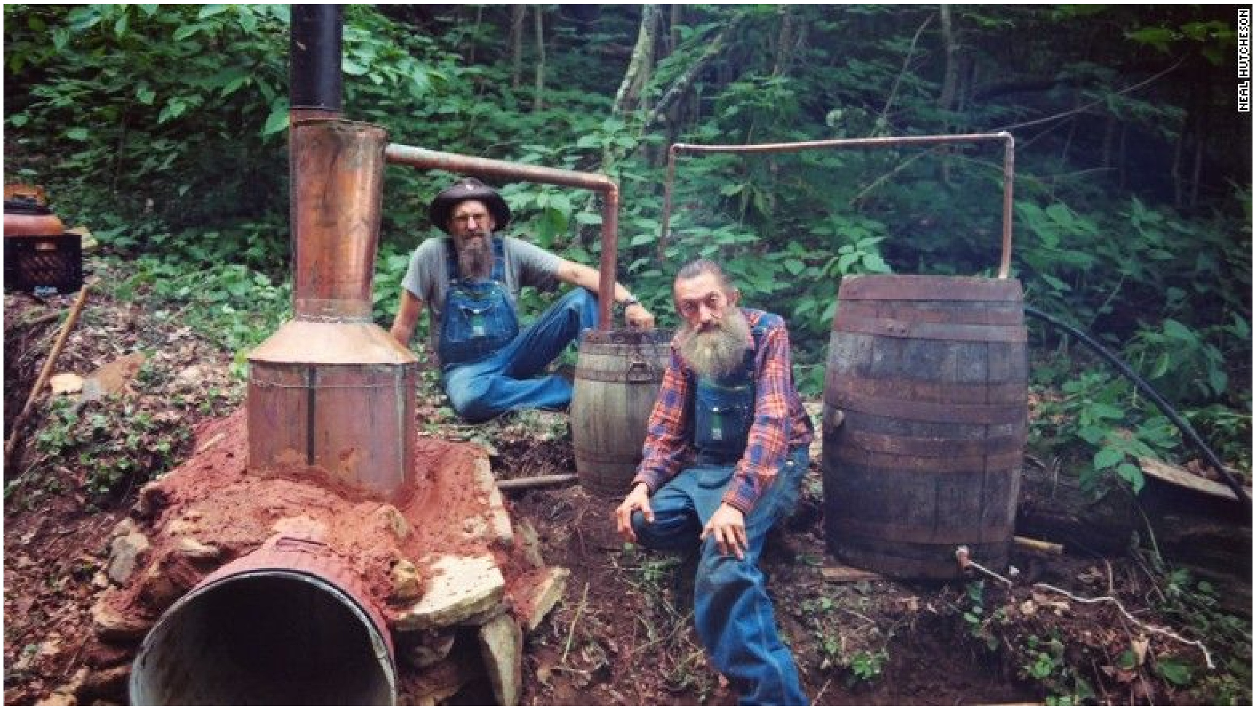
ISE Wired PoC Prescriptive Guide

Gary Quinn Security TSA - 2019

Summary

Appalachian moonshiners operate in quick fashion, building their operations from the ground up, brick by brick, for every run they make. Then they tear it all back down, move on and do it again elsewhere. ISE wired demonstrations & use cases are a lot like that, lots of moving parts that can prove daunting if you've never done it before and highly combustible when done incorrectly.

This guide is for those inexperienced individuals.. It's only intended to show some nifty and powerful use cases that a lot of customers either want or don't know they want. There are tons of other content out there for specific knobs or capabilities, but this is looking to be a more complete guide.



"Popcorn" Sutton and J.B. Rader

Diagram

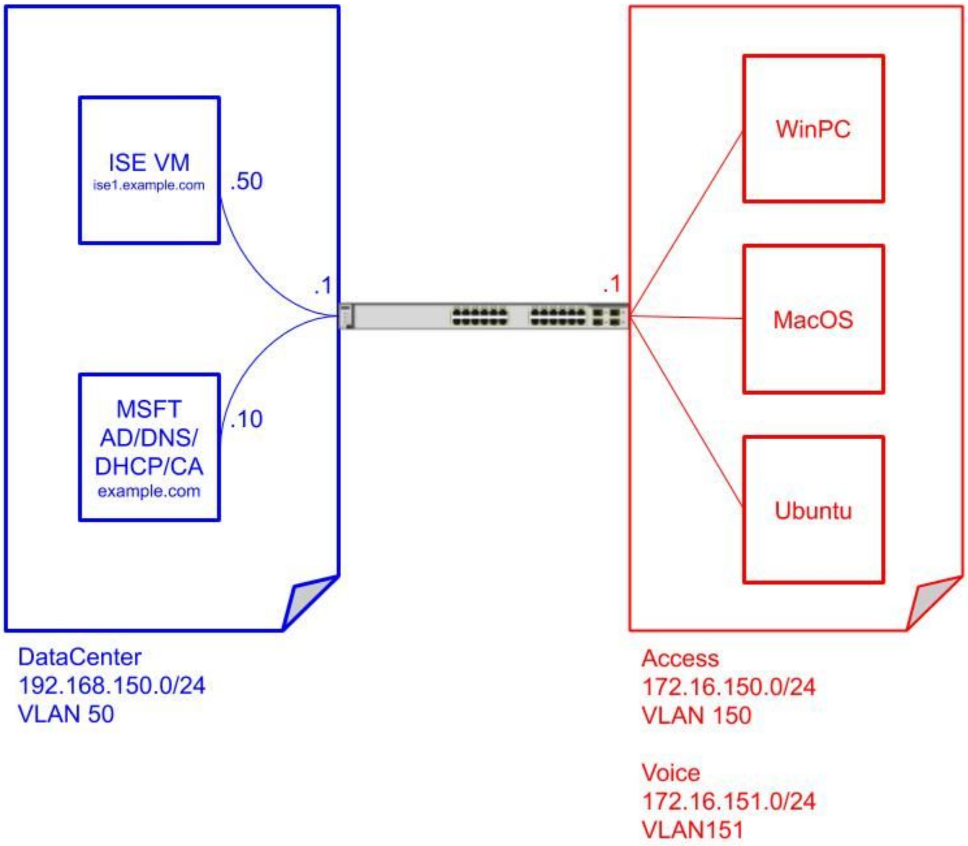


Diagram Note

This was done largely on:

- Standalone ESXi 6.5.0 Update 2 (Build 10884925)/Client version 1.33.1
    - Intel Nuc Skull Canyon (newer "Canyon" models available). Mine has 1TB and 32GB (the max) memory
    - This may be even easier if you have a bare metal Windows Server and load up ISE in a Hyper-V VM.
- Catalyst 3560-CX switch (Any Catalyst that switches/routes should work great, bonus if it has PoE)
- Various endpoints, however you can get them wired. Add in Rasperry PIs and IP Telephones

Code Versions

Platform	Version	Notes
ISE	2.6 Patch1 (whatever's current)	ISE-2.6.0.156-virtual-SNS3615-SNS3655-200.ova
Win Server	2012R2	Any modern Win server works
Windows Client	Win10 1903	Or whatever's current
Linux	Ubuntu 18 LTS	Current
MacOS	10.14.5	
Catalyst 3560-CX	15.2(6)E2	

ISE Installation

Summary

Hopefully you know the general steps to install an ISE VM. This will note tips/tricks as we go.

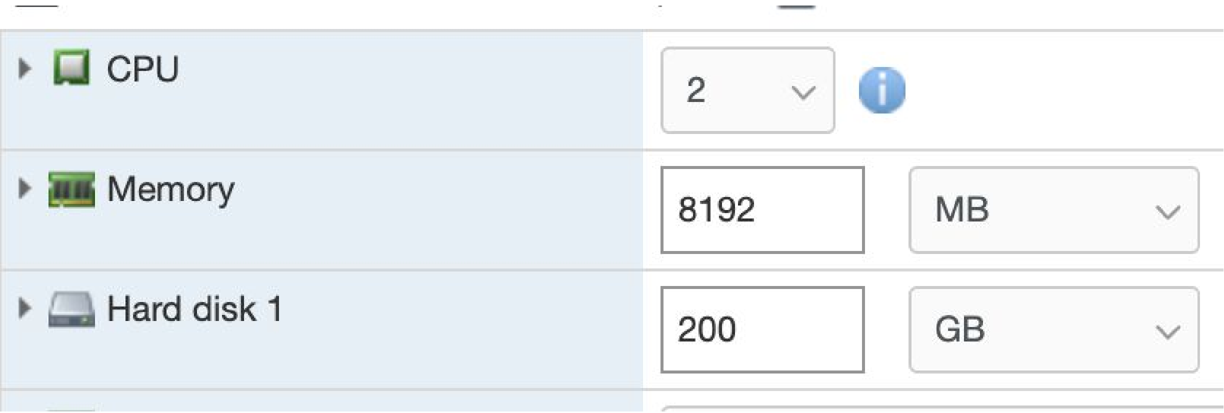
This published guide is also quite helpful in installing on VMware (as well as hyper-v and KVM).

VM Resources

Note 200GB Thick Provisioned. For vCPUs, did 1 core x 2 Sockets (the default eval OVA install). 8GB mem by default. Note you can always slide these higher to suit taste.

vNic was all e1000 (the default OVA option). 6 vNics were installed. Left them all on the same network and only connected one of them.

Note ISE will install with 100GB but most likely won't be able to be upgraded to newer versions because the disk space isn't available just to do the upgrade. Might be fine just for one and down proof of concepts.



CPU: 2

Memory: 8192 MB

Hard disk 1: 200 GB

Catalyst3560 Configuration

```
aaa group server radius lab
 server name lab
!
aaa authentication dot1x default group lab
aaa authorization network default group lab
aaa accounting dot1x default start-stop group lab
!
!
!
!
!
aaa server radius dynamic-author
 client 192.168.150.50 server-key [password]
!
!
!
device-sensor filter-list cdp list cdp-list
 tlv name device-name
 tlv name address-type
 tlv name capabilities-type
 tlv name platform-type
!
device-sensor filter-list lldp list lldp-list
 tlv name system-name
 tlv name system-description
!
device-sensor filter-list dhcp list dhcp-list
 option name host-name
 option name domain-name
 option name requested-address
 option name parameter-request-list
 option name class-identifier
 option name client-identifier
device-sensor filter-spec dhcp include list dhcp-list
device-sensor filter-spec lldp include list lldp-list
device-sensor filter-spec cdp include list cdp-list
device-sensor accounting
device-sensor notify all-changes
ip routing
!
!
ip dhcp snooping vlan 1,51-53,99,250-252
no ip dhcp snooping information option
```

```
ip dhcp snooping
no ip igmp snooping
!
!
!
!
!
!
!
!
dot1x system-auth-control
!
device classifier
!
!
!
!
!
lldp run
!
!
!
!
!
interface GigabitEthernet0/1
 description Uplink
 switchport mode trunk
 ip dhcp snooping trust
!
interface GigabitEthernet0/8
 description Link to ISE PassThrough
 switchport access vlan 250
 switchport mode access
 switchport voice vlan 251
 ip access-group ACL-DEFAULT in
 authentication host-mode multi-auth
 authentication open
 authentication order mab
 authentication priority mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate server
 mab
 dot1x pae authenticator
 dot1x timeout quiet-period 10
 dot1x timeout tx-period 2
 spanning-tree portfast edge
!
interface Vlan150
 description Server VLAN
 ip address 192.168.150.1 255.255.255.0
!
interface Vlan250
 description Access VLAN
 ip address 172.16.150.1 255.255.255.0
 ip helper-address 192.168.150.10
!
ip http server
ip http secure-server
ip http secure-active-session-modules none
!
ip access-list extended ACL-DEFAULT
 permit ip any host 192.168.150.10
 permit ip any host 192.168.150.50
 permit udp any eq bootpc any eq bootps
 deny   ip any any
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL
 deny   ip any host 192.168.150.10
 deny   ip any host 192.168.150.50
 deny   udp any eq bootps any
 deny   udp any any eq bootpc
 deny   udp any eq bootpc any
 permit tcp any any eq www
 permit tcp any any eq 443
!
snmp-server community [community] RO
snmp-server community [community] RW
snmp ifmib ifindex persist
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
!
radius server lab
 address ipv4 192.168.150.50 auth-port 1812 acct-port 1813
```

```
pac key [secret]
```

Windows Server Setup

General Setup

I had some spare windows server activation keys laying around from MSDN days. Most customers will bring their own AD so a lot of this will largely be handled prior.

I used the default VMWare settings for Win2012 which is:

- 1 vCPU
- 40GB Disk (thick provisioned)
- 4GB Memory

Check the time in the VM (mine defaulted to 8 hours off).

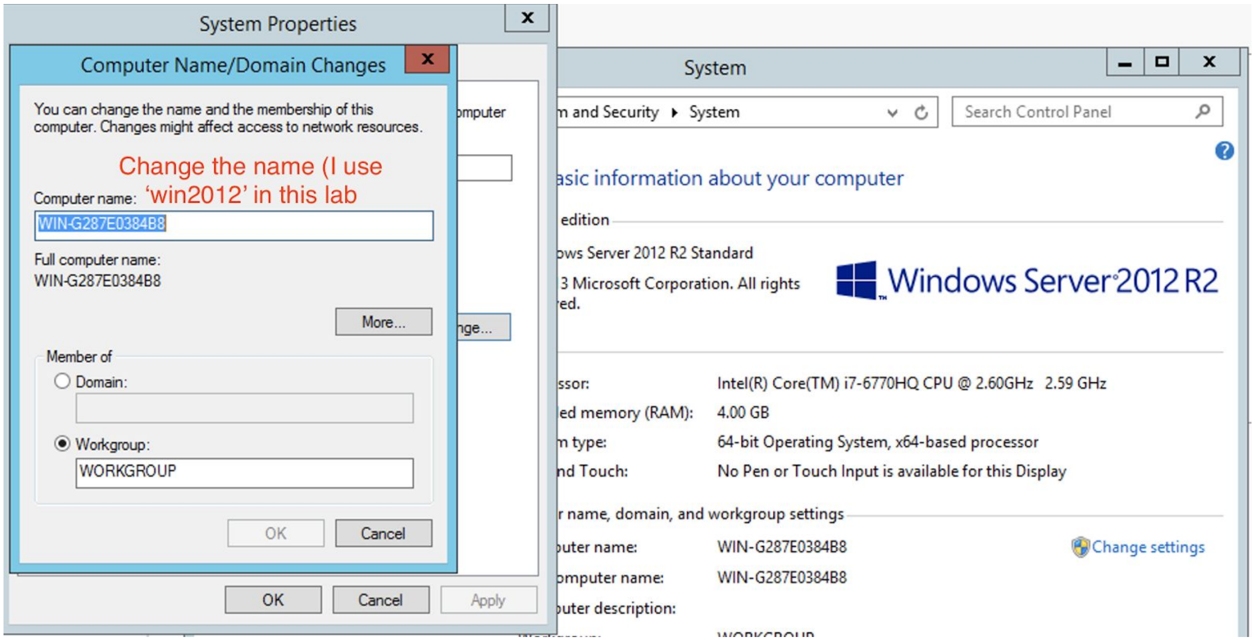
On install I immediately hardcoded a static IP (192.168.150.10) and a reachable name server (Umbrella's 208.67.222.222/208.67.220.220 are always great). This is purely for patching and further server function turnups

Note this initial patching takes a long time. Probably a good hour of fetching/installing. 3GB+ in updates, 3 reboots.

Installed the vmware guest tools after all the patching

Change the server name from the auto generated name (not crucial but not simplifies things)

Tip: I use 'example.com' as my AD name. While you can use anything you want, it's discouraged to use .local domains as they have special meaning for mDNS applications and some Linux OSs will not care for resolving .local domains as a standard domain. See this link for more information on this issue.



You can change the name and the membership of this computer. Changes might affect access to network resources.

Change the name (I use 'win2012' in this lab

Computer name: WIN-G287E0384B8

Full computer name:
WIN-G287E0384B8

Member of
○ Domain:
● Workgroup: WORKGROUP

asic information about your computer

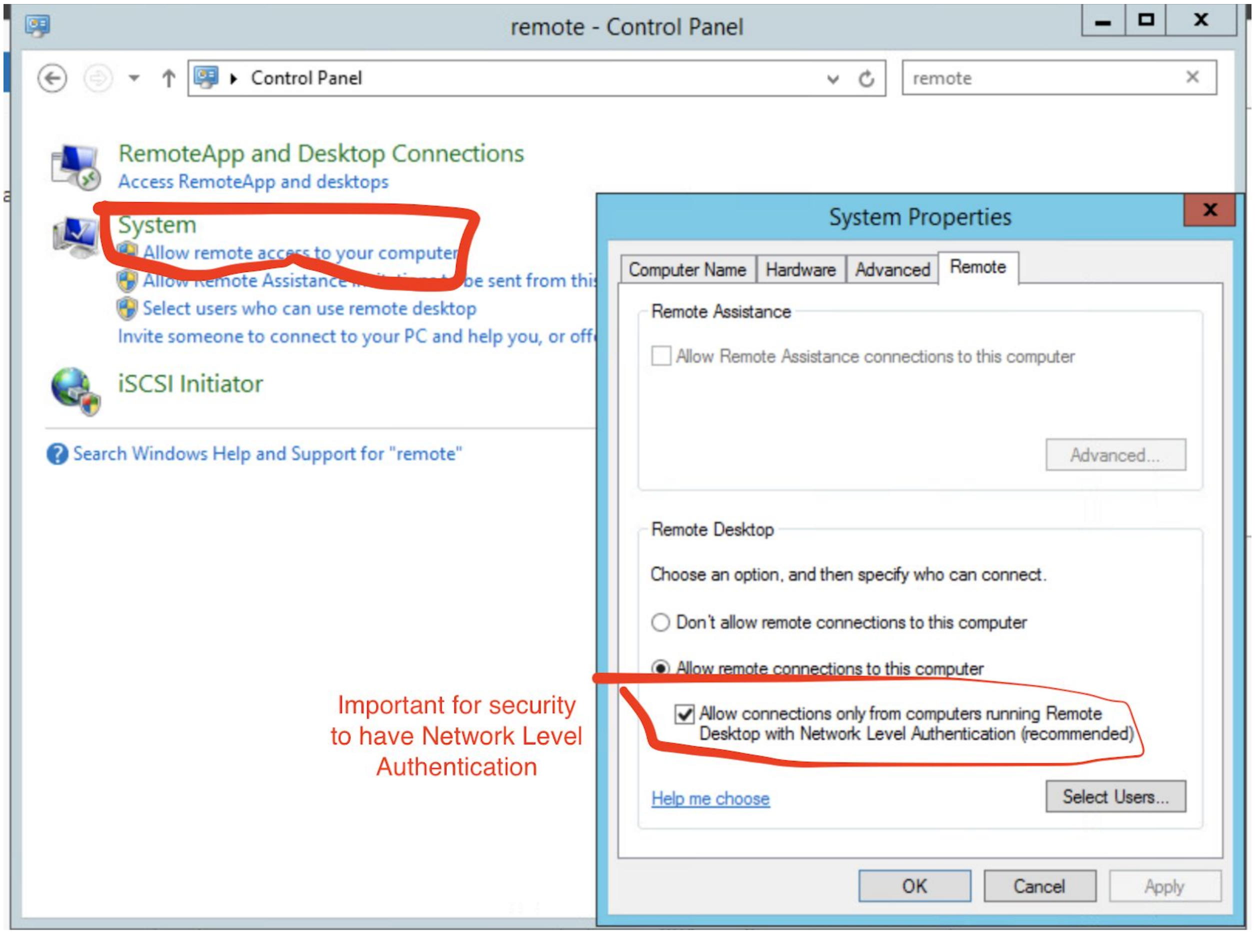
edition
ows Server 2012 R2 Standard
3 Microsoft Corporation. All rights
ed.

ssor: Intel(R) Core(TM) i7-6770HQ CPU @ 2.60GHz 2.59 GHz
ed memory (RAM): 4.00 GB
n type: 64-bit Operating System, x64-based processor
nd Touch: No Pen or Touch Input is available for this Display

r name, domain, and workgroup settings
puter name: WIN-G287E0384B8
omputer name: WIN-G287E0384B8
puter description:

Remote Desktop Access (Optional)

Found it tremendously helpful to enable RDP services to the server to configure the other settings.


remote - Control Panel
Control Panel
remote
RemoteApp and Desktop Connections
Access RemoteApp and desktops
System
Allow remote access to your computer
Select users who can use remote desktop
iSCSI Initiator
Search Windows Help and Support for "remote"
System Properties
Computer Name
Hardware
Advanced
Remote
Advanced...
Help me choose
Select Users...
OK
Cancel
Apply

Remote Assistance

☐ Allow Remote Assistance connections to this computer

Remote Desktop

Choose an option, and then specify who can connect.

○ Don't allow remote connections to this computer

● Allow remote connections to this computer

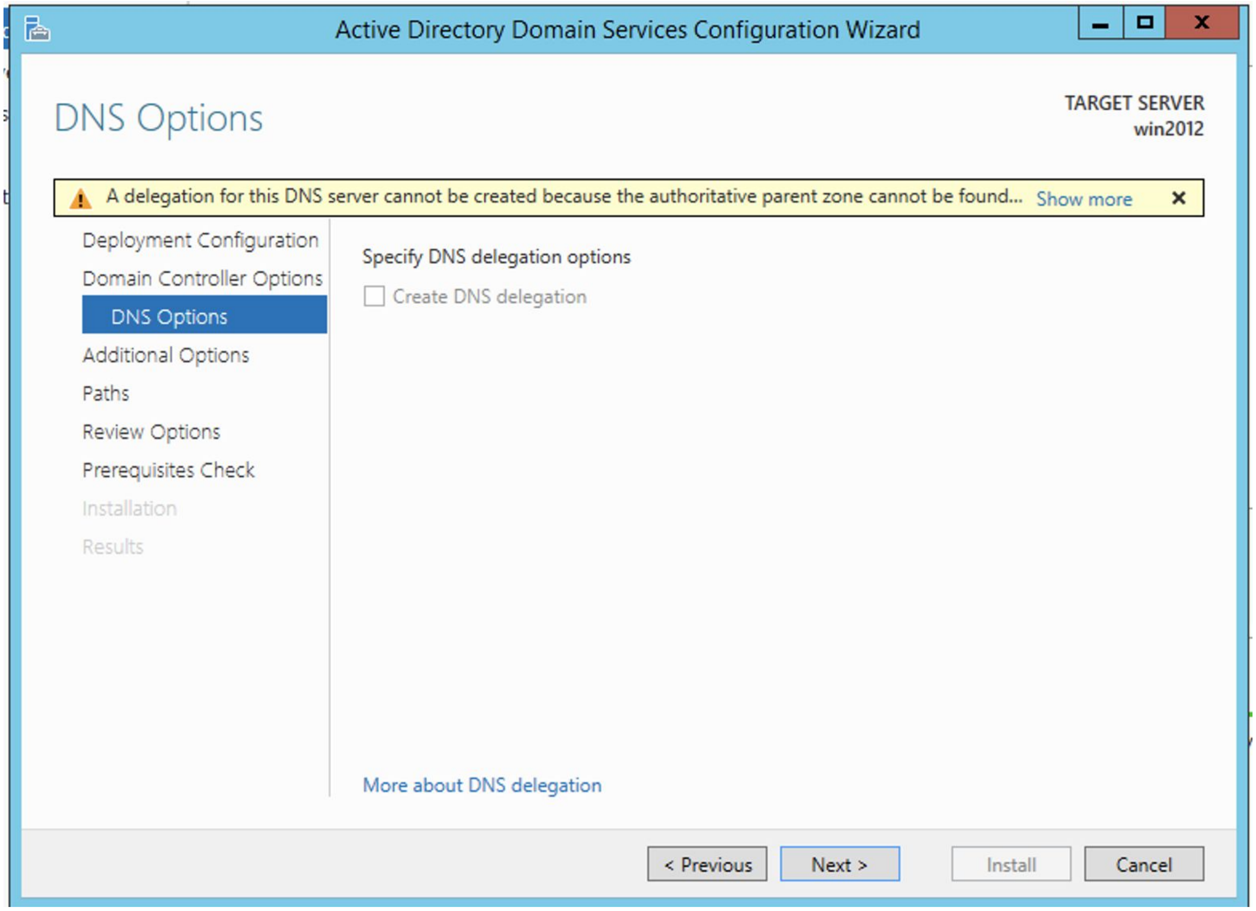
☑ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended)

Important for security to have Network Level Authentication

Active Directory Domain Services

This online guide should be easy enough to follow to setup ADDS for the first time. There are other, similar links out there to help. The biggest takeway is to not get hung up about no DNS server turned up (this setup will enable DNS services on this VM).

This is the message you can safely skip over, the server promotion will create all the required DNS server/zone configurations.

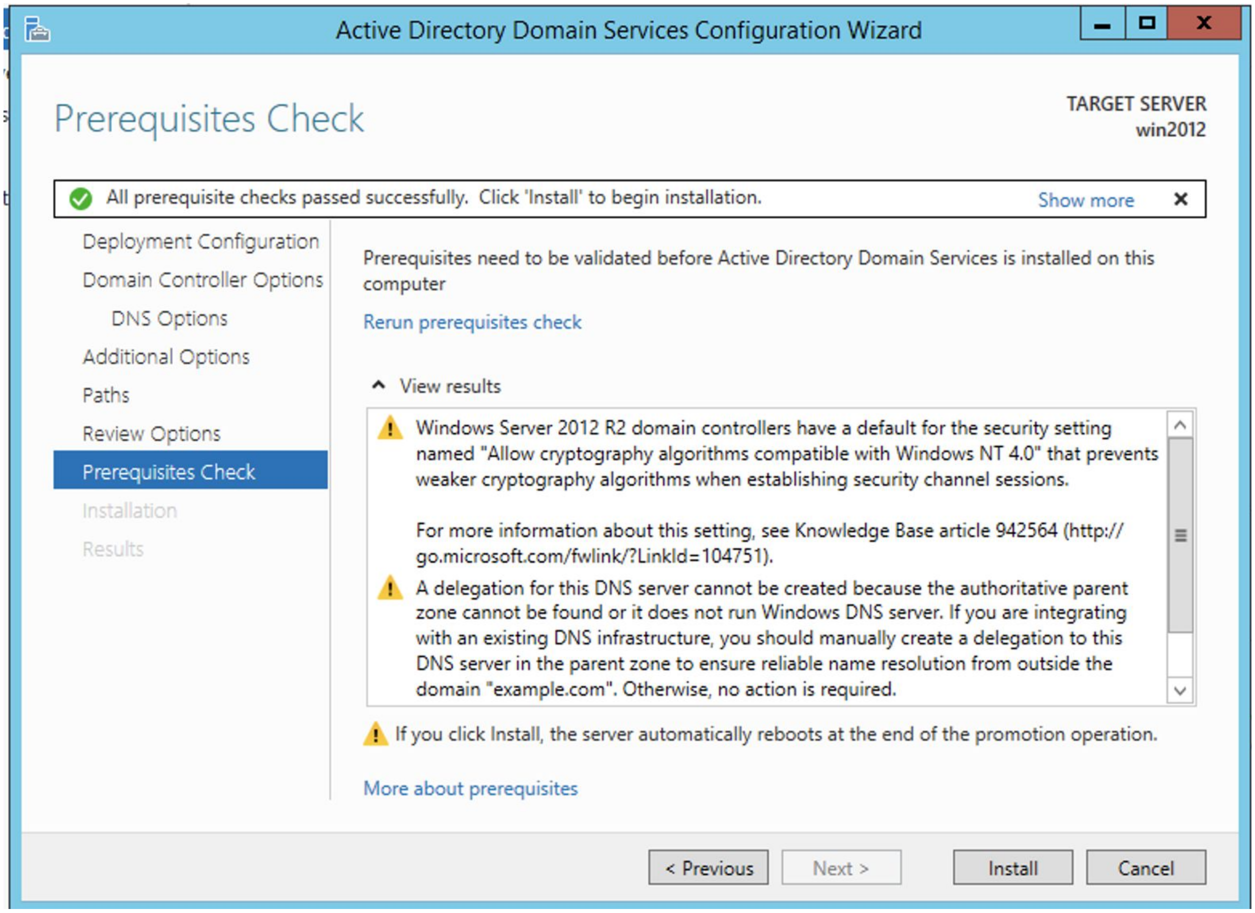


A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found...

Specify DNS delegation options

☐ Create DNS delegation

And you can ignore these warnings:



All prerequisite checks passed successfully. Click 'Install' to begin installation.

Prerequisites need to be validated before Active Directory Domain Services is installed on this computer

Windows Server 2012 R2 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions.

For more information about this setting, see Knowledge Base article 942564 (http://go.microsoft.com/fwlink/?LinkId=104751).

A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain "example.com". Otherwise, no action is required.

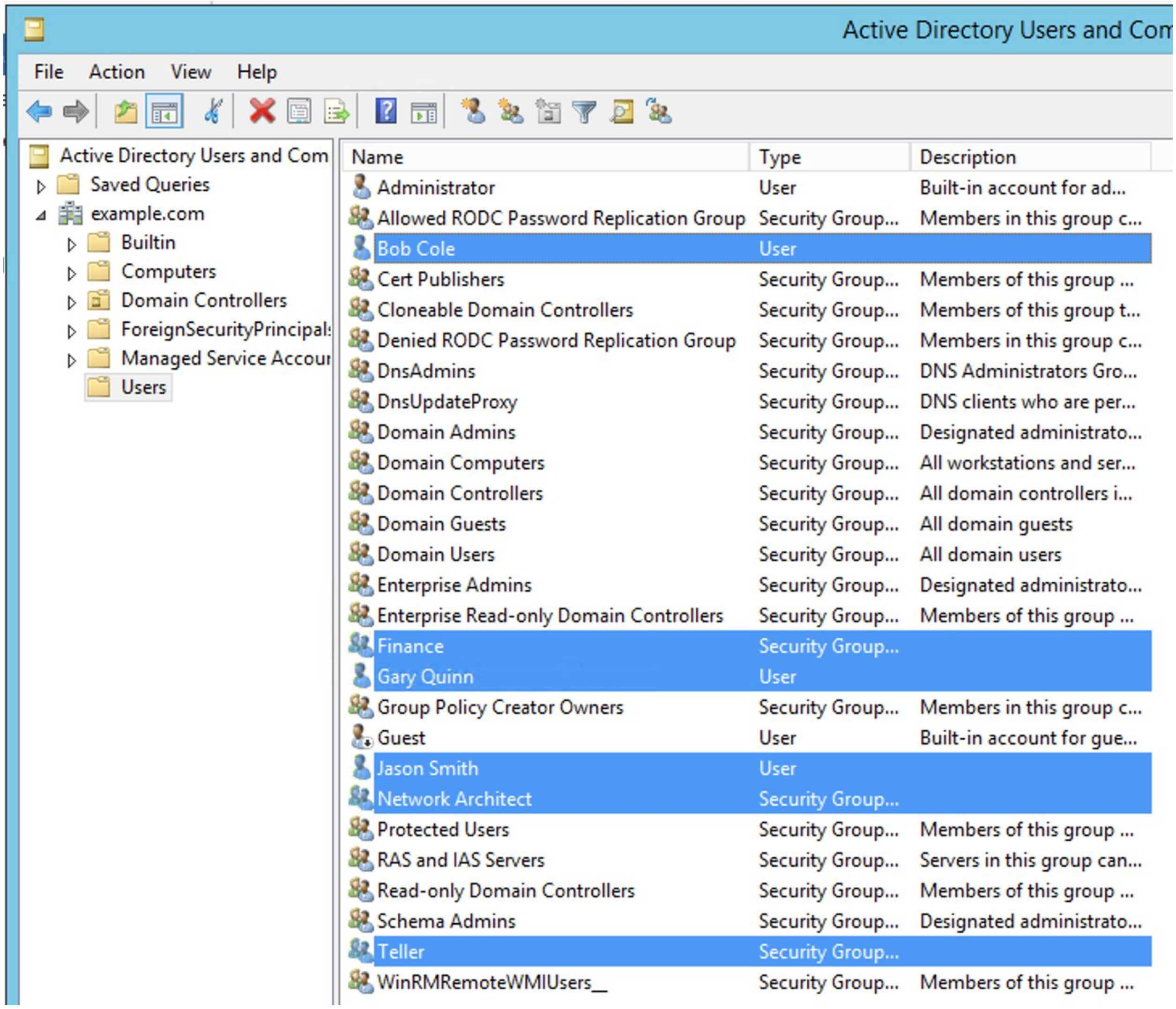
If you click Install, the server automatically reboots at the end of the promotion operation.

Users and Groups

Example Inc is a Financial institution (a Credit Union or a Bank) and as such there will be three different roles that will directly influence IP access. These are the accounts we'll be creating (and corresponding groups):

Username	Role (Group)	Permissions	Notes
gaquinn (Gary Quinn)	Network Architect	Full Access	
bcole (Bob Cole)	Teller	Only access to Teller Subnet	
jsmith (Jason Smith)	Finance	Finance subnets and Internet access	

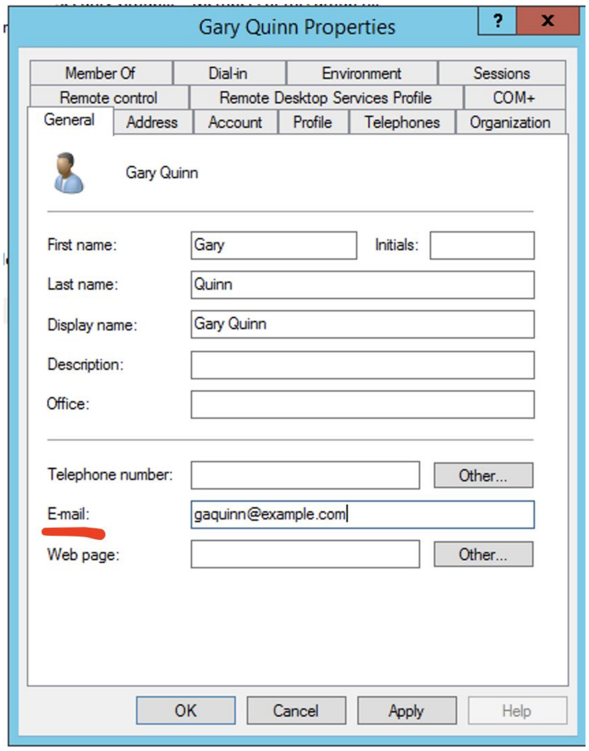
My finished product looks like this:



- Active Directory Users and Com
  - Saved Queries
  - example.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Managed Service Accour
    - Users

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Password Replication Group	Security Group...	Members in this group c...
Bob Cole	User	
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
Denied RODC Password Replication Group	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Read-only Domain Controllers	Security Group...	Members of this group ...
Finance	Security Group...	
Gary Quinn	User	
Group Policy Creator Owners	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Jason Smith	User	
Network Architect	Security Group...	
Protected Users	Security Group...	Members of this group ...
RAS and IAS Servers	Security Group...	Servers in this group can...
Read-only Domain Controllers	Security Group...	Members of this group ...
Schema Admins	Security Group...	Designated administrato...
Teller	Security Group...	
WinRMRemoteWMIUsers__	Security Group...	Members of this group ...

Pro Tip Add in email addresses into the user accounts. This value is used for automatic client certification generation in the CA step later in this guide



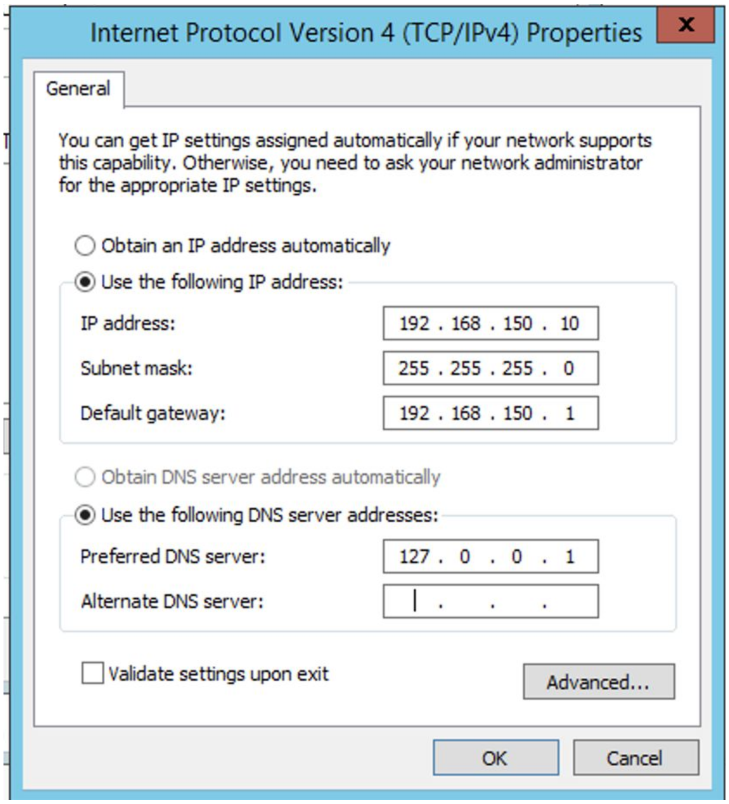
Gary Quinn Properties

Gary Quinn

First name: Gary
Initials:
Last name: Quinn
Display name: Gary Quinn
Description:
Office:
Telephone number:
E-mail: gaquinn@example.com
Web page:

DNS Settings

After ADDS installation and promotion DNS server is properly installed and these should be where we are:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

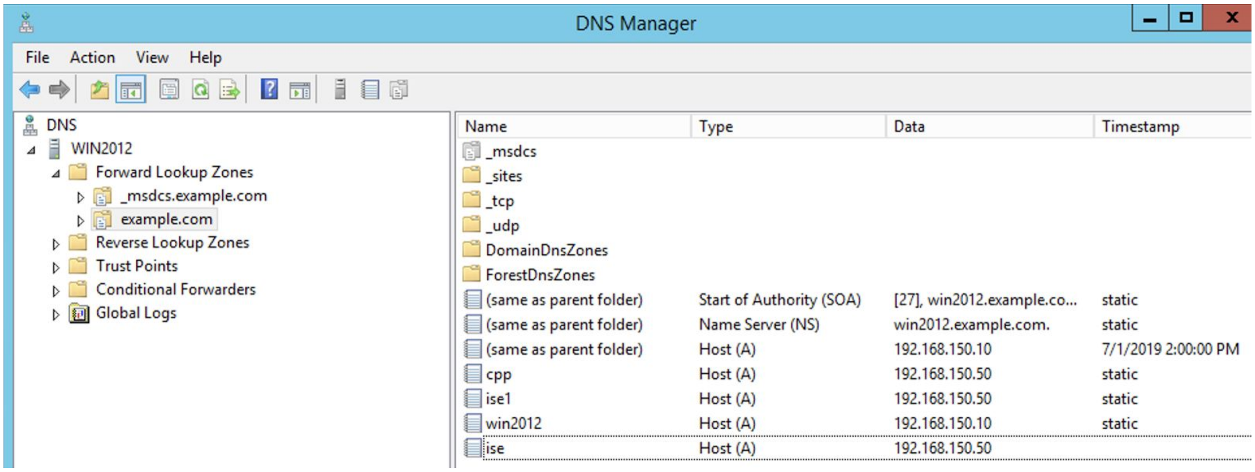
○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 150 . 10
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 150 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 127 . 0 . 0 . 1
Alternate DNS server: . . .

☐ Validate settings upon exit

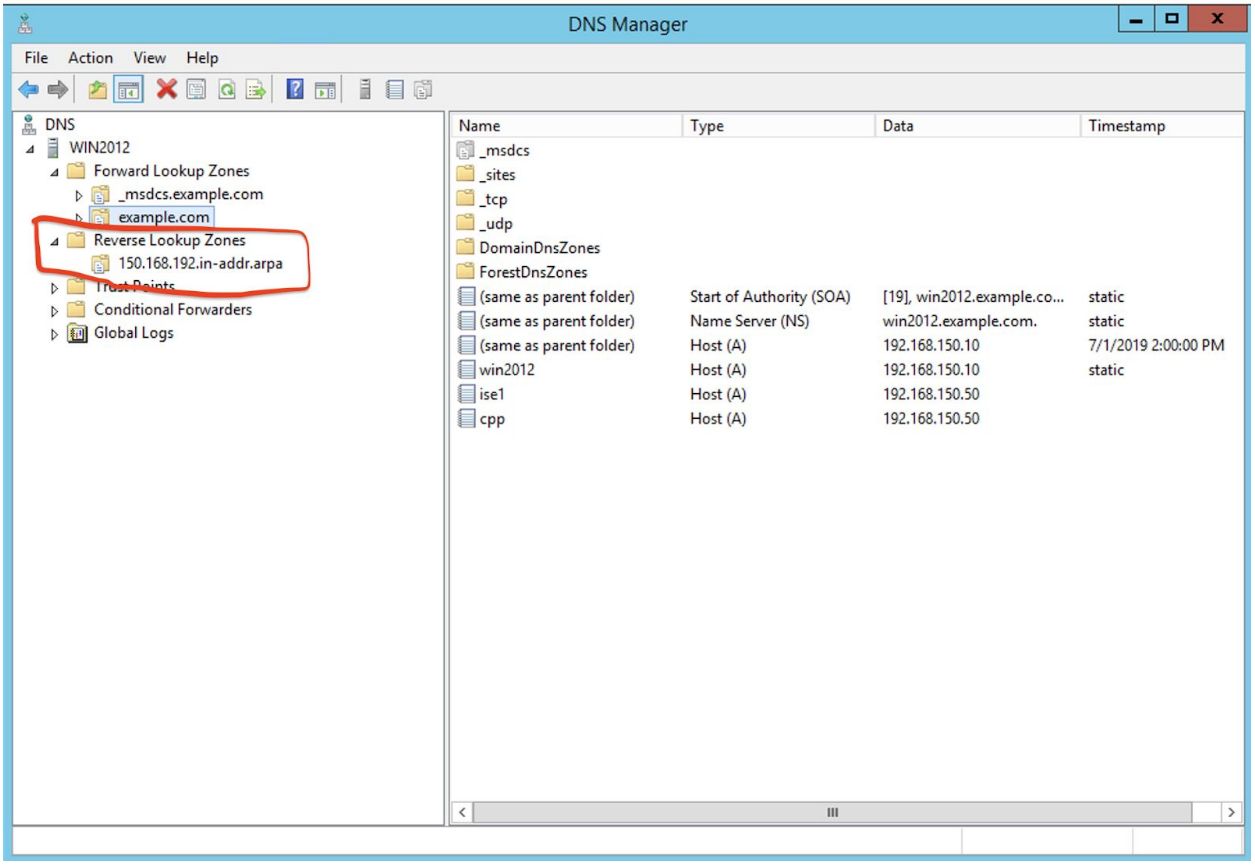


Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[27], win2012.example.co...	static
(same as parent folder)	Name Server (NS)	win2012.example.com.	static
(same as parent folder)	Host (A)	192.168.150.10	7/1/2019 2:00:00 PM
cpp	Host (A)	192.168.150.50	static
ise1	Host (A)	192.168.150.50	static
win2012	Host (A)	192.168.150.10	static
ise	Host (A)	192.168.150.50	

Some DNS records need to be created for ISE to function. They're listed below:

DNS Record	Function	Note
ise1.example.com	Staple Record	Used for multi deployments and Posturing
cpp.example.com	Client Provisioning Portal	Used for Posturing

This is what mine looks like at this point. Note that the reverse lookup zone must be manually created before you make the new records. Just right click and create new, pretty easy.



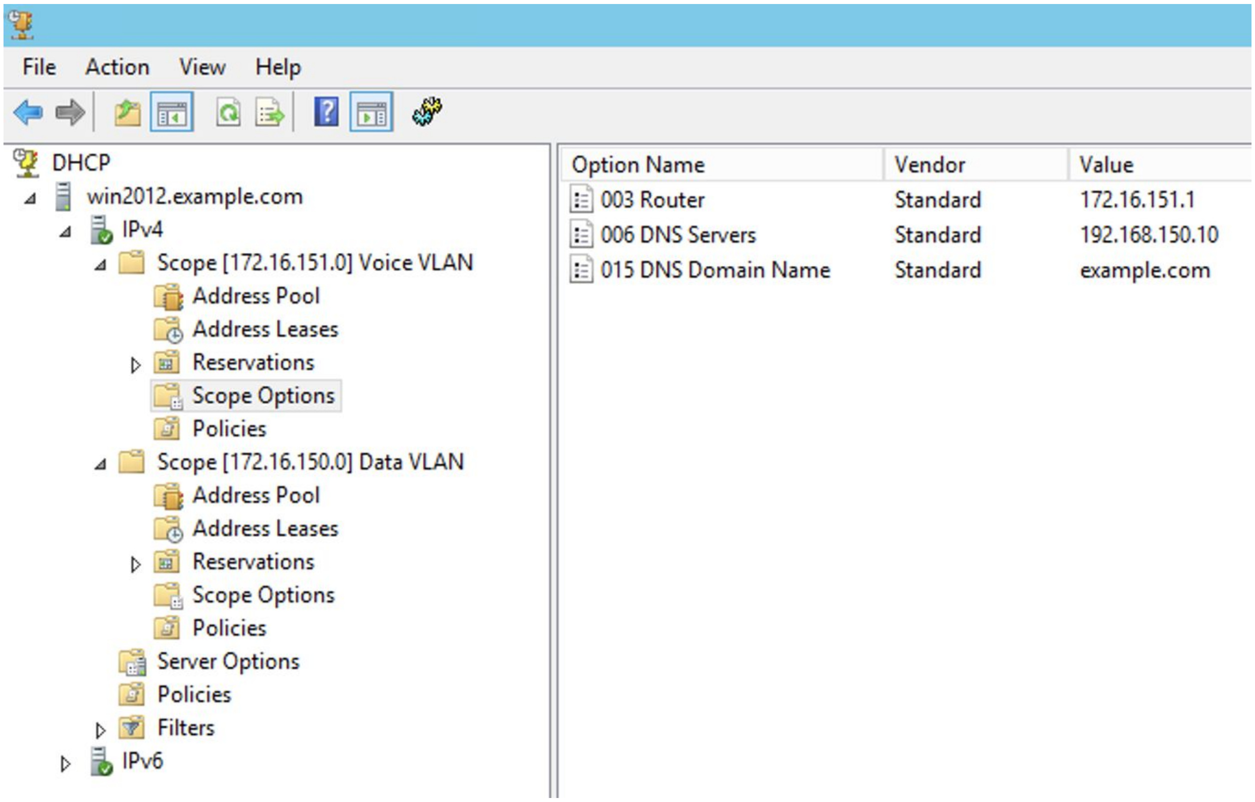
Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[19], win2012.example.co...	static
(same as parent folder)	Name Server (NS)	win2012.example.com.	static
(same as parent folder)	Host (A)	192.168.150.10	7/1/2019 2:00:00 PM
win2012	Host (A)	192.168.150.10	static
ise1	Host (A)	192.168.150.50	
cpp	Host (A)	192.168.150.50	

DHCP

I'm using MS DHCP server in my lab because that's what most organizations will be using so I'm enclosing it here for completeness. The DHCP server is installed by the same 'Add Roles and Features' wizard, taking the defaults.

I loaded up two DHCP scopes (one for Voice and one for Data). Additional ones could be used for Guest, Quarantine, etc.

What mine looks like at this step:



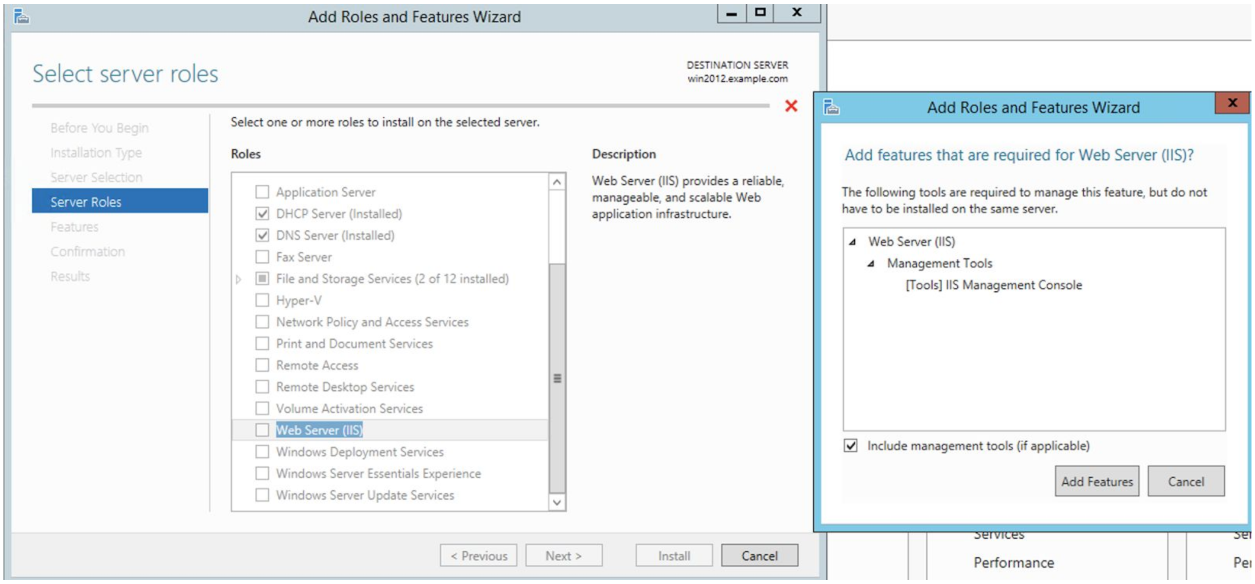
Option Name	Vendor	Value
003 Router	Standard	172.16.151.1
006 DNS Servers	Standard	192.168.150.10
015 DNS Domain Name	Standard	example.com

Certificate Authority

The certificate authority configuration is probably the most confusing step of this build so I will try to be as step-by-step as possible:

IIS Server

The IIS Server is required in order to access the Certificate Services web interface, so install that before the CA. Just take the defaults:



Select server roles

DESTINATION SERVER
win2012.example.com

Select one or more roles to install on the selected server.

Roles

- ☐ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ▨ File and Storage Services (2 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Essentials Experience
- ☐ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

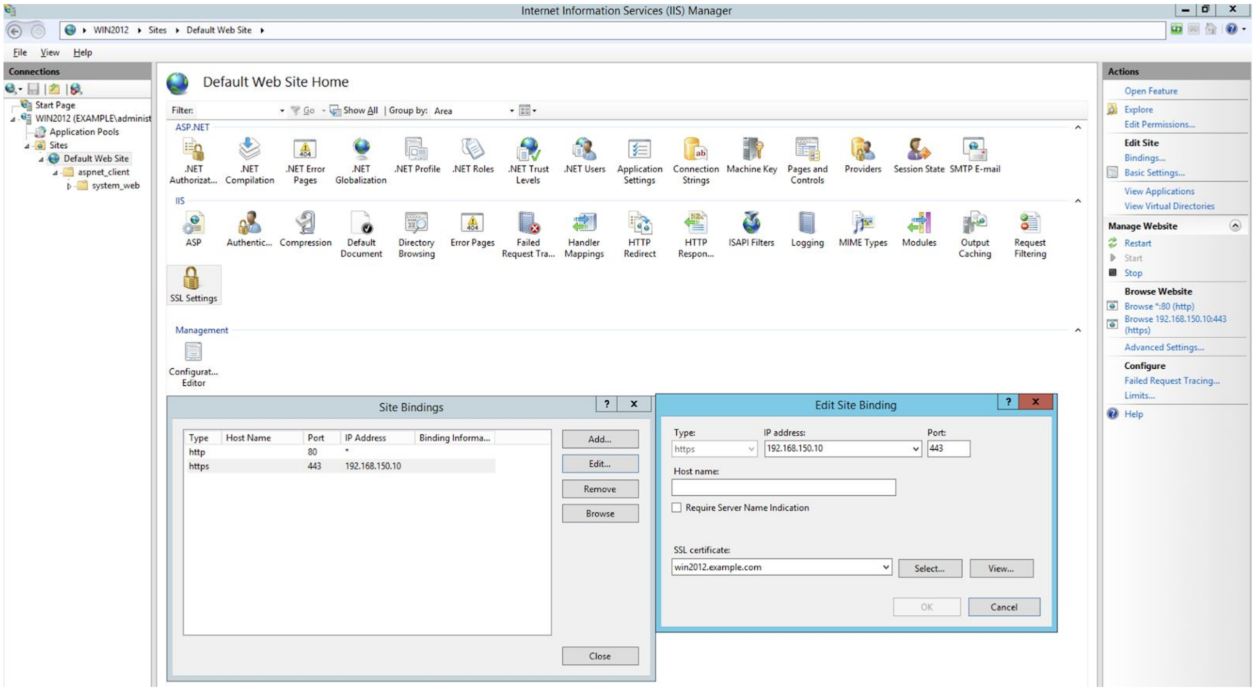
Add features that are required for Web Server (IIS)?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Web Server (IIS)
  - Management Tools
    - [Tools] IIS Management Console

☑ Include management tools (if applicable)

Optional: Enable HTTPS on the web server (you may have to bounce back to this step after you install the CA server). While not required, it's good security hygiene



Site Bindings

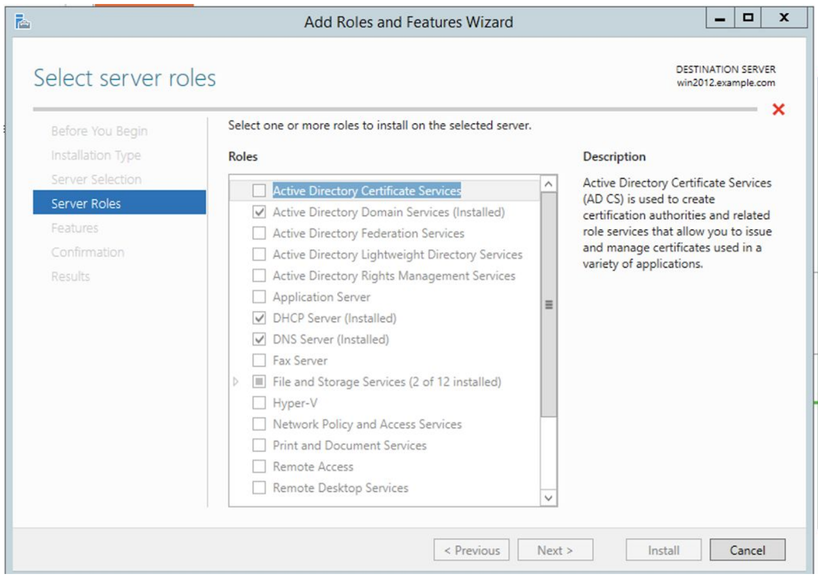
Type	Host Name	Port	IP Address	Binding Informa...
http		80	*	
https		443	192.168.150.10	

Edit Site Binding

Type: https
IP address: 192.168.150.10
Port: 443
Host name:
☐ Require Server Name Indication
SSL certificate: win2012.example.com

CA (Certificate Authority) Install

I take several passes at this. The first is to install the CA and configure the CA certificate



Select server roles

DESTINATION SERVER
win2012.example.com

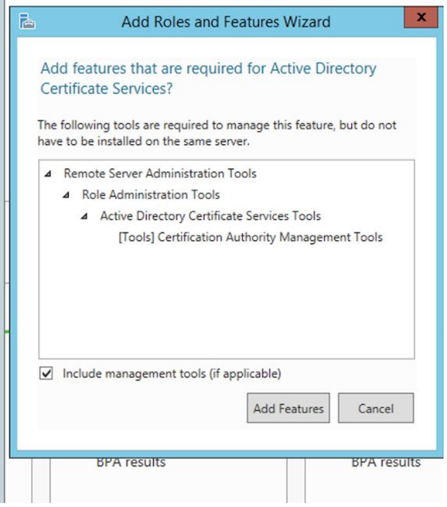
Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- ☐ Fax Server
- ▨ File and Storage Services (2 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

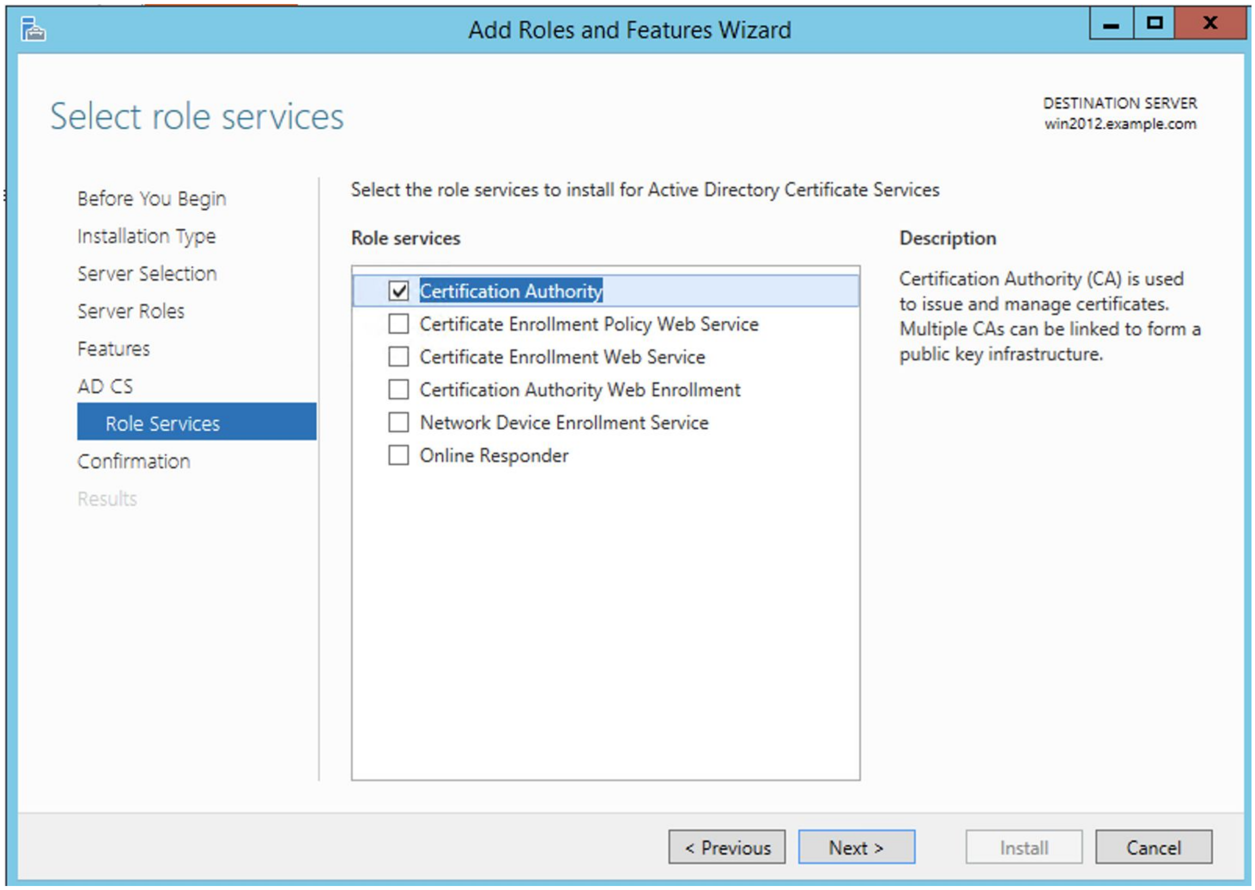


Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Certification Authority Management Tools

☑ Include management tools (if applicable)



Select role services

DESTINATION SERVER
win2012.example.com

Select the role services to install for Active Directory Certificate Services

Role services

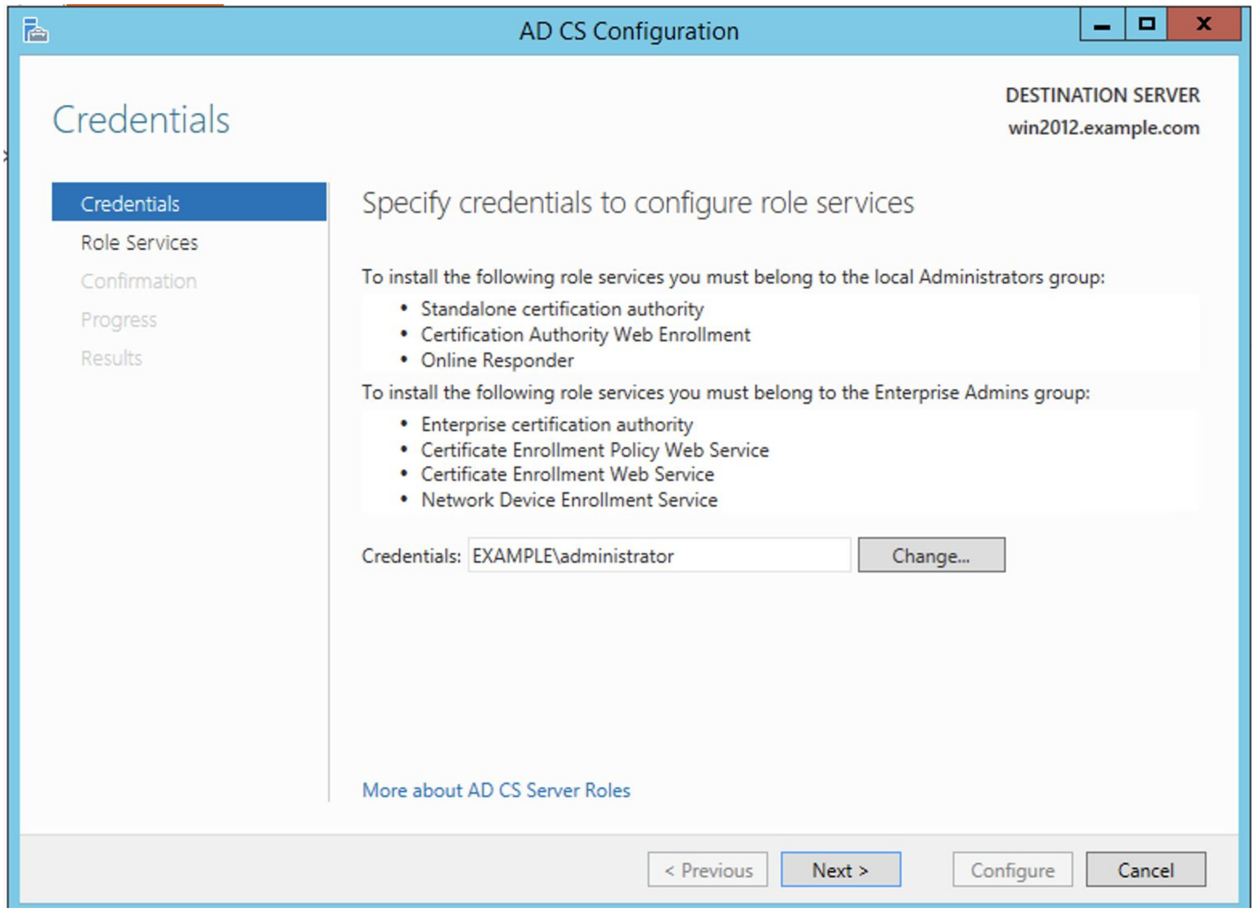
- ☑ Certification Authority
- ☐ Certificate Enrollment Policy Web Service
- ☐ Certificate Enrollment Web Service
- ☐ Certification Authority Web Enrollment
- ☐ Network Device Enrollment Service
- ☐ Online Responder

Description

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

CA (Certificate Authority) Configuration

These are most of the screenshots of the CA configuration (if a step is missing, take the default)



Specify credentials to configure role services

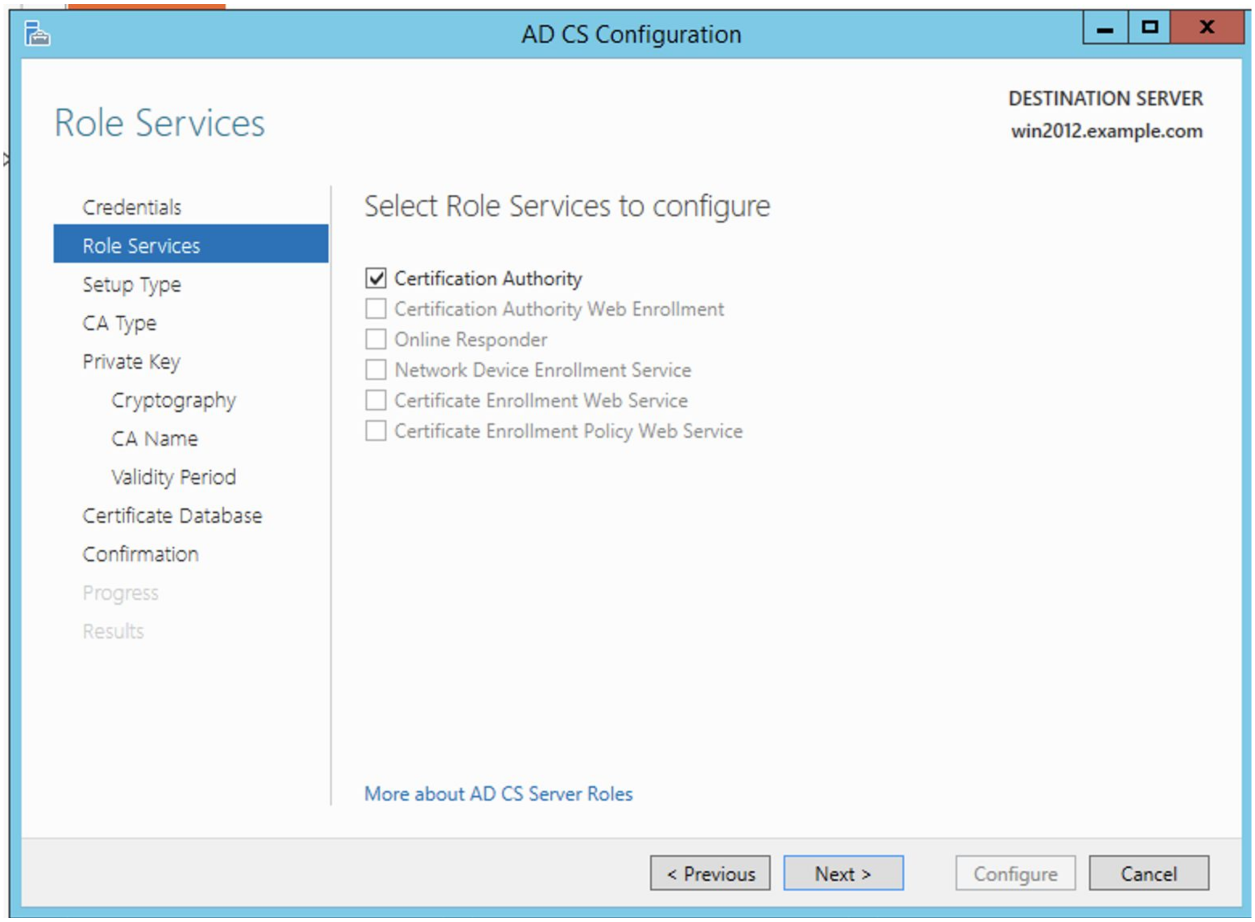
To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: EXAMPLE\administrator

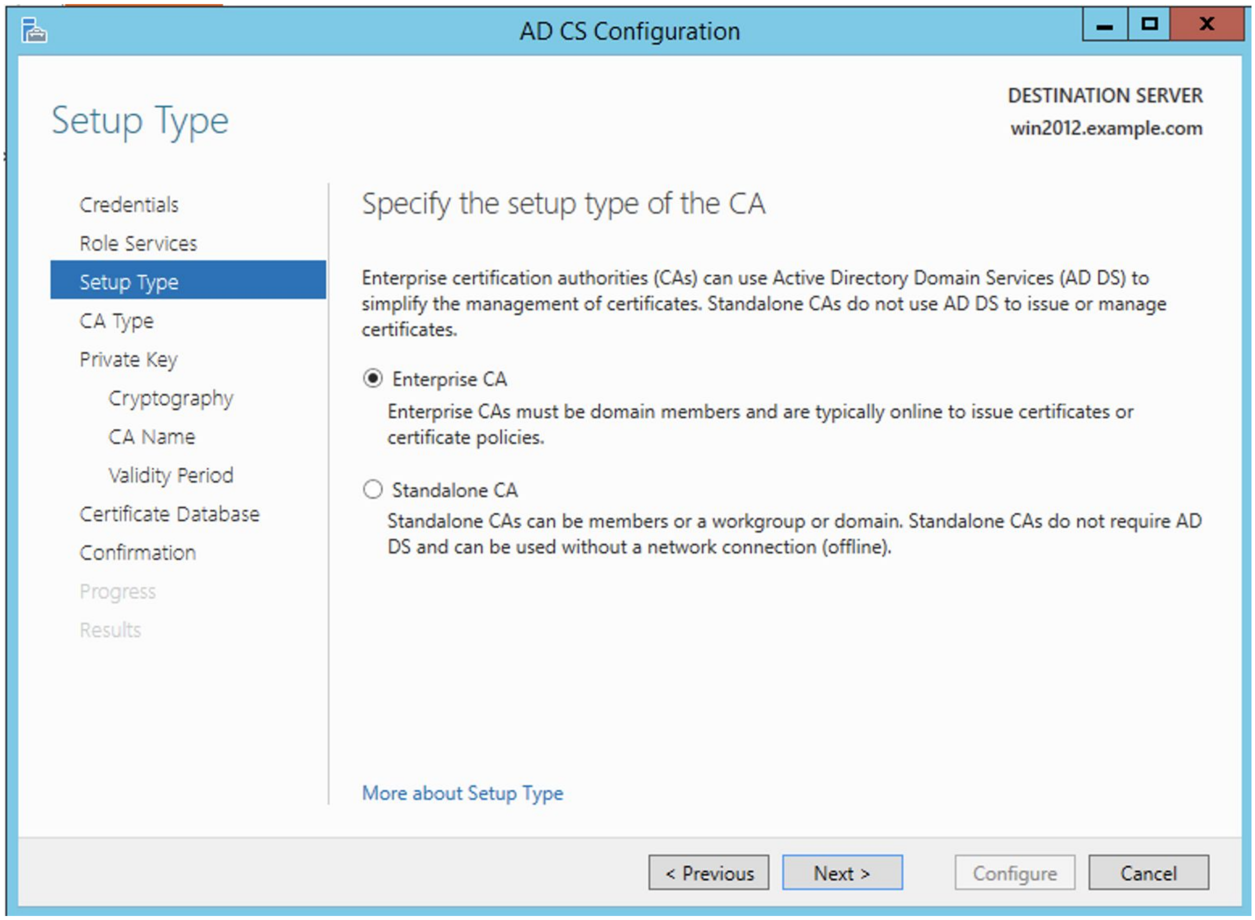


Role Services

DESTINATION SERVER
win2012.example.com

Select Role Services to configure

☑ Certification Authority
☐ Certification Authority Web Enrollment
☐ Online Responder
☐ Network Device Enrollment Service
☐ Certificate Enrollment Web Service
☐ Certificate Enrollment Policy Web Service



Specify the setup type of the CA

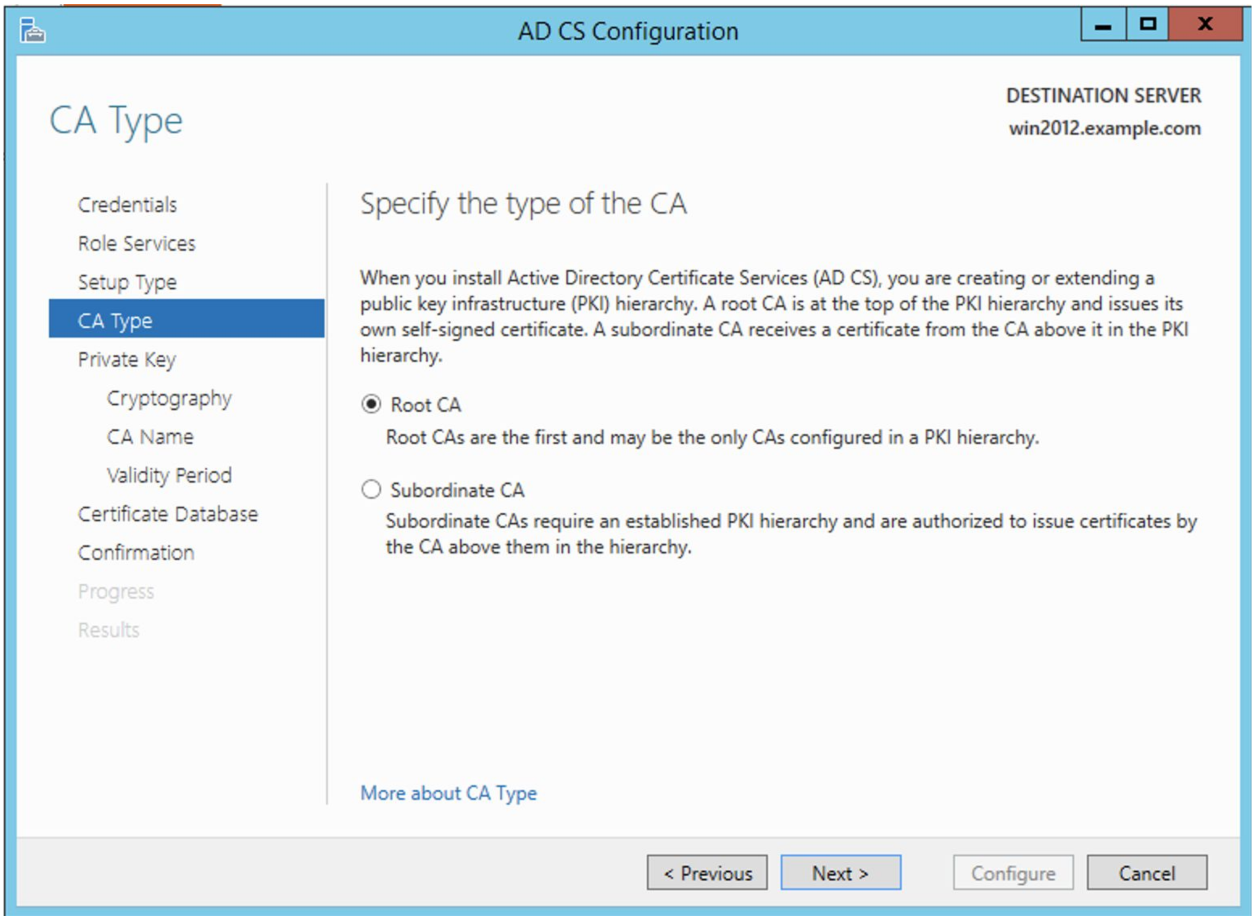
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

○ Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).



