

Configure TACACS+ Authentication Domain on UCS Manager with ISE Server

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration](#)

[TACACS+ Configuration on ISE](#)

[Setup of TACACS+ on ISE](#)

[Configure the attributes and rules on ISE](#)

[TACACS+ Configuration on UCSM](#)

[Create roles for users](#)

[Create a TACACS+ Provider](#)

[Create a TACACS+ Provider Group](#)

[Create an Authentication Domain](#)

[Troubleshoot](#)

[Common TACACS+ Issues on UCSM](#)

[UCSM Review](#)

[Common TACACS Issues on ISE](#)

[ISE Review](#)

[Related Information](#)

Introduction

This document describes the configuration of Terminal Access Controller Access-Control System Plus (TACACS+) authentication on Unified Compute System Manager (UCSM). TACACS+ is a network protocol that is used for Authentication, Authorization and Accountability services (AAA), it provides a centralized method to manage Network Access Devices (NAD) where you can administer and create rules through a server, in this use case scenario we will use Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco UCS Manager (UCSM)
- Terminal Access Controller Access-Control System Plus (TACACS+)
- Identity Services Engine (ISE)

Components Used

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

- UCSM 4.2(3d)
- Cisco Identity Services Engine (ISE) version 3.2

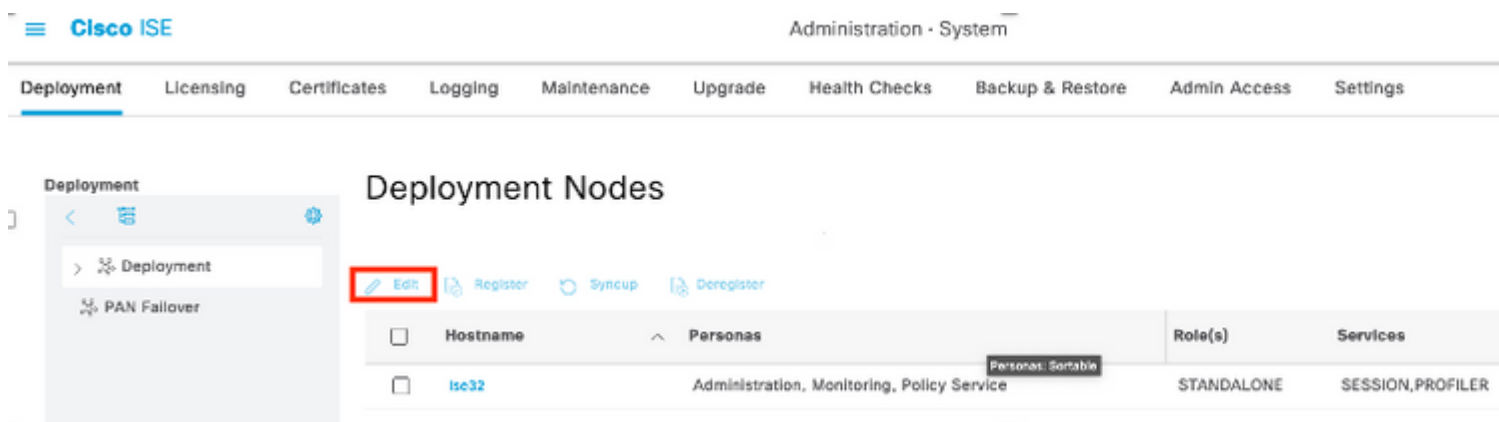
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configuration

TACACS+ Configuration on ISE

Setup of TACACS+ on ISE

Step 1. The first task is to review if the ISE has the correct capabilities to handle TACACS+ authentications for such you need to check if within the Policy Service Node (PSN) desired you have the feature for **Device Admin Service**, browse through the menu **Administration > System > Deployment**, select the node where the ISE will perform TACACS+ and then select the button edit.



The screenshot shows the Cisco ISE Administration console. The top navigation bar includes 'Cisco ISE' and 'Administration - System'. Below this is a menu with 'Deployment', 'Licensing', 'Certificates', 'Logging', 'Maintenance', 'Upgrade', 'Health Checks', 'Backup & Restore', 'Admin Access', and 'Settings'. The 'Deployment' menu is expanded, showing 'Deployment' and 'PAN Failover'. The main content area is titled 'Deployment Nodes' and contains a table with columns for 'Hostname', 'Personas', 'Role(s)', and 'Services'. The 'isc32' node is listed with the personas 'Administration, Monitoring, Policy Service'. The 'Edit' button for this node is highlighted with a red box. A tooltip for 'Personas: Sortable' is visible over the 'Personas' column.

Hostname	Personas	Role(s)	Services
isc32	Administration, Monitoring, Policy Service	STANDALONE	SESSION, PROFILER

Step 2. Scroll down until you see the corresponding feature called **Device Administration Service** (notice that for this feature to be enabled you need first to have Policy Server persona enabled on the node and moreover have licenses for TACACS+ available in your deployment), select that checkbox, and then save the configuration:

Cisco ISE Administration - System

Deployment | Licensing | Certificates | Logging | Maintenance | Upgrade | Health Checks | Backup & Restore | Admin Access | Settings

Other Monitoring Node

Dedicated Mnt

Policy Service

Enable Session Services

Include Node in Node Group: None

Enable Profiling Service

Enable Threat Centric NAC Service

Enable SXP Service

Enable Device Admin Service

Enable Passive Identity Service

pxGrid

Step 3. Configure the Network Access Device (NAD) that will use the ISE as TACACS+ as server, navigate to the menu **Administration > Network Resources > Network Devices** then select the button **+Add**.

