

ISE TACACS+ Configuration Guide for Cisco IOS Based Network Devices

Secure Access How-to User Series

**Author: Technical Marketing, Policy and Access, Security Business
Group, Cisco Systems**

Date: January 2016

Table of Contents

Table of Contents	2
About This Guide	3
Overview	3
Using This Guide	3
Components Used	3
ISE Configuration for Device Administration	4
Licensing Device Administration on ISE	4
Enabling Device Administration on ISE	4
Device Administration Work Center	5
Network Device and Network Device Groups	5
Identity Stores	7
TACACS Profiles	8
IOS HelpDesk Privilege	8
IOS Admin Privilege	8
TACACS Command Sets	9
HelpDesk Commands	9
IOS Security Commands	9
Permit All Commands	10
Device Admin Policy Sets	10
IOS Configuration for TACACS+	13
TACACS+ Authentication and Fallback	13
TACACS+ Command Authorization	14
TACACS+ Command Accounting	15
What's Next?	16

About This Guide

Overview

Terminal Access Controller Access Control System Plus (TACACS+) is a client-server protocol that provides centralized security control for management access to routers and many other types of network access devices. TACACS+ provides these AAA services:

- Authentication – Who the users are
- Authorization – What they are allowed to do
- Accounting – Who did what and when

This document provides configuration examples for TACACS+ with the Cisco Identity Services Engine (ISE) as the TACACS+ server and a Cisco IOS network device as the TACACS+ client.

Using This Guide

This guide divides the activities into two parts to enable ISE to manage administrative access for Cisco IOS based network devices.

- Part 1 – Configure ISE for Device Admin
- Part 2 – Configure Cisco IOS for TACACS+

Components Used

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

- ISE VMware virtual appliance, Release 2.0
- Cisco Cloud Services Router 1000V (CSRv), Cisco IOS XE Version 03.16.00.S

It works on most of Cisco IOS devices, except for Cisco IOS-XR, such as ASR9000, which uses user task groups instead of privilege levels.

The materials in this document are created from the devices in a lab environment. All of the devices are started with a cleared (default) configuration.

ISE Configuration for Device Administration

Licensing Device Administration on ISE

Device Administration(TACACS+) is licensed per deployment, but requires existing and valid ISE base or mobility licenses.

Enabling Device Administration on ISE

The Device Administration service (TACACS+) is not enabled by default in an ISE node. The first step is to enable it.

- Step 1 Log in to the ISE admin web portal using one of the supported browsers.
- Step 2 Navigate to **Administration > System > Deployment**. Select the check box next to the ISE node and click **Edit**.

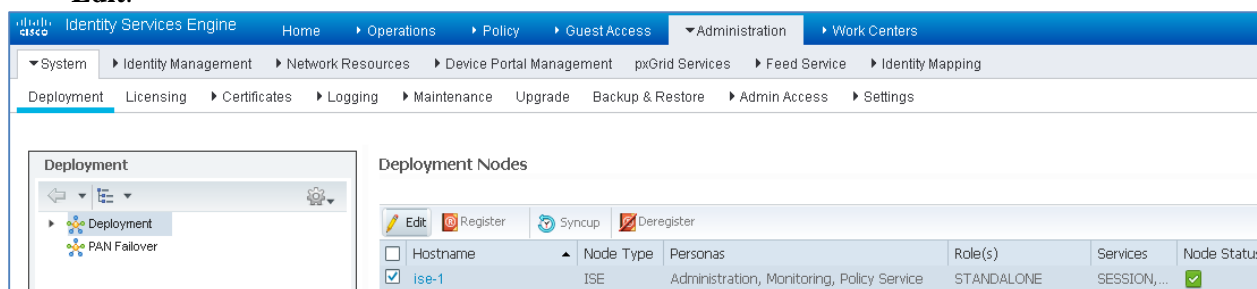


Figure 1. ISE Deployment Page

- Step 3 Under **General Settings**, scroll down and select the check box next to **Enable Device Admin Service**.

