



Cisco TrustSec™ 2.0: Design and Implementation Guide

Contents

Contents.....	2
Introduction	4
What is the Cisco TrustSec System?	4
About This Document.....	4
Scenario Overview	5
<i>Architecture</i>	5
<i>Components</i>	6
<i>Enforcement Discussion</i>	9
Predeployment Check List.....	11
Common Configuration: All Use Cases.....	13
Introduction	13
Universal Cisco ISE Configuration	13
<i>General Settings – Certificates and Certificate Authorities</i>	13
<i>Active Directory Integration</i>	18
Universal Cisco ISE Configuration – Device Profiling	25
Universal Cisco ISE Configuration: Guest.....	37
<i>Introduction</i>	37
Supplicant Configuration.....	48
<i>Cisco AnyConnect Network Access Manager</i>	48
<i>IP Phones</i>	58
Switches – Universal Global Configuration Commands.....	59
<i>Example Global Configuration</i>	64
Switches: Universal Switchport Configuration.....	65
Wireless – Universal Configuration	69
Base-Identity Use Cases	81
Introduction	81
Phase 1: Monitor Mode	85
<i>Configure Monitor Mode</i>	85
<i>Monitoring in Monitor Mode</i>	94
Phase 2: Authenticated Mode.....	99
<i>Wired Access</i>	99
<i>Wireless Access</i>	107
<i>Elaboration on Wireless Access</i>	108
<i>Wireless in Branch Offices</i>	108
<i>Web Authentication</i>	109
<i>Committing to Authenticated Mode</i>	118
Phase 3: Enforcement Mode	120
<i>Wired Access</i>	120
<i>Wireless: Bring Your Own Device</i>	125
Cisco IP Phones.....	128
<i>Certificates</i>	128

<i>Device Behind Phone Disconnects: The Link State Problem</i>	139
Expanded Services	141
Introduction to Security Group Access	141
SGA Use Cases.....	141
<i>Access Layer to Data Center</i>	141
<i>Intra-Data Center Enforcement</i>	143
<i>Additional Security Group Access Information</i>	156
Posture Assessment.....	161
<i>Introduction</i>	161
<i>Client Provisioning</i>	161
<i>Posture Policy</i>	161
<i>Authorization Policy</i>	161
<i>Cisco NAC Agent 4.9.0 Discovery Process</i>	170
Appendix A: Cisco ISE Design Notes	171
Standalone:.....	171
Basic 2-Node Deployment:	171
Distributed Deployment, Up to 10,000 Endpoints.....	172
Distributed Deployment, Up to 100,000 Endpoints.....	172
Appendix B: References	178
Switch Configuration Guides:	178

Introduction

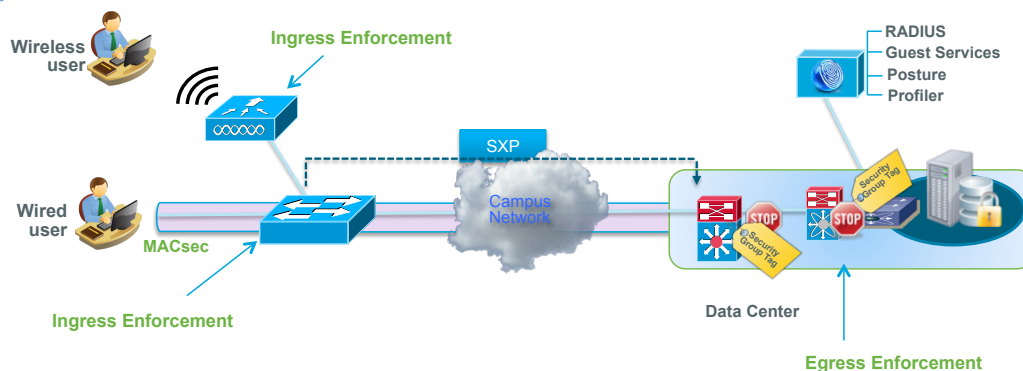
What is the Cisco TrustSec System?

The Cisco TrustSec® System is an advanced Network Access Control and Identity Solution that is integrated into the Network Infrastructure. It is a fully tested, validated solution where all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

Unlike overlay Network Access Control solutions, the Cisco TrustSec system utilizes the access layer devices (switches, wireless controllers, etc.) for enforcement. Functions that were commonly handled by appliances and other overlay devices, such as URL redirection for web authentications, are now handled by the switch itself.

The Cisco TrustSec system not only combines standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, it also has many more advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

Figure 1: Cisco TrustSec Architecture Overview



About This Document

This document describes the best practice for Cisco TrustSec deployments. It is a validated system that has undergone thorough architectural design development and lab testing. For a configuration or feature to be included in this document, it must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution they will not be included in this document. The Cisco TrustSec team at Cisco strives to provide regular updates to this document that will include new features as they become available, and are integrated into the Cisco TrustSec test plans, pilot deployments, and system revisions (i. e., Cisco TrustSec 2.1).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in this document. (Example: certain 802.1X timers and local web authentication)

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for Cisco TrustSec deployment as prescribed by best practices to ensure a successful project deployment.

Warning: The document has been designed to be followed from beginning to end – bypassing sections may have undesirable results.

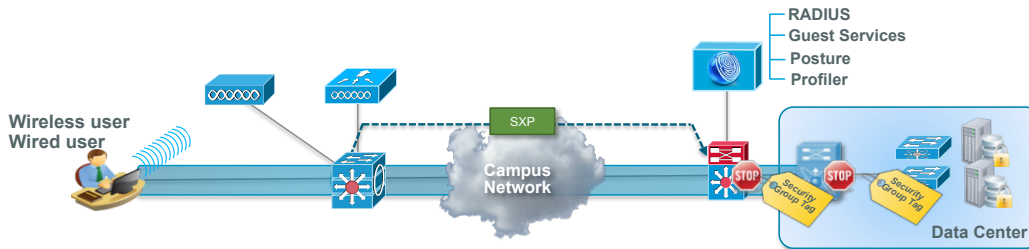
Scenario Overview

Architecture

Figure 2 depicts an end-to-end Cisco TrustSec architecture. While all the scenarios pictured in Figure 1 were part of the solutions test, this document will focus on the wired and wireless user scenarios along with SGA enforcement in the Data Center only. No VPN or VDI scenarios are covered in this version.

This document focuses on Authentication in the access layer of the network, applying ingress filter control (control at the entry point to the network). Additionally, future capabilities will use the power of a Cisco® infrastructure to allow tagging of traffic at the ingress point and enforcement of that control at egress.

Figure 2: Cisco TrustSec Architecture



In the previous release of Cisco TrustSec (1.99), the solution provided basic network access control by integrating 802.1X technologies with Cisco Catalyst® Switch families, Cisco Secure Access Control System 5.2 (ACS), and Cisco Secure Services Client 5.1 (Cisco SSC). With those products, managed users and devices authenticate to the network using 802.1X authentication and are authorized based on various attributes such as user role, device role, location, and time. The Cisco TrustSec 1.99 solution also added an ability to serve guest users for wired networks by integrating Cisco NAC Guest Server 2.03, making the whole guest management lifecycle much easier. Authenticated sponsors can provision guest accounts, notify users, manage duration of guest access, and monitor the account validity.

With the introduction of Cisco TrustSec 2.0, we are going to have 3 major changes on top of the previous release:

First, we have consolidated the functions from Cisco ACS 5.0 and Cisco NAC Guest Server 2.0 into the Cisco Identity Services Engine 1.0 (ISE). Cisco ISE is Cisco's next-generation policy server that provides authentication and authorization infrastructure to the Cisco TrustSec solution. It also provides two other critical services. The first service is to provide a way to profile endpoint device type automatically based on attributes Cisco ISE receives from various information sources. This service (called Profiler) provides equivalent functions to what Cisco has previously offered with the Cisco NAC Profiler appliance. Another important service that Cisco ISE provides is to scan endpoint compliancy; for example, AV/AS software installation and its definition file validity (known as Posture). Cisco has been previously providing this exact posture function only with the Cisco NAC Appliance. Cisco ISE provides an equivalent level of functionality, and it is integrated with 802.1X authentication mechanisms.

Secondly, Cisco TrustSec 2.0 adds support for Wireless user access. With Cisco TrustSec 2.0, Cisco ISE provides the same authentication methods regardless of user access methods, which could be from wired line or Wi-Fi connection. Cisco ISE is also used to provide profiling mechanisms of mobile devices such as Apple iDevices (iPhone, iPad, and iPod), Android-based smartphones, and others. For 802.1X users, Cisco ISE can provide the same level of services such as profiling and posture scanning. Guest services on Cisco ISE can also be integrated with the Cisco Wireless LAN Controller by redirecting web authentication requests to Cisco ISE for authentication.

The last major change in the Cisco TrustSec 2.0 revision is the introduction of Security Group Access (SGA) with Cisco ISE integration. Security Group Access (SGA) is a technology where a unique security tag is used to filter traffic from a specific source to a specific destination. For instance, a contractor authenticates to the network using the Web Authentication portal, and that contractor can be assigned to a specific security group named: CONTRACTOR. All the traffic this user is going to inject into the network will be tagged as CONTRACTOR and routed to the point where policy is enforced. When this tagged traffic reaches to the point where the destination resource is connected, the network infrastructure enforces a policy known as the Security Group Access Control List (SGACL). SGA moves the traffic filtering point from traditional ingress enforcement to egress enforcement, making the system much more scalable to support today's business requirements.

Components

Table 1: Cisco TrustSec 2.0 System Tested Components

Component	Hardware	Features Tested	Cisco IOS® Software Release
Cisco Identity Services Engine (ISE)	Any: 1121/3315, 3355, 3395, VMware	Integrated AAA, policy server, and services (guest, profiler, and posture)	ISE 1.0(377)
Cisco Catalyst 29xx Switch Cisco Catalyst 3xxx Switches	2960, 2960S, 3560, 3560E, 3560X, 3750, 3750E, 3750X	Basic Identity features, 802.1X authentication, Profiling, and Change of Authorization (CoA)	12.2(55)SE3
	3560X, 3750X	MACsec Switch-to-Switch	15.0(1)SE1
Cisco Catalyst 4500 Switches	Not tested in 2.0	Not tested in 2.0	Not tested in 2.0
Cisco Catalyst 6500 Switches	Supervisor Engine 32 and Supervisor Engine 720	Basic Identity Feature, 802.1X authentication, SXP, SXP IPv6, VRF-Aware Cisco TrustSec security, Profiling, and Change of Authorization (CoA)	12.2(33)SX17
	Supervisor Engine 2T	Basic Identity Features, 802.1X authentication, SXP, MACsec Switch-to-Switch, SGT and SGACL enforcement, Profiling, and Change of Authorization (CoA)	12.2(50)SY
Cisco Nexus® 7000 Switches		MACsec switch-to-switch, SGT, and SGACL enforcement	5.2.1
Cisco AnyConnect™ technology		Integration of 802.1X supplicant (no MACsec)	AnyConnect 3.0.0631
Wireless LAN Controller (WLC)		Profiling and Change of Authorization (CoA)	Unified Wireless 7.0.116
Cisco ASR 1000 Series Aggregation Services Router	Cisco ASR 1000 Series Route Processor 1 (RP1) and RP2, 1001, 1002, 1004, 1006, and 1013; Cisco ASR 1000 Series Embedded Services Processor 10 (ESP10), ESP20, and ESP40; and Cisco ASR 1000 Series SPA Interface Processor 10 (SIP10) and SIP40	SGA integration – SXP/SGT for tagging at WAN aggregation layer or extranet	3.4
Cisco IP Phone	Cisco Unified IP Phone 7960 and 7961; 7962 and 7969; and 7940, 7941, and 7942	Cisco IP Phones tested in the system-level test	

Note: Cisco Catalyst 4500 Series Switches did not participate in the testing of the Cisco TrustSec 2.0 Solution. The features required were not available at the time of the testing, even though they are today. As of October, 2011: Cisco IOS Software Release 15.0(2)SG1 is the recommended version for interaction with Cisco ISE in a Cisco TrustSec deployment. The Cisco Catalyst 4500 switch will be part of the Cisco TrustSec 2.1 System.

Note: Cisco ISE 1.0 Maintenance Release 2 (Cisco ISE 1.0.4(573)) is available from Cisco.com; this release is highly recommended for all customers for upgrade.