Cisco ISE Administration - Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences

Network Devices

Default Device

Device Security Settings

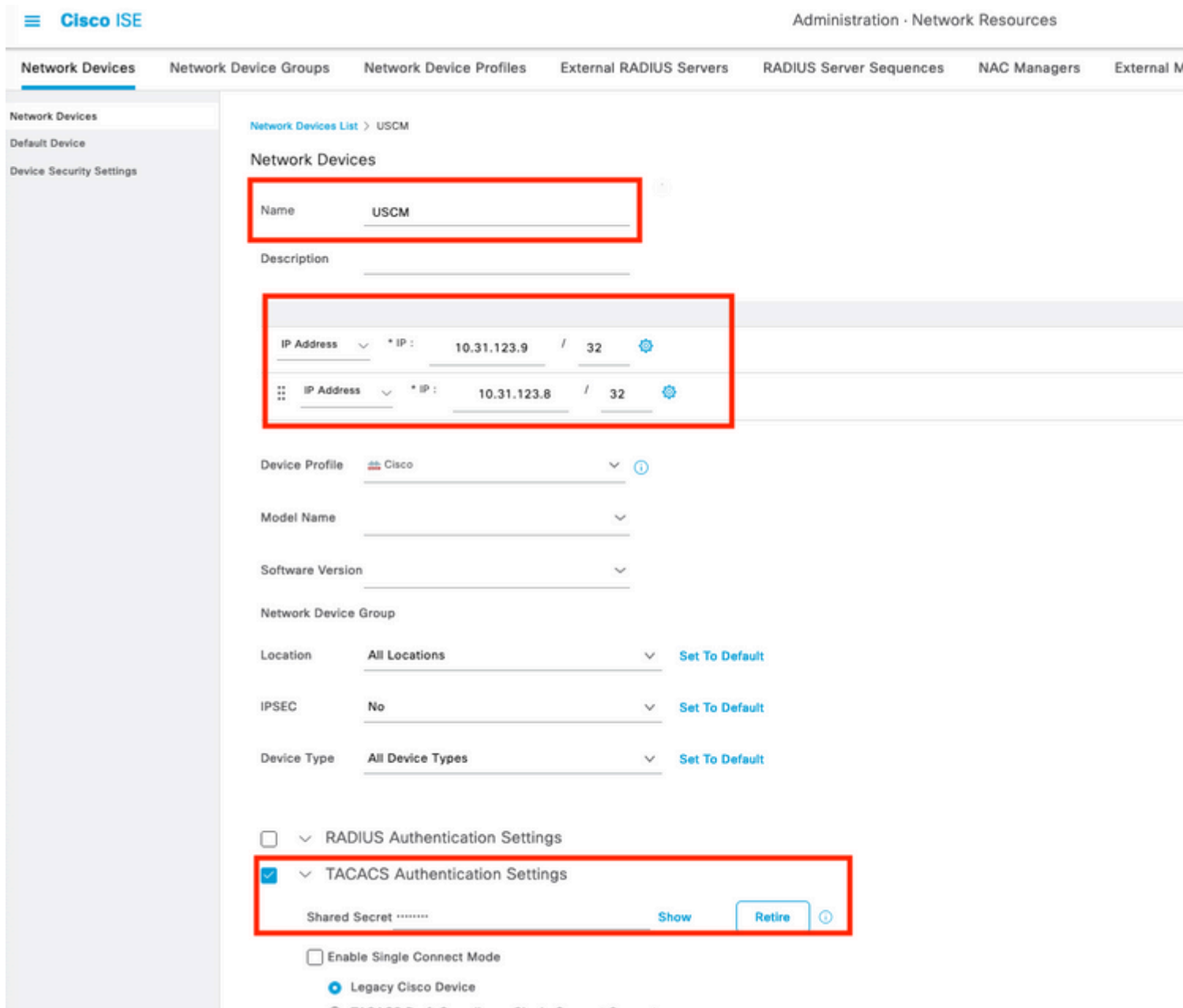
Network Devices

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type
No data					

Step 4. In this section configure :

- A name for the UCSM to be the TACACS+ client.
- The IP addresses that the UCSM use to send request to ISE.
- TACACS+ Shared Secret , this is the password that will be used to encrypt the packets between the

UCSM and ISE



Note: For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Manager.


Configure the attributes and rules on ISE

Step 1. Create a TACACS+ profile, navigate to the menu **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**, then select **Add**

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

Conditions >
Network Conditions >
Results v
Allowed Protocols
TACACS Command Sets
TACACS Profiles

TACACS Profiles

 **Add** Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile

Step 2. In this section configure the profile with a name and in the **Custom Attributes** section, select **Add**, next create a one attribute of characteristic MANDATORY, name it as cisco-av-pair and in the value select one of the roles available within the UCSM and input that as a shell role, in this example it will be used the role admin and the input selected needs to be `shell:roles=admin` as it shown below,

- Conditions >
- Network Conditions >
- Results v
 - Allowed Protocols
 - TACACS Command Sets
 - TACACS Profiles

Name
UCSM PROFILE ADMIN

Description

Task Attribute View **Raw View**

Common Tasks

Common Task Type **Shell** v

- Default Privilege _____ v (Select 0 to 15)
- Maximum Privilege _____ v (Select 0 to 15)
- Access Control List _____ v
- Auto Command _____ v
- No Escape _____ v (Select true or false)
- Timeout _____ v Minutes (0-9999)
- Idle Time _____ v Minutes (0-9999)

Custom Attributes

Add Trash v Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	cisco-av-pair	shell:roles=" admin"

In the same menu if you select the **Raw View** for the TACACS Profile, you can verify the corresponding configuration of the attribute that will be sent through ISE.

Overview Identities User Identity Groups Ext Id Sources Network Resources **Policy Elements** Device Administration

TACACS Profiles > UCSM PROFILE ADMIN
TACACS Profile

Name
UCSM PROFILE ADMIN

Description

Task Attribute View **Raw View**

Profile Attributes
cisco-av-pair=shell:roles=" admin"

Cancel Save

Note: The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider.

Step 3. Select on the tick and save your configuration.

Step 4. Create a **Device Admin Policy Set** to be used for your UCSM, navigate the menu **Work Centers > Device Administration > Device Admin Policy Sets**, then from an existent policy set select the gear icon to then select **Insert** new row above

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

Status	Policy Set Name	Description	Conditions
Default		Tacacs Default policy set	

Step 5. Name this new **Policy Set**, add conditions depending upon the characteristics of the TACACS+ authentications that will be ongoing from the UCSM server, and select as **Allowed Protocols > Default Device Admin**, save your configuration.

Policy Sets

Status	Policy Set Name	Description	Conditions
●	USCM ACCESS		DEVICE-Device Type EQUALS All Device Types
●	Default	Tacacs Default policy set	

Step 6. Select in the > view option and select in the **Authentication Policy** section, the external identity source from where the ISE will query the username and credentials that will be input in the UCSM, in this example the credentials correspond to Internal Users stored within ISE.

