**“As-Built” Documentation Template**

Document Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Author** | **Description** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[Project Summary 5](#_Toc467615881)

[ISE Implementation Details 5](#_Toc467615882)

[ISE Management and Portal URLs 6](#_Toc467615883)

[Installation 7](#_Toc467615884)

[Device Setup 7](#_Toc467615885)

[Initial Login 9](#_Toc467615886)

[System Configuration 11](#_Toc467615887)

[Administration 11](#_Toc467615888)

[Licensing 11](#_Toc467615889)

[ISE Certificates 11](#_Toc467615890)

[SMTP Server 12](#_Toc467615891)

[Logging 13](#_Toc467615892)

[Deployment 14](#_Toc467615893)

[Admin & Monitoring 15](#_Toc467615894)

[Policy Nodes 16](#_Toc467615895)

[Maintenance 17](#_Toc467615896)

[Repository 17](#_Toc467615897)

[Patch Management 18](#_Toc467615898)

[Admin Access 18](#_Toc467615899)

[Active Directory Integration 18](#_Toc467615900)

[Certificate Authentication 19](#_Toc467615901)

[Identity Groups 21](#_Toc467615902)

[Network Resources 22](#_Toc467615903)

[Web Portal Management 23](#_Toc467615904)

[Policy 24](#_Toc467615905)

[Policy Elements 24](#_Toc467615906)

[Conditions 24](#_Toc467615907)

[Authentication Conditions 25](#_Toc467615908)

[Profiling Conditions 27](#_Toc467615909)

[Results 29](#_Toc467615910)

[Authentication 31](#_Toc467615911)

[Authorization 33](#_Toc467615912)

[WLC Controller Configuration 33](#_Toc467615913)

[RADIUS Server Definitions 34](#_Toc467615914)

[Authentication 34](#_Toc467615915)

[Accounting 34](#_Toc467615916)

[SSID: SecurityLabCorp 35](#_Toc467615917)

[General Tab: 35](#_Toc467615918)

[Security Tabs: 35](#_Toc467615919)

[AAA Servers Tab 36](#_Toc467615920)

[Advanced Tab 37](#_Toc467615921)

[SSID: SecurityLabGuest 37](#_Toc467615922)

[General Tab 37](#_Toc467615923)

[Security Tabs 38](#_Toc467615924)

[AAA Servers Tab 39](#_Toc467615925)

[Advanced Tab 39](#_Toc467615926)

[ACLs 40](#_Toc467615927)

[ISE-ACL-WEBAUTH-REDIRECT 40](#_Toc467615928)

[COMPUTER ONLY 41](#_Toc467615929)

[GUEST 41](#_Toc467615930)

[PERMIT 42](#_Toc467615931)

[Reporting/Monitoring 42](#_Toc467615932)

# Project Summary

Identity Services Engine was deployed and configured for *<company>.* The goal of the project was to improve wired and wireless security, perform uniform access for corporate PCs and corporate-approved devices, and controlled guest access. This document lays out the as-built configuration.

ISE documentation can be found on [www.cisco.com](http://www.cisco.com) here:

[**http://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html**](http://www.cisco.com/c/en/us/support/security/identity-services-engine/tsd-products-support-series-home.html)

## ISE Implementation Details

The following is the information for the ISE appliances implemented.

***<ISE-Hostname>***

Model: *<VM-or-Appliance-type>*

Version: *<ISE-version>*

Patch: *<Patch-Number>*

IP Address: *<IP-address>*

Admin Role: *<Standby/Primary/Not Applicable>*

Monitor Role: *<Standby/Primary/Not Applicable>*

Personas: *<Any-Other-Personas>*

***<ISE-Hostname>***

Model: *<VM-or-Appliance-type>*

Version: *<ISE-version>*

Patch: *<Patch-Number>*

IP Address: *<IP-address>*

Admin Role: *<Standby/Primary/Not Applicable>*

Monitor Role: *<Standby/Primary/Not Applicable>*

Personas: *<Any-Other-Personas>*

***<ISE-Hostname>***

Model: *<VM-or-Appliance-type>*

Version: *<ISE-version>*

Patch: *<Patch-Number>*

IP Address: *<IP-address>*

Admin Role: *<Standby/Primary/Not Applicable>*

Monitor Role: *<Standby/Primary/Not Applicable>*

Personas: *<Any-Other-Personas>*

## ISE Management and Portal URLs

**Admin:**

https://<hostname-for-primary>

https://<hostname-for-secondary>

**Guest Portal:**

https://<Guest-URL>

**Guest Management Portal:**

https://<Guest-Management-URL>

# Installation

## Device Setup

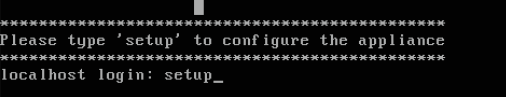
If ISE is provided as an appliance, installation should not be necessary – it will be installed. If ISE is being installed in a VM, the OS must be installed from the ISO image.

Configure the VM according to the instructions in the Hardware Installation Guide, and boot the *<VM/Appliance>* using the mounted ISO image.

**Figure 1 – Boot Option Selection**  


Select the boot option 1 and press Enter. The automated installation will proceed to build the custom Enterprise Red Hat Linux *<Depends-on-version-of-ISE>* OS.

The installation process can take 45 minutes of longer, depending on the underlying hardware. No user interaction is required until the base OS has finished installing. When the installation has completed, the VM will reboot.

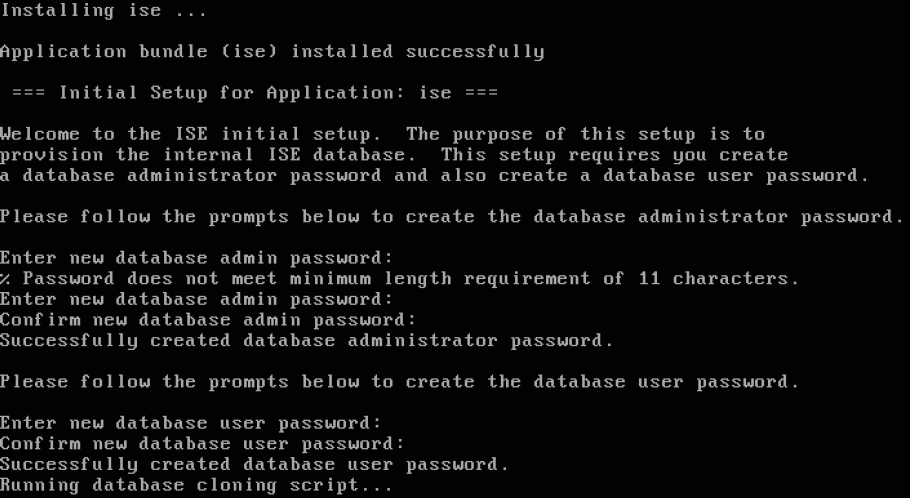
**Figure 2 – Enter CLI Setup**  


Type “setup” at the login prompt and press Enter.

The following information is required to configure the initial installation.

|  |  |
| --- | --- |
| **Option** | **Value** |
| Hostname | Must be registered in DNS |
| IP Address |  |
| Netmask |  |
| Default Gateway |  |
| DNS Domain | Use the Active Directory or LDAP domain |
| Primary Name Server | Must be accessible during the installation |
| Primary NTP Server | Must be accessible during the installation |
| Time Zone | Must be entered correctly or re-install might be required |
| Default Username |  |
| Password | Complex password required |

When the initial setup completes, you must set the password to allow the internal database.

**Figure 3 – Set Oracle Database Password**  


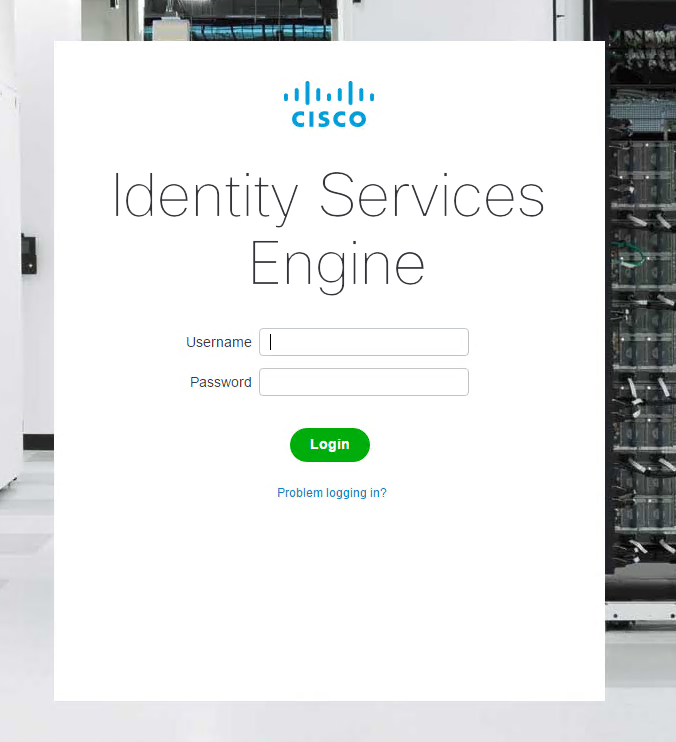
The passwords must be complex and have 8 characters. Confirm the installation from the command line by using:

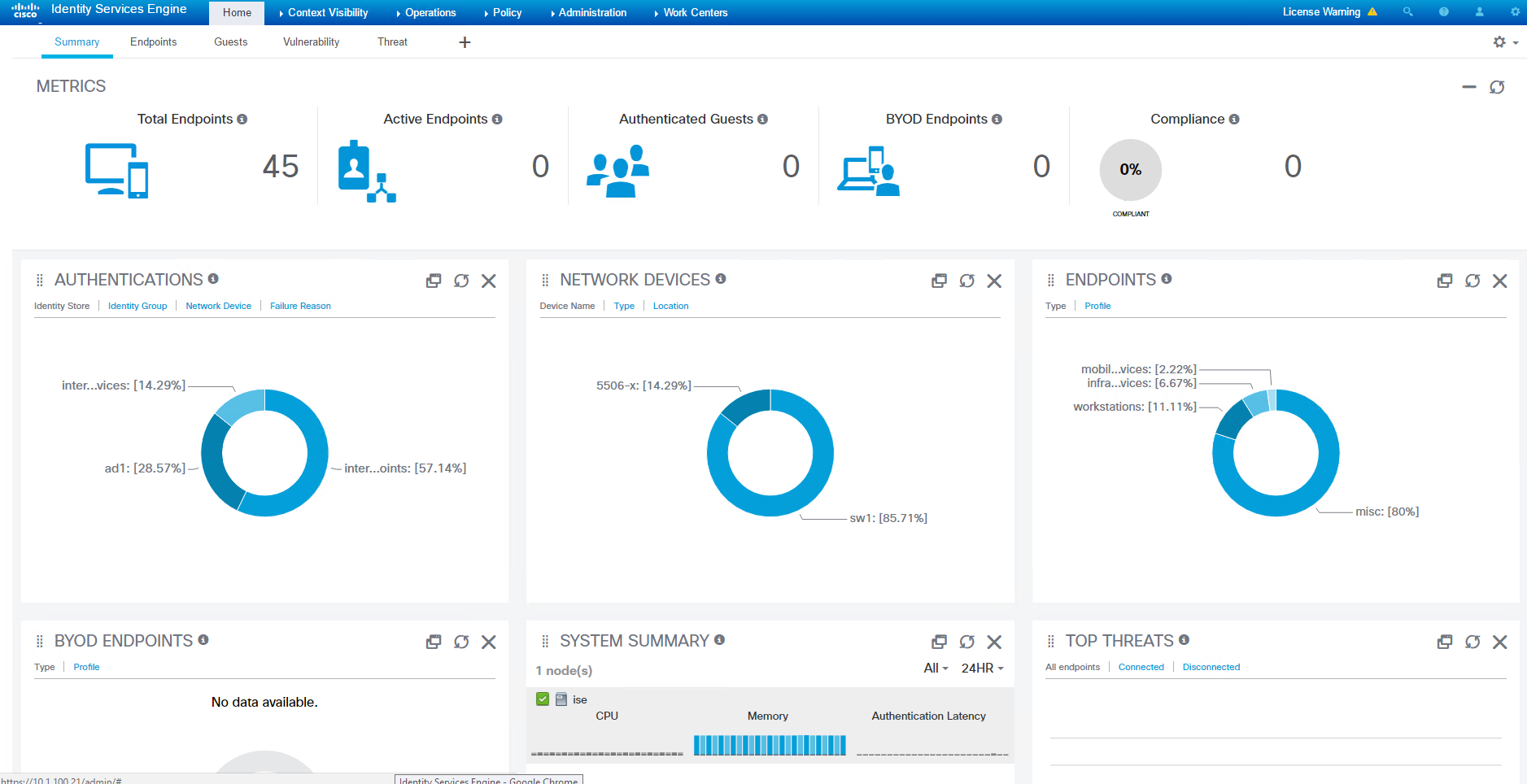
* **Show version**
* **Show inventory**
* **Show application status ise**
* **Show ntp**

# Initial Login

After the command line configuration, you can log into the web interface. Browse to the primary Admin and Monitor node.

