ISE Setup Guide

Any Internet Protocol (IP) addresses domain names, and phone numbers used in this document are not intended to be actual domains, addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are

shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The following VM settings are based on Evaluation requirements final destination requirements have yet to be determined

Create a new VM, customizing the settings below for your platform needs:

VMware

Compatibility: ESXi 6.5 virtual machine or greater

Guest OS Family: Linux

Guest OS Version: Red Hat Linux Enterprise 7 (64-Bit)

16 CPUs (Cores) (8 was used in a lab with cores per socket 1)

16 GB Memory

300 GB Thick Provision Lazily Zeroed

Network Adapter Type: (to be determined)

Connect CD/DVD to ISE Install ISO on datastore

Install ISE

Select 1 at boot: menu to install ISE using Cisco ISE Installation (Keyboard/Monitor)

Wait for the installation to complete (~20 mins)

The VM will reboot automatically upon completion

A Login prompt will appear. Type **Setup** and press **Enter**

Enter the following information as prompted, adjusting **bold** items to your site needs

Enter hostname[ ]: **ISE01**

Enter IP address[ ]: **10.0.0.4**

Enter IP netmask[ ]: **255.255.255.0**

Do you want to configure IPv6 address ?: **N**

Enter IP default gateway[]:**10.0.0.4**

Enter Default DNS Domain: **YourDomain.com**

Enter Primary nameserver[ ]: **10.0.0.2**

Add secondary nameserver? Y/N [N: **Y**

Enter NTP server[time.nist.gov]: **10.0.10.1**

Add another NTP server? Y/N [N]: **N**

Enter system timezone[UTC]: **PST8PDT** or **UTC**

Enable SSH service ?Y/N [N]: **Y**

Enter username [admin]:**admin**

Enter password: -note that nothing will appear on the screen

Enter password again:

The password must be a minimum of six characters in length and include at least one lowercase letter (a–z), one uppercase letter (A–Z), and one numeral (0–9).

Setup will continue for another 15 minutes and will restart the server

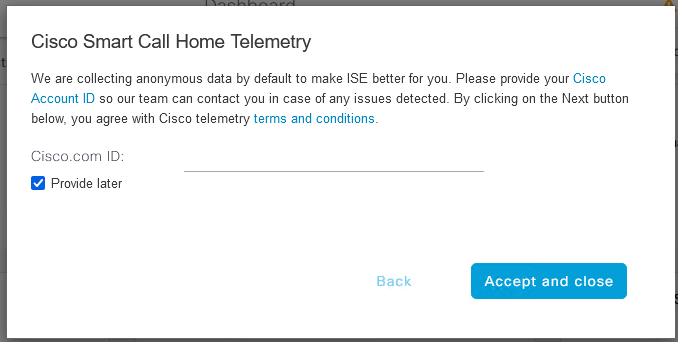
After setup completes run the command s*how application status ise* and verify Application Server is running before proceeding to the next step   
NOTE: This can take another 10 minutes or so

Once Application server is running open a browser and go to https://10.0.0.4/admin   
replace 10.0.0.4 with the IP address you used during setup

Accept any Risks or messages like “Warning: Potential Security Risk Ahead” this is due to ISE having its own self assigned certificate that we will fix this later. Click Advanced , then Accept the Risk and Continue

Login using the username and password used during setup

For the message “Cisco Smart Call Home Telemetry” check the box for **Provide Later, Next** then click the **Accept and Close**



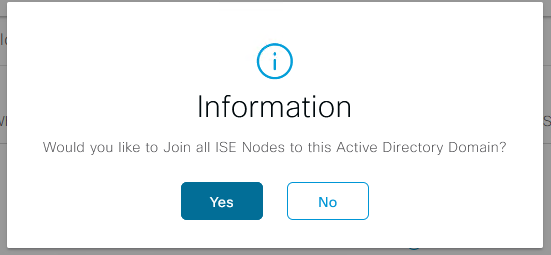
Join ISE to Active Directory Domain

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration > Identity Management > External Identity Sources > Active Directory**

Click **Add**

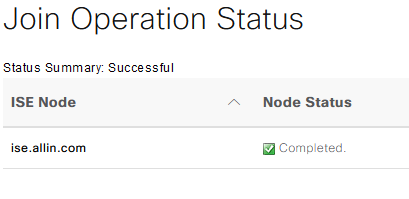
Enter your domain name in both the **Join Point Name** and **Active Directory Domain** boxes then click **Submit**

  
For the question: “**Would you like to join all ISE nodes to this Active Directory Domain?”**Click **Yes**



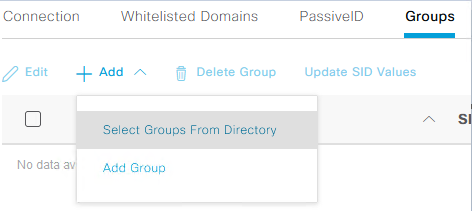
Put in Credentials\* > Then click **OK.***\*These credentials need the permission to search AD, Add workstation to a domain, and set attributes on a new machine account*Note: As for **Store Credentials** you would use this if you wanted to save the credentials for joining other ISE nodes.

Wait a moment after hitting OK and you should see a status message if it was successful or not: Node Status should be green for your domain if successful.

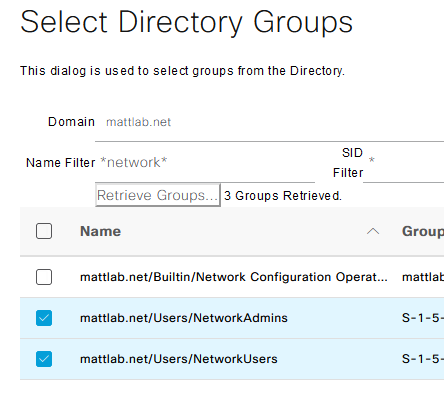
  
Add Active Directory Groups to ISE

At the same screen you were at to join AD, click the groups tab **Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration > Identity Management > External Identity Sources > Active Directory> “domain entry you created” > Groups**

Click **+Add**> **Select Groups from Directory**



In **Filter** put: **\*network\*** and click **Retrieve Groups**

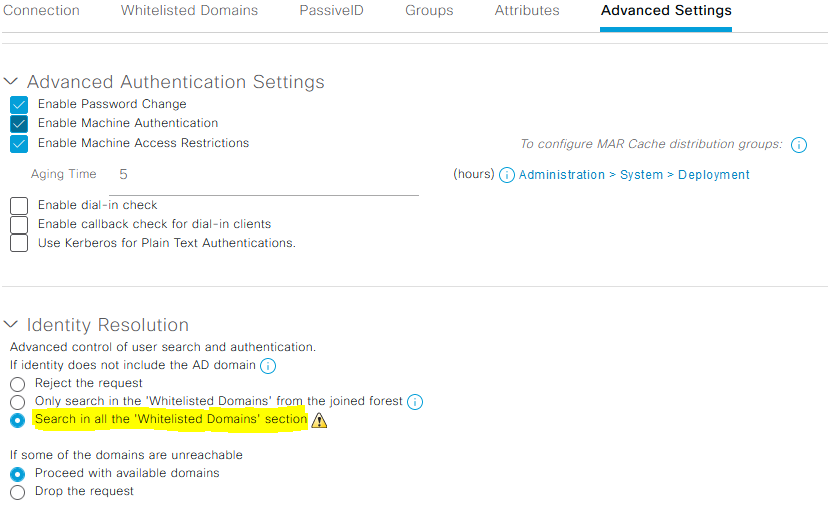


A list of AD groups will populate then **check the boxes** next to the Network Groups, then click **OK,** then **Save**

Set Identity Resolution Settings for Domain

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration >Identity Management > External Identity Sources > Active Directory > “domain entry you created” >Advanced Settings**

Check **“Search in all the 'Whitelisted Domains' section”** then **Save**



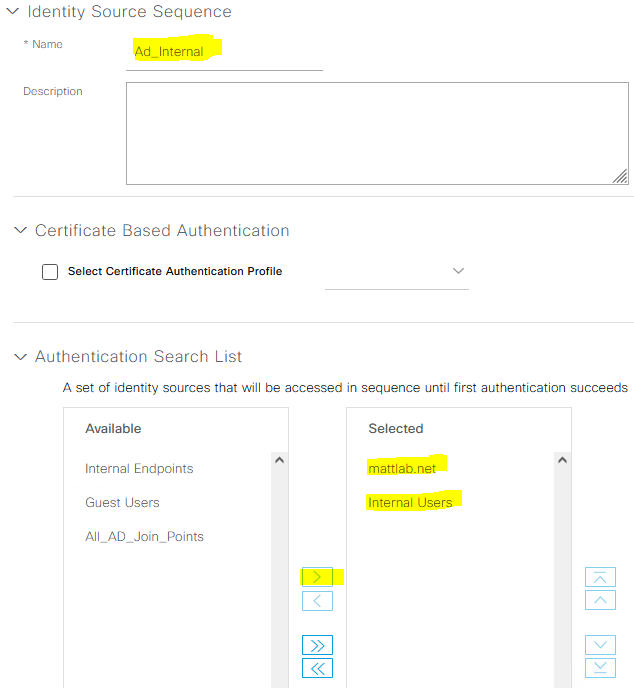
Create Identity Source Sequence

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration >Identity Management > Identity Source Sequences**