Policy Sets → USCM ACCESS

Status	Policy Set Name	Description	Conditions
●	USCM ACCESS		DEVICE-Device Type EQUALS All Device Types
Authentication Policy (1)			
Status	Rule Name	Conditions	
●	Default		

Step 7. Scroll down until the section named **Authorization Policy** until the **Default policy**, select the gear icon, and then insert one rule above.

Step 8. Name the new Authorization Rule, add conditions concerning the user that will be authenticated already as group membership, and in the **Shell Profiles** section add the TACACS profile that you configured previously, **save** the configuration.

Status	Rule Name	Conditions	Results	Command Sets
●	USCM ADMIN	InternalUser-IdentityGroup EQUALS User Identity Groups:Employee	Select from list	
●	Default		DenyAllCommand	

TACACS+ Configuration on UCSM

Log into Cisco UCS Manager GUI with a user with administrator privileges.

Create roles for users

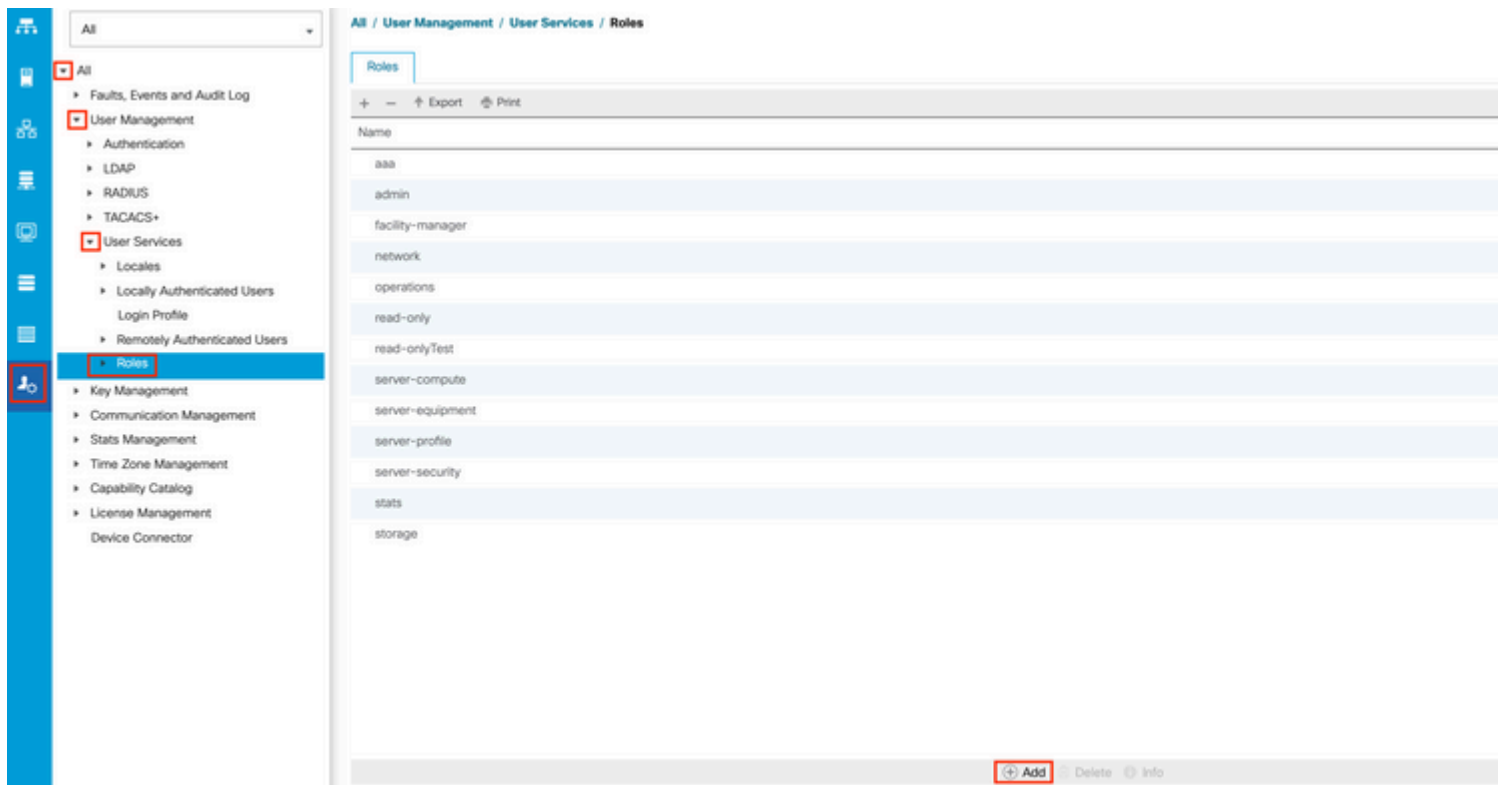
Step 1. In the Navigation pane, select the **Admin** tab.

Step 2. On the **Admin** tab, expand **All > User Management > User Services > Roles**.

Step 3. In the **Workpane**, select the **General** tab.

Step 4. Select **Add** for custom roles. This sample use default **Roles**.

Step 5. Verify name role matches with name configured previously on TACACS profile.