Enter an internal or external (AD) username/password and login to the system:



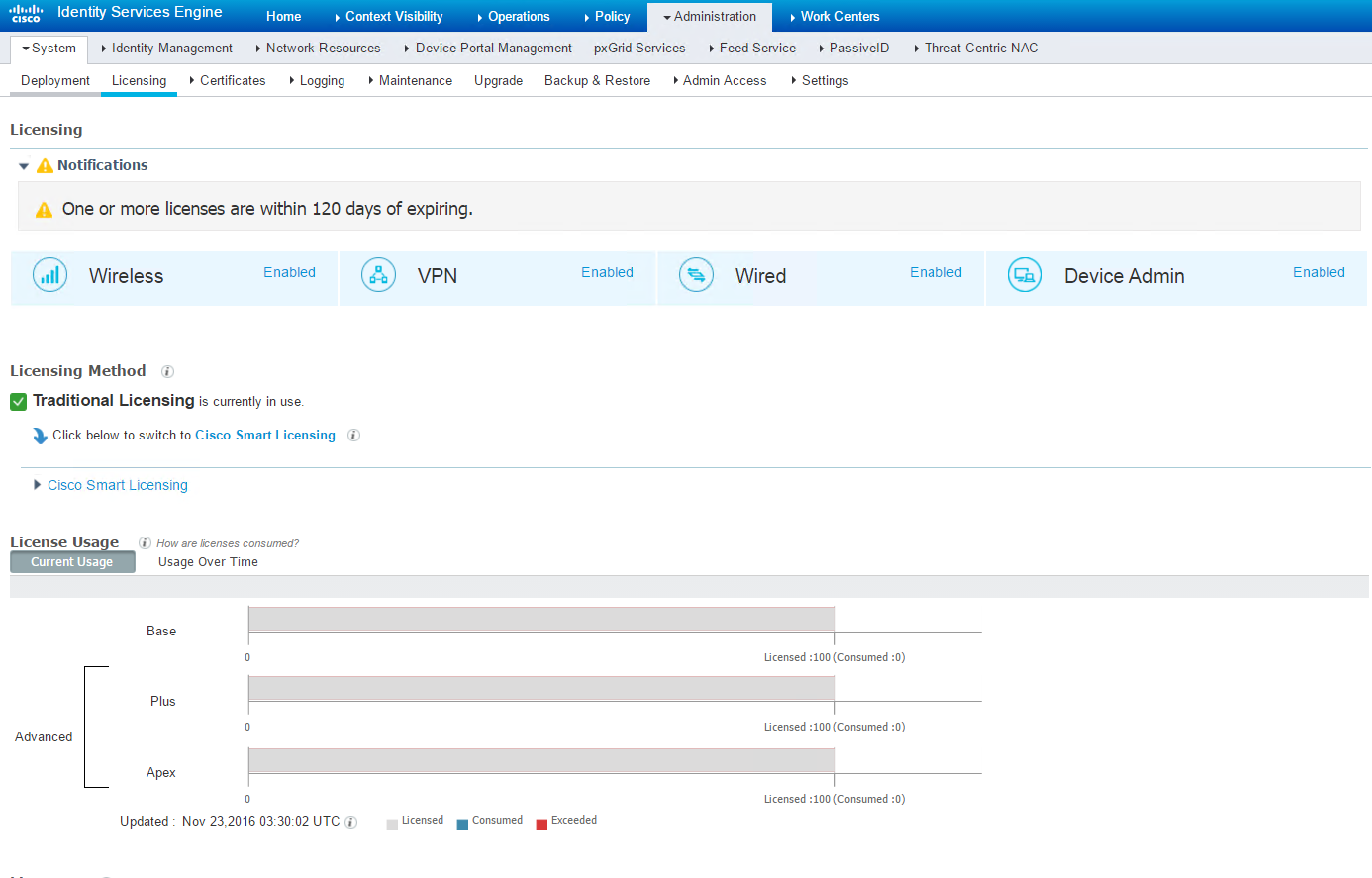
After logging in, you will be presented with the main ISE dashboard:

# System Configuration

## Administration

### Licensing

After registering the license PAK file with Cisco, the system will have a total of *<X>* base licenses, *<X>* plus licenses, and *<X>* Apex licenses:



### ISE Certificates

During the installation process the ISE units create a self-signed certificate. By default this certificate is utilized for the various web interfaces via SSL connections and also utilized for RADIUS/EAP operations.

When guest services are deployed within an ISE implementation the certificate tied to web services on an ISE device should be a public certificate to ensure that non-corporate assets will not experience a SSL certificate warning or error. In addition, digital certificates are needed from *<Company’s>* CA for machine and user based EAP-TLS authentication.

Certificate signing requests were generated for both Policy Nodes. The CSRs were utilized to obtain a certificate from *<Company’s>* internal PKI (MS Certificate Authority) CA. The same CSRs can be used to request certificates from a public certificate authority such as GoDaddy, VeriSign, etc. The internal MS CA certificate was imported and coupled to the RADIUS/EAP. In addition, the root CA certificate (*hostname-of-CA-server*) and all of the subordinate CA certificates (*hostname-of-Sub-CA-servers*) were imported to ISE as they are needed for authentications to properly “chain-up.” With the absence of public certificates, the internal certificates were also coupled to the web services. Once public certificates are obtained, they can be imported (along with any root and subordinate certificates) and tied to the web services.

With the additional certificates installed the self-signed certificate can be removed as they are no longer needed.

**Policy Node #1 -** *<Hostname>*



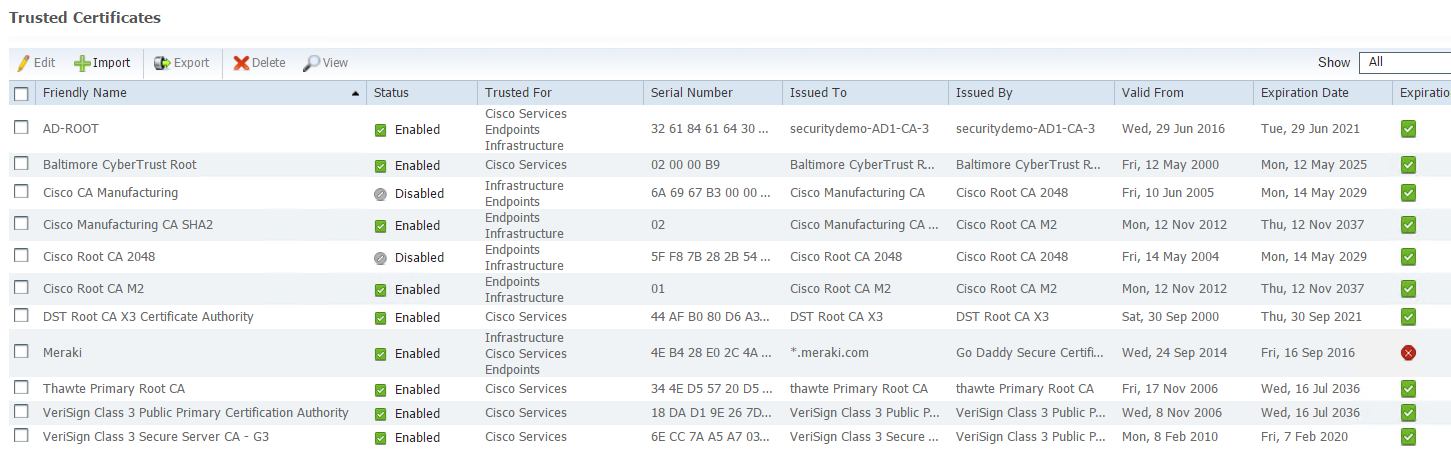
**Policy Node #2 -** *<Hostname>*

<Screenshot>

**Policy Node #3 -** *<Hostname>*

<Screenshot>

**Trusted CAs:**

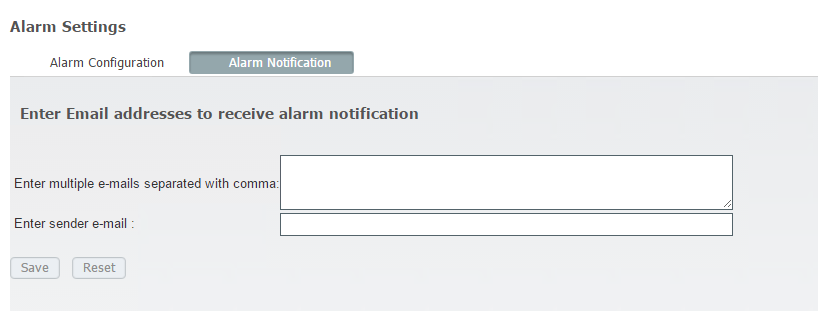


### SMTP Server

An SMTP relay server was specified in the SMTP server configuration section. The SMTP server is utilized for guest portal account activities and administrative alerts. The entry is on the **Administration>System>Settings>SMTP Server** screen.

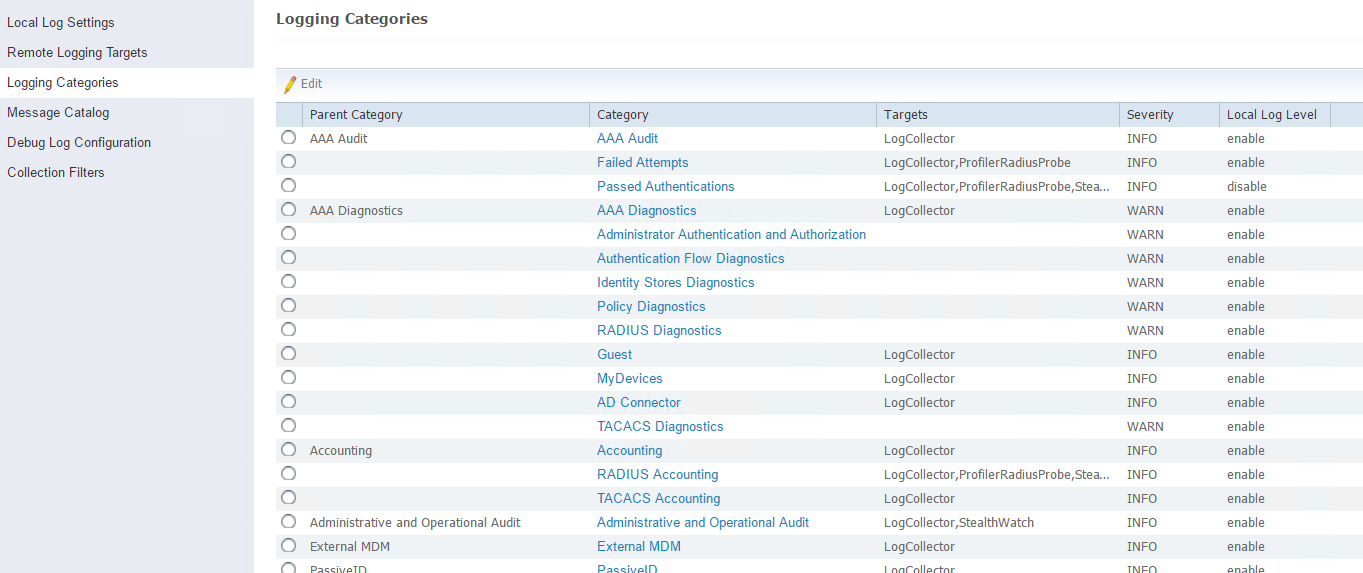


Additionally, an SMTP server was specified in the Email Settings under **Administration>Systems>Settings>Alarm Settings>Alarm Notification.** System alarm settings should also be modified to indicate what email recipients should receive the alerts.



### Logging

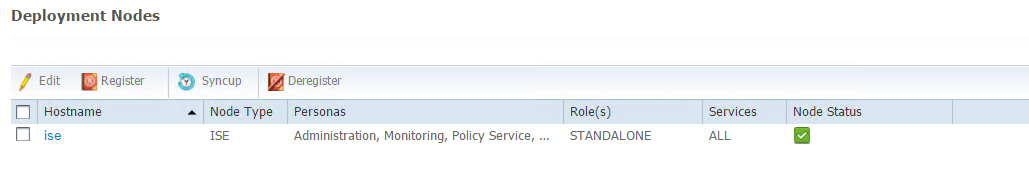
An external syslog server is highly recommended for usage with Cisco ISE. The Syslog server (*hostname*) was configured as a remote logging target. In addition, logs are configured to be retained locally for 60 days.

The logging categories and their levels can be configured and fine-tuned from the “Logging Categories” section:

### Deployment

By default an ISE appliance is configured in standalone mode. High availability can get configured between two ISE systems to provide fault tolerance. The following are the screen shots for the configuration of high availability. **Note**: If self-signed certificates are in use, the self-signed certificate of the secondary unit will need to be installed on the primary unit in order for an HA session to establish.

