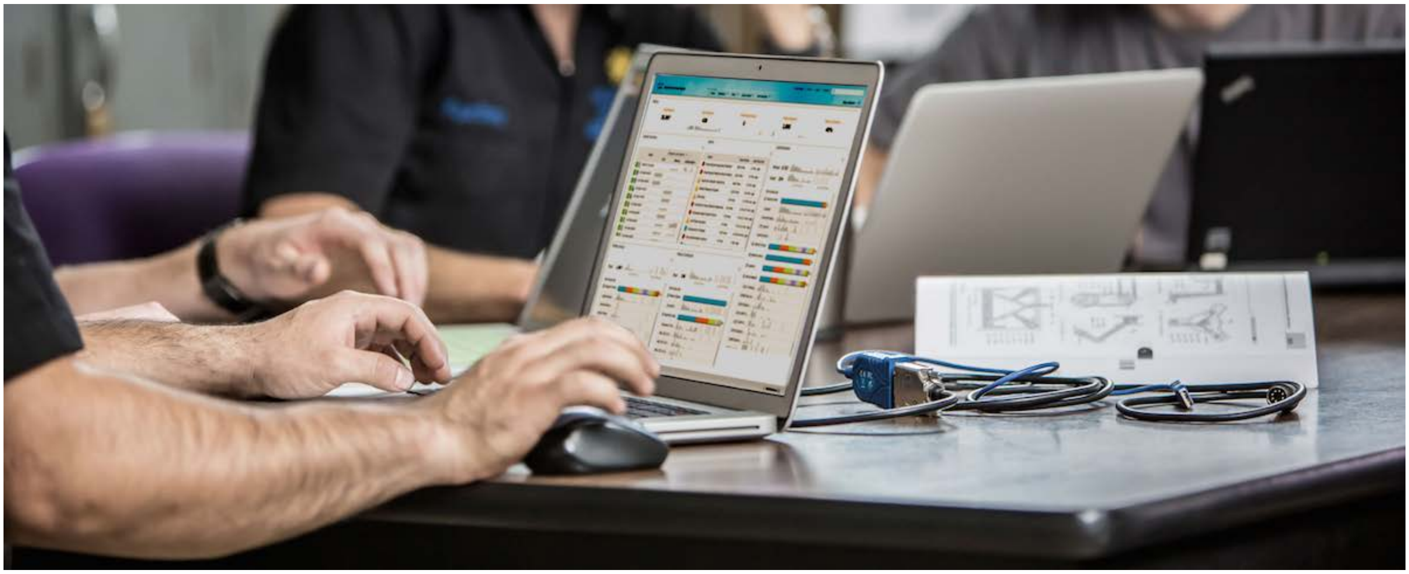


ISE TACACS+ Configuration Guide for Cisco ASA

Secure Access How-to User Series

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

Date: February 2016

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 Adaptive Security Appliance (ASA) as the TACACS+ client.

Using This Guide

This guide divides the activities into two parts to enable ISE to manage administrative access for Cisco ASA.

- Part 1 – Configure ISE for Device Administration
- Part 2 – Configure Cisco ASA 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 Adaptive Security Virtual Appliance (ASAv), Cisco ASA Software Version 9.5(2) and Adaptive Security Device Manager (ASDM) Version 7.5(2)
- Oracle Java™ SE Runtime Environment, build 1.7.0_40-b43

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

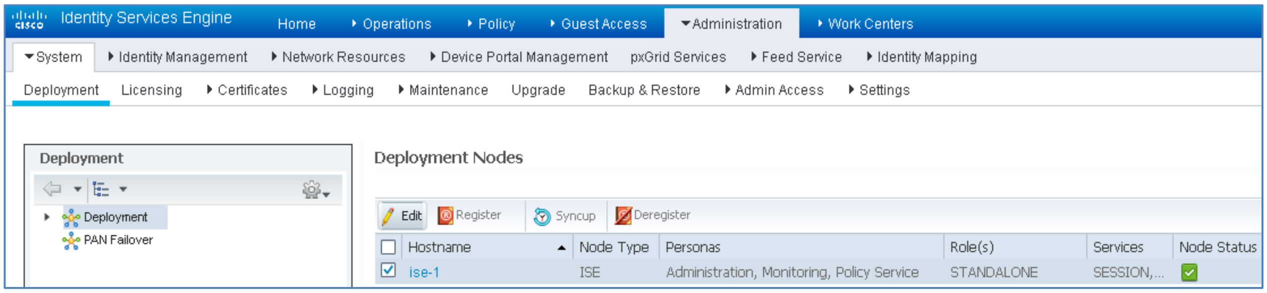
Device Administration (TACACS+) is licensed per deployment, but requires existing and valid ISE base or mobility licenses.

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.

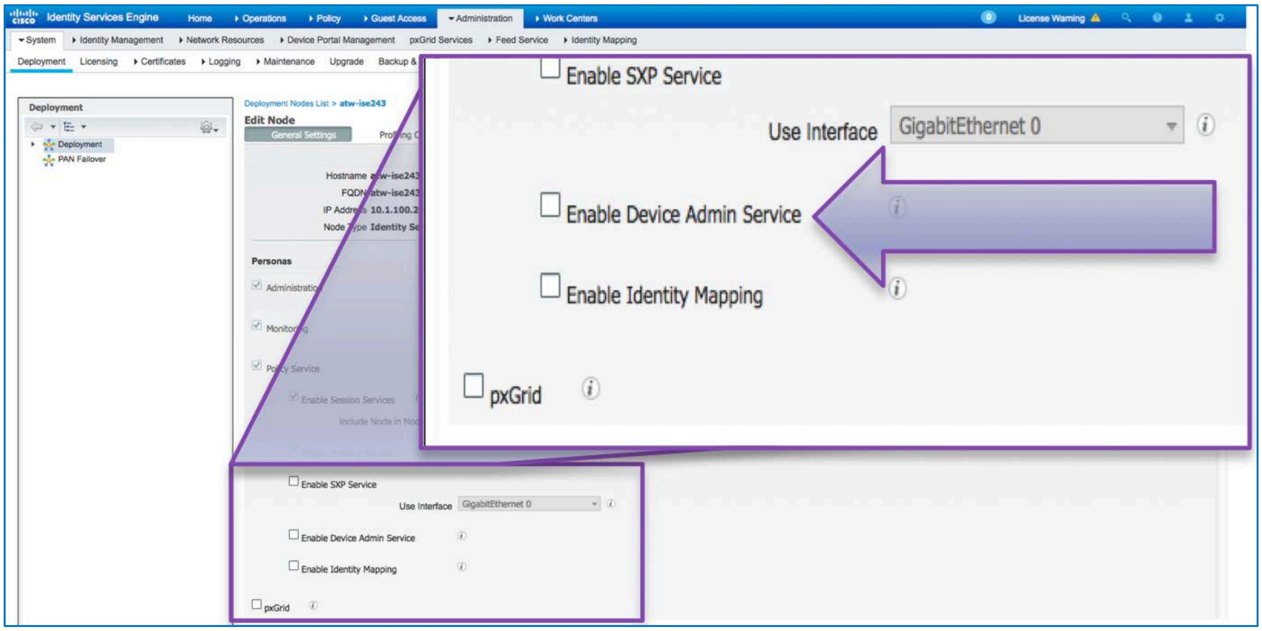
Step 2 Navigate to **Administration** > **System** > **Deployment**. Select the check box next to the ISE node and click **Edit**.