Note: In order to support SGA features, the image needs to be crypto image (K9). In order to support SGA (SGT, SGACL) with Cisco Catalyst 6500 switch Supervisor Engine 2T, the Supervisor Cisco IOS Software image needs to be Advanced IP Services or Enterprise Advanced. SGACL is not available with IP Base at the time of this document creation.

Table 2: Supplicants Tested in Cisco TrustSec 2.0

Vendor	Software	Supplicant
Microsoft	Windows 7	Wired Auto Config Service (Native Supplicant) Cisco Secure Services Client 5.1.1.17 Cisco AnyConnect 3.0.0631
	Windows Vista with SP2	Wired Auto Config Service (Native Supplicant) Cisco Secure Services Client 5.1.1.17 Cisco AnyConnect 3.0.0631
	Windows XP with SP3	Wired Auto Config Service (Native Supplicant) Cisco Secure Services Client 5.1.1.17 Cisco AnyConnect 3.0.0631
Apple	MacOS 10.6.5	Eapolclient (Native Supplicant)

In the architecture for this document, we have used various Cisco network devices to validate component interaction, functions, and integration. We have a Campus network segment, a Data Center network segment, a WAN segment, and a Branch-office segment. In the Campus network, a Cisco Catalyst 3560-X Series Switch is used for the access layer. A Cisco Catalyst 6500 switch with Supervisor Engine 2T is used to aggregate all access layer switches. This Cisco Catalyst 6500 Switch is connected to the Data Center segment, which consists of 2 sets of Cisco Nexus 7000 switches (Core and Distribution) using Virtual Device Context (VDC) technology, and a Cisco Catalyst 4948 Switch as the Data Center access (Top Of the Rack) switch.

Figure 3: Baseline Architecture for the Cisco TrustSec 2.0 Design and Implementation Guide.

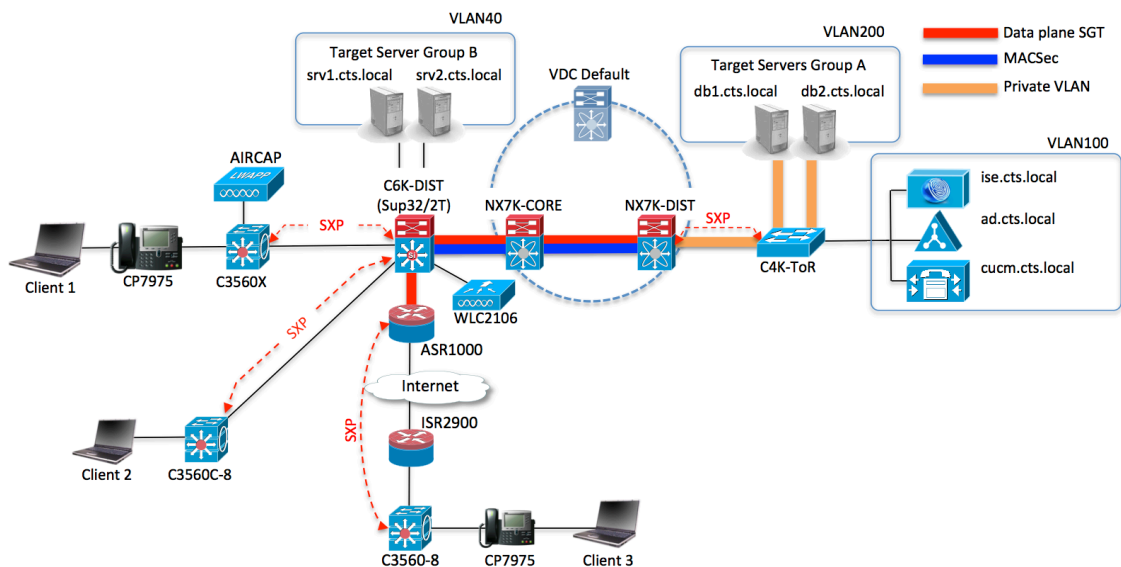


Table 3 lists the components (Non-network Equipment) and associated information.

Table 3: Components

Component	IP Address	Description
Microsoft Windows Server 2008	10.1.100.100/24	Active Directory, CA, DHCP, DNS
Cisco Unified Communications Manager	10.1.100.40/24	Communications Manager for IP Phone Voice service
Target Servers	10.1.40.100, 10.1.40.200, 10.1.200.100, 10.1.200.200/24	Servers to be used for SGACL access

Table 4: User Accounts in Active Directory:

Username	Group Membership	Password
employee1	Employees, Sponsors_Full, Domain Users	Cisco123
contractor1	Contractors, Domain Users	Cisco123
employee2	Employees, Sponsors, Domain Users	Cisco123
hr1	HR, Employees, Sponsors_Full, Domain Users	Cisco123
sales1	Sales, Employees, Sponsors, Domain Users	Cisco123
engineer1	Engineering, Employees, Sponsors, Domain Users	Cisco123

Enforcement Discussion

In the Cisco TrustSec 2.0 architecture, the system provides three major functions to allow more scalable network access control: authentication, classification, and authorization.

Authentication identifies endpoints by acquiring and validating the device credentials to ensure that only appropriate endpoints (including users and devices) are connecting to the network. In the authentication process, the system matches several endpoint attributes to specific policies in order to classify those endpoints into a certain category or group. After classifying endpoints, we can finally match the final policy to authorize endpoints in the network.

The Cisco TrustSec system provides three methods of authentication:

- 802.1X-based endpoint authentication. This process includes 802.1X-based user authentication as well as device authentication.
- MAC Authentication Bypass. This method is used to authenticate a device using its MAC Address as credential.
- Web Authentication using Captive Portal. This method is used when the endpoint is attended with a user but there is no 802.1X supplicant installed or enabled on the machine.

Table 5: Authentication Methods Summary

Methods	Description	Pros	Cons
802.1X	Uses IEEE 802.1X technology to authenticate endpoint in Layer 2 mode using Extended Authentication Protocol (EAP)	Standard-based authentication provides the most secure authentication methods.	Supplicant (agent) needs to be installed and running on the endpoint. Supplicant behavior can be different based on OS type and supplicant vendor type.
MAC Authentication Bypass (MAB)	When an endpoint is not equipped with an 802.1X supplicant (authenticating software) and no user is attended to this device (such as with network printers), the switch can be configured to send the endpoint MAC Address on behalf of the endpoint, to be used as its credential.	Easy way to provide an authentication method for non-802.1X devices. Useful when device such as Network Printers or IP Phone does not support 802.1X supplicant.	Least secure method; MAC Address is used for its credential, and this address can be easily spoofed. MAC Address needs to be stored in the database to be authenticated.
Web Authentication	User is prompted to provide credential on web browser. Method does not require any 802.1X supplicant; therefore it is used frequently for Guest Access Management.	Browser is needed to provide user credential. Since supplicant is not required, there is no OS dependency for this authentication method.	There are some variations in methods (Local Web Auth and Centralized Web Auth). VLAN assignment is not currently supported with wireless WebAuth.

After authenticating the endpoint, the Cisco TrustSec system can classify it and apply a specific policy for this endpoint. The process of applying policy is called authorization, and this process is used mainly for enforcement purposes. Cisco TrustSec security supports several authorization (enforcement) methods.

Table 6: Summary of Authorization Methods

Methods	Description	Pros	Cons
Dynamic VLAN Assignment (dVLAN)	<p>As an authorization, the VLAN attribute is returned by Cisco ISE to the switch or WLC.</p> <p>Result:</p> <p>Wired: The switchport that the endpoint is connected to is assigned to a specific VLAN and segmented.</p> <p>Wireless: The wireless clients traffic will be tagged out of the WLC into the wired network in the appropriate VLAN. Cisco WLCs will do this through a “dynamic interface” on the WLC.</p> <p>This authorization is based on RFC 3580 and utilizes RADIUS Attributes 64, 65, and 81.</p>	Easiest way to enforce and segment endpoints because this method is supported by standards: other vendor switches and AAA servers also support this method.	VLAN assignment can result in subnet change, and usually this change is not communicated to the endpoint. Detection of subnet change is completely based on OS/supplicant implementation. VLAN-to-VLAN policy control needs to be implemented to control traffic from one segment to others. Adding VLANs in the large corporate network can be costly.
Downloadable ACL (DACL) / Wireless ACL (wACL)	<p>Wired (DACL): Cisco ISE sends specific attributes that contain a set of Access Control Entries (ACEs) to the switch. Switch then apply this ACL to a session based on IP address of the endpoint.</p> <p>Wireless ACL (wACL): Cisco ISE sends the name of the ACL that is configured on the WLC. The WLC will apply that preconfigured ACL to the endpoints session.</p>	More flexible way to block traffic from source to certain destination. Since all ACLs are configured on Cisco ISE centrally, there is no need to change ACL on local switch. With Wireless all wACLs may be configured on the WLC or through WCS.	<p>Since ACL consumes TCAM space on the switch, the amount of ACLs that the switch downloads per user needs to be well examined and limited.</p> <p>wACLs may not be configured or managed via Cisco ISE today. They must be created on the WLC or through WCS.</p>
Security Group Tag / Security Group ACL	In an authorization process, authorized endpoint IP address is tagged with special Tag called Security Group Tag (SGT). This tag can be used in the network to be filtered when tagged traffic reaches an egress switch at the packet destination. Using SGACL, packet can be permitted / dropped based on the TAG value and policy.	Since SGT is used to classify user and filter traffic, the management of the access control becomes easier and more efficient than the other two methods. Also SGACL is a method to filter traffic right before the packet reaches out to destination resource. Therefore there is no effect on access switch TCAM space.	<p>In order to support SGT/SGACL, both software and hardware need to support this authorization method to be deployed.</p> <p>Wireless LAN controllers do not support SGT in 2.0. This function is slated for a near-future Cisco TrustSec release.</p>

Predeployment Check List

Table 7 shows a simple Pre-deployment Check List. Filling this out will help ensure you have some of the required basic information before beginning the Cisco TrustSec deployment. For a more complete High-Level Design, contact a certified Cisco Advanced Technology Partner for Cisco ISE / Cisco TrustSec deployments.

Table 7 Pre-Deployment Check List

Are the Switches and Wireless LAN Controllers running a supported Version?			
<input checked="" type="checkbox"/>	Model	Cisco IOS Software Release	
<input type="checkbox"/>	Cisco Catalyst 3750 Switch Cisco Catalyst 3560 Switch Cisco Catalyst 2960 Switch	12.2(55)SE3	
<input type="checkbox"/>	Cisco Catalyst 6500 Switch	12.2(33)SXJ1	
<input type="checkbox"/>	Cisco Wireless LAN Controller	7.0.116	
<input type="checkbox"/>	Cisco Nexus 7000 Switch	5.2.1	
Are the corporate endpoints running recommended versions (or newer)?			
<input checked="" type="checkbox"/>	Operating System	Minimum Version	Supplicant
<input type="checkbox"/>	Microsoft Windows 7	-	Dot3 Service Cisco SSC 5.1 SSC AnyConnect 3.0
<input type="checkbox"/>	Microsoft Windows Vista	Service Pack 2	Dot3 Service Cisco SSC 5.1 SSC AnyConnect 3.0
<input type="checkbox"/>	Microsoft Windows XP	Service Pack 3	Dot3 Service Cisco SSC 5.1 SSC AnyConnect 3.0
<input type="checkbox"/>	Apple Mac OS X	10.6.5 10.6.6 10.7.1	Native
Cisco Identity Services Engine			
<input checked="" type="checkbox"/>	Minimum Version	Personas Installed	Notes:
<input type="checkbox"/>	Cisco ISE 1.0.3.377		It is recommended to install Cisco ISE MR2 (1.0.4.573) because of bug fixes; however, that is not the version that was used in this system test. Best Practice: Use lowercase letters in hostnames Best Practice: Use UTC time zone
<input type="checkbox"/>		Administration Node	All Personas may be installed on a single Cisco ISE node or distributed across multiple Cisco ISE nodes. For more on Cisco ISE Deployment Design, see Appendix A: Cisco ISE Design
<input type="checkbox"/>		Monitoring Node	
<input type="checkbox"/>		Policy Services Node	

Note: There are no official acronyms for the Cisco ISE Personas. However, there are some common acronyms that may be heard throughout the industry: Admin Node (Policy Administration Point or PAP); Monitoring Node (Monitoring & Troubleshooting or M&T); Policy Service Node (PSN, Policy Decision Point or PDP).