Additional nodes can be registered by clicking the **Register** menu and then selecting the **Register an ISE node**



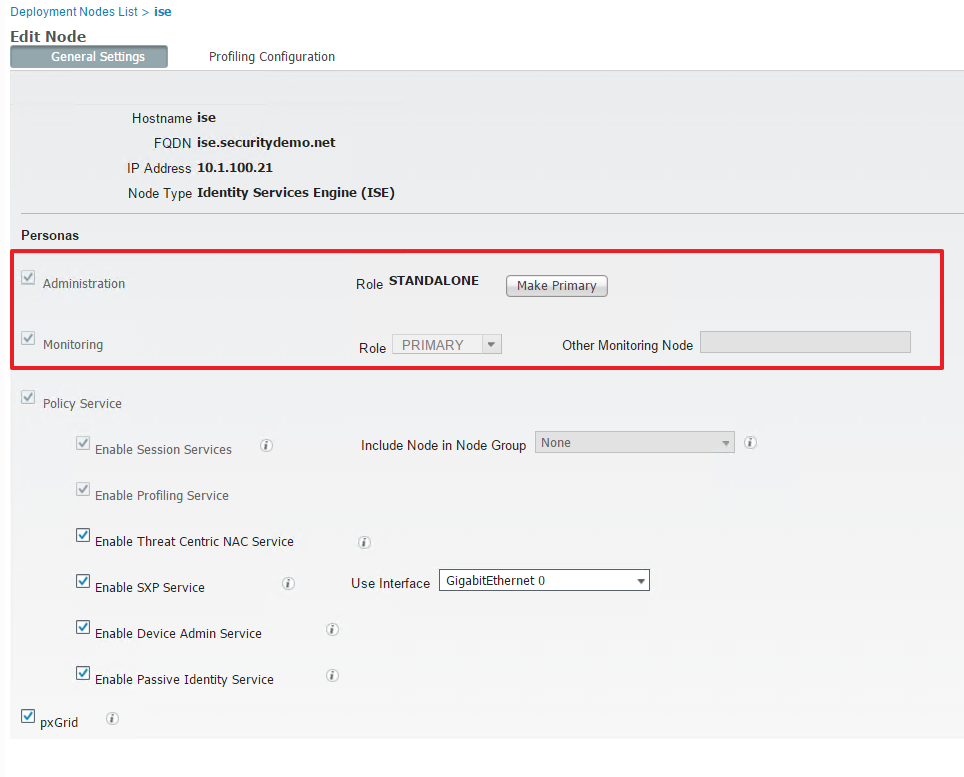
Once a node is successfully registered, the administrator can check the status of both the **Sync** and the **Database Replication** status:



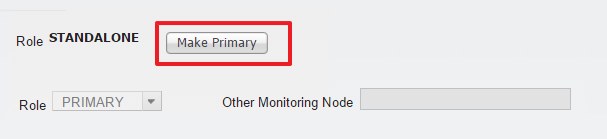
In a health environment, the node status should be green.

### Admin & Monitoring

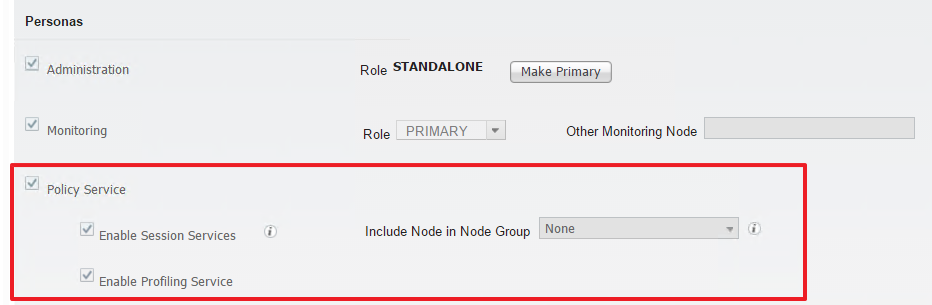
HA configurations and cluster settings can be set at the Administration->System->Deployment screen. Under the deployment tab *<primary-hostname>* and *<secondary-hostname>* are configured for the primary/secondary Admin and Monitoring Node. You can check the services running and current role by clicking on either one of the two nodes:

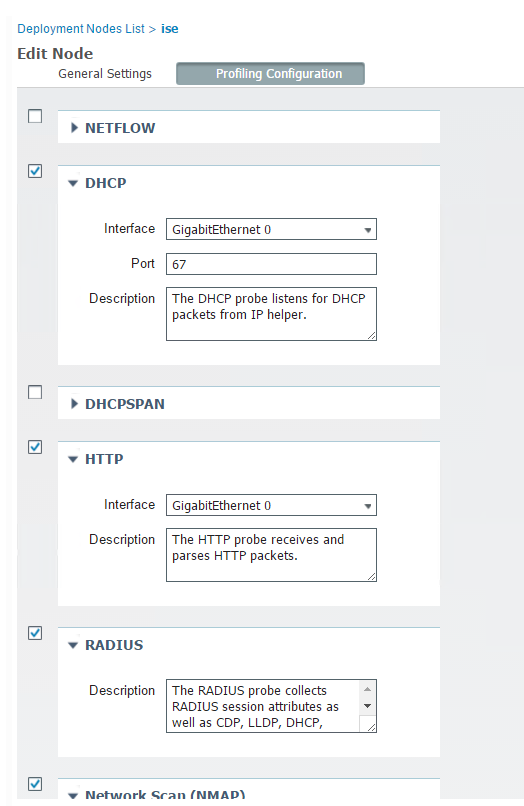


You can see from the screen shot above that *<hostname>*  is primary node for both **Administration** and **Monitoring** while the node is running the Policy Services.

**Note**: Only one node can be acting as a primary Admin node. If for some reason the current primary admin node fails an administrator has to manually promote the secondary node to become primary. This can be done by logging in to the secondary node, navigating to the **Deployment** section and clicking on the **Promote to Primary** button: 

### Policy Nodes

HA for the policy nodes is also configured in the same section of ISE. The administrator has to ensure that the **Policy Service** is running.  


To configure **Profiling,** click on the **Profiling Configuration** tab and enable the needed profiling probes. 

As part of this deployment, the following probes were configured on the policy nodes: *<fill in which probes were used>*

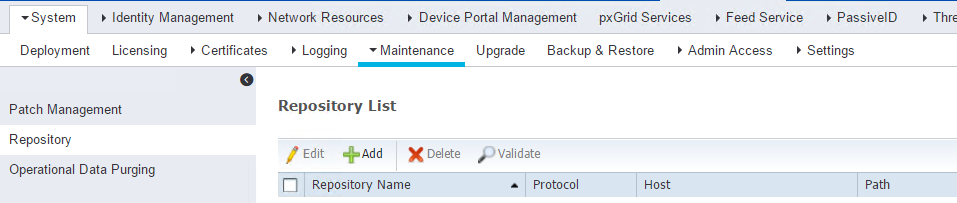
**Note:** DHCP SPAN and Netflow probes should be only enabled with caution and if absolutely needed.

Lastly, if the policy nodes are layer 2 adjacent, they can be placed in a **Node Group** with a multicast address assigned to the group. When a node in the group goes down, another node in the same group issues a CoA (Change of Authorization) for pending sessions on the failed node. In addition, a load balancer can be put in place to provide load sharing between the nodes in the group. If the policy nodes are in two separate physical locations, the nodes cannot be grouped.

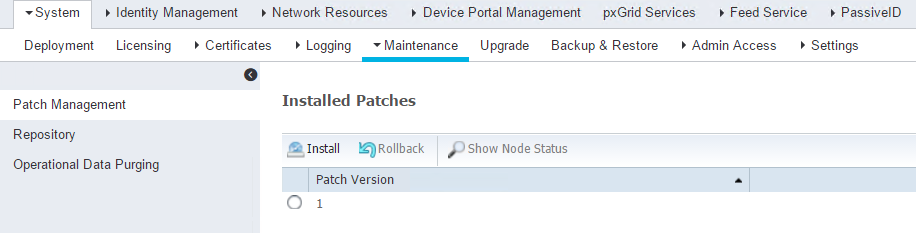
# Maintenance

## Repository

An FTP repository (*ip-address*) was configured so backups, restore, and software upgrades can be performed. The system is scheduled to perform automatic backups daily at *<time>* for the monitoring data and daily at *<time>* for the Admin data. In addition, the system is configured to purge data that is older than six months.



## Patch Management

The patch management menu allows an administrator to view, install and rollback system patches: 

## Admin Access

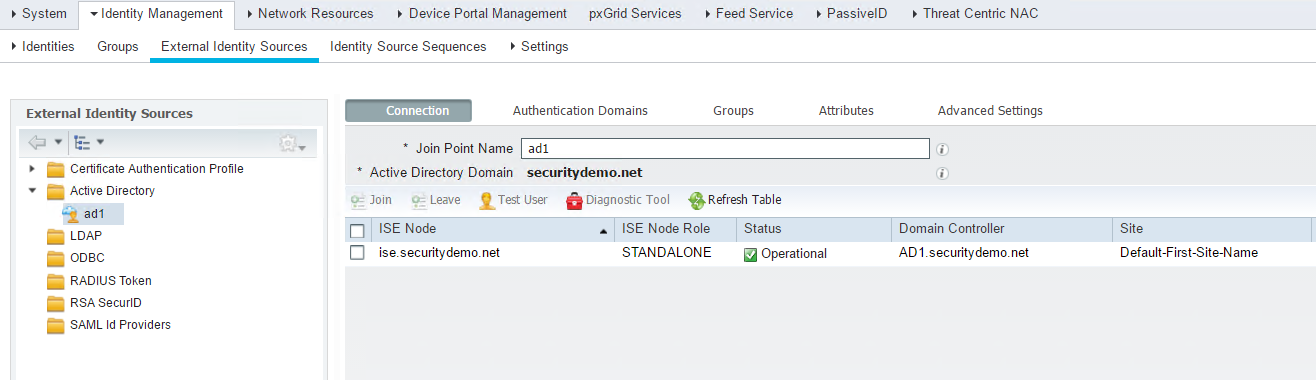
Administrative access to the ISE console can be gained either with the local username and password or via Active Directory account that is part of the *AD-Group* Active Directory Group

# Active Directory Integration

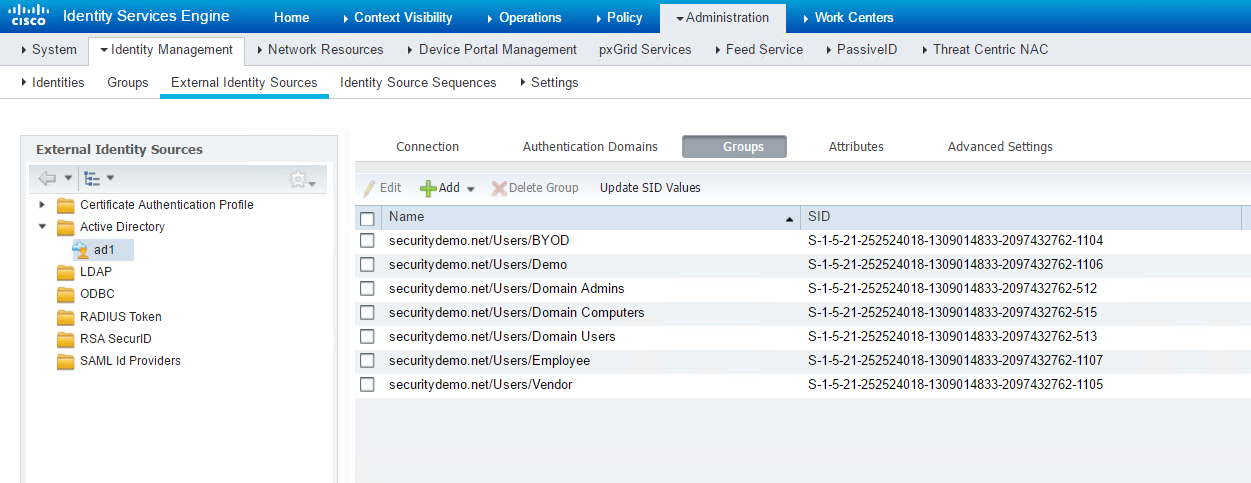
All ISE nodes were integrated to *<Company’s>* Active Directory to allow AD information to be used in authentication and authorization rules. When joining AD an account must be specified to join. An AD (*username*) service account was utilized for this purpose.

Joining Active Directory is done on the **Administration->Identity Management->External Identity Sources->Active Directory->Connection** screen. Click the join button and provide the service account information. The screen shot below shows the **Leave** button because the screenshot was taken after the system joined Active Directory.

**Note**: The join process needs to be performed on all ISE nodes. The **Test Connection** must be accomplished before the **Join** button will be available to select. Ensure accurate time and DNS settings before attempting join operation.