□	Hostname	Node Type	Personas	Role(s)	Services	Node Status
☑	ise-1	ISE	Administration, Monitoring, Policy Service	STANDALONE	SESSION,...	✓

Figure 1. ISE Deployment Page

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



Hostname atw-ise243

FQDN atw-ise243

IP Address 10.1.100.2

Node Type Identity Se

□ Enable SXP Service

Use Interface GigabitEthernet 0

□ Enable Device Admin Service

□ Enable Identity Mapping

□ pxGrid

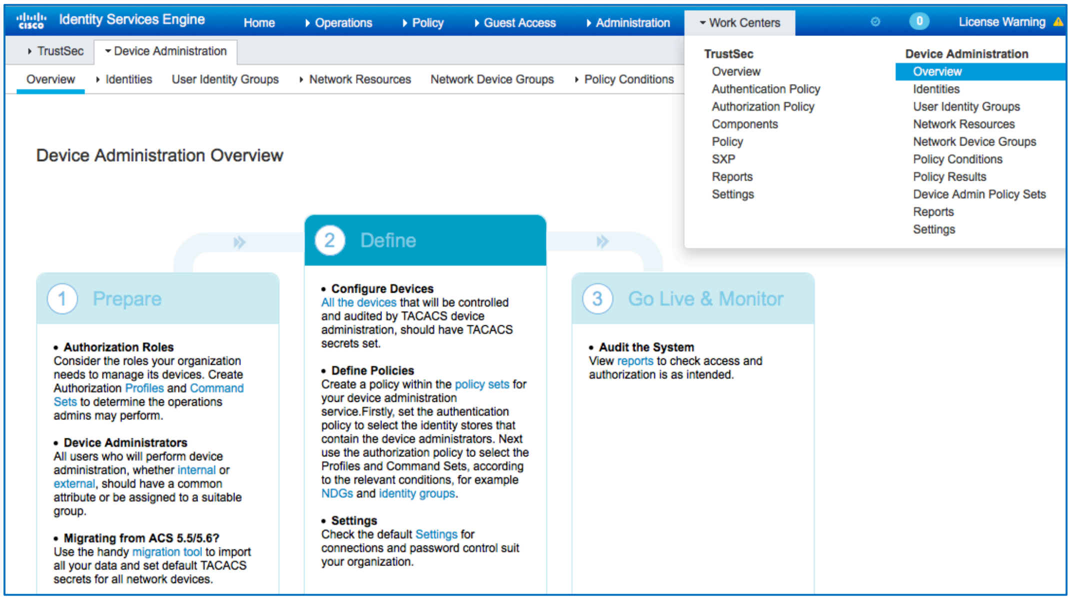
Figure 2. ISE Deployment General Settings

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**



Device Administration Overview

1 Prepare

- **Authorization Roles**
  Consider the roles your organization needs to manage its devices. Create Authorization Profiles and Command Sets to determine the operations admins may perform.
- **Device Administrators**
  All users who will perform device administration, whether internal or external, should have a common attribute or be assigned to a suitable group.
- **Migrating from ACS 5.5/5.6?**
  Use the handy migration tool to import all your data and set default TACACS secrets for all network devices.

2 Define

- **Configure Devices**
  All the devices that will be controlled and audited by TACACS device administration, should have TACACS secrets set.
- **Define Policies**
  Create a policy within the policy sets for your device administration service.Firstly, set the authentication policy to select the identity stores that contain the device administrators. Next use the authorization policy to select the Profiles and Command Sets, according to the relevant conditions, for example NDGs and identity groups.
- **Settings**
  Check the default Settings for connections and password control suit your organization.

3 Go Live & Monitor

- **Audit the System**
  View reports to check access and authorization is as intended.

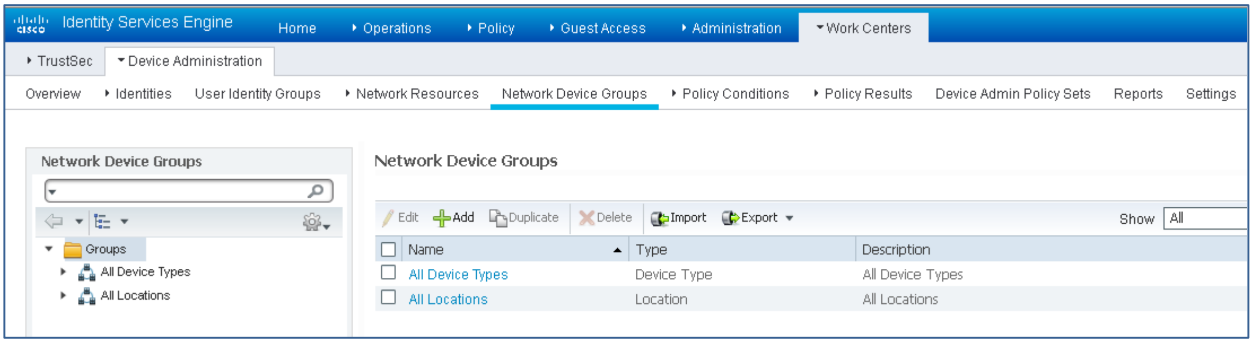
Figure 1. Device Admin Overview

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**

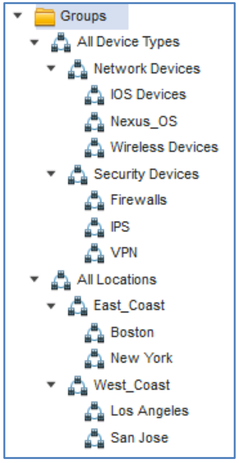


□	Name	Type	Description
□	All Device Types	Device Type	All Device Types
□	All Locations	Location	All Locations

Figure 2. 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.

