

# Configure TACACS+ Authentication on CIMC with ISE Server

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[TACACS+ Server-Side Configuration for Privilege Association](#)

[ISE Configuration Requirements](#)

[TACACS+ Configuration on CIMC](#)

[Verify](#)

[Verify Configuration from CLI in CIMC](#)

[Troubleshoot](#)

[ISE Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes the configuration of Terminal Access Controller Access-Control System Plus (TACACS+) authentication on Cisco Integrated Management Controller (CIMC).

TACACS+ is commonly used to authenticate network devices with a central server. Since release version 4.1(3b), Cisco IMC supports TACACS+ authentication. TACACS+ support on CIMC eases the effort to manage multiple user accounts that have access to the device. This feature is of help to periodically change user's credentials and manage user accounts remotely.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Integrated Management Controller (CIMC)
- Terminal Access Controller Access-Control System Plus (TACACS+)

### Components Used

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

- UCSC-C220-M4S
- CIMC Version: 4.1(3b)
- Cisco Identity Services Engine (ISE) version 3.0.0.458

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, ensure that you understand the potential impact of any command.

## Configure

### TACACS+ Server-Side Configuration for Privilege Association

The privilege level of the user is calculated based on the **cisco-av-pair** value configured for that user. A **cisco-av-pair** needs to be created on the TACACS+ server for and users cannot use any default TACACS+ attributes. The three syntaxes as shown below are supported for the **cisco-av-pair** attribute

For **admin** privilege:

```
cisco-av-pair=shell:roles="admin"
```

For **user** privilege:

```
cisco-av-pair=shell:roles="user"
```

For **read-only** privilege:

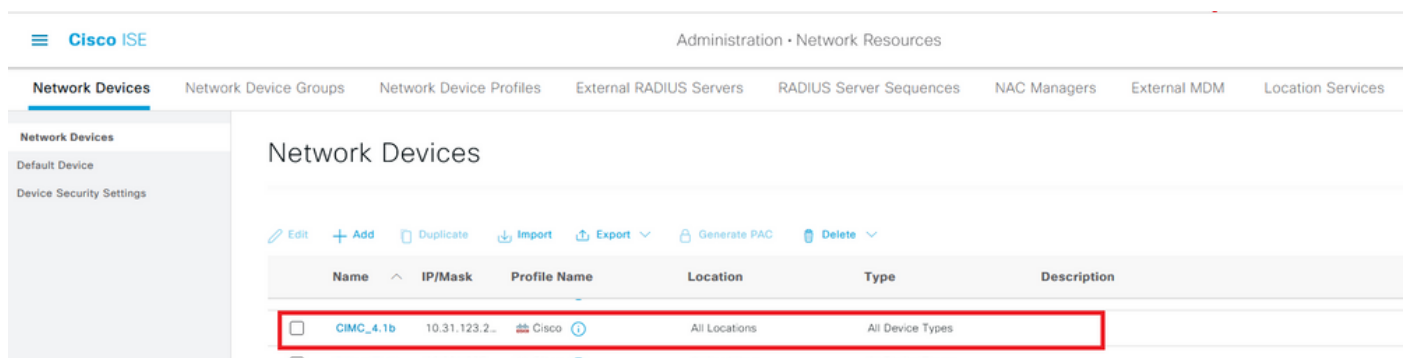
```
cisco-av-pair=shell:roles="read-only"
```

To support other devices, if other roles need to be added then they can be added with a comma as a separator. For example, UCSM supports **aaa**, so **shell:roles="admin,aaa"** can be configured and CIMC accepts this format.

**Note:** If **cisco-av-pair** is not configured on the TACACS+ server, then a user with that server has a **read-only** privilege.

### ISE Configuration Requirements

The management IP of the server must be allowed on the ISE Network Devices.



The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration · Network Resources'. Below this, there are several tabs: 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', 'NAC Managers', 'External MDM', and 'Location Services'. The 'Network Devices' tab is selected. On the left, there is a sidebar with 'Network Devices', 'Default Device', and 'Device Security Settings'. The main content area is titled 'Network Devices' and contains a table with columns: Name, IP/Mask, Profile Name, Location, Type, and Description. The table has two rows. The first row is highlighted with a red box and contains: 'CIMC\_4.1b', '10.31.123.2...', 'Cisco', 'All Locations', 'All Device Types', and an empty description. The second row contains: 'Prima\_Test', '10.201.232', 'Cisco', 'All Locations', 'All Device Types', and an empty description. Above the table, there are several action buttons: Edit, Add, Duplicate, Import, Export, Generate PAC, and Delete.

Shared Secret password to be entered on CIMC.