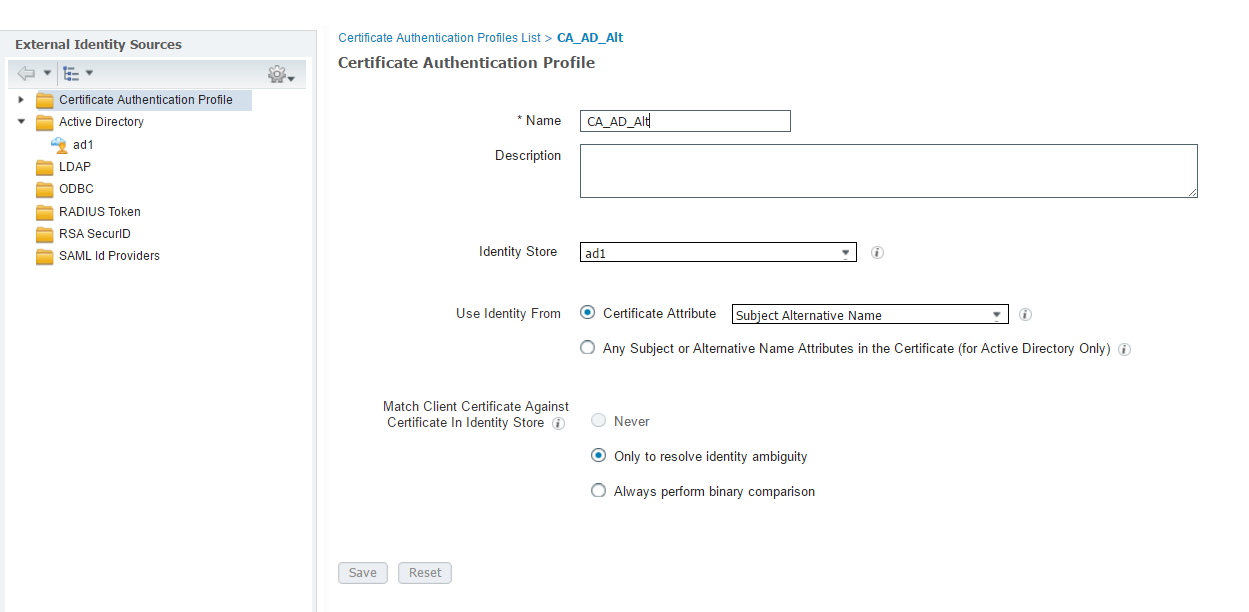
After the ISE systems are added to AD, groups need be mapped into the ISE identity store. This is accomplished through the Groups screen as shown below.



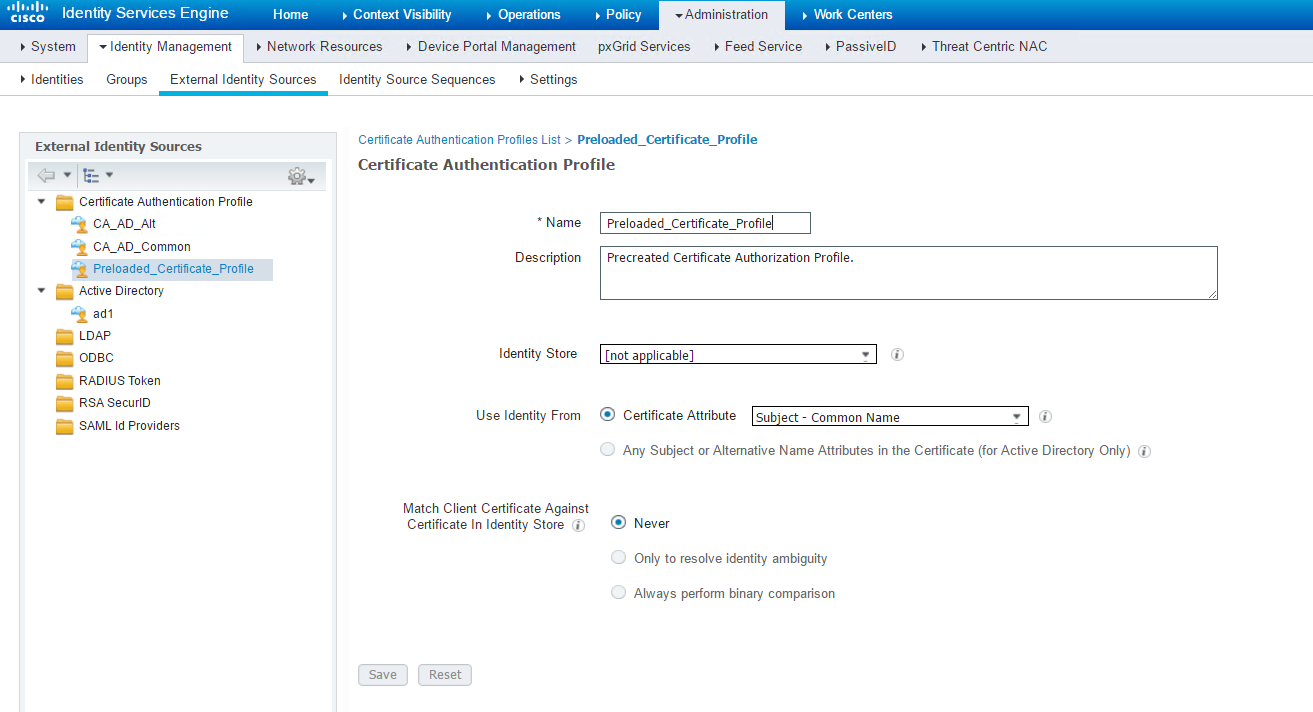
These groups can then be used in creating Policy Elements – Conditions. AD attributes can also be mapped into the ISE identity store to be utilized in Policy Elements – Conditions. The **Attributes** screen provides addition process.

# Certificate Authentication

Along with the integration to active directory, two “Certificate Authentication Profiles” were created to accommodate the EAP-TLS based machine and user authentications. In order to perform those authentications, ISE must check and match an X509 attribute that is presented by either the user or the machine. Thus, for corporate machine authentications a “Certificate Authentication Profile” was added (*Profile-Name*) which is using the “Subject Alternative Name ” for the X509 Username Attribute:



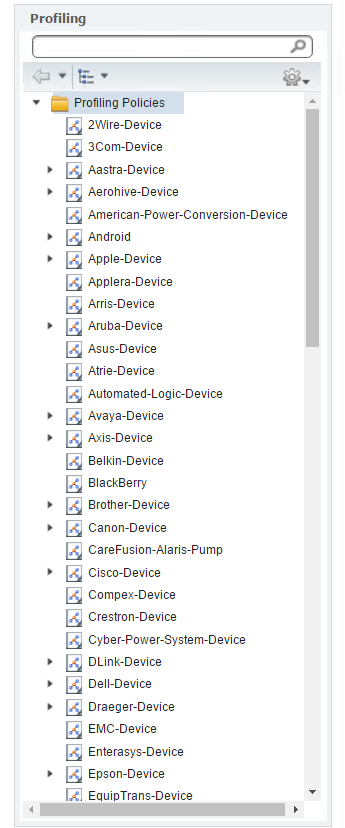
On the other hand, a different “Certificate Authentication Profile” (*Profile-Name*) was created for authentication of mobile devices provisioned through the MDM solution. For this profile, ISE is using the “Subject – Common Name” attribute:

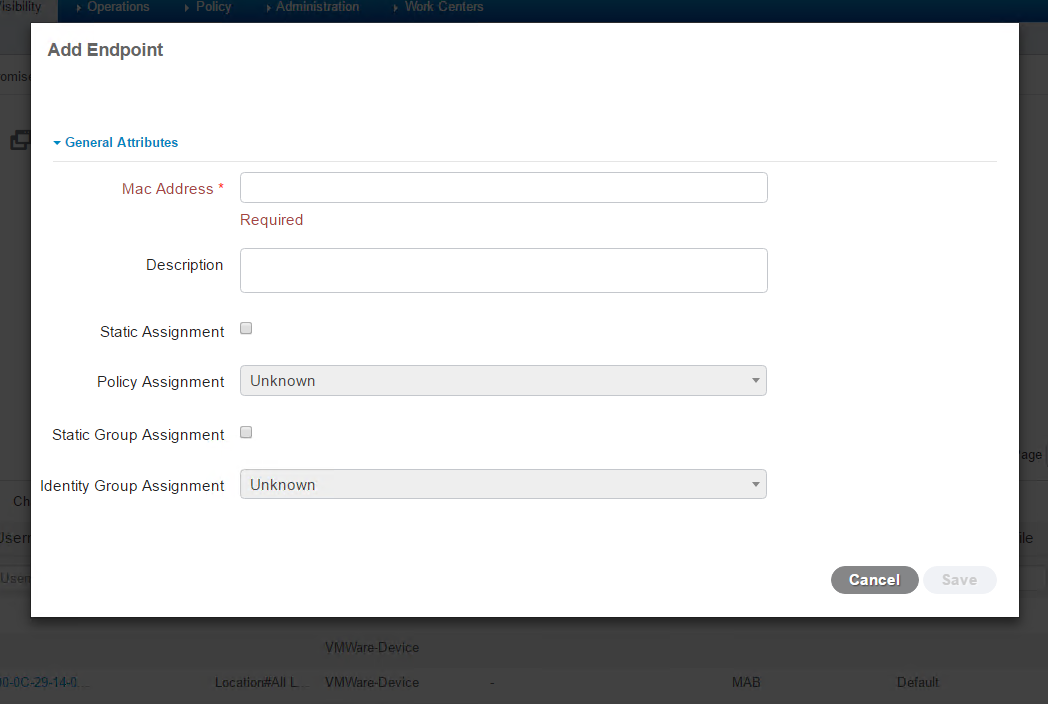


# Identity Groups

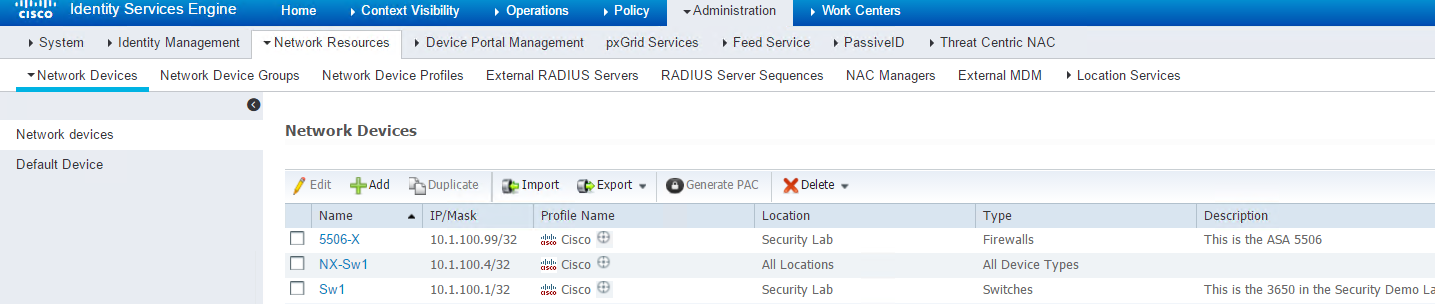
One of the building blocks of ISE policy is identity groups. Identity groups are groupings of MAC addresses that can be used in authentication and authorization rules. Identity groups can also be local user groups on the ISE system. MAC identity groups can be populated dynamically via profiling or statically defined. The Plus feature license is required for dynamic profiling of clients.

The identity groups that can be used in policy rules are located on the **Policy>Profiling>Profiling Policies** screen. There are a few predefined groups on the system (i.e. blacklist, profiled, unknown, etc.) and others are from dynamic profiling or statically defined. For this implementation both statically defined and dynamic (profiling) groups were created.



Static additions to either of these groups are created under the **Context Visibility>Endpoints** and choosing **Add**: 

