

Configure APIC for Device Administration with ISE and TACACS+

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Authentication Procedure](#)

[APIC Configuration](#)

[ISE Configuration](#)

[Verify](#)

[Troubleshoot](#)

Introduction

This document describes the procedure to integrate APIC with ISE for administrator users authentication with TACACS+ Protocol.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Application Policy Infrastructure Controller (APIC)
- Identity Services Engine (ISE)
- TACACS protocol

Components Used

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

- APIC version 4.2(7u)
- ISE version 3.2 Patch 1

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

Network Diagram



Integration Diagram

Authentication Procedure

Step 1. Log into the APIC application with Admin User Credentials.

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

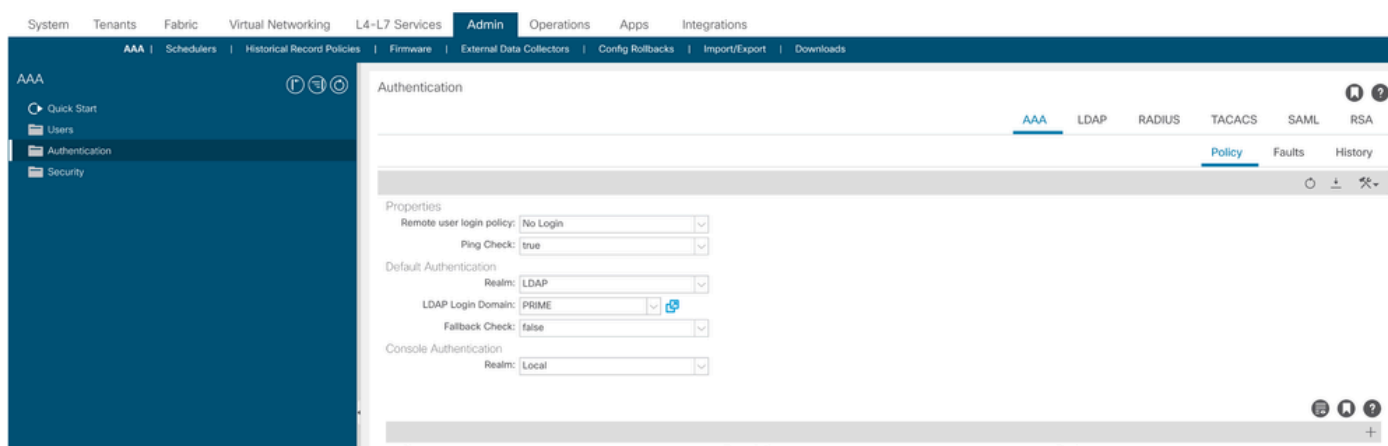
Step 3. Once authentication is successful, ISE sends a permit packet to authorize access to the APIC.

Step 4. ISE shows a successful authentication live log.

 **Note:** APIC replicates TACACS+ configuration to leaf switches that are part of the fabric.

APIC Configuration

Step 1. Navigate to **Admin > AAA > Authentication > AAA** and choose **+** icon in order to create a new login domain.



APIC login admin configuration

Step 2. Define a name and realm for the new Login Domain and click **+** under Providers in order to create a new provider.

Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
------	----------	-------------

Cancel

Submit

APIC login admin

Providers:

Name	Priority	Description
<input type="text" value="select an option"/>	<input type="text"/>	<input type="text"/>

Create TACACS+ Provider

Update Cancel

APIC TACACS Provider

Step 3. Define the ISE IP address or hostname, define a shared secret, and choose the management Endpoint Policy Group (EPG). Click **Submit** in order to add TACACS+ Provider to login admin.

Create TACACS+ Provider



Host Name (or IP Address):

Description:

Port:

Authorization Protocol: CHAP MS-CHAP PAP

Key:

Confirm Key:

Timeout (sec):

Retries:

Management EPG:

Server Monitoring: Disabled Enabled

Cancel

Submit

APIC TACACS Provider settings

Create Login Domain



Name:

Realm:

Description:

Providers:

Name	Priority	Description
52.13.89	1	

Cancel

Submit

Host Name	Description	Port	Timeout (sec)	Retries
52.13.89		49	5	1

TACACS Provider view

ISE Configuration

Step 1. Navigate to **≡ > Administration > Network Resources > Network Device Groups**. Create a Network Device Group under All Device Types.

≡ Cisco ISE

Network Devices

Network Device Groups

Network Device Profiles

External

Network Device Groups

All Groups

Choose group ▾



 Add
 Duplicate
 Edit
  Trash
  Show group members
  Import
  Export ▾
 

<input type="checkbox"/> Name	Description
<input type="checkbox"/> ▾ All Device Types	All Device Types
<input type="checkbox"/> APIC	

ISE Network Device Groups

Step 2. Navigate to **Administration > Network Resources > Network Devices**. Choose **Add** define APIC Name and IP address, choose APIC under Device Type and TACACS+ checkbox, and define the password used on APIC TACACS+ Provider configuration. Click **Submit**.