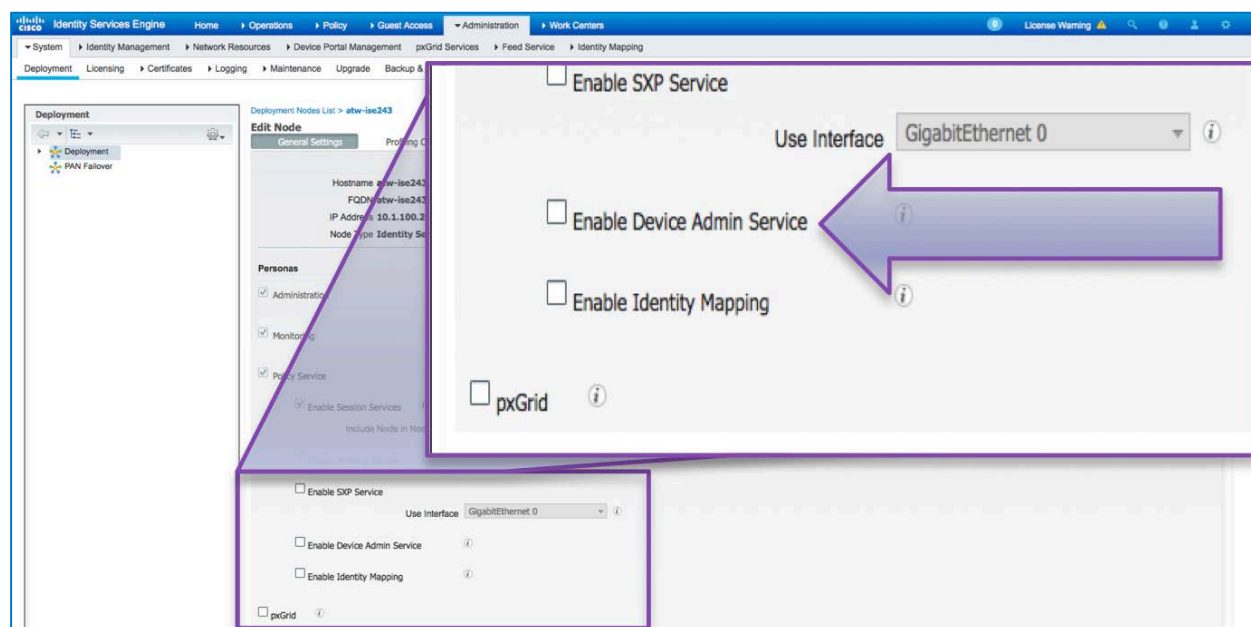


Figure 2. ISE Deployment General Settings

Step 4 Save the configuration. Device Admin Service is now enabled on ISE.

Device Administration Work Center

ISE 2.0 introduces Work Centers, each of which encompasses all the elements for a particular feature.

Step 1 Go to **Work Centers > Device Administration > Overview**

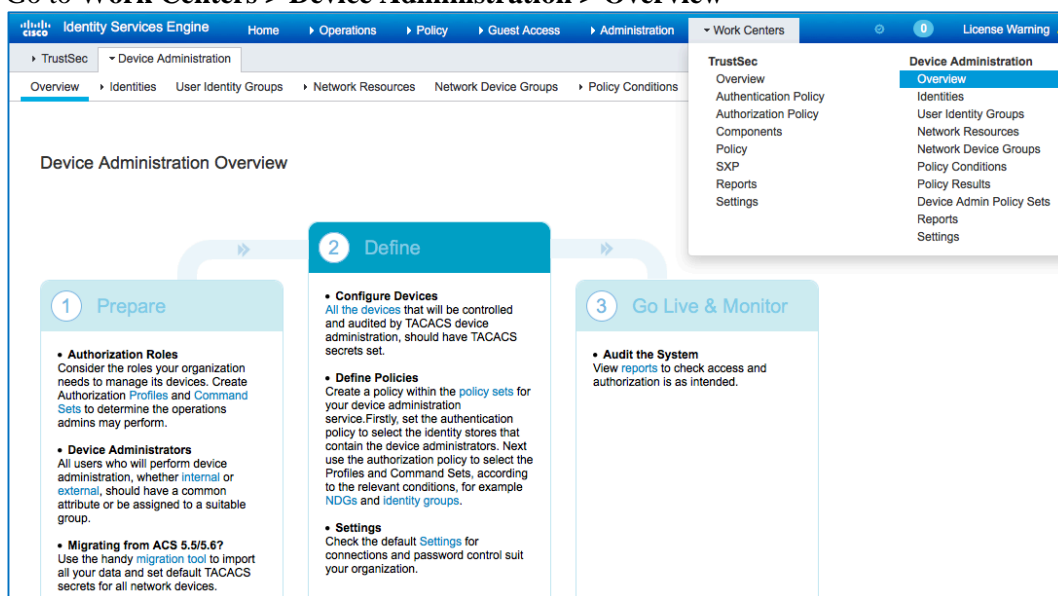


Figure 3. Device Admin Overview

The Device Administration Overview provides the high-level steps needed for the Device Admin Use Case.

Network Device and Network Device Groups

ISE provides powerful device grouping with multiple device group hierarchies. Each hierarchy represents a distinct and independent classification of network devices.