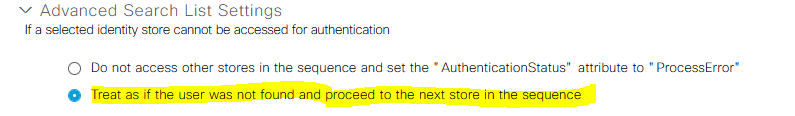
Click **Add**

Give your Identity Source Sequence a name, optional description, using the arrows add your AD join point such as “AD\_Internal” and “Internal Users” with AD being at the top of the list

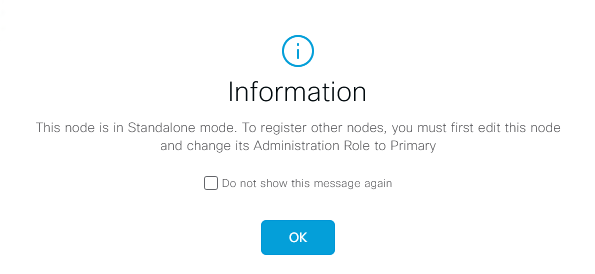
Click **Submit**



Select the option to **Treat as if the user was not found and proceed to the next store in the sequence**



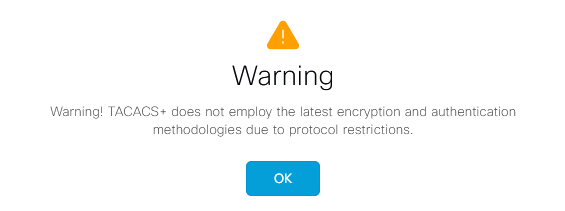
Enable TACACS for admin access

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration > System > Deployment** and Click **OK** to the informational message regarding standalone mode

Check the box next to your ISE Server and click **Edit**

Check box for **Enable Device Admin Service,** then **Save**

Click OK to “*Warning! TACACS+ does not employ the latest encryption and authentication methodologies due to protocol restrictions.”*

  
Network Device Groups

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Work Centers > Device Administration > Network Resources > Network Device Groups**

Click **Add**

Enter a name and optional description and set **Parent Group** to **All Device Types**

Click **Save**

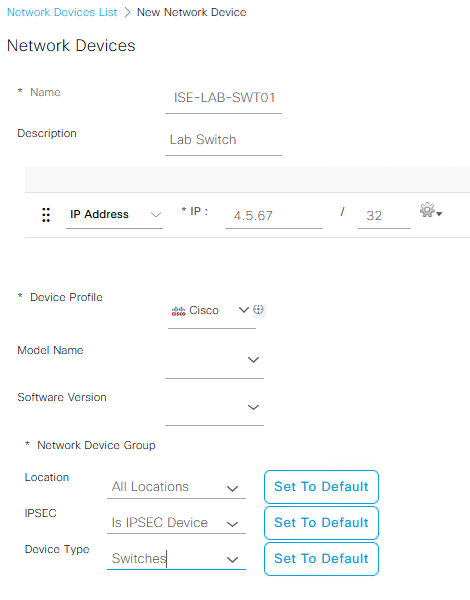
Add Devices to ISE

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Work Centers > Device Administration > Network Resources > Network Devices**

Click **Add**

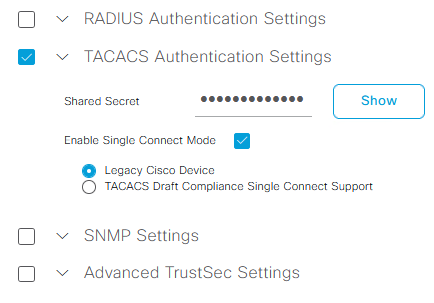
Note: you can add devices individually, by subnet or setup a profile to match all devices the below is how to add individually:

Enter a name, optional description, IP address, location (if applicable) and select the device type from the drop down



Check boxfor **TACACS Authentication and put in the password,** this will be the same password used for AAA on switches, routers and Firewalls

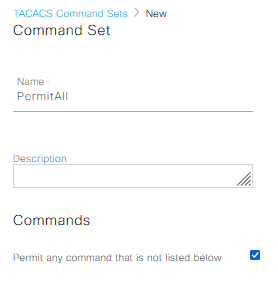
Check **Enable Single Connect Mode**

click **Save**

Define TACACS Command sets

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Work Centers >Device Administration > Policy Elements > Results > TACACS Command Sets**  
Click **Add** and name it **PermitAll** and check the box for **“Permit any command that is not listed below”**

Click **Submit**

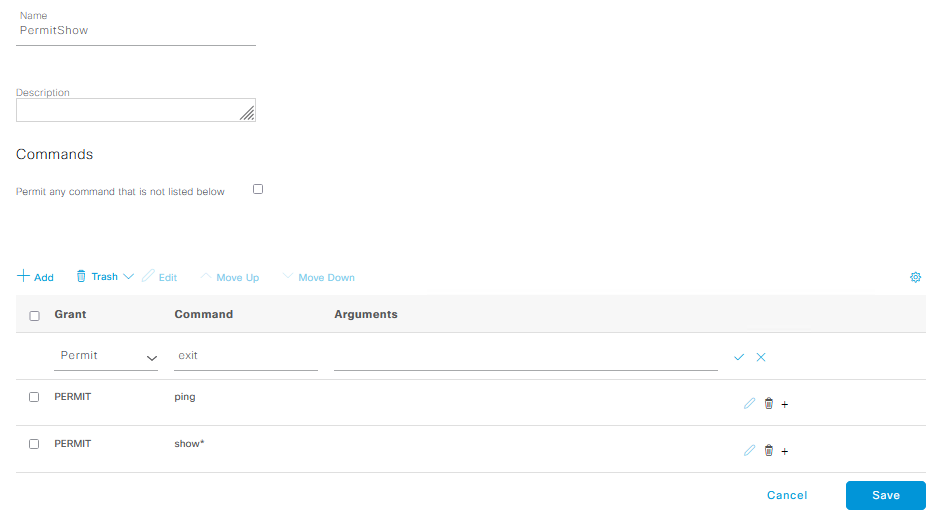


Click **Add**

Click and name it **PermitShow**

Click **Add,** use the drop down to choose **Permit** and enter **show\***, then the checkmark to apply and repeat for the following commands: **ping, traceroute, exit**

Click **Submit**

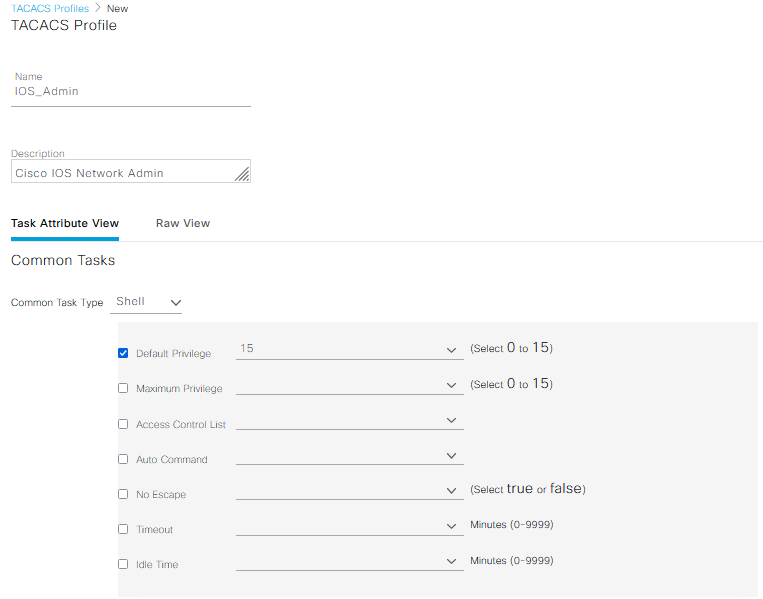
Define TACACS Profiles

Go to: **Policy Elements > Results > TACACS Profiles**

Click **Add**

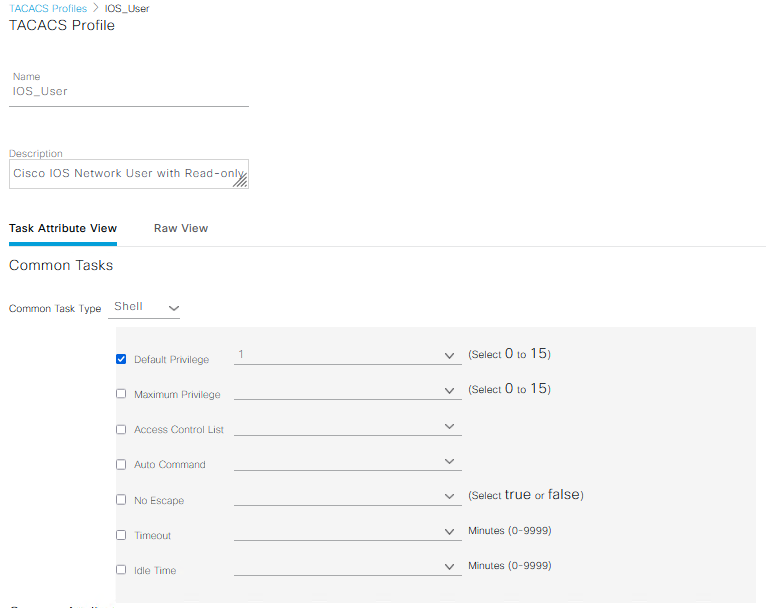
Enter a name for the profile, optional description, **Common Task Type** set to **Shell** and set the **Default Privilege** level to **15**