Network Devices

Default Device

Device Security Settings

Network Devices List > APIC-LAB

Network Devices

Name

APIC-LAB

Description

IP Address

* IP :

62.188.21

/

32

Device Profile

Cisco

Model Name

Software Version

Network Device Group

Location

All Locations

Set To Default

IPSEC

No

Set To Default

Device Type

APIC

Set To Default

☐ RADIUS Authentication Settings

☒ TACACS Authentication Settings

Shared Secret

Show

Retire




Repeat Step 1. and Step 2. for leaf switches.

Step 3. Use the instructions on this link in order to Integrate ISE with Active Directory;

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html>.



Note: This document includes both Internal users and AD Administrator groups as identity sources, however, the test is performed with the Identity Source of the internal users. The result is the same for AD groups.

Step 4. (Optional) Navigate to  > Administration > Identity Management > Groups. Choose  User Identity Groups and click  Add. Create one group for **read only Admin** users and **Admin** users.

Identity Groups

EQ



> Endpoint Identity Groups

> User Identity Groups

User Identity Groups

Edit

Add

Delete

Import

Export

	Name	Description
<input type="checkbox"/>	ALL_ACCOUNTS (default)	Default ALL_
<input type="checkbox"/>	APIC_RO	
<input type="checkbox"/>	APIC_RW	

Identity Group

Step 5. (Optional) Navigate to > Administration > Identity Management > Identity. Click **Add** and create one Read Only Admin user and Admin user. Assign each user to each group created in Step 4.

Users

Latest Manual Network Scan Res...

Network Access Users

Edit

Add

Change Status

Import

Export

Delete

Duplicate

	Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups
<input type="checkbox"/>	Enabled	APIC_ROUser					APIC_RO
<input type="checkbox"/>	Enabled	APIC_RWUser					APIC_RW

Step 6. Navigate to > Administration > Identity Management > Identity Source Sequence. Choose **Add**, define a name, and choose **AD Join Points** and **Internal Users** Identity Source from the list. Choose **Treat as if the user was not found** and proceed to the next store in the sequence under **Advanced Search List Settings** and click **Save**.

Identities

Groups

External Identity Sources

Identity Source Sequences

Settings

Identity Source Sequence

* Name

APIC_ISS

Description

Certificate Based Authentication

☐

Select Certificate Authentication Profile



Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available

Internal Endpoints

Guest Users

All_AD_Join_Points



Selected

iselab

Internal Users



Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

☐

Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"


☒

Treat as if the user was not found and proceed to the next store in the sequence

Identity Source Sequence

7. Navigate to > Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols. Select **Add**, define a name and uncheck **Allow CHAP** and **Allow MS-CHAPv1** from Authentication protocol list. Select

Save.



OverviewIdentitiesUser Identity GroupsExt Id SourcesNetwork Resources

Conditions>Network Conditions>Resultsv

Allowed ProtocolsTACACS Command SetsTACACS Profiles

Allowed Protocols Services List > TACACS Protocol

Allowed Protocols

NameTACACS Protocol

Description

Allowed Protocols

Authentication Protocols

Only Authentication Protocols relevant to TACACS are displayed.

☒ Allow PAP/ASCII☐ Allow CHAP☐ Allow MS-CHAPv1

TACACS Allow Protocol

8. Navigate to  > Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. Click **add** and create two profiles based on the attributes on the list under **Raw View**. Click **Save**.

- **Admin User:** cisco-av-pair=shell:domains=all/admin/
- **Read Only Admin User:** cisco-av-pair=shell:domains=all/read-all



Note: In case of space or additional characters, the authorization phase fails.

OverviewIdentitiesUser Identity GroupsExt Id SourcesNetwork ResourcesPolicy ElementsDevice Administration

Conditions>Network Conditions>Results▼Allowed ProtocolsTACACS Command SetsTACACS Profiles

TACACS Profiles > APIC ReadWrite Profile

TACACS Profile

NameAPIC ReadWrite Profile

Description

Task Attribute ViewRaw View

Profile Attributes

cisco-av-pair=shell:domains=all/admin/

CancelSave

TACACS Profile

OverviewIdentitiesUser Identity GroupsExt Id SourcesNetwork Resources


Conditions>Network Conditions>Results▼Allowed ProtocolsTACACS Command SetsTACACS Profiles

TACACS Profiles

RefreshAddDuplicateTrash▼Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	APIC ReadOnly Profile	Shell	
<input type="checkbox"/>	APIC ReadWrite Profile	Shell	

TACACS Admin and ReadOnly Admin Profiles

Step 9. Navigate to  > Work Centers > Device Administration > Device Admin Policy Set . Create a New Policy Set, define a name, and choose the device type APIC created in Step 1. Choose TACACS Protocol created in Step 7. as allowed Protocol, and click Save.

