ISE 2.3+ TACACS+ IPv6 Configuration Guide for Cisco IOS Based Network Devices with new Policy UI

Secure Access How-to User Series

Author: Krishnan Thiruvengadam

Technical Marketing, Policy and Access, , Cisco Systems

Date: July 6, 2018

Table of Contents

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 2.3
- 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

Step 1 Device Administration (TACACS+) is licensed per deployment, but requires existing and valid ISE base or mobility licenses. Go to **Administration > System > Licensing**. Verify that the licensing for Device Admin is Enabled.

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.

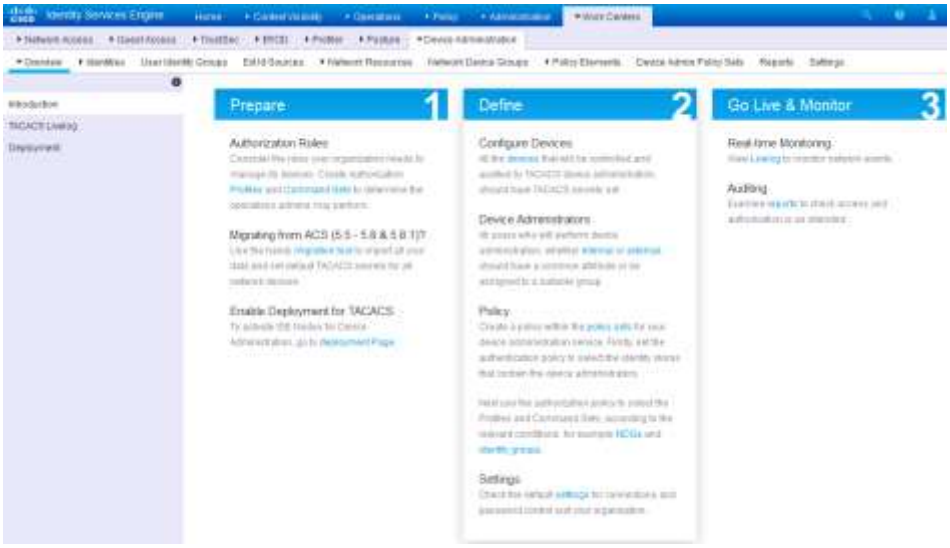
Step 2 Log in to the ISE admin web portal using one of the supported browsers.

Device Administration Work Center

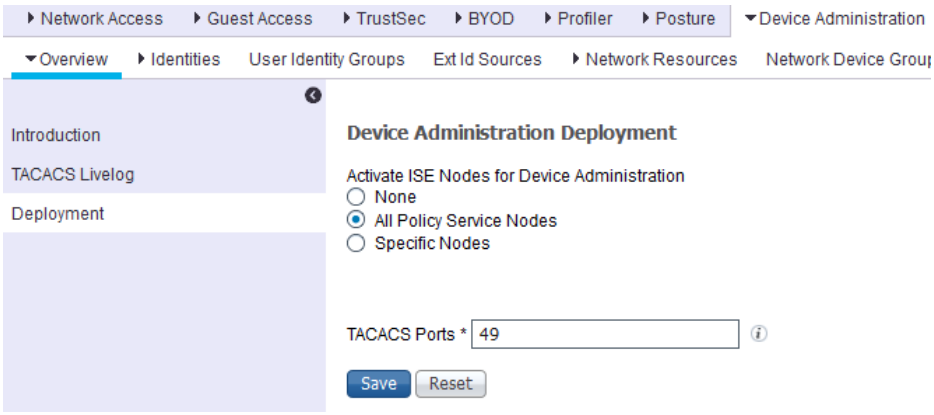
Starting with ISE 2.0, a Work Center encompasses all elements for an ISE feature, such as Device Administration.

Step 3 Navigate to **Work Centers > Device Administration**. You will land in the **Overview > Introduction**, which is the default screen for this menu.

It outlines three stages for Device Administration – Prepare, Define, and Go Live & Monitor. The submenus under Device Administration are entities to accomplish various tasks for this feature.



Step 4 Select **Deployment** from the left-hand pane to jump to the page Device Administration Deployment. Since this ISE is standalone, select either [⦿ **All Policy Service Nodes] or [⦿ Specific Nodes] and select ☑ your ISE node (e.g:ise-1.demo.local)**, under Activate ISE Nodes for Device Administration.