Step 1 Navigate to **Work Centers > Device Administration > Network Device Groups**

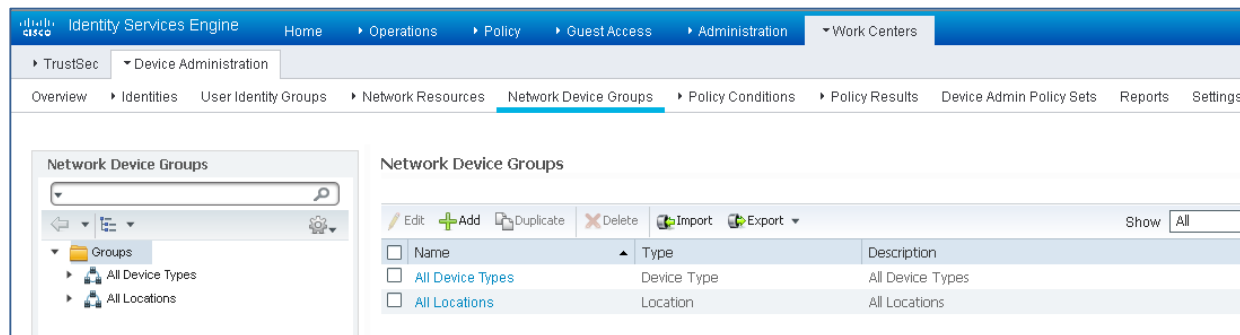


Figure 4. Network Device Groups

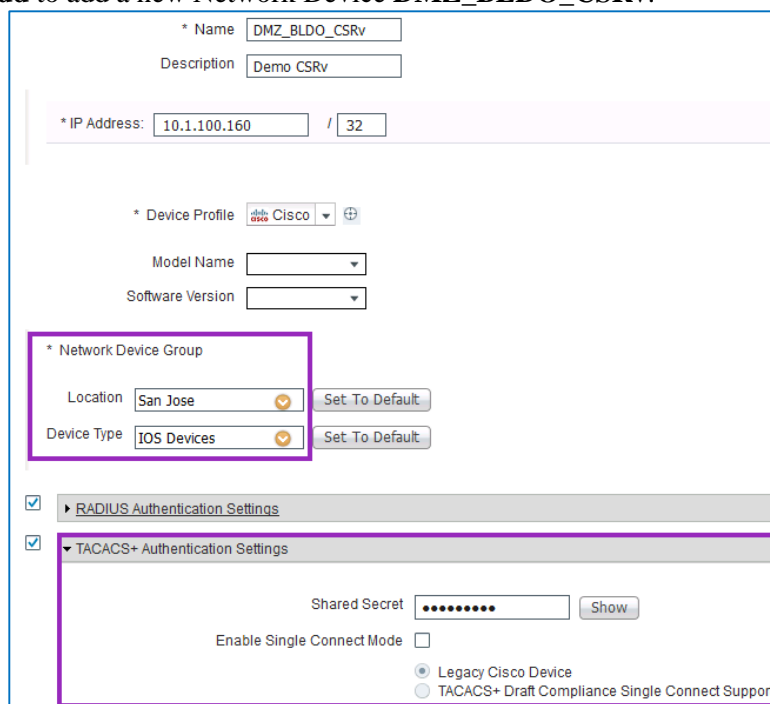
All Device Types and All Locations are default hierarchies provided by ISE. You may add your own hierarchies and define the various components in identifying a Network Device which can be used later in the Policy Conditions.

Step 2 After defining hierarchies, the Network Device Groups will look similar to the following:



Figure 5. Network Device Group Tree View

Step 3 Now, add a CSRv as a Network Device. Go to **Work Centers > Device Administration > Network Resources**. Click **Add** to add a new Network Device **DMZ_BLDO_CSRv**.



The form shows the configuration for a new Network Device. The fields are as follows:

- Name:** DMZ_BLDO_CSRv
- Description:** Demo CSRv
- IP Address:** 10.1.100.160 / 32
- Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:**
 - Location:** San Jose
 - Device Type:** IOS Devices
- Authentication Settings:**
 - RADIUS Authentication Settings:** (checked)
 - TACACS+ Authentication Settings:** (checked)
 - Shared Secret:** (masked with dots)
 - Enable Single Connect Mode:** (unchecked)
 - Legacy Cisco Device:** (selected)
 - TACACS+ Draft Compliance Single Connect Support:** (unchecked)

Figure 6. Adding Network Device

Enter the IP address of the Device and make sure to map the Location and Device Type for the Device. Finally, Enable the **TACACS+ Authentication Settings** and specify the Shared Secret.

Identity Stores

This section defines an Identity Store for the Device Administrators, which can be the ISE Internal Users and any supported External Identity Sources. Here uses Active Directory (AD), an External Identity Source.

- Step 1** Go to **Administration > Identity Management > External Identity Stores > Active Directory**. Click **Add** to define a new AD Joint Point. Specify the Join Point name and the AD domain name and click **Submit**.