Active Directory		
<input checked="" type="checkbox"/>	Service	Information
<input type="checkbox"/>	AD Domain	Domain Name:
<input type="checkbox"/>	AD Sites and Services	Will the Domain Controller Selection be predictable, based on the source subnet of the client?
<input type="checkbox"/>	Multiple Domains?	Will there be Multiple Domains? If so, Trust-Relationships will be required.

Make note of other Network and Endpoint Services:		
<input checked="" type="checkbox"/>	Service	Information
<input type="checkbox"/>	NTP Servers	
<input type="checkbox"/>	DNS Servers	
<input type="checkbox"/>	DHCP Servers	
<input type="checkbox"/>	LDAP (non-AD) Servers	
<input type="checkbox"/>	Certificate Services (PKI)	
<input type="checkbox"/>	One-Time Password (OTP) Servers	
<input type="checkbox"/>	Antivirus Products	
<input type="checkbox"/>	Antispyware Products	
<input type="checkbox"/>	Software Distribution / Remediation Services	

Common Configuration: All Use Cases

Introduction

Within this document, we describe the recommended path for deployment and a few different options depending on the level of security needed in your environment. This section provides a “universal configuration” that applies to all deployment models and stages while following deployment best practices.

Universal Cisco ISE Configuration

Note: This stage of the document assumes you have already successfully installed Cisco ISE.

See http://www.cisco.com/en/US/docs/security/ise/1.0.4/user_guide/ise104_user_guide.html for the Cisco ISE user guide. We will follow Cisco ISE as a single node installation. For information on Cisco ISE design and scale, see [Appendix A: Cisco ISE Design](#).

General Settings – Certificates and Certificate Authorities

When installing Cisco ISE, it generates a default, self-signed certificate. While this is usually good enough for labs and demonstrations, it is not good practice to put Cisco ISE into production with a self-signed certificate.

Note: Time synchronization is extremely important to certificate operations. Ensure that you have configured NTP and have the correct time.

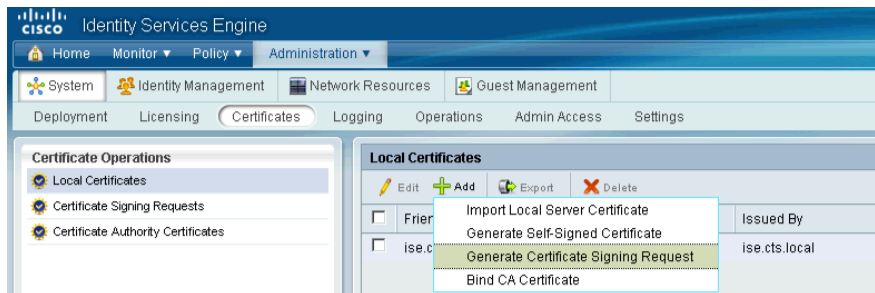
Cisco ISE Configuration – Certificates and Trusting the CA

Note: For Certificate Chains: The entire chain should be imported successfully before the Certificate Request is created.

Procedure 1 Request a Certificate from the Certificate Authority.

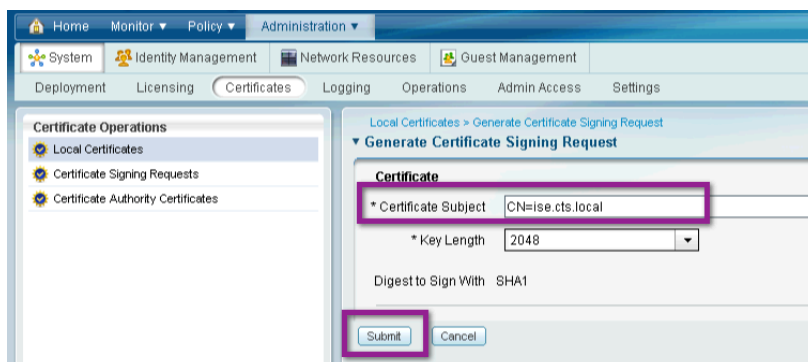
Step 1 Go to Administration → System → Certificates → Local Certificates

Step 2 Click Add → Generate Certificate Signing Request

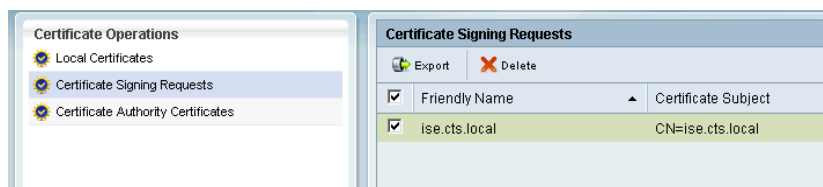


Step 3 Enter the fully qualified domain name (FQDN) for the Cisco ISE node into the **Certificate Subject** field, and click **Submit**.

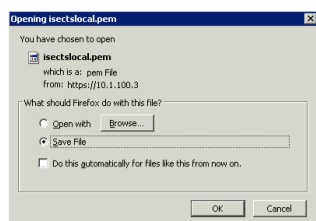
Note: The FQDN is the full name of the Cisco ISE Node ([hostname].[domain name]) and it is case-sensitive.



Step 4 Click **Certificate Signing Requests** and select your new request. Click **Export**.



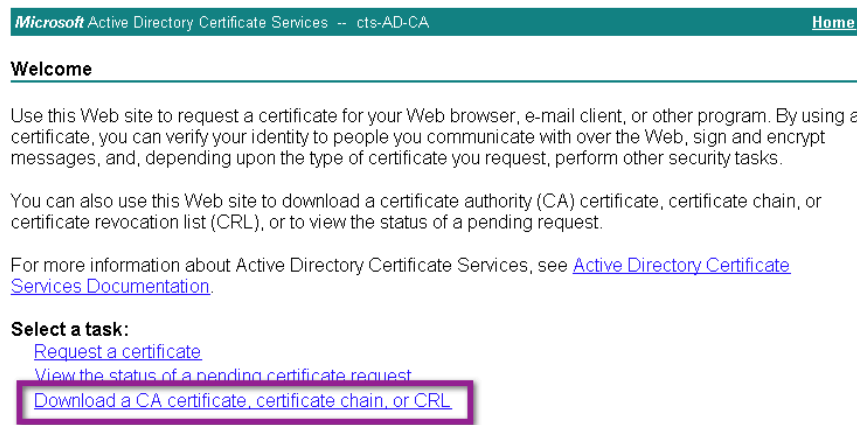
Step 5 Save the .pem file to an easily accessible location.



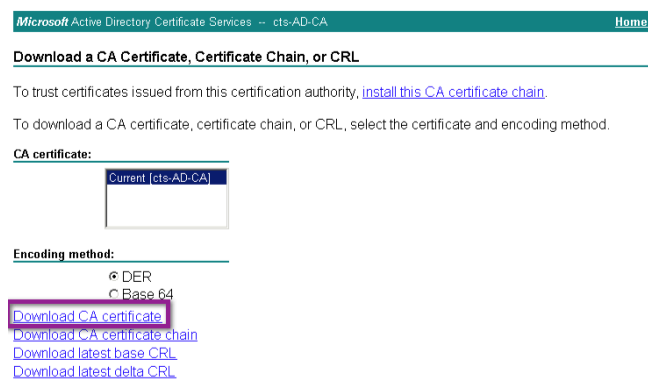
Procedure 2 Download the Certificate Authority root certificate, and issue a certificate for Cisco ISE.

Step 1 Browse to your CA. Click "Download a CA certificate, certificate chain, or CRL".

Note: We are using a Microsoft Certificate Authority; therefore we are browsing to <http://ad.cts.local/crtsrv/>. Depending on the Certificate Authority in your organization, the certificate request will follow a different procedure. When using the Microsoft CA, it has been noted that using Internet Explorer will provide a better experience.



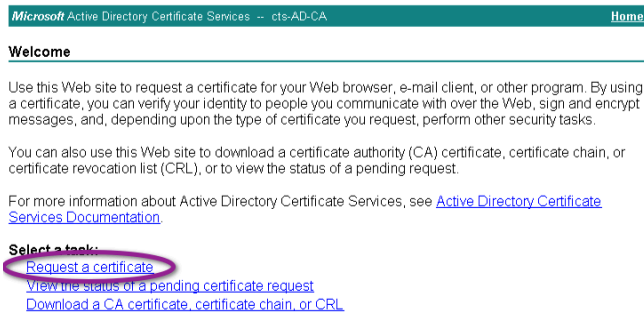
Step 2 Click "Download CA certificate".



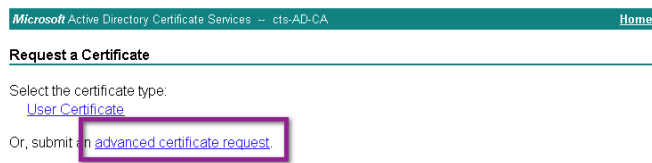
Step 3 Save the resulting .cer file in a location that can be easily accessed later. Name the file something unique, such as "RootCert.cer".

Step 4 Click Home, in the upper right corner.

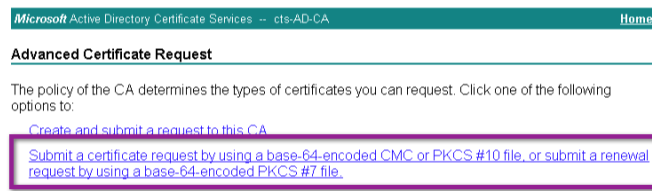
Step 5 Click "Request a Certificate".



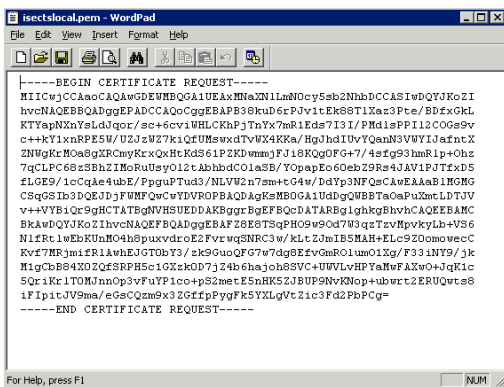
Step 6 Click "advanced certificate request".



Step 7 Select the option of using a base-64-encoded CiscoWorks 2000 Management Connection (CMC).



Step 8 Open the .pem file saved in Procedure 2 with WordPad (or another text editor). Highlight the entire contents of this file and Select **Edit** → **Copy**.



Step 9 Paste the contents from the certificate request .pem file into the text box in the Certificate Authority Window. Certificate Template should be set to "Web Server".

