

配置最初3.1 TACACS认证ISE 2.x

目录

[简介](#)

[要求](#)

[配置](#)

[填装配置](#)

[ISE配置](#)

[故障排除](#)

简介

本文描述如何配置头等基础设施通过与ISE 2.x的TACACS验证。

要求

思科建议您有这些主题基础知识：

- 身份服务引擎(ISE)
- 头等基础设施

配置

思科最初网络控制系统3.1

思科身份服务引擎2.0或以上。

(注意:ISE只支持开始与版本2.0的TACACS，然而配置最初使用Radius是可能的。最初包括RADIUS属性列表除TACACS之外，如果您会喜欢使用Radius，与ISE或第三方解决方案早版本。)

头等配置

对以下屏幕的Navigate：管理/用户用户、角色& AAA如下所示。

一旦那里，选择TACACS+服务器选项卡，然后请选择在右上角的添加TACACS+服务器选项，并且精选请去。

在Next屏幕上TACACS服务器条目的配置是可用的(这将必须为每个单个TACACS服务器执行)

Administration / Users / Users, Roles & AAA

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

Add TACACS+ Server

IP Address
 DNS Name
 * Port
 Shared Secret Format
 * Shared Secret
 * Confirm Shared Secret
 * Retransmit Timeout (secs)
 * Retries
 Authentication Type
 Local Interface IP

Save Cancel

您将需要输入服务器的IP地址或DNS地址，以及共享密钥。并且请注意您希望使用的本地接口IP，此同样IP地址在ISE需要稍后用于AAA客户端。

为了完成在最初的配置。您将需要启用TACACS在管理/用户/用户、角色& AAA下在AAA模式设置选项卡下。

(注意:推荐检查Enable (event) fallback到仅地方选择权，与在服务器响应或无响应或失败选项，特别是当测试配置)时

Administration / Users / Users, Roles & AAA

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

AAA Mode Settings

AAA Mode Local RADIUS TACACS+ SSO

Enable fallback to Local ONLY on no server respon:

Save

ISE配置

配置最初作为ISE的一个AAA客户端在工作区/设备管理/network资源/network设备/添加

Identity Services Engine

Home Context Visibility Operations Policy Administration Work Centers License Warning

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration

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

Network Devices

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete Show All

Name	IP/Mask	Profile Name	Location	Type	Description
No data available					

输入头等服务器的信息。您需要包括的需要的属性命名，IP地址，选择TACACS和共享塞克雷的选项。您可以另外希望添加设备类型，特别地最初，为了稍后使用作为一个条件对于授权规则或其他信息，然而这可选。

Network Devices List > New Network Device

Network Devices

* Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

Location

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device
 TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

然后请创建TACACS配置文件结果发送从ISE的需要的属性填装，提供正确级别访问。导航对工作区/Policy结果/TACACS配置文件并且选择添加选项。

Identity Services Engine

Home > Operations > Policy > Guest Access > Administration > Work Centers

TrustSec > Device Administration

Overview > Identities > User Identity Groups > Network Resources > Network Device Groups > Policy Conditions > Policy Results