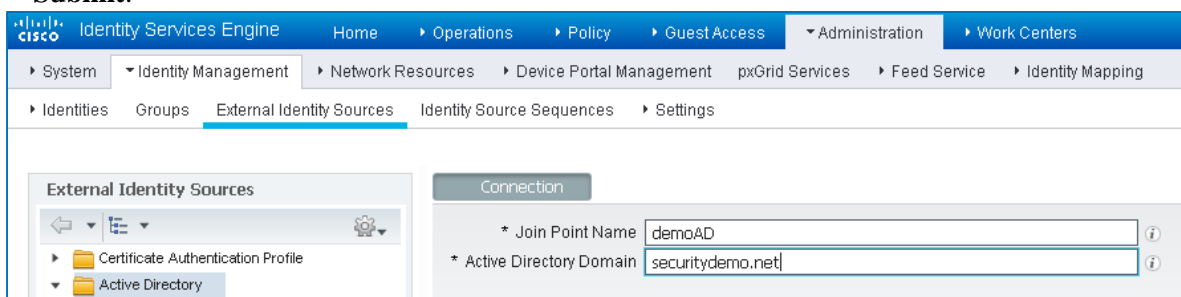


Figure 3. Adding AD Join Point

- Step 2** Click **Yes** when prompted “Would you like to Join all ISE Nodes to this Active Directory Domain?” Input the credentials with AD join privileges, and **Join** ISE to AD. Check the Status to verify it operational.

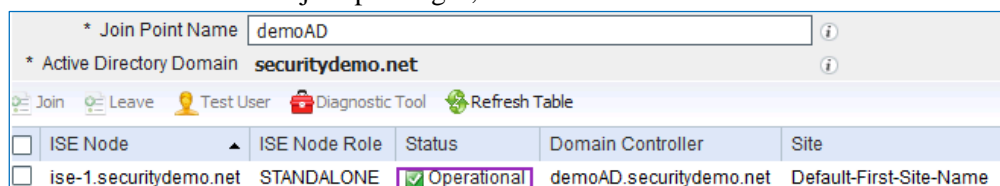


Figure 4. Joining ISE to AD

- Step 3** Go to the **Groups** tab, and click **Add** to get all the groups needed based on which the users are authorized for the device access. The following example shows the groups used in the Authorization Policy in this guide

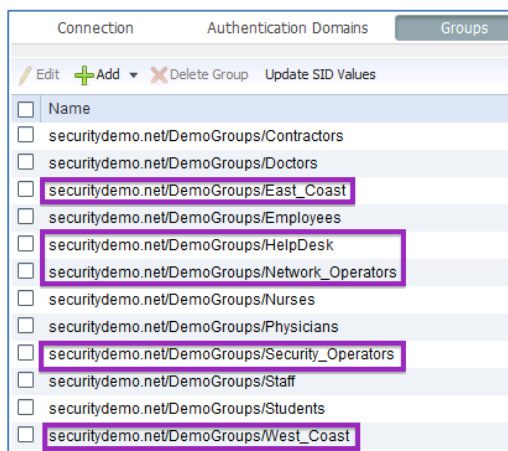


Figure 5. AD Groups

TACACS Profiles

Cisco IOS provides 16 levels of access privileges. Three are defined by default:

Privilege level 0 – permits *disable*, *enable*, *exit*, *help*, and *logout* commands. Since the minimal accessible level after login is 1, all the commands in this level-0 are available to all users.

Privilege level 1 – non-privileged or user EXEC mode is the default level for a logged-in user. The shell prompt is the device name followed by an angle bracket, for example “Router>”.

Privilege level 15 – privileged EXEC mode is the level after the enable command. The shell prompt is the device hostname followed by the pound sign, e.g. “Router#”.

With EXEC authorization, an IOS device sends a TACACS+ authorization request to the AAA server right after authentication to check whether the user is allowed to start a shell (EXEC) session. Here we configure ISE to push two attributes to customize it per-user:

Default Privilege: Specifies the initial (default) privilege level for the shell session. Authorized users land in this level instead of 1. If this level provides enough access, the users need not use the enable command.

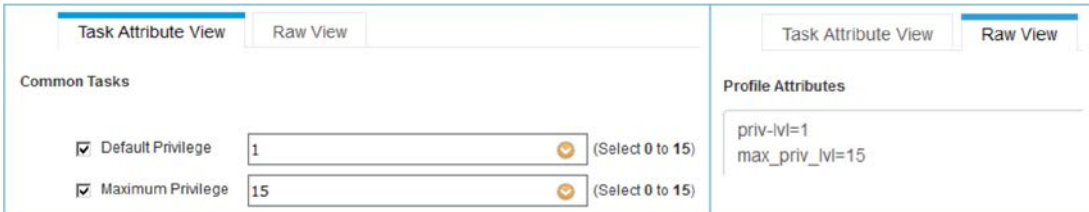
Maximum Privilege: Specifies the maximum level permitted for the shell session. Authorized users can log in with a lower default level and use the enable command to move to a higher level, up-to the value assigned by this attribute.