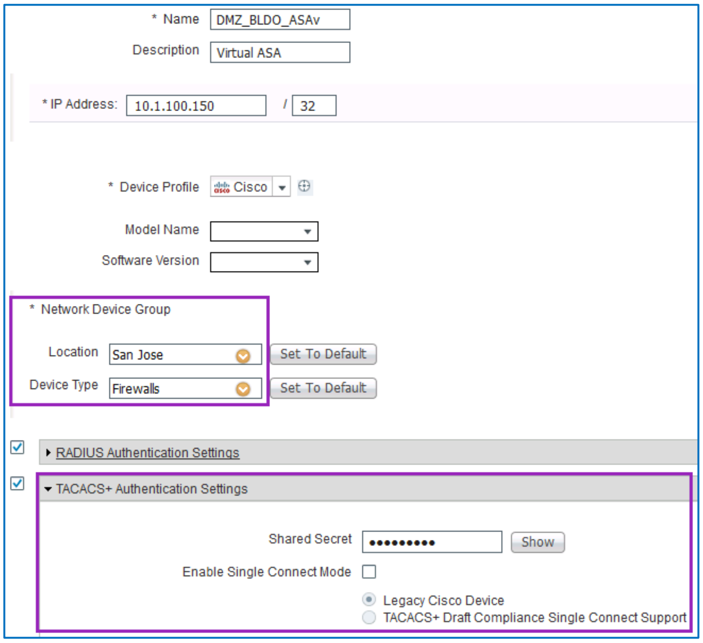
Step 2 After defining hierarchies, the Network Device Groups will look similar to the following:



- Groups
  - All Device Types
    - Network Devices
      - IOS Devices
      - Nexus_OS
      - Wireless Devices
    - Security Devices
      - Firewalls
      - IPS
      - VPN
  - All Locations
    - East_Coast
      - Boston
      - New York
    - West_Coast
      - Los Angeles
      - San Jose

Figure 3. Network Device Group Tree View

Step 3 Now, add an ASAv as a Network Device. Go to **Work Centers** > **Device Administration** > **Network Resources.** Click **+Add** to add a new Network Device **DMZ_BLDO_ASAv**.



* Name: DMZ_BLDO_ASAv

Description: Virtual ASA

* IP Address: 10.1.100.150 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: San Jose [Set To Default]

Device Type: Firewalls [Set To Default]

☑ RADIUS Authentication Settings

☑ TACACS+ Authentication Settings

Shared Secret: •••••••••• [Show]

Enable Single Connect Mode □

● Legacy Cisco Device

○ TACACS+ Draft Compliance Single Connect Support

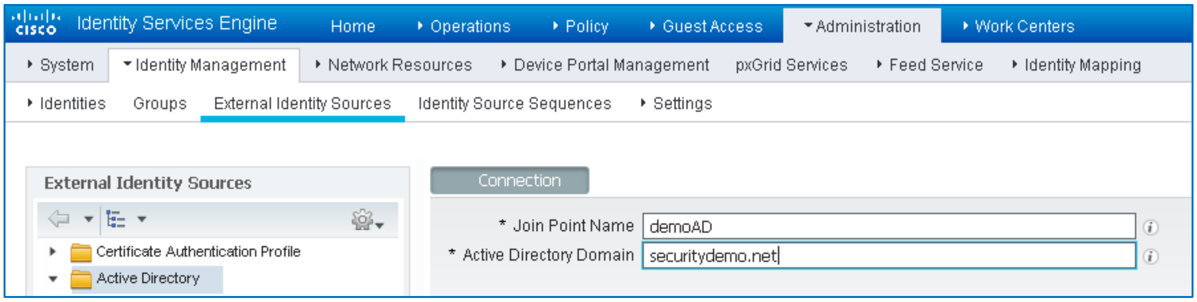
Figure 4. Adding Network Device

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**.

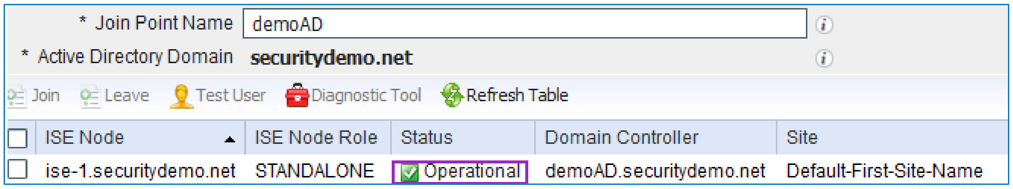


* Join Point Name: demoAD

* Active Directory Domain: securitydemo.net

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.



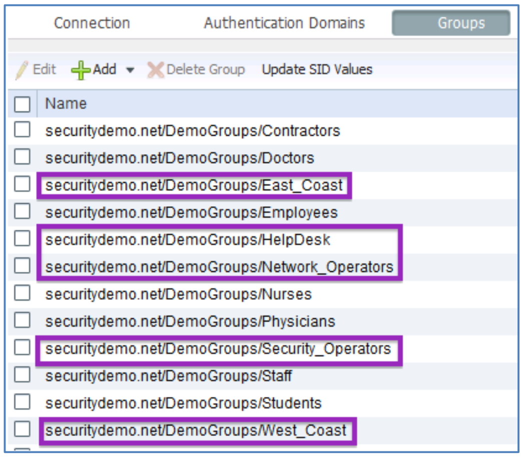
* Join Point Name: demoAD

* Active Directory Domain: **securitydemo.net**

☐	ISE Node	ISE Node Role	Status	Domain Controller	Site
☐	ise-1.securitydemo.net	STANDALONE	✓ Operational	demoAD.securitydemo.net	Default-First-Site-Name

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



☐	Name
☐	securitydemo.net/DemoGroups/Contractors
☐	securitydemo.net/DemoGroups/Doctors
☐	securitydemo.net/DemoGroups/East_Coast
☐	securitydemo.net/DemoGroups/Employees
☐	securitydemo.net/DemoGroups/HelpDesk
☐	securitydemo.net/DemoGroups/Network_Operators
☐	securitydemo.net/DemoGroups/Nurses
☐	securitydemo.net/DemoGroups/Physicians
☐	securitydemo.net/DemoGroups/Security_Operators
☐	securitydemo.net/DemoGroups/Staff
☐	securitydemo.net/DemoGroups/Students
☐	securitydemo.net/DemoGroups/West_Coast

Figure 5. AD Groups

TACACS Profiles

Cisco ASA provides 16 levels of access privileges for command authorization. Three are defined by default:

> Privilege level 0 – permits *show checksum*, *show curpriv*, *show history*, *show version*, *enable*, *help*, *login*, *logout*, *pager*, *show pager*, *clear pager*, and *quit* 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 “ciscoasa>”.
>
> 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. “ciscoasa#”.