Step 5 Click **Save** when done.

Note 1 TACACS+ Ports are configurable here. This was new in ISE 2.1.

Network Device and Network Device Groups

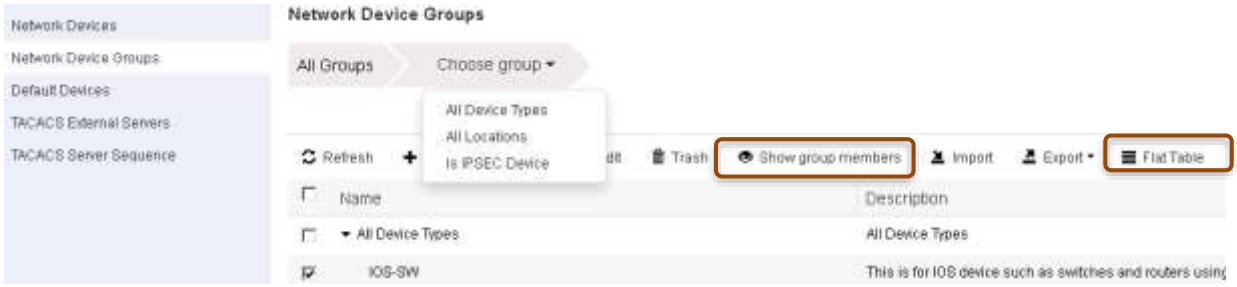
ISE provides powerful device grouping with multiple device group hierarchies. Each hierarchy represents a distinct and independent classification of network devices. It is recommended to create Network Device Groups based on Device Types, locations and other criteria and use this in Policy Sets.

ISE 2.3 supports 6 level hierarchy and 10,000 Network Device Groups.

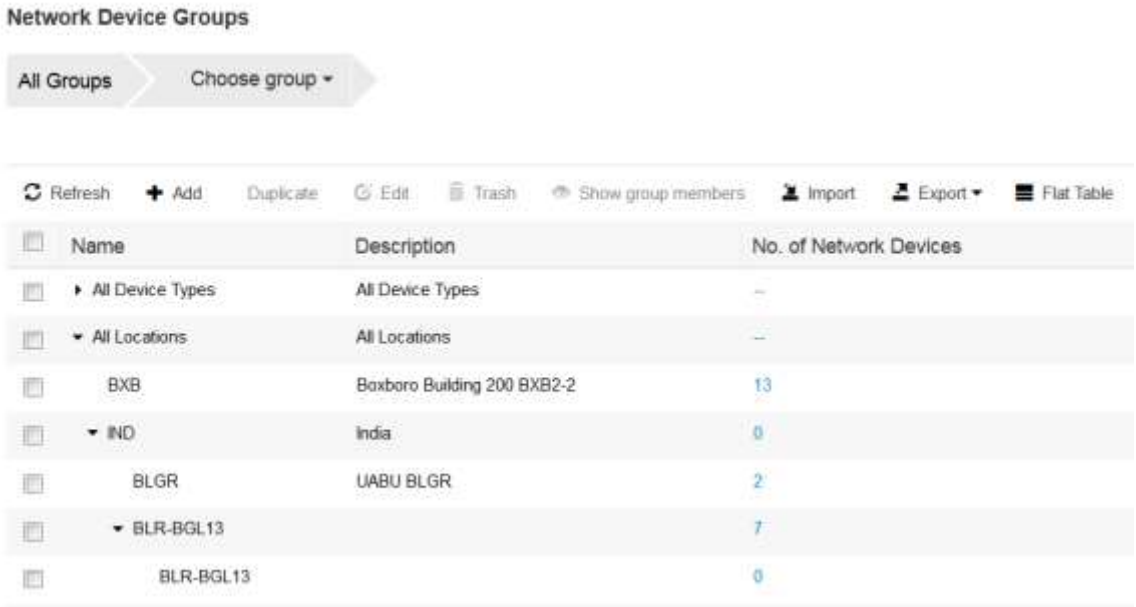
Step 1 Navigate to **Work Centers > Device Administration > Network Resources**. Click on **Device Groups** from the left side panel. ISE UI has the option of viewing the table as a **Tree** or a **Flat table**. By default the view has a Tree format.