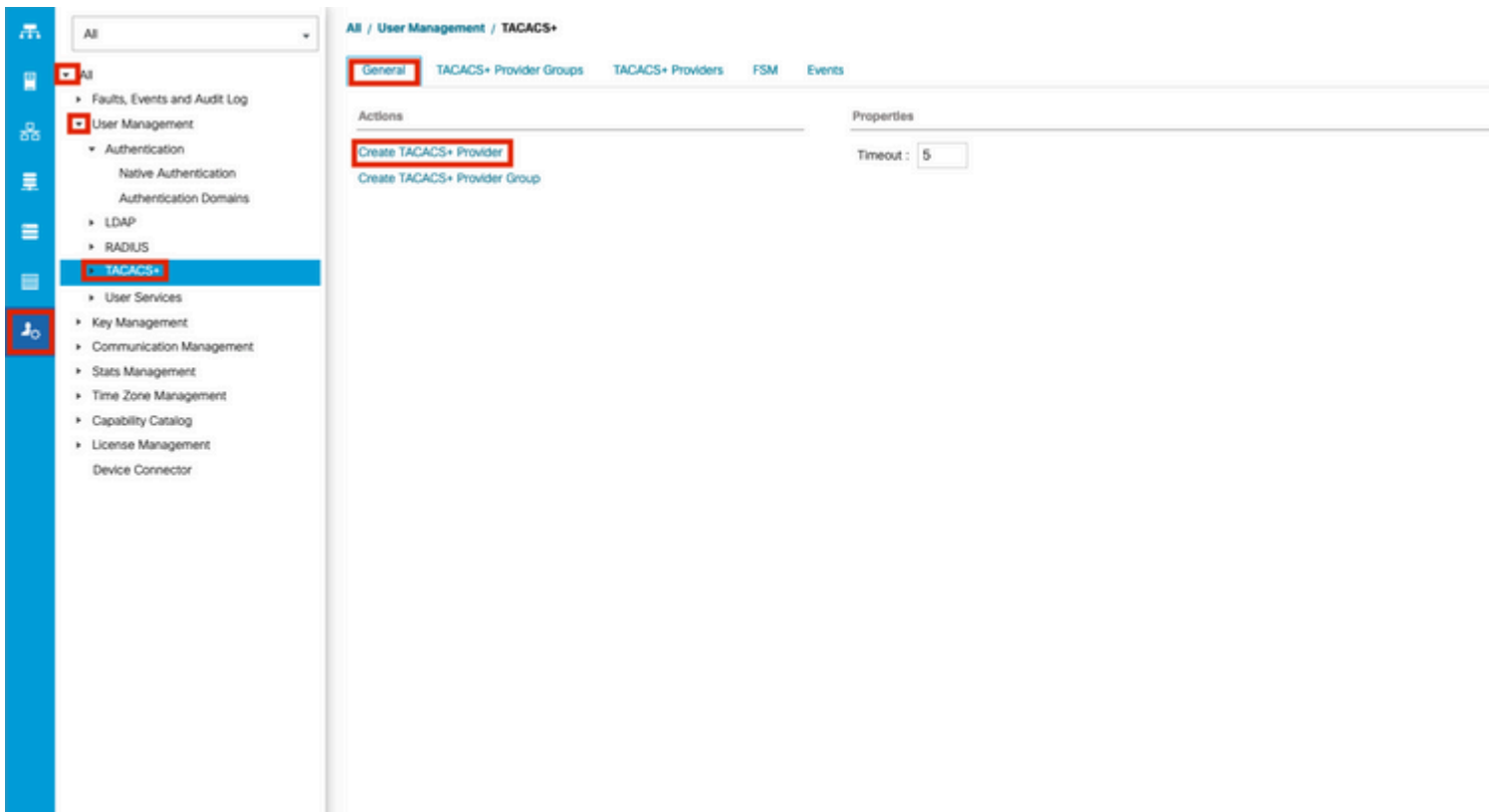
Create a TACACS+ Provider

Step 1. In the Navigation pane, select the **Admin** tab.

Step 2. On the **Admin** tab, expand **All > User Management > TACACS+**.

Step 3. In the **Workpane**, select the **General** tab.

Step 4. In the **Actions** area, select **Create TACACS+ Provider**.



â€f

Step 5. In the **Create TACACS+ Provider** wizard, input the appropriate information.

- In the **Hostname** field, type the IP address or hostname of TACACS+ Server.
- In the **Order** field, The order in which Cisco UCS uses this provider to authenticate users.

Enter an integer between 1 and 16, or enter lowest-available or 0 (zero) if you want Cisco UCS to assign the next available order based on the other providers defined in this Cisco UCS instance.

- In the **Key** field, The SSL encryption key for the database.
- In the **Confirm Key** field, The SSL encryption key repeated for confirmation purposes.
- In the **Port** field, The port through which Cisco UCS communicate with the TACACS+ database (Port 49 default port).
- In the **Timeout** field, The length of time in seconds the system spend trying to contact the TACACS+ database before it times out.

Create TACACS+ Provider

Hostname/FQDN (or IP Address) : 10.31.123.57

Order : lowest-available

Key : *****

Confirm Key : *****

Port : 49

Timeout : 5

OK Cancel

Step 6. Select **Ok**.

Note: If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.

