

CSM TACACS Integration with ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Network Diagram](#)

[Authentication Procedure](#)

[ISE Configuration](#)

[CSM Configuration](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes the procedure to integrate Cisco Security Manager (CSM) with Identity Services Engine (ISE) for administrator users authentication with TACACS+ Protocol.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Security Manager (CSM).
- Identity Services Engine (ISE).
- TACACS protocol.

Components Used

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

- CSM Server version 4.22
- ISE version 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, ensure that you understand the potential impact of any command.

Background Information

By default, Cisco Security Manager (CSM) uses an Authentication mode called Ciscoworks to

authenticate and authorize users locally, in order to have a centralized authentication method you can use Cisco Identity Service Engine through the TACACS protocol.

Configure

Network Diagram



Authentication Procedure

Step 1. Log into the CSM application with the credentials of the Admin User.

Step 2. Authentication process triggers and ISE validates the credentials locally or through Active Directory.

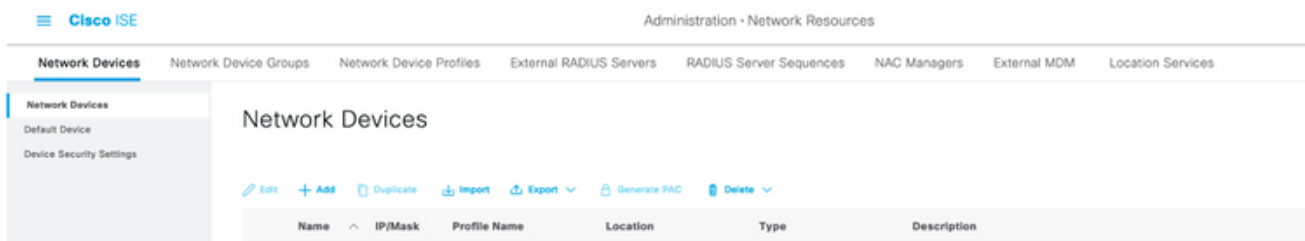
Step 3. Once authentication is successful ISE sends a permit packet to authorize access to the CSM.

Step 4. CSM maps the username with the local user role assignment.

Step 5. ISE shows a successful authentication live log.

ISE Configuration

Step 1. Select the three lines icon  located in the upper left corner and navigate to **Administration > Network Resources > Network Devices**.



Step 2. Select the **+Add** button and enter the proper values for Network Access Device Name and IP Address, then verify the **TACACS Authentication Settings** checkbox and define a shared secret. Select the **Submit** button.

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Managers | External MDM | Location Services

Network Devices List > New Network Device

Network Devices

Name: CSM432

Description:

IP Address: 10.88.243.42 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: All Locations [Set To Default](#)

IPSEC: Is IPSEC Device [Set To Default](#)

Device Type: All Device Types [Set To Default](#)

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret: [Show](#)

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connect Support

SNMP Settings

Advanced TrustSec Settings

[Submit](#) [Cancel](#)



Step 3. Select the three lines icon located in the upper left corner and navigate to **Administration > Identity Management > Groups**.

≡ Cisco ISE Administration • Identity Management

Identities **Groups** External Identity Sources Identity Source Sequences Settings

Identity Groups

EQ

< [Icon] [Icon]

> Endpoint Identity Groups

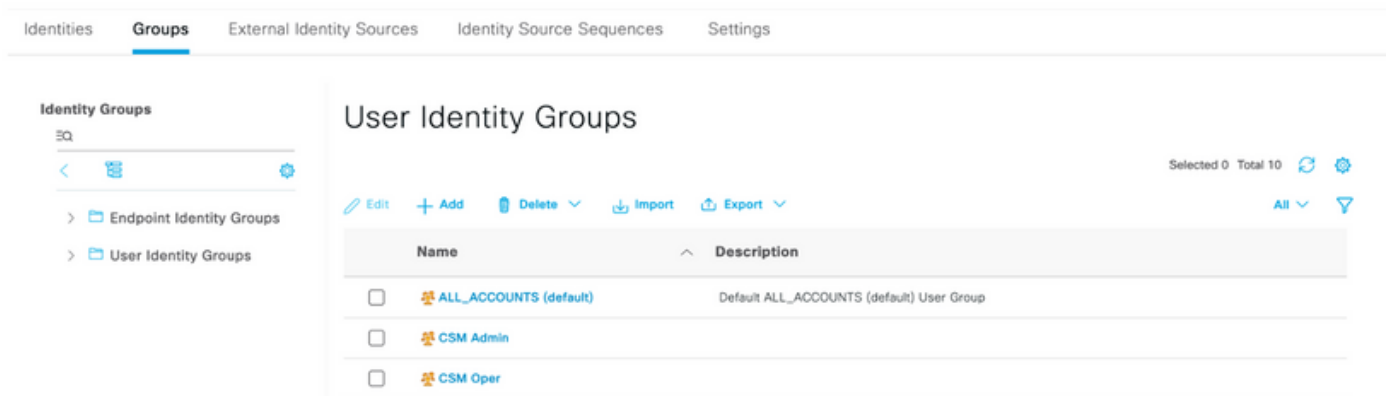
> **User Identity Groups**

User Identity Groups

[Edit](#) [+ Add](#) [Delete](#) [Import](#) [Export](#)

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

Step 4. Navigate to the **User Identity Groups** folder and select the **+Add** button. Define a name and select **Submit** button.



The screenshot shows the 'User Identity Groups' management page. The top navigation bar includes 'Identities', 'Groups' (selected), 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. On the left, a sidebar shows 'Identity Groups' with a search bar and a tree view containing 'Endpoint Identity Groups' and 'User Identity Groups'. The main content area is titled 'User Identity Groups' and features a toolbar with 'Edit', '+ Add', 'Delete', 'Import', and 'Export' buttons. Below the toolbar is a table with columns 'Name' and 'Description'. The table lists three groups: 'ALL_ACCOUNTS (default)' with description 'Default ALL_ACCOUNTS (default) User Group', 'CSM Admin', and 'CSM Oper'. Each row has a checkbox for selection. The top right of the main area shows 'Selected 0 Total 10' and icons for refresh and settings.

Note: This example creates CSM Admin and CSM Oper Identity groups. You can repeat Step 4 for each type of Admin Users on CSM



Step 5. Select the three lines icon and navigate to **Administration > Identity Management > Identities**. Select the **+Add** button and define the username and password, then select the group where the user belongs to. In this example, creates the **csmadmin** and **csmoper** users and assigned to CSM Admin and CSM Oper group respectively.

