Configure ISE 2.0 TACACS+ Authentication Command Authorization

Contents

Introduction

This document describes how to configure TACACS+ Authentication and Command Authorization based on Microsoft Active Directory (AD) group membership.

Background Information

To configure TACACS+ Authentication and Command Authorization based on Microsoft Active Directory (AD) group membership of a user with Identity Service Engine (ISE) 2.0 and later, ISE uses AD as an external identity store to store resources such as users, machines, groups, and attributes.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco IOS Router is fully operational
- Connectivity between Router and ISE.
- ISE Server is bootstrapped and has connectivity to Microsoft AD

Components Used

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

- Cisco Identity Service Engine 2.0
- Cisco IOS® Software Release 15.4(3)M3
- Microsoft Windows Server 2012 R2

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.

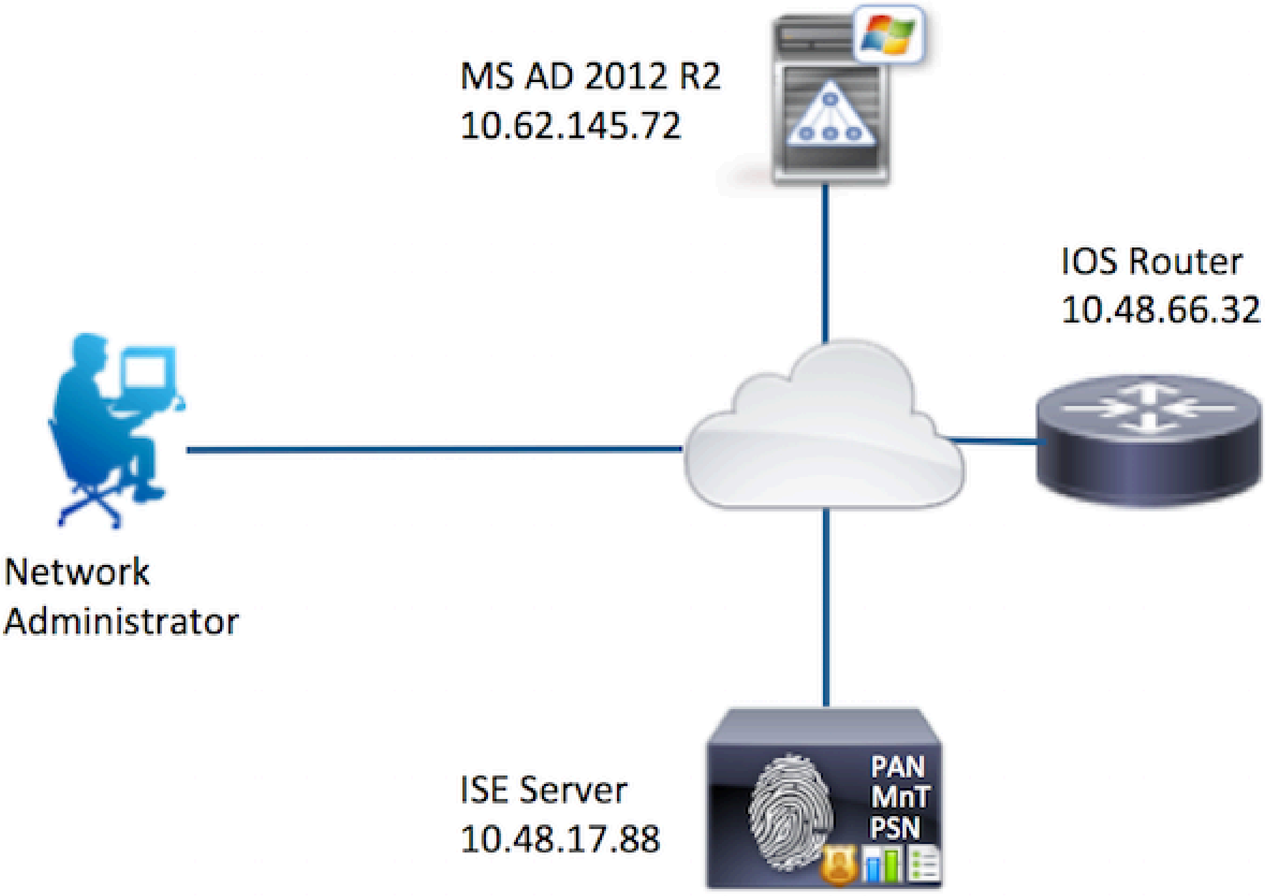
Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure

The aim of the configuration is to:

- Authenticate telnet user via AD
- Authorize telnet user so it is placed into privileged EXEC mode after the login
- Check and send every executed command to ISE for verification

Network Diagram

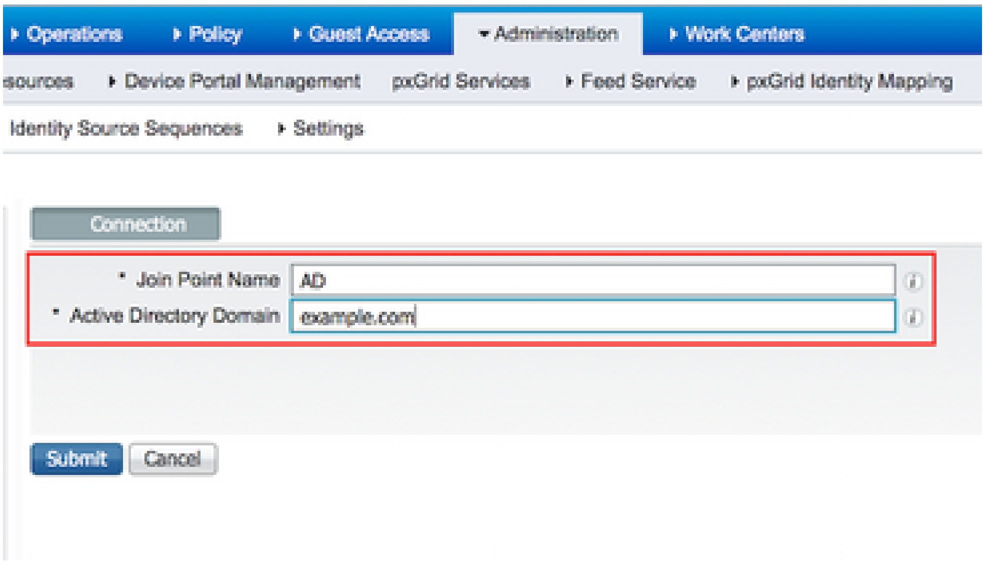


Configurations

Configure ISE for Authentication and Authorization

Join ISE 2.0 to Active Directory

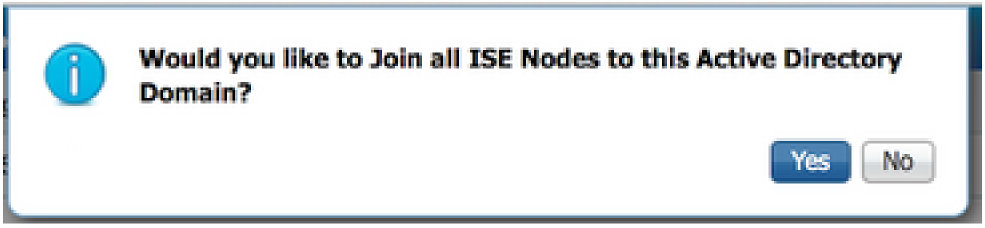
1. Navigate to **Administration > Identity Management > External Identity Stores > Active Directory > Add**. Provide the Join Point Name, Active Directory Domain and click **Submit.**



* Join Point Name: AD

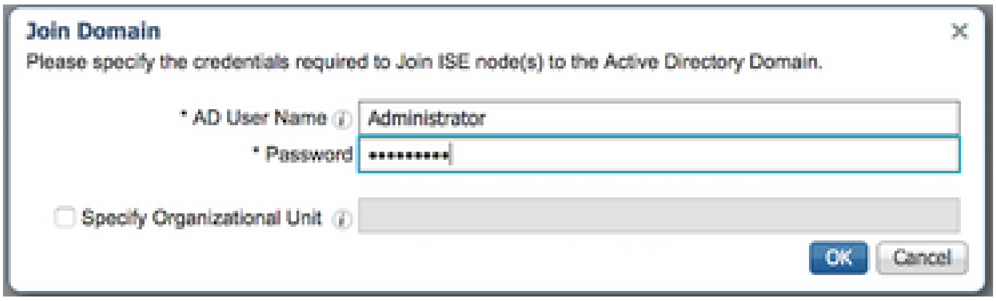
* Active Directory Domain: example.com

2. When prompted to Join all ISE Nodes to this Active Directory Domain, click **Yes.**



Would you like to Join all ISE Nodes to this Active Directory Domain?