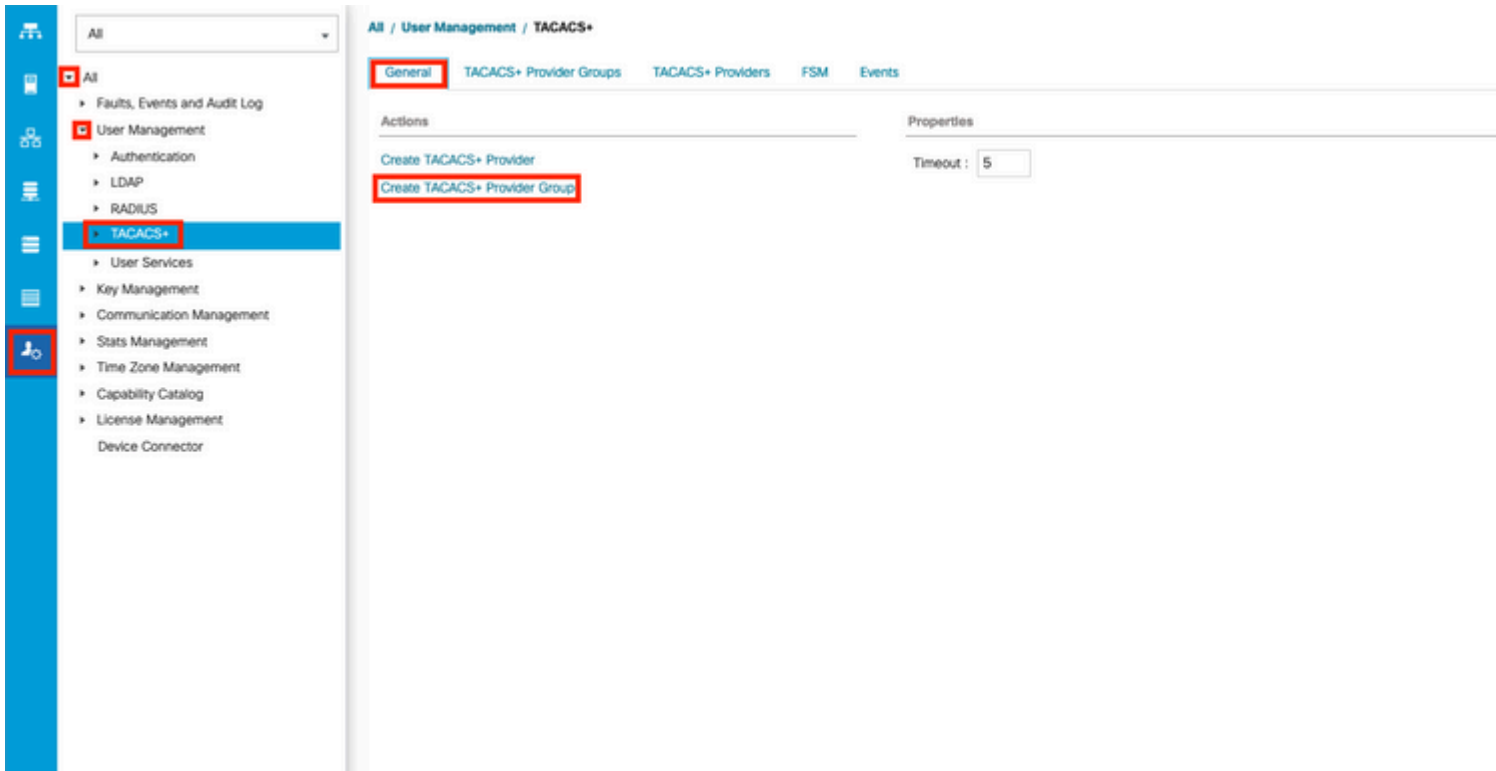
Create a TACACS+ Provider Group

Step 1. In the **Navigation** pane, select the **Admin** tab.

Step 2. On the **Admin** tab, expand **All > User Management > TACACS+**.

Step 3. In the **Work** pane, select the **General** tab.

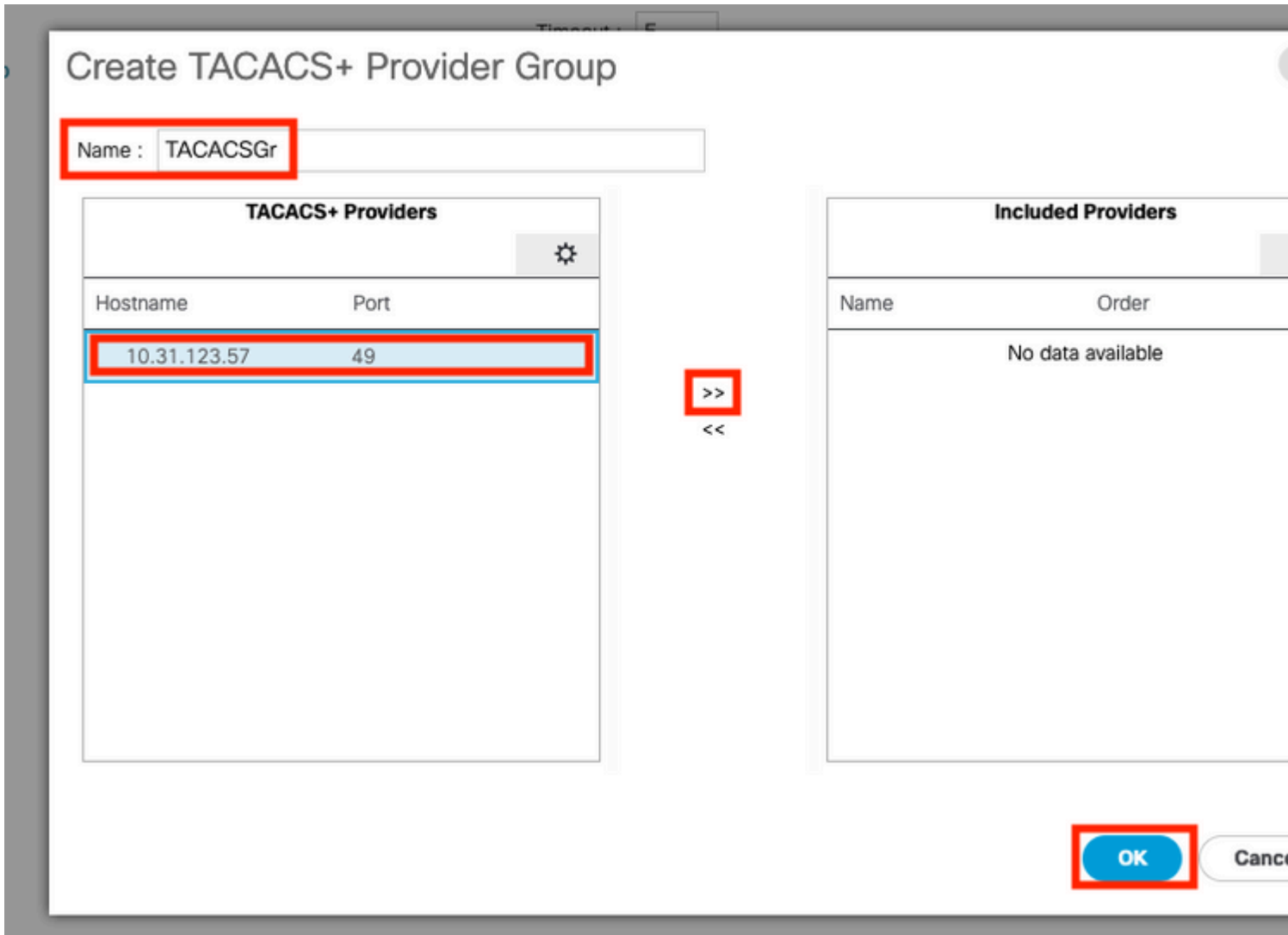
Step 4. In the **Actions** area, select **Create TACACS+ Provider Group**.



â€f

Step 5. In the **Create TACACS+ Provider Group** dialog box, enter the information requested.

- In the **Name** field, enter a unique name for the group.
- In the **TACACS+ Providers** table, choose the providers to include in the group.
- Select the >> button to add the providers to the Included Providers table.



Step 6. Select **Ok**.