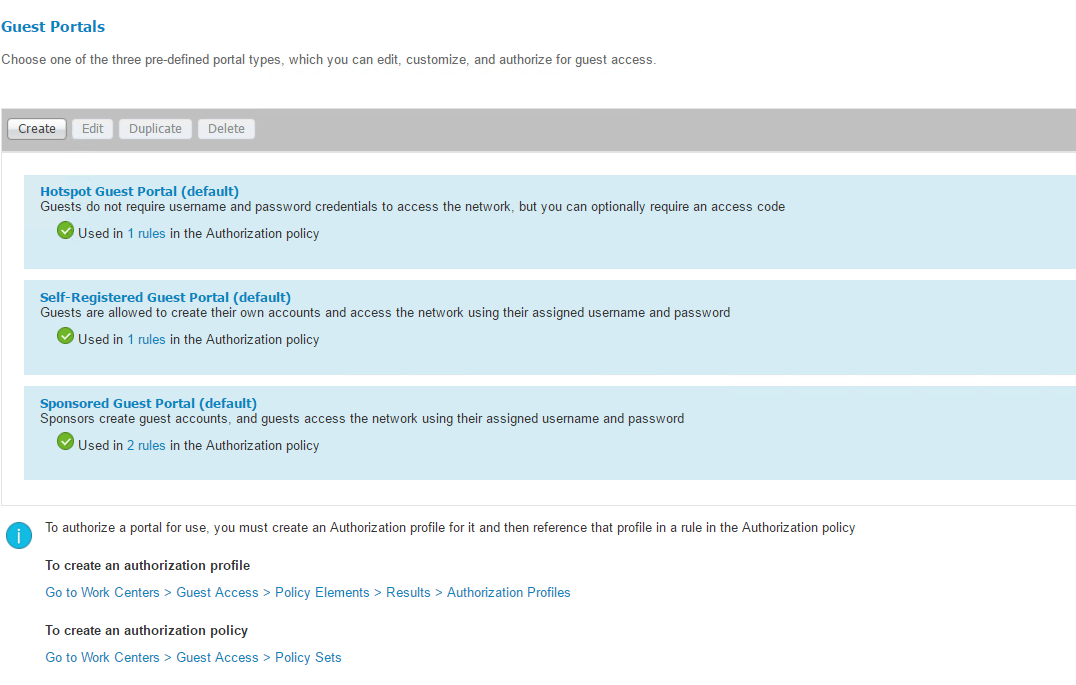
# Network Resources

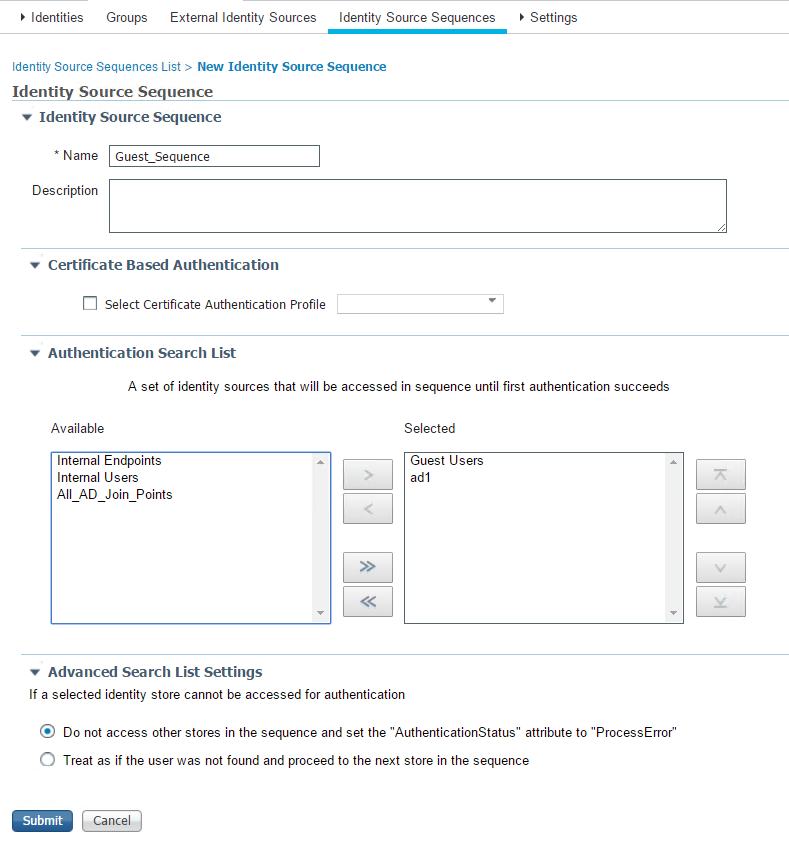
NADs (Network Access Devices) and their groups, external radius servers and their sequence, and NAC managers are all defined under “Network Resources.” For this deployment, *<Company-Name>* has defined three types of NADs: Cisco Switches, ASAs and Cisco Wireless LAN Controllers. In addition, two types of parent device locations groups were created (Monitor and Full Production) to assist with the deployment and migration from “Monitor” to full production “Closed” mode.   


*<Add Picture of Network Device Groups>*

# Web Portal Management

The default “Guest Portal” was configured to act as an authentication medium for contractors and guests that brought their own devices.



The portal is tied to the GUEST-REDIRECT Authorization Profile for authenticating users. The sequence is configured to look up both internal (Guest) and external (AD) groups:  


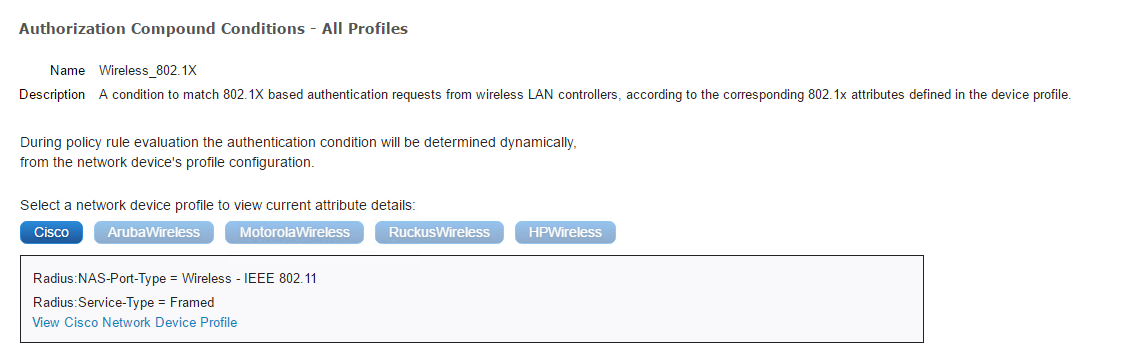
Additional custom portals can be configured, uploaded and utilized utilizing the public ISE Portal Builder located at: <https://isepb.cisco.com/>

# Policy

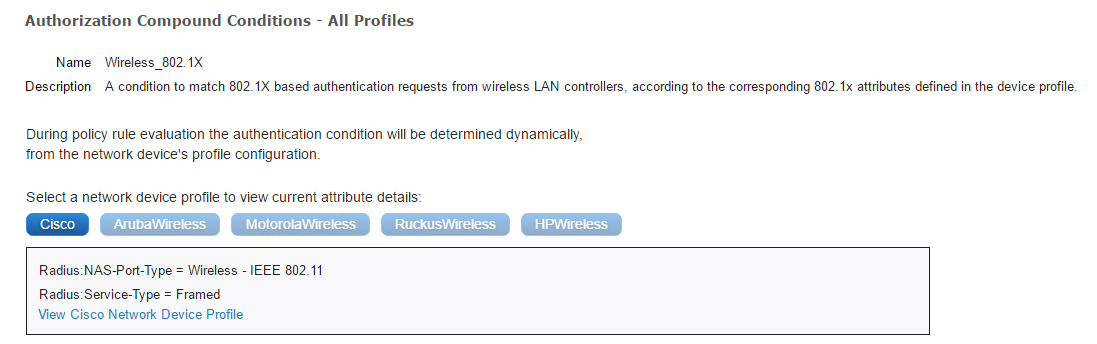
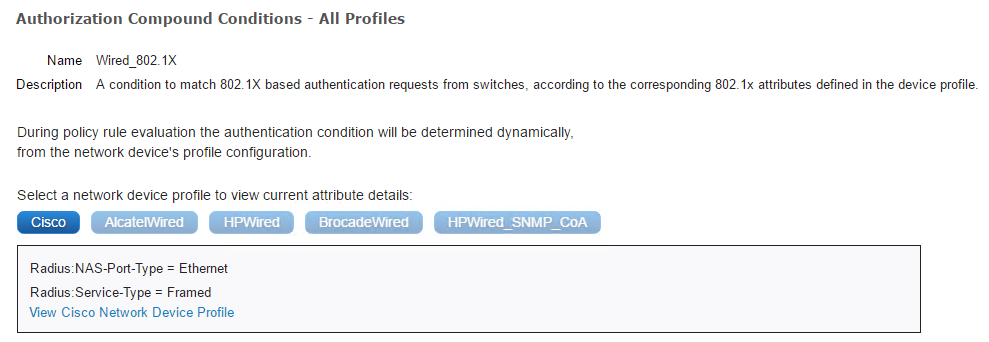
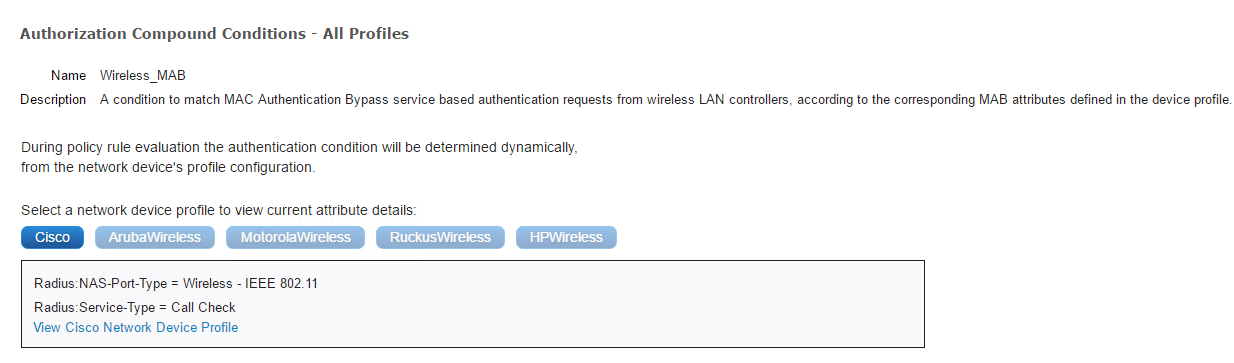
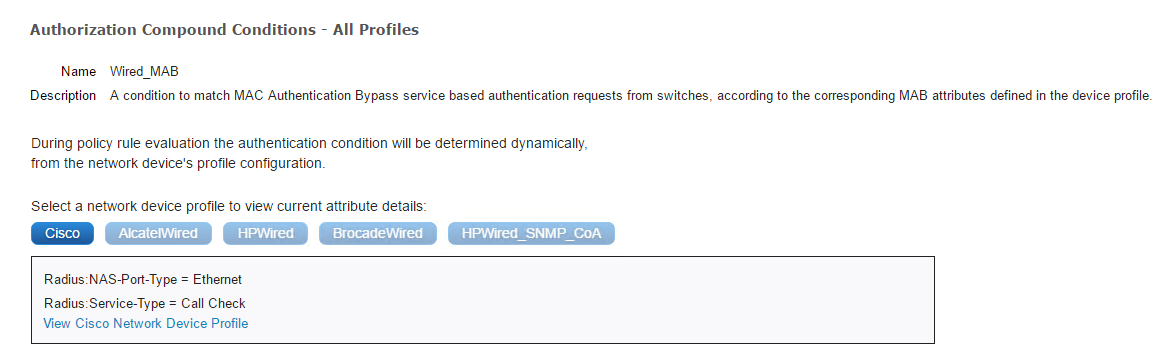
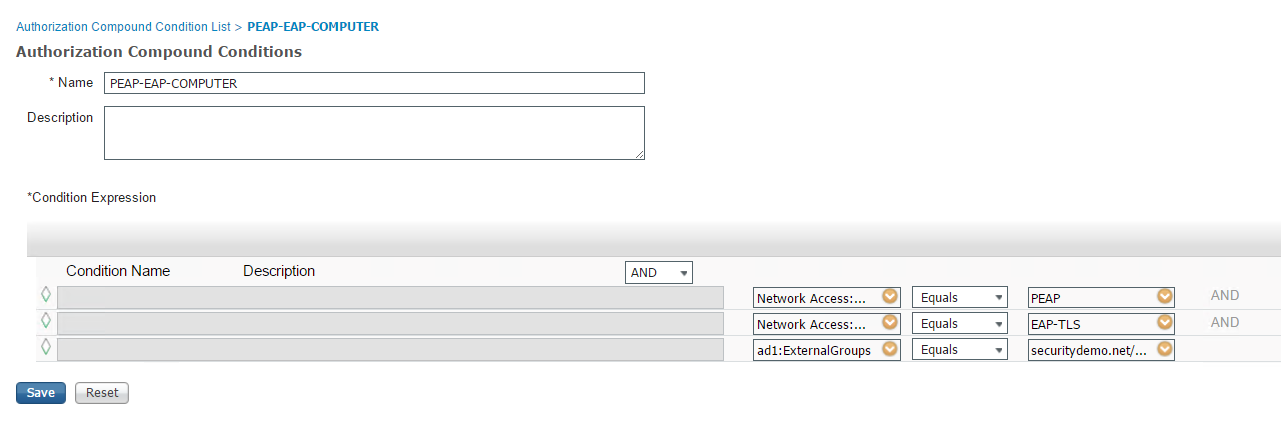
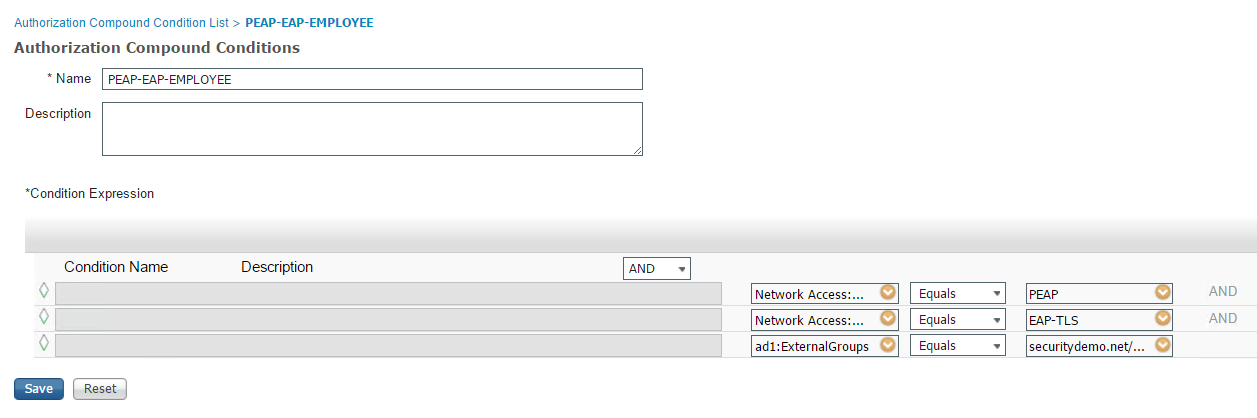
## Policy Elements

### Conditions

The next building block of policy is called conditions. A condition is a set of criteria that must be met (or not met) in order for an authorization, authentication or profiling rule to be matched. AD group membership, authenticating device, and type of authentication are examples of conditions. Conditions can contain one set of criteria (simple) or multiple criteria (compound). Compound conditions utilizes Boolean operators “AND” and “OR” to build the conditional rule. ISE allows you to define compound conditions or create them inline when defining your authorization rules.