3. Provide AD User Name and Password, click **OK**.



Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name: Administrator

* Password: ••••••••••

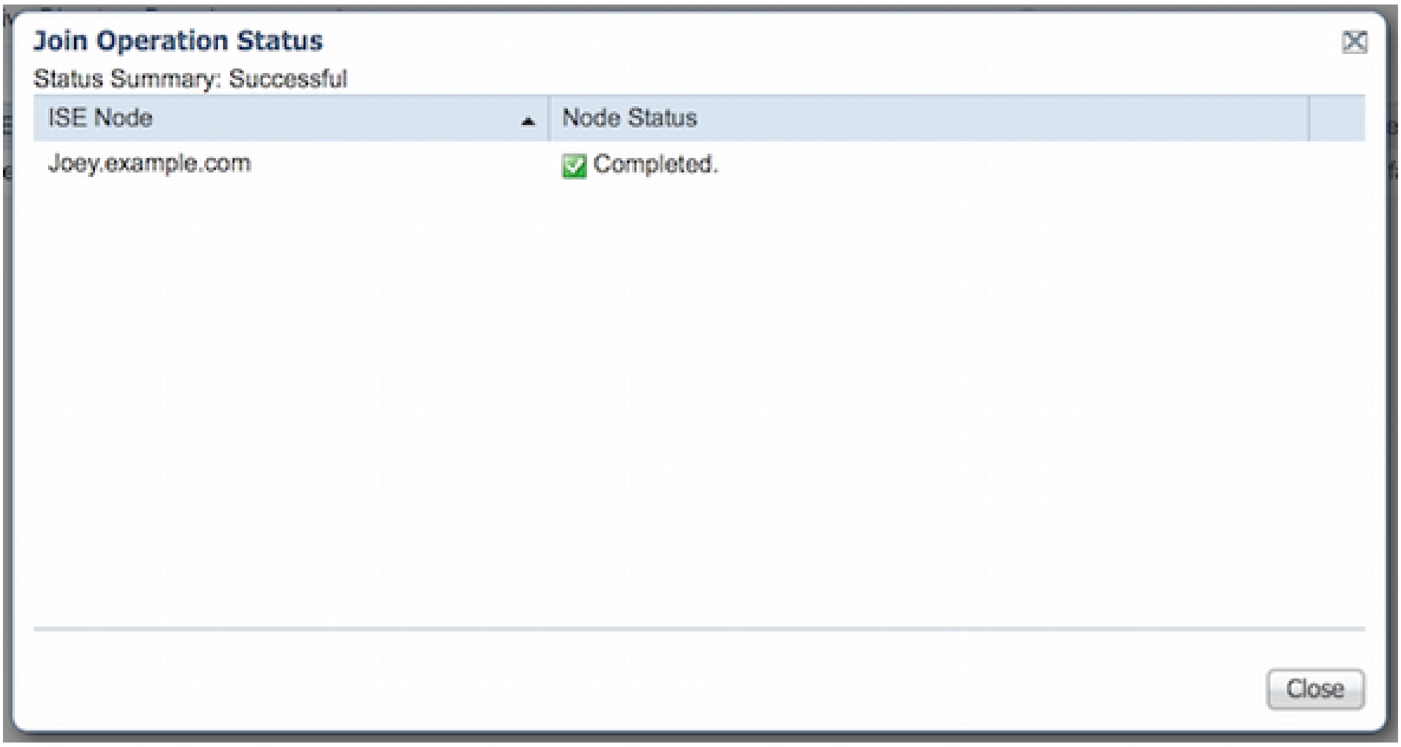
□ Specify Organizational Unit

AD account required for domain access in ISE can have either of these:

- Add workstations to domain user right in respective domain
- Create Computer Objects or Delete Computer Objects permission on respective computers container where ISE machine's account is created before it joins ISE machine to the domain

> **Note**: Cisco recommends to disable the lockout policy for the ISE account and configure the AD infrastructure to send alerts to the admin if a wrong password is used for that account. When the wrong password is entered, ISE does not create or modify its machine account when it is necessary and therefore possibly deny all authentications.

4. Review Operation Status. Node Status must show up as Completed. Click **Close**.

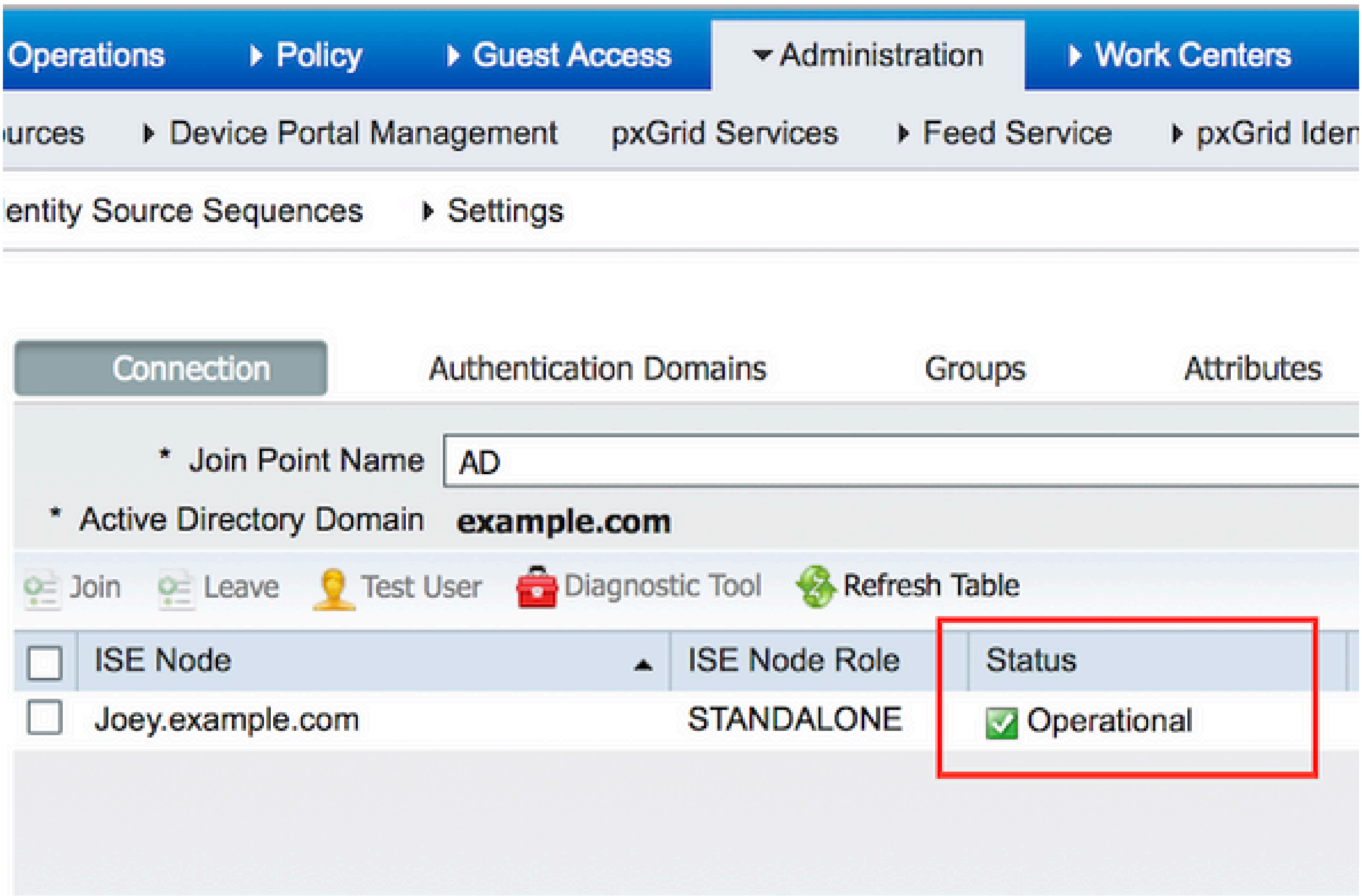


Join Operation Status

Status Summary: Successful

ISE Node	Node Status
Joey.example.com	✓ Completed.