Microsoft Active Directory Certificate Services -- cts-AD-CA Home

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):

```
N1fRt1wEbKUnMO4h8puxvdr0E2FvqwSNRC3w/kL
Rvz7MRjmiFRIAwHEJGTObY3/zk9GuoQFG7w7dg8E
M1gCbB84X0ZQFSRPHSc1GXzkOD7j24b6hajoh8SV
5Qr1Rt1T0HJnnOp3vFuYP1co+pS2metE5nHK5ZJB
iF1p1tJV9ma/eG8CQzm9x3ZGfFpFgFk5YXLgVtZ
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Step 10 Click Submit.

Step 11 Click "Download certificate".

Microsoft Active Directory Certificate Services -- cts-AD-CA Home

Certificate Issued

The certificate you requested was issued to you.

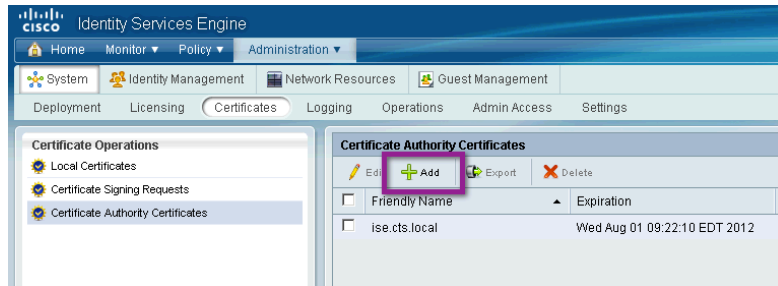
☒ DER encoded or ☐ Base 64 encoded

[Download certificate](#) [Download certificate chain](#)

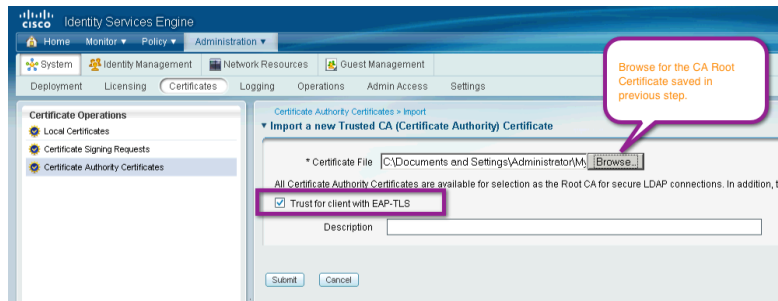
Step 12 Save the resulting .cer file in a location that can be easily accessed later. Name the file something unique, such as "ISECert.cer".

Procedure 3 Install the Root Certificate in Cisco ISE to be trusted for 802.1X.

Step 1 In the Cisco ISE administrative interface, navigate to Administration → System → Certificates → Certificate Authority Certificates. Click “Add”.



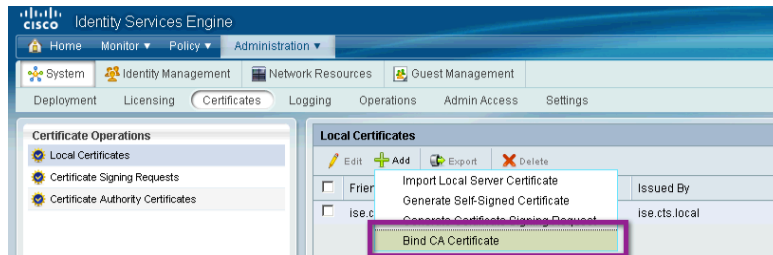
Step 2 Browse for the Root CA Certificate saved in Step 3. Select the Check Box for “Trust for client with EAP-TLS”. Click Submit.



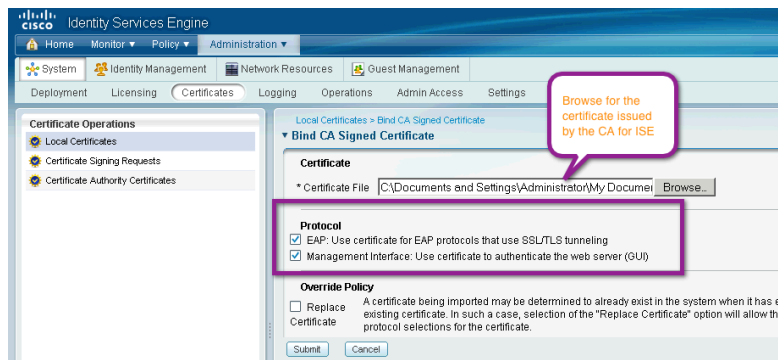
Procedure 4 Install the new local Certificate.

Now that the Root CA is trusted, it is time to replace the self-signed certificate with the CA-issued certificate, and delete the completed Certificate Signing Request.

Step 1 From Administration → System → Certificates → Local Certificates, Click Add → Bind CA Certificate.



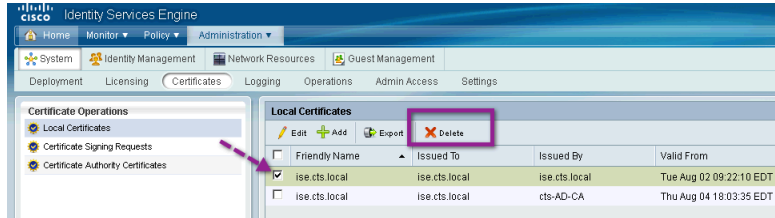
Step 2 Browse for the certificate issued by the CA for Cisco ISE. Select both the EAP and Management Interface check boxes. Click Submit.



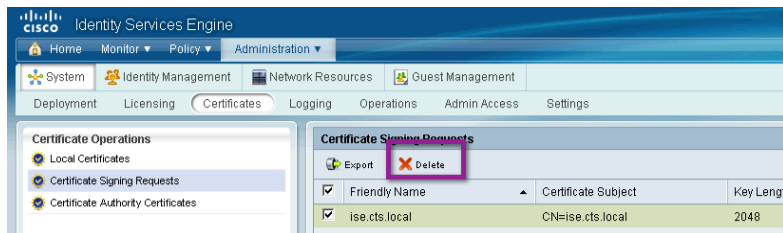
Note: If you did not create the certificate request with the same full name as the Cisco ISE server, you will receive an error message. Delete the old Certificate Signing Request, and start again.

Procedure 5 Clean Up Old Certificates and CSRs

Step 1 Delete the Old Certificate. Select the Self-Signed Certificate and Click Delete.



Step 2 Click "Certificate Signing Requests". Select the Certificate Signing Request (CSR), and delete.



Active Directory Integration

The single most common Policy Information Point (PiP) used with Cisco TrustSec deployments is Active Directory. Cisco ISE uses an Active Directory connector where each Cisco ISE node in a Cisco TrustSec deployment will join the AD Domain, and access AD resources just like any other Windows domain member. This scenario allows for tremendous increase in speed, ease of use, and flexibility when using Active Directory with Cisco TrustSec security.

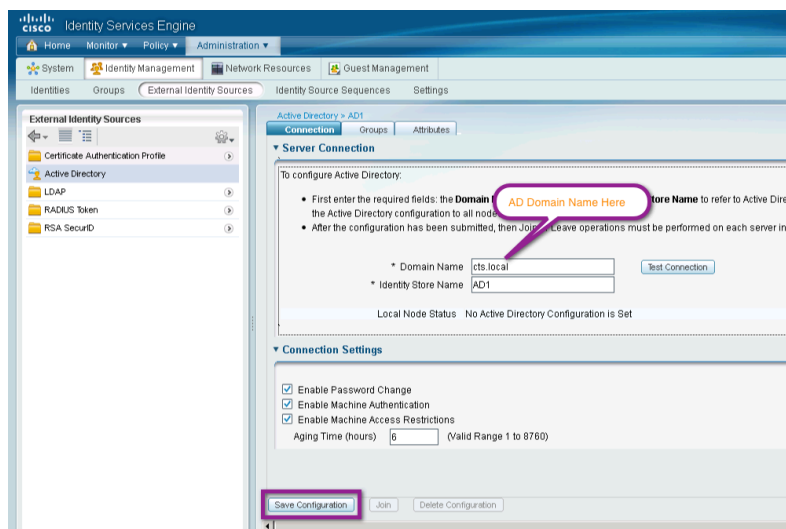
Best Practice: Both Time Synchronization and DNS are critical to a solid integration with Active Directory. Therefore, always use Network Time Protocol (NTP) and always ensure DNS is configured correctly, with reverse-DNS pointers for all Active Directory Servers.

Procedure 1 Join the Domain.

Note: Each Cisco ISE node joins the domain separately. The following is a list of ports that must be open between all Cisco ISE Nodes and Active Directory: SMB(TCP/445); KDC(TCP/88); Global Catalog(TCP/3268 & 3289); KPASS(TCP/464), NTP(UDP/123); LDAP(TCP & UDP/389), and LDAPS(TCP/636).

Step 1 Administration → Identity Management → External Identity Sources → Active Directory

Step 2 Enter the AD Domain Name and click **Save Configuration**.



Step 3 Click Join.

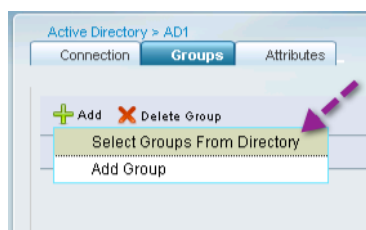
A “Join Domain” pop-up window will appear. Enter a username and password for an AD account with rights to join a workstation to the domain, such as “administrator”.

Note: Time synchronization is extremely important to successfully join the domain. Ensure you have the correct Time and have configured NTP.



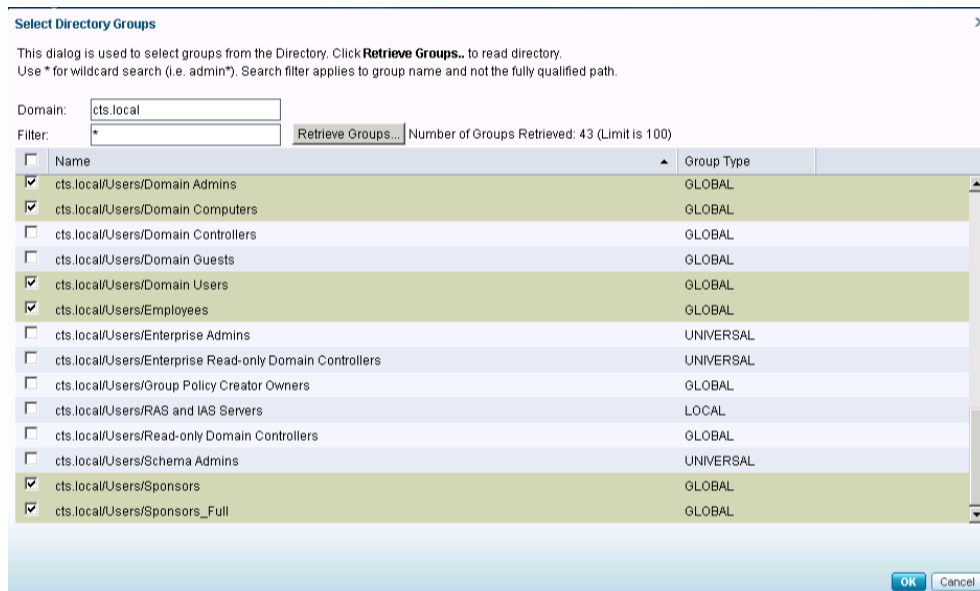
Step 4 Click Groups → Add → Select Groups From Directory.

Cisco ISE allows a network administrator to select specific groups and attributes from Active Directory. This scenario enables faster lookup times when authenticating a user against AD. It also ensures that when building policy related to AD groups, the administrator needs to look through only a small list instead of every group in AD.

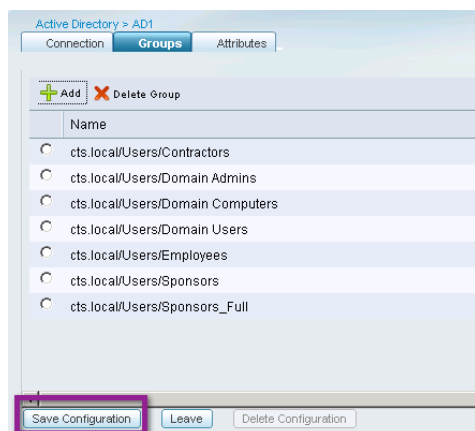


Step 5 Select groups that you will want to use in policy decisions.

Select groups that will be used in your Network Access Policies later. Common groups would be: Domain Computers, Contractors, Employees, Domain Users, and more. Groups may be added and removed at any time.



Step 6 After selecting all necessary groups, click OK. Then click Save Configuration.



Cisco ISE Configuration – Base Authentication Policy

Identity sequences are used in only ISE to provide a single “object” that is actually a sequence of Identity Stores that only ISE will query when validating credentials. In our configuration example, we will create an identity sequence that queries the following identity stores in order:

Active Directory → Internal Hosts → Internal Users

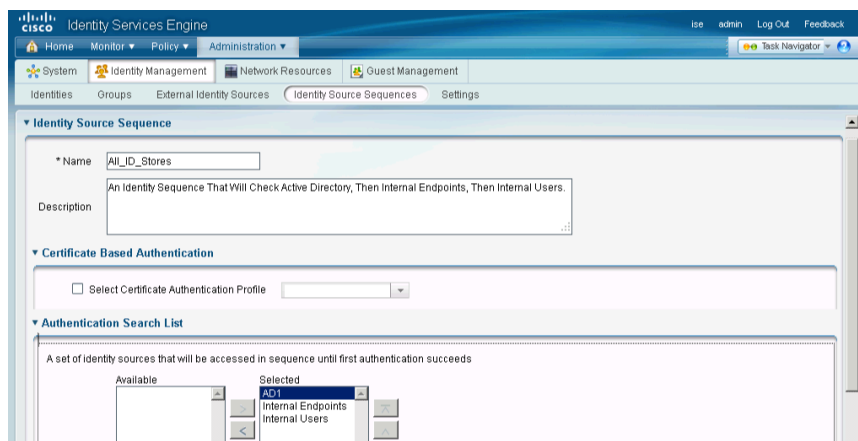
Procedure 1 Create an Identity Sequence.

Step 1 Navigate to Administration → Identity Management → Identity Source Sequences.

Step 2 There are two Identity Source Sequences by default.

Step 3 Click **Add**.

Step 4 Name the Identity Sequence “**All_ID_Stores**”. Add the identity stores in the order shown in the following screenshot:



Step 5 Scroll to the bottom, and Click **Submit**

Cisco ISE Configuration – Add Network Devices

Any switch or Wireless LAN Controller that may be sending RADIUS requests to Cisco ISE to authenticate and authorize network clients should be added to Cisco ISE. While Cisco ISE does provide a “Default Device” that may be configured to allow any network device to send RADIUS Requests, it is not a good security practice to use this feature.

In order to provide a thorough level of Policy creation, as well as detailed levels of reporting, it is recommended to add all devices individually to Cisco ISE, and to use Network Device Groups (NDGs) to organize those network devices appropriately.