Click **Submit**

  
Click **Add**

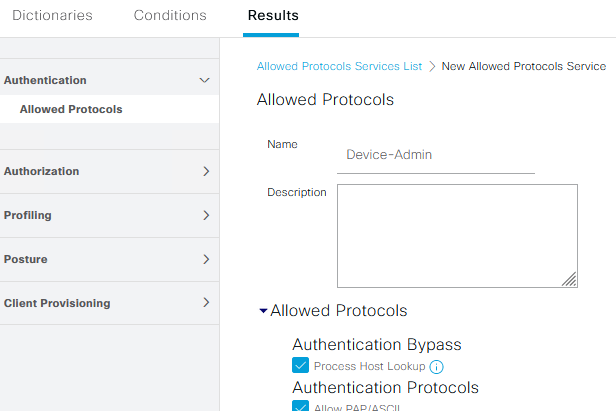
Enter a name for the profile such as **IOS\_User**, optional description, **Common Task Type** set to **Shell** and set the **Default Privilege** level to **1**

Click **Submit**



Define Allowed Protocols

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) > **Policy > Policy Elements > Results > Authentication > Allowed Protocols > +Add** create new, give it name like *Device-Admin*



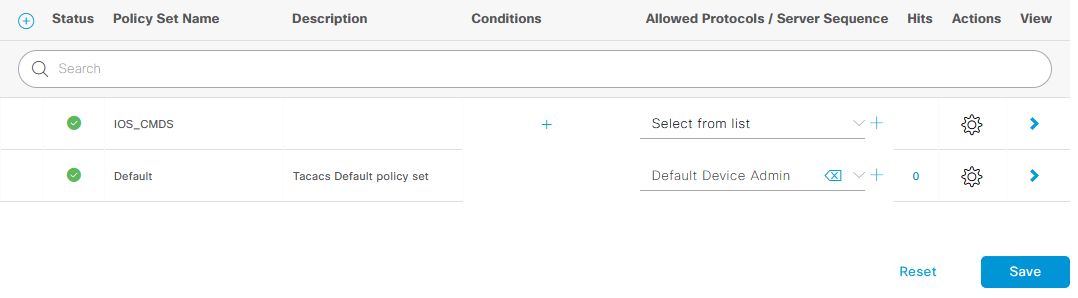
**What we check/uncheck will be defined later**

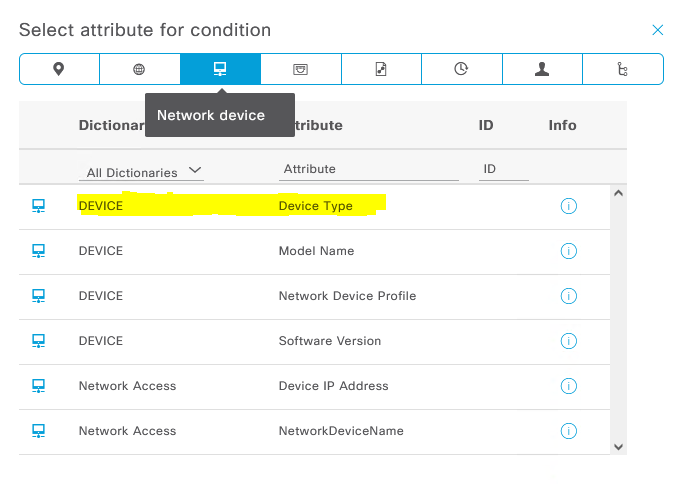
Click **Submit**

Attach Policy sets to TACACS Command Sets

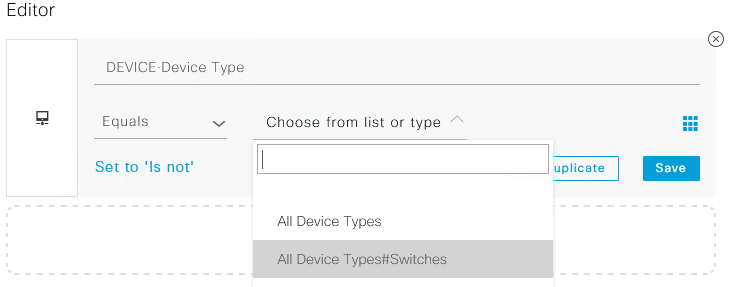
**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) > **Work Centers > Device Administration > Device Admin Policy Sets**

Click the **+** (plus) next to Status. Name this policy like *IOS\_CMDS*, then click the **+** (plus) under conditions for this new Policy Set



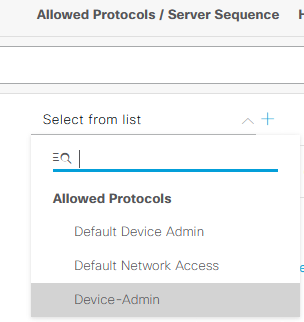
In the Conditions Studio window click the “**Click to Add an Attribute”** and choose **Device Device Type**

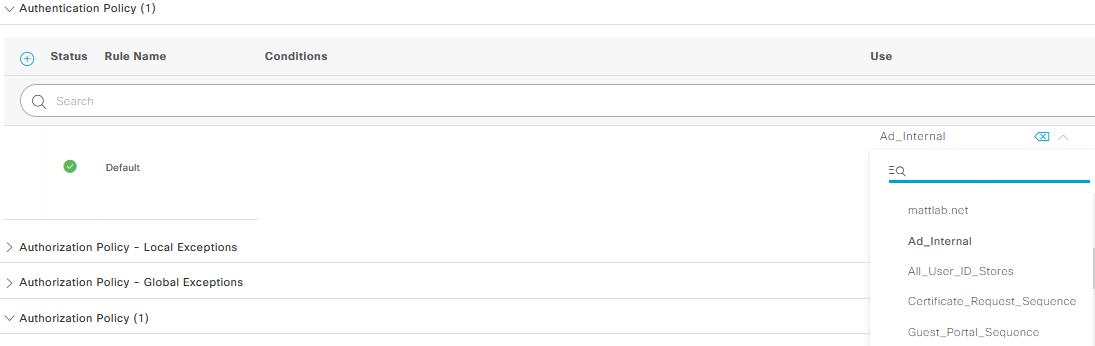
Click the **“Choose from list or type” to set to: All Device types#Switches**



Click **Use**

Under Allowed Protocols/ Server Sequence click the **Select from List** drop down to choose the policy you created such as Device-Admin click **Save**



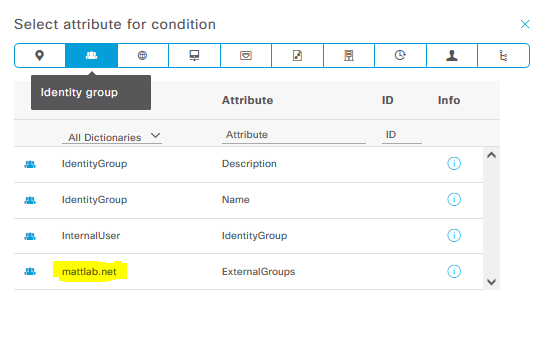
Under **View** click the **>** for your policy set name and click the **>** to expand **Authentication Policy.** Under **Use** change the drop down to the Identity Source Sequence you created such as AD\_Internal ****  
Click **Save**

Click the **>** to expand **Authorization Policy**

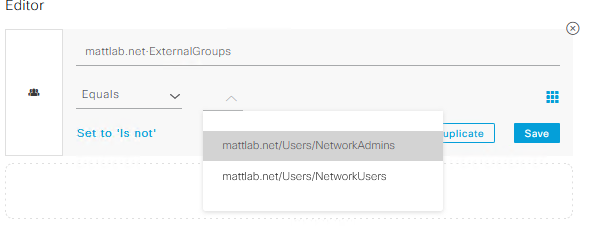
Click the **+** (plus) next to Status and give this a name of **Network Admins**

Click the **+** (plus) under Conditions to open the **Conditions Studio**

In the **Conditions Studio** click the “**Click to add an attribute**” and click the **Identity Group** icon you should see your *AD join point name* and select it

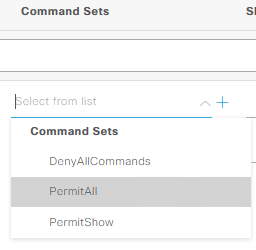


Set the Editor to **Equals** then click the **JoinPointDomainName/NetworkAdminGroupName**

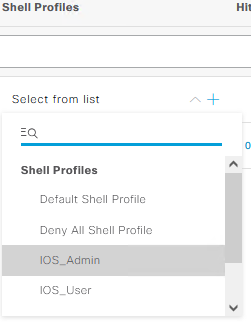


Scroll down click **Use**

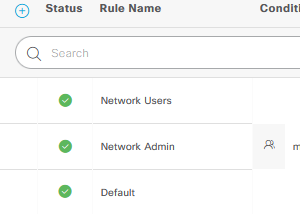
For the drop down under **Command Sets** and Select **PermitAll**



