|  |
| --- |
| Aston Technologies Inc. |
| Cisco Identity Services Engine (ISE) Device Administration |
| An Aston training document explaining how to deploy Device Administration with Cisco ISE |

Contents

[Contents 2](#_Toc493510420)

[Introduction 3](#_Toc493510421)

[Lab Diagram 4](#_Toc493510422)

[ISE Configuration 5](#_Toc493510423)

[Device TACACS Configuration 11](#_Toc493510424)

[ISE-CORE-SWITCH Configuration 11](#_Toc493510425)

[ISE-ACCESS-SWITCH Configuration 14](#_Toc493510426)

[ISE-ASA Configuration 15](#_Toc493510427)

[WLC Configuration 19](#_Toc493510428)

[Conclusion 22](#_Toc493510429)

Introduction

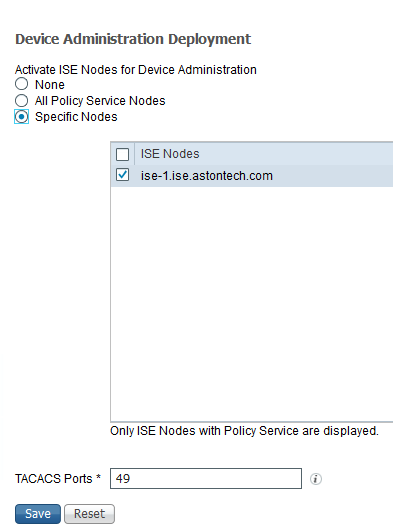
In this lab, we will walk through the process of configuring device administration using TACACS. This is a new(er) feature that was released in ISE 2.0. There has been a lot of debate among engineers if adding TACACS to ISE was a good idea but the majority of customers demanded it since they wanted to completely replace ACS. In a large environment, it might be a good idea to have a separate ISE PSNs or deployment for Device Administration but here in our lab environment it will be a nonissue. Let’s get started.

Lab Diagram

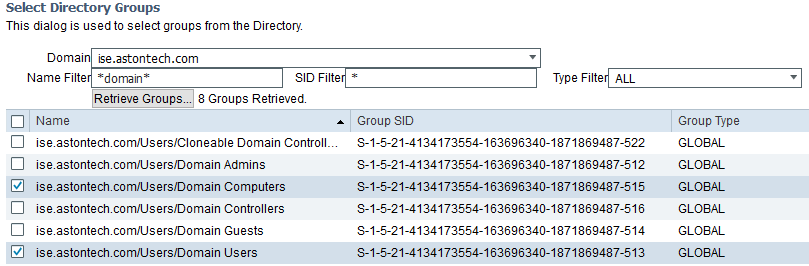


ISE Configuration

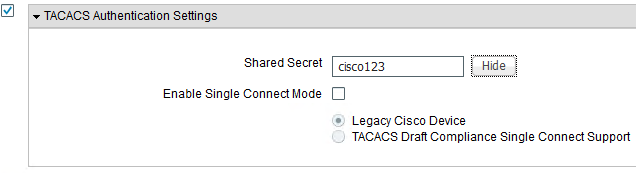
First thing we need to do is to enable Device Administration in ISE. Go to **Work Centers > Device Administration > Overview > Deployment**. Click on **All Policy Service Nodes** or **Specific Nodes**. It really doesn’t matter since we only have one node at this point. Then **Save**.



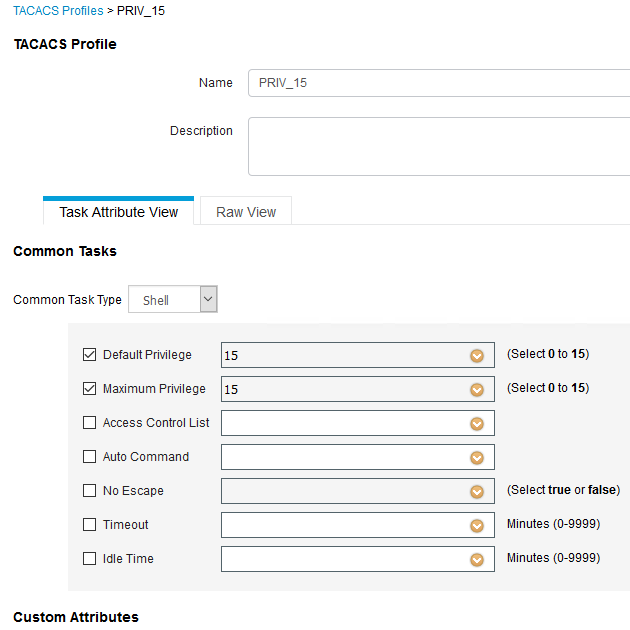
Go to **Ext ID Sources > Active Directory > ASTON-AD > Groups** and add the **Domain Users** group. We are going to pretend that group is for our Network Support team.