By default, all commands in ASA are either privilege level 0, 1 or 15. ASDM role-based control predefines three ASDM user roles – Level 15 (Admin), Level 5 (Read Only), and Level 3 (Monitor Only). We will use them in ISE policies and set them up later in ASDM Defined User Roles.

With EXEC authorization, an ASA 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. ISE may push these two attributes to customize it per-user:

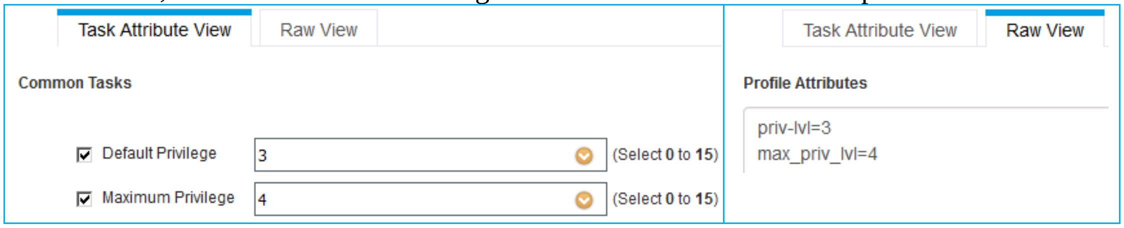
> Default Privilege: Specifies the initial (default) privilege level for the shell session. Authorized users land in this level instead of 1.
>
> Maximum Privilege: Specifies the maximum level permitted for the shell session. Authorized users can log in with a lower default level and use the enable command to move to a higher level, up-to the value assigned by this attribute. With external AAA servers, ASA allows enable to 15 only.

ASA Monitor Only

This is to restrict the user to the Home and Monitoring panes in ASDM.

Step 1 On the ISE Administrative Web Portal, go to **Work Centers** > **Device Administration** > **Policy Results** > **TACACS Profiles.** Add a new TACACS Profile and name it **ASA Monitor Only**.

Step 2 Scroll down to the **Common Tasks** section. Enable the Default Privilege with a value of 3 from the drop-down selector, and the Maximum Privilege with a value of 4 from the drop-down.



Common Tasks

☑ Default Privilege 3 (Select 0 to 15)

☑ Maximum Privilege 4 (Select 0 to 15)

Profile Attributes

priv-lvl=3
max_priv_lvl=4

Figure 6. TACACS Profile for ASA Monitor Only

The maximum privilege of 4 is for illustration only but not used in our case because ASA enable allows for 15 only when using an external AAA server.

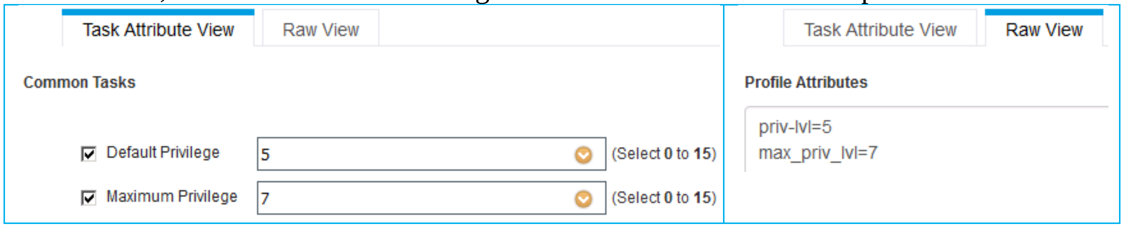
Step 3 Click **Submit** to save the profile.

ASA Read Only

This is to give the user read-only access in ASDM.

Step 1 Add a new TACACS Profile and name it **ASA Read Only**.

Step 2 Scroll down to the **Common Tasks** section. Enable the Default Privilege with a value of 5 from the drop-down selector, and the Maximum Privilege with a value of 7 from the drop-down.



Common Tasks

☑ Default Privilege 5 (Select 0 to 15)

☑ Maximum Privilege 7 (Select 0 to 15)

Profile Attributes

```
priv-lvl=5
max_priv_lvl=7
```

Figure 7. TACACS Profile for ASA Read Only

The maximum privilege of 7 is for illustration only but not used in our case because ASA enable allows for 15 only when using an external AAA server.

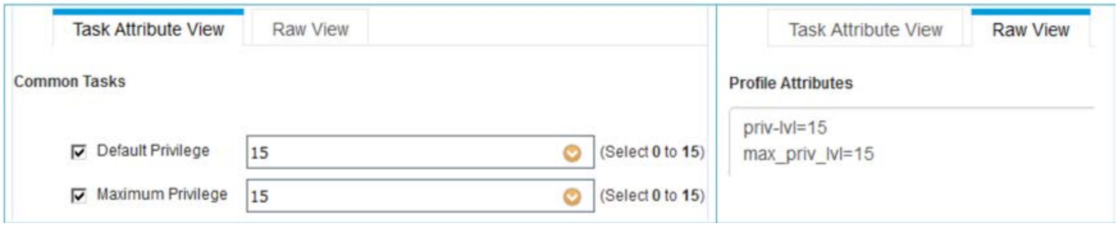
Step 3 Click **Submit** to save the profile.

ASA Admin

This is to grant unrestrictive access in ASDM.

Step 1 Add another profile and name it **ASA Admin**.

Step 2 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.



Common Tasks

☑ Default Privilege 15 (Select 0 to 15)

☑ Maximum Privilege 15 (Select 0 to 15)

Profile Attributes

```
priv-lvl=15
max_priv_lvl=15
```

Figure 8. TACACS Profile for ASA_Admin

The maximum privilege of 15 is used at ASA CLI when the user issues “enable” at the user EXEC mode.

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

TACACS Command Sets

ASA command authorization queries the configured TACACS+ server to verify whether the device administrators are authorized to issue the commands, regardless of the privilege levels.

We define four commands sets – HelpDesk_Commands, Permit_All_Commands, ASA Basic, and ASA_ReadOnly_Extra.

HelpDesk Commands

This is the same as that in the guide for IOS devices. Please skip this section if it already defined.

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	undebug	
PERMIT	traceroute	
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, 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 3 Click the check mark • at the end of each entry to keep the line.

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

Permit All Commands

This is the same as that in the guide for IOS devices. Please skip this section if it already defined.