For the drop down under **Shell Profiles** Select **IOS\_Admin**

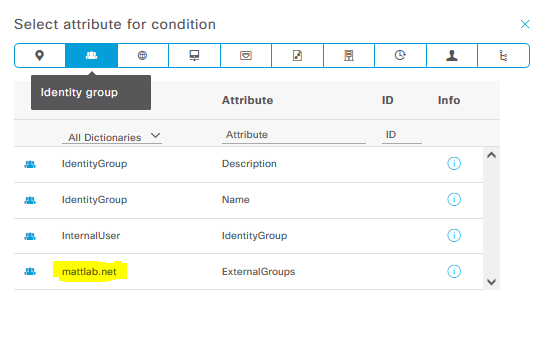


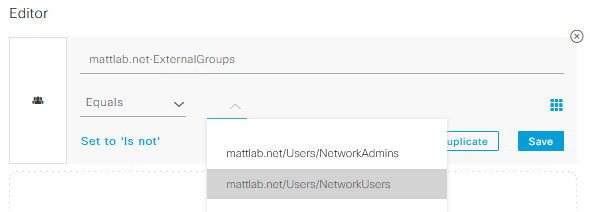
Click the **+** (plus) next to Status and give this a name of **Network Users**



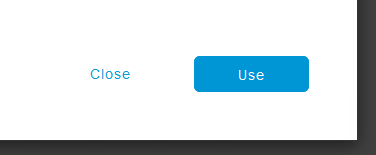
Click the **+** (Plus) under Conditions to open the **Conditions Studio**

In the **Conditions Studio** click the “**Click to add an attribute**” and click the Identity group icon you should see your *AD join point name* then select it

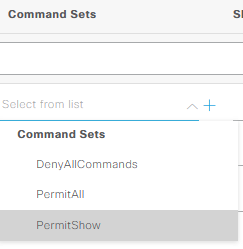


Set the Editor to **Equals** then click the **JoinPointDomainName/NetworkUserGroupName**

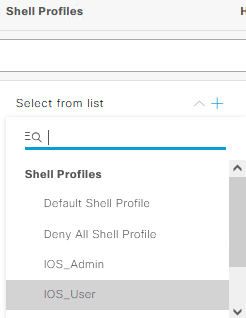
click **Use**

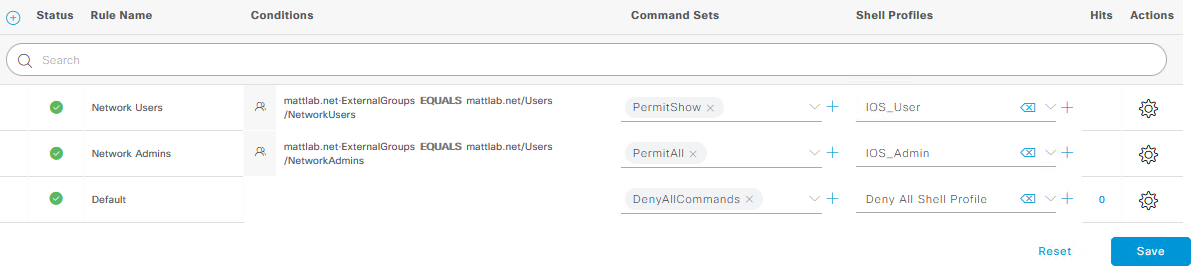


For the drop down under **Command Sets** and Select **PermitShow**



For the drop down under **Shell Profiles** Select **IOS\_User**



****Click **Save**

Patching ISE

Prior to downloading most recent patch go to the DoD repository or Cisco download page. Hover over the download link and a small window will pop up. This window will contain information about that particular download. The information includes the MD5 and SHA512 checksum value of that file.

Frequency from Cisco is anywhere between 45 to 3 months. patches are cumulative - all new have previous patches in them. In order to configure licensing to work in air-gapped networks ISE needs to be on at least patch 2. **Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration >System > Maintenance > Patch Management > Install**

When you apply “patch 3” the system will appear unresponsive and look like it wants to crash please wait at least 30 minutes ,ISE might restart

to check patch is applied

Gear > server information

DOD Banner

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration >System > Admin Access**

From left side **Settings > Access >** check box for **GUI > Pre-login banner** and **CLI > Pre-login banner**

Paste in the following from the attachment for both boxes

****Click **Save**

Licensing ISE

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration >System > Licensing**

Select **Permanent License Reservation Is this how its done with 3.x?**

**Link to permanent license Reservation**

**"Permanent License Reservation is a licensing method that is available by approval only. Contact your Cisco account manager to determine if Permanent License Reservation can be used in your environment."**

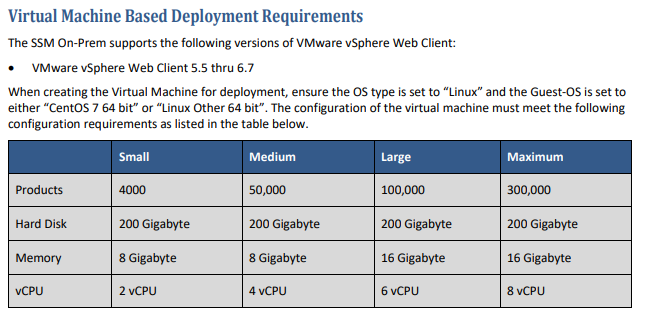
Each install of ISE needs the following:

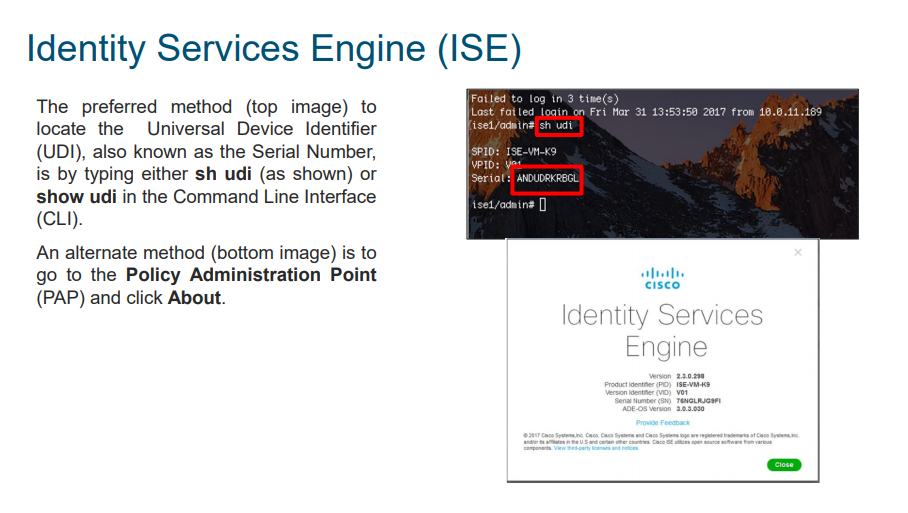
* VM
* Device admin – this is for TACACS functions at least one is needed possibly more per each switch router you have in ISE
* Base licensing – this is for RADIUS clients and it’s based on qty per session (you can always add more later)

To get info need to for licensing > Gear at the top right of ISE> About Identity Services Engine> PID, VID and serial will be displayed

Cisco account is needed you can download license file here: <https://software.cisco.com/> or  <http://www.cisco.com/go/license>

SSM On-Prem

https://www.cisco.com/web/software/286326948/158268/SSM\_On-Prem\_8\_Installation\_Guide.pdf



Each node in a cluster shares licensing

**We need Smart Licensing for Air-Gapped Networks**

**“Permanent License Reservation”**

https://www.cisco.com/c/en/us/td/docs/security/ise/3-0/admin\_guide/b\_ISE\_admin\_3\_0/m\_Licensing30.html

Old license for 2.x? go here: https://mycase.cloudapps.cisco.com/swl

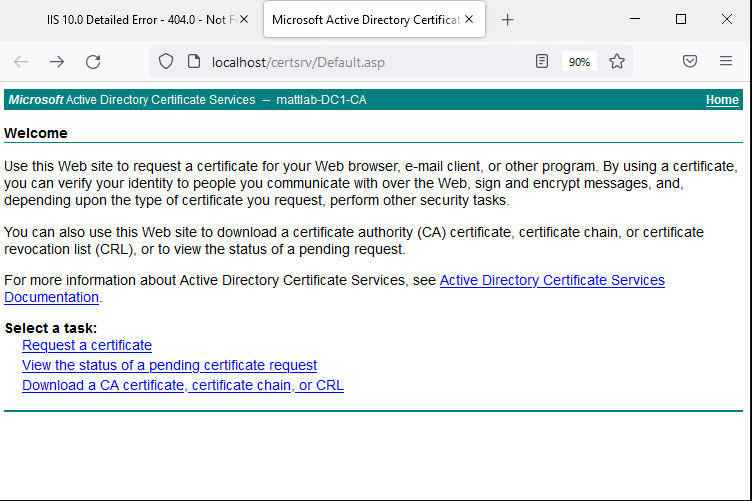
PKI and Certificate Setup

Step 1

Download Cert from CA server to for ISE

Go to: https://<RootCAServerFQDN>/certserv, login with your AD creds

"Download a CA certificate"> select Base 64> Download CA Certificate



Step 2

Install the CAs cert into ISE (optional to rename it to Root CA cert)

