

CSM TACACS-Integration mit ISE

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Netzwerkdigramm](#)

[Authentifizierungsverfahren](#)

[ISE-Konfiguration](#)

[CSM-Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument wird das Verfahren zur Integration von Cisco Security Manager (CSM) in Identity Services Engine (ISE) für die Authentifizierung von Administratoren-Benutzern mit dem TACACS+-Protokoll beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CSM-Server, Version 4.22
- ISE Version 3.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Standardmäßig verwendet der Cisco Security Manager (CSM) einen Authentifizierungsmodus namens CiscoWorks, um Benutzer lokal zu authentifizieren und zu autorisieren. Um über eine zentralisierte Authentifizierungsmethode zu verfügen, können Sie die Cisco Identity Service Engine über das TACACS-Protokoll verwenden.

Konfiguration

Netzwerkdiagramm



Authentifizierungsverfahren

Schritt 1: Melden Sie sich mit den Anmeldeinformationen des Admin-Benutzers bei der CSM-Anwendung an.

Schritt 2: Authentifizierungsprozess-Trigger und die ISE validiert die Anmeldeinformationen lokal oder über Active Directory.


Schritt 3: Sobald die Authentifizierung erfolgreich war, sendet die ISE ein Genehmigungspaket, um den Zugriff auf den CSM zu autorisieren.

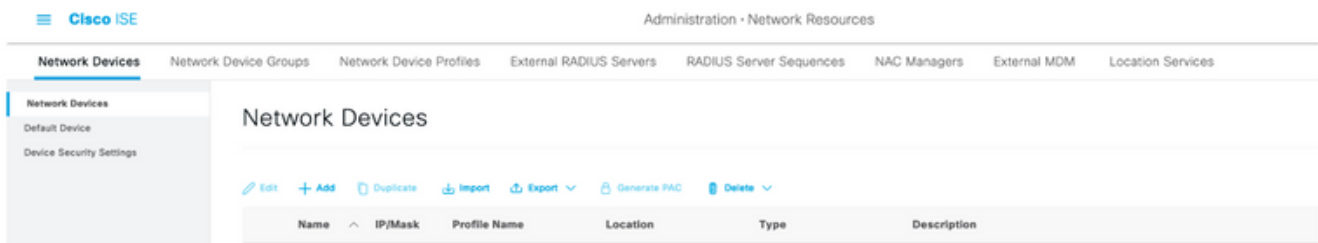
Schritt 4: Der CSM ordnet den Benutzernamen der lokalen Benutzerrollenzuweisung zu.

Schritt 5: Die ISE zeigt ein erfolgreiches Authentifizierungs-Live-Protokoll an.

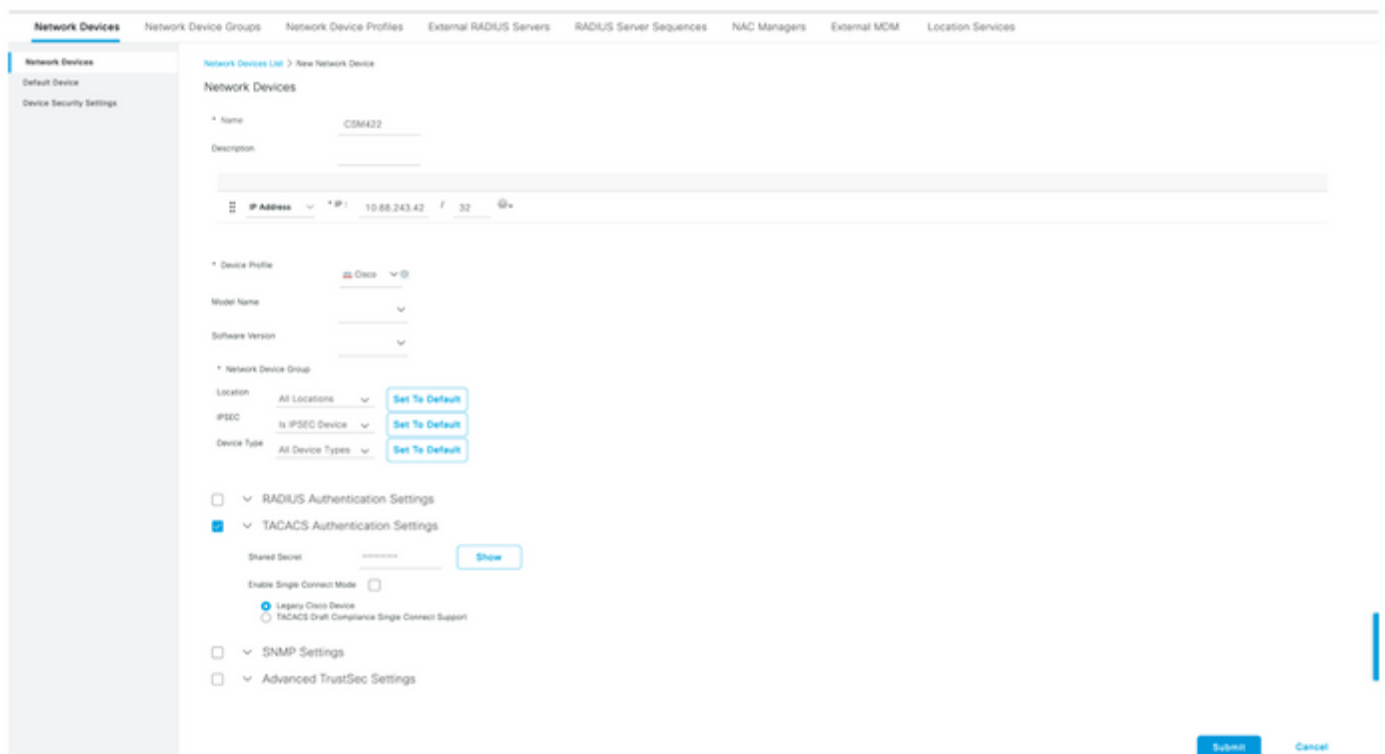
ISE-Konfiguration



Schritt 1: Wählen Sie das Symbol für drei Leitungen  Navigieren Sie in der linken oberen Ecke zu **Administration > Network Resources > Network Devices (Verwaltung > Netzwerkressourcen > Netzwerkgeräte)**.



Schritt 2: Wählen Sie die Schaltfläche **+Hinzufügen**, und geben Sie die korrekten Werte für den Namen und die IP-Adresse des Netzwerkzugriffsgeräts ein. Aktivieren Sie anschließend das Kontrollkästchen **TACACS Authentication Settings** (TACACS-Authentifizierungseinstellungen), und definieren Sie einen gemeinsamen geheimen Schlüssel. Wählen Sie die Schaltfläche **Senden**.



Schritt 3: Wählen Sie das Symbol für drei Leitungen Navigieren Sie in der linken oberen Ecke zu **Administration > Identity Management > Groups** (Verwaltung > Identitätsverwaltung > Gruppen).

Identity Groups

EQ



- > Endpoint Identity Groups
- > **User Identity Groups**

User Identity Groups

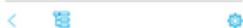
Edit + Add Delete Import Export

<input type="checkbox"/>	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

Schritt 4: Navigieren Sie zum Ordner **Benutzeridentitätsgruppen**, und wählen Sie die Schaltfläche **+Hinzufügen** aus. Definieren Sie einen Namen, und wählen Sie die Schaltfläche **Senden**.