Policy Sets

ResetReset Policyset HitcountsSave

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search							
✓	APIC		DEVICE-Device Type EQUALS All Device TypesRAPIC	TACACS Protocol	55		

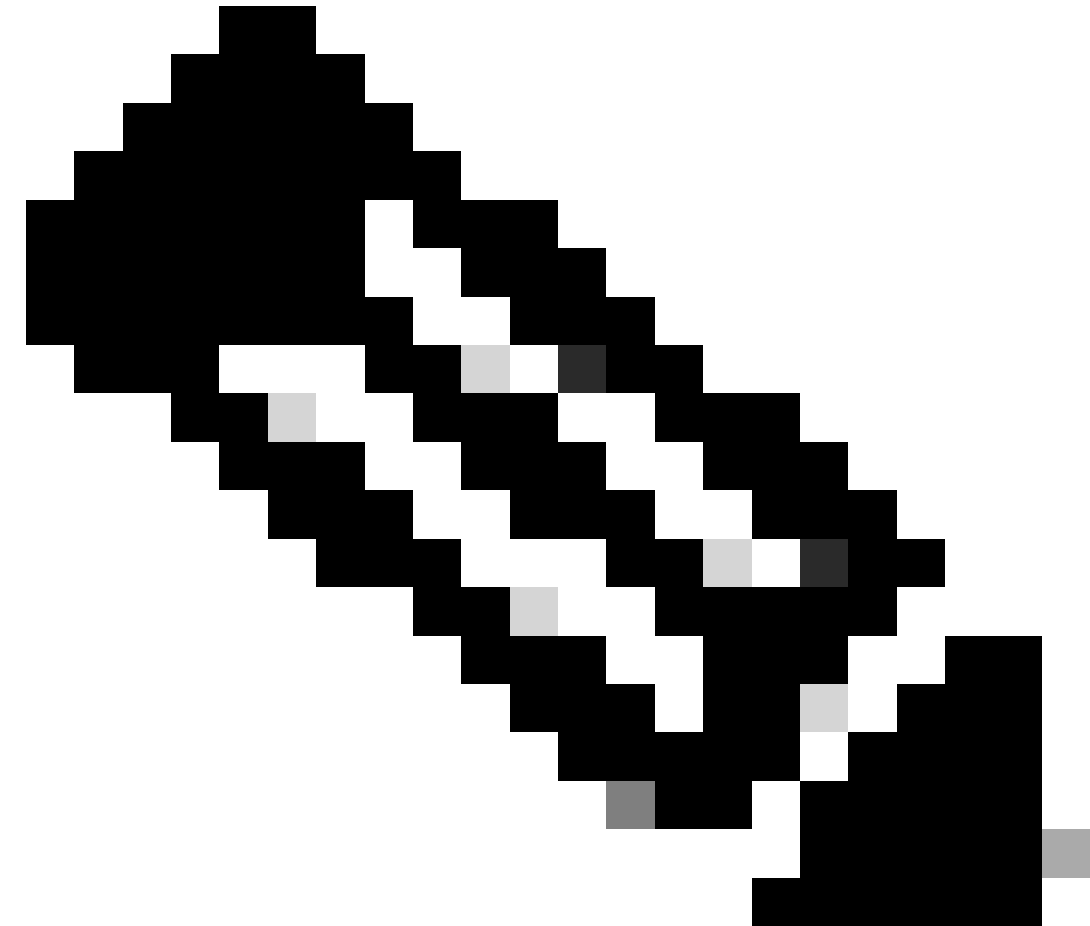
TACACS Policy Set

Step 10. Under new Policy Set click the right arrow > and create an authentication policy. Define a name and choose the device IP address as the condition. Then choose the Identity Source Sequence created in Step 6.

Authentication Policy (2)

Status	Rule Name	Conditions	Use	Hits	Actions
Search					
✓	APIC Authentication Policy	Network Access-Device IP Address EQUALS 188.21	APIC_ISS	55	
				> Options	

Authentication Policy



Note: Location or other attributes can be used as an Authentication condition.

Step 11. Create an Authorization profile for each Admin User type, define a name, and choose an internal user and/or AD user group as the condition. Additional conditions such as APIC can be used. Choose the proper shell profile on each authorization policy and click Save.