We will define two TACACS Profiles – `IOS_HelpDesk_Privilege` and `IOS_Admin_Privilege`

IOS HelpDesk Privilege

For helpdesk troubleshooting, the commands at Level-1 are usually sufficient, so we assign that as the default privilege to the helpdesk analysts. Occasionally they need more privileges, so we allow 15 as their maximum privilege level.

- Step 1** On the ISE GUI, go to **Work Centers > Device Administration > Policy Results > TACACS Profiles**. Add a new TACACS Profile and name it **IOS_HelpDesk_Privilege**.
- Step 2** Scroll down to the **Common Tasks** section. Enable the Default Privilege with a value of 1 from the drop-down selector, and the Maximum Privilege with a value of 15 from the drop-down.



Task Attribute View		Raw View	
Common Tasks			
<input checked="" type="checkbox"/> Default Privilege	1	(Select 0 to 15)	
<input checked="" type="checkbox"/> Maximum Privilege	15	(Select 0 to 15)	

Task Attribute View		Raw View	
Profile Attributes			
priv-lvl=1 max_priv_lvl=15			

Figure 6. TACACS Profile for `IOS_HelpDesk_Privilege`

Click **Save** to save the profile.

IOS Admin Privilege

Network administrators need more privileges in general so defaulted to Level-15 directly.

Step 3 Add another profile and name it **IOS_Admin_Privilege**.

Step 4 Scroll down to the **Common Tasks** section. Enable the Default Privilege with a value of 15 from the drop-down selector, and the Maximum Privilege with a value of 15 from the drop-down.

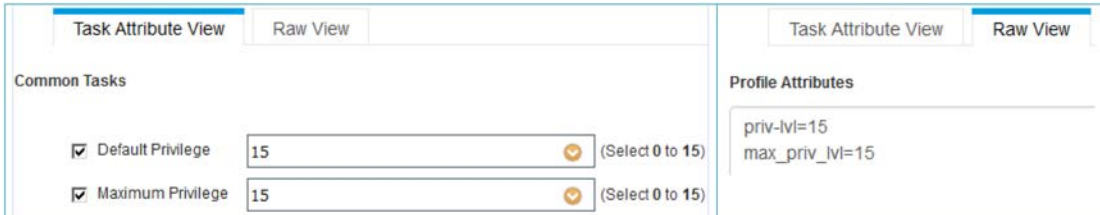


Figure 7. TACACS Profile for IOS_Admin_Privilege

Click **Save** to save the profile.

TACACS Command Sets

IOS command authorization queries the configured TACACS+ server to verify whether the device administrators are authorized to issue the commands. ISE can provide a list of commands granted to the users to fine tune which commands are available at various privilege levels.

We define three commands sets -- HelpDesk_Commands, IOS_Security_Commands, and Permit_All_Commands.

HelpDesk Commands

Step 1 On the ISE GUI, go to **Work Centers > Device Administration > Policy Results > TACACS Command Sets**. Add a new set and name it **HelpDesk_Commands**.

Step 2 Click **+Add** to configure entries to the set:

Grant	Command	Argument
PERMIT	debug	
PERMIT	undebg	
PERMIT	tracertoute	
DENY	ping	^([0-9]{1,3})\.([0-9]{1,3})\.([0-9]{1,3})\.255\$
PERMIT	ping	
PERMIT	show	

We allow helpdesk analysts to perform debug, undebg, tracertoute, and show. For ping, they are restricted from broadcast pings, assuming the network subnets with broadcast addresses ending with .255, as shown in the regular expression in the argument column.

Step 3 Click the check mark ✓ at the end of each entry to keep the line.

Step 4 Click **Save** to persist the command set.

IOS Security Commands

Step 5 Add a new set and name it **IOS_Security_Commands**.

Step 6 Click **+Add** to configure entries to the set:

Grant	Command	Argument
PERMIT	config*	

DENY_ALWAYS	interface	GigabitEthernet 1
DENY_ALWAYS	interface	GigabitEthernet ([0-9]{1,3}) 0
PERMIT	interface	
PERMIT	shut	
PERMIT	no	shut

In this sample command set, security administrators may perform shut and no shut operations on any interfaces except the two types of interfaces specified in the **DENY_ALWAYS** entries, where the second type designates an interface pattern GigabitEthernet <0-999>/0.

Step 7 Click the check mark ✓ at the end of each entry to keep the line.

Step 8 Click **Save** to persist the command set.