Cisco ISE Administration - Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

Network Access Users List > csmadmin

Network Access User

Name: csmadmin

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: * Login Password: * Re-linear Password: * Create Password: *

Generate Password

User Information

First Name: Last Name:

Account Options

Description: Change password on next login:

Account Disable Policy

Disable account if date exceeds: 2021-05-15 (every min=60)

User Groups

CSM Admin

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Res...

Network Access Users

Selected 0 Total 2

Edit + Add Change Status Import Export Delete Duplicate All

Status	Name	Description	First Name	Last Name	Email Address	User Identity Grou...	Ad...
<input type="checkbox"/>	Enabled csmadmin					CSM Admin	
<input type="checkbox"/>	Enabled csmoper					CSM Oper	



Step 6. Select and navigate to **Administration > System > Deployment**. Select the hostname node and enable **Device Admin Service**

Hostname	Personas	Role(s)	Services	Node Status
Ise30	Administration, Monitoring, Policy Service	STANDALONE	IDENTITY MAPPING, SESSION, PROFILER, DE...	✔

> Enable SXP Service ⓘ

Enable Device Admin Service ⓘ


Enable Passive Identity Service ⓘ

Note: In case of Distributed Deployment, select the PSN node that handles TACACS requests

Step 7. Select the three lines icon and navigate to **Administration > Device Administration > Policy Elements**. Navigate to **Results > TACACS Command Sets**. Select **+Add** button, define a name for the Command Set and enable the **Permit any command that is not listed below** the checkbox. Select **Submit**.

The screenshot shows the Cisco ISE interface for configuring TACACS Command Sets. The 'Policy Elements' tab is active, and the 'TACACS Command Sets' section is expanded. A new command set is being created with the name 'Permit all'. The 'Description' field is empty. The 'Commands' section has the checkbox 'Permit any command that is not listed below' checked. At the bottom, there are 'Cancel' and 'Submit' buttons.

Step 8. Select three lines icon located in the upper left corner and navigate to **Administration-**

>**Device Administration->Device Admin Policy Sets.** Select  located below Policy Sets title, define a name and select the + button in the middle to add a new condition.

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	CSM Administrators		+	Select from list	+		
	Default	Tacacs Default policy set		Default Device Admin	0		

Step 9. Under Condition window, select add an attribute and then select **Network Device** Icon followed by Network access device IP address. Select **Attribute Value** and add the CSM IP address. Select **Use** once done.

Conditions Studio

Library

Search by Name



No conditions found - reset filters.

Editor

Network Access-Device IP Address

Equals

[Set to 'Is not'](#) Duplicate Save

NEW | AND | OR


Close


Use

Step 10. Under allow protocols section, select **Device Default Admin.** Select **Save**

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	CSM 4.22		Network Access-Device IP Address EQUALS 10.88.243.42	Default Device Admin	+	0	


Step 11. Select the right arrow  icon of the Policy Set to Define authentication and authorization policies

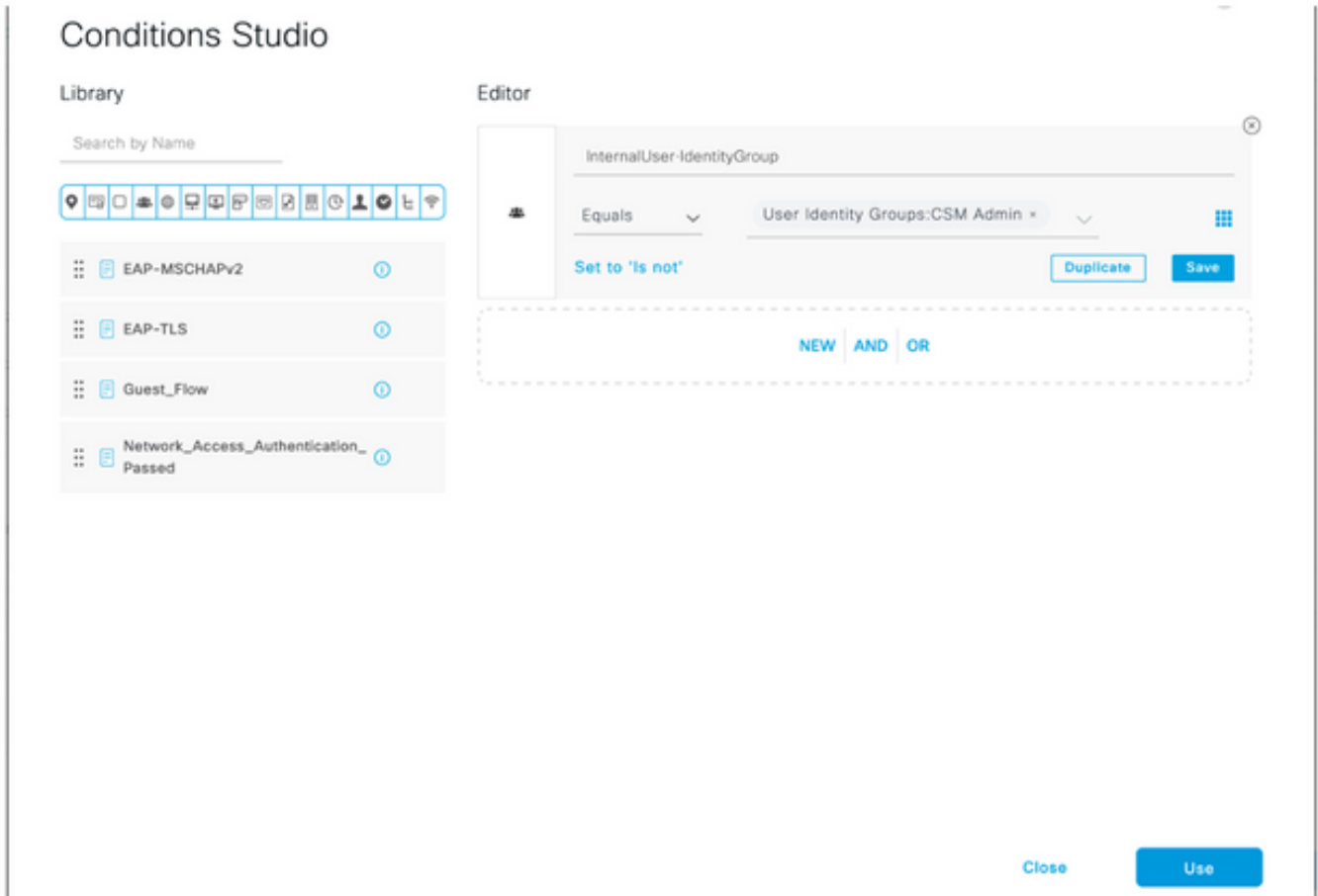
Step 12. Select  located below Authentication Policy title, define a name and select the + in the middle to add a new condition. Under Condition window, select add an attribute and then select **Network Device** icon followed by Network access device IP address. Select **Attribute Value** and add the CSM IP address. Select **Use** once done

Step 13. Select **Internal Users** as the Identity Store and Select **Save**



Note: Identity Store can be changed to AD store if ISE is joined to an Active Directory.