Note: For Bulk import of Network Devices and assignment of those devices to their respective NDGs, Cisco ISE provides an Import / Export mechanism. See the Cisco ISE User Guide (http://www.cisco.com/en/US/docs/security/ise/1.0.4/user_guide/ise104_user_guide.html) for more detailed instructions.

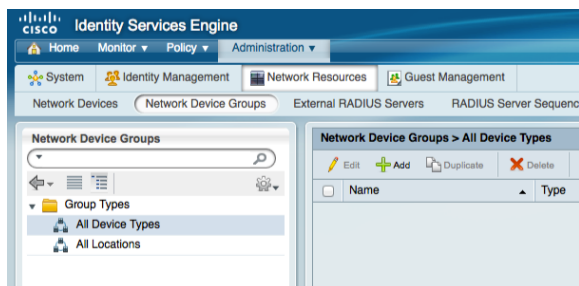
Procedure 1 Configure Network Device Groups.

Network Device Groups (NDGs) are a very powerful tool, when used appropriately. Cisco ISE has the power to use any number of attributes when it makes policy decisions. Network Device Group (NDG) membership is one such attribute that can be used as a policy condition.

Best practice: Always use NDGs for Device Types and Location at a minimum.

An example could be the creation of an NDG for switches, another for VPN devices, and a third group for Wireless LAN Controllers (WLCs).

Step 1 Go to Administration → Network Resources → Network Device Groups.



By default there are two top-level NDG types: All Device Types and All Locations. These types are a good start for most deployments. Your deployment may need to create multiple location sub-groups. The possibilities are virtually limitless (see the sample hierarchy that follows).

The group structure is hierarchical. So with an example group structure of: All Locations → North America → US → SJC → Building 18 → 3rd Floor, you can use any level of the group hierarchy in your policy. In other words, you can select “US” in your policy and get every device in every group underneath “US”.

Step 2 Expand Group Types.

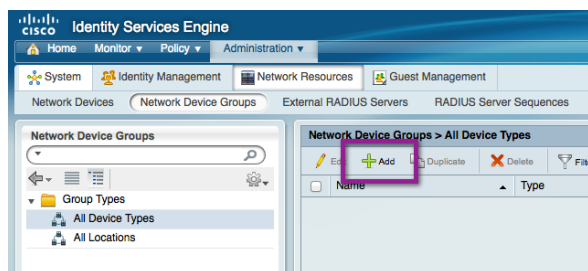
Note:

To create a Root NDG, click **Group Types** and click **Add**.

To create a child NDG, choose the root NDG add a child NDG, and click **Add**.

For the purposes of this document, we are going to create a Child NDG for both Device Type and Locations.

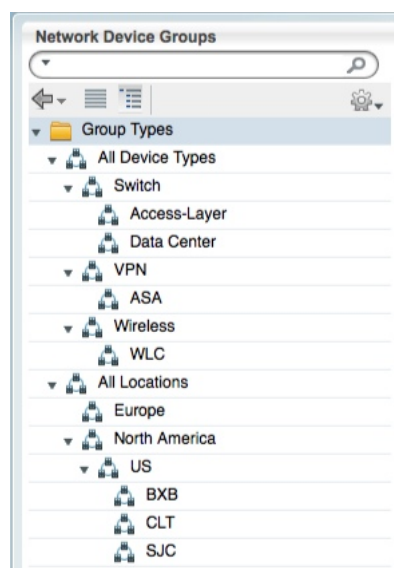
Step 3 Select All Device Types. Click Add



Step 4 Enter the name "Switch" in the Name Field.

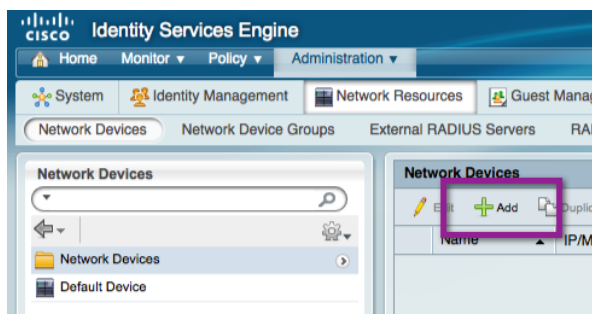
Step 5 Click Submit.

Repeat the process to build out your desired NDG hierarchy. Here is an example hierarchy:



Procedure 2 Add Network Device.

Step 1 Go to Administration → Network Resources → Network Devices.



Step 2 Click Add.

Step 3 Fill out the Name, IP Address, Network Device Group, Authentication Settings, and SNMP Settings sections.

Section	Purpose
General Settings	
Name	Use a name that is easy to distinguish later. The name will display in all the monitoring / dashboards / reporting later.
Description	Optional
IP Address	Must match the source interface chosen for RADIUS communication in the switch configuration section. Best practice is to use Loopback interfaces for management.
Model Name	Optional
Software Version	Optional

Section	Purpose
Network Device Group	
Location	Be as specific as possible.
Device Type	Be as specific as possible.
Authentication Settings	
Protocol	Will be prepopulated as RADIUS.
Shared Secret	Must match the RADIUS key configured on the switch.
SNMP Settings (used for device profiling)	
SNMP Version	Select the version in use in your organization.
SNMP RO Community	SNMP is used only for device profiling purposes. Cisco ISE will probe the switch for contents of Cisco Discovery Protocol tables, LLDP tables, and more.
SNMP Username	Used with SNMPv3 – must match the configuration on the switch.
Security Level	Used with SNMPv3 – must match the configuration on the switch.
Auth Protocol	Used with SNMPv3 – must match the configuration on the switch.
Privacy Protocol	Used with SNMPv3 – must match the configuration on the switch.
Polling Interval	It is not recommended to change the default polling interval: 3,600 sec
Link Trap Query	Configures Cisco ISE to accept linkup / linkdown SNMP traps from the switch. Leave this check box selected.
MAC Trap Query	Configures Cisco ISE to accept mac-address-table type traps from the switch. Leave this check box selected.
Security Group Access (SGA) – Not used at this stage of our deployment guide. This section will be revisited later, in the SGA section.	
Device Configuration Deployment – Not used at this stage of our deployment guide. This section will be revisited later, in the SGA section.	

The screenshot shows the 'New Network Device' configuration page in Cisco ISE. The form includes the following fields and callouts:

- Name:** SJC18-sw-1. Callout: "Name the device something easy to distinguish."
- Description:** Access-Layer Switch in
- IP Address:** 192.168.252.1 / 32. Callout: "Must match the Source-Interface commands on the switch"
- Model Name:** 3750-X. Callout: "Optional"
- Software Version:** (empty dropdown)
- Network Device Group:**
 - Location:** SJC. Callout: "Be as specific as possible"
 - Device Type:** Access-Layer
- Authentication Settings:**
 - Enable Authentication Settings:** ☒
 - Protocol:** RADIUS. Callout: "Must match the RADIUS key on the Switch"
 - Shared Secret:** (masked with asterisks) [Show]
- SNMP Settings:**
 - SNMP Version:** 2c
 - SNMP RO Community:** TrustSecRO. Callout: "Used for Profiling.. Read-Only, write access is not necessary."
 - SNMP Username:** (empty)
 - Security Level:** (empty dropdown)
 - Auth Protocol:** (empty dropdown)
 - Auth Password:** (masked) [Show]
 - Privacy Protocol:** (empty dropdown)
 - Privacy Password:** (masked) [Show]
 - Polling Interval:** 3,600 seconds (Valid Range 600 to 86400)
 - Link Trap Query:** ☒
 - MAC Trap Query:** ☒

Step 4 Click **Submit**. Repeat for all network devices (aka: Policy Enforcement Points).

Note: For bulk administration, network devices may be imported via CSV file. See the Cisco ISE user guide for more information.

Universal Cisco ISE Configuration – Device Profiling

Profiling design requires a lot of thought and planning.

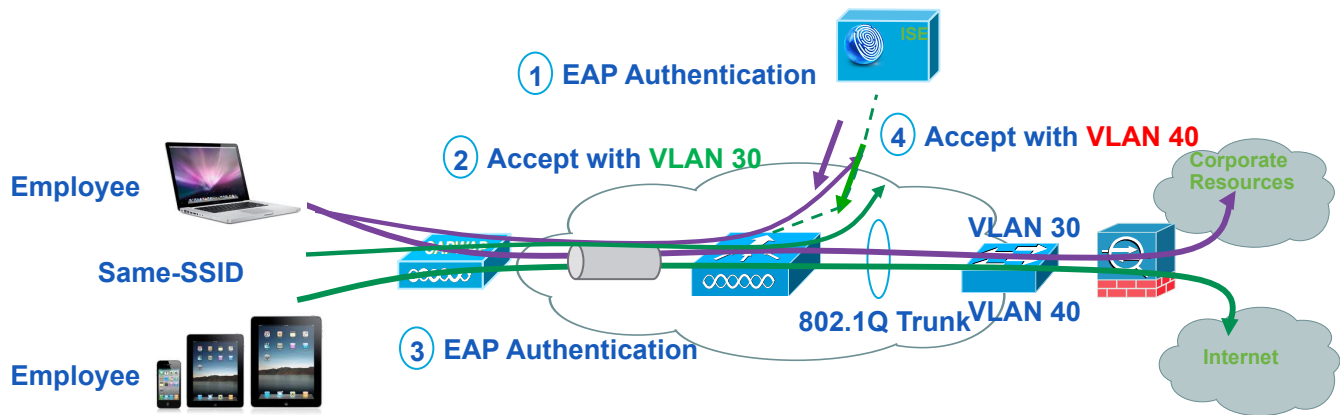
The Cisco ISE Profiler is the component of the ISE platform that is responsible for endpoint detection and classification. It does so by using an array of probes (Sensors) that collect attributes about an endpoint and a policy-based mechanism that evaluates the attributes to match the endpoint with a predefined profile.

The result of the collection and classification from the profiler are then used as conditions in the authentication and authorization policies. The classification result of profiling can be used to invoke a different authorization result.