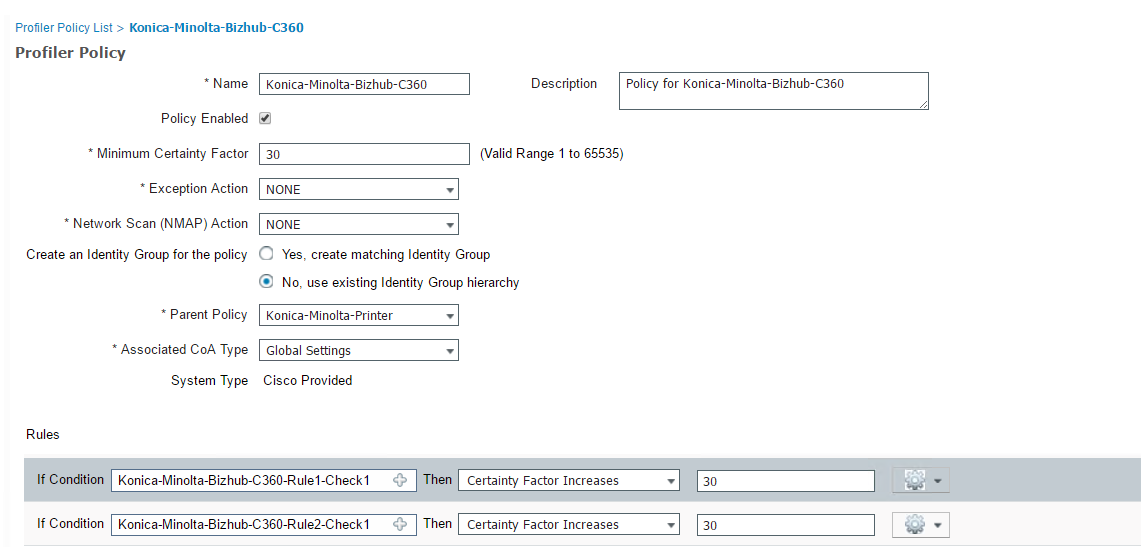
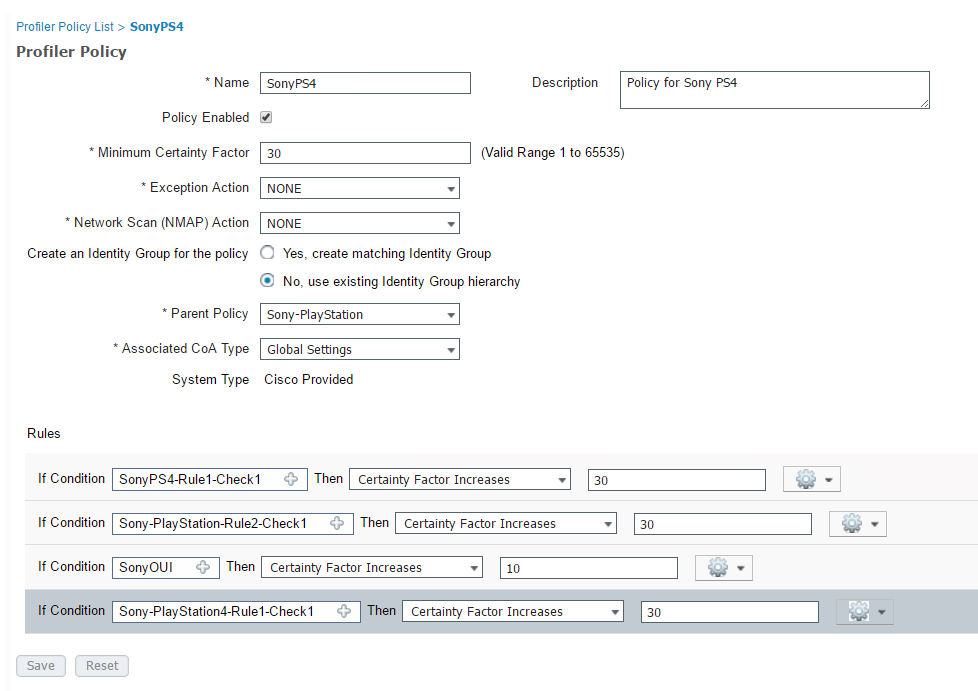
Conditions are configured on **the Policy>Policy Elements>Conditions** screen. Below is an example of an authentication compound to verify that an 802.1X authentication was sources from a wireless device. Both the conditions of RADIUS service type of “framed” and RADIUS NAS port type of “wireless” is required for this condition to be met.  


### Authentication Conditions

* Condition to match RADIUS attributes to validate authentication is originating from a wired device using 802.1x.  
  
* Condition to match RADIUS attributes to validate authentication is originating from a wired device using 802.1X  
  
* Condition to match RADIUS attributes to validate authentication is originating from a wireless device using MAB  
  
* Condition to match RADIUS attributes to validate authentication is originating from a wired device using MAB  
  
* Custom condition to validate that a machine is part of the **Domain Computers** Active Directory Group, using PEAP as the EAP Tunnel, and EAP-TLS as the EAP Authentication type  
  
* Custom condition to validate that a machine is part of the **Domain Users** Active Directory Group, using PEAP as the EAP Tunnel, and EAP-TLS as the EAP Authentication type  
  

### Profiling Conditions

Profiling conditions are used to account for several devices that ISE profiled in the environment

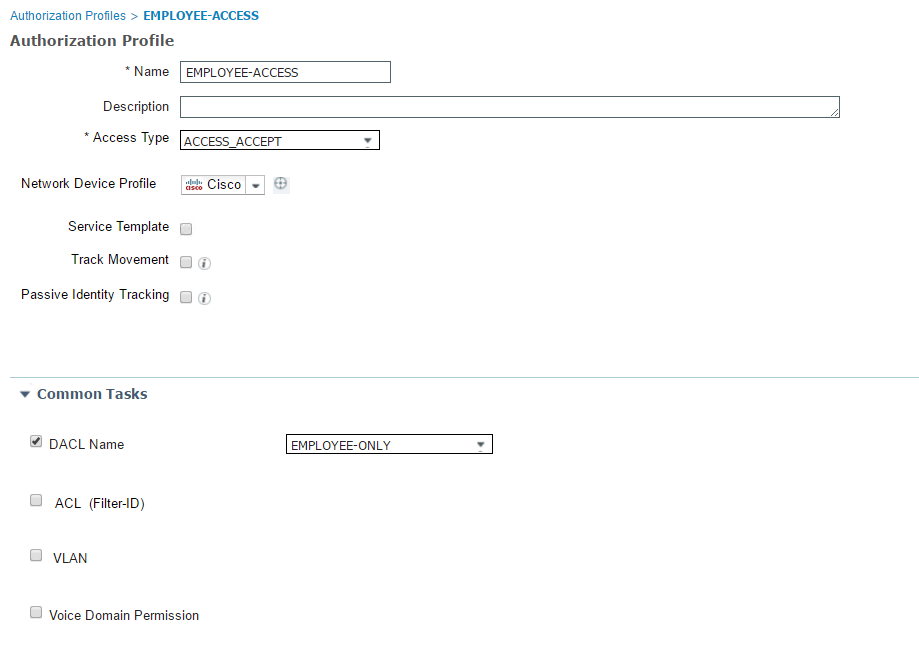
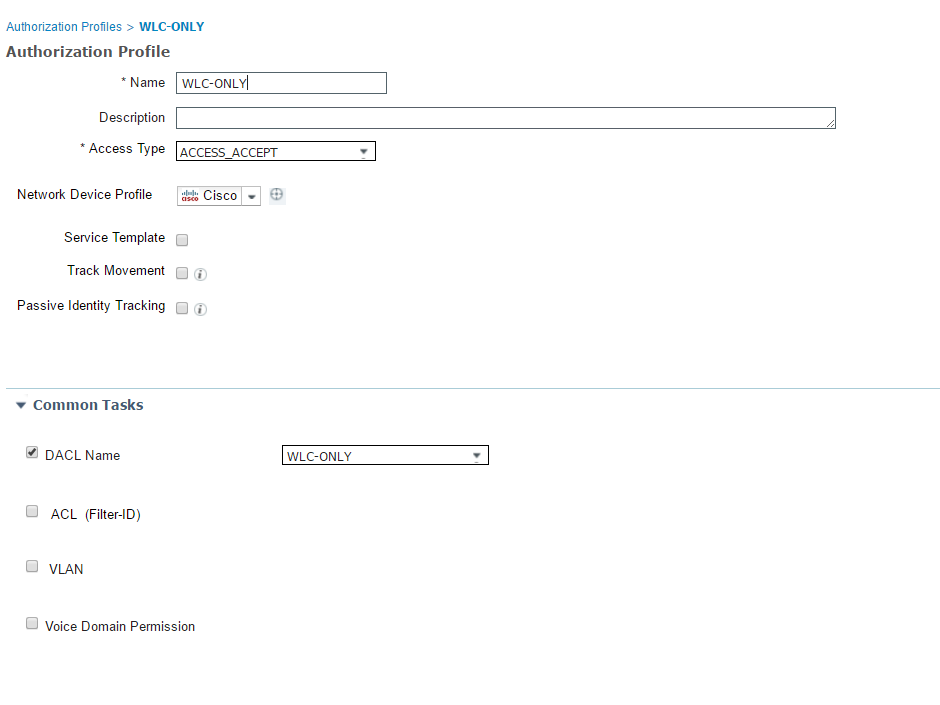
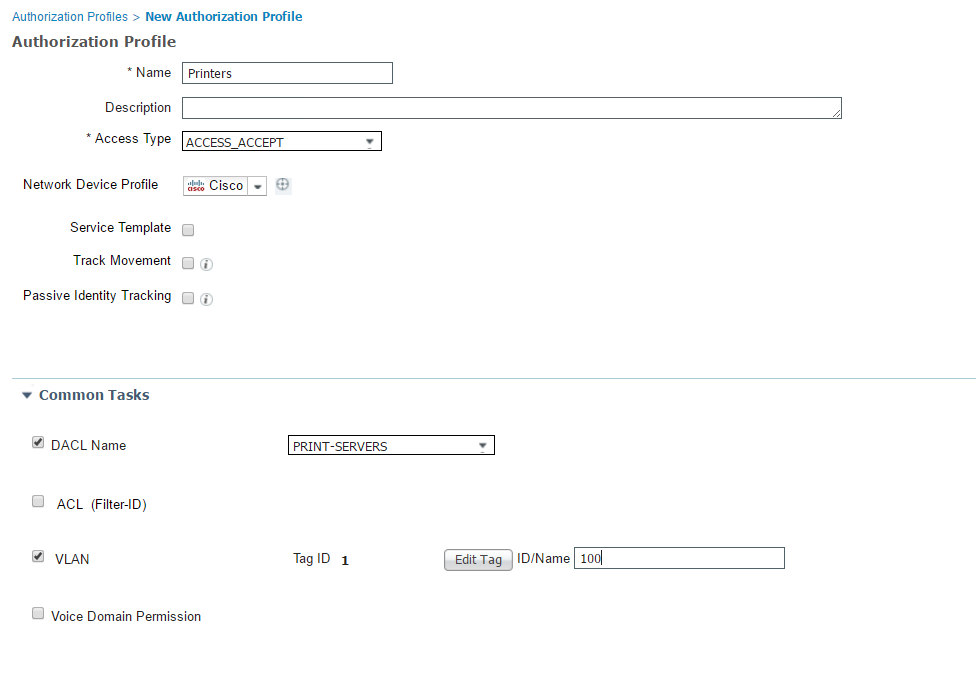
* **Konica Minolta Bizhub C360** Condition – Checks and confirms that SNMP:hrDeviceDescr contains “KONICA MINOLTA bizhub C360,” SNMP:sysDescr contains “KONICA MINOLTA bizhub C360,” MAC:OUI contains “Konica,” and DHCP:dhcp-parameter-request-list matches “^1, 3, 23, 6, 15$|^1, 3, 6, 15, 44$|^1, 3, 6, 15, 44, 46$|^1, 3, 6, 44, 46$”  
  
* **Sony Playstation PS4** Condition – Checks and confirms that MAC OUI is for ”Sony”, DHCP-class-identifier equals “PS4”, IP user-agent contains “Playstation 4”, and dhcpv6-vendor-class equals “PS4”  
  