Authorization Policy (3)

Status	Rule Name	Conditions	Results	Command Sets	Shell Profiles	Hits	Actions
✓	APIC Admin RO	AND <ul style="list-style-type: none"> Network Access Device IP Address EQUALS 188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RO 			APIC ReadOnly Profile	34	
✓	APIC Admin User	AND <ul style="list-style-type: none"> Network Access Device IP Address EQUALS 188.21 IdentityGroup-Name EQUALS User Identity Groups:APIC_RW OR Iselab-ExternalGroups EQUALS ciscoise.lab/BuiltIn/Administrators 			APIC ReadWrite Profile	15	
✓	Default		DenyAllCommands		Deny All Shell Profile	0	

TACACS Authorization profile

Verify

Step 1. Log in on APIC UI with User Admin credentials. Choose the TACACS option from the list.

APIC

Version 4.2(7u)

CISCO

User ID

Password

Domain

Login

APIC Log in

Step 2. Verify the access on APIC UI and proper policies are applied on TACACS Live logs.

Welcome to APIC

What's new in version 4.2(7u)



New Features

- Floating L3out
 - Docker EE (Kubernetes) container integration
 - L4-L7 Services support in vPod
 - Backup PBR destination
 - Support for 64 Remote Leaf pairs
- UI Enhancements:
 - User-defined UI banner
 - First Time Setup wizard
 - Simplified L3Out creation
 - EPG to leafs deployment view

[View Release Notes](#)

Getting Started

[What's New in v4.2\(7u\)](#)

[Online Videos \(YouTube™\)](#)

[View All Tutorial Videos](#)

Explore

[Configuration Guides](#)

[Knowledge Base Articles](#)

[APIC Communities](#)

Support

[Online Help](#)

[Troubleshooting](#)

[Documentation](#)

☐ Do not show on login

[Review First Time Setup](#)

[Get Started](#)

APIC Welcome message

Repeat Steps 1 and 2 for Read Only Admin users.

☰ Cisco ISE

Operations · TACACS

Live Logs

🔄 Export To ▼

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Devic...
×	▼		Identity	▼	Authentication Policy	Authorization Policy	Ise Node	Network Device N:
Apr 20, 2023 10:14:42.4...	✓	🔒	APIC_ROUser	Authorizat...		APIC >> APIC Admin RO	PAN32	APIC-LAB
Apr 20, 2023 10:14:42.2...	✓	🔒	APIC_ROUser	Authentic...	APIC >> APIC Authentication Po...		PAN32	APIC-LAB

Last Updated: Fri Apr 21 2023 00:14:53 GMT+0200 (Central European Summer Time)

TACACS+ Live Logs

Troubleshoot

Step 1. Navigate to ☰ > Operations > Troubleshoot > Debug Wizard. Choose TACACS and click Debug Nodes.

Debug Profile Configuration

Debug Wizard contains predefined debug templates with the help of which you can troubleshoot issues on ISI

 [Add](#)  [Edit](#)  [Remove](#)  [Debug Nodes](#)

<input type="checkbox"/>	Name	Description	Status
<input type="checkbox"/>	802.1X/MAB	802.1X/MAB	DISABLED
<input type="checkbox"/>	Active Directory	Active Directory	DISABLED
<input type="checkbox"/>	Application Server Issues	Application Server Issues	DISABLED
<input type="checkbox"/>	BYOD portal/Onboarding	BYOD portal/Onboarding	DISABLED
<input type="checkbox"/>	Context Visibility	Context Visibility	DISABLED
<input type="checkbox"/>	Guest portal	Guest portal	DISABLED
<input type="checkbox"/>	Licensing	Licensing	DISABLED
<input type="checkbox"/>	MnT	MnT	DISABLED
<input type="checkbox"/>	Posture	Posture	DISABLED
<input type="checkbox"/>	Profiling	Profiling	DISABLED
<input type="checkbox"/>	Replication	Replication	DISABLED
<input checked="" type="checkbox"/>	TACACS	TACACS	DISABLED

Debug Profile Configuration

Step 2. Choose the node that receives the traffic and click Save.

Operations - Troubleshoot

Diagnostic Tools
Download Logs
Debug Wizard

Debug Profile Configuration
Debug Log Configuration

Debug Profile Configuration > Debug Nodes

Debug Nodes

Selected profile

TACACS

Choose on which ISE nodes you want to enable this profile.

Filter

<input type="checkbox"/> Host Name	Persona	Role
<input checked="" type="checkbox"/> PAN32.ciscoise.lab	Administration, Monitoring, Policy Service	PRI(A), PRI(M)
<input type="checkbox"/> SPAN32.ciscoise.lab	Administration, Monitoring, Policy Service, ...	SEC(A), SEC(M)

Cancel

Save

Debug Nodes Selection

Step 3. Perform a new test and download the logs under Operations > Troubleshoot > Download logs as shown:

AcsLogs, 2023-04-20 22:17:16, 866, DEBUG, 0x7f93cab7700, cntx=0004699242, sesn= PAN32/469596415/70, CPMSession

In case debugs do not show authentication and authorization information, validate this:

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