CA Type

DESTINATION SERVER
win2012.example.com

Specify the type of the CA

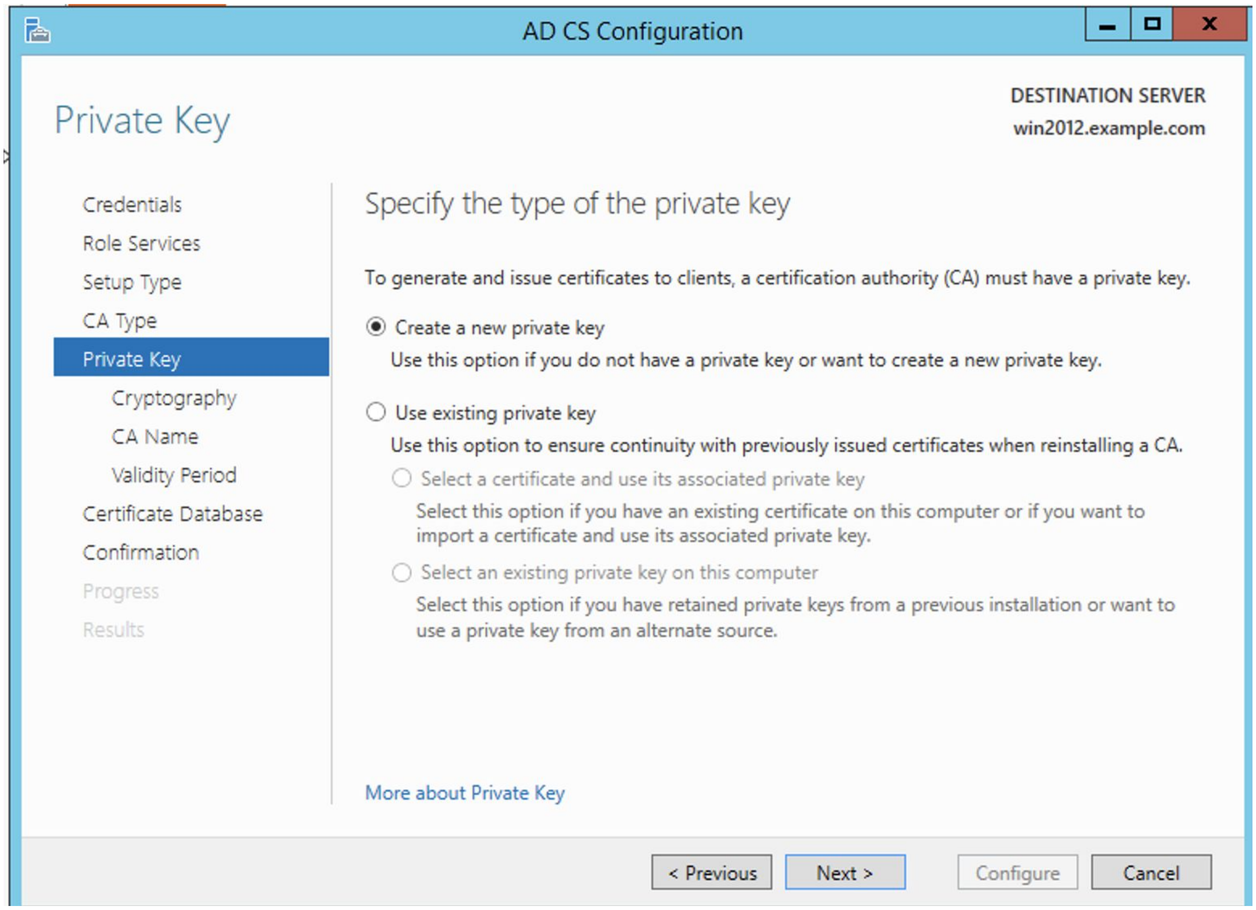
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

● Root CA

Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA

Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.



Private Key

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

● Create a new private key

Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key

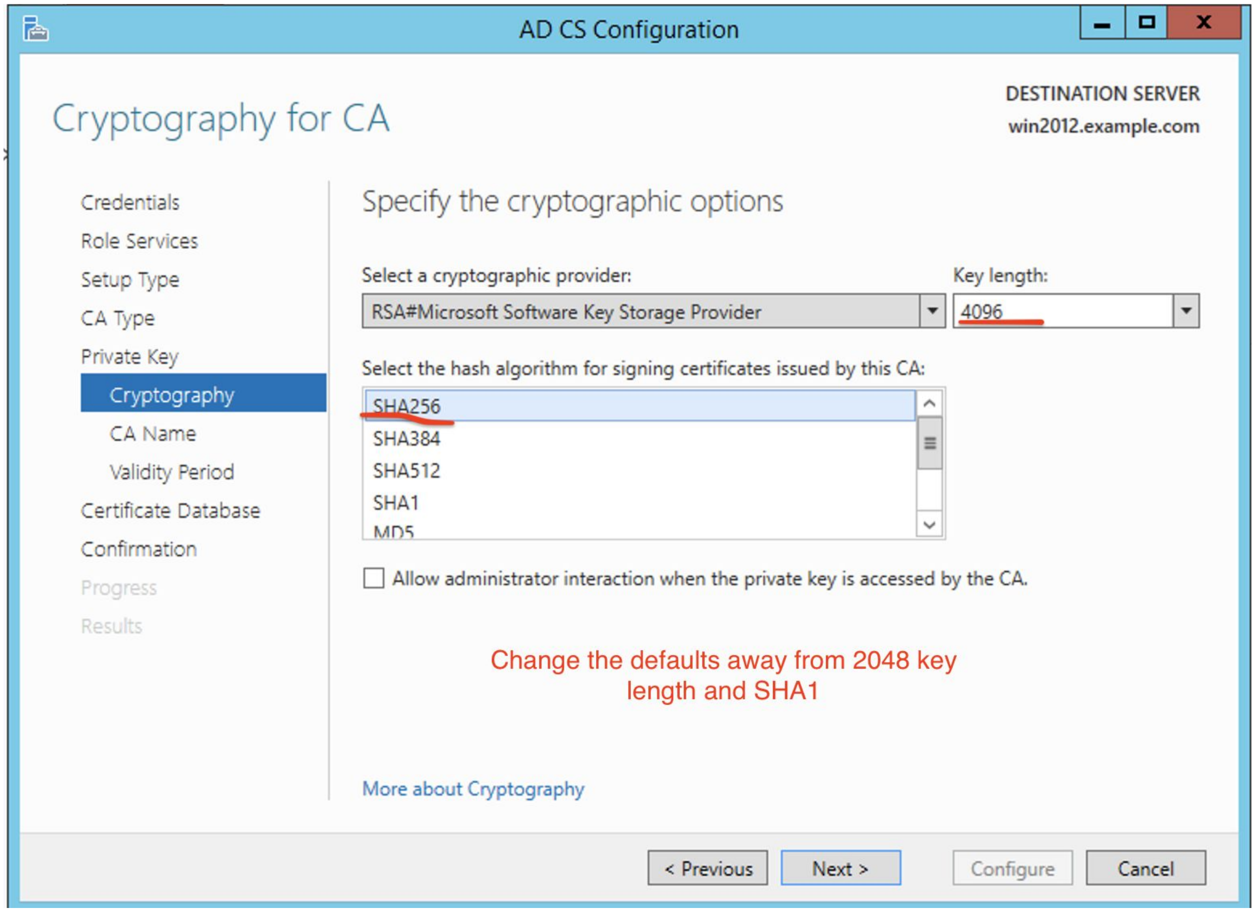
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ Select a certificate and use its associated private key

Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer

Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.



Cryptography for CA

DESTINATION SERVER
win2012.example.com

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

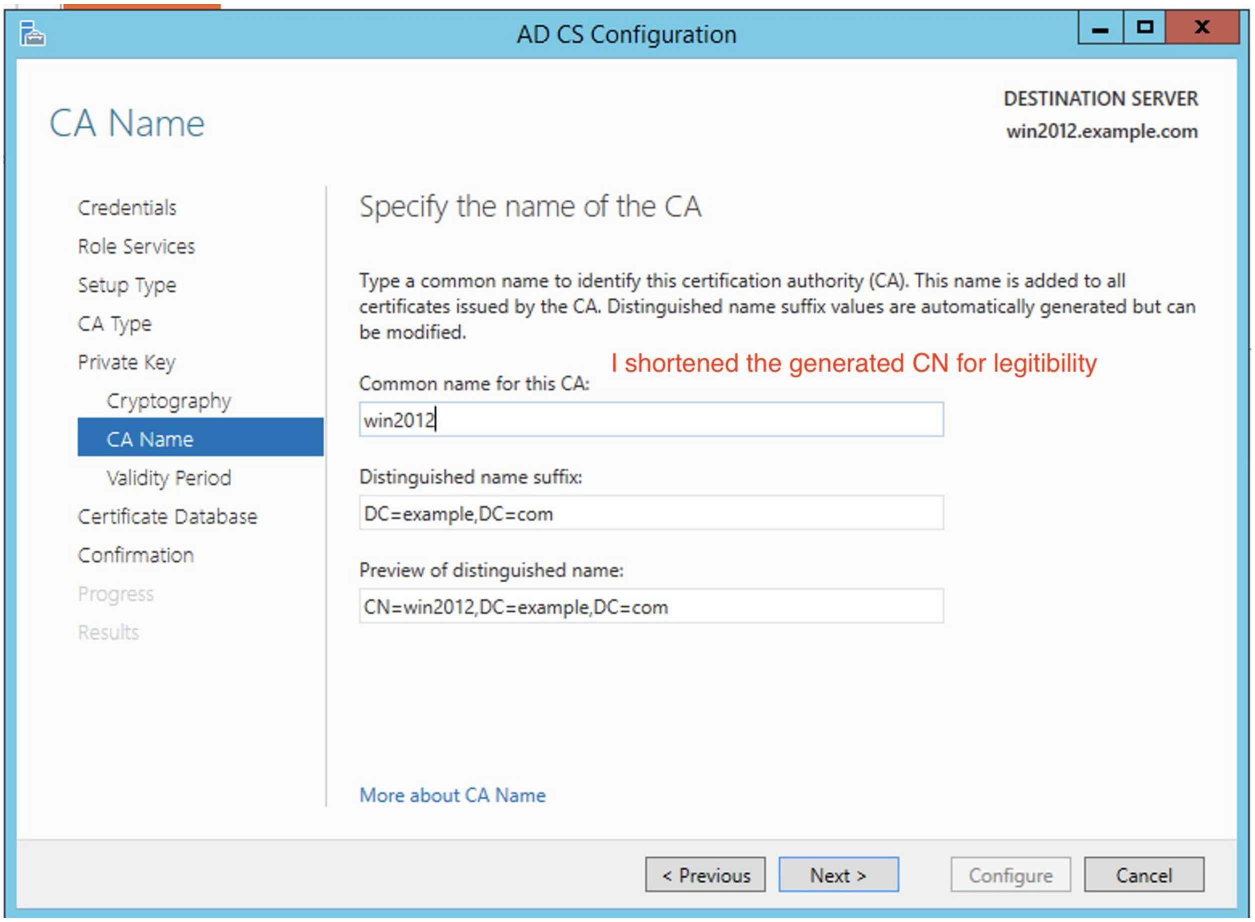
Key length: 4096

Select the hash algorithm for signing certificates issued by this CA:

- SHA256
- SHA384
- SHA512
- SHA1
- MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

Change the defaults away from 2048 key length and SHA1



Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

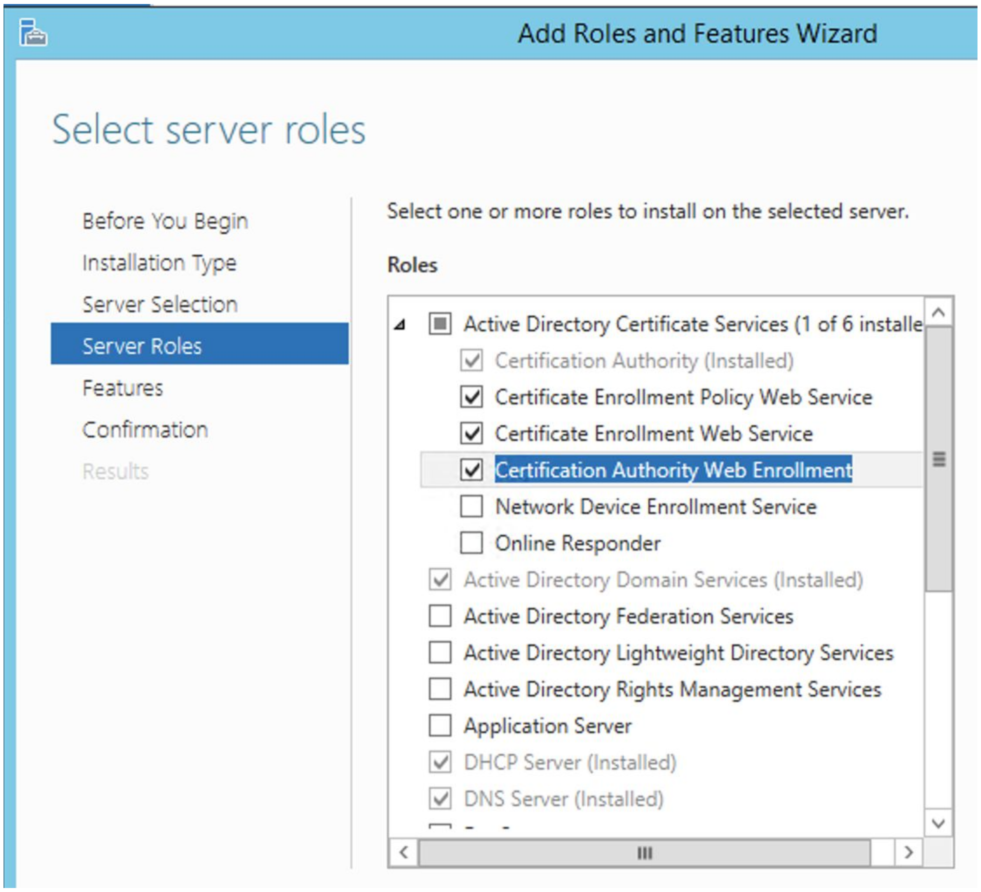
I shortened the generated CN for legitibility

Common name for this CA: win2012

Distinguished name suffix: DC=example,DC=com

Preview of distinguished name: CN=win2012,DC=example,DC=com

Now go back and install the Web Services for the CA, take the defaults.



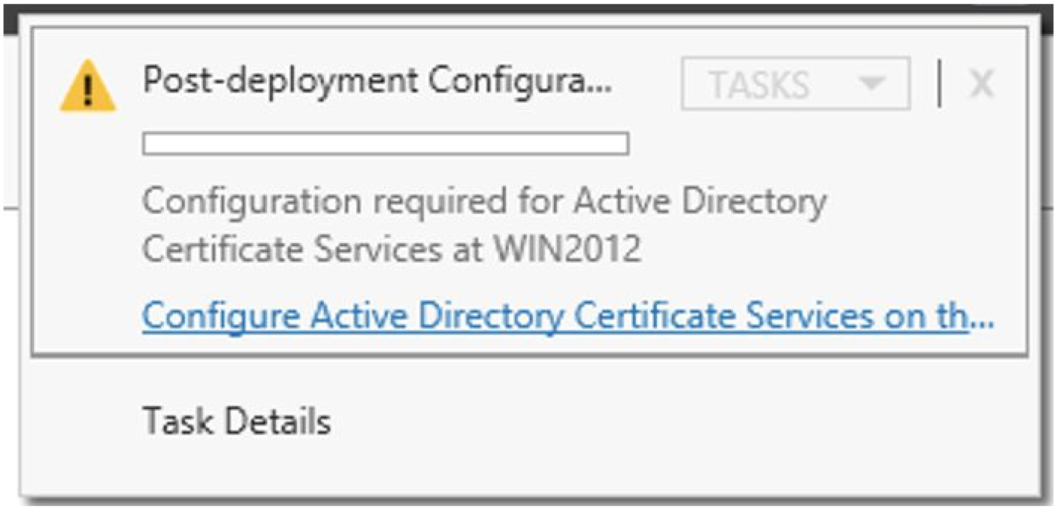
Select server roles

Select one or more roles to install on the selected server.

Roles

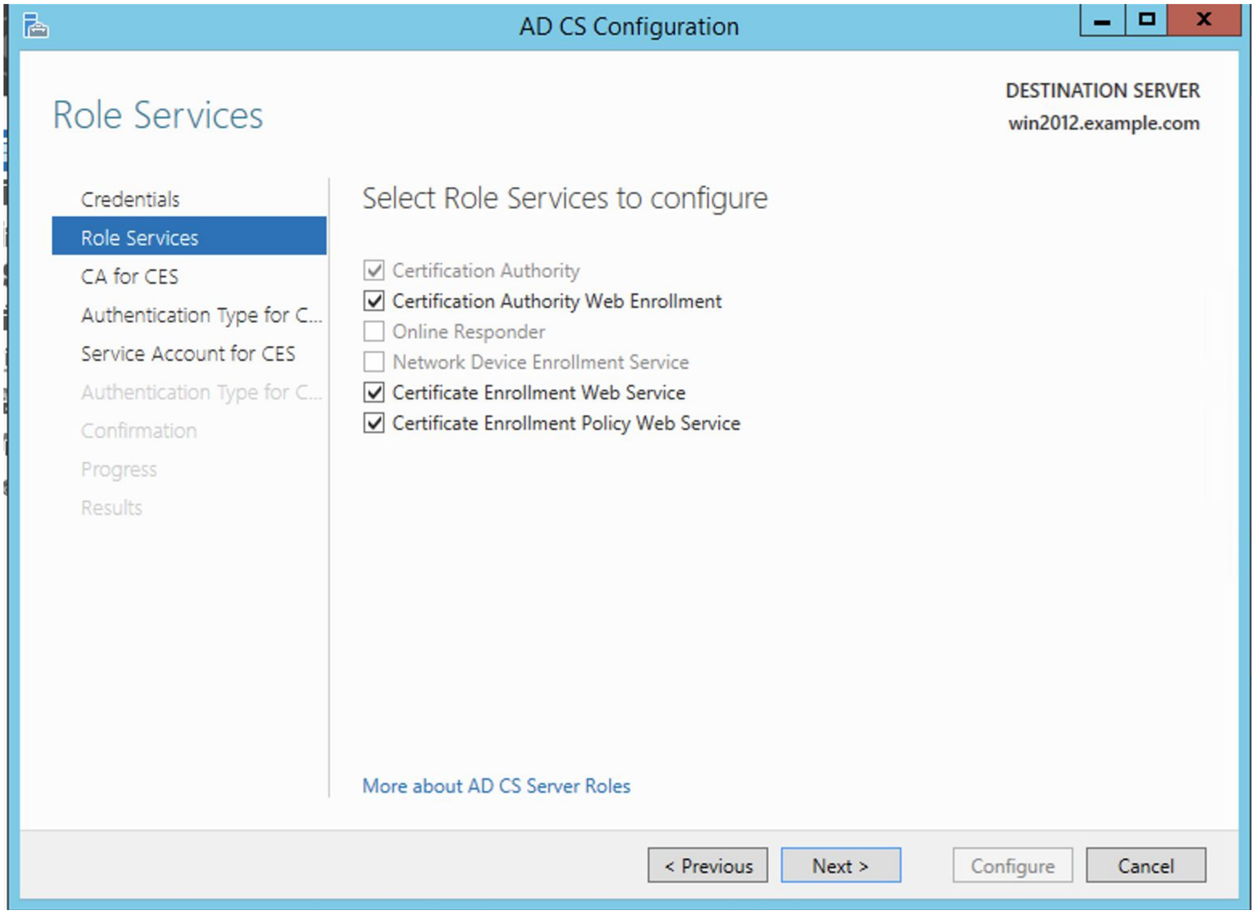
- ■ Active Directory Certificate Services (1 of 6 installe
  - ☑ Certification Authority (Installed)
  - ☑ Certificate Enrollment Policy Web Service
  - ☑ Certificate Enrollment Web Service
  - ☑ Certification Authority Web Enrollment
  - ☐ Network Device Enrollment Service
  - ☐ Online Responder
- ☑ Active Directory Domain Services (Installed)
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Application Server
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)

After installation of these new servers you may need to reboot in order for Windows Server to give you the option to Configure the new Web services:



Configuration required for Active Directory Certificate Services at WIN2012

Configure Active Directory Certificate Services on th...

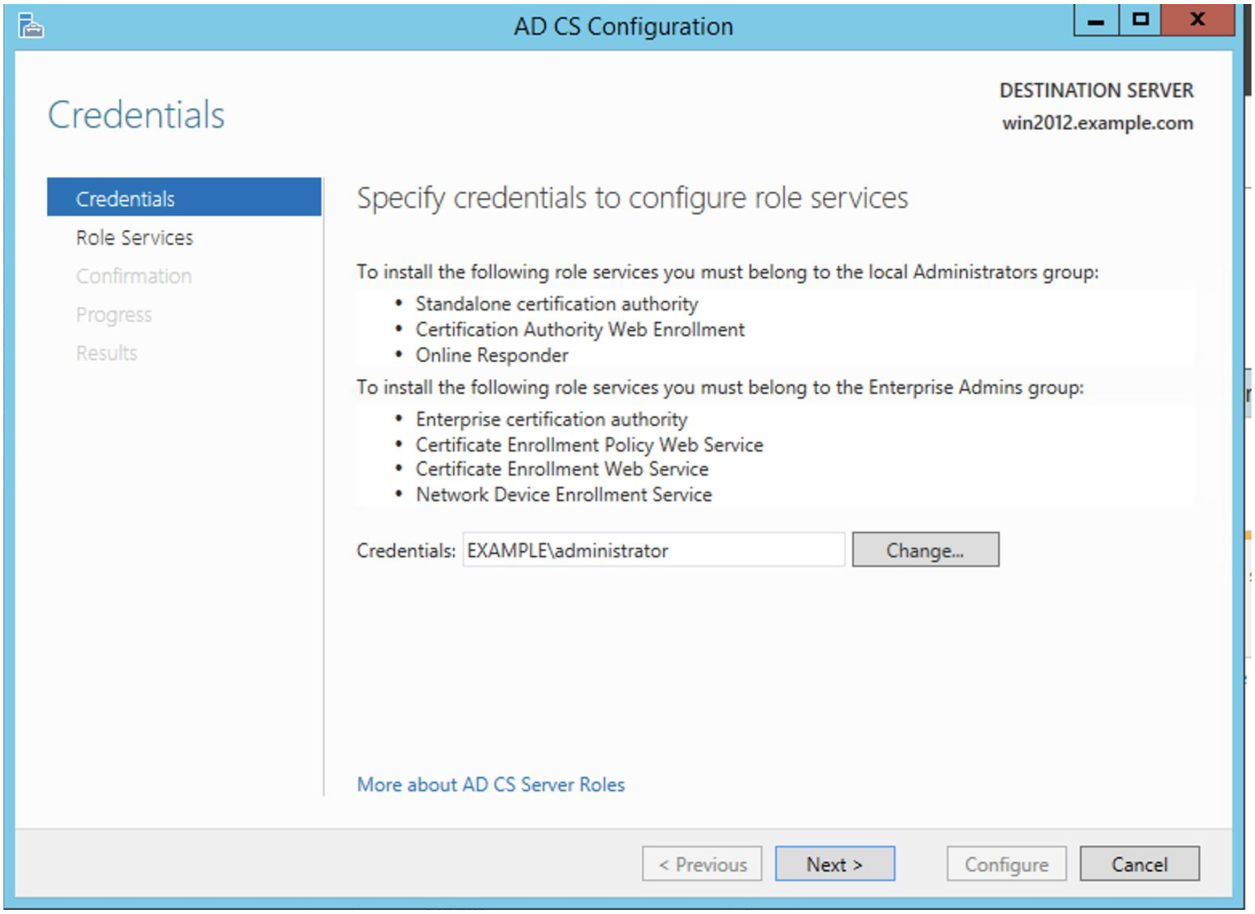


Role Services

DESTINATION SERVER
win2012.example.com

Select Role Services to configure

- ☑ Certification Authority
- ☑ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☑ Certificate Enrollment Web Service
- ☑ Certificate Enrollment Policy Web Service



Specify credentials to configure role services

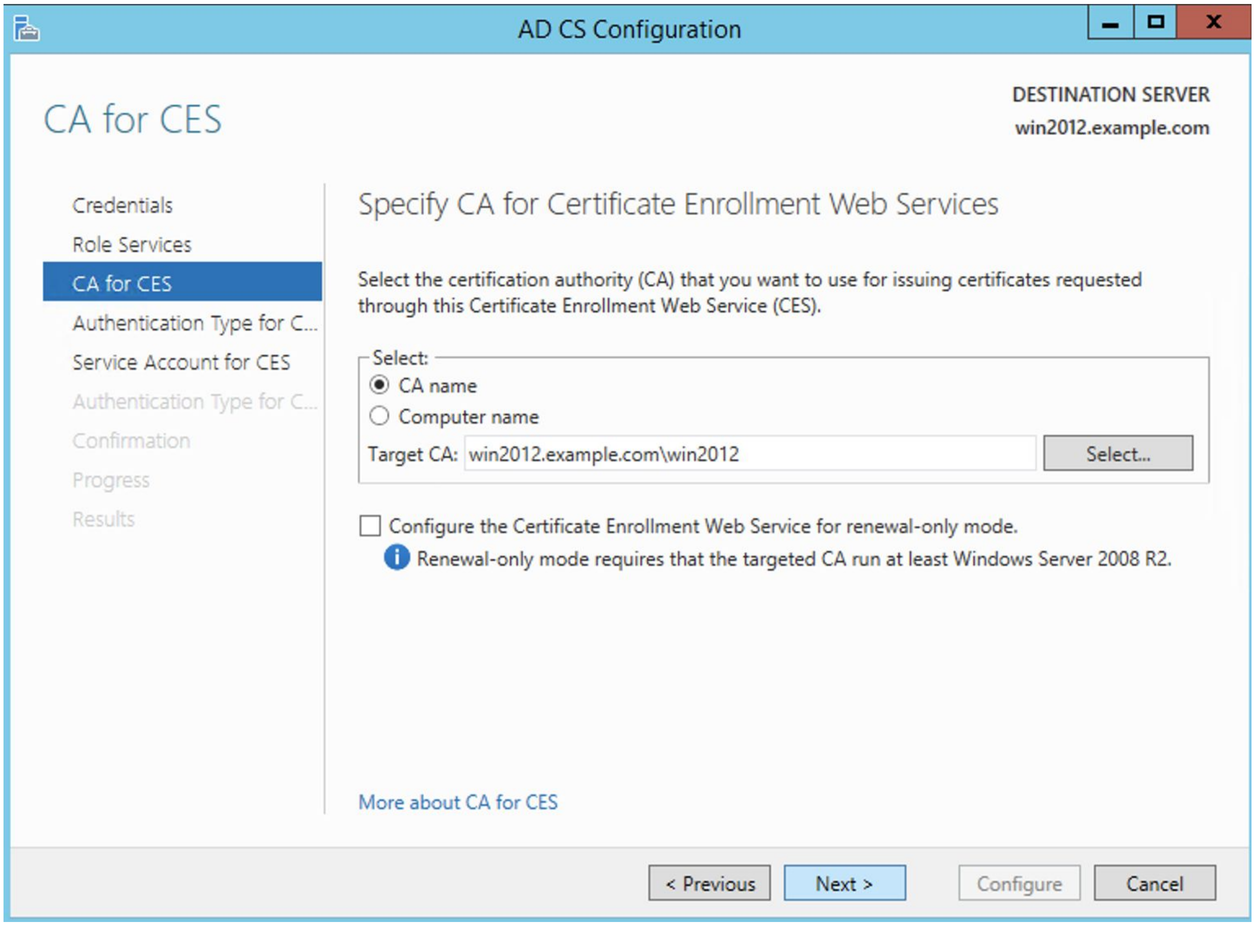
To install the following role services you must belong to the local Administrators group:

- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: EXAMPLE\administrator



Specify CA for Certificate Enrollment Web Services

Select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web Service (CES).

Select:

● CA name

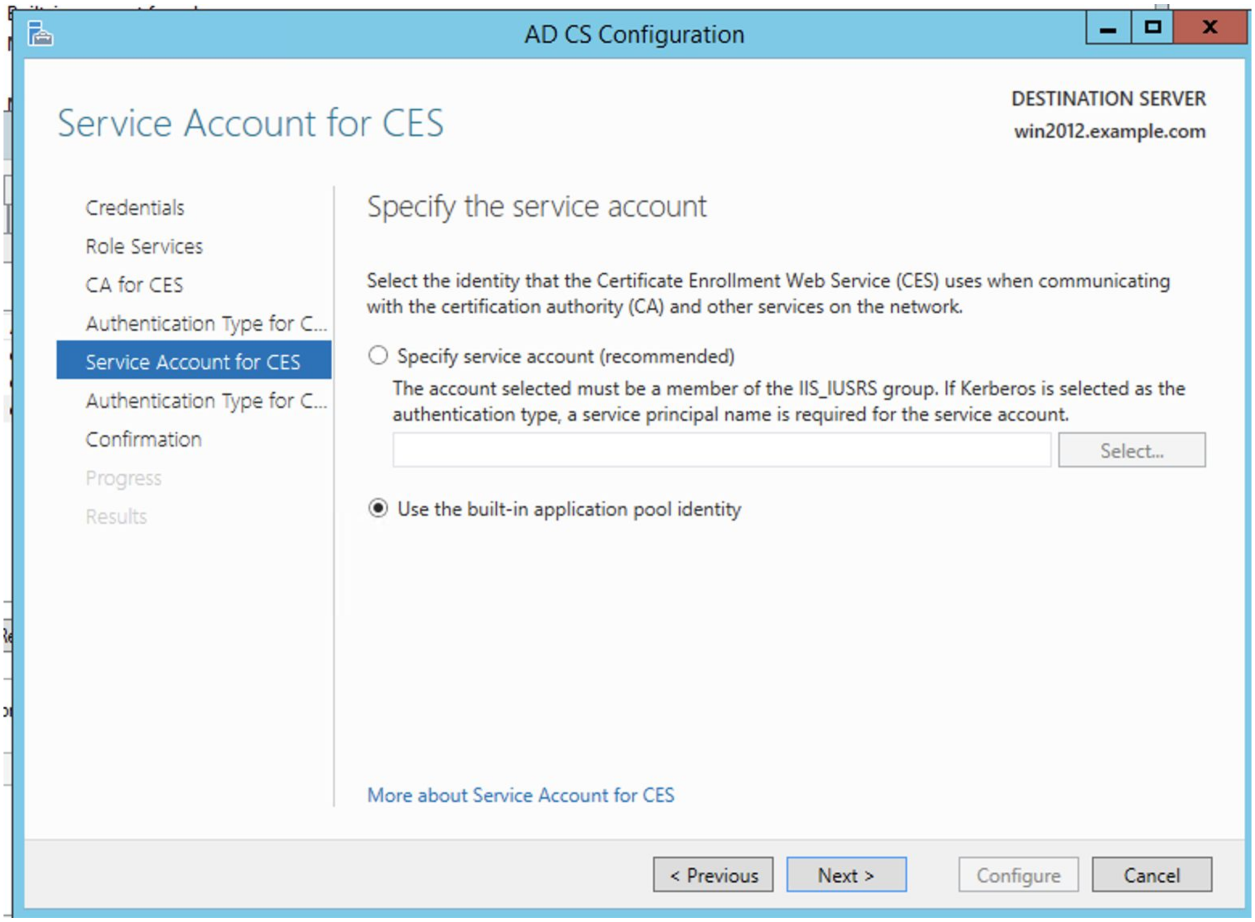
○ Computer name

Target CA: win2012.example.com\win2012

☐ Configure the Certificate Enrollment Web Service for renewal-only mode.

Renewal-only mode requires that the targeted CA run at least Windows Server 2008 R2.

I used the built in app pool instead of creating a service account



Service Account for CES

Specify the service account

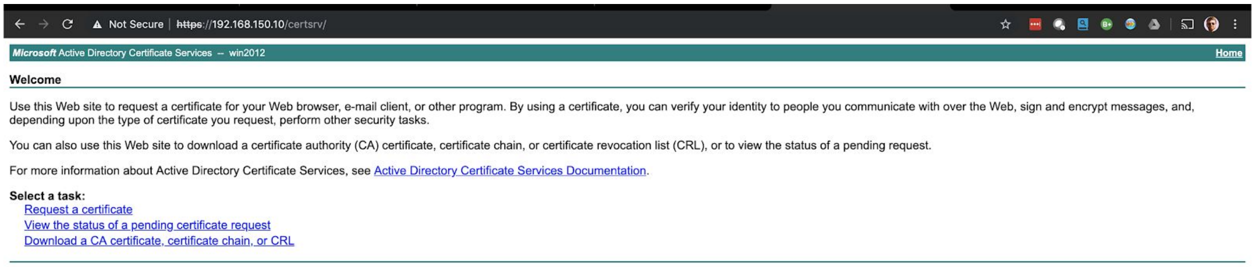
Select the identity that the Certificate Enrollment Web Service (CES) uses when communicating with the certification authority (CA) and other services on the network.

○ Specify service account (recommended)

The account selected must be a member of the IIS_IUSRS group. If Kerberos is selected as the authentication type, a service principal name is required for the service account.

● Use the built-in application pool identity

Lastly navigate to the URL (https://<name>/certsrv) and login (any user works but I used the Administrator account)


Not Secure
~~https~~://192.168.150.10/certsrv/
Microsoft Active Directory Certificate Services -- win2012
Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

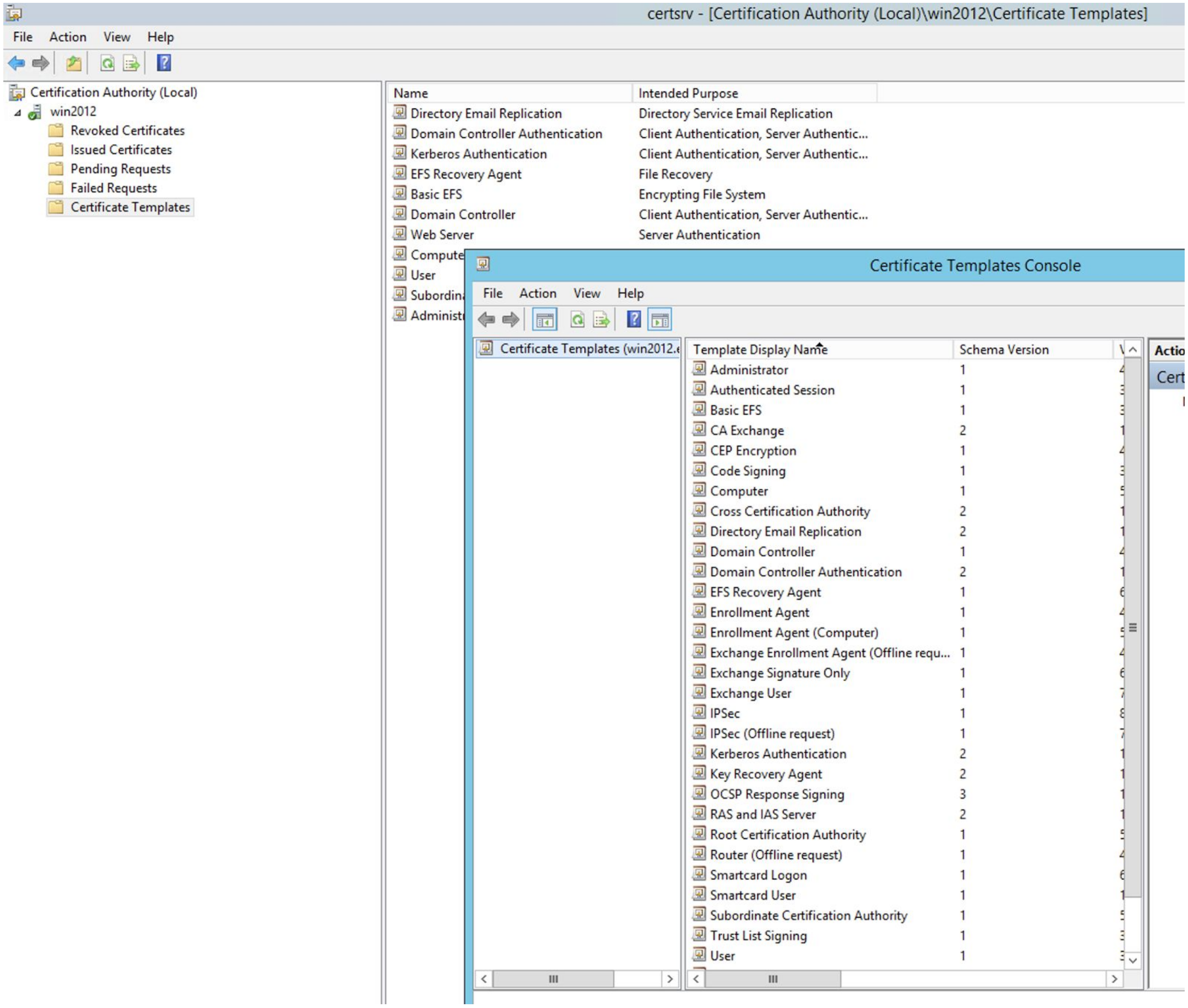
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:
- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL

CA Templates

The purpose of using CA Templates is to automatically provision each user and computer their own certificate when they log into the domain. The workstation (aka machine) certificate is automatically setup in AD but the user template needs to be built. As before, all relevant configurations are shown:

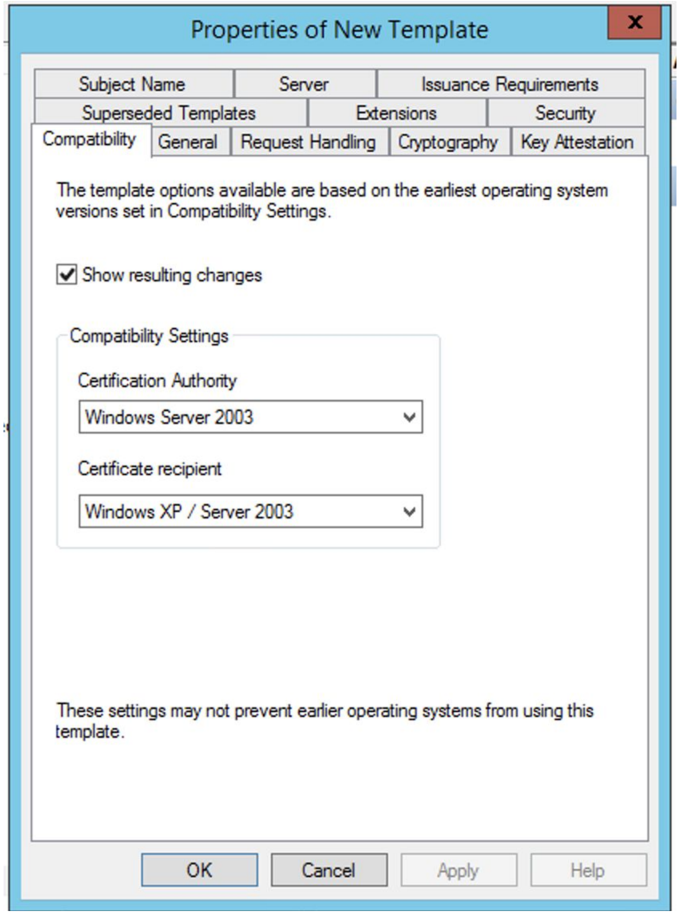
Right click on Certificate Templates and choose Manage. This should bring up the templates.


certsrv - [Certification Authority (Local)\win2012\Certificate Templates]
File
Action
View
Help
Certification Authority (Local)
win2012
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Certificate Templates Console
File
Action
View
Help
Certificate Templates (win2012.
Actio
Cert

Name	Intended Purpose
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
Web Server	Server Authentication
Compute	
User	
Subordin	
Administ	

Template Display Name	Schema Version
Administrator	1
Authenticated Session	1
Basic EFS	1
CA Exchange	2
CEP Encryption	1
Code Signing	1
Computer	1
Cross Certification Authority	2
Directory Email Replication	2
Domain Controller	1
Domain Controller Authentication	2
EFS Recovery Agent	1
Enrollment Agent	1
Enrollment Agent (Computer)	1
Exchange Enrollment Agent (Offline requ...	1
Exchange Signature Only	1
Exchange User	1
IPSec	1
IPSec (Offline request)	1
Kerberos Authentication	2
Key Recovery Agent	2
OCSP Response Signing	3
RAS and IAS Server	2
Root Certification Authority	1
Router (Offline request)	1
Smartcard Logon	1
Smartcard User	1
Subordinate Certification Authority	1
Trust List Signing	1
User	1

Right click on ‘User’ and choose ‘Duplicate’



The template options available are based on the earliest operating system versions set in Compatibility Settings.

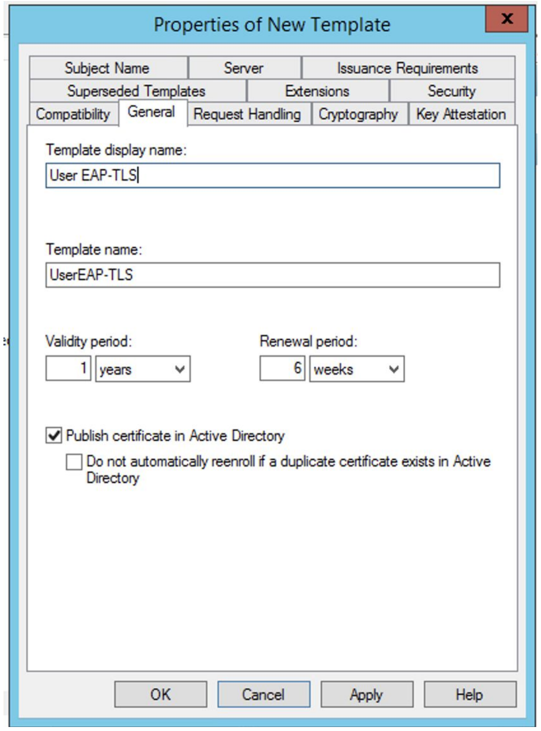
☑ Show resulting changes

Compatibility Settings

Certification Authority: Windows Server 2003

Certificate recipient: Windows XP / Server 2003

These settings may not prevent earlier operating systems from using this template.



Template display name: User EAP-TLS

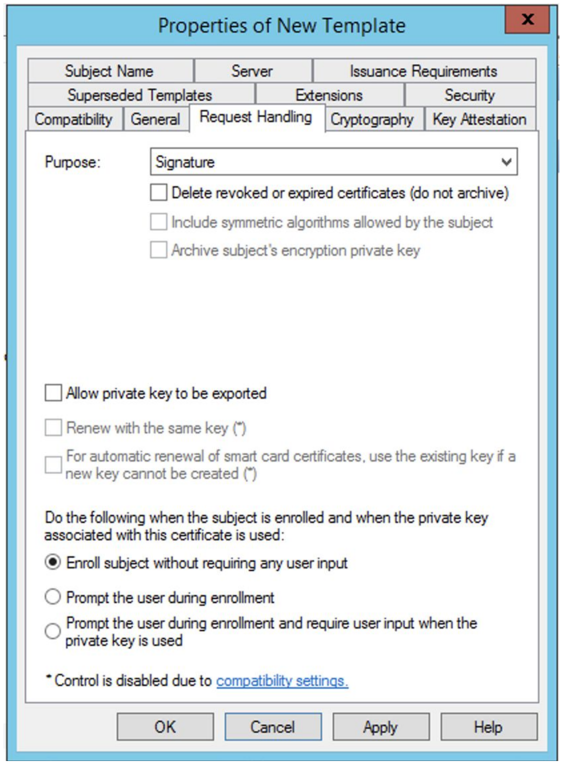
Template name: UserEAP-TLS

Validity period: 1 years

Renewal period: 6 weeks

☑ Publish certificate in Active Directory

☐ Do not automatically reenroll if a duplicate certificate exists in Active Directory



Purpose: Signature

☐ Delete revoked or expired certificates (do not archive)

☐ Include symmetric algorithms allowed by the subject

☐ Archive subject's encryption private key

☐ Allow private key to be exported

☐ Renew with the same key (*)

☐ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)

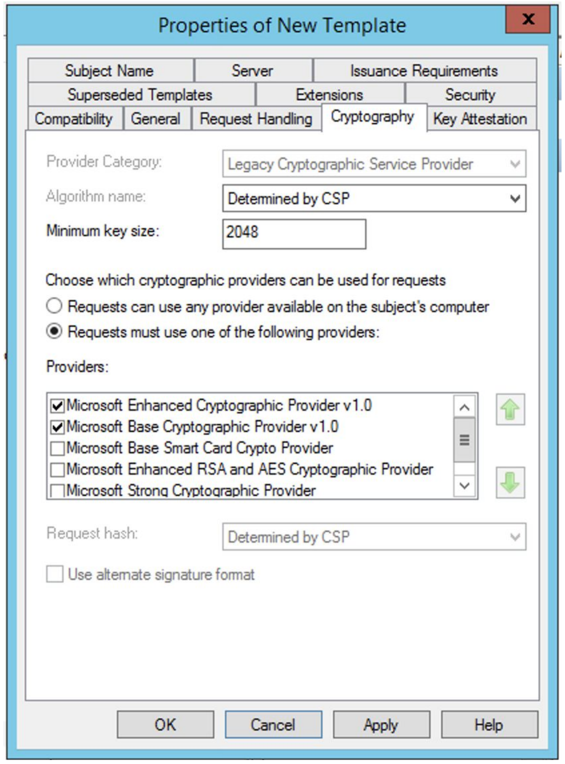
Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

* Control is disabled due to compatibility settings.



Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

○ Requests can use any provider available on the subject's computer

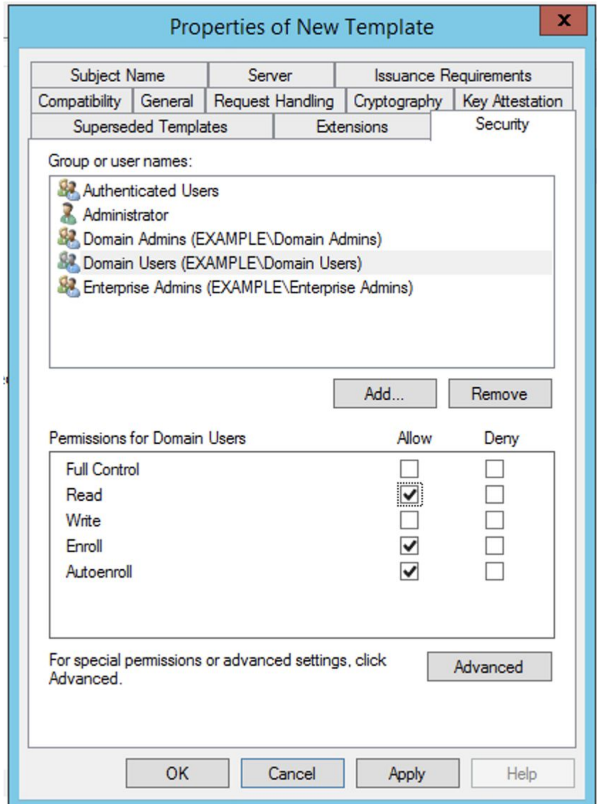
● Requests must use one of the following providers:

Providers:

☑ Microsoft Enhanced Cryptographic Provider v1.0
☑ Microsoft Base Cryptographic Provider v1.0
☐ Microsoft Base Smart Card Crypto Provider
☐ Microsoft Enhanced RSA and AES Cryptographic Provider
☐ Microsoft Strong Cryptographic Provider

Request hash: Determined by CSP

☐ Use alternate signature format

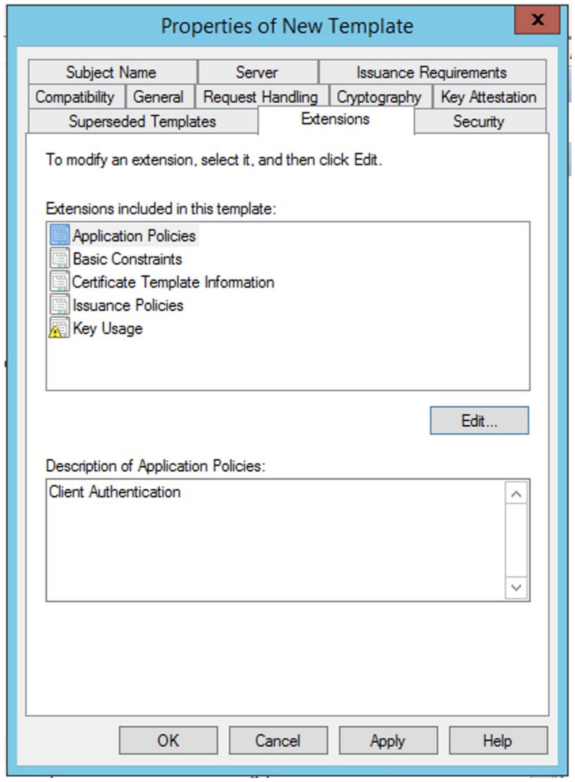


Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (EXAMPLE\Domain Admins)
- Domain Users (EXAMPLE\Domain Users)
- Enterprise Admins (EXAMPLE\Enterprise Admins)

Permissions for Domain Users	Allow	Deny
Full Control	☐	☐
Read	☑	☐
Write	☐	☐
Enroll	☑	☐
Autoenroll	☑	☐

For special permissions or advanced settings, click Advanced.



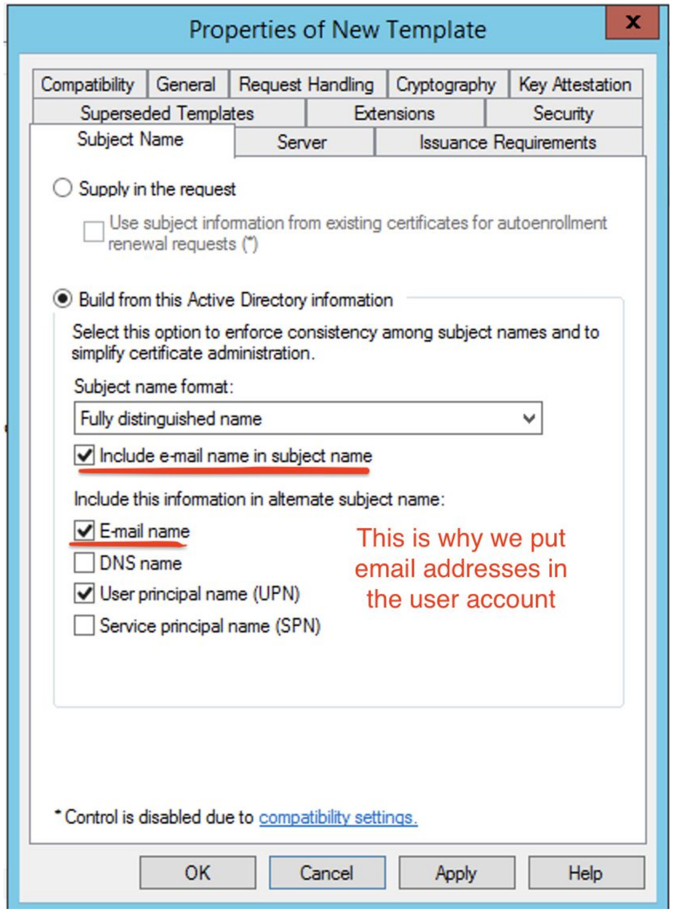
To modify an extension, select it, and then click Edit.

Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Client Authentication



○ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests (*)

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Fully distinguished name

☑ Include e-mail name in subject name

Include this information in alternate subject name:

☑ E-mail name

☐ DNS name

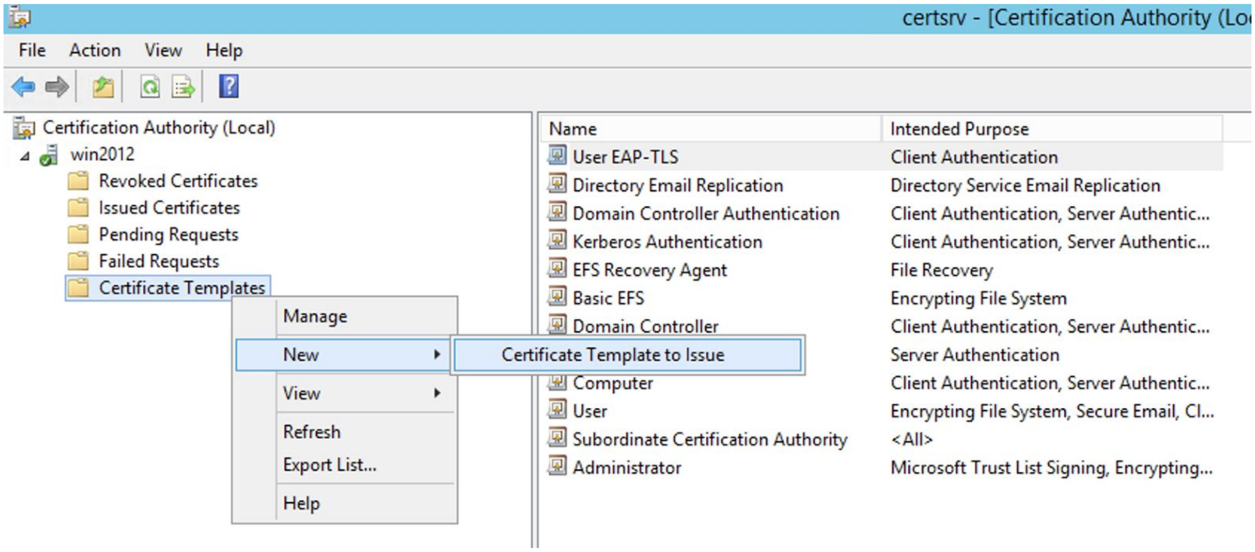
☑ User principal name (UPN)

☐ Service principal name (SPN)

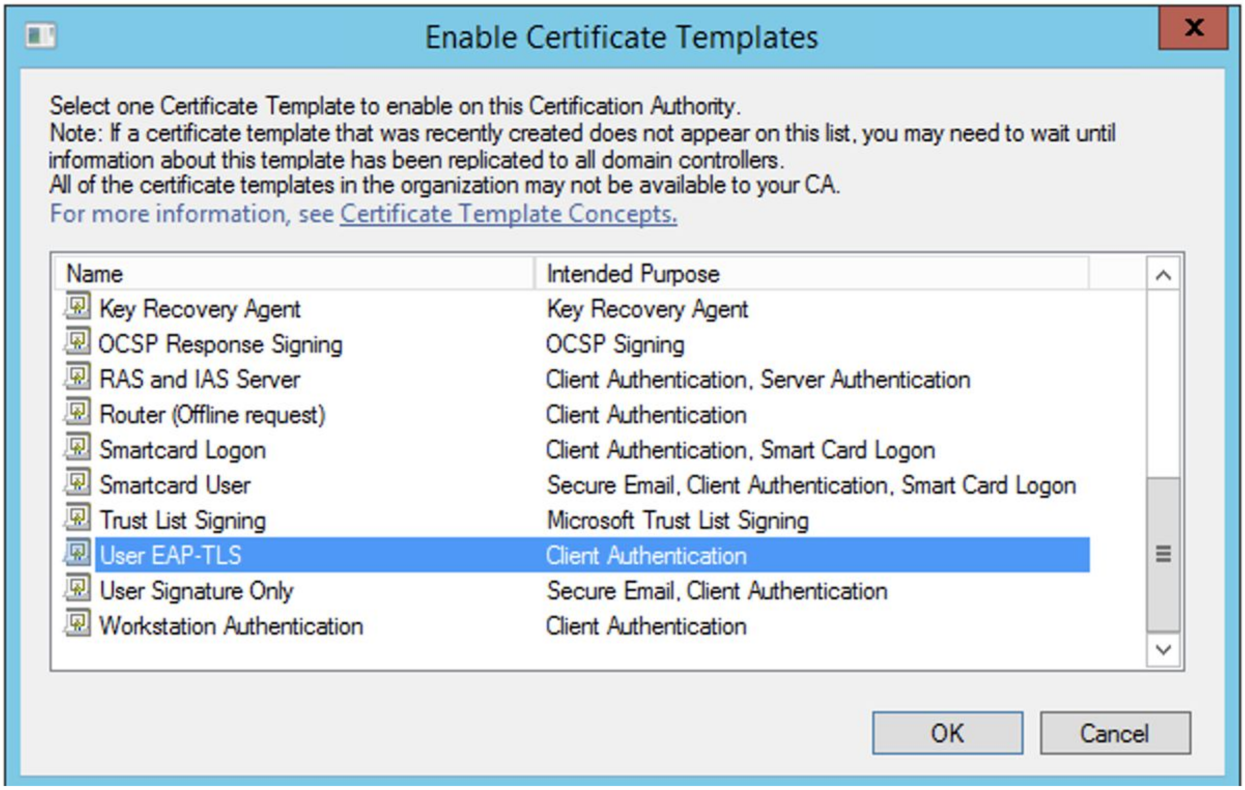
This is why we put email addresses in the user account

* Control is disabled due to compatibility settings.

Enable the new certificate template with the following:



Name	Intended Purpose
User EAP-TLS	Client Authentication
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authentic...
Kerberos Authentication	Client Authentication, Server Authentic...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentic...
	Server Authentication
Computer	Client Authentication, Server Authentic...
User	Encrypting File System, Secure Email, Cl...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting...



Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

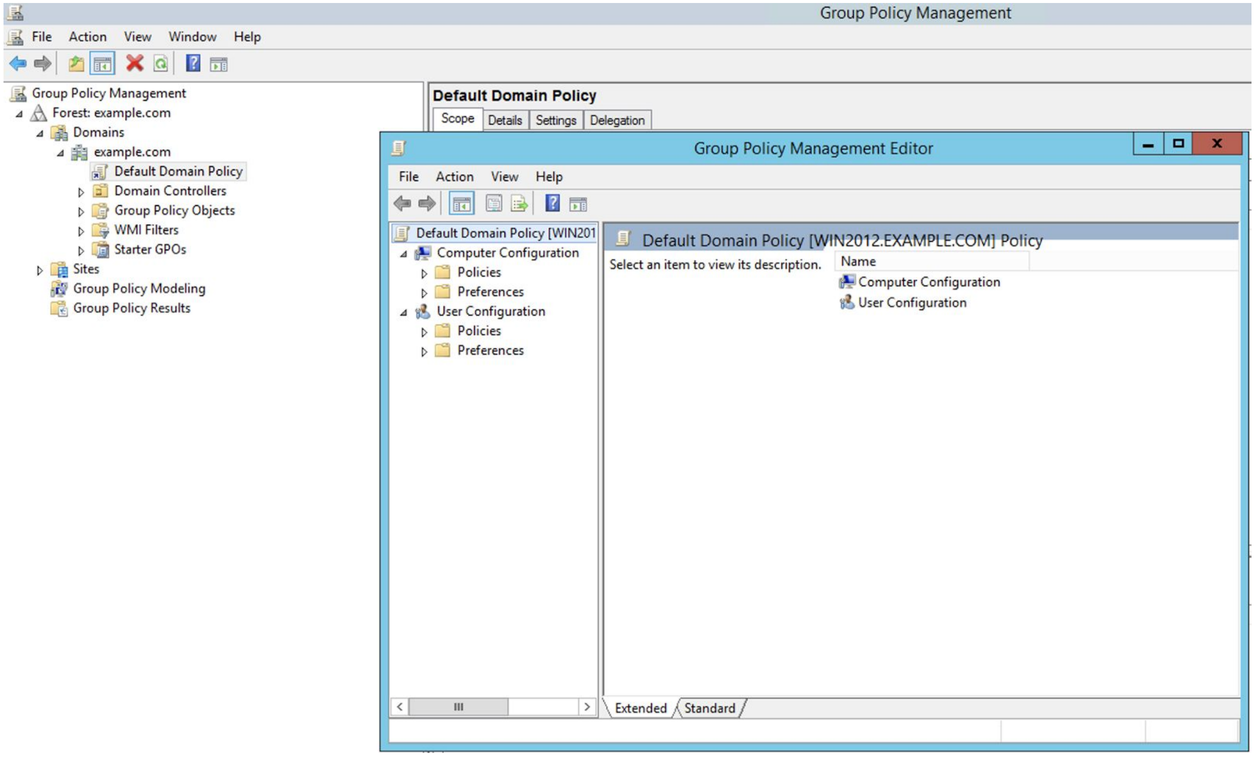
Name	Intended Purpose
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing
User EAP-TLS	Client Authentication
User Signature Only	Secure Email, Client Authentication
Workstation Authentication	Client Authentication

Repeat that for the Workstation Authentication template as well

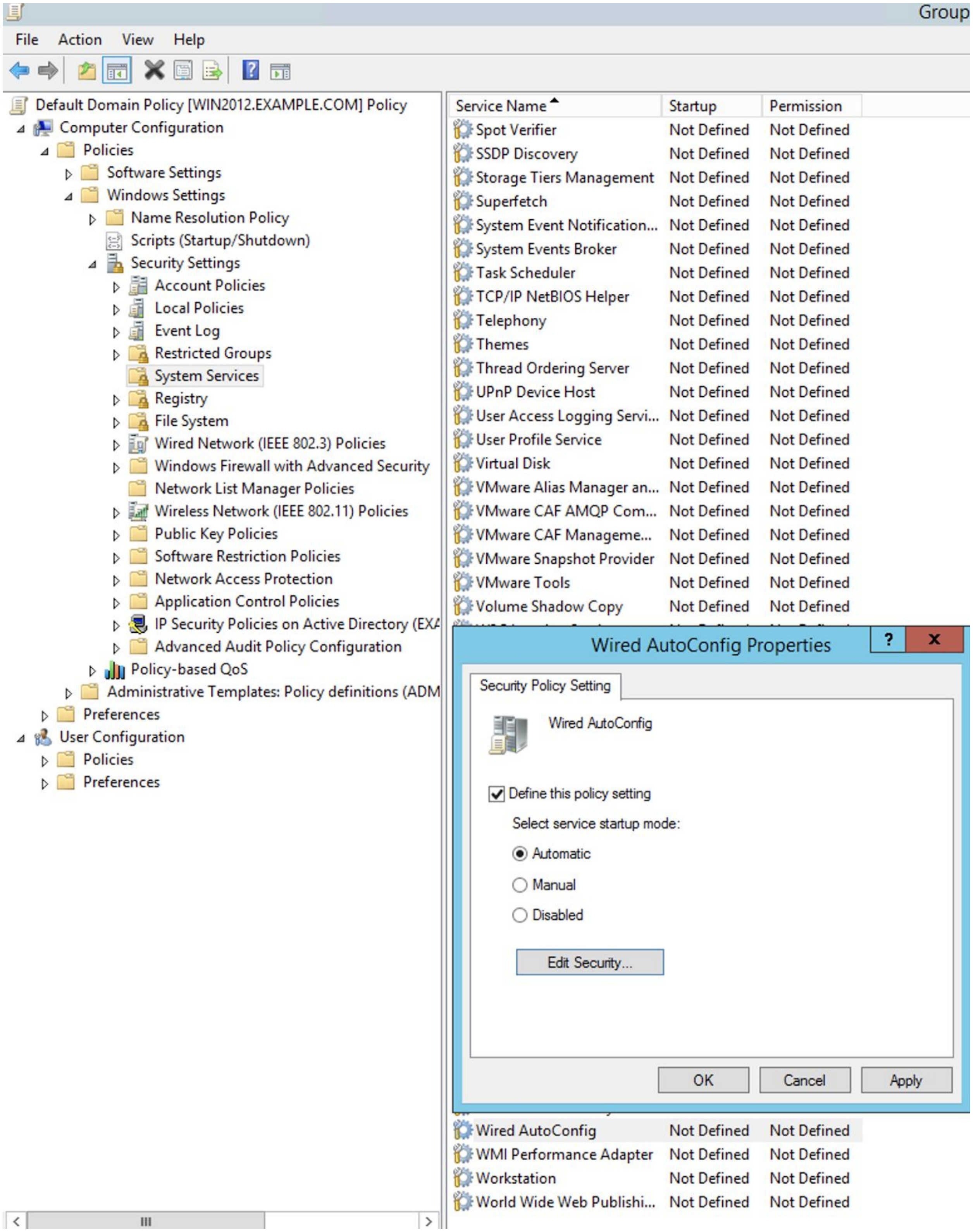
Group Policy Object

Now we can issue certificates automatically via GPO pushes. Let’s set that (we can control the method the clients connect by setting it on the Catalyst switchport).