Additional custom conditions can be written to accommodate other devices that do not have prebuilt profiling conditions in ISE. The conditions can be built based on the attributes that were collected from the “unknown” device during its attempt to authenticate to the network. Device attributes can be checked from **Context Visibility>Endpoints>***Endpoint*  


### Results

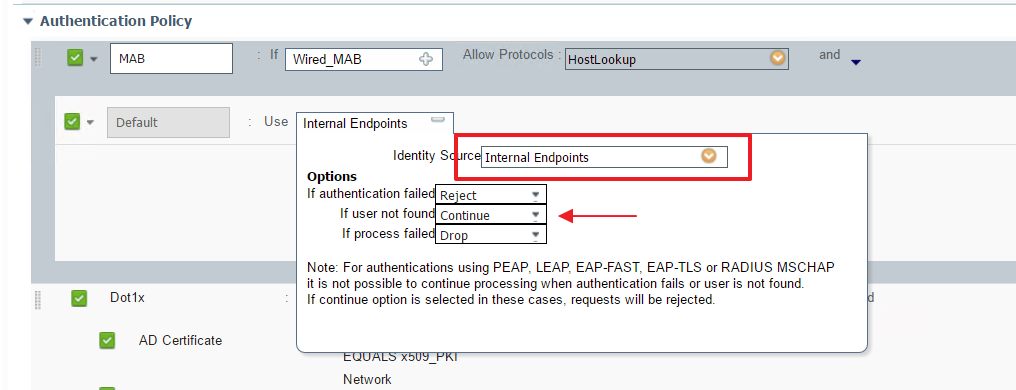
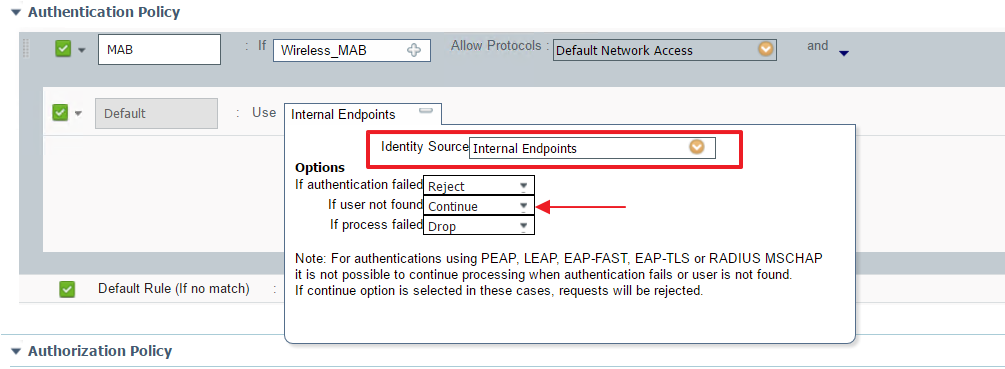
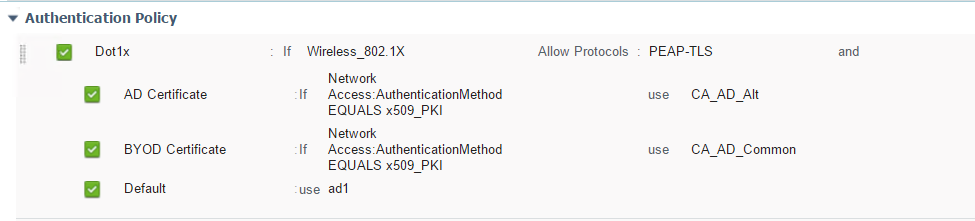
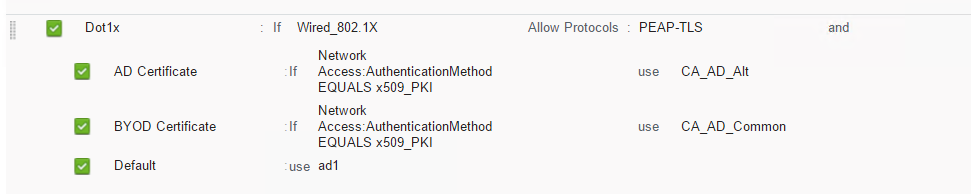
Another building block of policy is called results. A result is the action that will be taken when an authorization, authentication, profiling, or posture rule is matched. Examples of results that can be taken would be: permit access, restrict access via ACL assignment, download an ACL (DACL), require posture assessment, redirect to guest portal, or any number of returnable RADIUS attributes. Results show up in the permission column on the authorization rule screen in ISE.

Results are configured on the **Policy>Policy Elements>Results** screen. The following custom Authorization Profiles were configured as part of this ISE deployment.

* 1. Employee Access with:  
     **DACL:** EMPLOYEE-ACCESS  
     **Reauthentication:** 14400 seconds  
     **Radius:Idle-Timeout:** 180 seconds  
     
  2. WLC-Only with:  
     **DACL:** WLC-ONLY  
     **Radius:Idle-Timeout:** 180 seconds  
     
  3. Printers with:  
     **DACL:** PRINTER-SERVERS  
     **VLAN:** 100   
     **Radius:Idle-Timeout:** 180 seconds  
     

## Authentication

With the building blocks of the policy elements defined, the authentication policy can then be created based on those conditions. A total of four active authentication rules were configured for this deployment:

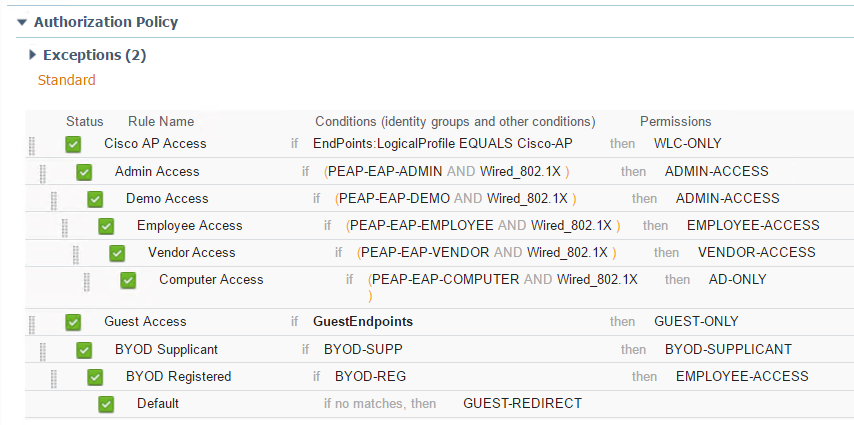
1. MAB-Wired – Allows MAB (MAC Authentication Bypass) over the wired network.   
   **Note** **#1**: The “Options” under the “Identity Source” was changed to “Continue” when users are not found during MAB authentication. Consequently, those users/machines that were not found in the system will be forwarded to the authorization rules for further inspections/decision process. This rule is what allows guest/contractors machines to be sent to the guest portal (Central Web Auth). The “Identity Source” for this rule is “Internal Endpoints”  
   
2. **MAB-Wireless** - Allows MAB (MAC Authentication Bypass) over the wireless network.   
   **Note #1:** The “Options” under the “Identity Source” was changed to “Continue” when users are not found during MAB authentication. Consequently, those users/machines that were not found in the system will be forwarded to the authorization rules for further inspections/decision process. This rule is what allows guest/contractors machines to be sent to the guest portal (Central Web Auth). The “Identity Source” for this rule is “Internal Endpoints”  
   
3. **Dot1X-Wireless** – Allows 802.1X wireless clients to authenticate using a digital certificate (EAP-TLS). The rule has two conditions:
   1. **AD Certificate**: Used by Corporate computers that are part of Active Directory and have a certificate pushed to them via Group Policy. The “Identity Source” for this rule is “CA\_AD\_Alt”
   2. **BYOD Certificate**: Used by mobile devices that have been issued a user certificate via ISE’s BYOD solution. The “Identity Source for this rule is “CA\_AD\_Common”  
      
4. **Dot1x Wired –** Allows 802.1x wired clients to authenticate using the BYOD or CA-issued digital certificate (EAP-TLS)  
   
5. **Default Rule –** Check other identity sources  
   

## Authorization

Authorization policy is the final aspect of ISE policy engine. The authorization policy ties together the use of policy elements and identity groups. If the rule conditions are met then the defined permissions are applied. The configuration of the authorization policy occurs on the **Policy>Policy Sets>***Policy-Set-Name***>Authorization** screen.

The screenshots provide a reference to be used with the above mentioned policies.

Current Authorization Policy:



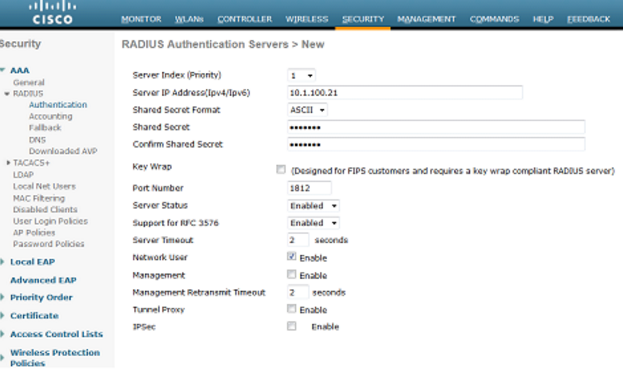
# WLC Controller Configuration

Now that ISE is configured to authenticate and authorize clients. The WLCs need to be configured in terms of RADIUS servers, network interfaces, access control lists, and SSIDs. The WLC devices will try to authenticate users in one of three ways:

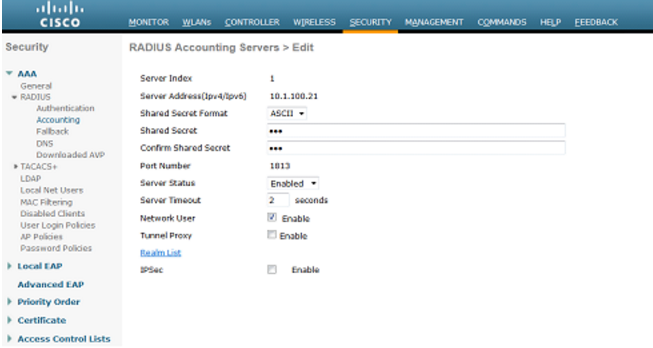
1. **802.1X** - If the client connects to the *<Name>* SSID then the WLC will authenticate the client to the ISE with 802.1X. Only EAP-TLS is allowed from the EAP types for this SSID. Users trying to connect with their AD username/password (PEAP-MS-CHAPv2) will NOT authenticate
2. **Web Authentication** – If the client connects to the *<Name2>* SSID then the WLC will forward the authentication request to ISE’s guest portal. There the consultant/guest/domain user will have to enter his/hers username/password
3. **MAB -** If the authenticating device is a Cisco Wireless Phone then the WLC will send the MAB request to ISE. During this process the wireless phone will be profiled and then allowed on the network

## RADIUS Server Definitions

### Authentication

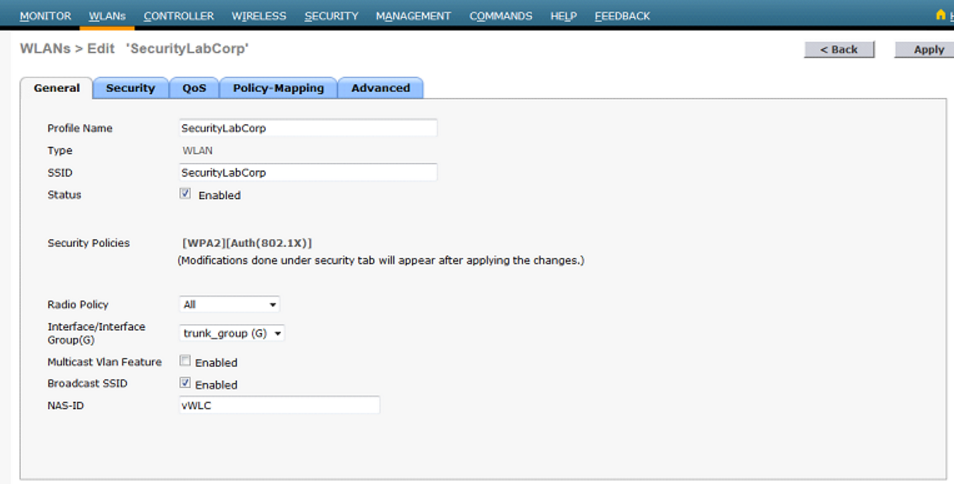
ISE Policy Nodes configured as Authentication Servers  