Identity Groups

EQ



- > Endpoint Identity Groups
- > **User Identity Groups**

User Identity Groups

Edit + Add Delete Import Export

Selected 0 Total 10

All

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/>	CSM Admin	
<input type="checkbox"/>	CSM Oper	

Hinweis: In diesem Beispiel werden Gruppen für CSM-Admin und CSM-Oper-Identität erstellt. Sie können Schritt 4 für jeden Administratorbenutzer-Typ im CSM wiederholen.



Schritt 5: Wählen Sie das Symbol für drei Leitungen und navigieren Sie zu **Administration > Identity Management > Identities**. Wählen Sie die Schaltfläche **+Hinzufügen**, legen Sie Benutzernamen und Kennwörter fest, und wählen Sie dann die Gruppe aus, der der Benutzer angehört. In diesem Beispiel werden die **csmadmin-** und **csmoper-** Benutzer erstellt und jeweils CSM Admin- bzw. CSM Oper-Gruppe zugewiesen.

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: _____ Re-linear Password: _____

* Login Password: _____ * Generate Password

These 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 (yyyy-mm-dd)

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	



Schritt 6: Auswählen und navigieren Sie zu **Administration > System > Deployment**. Wählen Sie den Hostnamen-Knoten aus, und aktivieren Sie den **Device Admin Service**.

Hostname	Personas	Role(s)	Services	Node Status
<input type="checkbox"/> Ise30	Administration, Monitoring, Policy Service	STANDALONE	IDENTITY MAPPING, SESSION, PROFILER, DE...	<input checked="" type="checkbox"/>

> Enable SXP Service ⓘ

Enable Device Admin Service ⓘ

Enable Passive Identity Service ⓘ

Hinweis: Im Fall einer verteilten Bereitstellung wählen Sie den PSN-Knoten aus, der TACACS-Anforderungen behandelt.

Schritt 7: Wählen Sie das Symbol für drei Zeilen aus, und navigieren Sie zu **Administration > Device Administration > Policy Elements (Verwaltung > Geräteverwaltung > Richtlinienelemente)**. Navigieren Sie zu **Ergebnisse > TACACS-Befehlsätze**. Wählen Sie **+Schaltfläche hinzufügen**, definieren Sie einen Namen für den Befehlsatz, und aktivieren Sie den Befehl **Zulassen für alle Befehle, die nicht unter dem Kontrollkästchen aufgeführt sind**. Wählen Sie **Senden** aus.

Cisco ISE Work Centers - Device Administration Evaluation Mode 39 Days

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

TACACS Command Sets > New Command Set

Name: Permit all

Description:

Commands


Permit any command that is not listed below

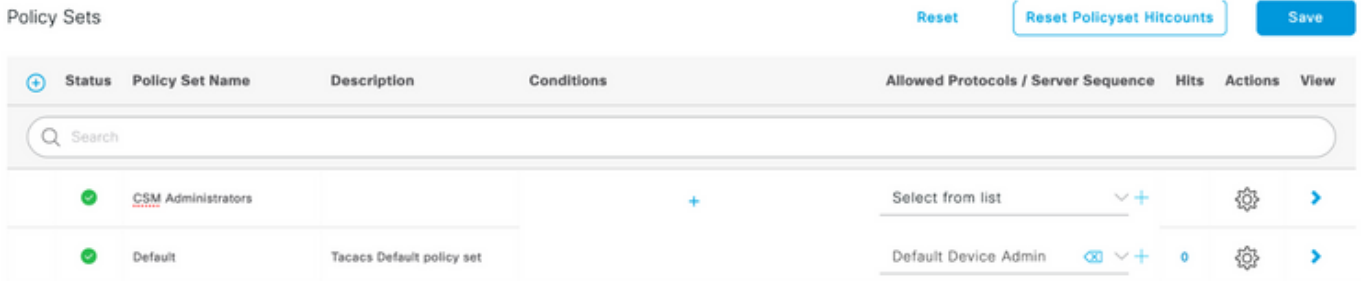
+ Add Trash Edit Move Up Move Down

Grant	Command	Arguments
No data found.		

Cancel Submit

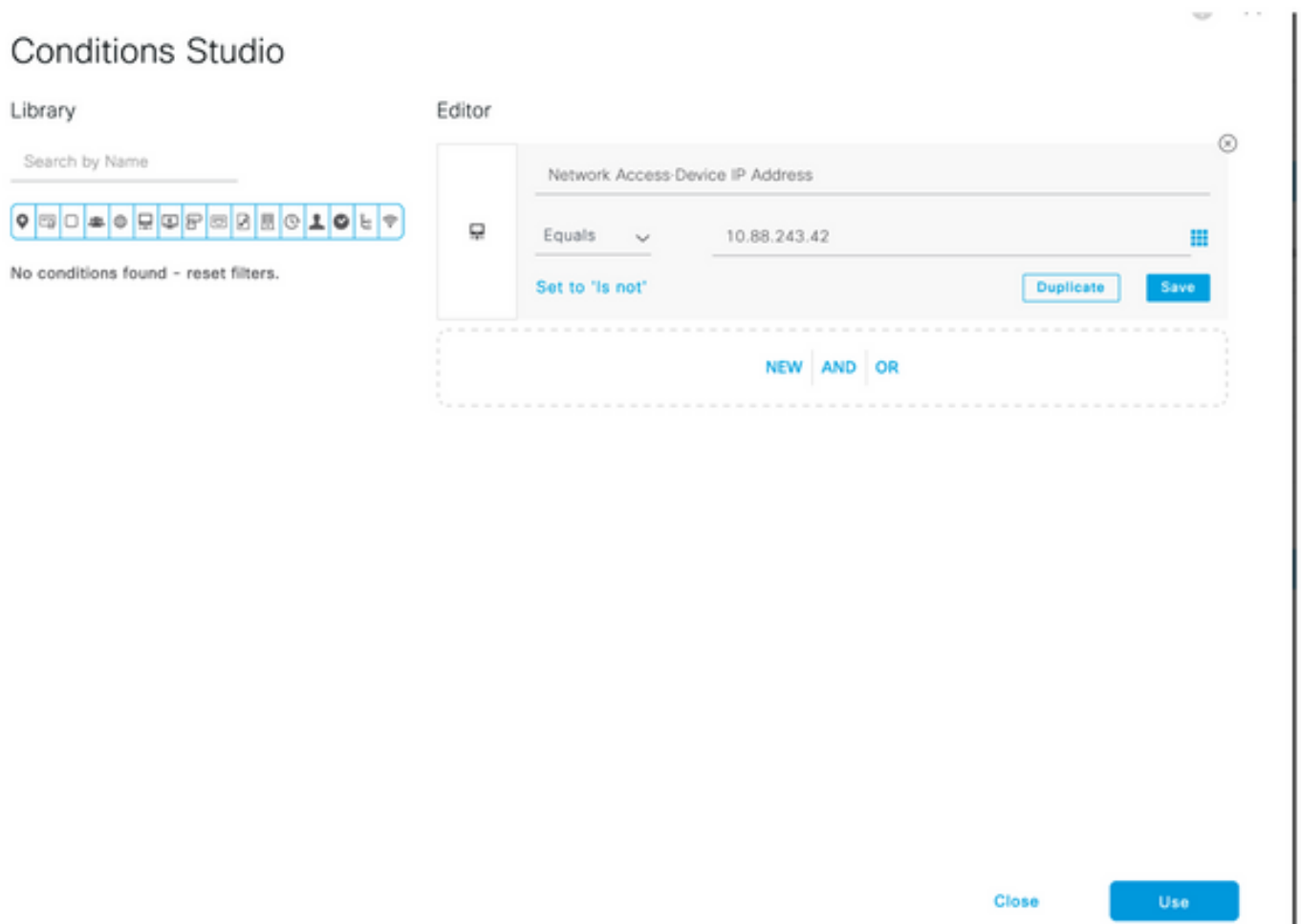
Schritt 8: Wählen Sie in der linken oberen Ecke das Symbol für drei Zeilen aus, und navigieren Sie zu **Administration (Verwaltung) > Device Administration (Geräteverwaltung) > Device Admin Policy**

Sets (Geräte-Admin-Richtliniensätze). Auswählen  unter "Policy Sets title" (Titel für Richtliniensätze) einen Namen definieren und die **+Schaltfläche** in der Mitte auswählen, um eine neue Bedingung hinzuzufügen.