Step 14. Select  located below Authorization Policy title, define a name and select the + button in the middle to add a new condition. Under the Condition window, select add an attribute and then select **the Identity Group** icon followed by **Internal User: Identity Group**. Select the CSM Admin Group and select **Use**.



Step 15. Under Command Set, select Permit all command set created in Step 7 and then select **Save**

Repeat Step 14 and 15 for the CSM Oper group

Authorization Policy (3)

Status	Rule Name	Conditions	Results			Hits	Actions
			Command Sets	Shell Profiles			
+	Search						
✓	<u>CSM Oper</u>	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Oper	Permit all ×	▼ +	Select from list	▼ +	0 ⚙️
✓	<u>CSM Admin</u>	InternalUser-IdentityGroup EQUALS User Identity Groups:CSM Admin	Permit all ×	▼ +	Select from list	▼ +	0 ⚙️
✓	Default		DenyAllCommands ×	▼ +	Deny All Shell Profile	🔒 ▼ +	0 ⚙️

Step 16 (Optional). Select three lines icon located in the upper left corner and Select **Administration>System>Maintenance>Repository**, select **+Add** to add a repository that is used to store TCP Dump file for troubleshooting purposes.

Step 17 (Optional). Define a repository Name, protocol, Server Name, path and Credentials. Select **Submit** once done.

Deployment Licensing Certificates Logging **Maintenance** Upgrade Health Checks Backup [Click here to do visibility setup Do not show this again.](#)

Patch Management
Repository
Operational Data Purging

[Repository List](#) > Add Repository

Repository Configuration

* Repository Name

* Protocol

Location

* Server Name

* Path

Credentials

* User Name

* Password

CSM Configuration

Step 1. Log in to the Cisco Security Manager Client application with the local admin account. From the menu navigate to **Tools > Security Manager Administration**