Note 2

Step 2 Click on the **Choose group** drop down to organize based on the device groups. Select the group from the list. Click on **Show group members** to view the Network devices in that particular Network device group. Click on the + to add a group **IOS-SW** under **All Device Types**



Step 3 In ISE 2.3, you can create Network device groups with only 32 characters and 6 level hierarchy. Here is an example of Network Device Group Hierarchy.



Step 4 Navigate to **Work Centers > Device Administration > Network Resources**. It displays the Network Devices screen. Click **+ Add** to add a new network device (using subnets) and fill in the data as below:

Note 3 For IPv6 this has to be the global IPv6 address of the network device. Link local IPv6 addresses are not supported here.

Name	**CSRv**
Description	-
IP Address	2001:EF8::1 / 64
Device Profile	Cisco
Model Name	-
Software Version	-
Device Type	IOS-SW
Location	SJC
☐ **RADIUS Authentication Settings**	
☑ **TACACS+ Authentication Settings**	
Shared Secret	ISEisC00L
Enable Single Connection Mode	☐ ◉ Legacy Cisco Device ○ TACACS+ Draft Compliance Single Connect Support
☐ **SNMP Settings**	
☐ **Advanced TrustSec Settings**	

Step 5 Click [**Save**] in the bottom left corner of the screen when done.

Note 4 IPv6 supports Single connect Mode also. Optionally you can try enabling Single Connect Mode with TACACS+ Draft Compliance Single Connect support option

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**.

Step 2 If the status shows *Not Joined*, tick ☑ the checkbox next to ISE node *ise-1.demo.local* and then click **Join**.

Step 3 In **Join Domain** pop-up window, fill in the **Active Directory administrator** username and password.

Step 4 Click **OK** to start the join operation. A window **Join Operation Status** will pop up. Wait until the node status turns **Completed**, and then click **Close**.

Step 5 The **Connection** tab shall show ad.securitydemo.net as the domain controller and Default-First-Site-Name as the site.

Step 6 Click on the tab **[Groups]** and look at the list of pre-configured AD groups. The groups we will use in the document are Contractors, Employees, and Staff, and map to T+ authorization policy rules such that

Staff → Admin

Employees → Security

Contractors → HelpDesk

As Staff is also member of Employees, we will arrange the Admin rules higher in priority. Please create the groups as needed in Active Directory for this.

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.

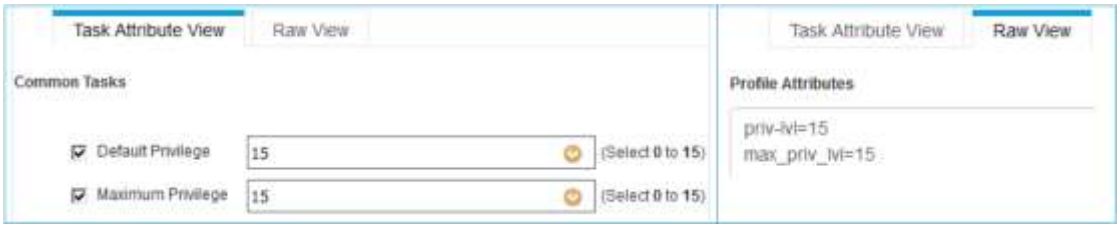
Step 3 Click **Save** to save the profile.

IOS Admin Privilege

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

Step 4 Add another profile and name it **IOS_Admin_Privilege**.

Step 5 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.



Step 6 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 have defined three commands sets – helpDeskCmds, iosSecurityCmds, and permitAllCmds. Go to **Step 11** for creating command sets manually.

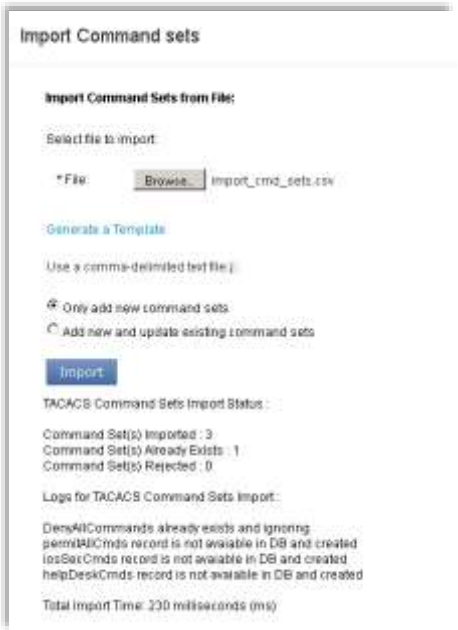
Alternatively, you can also create a csv file for all these command sets and import them. For importing command sets, please follow the steps below

Step 7 From the ISE UI, go to **Work Centers > Device Administration > Policy Elements > TACACS Command Sets.**

Step 8 Click **Import** from the list of options on the right panel.