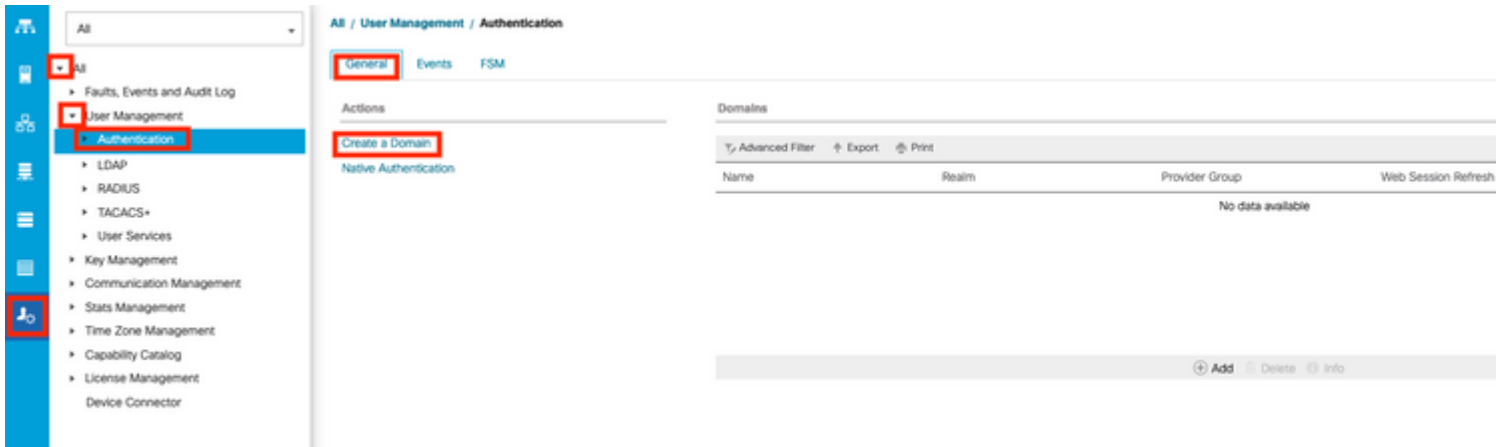
Create an Authentication Domain

Step 1. In the Navigation pane, select the **Admin** tab.

Step 2. On the **Admin** tab, expand **All > User Management > Authentication**

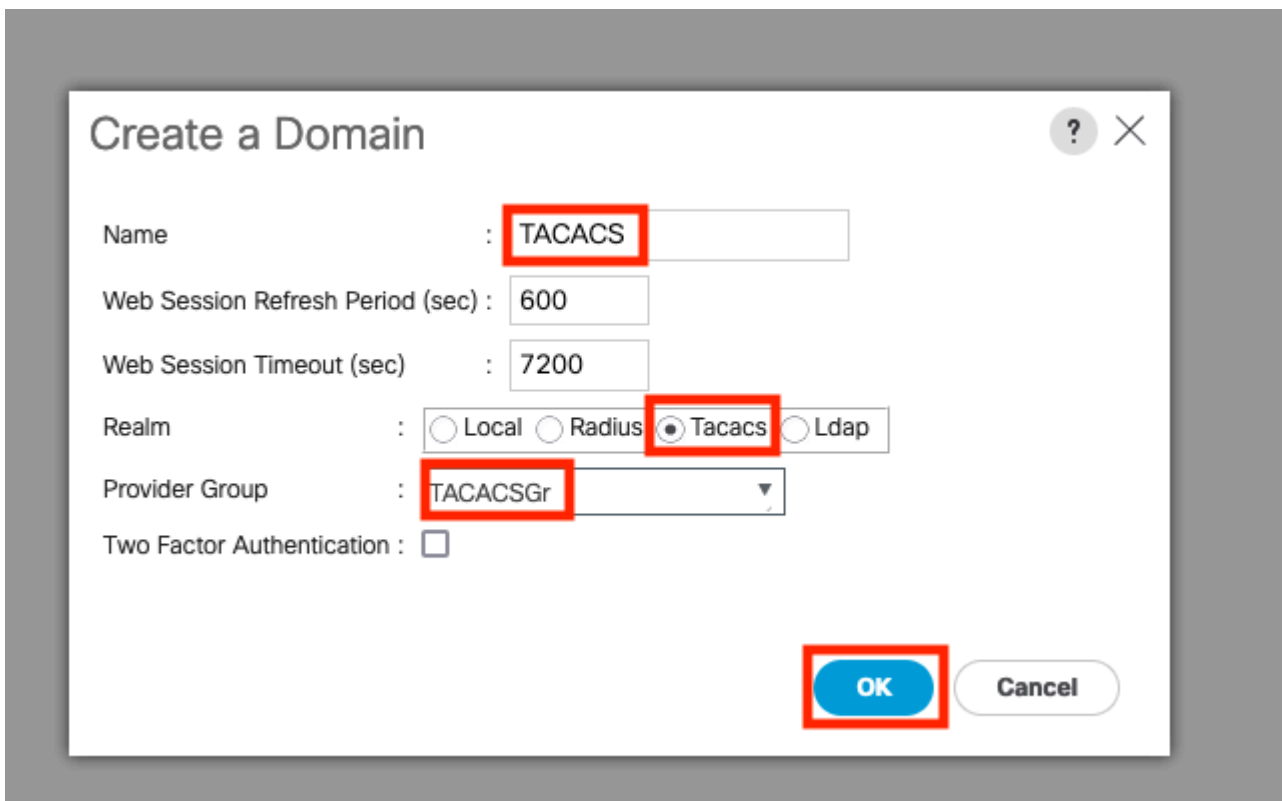
Step 3. In the **Workpane**, select the **General** tab.

Step 4. In the **Actions area**, select **Create a Domain**.



Step 5. In the **Create Domain** dialog box, enter the information requested.

- In the **Name** field, enter a unique name for the domain.
- In the **Realm**, select the Tacacs option.
- From the **Provider Group** drop-down list, select the TACACS+ provider group previously created and select **OK**



â€f

Troubleshoot

Common TACACS+ Issues on UCSM

- Wrong key or invalid characters.
- Wrong port.
- No communication with our provider due to a Firewall or Proxy rule.
- FSM is not 100%.

Verify UCSM TACACS+ configuration:

You must ensure that the UCSM has implemented the configuration checking the the status of the **Finite State Machine (FSM)** is shown as 100% complete.