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	⚙️	➔

Schritt 9: Wählen Sie im Fenster Bedingung die Option **Attribut** hinzufügen aus, und wählen Sie dann **Netzwerkgerät**-Symbol gefolgt von der IP-Adresse des Netzwerkzugriffsgeräts aus. Wählen Sie **Attributwert** aus, und fügen Sie die CSM-IP-Adresse hinzu. Wählen Sie **Nach** Beendigung **verwenden** aus.



Conditions Studio

Library

Search by Name

No conditions found - reset filters.

Editor

Network Access-Device IP Address

Equals 10.88.243.42

Set to 'is not' Duplicate Save

NEW AND OR

Close Use

Schritt 10: Wählen Sie im Abschnitt **Zulassen von Protokollen** die Option **Gerätstandardadministrator** aus. Wählen Sie **Speichern**


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		

Schritt 11: Wählen Sie den Pfeil nach rechts aus



Symbol des Policy Set zum Definieren von Authentifizierungs- und Autorisierungsrichtlinien


Schritt 12: Auswählen  unter dem Titel der Authentifizierungsrichtlinie einen Namen definieren und in der Mitte das + auswählen, um eine neue Bedingung hinzuzufügen. Wählen Sie im Fenster Bedingung die Option **Attribut** hinzufügen aus, und wählen Sie dann **Netzwerkgerät**-Symbol gefolgt von der IP-Adresse des Netzwerkzugriffsgärts aus. Wählen Sie **Attributwert** aus, und fügen Sie die CSM-IP-Adresse hinzu. Wählen Sie **Nach** Beendigung **verwenden aus**

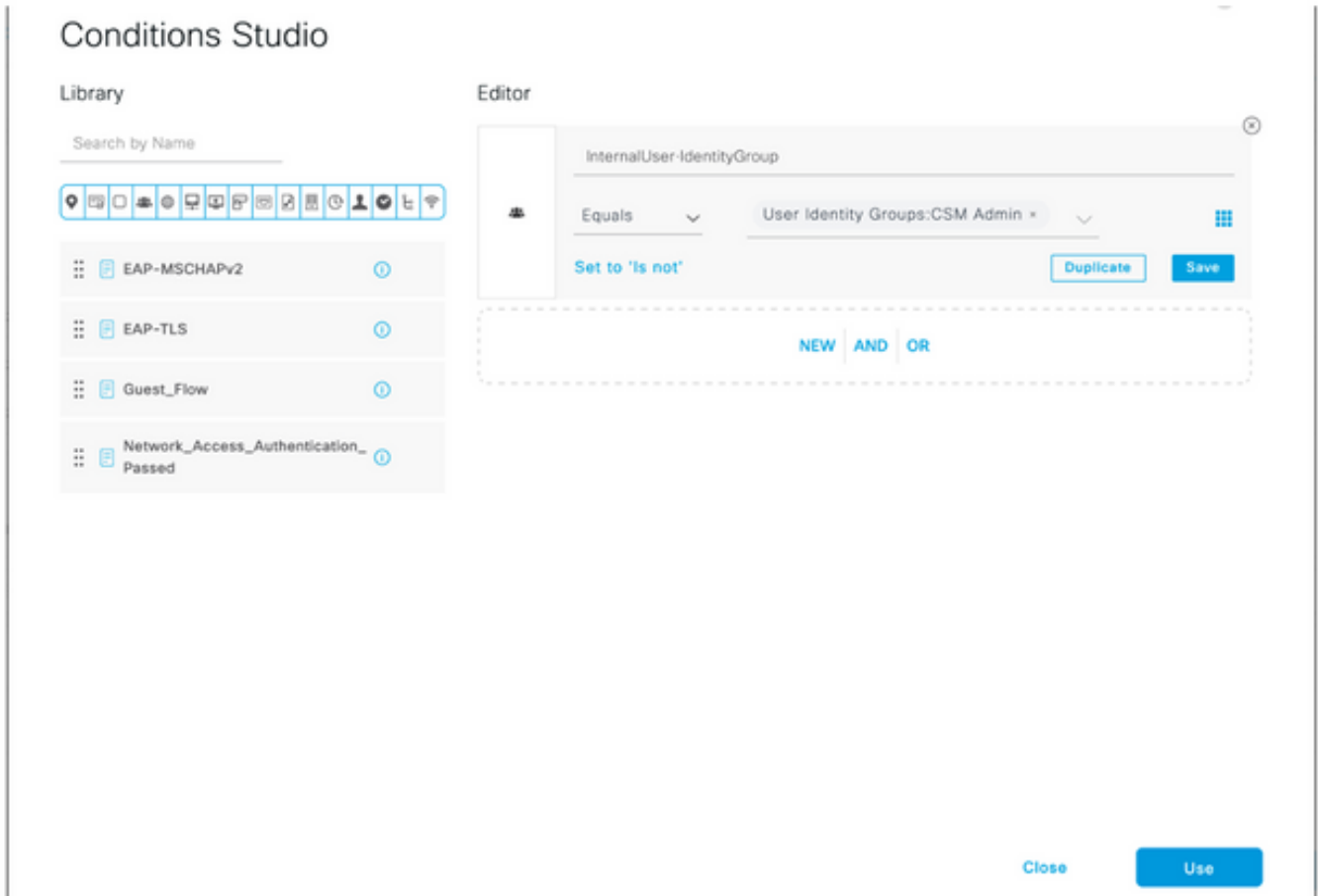
Schritt 13: Wählen Sie **Interne** Benutzer als Identitätsspeicher aus, und wählen Sie **Speichern aus**.

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	CSM Authentication	Network Access-Device IP Address EQUALS 10.88.243.42	Internal Users		

Hinweis: Der Identitätsspeicher kann in einen AD-Speicher geändert werden, wenn die ISE einem Active Directory hinzugefügt wird.

Schritt 14: Auswählen  definieren Sie unter dem Titel der Autorisierungsrichtlinie einen Namen, und wählen Sie in der Mitte die +-Schaltfläche aus, um eine neue Bedingung hinzuzufügen. Wählen Sie im Fenster Bedingung die Option **Attribut** hinzufügen aus, und wählen Sie dann **das Identitätsgruppensymbol** gefolgt von **Interner Benutzer aus: Identitätsgruppe**. Wählen Sie die CSM-Administratorgruppe aus, und wählen Sie **Verwenden aus**.



Schritt 15: Wählen Sie unter "Befehlssatz" die Option Gesamten in Schritt 7 erstellten Befehlssatz zulassen aus, und wählen Sie dann **Speichern aus**.

Wiederholen Sie die Schritte 14 und 15 für die Gruppe CSM Oper.