Step 9 A window opens up asking you to "Import Command Sets". Click **Browse** button to open the Windows explorer and go to the folder you saved the csv file, select the file by double clicking the file. You can use "**Generate a template**" option shown in screenshot below to create the csv file.

Step 10 Click **Import** button to complete the process. You will see the Import Status, Logs and the time taken as shown in the screenshot below.



helpDeskCmds Commands

Step 11 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 12 Click **+Add** to configure entries to the set:

Grant	Command	Argument
PERMIT	*debug	
PERMIT	traceroute	
DENY	ping	([0-9]{1,3}\.){3}255
PERMIT	ping	
PERMIT	show	

We allow helpdesk analysts to perform debug, undebug, traceroute, 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 13 Click the check mark ✓ at the end of each entry to keep the line.

Step 14 Click **Save** to persist the command set.

iosSecCmds Commands

Step 15 Add a new set and name it **IOS_Security_Commands**.

Step 16 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 17 Click the check mark ✓ at the end of each entry to keep the line.
Step 18 Click **Save** to persist the command set.

pemitAllCmds

Step 19 Add a new set and name it **Permit_All_Commands**.
Step 20 Tick the checkbox next to Permit any command that is not listed below ☑, and leave the command list empty.

Grant	Command	Argument

Step 21 Click **Save** to persist the command set.

ISE TACACS Policy Set (new UI)

ISE Device Admin uses policy sets, which can group polices based on the Network Device Groups or other criteria to filter and redirect the incoming requests to the corresponding authentication and authorization policy. 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**. You will see a new Policy set UI that is new in ISE 2.3. Observe the new tabular UI with Hits (hit counts).

Tool tips:

Click + **plus** button to create a new row above.

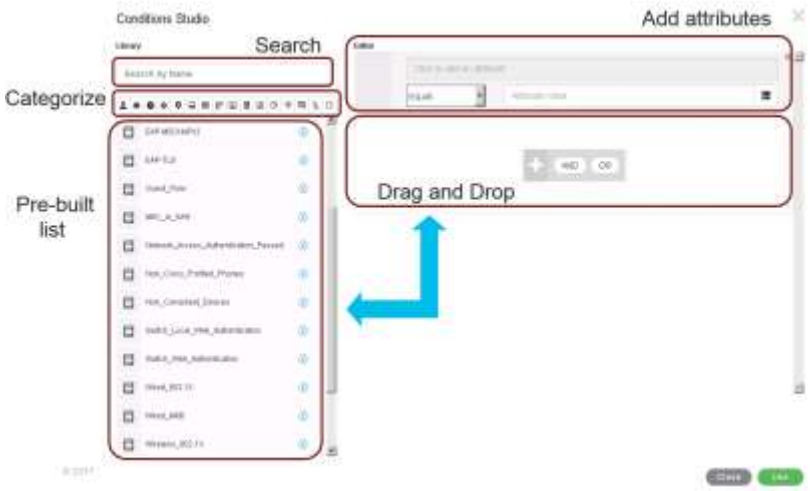
Click ⚙ **gear** button to create row above, below and duplicate the entries.

Click › **right arrow** button to expand the policy set to view the authentication/ authorization policies.

Step 2 Click + the button to insert a new row above to add a new Policy Set **IOS Devices**:

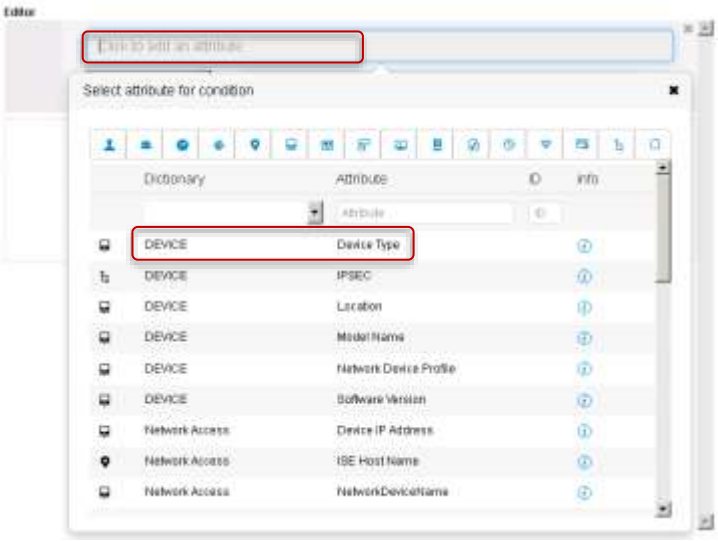
S	Name	Description	Conditions
✓	IOS Devices		DEVICE:Device Type EQUALS All Device Type#IOS-SW

Step 3 Click on the + button to add Conditions from the Conditions studio.



Step 4 The Pre-built list on the left will have some of the most utilized conditions that are made available in the Conditions Studio.

Step 5 To create a new condition, to the right of the screen under the **Editor, Click to add an attribute** from the list of pre-defined attributes in ISE.



Step 6 Choose the **Device Type** attribute from the list above and use **All Device Types#IOS-SW** as value as shown below. This was the Network Device Group we added for CSRv initially.

Step 7 Hover over the condition on the window highlighted above. You will see buttons appear to **Duplicate** or to **Save.** This allows you option to save the condition for future use.

You can go to **Step 8** directly if you want to skip saving the condition in the library. If this is a new condition that you are adding, use the option to create a new library condition. This condition will appear the conditions list in the Conditions Studio. As you create newer conditions, ISE UI will save all the new conditions for you in the Conditions Studio for future use.

Click **Save**. ISE UI will ask you to save as **existing library condition** or **new library condition.**

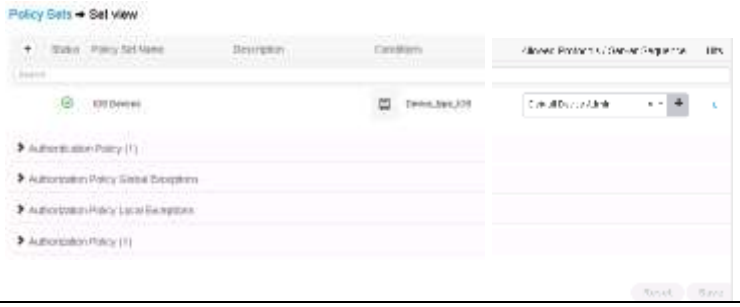
You can save the condition you just created as **"Device_Type_IOS**".

Step 8 Click on the **Use** button at the bottom right of the screen 

Step 9 Click the drop down  under the **Allowed protocol/Server Sequence** and choose **Default Device Admin** from the list. Click **Save.**

Step 10 Your policy set will look as shown below.

Step 11 Click the right › arrow to expand the policy sets as shown above. You will see the default authentication, authorization and exception policies listed as shown below.



Step 12 Define the Authentication Policy by clicking on the **Authentication Policy** option shown in screenshot above.

Step 13 In the Default rule under **Use,** click the drop down box that shows '**All_User_ID_Stores**' and change it to '**demoAD**'. Click **Save** at the bottom right of the screen. 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

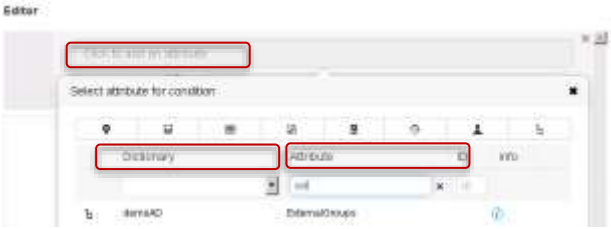
Step 14 Define the Authorization Policy by clicking the **Authorization Policy** option in the **Policy sets →Set view** screen. Here we define the authorization policy based on the user groups in Active directory.

Step 15 The procedure to create a new Policy set, authentication and authorization policy are the same. Use the procedure mentioned above to create 3 authorization rules defined as in the table below (or) follow the steps below.