TACACS Command Sets

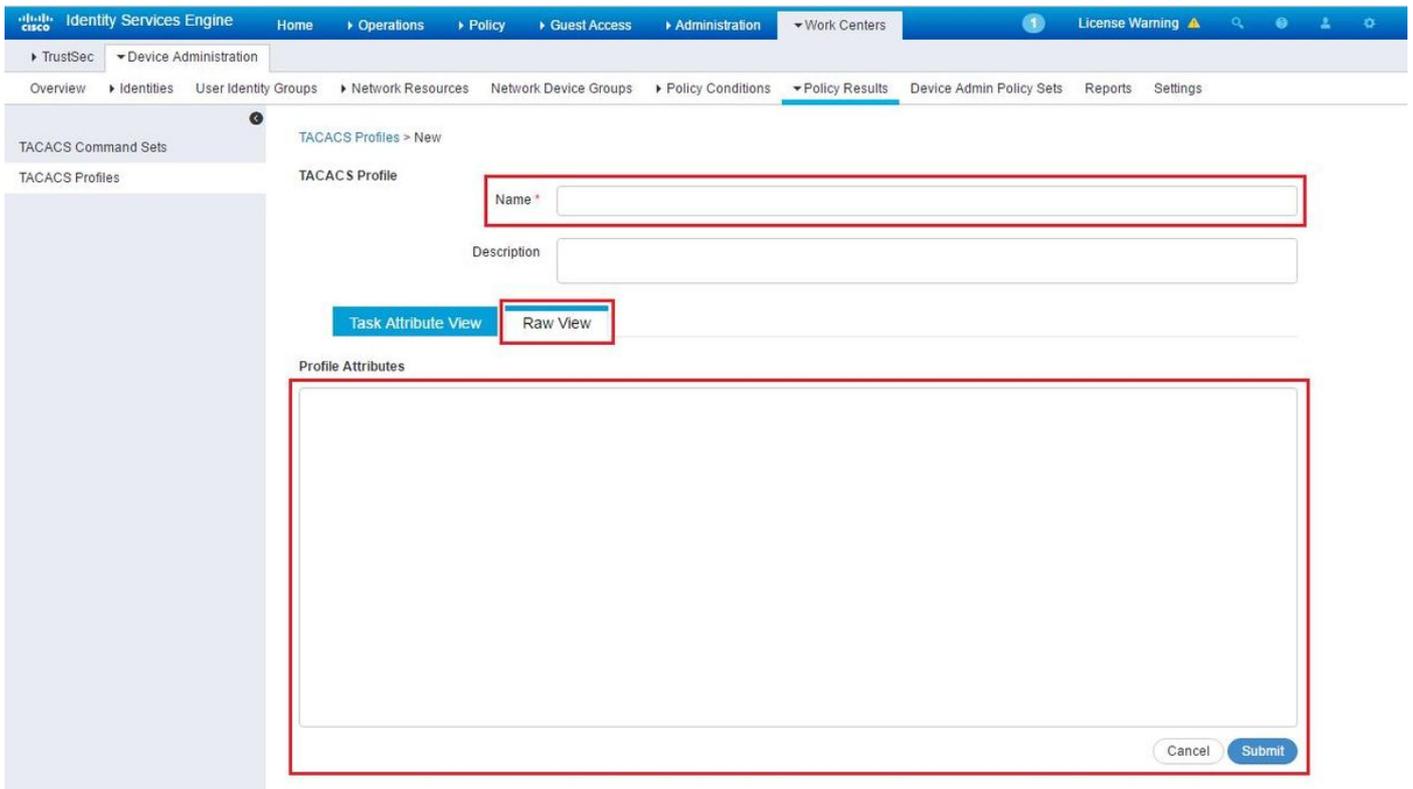
TACACS Profiles

Rows/Page 6 1 / 1 Go 6 Total Rows

Refresh **Add** Duplicate Trash Edit Filter

Name	Description

配置名称，并且请使用原始查看选项卡为了输入属性在配置文件属性方框下。属性将来自初级读本服务器。



获得属性在管理/用户用户、角色& AAA屏幕下，并且选择用户组选项卡。您选择您希望提供访问的社团级别。在此示例Admin选择适当的任务列表提供访问在左边。

Administration / Users / Users, Roles & AAA

AAA Mode Settings	User Groups			
Active Sessions	Group Name	Members	Audit Trail	View Task
Change Password	Admin	JP		Task List
Local Password Policy	Config Managers			Task List
RADIUS Servers	Lobby Ambassador	User1 , CostaRica , Yita		Task List
SSO Server Settings	Monitor Lite			Task List
SSO Servers	NBI Credential			Task List
TACACS+ Servers	NBI Read			Task List
User Groups	NBI Write			Task List
Users	North Bound API			Task List
	Root	root		Task List
	Super Users			Task List
	System Monitoring			Task List
	User Assistant			Task List
	User Defined 1			Task List
	User Defined 2			Task List
	User Defined 3			Task List
	User Defined 4			Task List
	mDNS Policy Admin			Task List