Right Click on Default Domain Policy and choose “edit”



Turn up the Wired Autoconfig (aka 802.1X) service in the following navigation:



- Default Domain Policy [WIN2012.EXAMPLE.COM] Policy
  - Computer Configuration
    - Policies
      - Software Settings
      - Windows Settings
        - Name Resolution Policy
        - Scripts (Startup/Shutdown)
        - Security Settings
          - Account Policies
          - Local Policies
          - Event Log
          - Restricted Groups
          - System Services
          - Registry
          - File System
          - Wired Network (IEEE 802.3) Policies
          - Windows Firewall with Advanced Security
          - Network List Manager Policies
          - Wireless Network (IEEE 802.11) Policies
          - Public Key Policies
          - Software Restriction Policies
          - Network Access Protection
          - Application Control Policies
          - IP Security Policies on Active Directory (EXA
          - Advanced Audit Policy Configuration
        - Policy-based QoS
      - Administrative Templates: Policy definitions (ADM
    - Preferences
  - User Configuration
    - Policies
    - Preferences

Service Name	Startup	Permission
Spot Verifier	Not Defined	Not Defined
SSDP Discovery	Not Defined	Not Defined
Storage Tiers Management	Not Defined	Not Defined
Superfetch	Not Defined	Not Defined
System Event Notification...	Not Defined	Not Defined
System Events Broker	Not Defined	Not Defined
Task Scheduler	Not Defined	Not Defined
TCP/IP NetBIOS Helper	Not Defined	Not Defined
Telephony	Not Defined	Not Defined
Themes	Not Defined	Not Defined
Thread Ordering Server	Not Defined	Not Defined
UPnP Device Host	Not Defined	Not Defined
User Access Logging Servi...	Not Defined	Not Defined
User Profile Service	Not Defined	Not Defined
Virtual Disk	Not Defined	Not Defined
VMware Alias Manager an...	Not Defined	Not Defined
VMware CAF AMQP Com...	Not Defined	Not Defined
VMware CAF Manageme...	Not Defined	Not Defined
VMware Snapshot Provider	Not Defined	Not Defined
VMware Tools	Not Defined	Not Defined
Volume Shadow Copy	Not Defined	Not Defined
Wired AutoConfig	Not Defined	Not Defined
WMI Performance Adapter	Not Defined	Not Defined
Workstation	Not Defined	Not Defined
World Wide Web Publishi...	Not Defined	Not Defined

Wired AutoConfig Properties

Security Policy Setting

Wired AutoConfig

☑ Define this policy setting

Select service startup mode:

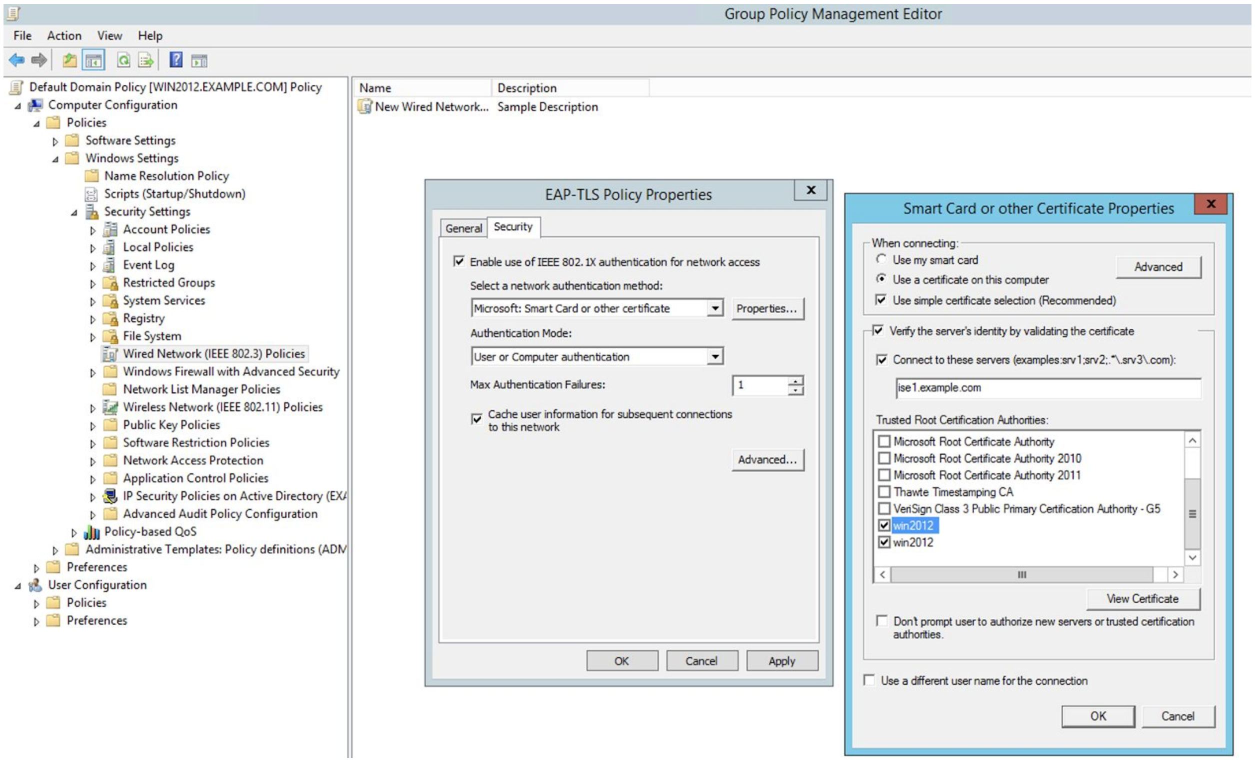
● Automatic

○ Manual

○ Disabled

Edit Security...

Enable the 802.1X configuration for the clients


Group Policy Management Editor
File
Action
View
Help
Default Domain Policy [WIN2012.EXAMPLE.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (EXA
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADM
Preferences
User Configuration
Policies
Preferences
Name
Description
EAP-TLS Policy Properties
General
Security
Properties...
Advanced...
OK
Cancel
Apply
Smart Card or other Certificate Properties
Advanced
View Certificate
OK
Cancel

New Wired Network... Sample Description

EAP-TLS Policy Properties – Security

☑ Enable use of IEEE 802.1X authentication for network access

Select a network authentication method: Microsoft: Smart Card or other certificate

Authentication Mode: User or Computer authentication

Max Authentication Failures: 1

☑ Cache user information for subsequent connections to this network

Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Verify the server's identity by validating the certificate

☑ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

ise1.example.com

Trusted Root Certification Authorities:

☐ Microsoft Root Certificate Authority

☐ Microsoft Root Certificate Authority 2010

☐ Microsoft Root Certificate Authority 2011

☐ Thawte Timestamping CA

☐ VeriSign Class 3 Public Primary Certification Authority - G5

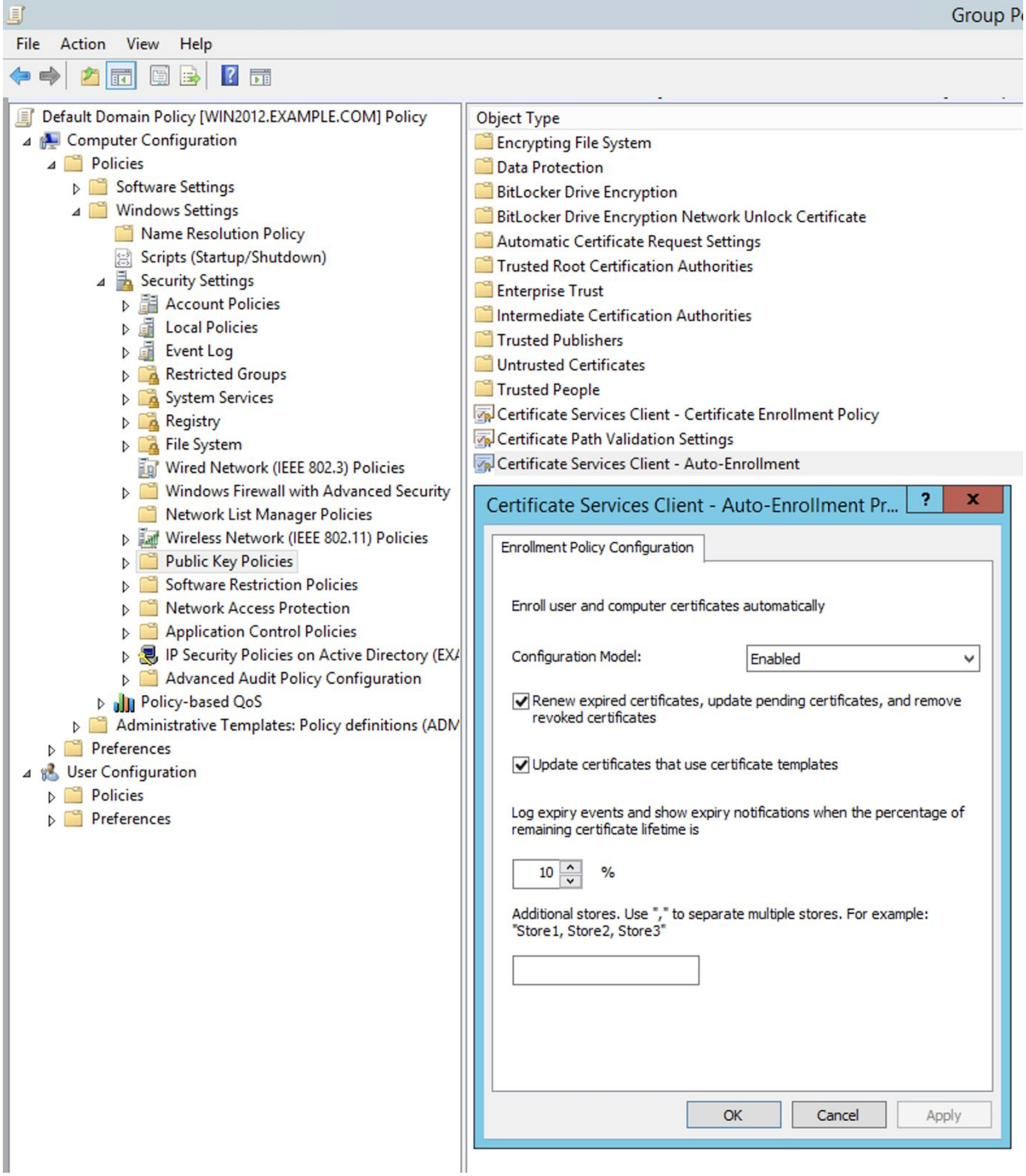
☑ win2012

☑ win2012

☐ Don't prompt user to authorize new servers or trusted certification authorities.

☐ Use a different user name for the connection

Enable the Computer Certificate Enrollment


Group P
File
Action
View
Help
Default Domain Policy [WIN2012.EXAMPLE.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (EXA
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADM
Preferences
User Configuration
Policies
Preferences
Object Type
Encrypting File System
Data Protection
BitLocker Drive Encryption
BitLocker Drive Encryption Network Unlock Certificate
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment
Certificate Services Client - Auto-Enrollment Pr...
?
X
Enrollment Policy Configuration
OK
Cancel
Apply

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

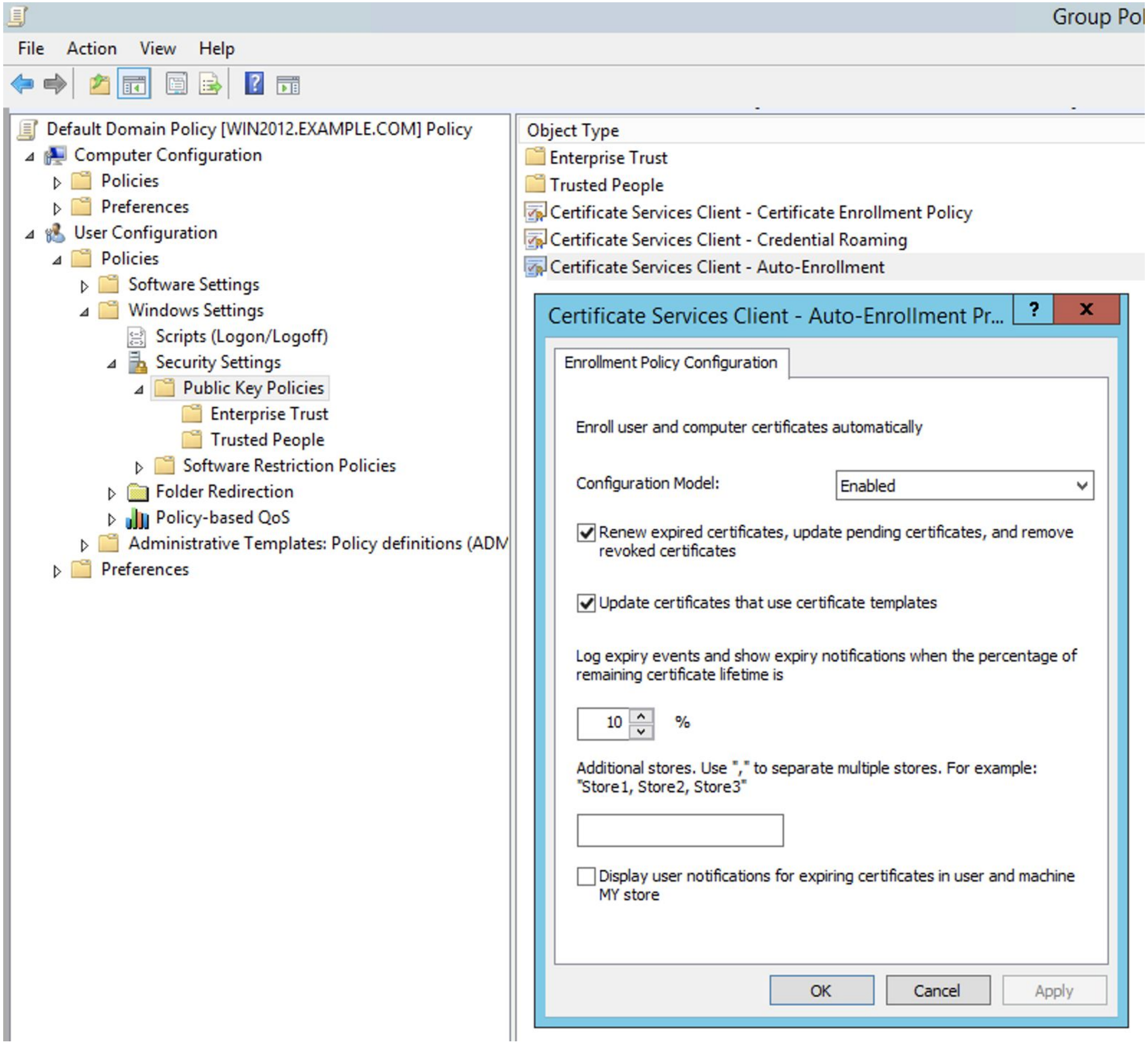
☑ Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

10 %

Additional stores. Use "," to separate multiple stores. For example: "Store1, Store2, Store3"

Enable it for the user:


Group Pol
File
Action
View
Help
Default Domain Policy [WIN2012.EXAMPLE.COM] Policy
Computer Configuration
Policies
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Scripts (Logon/Logoff)
Security Settings
Public Key Policies
Enterprise Trust
Trusted People
Software Restriction Policies
Folder Redirection
Policy-based QoS
Administrative Templates: Policy definitions (ADM
Preferences
Object Type
Enterprise Trust
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Services Client - Credential Roaming
Certificate Services Client - Auto-Enrollment
Certificate Services Client - Auto-Enrollment Pr...
?
X
Enrollment Policy Configuration
OK
Cancel
Apply

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

Log expiry events and show expiry notifications when the percentage of remaining certificate lifetime is

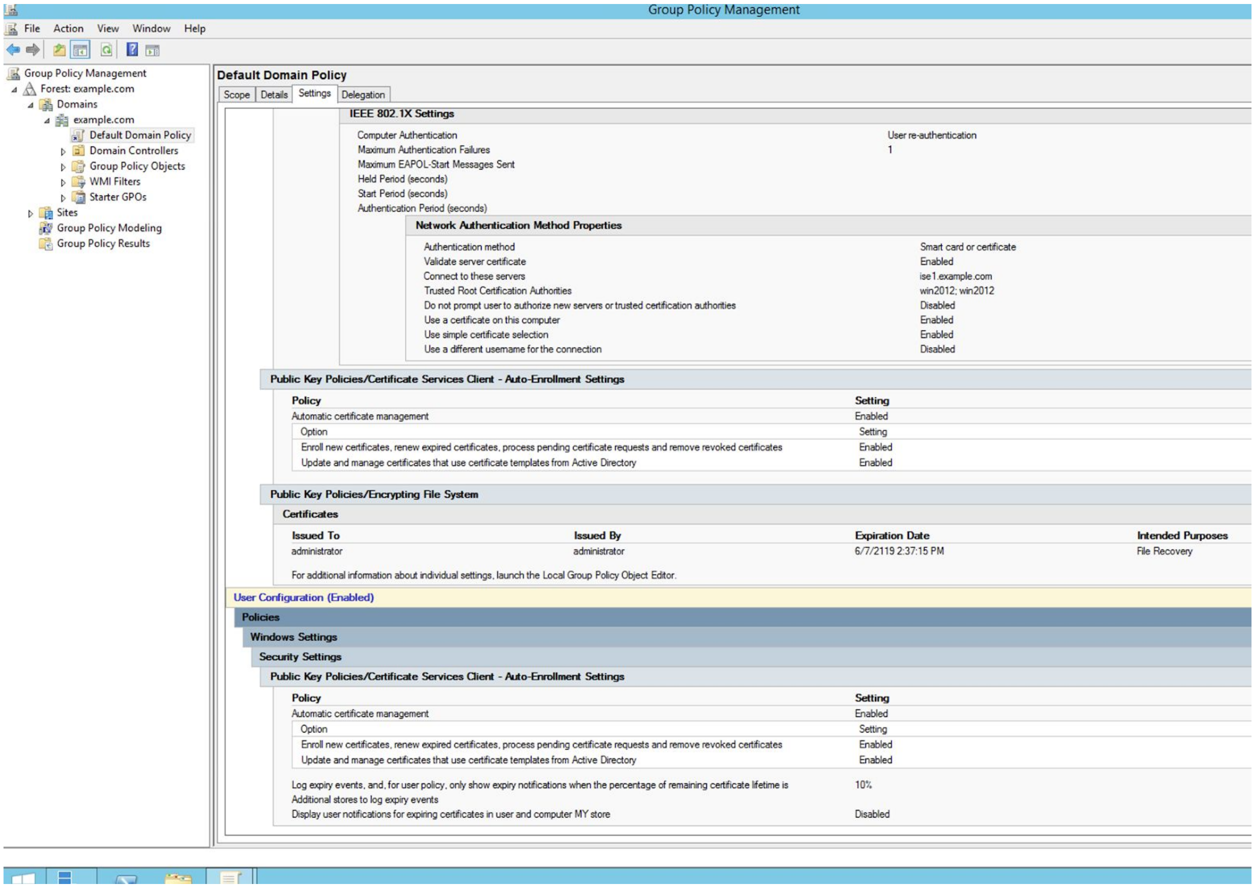
10 %

Additional stores. Use "," to separate multiple stores. For example: "Store1, Store2, Store3"

☐ Display user notifications for expiring certificates in user and machine MY store

Protip, if you find certificates are not being issued to your domain-joined Windows workstations, check the Event Viewer on the Server VM. The reasons will be logged there.

The Final GPO Policy should look something like this



Default Domain Policy

IEEE 802.1X Settings

Computer Authentication	User re-authentication
Maximum Authentication Failures	1
Maximum EAPOL-Start Messages Sent	
Held Period (seconds)	
Start Period (seconds)	
Authentication Period (seconds)	

Network Authentication Method Properties

Authentication method	Smart card or certificate
Validate server certificate	Enabled
Connect to these servers	ise1.example.com
Trusted Root Certification Authorities	win2012; win2012
Do not prompt user to authorize new servers or trusted certification authorities	Disabled
Use a certificate on this computer	Enabled
Use simple certificate selection	Enabled
Use a different username for the connection	Disabled

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings

Policy	Setting
Automatic certificate management	Enabled
Option	Setting
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates	Enabled
Update and manage certificates that use certificate templates from Active Directory	Enabled

Public Key Policies/Encrypting File System

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes
administrator	administrator	6/7/2119 2:37:15 PM	File Recovery

For additional information about individual settings, launch the Local Group Policy Object Editor.

User Configuration (Enabled)

Policies

Windows Settings

Security Settings

Public Key Policies/Certificate Services Client - Auto-Enrollment Settings

Policy	Setting
Automatic certificate management	Enabled
Option	Setting
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates	Enabled
Update and manage certificates that use certificate templates from Active Directory	Enabled

Log expiry events, and, for user policy, only show expiry notifications when the percentage of remaining certificate lifetime is	10%
Additional stores to log expiry events	
Display user notifications for expiring certificates in user and computer MY store	Disabled

ISE Configuration

Now we're getting to some ISE Configuration. We'll build using blocks and then pull it all together into a functioning, useful architecture.

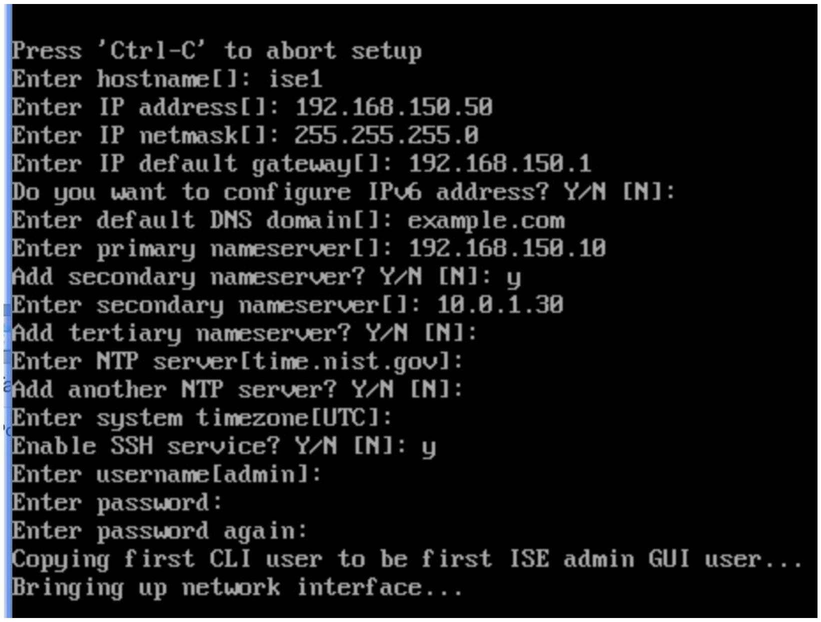
Bootstrapping

General

Just to level-set, this was my VM setup parameters for this lab. Two things of note here: the use of UTC versus local timezones. Just go with whatever your organization's standards are (most multi-timezone orgs will default to one timezone or possibly use UTC). Just note that ISE cannot easily (or even possibly) be changed from the timezone you pick here, so choose wisely.

Common Time Zones syntax are here for reference

Second point, I enabled SSH to the node. Most likely you wouldn't leave this available in a production environment and it can easily be turned off after install.



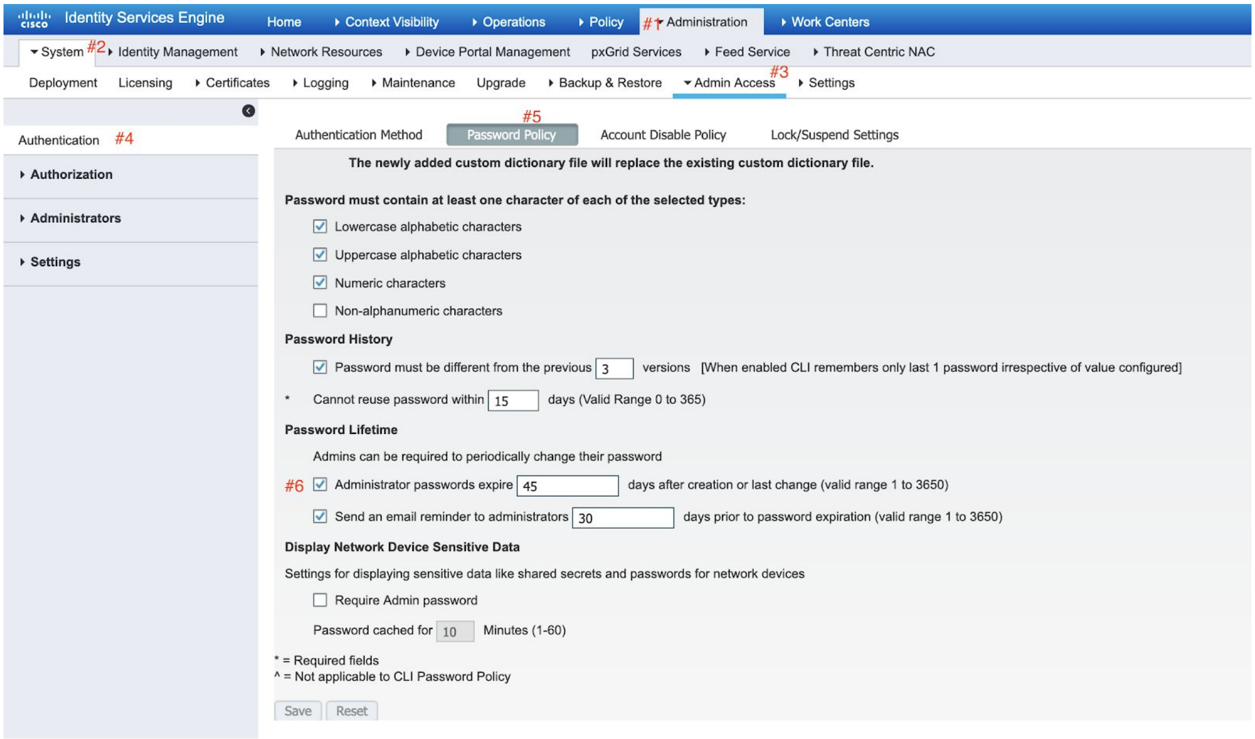
```
Press 'Ctrl-C' to abort setup
Enter hostname[]: ise1
Enter IP address[]: 192.168.150.50
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 192.168.150.1
Do you want to configure IPv6 address? Y/N [N]:
Enter default DNS domain[]: example.com
Enter primary nameserver[]: 192.168.150.10
Add secondary nameserver? Y/N [N]: y
Enter secondary nameserver[]: 10.0.1.30
Add tertiary nameserver? Y/N [N]:
Enter NTP server[time.nist.gov]:
Add another NTP server? Y/N [N]:
Enter system timezone[UTC]:
Enable SSH service? Y/N [N]: y
Enter username[admin]:
Enter password:
Enter password again:
Copying first CLI user to be first ISE admin GUI user...
Bringing up network interface...
```

ISE installs with a 90 day eval (all features enabled licensed). You can safely ignore any license warnings after you log into the GUI

Navigation Howto

I will reference GUI position by hierarchy. Basically ISE is configured top down by tabs and then left to right from the column slider and into the main page. Here's an example, I'd recommend you disable password expiration for the admin account by going to Administration--System--Admin Access--Authentication--Password Policy--Password Lifetime

Here's an example



The newly added custom dictionary file will replace the existing custom dictionary file.

Password must contain at least one character of each of the selected types:

☑ Lowercase alphabetic characters

☑ Uppercase alphabetic characters

☑ Numeric characters

☐ Non-alphanumeric characters

Password History

☑ Password must be different from the previous 3 versions [When enabled CLI remembers only last 1 password irrespective of value configured]

* Cannot reuse password within 15 days (Valid Range 0 to 365)

Password Lifetime

Admins can be required to periodically change their password

#6 ☑ Administrator passwords expire 45 days after creation or last change (valid range 1 to 3650)

☑ Send an email reminder to administrators 30 days prior to password expiration (valid range 1 to 3650)

Display Network Device Sensitive Data

Settings for displaying sensitive data like shared secrets and passwords for network devices

☐ Require Admin password

Password cached for 10 Minutes (1-60)

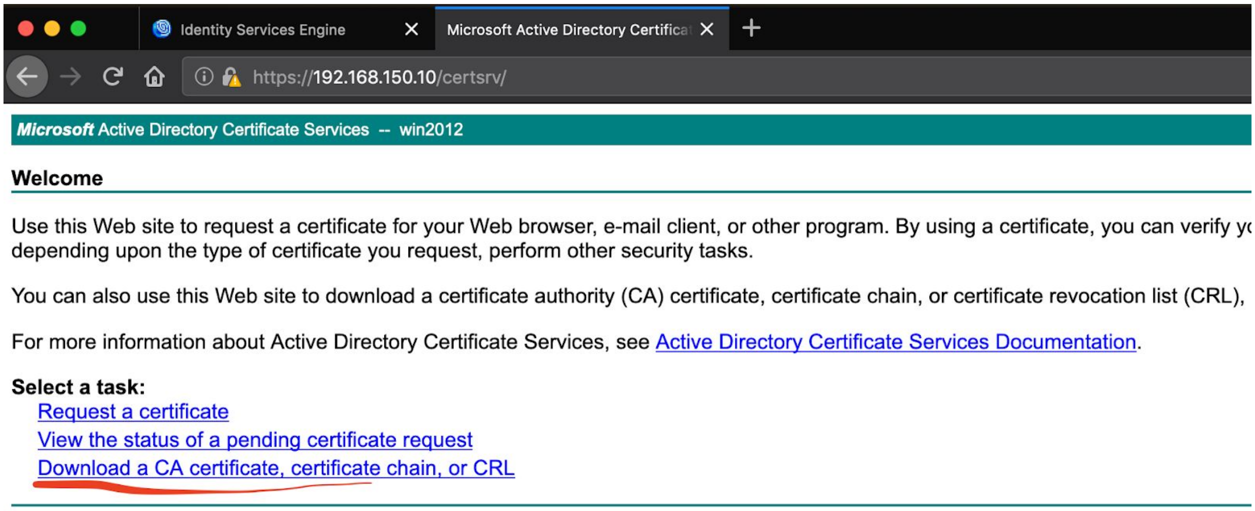
* = Required fields

^ = Not applicable to CLI Password Policy

Certificates

Certificates are used predominantly in ISE, to form EAP tunnels and serve web portals. For the use cases here we will only install 2 certs in ISE. One will be the internal CA root certificate and the second will be a wildcard certificate for ISE signed by the internal CA. Typically you will purchase a 3rd party certificate for ISE when used for Guest portals (which isn't a use case outlined here). Aaron Woland's cert tutorial is still excellent and available here.

First step is to grab the root CA by navigating to the CA URL @ http://<IP Address>/CertSrv (in my example I'm using https://192.168.150.10/CertSrv). Log in as the administrator user


Identity Services Engine
Microsoft Active Directory Certificat
https://192.168.150.10/certsrv/

Microsoft Active Directory Certificate Services -- win2012

Welcome

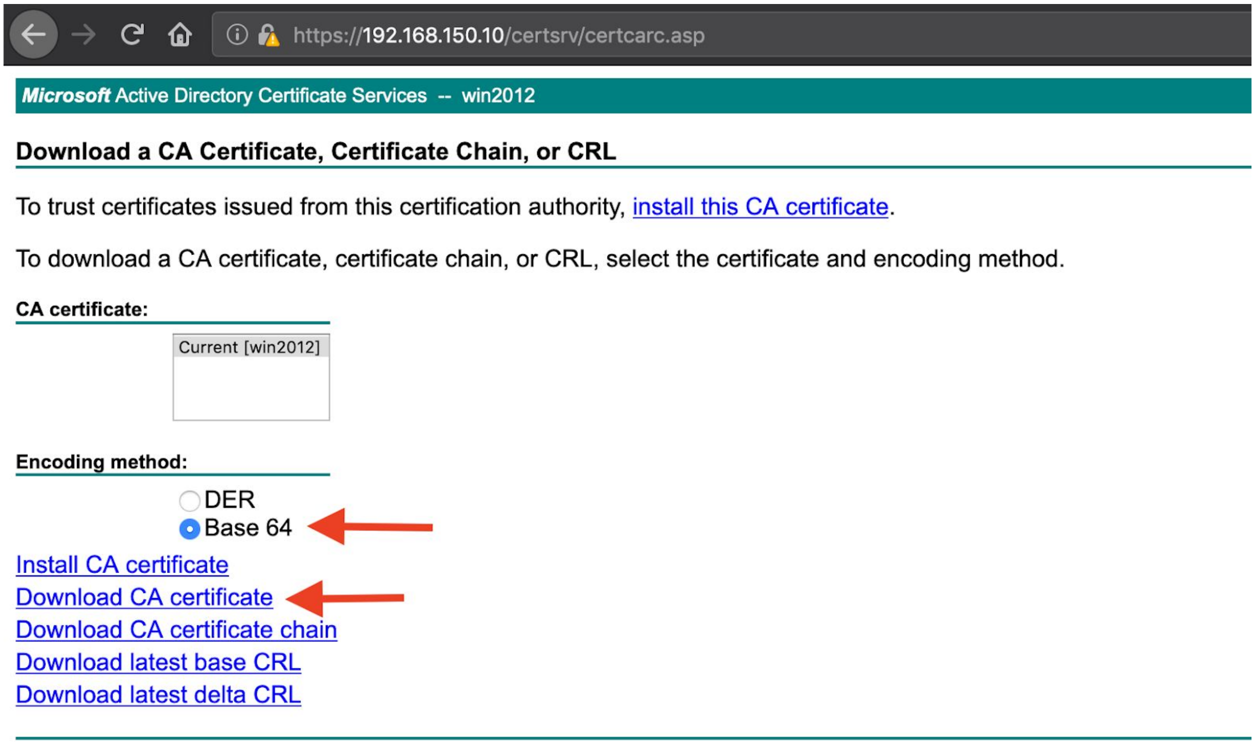
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify y
depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL),

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL



Microsoft Active Directory Certificate Services -- win2012

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [win2012]

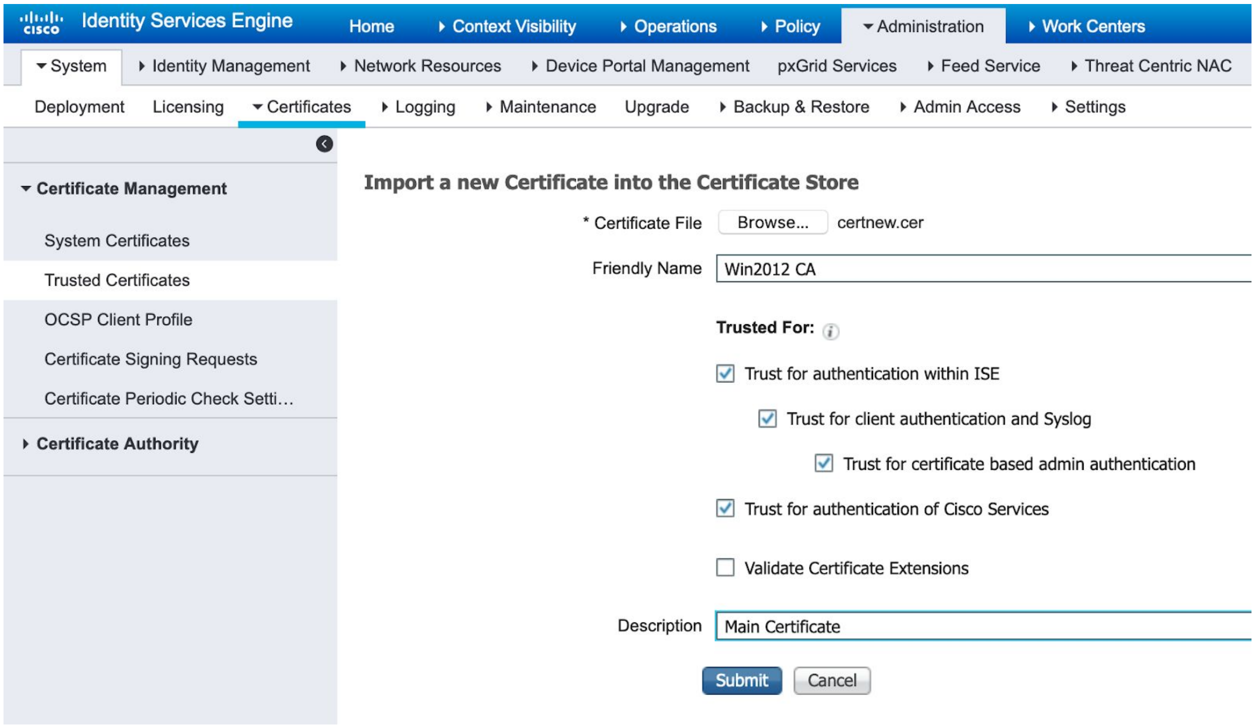
Encoding method:

○ DER
● Base 64

- Install CA certificate
- Download CA certificate
- Download CA certificate chain
- Download latest base CRL
- Download latest delta CRL

This downloads a file named certnew.cer. In the ISE GUI navigate to Administration--System--Certificates--Certificate Management--Trusted Certificates. Click Import

This is what mine looks like



Import a new Certificate into the Certificate Store

* Certificate File: certnew.cer

Friendly Name: Win2012 CA

Trusted For:

☑ Trust for authentication within ISE

☑ Trust for client authentication and Syslog

☑ Trust for certificate based admin authentication

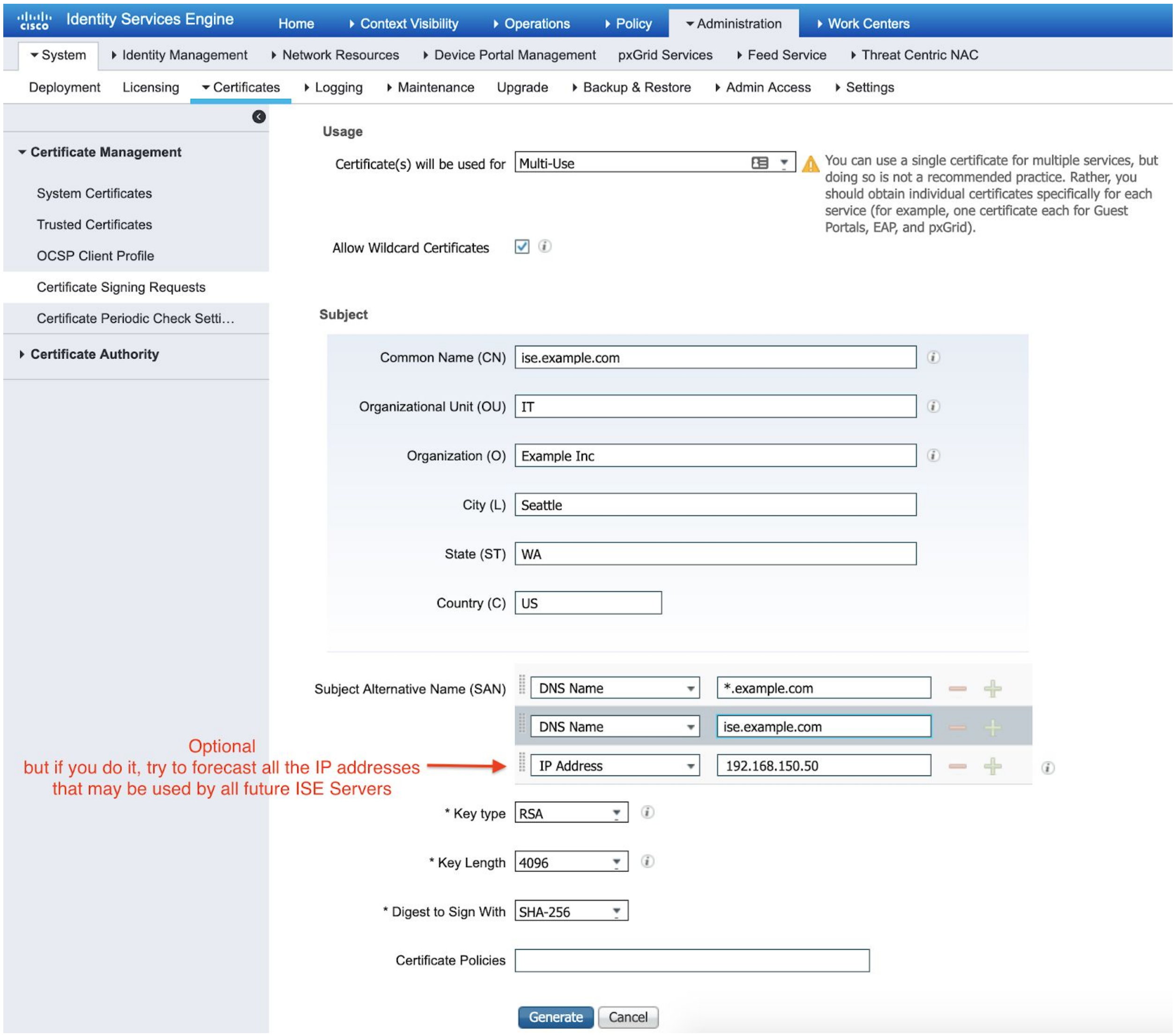
☑ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description: Main Certificate

Now it’s time to generate a CSR and have it signed by the WinCA. Navigate to Administration--System--Certificates--Certificate Management--Certificate Signing Requests and Click Generate CSR

My parameters look like this



Usage

Certificate(s) will be used for: Multi-Use

You can use a single certificate for multiple services, but doing so is not a recommended practice. Rather, you should obtain individual certificates specifically for each service (for example, one certificate each for Guest Portals, EAP, and pxGrid).

Allow Wildcard Certificates: ☑

Subject

Common Name (CN): ise.example.com

Organizational Unit (OU): IT

Organization (O): Example Inc

City (L): Seattle

State (ST): WA

Country (C): US

Subject Alternative Name (SAN):

DNS Name: *.example.com

DNS Name: ise.example.com

IP Address: 192.168.150.50

Optional
but if you do it, try to forecast all the IP addresses
that may be used by all future ISE Servers

* Key type: RSA

* Key Length: 4096

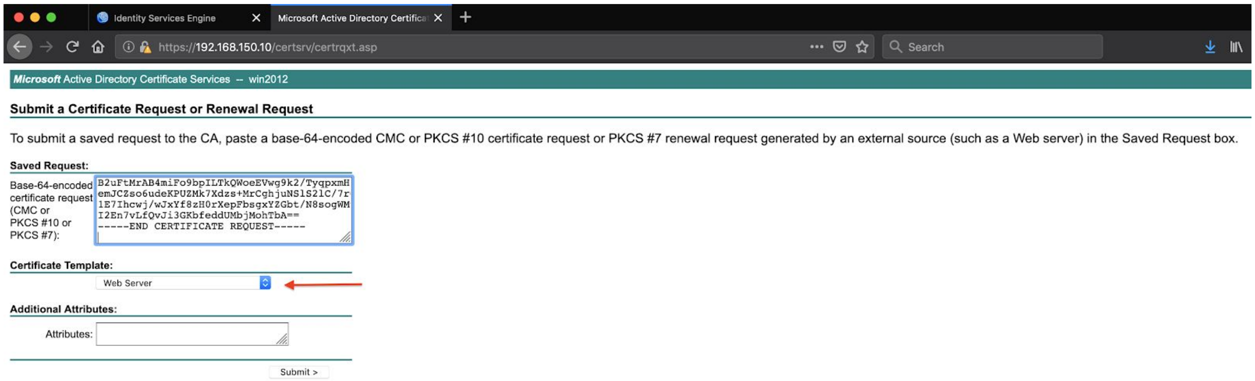
* Digest to Sign With: SHA-256

Certificate Policies:

The result is an option to export the CSR, so grab that file.

Navigate back to https://<ip address>/CertSrv and choose ‘Request a certificate’ and then ‘advanced certificate request’ (if you’re not logged in with an administrative account you may not have access to this option or the Web Server template we need.

Paste in the CSR text data and choose the web server template


Identity Services Engine
Microsoft Active Directory Certifica
https://192.168.150.10/certsrv/certrqxt.asp
Search

Microsoft Active Directory Certificate Services -- win2012

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
B2uFtMrAB4miFo9bpILTkQWoeEVwg9k2/TyqpxmH
emJCZso6udeKPUZMk7Xdzs+MrCghjuNS1S21C/7r
1E7Ihcwj/wJxYf8zH0rXepFbsgxYZGbt/N8sogWM
I2En7vLfQvJi3GKbfeddUMbjMohTbA==
-----END CERTIFICATE REQUEST-----
```

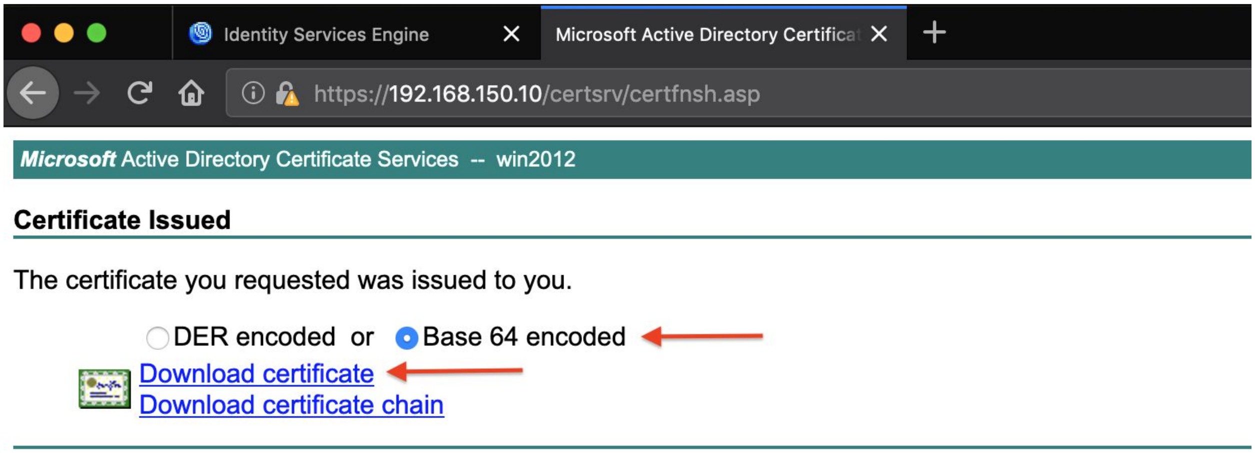
Certificate Template:

Web Server

Additional Attributes:

Attributes:

Click Submit and download the cert in Base64 format (should come down as ‘certnew.cer’ or possibly ‘certnew(1).cer’ if the Win CA cert is also in the directory.


Identity Services Engine
Microsoft Active Directory Certificat
https://192.168.150.10/certsrv/certfnsh.asp

Microsoft Active Directory Certificate Services -- win2012

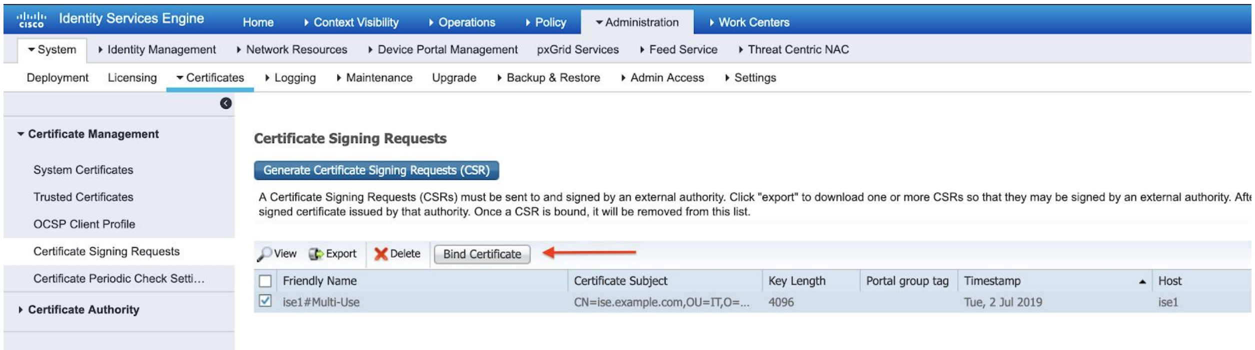
Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

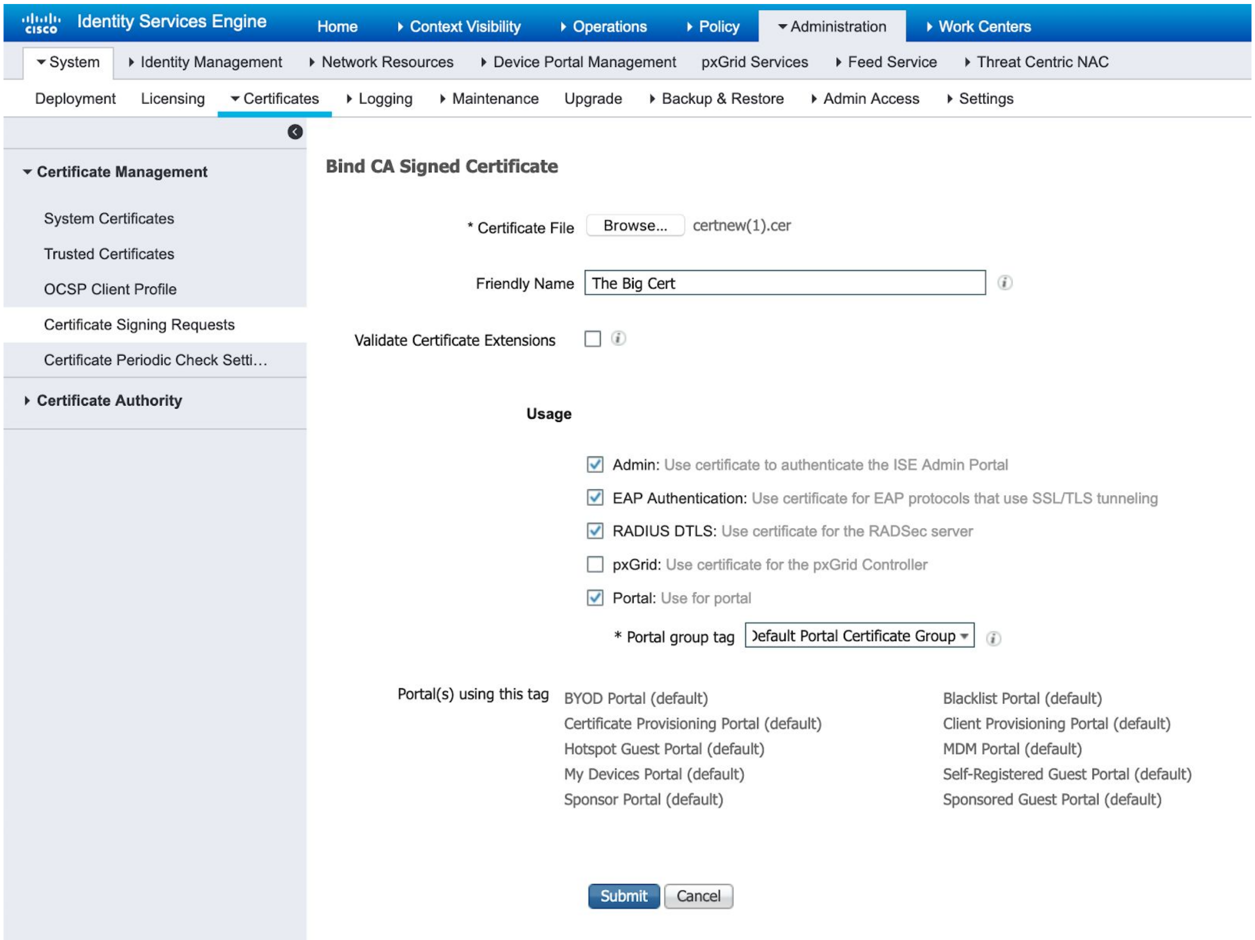
Back on ISE Administration--System--Certificates--Certificate Management--Certificate Signing Requests. You should see the CSR with an option to ‘bind’ the certificate to the CSR. Mine looks like this:



Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. Afte
signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

☐	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
☑	ise1#Multi-Use	CN=ise.example.com,OU=IT,O=...	4096		Tue, 2 Jul 2019	ise1



Bind CA Signed Certificate

* Certificate File: certnew(1).cer

Friendly Name: The Big Cert

Validate Certificate Extensions ☐

Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal
☑ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
☑ RADIUS DTLS: Use certificate for the RADSec server
☐ pxGrid: Use certificate for the pxGrid Controller
☑ Portal: Use for portal

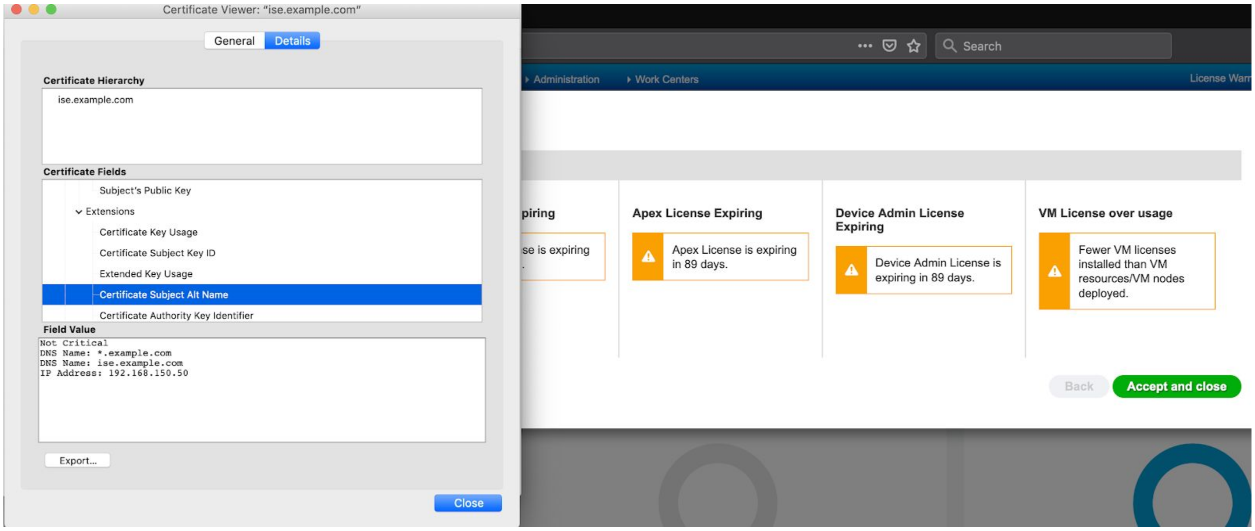
* Portal group tag: Default Portal Certificate Group

Portal(s) using this tag:

BYOD Portal (default)	Blacklist Portal (default)
Certificate Provisioning Portal (default)	Client Provisioning Portal (default)
Hotspot Guest Portal (default)	MDM Portal (default)
My Devices Portal (default)	Self-Registered Guest Portal (default)
Sponsor Portal (default)	Sponsored Guest Portal (default)

Note that I am use this one cert for pretty much every service (pxGrid certs require more permissions than the Web Server template so it cannot use this cert). Click submit. There will be several warnings as these services are moved off the self-signed cert and to this new one. At conclusion the server will restart.

After restart the Admin portal should now be serving this new certificate