Verify the configuration from the UCSM command line

```
<#root>
```

```
UCS-A#
```

```
scope security
```

```
UCS-A /security #
```

```
scope tacacs
```

```
UCS-A /security/tacacs #
```

```
show configuration
```

```
UCS-AS-MXC-P25-02-A# scope security
UCS-AS-MXC-P25-02-A /security # scope tacacs
UCS-AS-MXC-P25-02-A /security/tacacs # show configuration
scope tacacs
  enter auth-server-group TACACSGr
    enter server-ref 10.31.123.57
      set order 1
    exit
  exit
enter server 10.31.123.57
  set order 1
  set port 49
  set timeout 5
!   set key
  exit
  set timeout 5
exit
```

```
<#root>
```

```
UCS-A /security/tacacs #
```

```
show fsm status
```

```
[UCS-AS-MXC-P25-02-A /security/tacacs # show fsm status
```

```
FSM 1:  
  Status: Nop  
  Previous Status: Update Ep Success  
  Timestamp: 2023-06-24T20:54:05.021  
  Try: 0  
  Progress (%): 100  
  Current Task:
```

â€f

Verify the Tacacs configuration from the NXOS:

```
<#root>
```

```
UCS-A#
```

```
connect nxos
```

```
UCS-A(nx-os)#
```

```
show tacacs-server
```

```
UCS-A(nx-os)#
```

```
show tacacs-server groups
```



```
[UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server
timeout value:5
deadtime value:0
source interface:any available
Global Test Username:test
Global Test Password:*****
total number of servers:1

following TACACS+ servers are configured:
 10.31.123.57:
    available on port:49
    TACACS+ shared secret:*****
    timeout:5
[UCS-AS-MXC-P25-02-A(nx-os)# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
group tacacs:
  server 10.31.123.57 on port 49
  deadtime is 0
  vrf is management
group TACACSGr:
  server 10.31.123.57 on port 49
  deadtime is 0
  vrf is management
```

In order to test authentication from NX-OS, use the `test aaa` command (only available from NXOS).

Validate the configuration of our server:

```
<#root>
```

```
UCS-A(nx-os)#
```

```
test aaa server tacacs+
```

```
<TACACS+-server-IP-address or FQDN> <username> <password>
```

```
UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/lgpl-2.1.txt.
UCS-AS-MXC-P25-02-A(nx-os)# test aaa server tacacs+ 10.31.123.57 operator Cisc0123
```

UCSM Review

Reachability verification

```
<#root>
```

```
UCS-A#
```

```
connect local-mgmt
```

```
UCS-A(local-mgmt)#
```

```
ping
```

```
<TACACS+-server-IP-address or FQDN>
```

```
UCS-AS-MXC-P25-02-A# connect local-mgmt
pCisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
UCS-AS-MXC-P25-02-A(local-mgmt)# ping 10.31.123.57
PING 10.31.123.57 (10.31.123.57) from 10.31.123.8 : 56(84) bytes of data.
64 bytes from 10.31.123.57: icmp_seq=1 ttl=64 time=0.347 ms
64 bytes from 10.31.123.57: icmp_seq=2 ttl=64 time=0.309 ms
```

```
â€f
```

Port verification

```
<#root>
```

```
UCS-A#
```

```
connect local-mgmt
```

```
UCS-A(local-mgmt)#
```

```
telnet
```

```
<TACACS+-server-IP-address or FQDN> <Port>
```

```
UCS-AS-MXC-P25-02-A# connect local-mgmt
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
UCS-AS-MXC-P25-02-A(local-mgmt)# telnet 10.31.123.57 49
Trying 10.31.123.57...
Connected to 10.31.123.57.
Escape character is '^]'.

```

The most effective method to see errors is to enable the NXOS debug, with this output you can see the groups, the connection, and the error message that causes miscommunication.

- Open an SSH session to UCSM and log in with with any privileged user with admin permissions(preferably a local user), change to NX-OS CLI context and start the **terminal monitor**.

```
<#root>
```

```
UCS-A#
```

```
connect nxos
```

```
UCS-A(nx-os)#
```

```
terminal monitor
```

- Enable debug flags and verify the SSH session output to the log file.

```
<#root>
```

```
UCS-A(nx-os)#
```

```
debug aaa all
```

```
UCS-A(nx-os)#
```

```
debug aaa aaa-request
```

```
UCS-A(nx-os)#
```

```
debug tacacs+ aaa-request
```

```
UCS-A(nx-os)#
```

```
debug tacacs+ aaa-request-lowlevel
```

```
UCS-A(nx-os)#
```

```
debug tacacs+ all
```

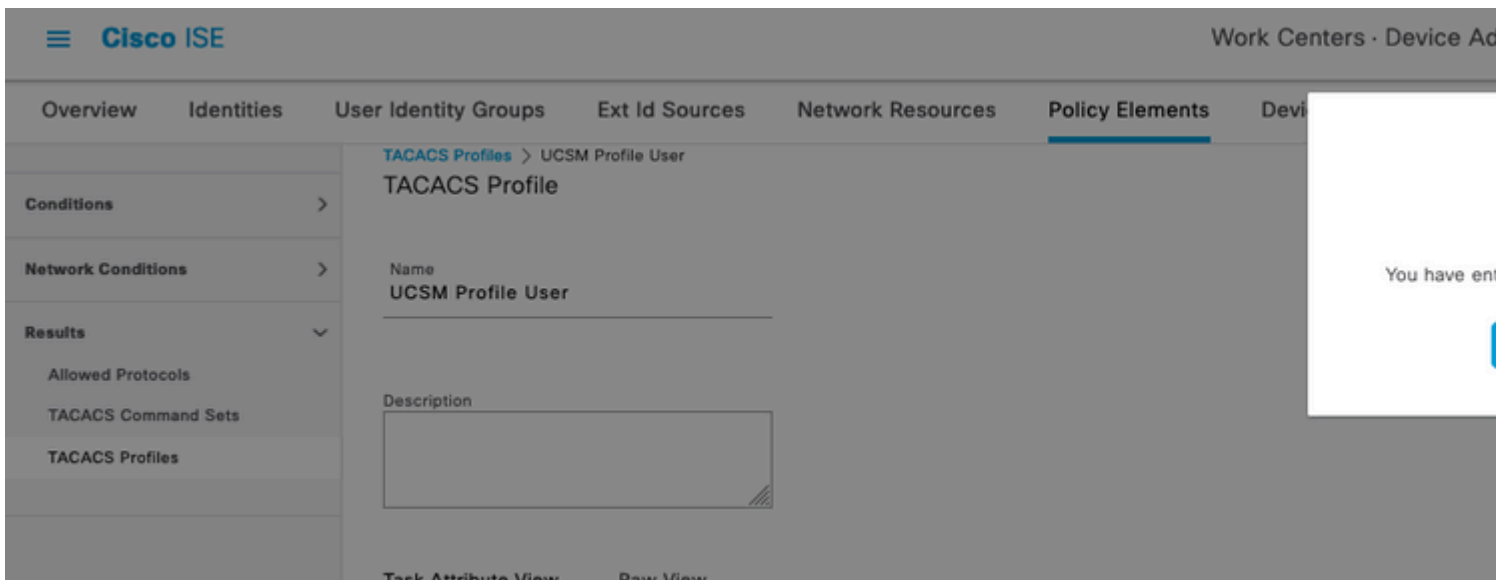
```
UCS-AS-MXC-P25-02-A# connect nxos
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2023, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source. This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0 or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.
UCS-AS-MXC-P25-02-A(nx-os)# terminal monitor
UCS-AS-MXC-P25-02-A(nx-os)# debug tacacs+ all
2023 Jun 26 04:42:22.104286 tacacs: event_loop(): calling process_rd_fd_set
2023 Jun 26 04:42:22.104311 tacacs: process_rd_fd_set: calling callback for fd 6
2023 Jun 26 04:42:22.104341 tacacs: fsrv didnt consume 182 opcode
2023 Jun 26 04:42:22.104994 tacacs: mts_message_handler: sdwrap_process_msg
2023 Jun 26 04:42:22.105011 tacacs: process_rd_fd_set: callback returned for fd 6
UCS-AS-MXC-P25-02-A(nx-os)# debug aaa all
```