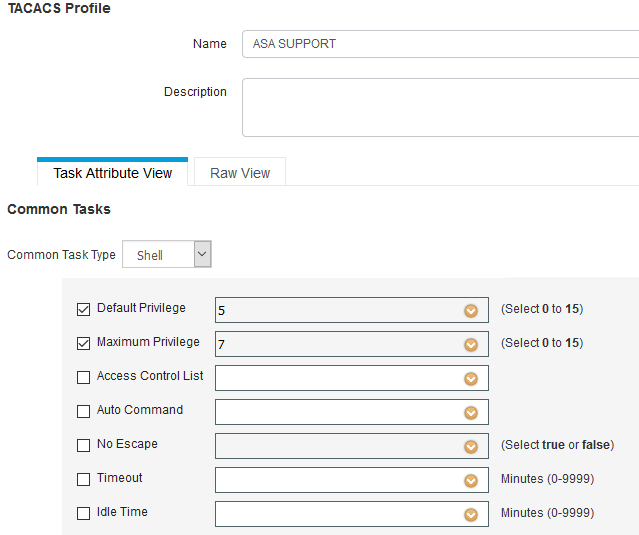
Next head over to **Network Resources > Network Devices**. We have our devices configured for RADIUS but now we need to add TACACS. Go into each of the network devices and click the **TACACS** checkbox and add the Shared Secret – **cisco123** then **Save**.



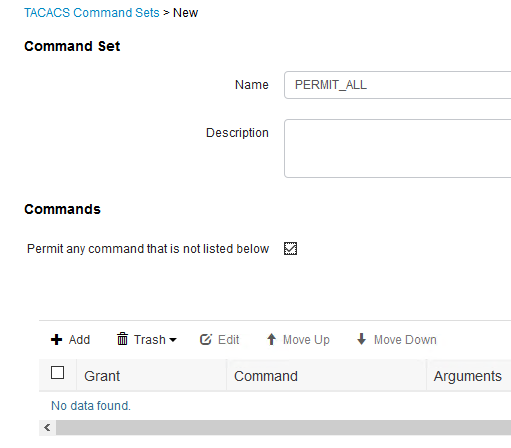
Once that’s done go to **Policy Elements > Results > TACACS** **Profiles**. When it comes to the WLC they have made this super easy. They already have what we need configured by default. We are going to create a profile to give Shell access at privilege level 15. Click **Add**. Name it **PRIV\_15** then set the **Default Privilege** and **Maximum Privilege** to **15**. Hit **Save**.



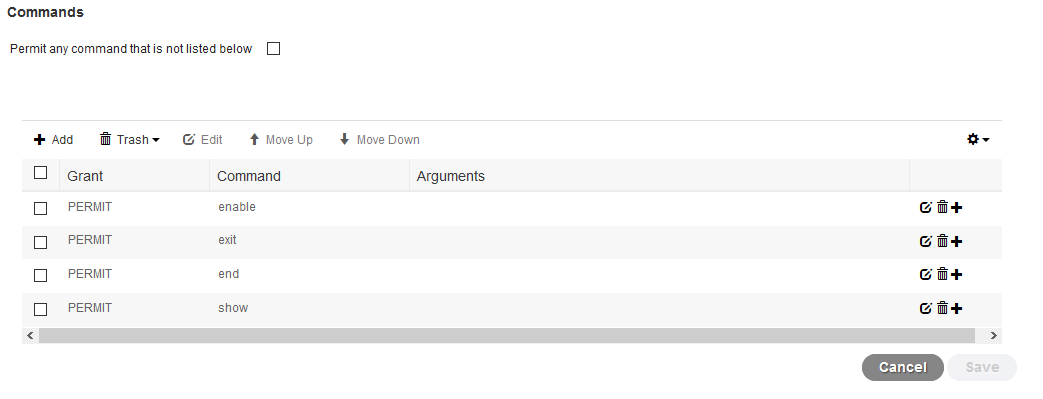
For the ASA, we’ll need to create a profile that we can use for the Network Support team for both CLI and ASDM. Create another Profile and name it **ASA SUPPORT**. Give a **Default Privilege** of **5** and **Maximum** of **7**. Then hit **Save**.