```
Not Critical
DNS Name: *.example.com
DNS Name: ise.example.com
IP Address: 192.168.150.50
```

se is expiring

Apex License is expiring in 89 days.

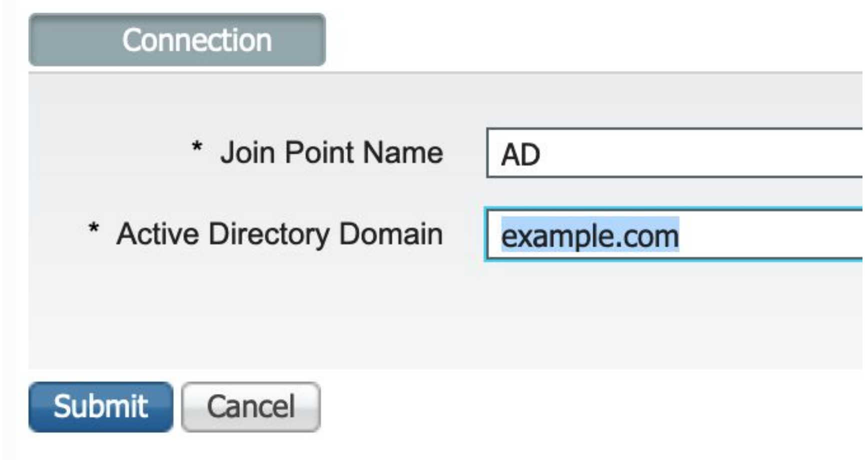
Device Admin License is expiring in 89 days.

Fewer VM licenses installed than VM resources/VM nodes deployed.

Active Directory

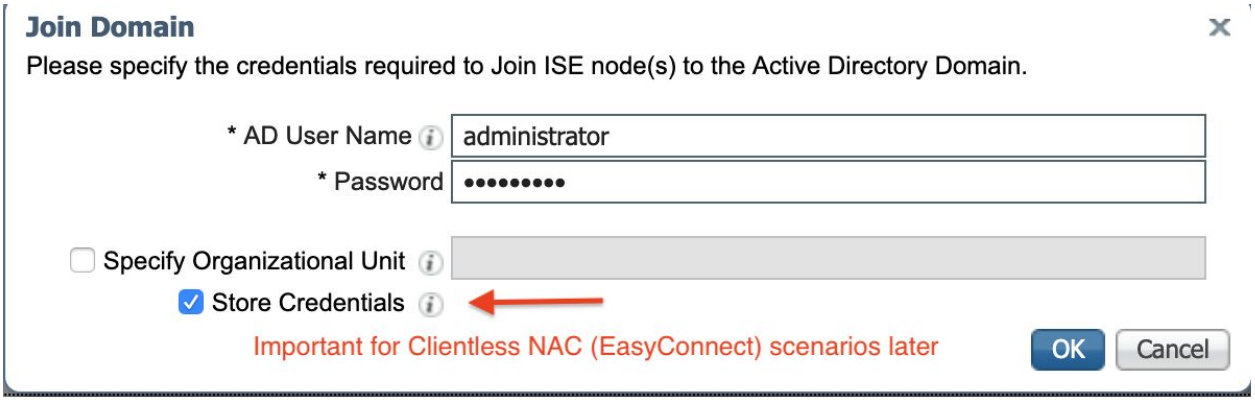
ISE servers must be joined to Active Directory in order to authenticate users against it and retrieve group memberships. We're going to join the example.com domain and select the three relevant AD groups that we will base policy off of.

Go to Administration--Identity Management--External Identity Sources--Active Directory. And select "Add"



* Join Point Name: AD

* Active Directory Domain: example.com



Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name: administrator

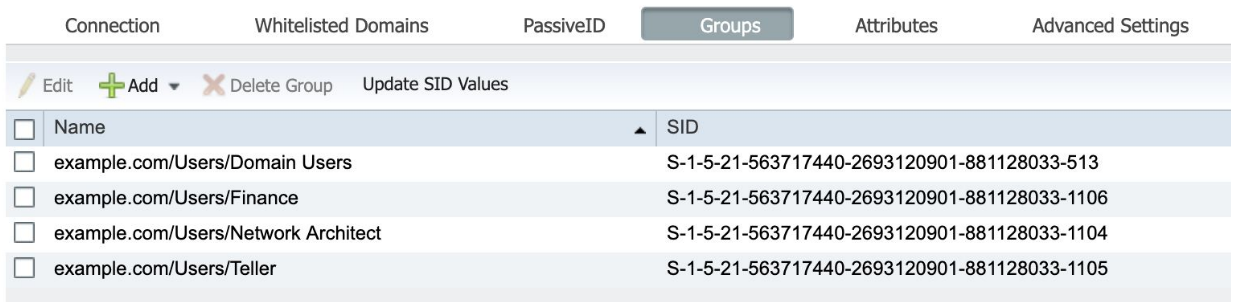
* Password: ••••••••••

☐ Specify Organizational Unit

☑ Store Credentials

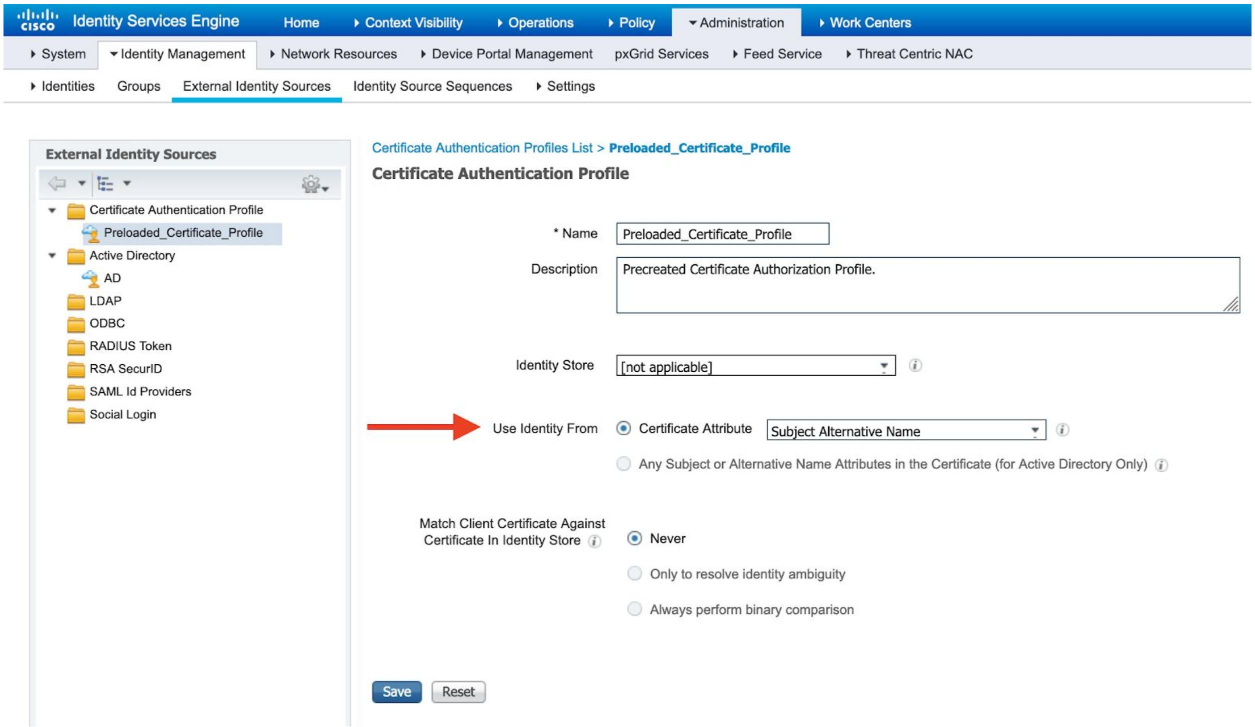
Important for Clientless NAC (EasyConnect) scenarios later

On Groups tab click "Add" and select the relevant groups for your use case



☐	Name	SID
☐	example.com/Users/Domain Users	S-1-5-21-563717440-2693120901-881128033-513
☐	example.com/Users/Finance	S-1-5-21-563717440-2693120901-881128033-1106
☐	example.com/Users/Network Architect	S-1-5-21-563717440-2693120901-881128033-1104
☐	example.com/Users/Teller	S-1-5-21-563717440-2693120901-881128033-1105

While you're in this section, go to Administration--Identity Management--External Identity Sources--Certificate Authentication Profile-Preloaded_Certificate_Profile. Change the default 'Use Identity From" selection to "Subject Alternative Name". See below. The reason this is used is that's where the Windows CA User template places the user's logon name (the CN contains their full name.)



Certificate Authentication Profiles List > **Preloaded_Certificate_Profile**

Certificate Authentication Profile

* Name: Preloaded_Certificate_Profile

Description: Precreated Certificate Authorization Profile.

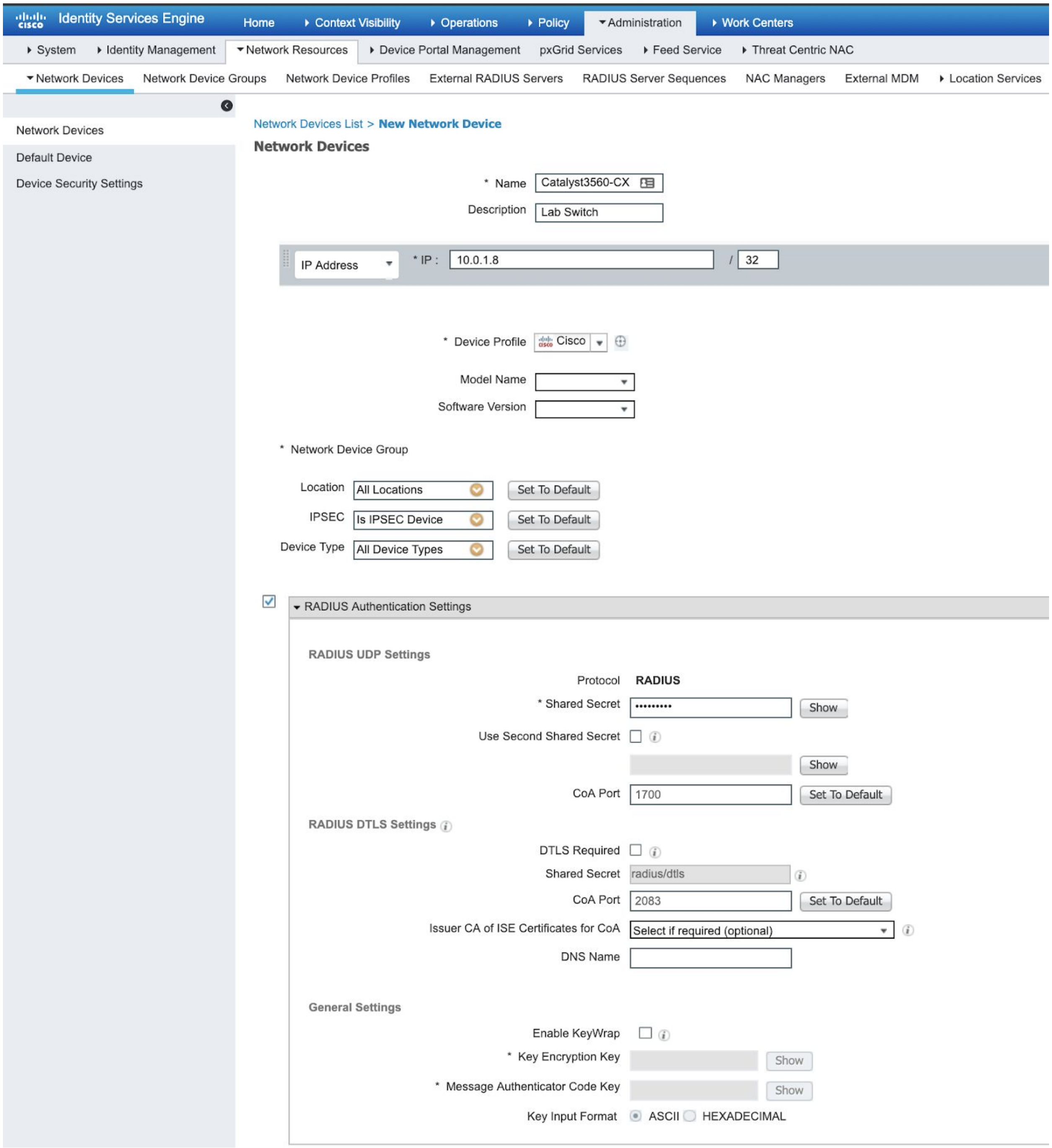
Identity Store: [not applicable]

Use Identity From:
- ● Certificate Attribute: Subject Alternative Name
- ○ Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store:
- ● Never
- ○ Only to resolve identity ambiguity
- ○ Always perform binary comparison

Add Switch

Adding the lab Catalyst Switch. Adding in SNMPv2c and RADIUS information. That’s at Administration--Network Resources--Network Devices



Network Devices List > **New Network Device**

Network Devices

* Name: Catalyst3560-CX

Description: Lab Switch

IP Address * IP : 10.0.1.8 / 32

* Device Profile: Cisco

Model Name:

Software Version:

* Network Device Group

Location: All Locations

IPSEC: Is IPSEC Device

Device Type: All Device Types

☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol: **RADIUS**

* Shared Secret: •••••••••

Use Second Shared Secret ☐

CoA Port: 1700

RADIUS DTLS Settings

DTLS Required ☐

Shared Secret: radius/dtls

CoA Port: 2083

Issuer CA of ISE Certificates for CoA: Select if required (optional)

DNS Name:

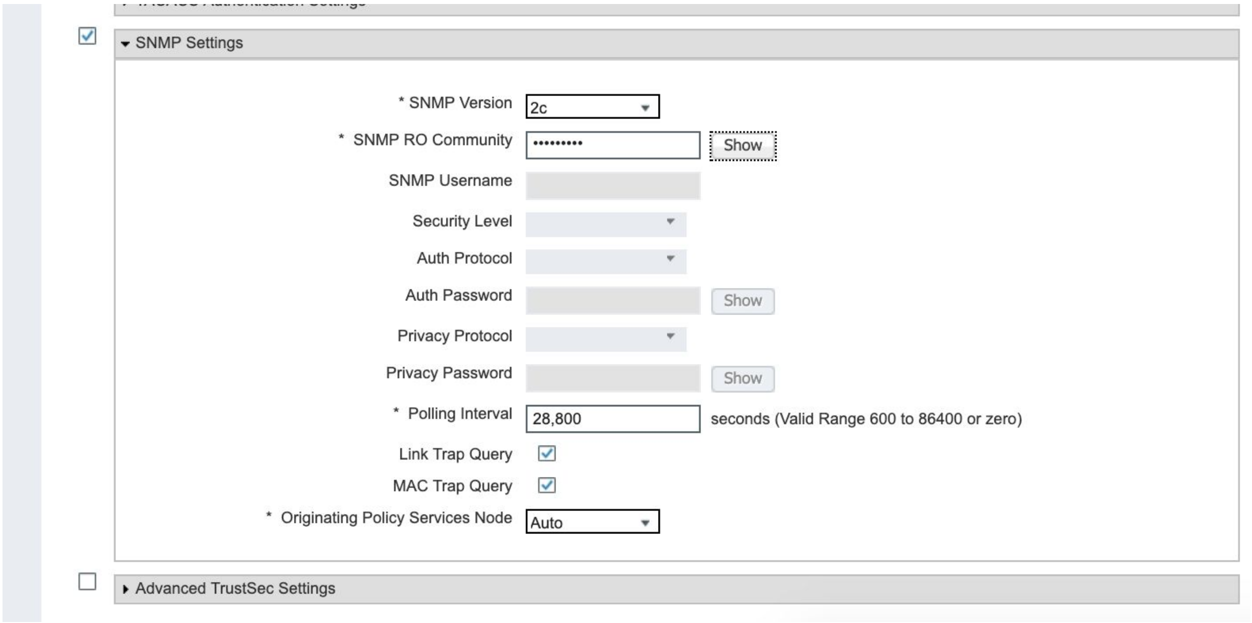
General Settings

Enable KeyWrap ☐

* Key Encryption Key:

* Message Authenticator Code Key:

Key Input Format: ● ASCII ○ HEXADECIMAL



☑ SNMP Settings

* SNMP Version: 2c

* SNMP RO Community: ••••••••• Show

SNMP Username:

Security Level:

Auth Protocol:

Auth Password: Show

Privacy Protocol:

Privacy Password: Show

* Polling Interval: 28,800 seconds (Valid Range 600 to 86400 or zero)

Link Trap Query: ☑

MAC Trap Query: ☑

* Originating Policy Services Node: Auto

☐ Advanced TrustSec Settings

Profiling

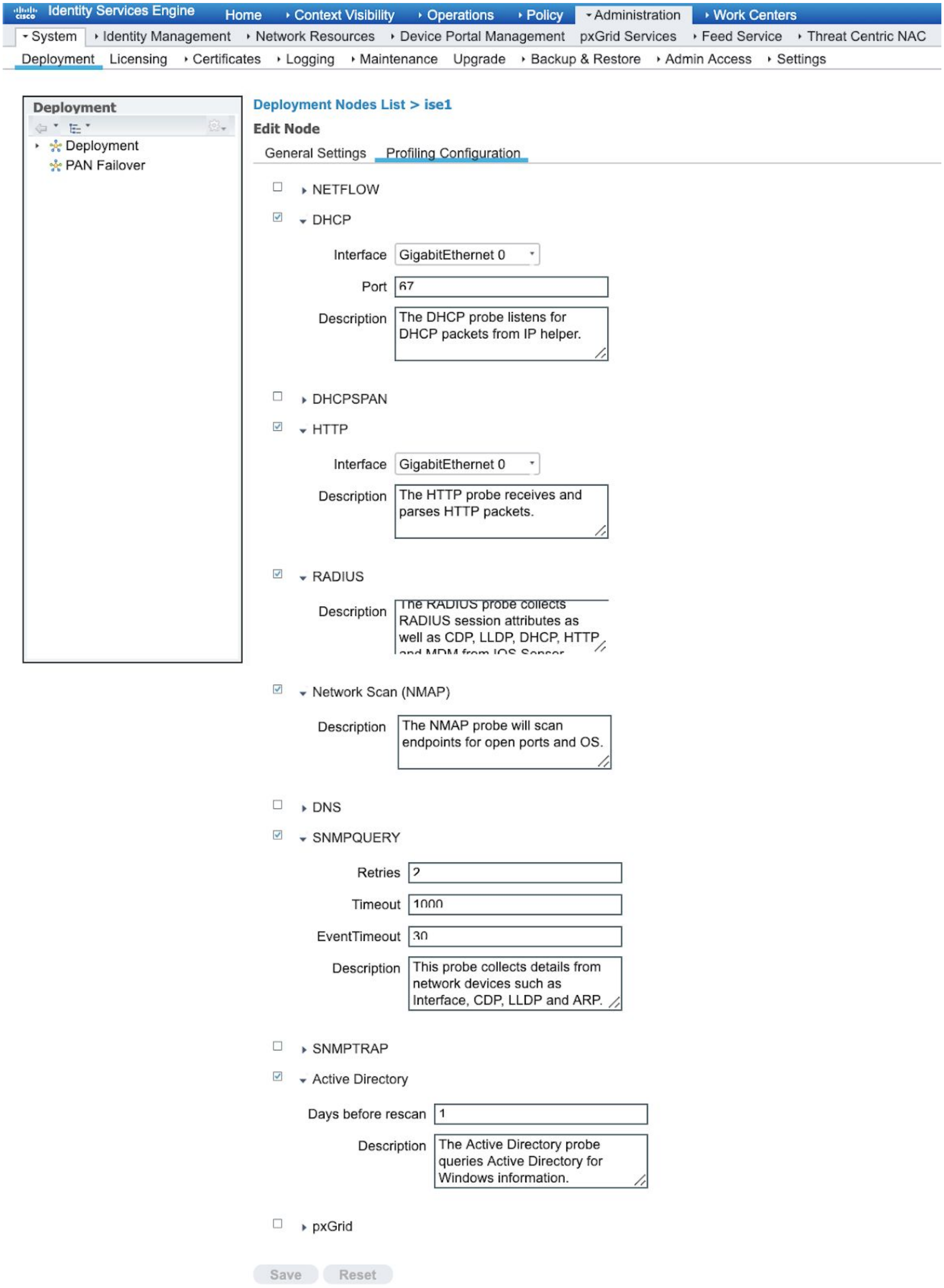
Now we're getting to the good stuff. Two excellent in-depth guides and tutorials can be found at ISE Profiling Design Guide by Craig Hyps/Thomas Howard and also Katherine McNamara's recent ISE Profiling Deep-Dive.

For the purposes of this article we'll try to confine profiling to as few probes as possible and make them across switch/wireless vendors (whenever possible).

Probe	Description	Notes	Enabled by Default
DHCP	Acquires Client information by its DHCP Discover Packet	One of the most powerful probes available	Yes
HTTP	Acquires HTTP User-Agent information if the endpoint is running a browser	Redirected web portals capture the user-agent without the HTTP probe explicitly enabled	No
RADIUS	Leverages Switch/WLC intelligence (the Device Sensor	Probably the most powerful probe and can be used instead of DHCP/HTTP	Yes

	feature) to provide MAC address, DHCP, CDP/LLDP, and HTTP User Agent info	probes if the switch/WLC supports it	
NMAP	Direct Querying of the endpoint to make more accurate profile matches	NMAP is available in some partial profile matches but not others by default (such as Windows Workstations) but can be directly enabled by default	Yes
SNMPQUERY	Direct Query of switches for MAC address, Port, CCDP/LLDP (among others)	Used for catchall endpoints that don't frequently authenticate or have static IP addresses	Yes
SNMPQUERY within NMAP	Part of the NMAP probe is to SNMP query the endpoint for more device information and rudimentary IoT authentication	This is useful to authenticate printers that serve the correct SNMP parameters back to ISE	(as part of NMAP probe)
Active Directory	Active Directory contains several attributes for Windows Joined Computers that can be used for profiling	Useful for determining endpoint OS and whether this is a corporate asset	Yes

These profiles are modified via Administration--System--Deployment--Deployment Nodes List--(server)--Profiling Configuration



Deployment Nodes List > ise1

Edit Node

☐ NETFLOW

☑ DHCP

Interface: GigabitEthernet 0

Port: 67

Description: The DHCP probe listens for DHCP packets from IP helper.

☐ DHCPSPAN

☑ HTTP

Interface: GigabitEthernet 0

Description: The HTTP probe receives and parses HTTP packets.

☑ RADIUS

Description: The RADIUS probe collects RADIUS session attributes as well as CDP, LLDP, DHCP, HTTP and MDM from IOS Sensor

☑ Network Scan (NMAP)

Description: The NMAP probe will scan endpoints for open ports and OS.

☐ DNS

☑ SNMPQUERY

Retries: 2

Timeout: 1000

EventTimeout: 30

Description: This probe collects details from network devices such as Interface, CDP, LLDP and ARP.

☐ SNMPTRAP

☑ Active Directory

Days before rescan: 1

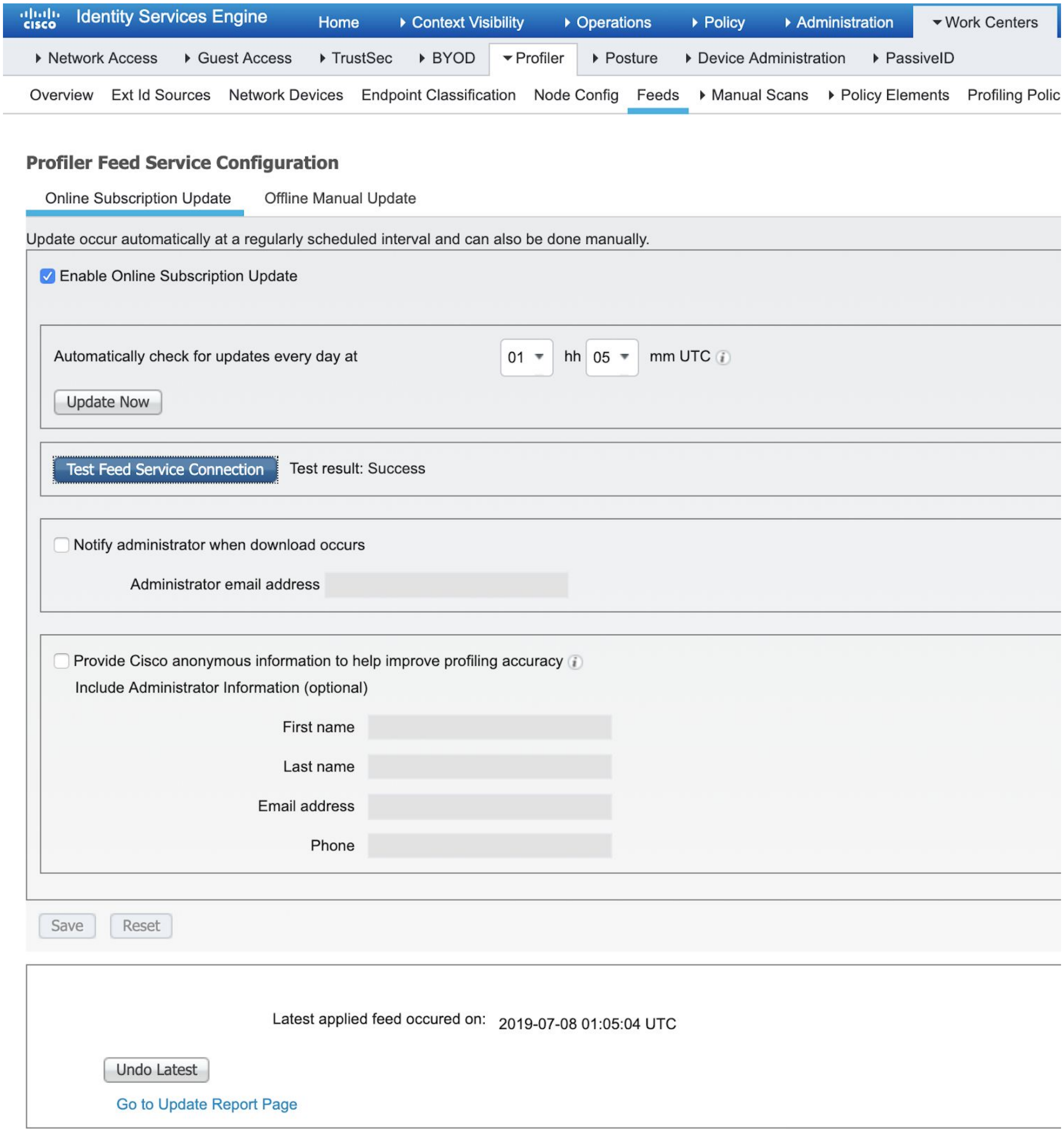
Description: The Active Directory probe queries Active Directory for Windows information.

☐ pxGrid

Feed Service

The ISE node needs to have Internet access to check for updated Feed profile information (checked nightly). It's enabled out of the box but can be sideloaded if needed.

Work Centers--Profiler--Feeds



Profiler Feed Service Configuration

Update occur automatically at a regularly scheduled interval and can also be done manually.

☑ Enable Online Subscription Update

Automatically check for updates every day at 01 hh 05 mm UTC

Test result: Success

☐ Notify administrator when download occurs

Administrator email address

☐ Provide Cisco anonymous information to help improve profiling accuracy

Include Administrator Information (optional)

First name

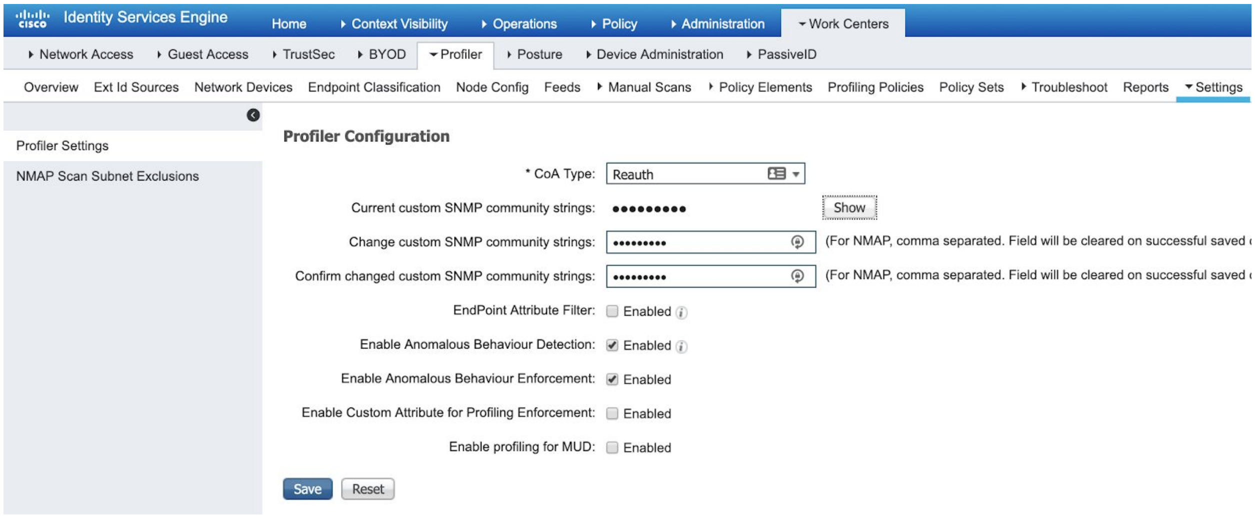
Last name

Email address

Phone

Latest applied feed occured on: 2019-07-08 01:05:04 UTC

If you will be using SNMP on endpoint devices (typically IoT like printers) set those custom community strings at Work Centers--Profiler--Settings--Profiler Settings.   You can set multiple strings, comma separated.



Profiler Configuration

* CoA Type: Reauth

Current custom SNMP community strings: ●●●●●●●●●

Change custom SNMP community strings: ••••••••• (For NMAP, comma separated. Field will be cleared on successful saved

Confirm changed custom SNMP community strings: ••••••••• (For NMAP, comma separated. Field will be cleared on successful saved

EndPoint Attribute Filter: ☐ Enabled

Enable Anomalous Behaviour Detection: ☑ Enabled

Enable Anomalous Behaviour Enforcement: ☑ Enabled

Enable Custom Attribute for Profiling Enforcement: ☐ Enabled

Enable profiling for MUD: ☐ Enabled

Profiling - Where are we now?

At this point in our network we have the following deployed:

- Active Directory Integration
- Profiling enabled on ISE
    - With NMAP/SNMP
- Switch defined in ISE with available SNMP read access
- Nothing special/additional on Cisco switch (note, going forward we would need more infrastructure configuration, such as enabling RADIUS on the switch to capture DHCP information or by adding DHCP helper addresses at the endpoint gateways… or adding a DHCP span tap). See section on Catalyst Config for reference

With this config ISE will begin profiling all the endpoints connected to switches (just my one lab switch for example). It will get MAC OUI, IP address (if it’s also collecting SNMP from upstream gateway that has the ARP cache). And depending on the Profiling policy set, NMAP/SNMP querying of the endpoint. NOTE, by default some endpoint profile types do not have NMAP actions enabled to minimize the chance ISE will interfere/disrupt the endpoint if it is actively scanned. Windows Workstations by default do not have NMAP scanning enabled but it can be by the user. Here’s another quirk of NMAP history, NMAP won’t scan udp/tcp 9001 because there are some printers out there that will print anything sent on those ports so reams of paper would be used filled with binary TLS headers, etc if NMAP scanned.

The Active Directory Probe isn’t doing much at this point either because we do not have the hostname of the endpoint and that is a prerequisite before we can check against Active

Directory for attributes for the endpoint. At this point one could enable the DNS probe to perform reverse DNS queries to get those names (which should work well as most AD joined endpoints update Dynamic DNS records).

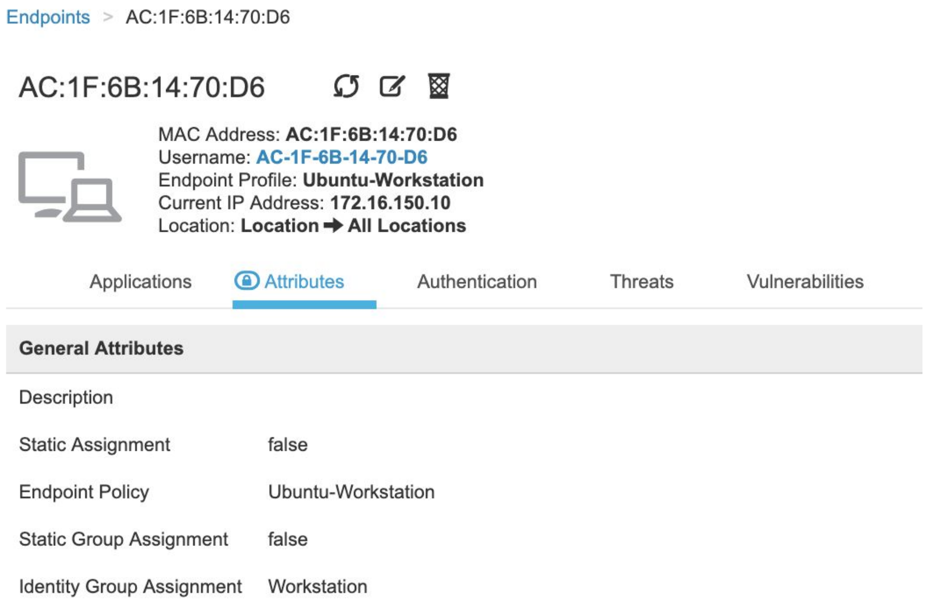
Profile Weighting (a quick tutorial)

It's important to note how ISE assigns an endpoint profile to an endpoint. There is a logical hierarchy that goes from less specific to more specific with each step requiring a 'Certainty Factor' threshold to qualify in each step. The endpoint profile will culminate in all the CF 'points' the endpoint has acquired   Take this example:

Workstation (minimum Certainty factor is 10)--Linux Workstation (min CF is 10)--Ubuntu (min CF is 20)

These are a series of gates. And endpoint must match the rules in Workstation to pass on to passing the rules in 'Linux Workstation' before it can be evaluated to be an Ubuntu OS. At the end of this process, a Ubuntu workstation will be at least 40 (though in practice will likely be much more as some profile rules contribute more than the minimum CF… or the endpoint matches several rules, adding more to its CF. The final CF determines whether ISE determines this is a Ubuntu Linux Workstation.

Here's an actual Ubuntu example:



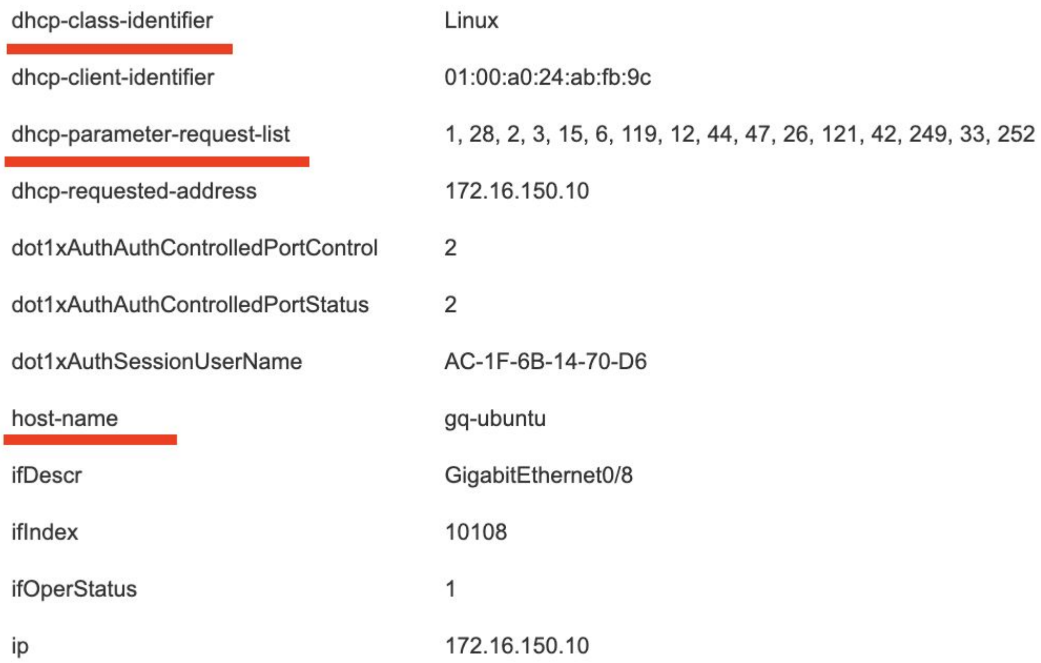
Endpoints > AC:1F:6B:14:70:D6

AC:1F:6B:14:70:D6

MAC Address: **AC:1F:6B:14:70:D6**
Username: **AC-1F-6B-14-70-D6**
Endpoint Profile: **Ubuntu-Workstation**
Current IP Address: **172.16.150.10**
Location: **Location ➔ All Locations**

General Attributes

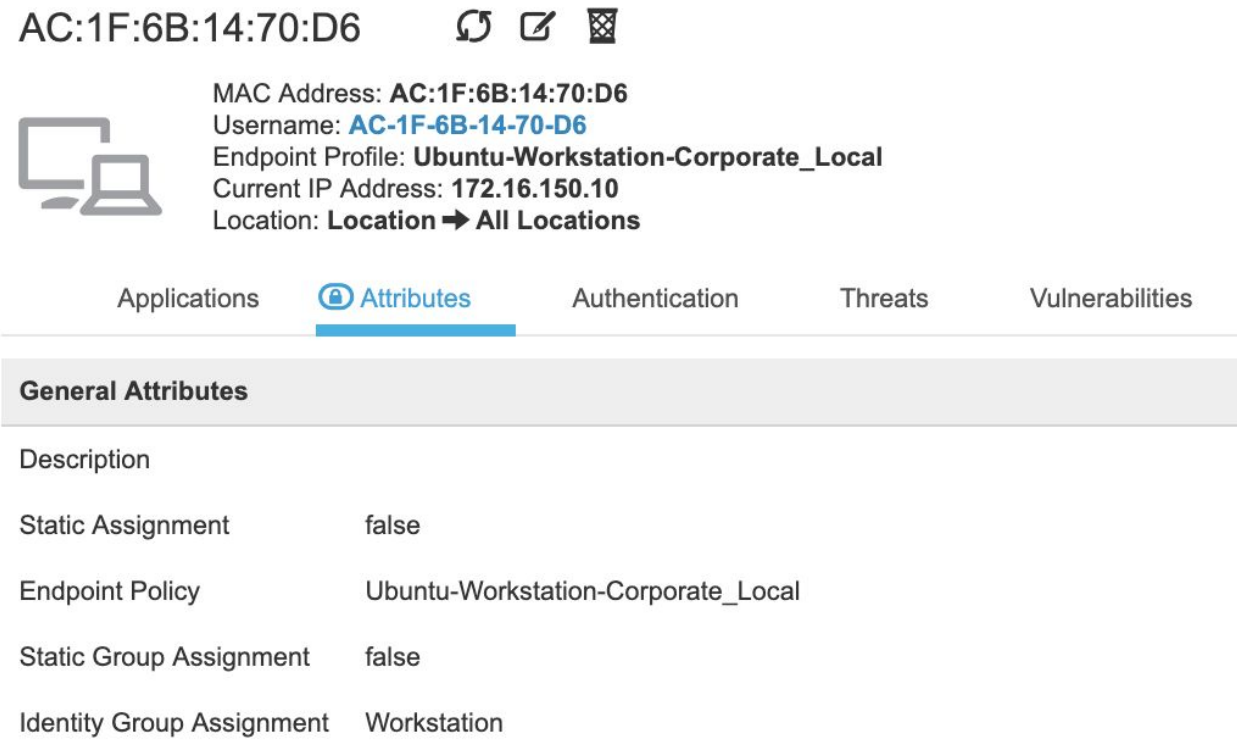
Description	
Static Assignment	false
Endpoint Policy	Ubuntu-Workstation
Static Group Assignment	false
Identity Group Assignment	Workstation



dhcp-class-identifier	Linux
dhcp-client-identifier	01:00:a0:24:ab:fb:9c
dhcp-parameter-request-list	1, 28, 2, 3, 15, 6, 119, 12, 44, 47, 26, 121, 42, 249, 33, 252
dhcp-requested-address	172.16.150.10
dot1xAuthAuthControlledPortControl	2
dot1xAuthAuthControlledPortStatus	2
dot1xAuthSessionUserName	AC-1F-6B-14-70-D6
host-name	gq-ubuntu
ifDescr	GigabitEthernet0/8
ifIndex	10108
ifOperStatus	1
ip	172.16.150.10

The underlined attributes were how it arrived at this decision. Dhcp-class-identifier is ‘Linux’ meets the Linux-Workstation profile. The DHCP parameter list and hostname (contains ‘ubuntu’) trips it into the Ubuntu-Workstation profile. The total certainty factor is 80 from these pieces.

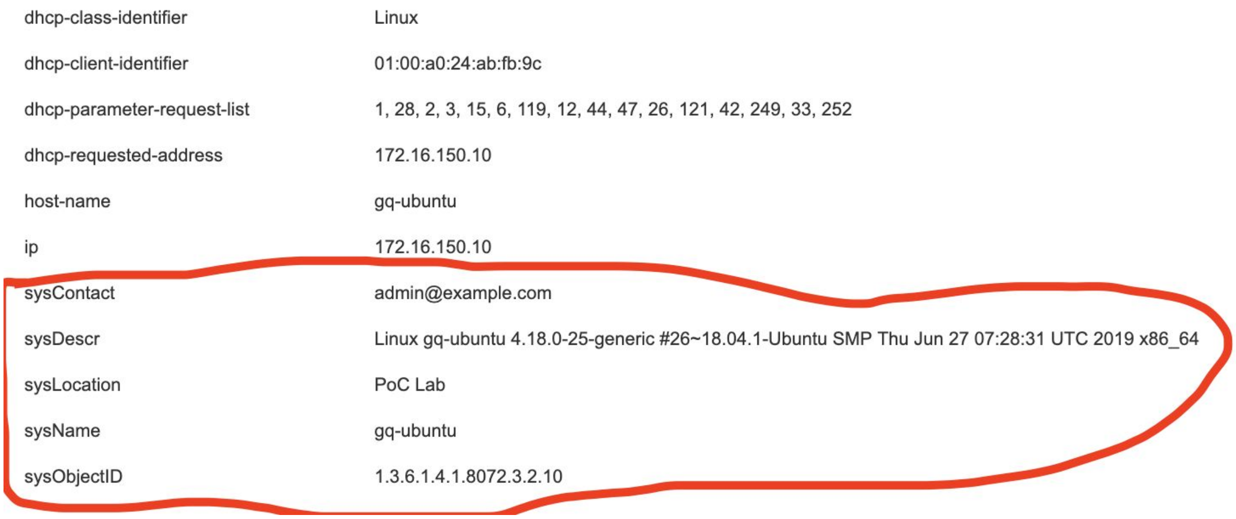
So let’s take it one step further and check if SNMP is running on this endpoint and that it has proper SysID values to assign it a ‘corporate’ profile setting (note this use case applies equally to any IoT device that can run SNMP agents).



MAC Address: **AC:1F:6B:14:70:D6**
Username: **AC-1F-6B-14-70-D6**
Endpoint Profile: **Ubuntu-Workstation-Corporate_Local**
Current IP Address: **172.16.150.10**
Location: **Location ➡ All Locations**

General Attributes

Description	
Static Assignment	false
Endpoint Policy	Ubuntu-Workstation-Corporate_Local
Static Group Assignment	false
Identity Group Assignment	Workstation



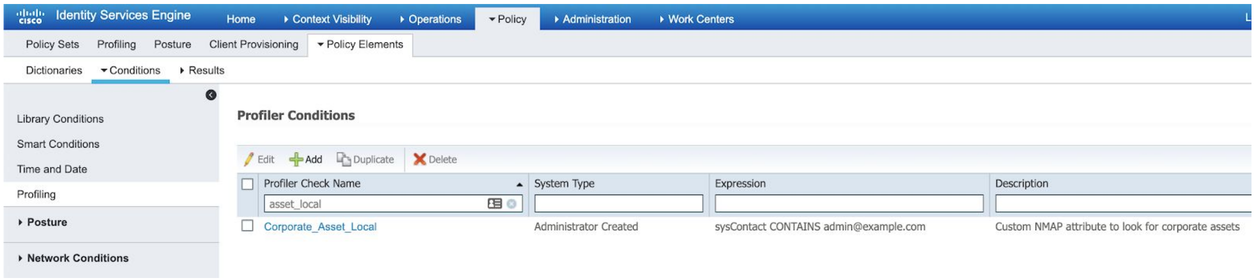
dhcp-class-identifier	Linux
dhcp-client-identifier	01:00:a0:24:ab:fb:9c
dhcp-parameter-request-list	1, 28, 2, 3, 15, 6, 119, 12, 44, 47, 26, 121, 42, 249, 33, 252
dhcp-requested-address	172.16.150.10
host-name	gq-ubuntu
ip	172.16.150.10
sysContact	admin@example.com
sysDescr	Linux gq-ubuntu 4.18.0-25-generic #26~18.04.1-Ubuntu SMP Thu Jun 27 07:28:31 UTC 2019 x86_64
sysLocation	PoC Lab
sysName	gq-ubuntu
sysObjectID	1.3.6.1.4.1.8072.3.2.10

The certainty factor is now 110 that this is a Ubuntu Workstation Corporate asset. So how did I build this policy?

Ubuntu Corporate Workstation Profile

So how did I build this policy for ‘Ubuntu-Workstation-Corporate_Local’?

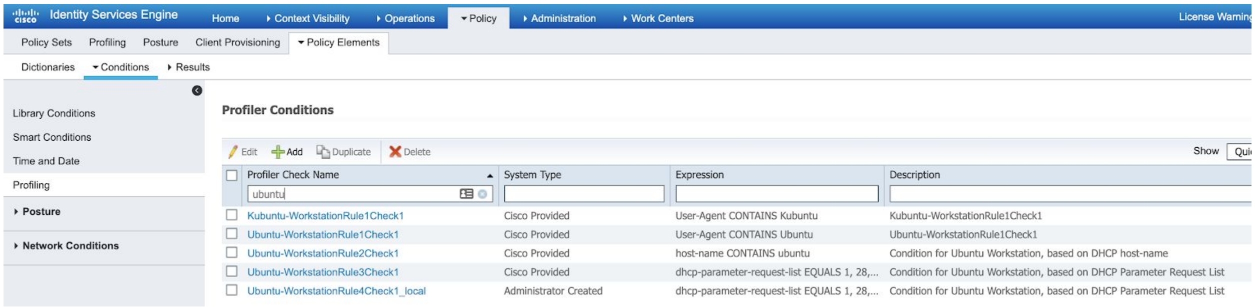
Start by adding a Profiling Condition that looks for a specific SNMP systemcontact (SysContact). Navigate to Policy--Policy Elements--Conditions--Profiling and add new (note I just used the contact, but you can make partial/exact matches on several SNMP values, like Description or location or name):



Profiler Conditions

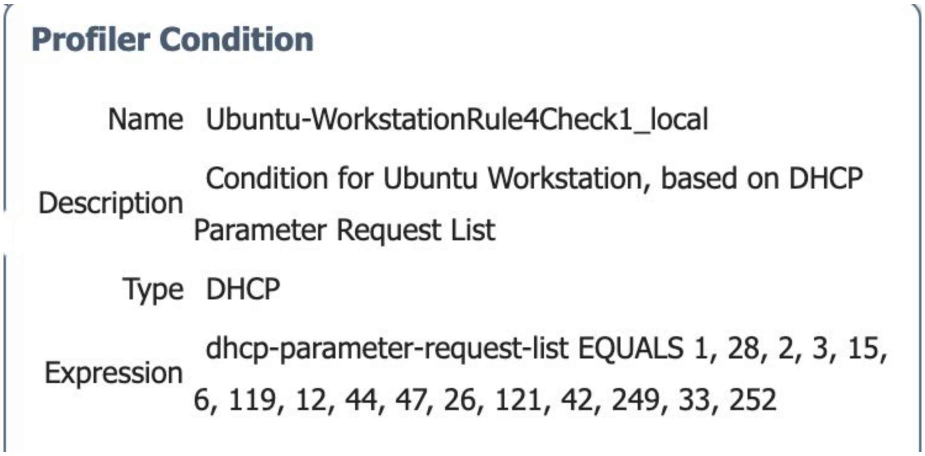
☐	Profiler Check Name	System Type	Expression	Description
	asset_local			
☐	Corporate_Asset_Local	Administrator Created	sysContact CONTAINS admin@example.com	Custom NMAP attribute to look for corporate assets

While you're here in the conditions, note that I added a custom Ubuntu check for a new set of DHCP requested parameters list because the feeder conditions did not match my lab Ubuntu 18.04.1LTS load. This is a great exercise for custom IoT devices and making custom matches (note a lot of customers will make custom matches for DHCP User Class ID to denote customer controlled assets):



Profiler Conditions

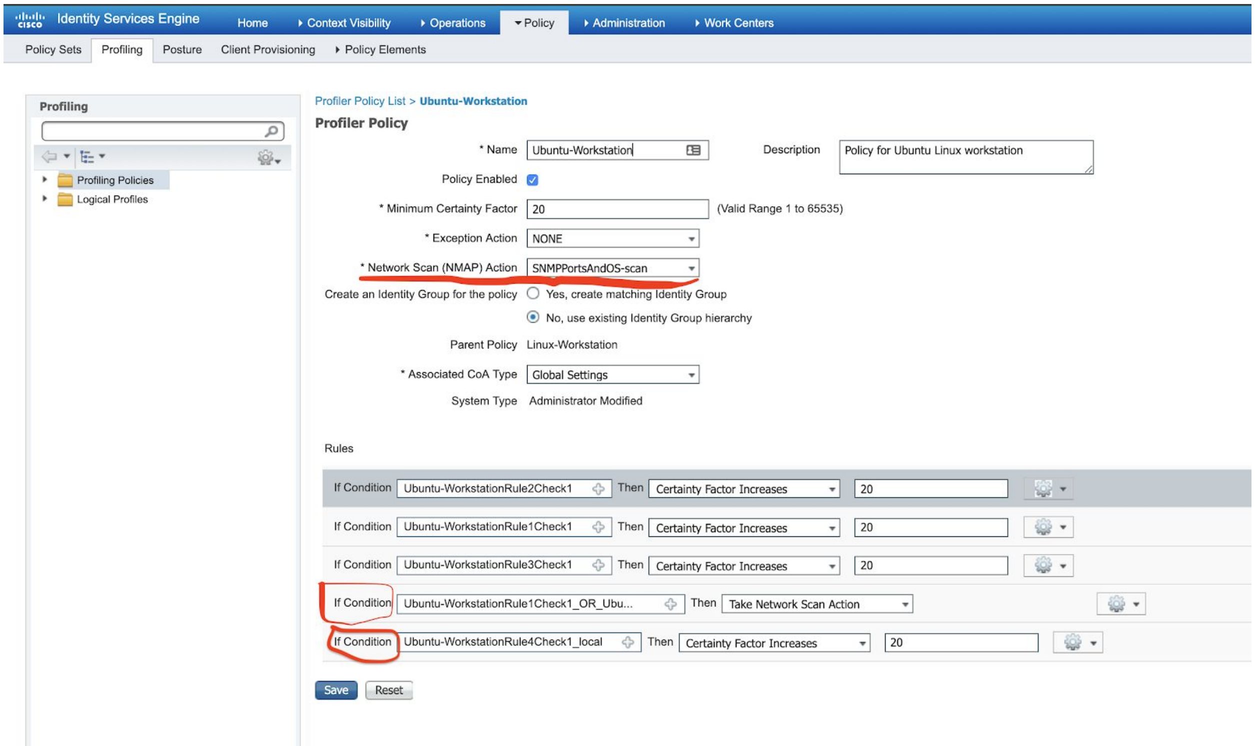
☐	Profiler Check Name	System Type	Expression	Description
	ubuntu			
☐	Kubuntu-WorkstationRule1Check1	Cisco Provided	User-Agent CONTAINS Kubuntu	Kubuntu-WorkstationRule1Check1
☐	Ubuntu-WorkstationRule1Check1	Cisco Provided	User-Agent CONTAINS Ubuntu	Ubuntu-WorkstationRule1Check1
☐	Ubuntu-WorkstationRule2Check1	Cisco Provided	host-name CONTAINS ubuntu	Condition for Ubuntu Workstation, based on DHCP host-name
☐	Ubuntu-WorkstationRule3Check1	Cisco Provided	dhcp-parameter-request-list EQUALS 1, 28,...	Condition for Ubuntu Workstation, based on DHCP Parameter Request List
☐	Ubuntu-WorkstationRule4Check1_local	Administrator Created	dhcp-parameter-request-list EQUALS 1, 28,...	Condition for Ubuntu Workstation, based on DHCP Parameter Request List



Profiler Condition

Name	Ubuntu-WorkstationRule4Check1_local
Description	Condition for Ubuntu Workstation, based on DHCP Parameter Request List
Type	DHCP
Expression	dhcp-parameter-request-list EQUALS 1, 28, 2, 3, 15, 6, 119, 12, 44, 47, 26, 121, 42, 249, 33, 252

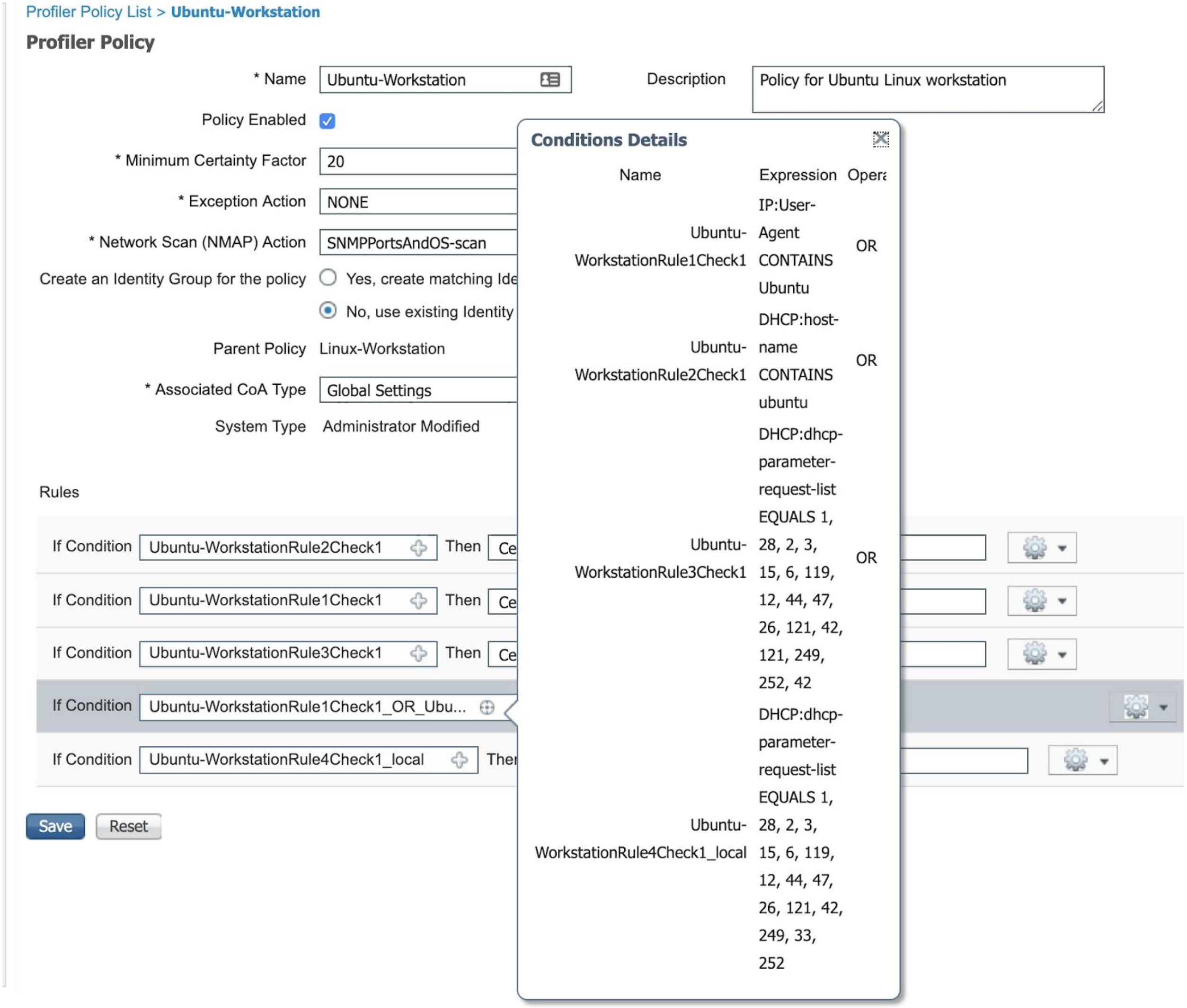
Next step is to tweak the built-in Profiler Policy for Ubuntu-Workstation. This is at Policy--Profiling--Profiling Policies--Ubuntu-Workstation. I made two tweaks. The first is I'm now checking for the updated DHCP Parameter List outlined above. Second tweak is I'm enabling an SNMP if any of the 4 Profiling conditions are met (you can see that in the following screenshots)



* Name: Ubuntu-Workstation
Description: Policy for Ubuntu Linux workstation
Policy Enabled: ☑
* Minimum Certainty Factor: 20 (Valid Range 1 to 65535)
* Exception Action: NONE
* Network Scan (NMAP) Action: SNMPPortsAndOS-scan
Create an Identity Group for the policy: ○ Yes, create matching Identity Group
● No, use existing Identity Group hierarchy
Parent Policy: Linux-Workstation
* Associated CoA Type: Global Settings
System Type: Administrator Modified

Rules

If Condition Ubuntu-WorkstationRule2Check1 Then Certainty Factor Increases 20
If Condition Ubuntu-WorkstationRule1Check1 Then Certainty Factor Increases 20
If Condition Ubuntu-WorkstationRule3Check1 Then Certainty Factor Increases 20
If Condition Ubuntu-WorkstationRule1Check1_OR_Ubu... Then Take Network Scan Action
If Condition Ubuntu-WorkstationRule4Check1_local Then Certainty Factor Increases 20



Profiler Policy List > **Ubuntu-Workstation**

Profiler Policy

* Name: Ubuntu-Workstation
Description: Policy for Ubuntu Linux workstation
Policy Enabled: ☑
* Minimum Certainty Factor: 20
* Exception Action: NONE
* Network Scan (NMAP) Action: SNMPPortsAndOS-scan
Create an Identity Group for the policy: ○ Yes, create matching Ide ● No, use existing Identity
Parent Policy: Linux-Workstation
* Associated CoA Type: Global Settings
System Type: Administrator Modified

Rules

If Condition Ubuntu-WorkstationRule2Check1 Then Ce
If Condition Ubuntu-WorkstationRule1Check1 Then Ce
If Condition Ubuntu-WorkstationRule3Check1 Then Ce
If Condition Ubuntu-WorkstationRule1Check1_OR_Ubu...
If Condition Ubuntu-WorkstationRule4Check1_local Ther

Conditions Details

Name	Expression	Opera
Ubuntu-WorkstationRule1Check1	IP:User-Agent CONTAINS Ubuntu	OR
Ubuntu-WorkstationRule2Check1	DHCP:host-name CONTAINS ubuntu	OR
Ubuntu-WorkstationRule3Check1	DHCP:dhcp-parameter-request-list EQUALS 1, 28, 2, 3, 15, 6, 119, 12, 44, 47, 26, 121, 42, 121, 249, 252, 42	OR
Ubuntu-WorkstationRule4Check1_local	DHCP:dhcp-parameter-request-list EQUALS 1, 28, 2, 3, 15, 6, 119, 12, 44, 47, 26, 121, 42, 249, 33, 252	

And that’s it, this one is done.

Ubuntu Corporate Asset Configuration (SNMP and DHCP)

For details on how I made Ubuntu be a “corporate asset”, install snmpd (use this guide). My snmpd.conf file includes these relevant lines (you can find their placement when you open your copy of /etc/snmp/snmpd.conf:

```
agentAddress udp:161,udp6:[::1]:161
rocommunity [community string]  192.168.150.0/24
sysLocation    PoC Rack
sysContact     admin@example.com
```

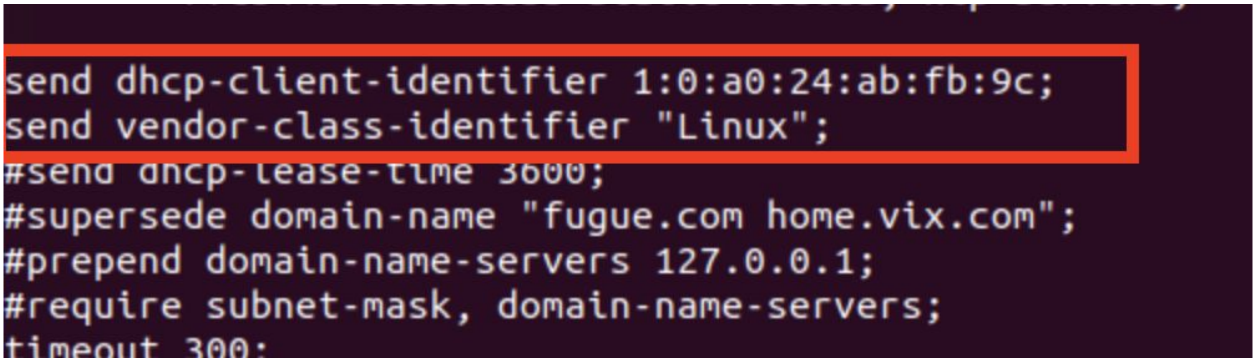
And for DHCP, edit /etc/dhclient.conf

Uncomment the line:

```
send dhcp-client-identifier [some string];
```

And add:

```
send vendor-class-identifier “Linux”;
```



```
send dhcp-client-identifier 1:0:a0:24:ab:fb:9c;
send vendor-class-identifier "Linux";
#send dhcp-lease-time 3600;
#supersede domain-name "fugue.com home.vix.com";
#prepend domain-name-servers 127.0.0.1;
#require subnet-mask, domain-name-servers;
timeout 300;
```

For Windows workstations using the built-in Active Directory Probe nicely handles if it’s a company asset instead of doing SNMP checking. That will be called out in the Easy Connect section next.

Logical Profiles

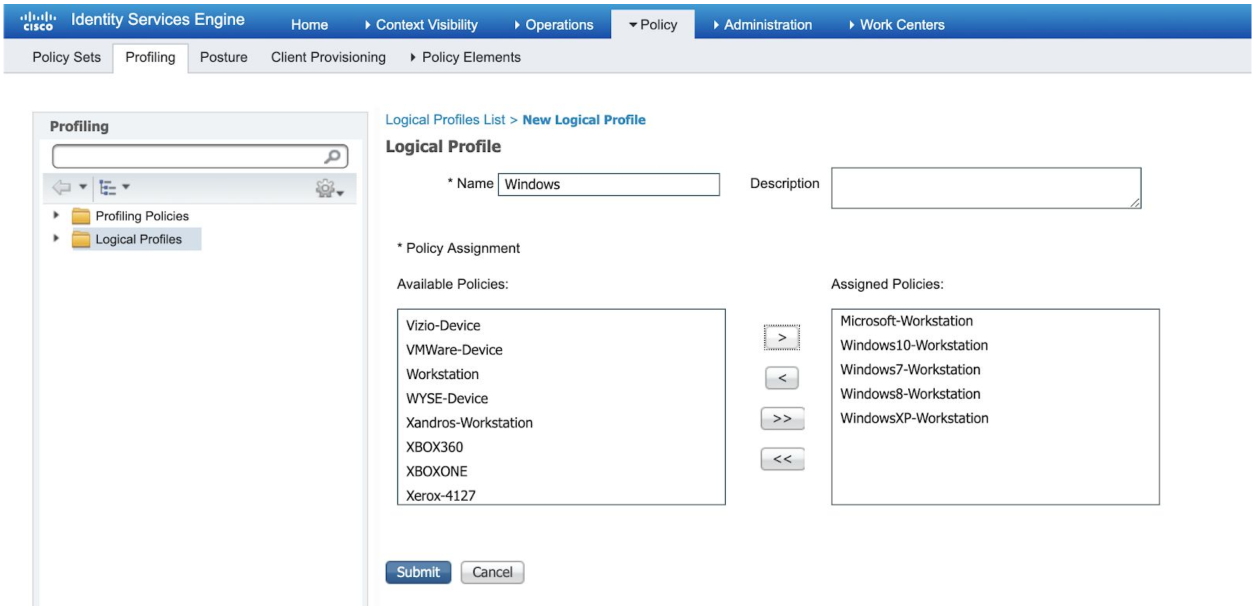
Logical Profiles are a grouping of several profiling policies that will be invoked in future policy actions. I’ll simply make these three now and their use will be apparent later on. And also for more information.

Name	Purpose
Windows	To group all Windows OS Workstations
MacOS	To group all Windows OS Workstations
Approved Linux Workstations	All Linux workstations that respond to SNMP querying

Navigate to Policy--Profiling--Logical Profiles

Click “Add” and fill out these Logical Profiles:

Windows



Logical Profiles List > **New Logical Profile**

Logical Profile

* Name: Windows

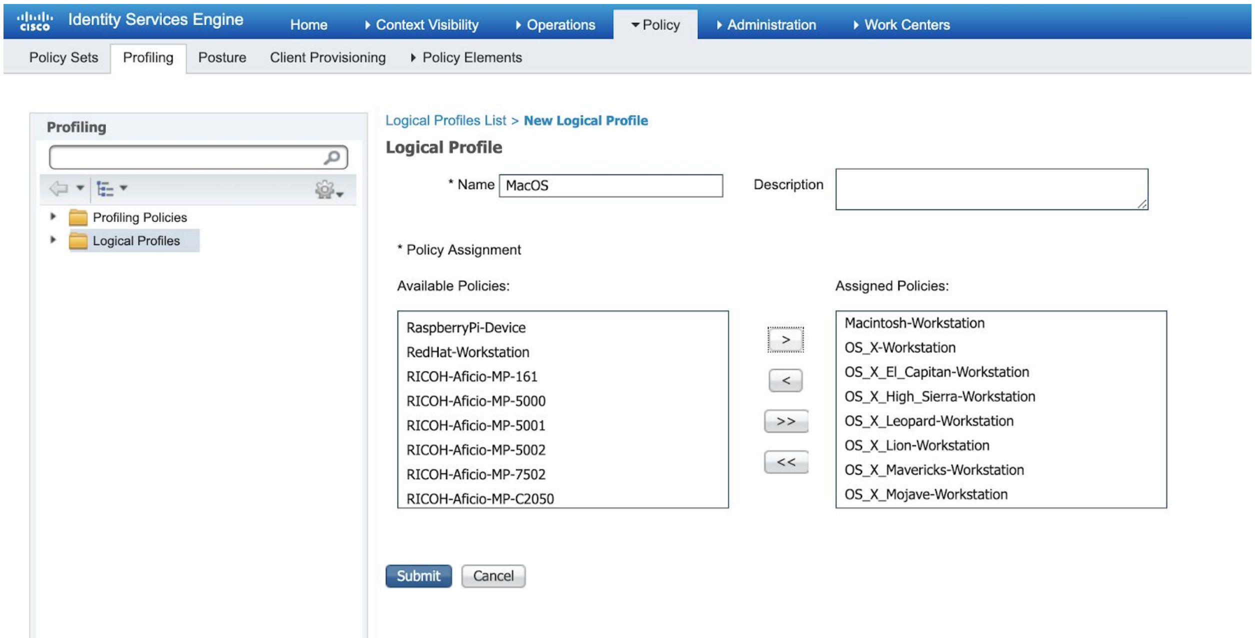
Description:

* Policy Assignment

Available Policies:
- Vizio-Device
- VMWare-Device
- Workstation
- WYSE-Device
- Xandros-Workstation
- XBOX360
- XBOXONE
- Xerox-4127

Assigned Policies:
- Microsoft-Workstation
- Windows10-Workstation
- Windows7-Workstation
- Windows8-Workstation
- WindowsXP-Workstation

MacOS



Logical Profiles List > **New Logical Profile**

Logical Profile

* Name: MacOS

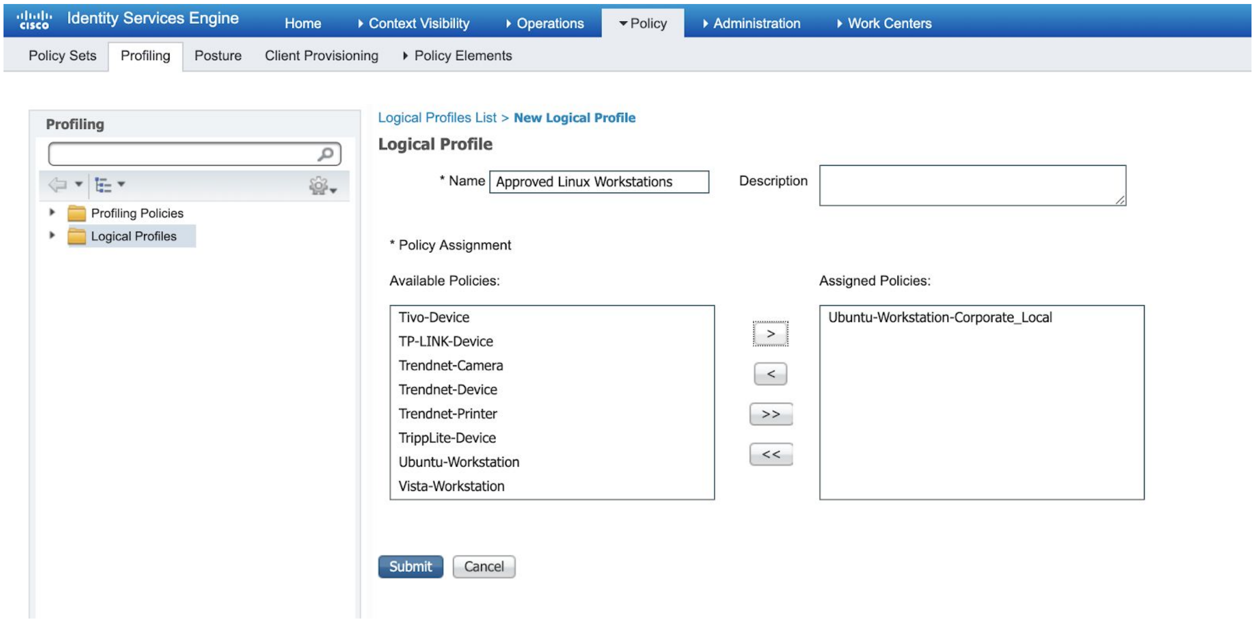
Description:

* Policy Assignment

Available Policies:
- RaspberryPi-Device
- RedHat-Workstation
- RICOH-Aficio-MP-161
- RICOH-Aficio-MP-5000
- RICOH-Aficio-MP-5001
- RICOH-Aficio-MP-5002
- RICOH-Aficio-MP-7502
- RICOH-Aficio-MP-C2050

Assigned Policies:
- Macintosh-Workstation
- OS_X-Workstation
- OS_X_El_Capitan-Workstation
- OS_X_High_Sierra-Workstation
- OS_X_Leopard-Workstation
- OS_X_Lion-Workstation
- OS_X_Mavericks-Workstation
- OS_X_Mojave-Workstation

Linux (note that you could easily add multiple “flavors” of Linux desktops with this construct)



* Name: Approved Linux Workstations

Description:

* Policy Assignment

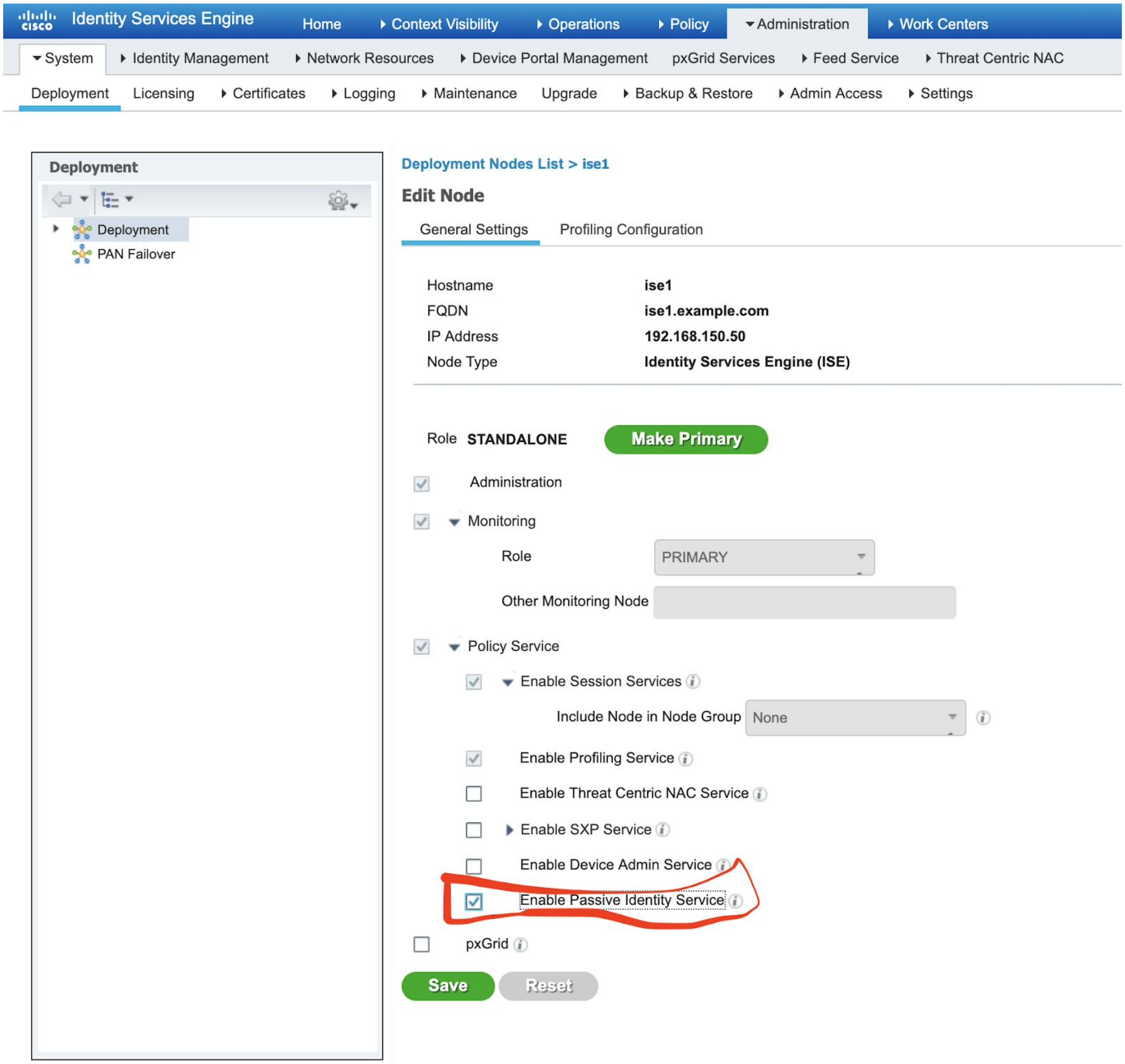
Available Policies:
- Tivo-Device
- TP-LINK-Device
- Trendnet-Camera
- Trendnet-Device
- Trendnet-Printer
- TrippLite-Device
- Ubuntu-Workstation
- Vista-Workstation

Assigned Policies:
- Ubuntu-Workstation-Corporate_Local

Easy Connect/PassiveID

Definition: PassiveID identifies Active Directory users logging into AD joined computers (it's the basis of the ISE-PIC offering but the same capability is in the main ISE suite). It's completely out of band feature and does not require any participation/configuration from any switch/wlc. It's basically between ISE and Active Directory. There are several probes that can get this data but I will just be using WMI. To enable PassiveID and learn more see this guide. Showing config steps here for completeness:

Administration--System--Deployment--Deployment--Node General Settings



Edit Node

Hostname	**ise1**
FQDN	**ise1.example.com**
IP Address	**192.168.150.50**
Node Type	**Identity Services Engine (ISE)**

Role **STANDALONE**

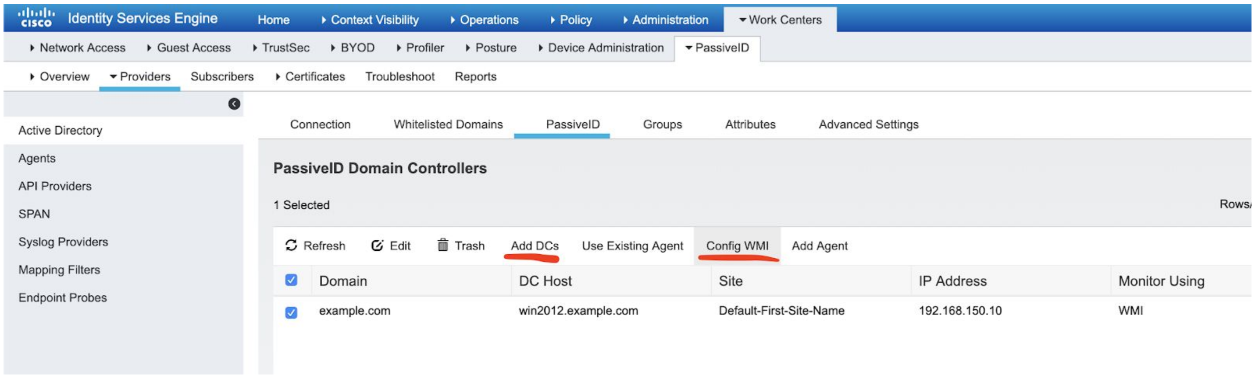
☑ Administration

☑ Monitoring
- Role: PRIMARY
- Other Monitoring Node:

☑ Policy Service
- ☑ Enable Session Services
  - Include Node in Node Group: None
- ☑ Enable Profiling Service
- ☐ Enable Threat Centric NAC Service
- ☐ Enable SXP Service
- ☐ Enable Device Admin Service
- ☑ Enable Passive Identity Service

☐ pxGrid

Begin monitoring the Domain Controller(s) for login data here: Work Centers--PassiveID--Providers--Active Directory--PassiveID



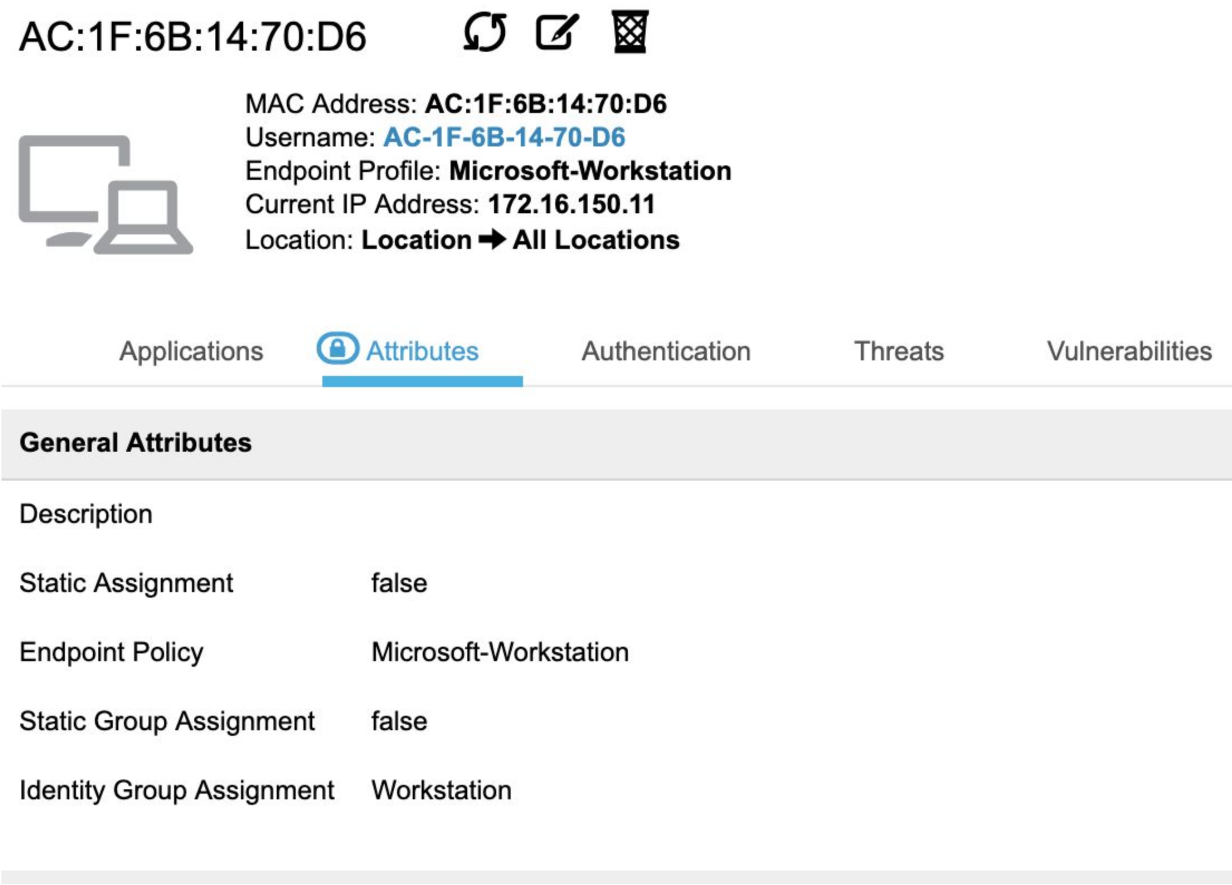
PassiveID Domain Controllers

1 Selected

☑	Domain	DC Host	Site	IP Address	Monitor Using
☑	example.com	win2012.example.com	Default-First-Site-Name	192.168.150.10	WMI

I manually ‘Add(ed) DC’ and then click Config WMI (it will log into the DC using previously provided AD admin credentials.

Then I loaded up a Win10 computer. Before it was added to the domain, this is how it was profiled.

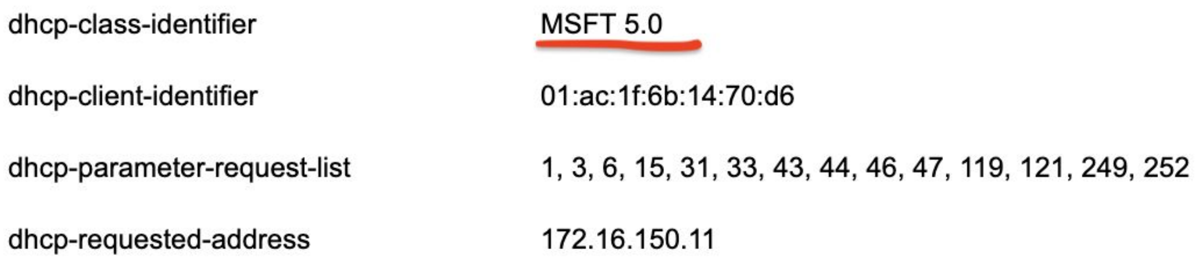


AC:1F:6B:14:70:D6

MAC Address: **AC:1F:6B:14:70:D6**
Username: **AC-1F-6B-14-70-D6**
Endpoint Profile: **Microsoft-Workstation**
Current IP Address: **172.16.150.11**
Location: **Location → All Locations**

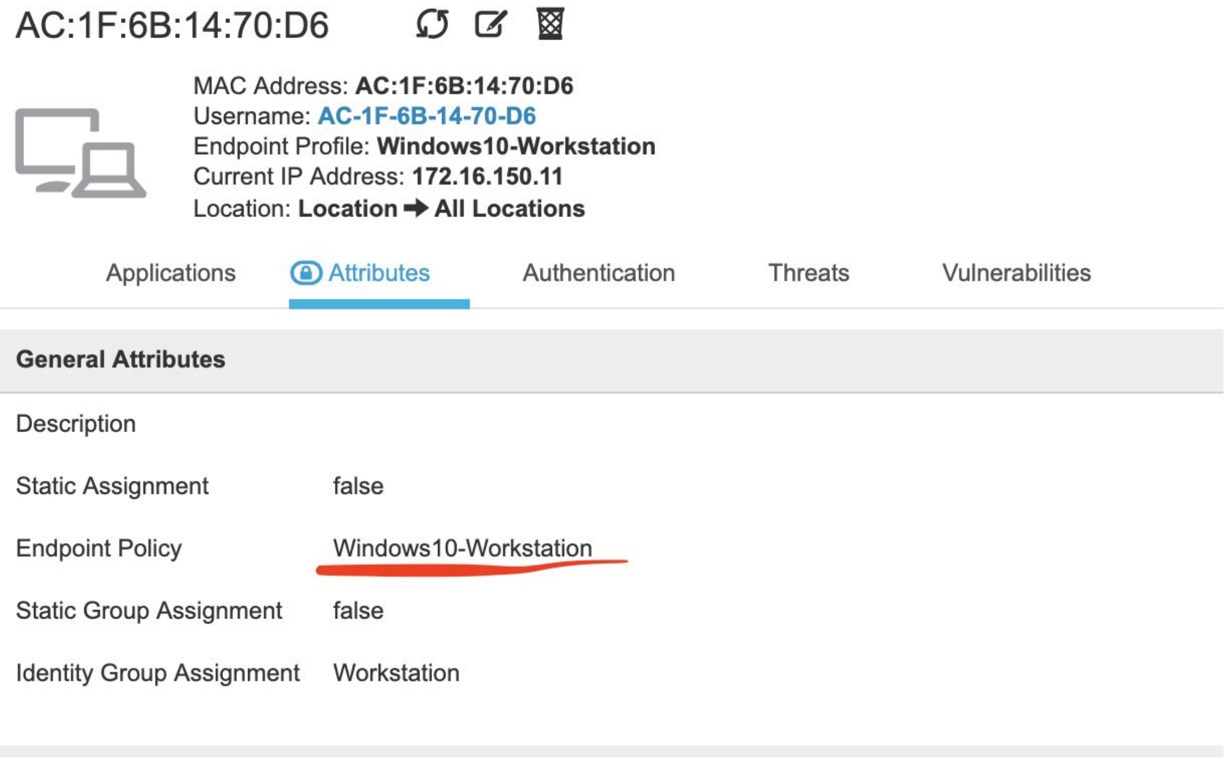
General Attributes

Description	
Static Assignment	false
Endpoint Policy	Microsoft-Workstation
Static Group Assignment	false
Identity Group Assignment	Workstation



dhcp-class-identifier	MSFT 5.0
dhcp-client-identifier	01:ac:1f:6b:14:70:d6
dhcp-parameter-request-list	1, 3, 6, 15, 31, 33, 43, 44, 46, 47, 119, 121, 249, 252
dhcp-requested-address	172.16.150.11

And after I joined it to the domain

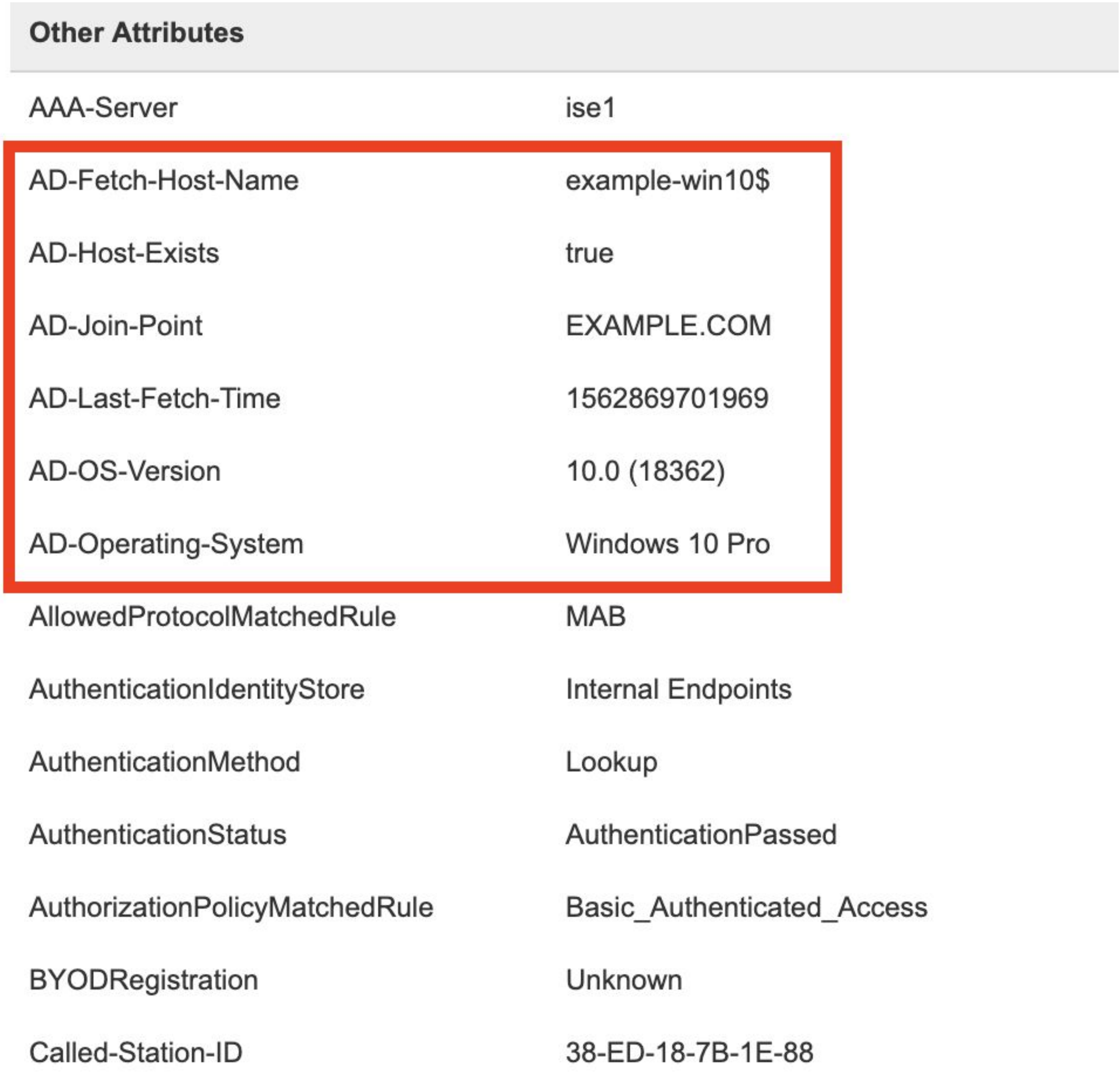


AC:1F:6B:14:70:D6

MAC Address: **AC:1F:6B:14:70:D6**
Username: **AC-1F-6B-14-70-D6**
Endpoint Profile: **Windows10-Workstation**
Current IP Address: **172.16.150.11**
Location: **Location → All Locations**

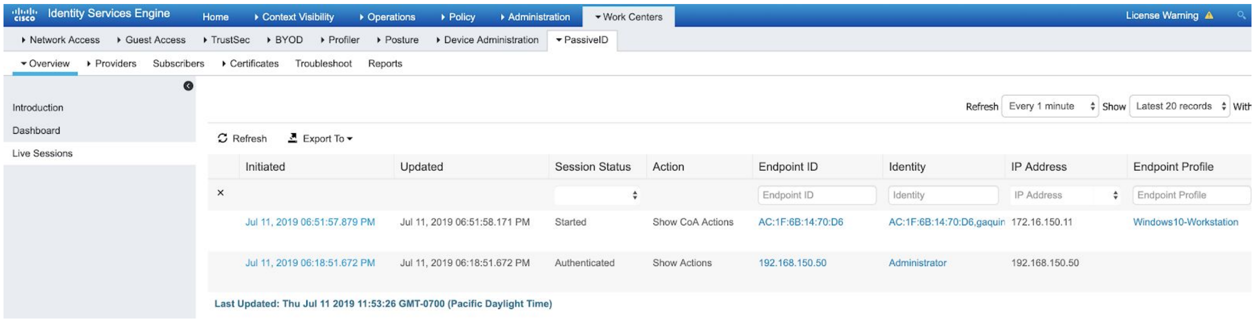
General Attributes

Description	
Static Assignment	false
Endpoint Policy	Windows10-Workstation
Static Group Assignment	false
Identity Group Assignment	Workstation



Other Attributes	
AAA-Server	ise1
AD-Fetch-Host-Name	example-win10$
AD-Host-Exists	true
AD-Join-Point	EXAMPLE.COM
AD-Last-Fetch-Time	1562869701969
AD-OS-Version	10.0 (18362)
AD-Operating-System	Windows 10 Pro
AllowedProtocolMatchedRule	MAB
AuthenticationIdentityStore	Internal Endpoints
AuthenticationMethod	Lookup
AuthenticationStatus	AuthenticationPassed
AuthorizationPolicyMatchedRule	Basic_Authenticated_Access
BYODRegistration	Unknown
Called-Station-ID	38-ED-18-7B-1E-88

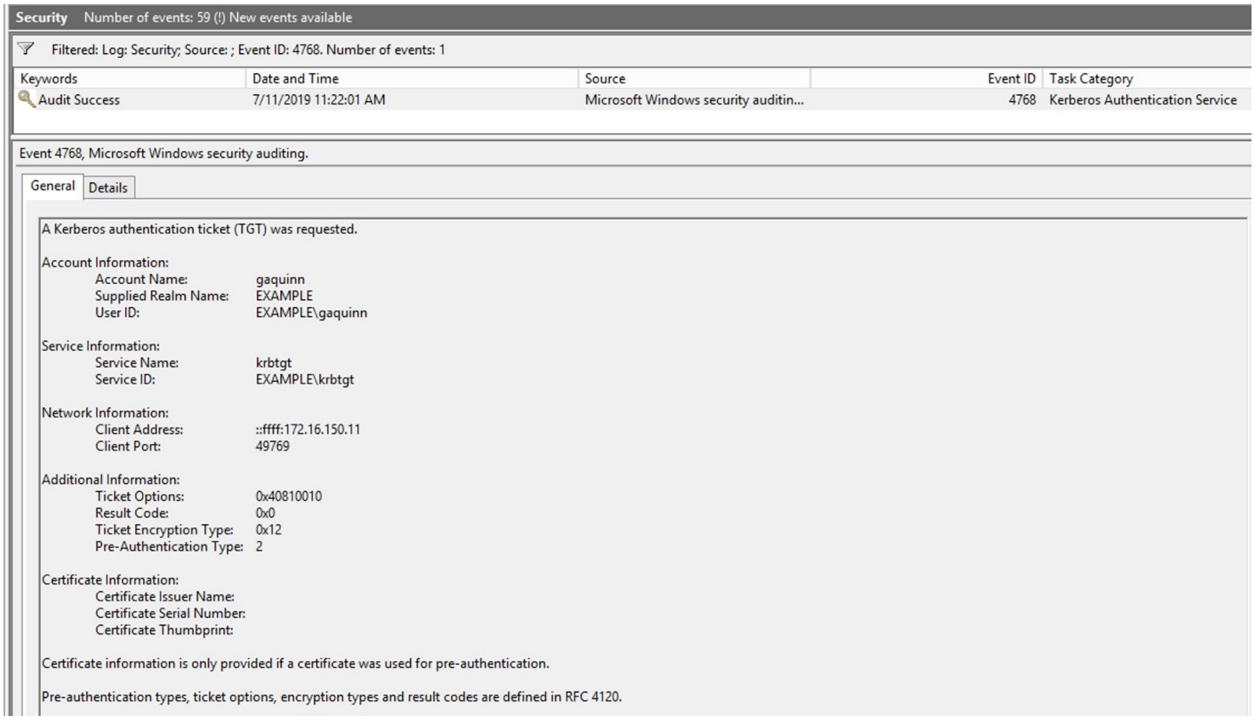
PassiveID shows the user at Work Centers--PassiveID--Overview--Live Sessions



Refresh Every 1 minute Show Latest 20 records With

Initiated	Updated	Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile
Jul 11, 2019 06:51:57.879 PM	Jul 11, 2019 06:51:58.171 PM	Started	Show CoA Actions	AC:1F:6B:14:70:D6	AC:1F:6B:14:70:D6,gaquin	172.16.150.11	Windows10-Workstation
Jul 11, 2019 06:18:51.672 PM	Jul 11, 2019 06:18:51.672 PM	Authenticated	Show Actions	192.168.150.50	Administrator	192.168.150.50	

Last Updated: Thu Jul 11 2019 11:53:26 GMT-0700 (Pacific Daylight Time)



Security Number of events: 59 (!) New events available

Filtered: Log: Security; Source: ; Event ID: 4768. Number of events: 1

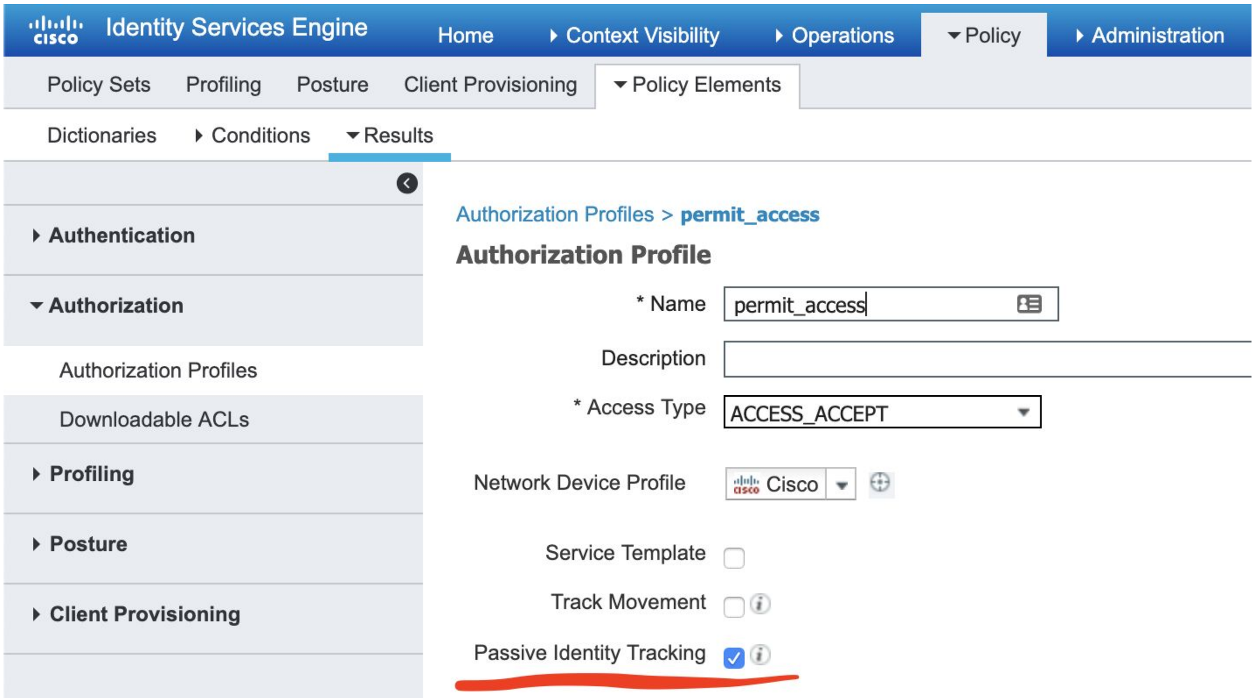
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	7/11/2019 11:22:01 AM	Microsoft Windows security auditin...	4768	Kerberos Authentication Service

Event 4768, Microsoft Windows security auditing.