Authorization Policy (3)

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

Schritt 16 (optional). Wählen Sie in der linken oberen Ecke drei Zeilen-Symbol aus, und wählen Sie **Administration > System>Maintenance>Repository aus**, wählen Sie **+Add**, um ein Repository hinzuzufügen, das zum Speichern von TCP-Dump-Dateien für die Fehlerbehebung verwendet wird.

Schritt 17 (optional). Definieren Sie einen Projektnamen, ein Protokoll, einen Servernamen, einen Pfad und Anmeldeinformationen. Wählen Sie abschließend **Senden** aus.

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-Konfiguration

Schritt 1: Melden Sie sich mit dem lokalen Administratorkonto bei der Cisco Security Manager Client-Anwendung an. Navigieren Sie im Menü zu **Extras > Sicherheitsmanager-Verwaltung**.

Cisco Security Manager
Version 4.22.0 Service Pack 1

Server Name

Username

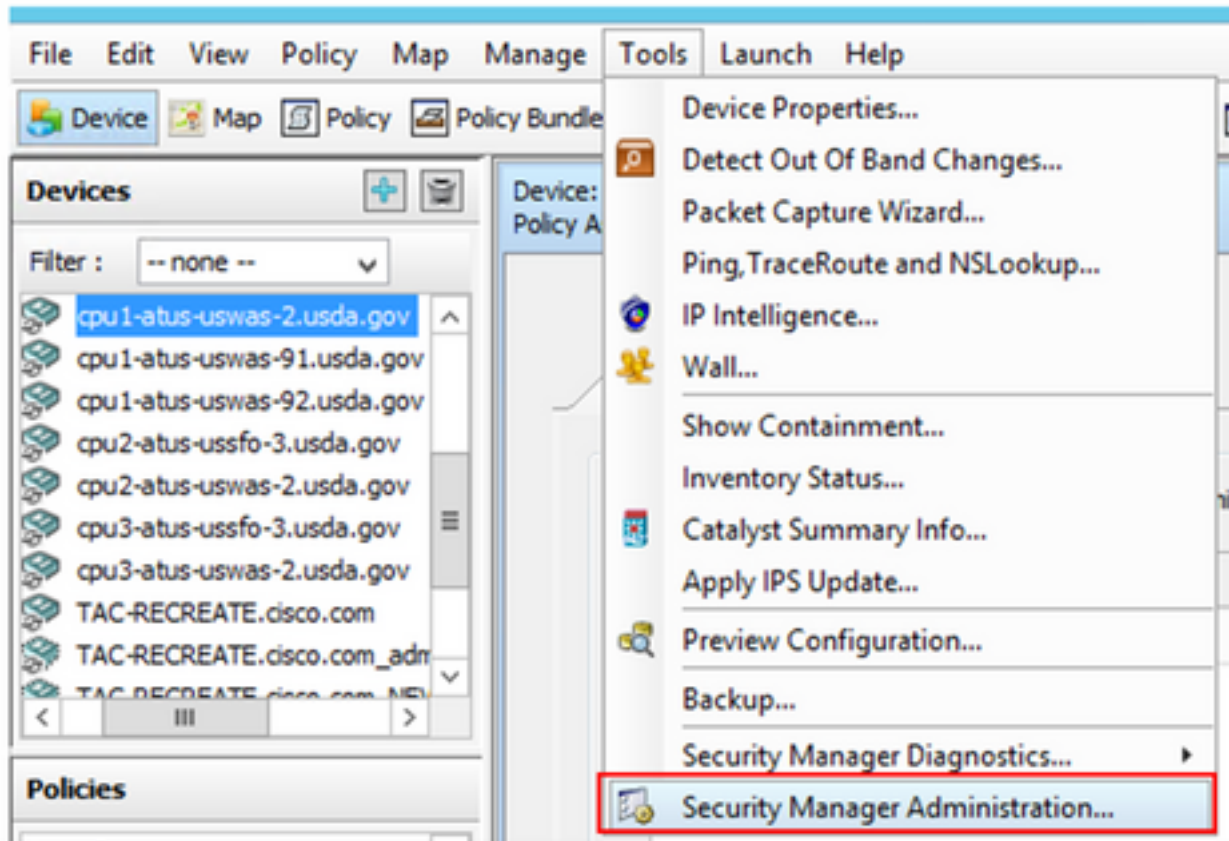
Password

Default View

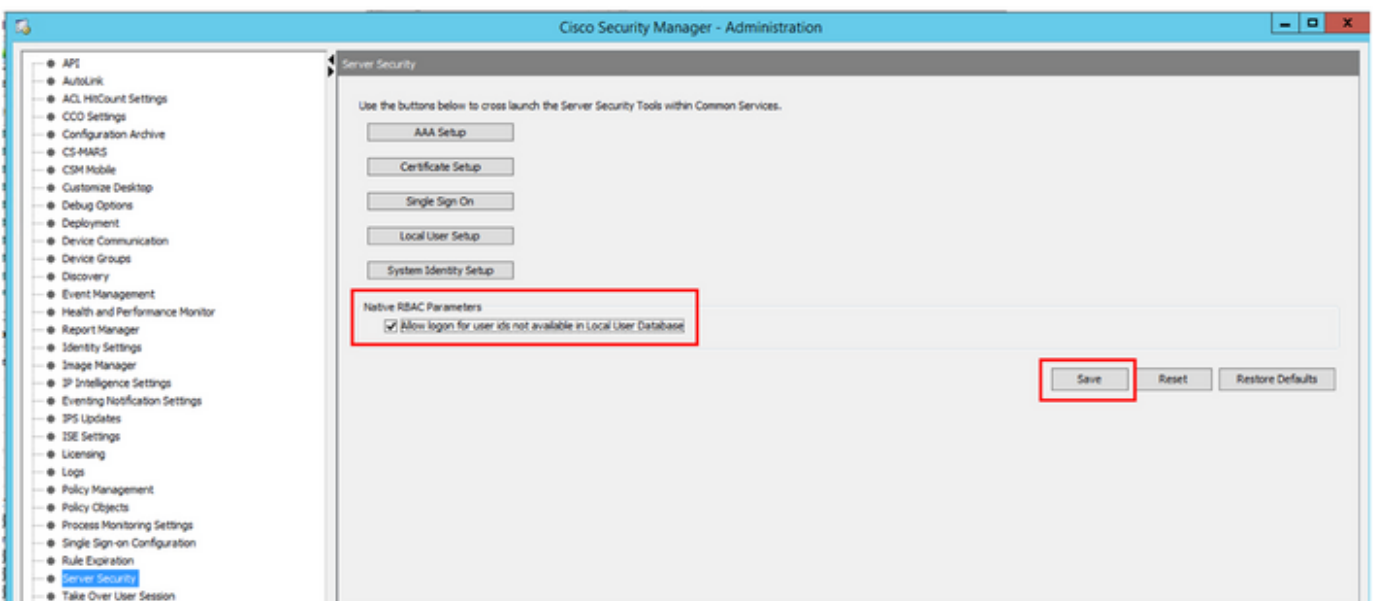
[Login](#) [Help](#)

© 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.