5. Status of AD is Operational.



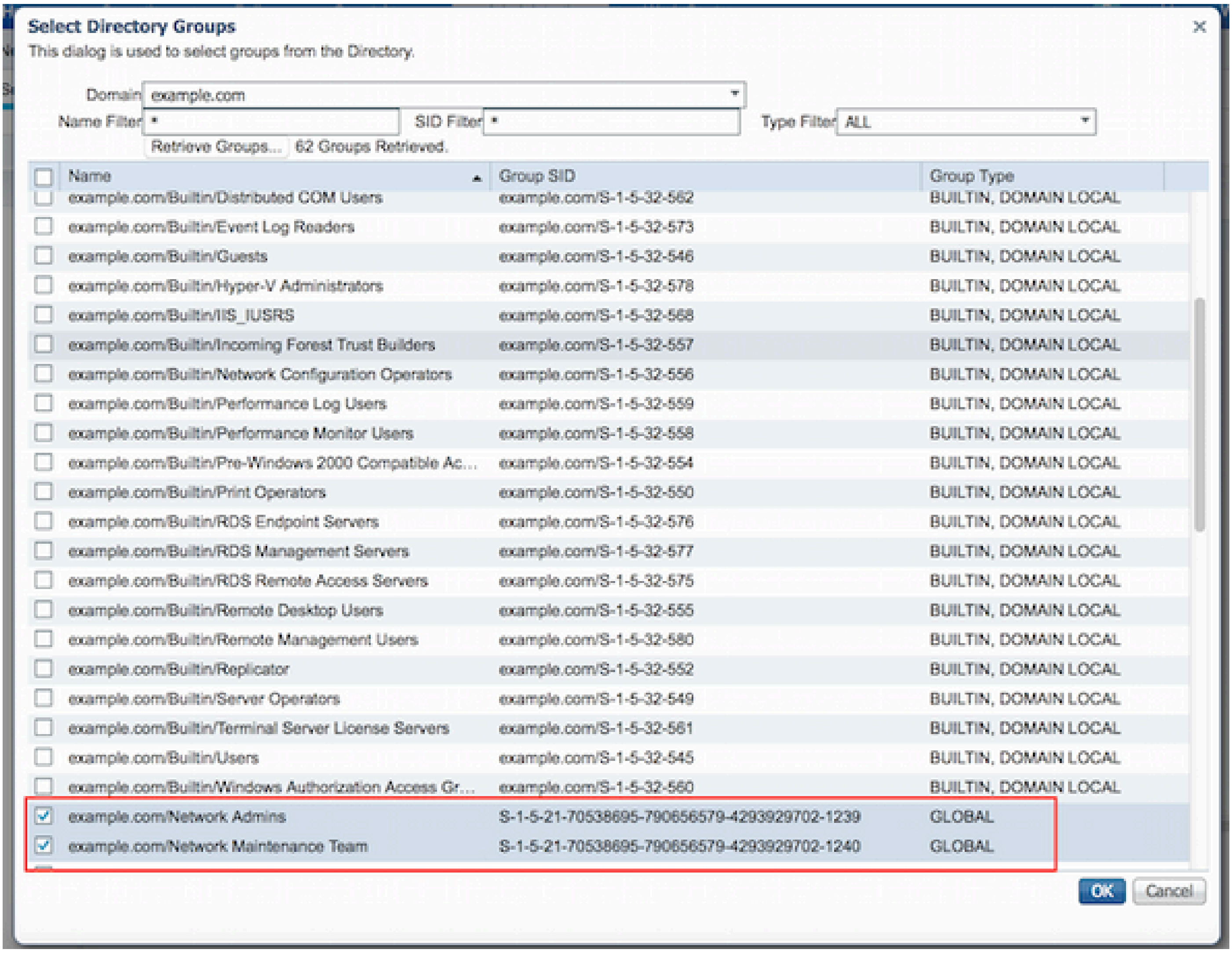
* Join Point Name: AD

* Active Directory Domain: **example.com**

□	ISE Node	ISE Node Role	Status
□	Joey.example.com	STANDALONE	☑ Operational

6. Navigate to **Groups > Add > Select Groups From Directory > Retrieve Groups.** Select **Network Admins** AD Group and **Network Maintenance Team** AD Group checkboxes, as shown in this image.

> **Note**: User admin is member of Network Admins AD Group. This user has full access privileges. This user is a member of Network Maintenance Team AD Group. This user is able to execute only show commands.



Select Directory Groups

This dialog is used to select groups from the Directory.

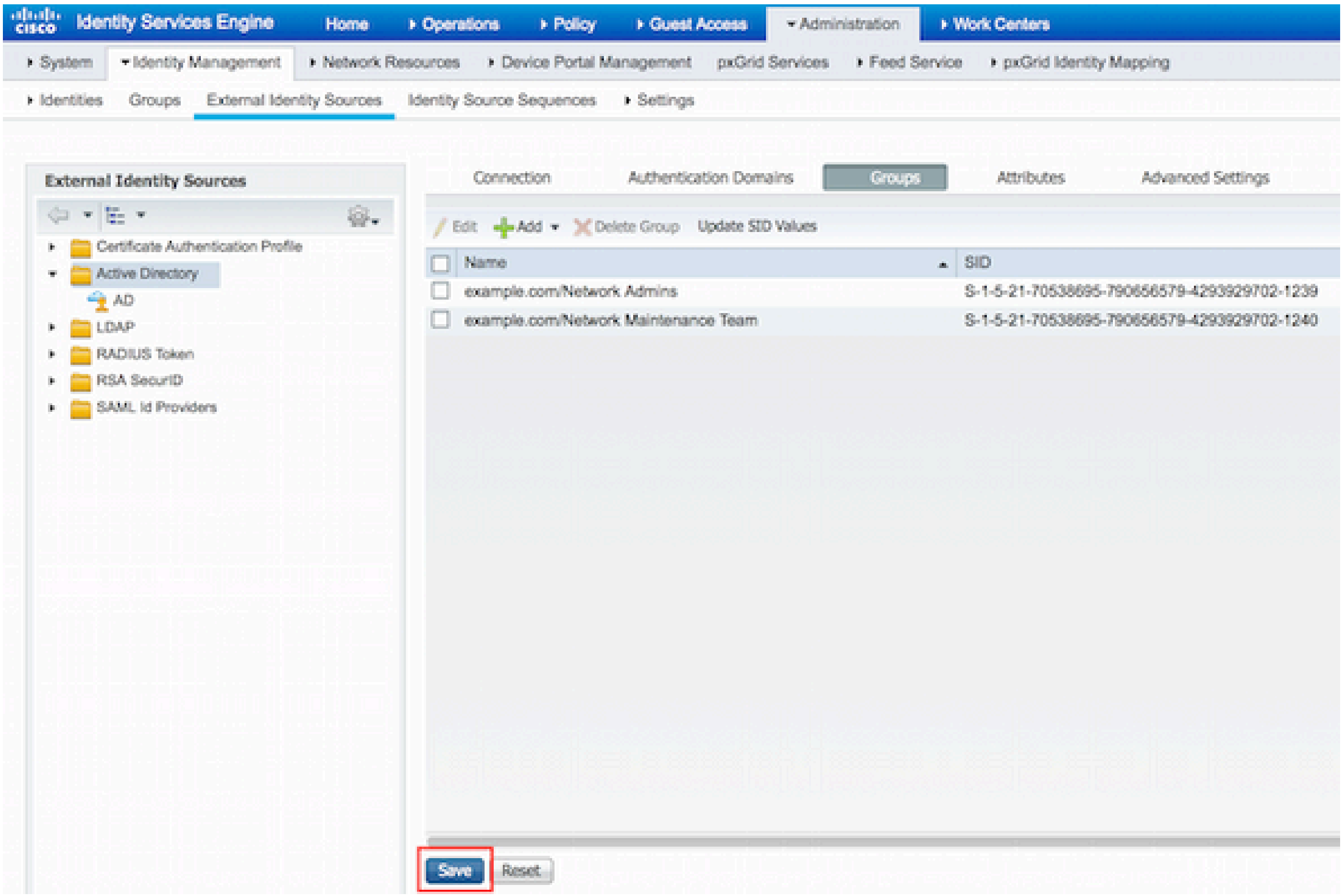
Domain: example.com

Name Filter: *   SID Filter: *   Type Filter: ALL

Retrieve Groups... 62 Groups Retrieved.