Step 1 Add a new set and name it **Permit_All_Commands**.

Step 2 Tick the checkbox next to Permit any command that is not listed below ☑, and leave the command list empty.

Grant	Command	Argument

Step 3 Click **Submit** to persist the command set.

ASA Basic

Step 1 Add a new set and name it **ASA Basic**.

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

Grant	Command	Argument
PERMIT	show	checksum|curpriv|history|pager|version
PERMIT	enable	
PERMIT	help	
PERMIT	login	
PERMIT	logout	
PERMIT	pager	
PERMIT	clear	pager
PERMIT	quit	
PERMIT	exit	

The first entry demonstrates a list of acceptable arguments to follow the command **`show`**. It matches any of `show checksum`, `show curpriv`, `show history`, `show pager`, and `show version`.

Step 3 Click the check mark √ at the end of each entry to keep the line.
Step 4 Click **Submit** to persist the command set.

ASA ReadOnly Extra

Step 1 Add a new set and name it **ASA ReadOnly Extra**.
Step 2 Click ✚**Add** to configure entries to the set:

Grant	Command	Argument
PERMIT	more	
PERMIT	dir	
PERMIT	export	

Step 3 Click the check mark • at the end of each entry to keep the line.
Step 4 Click **Submit** to persist the command set.

Device Admin Policy Sets

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

ASDM is driven by menus and other graphical user-interface elements so ASDM access will need more commands allowed compared to ASA CLI.

We will define two policy sets – one to authorize for ASDM access and the other for the rest of ASA administrative access.

ASDM Authz

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

S	Name	Description	Conditions
√	ASDM Authz		DEVICE:Device Type EQUALS Device Type#All Device Types#Network Devices#Firewalls AND TACACS:Type EQUALS Authorization AND TACACS:Port EQUALS 443

Figure 9. Policy Set Condition for ASDM Authz

ASDM authorization requests are sent with 443 as the value for TACACS port when using the default HTTPS port. Update the value for this condition to the customized port if ASDM uses an alternative port.

Step 2 Create the Authentication Policy. For Authentication, we use the AD as the ID Store and will be used to identify the username in the authorization requests.

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

Figure 10. Authentication Policy for ASDM Authz

Step 3 Define the Authorization Policy. ASDM access is governed by the three pre-defined privilege levels so we will give Permit_All_Commands to all authenticated administrators for simplicity.

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	Permit_All_Commands	ASA Monitor Only
√	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	Permit_All_Commands	ASA Monitor Only
√	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	Permit_All_Commands	ASA Admin
√	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	Permit_All_Commands	ASA Admin
√	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	ASA Read Only

S	Rule Name	Conditions	Command Sets	Shell Profiles
√	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	ASA Read Only
√	Default	if no matches, then	DenyAllCommands	

Figure 11. Authorization Policy for ASDM Authz

ASA Regular

Step 1 Navigate to **Work Centers** > **Device Administration** > **Device Admin Policy Sets**. Select the existing policy set ***ASDM Authz*** and [Duplicate Below]. As the new policy set ranks below the previous, its conditions can be less specific. Update the duplicated copy and condition it solely on Device Type as below:

S	Name	Description	Conditions
√	ASA Regular		DEVICE:Device Type EQUALS Device Type#All Device Types#Network Devices#Firewalls

Figure 12. Policy Set Condition for ASA Regular

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 13. Authentication Policy for ASA Regular

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. ASA. The shell profiles are mainly for ASDM access and for ASA CLI with local command authorization on ASA.

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	ASA_Basic AND HelpDesk_Commands	ASA Monitor Only
√	HelpDesk East	DEVICE:Location CONTAINS All Locations#East_Coast AND	ASA_Basic AND HelpDesk_Commands	ASA Monitor Only

S	Rule Name	Conditions	Command Sets	Shell Profiles
		demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/East_Coast AND demoAD:ExternalGroups EQUALS securitydemo.net/DemoGroups/HelpDesk		
√	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	Permit_All_Commands	ASA Admin
√	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	Permit_All_Commands	ASA Admin
√	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	ASA_Basic AND HelpDesk_Commands AND ASA_ReadOnly_Commands	ASA Read Only
√	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	ASA_Basic AND HelpDesk_Commands AND ASA_ReadOnly_Commands	ASA Read Only
√	Default	if no matches, then	DenyAllCommands	

Figure 14. Authorization Policy for ASA Regular

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

ASA Configuration for TACACS+

Before configuring TACACS+, IP addressing and good remote connection protocols need first configured. The following exemplifies how to enable SSH for the ASA CLI access and HTTP for the ASDM access.

```
hostname ASAv
domain-name securitydemo.net

crypto key generate rsa modulus 2048 noconfirm

console timeout 0

interface Management0/0
 management-only
 nameif management
 security-level 100
 ip address 10.1.100.150 255.255.255.0
 no shutdown

route management 0.0.0.0 0.0.0.0 10.1.100.1 1

ssh 10.1.100.0 255.255.255.0 management
ssh timeout 30
ssh version 2

http server enable
http 10.1.100.0 255.255.255.0 management

username sec-admin password ISEisC00L privilege 15

aaa authentication ssh console LOCAL
aaa authentication enable console LOCAL
aaa authorization exec LOCAL auto-enable
```

Since the sample network device has a valid IP address at this stage, we can SSH to it 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.

Starting Version 9.5(1), ASA has separate routing table for management-only interfaces. We add a default route to connect the file server that is not in any connected subnet(s).

The *auto-enable* option for EXEC authorization was added in ASA Version 9.2(1) to make the enable behavior in ASA closer to Cisco IOS so that a device administrator with sufficient privileges needs not enter the password a second time.

To use ASDM, we would need to upload the ASDM binary to disk0: on ASA; for example,

```
copy http://a.web.file.server/path/to/asdm-752.bin disk0:/
```

If the Cisco ASDM-IDM Launcher not yet installed, use a web browser to go to https://10.1.100.150/admin and click either [Install ASDM Launcher] or [Run ASDM]. Without a global enable password, we may point the ASDM-IDM launcher to 10.1.100.150 and login either with empty username and password or use the local-admin credential.

TACACS+ AAA on a Cisco ASA 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

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

```
aaa-server demoTG protocol tacacs+
aaa-server demoTG (management) host 10.1.100.21
 key ISEisC00L

clear configure aaa

aaa authentication ssh console demoTG LOCAL
aaa authentication enable console demoTG LOCAL
aaa authentication http console demoTG LOCAL
aaa authentication secure-http-client
```

We have thus switched to TACACS+ to authenticate the access for SSH and ASDM. All successful logins using TACACS+ for SSH have the privilege level 1 and those for ASDM have the privilege level 15.