CISCO



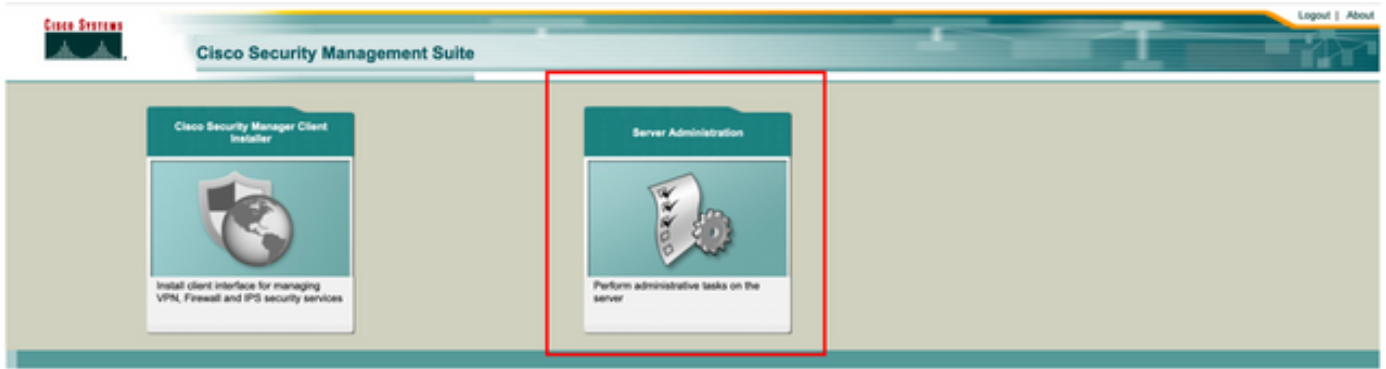
Schritt 2: Aktivieren Sie das Kontrollkästchen unter **Native RBAC Parameters**. Wählen Sie **Speichern** und **Schließen**



Schritt 3: Wählen Sie im Menü **Datei > Senden aus**. **Datei > Senden**.

Hinweis: Alle Änderungen müssen gespeichert werden, falls Konfigurationsänderungen erforderlich sind.

Schritt 4: Navigieren Sie zu CSM Management UI, geben Sie https://<enter_CSM_IP_Address_ein.> und wählen Sie **Server Administration** aus.

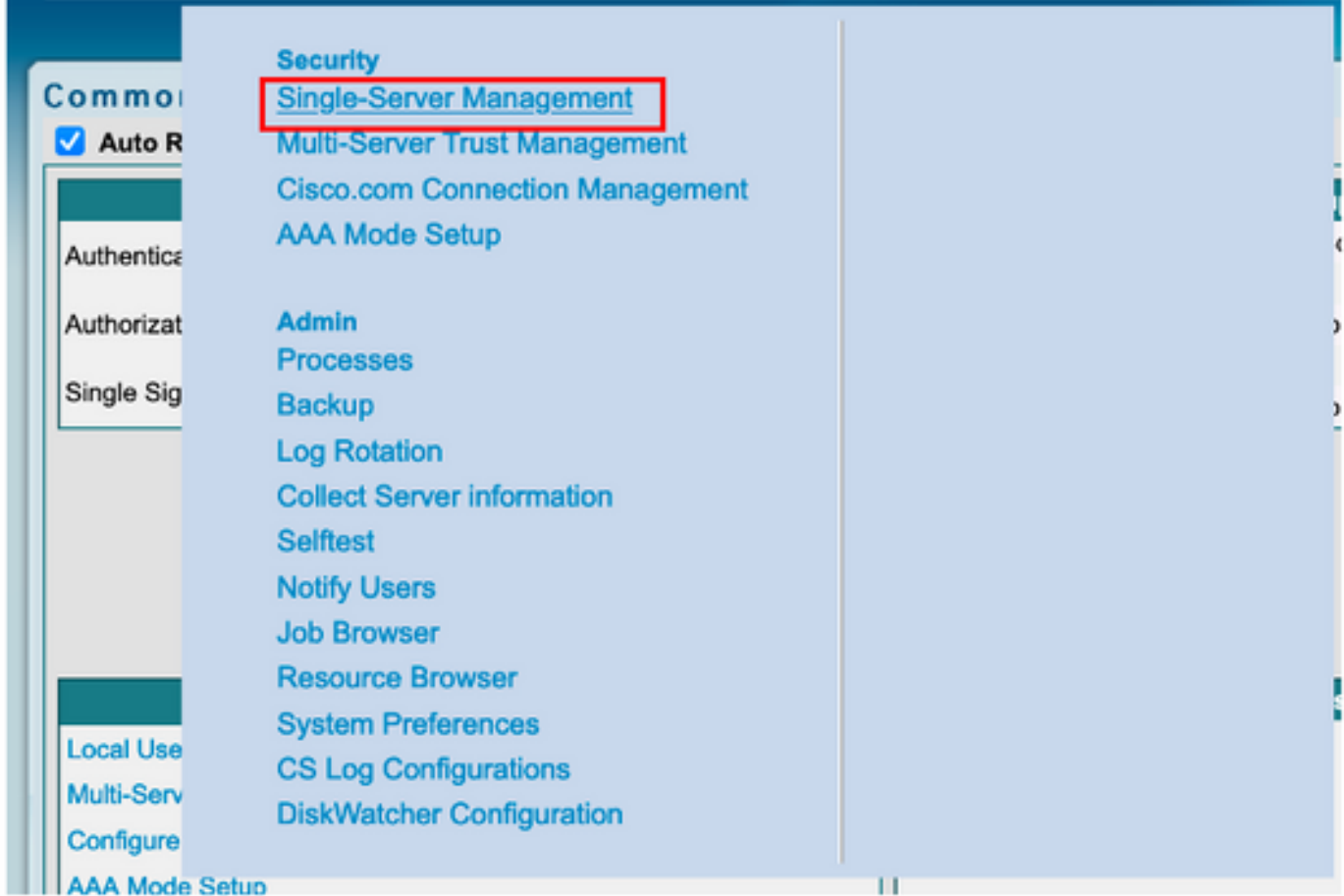


Hinweis: Die Schritte 4 bis 7 zeigen die Prozedur zur Definition der Standardrolle für alle Administratoren, die nicht auf der ISE definiert sind. Diese Schritte sind optional.