The figure below is an example of a differentiated device policy based on profiling:

- Users, using the same SSID, can be associated to different wired VLAN interfaces after EAP authentication.
 - Employees using corporate laptop with their AD user id assigned to VLAN 30 = Full network access
 - Employees using personal iPads/iPhones with their AD user id assigned to VLAN 40 = Internet only

Figure 4: Example of Differentiated Device Policy



Cisco ISE Configuration – Enable Device Profiling Probes

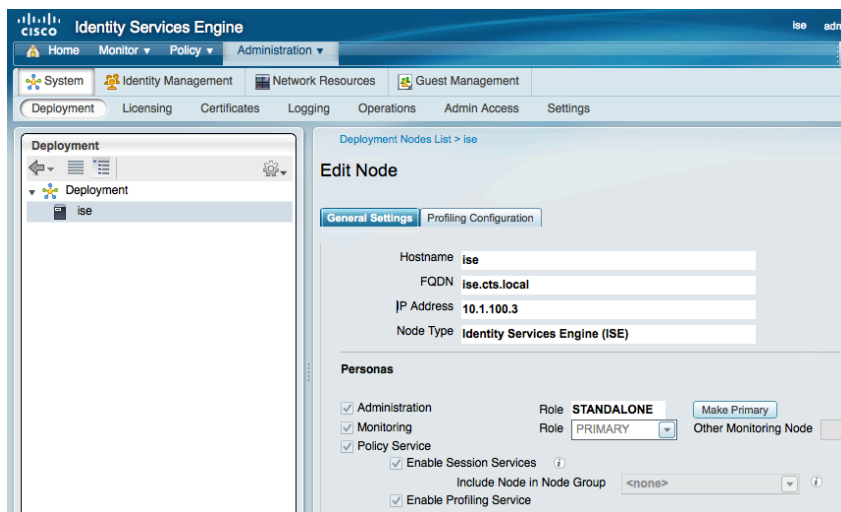
At this stage we will enable Profiling Probes on the Cisco ISE device. In a distributed deployment, profiling probes would generally be enabled on all the Policy Service Nodes (sometimes referred to as Policy Decision Points or PDPs). The specific details of which probes to enable and where to enable them can be complex and should be addressed in the high-level design process.

Procedure 1 Enable the Profiling Probes.

Step 1 Navigate to Administration → System → Deployment.

Step 2 Select the Policy Service Node.

This node may be a single Cisco ISE node as depicted here. Or, if your Cisco TrustSec deployment is distributed, then you should select one of the nodes configured for Policy Service. You will repeat these steps for each Policy Service node in the deployment.



Step 3 Ensure that “**Enable Profiling Service**” is checked.

Step 4 Click the Profiling Configuration Tab.

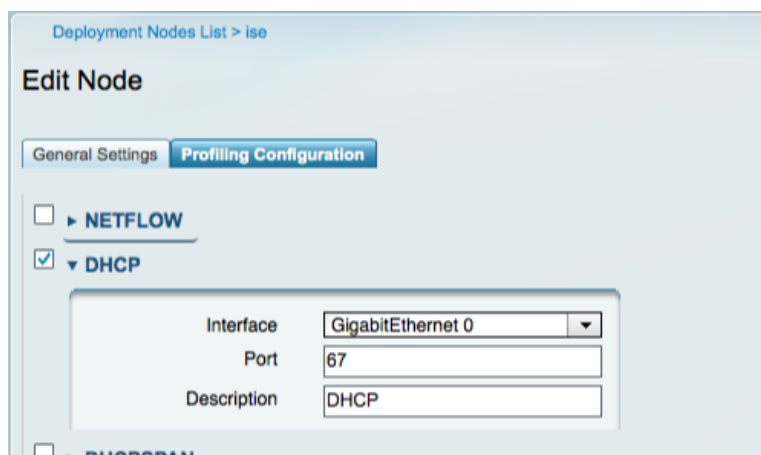
NetFlow: The NetFlow probe will not be enabled in this guide.

NetFlow is a very powerful tool, but its implementation must be thought out and implemented carefully. There are certain Cisco TrustSec implementations where NetFlow will be crucial. However, one of the important aspects of NetFlow is understanding what data to send from the infrastructure. This configuration is considered out of the scope of this guide, but will be in either a specific follow-on guide or in a future version of a Cisco TrustSec implementation guide.

Step 5 Enable the check box for **DHCP**.

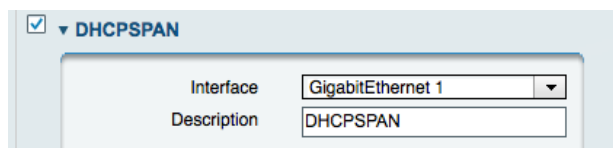
This is the **DHCP IP Helper probe**. It will listen to packets forwarded to it from the DHCP IP helper configured on the switch or other Layer 3 device. The IP Helper probe will listen to traffic from the DHCP client to server only (DHCPDISCOVER and DHCPREQUEST).

Enable this probe on a particular interface, or on all interfaces.



Step 6 Enable the check box for **DHCPSPAN**.

The **DHCP Span probe** will listen to packets forwarded to it from the SPAN session configured on the switch. This probe will listen to all of the DHCP traffic.



When a switchport is configured to be a SPAN (switchport analyzer) destination, the port no longer functions in normal ways. The interface connected to the SPAN destination port is expected to be in “promiscuous mode”, meaning the interface is expected to be capturing all traffic that enters the port, and will not respond to directed communications.

With that understanding, it is recommended to dedicate one or more interfaces of the Cisco ISE server to be put into promiscuous mode for the DHCPSPAN and HTTP probes. For the purposes of this guide, we will dedicate the GigabitEthernet 1 interface to be a SPAN destination.

Note: When using an interface on the Cisco ISE other than GigabitEthernet 0, enter the CLI and type **no shutdown** at interface configuration mode to enable the interface.

Please see the “Add Network Device” procedure for the switch configuration.

To configure the SPAN (monitor session) on the switchport, please see the “Configure the SPAN session on the Switch” procedure.

Step 7 Enable the check box for **HTTP**.

The **HTTP Span probe** will listen for HTTP packets on the specified interface and parse them to augment endpoints with HTTP attributes. The HTTP probe will capture traffic emanating from the endpoint and going to port 80 to detect what user agent as well as any other HTTP attributes are present within the HTTP request.

The HTTP data is very important for mobile device recognition, among other things. Use of HTTP will also require some design consideration and should be a part of the High-Level Design (HLD).

Step 8 Enable the check box for **RADIUS**.

The **RADIUS probe** will help detect endpoints based on RADIUS information. Table 8 lists known attributes collected by the RADIUS probe.

Table 8 Attributes Collected by RADIUS Probe

User-Name	Framed-IP-Address	Acct-Session-Time
NAS-IP Address	Calling-Station-ID	Acct-Terminate-Cause
NAS-Port	Acct-Session-ID	

The RADIUS Probe may also trigger DNS and SNMP Query collection events (if enabled).

Step 9 Enable the check box for **DNS**.

The DNS probe in your Cisco ISE deployment allows the profiler to look up an endpoint and gets the fully qualified domain name (FQDN) of that endpoint.

A reverse DNS lookup will be completed only when an endpoint detected by the DHCP, RADIUS, HTTP, and SNMP probes contains the following attributes, meaning that, for DNS lookup, at least one of the following probes needs to be enabled along with the DNS probe:

- DHCP IP Helper, DHCP Span – “dhcp-requested-address”
- RADIUS Probe – “Framed-IP-Address”
- SNMP Probe – “cdpCacheAddress”
- HTTP Probe – “Source IP”

Step 10 Enable the check box for **SNMPQUERY**.

Note: When you configure SNMP settings on the network devices, you need to ensure in addition that Cisco Discovery Protocol is enabled on all the ports of the network devices. If you disable Cisco Discovery Protocol on any of the ports on the network devices, then you may not be able to profile properly because you will miss the Cisco Discovery Protocol information of all the connected endpoints.

The SNMPQuery probe polls all of the SNMP-enabled Network Devices at configured polling intervals. This feature requires the configuration of SNMP parameters in the Add Network Device section.

The SNMPQuery probe queries the following MIBS:

- system
- cdpCacheEntry
- cLApEntry (If device is WLC)
- cldcClientEntry (If device is WLC)

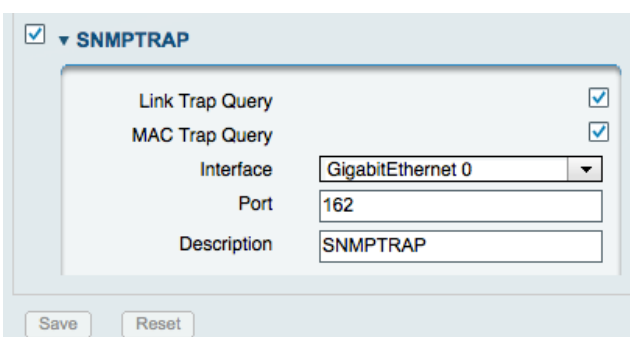
LinkUp/MAC Notification/RADIUS Acct Start event queries:

- interface data (ifIndex, ifDesc, etc.)
- Port and VLAN data
