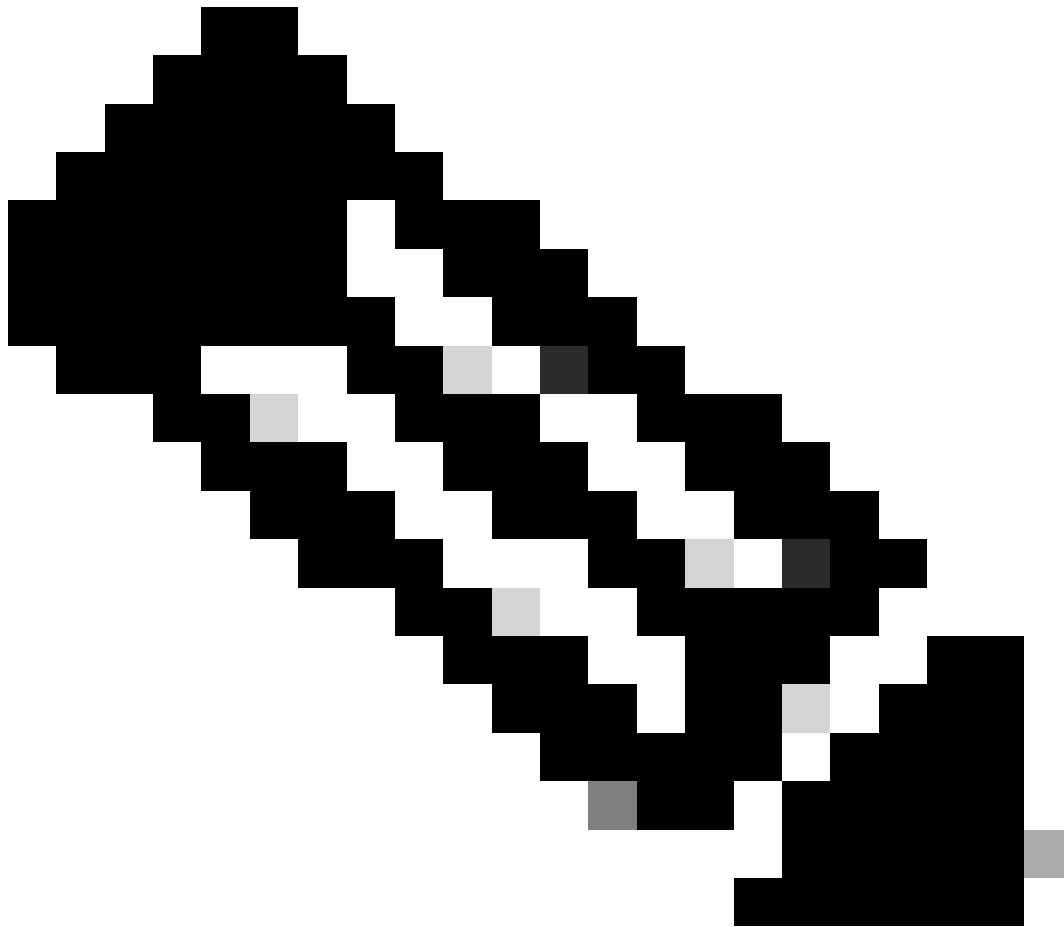
1.登录到Catalyst Center Web界面。

- 导航至：

主菜单>System >设置>外部服务>身份验证和策略服务器

2.添加新服务器。您可以选择ISE或AAA。

- 在本演示中，使用AAA服务器选项。



注意：Catalyst Center集群只能配置一个ISE集群。

3.配置这些选项，然后保存：

- 输入AAA服务器的IP地址。
- 添加Shared Secret (在Cisco ISE网络资源中配置的相同密钥) 。
- 将Advanced Settings切换到On。
- 选中TACACS选项。

Add AAA server

×

Server IP Address*
10.88.244.180

Shared Secret*
.....

SHOW

Advanced Settings

Protocol

☒ RADIUS

☒ TACACS

☐ Enable KeyWrap

Authentication Port*
1812

Accounting Port*
1813

Port
49

Retries*
3

Timeout (seconds)*
4

身份验证和策略服务器

External Ser

External Services

Authentication and Policy Servers

Authentication and Policy Servers

Use this form to specify the servers that authenticate Catalyst Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