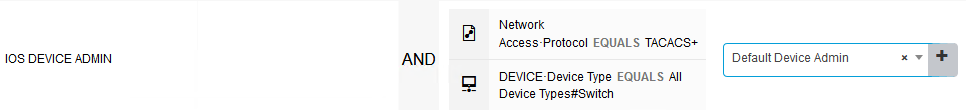
Next let’s create a few Command Sets. One to permit all commands and another to permit only show commands. Click **Add**. Name the first one **PERMIT\_ALL**. Click the checkbox that says **Permit any command that is not listed below** and hit **Submit**.



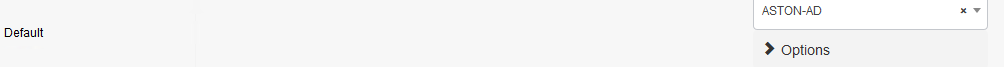
Next Add another Command set to allow only show commands. Name it **SHOW\_COMMANDS\_ONLY**. Add in the commands **PERMIT show, exit, end** and **enable** then hit **Submit**.



It’s time to create our policies. Go to **Device Admin** **Policy Sets**. Click the **Plus sign**. Name it **IOS Device Admin** for conditions add **Network Access:Protocol EQUALS TACACS+** AND **DEVICE: Device Type EQUALS all Device Types#Switch**. We don’t really need to call out the protocol in the selection rules since ISE does that automatically but we’ll add it just for fun. Set the **Allowed Protocols** to **Default Device Admin**.

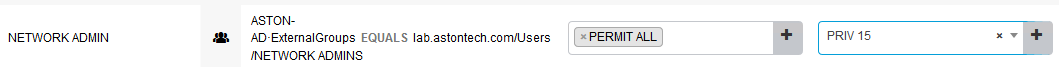


For Authentication Policy since we are just using AD for an Identity Source let’s change that to **ASTON\_AD**. Everything else can stay default.

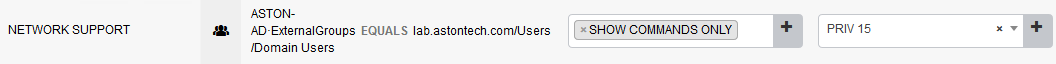


For the Authorization Policy, we are going to create a rule for Network Admins that have full access to all the devices and one to allow only Show commands for our Network Support team. Like I mentioned before we are going to pretend that our Domain User group is the Network Support group.

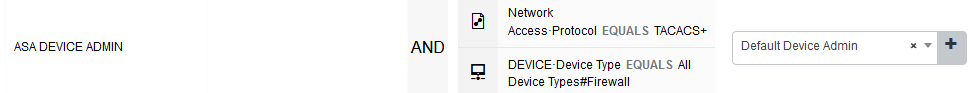
Click on the **Tacacs\_Default** policy and **Insert New Rule Above**. Name it **NETWORK ADMIN**. We want to match on our **Network Admins** AD group. For command sets **– PERMIT\_ALL** and Shell Profiles – **PRIV\_15**.



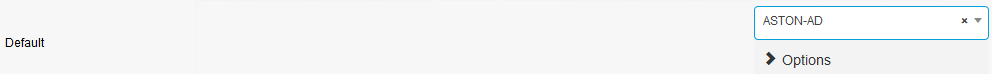
Let’s Duplicate that rule below and edit it. Change the name to **NETWORK SUPPORT**. Change the AD group to **Domain Users** the command set to **SHOW\_COMMANDS\_ONLY** and keep **PRIV\_15** as the Shell Profile.



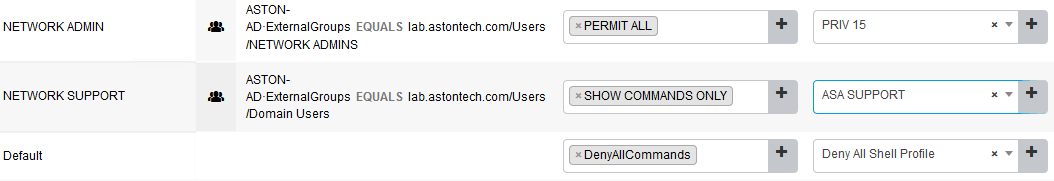
Now we are going to do pretty much the same thing for ASA. Add a new Policy Set and Name **it ASA Device Admin**. Conditions are going to be **Network Access:Protocol Equals TACACS+ AND DEVICE: Device Type Equals All Device Types#Firewall**.