Permit All Commands

Step 9 Add a new set and name it **Permit_All_Commands**.

Step 10 Tick the checkbox next to ☐ Permit any command that is not listed below ☒, and leave the command list empty.

Grant	Command	Argument
-------	---------	----------

Step 11 Click **Save** to persist the command set.

Device Admin Policy Sets

Policy Sets are enabled by default for Device Admin. Policy Sets can divide policies based on the Device Types so to ease application of TACACS profiles. For example, Cisco IOS devices use Privilege Levels and/or Command Sets whereas WLC devices use Custom Attributes.

Step 1 Navigate to **Work Centers > Device Administration > Device Admin Policy Sets**. Add a new Policy Set **IOS Devices**:

S	Name	Description	Conditions
✓	IOS Devices		DEVICE:Device Type EQUALS Device Type#All Device Types#Network Devices#IOS Devices

Figure 8. Policy Set Condition

Step 2 Create the Authentication Policy. For Authentication, we use the AD as the ID Store.

Authentication Policy	
✓	Default Rule (if no match) : Allow Protocols : Default Device Admin and use: demoAD

Figure 9. Authentication Policy

Step 3 Define the Authorization Policy. Here we define the authorization policy based on the user groups in AD and the location of the device. For example, the users in AD group West Coast can access only the devices located in West Coast.

S	Rule Name	Conditions	Command Sets	Shell Profiles
✓	HelpDesk West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk	HelpDesk_Commands	IOS_HelpDesk_Privilege
✓	HelpDesk East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk	HelpDesk_Commands	IOS_HelpDesk_Privilege
✓	Security West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators	IOS_Security_Commands AND HelpDesk_Commands	IOS_Admin_Privilege
✓	Security East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Security_Operators	IOS_Security_Commands AND HelpDesk_Commands	IOS_Admin_Privilege
✓	Admin West	DEVICE:Location CONTAINS All Locations#West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/West_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators	Permit_All_Commands	IOS_Admin_Privilege
✓	Admin East	DEVICE:Location CONTAINS All Locations#East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/Network_Operators	Permit_All_Commands	IOS_Admin_Privilege

S	Rule Name	Conditions	Command Sets	Shell Profiles
✓	Default	if no matches, then	DenyAllCommands	

Figure 10. Authorization Policy

We are now done with the ISE configuration for Device Admin for IOS devices.

IOS Configuration for TACACS+

TACACS+ AAA on a Cisco IOS device can be configured in the following sequence:

1. Enable TACACS+ Authentication and Fallback
2. Enable TACACS+ Command Authorization
3. Enable TACACS+ Command Accounting

TACACS+ Authentication and Fallback

Before configuring TACACS+, SSH or a good remote connection protocol needs first configured. The following example configuration shows how to enable SSH.

```
hostname CSRv
no ip domain-lookup
ip domain-name securitydemo.net
crypto key generate rsa modulus 2048

ip ssh version 2

enable secret ISEisCOOL
username local-admin privilege 15 secret ISEisCOOL

aaa new-model
aaa authentication login CON none
aaa authentication login default local

interface GigabitEthernet1
 ip address 10.1.100.160 255.255.255.0

ip access-list extended vtyAccess
 permit tcp 10.1.100.0 0.0.0.255 any eq 22

line con 0
 exec-timeout 0 0
 login authentication CON
 logging synchronous

!! Below assumes only 5 VTY lines (from 0 to 4)
line vty 0 4
 access-class vtyAccess in
 transport input ssh
 logging synchronous
```

Since we have a valid IP address for the above sample network device at this stage, we can SSH to this IOS device from a client in 10.1.100.0/24 while the console login remains no authentication. Note that we disable EXEC timeout for CONSOLE so to avoid possible access issue during AAA configuration.

TACACS+ authentication can be enabled with a configuration similar to the following:

```
tacacs server ise-1
  address ipv4 10.1.100.21
  key ISEisC00L

aaa group server tacacs+ demoTG
  server name ise-1

aaa authentication login VTY group demoTG local
aaa authentication enable default group demoTG enable

line vty 0 4
  login authentication VTY
```

We have thus switched to TACACS+ to authenticate the VTY lines. Note that the “enable” authentication has the default list only so both VTY and CONSOLE use TACACS+ to authenticate “enable” access.

In the events that the configured TACSACS+ server becomes unavailable, the login authentication falls back to use the “local” user database while the enable authentication to the “enable” secret.

TACACS+ Command Authorization

EXEC Authorization is a special form of command authorization. It happens right after a user login and can be enabled by adding the following:

```
aaa authorization exec CON none
aaa authorization console
aaa authorization exec VTY group demoTG local if-authenticated

line con 0
  authorization exec CON

line vty 0 4
  authorization exec VTY
```

At this point, the shell profiles with the default privilege attribute apply to new SSH sessions.