□	Name	Group SID	Group Type
□	example.com/Builtin/Distributed COM Users	example.com/S-1-5-32-562	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Event Log Readers	example.com/S-1-5-32-573	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Guests	example.com/S-1-5-32-546	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Hyper-V Administrators	example.com/S-1-5-32-578	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/IIS_IUSRS	example.com/S-1-5-32-568	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Incoming Forest Trust Builders	example.com/S-1-5-32-557	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Network Configuration Operators	example.com/S-1-5-32-556	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Performance Log Users	example.com/S-1-5-32-559	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Performance Monitor Users	example.com/S-1-5-32-558	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Pre-Windows 2000 Compatible Ac...	example.com/S-1-5-32-554	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Print Operators	example.com/S-1-5-32-550	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/RDS Endpoint Servers	example.com/S-1-5-32-576	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/RDS Management Servers	example.com/S-1-5-32-577	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/RDS Remote Access Servers	example.com/S-1-5-32-575	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Remote Desktop Users	example.com/S-1-5-32-555	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Remote Management Users	example.com/S-1-5-32-580	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Replicator	example.com/S-1-5-32-552	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Server Operators	example.com/S-1-5-32-549	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Terminal Server License Servers	example.com/S-1-5-32-561	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Users	example.com/S-1-5-32-545	BUILTIN, DOMAIN LOCAL
□	example.com/Builtin/Windows Authorization Access Gr...	example.com/S-1-5-32-560	BUILTIN, DOMAIN LOCAL
☑	example.com/Network Admins	S-1-5-21-70538695-790656579-4293929702-1239	GLOBAL
☑	example.com/Network Maintenance Team	S-1-5-21-70538695-790656579-4293929702-1240	GLOBAL

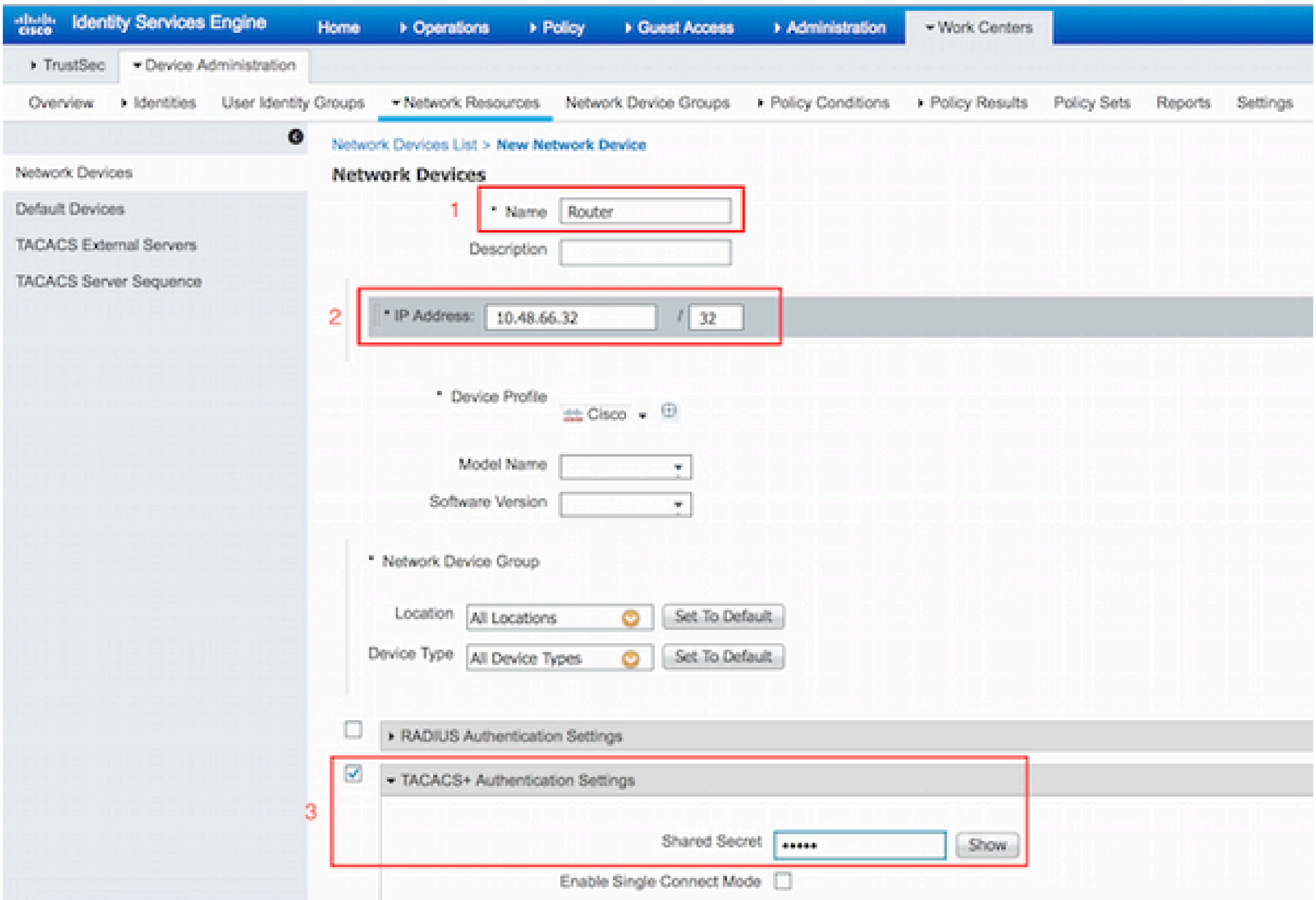
7. Click **Save** to save retrieved AD Groups.



☐	Name	SID
☐	example.com/Network Admins	S-1-5-21-70538695-790656579-4293929702-1239
☐	example.com/Network Maintenance Team	S-1-5-21-70538695-790656579-4293929702-1240

Add Network Device

Navigate to **Work Centers > Device Administration > Network Resources > Network Devices**. Click **Add**. Provide Name, IP Address, select **TACACS+ Authentication Settings** checkbox and provide Shared Secret key.



Network Devices

1 * Name: Router

Description:

2 * IP Address: 10.48.66.32 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations

Device Type: All Device Types

□ RADIUS Authentication Settings

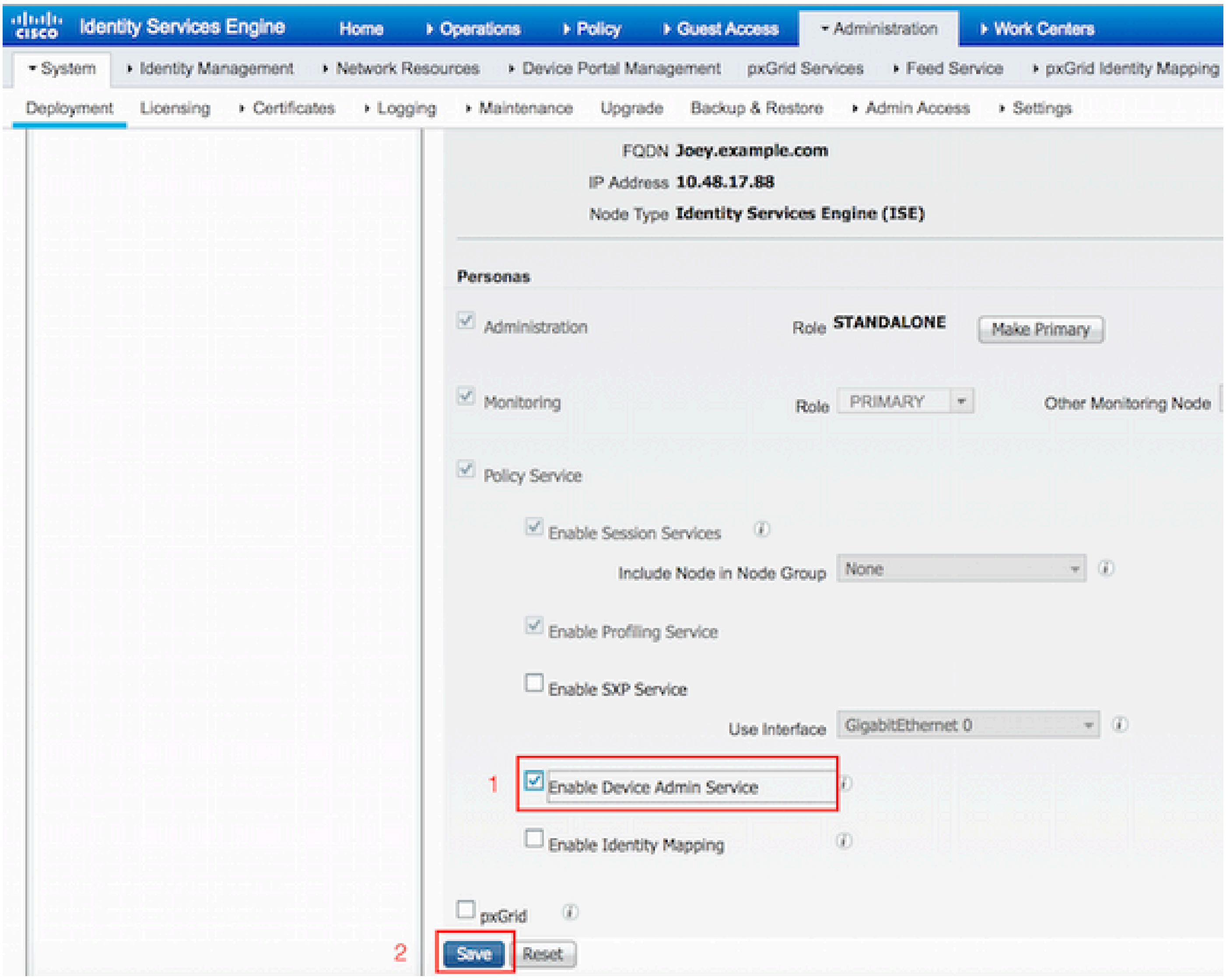
3 ☑ TACACS+ Authentication Settings

Shared Secret: •••••

Enable Single Connect Mode □

Enable Device Admin Service

Navigate to **Administration > System > Deployment.** Choose required Node. Choose **Enable Device Admin Service** checkbox and click **Save.**



FQDN **Joey.example.com**
IP Address **10.48.17.88**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration Role **STANDALONE**

☑ Monitoring Role PRIMARY Other Monitoring Node

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

□ Enable SXP Service

Use Interface GigabitEthernet 0

☑ Enable Device Admin Service

□ Enable Identity Mapping

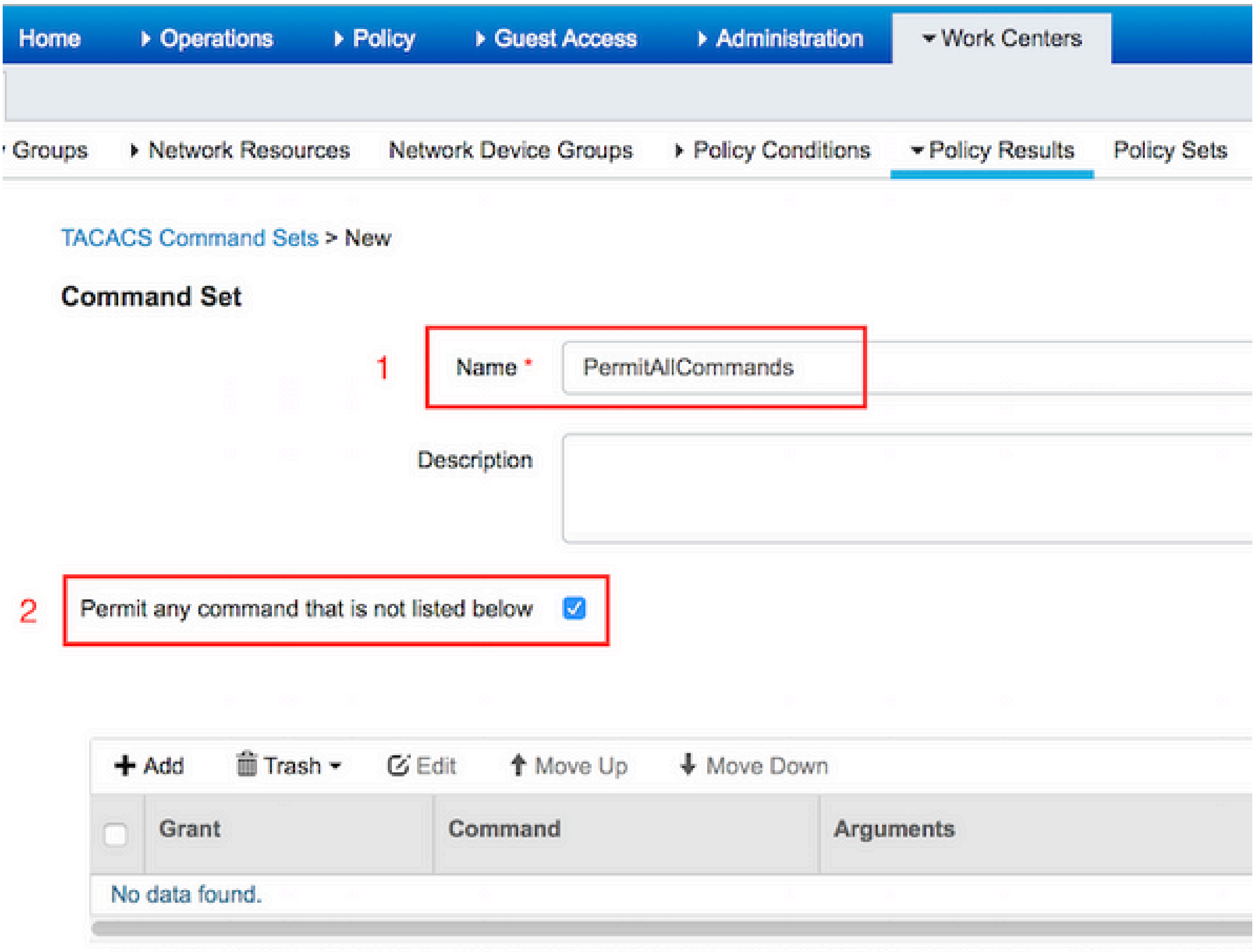
□ pxGrid

Note: For TACACS you need to have separate licenses installed.

Configure TACACS Command Sets

Two command sets are configured. First **PermitAllCommands** for the user admin which allows all commands on the device. Second **PermitShowCommands** for user user which allows only show commands.

1. Navigate to **Work Centers > Device Administration > Policy Results > TACACS Command Sets.** Click **Add.** Provide the Name **PermitAllCommands**, choose **Permit any command** checkbox that is not listed and click **Submit.**