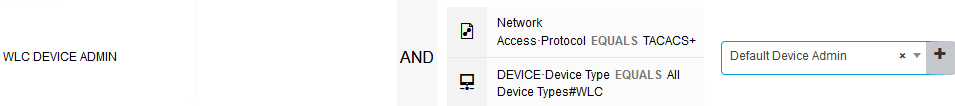
Change the Authentication Policy to use **ASTON-AD**.



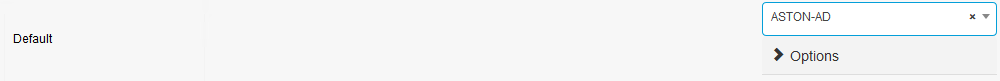
For the Authorization Policy, it’s going to be pretty much the same thing as with the IOS Policy Set except for the support rule will get the **ASA SUPPORT** Shell Profile.



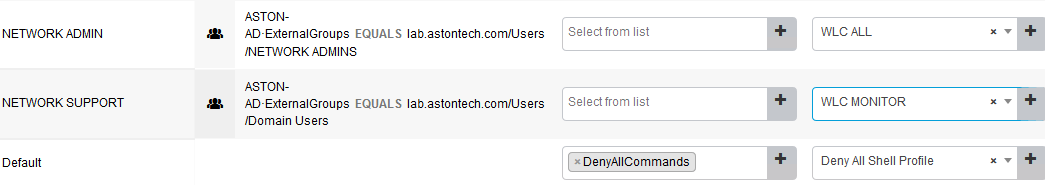
Now for the WLC. Create a new Policy Set and name it **WLC Device Admin**. Add the following configuration.



For the Authentication Policy change the Identity source to **ASTON-AD**.



For the Authorization Policy create two policy as we did before except this time we aren’t going to specify a Command Set. For the **Network Admin** rule the shell profile is going to be **WLC ALL**, which is full access. The Network Support rule will get **WLC MONITOR** which is read only.



Device TACACS Configuration

ISE-CORE-SWITCH Configuration

Let’s start with the core switch since we haven’t configured any AAA on that switch yet. Log into the core switch with the username **admin** and password **cisco**.

First thing we need to do is to enable AAA new-model.

aaa new-model

Next is to configure ISE as a TACACS server.

tacacs server ISE

address ipv4 172.16.100.50

key cisco123

Then we’ll create a server group for TACACS.

aaa group server tacacs+ ISE-TAC

server name ISE

We want to specify a source interface to send the TACACS requests from which is the address we added to ISE.

ip tacacs source-interface Loopback0

For this lab, we don’t want to use ISE authentication for console access. Let’s create a method list so that we use local creds instead.

aaa authentication login CONSOLE local

!

line con 0

login authentication CONSOLE

Now for everything else we want to use ISE to authenticate our users and if ISE is unavailable we want to fall back to local credentials.

aaa authentication login default group ISE-TAC local

When we sign into this switch we want to drop into whatever Privilege level we have configured ISE to give to the user.

aaa authorization exec default group ISE-TAC local

To enforce our command sets we need to add a few commands. The second one to enable command authorization and the first one to authorize commands that are run from privilege level 15. You will need to log out and back in with your AD creds after running these commands.

aaa authorization commands 15 default group ISE-TAC local

aaa authorization config-commands

The last couple AAA commands are to send accounting start-stop messages to ISE. So when someone logs in and out and when commands are run accounting messages will be sent to ISE.

aaa accounting exec default start-stop group ISE-TAC

aaa accounting commands 15 default start-stop group ISE-TAC

Here is the whole config:

aaa new-model

!

tacacs server ISE

address ipv4 172.16.100.50

key cisco123

!

!

aaa group server tacacs+ ISE-TAC

server name ISE

!

ip tacacs source-interface Loopback0

!

aaa authentication login default group ISE-TAC local

aaa authentication login CONSOLE local

aaa authorization exec default group ISE-TAC local

aaa authorization commands 15 default group ISE-TAC local

aaa authorization config-commands

aaa accounting exec default start-stop group ISE-TAC

aaa accounting commands 15 default start-stop group ISE-TAC

!