- Now open a new GUI or CLI session and attempt to log in as a remote user (TACACS+).
- Once you received a login failure message, turn off the debugs closing the session or with below command.

```
UCS-A(nx-os)# undebug all
```

Common TACACs Issues on ISE

- Within ISE the following behavior is displayed while attempting to configure a the tacacs profile in the attributes that are needed for UCSM to assign the corresponding roles for admin or any other role, select on the save button and the following behavior is seen :



This error is due to the following bug <https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc91917> , please ensure that you have where this defect has been addressed.

ISE Review

Step 1. Review if the TACACS+ serviceability is running, this can be checked in:

- GUI: Review if you have the node listed with the service DEVICE ADMIN in **Administration > System > Deployment.**
- CLI: Run the command **show ports | include 49** to confirm that there are connections in the TCP port that belong to TACACS+

```
<#root>
```

```
ise32/admin#
```

```
show ports | include 49
```

```
tcp: 169.254.4.1:49, 169.254.2.1:49, 169.254.4.1:49, 10.31.123.57:49
```

Step 2. Confirm if there are livelogs concerning TACACS+ authentications attempts : this can be checked in the menu **Operations > TACACS > Live logs** ,

Depending upon the failure reason you can adjust your configuration or address the cause of failure.

Live Logs

Export To

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...	Network Devic...	Device Type
Jun 25, 2023 12:30:16.8...	●	🔒	INVALID	Authentic...	Default >> Default		ise32	USCM	10.31.123.8	Device Type#All ...
Jun 25, 2023 12:20:38.7...	●	🔒		Authentic...			ise32		10.31.123.9	
Jun 25, 2023 12:20:02.2...	●	🔒		Authentic...			ise32		10.31.123.9	

Step 3. In case you don't see any livelog, proceed to take a packet capture navigate to the menu **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump**, select on add

Diagnostic Tools

- General Tools
 - RADIUS Authentication Troubl...
 - Execute Network Device Com...
 - Evaluate Configuration Validat...
 - Posture Troubleshooting
 - Agentless Posture Troublesho...
 - EndPoint Debug
- TCP Dump
- Session Trace Tests
- TrustSec Tools

TCP Dump

The TCP Dump utility page is to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear

Refresh Add Edit Trash Start Stop Download

Host Name	Network Interface	Filter	File Name	Reposito...	File S...	Number of ...	Time Limit	Promiscuous M...	Status
-----------	-------------------	--------	-----------	-------------	-----------	---------------	------------	------------------	--------

No data found.

Select the Policy Service node from where the UCSM is sending the authentication and then in filters proceed to input ip host X.X.X.X corresponding the IP of the UCSM from where the authentication is being sent, name the capture and scroll down to save, run the capture and log in from the UCSM .

Diagnostic Tools Download Logs Debug Wizard

General Tools

- RADIUS Authentication Troubl...
- Execute Network Device Com...
- Evaluate Configuration Validat...
- Posture Troubleshooting
- Agentless Posture Troublesho...
- EndPoint Debug

TCP Dump

Session Trace Tests

TrustSec Tools

TCP Dump > New

Add TCP Dump

Add TCP Dump packet for monitoring on a network interface and troubleshoot problems on the network as they appear.

Host Name*
ise32

Network Interface*
GigabitEthernet 0 [Up, Running]

Filter
ip host 10.31.123.7

E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name
taccap

Repository

File Size
10 Mb

Limit to
1 File(s)

Time Limit
5 Minute(s)

Promiscuous Mode

Cancel Save Save and Run

Step 4. Enable the component runtime-AAA in debug within the PSN from where the authentication is being performed in **Operations > Troubleshoot > Debug Wizard > Debug log configuration**, select PSN node , select then next in edit button .

Debug Profile Configuration

Debug Log Configuration

Node List

 Edit  Reset to Default

Node Name	Replication Role
<input type="radio"/> ise32	STANDALONE

Look for the component runtime-AAA and change its level to debug to then reproduce the issue again, and proceed to analyze the logs .

Debug Profile Configuration

Debug Log Configuration

Node List > ise32.example.com

Debug Level Configuration

 Edit  Reset to Default

Component Name	Log Level	Description
runtime-AAA	×	
<input type="radio"/> runtime-AAA	DEBUG	AAA runtime messages (prtt)

Note: For further information please refer to the video in the Cisco Youtube's channel How to Enable Deubgs on ISE 3.x Versions <https://www.youtube.com/watch?v=E3USz8B76c8> .

Related Information

[Cisco UCS Manager Administration Management Guide](#)