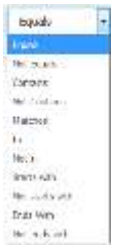
S	Rule Name	Conditions	Command Sets	Shell Profiles
✓	Admin	demoAD:ExternalGroups EQUALS demo.local/HCC/Groups/Staff	permitAllCmds	iosAdminPrivs
✓	Security	demoAD:ExternalGroups EQUALS demo.local/HCC/Groups/Employees	iosSecCmds	iosAdminPrivs
✓	HelpDesk	demoAD:ExternalGroups EQUALS demo.local/HCC/Groups/Contractors	helpDeskCmds	iosHelpDeskPrivs
✓	Default	if no matches, then	Deny All Shell Profile	

Step 16 From the Conditions studio right panel **Click to add an attribute** as shown in screenshot below.

Step 17 Select **demoAD** as the Dictionary and "**External Groups**" attribute available in the list. You can use the filters for this too as shown above.



Step 18 Select the right operator from the drop down window. Choose the value as in the table above



Step 19 Click **Submit** to save the policy set.

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
4. Test accessing CSRv router with different credentials

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 ISEisC00L
username local-admin privilege 15 secret ISEisC00L

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

ipv6 unicast-routing
interface GigabitEthernet1
 ip address 10.1.100.160 255.255.255.0
 ipv6 enable
 ipv6 address 2001:ef8::1/64
  no shutdown

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

ipv6 access-list vtyaccessv6
 permit tcp 2001:EF8::/64 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 vtyAccessv6 in
 transport input ssh
 logging synchronous
```

At this stage, we can SSH to this IOS device from a client in 2001:EF8::/64 subnet using the configured local user while the console login remains without authentication. Note that we disable EXEC timeout for CONSOLE so to avoid possible access issue during AAA configuration.

Step 1 Start a new PuTTY window to SSH to 2001:ef8::1 (CSRv's IP) login as *Local-admin/ISEisC00L* and enable using the same password *ISEisC00L*.

Step 2 Issue "exit" after the previous step tested ok to close the test SSH session window.

Next, we will enable TACACS+ authentication.

Step 3 Back to the console window for CSRv, and issue the following command lines.

```
conf t

tacacs server ise-1
 address ipv6 2001:ef8::250:56ff:febd:1aa4
 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

end
```

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+ EXEC Authorization

EXEC Authorization is a special form of command authorization. It happens right after a user login to verify the users' privileges.

Step 4 At the CSRv console, issue the following to initiate EXEC authorization.

```
conf t

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

end
```

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

TACACS+ Command Authorization

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+.

Testing TACACS+ User Access to CSRv

Step 1 Use PuTTY to launch a new session to SSH to 2001:ef8::1 (CSRv's IP), login in turn as various users given in the table below.

Step 2 Make sure you create 3 users employee1

Check the results at PuTTY SSH CLI and ISE Admin web console. The table below lists the expected results.

Login Users	**Expected Results**	
	PuTTY SSH CLI	**ISE T+ Live Logs @ Work Center > Device Administration > Overview > TACACS Livelog**
local-admin	*Access denied*	***Message Text*** *: Authentication Failed:* ***Failure reason****: Subject not found in the applicable Identity Store* ***Remote Address****:* 2001:EF8::DDE3:DD41:xxxx:xxxx *(Open up a* ***command prompt window*** *from the Client machine and type* ***ipconfig/all*** *to verify the IPv6 address)*
employee1	*Get privileged mode CLI prompt "#"*	*Authentication and Session Authorization succeeded (Two log entries). Observe the Authorization Policy, Shell profiles, Remote Address used in Authorization logs.*

contractor1	*Get user mode CLI prompt ">"* *Then, enable OK*	*Authentication and Session Authorization succeeded (Two log entries). Observe the difference in Authorization Policy, Shell profiles used in Authorization logs.* *Observe* ***Authentication Service*** *attribute is enable* ***Optional:*** *Observe the Device Port in the logs, go back to the router(original session using 10.0.0.1) and execute the command "sh line" to view the lines used.*
student1	*Access denied.*	***Message Text*** *Failed-Attempt: Authentication failed* ***Failure Reason*** *13036 Selected Shell Profile is DenyAccess* ***Response*** *{AuthenticationResult=Passed; AuthorizationFailureReason=ShellProfileDenyAuthorization; Authen-Reply-Status=Fail; }*

Note 5 Even if the authentication is successful if the authorization is denied, the user will not be able to access the network device result in failed authentication. This is different behavior than ISE releases before.

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                 idle                 01:54:52
*  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' authen_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.

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

>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>End of Document<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<