Cisco Security Manager
Version 4.22.0 Service Pack 1

Server Name

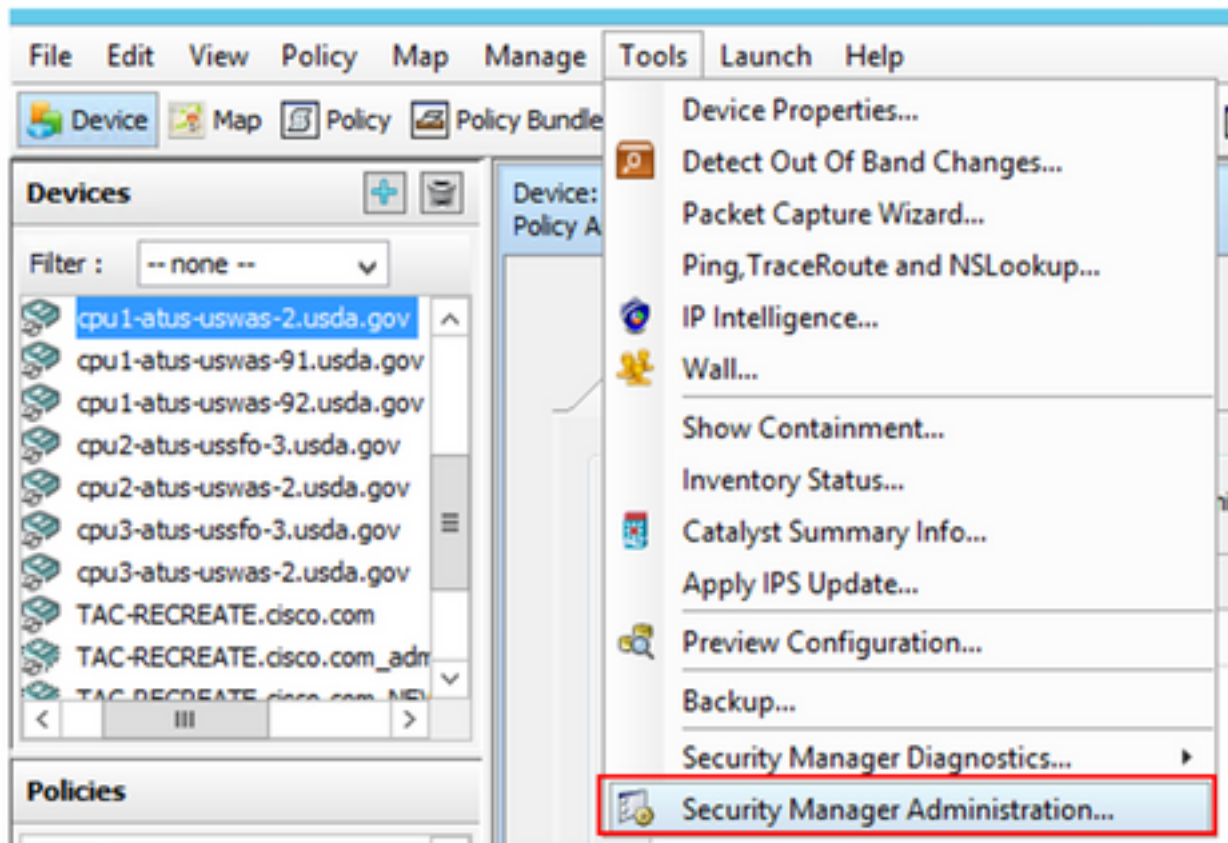
Username

Password

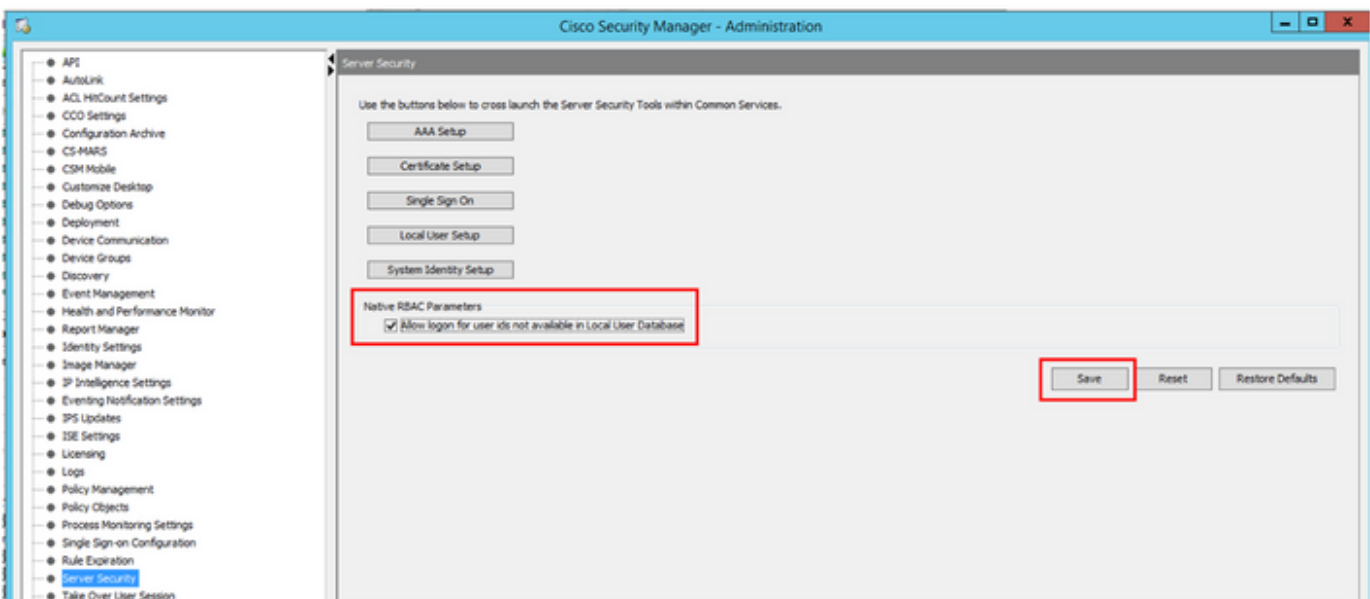
Default View

[Login](#) [Help](#)

© 2020 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.



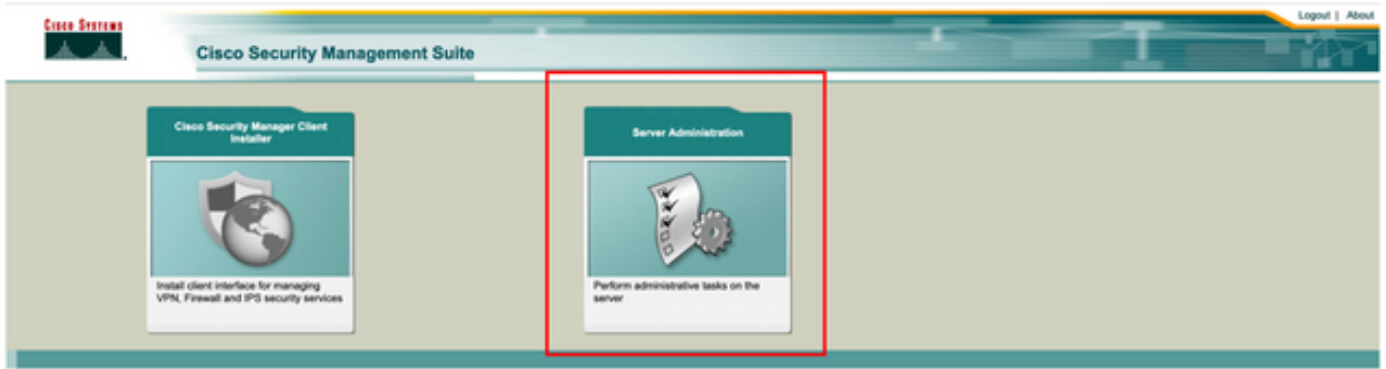
Step 2. Check the box under **Native RBAC Parameters**. Select **Save** and **Close**



Step 3. From the menu select **File > Submit. File > Submit.**

Note: All changes must be saved, in case of configuration changes those need to be submitted and deployed.

Step 4. Navigate to CSM Management UI and type https://<enter_CSM_IP_Address> and select **Server Administration**.



Note: Steps 4 to 7 show the procedure to define the default role for all administrators that are not defined on ISE. These steps are optional.

Step 5. Validate the authentication mode is set to **CiscoWorks Local** and **Online** userID is the local admin account created on CSM.

Common Services Home

Version: 4.2.2

Last Updated: Sat Apr 17 14:11:20 PDT 2021

Security		Backup		Recently Completed Jobs				
Authentication Mode	CiscoWorks Local	Backup Schedule	Not Scheduled	Job ID	Job Type	Status	Description	Completed At
Authorization Mode	CiscoWorks Local	Last Backup Completed at	Not found or unable to detect	1001.1370	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 17 05:01:56 PDT 2021
Single Sign-on Mode	Standalone	Recent Backup Status	Not found or unable to detect	1001.1369	SystemCheckUtility	Succeeded	SysCheckTest	Fri Apr 16 05:00:58 PDT 2021
				1001.1368	SystemCheckUtility	Succeeded	SysCheckTest	Thu Apr 15 05:00:57 PDT 2021
				1001.1367	SystemCheckUtility	Succeeded	SysCheckTest	Wed Apr 14 05:00:55 PDT 2021
				1001.1366	SystemCheckUtility	Succeeded	SysCheckTest	Tue Apr 13 05:00:54 PDT 2021
				1001.1365	SystemCheckUtility	Succeeded	SysCheckTest	Mon Apr 12 05:00:56 PDT 2021
				1001.1364	SystemCheckUtility	Succeeded	SysCheckTest	Sun Apr 11 05:00:55 PDT 2021
				1001.1363	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 10 05:00:56 PDT 2021

System Tasks	Online Users	Management Tasks	Reports
Local User Setup Multi-Server Trust Management Configure Single Sign-On AAA Mode Setup	Number of Online users: 1 Online User ID(s): admin Send Message	Schedule Backup Check for Software Updates Check for Device Updates Collect Server Information	Permission Report Log File Status Process Status System Audit Log