Network Devices

Network Device Groups

Network Device Profiles

External RADIUS Servers

RADIUS Server

Network Devices

Default Device

Device Security Settings

Network Devices List > CIMC\_4.1b

Network Devices

\* Name CIMC\_4.1b

Description

IP Address \* IP: 10.31.123.27 / 32

\* Device Profile Cisco

Model Name

Software Version

\* Network Device Group

Location All Locations

IPSEC No

Device Type All Device Types

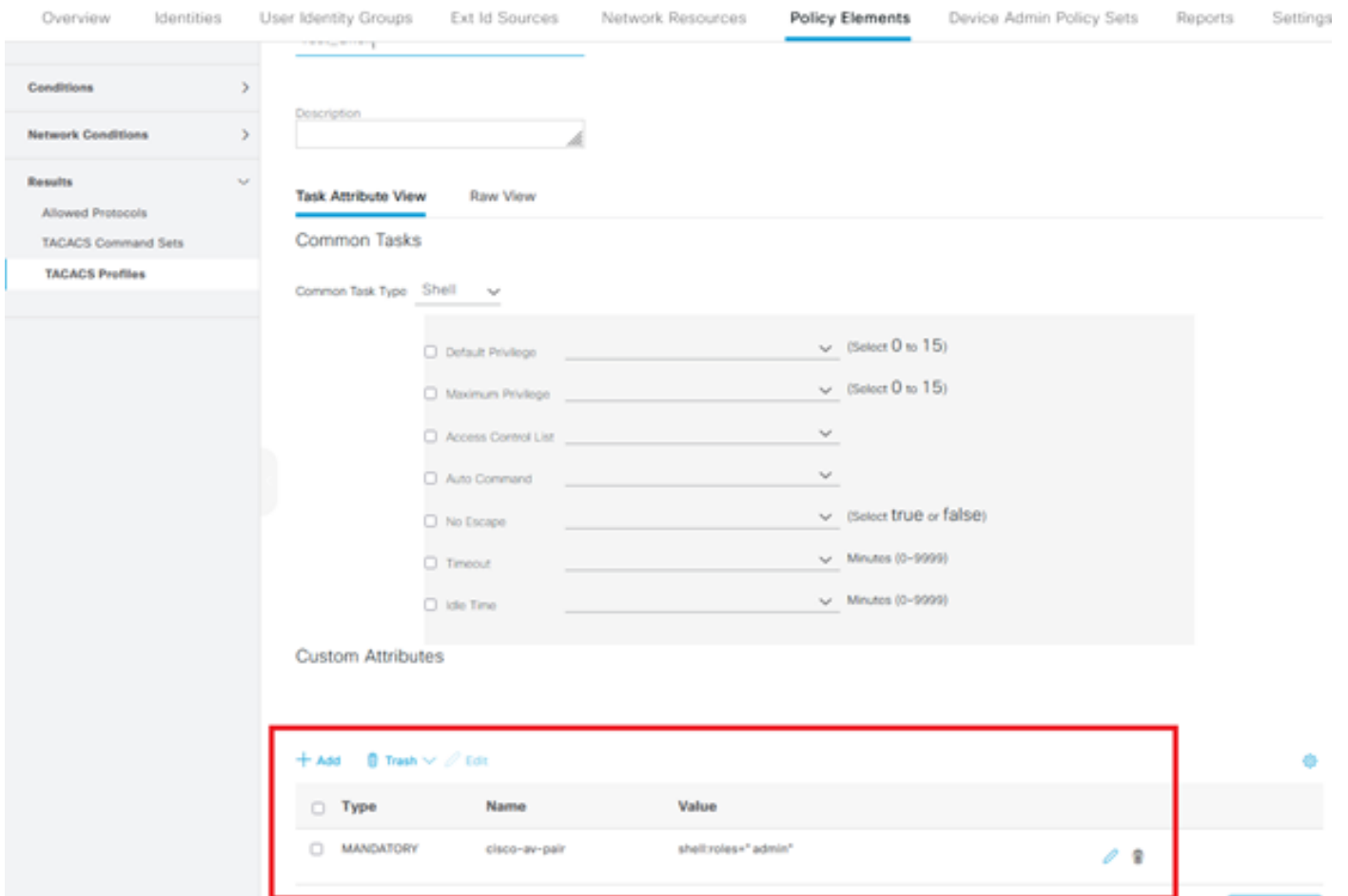
TEST TEST

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret Cisco123

Shell Profile with **cisco-av-pair** attribute with admin permissions.



## TACACS+ Configuration on CIMC

Step 1. Navigate to **Admin > User Management > TACACS+**

Step 2. Select the checkbox to enable **TACACS+**

Step 3. A new server can be added at any of the 6 rows specified in the table. Click on the row or select the row and click on the **edit** button on top of the table, as shown in this image.