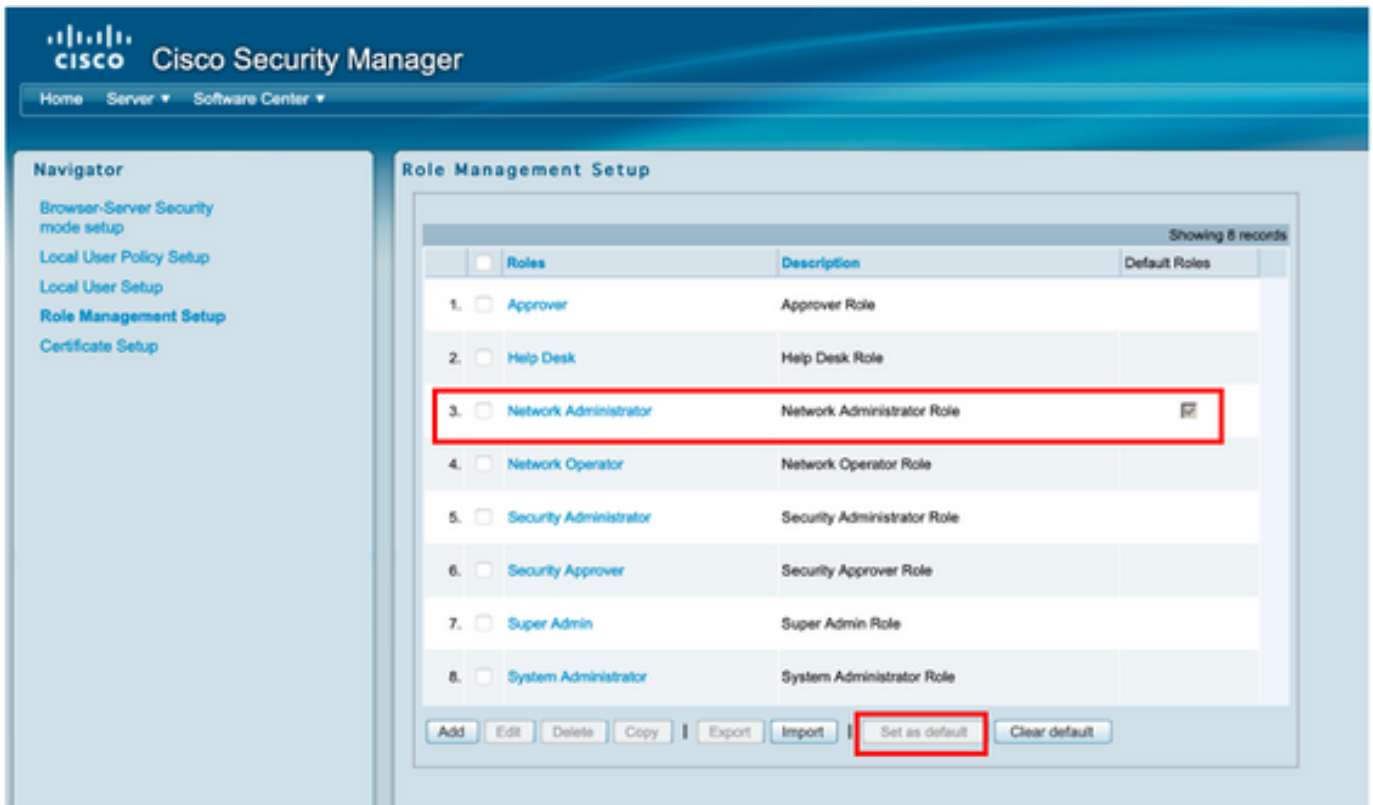
Schritt 5: Validieren Sie, ob der Authentifizierungsmodus auf **CiscoWorks Local (Lokal)** und **Online-BenutzerID** (Online-Benutzer-ID) festgelegt ist, ist das lokale Administratorkonto, das auf CSM erstellt wurde.

Job ID	Job Type	Status	Description	Completed At
1001.1370	SystemCheckUtility	Succeeded	SysCheckTest	Sat Apr 17 05:01:56 PDT 2021
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

Schritt 6: Navigieren Sie zu **Server**, und wählen Sie **Einzelserver-Management** aus.



Schritt 7: Wählen Sie Role Management Setup (Rollenverwaltungs-Setup) aus, und wählen Sie die Standardberechtigung aus, die alle Admin-Benutzer bei der Authentifizierung erhalten. In diesem Beispiel wird der Netzwerkadministrator verwendet. Wählen Sie anschließend **die Standardeinstellung** aus.



Schritt 8: Wählen Sie **Server > AAA Mode Setup Role (Servermodus > AAA-Modus-Setup-Rolle)** aus und wählen Sie dann **TACACS+**-Option aus. Wählen Sie schließlich **Change** aus, um ISE-Informationen hinzuzufügen.





Schritt 9: Definieren Sie ISE-IP-Adresse und -Schlüssel. Optional können Sie die Option auswählen, die allen lokalen Authentifizierungsbenutzern oder nur einem Benutzer erlaubt, wenn die Anmeldung fehlschlägt. In diesem Beispiel ist der Nur-Admin-Benutzer als Fallbackmethode zulässig. Wählen Sie **OK**, um die Änderungen zu speichern.

The screenshot shows the 'Login Module Options' dialog box. It contains the following fields and options:

- Selected Login Module: TACACS+
- Description: Cisco Prime TACACS+ login module
- Server: 10.122.112.4
- Port: 49
- SecondaryServer: (empty)
- SecondaryPort: 49
- TertiaryServer: (empty)
- TertiaryPort: 49
- Key: (masked with dots)
- Debug: True False
- Login fallback options:
 - Allow all Local Authentication users to fallback to the Local Authentication login.
 - Only allow the following user(s) to fallback to the Local Authentication login if preceding login fails:
 - admin (comma separated)
 - Allow no fallbacks to the Local Authentication login.

At the bottom right, there are 'OK' and 'Cancel' buttons.

Login Module Change Summary

Login Module changes updated.

OK

Schritt 10: Wählen Sie **Server > Einzelserver-Management** aus, wählen Sie dann **Lokales Benutzer-Setup** aus, und wählen Sie **Hinzufügen** aus.



Cisco Security Manager

Home Server Software Center

Navigator

- Browser-Server Security mode setup
- Local User Policy Setup
- Local User Setup**
- Role Management Setup
- Certificate Setup

Local User Setup

Showing 206 records

	Users
1.	<input type="checkbox"/> Aaron.Logan
2.	<input type="checkbox"/> Adrian.Lotreal
3.	<input type="checkbox"/> Adrian.Richards
4.	<input type="checkbox"/> ahohenstein
5.	<input type="checkbox"/> Aida.Aguilar
6.	<input type="checkbox"/> Alaric.Castain
7.	<input type="checkbox"/> alem.weldehmanot
8.	<input type="checkbox"/> allen.spiegel
9.	<input type="checkbox"/> Andrew.OConnor
10.	<input type="checkbox"/> Anwar.Khan
11.	<input type="checkbox"/> amand.amith
12.	<input type="checkbox"/> Bernard.Aiston
13.	<input type="checkbox"/> bthess
14.	<input type="checkbox"/> Bill.Mason
15.	<input type="checkbox"/> bill.nash
16.	<input type="checkbox"/> Billy.Vaughan
17.	<input type="checkbox"/> bpiotnik
18.	<input type="checkbox"/> Bruffler.Sorenson

Select items then take an action

Import Users Export Users Edit Delete **Add** Modify My Profile

Schritt 11: Definieren Sie in Schritt 5 im ISE-Konfigurationsabschnitt denselben Benutzernamen und dasselbe Kennwort, das für die ISE erstellt wurde. In diesem Beispiel werden **Rollen für die Autorisierung von Aufgaben** csmoper und **Help Desk** verwendet. Wählen Sie **OK**, um den Administrator-Benutzer zu speichern.