!

line con 0

login authentication CONSOLE

!

end

Test your access to the core switch with your AD account. You should have unrestricted access to the device. For the testing the Network support rule. Add a Domain User to test with - **user1** with a password of **qwe123$!**. That user should only be able to run show commands.



Check the ISE TACACS live logs and see what’s happening with each user.

ISE-ACCESS-SWITCH Configuration

We’ll have pretty much the same config on the Access switch so I’m not going to walk through each command. The only difference is that we’ll be removing the method list that we added previously for local authentication. Here is the config for the Access switch:

Conf t

!

tacacs server ISE

address ipv4 172.16.100.50

key cisco123

!

aaa group server tacacs+ ISE-TAC

server name ISE

!

ip tacacs source-interface Loopback0

!

line vty 0 15

no login authentication VTY

!

no aaa authentication login VTY local

no aaa authorization exec VTY local

!

aaa authentication login default group ISE-TAC local

aaa authorization exec default group ISE-TAC local

aaa accounting exec default start-stop group ISE-TAC

aaa accounting commands 15 default start-stop group ISE-TAC

!

aaa authorization commands 15 default group ISE-TAC local

aaa authorization config-commands

!

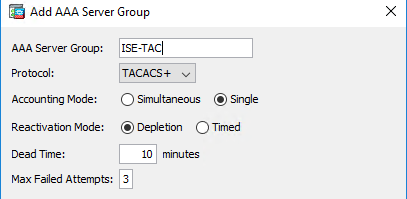
end

Test again with your AD creds and the user account to make sure that the results are as expected.

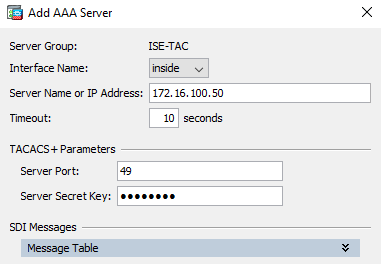
ISE-ASA Configuration

Login to the ASA. You can do this with ASDM or CLI whichever you prefer, I’ll cover both. Username is **admin** and the password is **cisco**. There is no enable password if you are configuring via CLI.

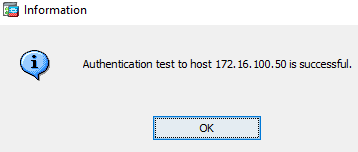
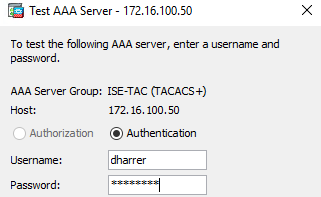
First, we’ll do ASDM. Go to **Configuration > Device Management > Users/AAA > AAA Server Groups** and click **Add.** Name the group **ISE-TAC** and change the protocol to **TACACS+** and hit **OK**.



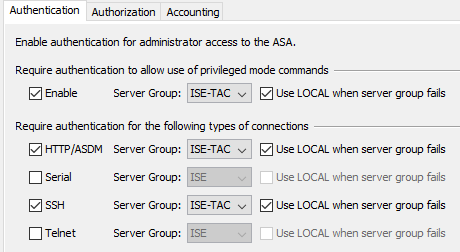
Then down in the box that says **Servers in the Selected Group** hit **Add**. The interface will be the **inside** add the ISE server’s IP address (172.16.100.50) and Secret Key of **cisco123**. Then hit **OK** and **Apply**.



Hit the Test button and do a quick test with your creds and make sure you can communicate with ISE.

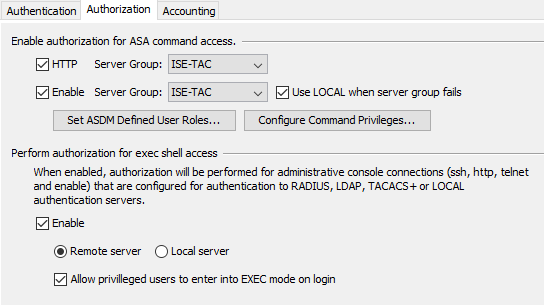


Go to **Configuration > Device Management > Users/AAA > AAA Access > Authentication** and configure the following settings and **Apply**:

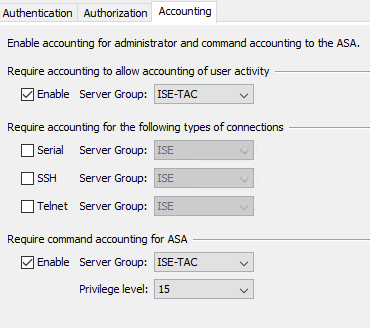


**Log out** of ASDM and sign in with your AD creds.

After signing back in go back to **AAA Access** configuration then to the **Authorization** tab and configure the following:



Lastly go to the **Accounting** tab and configure the following then hit **Apply**:



Here is the CLI config:

!

aaa-server ISE-TAC protocol tacacs+

!

aaa-server ISE-TAC (inside) host 172.16.100.50

key cisco123

!