Add

Export

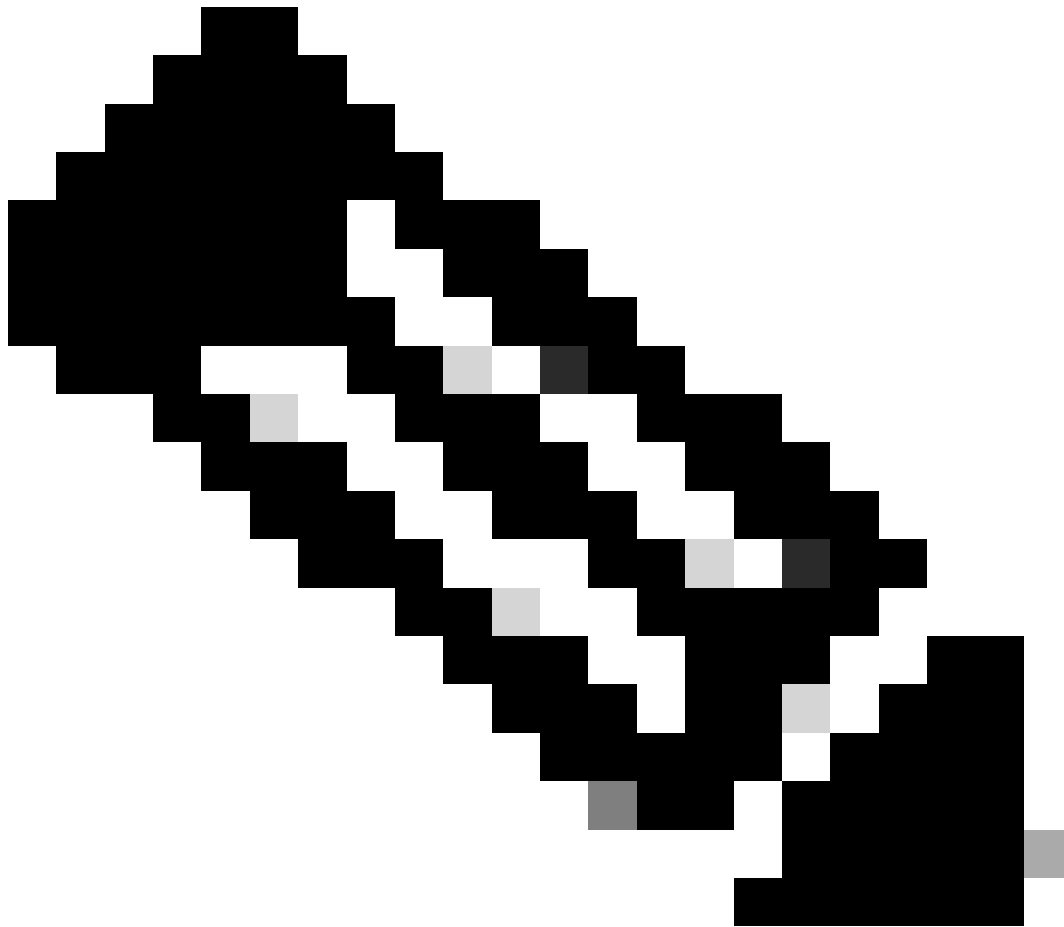
IP Address	Protocol	Type	Status	Actions
192.168.31.228	RADIUS	ISE	INACTIVE	⋮
10.88.244.180	RADIUS_TACACS	AAA	ACTIVE	⋮

高级设置

启用并配置外部身份验证。

- 1.定位至“外部验证”页：

主菜单>System >用户和角色>外部身份验证
- 2.添加AAA属性cisco-av-pair，然后单击Update以保存更改。



注意：由于TACACS+的默认属性已经是cisco-av-pair，因此此步骤不是强制性的，但此步骤被视为明确配置它的最佳实践。

3.在主AAA服务器下，选择之前配置的AAA服务器。

- 单击View Advanced Settings以显示其他选项。
- 选择TACACS+选项。
- 输入在Cisco ISE的Network Resource中配置的Shared Secret。
- 单击Update保存更改。

4.启用外部用户复选框。

- 此操作会自动保存配置。

Catalyst Center

System / Users & Roles

User Management

Role Based Access Control

External Authentication

External Authentication

Cisco Catalyst Center supports external Authentication, Authorization and Accounting (AAA) servers for access control. If you are using an external server for authentication and authorization of external users, you should enable external authentication in Cisco Catalyst Center. The default AAA attribute setting matches the default user profile attribute.
TACACS protocol default AAA attribute value is "cisco-av-pair".
RADIUS protocol default AAA attribute value is "Cisco-AVPair".
Change is only required if your AAA server has a custom attribute in the user profile.
On the AAA server, the format of the AAA attribute value is "Role=role1". On the Cisco Identity Services Engine (Cisco ISE) server, while configuring RADIUS or TACACS profile, the user may select or input "cisco-av-pair" as AAA attribute.
For example, you might manually select & configure the AAA attribute as "cisco-av-pairRole=SUPER-ADMIN-ROLE" or "Cisco-AVPairRole=SUPER-ADMIN-ROLE".

☒ Enable External User

AAA Attribute

AAA attribute

cisco-av-pair

Reset to Default

Update

AAA Server(s)

Primary AAA Server

IP address

10.88.244.180

Shared Secret

Shared Secret

info

Hide Advanced Settings

☐ RADIUS

☒ TACACS

Port

49

Retries

3

Timeout (seconds)

4

Update

Secondary AAA Server

IP address

10.88.244.180

Shared Secret

Shared Secret

info

View Advanced Settings

☐ RADIUS

☒ TACACS

Port

49

Retries

3

Timeout (seconds)

4

Update

Success

Successfully saved external authentication settings.