Further TACACS+ Command Authorization for the configuration mode and for various privilege levels can be enabled by adding the following:

```
aaa authorization config-commands
aaa authorization commands 1 VTY group demoTG local if-authenticated
aaa authorization commands 15 VTY group demoTG local if-authenticated

line vty 0 4
  authorization commands 1 VTY
  authorization commands 15 VTY
```

TACACS+ Command Accounting

Command accounting sends info about each command executed, which includes the command, the date, and the username. The following adds to the previous configuration example to enable this accounting feature:

```
aaa accounting exec default start-stop group demoTG
aaa accounting commands 1 default start-stop group demoTG
aaa accounting commands 15 default start-stop group demoTG
```

Here uses the default method list as we need not distinct accounting based on connection types.

We are done with the IOS configuration for TACACS+.

What's Next?

Configuration for Device Admin for Cisco IOS is completed. We will need to validate the configuration.

- Step 1 SSH and log into the IOS devices as various roles.
- Step 2 Once on the device command-line interface (CLI), verify that the user has access to the right commands. For example, a Helpdesk user should be able to ping a regular IP address (e.g. 10.1.10.1) but denied to ping a broadcast address (e.g. 10.1.10.255).
- Step 3 To show the user connections, issue

```
show users
```

A sample output is shown below:

```
CSRv#show users
   Line      User      Host(s)      Idle      Location
   0 con 0
*  1 vty 0    neo      idle        00:00:00  10.1.100.6
...
```

- Step 4 The following debugs are useful in troubleshooting TACACS+:

```
debug aaa authorization
debug tacacs
debug tacacs packet
```

Here is a sample debug output:

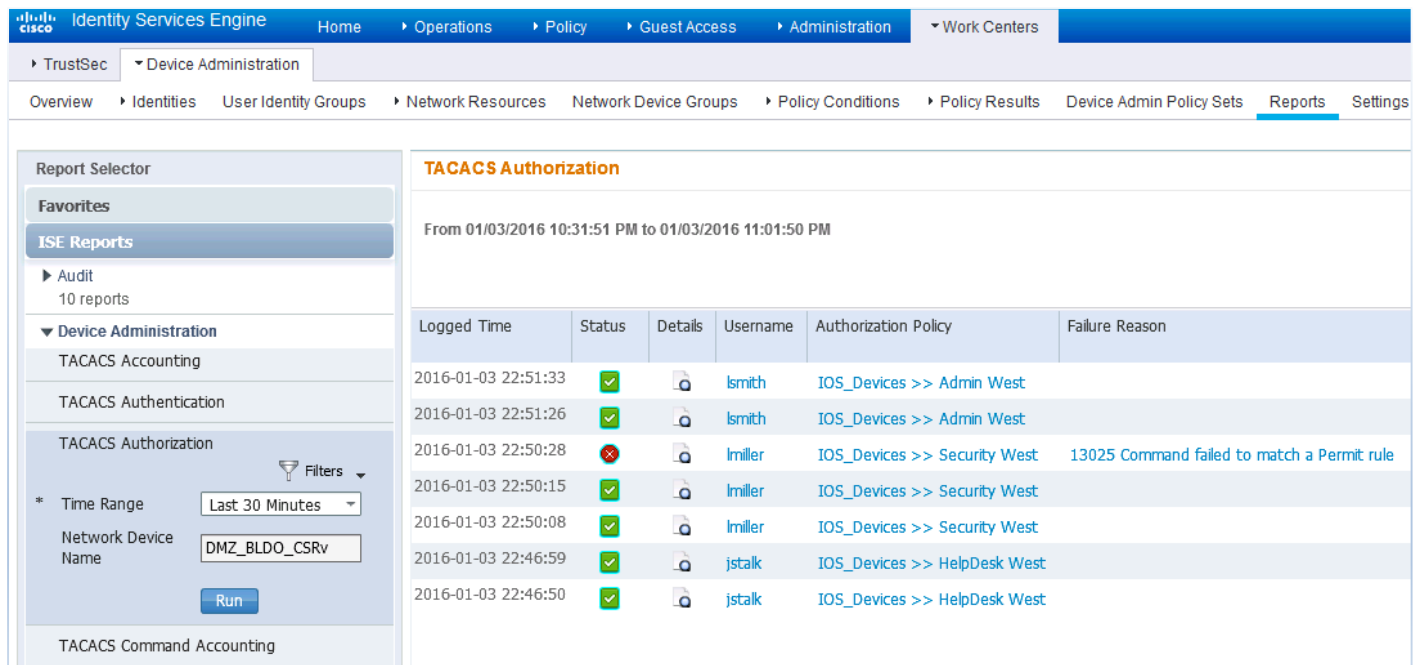
```
CSRv#debug tacacs
TACACS access control debugging is on
...
*Jan 4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): Port='tty2' list='VTY' service=CMD
*Jan 4 06:24:43.001: AAA/AUTHOR/CMD: tty2 (2087247696) user='admin'
*Jan 4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): send AV service=shell
*Jan 4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): send AV cmd=debug
*Jan 4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): send AV cmd-arg=tacacs
*Jan 4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): send AV cmd-arg=<cr>
*Jan 4 06:24:43.001: tty2 AAA/AUTHOR/CMD(2087247696): found list "VTY"
*Jan 4 06:24:43.001: tty2 AAA/AUTHOR/CMD (2087247696): Method=demoTG (tacacs+)
*Jan 4 06:24:43.001: AAA/AUTHOR/TAC+: (2087247696): user=admin
*Jan 4 06:24:43.001: AAA/AUTHOR/TAC+: (2087247696): send AV service=shell
*Jan 4 06:24:43.001: AAA/AUTHOR/TAC+: (2087247696): send AV cmd=debug
*Jan 4 06:24:43.001: AAA/AUTHOR/TAC+: (2087247696): send AV cmd-arg=tacacs
*Jan 4 06:24:43.001: AAA/AUTHOR/TAC+: (2087247696): send AV cmd-arg=<cr>
*Jan 4 06:24:43.203: AAA/AUTHOR (2087247696): Post authorization status = PASS_ADD
*Jan 4 06:24:43.203: AAA/MEMORY: free_user (0x7FF239502490) user='admin' ruser='CSRv'
port='tty2' rem_addr='10.1.100.203' authn_type=ASCII service=NONE priv=15 vrf= (id=0)
...
```