!

aaa authentication enable console ISE-TAC LOCAL

no aaa authentication http console LOCAL

aaa authentication http console ISE-TAC LOCAL

no aaa authentication ssh console LOCAL

aaa authentication ssh console ISE-TAC LOCAL

aaa authorization http console ISE-TAC

aaa authorization exec authentication-server

aaa accounting enable console ISE-TAC

aaa accounting command privilege 15 ISE-TAC

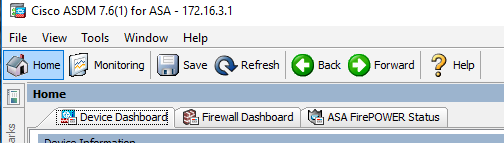
aaa authorization command ISE-TAC LOCAL

!

Now that we have the ASA configured. Let’s test access level for the CLI and ASDM. Log into the ASA via CLI with your AD account. You should have unrestricted access to run any command. Test with the user1 account. You should only have access to run show commands.

Login to ASDM. If you configured your AAA with ASDM we know that your account has full access since we were able to apply the authorization commands but we can test anyways. Try making a change to something inconsequential like configuring one of the interfaces that we aren’t using.

If that’s successful, log out of ASDM and sign in with the user1 account. Now you’ll notice that the configuration tab is gone.

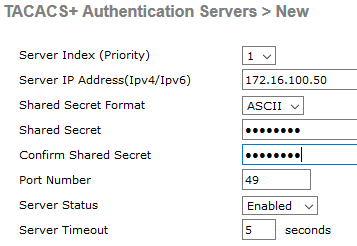


WLC Configuration

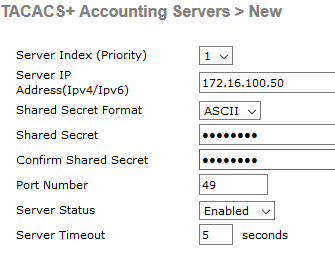
Open a web browser and go to <https://wlc.ise.astontech.com/> and log in with username admin and password qwe123$!. Hit the Advanced tab in the upper right corner.



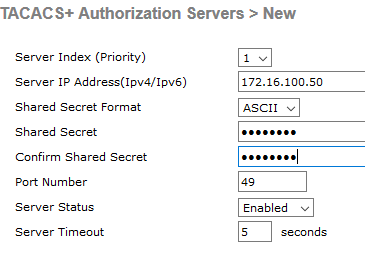
Go to **Security > AAA > TACACS+ > Authentication** and hit **New**. Configure the following with the Shared Secret being **cisco123**:



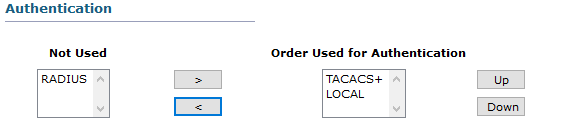
Same thing for **Accounting**:



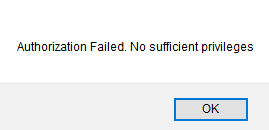
Same for Authorization:



Now we need to change the Priority Order. Go to **Priority Order > Management User**. Add **TACACS+** to the list, move it to the top and remove **RADIUS**. Then hit **Apply**.



Now let’s test this out. Log out of your current session and login back in with your AD creds. You should have full access to the WLC. Try adding another Accounting TACACS+ server and then delete it. If that is working log out again and sign in with the user1 account and try the same thing. You should get an Authorization Failed message.



Check the ISE Live Logs and take a look at what got applied when you authenticated for each user.

Conclusion

In this lab, we have:

* Enabled Device Administration in our ISE deployment
* Added our Domain Users group to simulate our Network Support team
* Configured TACACS for our Network Devices in ISE
* Created TACACS Profiles for Shell Access
* Configured our TACACS Command Sets
* Configured our Device Admin Policy Sets for our device types:
  + ASA
  + IOS Switches
  + WLC

In the next lab, we are going to cover Remote Access VPN via Anyconnect and the ASA.