In ISEgo to **Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose  **Administration> Certificates > Trusted Certificates > + Import**

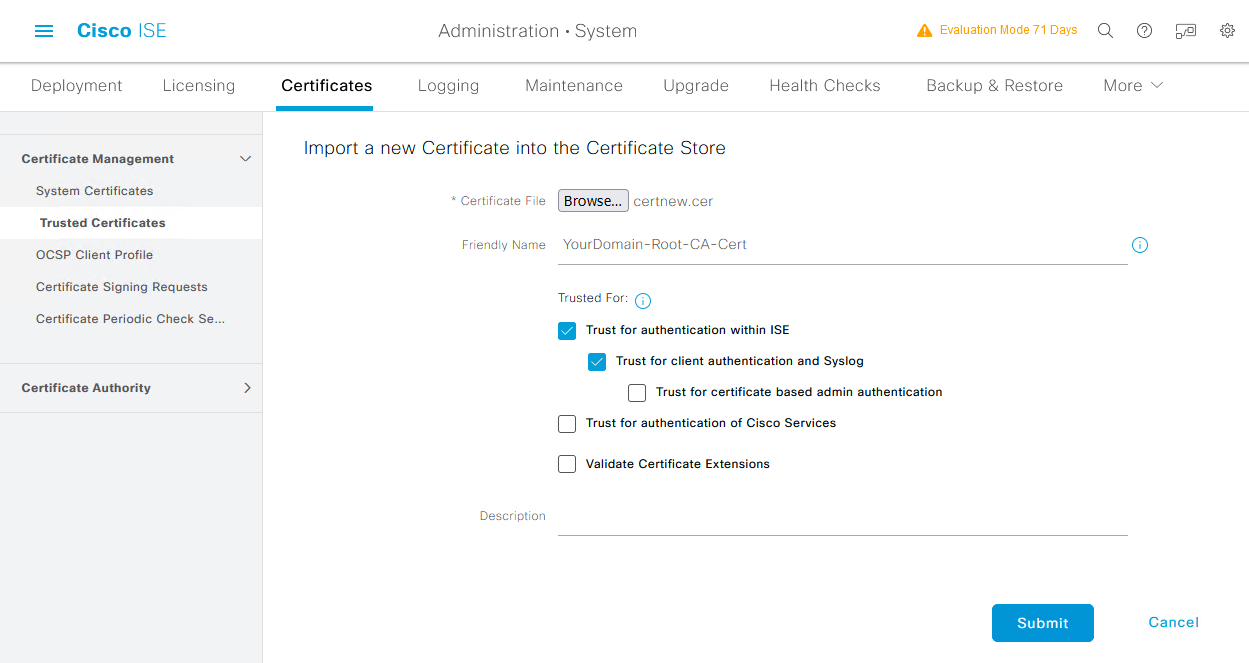
Browse to the certificate file downloaded from Step 1

Set Friendly name to YOURDOMAIN\_CA (or something memorable)

Check boxes for:

* + Trust for Authentication
  + Trust for client authentication and syslog **<-** need to verify this

Click Submit



Step 3 - Generate CSR from ISE for signing its certificate from the CA

Go to **ISE Administration> Certificates > Certificate Signing Requests >** Click **Generate Certificate (CSR) Signing Request**

Make sure the **Certificate(s) will be used for**: is set to **Multi-Use**

**Check** the **box** for your **ISE Node(s)**

**Common Name (CN)**: The CN should be a fully qualified domain name (FQDN) that will resolve via DNS to the IP address of the ISE node.

**Organizational Unit (OU):** This is the division of the organization that is controlling the device for which the certificate is being used.

**Organization (O):** This should be the organization the certificate is meant to represent—that is, the name of the organization that is implementing ISE.

**City (Locality) (L)**: This is often used to denote the city where the entity resides.

**State (ST)**: This is the state or province the entity resides in.

Country (C): This is the country that the entity resides in.

For Subject Alternative Name (SAN)

Set the drop downs and + for

* **DNS Name** and enter in the FQDN
* **DNS Name** and enter the hostname
* **IP address**

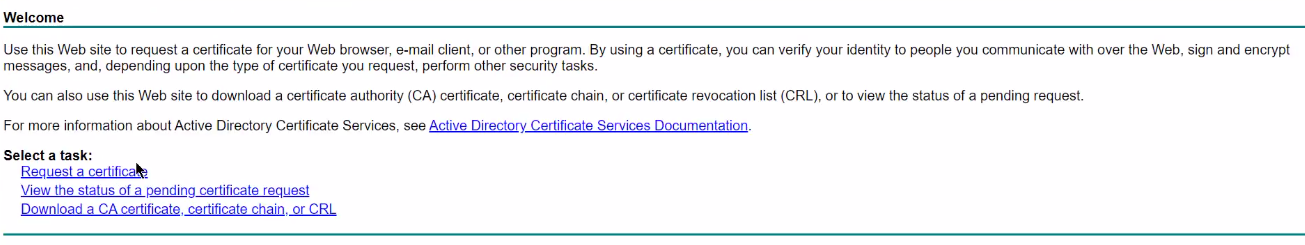
Leave **Key type**, **Key Length** and **Digest** to sign with at **defaults**

Click **Generate**

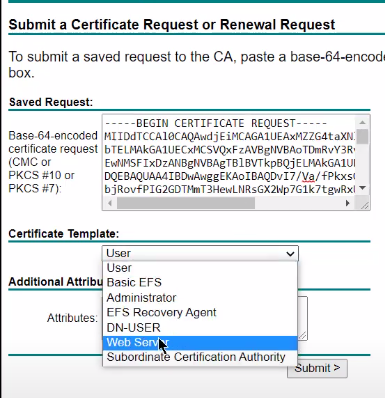
Go back to your Root CA at: <https://RootCAServerFQDN/certserv>

click **Request a certificate**

**Advanced certificate request**



Open the .pem file in notepad and copy the entire contents and paste it in the Base-64-encoded box



Choose **Web-Server**

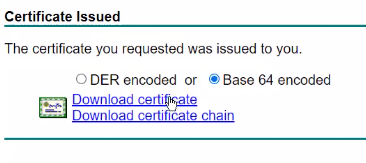
*San Attributes? Need to confirm is 100% required*

Add the following to attributes:

*San:dns=<FQDN>&dns=<HOSTNAME>&ipaddress=1.2.3.4*

and click **Submit**

Choose **Base 64 encoded** then **Download Certificate**



Rename this file to Signed-Cert

Go back to ISE > Administration > System> Certificates> Certificate Signing Request

**Check** the **Box** next to your server and then **Bind Certificate**

Browse to the Signed cert file , give it a friendly name like CA\_Signed\_Cert

Check boxes for : and OK to any warning messages

* Admin
* EAP Authentication
* RADIUS DLTS

Submit

ISE will restart its application server which takes around 7 minutes to complete

You can also check the progress of the configuration backup from the CLI

ise/admin# **show application status ise**

Log back into ISE and you should now no longer see certificate warnings

Turn on FIPS Mode

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration >System >Settings> FIPS Mode**

Change drop down to **Enabled** Click **OK** to the Warning then **Save** then restart the server

Enable FIPS Mode in Cisco ISE to ensure DRBG is used for all RNG functions.

Deploying ISE Multi node “Distributed Install\*

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Menu > Menu > Something Else**

Click **OK**

More stuff here

Backup and Restore ISE

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Menu > Menu > Something Else**

Click **OK**

**Configuration Data**

**Operational data**

**ISE Certificates – done via CLI**

**Config repo first:**

[**https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/215348-how-to-configure-repository-on-identity.html**](https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/215348-how-to-configure-repository-on-identity.html)

**Do the needful:**

[**https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215355-how-to-take-configuration-and-operation.html**](https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215355-how-to-take-configuration-and-operation.html)

**restore preformed via CLI? Need to test with a near expiring ISE instal**

Device Tracking Policy – not used?

