

# Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Configurations](#)

[Add ACS as TACACS Server in PI](#)

[AAA Mode Settings in PI](#)

[Retrieve user role attributes from PI](#)

[Configure ACS 4.2](#)

[Verify](#)

[Troubleshoot](#)

## Introduction

This document describes the configuration example for Terminal Access Controller Access-Control System (TACACS+)

authentication and authorization on the Cisco Prime Infrastructure (PI) application.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Define PI as a client in the Access Control Server (ACS)
- Define the IP address and an identical shared-secret key on the ACS and PI

### Components Used

The information in this document is based on these software and hardware versions:

- ACS Version 4.2
- Prime Infrastructure release 3.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configure

### Configurations

## Add ACS as TACACS Server in PI

Complete these steps in order to add ACS as a TACACS server:

Step 1. Navigate to **Administration > Users > Users, Roles & AAA** in PI

Step 2. From the left sidebar menu, select **TACACS+ Servers**, under **Add TACACS+ servers** click **Go** and the page appears as shown in the image:

The screenshot shows the Cisco Prime Infrastructure interface. The breadcrumb navigation is Administration / Users / Users, Roles & AAA. The left sidebar menu includes AAA Mode Settings, Active Sessions, Change Password, Local Password Policy, RADIUS Servers, SSO Server Settings, SSO Servers, TACACS+ Servers (highlighted), User Groups, and Users. The main content area is titled 'Add TACACS+ Server' and contains the following fields:

- IP Address
- DNS Name
- \* Port: 49
- Shared Secret Format: ASCII
- \* Shared Secret
- \* Confirm Shared Secret
- \* Retransmit Timeout: 5 (secs)
- \* Retries: 1
- Authentication Type: PAP
- Local Interface IP: 10.106.68.130

Buttons: Save, Cancel

Step 3. Add the IP address of the ACS server.

Step 4. Enter the TACACS+ shared secret configured in ACS server.

Step 5. Re-enter the shared secret in the **Confirm Shared Secret** text box.

Step 6. Leave the rest of the fields on their default setting.

Step 7. Click **Submit**.

## AAA Mode Settings in PI

In order to choose an Authentication, Authorization, and Accounting (AAA) mode, complete these steps:

Step 1. Navigate to **Administration > AAA**.

Step 2. Choose **AAA Mode** from the left sidebar menu, you can see the page as shown in the image:



Step 3. Select **TACACS+**.

Step 4. Check the **Enable Fallback to Local** box, if you want the administrator to use the local database when the ACS server is not reachable. This is a recommended setting.

## Retrieve user role attributes from PI

Step 1. Navigate to **Administration > AAA > User Groups**. This example shows administrator authentication. Look for the **Admin Group Name** in the list and click the **Task List** option on the right, as shown in the image:

AAA Mode Settings	User Groups			
Active Sessions	Group Name	Members	Audit Trail	View Task
Change Password	<a href="#">Admin</a>	virtual		<a href="#">Task List</a>
Local Password Policy	<a href="#">Config Managers</a>			<a href="#">Task List</a>
RADIUS Servers	<a href="#">Lobby Ambassador</a>			<a href="#">Task List</a>
SSO Server Settings	<a href="#">Monitor Lite</a>			<a href="#">Task List</a>
SSO Servers	<a href="#">NBI Credential</a>			<a href="#">Task List</a>
TACACS+ Servers	<a href="#">NBI Read</a>			<a href="#">Task List</a>
User Groups	<a href="#">NBI Write</a>			<a href="#">Task List</a>
Users	<a href="#">North Bound API</a>			<a href="#">Task List</a>
	<a href="#">Root</a>	root		<a href="#">Task List</a>
	<a href="#">Super Users</a>			<a href="#">Task List</a>
	<a href="#">System Monitoring</a>	virtual		<a href="#">Task List</a>

Once you click **Task List** option, the window appears, as shown in the image:

### 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=View Alerts and Events
task1=Run Job
task2=Device Reports
task3=Alarm Stat Panel Access
task4=RADIUS Servers
task5=Raw NetFlow Reports
task6=Credential Profile Delete Access
task7=Compliance Audit Fix Access
task8=Network Summary Reports
task9=Discovery View Privilege
task10=Configure ACS View Servers
task11=Run Reports List
task12=View CAS Notifications Only
task13=Administration Menu Access
task14=Monitor Clients
task15=Configure Guest Users
task16=Monitor Media Streams
task17=Configure Lightweight Access Point
Templates
task18=Monitor Chokepoints
task19=Maps Read Write
task20=Administrative privileges under Manage and
```

#### RADIUS Custom Attributes

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

```
NCS:role0=Admin
NCS:task0=View Alerts and Events
NCS:task1=Run Job
NCS:task2=Device Reports
NCS:task3=Alarm Stat Panel Access
NCS:task4=RADIUS Servers
NCS:task5=Raw NetFlow Reports
NCS:task6=Credential Profile Delete Access
NCS:task7=Compliance Audit Fix Access
NCS:task8=Network Summary Reports
NCS:task9=Discovery View Privilege
NCS:task10=Configure ACS View Servers
NCS:task11=Run Reports List
NCS:task12=View CAS Notifications Only
NCS:task13=Administration Menu Access
NCS:task14=Monitor Clients
NCS:task15=Configure Guest Users
NCS:task16=Monitor Media Streams
NCS:task17=Configure Lightweight Access Point
Templates
NCS:task18=Monitor Chokepoints
NCS:task19=Maps Read Write
NCS:task20=Administrative privileges under Manage
```

Step 2. Copy these attributes and save it on a notepad file.

Step 3. You may need to add custom virtual domain attributes in the ACS server. Custom virtual domain attributes are available in the bottom of same Task list page.

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

Step 4. Click on **click here** option to get Virtual domain attribute page, and you can see the page, as shown in the image:



## Configure ACS 4.2

Step 1. Log in to the **ACS Admin GUI**, and navigate to **Interface Configuration > TACACS+** page.

Step 2. Create new service for prime. This example shows a service name configured with name **NCS**, as shown in the image:

### New Services

		Service	Protocol
<input checked="" type="checkbox"/>	<input type="checkbox"/>	ciscowlc	common
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Wireless-WCS	HTTP
<input checked="" type="checkbox"/>	<input type="checkbox"/>	NCS	HTTP
<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	<input type="checkbox"/>		

Step 3. Add all the attributes from notepad created in Step 2 to user or Group configuration. Ensure to add virtual-domain attributes.

**NCS HTTP**

**Custom attributes**

```
virtual-domain0=ROOT-DOMAIN
role0=Admin
task0=View Alerts and Events
task1=Device Reports
task2=RADIUS Servers
task3=Alarm Stat Panel Access
```

Step 4. Click **Ok**.

## Verify

Log in to the prime with the new user name you created and confirm that you have the **Admin** role.

# Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Review `usermgmt.log` from prime root CLI available in `/opt/CSCOlumos/logs` directory. Check if there are any error messages.

This example shows a sample of error message, which could be due to various reasons like connection refused by a firewall, or any intermediate device etc.