Command Set

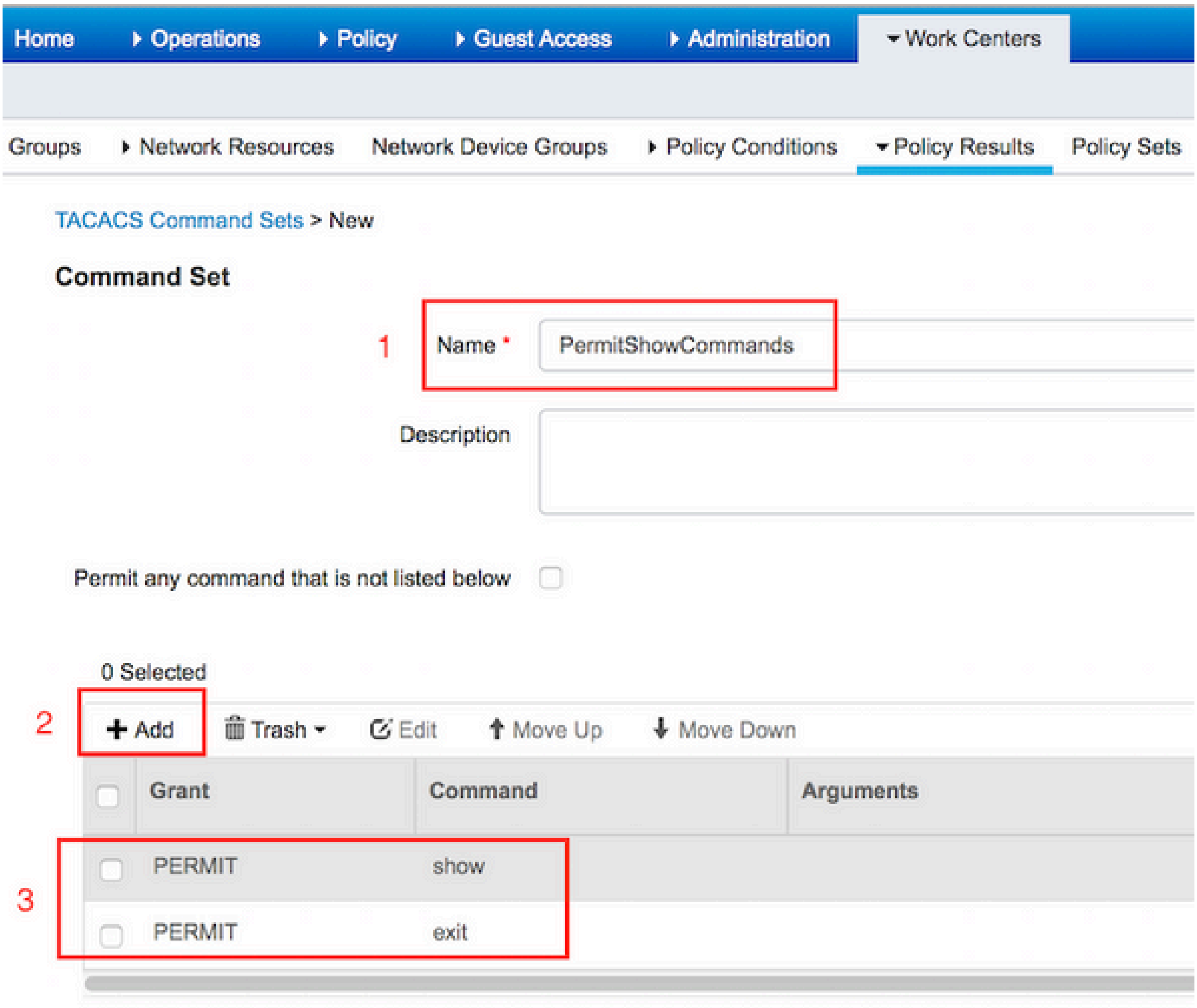
Name * PermitAllCommands

Description

Permit any command that is not listed below ☑

□	Grant	Command	Arguments
No data found.			

2. Navigate to **Work Centers > Device Administration > Policy Results > TACACS Command Sets.** Click **Add.** Provide the Name **PermitShowCommands**, click **Add** and permit **show** and **exit** commands. By default if Arguments is left blank, all arguments are be included. Click **Submit.**



Name * PermitShowCommands

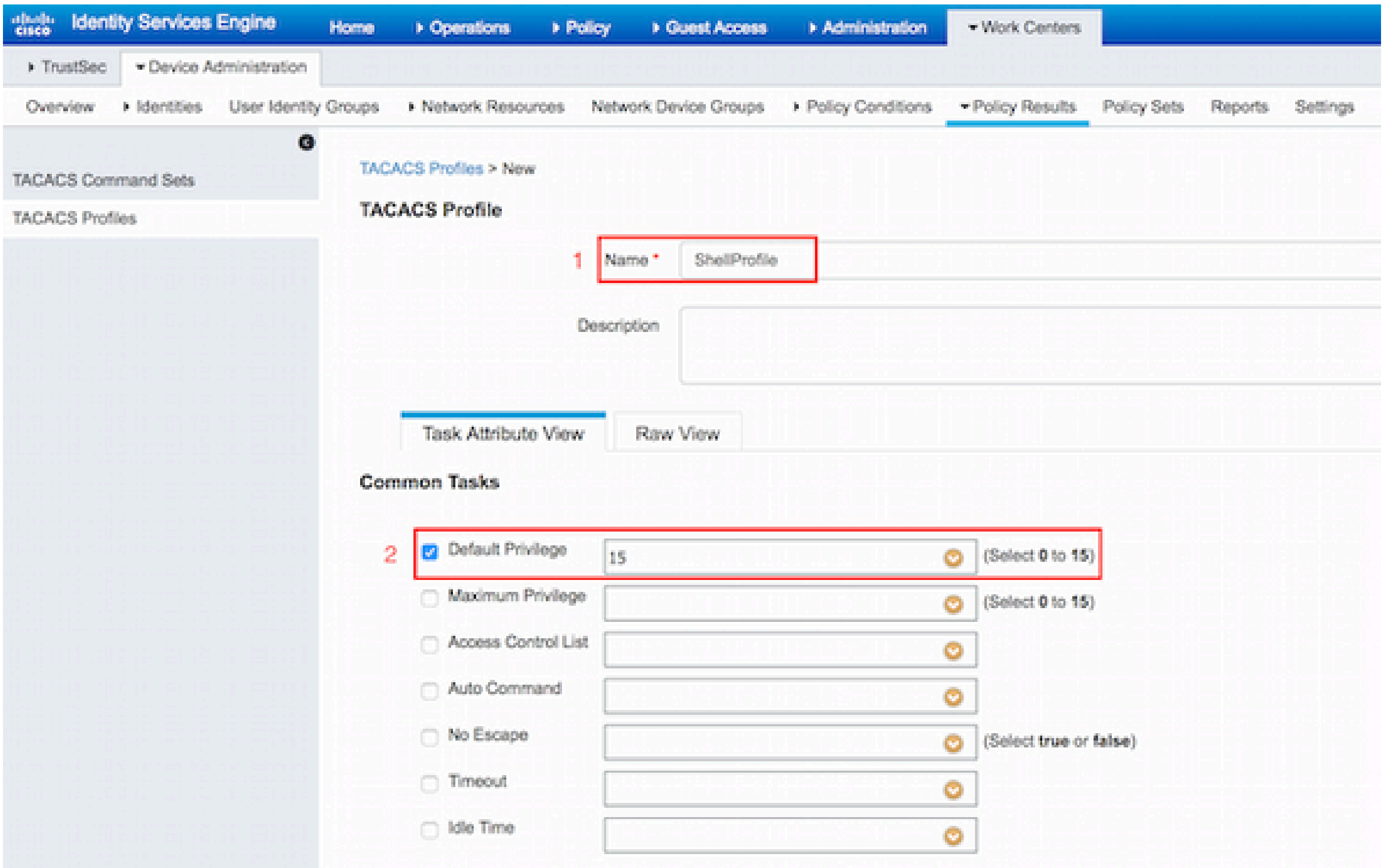
Description

Permit any command that is not listed below □

□	Grant	Command	Arguments
□	PERMIT	show	
□	PERMIT	exit	

Configure TACACS Profile

Single TACACS Profile is configured. TACACS Profile is the same concept as Shell Profile on ACS. Actual command enforcement is done via command sets. Navigate to **Work Centers > Device Administration > Policy Results > TACACS Profiles.** Click **Add.** Provide Name ShellProfile, select **Default Privilege** checkbox and enter the value of 15. Click **Submit.**



TACACS Profile

1 Name * ShellProfile

Description

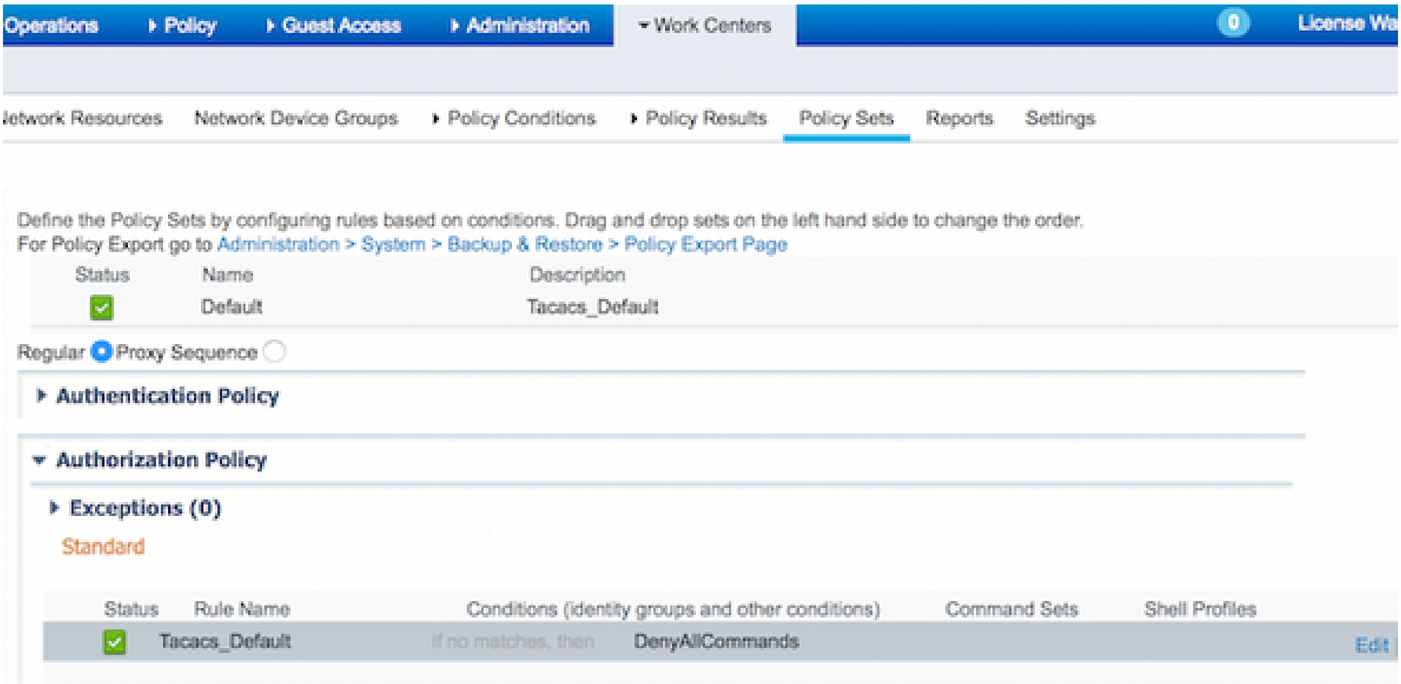
Common Tasks

2 ☑ Default Privilege	15	(Select **0** to **15**)
☐ Maximum Privilege		(Select **0** to **15**)
☐ Access Control List		
☐ Auto Command		
☐ No Escape		(Select **true** or **false**)
☐ Timeout		
☐ Idle Time		

Configure TACACS Authorization Policy

Authentication Policy by default points to All_User_ID_Stores, which includes AD, so it is left unchanged.