复制所有TACACS自定义属性。

AAA Mode Settings

Active Sessions

Change Password

Local Password Policy

RADIUS Servers

SSO Server Settings

SSO Servers

TACACS+ Servers

User Groups

Users

Task List

Please copy and paste the appropriate protocol data below into the custom/vendor-specific attribute field in your AAA server.

TACACS+ Custom Attributes

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
task14=Incidents Alarms Events Access
task15=TAC Case Management Tool
task16=Configure Autonomous Access Point Templates
task17=Import Policy Update
task18=PnP Profile Read-Write Access
task19=SSO Server AAA Mode
task20=Alarm Resource Access
```

RADIUS Custom Attributes

If the size of the RADIUS attributes on your AAA server is more than 4096 bytes, Please copy ONLY role attributes, application will retrieve the associated TASKS

```
NCS:role0=Admin
NCS:task0=Discovery Schedule Privilege
NCS:task1=Mesh Reports
NCS:task2=Saved Reports List
NCS:task3=Monitor Menu Access
NCS:task4=Device WorkCenter
NCS:task5=Inventory Menu Access
NCS:task6=Add Device Access
NCS:task7=Config Audit Dashboard
NCS:task8=Custom NetFlow Reports
NCS:task9=Apic Controller Read Access
NCS:task10=Configuration Templates Read Access
NCS:task11=Alarm Policies Edit Access
NCS:task12=High Availability Configuration
NCS:task13=View Job
NCS:task14=Incidents Alarms Events Access
NCS:task15=TAC Case Management Tool
NCS:task16=Configure Autonomous Access Point Templates
NCS:task17=Import Policy Update
NCS:task18=PnP Profile Read-Write Access
NCS:task19=SSO Server AAA Mode
NCS:task20=Alarm Resource Access
```

Virtual Domain custom attributes are mandatory. To add custom attributes related to Virtual Domains, please click [here](#).

然后请粘贴他们在配置文件的原始视图部分在ISE的。

Identity Services Engine

Home Operations Policy Guest Access Administration Work Centers

TrustSec Device Administration

Overview Identities User Identity Groups Network Resources Network Device Groups Policy Conditions Policy Results Device Admin Policy Sets Reports Settings

TACACS Command Sets

TACACS Profiles

TACACS Profiles > New

TACACS Profile

Name * Prime

Description

Task Attribute View Raw View

Profile Attributes