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

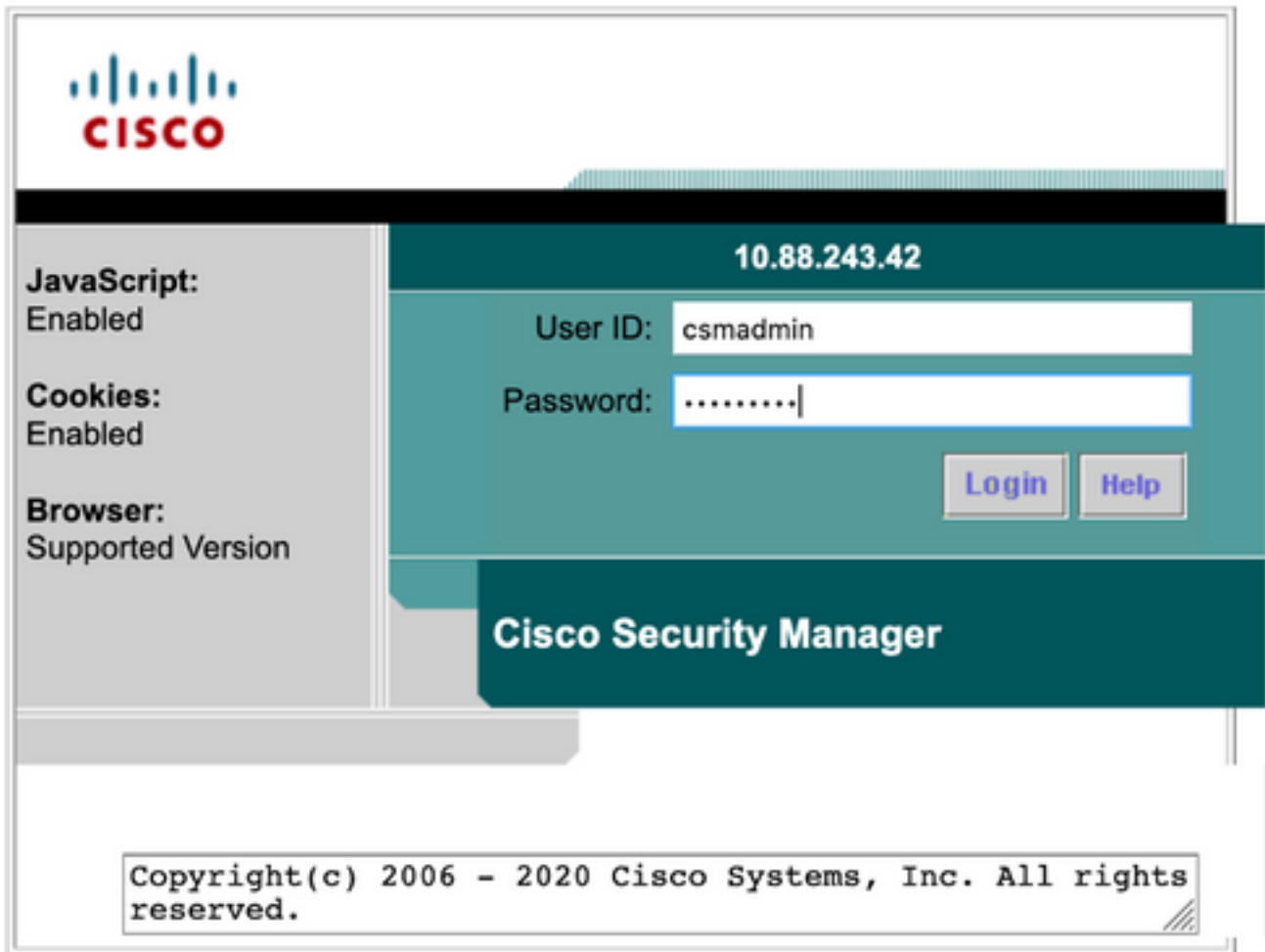
Device level Authorization

Not Applicable

Überprüfung

Benutzeroberfläche des Cisco Security Manager-Clients

Schritt 1: Öffnen Sie einen neuen Fensterbrowser, und geben Sie <https://<enter CSM IP Address>> ein. Verwenden Sie im Abschnitt zur ISE-Konfiguration den Benutzernamen und das Kennwort **csmadmin**, der in Schritt 5 erstellt wurde.



Erfolgreiche Anmeldung beim Versuch kann in ISE TACACS-Live-Protokollen überprüft werden

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	Authorization Policy	ise30	CSM422

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

Cisco Security Manager Client-Anwendung

Schritt 1: Melden Sie sich mit dem Helpdesk-Administratorkonto bei der Cisco Security Manager Client-Anwendung an.



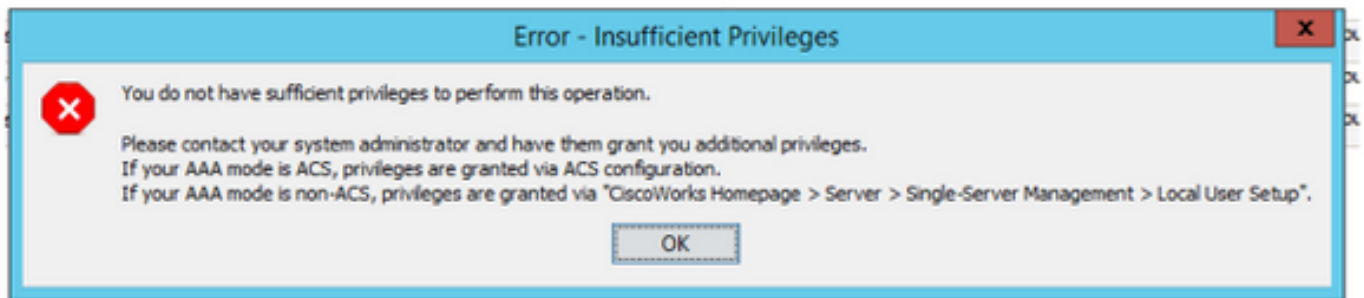
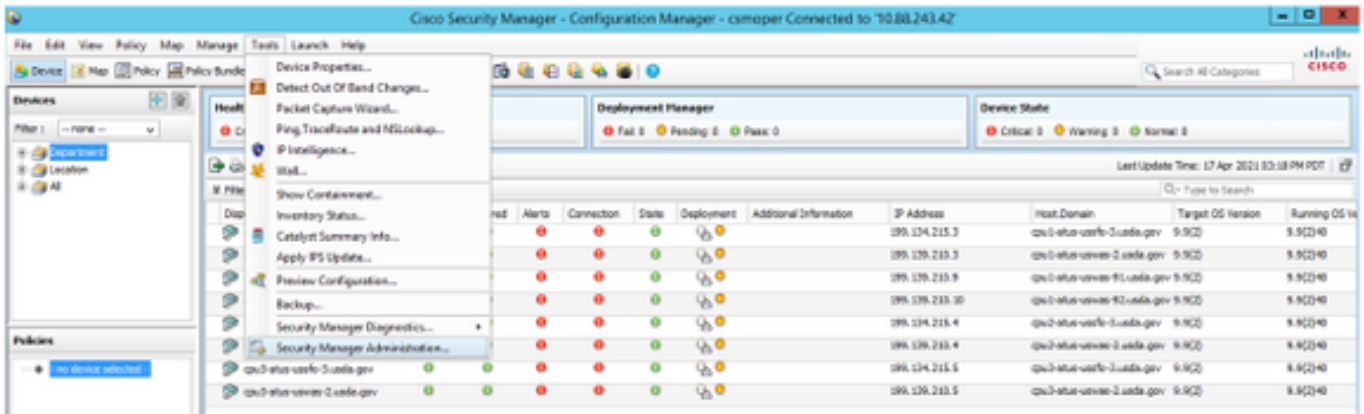
Erfolgreiche Anmeldung beim Versuch kann in ISE TACACS-Live-Protokollen überprüft werden

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

Schritt 2: Wählen Sie im Menü CSM-Client-Anwendung **Extras > Sicherheitsmanager-Verwaltung**, eine Fehlermeldung weist darauf hin, dass ein Mangel an Berechtigungen angezeigt werden muss.



Schritt 3: Wiederholen Sie die Schritte 1 bis 3 mit dem **csmadmin**-Konto, um zu überprüfen, ob diesem Benutzer die entsprechenden Berechtigungen erteilt wurden.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Kommunikationsvalidierung mit dem TCP-Dump-Tool auf der ISE

Schritt 1. Melden Sie sich bei der ISE an, navigieren Sie zum Symbol für drei Zeilen in der linken oberen Ecke, und wählen Sie **Operations > Troubleshoot > Diagnostic Tools (Vorgänge > Fehlerbehebung > Diagnosetools)** aus.