Step 6. Navigate to **Sever** and select **Single-Server Management**



Common

Auto R

Authentica

Authorizat

Single Sig

Local Use

Multi-Serv

Configure

AAA Mode Setup

Security

Single-Server Management

Multi-Server Trust Management

Cisco.com Connection Management

AAA Mode Setup

Admin

Processes

Backup

Log Rotation

Collect Server information

Selftest

Notify Users

Job Browser

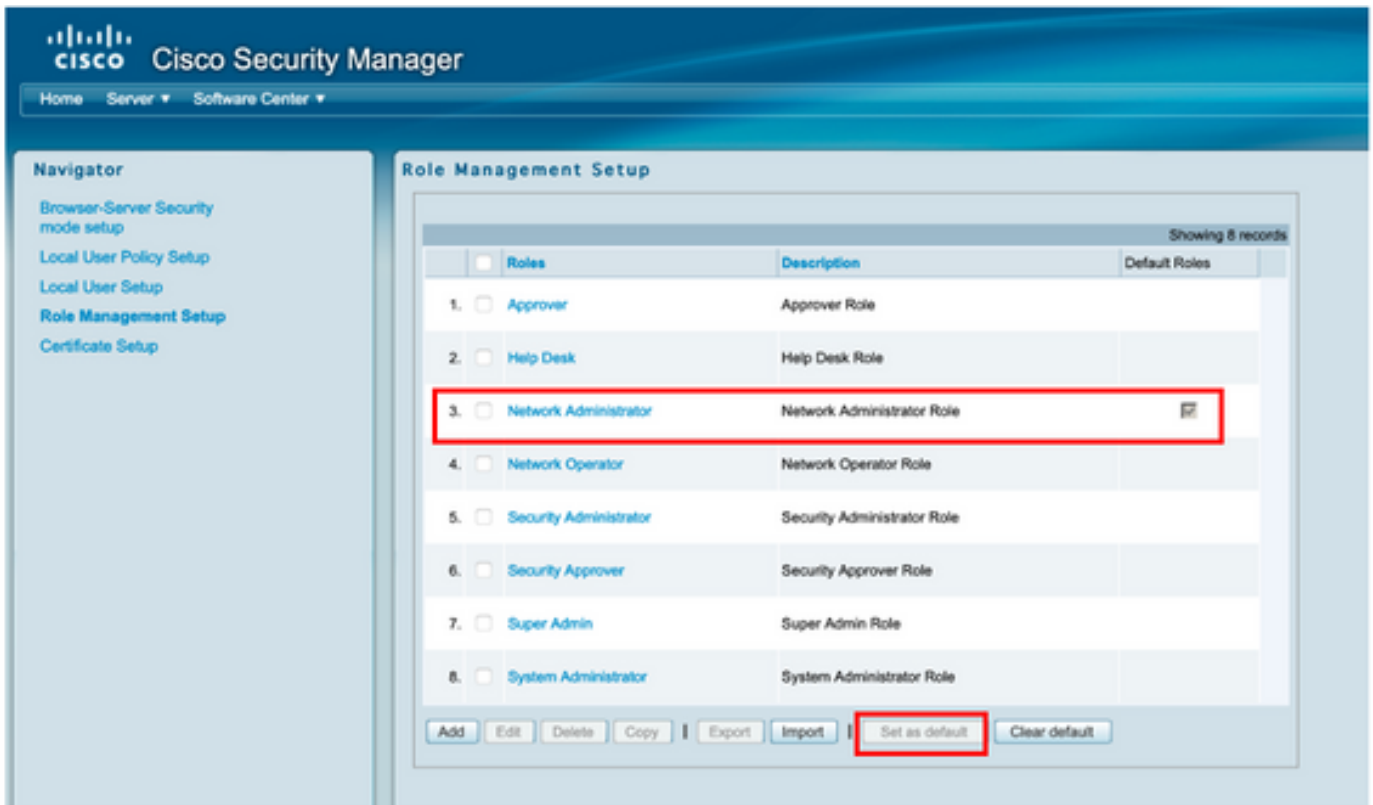
Resource Browser

System Preferences

CS Log Configurations

DiskWatcher Configuration

Step 7. Select Role Management Setup and select the default privilege all admin users receive upon authentication. For this example, Network Administrator is used. Once selected select **set as default**.

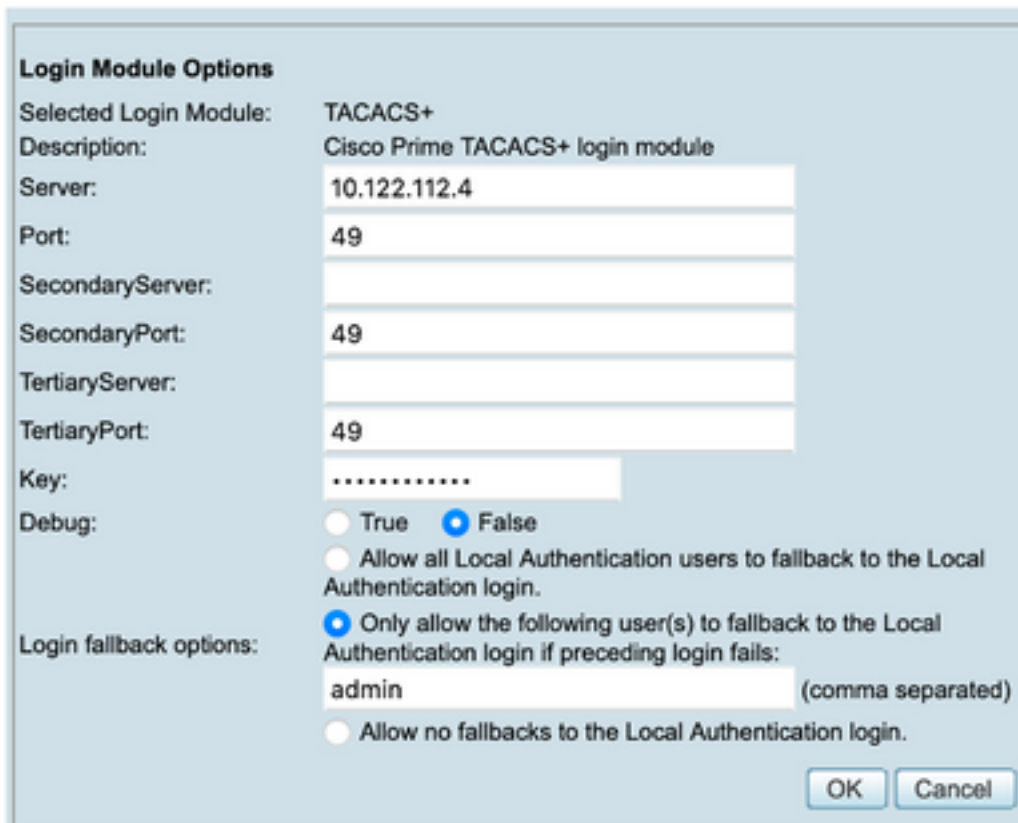


Step 8. Select **Server>AAA Mode Setup Role** and then select **TACACS+** option, finally select **change** to add ISE information.





Step 9. Define ISE Ip address and Key, optionally you can select the option to allow all local authentication users or only one user if the log in fails. For this example, the Only admin user is allowed as a fallback method. Select **Ok** to save the changes.