```
role0=Admin
task0=Discovery Schedule Privilege
task1=Mesh Reports
task2=Saved Reports List
task3=Monitor Menu Access
task4=Device WorkCenter
task5=Inventory Menu Access
task6=Add Device Access
task7=Config Audit Dashboard
task8=Custom NetFlow Reports
task9=Apic Controller Read Access
task10=Configuration Templates Read Access
task11=Alarm Policies Edit Access
task12=High Availability Configuration
task13=View Job
```

Cancel Submit

虚拟域自定义属性是必须。根域信息可以被找到在头等管理下 -> 虚拟域。

Cisco Prime Infrastructure

Virtual Domain ROOT-DOMAIN | root

Monitor Configuration Inventory Maps Services Reports Administration

Administration > Virtual Domains

Virtual Domains

Virtual Domains

ROOT-DOMAIN

Virtual Domains > ROOT-DOMAIN

ROOT-DOMAIN

Virtual domains are logical groupings of devices and are used to control who can administer a group. After you add devices to Prime Infrastructure, you can configure virtual domains. Virtual domain filters allow users to configure devices, view alarms, and generate reports their assigned part of the network only.

* Name ROOT-DOMAIN

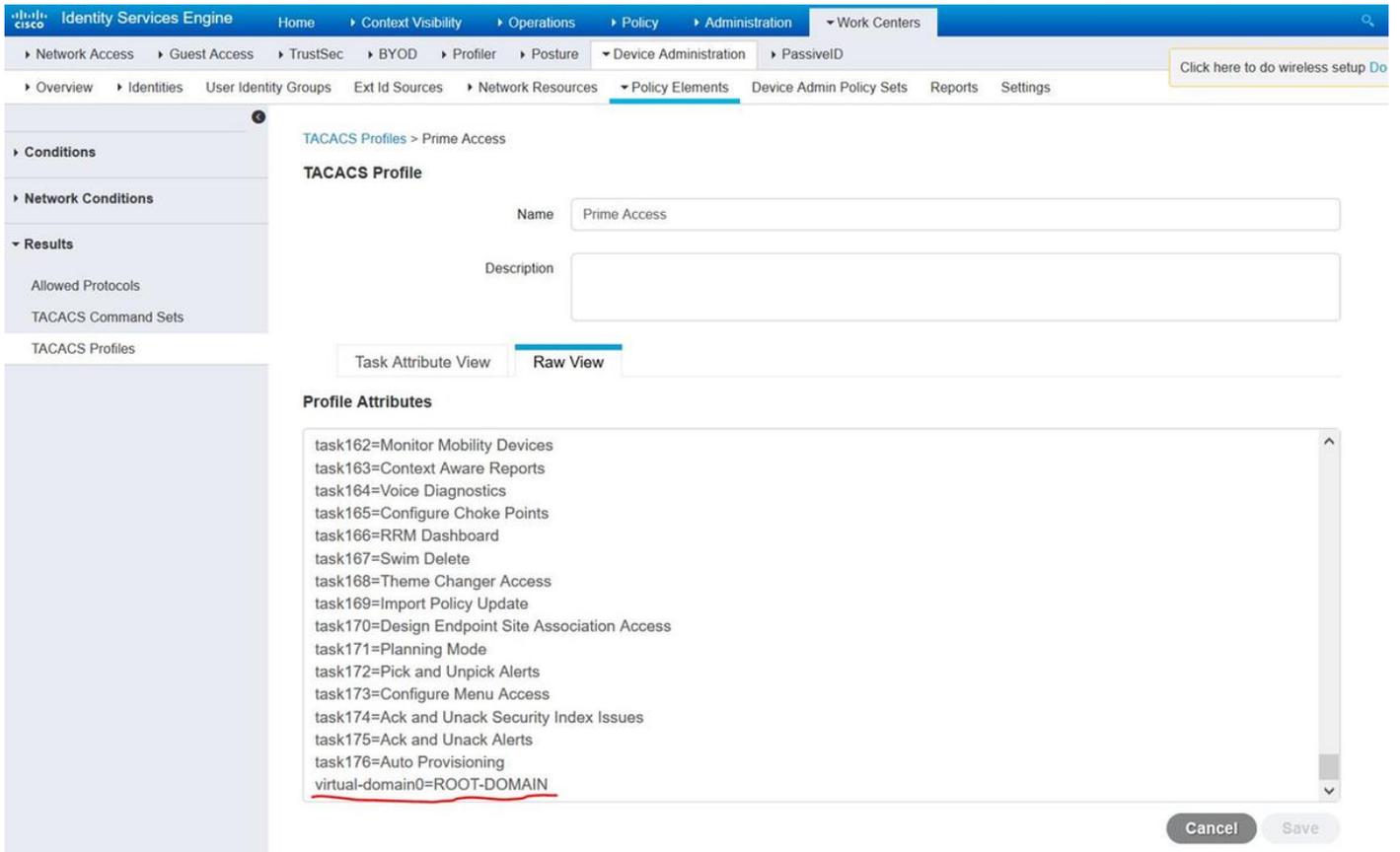
Time Zone -- Select Time Zone --

Email Address

Description ROOT-DOMAIN

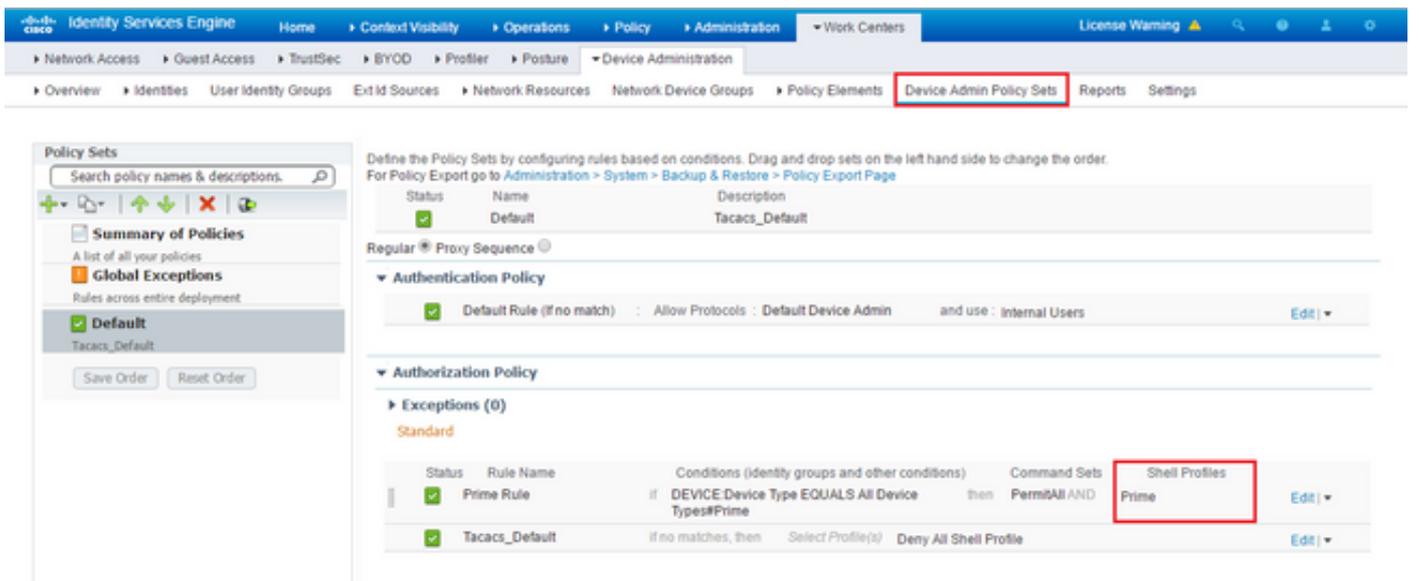
Submit Cancel

头等虚拟域名称必须被添加作为属性virtual-domain0="virtual域名”



一旦那执行所有您需要执行将创建规则分配在上一步创建的Shell配置文件，根据工作区/设备管理/设备Admin策略设置

(注意:“情况”根据部署将变化，然而您可以特定使用“设备类型”最初或另外一种过滤器例如最初的IP地址，作为一个“调节”，以便此规则适当地过滤请求)



这时配置应该完成。

故障排除

如果此配置不成功，并且，如果本地后退选项是在最初的enable (event)，您能通过删除最初的IP地址强制从ISE的一故障切换。这将造成ISE不响应和强制使用本地凭证。如果本地fallback在拒绝配置执行，本地帐户将运作并且提供存取对于客户。

如果ISE显示成功认证和匹配正确规则然而最初仍然拒绝您在配置文件可以希望将属性仔细检查正确地配置的请求，并且另外的属性没有发送。