Step 5 From the ISE GUI, navigate to **Operations > TACACS LiveLog**. All the TACACS authentication and authorization requests are captured here, and the details button provides detailed information about why a particular transaction passed/failed.








Username ⁱ	Type	Authorization Policy ⁱ	Network Device Name ⁱ	Remote Address ⁱ	Matched Comman... ⁱ	Shell Profile ⁱ
lsmith	Authorization	IOS_Devices >> Admin West	DMZ_BLDO_CSRv	10.1.100.203	Permit_All_Commands	
lsmith	Authorization	IOS_Devices >> Admin West	DMZ_BLDO_CSRv	10.1.100.203		IOS_Admin_Privilege
lsmith	Authentication		DMZ_BLDO_CSRv	10.1.100.203		
lmiller	Authorization	IOS_Devices >> Security West	DMZ_BLDO_CSRv	10.1.100.203		
lmiller	Authorization	IOS_Devices >> Security West	DMZ_BLDO_CSRv	10.1.100.203	IOS_Security_Com...	
lmiller	Authorization	IOS_Devices >> Security West	DMZ_BLDO_CSRv	10.1.100.203		IOS_Admin_Privilege
lmiller	Authentication		DMZ_BLDO_CSRv	10.1.100.203		
jstalk	Authorization	IOS_Devices >> HelpDesk West	DMZ_BLDO_CSRv	10.1.100.203	HelpDesk_Commands	
jstalk	Authorization	IOS_Devices >> HelpDesk West	DMZ_BLDO_CSRv	10.1.100.203		IOS_HelpDesk_Privilege
jstalk	Authentication		DMZ_BLDO_CSRv	10.1.100.203		

Figure 11. TACACS LiveLogs

Step 6 For historic reports: Go to **Work Centers > Device Administration > Reports > Device Administration** to get the authentication, authorization, and accounting reports.



The screenshot shows the Cisco Identity Services Engine (ISE) GUI. The top navigation bar includes Home, Operations, Policy, Guest Access, Administration, and Work Centers. The left sidebar shows the navigation tree with TrustSec, Device Administration, and Reports. The main content area displays the TACACS Authorization report for the time range 01/03/2016 10:31:51 PM to 01/03/2016 11:01:50 PM. The report table lists logged times, status, details, usernames, authorization policies, and failure reasons.

Logged Time	Status	Details	Username	Authorization Policy	Failure Reason
2016-01-03 22:51:33	✓		lsmith	IOS_Devices >> Admin West	
2016-01-03 22:51:26	✓		lsmith	IOS_Devices >> Admin West	
2016-01-03 22:50:28	✗		lmiller	IOS_Devices >> Security West	13025 Command failed to match a Permit rule
2016-01-03 22:50:15	✓		lmiller	IOS_Devices >> Security West	
2016-01-03 22:50:08	✓		lmiller	IOS_Devices >> Security West	
2016-01-03 22:46:59	✓		jstalk	IOS_Devices >> HelpDesk West	
2016-01-03 22:46:50	✓		jstalk	IOS_Devices >> HelpDesk West	