The “enable” authentication line is for all types of connections so both VTY and CONSOLE use TACACS+ to authenticate “enable” access. Only the administrators with 15 as the maximum privilege level are able to issue “enable” successfully, because AAA authentication for “enable” is carried out without argument and defaulted to 15.

In the events that the configured TACSACS+ server becomes unavailable, both login and enable authentications fall back to use the “local” user database. The users allowed to fall back access should have their local passwords synchronized with the external AAA server for transparent accesses.

Command Authorization

EXEC 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 authentication-server auto-enable
```

As noted previously, `auto-enable` is added in ASA 9.2(1) so skip this option if ASA running older codes. At this point, the shell profiles with the *default* privilege attribute apply to new SSH sessions.

Starting with Version 9.4(1) ASA separates the EXEC authorization for ASDM from the other types of connections, so we also add:

```
aaa authorization http console demoTG
```

Local Command Authorization

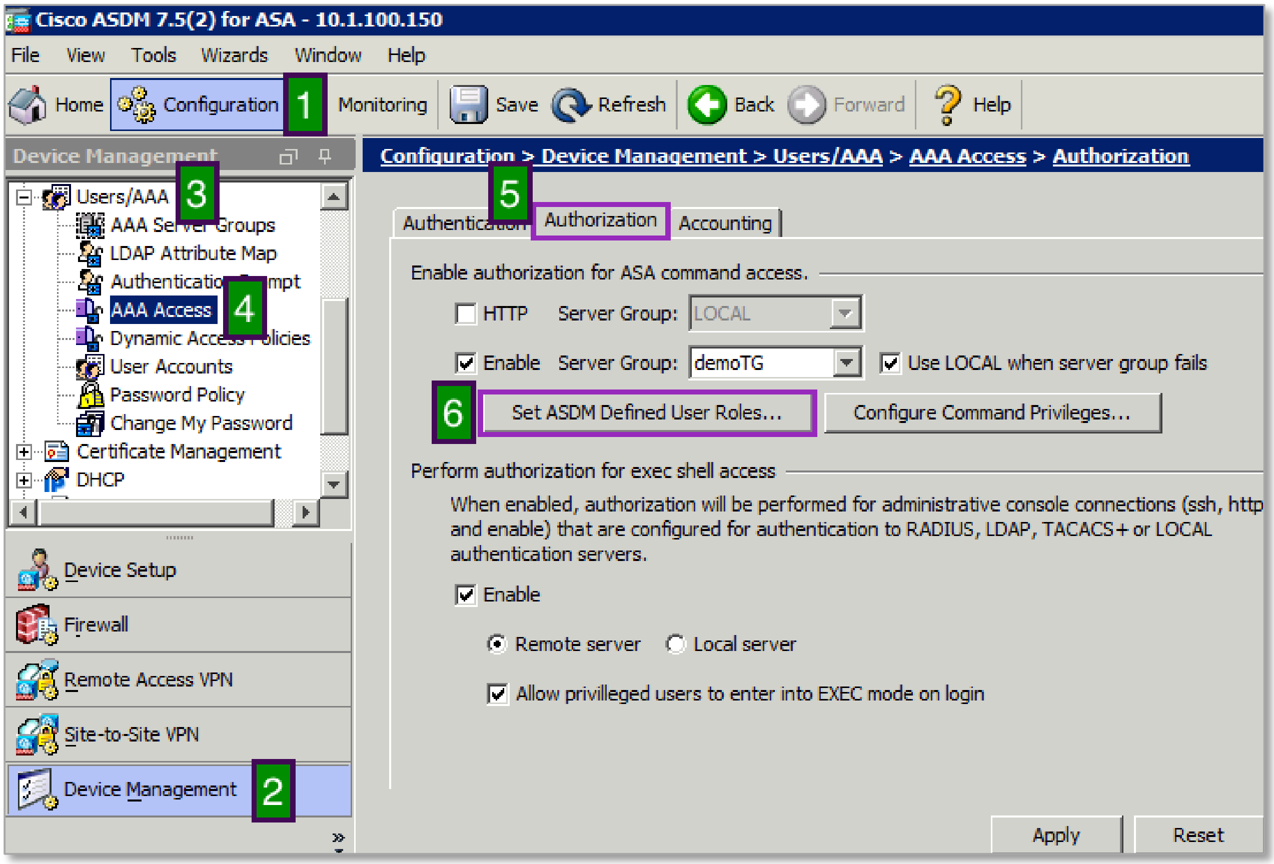
Local command authorization allows administrators to use the commands assigned to their privilege levels or below. It is configured as the following:

```
aaa authorization command LOCAL
```

ASDM Defined User Roles

ASDM Defined User Roles represent three privilege levels (3, 5, and 15) for ASDM access. To setup them up, ASDM reassigns commands to the three privilege levels. They are then used either in local command authorization directly or as the fall back for TACACS+ command authorization.

Login to ASDM as an ASA admin with full access, navigate to **Configuration** > **Device Management** > **Users/AAA** > **AAA Access** > **Authorization** and click on the button [Set ASDM Defined User Roles...]. Click [Yes] in the pop-up window **ASDM Defined User Roles Setup**.



Configuration > Device Management > Users/AAA > AAA Access > Authorization

Authentication | Authorization | Accounting

Enable authorization for ASA command access.

☐ HTTP Server Group: LOCAL

☑ Enable Server Group: demoTG ☑ Use LOCAL when server group fails

[Set ASDM Defined User Roles...] [Configure Command Privileges...]

Perform authorization for exec shell access

When enabled, authorization will be performed for administrative console connections (ssh, http and enable) that are configured for authentication to RADIUS, LDAP, TACACS+ or LOCAL authentication servers.

☑ Enable

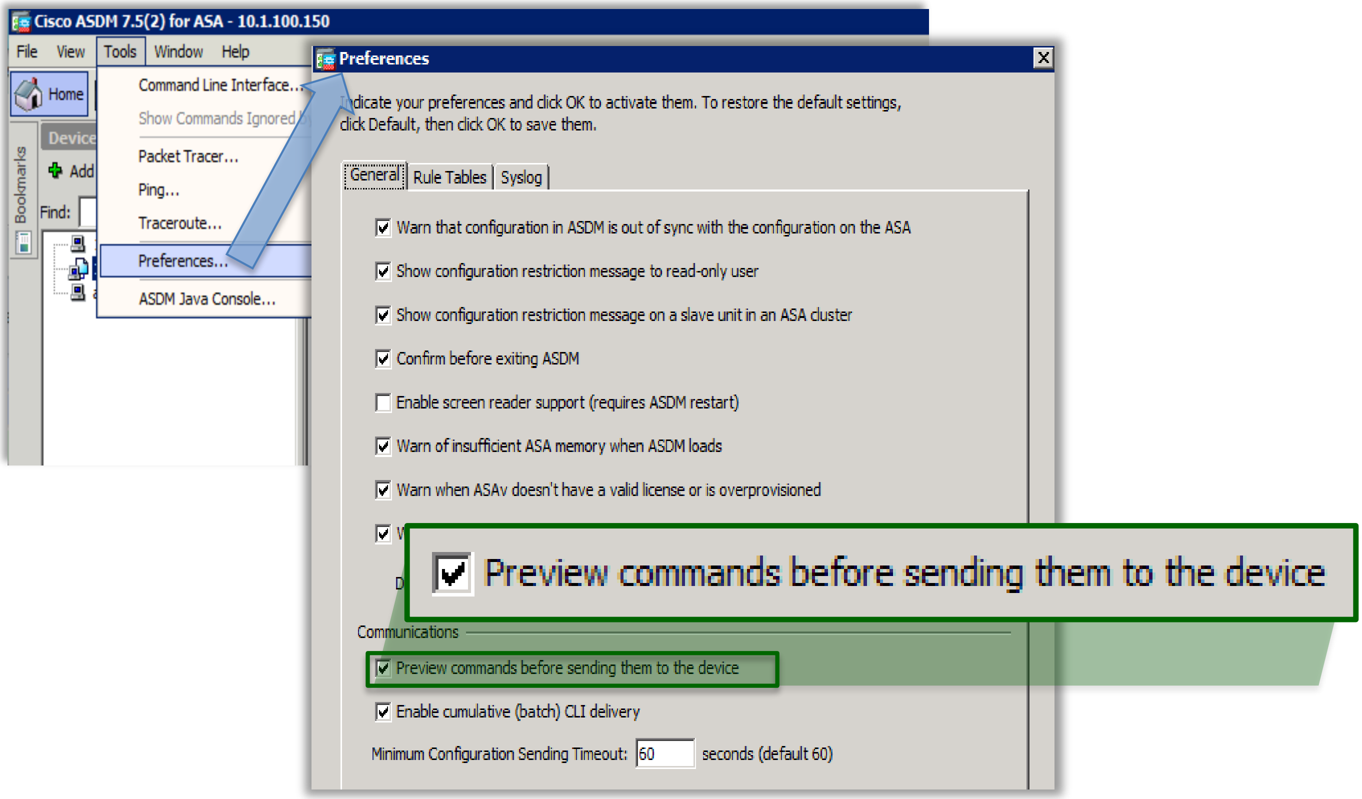
● Remote server ○ Local server

☑ Allow privilleged users to enter into EXEC mode on login

[Apply] [Reset]

Figure 15. Set ASDM Defined User Roles

To see the list of privilege commands configured for this, we may turn on the option [☑ Preview commands before sending them to the device] in the ASDM Preferences, as shown in Figure 16 below. Hit [Apply] to send the configuration to ASA and, if the preview option enabled, click [Send] in the ***Preview CLI Commands*** pop-up window.



Preferences

Indicate your preferences and click OK to activate them. To restore the default settings, click Default, then click OK to save them.

General | Rule Tables | Syslog

☑ Warn that configuration in ASDM is out of sync with the configuration on the ASA

☑ Show configuration restriction message to read-only user

☑ Show configuration restriction message on a slave unit in an ASA cluster

☑ Confirm before exiting ASDM

□ Enable screen reader support (requires ASDM restart)

☑ Warn of insufficient ASA memory when ASDM loads

☑ Warn when ASAv doesn't have a valid license or is overprovisioned

Communications

☑ Preview commands before sending them to the device

☑ Enable cumulative (batch) CLI delivery

Minimum Configuration Sending Timeout: 60 seconds (default 60)

Figure 16. ASDM Preference to Preview commands before sending to the ASA

TACACS+ Command Authorization

To use TACACS+ command authorization, configure the following:

```
aaa authorization command demoTG LOCAL
```

This overrides the lists available for each of the privilege levels and the command list from the TACACS+ server may include commands from higher privilege levels than the administrators’ current privilege levels.

TACACS+ Accounting

ASA may be enabled to log administrative user activities to a TACACS+ server group by

```
aaa accounting ssh console demoTG
aaa accounting serial console demoTG
aaa accounting enable console demoTG
```

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 command demoTG
```

This sends accounting messages for any commands, other than “show” commands. It can take an optional privilege keyword to specify the minimal privilege level; e.g. “`aaa accounting command privilege 3 demoTG`” will send command accountings for those in Level 3 or above, except for “show”.

We are done with the ASA configuration for TACACS+.

What’s Next?

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

Step 1 SSH and log into the ASA 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 ssh sessions
show asdm sesssions
show curpriv
```

A sample output is shown below:

```
ASAv# show ssh sessions

SID Client IP       Version Mode Encryption Hmac     State            Username
2   10.1.100.6      2.0     IN   aes256-ctr sha1     SessionStarted   hellen
                            OUT  aes256-ctr sha1     SessionStarted   hellen
ASAv# show asdm sessions
0 10.1.100.6
AASAv# show curpriv
Username : hellen
Current privilege level : 3
Current Mode/s : P_PRIV
...
```

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