Navigate to **Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Edit > Insert New Rule Above.**



Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
✓	Default	Tacacs_Default

Regular ● Proxy Sequence ○

▸ Authentication Policy

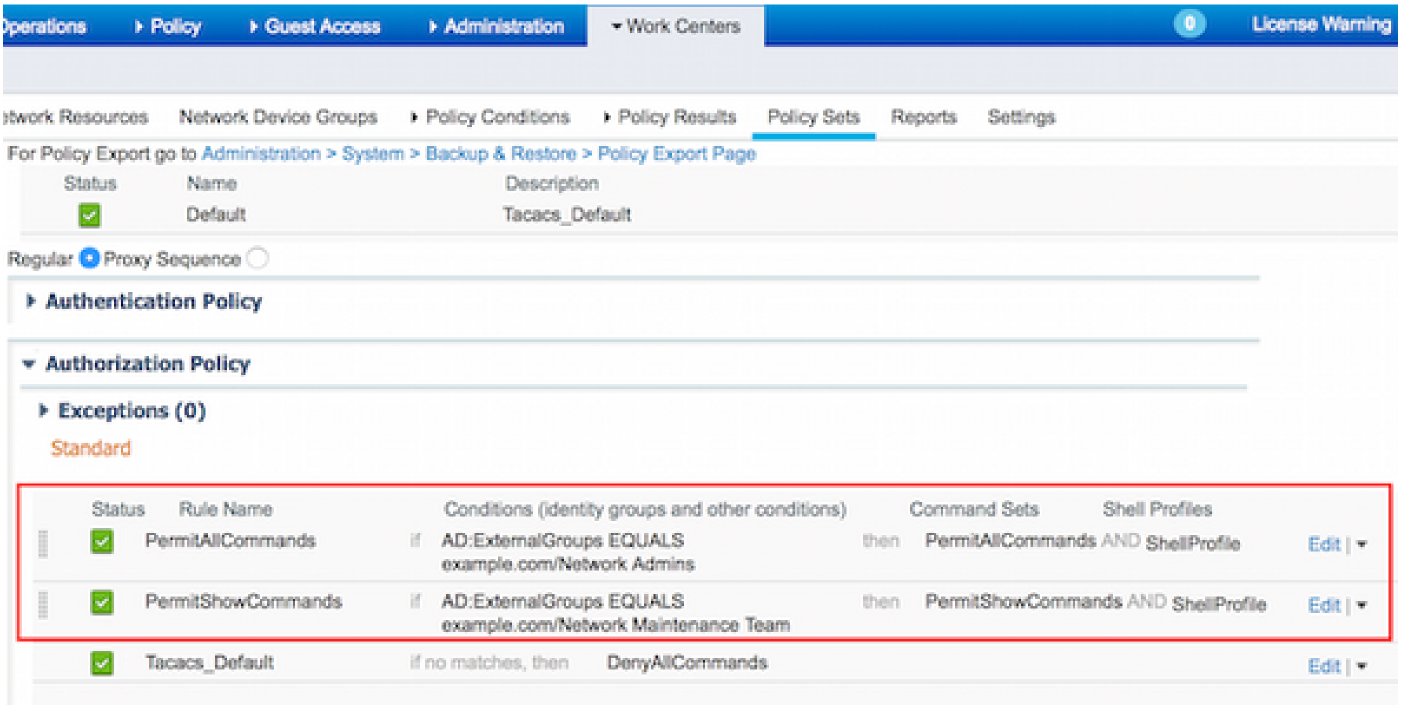
▾ Authorization Policy

▸ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
✓	Tacacs_Default	if no matches, then	DenyAllCommands	

Two authorization rules are configured; first rule assigns TACACS profile ShellProfile and command Set PermitAllCommands based on Network Admins AD Group membership. Second rule assigns TACACS profile ShellProfile and command Set PermitShowCommands based on Network Maintenance Team AD Group membership.



For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
✓	Default	Tacacs_Default

Regular ● Proxy Sequence ○

▸ Authentication Policy

▾ Authorization Policy

▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Command Sets		Shell Profiles	
✓	PermitAllCommands	if	AD:ExternalGroups EQUALS example.com/Network Admins	then	PermitAllCommands	AND	ShellProfile	Edit | ▾
✓	PermitShowCommands	if	AD:ExternalGroups EQUALS example.com/Network Maintenance Team	then	PermitShowCommands	AND	ShellProfile	Edit | ▾
✓	Tacacs_Default	if no matches, then	DenyAllCommands					Edit | ▾

Configure the Cisco IOS Router for Authentication and Authorization

Complete these steps in order to configure Cisco IOS Router for Authentication and Authorization.

1. Create a local user with full privilege for fallback with the **username** command as shown here.

```
username cisco privilege 15 password cisco
```

2. Enable aaa new-model. Define TACACS server ISE, and place it in the group ISE_GROUP.

```
aaa new-model

tacacs server ISE
 address ipv4 10.48.17.88
 key cisco
aaa group server tacacs+ ISE_GROUP
 server name ISE
```

> **Note**: Server key matches the one defined on ISE Server earlier.

3. Test the TACACS server reachability with the test **aaa** command as shown.

```
Router#test aaa group tacacs+ admin Krakow123 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

The output of the previous command shows that the TACACS server is reachable and the user has been successfully authenticated.

4. Configure login and enable authentications and then use the exec and command authorizations as shown.

```
aaa authentication login AAA group ISE_GROUP local
aaa authentication enable default group ISE_GROUP enable
aaa authorization exec AAA group ISE_GROUP local
aaa authorization commands 0 AAA group ISE_GROUP local
aaa authorization commands 1 AAA group ISE_GROUP local
aaa authorization commands 15 AAA group ISE_GROUP local
aaa authorization config-commands
```

Note: Method list created is named AAA, which is used later, when it is assigned to line vty.

5. Assign method lists to line vty 0 4.

```
line vty 0 4
 authorization commands 0 AAA
 authorization commands 1 AAA
 authorization commands 15 AAA
 authorization exec AAA
 login authentication AAA
```

Verify

Cisco IOS Router Verification

1. Telnet to the Cisco IOS Router as admin who belongs to the full-access group in AD. Network Admins group is the group in AD which is mapped to ShellProfile and PermitAllCommands Command set on the ISE. Try to run any command to ensure full access.