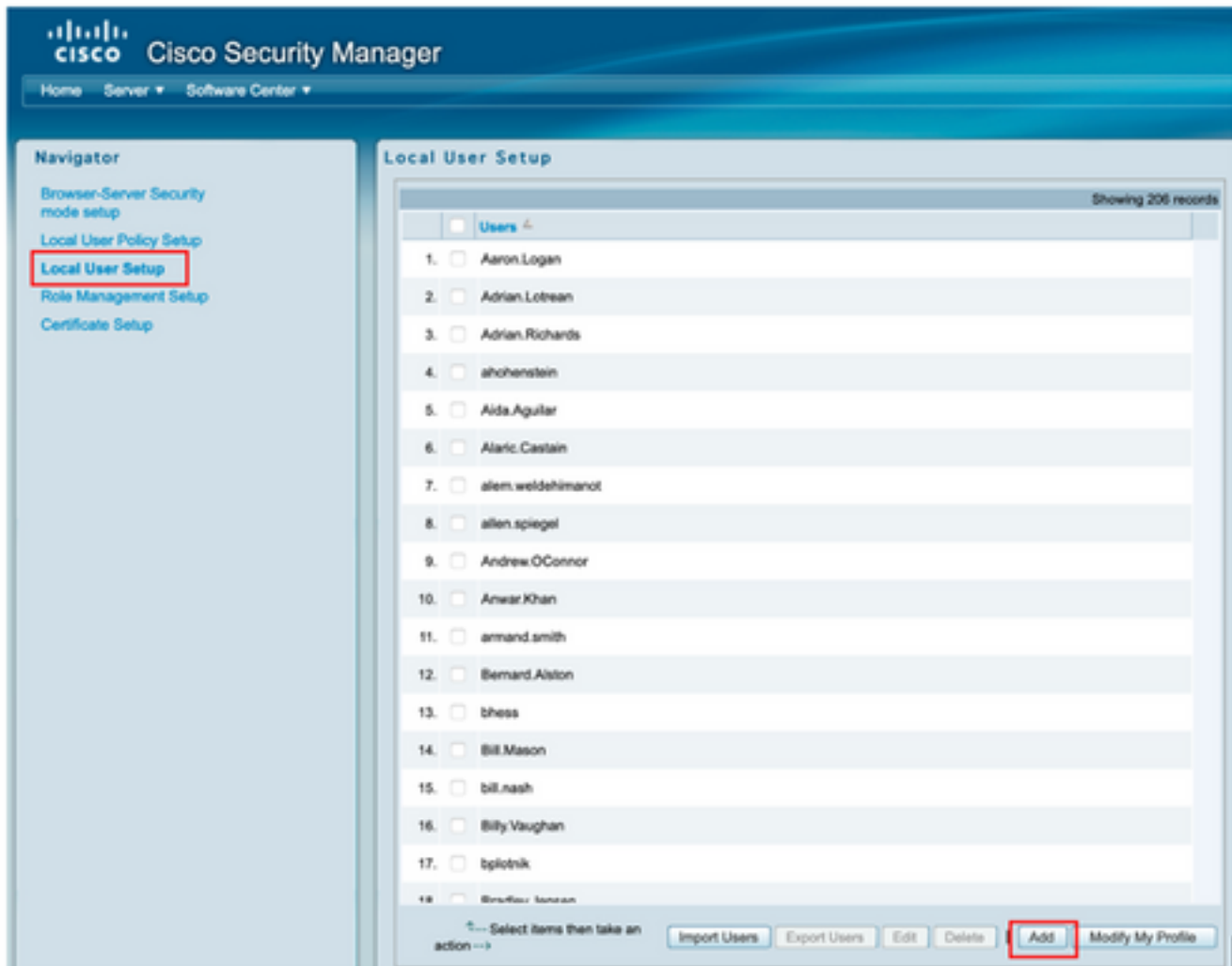
Login Module Change Summary

Login Module changes updated.

OK

Step 10. Select **Server > Single Server Management**, then select **Local User Setup** and select **add**.





Step 11. Define the same username and password created on ISE on step 5 under the ISE configuration section, **csmoper** and **Help Desk task authorization roles** are used in this example. Select **OK** in order to save the admin user.

User Information

User Login Details

Username:

Password: Verify Password:

Email:

Authorization Type

Select an option: Full Authorization Enable Task Authorization Enable Device Authorization

Roles

- Help Desk
- Approver
- Network Operator
- Network Administrator
- System Administrator
- Super Admin
- Security Administrator
- Security Approver