Schritt 2: Wählen Sie unter **Allgemeine Tools** die Option **TCP-Dumps** und dann **Add+ aus**. Wählen Sie Hostname, Network Interface File Name, Repository und optional einen Filter aus, um nur den Kommunikationsfluss der CSM-IP-Adresse zu erfassen. Wählen Sie **Speichern und Ausführen**

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

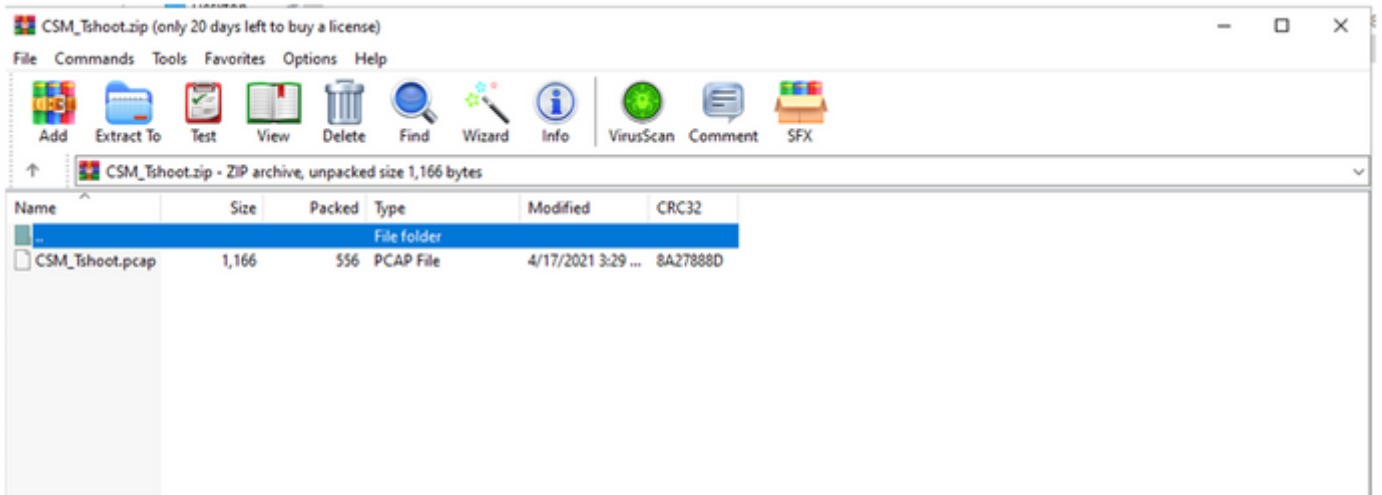
Cancel Save Save and Run

Schritt 3: Melden Sie sich bei der CSM-Clientanwendung oder der Client-Benutzeroberfläche an, und geben Sie die Administratoranmeldeinformationen ein.

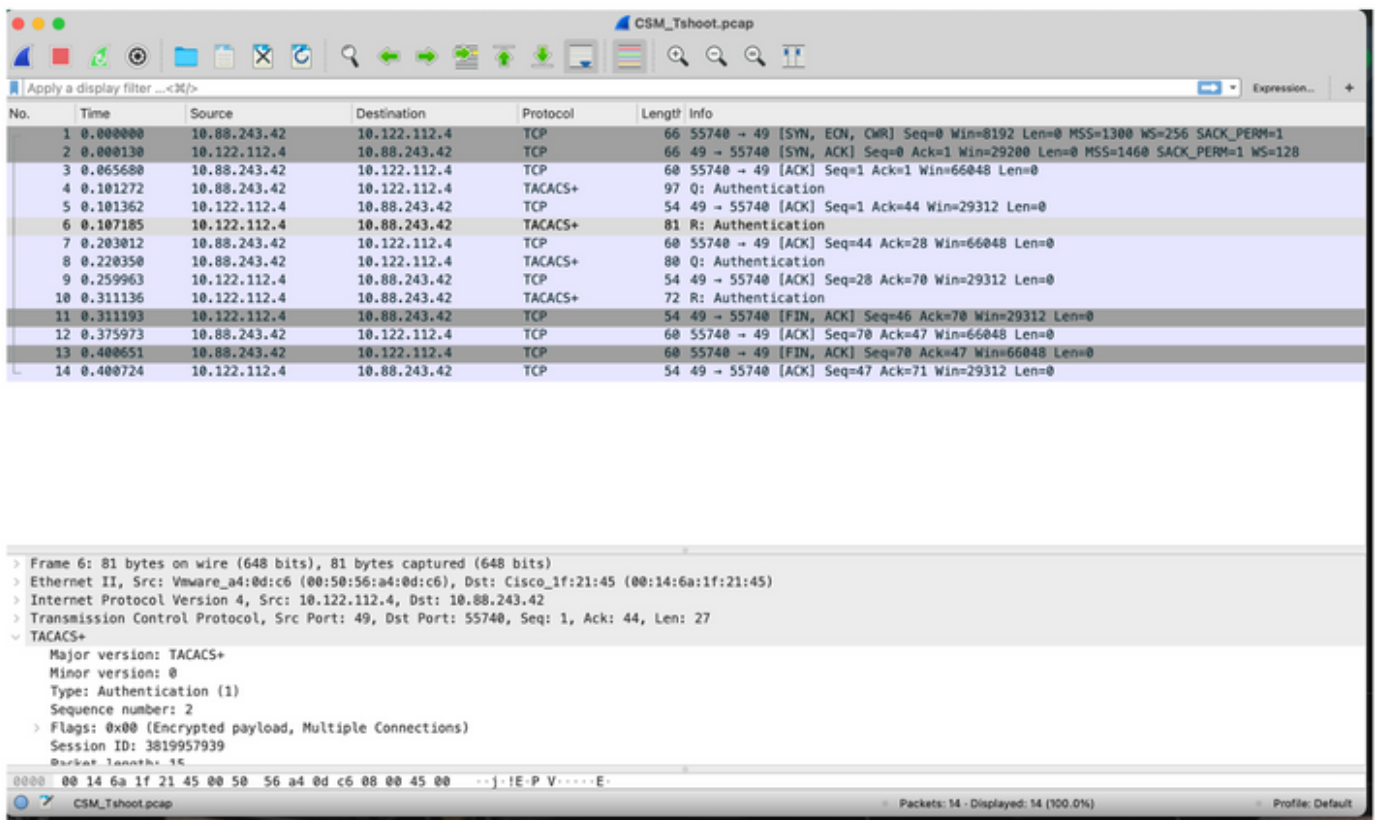
Schritt 4: Wählen Sie auf der ISE die Schaltfläche **Stopp** aus, und überprüfen Sie, ob die pcap-Datei an das definierte Repository gesendet wurde.

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



Schritt 5: Öffnen Sie die pcap-Datei, um die erfolgreiche Kommunikation zwischen CSM und ISE zu überprüfen.



Wenn in der pcap-Datei keine Einträge angezeigt werden, überprüfen Sie Folgendes:

1. Der Device Administration Service ist auf ISE-Knoten aktiviert.
2. Die richtige ISE-IP-Adresse wurde zur CSM-Konfiguration hinzugefügt.
3. Falls sich eine Firewall in der Mitte befindet, überprüfen Sie, ob Port 49 (TACACS) zulässig ist.