```
Username:admin
Password:

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes
Router(config-isakmp)#exit
Router(config)#exit
Router#
```

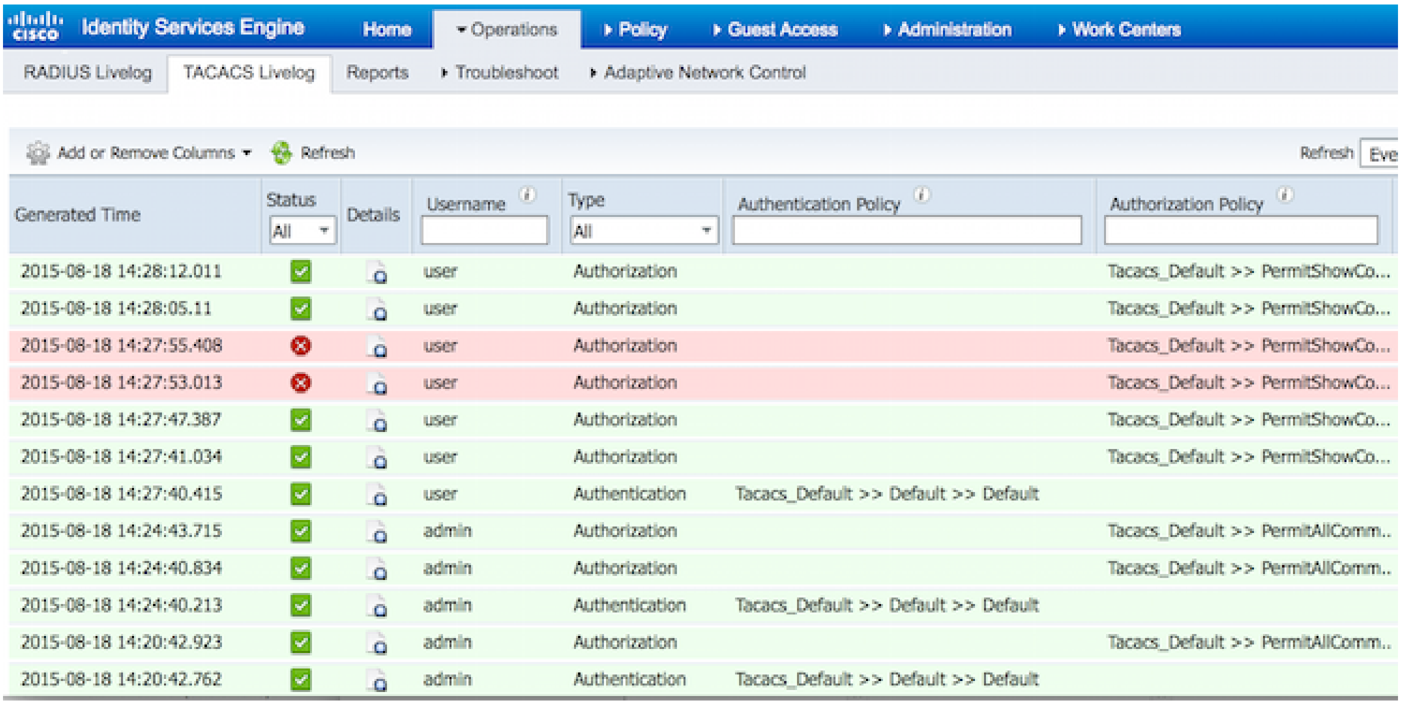
2. Telnet to the Cisco IOS Router as user who belongs to the limited access group in AD. Network Maintenance Team group is the group in AD which is mapped to **ShellProfile** and **PermitShowCommands** Command set on the ISE. Try to run any command to ensure that only show commands can be issued.

```
Username:user
Password:

Router#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.48.66.32     YES NVRAM  up                    up

Router#ping 8.8.8.8
Command authorization failed.

Router#configure terminal
Command authorization failed.
```

```
Router#show running-config | include hostname
hostname Router
Router#
```

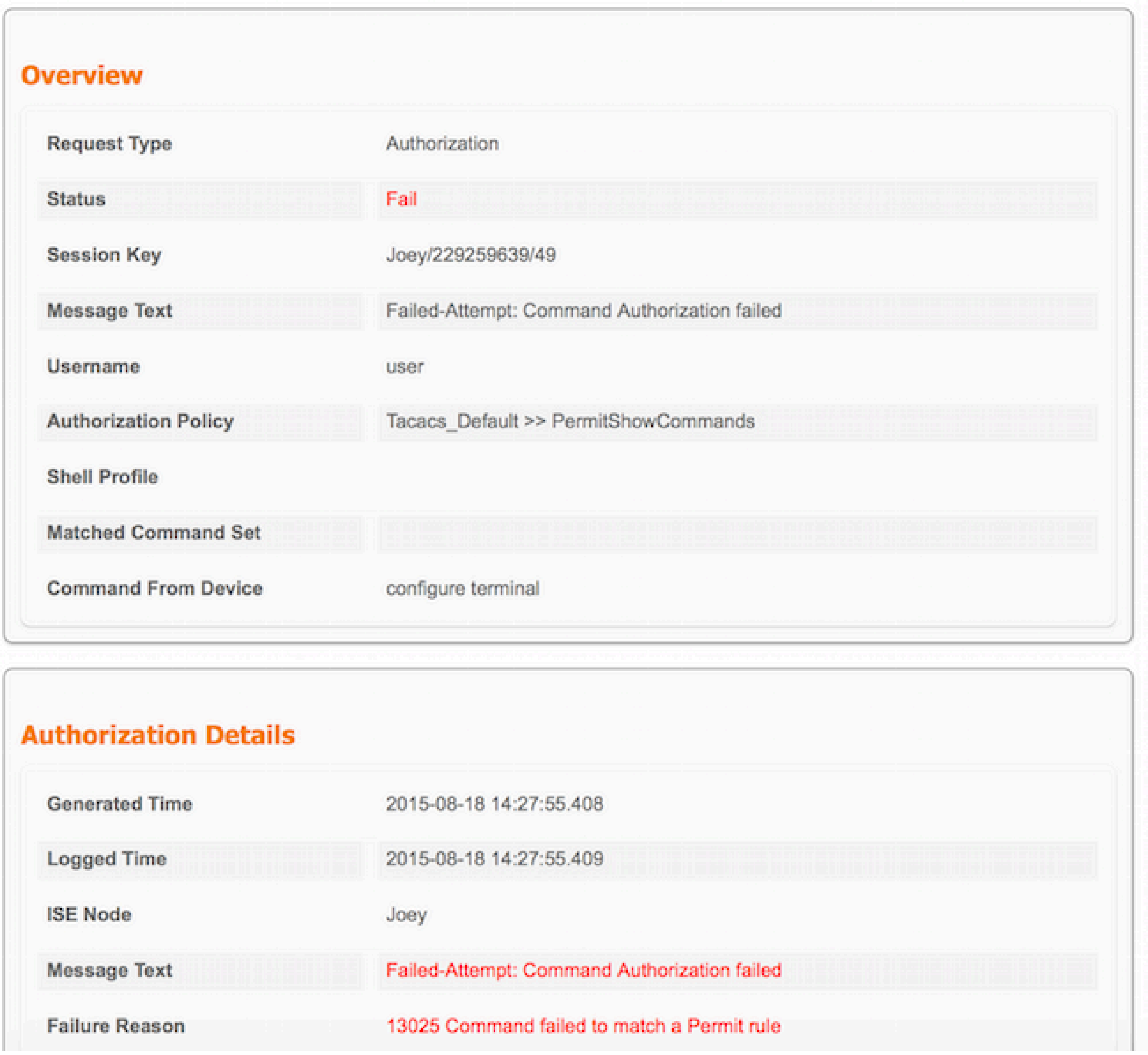
ISE 2.0 Verification

1. Navigate to **Operations > TACACS Livelog.** Ensure that the attempts done are seen.



Generated Time	Status All	Details	Username	Type All	Authentication Policy	Authorization Policy
2015-08-18 14:28:12.011	✓	🔍	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:28:05.11	✓	🔍	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:55.408	✗	🔍	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:53.013	✗	🔍	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:47.387	✓	🔍	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:41.034	✓	🔍	user	Authorization		Tacacs_Default >> PermitShowCo...
2015-08-18 14:27:40.415	✓	🔍	user	Authentication	Tacacs_Default >> Default >> Default	
2015-08-18 14:24:43.715	✓	🔍	admin	Authorization		Tacacs_Default >> PermitAllComm..
2015-08-18 14:24:40.834	✓	🔍	admin	Authorization		Tacacs_Default >> PermitAllComm..
2015-08-18 14:24:40.213	✓	🔍	admin	Authentication	Tacacs_Default >> Default >> Default	
2015-08-18 14:20:42.923	✓	🔍	admin	Authorization		Tacacs_Default >> PermitAllComm..
2015-08-18 14:20:42.762	✓	🔍	admin	Authentication	Tacacs_Default >> Default >> Default	

2. Click the details of one of the red reports. Failed command executed earlier can be seen.



Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229259639/49
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> PermitShowCommands
Shell Profile	
Matched Command Set	
Command From Device	configure terminal

Authorization Details

Generated Time	2015-08-18 14:27:55.408
Logged Time	2015-08-18 14:27:55.409
ISE Node	Joey
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

Troubleshoot

Error: 13025 Command failed to match a Permit rule

Check the SelectedCommandSet attributes to verify that the expected Command Sets were selected by the Authorization policy.

Related Information

Technical Support & Documentation - Cisco Systems

ISE 2.0 Release Notes

ISE 2.0 Hardware Installation Guide

ISE 2.0 Upgrade Guide

ACS to ISE Migration Tool Guide

ISE 2.0 Active Directory Integration Guide

ISE 2.0 Engine Administrator Guide