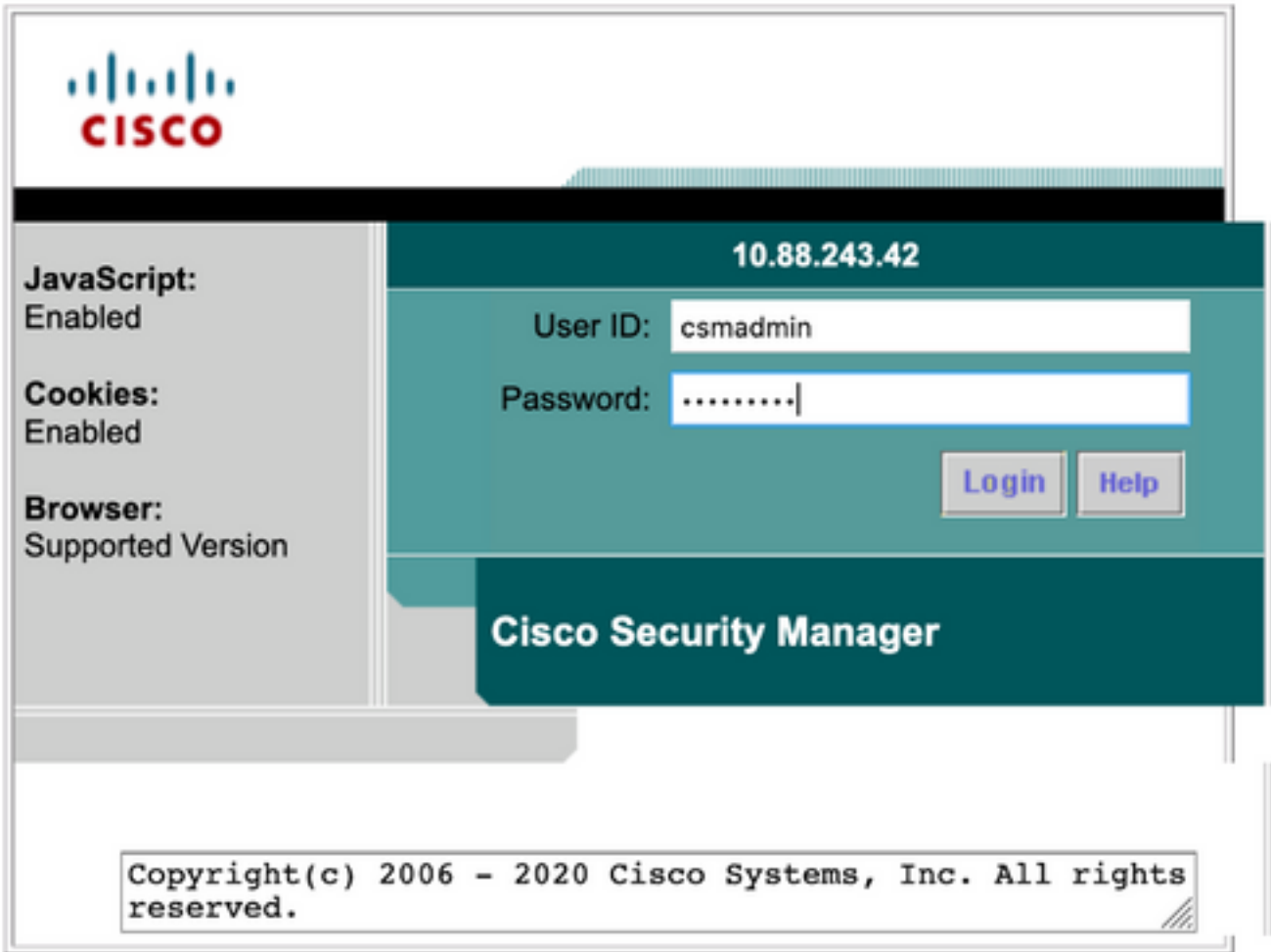
Device level Authorization

Not Applicable

Verify

Cisco Security Manager Client UI

Step 1. Open a new window browser and type <https://<enter CSM IP Address>>, use **csmadmin** username and password created on step 5 under the ISE configuration section.



Successful log in the attempt can be verified on ISE TACACS live logs

Cisco ISE Operations - TACACS Evaluation Made 39 Days

Live Logs

Refresh Every 3 seconds Show Latest 20 records Within Last 3 hours

Refresh Export To Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic.
Apr 17, 2021 02:34:54.1...	✓		csmadmin	Authentic...	CSM 4.22 >> Default		ise30	CSM422

Last Updated: Sat Apr 17 2021 09:37:58 GMT-0500 (Central Daylight Time) Records Shown: 1

Cisco Security Manager Client application

Step 1. Log in to the Cisco Security Manager Client application with the helpdesk admin account.



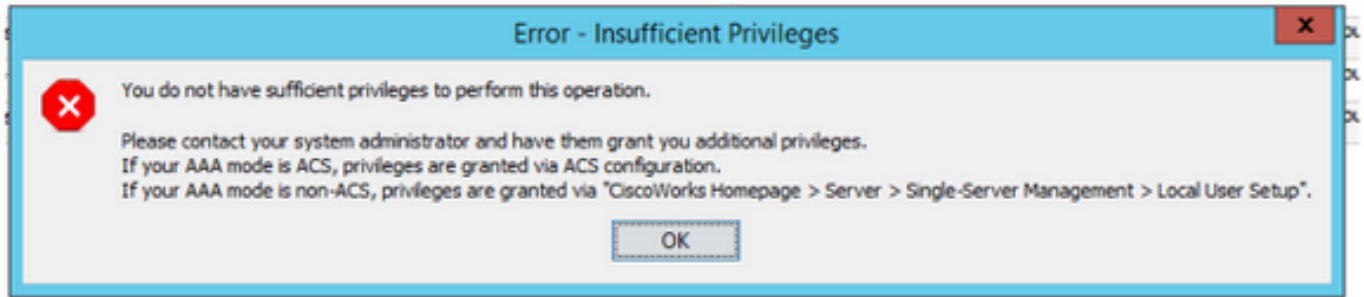
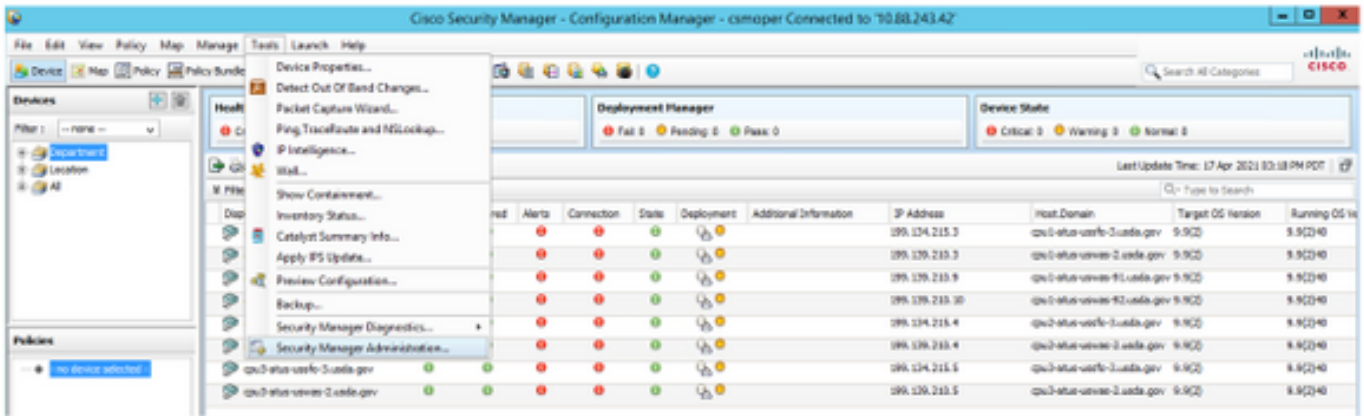
Successful log in the attempt can be verified on ISE TACACS live logs

Live Logs

Refresh Every 3 seconds Show Latest 20 records Within Last 3 hours Filter

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic.
Apr 17, 2021 03:05:58.5...	✓		csmoper	Authentic...	CSM 4.22 >> Default		ise30	CSM422

Step 2. From the CSM client application menu select **Tools > Security Manager Administration**, an error message indicates lack of privilege must appear.



Step 3. Repeat steps 1 to 3 with **csmadmin** account to validate the proper permissions have been provided to this user.

Troubleshoot

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

Communication validation with TCP Dump tool on ISE

Step 1. Log in on ISE and navigate to the three lines icon located in the upper left corner and select **Operations>Troubleshoot>Diagnostic Tools**.