```
A Kerberos authentication ticket (TGT) was requested.

Account Information:
	Account Name:		gaquinn
	Supplied Realm Name:	EXAMPLE
	User ID:		EXAMPLE\gaquinn

Service Information:
	Service Name:		krbtgt
	Service ID:		EXAMPLE\krbtgt

Network Information:
	Client Address:		::ffff:172.16.150.11
	Client Port:		49769

Additional Information:
	Ticket Options:		0x40810010
	Result Code:		0x0
	Ticket Encryption Type:	0x12
	Pre-Authentication Type:	2

Certificate Information:
	Certificate Issuer Name:
	Certificate Serial Number:
	Certificate Thumbprint:

Certificate information is only provided if a certificate was used for pre-authentication.

Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.
```

To get the passiveID record in as an attribute to the endpoint we need to modify the Authorization Profile to track PassiveID. That is done at Policy--Policy Elements--Results--Authorization--Authorization Profiles

I created a new profile specifically to track PassiveID



Authorization Profiles > **permit_access**

Authorization Profile

* Name: permit_access

Description:

* Access Type: ACCESS_ACCEPT

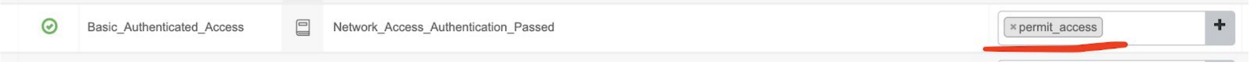
Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

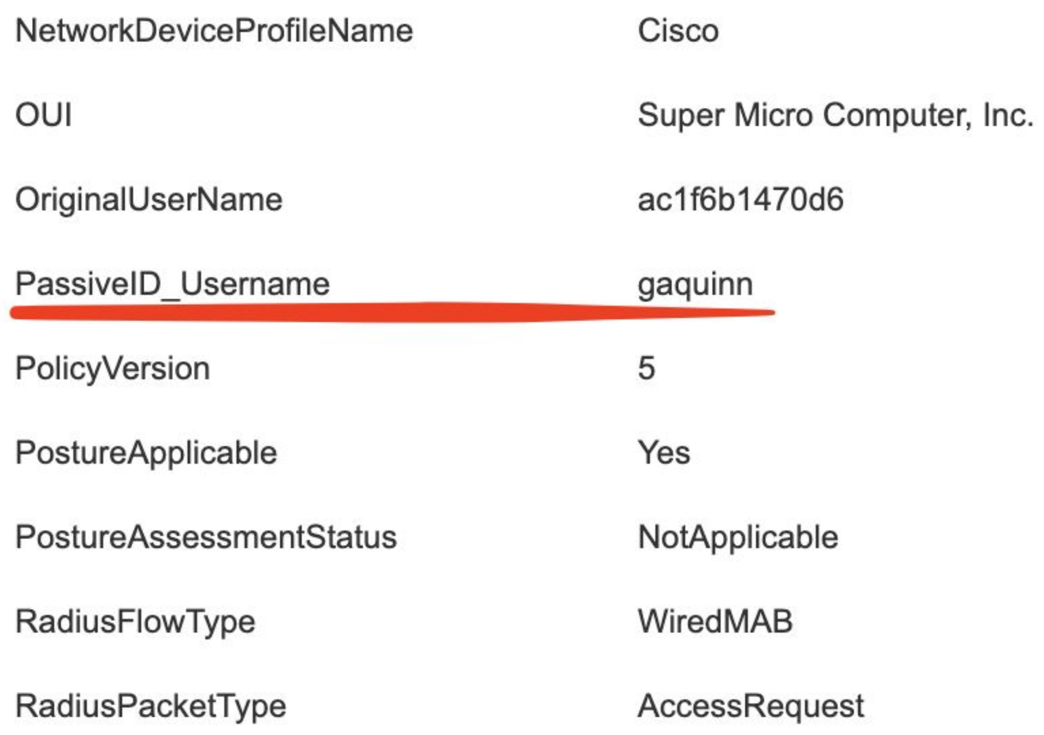
Passive Identity Tracking ☑

And apply that profile to the Policy step this host is hitting (Policy--Policy Sets--Default--Authorization Policy):



Basic_Authenticated_Access	Network_Access_Authentication_Passed	permit_access

Now the attributes tab of the endpoint shows that gaquinn is logged into this endpoint



NetworkDeviceProfileName	Cisco
OUI	Super Micro Computer, Inc.
OriginalUserName	ac1f6b1470d6
PassiveID_Username	gaquinn
PolicyVersion	5
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
RadiusFlowType	WiredMAB
RadiusPacketType	AccessRequest

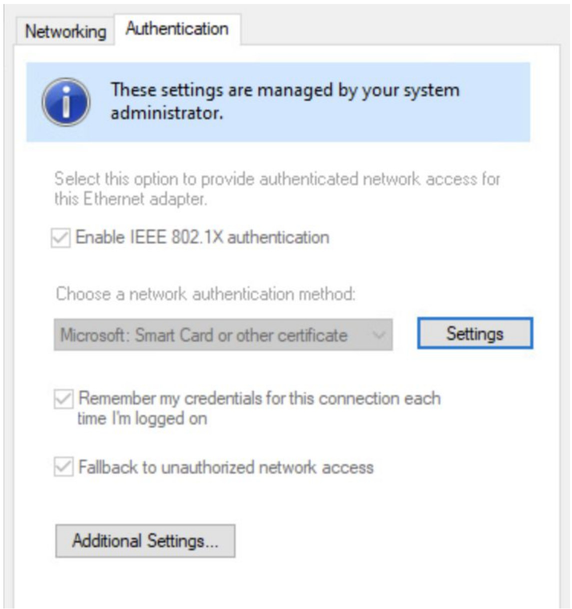
Summary

There has been no NAC at this point. We’re profiling endpoints and determining corporate asset Linux and windows 10 workstations (with user identity).

EasyConnect utilizes this PassiveID information to enforce real NAC policies (such as deny access or grant partial network access).

Another advanced use case for PassiveID is to use Machine certificates for 802.1X access but also capture real person identity on the machine. This can be powerful instead of granting user certificates.

And by the way, when I joined this windows 10 client, GPO autoconfigured its 802.1X NAC settings (not yet used since the switch isn’t configured for it) and pushed certificates to it (machine and user). Here is what it looks like on the client side (which will be used later):



These settings are managed by your system administrator.

Select this option to provide authenticated network access for this Ethernet adapter.

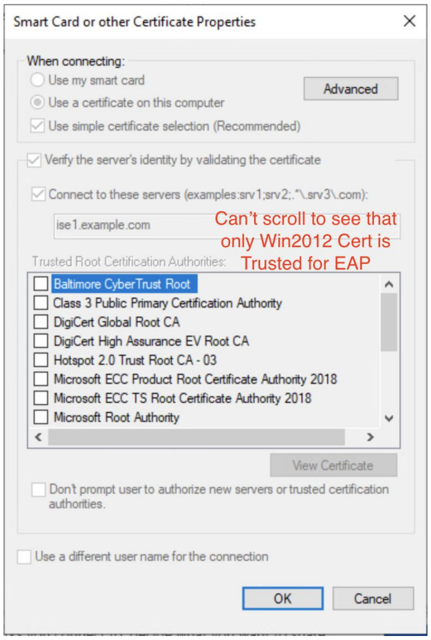
☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Smart Card or other certificate

☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access



When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Verify the server's identity by validating the certificate

☑ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

ise1.example.com

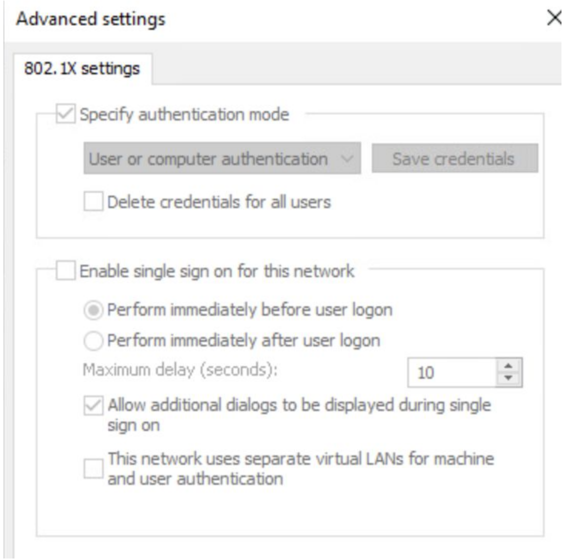
Can't scroll to see that only Win2012 Cert is Trusted for EAP

Trusted Root Certification Authorities:

☐ Baltimore CyberTrust Root
☐ Class 3 Public Primary Certification Authority
☐ DigiCert Global Root CA
☐ DigiCert High Assurance EV Root CA
☐ Hotspot 2.0 Trust Root CA - 03
☐ Microsoft ECC Product Root Certificate Authority 2018
☐ Microsoft ECC TS Root Certificate Authority 2018
☐ Microsoft Root Authority

☐ Don't prompt user to authorize new servers or trusted certification authorities.

☐ Use a different user name for the connection



☑ Specify authentication mode

User or computer authentication

☐ Delete credentials for all users

☐ Enable single sign on for this network

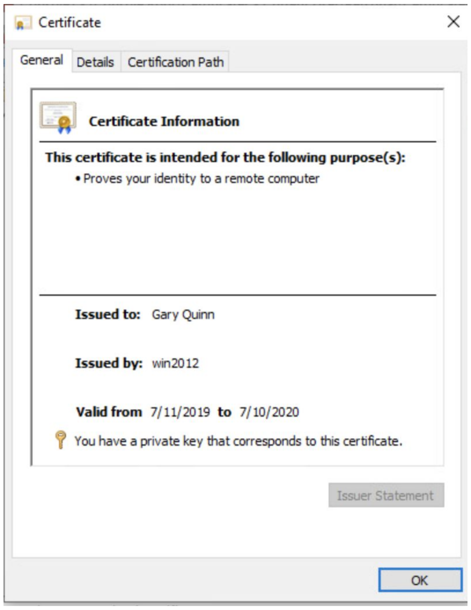
● Perform immediately before user logon

○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

☐ This network uses separate virtual LANs for machine and user authentication



Certificate Information

This certificate is intended for the following purpose(s):

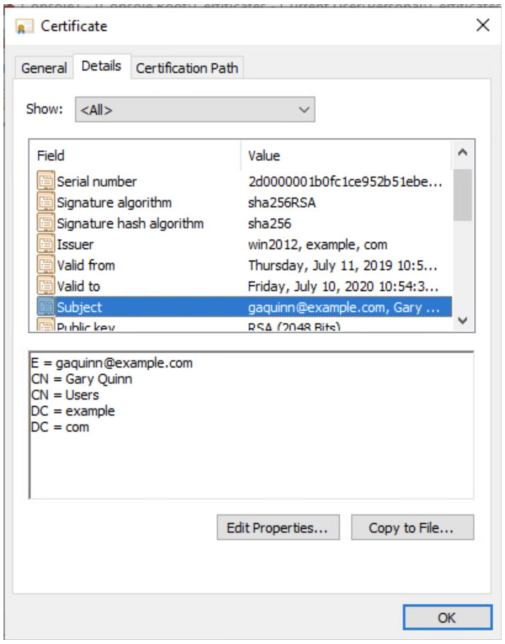
- Proves your identity to a remote computer

Issued to: Gary Quinn

Issued by: win2012

Valid from 7/11/2019 **to** 7/10/2020

You have a private key that corresponds to this certificate.



Show: <All>

Field	Value
Serial number	2d0000001b0fc1ce952b51ebe...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	win2012, example, com
Valid from	Thursday, July 11, 2019 10:5...
Valid to	Friday, July 10, 2020 10:54:3...
Subject	gaquinn@example.com, Gary ...
Public key	RSA (2048 Bits)

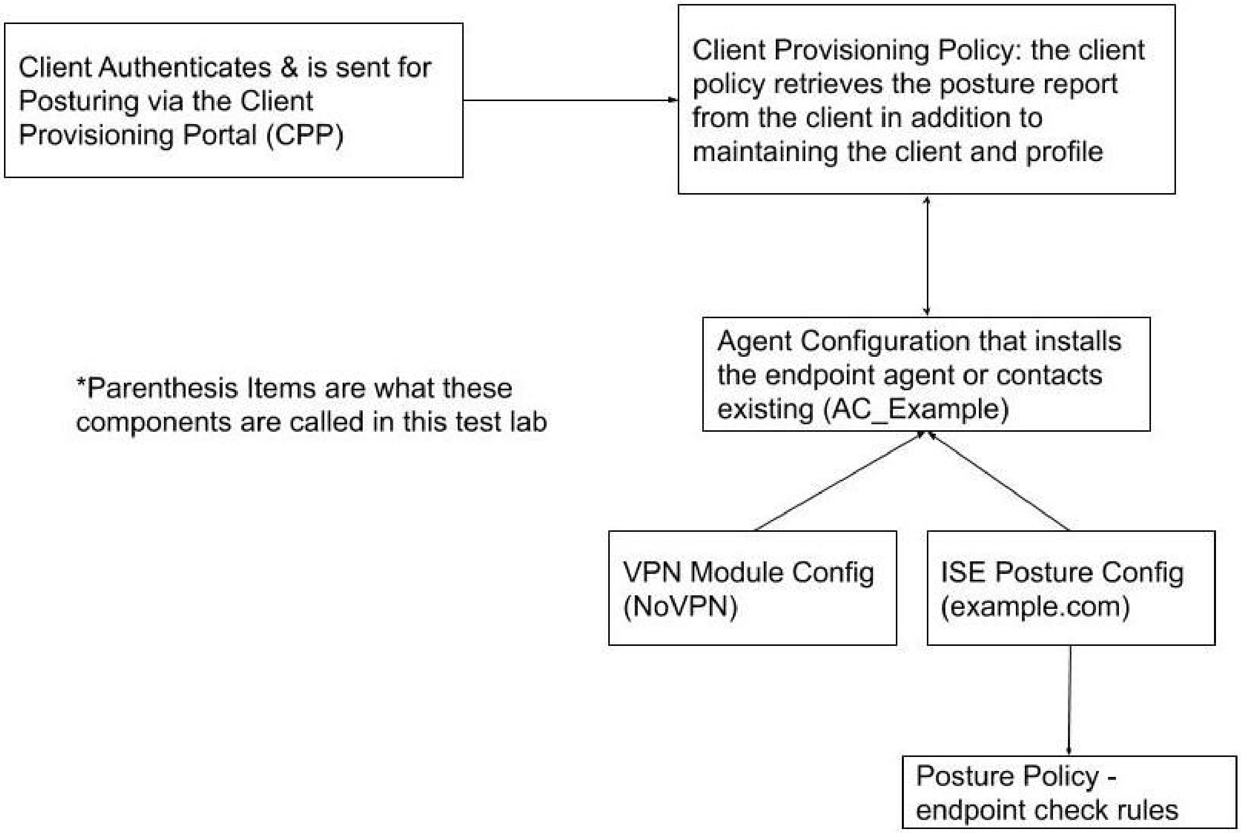
E = gaquinn@example.com
CN = Gary Quinn
CN = Users
DC = example
DC = com

Client Provisioning

Objective: Now we're getting into actual policy creation and enforcement. It'll be more Policy and Portals at this point. This Client Provisioning Portal is dual purposed: to provision Anyconnect for clients that don't have it and to receive the posture report from the client (in the same motion if the client is being installed for the first time).

For reference, here is how the pieces of client provisioning fit in ISE:

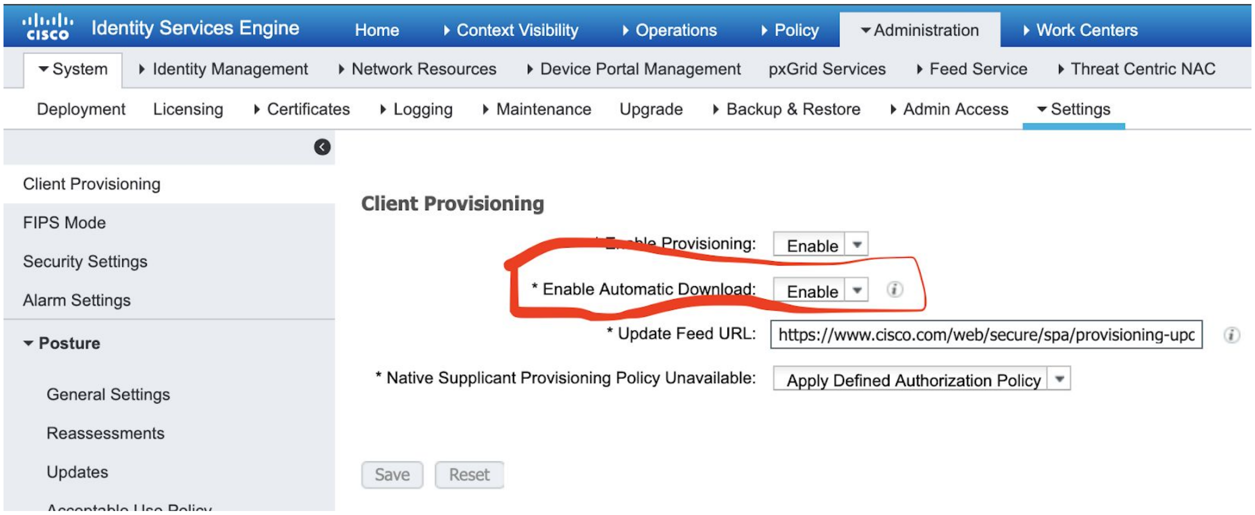
ISE Client Provision and Posture Checking


Client Authenticates & is sent for Posturing via the Client Provisioning Portal (CPP)
Client Provisioning Policy: the client policy retrieves the posture report from the client in addition to maintaining the client and profile
Agent Configuration that installs the endpoint agent or contacts existing (AC_Example)
*Parenthesis Items are what these components are called in this test lab
VPN Module Config (NoVPN)
ISE Posture Config (example.com)
Posture Policy - endpoint check rules

Bootstrapping ISE

Enable automatic client downloading (they can be downloaded one by one but this can shortcut it). Note we will have to manually upload the anyconnect client in a subsequent step.

This is at Administration--System--Settings--Client Provisioning



Client Provisioning

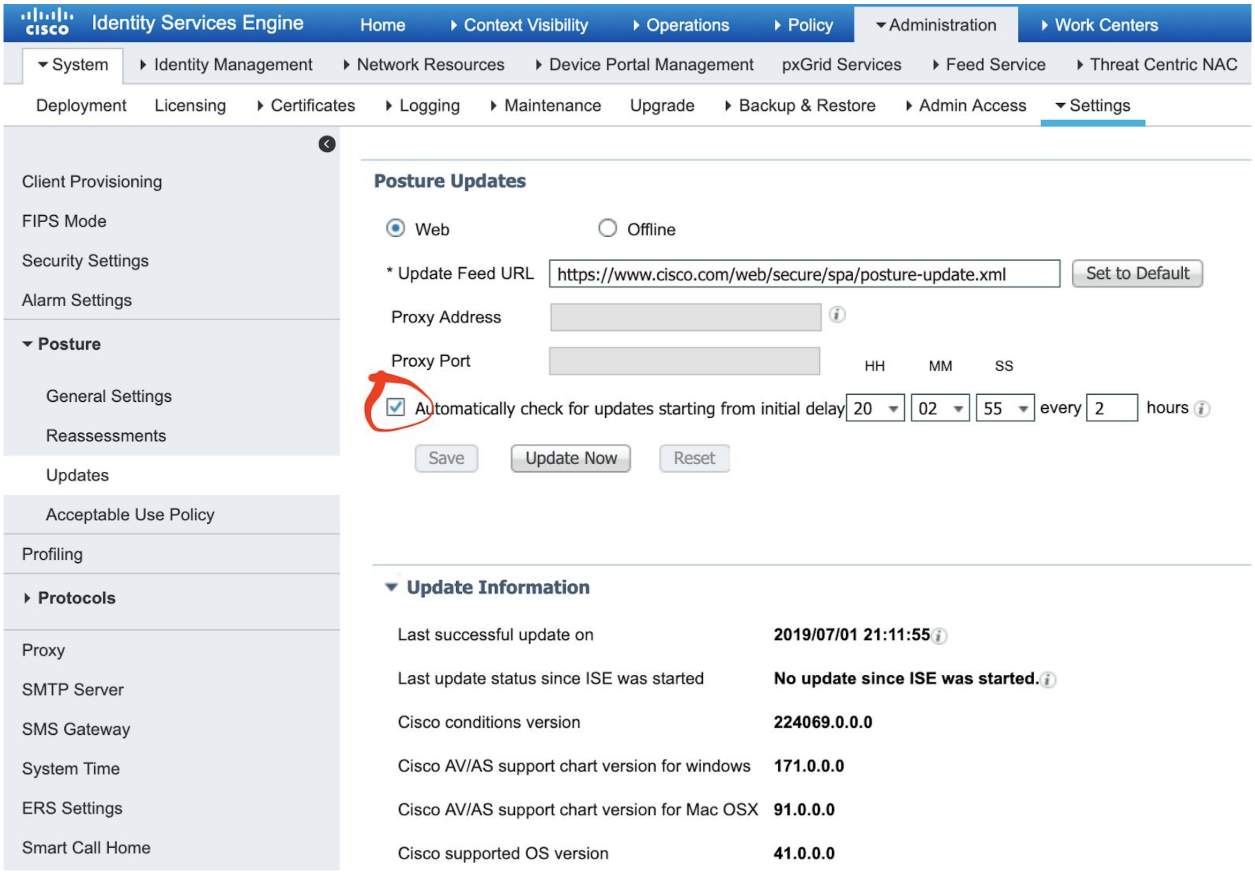
* Enable Provisioning: Enable

* Enable Automatic Download: Enable

* Update Feed URL: https://www.cisco.com/web/secure/spa/provisioning-upc

* Native Supplicant Provisioning Policy Unavailable: Apply Defined Authorization Policy

While you're in this same section make an update to Posture--Updates. Set it to automatically check for updates and click the 'update now' button.



Posture Updates

● Web ○ Offline

* Update Feed URL: https://www.cisco.com/web/secure/spa/posture-update.xml

Proxy Address:

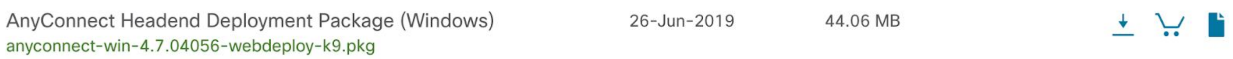
Proxy Port:

☑ Automatically check for updates starting from initial delay 20 (HH) 02 (MM) 55 (SS) every 2 hours

Update Information

Last successful update on	**2019/07/01 21:11:55**
Last update status since ISE was started	**No update since ISE was started.**
Cisco conditions version	**224069.0.0.0**
Cisco AV/AS support chart version for windows	**171.0.0.0**
Cisco AV/AS support chart version for Mac OSX	**91.0.0.0**
Cisco supported OS version	**41.0.0.0**

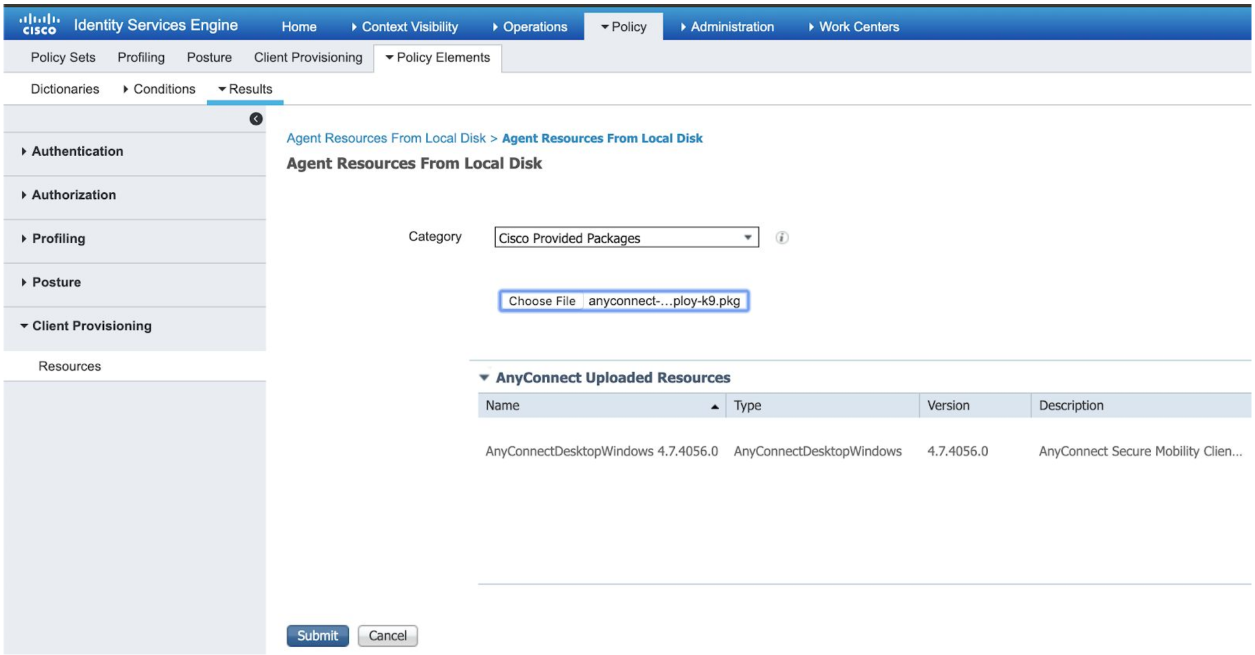
Download Anyconnect clients from Cisco's website.
I downloaded this windows client (same logic applies for mac os)



AnyConnect Headend Deployment Package (Windows) 26-Jun-2019 44.06 MB
anyconnect-win-4.7.04056-webdeploy-k9.pkg

Now let's move over to Policy--Policy Elements--Results--Client Provisioning--Resources

Choose "Add from Local Disk" and specify that it's a Cisco provided package.



Agent Resources From Local Disk > **Agent Resources From Local Disk**

Agent Resources From Local Disk

Category: Cisco Provided Packages

Choose File anyconnect-...ploy-k9.pkg

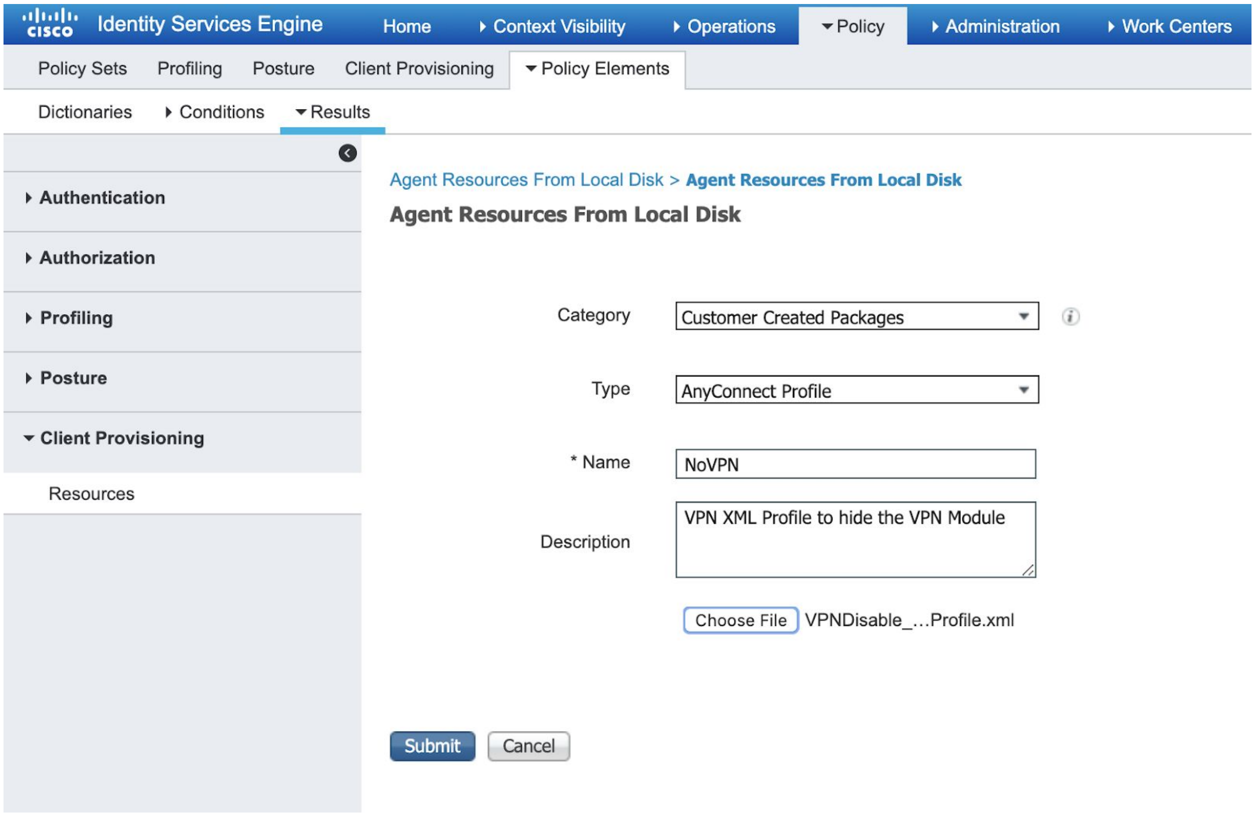
AnyConnect Uploaded Resources

Name	Type	Version	Description
AnyConnectDesktopWindows 4.7.4056.0	AnyConnectDesktopWindows	4.7.4056.0	AnyConnect Secure Mobility Clien...

Also grab the VPN_Service_Disable profile from here and upload it the same way (except it's a "Customer Created Package"). It's pasted here for completeness (save it to your file system with .xml extension)

```
<?xml version="1.0" encoding="utf-8"?>
<!--
    Cisco AnyConnect VPN Profile -

    This profile is a sample intended to allow for the disabling of VPN service
    for those installations that do not require VPN support.
-->
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd">
  <ClientInitialization>
```