### TACACS+ Properties

Enabled:  1 ←

Fallback only on no connectivity:

Timeout (for each server):  (5 - 30 Seconds)

### Server List

Selected 0 / Total 6

ID	IP Address or Host Name	Port	Server Key
<input type="radio"/> 1			
<input type="radio"/> 2			
<input type="radio"/> 3			
<input type="radio"/> 4			
<input type="radio"/> 5			
<input type="radio"/> 6			

**Note:** In the case where a user has enabled TACACS+ fallback on no connectivity option, CIMC enforces that the first authentication precedence must always be set to TACACS+ otherwise the fallback configuration might become irrelevant.

Step 4. Fill in the IP address or hostname, port, and Server key/Shared secret and **Save** the configuration.

### Server List

Selected 0 / Total 6

ID	IP Address or Host Name	Port	Server Key	Confirm Server Key
1	<input type="text" value="10.31.126.220"/>	<input type="text" value="49"/>	<input type="text" value="*****"/>	<input type="text" value="*****"/>
2				
3				
4				
5				

Save | Cancel

3 ↑

Cisco IMC supports up to six TACACS+ remote servers. Once a user is successfully authenticated, the username is appended with (TACACS+).



Refresh | ? | i

This is also displayed in the Session Management

### Sessions

Selected 0 / Total 1 ⚙

Terminate Session				
	Session ID	User Name	IP Address	Session Type
<input type="checkbox"/>	81	tacacs_user (TACACS+)	10.24.92.202	webgui

## Verify

- A maximum of 6 TACACS+ servers can be configured on the CIMC.
- The secret key associated with the server can be of a maximum 64 characters in length.
- The timeout can be configured between 5 and 30 seconds (which evaluates to the max as 180 seconds to be in line with LDAP).
- If a TACACS+ server needs to use the service name to create the **cisco-av-pair**, then users need to use **Log in** as the service name.
- No redfish support to modify the configurations.

## Verify Configuration from CLI in CIMC

- Verify if TACACS+ is enabled.

```
C220-WZP22460WCD# scope tacacs+
C220-WZP22460WCD /tacacs+ # show detail
TACACS+ Settings:
Enabled: yes
Fallback only on no connectivity: no
Timeout(for each server): 5
```

- Verify configuration details per server.

```
C220-WZP22460WCD /tacacs+ # scope tacacs-server 1
C220-WZP22460WCD /tacacs+/tacacs-server # show detail
Server Id 1:
Server IP address/Hostname: 10.31.126.220
Server Key: *****
Server Port: 49
```

## Troubleshoot

- Ensure that TACACS+ Server IP is reachable from the CIMC and the port is configured correctly.
- Ensure that the **cisco-av-pair** is correctly configured on the TACACS+ server.
- Check if the TACACS+ server is reachable (IP and port).
- Make sure the secret key or credentials match with the ones configured on the TACACS+ server.
- If you can log in with TACACS+ but only have **read-only** permissions, verify if cisco-av-pair has the correct syntax on the TACACS+ server.

## ISE Troubleshoot

- Verify Tacacs Live logs for one of the authentication attempts. Status must be **Pass**.

### Overview

Request Type	Authorization
Status	Pass
Session Key	ise30baaamex/408819883/155352
Message Text	Device-Administration: Session Authorization succeeded
Username	tacacs_user
Authorization Policy	New Policy Set 1 >> Authorization Rule 1
Shell Profile	Test_Shell
Matched Command Set	
Command From Device	

- Verify the response has the correct **cisco-av-pair** attribute configured.

## Other Attributes

ConfigVersionId	933
DestinationIPAddress	10.31.126.220
DestinationPort	49
UserName	tacacs_user
Protocol	Tacacs
RequestLatency	53
Type	Authorization
Service-Argument	login
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
AuthenticationIdentityStore	Internal Users
AuthenticationMethod	Lookup
SelectedAccessService	Default Device Admin
IdentityGroup	User Identity Groups:ALL_ACCOUNTS (default)
SelectedAuthenticationIdenti...	Internal Users
AuthenticationStatus	AuthenticationPassed
UserType	User
CPMSessionID	50617983410.31.123.2734354Authorization506179834
IdentitySelectionMatchedRule	Default
TEST	TEST#TEST
Network Device Profile	Cisco
IPSEC	IPSEC#Is IPSEC Device#No
EnableFlag	Enabled
Response	{Author-Reply-Status=PassAdd; AVPair=cisco-av-pair=shell:roles=" admin" ; }

## Related Information

- [TACACS+ Authentication Cisco UCS-C](#)
- [Technical Support & Documentation - Cisco Systems](#)
- [Configure ISE 2.0: IOS TACACS+ Authentication and Command Authorization based on AD group membership](#)