Step 2. Under **General tools** select **TCP Dumps** and then select **Add+**. Select Hostname, Network Interface File Name, Repository, and optionally a filter to gather only CSM IP address communication flow. Select **Save and Run**

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

Add TCP Dump

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

Host Name *
ise30

Network Interface *
GigabitEthernet 0

Filter
ip host 10.88.243.42

E.g: ip host 10.77.122.123 and not 10.177.122.119

File Name
CSM_Tshoot

Repository
VMRepository

File Size
100 Mb

Limit to
1 File(s)

Time Limit
5 Minute(s)

Promiscuous Mode

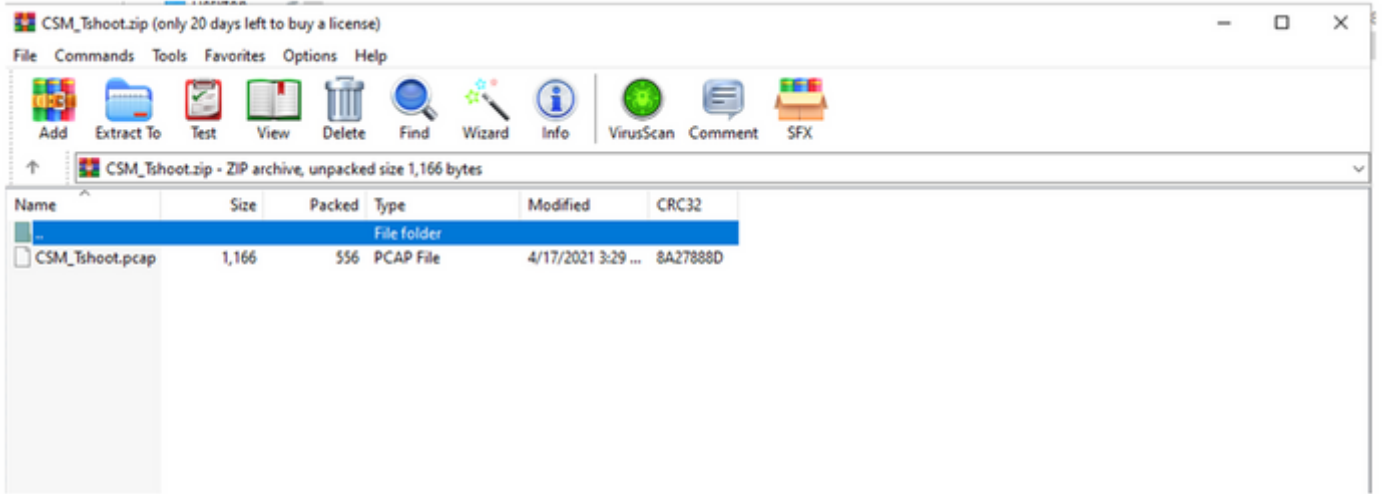
Cancel Save Save and Run

Step 3. Log in on CSM client application or Client UI and type the admin credentials.

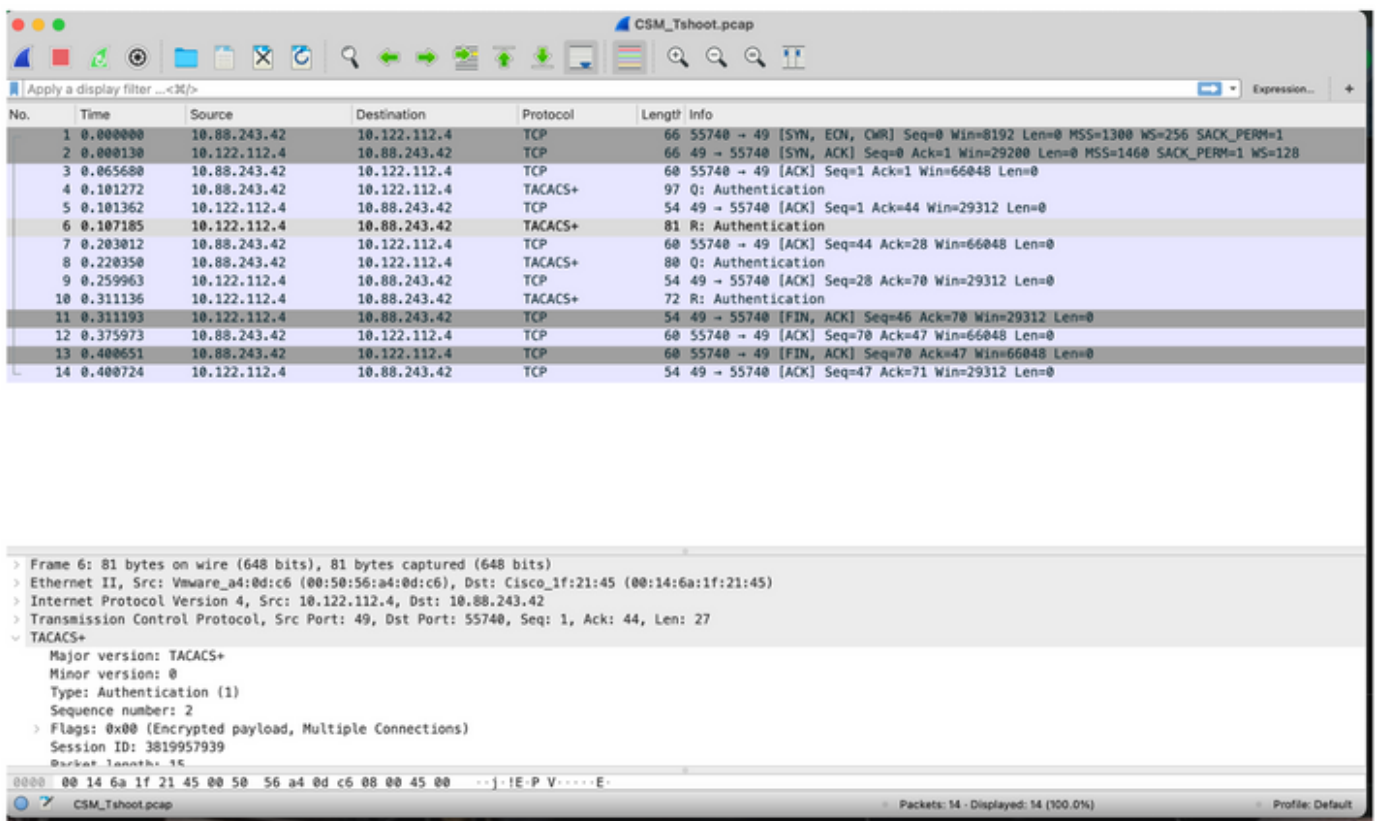
Step 4. On ISE, Select **the Stop** button and verify the pcap file has been sent to the defined repository.

Refresh Add Edit Trash Start Stop Download Filter

<input type="checkbox"/>	Host Name	Network Interface	Filter	File Name	Repository	File S...	Number o
<input type="checkbox"/>	ise30.ciscoise.lab	GigabitEthernet 0	ip host 10.88.243.42	CSM_Tshoot	VMReposit...	100	1



Step 5. Open the pcap file to validate the successful communication between CSM and ISE.



If no entries are shown on pcap file validate the following:

1. Devices Administration service is enabled on ISE node
2. Right ISE IP address has been added on CSM configuration
3. In case of a firewall is in the middle verify port 49 (TACACS) is permitted.