### Accounting

The same ISE Policy Nodes are added as Accounting Servers  


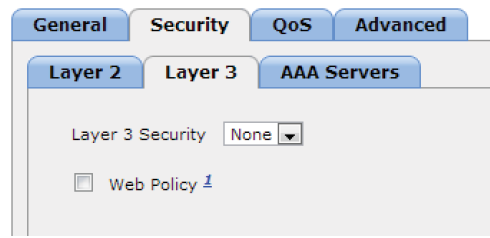
## SSID: SecurityLabCorp

### General Tab:

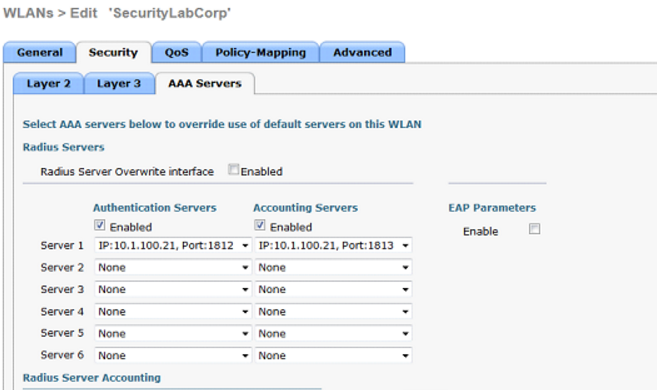


### Security Tabs:

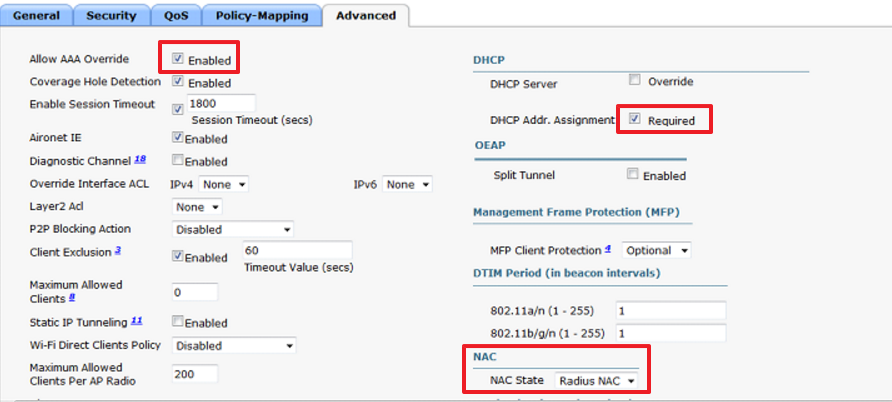
Layer 2 security will be WPA+WPA2 with WPA2 policy and 802.1x for key management.  

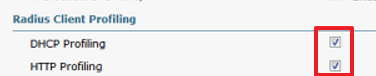

Layer 3 security will be blank for this SSID.  


### AAA Servers Tab

This is where the previously defined ISE Policy Servers are selected.  


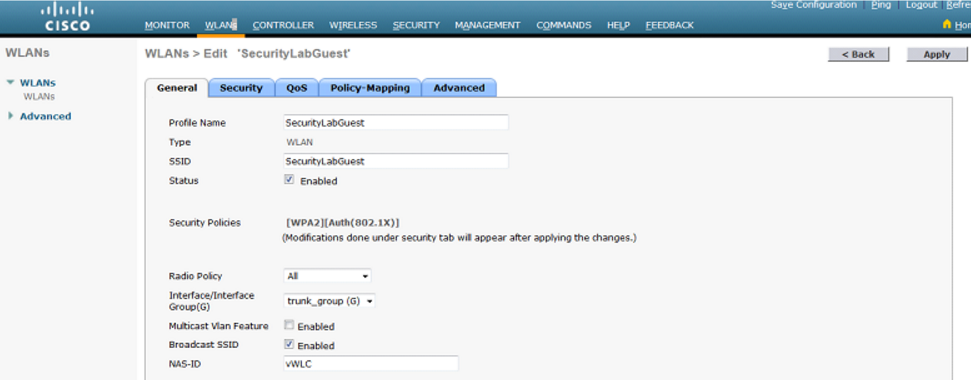
### Advanced Tab

Ensure that AAA override, DHCP Addr. Assignment, RADIUS NAC, DHCP Profiling and HTTP Profiling are enabled.   


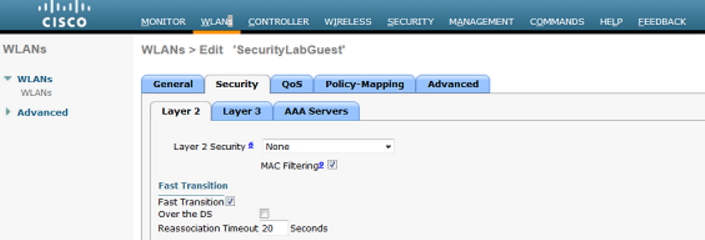


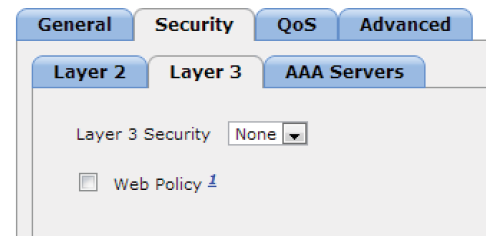
## SSID: SecurityLabGuest

### General Tab

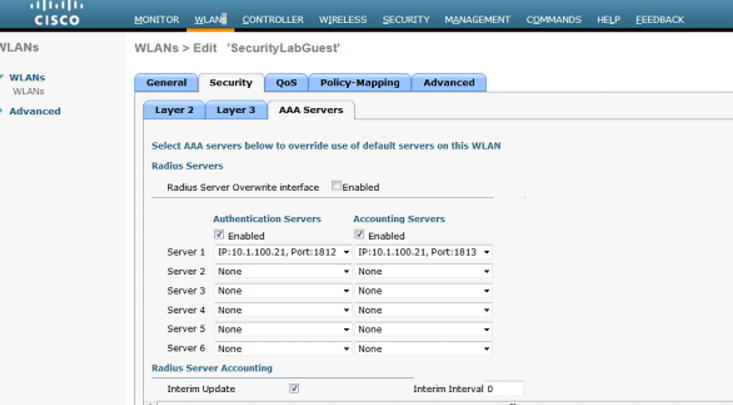


### Security Tabs

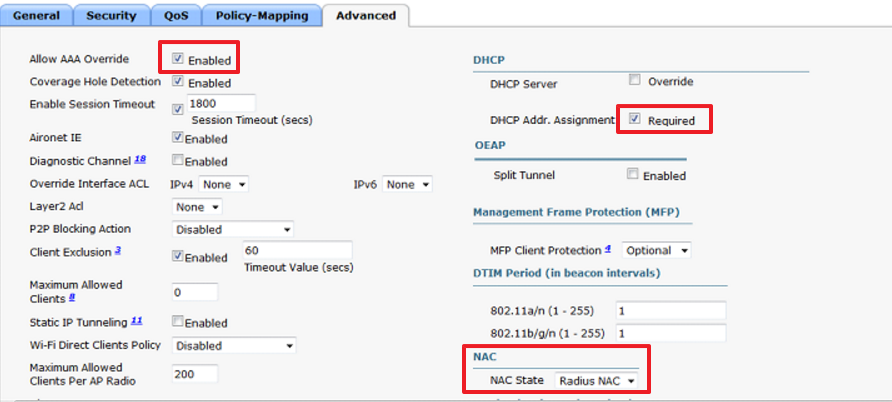
The layer 2 security is set to Open and MAC Filtering is enabled. This forces clients to be redirected to ISE and makes central web authentication possible.   


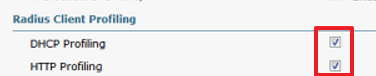
Layer 3 Security will be blank for this SSID.  


### AAA Servers Tab

This is where the previously defined ISE Policy Servers are selected.  


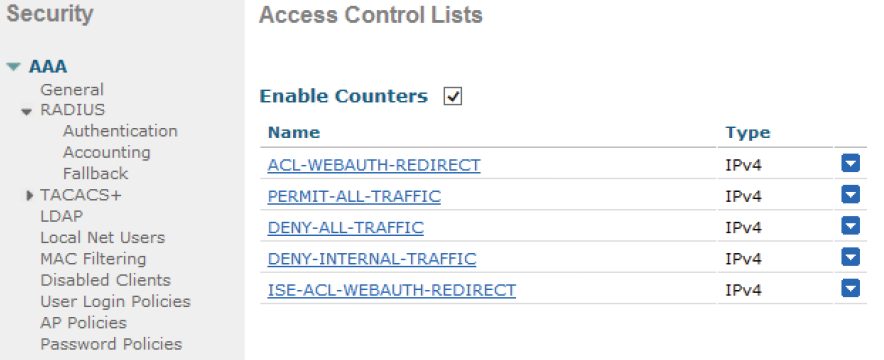
### Advanced Tab

Ensure that AAA override, DHCP Addr. Assignment, RADIUS NAC, DHCP Profiling and HTTP Profiling are enabled.   




## ACLs

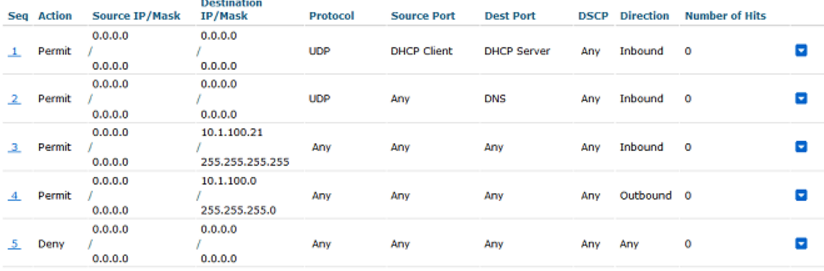
The WLCs do not support downloadable ACLs (dACLs), therefor the ACLs utilized in the ISE authorization profiles are required to be predefined on the WLCs.



The WLC’s ACLs are then referenced as Airspace ACL Name in ISE under the Authorization Profile.

### ISE-ACL-WEBAUTH-REDIRECT

This is the ACL that will be used for WebAuth redirects in the future.

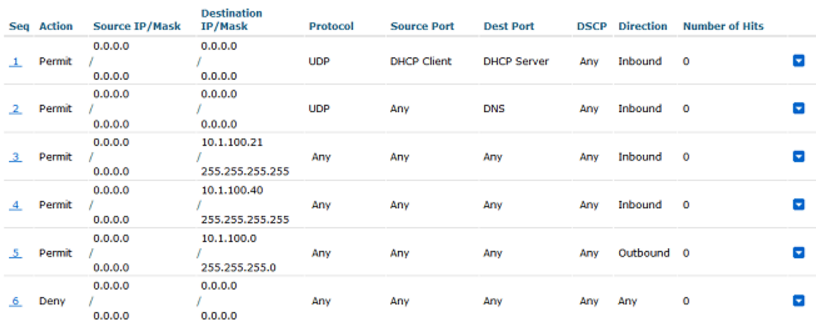


Here's the breakdown of the ACEs:

1. Allows the endpoint to get an IP address
2. Allows the endpoint to use DNS which will be necessary to communicate with ISE
3. Allows the endpoint to communicate with ISE
4. Allows outbound traffic from my server subnet to the client.
5. Everything else is denied

### COMPUTER ONLY

This is the ACL used for corporate computers that a user is not logged into.

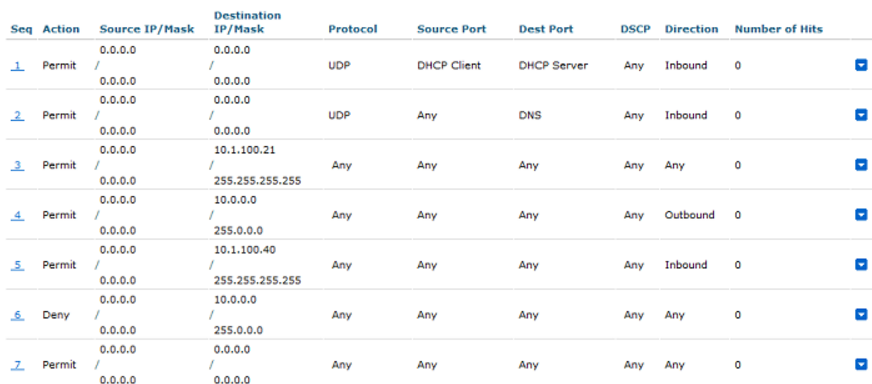


Here's a breakdown of the rules:

1. Allows the endpoint to get an IP address
2. Allows the endpoint to use DNS
3. Allows the endpoint to communicate with ISE
4. Allows the endpoint to receive traffic from server subnet
5. Everything else is denied

### GUEST

This is my ACL for guest on the network.



Here's a breakdown of the rules:

1. Allows an endpoint to get an IP address
2. Allows an endpoint to use my DNS server
3. Allows an endpoint to communicate with ISE server
4. This permits traffic back from any 10.0.0.0/8 subnet to this endpoint.
5. This permits this endpoint to communicate with AD server
6. Denies the endpoint from reaching any of the internal
7. Permits everything else so the Guest has internet access

### PERMIT



# Reporting/Monitoring

There are several ways to monitor/report on the functioning of an ISE environment:

1. On the WLC:
   1. Search for Username for secure SSID
   2. Search for MAC address for guest SSID
2. On the ISE GUI:
   1. **Operations>RADIUS Livelog** (Only tracks recent entries)
   2. **Operations>Reporting>Favorites** (RADUIS Auth Reports)
   3. **Operations>Reports>ISE Reports>Top Authorizations By User**
   4. **Operations>Reports>ISE Reports>RADIUS Authentications**
   5. **Operations>Reports>ISE Reports>Authentication Summary**