```
debug aaa common
debug tacacs
```

Here is a sample debug output:

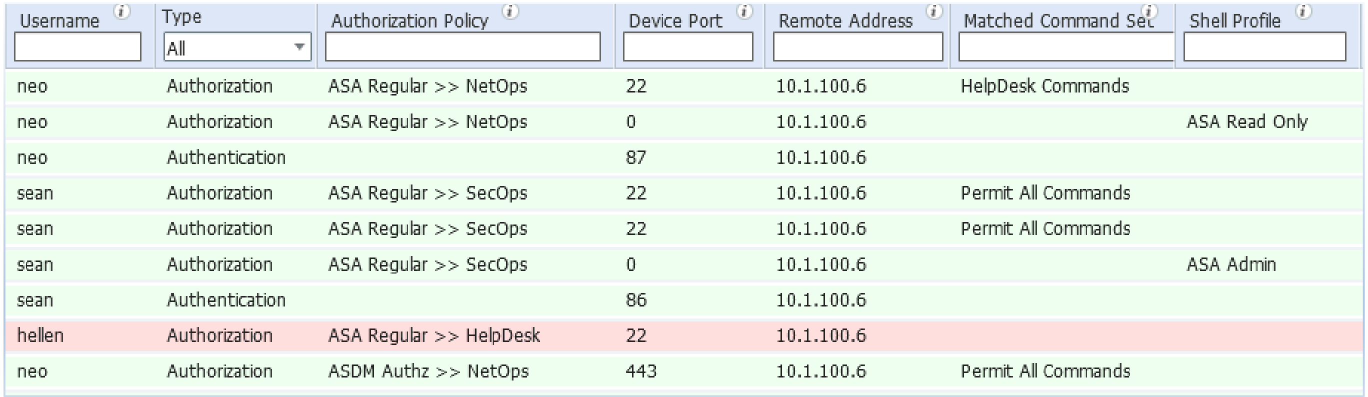
```
mk_pkt - type: 0x1, session_id: 495
 user: neo
 Tacacs packet sent
Sending TACACS Start message. Session id: 495, seq no:1
Received TACACS packet. Session id:1117437566  seq no:2
tacp_procpkt_authen: GETPASS
mk_pkt - type: 0x1, session_id: 495
mkpkt_continue - response: ***
 Tacacs packet sent
Sending TACACS Continue message. Session id: 495, seq no:3
Received TACACS packet. Session id:1117437566  seq no:4
tacp_procpkt_authen: PASS
TACACS Session finished. Session id: 495, seq no: 3

mk_pkt - type: 0x2, session_id: 496
mkpkt - authorize user: neo
 Tacacs packet sent
Sending TACACS Authorization message. Session id: 496, seq no:1
Received TACACS packet. Session id:63315798  seq no:2
tacp_procpkt_author: PASS_ADD
tacp_procpkt_author: PASS_REPL
```

```
Attributes = priv-lvl
TACACS Session finished. Session id: 496, seq no: 1

mk_pkt - type: 0x2, session_id: 498
mkpkt - authorize user: neo
cmd=ping
cmd-arg=10.1.1.255  Tacacs packet sent
Sending TACACS Authorization message. Session id: 498, seq no:1
Received TACACS packet. Session id:244563180  seq no:2
tacp_procpkt_author: FAIL
TACACS Session finished. Session id: 498, seq no: 1
...
```

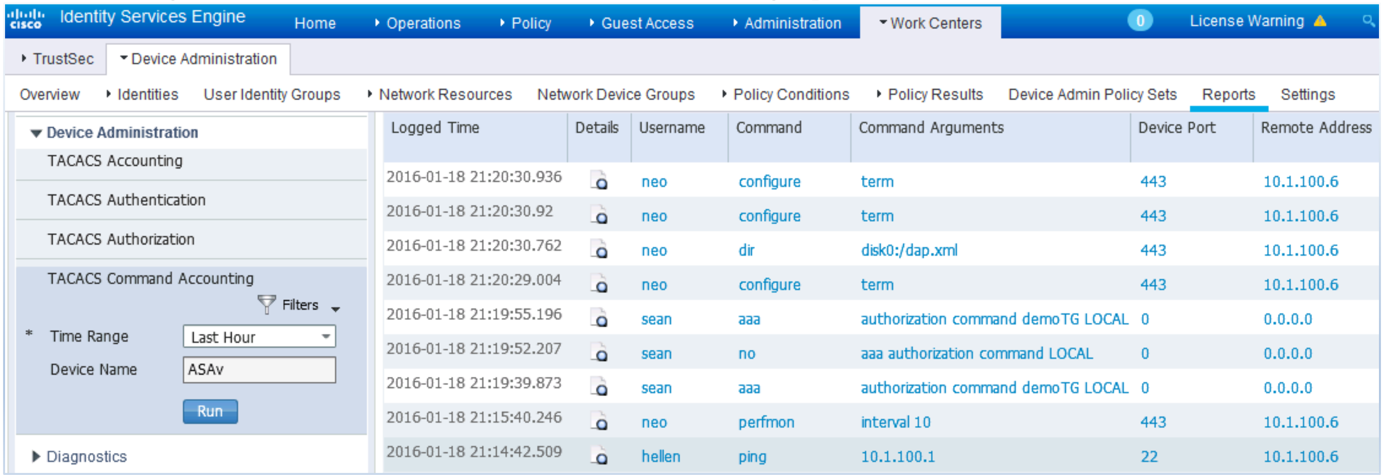
Step 5 From the ISE GUI, navigate to **Operations** > **TACACS Livelog**. All the TACACS authentication and authorization requests are captured here, and the details button provides detailed information about why a particular transaction passed/failed.



Username	Type	Authorization Policy	Device Port	Remote Address	Matched Command Sec	Shell Profile
	All					
neo	Authorization	ASA Regular >> NetOps	22	10.1.100.6	HelpDesk Commands	
neo	Authorization	ASA Regular >> NetOps	0	10.1.100.6		ASA Read Only
neo	Authentication		87	10.1.100.6		
sean	Authorization	ASA Regular >> SecOps	22	10.1.100.6	Permit All Commands	
sean	Authorization	ASA Regular >> SecOps	22	10.1.100.6	Permit All Commands	
sean	Authorization	ASA Regular >> SecOps	0	10.1.100.6		ASA Admin
sean	Authentication		86	10.1.100.6		
hellen	Authorization	ASA Regular >> HelpDesk	22	10.1.100.6		
neo	Authorization	ASDM Authz >> NetOps	443	10.1.100.6	Permit All Commands	

Figure 17. TACACS Livelogs

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



* Time Range: Last Hour

Device Name: ASAv

Logged Time	Details	Username	Command	Command Arguments	Device Port	Remote Address
2016-01-18 21:20:30.936		neo	configure	term	443	10.1.100.6
2016-01-18 21:20:30.92		neo	configure	term	443	10.1.100.6
2016-01-18 21:20:30.762		neo	dir	disk0:/dap.xml	443	10.1.100.6
2016-01-18 21:20:29.004		neo	configure	term	443	10.1.100.6
2016-01-18 21:19:55.196		sean	aaa	authorization command demoTG LOCAL	0	0.0.0.0
2016-01-18 21:19:52.207		sean	no	aaa authorization command LOCAL	0	0.0.0.0
2016-01-18 21:19:39.873		sean	aaa	authorization command demoTG LOCAL	0	0.0.0.0
2016-01-18 21:15:40.246		neo	perfmon	interval 10	443	10.1.100.6
2016-01-18 21:14:42.509		hellen	ping	10.1.100.1	22	10.1.100.6

Figure 18. TACACS Reports