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Menu > Menu > Something Else**

Click **OK**

**Enable the device tracking policy #device-tracking policy policy-name**

**Enable tracking in in the policy# tracking enable**

**Attach the policy**

Splunk Setup – need to define these steps

**Splunk Cisco ISE App?**

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration > System > Logging> Remote Logging Targets**

Click **+ Add**[**https://community.cisco.com/t5/security-documents/identity-services-engine-and-splunk-apps-configuration-guide/ta-p/3735814**](https://community.cisco.com/t5/security-documents/identity-services-engine-and-splunk-apps-configuration-guide/ta-p/3735814%20)

RADIUS, MAB and 802.1X Wired Setup

[**https://youtu.be/5oLzYpYoojc**](https://youtu.be/5oLzYpYoojc)

**Enable RADIUS for your network devices:**

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) > **Work Centers > Device Administration > Network Resources > Network Devices** > RADIUS: check box for RADIUS

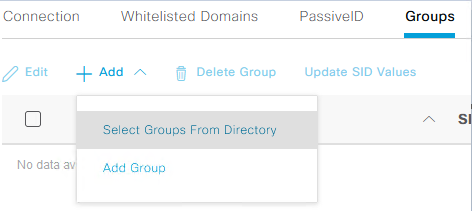
shared secret: RADIUS\_PASSWORD (replace with the same password used on the switches)

leave all other others as default, then submit/save

Add additional Active Directory Groups to ISE

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Administration > Identity Management > External Identity Sources > Active Directory> “domain entry you created” > Groups**

Click **+Add**> **Select Groups from Directory**



In **Filter** put: **\***Computer**\*** and click **Retrieve Groups,** select **Domain Computers** then repeat by searching for \*Users\* and select **Domain Users**

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) Policy > Policy sets > click the + in middle of the screen to create a new policy set and change the name to DOT1x

click the + to modify it> drag and drop 802.1x Wired> click the AND then NEW (the inside one) >

"Click to add an attribute" > Dictionary > DEVICE> Device Type>"Choose from a list or type">

"All Device Types#Switch#All\_in\_Switch"> click USE (scroll down typically at the bottom of the screen) >In Allowed Protocols set to: Default Network Access >SAVE

click the "**>**" under view column to expand the policy set details > click the ">" to expand out the Authentication policy >

click the + (middle of the screen to create an Authentication rule and name it Dot1x > click the + to modify it > drag and drop the Wired\_802.1x > USE > set the use drop down to your "AD Domain entry" > set Default below it to DenyAccess by clicking ALL\_USER\_ID\_STORES > type: deny select "Deny Access" Click the "**>**" to expand out Authorization Policy > click the + to create a new authorization rule and name it Admin Access > click the + to modify it > "click to add and attribute"> dictonary to your "AD Domain entry"> Your AD name ExternalGroups >

"Choose from a List or type " set to adname.com/Builtin/DomainAdmins

Note: replace adname.com and /DomainAdmins with your appropriate domain and groups

Click USE

Profiles > PermitAcccess > SAVE

Note: in default policy sets make sure to disable all defaults by:

Policy >Policy Sets > ">" by View to Modify > click the ">" by Authentication Policy and under status column click all items to disable and the icon by it will turn to X then click the ">" by Authorization Policy to expand out and disable all items inside the click SAVE

Policy Sets and DACL

\*Normally a DACL would be used in production but this will be added later \*

this is to add workstation and server access so they can also gain network access

existing Dot1x Policy > click the ">" to modify the Dot1x policy set > click the ">" to modify the Authorization policy > click the gear > duplicate below> name the rule: Machine Authentication> click the existing condition and change the .../Administrators (you have click the tiny x to remove the existing) to ../Domain Computers. USE > SAVE

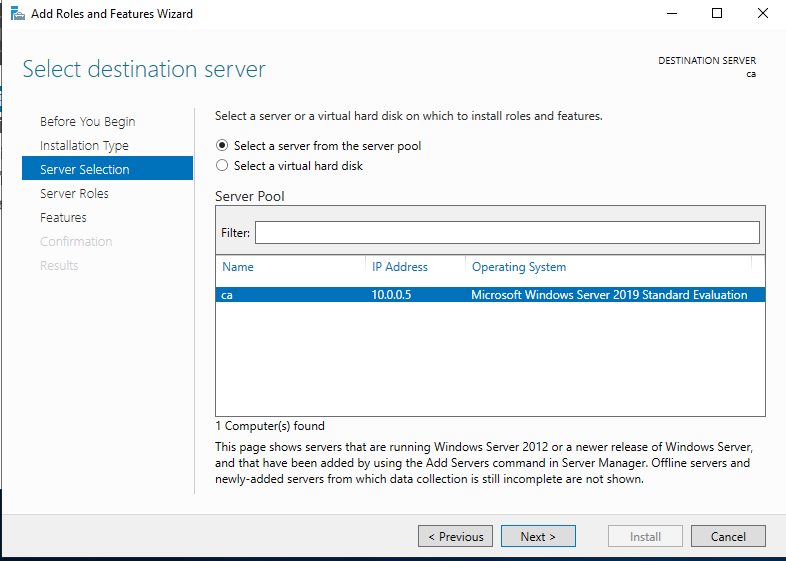
**Certificate Server Setup – need to confirm best practice or not**

\*Skip Certificate server setup if one already exists\*

Step 1 Roles and features

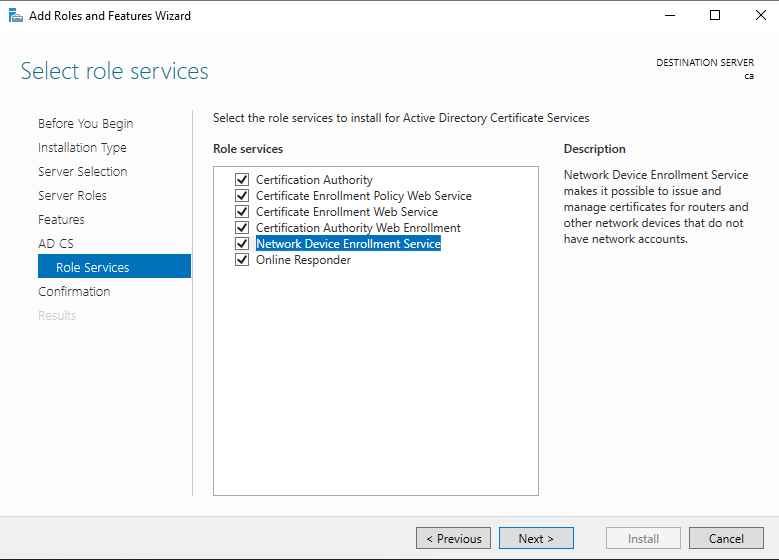
Server Manager > Add Roles and Features> Role-based or Feature-based installation

Select a server from the server pool, Next

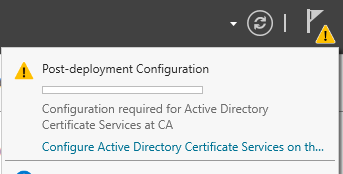


Select Active Directory Certificate Services, then Add Features to the popup, Next, Next

Select all items, and Add Features to any popups that might occur



Click the Exclamation mark > Configure Active Directory Certificate Services on the…

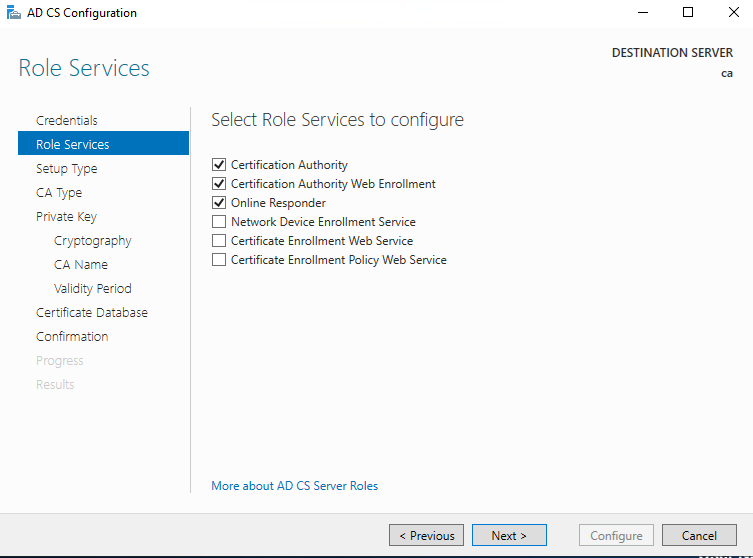


Click Next then just check 1st 3 options to configure first, then Next

Certificate Authority

Certificate Authority Web Enrollment

Online responder



Enterprise CA

Root CA

Create new Private key pair

SHA 256

Validly 5 years (default)

AD CS Configuration

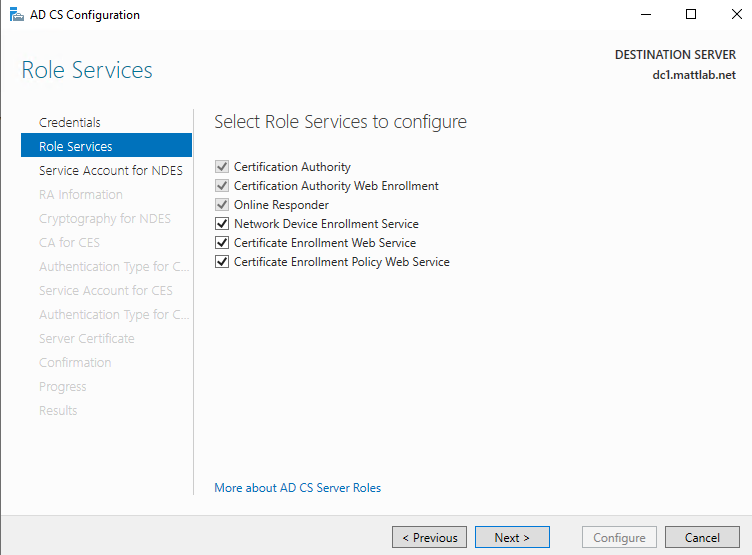
Do you want to configure additional services? Yes