```
    <ServiceDisable>true</ServiceDisable>
  </ClientInitialization>
</AnyConnectProfile>
```



Category: Customer Created Packages

Type: AnyConnect Profile

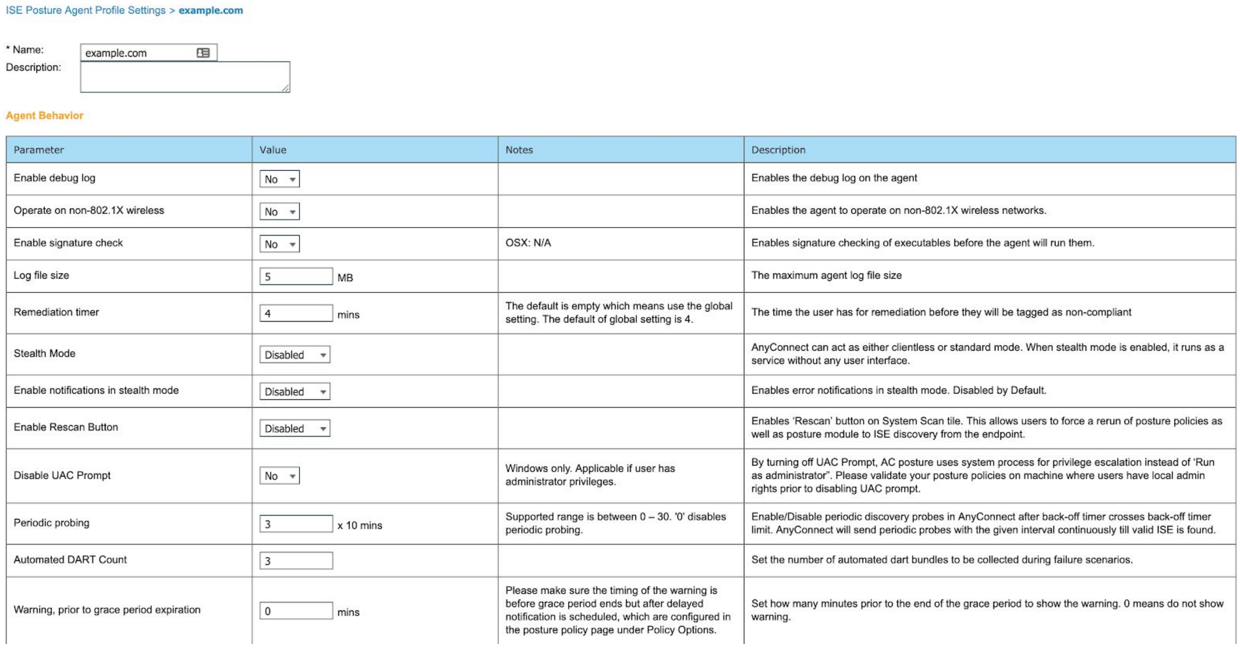
* Name: NoVPN

Description: VPN XML Profile to hide the VPN Module

VPNDisable_...Profile.xml

ISE Posture Configuration Profile

This is the configuration that tells the client how to connect to ISE and whether to show itself to users (aka Stealth Mode). We'll build a simple one from scratch here but is generally ok for production use. Go to Policy--Policy Elements--Results--Client Provisioning and Click 'Add' and then 'Anyconnect Posture Profile'. Mine looks like this (note you can toggle stealthmode and stealthmode notifications in this page). For more info and caveats on stealthmode check this guide. Basically stealthmode is exactly what it sounds like: Anyconnect will run as a service and no information will be shown to the enduser.



ISE Posture Agent Profile Settings > **example.com**

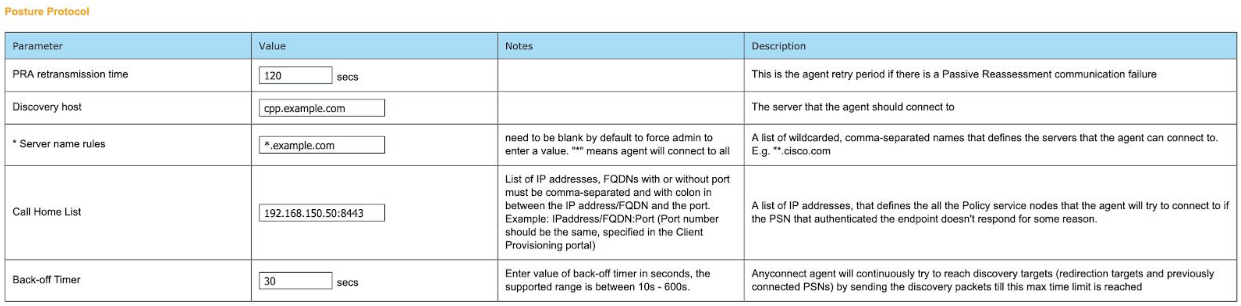
* Name: example.com
Description:

Agent Behavior

Parameter	Value	Notes	Description
Enable debug log	No		Enables the debug log on the agent
Operate on non-802.1X wireless	No		Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	OSX: N/A	Enables signature checking of executables before the agent will run them.
Log file size	5 MB		The maximum agent log file size
Remediation timer	4 mins	The default is empty which means use the global setting. The default of global setting is 4.	The time the user has for remediation before they will be tagged as non-compliant
Stealth Mode	Disabled		AnyConnect can act as either clientless or standard mode. When stealth mode is enabled, it runs as a service without any user interface.
Enable notifications in stealth mode	Disabled		Enables error notifications in stealth mode. Disabled by Default.
Enable Rescan Button	Disabled		Enables 'Rescan' button on System Scan tile. This allows users to force a rerun of posture policies as well as posture module to ISE discovery from the endpoint.
Disable UAC Prompt	No	Windows only. Applicable if user has administrator privileges.	By turning off UAC Prompt, AC posture uses system process for privilege escalation instead of 'Run as administrator". Please validate your posture policies on machine where users have local admin rights prior to disabling UAC prompt.
Periodic probing	3 x 10 mins	Supported range is between 0 – 30. '0' disables periodic probing.	Enable/Disable periodic discovery probes in AnyConnect after back-off timer crosses back-off timer limit. AnyConnect will send periodic probes with the given interval continuously till valid ISE is found.
Automated DART Count	3		Set the number of automated dart bundles to be collected during failure scenarios.
Warning, prior to grace period expiration	0 mins	Please make sure the timing of the warning is before grace period ends but after delayed notification is scheduled, which are configured in the posture policy page under Policy Options.	Set how many minutes prior to the end of the grace period to show the warning. 0 means do not show warning.

The only defaults I changed are in the Posture Protocol Section shown below. Note that this is to give the client automatic information on how to find a Posture server without a formal URL redirection happening at login. See this tech note on this new capability in 2.2.

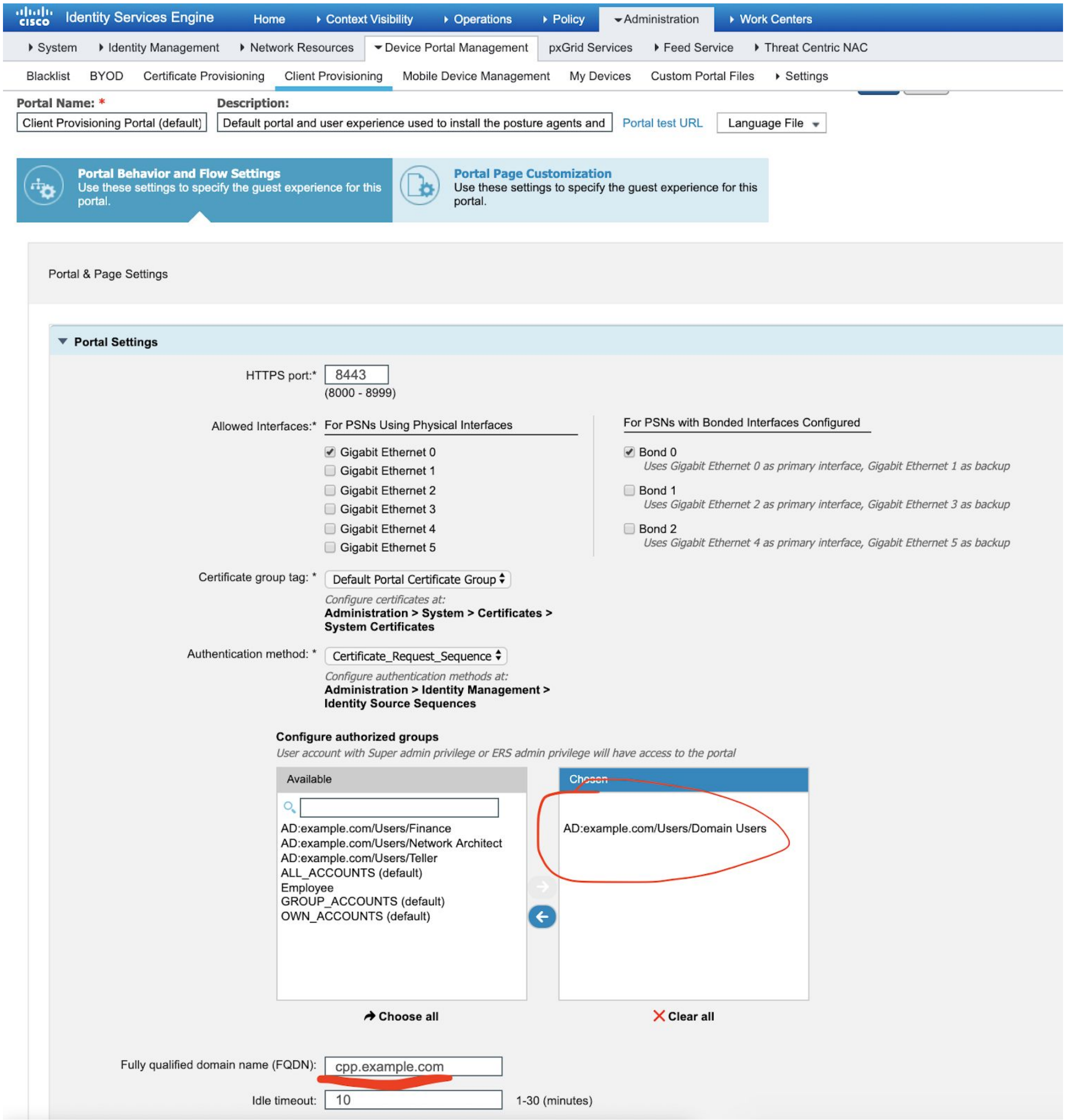
Previously it was advised to create a cpp.example.com DNS A Record. CPP is an acronym for 'client provisioning portal'. This piece informs the client to connect to this portal without a URL redirection.



Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Discovery host	cpp.example.com		The server that the agent should connect to
* Server name rules	*.example.com	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com
Call Home List	192.168.150.50:8443	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

We must also tell the CPP portal that its name is 'cpp.example.com'. That's set at Administration--Device Portal Management--Client Provisioning. Click the default portal labeled 'Client Provisioning Portal (default)'. And put in that quick change (and also add in *who* can use this portal). Customization of the Portal is also set here but we'll leave it as defaults.



Portal Name: * Client Provisioning Portal (default)

Description: Default portal and user experience used to install the posture agents and

Portal Settings

HTTPS port:* 8443
(8000 - 8999)

Allowed Interfaces:*

For PSNs Using Physical Interfaces
- ☑ Gigabit Ethernet 0
- ☐ Gigabit Ethernet 1
- ☐ Gigabit Ethernet 2
- ☐ Gigabit Ethernet 3
- ☐ Gigabit Ethernet 4
- ☐ Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured
- ☑ Bond 0
  Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
- ☐ Bond 1
  Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
- ☐ Bond 2
  Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: * Default Portal Certificate Group
Configure certificates at:
Administration > System > Certificates > System Certificates

Authentication method: * Certificate_Request_Sequence
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences

Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal

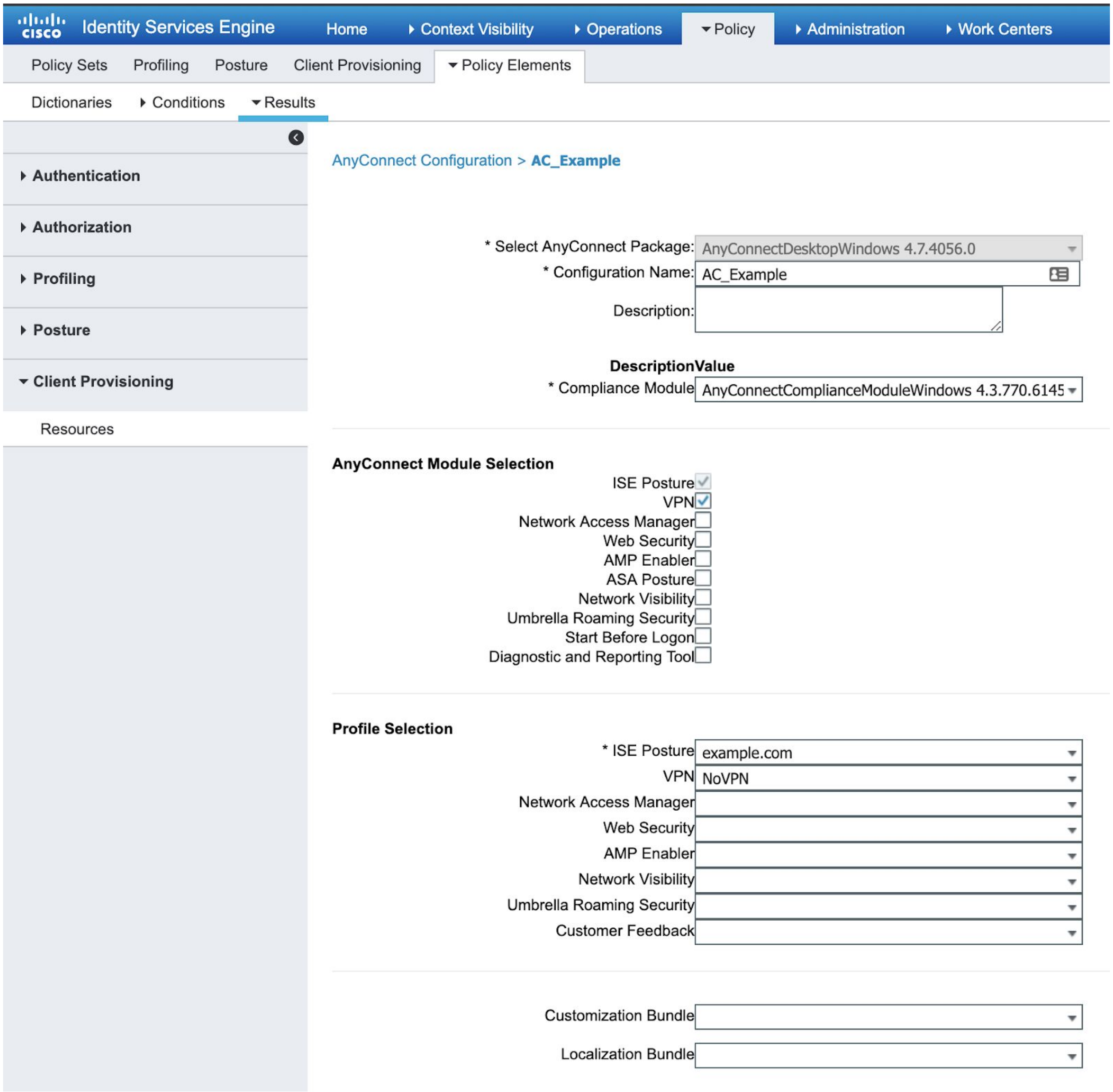
Available
AD:example.com/Users/Finance
AD:example.com/Users/Network Architect
AD:example.com/Users/Teller
ALL_ACCOUNTS (default)
Employee
GROUP_ACCOUNTS (default)
OWN_ACCOUNTS (default)

Chosen
AD:example.com/Users/Domain Users

Fully qualified domain name (FQDN): cpp.example.com

Idle timeout: 10 1-30 (minutes)

Now we need to create an Anyconnect Configuration that ties together the NoVPN profile and the Posture Config. Head back to Policy--Policy Elements--Results--Client Provisioning--Reources. Click ‘Add’ and Anyconnect Config. Mine is named AC_Example and is shown below (note for values not shown, they were the defaults)



AnyConnect Configuration > **AC_Example**

* Select AnyConnect Package: AnyConnectDesktopWindows 4.7.4056.0
* Configuration Name: AC_Example
Description:

DescriptionValue
* Compliance Module AnyConnectComplianceModuleWindows 4.3.770.6145

AnyConnect Module Selection

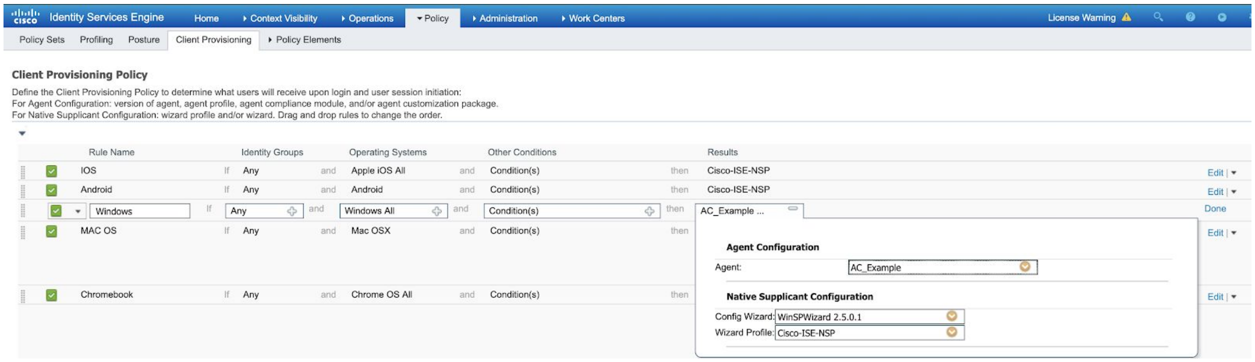
ISE Posture ☑
VPN ☑
Network Access Manager ☐
Web Security ☐
AMP Enabler ☐
ASA Posture ☐
Network Visibility ☐
Umbrella Roaming Security ☐
Start Before Logon ☐
Diagnostic and Reporting Tool ☐

Profile Selection

* ISE Posture example.com
VPN NoVPN
Network Access Manager
Web Security
AMP Enabler
Network Visibility
Umbrella Roaming Security
Customer Feedback

Customization Bundle
Localization Bundle

Now we have to tell ISE to deliver this Anyconnect Config when a user is sent to the Client Provisioning Policy. That is Policy--Client Provisioning--Client Provisioning Policy. It defaults Windows and MAC OS to use the temporal scanning policy. We'll set the Windows one to use the new AC config for a full agent



Client Provisioning Policy

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

	Rule Name		Identity Groups		Operating Systems		Other Conditions		Results
☑	IOS	If	Any	and	Apple iOS All	and	Condition(s)	then	Cisco-ISE-NSP
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP
☑	Windows	If	Any	and	Windows All	and	Condition(s)	then	AC_Example ...
☑	MAC OS	If	Any	and	Mac OSX	and	Condition(s)	then	
☑	Chromebook	If	Any	and	Chrome OS All	and	Condition(s)	then	

Agent Configuration

Agent: AC_Example

Native Supplicant Configuration

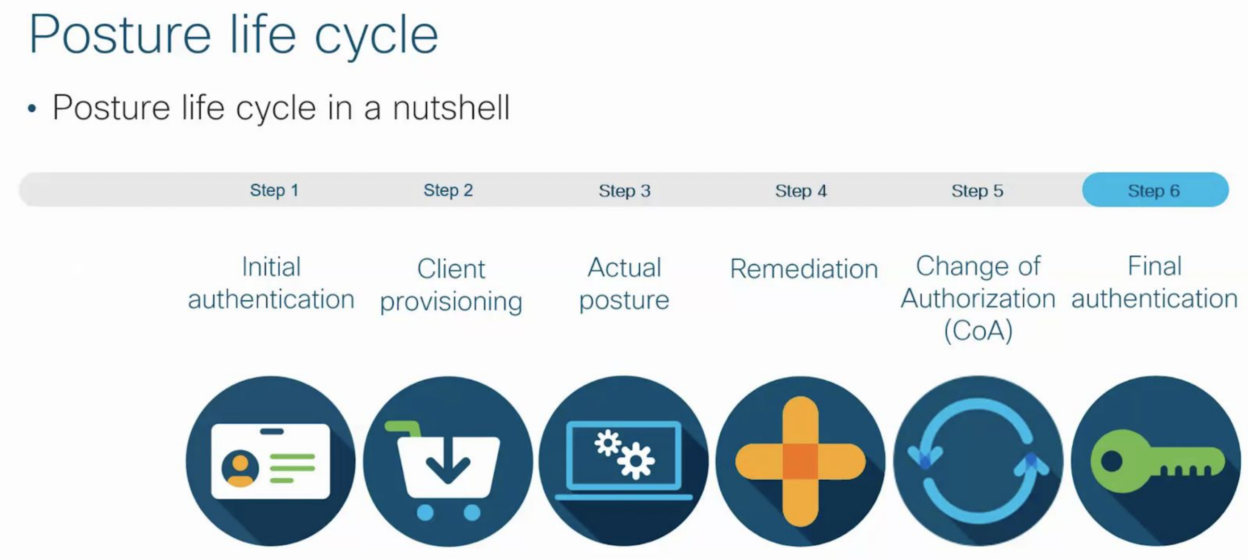
Config Wizard: WinSPWizard 2.5.0.1
Wizard Profile: Cisco-ISE-NSP

Note we’re not done yet. In the General Policy setting we’ll reference how to send clients to CPP to get their agent and its configuration.

Posture

The Posture Policy is the set of policy rules and remediations that the client’s endpoint must satisfy to be considered compliant. A full list of items that can be checked is here.

At a high level Posture authentications are handled by these 6 steps:

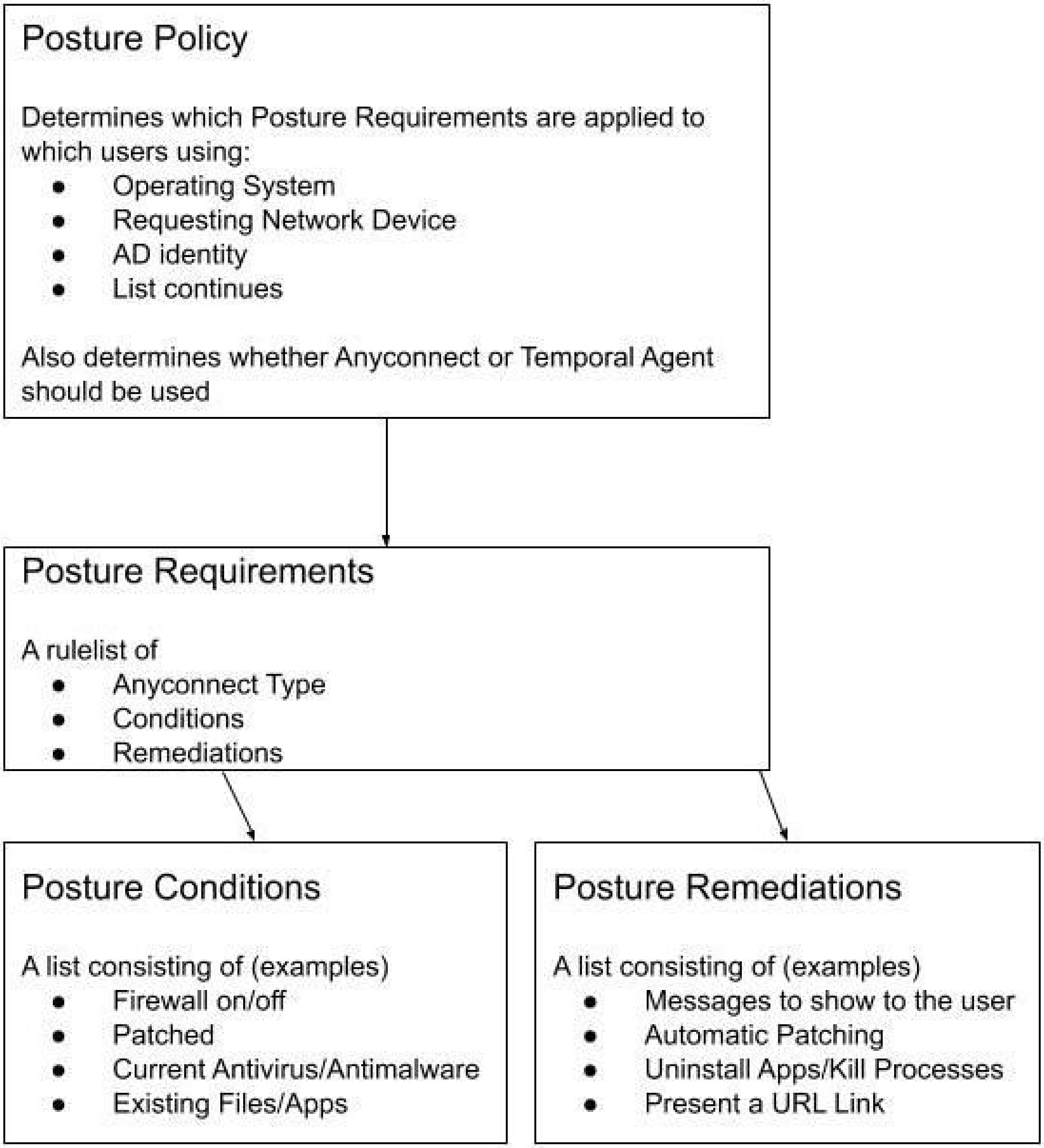


Posture life cycle

- Posture life cycle in a nutshell

Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
Initial authentication	Client provisioning	Actual posture	Remediation	Change of Authorization (CoA)	Final authentication

I made a handy picture for how Posture Policy components are used:



Posture Policy

Determines which Posture Requirements are applied to which users using:

- Operating System
- Requesting Network Device
- AD identity
- List continues

Also determines whether Anyconnect or Temporal Agent should be used

Posture Requirements

A rulelist of

- Anyconnect Type
- Conditions
- Remediations

Posture Conditions

A list consisting of (examples)

- Firewall on/off
- Patched
- Current Antivirus/Antimalware
- Existing Files/Apps

Posture Remediations

A list consisting of (examples)

- Messages to show to the user
- Automatic Patching
- Uninstall Apps/Kill Processes
- Present a URL Link

For the purposes of this document we will simply check for these five:

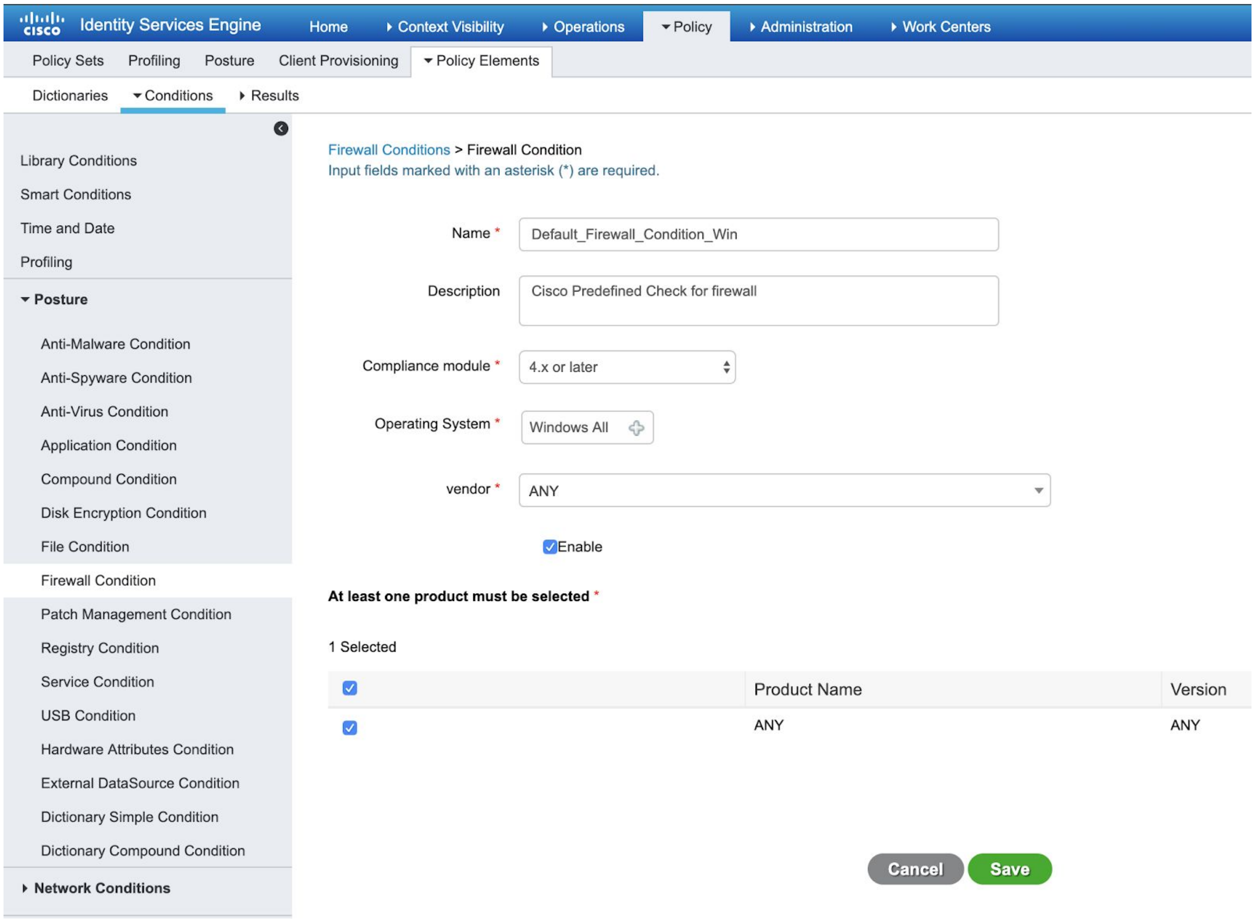
Requirement	Remediation	Note
Endpoint Firewall Running	Message to the user	Anyconnect can automatically enable the FW.
Missing file in the file system	Message noting that this not a corporate image	Registry files, processes can also be used

Running AntiMalware	Message to the user	Any AntiMalware will satisfy this
Hardware Inventory	N/A	Retrieves the hardware profile
Installed/Running Program Inventory	N/A	Retrieves the software profile

First step is to build the requirements (note, looking at the above flow image, we're going from the bottom up instead of top down). All but the file check condition from the table are built-in but I will show them all here for completeness.

Conditions

Navigate to Policy--Policy Elements--Conditions--Posture. Take note of the built-in Firewall (note the built-in Firewall check looks for any running firewall but a user defined condition can look for specific firewall(s) that the organization may use.



Firewall Conditions > Firewall Condition

Input fields marked with an asterisk (*) are required.

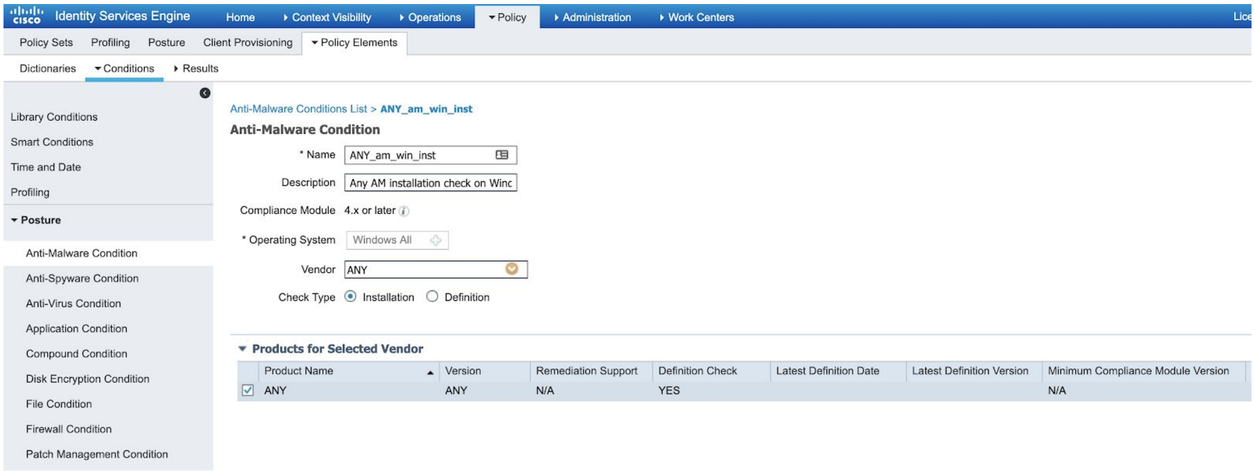
Name *	Default_Firewall_Condition_Win
Description	Cisco Predefined Check for firewall
Compliance module *	4.x or later
Operating System *	Windows All
vendor *	ANY

☑ Enable

At least one product must be selected *

1 Selected

☑	Product Name	Version
☑	ANY	ANY



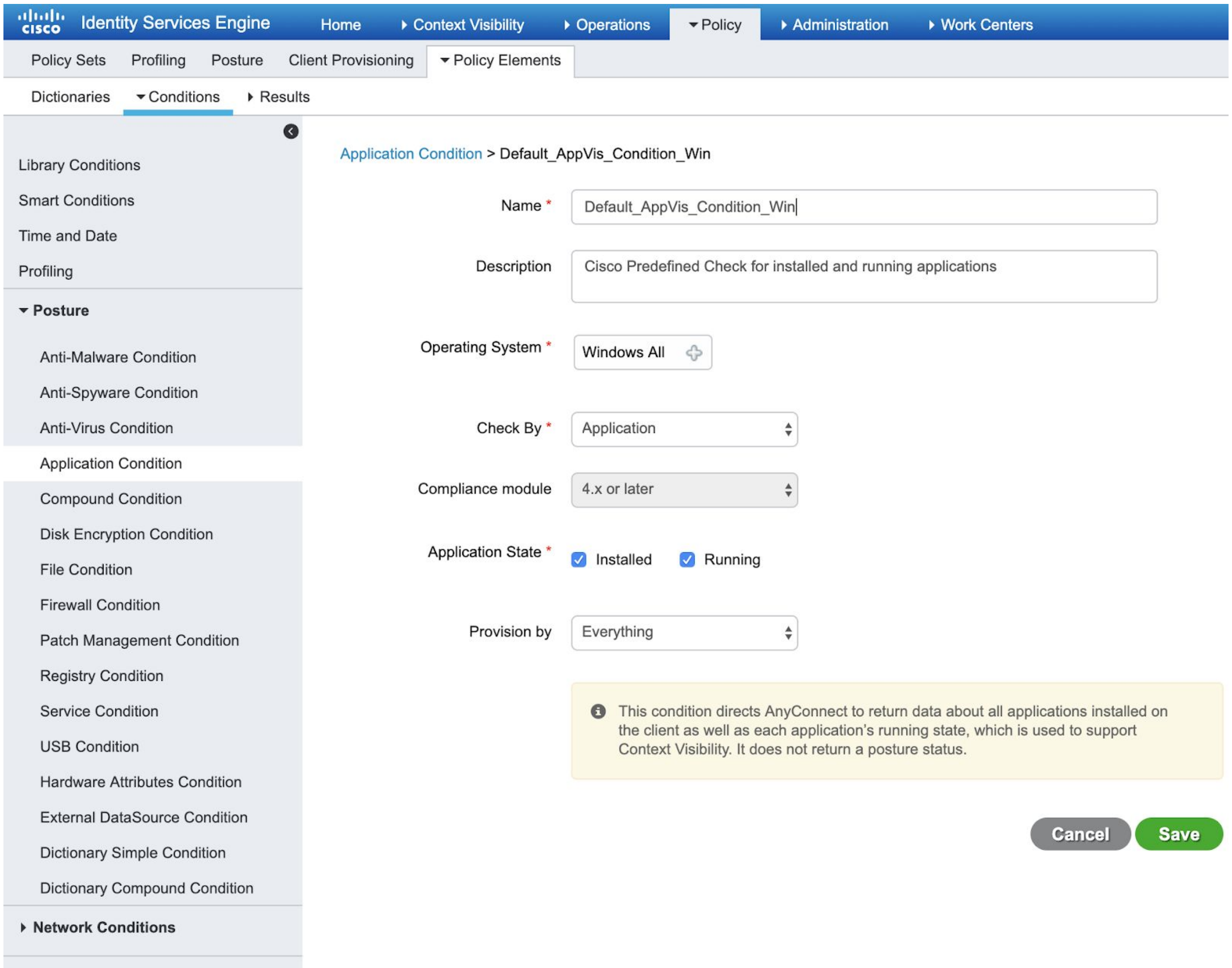
Anti-Malware Conditions List > **ANY_am_win_inst**

Anti-Malware Condition

* Name	ANY_am_win_inst
Description	Any AM installation check on Winc
Compliance Module	4.x or later
* Operating System	Windows All
Vendor	ANY
Check Type	● Installation ○ Definition

Products for Selected Vendor

	Product Name	Version	Remediation Support	Definition Check	Latest Definition Date	Latest Definition Version	Minimum Compliance Module Version
☑	ANY	ANY	N/A	YES			N/A



Application Condition > Default_AppVis_Condition_Win

Name * Default_AppVis_Condition_Win

Description Cisco Predefined Check for installed and running applications

Operating System * Windows All

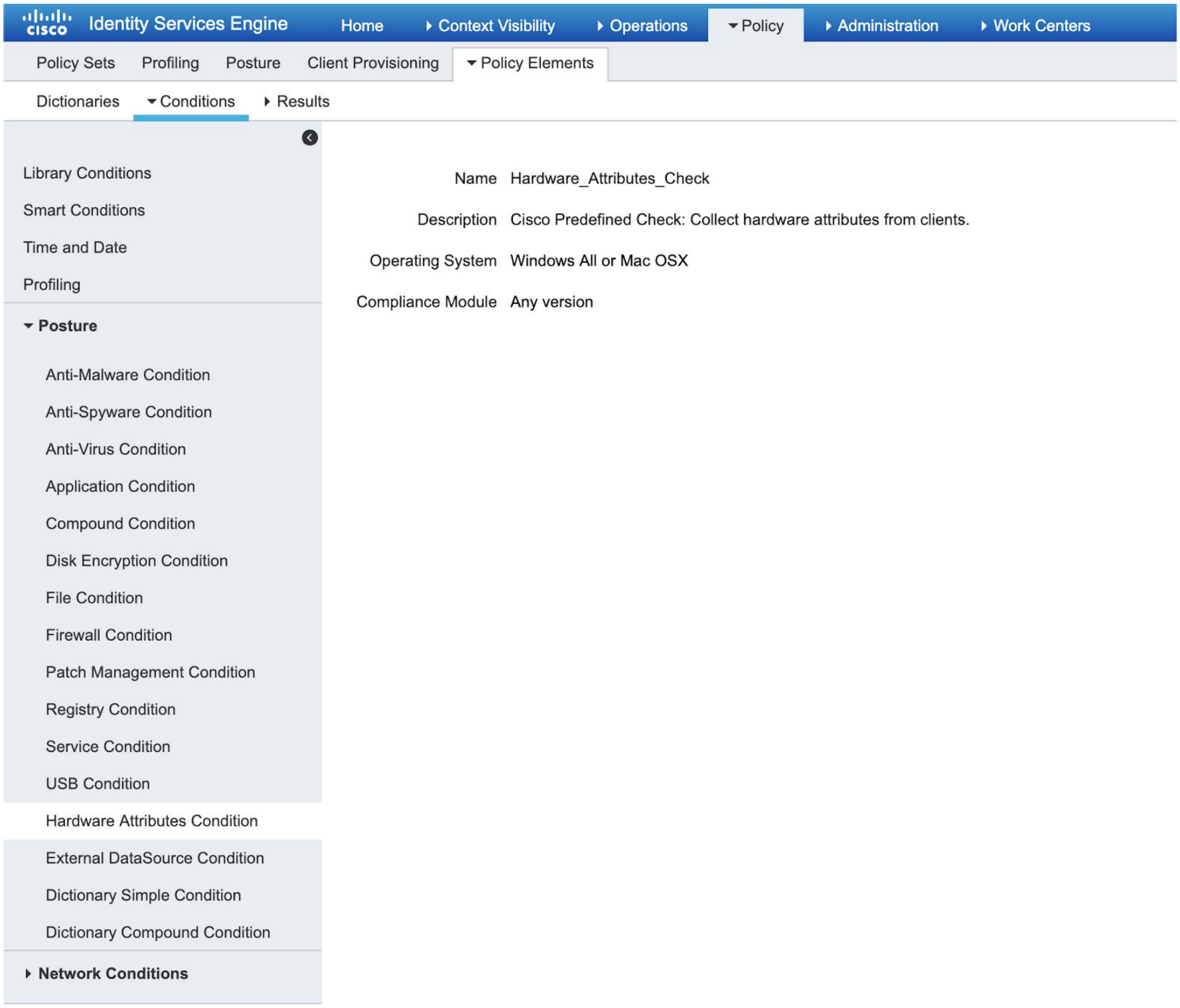
Check By * Application

Compliance module 4.x or later

Application State * ☑ Installed ☑ Running

Provision by Everything

This condition directs AnyConnect to return data about all applications installed on the client as well as each application's running state, which is used to support Context Visibility. It does not return a posture status.



Name Hardware_Attributes_Check

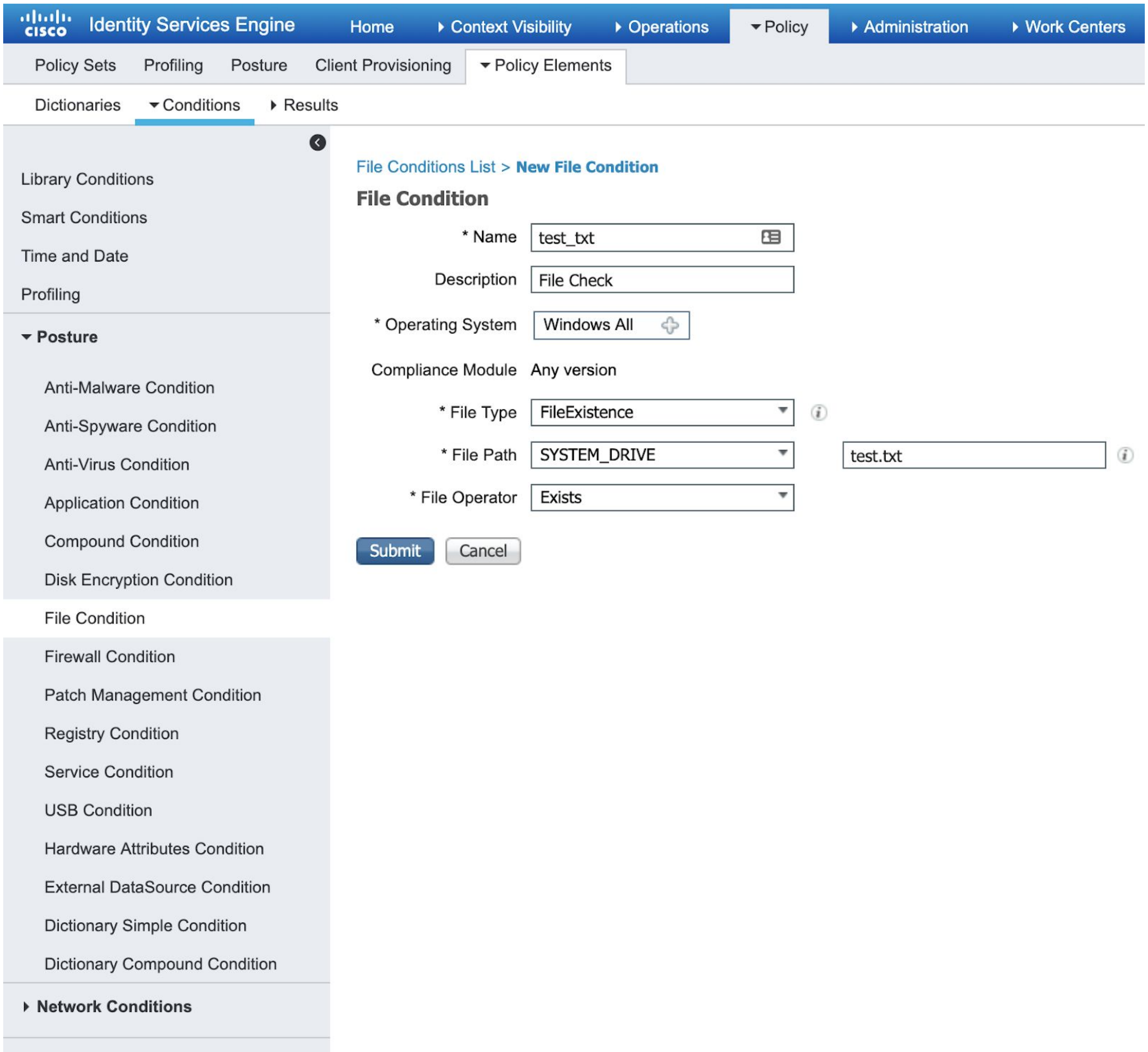
Description Cisco Predefined Check: Collect hardware attributes from clients.

Operating System Windows All or Mac OSX

Compliance Module Any version

Let’s add the three new ones starting with a File Condition that looks for a specific file on the file system (useful for fingerprinting Gold Image loads or potentially for out of date images). Looking for registry keys or Services.

Navigate to File Conditions and click ‘add’. I picked generic options but there is more power to find a specific hash file (or file date) in any specific place in the file system. I’m only looking for c:\test.txt on windows operating systems.



File Condition

* Name: test_txt

Description: File Check

* Operating System: Windows All

Compliance Module: Any version

* File Type: FileExistence

* File Path: SYSTEM_DRIVE test.txt

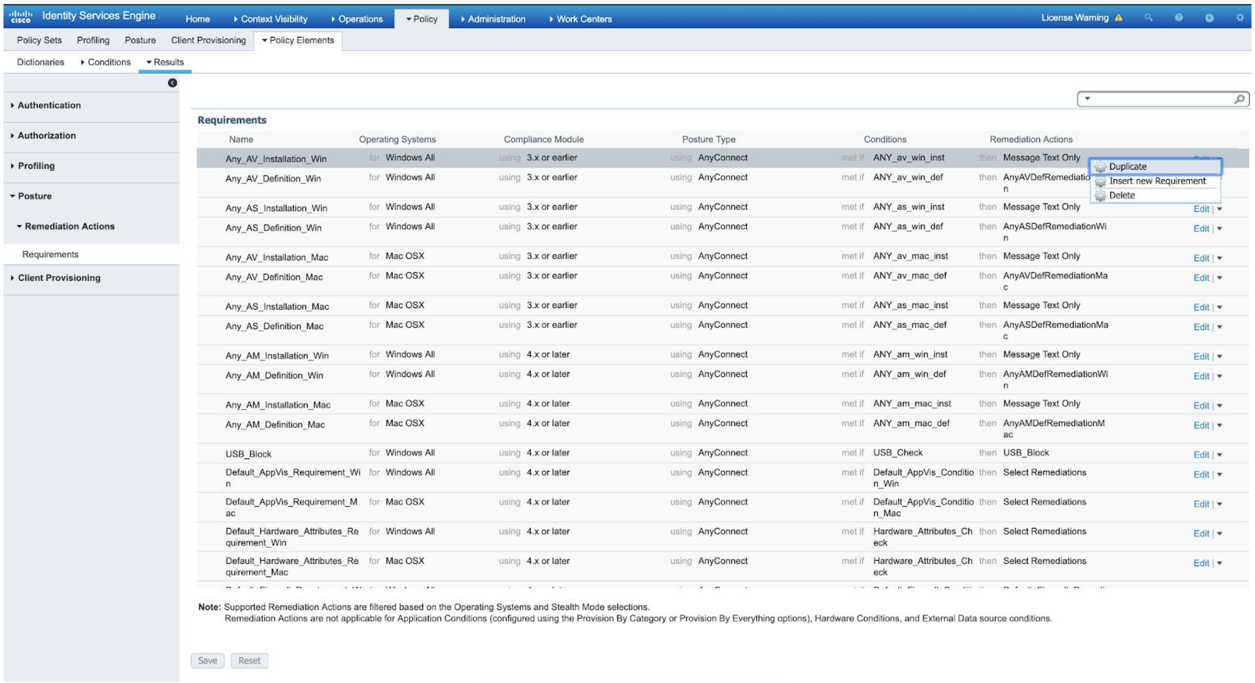
* File Operator: Exists

Requirements

Now that the conditions are built, let’s wrap them as Requirements. We only need to create a new one for the custom File Check one.

Navigate to Policy--Policy Elements--Results--Posture--Requirements

I wish there was an ‘add’ button but instead you create new Requirements by hovering by the Edit button of an existing rule and choose ‘Insert New Requirement’. Demonstrated here:

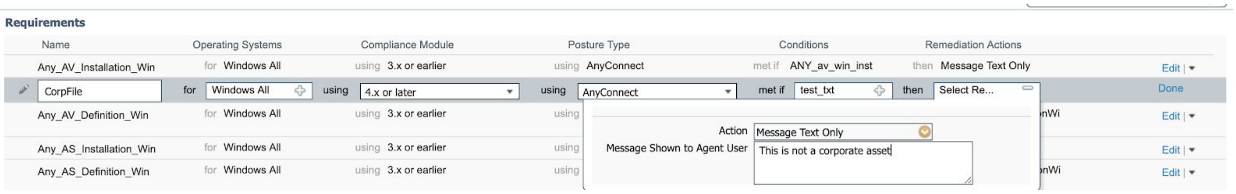


Requirements

Name	Operating Systems	Compliance Module	Posture Type	Conditions	Remediation Actions	
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_av_win_inst	then Message Text Only	
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_av_win_def	then AnyAVDefRemediation	
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_as_win_inst	then Message Text Only	Edit | ▾
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_as_win_def	then AnyASDefRemediationWin	Edit | ▾
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_av_mac_inst	then Message Text Only	Edit | ▾
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_av_mac_def	then AnyAVDefRemediationMac	Edit | ▾
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_inst	then Message Text Only	Edit | ▾
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using AnyConnect	met if ANY_as_mac_def	then AnyASDefRemediationMac	Edit | ▾
Any_AM_Installation_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_win_inst	then Message Text Only	Edit | ▾
Any_AM_Definition_Win	for Windows All	using 4.x or later	using AnyConnect	met if ANY_am_win_def	then AnyAMDefRemediationWin	Edit | ▾
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_inst	then Message Text Only	Edit | ▾
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if ANY_am_mac_def	then AnyAMDefRemediationMac	Edit | ▾
USB_Block	for Windows All	using 4.x or later	using AnyConnect	met if USB_Check	then USB_Block	Edit | ▾
Default_AppVis_Requirement_Win	for Windows All	using 4.x or later	using AnyConnect	met if Default_AppVis_Condition_Win	then Select Remediations	Edit | ▾
Default_AppVis_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Default_AppVis_Condition_Mac	then Select Remediations	Edit | ▾
Default_Hardware_Attributes_Requirement_Win	for Windows All	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Check	then Select Remediations	Edit | ▾
Default_Hardware_Attributes_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Hardware_Attributes_Check	then Select Remediations	Edit | ▾

Note: Supported Remediation Actions are filtered based on the Operating Systems and Stealth Mode selections.
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.

My File System Check is listed here (note test_txt will be found in that box under User Defined Conditions--File Conditions):

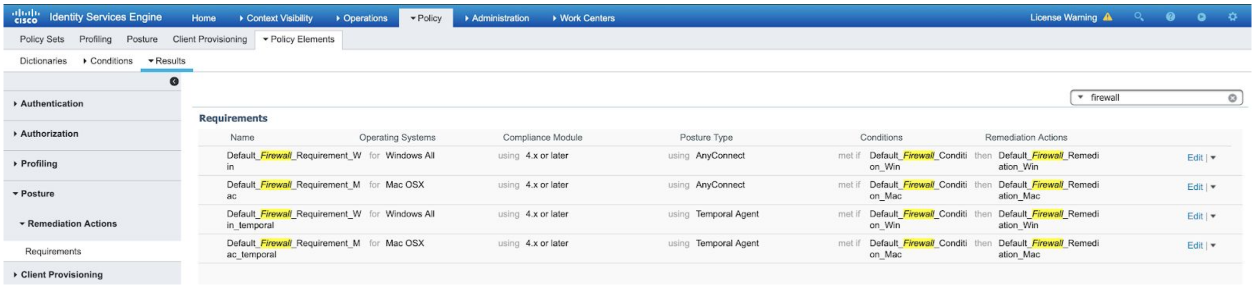


Requirements

Name	Operating Systems	Compliance Module	Posture Type	Conditions	Remediation Actions	
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using AnyConnect	met if ANY_av_win_inst	then Message Text Only	Edit | ▾
CorpFile	for Windows All	using 4.x or later	using AnyConnect	met if test_txt	then Select Re...	Done
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	using		nWi	Edit | ▾
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	using			Edit | ▾
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	using		nWi	Edit | ▾

Action: Message Text Only
Message Shown to Agent User: This is not a corporate asset

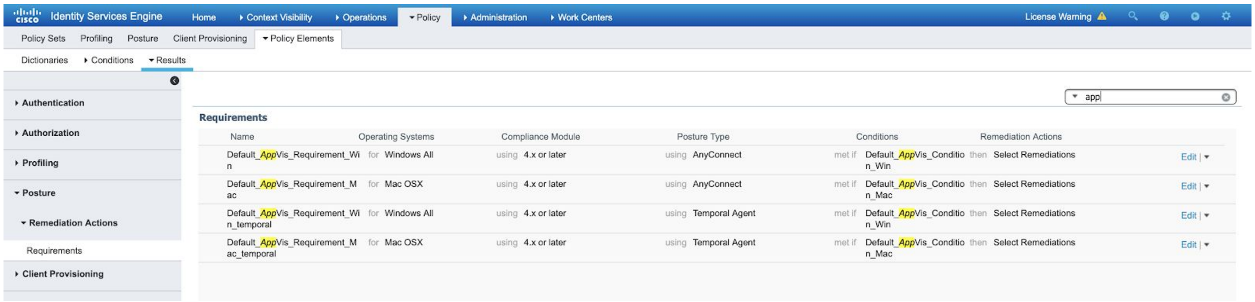
Note the other Requirements from the table are built in but they are screenshot here for completeness



firewall

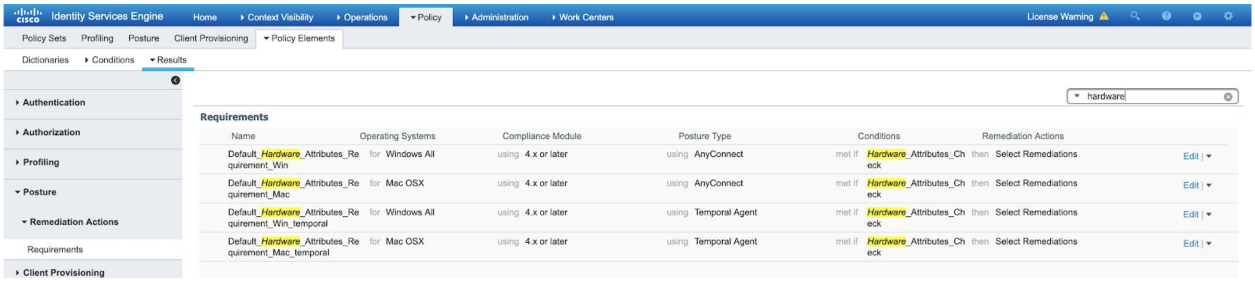
Requirements

Name	Operating Systems	Compliance Module	Posture Type	Conditions	Remediation Actions	
Default_*Firewall*_Requirement_Win	for Windows All	using 4.x or later	using AnyConnect	met if Default_*Firewall*_Condition_Win	then Default_*Firewall*_Remediation_Win	Edit | ▾
Default_*Firewall*_Requirement_Mac	for Mac OSX	using 4.x or later	using AnyConnect	met if Default_*Firewall*_Condition_Mac	then Default_*Firewall*_Remediation_Mac	Edit | ▾
Default_*Firewall*_Requirement_Win_temporal	for Windows All	using 4.x or later	using Temporal Agent	met if Default_*Firewall*_Condition_Win	then Default_*Firewall*_Remediation_Win	Edit | ▾
Default_*Firewall*_Requirement_Mac_temporal	for Mac OSX	using 4.x or later	using Temporal Agent	met if Default_*Firewall*_Condition_Mac	then Default_*Firewall*_Remediation_Mac	Edit | ▾



Requirements

Name		Operating Systems		Compliance Module		Posture Type		Conditions		Remediation Actions	
Default_AppVis_Requirement_Win	for	Windows All	using	4.x or later	using	AnyConnect	met if	Default_AppVis_Condition_Win	then	Select Remediations	Edit
Default_AppVis_Requirement_Mac	for	Mac OSX	using	4.x or later	using	AnyConnect	met if	Default_AppVis_Condition_Mac	then	Select Remediations	Edit
Default_AppVis_Requirement_Win_temporal	for	Windows All	using	4.x or later	using	Temporal Agent	met if	Default_AppVis_Condition_Win	then	Select Remediations	Edit
Default_AppVis_Requirement_Mac_temporal	for	Mac OSX	using	4.x or later	using	Temporal Agent	met if	Default_AppVis_Condition_Mac	then	Select Remediations	Edit



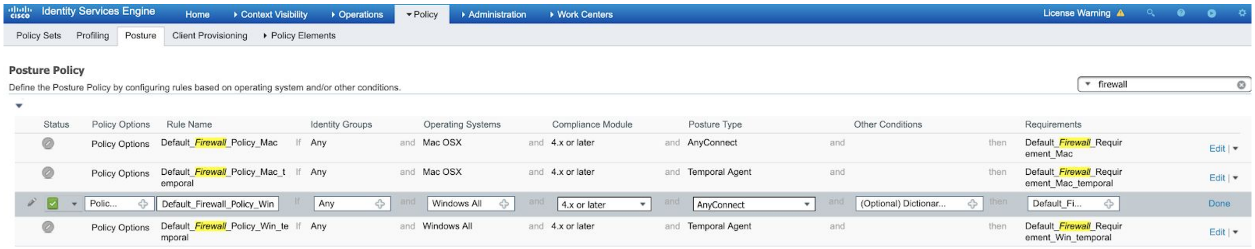
Requirements

Name		Operating Systems		Compliance Module		Posture Type		Conditions		Remediation Actions	
Default_Hardware_Attributes_Requirement_Win	for	Windows All	using	4.x or later	using	AnyConnect	met if	Hardware_Attributes_Check	then	Select Remediations	Edit
Default_Hardware_Attributes_Requirement_Mac	for	Mac OSX	using	4.x or later	using	AnyConnect	met if	Hardware_Attributes_Check	then	Select Remediations	Edit
Default_Hardware_Attributes_Requirement_Win_temporal	for	Windows All	using	4.x or later	using	Temporal Agent	met if	Hardware_Attributes_Check	then	Select Remediations	Edit
Default_Hardware_Attributes_Requirement_Mac_temporal	for	Mac OSX	using	4.x or later	using	Temporal Agent	met if	Hardware_Attributes_Check	then	Select Remediations	Edit

Posture Policy

This is where everything comes together. The Policy isn't a 'first match exit' style. So the order does not matter. Everything that matches a user/operating system/and other defined criteria, will be subjected to the Posture rule. An endpoint is considered compliant if it checks true for every posture rule it's subjected to. Most of the items we're using in our scenario just need to be enabled (they're already written). Navigate to Policy--Posture.

Enable the Firewall requirement for Windows/Anyconnect like so (click 'Edit' in the far right and change the status column on the far left):

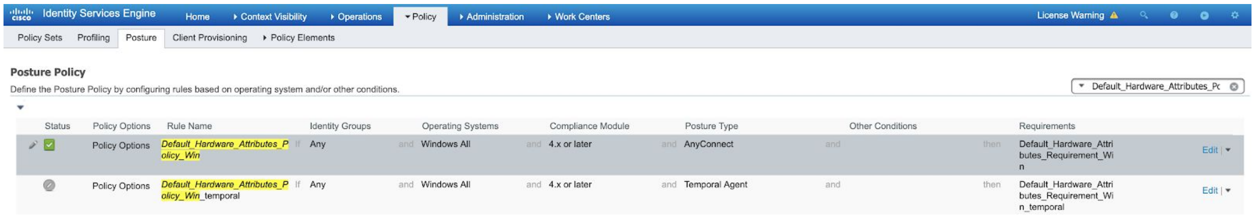


Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions		Requirements	
○	Policy Options	Default_Firewall_Policy_Mac	If	Any	and	Mac OSX	and	4.x or later	and	AnyConnect	and		then	Default_Firewall_Requirement_Mac	Edit
○	Policy Options	Default_Firewall_Policy_Mac_temporal	If	Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and		then	Default_Firewall_Requirement_Mac_temporal	Edit
☑	Polic...	Default_Firewall_Policy_Win	If	Any	and	Windows All	and	4.x or later	and	AnyConnect	and	(Optional) Dictionar...	then	Default_Fi...	Done
○	Policy Options	Default_Firewall_Policy_Win_temporal	If	Any	and	Windows All	and	4.x or later	and	Temporal Agent	and		then	Default_Firewall_Requirement_Win_temporal	Edit

Hardware:

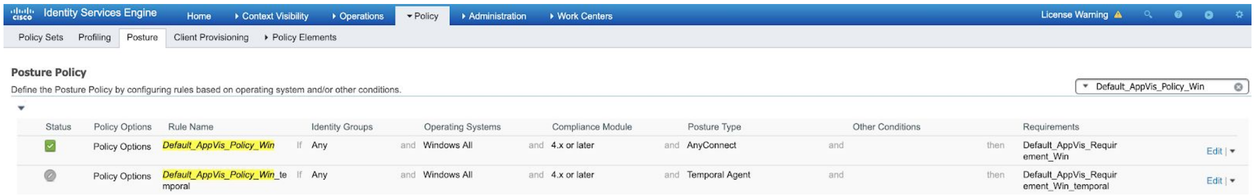


Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Status	Policy Options	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions		Requirements	
☑	Policy Options	Default_Hardware_Attributes_Policy_Win	If	Any	and	Windows All	and	4.x or later	and	AnyConnect	and		then	Default_Hardware_Attributes_Requirement_Win	Edit
○	Policy Options	Default_Hardware_Attributes_Policy_Win_temporal	If	Any	and	Windows All	and	4.x or later	and	Temporal Agent	and		then	Default_Hardware_Attributes_Requirement_Win_temporal	Edit

Application Visibility:



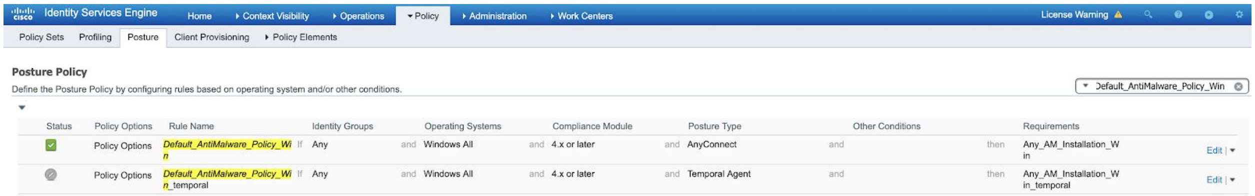
Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Default_AppVis_Policy_Win

Status	Policy Options	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions		Requirements	
☑	Policy Options	*Default_AppVis_Policy_Win*	If	Any	and	Windows All	and	4.x or later	and	AnyConnect	and		then	Default_AppVis_Requirement_Win	Edit
○	Policy Options	*Default_AppVis_Policy_Win*_temporal	If	Any	and	Windows All	and	4.x or later	and	Temporal Agent	and		then	Default_AppVis_Requirement_Win_temporal	Edit

Antimalware:



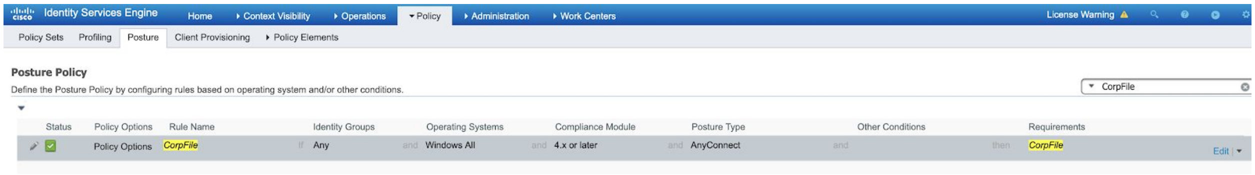
Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Default_AntiMalware_Policy_Win

Status	Policy Options	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions		Requirements	
☑	Policy Options	*Default_AntiMalware_Policy_Win*	If	Any	and	Windows All	and	4.x or later	and	AnyConnect	and		then	Any_AM_Installation_Win	Edit
○	Policy Options	*Default_AntiMalware_Policy_Win*_temporal	If	Any	and	Windows All	and	4.x or later	and	Temporal Agent	and		then	Any_AM_Installation_Win_temporal	Edit

And lastly create the File Policy check by clicking ‘Edit’ beside any rule and ‘Insert New Policy’. Mine looks like this:



Posture Policy

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

CorpFile

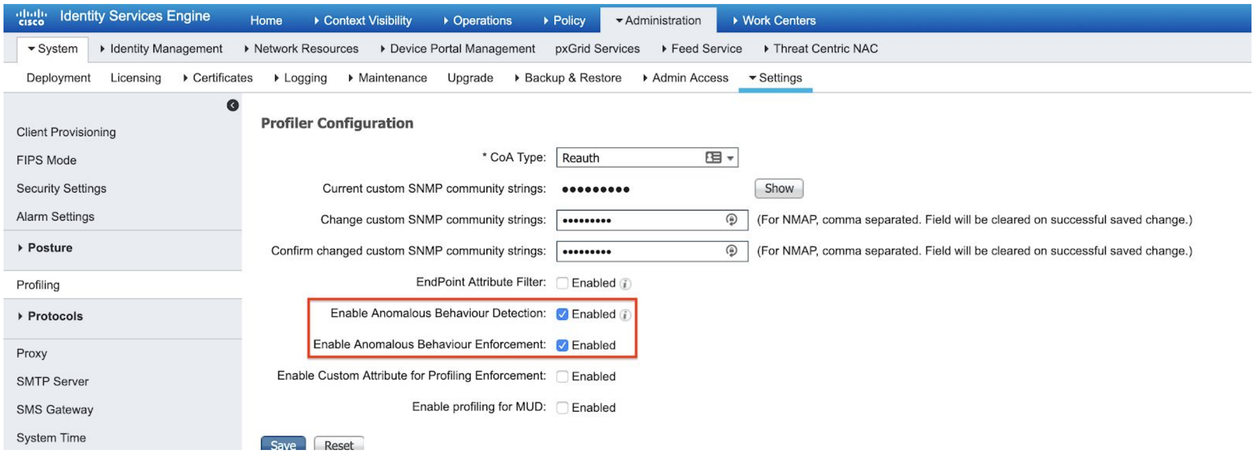
Status	Policy Options	Rule Name		Identity Groups		Operating Systems		Compliance Module		Posture Type		Other Conditions		Requirements	
☑	Policy Options	*CorpFile*	If	Any	and	Windows All	and	4.x or later	and	AnyConnect	and		then	*CorpFile*	Edit

Anomalous Behavior Detection

This is an antispoof policy to determine if security controls are being evaded. Basically it’s looking to see if someone is mac spoofing a printer/phone or is just completely different than what the authentic MAC address is presenting. The exact configuration and detailed capabilities are documented here.

In this guide we will enable detection and enforcement. In production I’d advise caution and begin with Detection to minimize potential disruption. Note it’s unlikely to trip this feature in a PoV or trial, without explicitly trying to.

Enable the feature with Administration--System--Settings--Profiling.



Profiler Configuration

* CoA Type: Reauth

Current custom SNMP community strings: ●●●●●●●●● Show

Change custom SNMP community strings: ••••••••• (For NMAP, comma separated. Field will be cleared on successful saved change.)

Confirm changed custom SNMP community strings: ••••••••• (For NMAP, comma separated. Field will be cleared on successful saved change.)

EndPoint Attribute Filter: ☐ Enabled

Enable Anomalous Behaviour Detection: ☑ Enabled

Enable Anomalous Behaviour Enforcement: ☑ Enabled

Enable Custom Attribute for Profiling Enforcement: ☐ Enabled

Enable profiling for MUD: ☐ Enabled

The Policy to use this new feature will be documented in the General Policy section coming up next.

General Policy

This section puts together all the constructs and applies it to incoming user authentication requests. Notably the Authentication and Authorization steps.

Bootstrapping

This builds out the building blocks of Authorization Policies, notably dACLs and Authorization Profiles. But starts with Captive Portals

Captive Portals

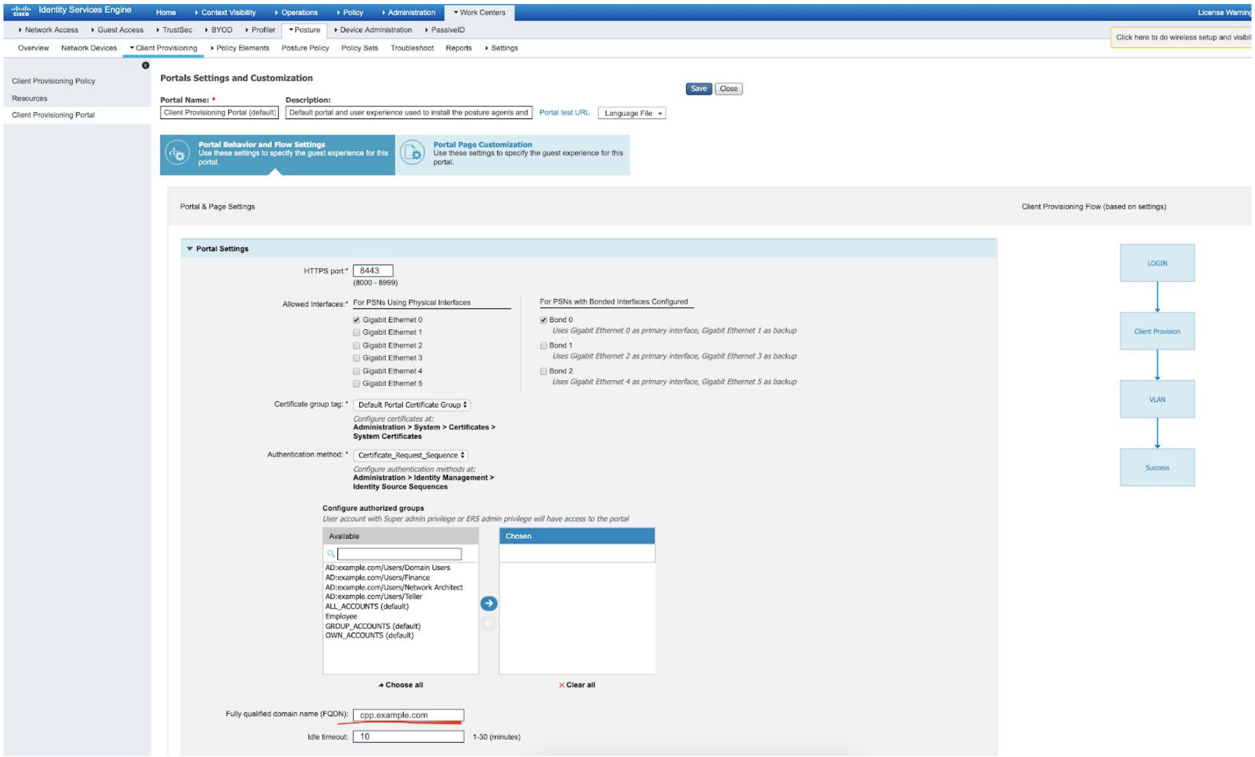
We'll be creating three captive portals that are doing different things. Defined:

Client Provisioning Portal - Users are sent to this portal to be provisioned (and then postured) with Anyconnect. Or if Anyconnect is already installed, perform posture only.

Profiling Portal - Technically a Hot Spot portal to present a user with a webpage stating that the network is trying to ascertain what kind of endpoint this is. ISE should be able to grab a user-agent string from the endpoint, assign a profile and then re-send it through the Authorization policy again.

Central Web Authentication - Used for MAC and Linux endpoints that are not supported with PassiveID in order for them to authenticate to the network.

For Client Provisioning Portal (CPP), navigate to Work Centers--Posture--Client Provisioning--Client Provisioning Portal. Note the built-in portal named: Client Provisioning Portal (default). We can use this same portal, just give it a FQDN (cpp.example.com) as in this picture:



Portals Settings and Customization

Portal Name: * Client Provisioning Portal (default)

Description: Default portal and user experience used to install the posture agents and

Portal & Page Settings

Portal Settings

HTTPS port:* 8443
(8000 - 8999)

Allowed Interfaces:*

For PSNs Using Physical Interfaces
☑ Gigabit Ethernet 0
☐ Gigabit Ethernet 1
☐ Gigabit Ethernet 2
☐ Gigabit Ethernet 3
☐ Gigabit Ethernet 4
☐ Gigabit Ethernet 5

For PSNs with Bonded Interfaces Configured
☑ Bond 0
Uses Gigabit Ethernet 0 as primary interface, Gigabit Ethernet 1 as backup
☐ Bond 1
Uses Gigabit Ethernet 2 as primary interface, Gigabit Ethernet 3 as backup
☐ Bond 2
Uses Gigabit Ethernet 4 as primary interface, Gigabit Ethernet 5 as backup

Certificate group tag: * Default Portal Certificate Group
Configure certificates at:
Administration > System > Certificates > System Certificates

Authentication method: * Certificate_Request_Sequence
Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences

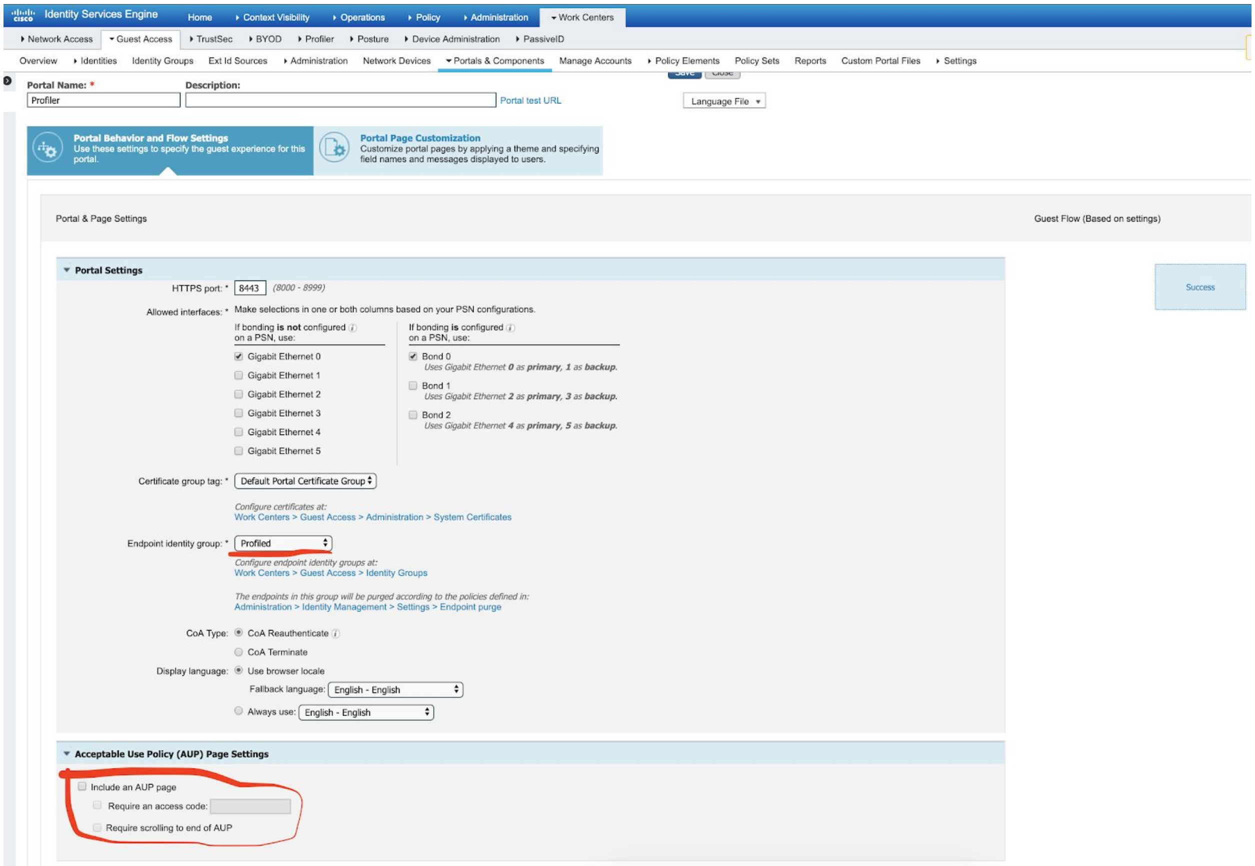
Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal

Available	Chosen
AD:example.com/Users/Domain Users AD:example.com/Users/Finance AD:example.com/Users/Network Architect AD:example.com/Users/Teller ALL_ACCOUNTS (default) Employee GROUP_ACCOUNTS (default) OWN_ACCOUNTS (default)	

Fully qualified domain name (FQDN): cpp.example.com

Idle timeout: 10 1-30 (minutes)

Profiling Portal. Navigate to Work Centers--Guest Access--Portals & Components--Guest Portals. Click 'Create' and 'Hotspot Guest Portal'. Mine looks like the below. Click to save when done.



Portal Name: * Profiler

Description:

Portal test URL

Portal Settings

HTTPS port: * 8443 *(8000 - 8999)*

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

If bonding **is not** configured on a PSN, use:	If bonding **is** configured on a PSN, use:
☑ Gigabit Ethernet 0	☑ Bond 0 *Uses Gigabit Ethernet **0** as **primary**, **1** as **backup**.*
☐ Gigabit Ethernet 1	☐ Bond 1 *Uses Gigabit Ethernet **2** as **primary**, **3** as **backup**.*
☐ Gigabit Ethernet 2	☐ Bond 2 *Uses Gigabit Ethernet **4** as **primary**, **5** as **backup**.*
☐ Gigabit Ethernet 3	
☐ Gigabit Ethernet 4	
☐ Gigabit Ethernet 5	

Certificate group tag: * Default Portal Certificate Group

Configure certificates at:
Work Centers > Guest Access > Administration > System Certificates

Endpoint identity group: * Profiled

Configure endpoint identity groups at:
Work Centers > Guest Access > Identity Groups

The endpoints in this group will be purged according to the policies defined in:
Administration > Identity Management > Settings > Endpoint purge

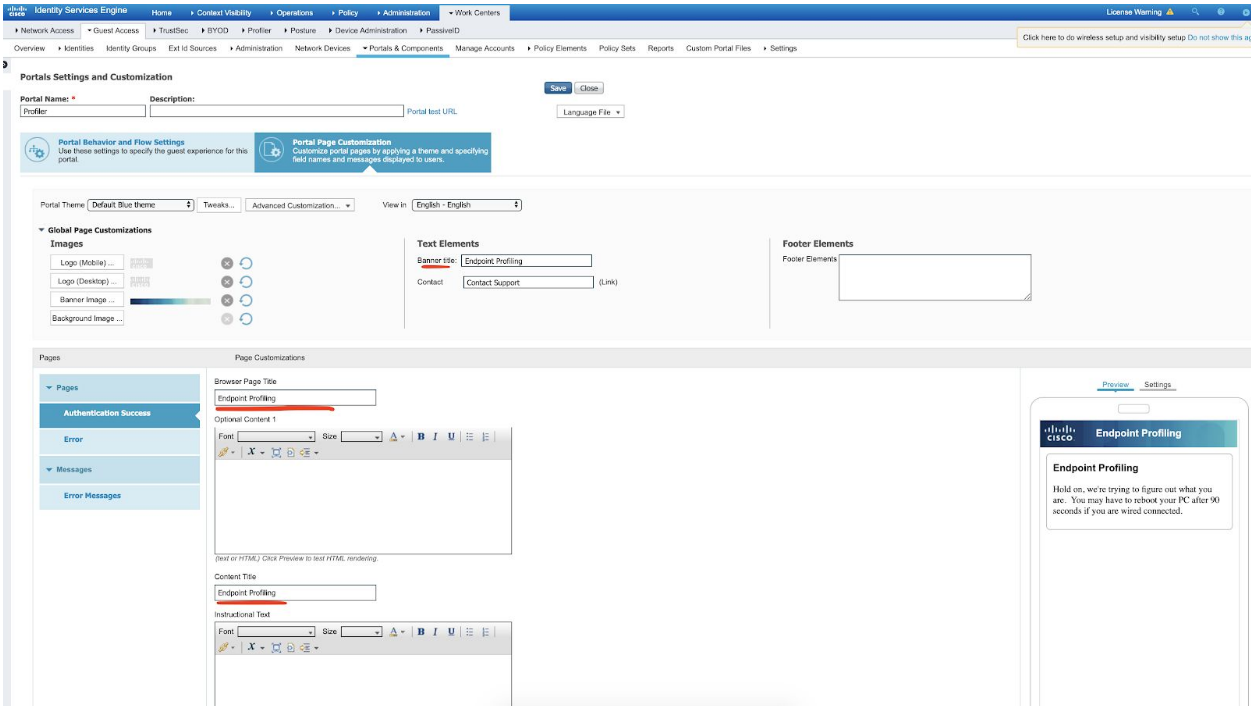
CoA Type: ● CoA Reauthenticate
○ CoA Terminate

Display language: ● Use browser locale
Fallback language: English - English
○ Always use: English - English

Acceptable Use Policy (AUP) Page Settings

☐ Include an AUP page
☐ Require an access code:
☐ Require scrolling to end of AUP

And let’s click the Portal Page Customization to add a little more info for the user to see if they land on this portal:



Click here to do wireless setup and visibility setup Do not show this ag

Portals Settings and Customization

Portal Name: * Profiler

Description:

Portal Theme: Default Blue theme

View in: English - English

Global Page Customizations

Images

Text Elements

Banner title: Endpoint Profiling

Contact: Contact Support (Link)

Footer Elements

Footer Elements:

Pages

Page Customizations

Browser Page Title: Endpoint Profiling

Optional Content 1

(text or HTML) Click Preview to test HTML rendering.

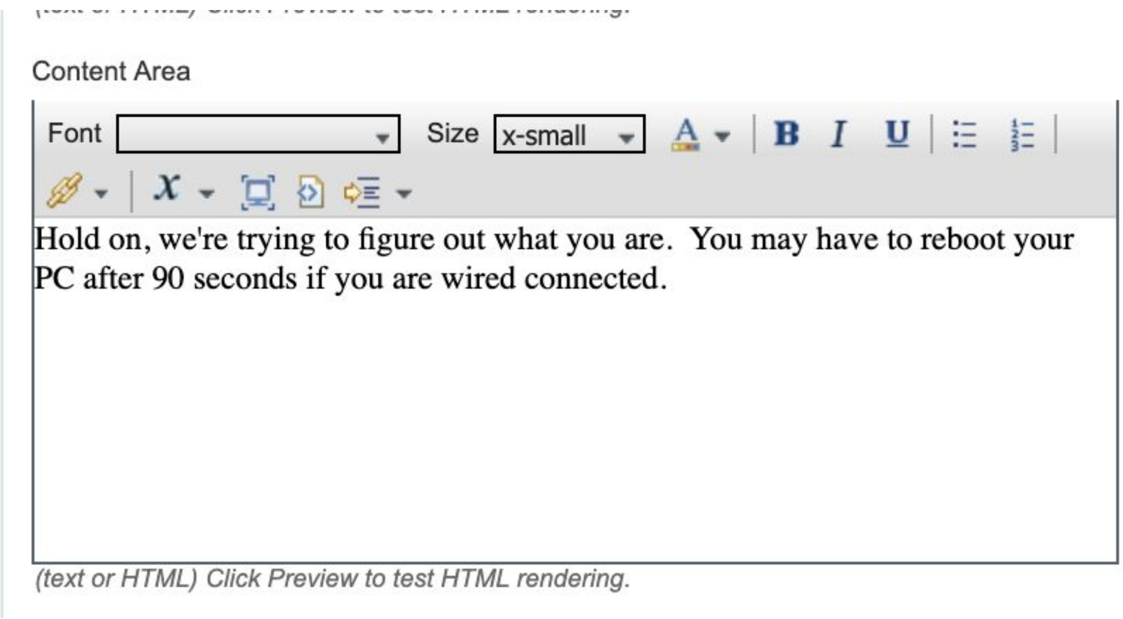
Content Title: Endpoint Profiling

Instructional Text

Endpoint Profiling

Endpoint Profiling

Hold on, we're trying to figure out what you are. You may have to reboot your PC after 90 seconds if you are wired connected.



Content Area

Size: x-small

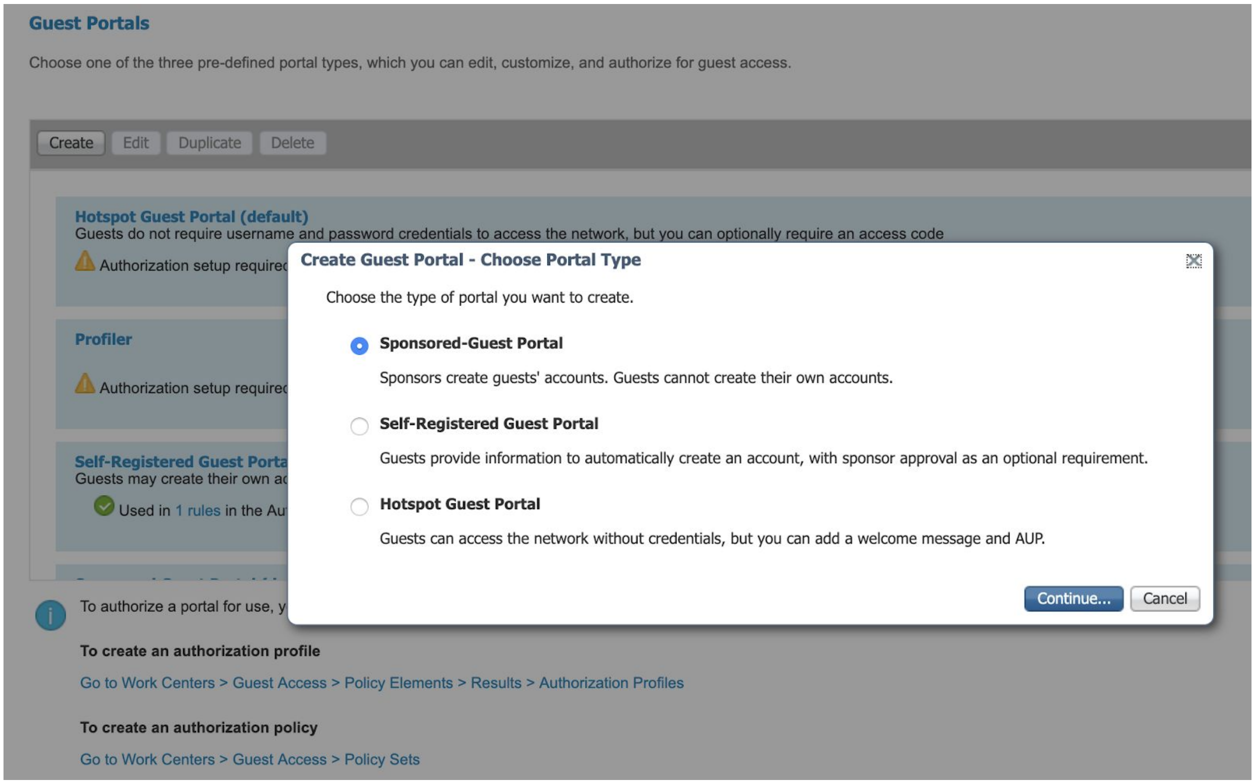
Hold on, we're trying to figure out what you are. You may have to reboot your PC after 90 seconds if you are wired connected.

(text or HTML) Click Preview to test HTML rendering.

(Hold on, we're trying to figure out what you are. You may have to reboot your PC after 90 seconds if you are wired connected.)

Central Web Authentication

As before, navigate to Work Centers--Guest Access--Portals & Components--Guest Portals. Click Create and choose “Sponsored-Guest Portal” as the type.



Guest Portals
Create
Edit
Duplicate
Delete
Hotspot Guest Portal (default)
Authorization setup required
Profiler
Authorization setup required
Self-Registered Guest Porta
Used in 1 rules in the Au
Continue...
Cancel

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

Guests do not require username and password credentials to access the network, but you can optionally require an access code

Guests may create their own ac

To authorize a portal for use, y

To create an authorization profile

Go to Work Centers > Guest Access > Policy Elements > Results > Authorization Profiles

To create an authorization policy

Go to Work Centers > Guest Access > Policy Sets

Create Guest Portal - Choose Portal Type

Choose the type of portal you want to create.

● **Sponsored-Guest Portal**

Sponsors create guests' accounts. Guests cannot create their own accounts.

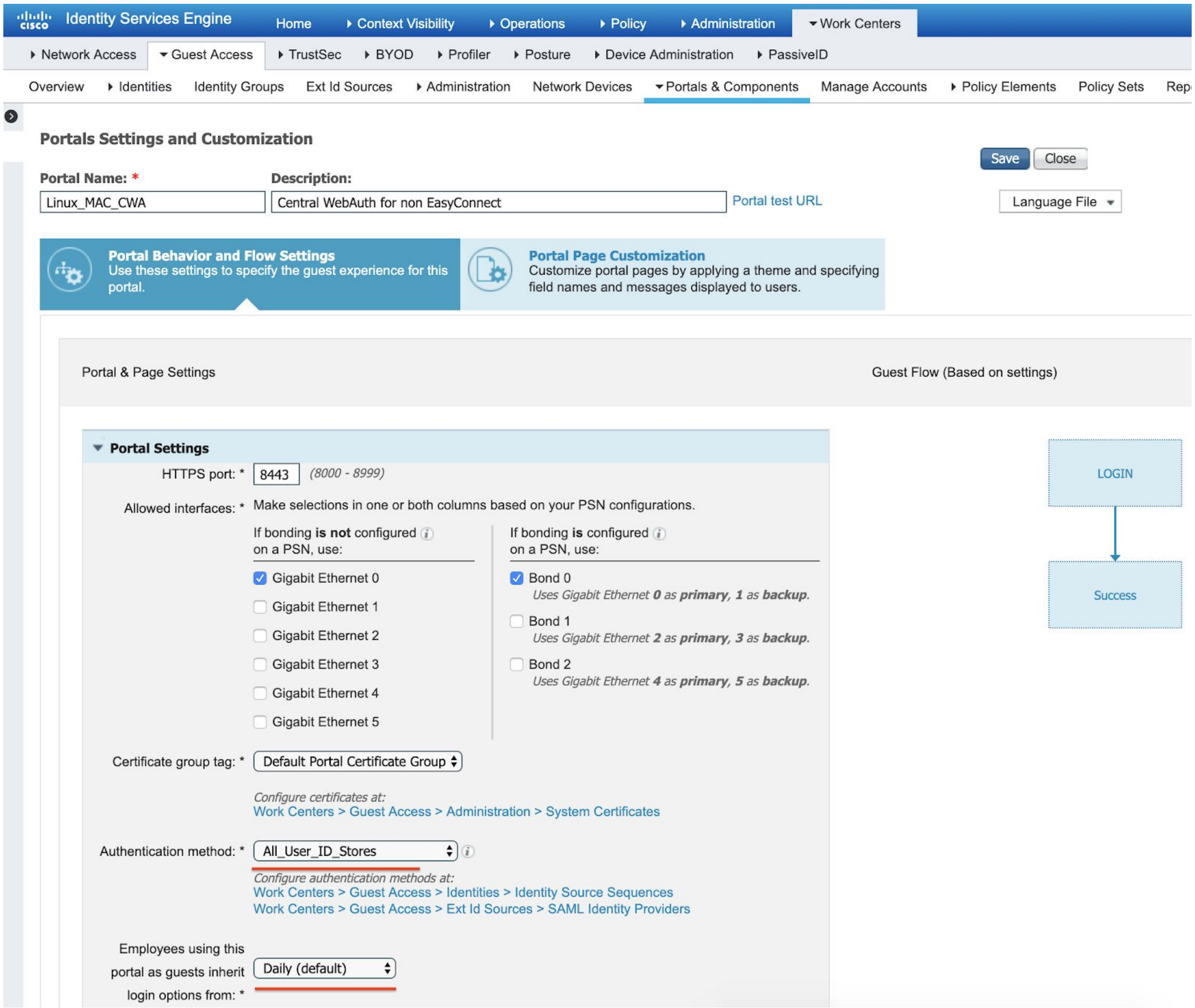
○ **Self-Registered Guest Portal**

Guests provide information to automatically create an account, with sponsor approval as an optional requirement.

○ **Hotspot Guest Portal**

Guests can access the network without credentials, but you can add a welcome message and AUP.

Here is a look at my CWA. I take out most of the steps to make it as frictionless as possible. Most things are deselected (illustrated here)



Portals Settings and Customization

Portal Name: * Linux_MAC_CWA

Description: Central WebAuth for non EasyConnect

Portal Settings

HTTPS port: * 8443 *(8000 - 8999)*

Allowed interfaces: * Make selections in one or both columns based on your PSN configurations.

If bonding **is not** configured on a PSN, use:	If bonding **is** configured on a PSN, use:
☑ Gigabit Ethernet 0	☑ Bond 0 *Uses Gigabit Ethernet **0** as **primary**, **1** as **backup**.*
☐ Gigabit Ethernet 1	☐ Bond 1 *Uses Gigabit Ethernet **2** as **primary**, **3** as **backup**.*
☐ Gigabit Ethernet 2	☐ Bond 2 *Uses Gigabit Ethernet **4** as **primary**, **5** as **backup**.*
☐ Gigabit Ethernet 3	
☐ Gigabit Ethernet 4	
☐ Gigabit Ethernet 5	

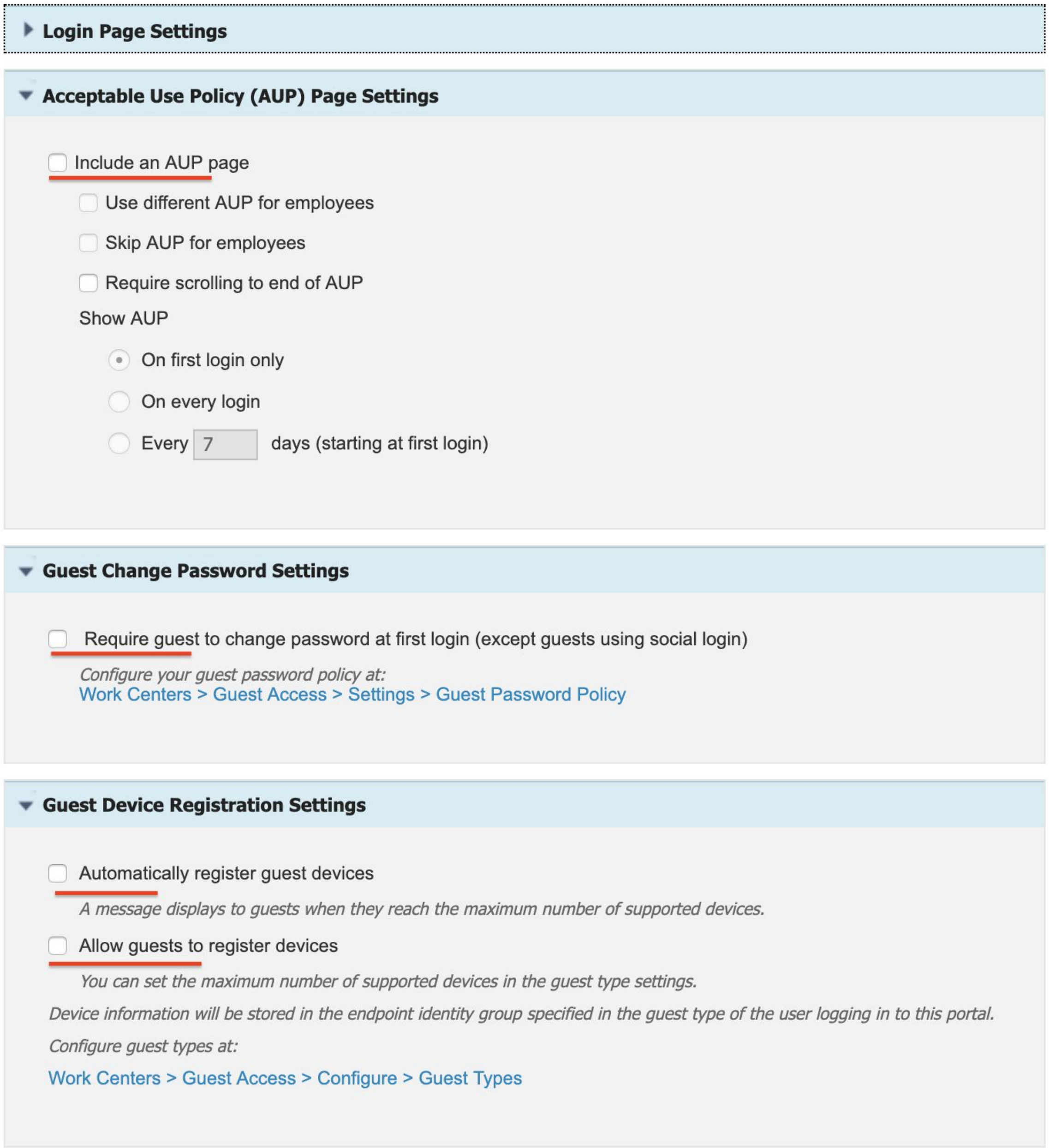
Certificate group tag: * Default Portal Certificate Group

Configure certificates at:
Work Centers > Guest Access > Administration > System Certificates

Authentication method: * All_User_ID_Stores

Configure authentication methods at:
Work Centers > Guest Access > Identities > Identity Source Sequences
Work Centers > Guest Access > Ext Id Sources > SAML Identity Providers

Employees using this portal as guests inherit login options from: * Daily (default)



Login Page Settings

Acceptable Use Policy (AUP) Page Settings

☐ Include an AUP page

- ☐ Use different AUP for employees
- ☐ Skip AUP for employees
- ☐ Require scrolling to end of AUP

Show AUP

- ● On first login only
- ○ On every login
- ○ Every 7 days (starting at first login)

Guest Change Password Settings

☐ Require guest to change password at first login (except guests using social login)

Configure your guest password policy at:
Work Centers > Guest Access > Settings > Guest Password Policy

Guest Device Registration Settings

☐ Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

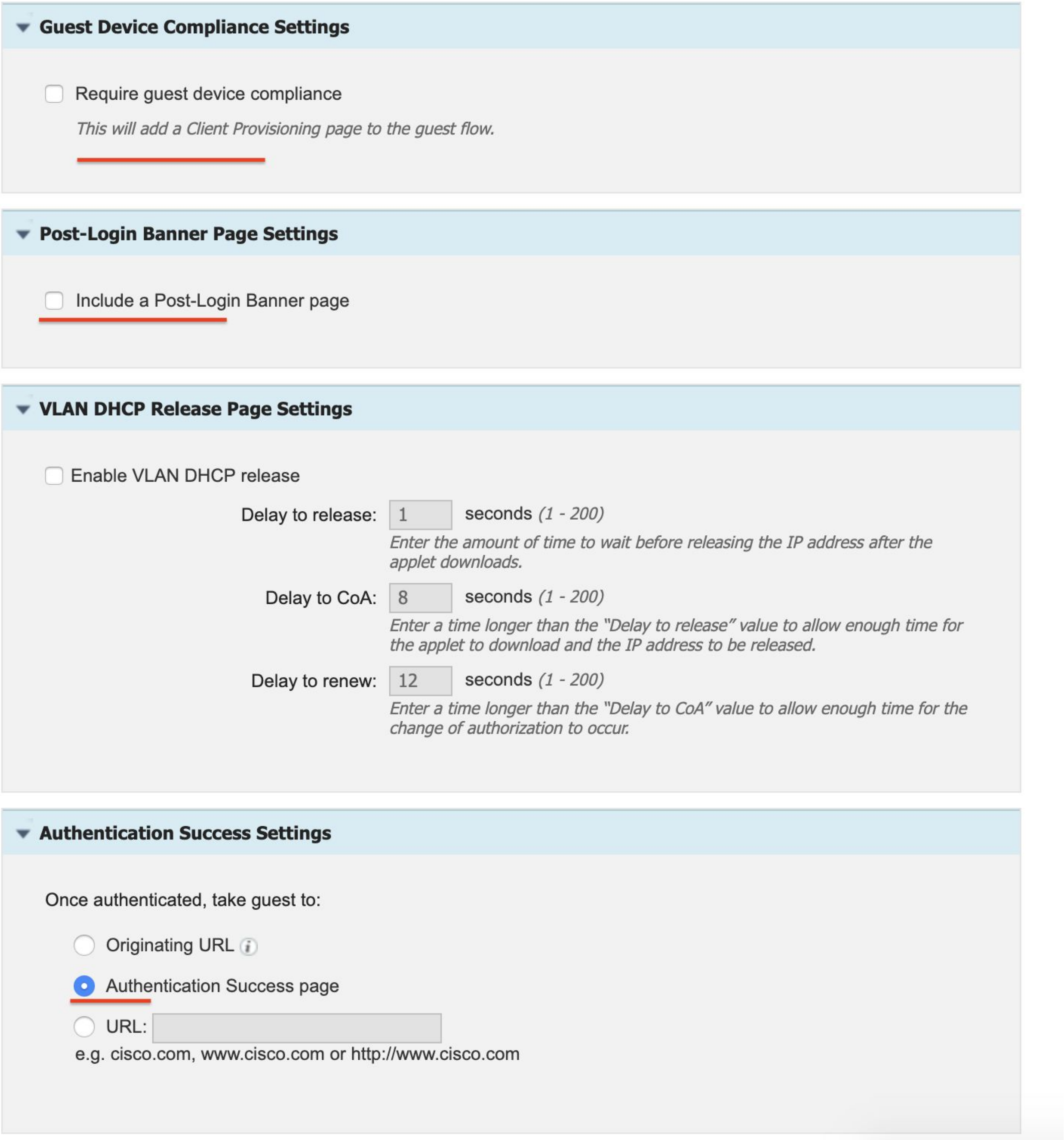
☐ Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

Work Centers > Guest Access > Configure > Guest Types



Guest Device Compliance Settings

☐ Require guest device compliance

This will add a Client Provisioning page to the guest flow.

Post-Login Banner Page Settings

☐ Include a Post-Login Banner page

VLAN DHCP Release Page Settings

☐ Enable VLAN DHCP release

Delay to release: 1 seconds *(1 - 200)*

Enter the amount of time to wait before releasing the IP address after the applet downloads.

Delay to CoA: 8 seconds *(1 - 200)*

Enter a time longer than the "Delay to release" value to allow enough time for the applet to download and the IP address to be released.

Delay to renew: 12 seconds *(1 - 200)*

Enter a time longer than the "Delay to CoA" value to allow enough time for the change of authorization to occur.

Authentication Success Settings

Once authenticated, take guest to:

○ Originating URL

● Authentication Success page

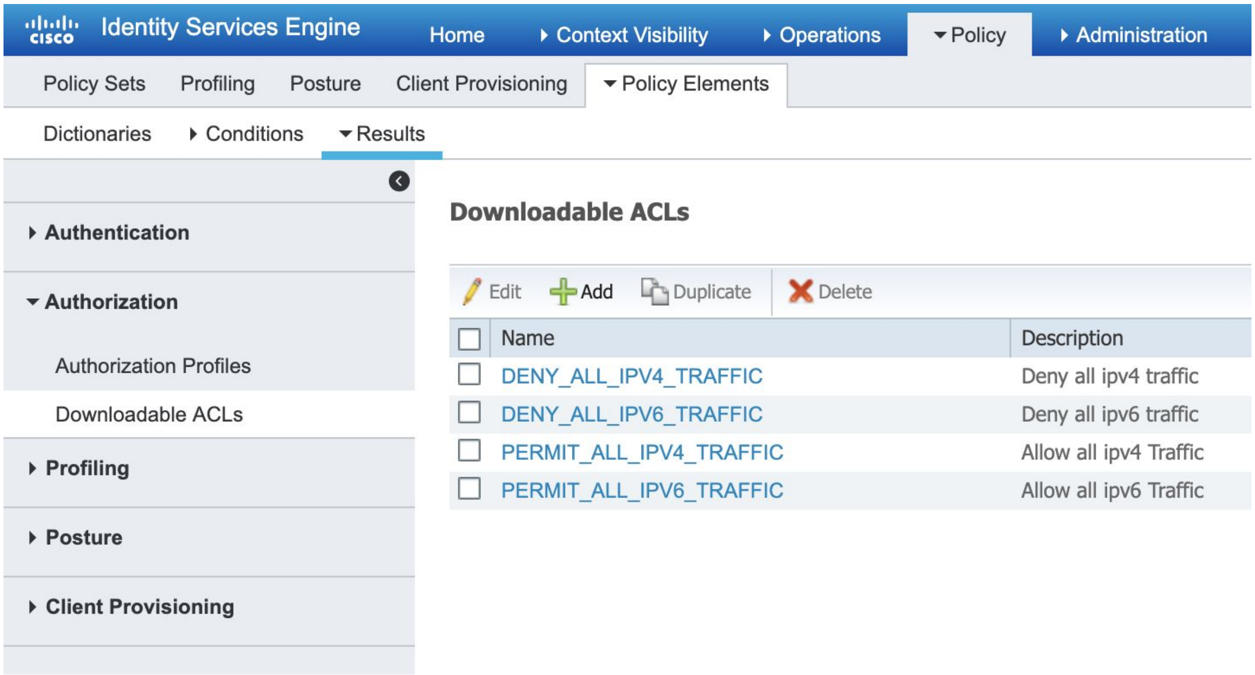
○ URL:

e.g. cisco.com, www.cisco.com or http://www.cisco.com

Downloadable ACLS (dACLS)

This section will build the dACLS that will be used throughout the Policies. All dACLs are housed in Policy--Policy Elements--Authorization--Downloadable ACLS.

This is the included list:

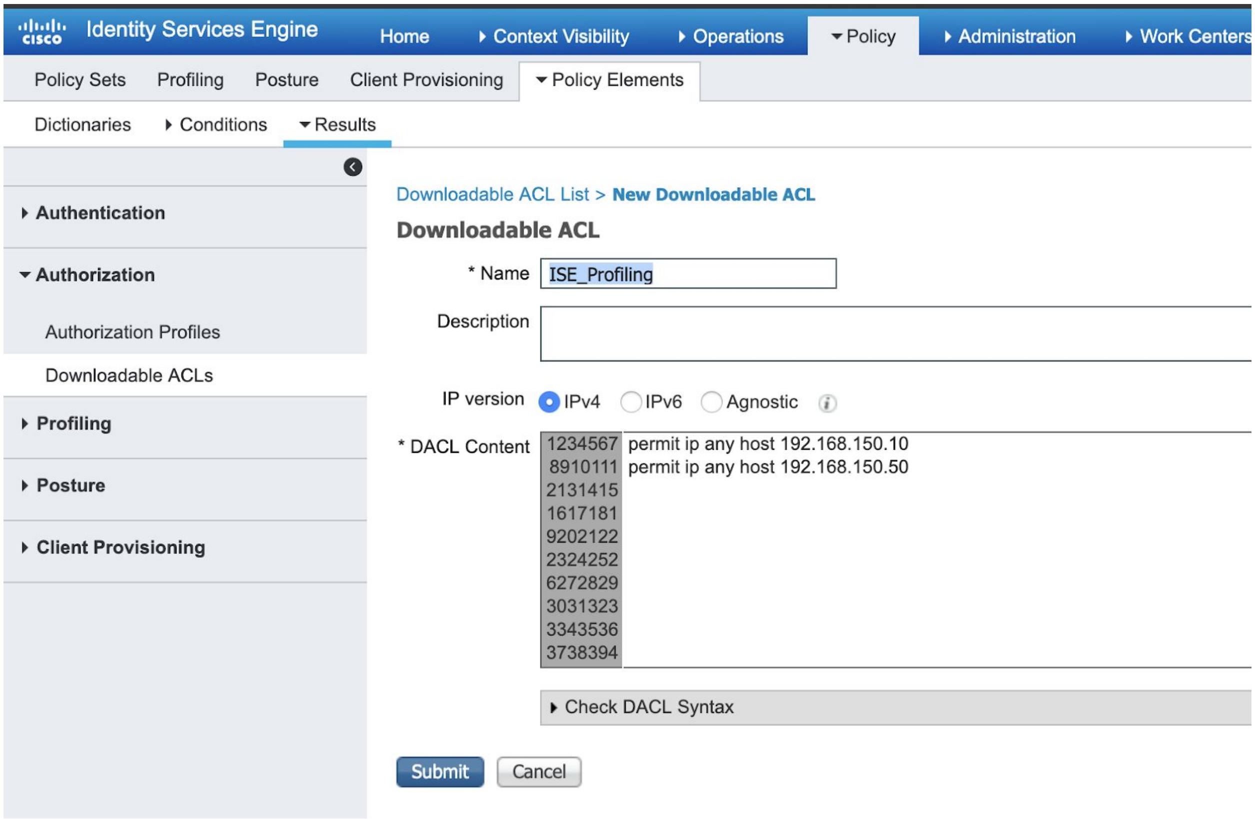


Downloadable ACLs

☐	Name	Description
☐	DENY_ALL_IPV4_TRAFFIC	Deny all ipv4 traffic
☐	DENY_ALL_IPV6_TRAFFIC	Deny all ipv6 traffic
☐	PERMIT_ALL_IPV4_TRAFFIC	Allow all ipv4 Traffic
☐	PERMIT_ALL_IPV6_TRAFFIC	Allow all ipv6 Traffic

ISE_Profiling