外部身份验证

验证

1. 打开新的浏览器会话或使用Incognito Mode，并使用在Cisco ISE中配置的用户帐户登录Catalyst Center网页。
2. 从Catalyst Center，确认登录成功。



登录使用ISE配置Catalyst Center外部身份验证TACACS

3. 从Cisco ISE，验证日志：

Operations > TACACS > Live Logs

- 验证状态:通过
- 授权状态：通过

Cisco ISE

Operations - TACACS

License Warning

Live Logs

Export To

Refresh: Never, Show: Latest 20 records, Within: Last 3 hours

Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Isa Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
X			Identity		Authentication Policy	Authorization Policy	Isa Node	Network Device Name	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Command	Shell Profile
Sep 12, 2025 12:12:20.801...			cisco-user	Authentication	CatC_TACACS_Profile >> Auth...	CatC_TACACS_Profile >> Authori...	isa-mac1	Catalyst-Centr_8	10.88.244.160	Device Type680 D...	LocationRAI Locat...	console		10.189.17.203		CatC_TACACS_Pi...
Sep 12, 2025 12:12:20.798...			cisco-user	Authentication	CatC_TACACS_Profile >> Default		isa-mac1	Catalyst-Centr_8	10.88.244.160	Device Type680 D...	LocationRAI Locat...	console		10.189.17.203		

Last Updated: Thu Sep 11 2025 18:16:58 GMT-0800 (Central Standard Time)

Records Shown: 2

实时日志

4. 在Authorization Details中，与下一个输出进行比较：
- 消息文本：Device-Administration:会话授权成功
 - 所有响应属性：cisco-av-pair=Role=SUPER-ADMIN-ROLE

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes	
All Response Attributes	cisco-av-pair=Role=SUPER-ADMIN-ROLE

cisco-av-pair=Role=SUPER-ADMIN-ROLE

故障排除

以下是您在集成过程中可能会遇到的一些常见问题以及如何识别它们：

1.属性配置错误

Catalyst Center中的症状：登录凭据无效



Cisco Catalyst Center

The bridge to possible

 Invalid Login Credentials

Username

catc-user

Password

[SHOW](#)

Log In

属性配置错误

- 思科ISE中的症状（TACACS日志）：

- 身份验证:通过
- 授权:通过

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device...	Network Device...	Device Type	Location	Device Port	Failure Reason	Remote Address	Matched Comm...	Shell Profile
Sep 12, 2025 12:12:26.861...			catc-user	Authentication	CatC_TACACS_Profile	CatC_TACACS_Profile >> Authoriz...	ise-mst1	Catalyst-Center_8	10.88.244.160	Device TypeAAA S...	LocationAAA Locat...	console		10.188.17.203		CatC_TACACS_Pt...
Sep 12, 2025 12:12:26.798...			catc-user	Authentication	CatC_TACACS_Profile	CatC_TACACS_Profile >> Default	ise-mst1	Catalyst-Center_8	10.88.244.160	Device TypeAAA S...	LocationAAA Locat...	console		10.188.17.203		

属性配置错误

- 可能的原因：
 - 属性值中存在空格。

示例：

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes

All Response Attributes cisco-av-pair=Role=SUPER-ADMIN-ROLE

属性配置错误

- 属性配置不正确，缺少Role=关键字。

示例：

Authorization Details

Generated Time	2025-09-12 00:12:20.801 +0:00
Logged Time	2025-09-12 00:12:20.801
Epoch Time (sec)	1757635940
ISE Node	ise-mxc1
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	catc-user
Network Device Name	Catalyst-Center_6
Network Device IP	10.88.244.160
Network Device Groups	IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations
Device Port	console
Remote Address	10.189.17.203

Authorization Attributes

All Request Attributes

All Response Attributes cisco-av-pair=Role=SUPER-ADMIN-ROLE

属性配置错误

2.共享密钥不匹配

- 症状：Catalyst Center和Cisco ISE之间的身份验证数据包失败。

- 可能的原因：在ISE的网络资源中配置的共享密钥与Catalyst Center > External Authentication页面中配置的共享密钥不匹配。

如何验证：

- 检查ISE中的网络资源配置。
- 将共享密钥与Catalyst Center > External Authentication下的配置进行比较。

示例：

Authentication Details

Generated Time 2025-09-11 18:22:24.078000 +00:00

Logged Time 2025-09-11 18:22:24.078

Epoch Time (sec) 1757614944

ISE Node ise-mxc1

Message Text Failed-Attempt: Authentication failed

Failure Reason 13011 Invalid TACACS+ request packet - possibly mismatched Shared Secrets

Resolution

Root Cause

Username

Network Device Name Catalyst-Center_6

Network Device IP 10.88.244.160

Network Device Groups IPSEC#Is IPSEC Device#No,DNAC#DNAC Devices,Location#All Locations,Device Type#All Device Types

Device Type Device Type#All Device Types

Location Location#All Locations

Device Port

Remote Address

共享密钥不匹配

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。