Check the last 3 items

Network device Enrollment

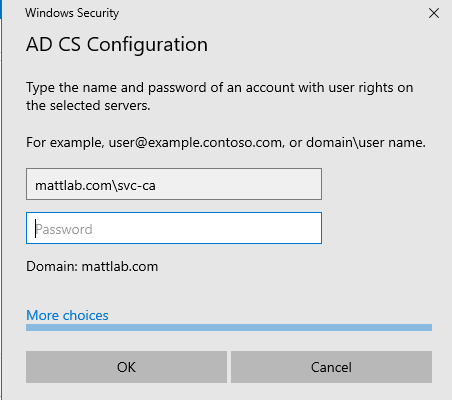
Certificate Enrollment

Certificate Enrollment policy web service



Specify service account > select > enter a domain account that is a member of a local IIS\_IURS group on the CA server - best practice is a service account (or admin)

keep all defaults



\*If you do not know who this account is Start > Run > lusrmgr.msc > Groups> open IIS\_IUSRS

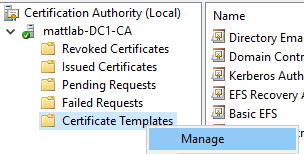
Keep all defaults

You may have to do this a second time…

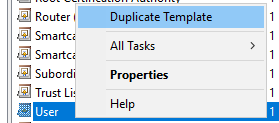
Choose an existing certificate - this should be the existing CA server

**Certificate Setup**

Server manager > Certificate Authority> expand out Domain-CA> Certificate Templates > right click Manage



Right click on User > Duplicate Template >



General tab> Change name to *GPO-User*

Request Handling tab> uncheck Allow private key to be Exported

Security tab> Select Domain Users and set permissions to

Read

Write

Enroll

Autoenroll

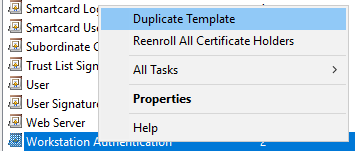
Subject Name tab> uncheck "Include Email Name in Subject Name" and "Email Name"

Verify the following is checked: User Principal Name (UPN)

Subject Name Format is set to: Fully Distinguished Name

Extensions tab> select Application Policies > Edit.. > add> select Server Authentication > Ok to close

Right click on Workstation Authentication > Duplicate Template >



General tab> Change name to *GPO-Computer*

Security tab> Select Domain Computers and set permissions to

Read

Write

Enroll

Auto enroll

Subject Name tab> check only:

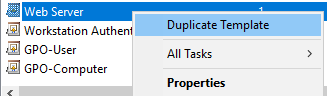
DNS Name

Universal Principal Name (UPN)

set drop down to Subject Name: None

Extensions tab> select Application Policies > Edit. > add> select Server Authentication> ok > ok > ok

Right click on Web Server > Duplicate Template >



General tab> Change name to *PXGrid*

Subject Name tab> check only:

DNS Name

Universal Principal Name (UPN)

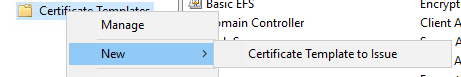
set drop down to Subject Name: None

Extensions tab> select Application Policies > Edit. > Add> select Client Authentication and verify it has server Authentication (if not then add it too)

Subject Name tab > verify Supply in the Request is set

Click ok and close out the Certificate Template Console

Right click on Certificate Templates > New > Certificate Template to Issue



Ctrl click GPO-Computer, GPO-User and PXGrida dn click ok

These templates should now be present in Certificate Templates

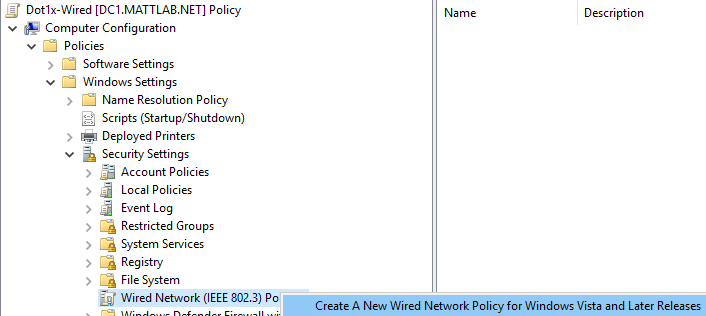
**Setup Group Policy for Dot1x**

Open AD > Group Policy Management> Expand out your domain

Right click on an OU or whole domain > Create a GPO in the Domain and Link it here> name it Dot1x-Wired

Right click Edit and expand out:

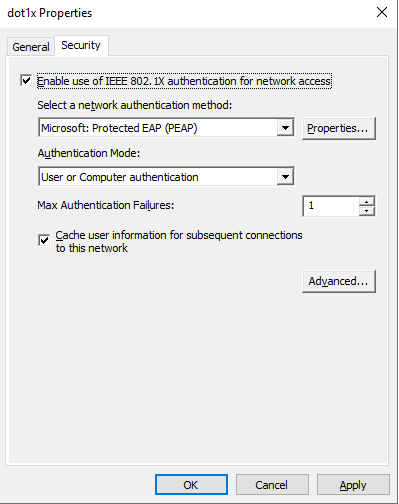
**Computer Configuration> Polices > Windows Settings > Security Settings**



Right click on **Wired Network (IEEE 802.3 Polices** > Create a New Wired Network Policy..

Rename this policy to Dot1x

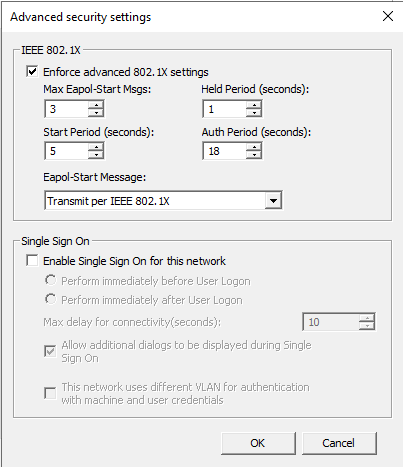
Security tab>



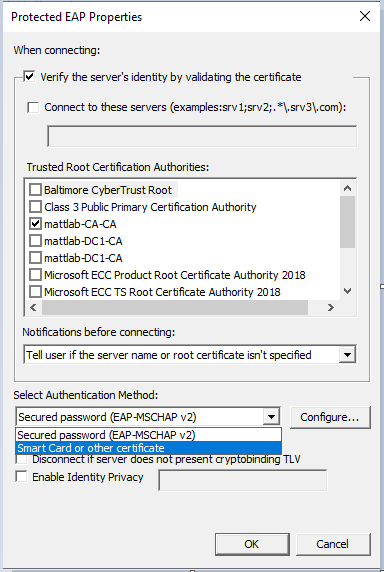
EO uses “Computer Only” not “User or Computer Authentication”

EO uses 10 for “Max Authentication Failures”

Advanced > check box for enforce Advanced 8021x Settings, then OK



Properties tab> select the certs from the trusted Root Certification Authorities and set the Select Authentication Method to : Smart Card or Other Certificate, then OK

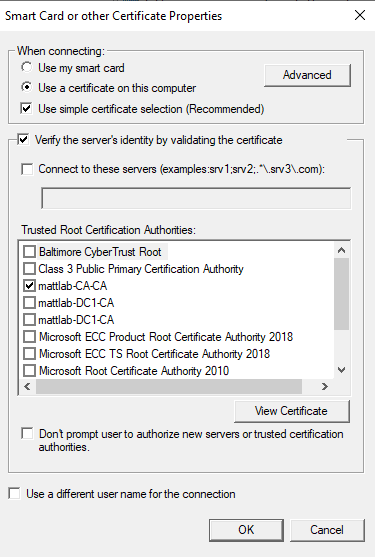


EO does not have “Verify the servers identity…” checked

EO has “Fast Reconnect” checked

Click **Configure**

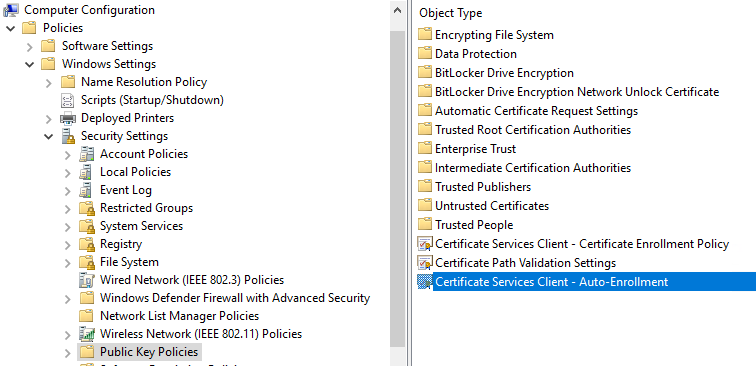
Select Certificates from the CA server , ok then close out the properties window



EO has “Verify the server’s identity…” unchecked

Enable Auto Enrollment Group Policy

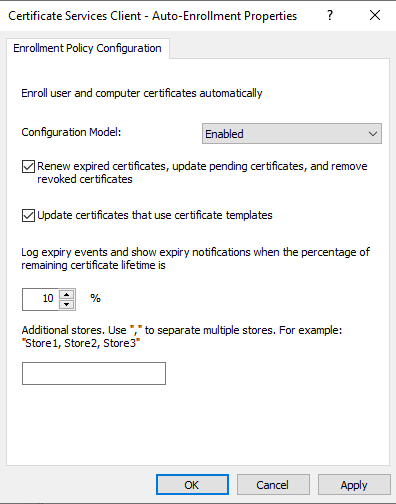
Open **Computer Configuration> Polices > Windows Settings > Security Settings > Public Key Polices**