```
#This will allow the endpoint to use AD DNS and Kerberos and permits access to ISE for
#NMAP probing and captive portals
permit ip any host 192.168.150.10
permit ip any host 192.168.150.50
```



Downloadable ACL

* Name: ISE_Profiling

Description:

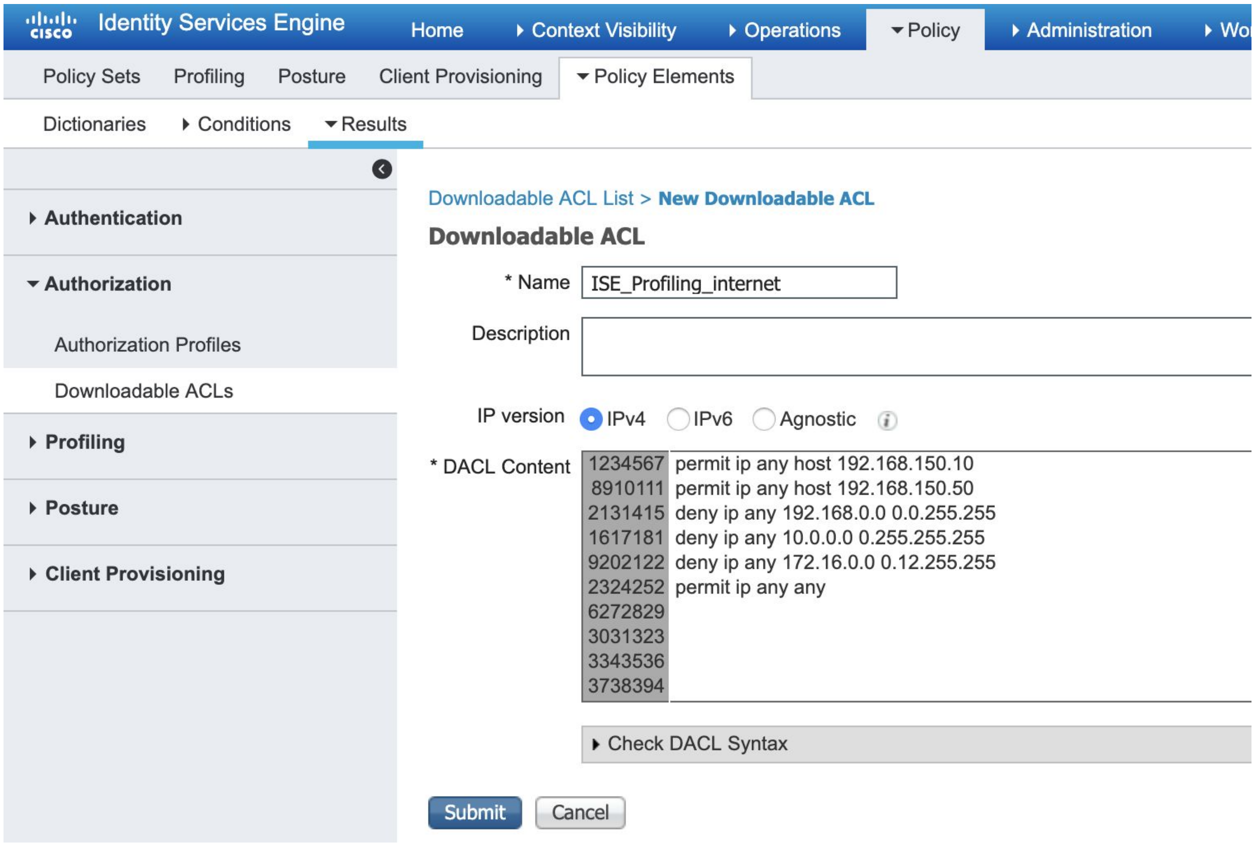
IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
permit ip any host 192.168.150.10
permit ip any host 192.168.150.50
```

ISE_Profiling_internet

```
#same as above but gives the endpoint Internet Access
#this may be useful for posture conditions when the computer needs Windows updates or smartscreen
#to run
permit ip any host 192.168.150.10
permit ip any host 192.168.150.50
deny ip any 192.168.0.0 0.0.255.255
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.12.255.255
permit ip any any
```



Downloadable ACL

* Name: ISE_Profiling_internet

Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

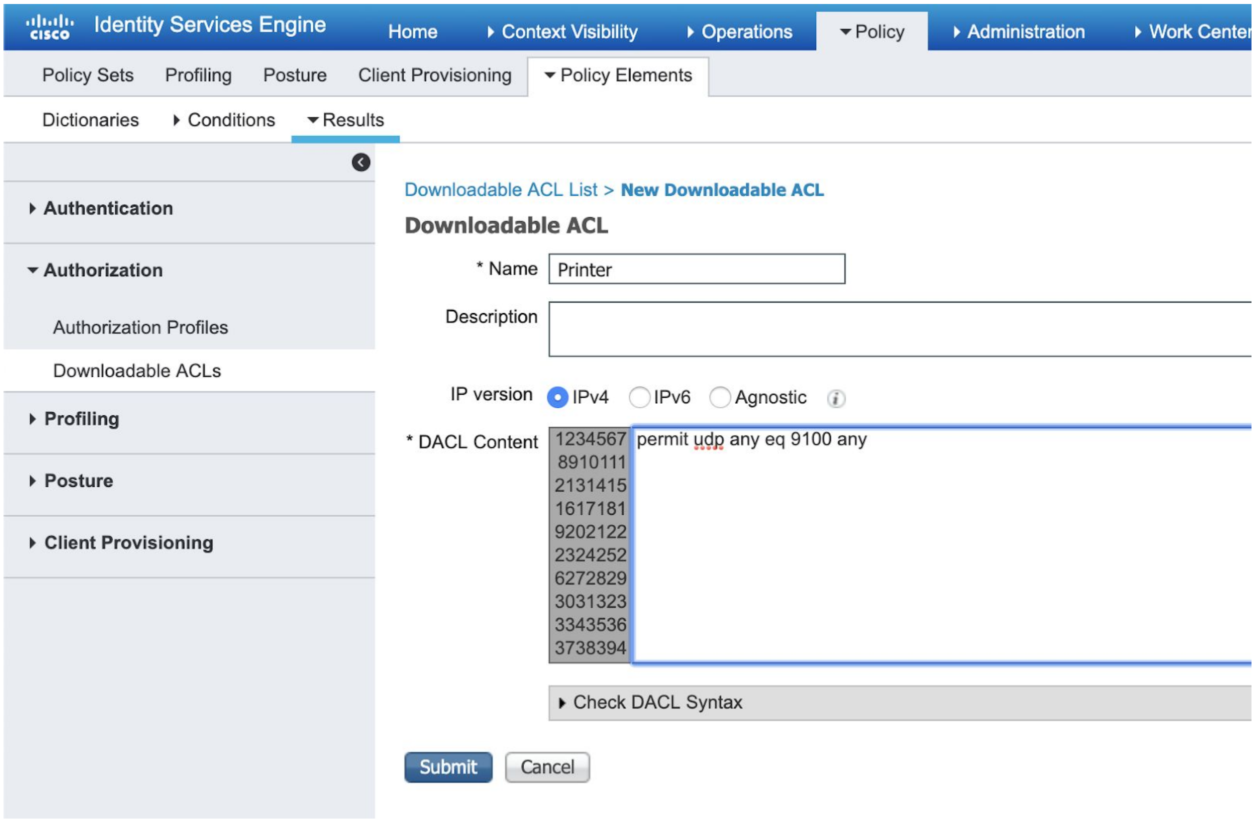
* DACL Content

```
permit ip any host 192.168.150.10
permit ip any host 192.168.150.50
deny ip any 192.168.0.0 0.0.255.255
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.12.255.255
permit ip any any
```

Printer

#useful to only allow profiled printers to accept print jobs

```
permit udp any eq 9100 any
```



Downloadable ACL

* Name: Printer

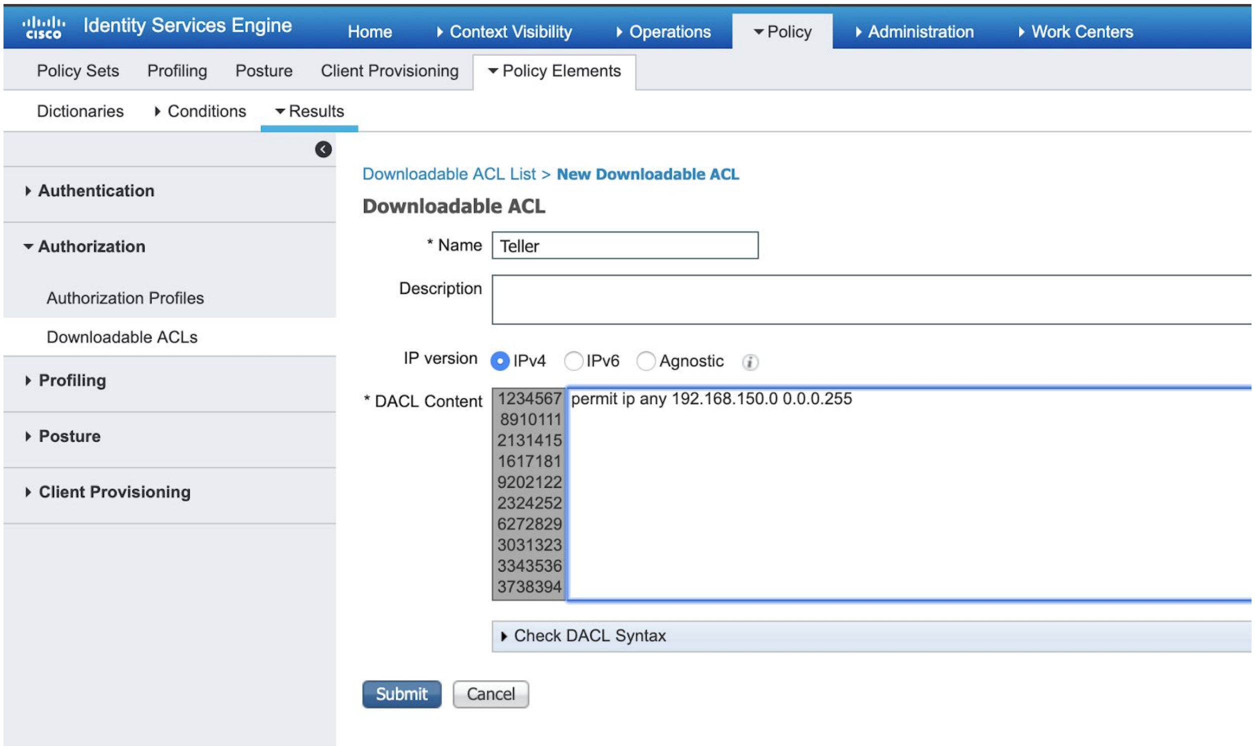
Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
permit udp any eq 9100 any
```

Teller
#dACL for Tellers to access the DC but nothing else
permit ip any 192.168.150.0 0.0.0.255



* Name: Teller

Description:

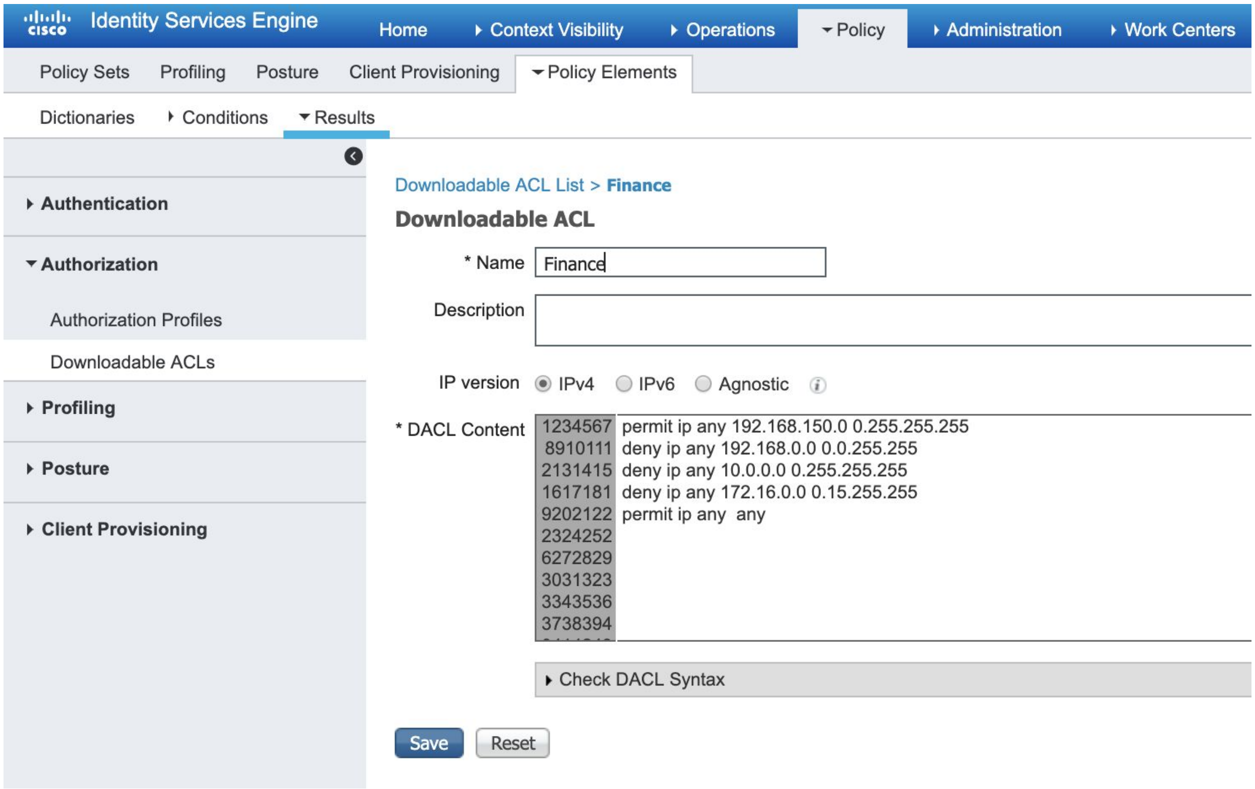
IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content:

```
permit ip any 192.168.150.0 0.0.0.255
```

Finance

This dACL allows Finance to get to the DC but no other RFC1918 space. Also allows internet access



Downloadable ACL

* Name: Finance

Description:

IP version: ● IPv4 ○ IPv6 ○ Agnostic

* DACL Content

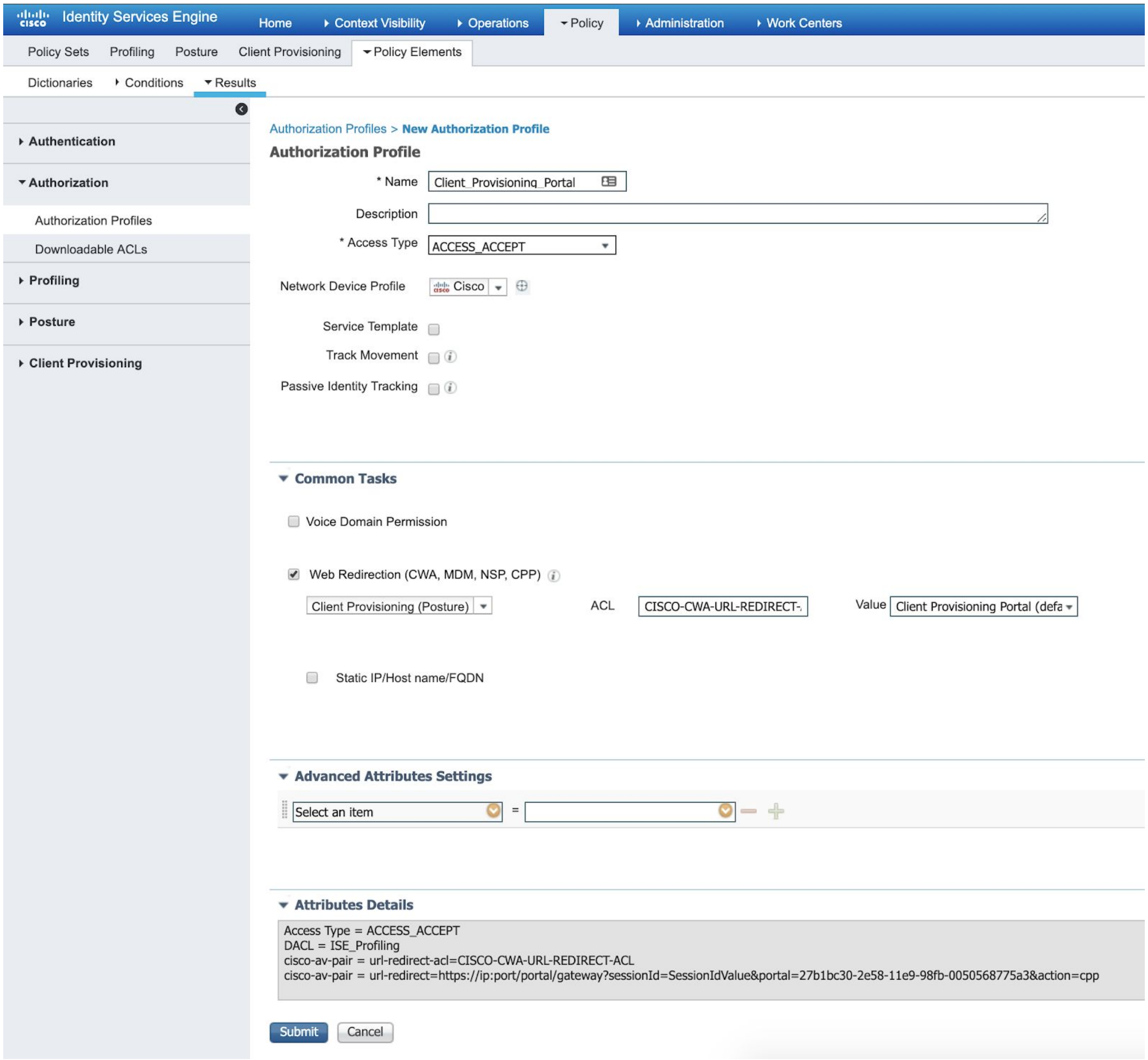
```
permit ip any 192.168.150.0 0.255.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
permit ip any  any
```

Authorization Profiles

To set the authorization profiles navigate to Policy--Policy Elements--Results--Authorization Profiles. Click Add

The Client Provisioning Portal Policy. This policy steers the session to the CPP portal. It also applies a dACL to the user and cites a named ACL for web redirection (that must live on the switch). That redirect ACL is listed here for completeness:

```
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL
 deny   ip any host 192.168.150.10
 deny   ip any host 192.168.150.50
 deny   udp any eq bootps any
 deny   udp any any eq bootpc
 deny   udp any eq bootpc any
 permit tcp any any eq www
```



Authorization Profile

* Name: Client_Provisioning_Portal

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

☐ Voice Domain Permission

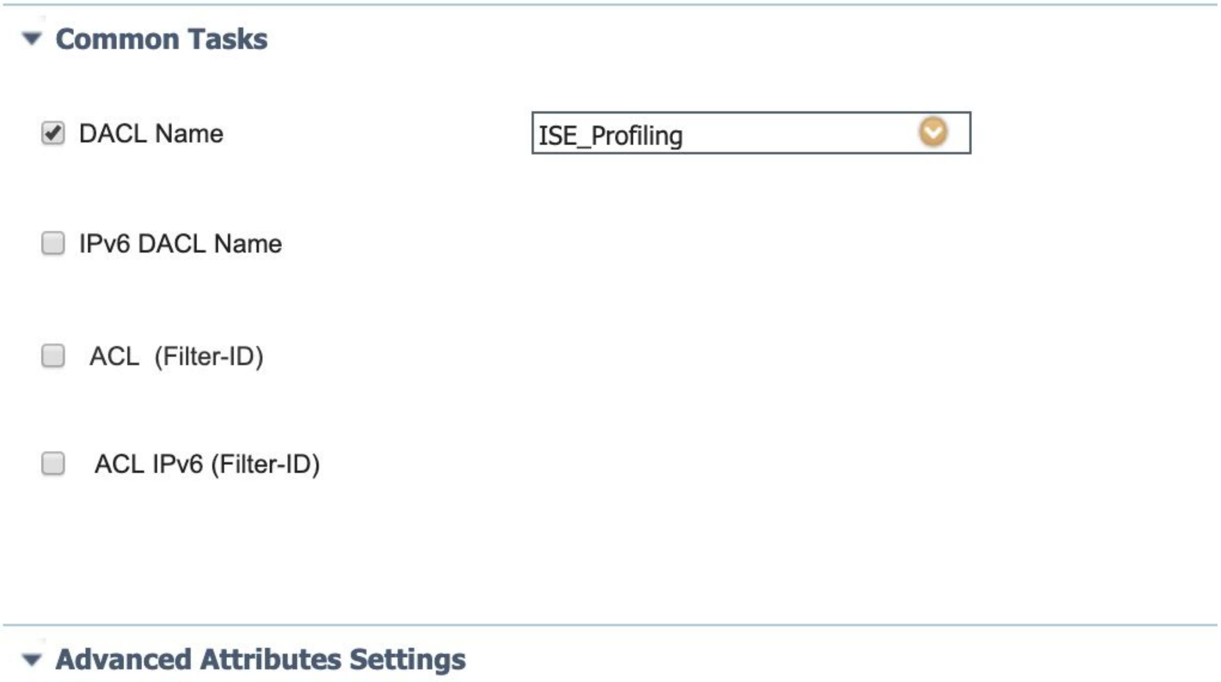
☑ Web Redirection (CWA, MDM, NSP, CPP)

Client Provisioning (Posture) ACL: CISCO-CWA-URL-REDIRECT-, Value: Client Provisioning Portal (defa

☐ Static IP/Host name/FQDN

Select an item =

```
Access Type = ACCESS_ACCEPT
DACL = ISE_Profiling
cisco-av-pair = url-redirect-acl=CISCO-CWA-URL-REDIRECT-ACL
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=27b1bc30-2e58-11e9-98fb-0050568775a3&action=cpp
```



Common Tasks

☑ DACL Name ISE_Profiling

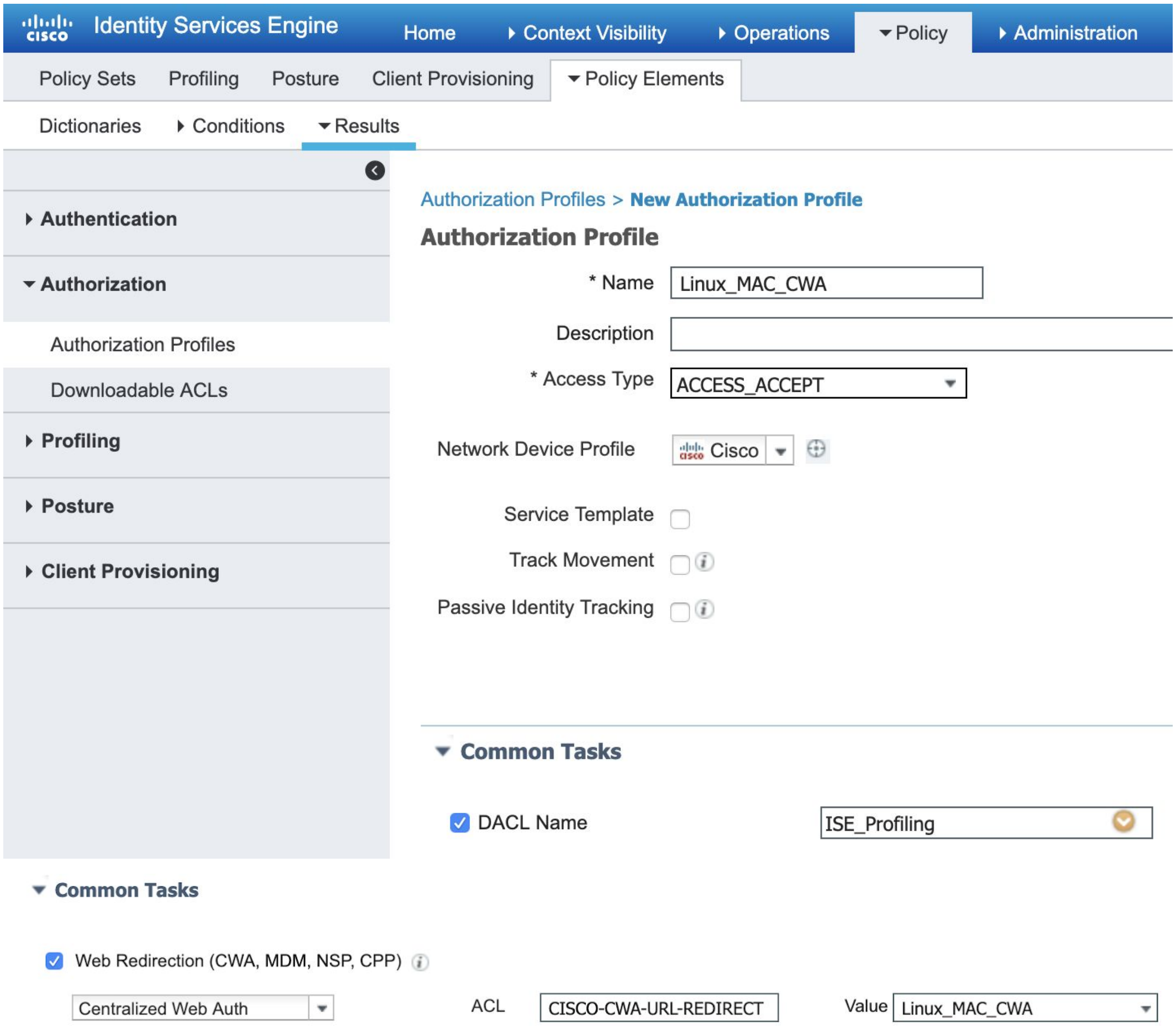
☐ IPv6 DACL Name

☐ ACL (Filter-ID)

☐ ACL IPv6 (Filter-ID)

Advanced Attributes Settings

Central Web Authentication policy for sending (approved) Linux workstations and MacOS endpoints in order to retrieve their AD credentials in order to gain access



Authorization Profiles > New Authorization Profile

Authorization Profile

* Name: Linux_MAC_CWA

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

Common Tasks

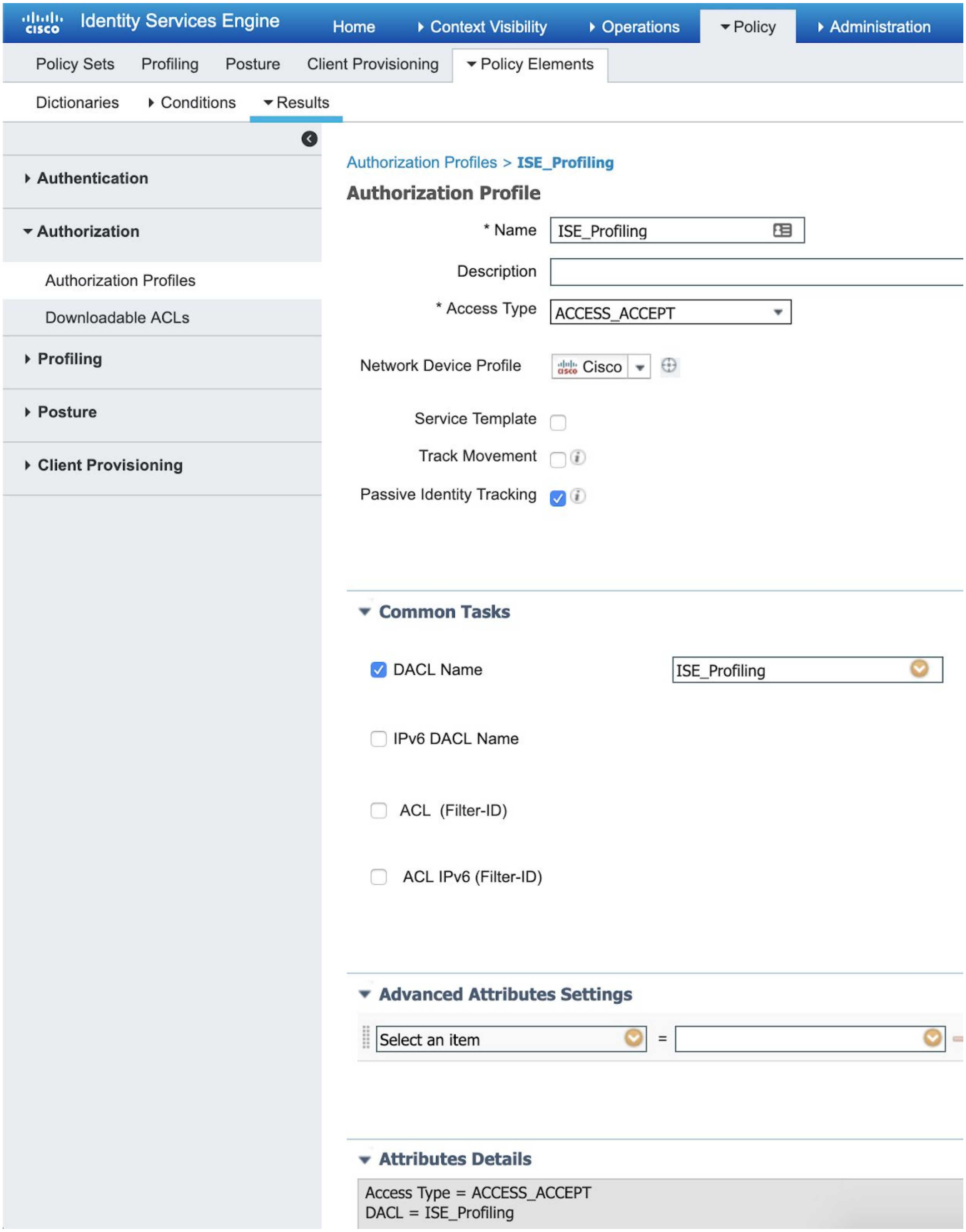
☑ DACL Name: ISE_Profiling

Common Tasks

☑ Web Redirection (CWA, MDM, NSP, CPP)

Centralized Web Auth — ACL: CISCO-CWA-URL-REDIRECT — Value: Linux_MAC_CWA

Profiling Policy, this will be a policy that grants limited access to the network while ISE inspects it.



Authorization Profiles > **ISE_Profiling**

Authorization Profile

* Name: ISE_Profiling

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☑

Common Tasks

☑ DACL Name: ISE_Profiling

☐ IPv6 DACL Name

☐ ACL (Filter-ID)

☐ ACL IPv6 (Filter-ID)

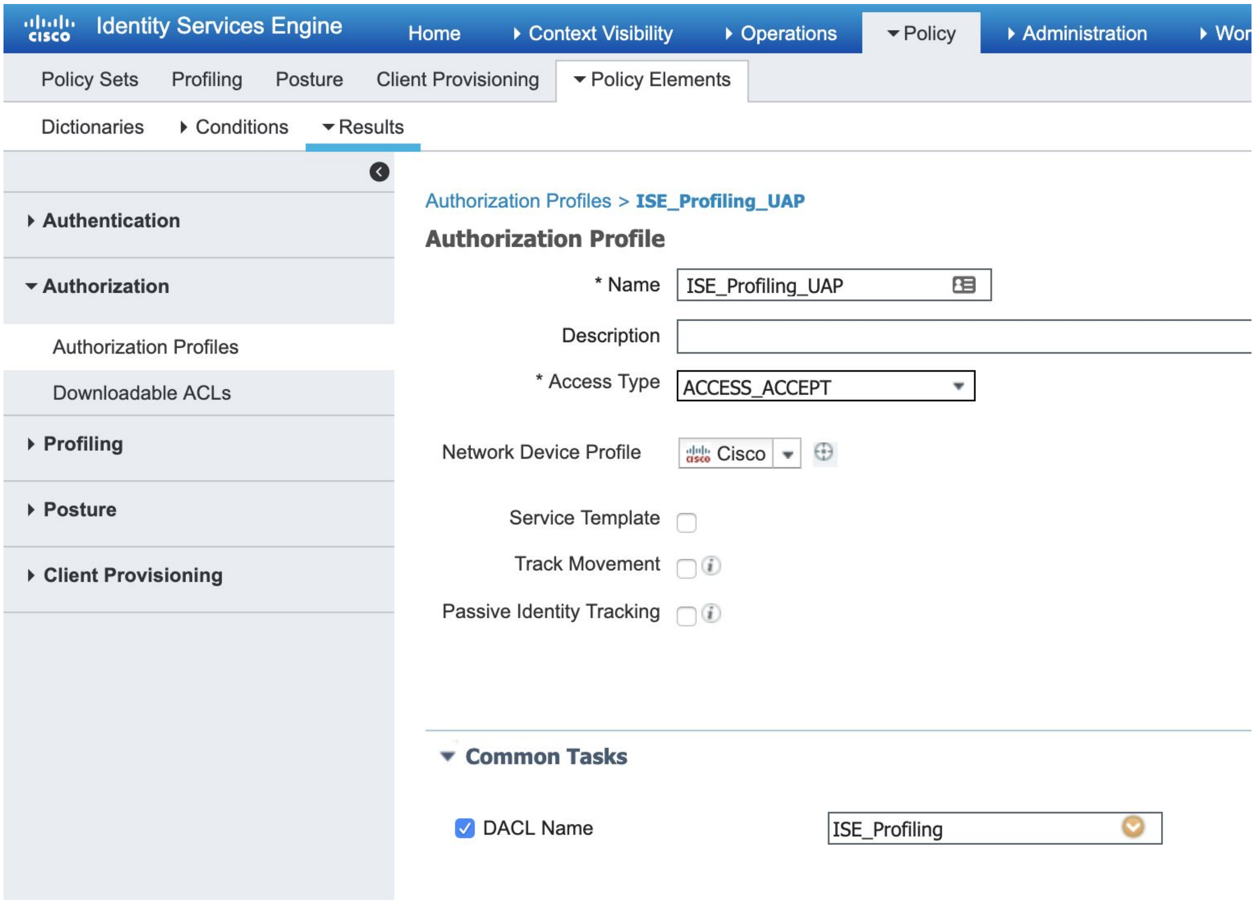
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = ISE_Profiling

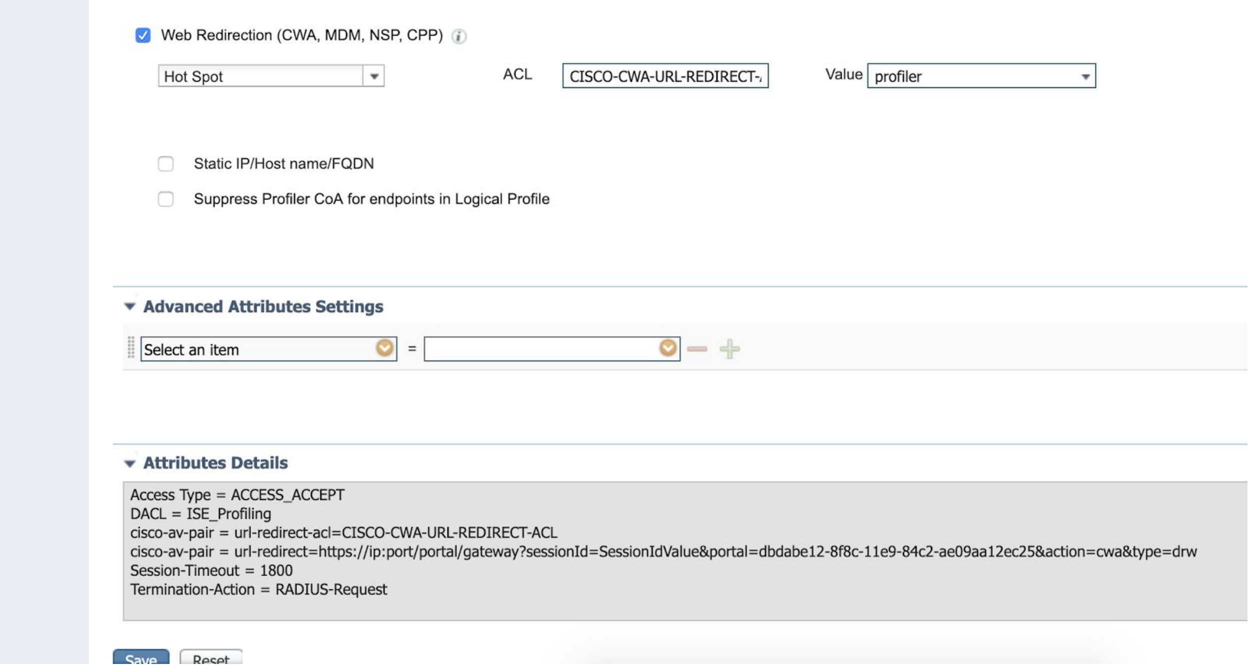
ISE Profiling Policy with User Acceptance Policy (basically the same as above but includes a Hot Spot Redirection so ISE can capture the user agent string if the endpoint is running a browser



Authorization Profile

* Name: ISE_Profiling_UAP
Description:
* Access Type: ACCESS_ACCEPT
Network Device Profile: Cisco
Service Template ☐
Track Movement ☐
Passive Identity Tracking ☐

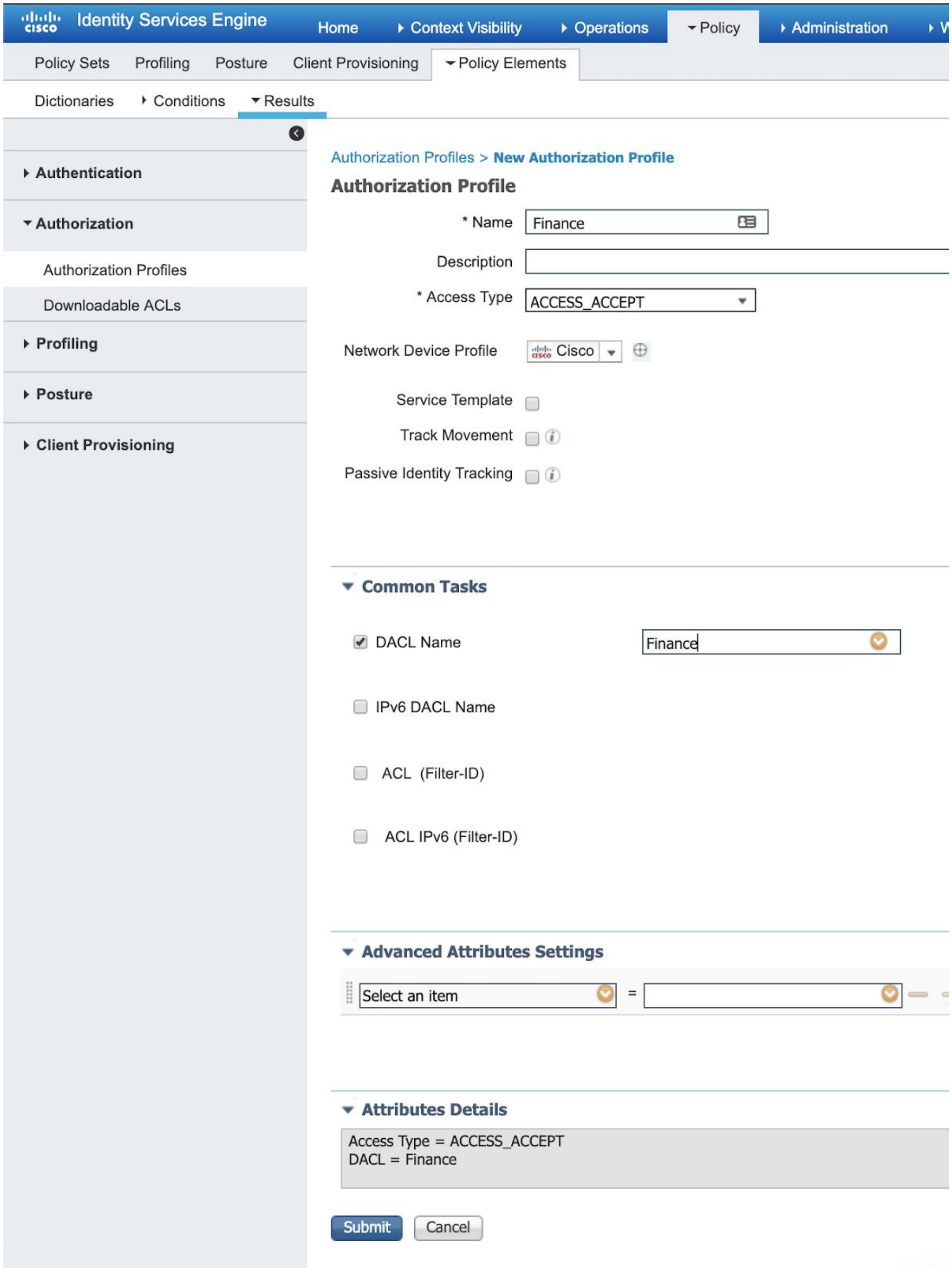
☑ DACL Name: ISE_Profiling



☑ Web Redirection (CWA, MDM, NSP, CPP)
Hot Spot — ACL: CISCO-CWA-URL-REDIRECT- — Value: profiler
☐ Static IP/Host name/FQDN
☐ Suppress Profiler CoA for endpoints in Logical Profile

```
Access Type = ACCESS_ACCEPT
DACL = ISE_Profiling
cisco-av-pair = url-redirect-acl=CISCO-CWA-URL-REDIRECT-ACL
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=dbdabe12-8f8c-11e9-84c2-ae09aa12ec25&action=cwa&type=drw
Session-Timeout = 1800
Termination-Action = RADIUS-Request
```

Finance Authorization Policy (for users that are in the Finance AD group)



Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name: Finance

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

Common Tasks

☑ DACL Name: Finance

☐ IPv6 DACL Name

☐ ACL (Filter-ID)

☐ ACL IPv6 (Filter-ID)

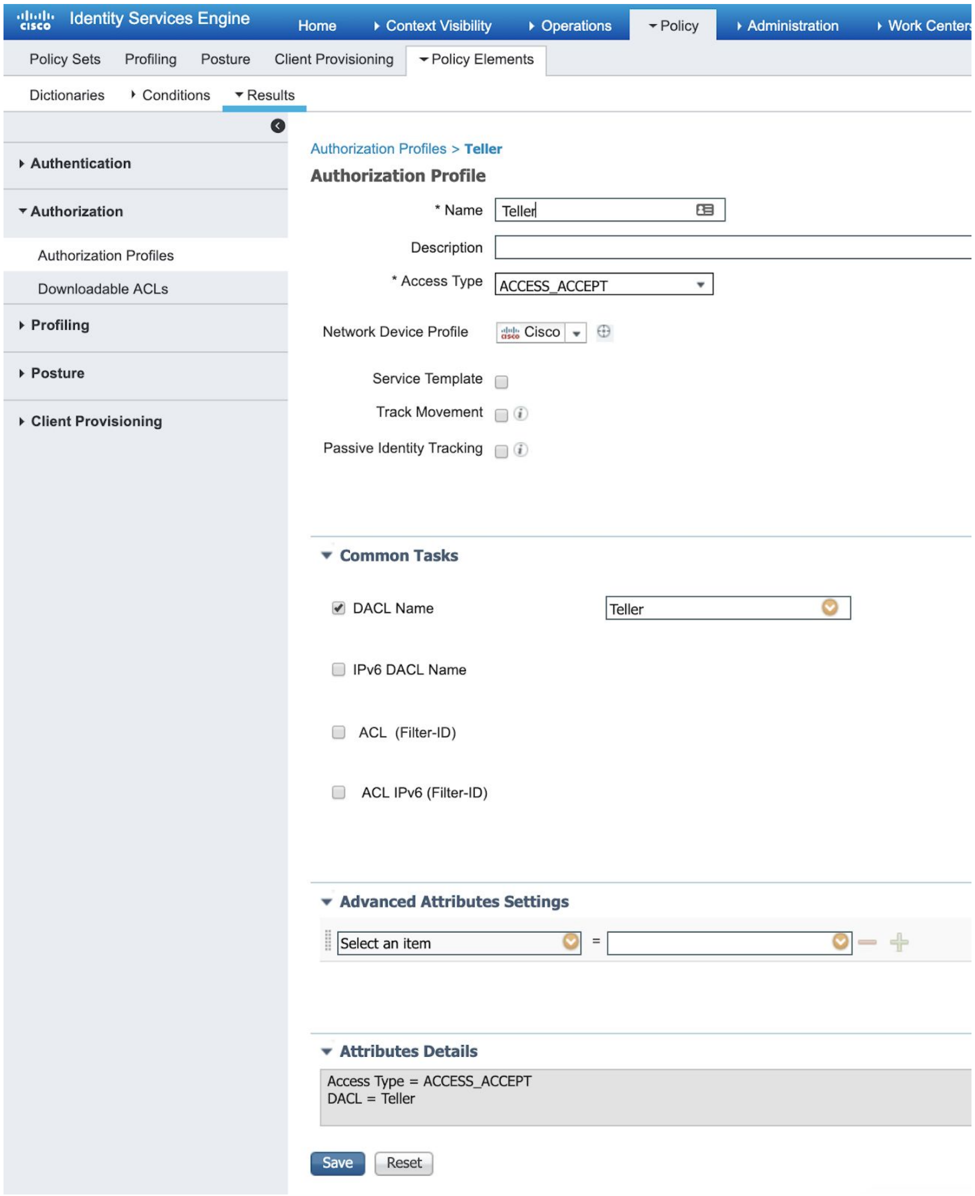
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = Finance

Teller Authorization Policy (for users that are in the Teller AD group)



Authorization Profiles > **Teller**

Authorization Profile

* Name: Teller

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

Common Tasks

☑ DACL Name: Teller

☐ IPv6 DACL Name

☐ ACL (Filter-ID)

☐ ACL IPv6 (Filter-ID)

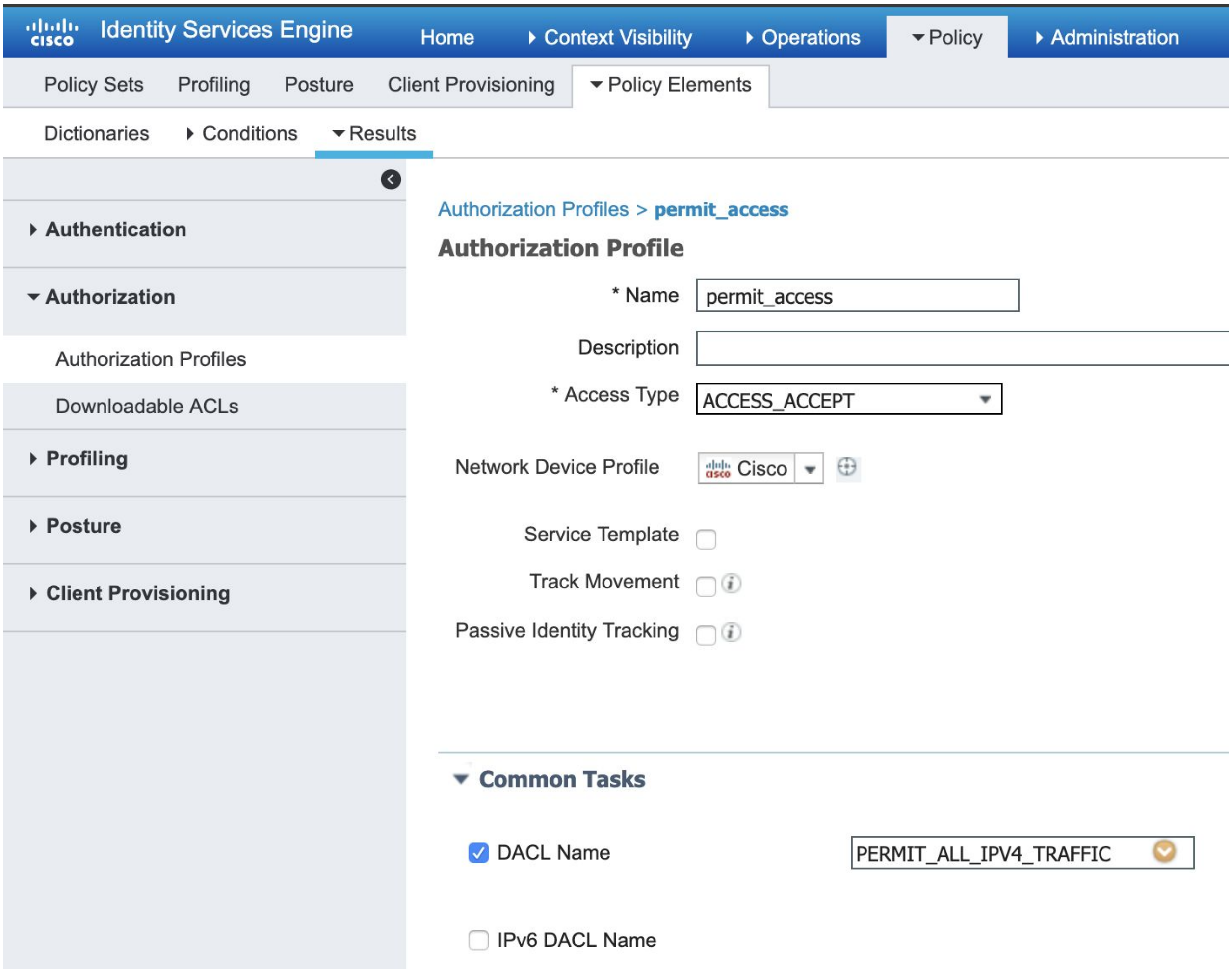
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = Teller

For Network Architects (or really anyone that needs full access) this policy will lay down a permit ip any any dACL



Authorization Profiles > **permit_access**

Authorization Profile

* Name: permit_access

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☐

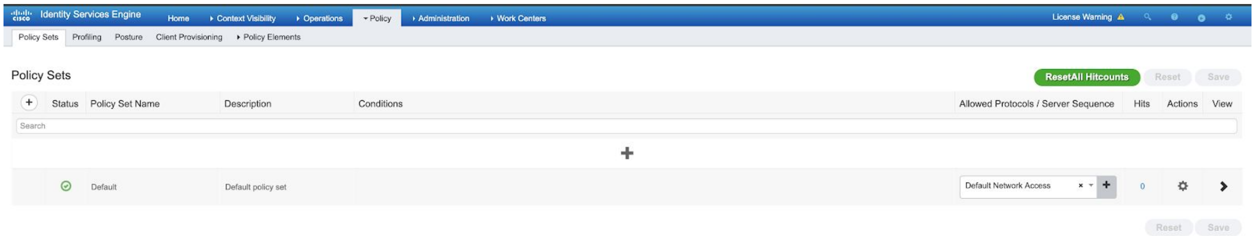
Common Tasks

☑ DACL Name: PERMIT_ALL_IPV4_TRAFFIC

☐ IPv6 DACL Name

Authentication Policy MAB

We will notably use the defaults whenever possible. Navigate to Policy--Policy Sets. It should look like this (the default):



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Default	Default policy set		Default Network Access	0		

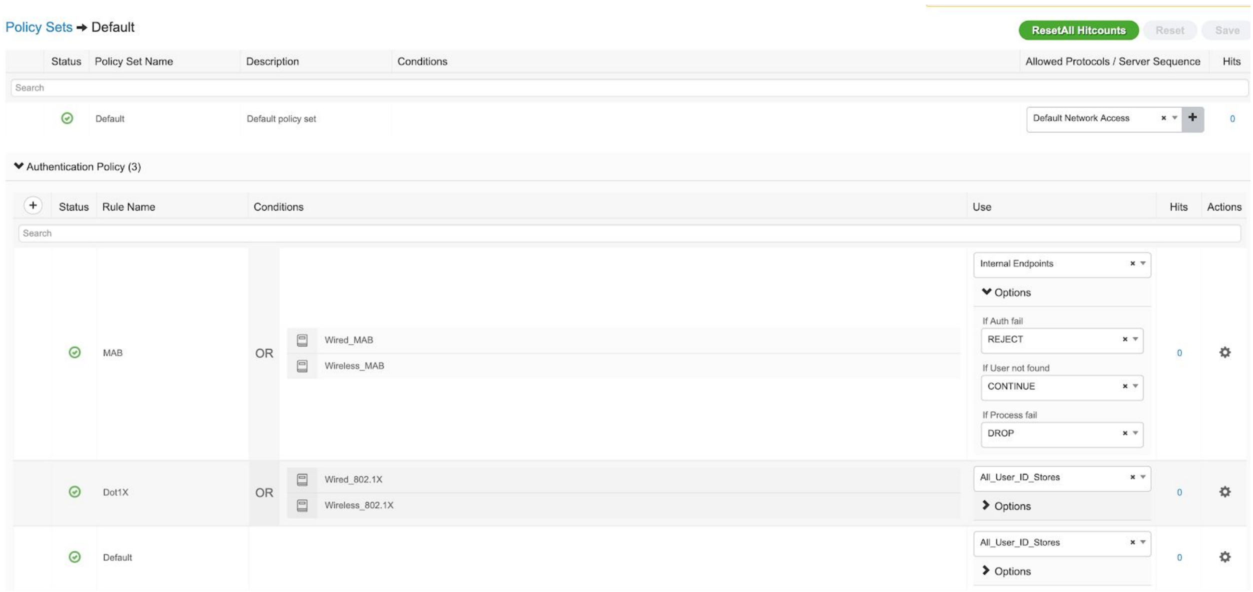
Profiling Authorization Rules

This use case is straight wired MAC Auth Bypass (MAB) and profiling. Simply stated there are only two Authorization rules:

if Windows OS (notably determined by DHCP/RADIUS/AD probes), only allow it access to AD infrastructure and to ISE for PassiveID (used in another use case).

If Anything else, only allow it access to AD/ISE but also provide it with a Hotspot captive portal in order to do HTTP User Agent detection and provide for an NMAP scan.

Slide into this Default Policy and it should look like this



Policy Sets → Default

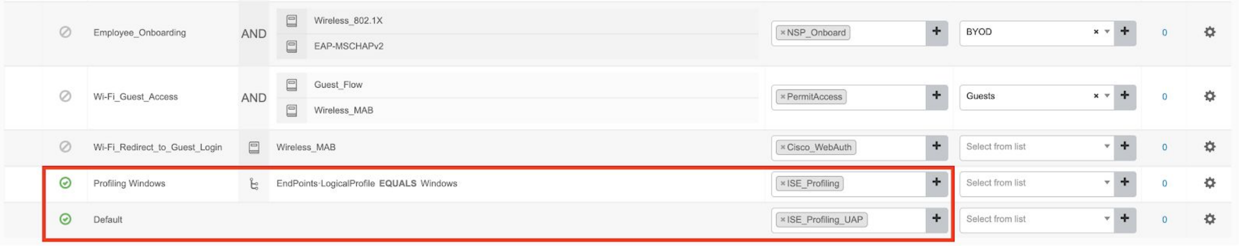
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	0

Authentication Policy (3)

Status	Rule Name		Conditions	Use	Hits	Actions
✓	MAB	OR	Wired_MAB Wireless_MAB	Internal Endpoints Options If Auth fail: REJECT If User not found: CONTINUE If Process fail: DROP	0	⚙
✓	Dot1X	OR	Wired_802.1X Wireless_802.1X	All_User_ID_Stores Options	0	⚙
✓	Default			All_User_ID_Stores Options	0	⚙

Expand the Authorization Policy section and there will be 12 built-in items.

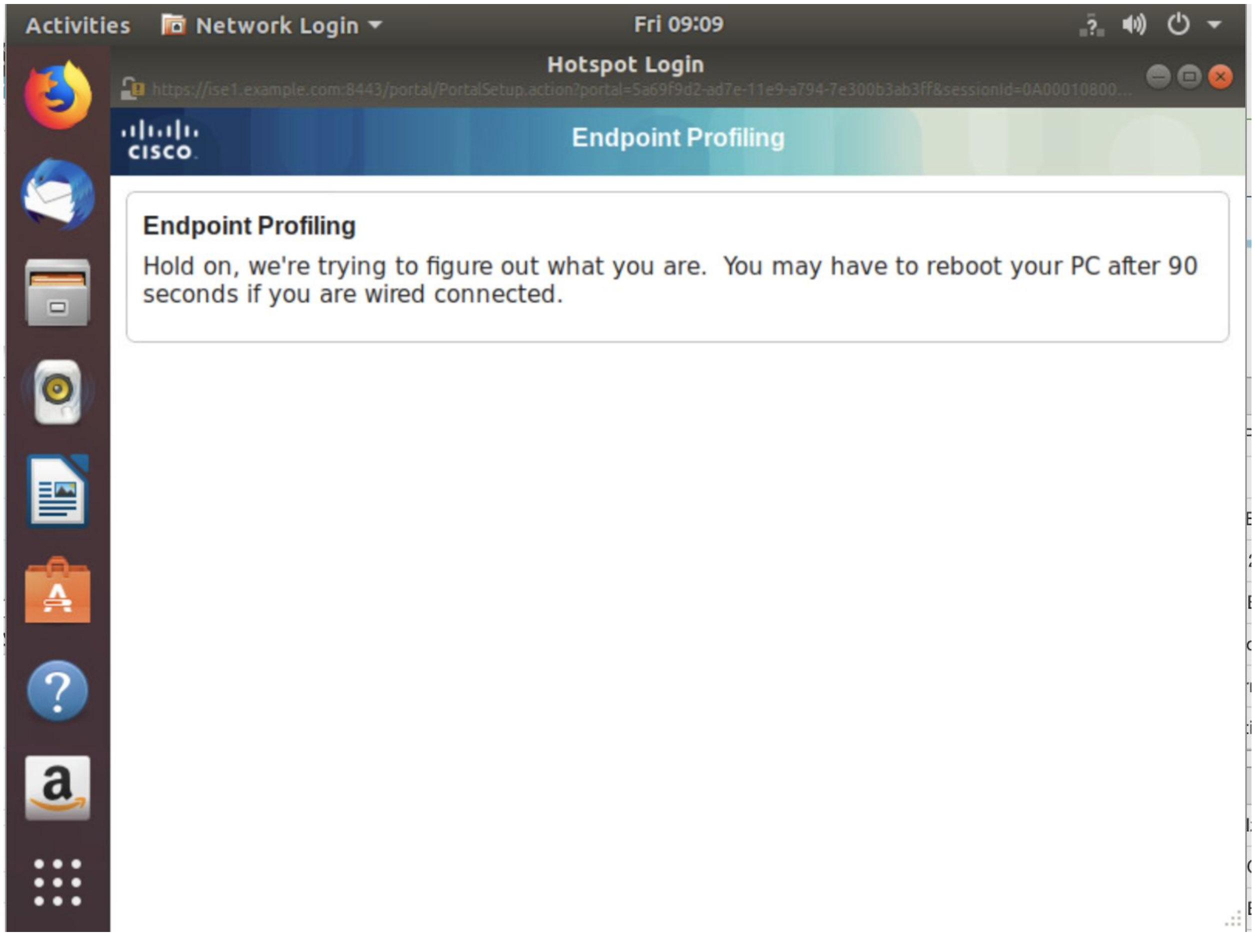
The item (next to the end) is “Basic_Authenticated_Access”. This is a catchall that will permit all access. We’ll change it (and the very last one named “Default”) so they will be *Authenticating* rules. It should look like this when finished:



⊘	Employee_Onboarding	AND	Wireless_802.1X EAP-MSCHAPv2	× NSP_Onboard	BYOD	0
⊘	Wi-Fi_Guest_Access	AND	Guest_Flow Wireless_MAB	× PermitAccess	Guests	0
⊘	Wi-Fi_Redirect_to_Guest_Login		Wireless_MAB	× Cisco_WebAuth	Select from list	0
✓	Profiling Windows		EndPoints·LogicalProfile **EQUALS** Windows	× ISE_Profiling	Select from list	0
✓	Default			× ISE_Profiling_UAP	Select from list	0

With this config not much access will be granted. Only phones and printers (the default rules) will be allowed. And any detected Windows workstations will only be able to communicate to AD (including DNS) and ISE. Non Windows workstations will be hit with a captive portal

For example:


Activities
Network Login
Fri 09:09
Hotspot Login
https://ise1.example.com:8443/portal/PortalSetup.action?portal=5a69f9d2-ad7e-11e9-a794-7e300b3ab3ff&sessionId=0A00010800...
cisco

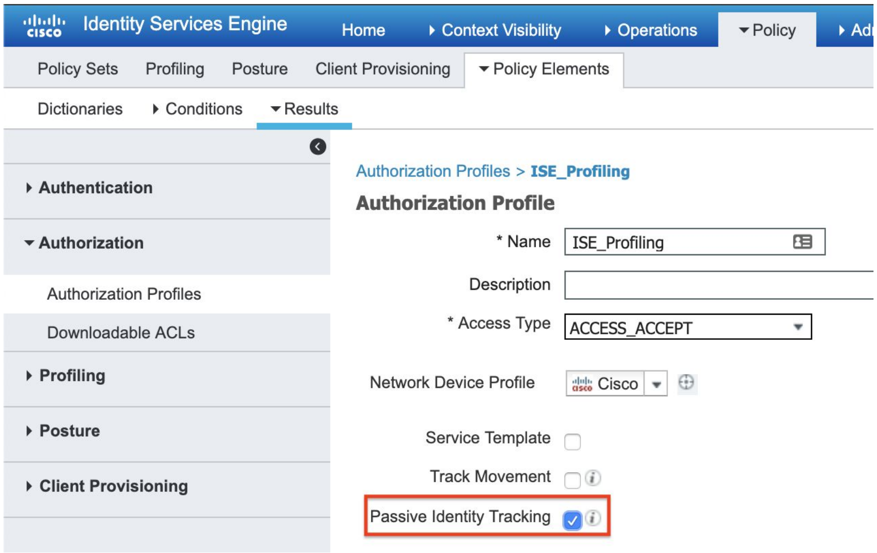
Endpoint Profiling

Endpoint Profiling

Hold on, we're trying to figure out what you are. You may have to reboot your PC after 90 seconds if you are wired connected.

Easy Connect Authorization

Now that we have Profiling at work, it’s just another couple of Authorization rules to put in Easy Connect identity AND segmentation. First housekeeping: we have to tell ISE that any endpoints that land on the ISE_Profiling (and ISE_Profiling_UAP for good measure) need to be checked against Windows AD for AD logons. Navigate to Policy--Policy Elements--Results--Authorization--Authorization Profiles. And edit those two like so:



Authorization Profiles > **ISE_Profiling**

Authorization Profile

* Name: ISE_Profiling

Description:

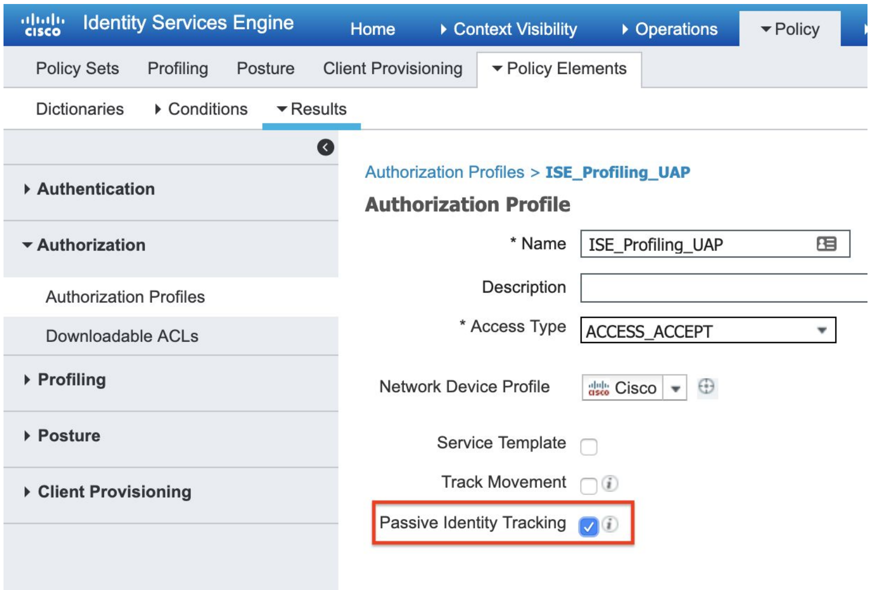
* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Passive Identity Tracking ☑



Authorization Profiles > **ISE_Profiling_UAP**

Authorization Profile

* Name: ISE_Profiling_UAP

Description:

* Access Type: ACCESS_ACCEPT

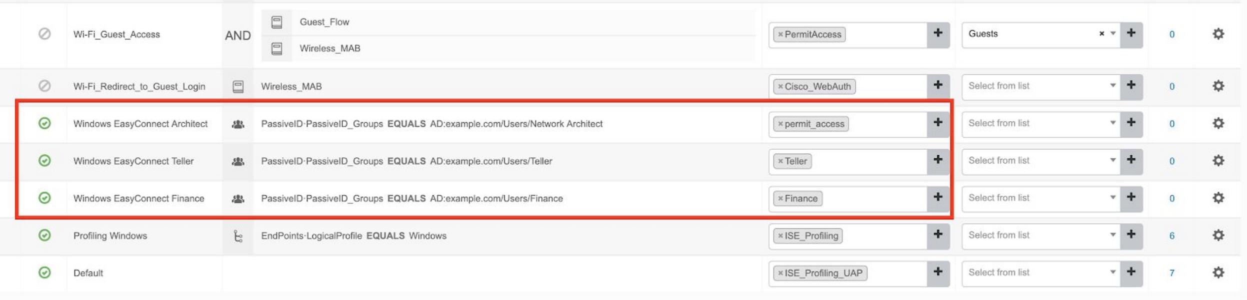
Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

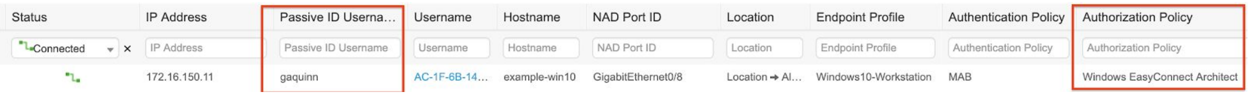
Passive Identity Tracking ☑

Now, we just need to add in new authorization rules that will send a unique dACL based on AD group membership:

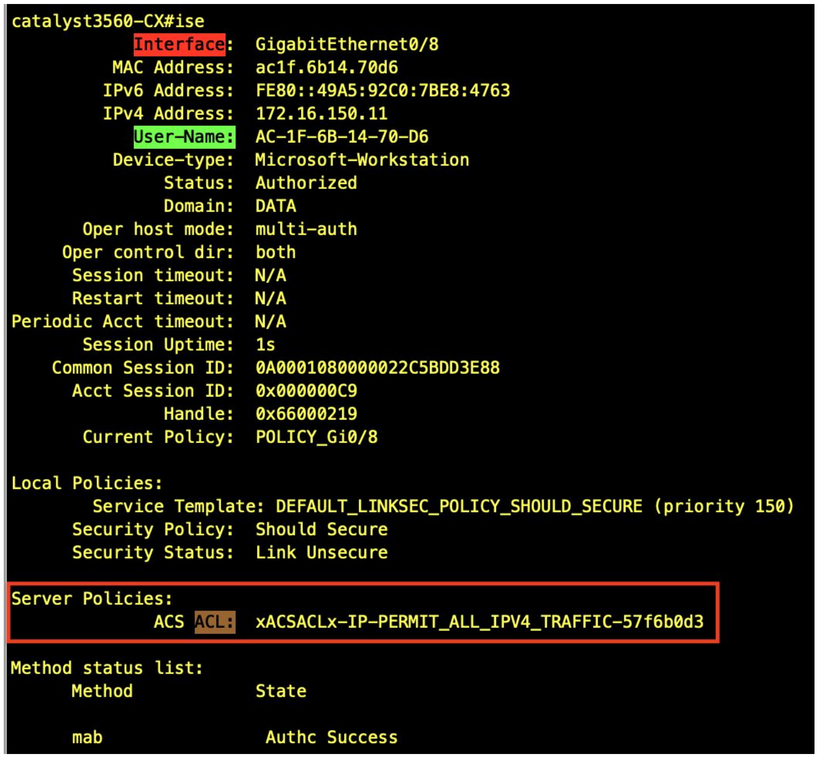


⊘	Wi-Fi_Guest_Access	AND	Guest_Flow Wireless_MAB	× PermitAccess	Guests	0	⚙
⊘	Wi-Fi_Redirect_to_Guest_Login		Wireless_MAB	× Cisco_WebAuth	Select from list	0	⚙
✓	Windows EasyConnect Architect		PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Network Architect	× permit_access	Select from list	0	⚙
✓	Windows EasyConnect Teller		PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Teller	× Teller	Select from list	0	⚙
✓	Windows EasyConnect Finance		PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Finance	× Finance	Select from list	0	⚙
✓	Profiling Windows		EndPoints·LogicalProfile **EQUALS** Windows	× ISE_Profiling	Select from list	6	⚙
✓	Default			× ISE_Profiling_UAP	Select from list	7	⚙

And that’s all. Some sample testing:

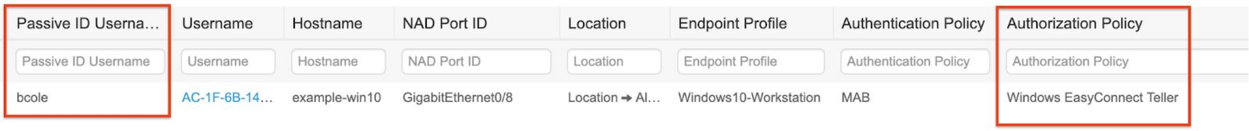


Status	IP Address	Passive ID Userna…	Username	Hostname	NAD Port ID	Location	Endpoint Profile	Authentication Policy	Authorization Policy
Connected	IP Address	Passive ID Username	Username	Hostname	NAD Port ID	Location	Endpoint Profile	Authentication Policy	Authorization Policy
	172.16.150.11	gaquinn	AC-1F-6B-14…	example-win10	GigabitEthernet0/8	Location ➔ Al…	Windows10-Workstation	MAB	Windows EasyConnect Architect

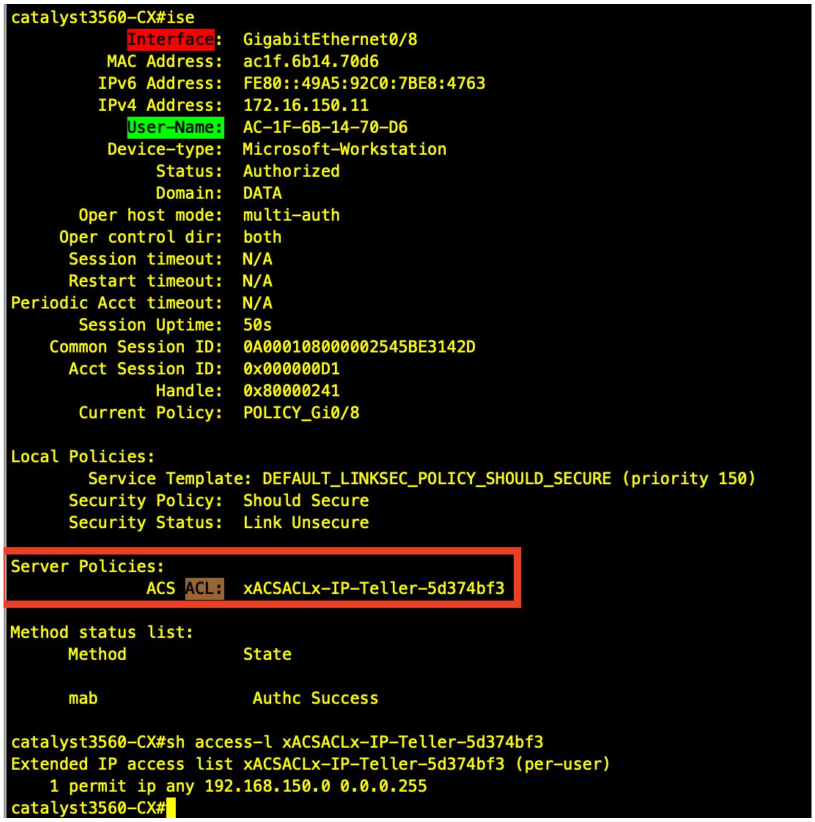