Change to Enabled

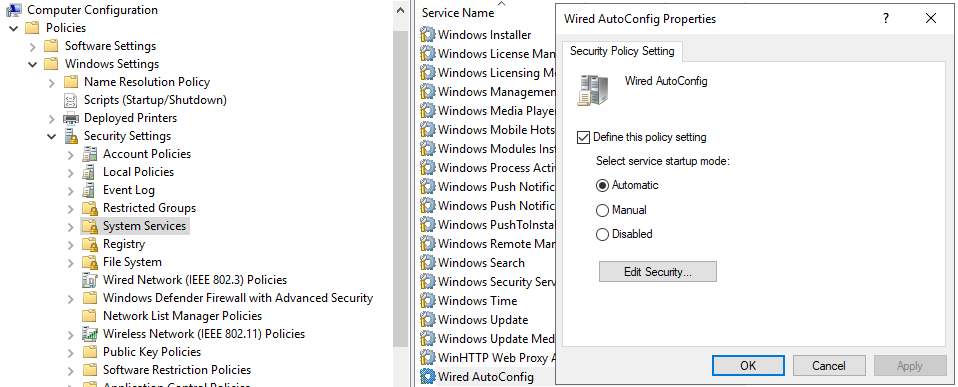
Check boxes for Renew Expired Certificates…

Update Certificates that use Certificate Templates



**Enforce Wired Auto Config by Group Policy**

Open: **Computer Configuration> Polices > Windows Settings > Security Settings> System Services> Open Wired AutoConfig and Define this policy and set to Automatic**



**Automatically have certificates issued to user or workstation**

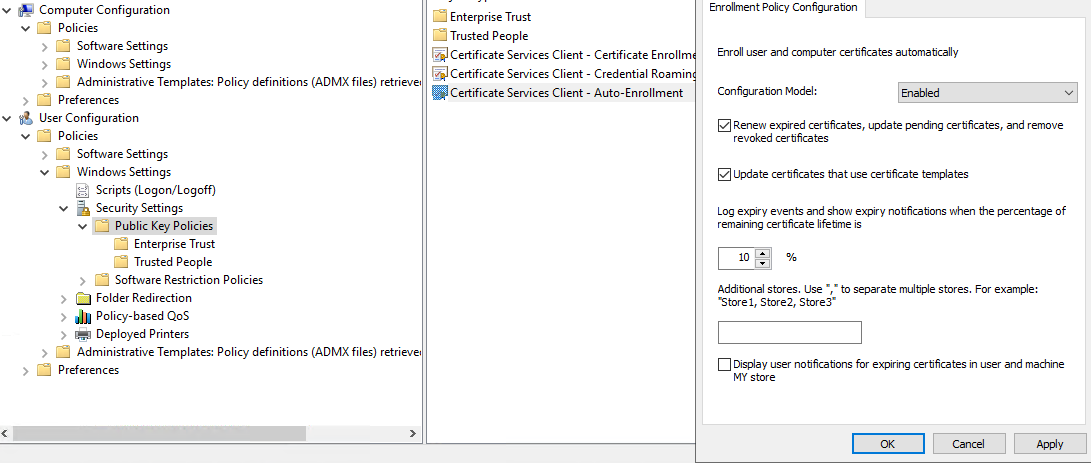
User Configuration > Policies > Window Settings> Security Settings > Public Key Polices

Open Certificate Services Client – Auto Enrollment

Check boxes for Renew Expired Certificates…

Update Certificates that use Certificate Templates

Ok then close out Group policy Management



**Gpupdate /force** on both the AD and workstation you are verifying

Troubleshooting:

If you are not receiving changes make sure workstations are in the correct OU

Verify Endpoints are receiving certs when logging in:

Open MMC > Add/Remove snap in > Certificates > add

On CA server Side:

Certificate Authority > Issued Certificates

MAB - Adding allowed devices – Needs further defining

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Menu > Menu > Something Else**

Click **OK ….**

**Work Centers > Network Access > Identities > Endpoints > + Add**

**Alternately connect the device to the network and allow the mac address**

Configuration for Cisco Network Devices

**TACACS Config:**

|  |
| --- |
| aaa new-model  !  aaa group server tacacs+ TACACS-ISE  server name ISE01  !  aaa authentication login ISE-VTY group TACACS-ISE local  aaa authentication login CONSOLE local  aaa authentication enable default group TACACS-ISE enable  !  aaa authorization config-commands  aaa authorization exec ISE-VTY group TACACS-ISE local if-authenticated  aaa authorization commands 1 ISE-VTY group TACACS-ISE local if-authenticated  aaa authorization commands 15 ISE-VTY group TACACS-ISE local if-authenticated  !  aaa accounting exec default start-stop group TACACS-ISE  aaa accounting commands 1 default start-stop group TACACS-ISE  aaa accounting commands 15 default start-stop group TACACS-ISE  aaa accounting system default start-stop group TACACS-ISE  !  username kjohnson privilege 15 secret 5 <password>  !  tacacs server ISE01  address ipv4 1.2.3.4  key <Matching\_Password\_Used\_on\_ISE>  !  line con 0  privilege level 15  logging synchronous  login authentication CONSOLE  !  Line vty 0 4  privilege level 15  authorization commands 1 ISE-VTY  authorization commands 15 ISE-VTY  authorization exec ISE-VTY  login authentication ISE-VTY  transport input ssh  Line vty 5 15  privilege level 15  authorization commands 1 ISE-VTY  authorization commands 15 ISE-VTY  authorization exec ISE-VTY  login authentication ISE-VTY  transport input ssh |

**Radius Config:**

|  |
| --- |
| aaa new-model  aaa session-id common  radius server ISE01  address ipv4 10.0.10.4 auth-port 1812 acct-port 1813  key <Matching\_Password\_Used\_on\_ISE>  !  aaa group server radius ISE-RADIUS  server name ISE01  aaa authentication dot1x default group RADIUS-ISE local  !  aaa authorization network default group RADIUS-ISE local  !  aaa accounting update newinfo  aaa accounting dot1x default start-stop group RADIUS-ISE local  aaa accounting update newinfo periodic 2880  !  dot1x system-auth-control  ip radius source vlan 100  or ip radius source-interface vlan 100 ?  aaa server radius dynamic-author  client 10.0.10.4 server-key <Matching\_Password\_Used\_on\_ISE>  !  radius-server vsa send accounting  radius-server vsa send authentication  radius-server attribute 6 on-for-login-auth  radius-server attribute 8 include-in-access-req  radius-server attribute 25 access-request include  radius-server deadtime 15 🡨investigate ideal deadtime  !  ! add helper address on any SVI that has DHCP helper address so ISE can profile those requests, IP address is of your ISE servers  interface vlan 10  ip helper-address 10.0.10.4  !  ! Interface Commands  !  interface Te1/0/48  description \*\*\*DOT1x TEST Interface\*\*\*  switchport mode access  switchport access vlan 20  spanning-tree portfast  authentication host-mode multi-domain  authentication order mab dot1x  authentication priority dot1x mab  authentication port-control auto  dot1x pae authenticator  mab  dot1x timeout tx-period 10 |

**Verification commands**

**#Show authentication sessions interface fa 0/1**

Troubleshooting and tips

Test tacacs connection:

#test aaa group ISE-TACACS-GROUP <username> <password>Legacy

“No authoritative response from server” solution: \_\_\_\_

Reset ISE back to Factory defaults: Application reset-config ISE

On PC :

Try to connect to the local area network, enter password if prompted, check if we get network

access

On switch :

Use following commands to verify dot1x:

Show authentication session interface <interface-name > detail

Show radius statistics

Show run interface <interface name >

Sh run | in dot1x

Show dot1x interface <interface-name>

On ISE :

Go to operations>radius live logs > check the logs to see passed or failed authentication.

Note : you can filter logs based on mac address or username

Troubleshooting tools for wired dot1x:

On PC :

Check event-viewer.log from windows PC

On switch :

Following debug commands can be executed on switch to troubleshoot issue in detail:

Debug dot1x events

Debug radius

Debug epm events

Debug aaa authentication

Debug aaa authorization

Debug Authentication feature all

Debug mab all

On ISE :

On ISE GUI, go to administration > logging > debug log configuration:

Click on ISE node name , In the component list name, search for runtime-aaa, change it’s

level to “debug”

Now to Operations > Download logs > Troubleshoot > debug logs and download prrt-server.

log to check aaa related logs on

Or

Go to Operations > Download logs > create support bundle and collect the full

encrypted log bundle

Template Header Copy and paste this

**Menu** icon ([](https://www.cisco.com/c/dam/en/us/td/i/400001-500000/440001-450000/440001-441000/440197.jpg)) and choose **Menu > Menu > Something Else**

Click **OK**

STIG changes

Adjust Password Policy

Administration> System > Admin >Access > Password Policy

Make changes needed