```
catalyst3560-CX#ise
            Interface:  GigabitEthernet0/8
          MAC Address:  ac1f.6b14.70d6
         IPv6 Address:  FE80::49A5:92C0:7BE8:4763
         IPv4 Address:  172.16.150.11
            User-Name:  AC-1F-6B-14-70-D6
          Device-type:  Microsoft-Workstation
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  1s
    Common Session ID:  0A0001080000022C5BDD3E88
      Acct Session ID:  0x000000C9
               Handle:  0x66000219
       Current Policy:  POLICY_Gi0/8

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
      Security Status:  Link Unsecure

Server Policies:
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

Method status list:
      Method            State

      mab                Authc Success
```

When Bob Cole logs in (same workstation) his permissions change to match his Teller role:



Passive ID Userna…	Username	Hostname	NAD Port ID	Location	Endpoint Profile	Authentication Policy	Authorization Policy
Passive ID Username	Username	Hostname	NAD Port ID	Location	Endpoint Profile	Authentication Policy	Authorization Policy
bcole	AC-1F-6B-14…	example-win10	GigabitEthernet0/8	Location ➔ Al…	Windows10-Workstation	MAB	Windows EasyConnect Teller



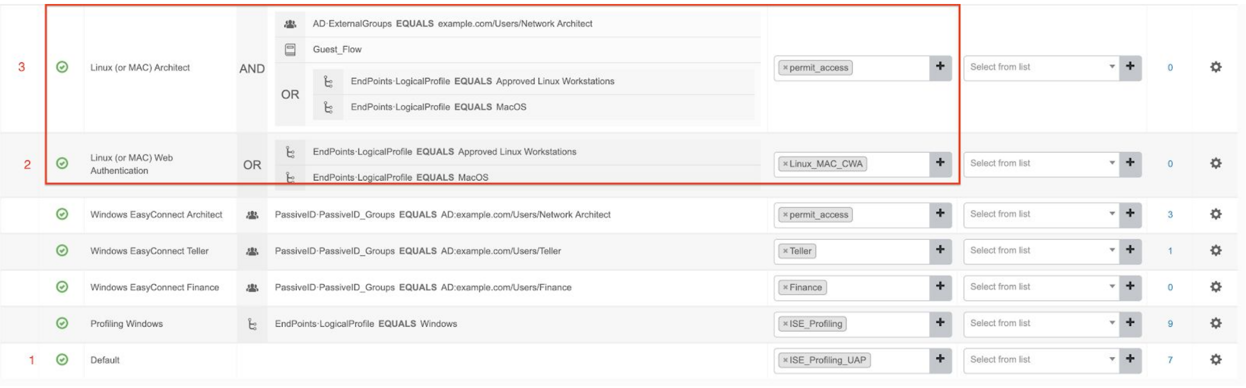
```
catalyst3560-CX#ise
            Interface:  GigabitEthernet0/8
          MAC Address:  ac1f.6b14.70d6
         IPv6 Address:  FE80::49A5:92C0:7BE8:4763
         IPv4 Address:  172.16.150.11
            User-Name:  AC-1F-6B-14-70-D6
          Device-type:  Microsoft-Workstation
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  N/A
       Session Uptime:  50s
    Common Session ID:  0A000108000002545BE3142D
      Acct Session ID:  0x000000D1
               Handle:  0x80000241
       Current Policy:  POLICY_Gi0/8

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
      Security Status:  Link Unsecure

Server Policies:
              ACS ACL:  xACSACLx-IP-Teller-5d374bf3

Method status list:
      Method            State

      mab                Authc Success

catalyst3560-CX#sh access-l xACSACLx-IP-Teller-5d374bf3
Extended IP access list xACSACLx-IP-Teller-5d374bf3 (per-user)
    1 permit ip any 192.168.150.0 0.0.0.255
catalyst3560-CX#
```

Ubuntu (and MAC) Connect Authorization

This one is pretty simple, just need to add in a few lines. At this point we've discovered corporate asset Linux. So now we present those endpoints with a captive portal to pass its AD credentials. Based on those creds we grant it access and push the relevant dACL. See the new rules (note we could also add in duplicates for Teller and Finance but are leaving it for just Architects because most likely those would be who would have that access).

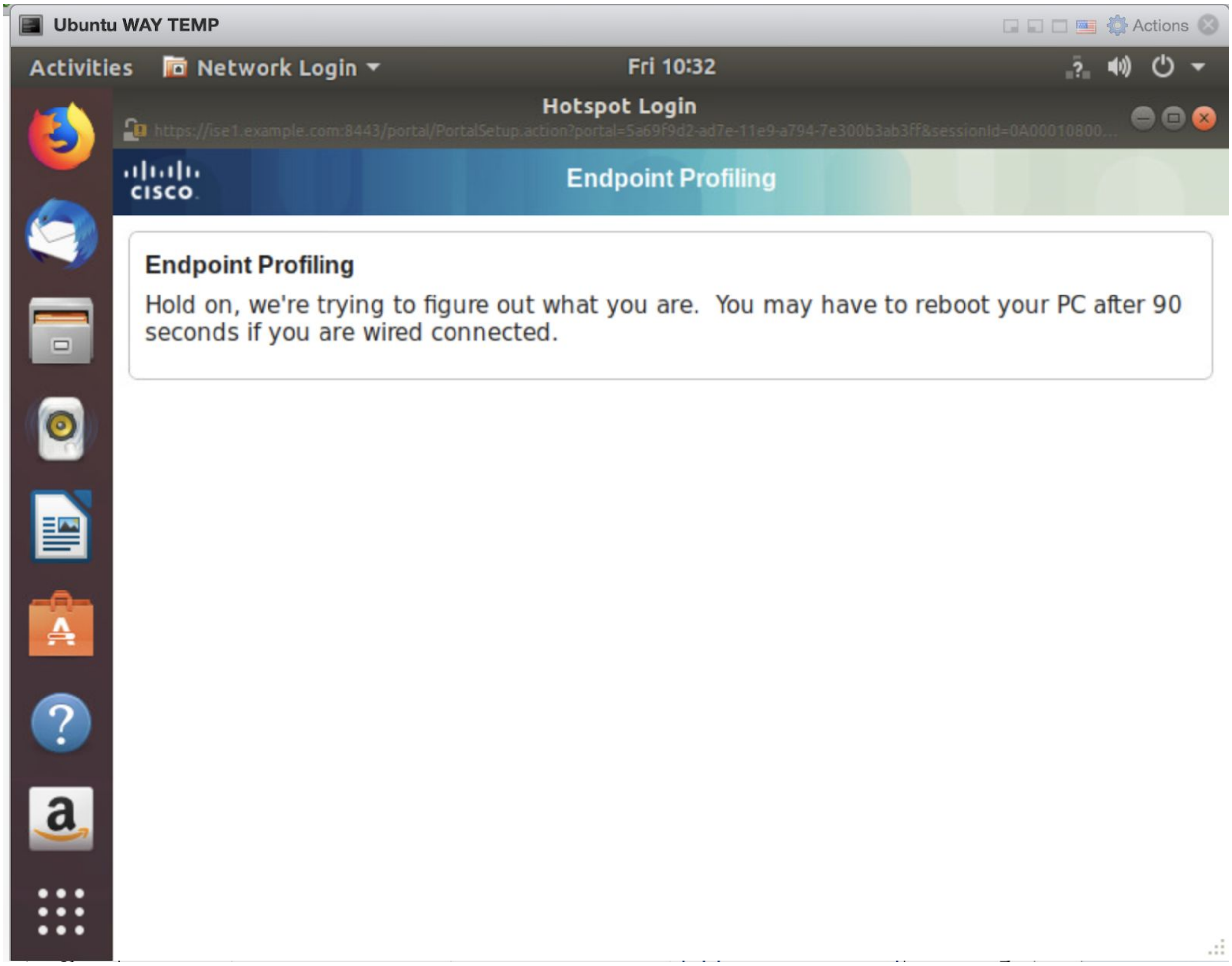
I number the steps the endpoint would take through this sequence:

1. Brand new endpoints would go to step 1 where we NMAP/SNMP scan and determine if it's a Corporate Linux workstation (or MacOS). This is only done for the very first time an endpoint is ever seen
2. This presents the Corporate Linux workstation or MacOS a Captive Portal to retrieve and authenticate their AD Credentials
3. This is where we send enforcements to the switchport if the Corp Linux/MacOS workstation if the user's account is in the Architect AD group. Note the 'guest_flow' qualifier, that is a built-in construct that basically says we won't apply this rule unless the session has been previously authenticated by a Captive Portal



3	✓	Linux (or MAC) Architect	AND	AD·ExternalGroups **EQUALS** example.com/Users/Network Architect Guest_Flow OR EndPoints·LogicalProfile **EQUALS** Approved Linux Workstations EndPoints·LogicalProfile **EQUALS** MacOS	× permit_access	Select from list	0	⚙
2	✓	Linux (or MAC) Web Authentication	OR	EndPoints·LogicalProfile **EQUALS** Approved Linux Workstations EndPoints·LogicalProfile **EQUALS** MacOS	× Linux_MAC_CWA	Select from list	0	⚙
	✓	Windows EasyConnect Architect		PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Network Architect	× permit_access	Select from list	3	⚙
	✓	Windows EasyConnect Teller		PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Teller	× Teller	Select from list	1	⚙
	✓	Windows EasyConnect Finance		PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Finance	× Finance	Select from list	0	⚙
	✓	Profiling Windows		EndPoints·LogicalProfile **EQUALS** Windows	× ISE_Profiling	Select from list	9	⚙
1	✓	Default			× ISE_Profiling_UAP	Select from list	7	⚙

From the client's perspective it would look like the following. Note that the text shown to the user (along with branding and color schemes) are customizable. Also it is possible to have ISE immediately CoA reauth this first step when we determine this is a Corporate Linux endpoint. But decided to keep it simpler for this. And even those measurements would not work if the endpoint is hardwired behind an IP Phone.



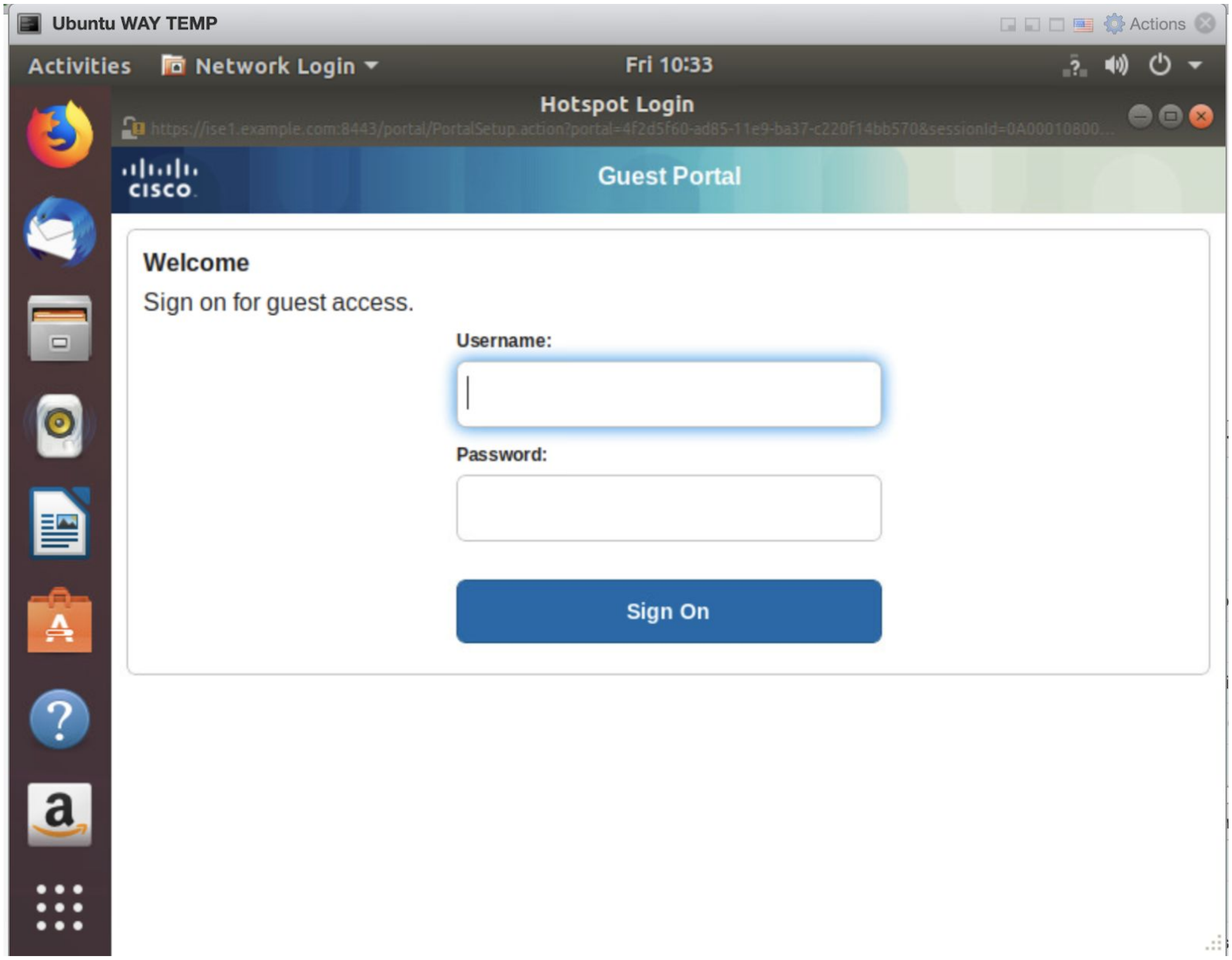
Hotspot Login

https://ise1.example.com:8443/portal/PortalSetup.action?portal=5a69f9d2-ad7e-11e9-a794-7e300b3ab3ff&sessionId=0A00010800...

Endpoint Profiling

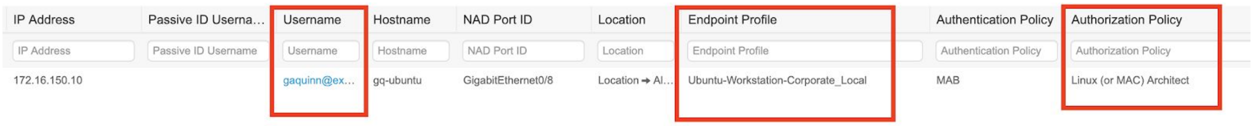
Endpoint Profiling

Hold on, we're trying to figure out what you are. You may have to reboot your PC after 90 seconds if you are wired connected.


Ubuntu WAY TEMP
Actions
Activities
Network Login
Fri 10:33
Hotspot Login
https://ise1.example.com:8443/portal/PortalSetup.action?portal=4f2d5f60-ad85-11e9-ba37-c220f14bb570&sessionId=0A00010800...
Guest Portal
Username:
Password:
Sign On

Welcome

Sign on for guest access.

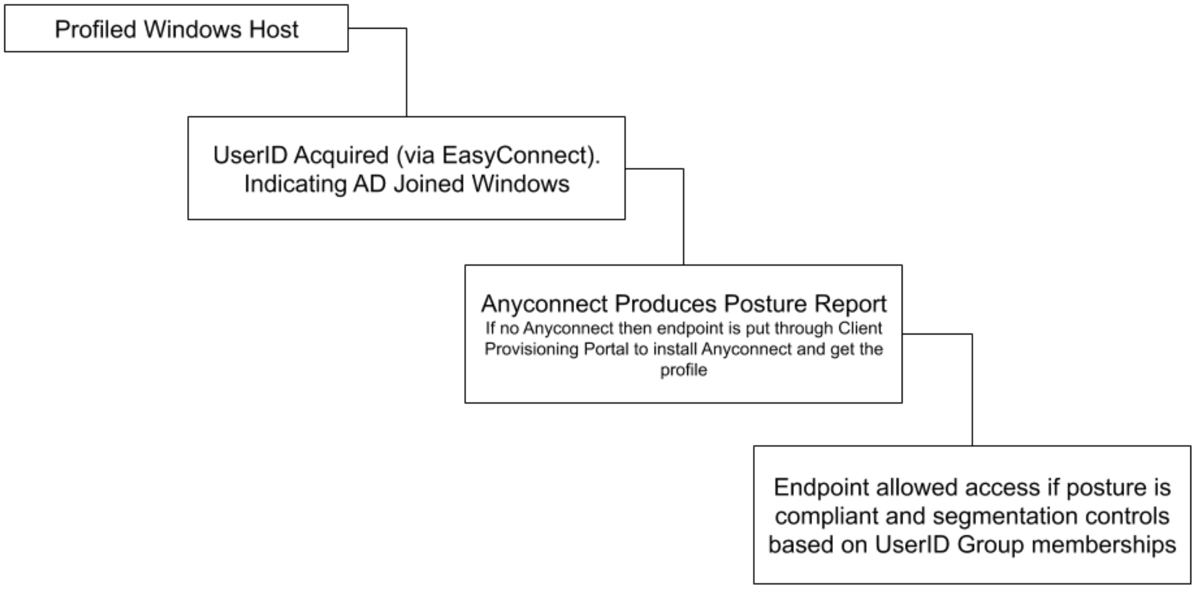


IP Address	Passive ID Userna…	Username	Hostname	NAD Port ID	Location	Endpoint Profile	Authentication Policy	Authorization Policy
IP Address	Passive ID Username	Username	Hostname	NAD Port ID	Location	Endpoint Profile	Authentication Policy	Authorization Policy
172.16.150.10		gaquinn@ex…	gq-ubuntu	GigabitEthernet0/8	Location ➔ Al…	Ubuntu-Workstation-Corporate_Local	MAB	Linux (or MAC) Architect

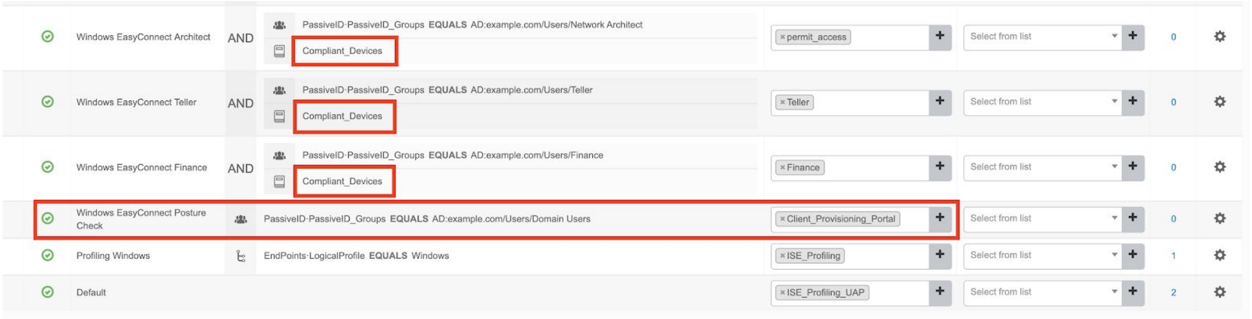
This same flow would work fine for MacOS. And you can further disaggregate the policy to say only admins and developers can use Linux workstations and only Marketing and C-Suites use MacOS for an example.

Posture

Now we'll stitch in Posture checking. We'll use a very narrow use case of Windows (though MacOS can easily be added with that flow and will be screenshotted for reference). The "waterfall" flow is illustrated here. The first two blocks already exist per the config at this point and the constructs for the last two also exist, we just need to get it in policy.


Profiled Windows Host
UserID Acquired (via EasyConnect). Indicating AD Joined Windows
Anyconnect Produces Posture Report
If no Anyconnect then endpoint is put through Client Provisioning Portal to install Anyconnect and get the profile
Endpoint allowed access if posture is compliant and segmentation controls based on UserID Group memberships

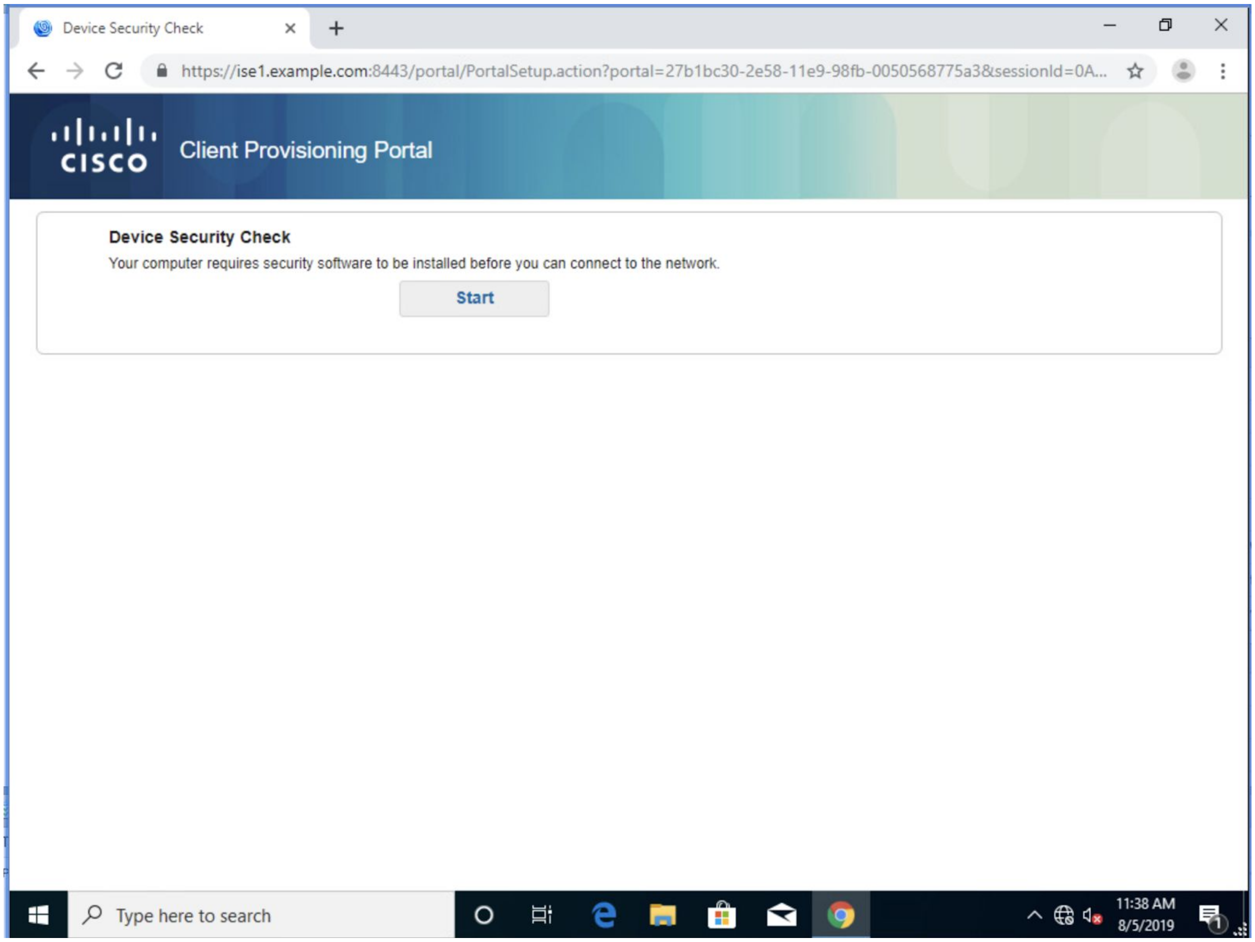
The new policy steps listed here (and should be available for you at this point in the guide if you've built these blocks from previous steps):



✓	Windows EasyConnect Architect	AND	PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Network Architect Compliant_Devices	× permit_access	Select from list	0
✓	Windows EasyConnect Teller	AND	PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Teller Compliant_Devices	× Teller	Select from list	0
✓	Windows EasyConnect Finance	AND	PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Finance Compliant_Devices	× Finance	Select from list	0
✓	Windows EasyConnect Posture Check		PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Domain Users	× Client_Provisioning_Portal	Select from list	0
✓	Profiling Windows		EndPoints·LogicalProfile **EQUALS** Windows	× ISE_Profiling	Select from list	1
✓	Default			× ISE_Profiling_UAP	Select from list	2

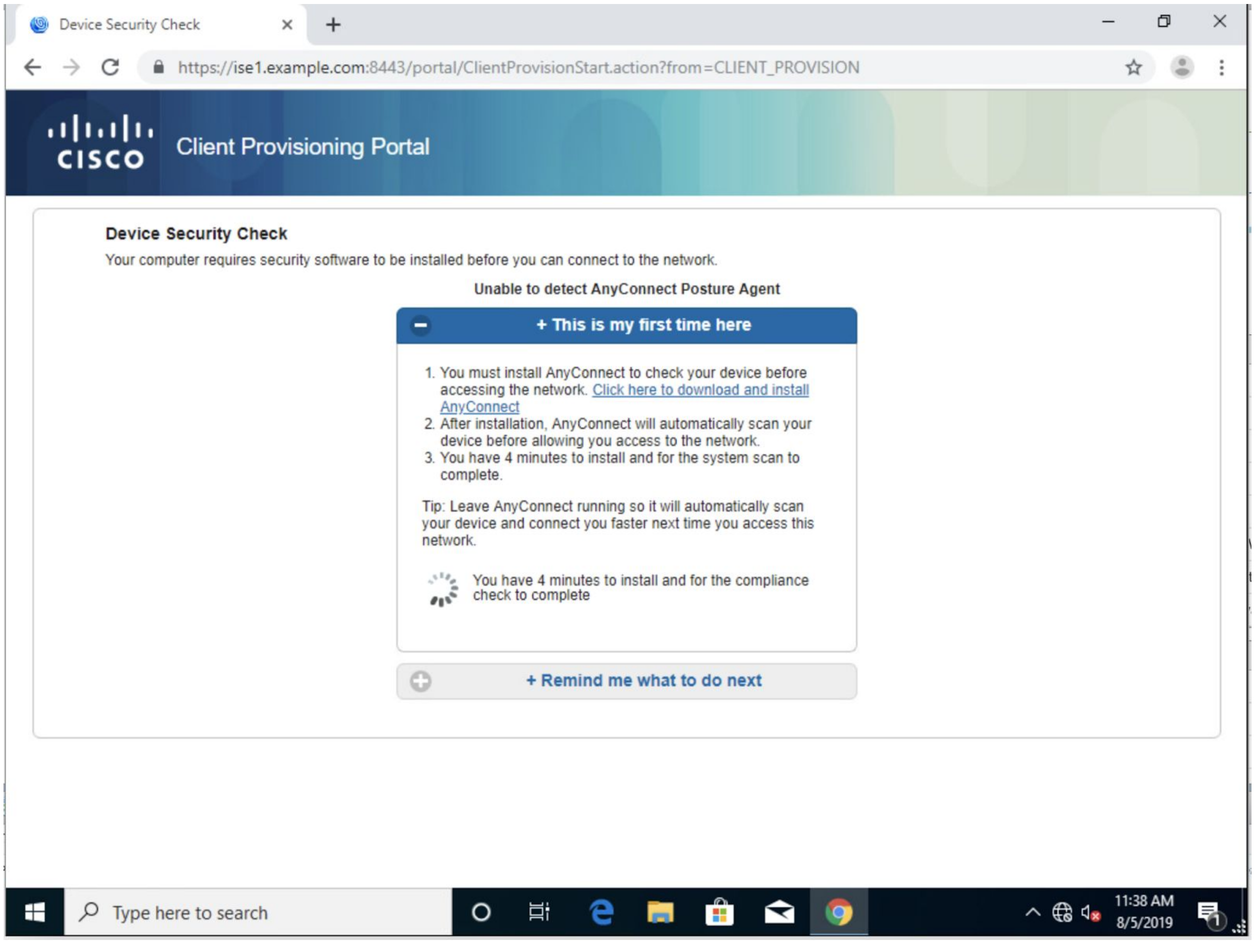
So what does look like for an end-user's perspective? Let's see for a brand new AD Joined computer that has not been seen and does not have Anyconnect software.

First step is user is redirected to the captive portal where they'll be pushed to download and install Anyconnect Client, illustrated here. Note that client would most likely be deployed through software distribution channels like SCCM but can be deployed (and updated) this way. Also note that the smartscreen notice is illustrating that the endpoint cannot reach Microsoft over the Internet and can be taken out of the end-user visibility but is left here for information.


Device Security Check
https://ise1.example.com:8443/portal/PortalSetup.action?portal=27b1bc30-2e58-11e9-98fb-0050568775a3&sessionId=0A...
cisco
Client Provisioning Portal
Start
Type here to search
11:38 AM
8/5/2019

Device Security Check

Your computer requires security software to be installed before you can connect to the network.


Device Security Check
https://ise1.example.com:8443/portal/ClientProvisionStart.action?from=CLIENT_PROVISION
cisco
Client Provisioning Portal
Type here to search
11:38 AM
8/5/2019

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect AnyConnect Posture Agent

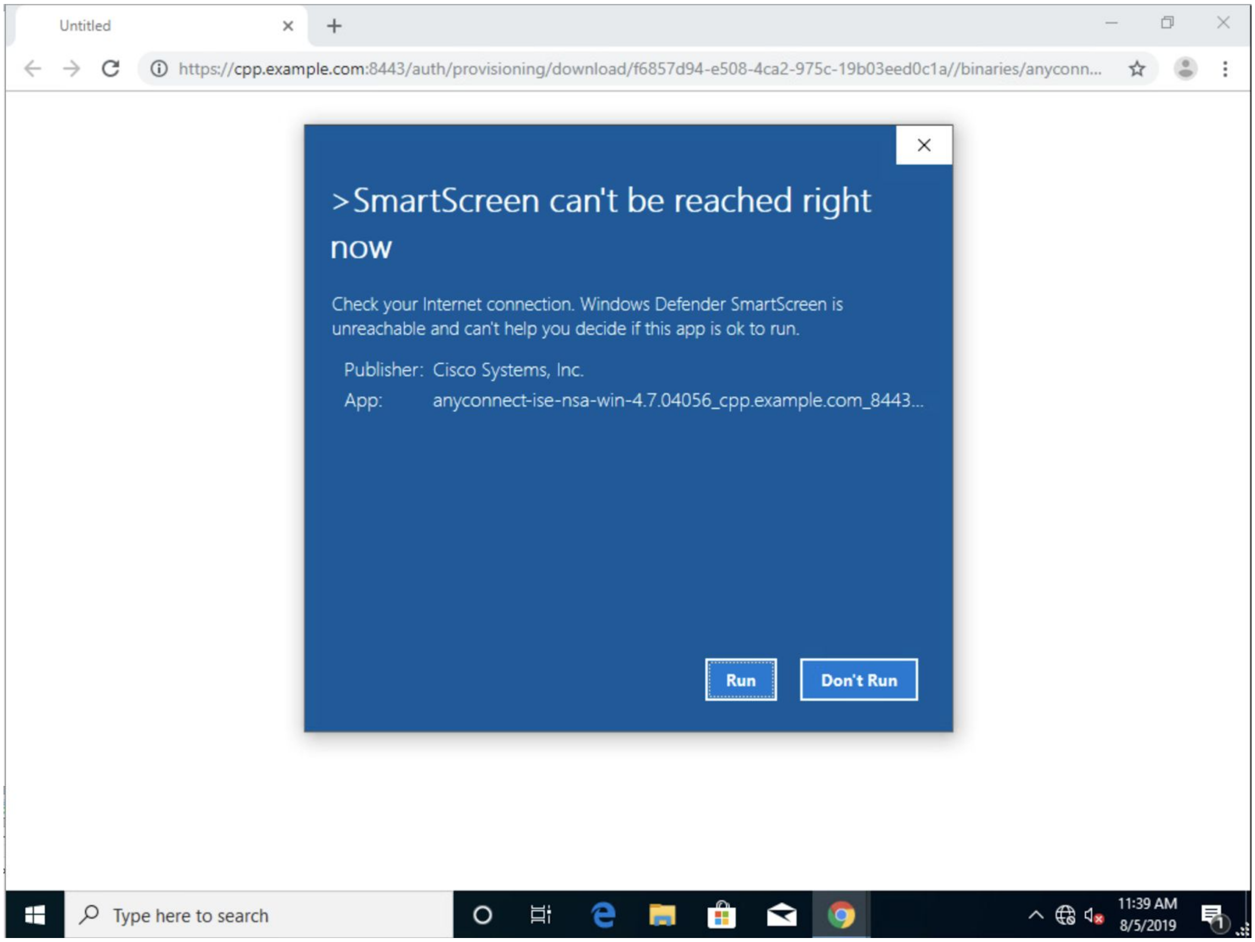
+ This is my first time here

1. You must install AnyConnect to check your device before accessing the network. Click here to download and install AnyConnect
2. After installation, AnyConnect will automatically scan your device before allowing you access to the network.
3. You have 4 minutes to install and for the system scan to complete.

Tip: Leave AnyConnect running so it will automatically scan your device and connect you faster next time you access this network.

You have 4 minutes to install and for the compliance check to complete

+ Remind me what to do next

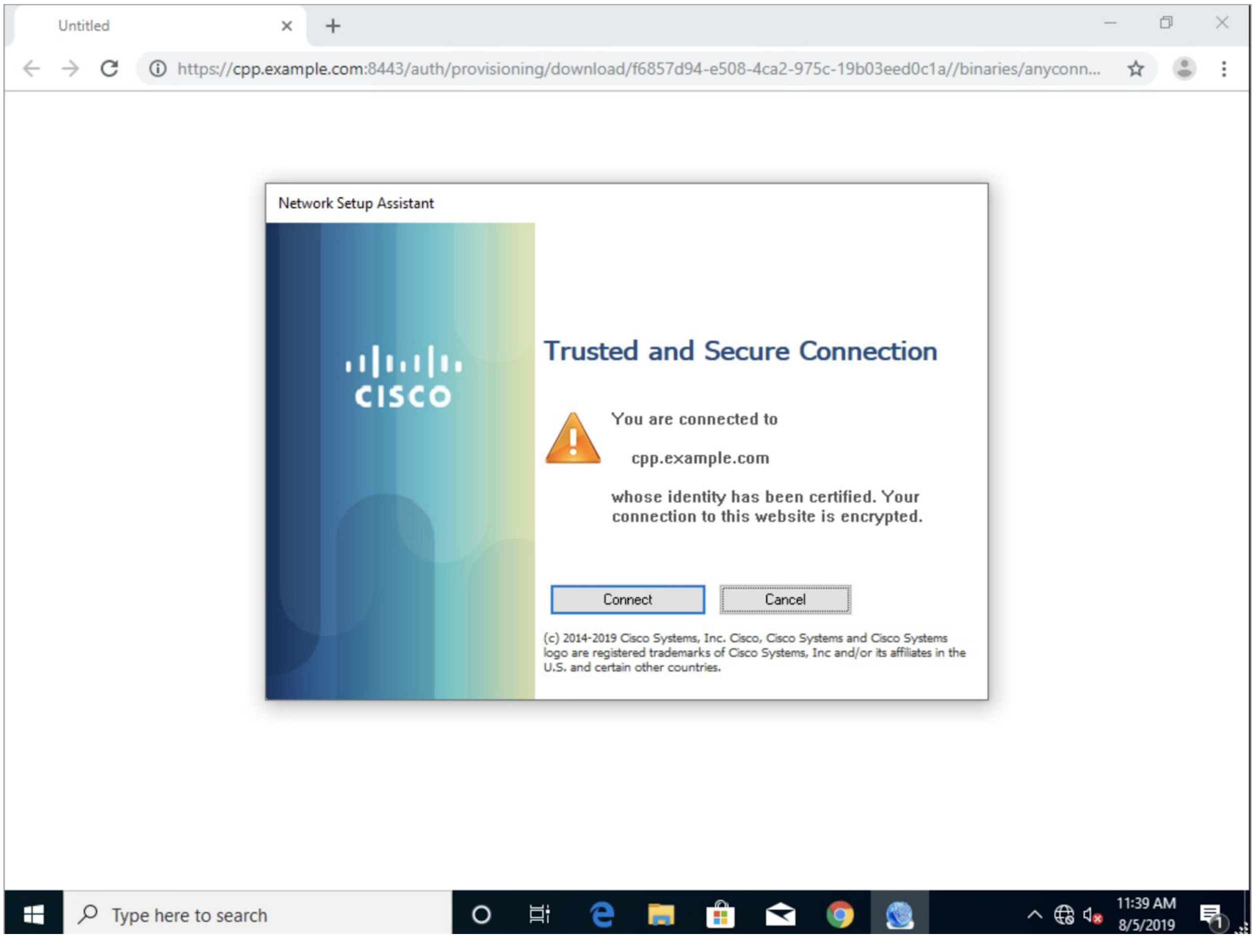


https://cpp.example.com:8443/auth/provisioning/download/f6857d94-e508-4ca2-975c-19b03eed0c1a//binaries/anyconn...

>SmartScreen can't be reached right now

Check your Internet connection. Windows Defender SmartScreen is unreachable and can't help you decide if this app is ok to run.

Publisher: Cisco Systems, Inc.
App: anyconnect-ise-nsa-win-4.7.04056_cpp.example.com_8443...



https://cpp.example.com:8443/auth/provisioning/download/f6857d94-e508-4ca2-975c-19b03eed0c1a//binaries/anyconn...

Trusted and Secure Connection

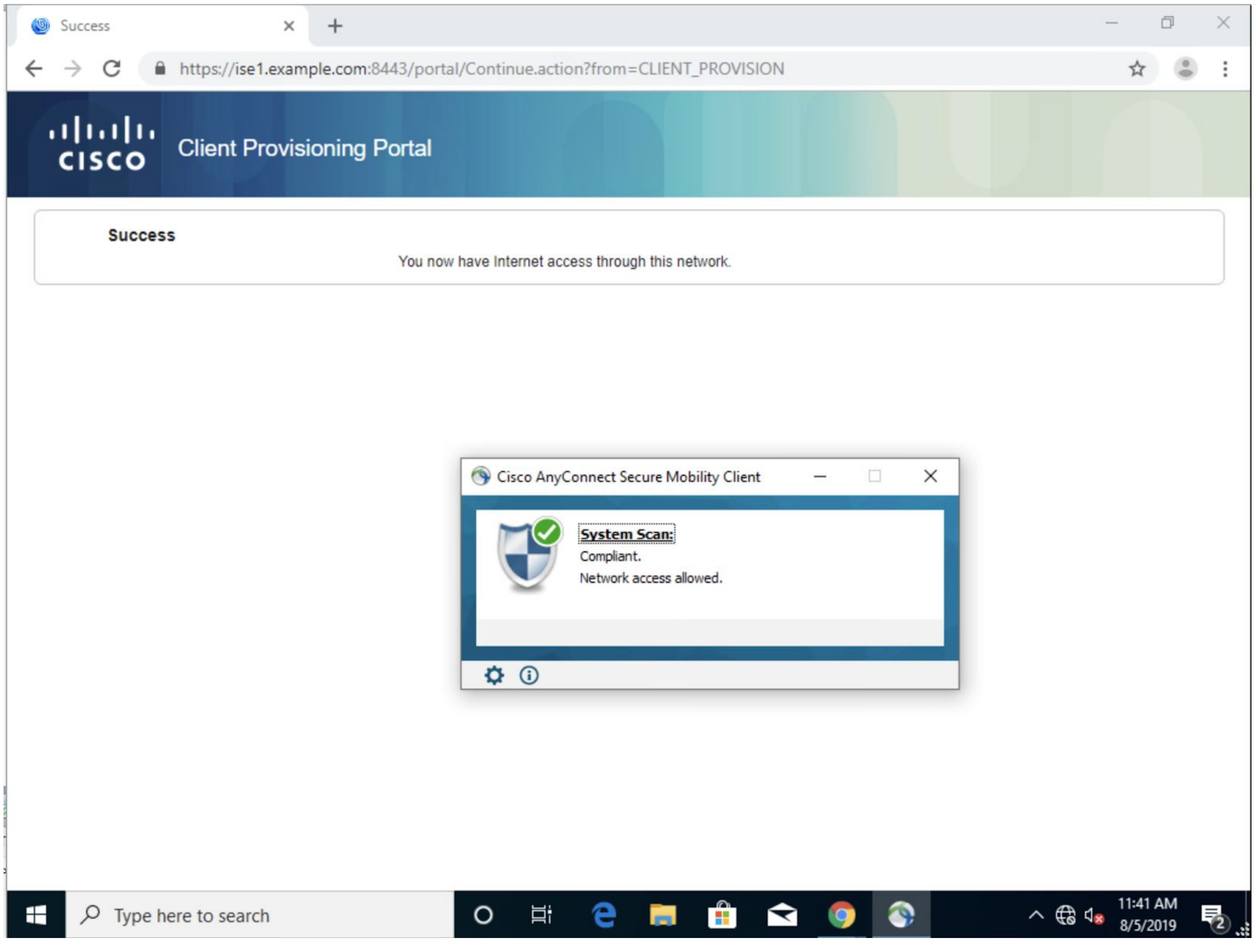
You are connected to

cpp.example.com

whose identity has been certified. Your connection to this website is encrypted.

(c) 2014-2019 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

Note that Windows is showing lack of Internet access (the system tray indication beside the speaker icon); which is fitting since Bob Cole's role does not have Internet access, only limited internal access. This notification can be disabled in Windows GPO.


Success
https://ise1.example.com:8443/portal/Continue.action?from=CLIENT_PROVISION
CISCO
Client Provisioning Portal
Type here to search
11:41 AM
8/5/2019

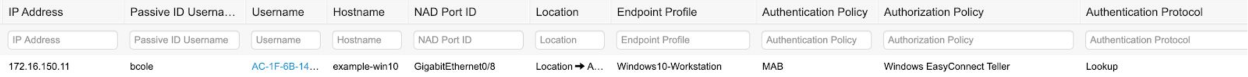
Success

You now have Internet access through this network.

Cisco AnyConnect Secure Mobility Client

System Scan:
Compliant.
Network access allowed.

And the view for ISE is below:

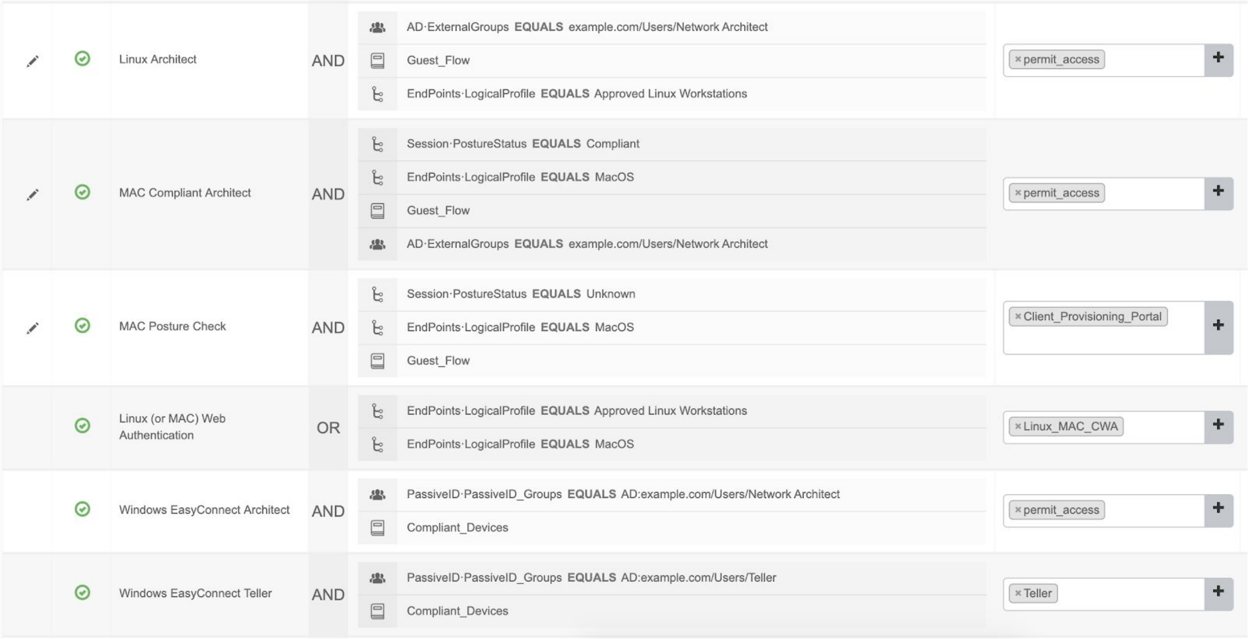


IP Address	Passive ID Userna…	Username	Hostname	NAD Port ID	Location	Endpoint Profile	Authentication Policy	Authorization Policy	Authentication Protocol
IP Address	Passive ID Username	Username	Hostname	NAD Port ID	Location	Endpoint Profile	Authentication Policy	Authorization Policy	Authentication Protocol
172.16.150.11	bcole	AC-1F-6B-14…	example-win10	GigabitEthernet0/8	Location ➔ A…	Windows10-Workstation	MAB	Windows EasyConnect Teller	Lookup

And the posture report for this endpoint

PostureAgentVersion	AnyConnect Posture Agent for Windows 4.7.04056
PostureApplicable	Yes
PostureAssessmentStatus	NotApplicable
PostureOS	Windows 10 Professional 64-bit
PostureReport	Default_Firewall_Policy_Win\;Passed\;(Default_Firewall_Requirement_Win:Mandatory:Passed:Passed_Conditions[fw_enabled_v4_fw_ANY_ANY_ANY]:Failed_Conditions[]:Skipped_Conditions[]), Default_AntiMalware_Policy_Win\;Passed\;(Any_AM_Installation_Win:Mandatory:Passed:Passed_Conditions[am_inst_v4_ANY_vendor]:Failed_Conditions[]:Skipped_Conditions[])
PostureStatus	Compliant

Bonus Credit: this is what it looks like for MacOS Captive Portal and Anyconnect Posture (splitting out MAC and Linux policies from above, it will work just fine)

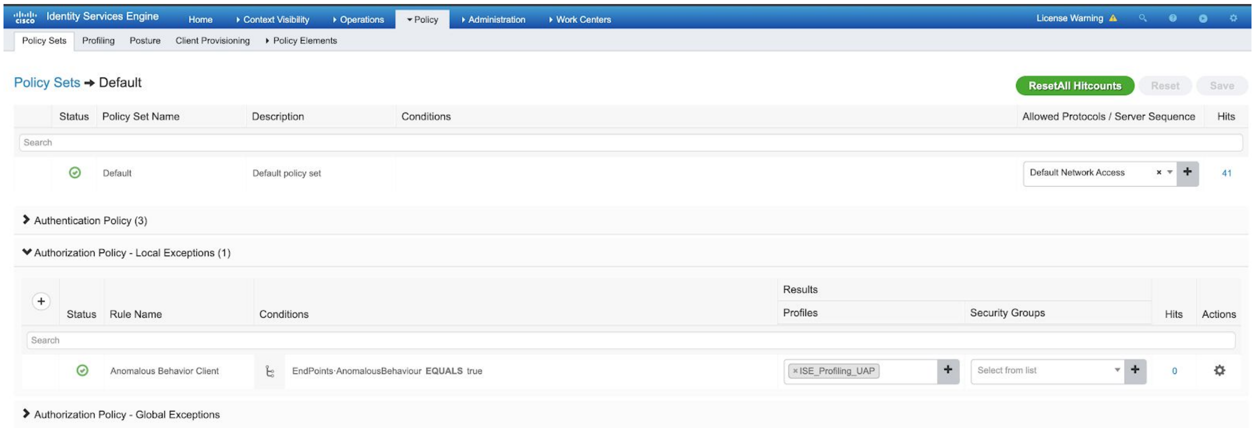


Rule Name		Conditions	Profiles
Linux Architect	AND	AD·ExternalGroups **EQUALS** example.com/Users/Network Architect Guest_Flow EndPoints·LogicalProfile **EQUALS** Approved Linux Workstations	permit_access
MAC Compliant Architect	AND	Session·PostureStatus **EQUALS** Compliant EndPoints·LogicalProfile **EQUALS** MacOS Guest_Flow AD·ExternalGroups **EQUALS** example.com/Users/Network Architect	permit_access
MAC Posture Check	AND	Session·PostureStatus **EQUALS** Unknown EndPoints·LogicalProfile **EQUALS** MacOS Guest_Flow	Client_Provisioning_Portal
Linux (or MAC) Web Authentication	OR	EndPoints·LogicalProfile **EQUALS** Approved Linux Workstations EndPoints·LogicalProfile **EQUALS** MacOS	Linux_MAC_CWA
Windows EasyConnect Architect	AND	PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Network Architect Compliant_Devices	permit_access
Windows EasyConnect Teller	AND	PassiveID·PassiveID_Groups **EQUALS** AD:example.com/Users/Teller Compliant_Devices	Teller

Anomalous Behavior Detection

Probably the simplest configuration of all. You can review (and make sure you enabled the service) the section detailing what this capability is.

The policy for making use of it is super easy. Go to Policy--Policy Sets--Default--Authorization Policy - Local Exceptions. Add in what you see below:



Policy Sets → Default

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Default	Default policy set		Default Network Access	41

Authentication Policy (3)

Authorization Policy - Local Exceptions (1)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	Anomalous Behavior Client	EndPoints·AnomalousBehaviour **EQUALS** true	ISE_Profiling_UAP	Select from list	0	⚙

Authorization Policy - Global Exceptions

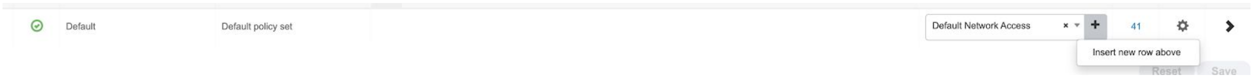
Basically if an endpoint acquires the Anomalous attribute flag it will immediately be boxed in and only be able to communicate with the ISE servers. Other options could be to add in more remediation servers or simply deny access outright (and follow up notification).

802.1X Variant

This is the penultimate section and will simply illustrate how this policy would look using 802.1X instead of MAB to make the authentication flows happen. Everything else (profiling and posture notably) are exactly the same. If you followed the section on GPO and Client Certificates, the Windows endpoints should try for 802.1X EAP-TLS using their certificates.

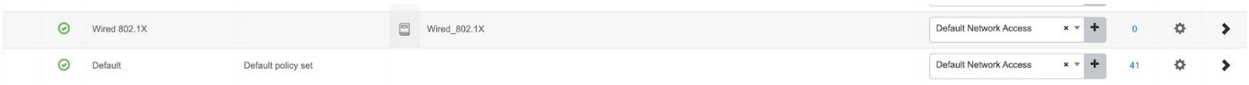
Note this could be combined with MAB policies: Windows workstations could use 802.1X and Mac/Linux/IoT can use MAB.

Go to Policy--Policy--Sets. Add a new Policy set by clicking on the gear on the right hand side of the Default policy and choose “insert new row above”



Default | Default policy set | Default Network Access | 41

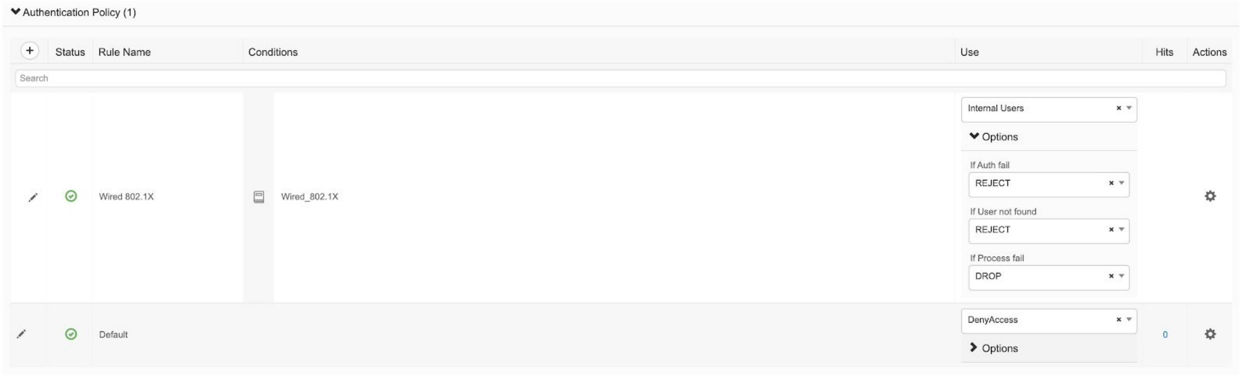
Make yours look like mine (basically any wired 802.1X requests will take the new policy set because it’s ordered sooner):



Wired 802.1X | Wired_802.1X | Default Network Access | 0

Default | Default policy set | Default Network Access | 41

Authentication Policy

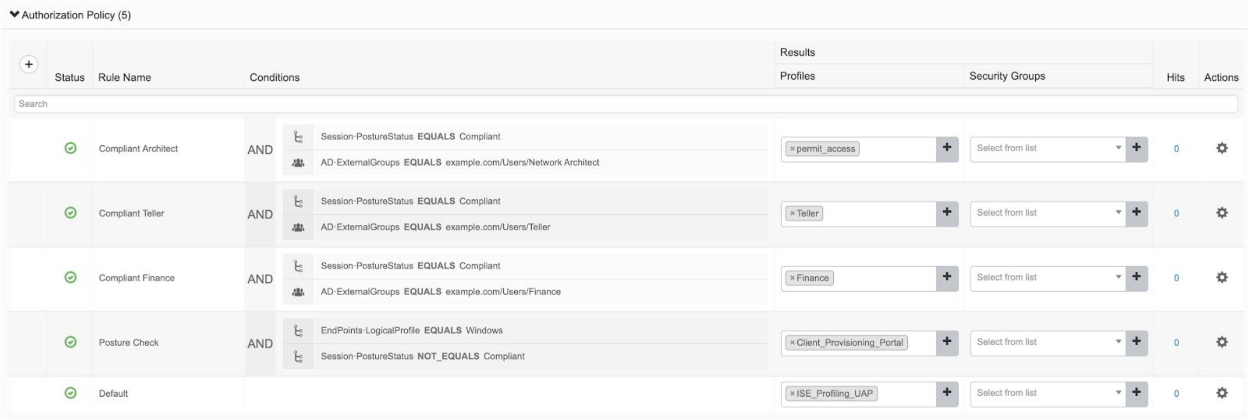


Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
	Wired 802.1X	Wired_802.1X	Internal Users Options If Auth fail: REJECT If User not found: REJECT If Process fail: DROP		
	Default		DenyAccess Options	0	

Authorization Policy

One little tweak you'll notice is I negate Posture Compliance so that only endpoints that are not checked as compliant will match it. That signals to ISE that this endpoint needs to go through the Client Provisioning Portal to be checked or to have a client installed and then be checked for compliance.



Authorization Policy (5)

Status	Rule Name		Conditions	Results: Profiles	Results: Security Groups	Hits
✓	Compliant Architect	AND	Session·PostureStatus **EQUALS** Compliant AD·ExternalGroups **EQUALS** example.com/Users/Network Architect	permit_access	Select from list	0
✓	Compliant Teller	AND	Session·PostureStatus **EQUALS** Compliant AD·ExternalGroups **EQUALS** example.com/Users/Teller	Teller	Select from list	0
✓	Compliant Finance	AND	Session·PostureStatus **EQUALS** Compliant AD·ExternalGroups **EQUALS** example.com/Users/Finance	Finance	Select from list	0
✓	Posture Check	AND	EndPoints·LogicalProfile **EQUALS** Windows Session·PostureStatus **NOT_EQUALS** Compliant	Client_Provisioning_Portal	Select from list	0
✓	Default			ISE_Profiling_UAP	Select from list	0

Conclusion

You made it to the end. Hopefully you found this helpful in general or even partially. Some new tips and tricks are always beneficial. ISE is a quality product that takes some skill and risk to master… as you can see most of it is having it work well with AD and network infrastructure. Ask questions and try to make it do new and different things and you will most likely be rewarded for your efforts. Happy NAC'ing!