- Session Data (if interface type is Ethernet)
- Cisco Discovery Protocol data (if device is Cisco)

For distributed deployments, NAD polling is distributed among enabled SNMP query probes.

Note: SNMP Trap-triggered queries are queued to same node for SNMP Query probe. If local SNMP Query probe is not enabled, then those queries are dropped.

Step 11 Enable the check box for **SNMPTRAP**.



Step 12 Ensure the Link Trap Query and MAC Trap Query options are enabled.

The SNMP Trap receives information from the configured NADs that support MAC notification, linkup, linkdown, and informs. For SNMPTrap to be fully functional, you must also enable the SNMPQuery probe. The SNMPTrap probe receives information from the specific NADs when ports come up or go down and endpoints disconnect or connect to your network. The In order to make this feature functional, you must configure the NAD to send SNMP traps. Information received from the SNMP traps will not create a new endpoint in Cisco ISE but it will potentially be used for profiling.

Note: SNMP informs are supported.

Step 13 Click **Save**.

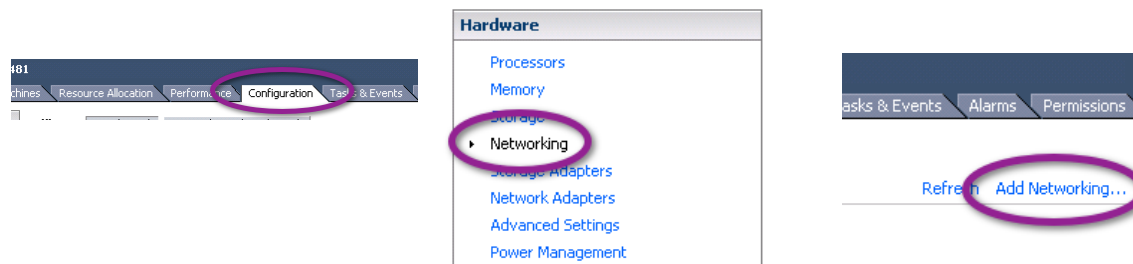
Procedure 2 (Optional) Configure a Promiscuous VMware Network.

If Cisco ISE is deployed in a Virtual Environment, it is important to configure the VMware networking appropriately to allow a promiscuous interface to work properly. If Cisco ISE is deployed in a physical appliance form factor, then move ahead to the “Configure the SPAN session on the Switch” section.

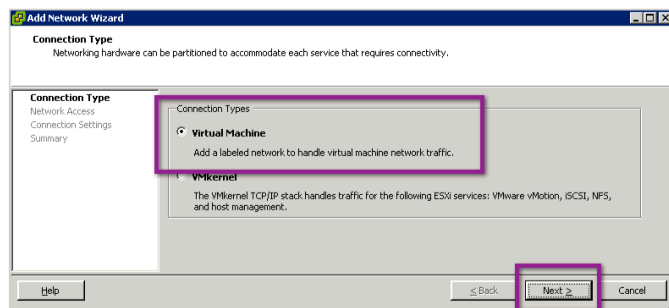
This Procedure will configure and dedicate an interface on the VMware ESX Server as a promiscuous interface. If the physical interface on the ESX server cannot be dedicated for SPAN, follow Procedure 3 later in this document.

Note: If deploying with VMware, pay close attention to the specs listed in the install guide and in Appendix A: Cisco ISE design. Specifically, disk size can be a real concern. It can be catastrophic to a deployment if Cisco ISE is running in VMware with a lot of logged events and it runs out of disk space. Always follow the recommendations for VMware sizing.

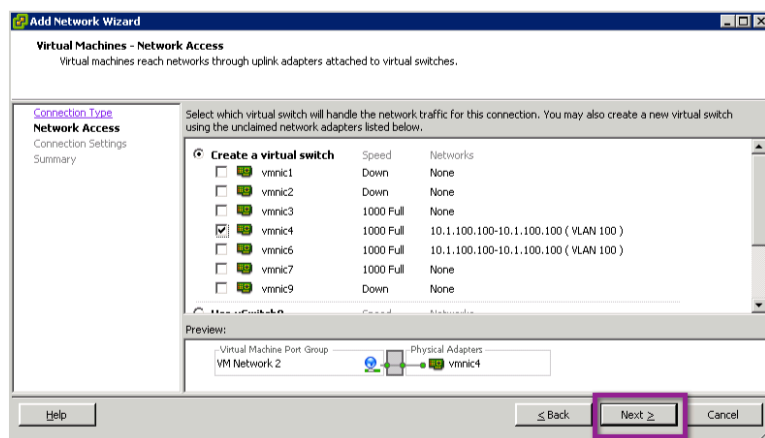
Step 1 Select the physical ESX server in VMware VSphere client. Select **Configuration** → **Networking**, and then choose **Add Networking**.



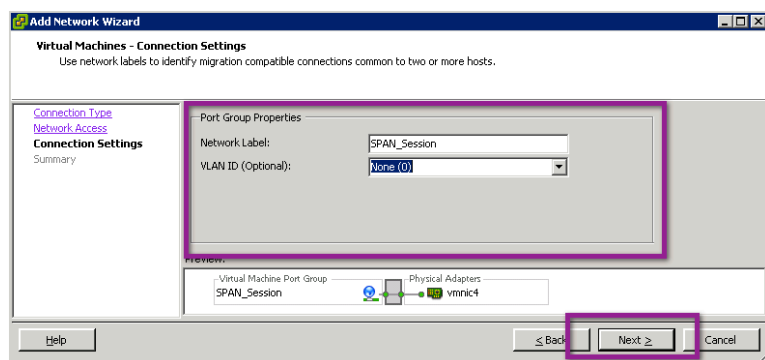
Step 2 The *Add Network Wizard* is launched. Choose a **Virtual Machine** connection Type, and click **Next**.



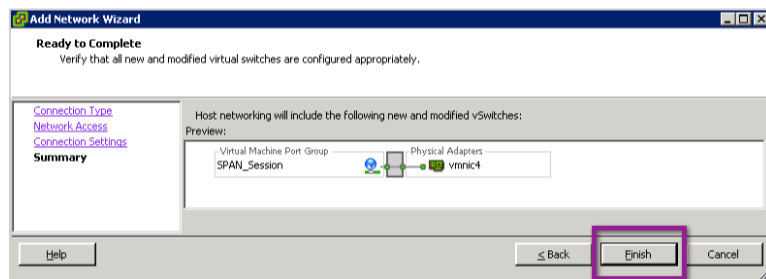
Step 3 Select the Physical Interface that will be connected to the SPAN port on the switch. Click Next.



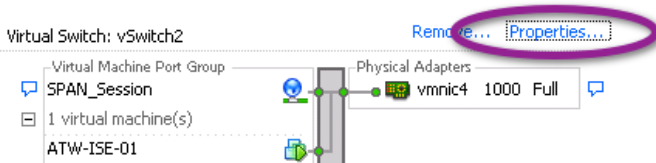
Step 4 Name the network **SPAN_Session**, or any other logical name.



Step 5 Select Finish.



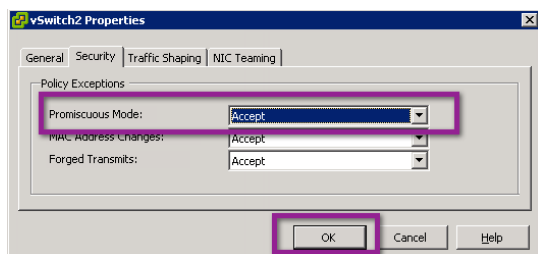
Step 6 Enable Promiscuous traffic into the newly created vSwitch. Select properties on the new vSwitch.
By default, any VMware network will reject Promiscuous traffic.



Step 7 Highlight the new vSwitch. Choose **Edit**.

Step 8 Select the Security tab.

Step 9 Select **“Accept”** from the Promiscuous Mode drop-down menu. Click **OK**.



Step 10 Close the vSwitch Properties window.

Step 11 Edit the Cisco ISE Virtual Machine Settings.

Basic Tasks

Power Off the virtual machine

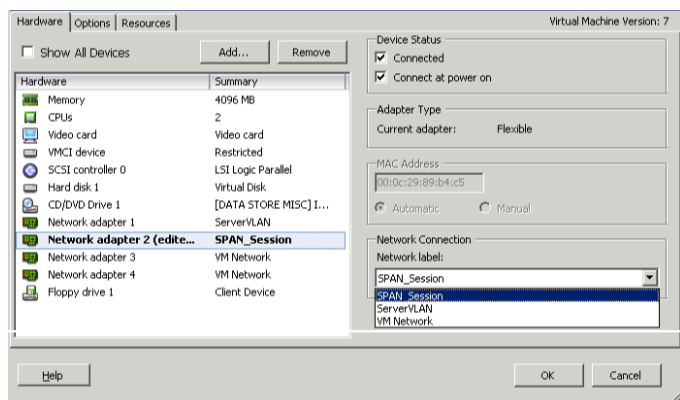
Suspend the virtual machine

Edit virtual machine settings

Step 12 Select the appropriate Network Adaptor for Cisco ISE (usually Network Adaptor 2, for GigabitEthernet1 in Cisco ISE).

Step 13 Ensure that it is **Connected**, and will **Connect at power on**.

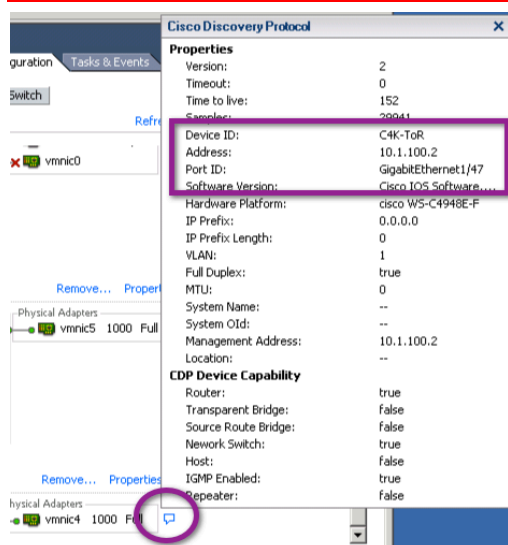
Step 14 From the Network Connection drop-down menu, select the newly created “SPAN_Session” network.



Step 15 Click **OK**.

Step 16 Make note of the switch port that the promiscuous interface is connected to, for use in the next section.

Note: ESX has a user-friendly feature of displaying Cisco Discovery Protocol information for its connected interfaces. See the following screen shot to see this display.

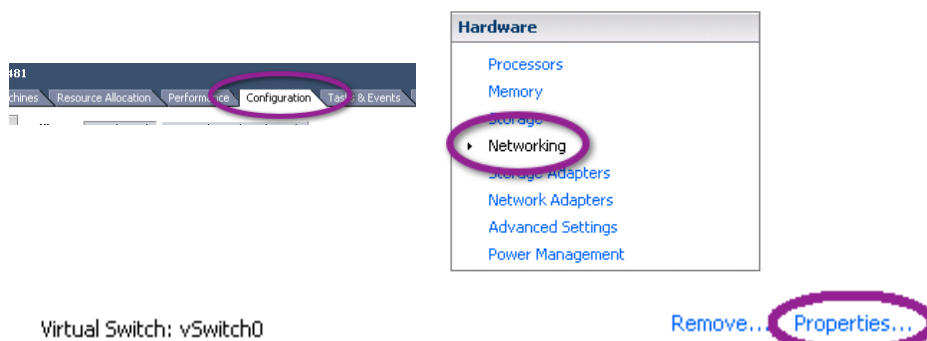


Procedure 3 (Optional) Configure a Promiscuous VMware Port Group.

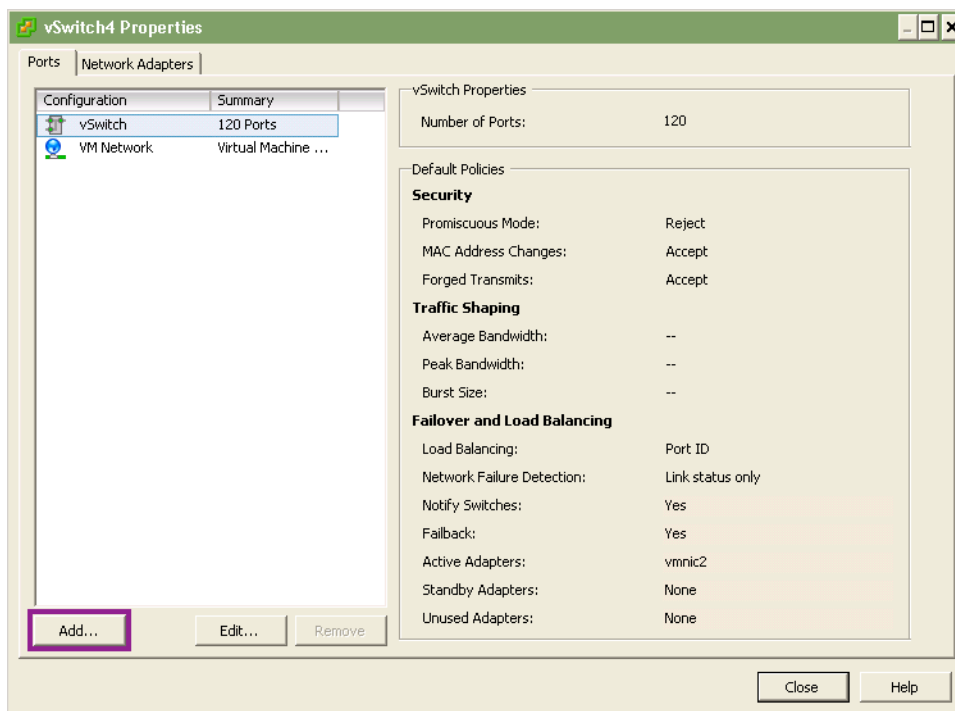
A second approach to configuring a promiscuous VMware Network is to create a promiscuous port group on an existing vSwitch. This deployment is important if it is either not possible to dedicate a physical SPAN port to the Cisco ISE Virtual Machine or if the nature of virtual deployment is such that not all traffic can be copied from the physical switch and must be obtained from the vSwitch itself.

Step 1 Select the physical ESX server in VMware VSphere client.

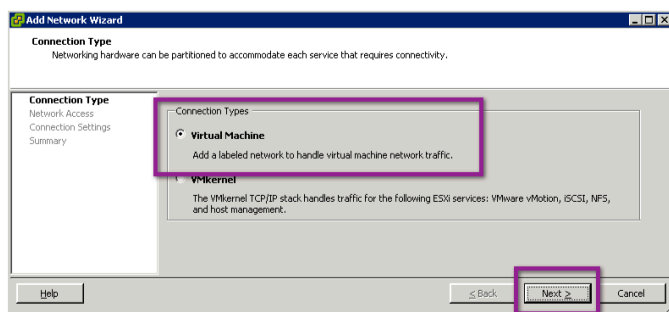
Step 2 Select **Configuration** → **Networking**, and then choose your vSwitch and click “**Properties**”.



Step 3 In the vSwitch Properties window under the Ports Tab, click **Add** at the bottom left.



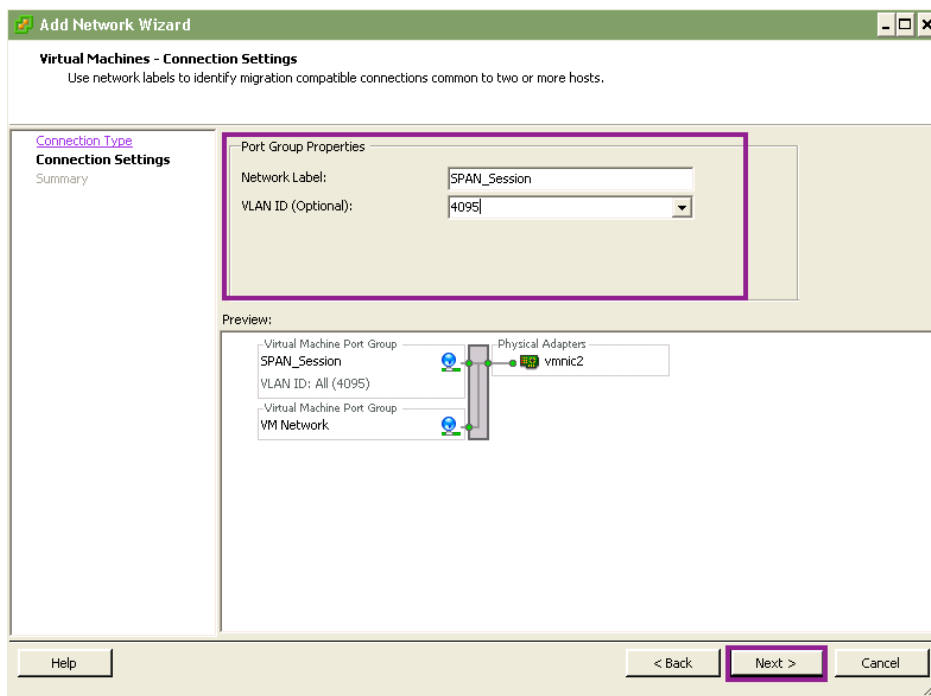
Step 4 The Add Network Wizard is launched. Choose a “**Virtual Machine**” connection Type, and click **Next**.



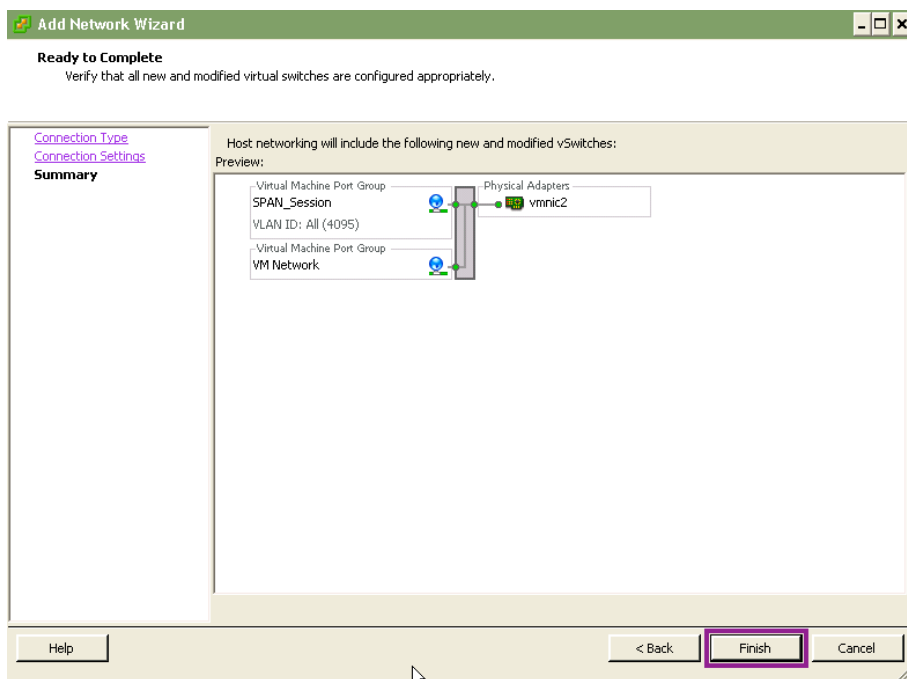
Step 5 Name the port group “SPAN_Session”, or any other logical name.

Step 6 Set the VLAN to **4095** and click **Next**.

Note: This VLAN is a special VMware VLAN that listens to all other VLANs on that vSwitch.



Step 7 Select **Finish**.

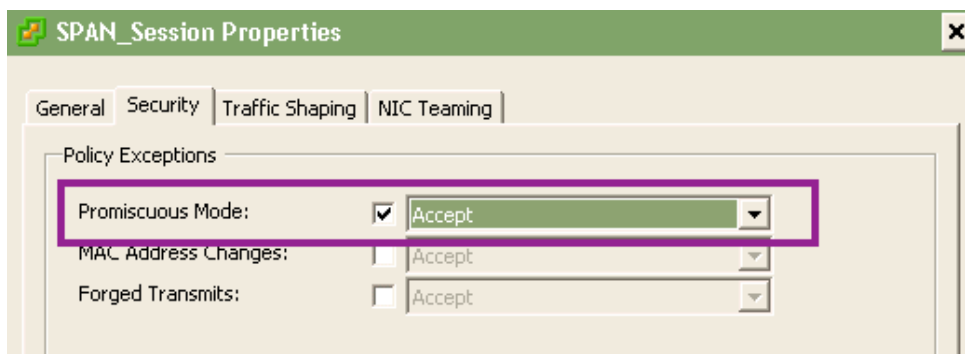


Step 8 Highlight the new port group.

Step 9 Choose **Edit**.

Step 10 Select the Security tab.

Step 11 Select “Accept” from the Promiscuous Mode drop-down menu. Click OK.



Step 12 Close the vSwitch Properties window.

Step 13 Edit the Cisco ISE Virtual Machine Settings.

Basic Tasks

Power Off the virtual machine

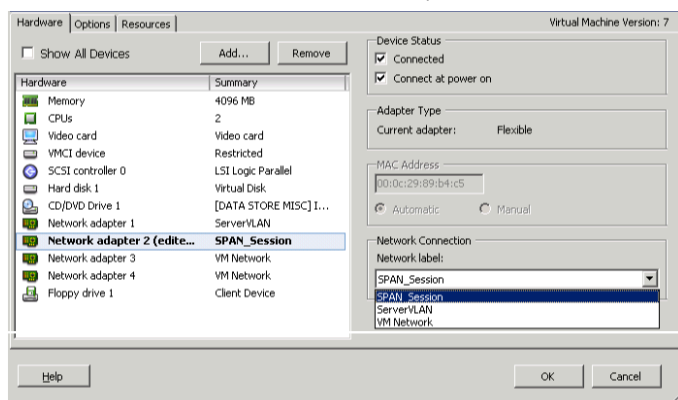
Suspend the virtual machine

Edit virtual machine settings

Step 14 Select the appropriate Network Adaptor for Cisco ISE (usually Network Adaptor 2 for GigabitEthernet1 in Cisco ISE).

Step 15 Ensure that it is **Connected** and will **Connect at power on**.

Step 16 From the Network Connection drop-down menu, select the newly created “SPAN_Session” network.



Step 17 Click OK.

Procedure 4 Configure the SPAN session on the Switch.

Step 1 Enter Global Configuration.

Step 2 Configure the SPAN session source. An example follows:

```
C4K-ToR(config)#monitor session 1 source vlan 100 both
```

Step 3 Configure the SPAN session destination. An example follows:

```
C4K-ToR(config)#monitor session 1 destination interface g 1/47
```

Step 4 Verify the port is now in monitoring mode.

```
C4K-ToR(config)#do show int status | i 47
Gi1/47 monitoring 1 a-full a-1000 10/100/1000-TX
```

Procedure 5 Configure the ip-helper Statements.

To work along with the DHCP probe for Cisco ISE profiling, the Cisco ISE Policy Node(s) should be added to the ip helper-address statements on the Layer 3 interfaces in the network. This node addition will send a copy of all DHCP requests to Cisco ISE in addition to the production DHCP servers in the environment.

Step 1 Enter Global Configuration mode.

Step 2 Enter the Interface configuration mode for the Access VLAN Layer 3 interface and add Cisco ISE as another destination for ip helper-address. An example follows:

```
interface Vlan10
ip address 10.1.10.1 255.255.255.0
ip helper-address 10.1.100.100  ! - this is the DHCP Server
ip helper-address 10.1.100.3    ! - this is the ISE Server
```

Universal Cisco ISE Configuration: Guest

Introduction

Cisco TrustSec security helps organizations secure guest access to corporate networks, helping ensure that guest and visitor traffic remains segregated from internal networks and assess incoming computers for threats that may affect network availability and security. Cisco ISE offers centralized guest access management and enforcement for wired and wireless users, and can integrate easily with wireless solutions, third-party guest access portals, and billing providers.

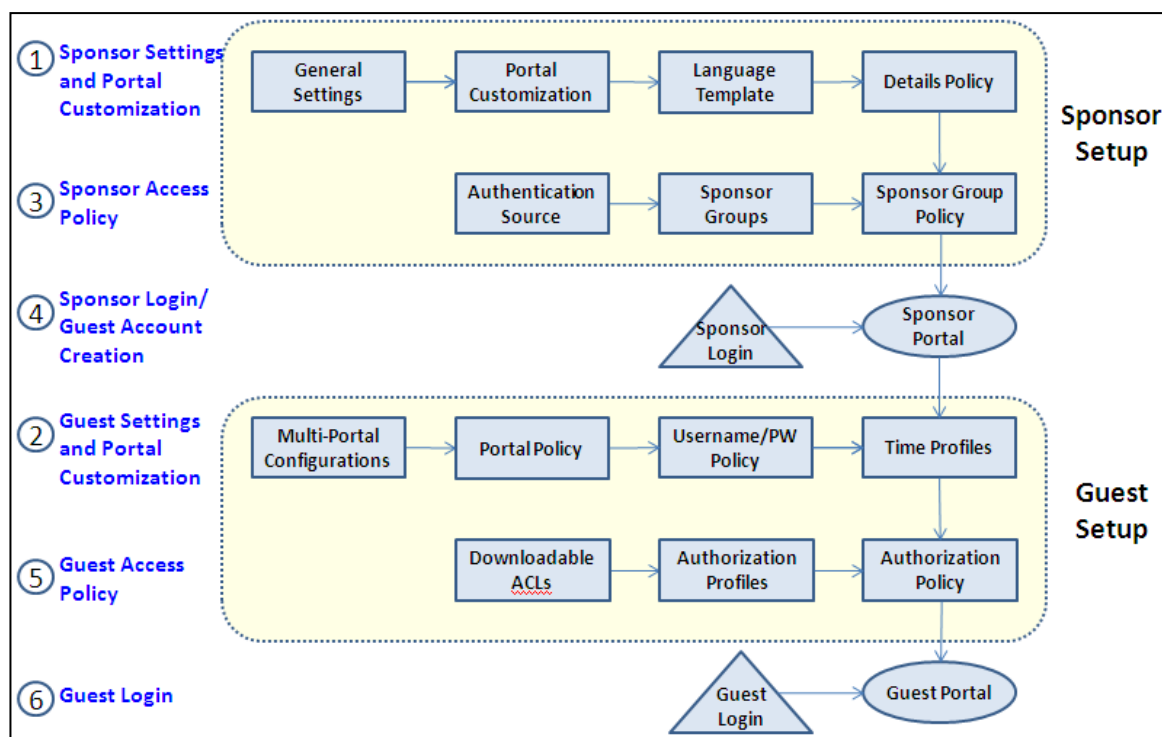
Cisco ISE Guest service allows guests, visitors, contractors, consultants, or customers to perform an HTTP or HTTPS login to access a network whether that network is a corporate intranet or the public Internet. The network is defined through a VLAN or a downloadable access control list (DACL) configuration in the network access device (NAD). Cisco ISE offers a simple, client-configurable Sponsor Portal for creating and managing Guest User accounts. Cisco ISE also supports default and customizable Guest Login Portals to handle Guest User login. Guest service provisions a guest account for the amount of time specified when the account is created.

In this section we will review the overall workflow for configuring Cisco ISE Guest Services, including sponsor setup, guest setup, and configuration of authorization policies for guest access.

Guest Services exposes two web portals. The first is the Guest User portal for Guest User login, Acceptable Use Policy acknowledgment, changing of passwords, and self-registration. The second web portal is a Sponsor Portal for Sponsors to create, update, and manage Guest User accounts.

The main steps in configuring guest services are shown in Figure 5. Note that in some cases tasks may be applicable to both sponsor and guest configuration.

Figure 5: Logical Grouping of Configuration Tasks



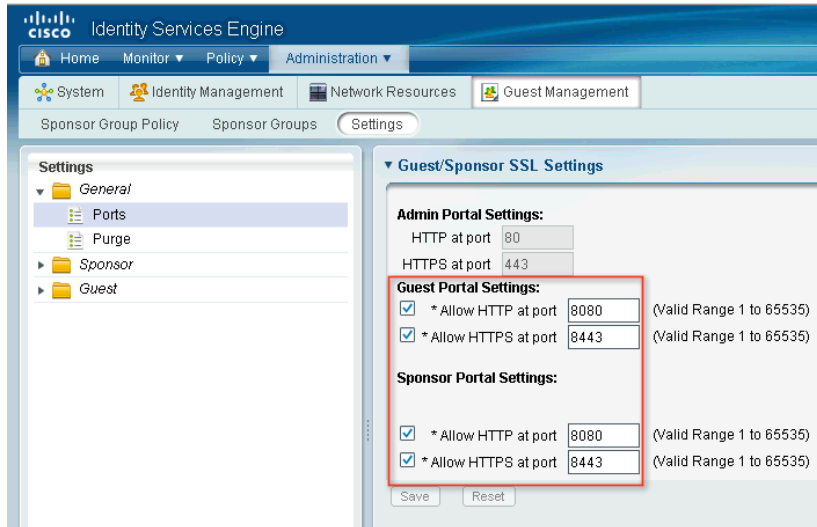
Procedure 1 Configure Sponsor System Settings.

Prior to configuration of sponsor or guest access policies, ensure that the guest service is enabled on Cisco ISE.

Step 1 Navigate to Administration → Guest Management → Settings → General → Ports.

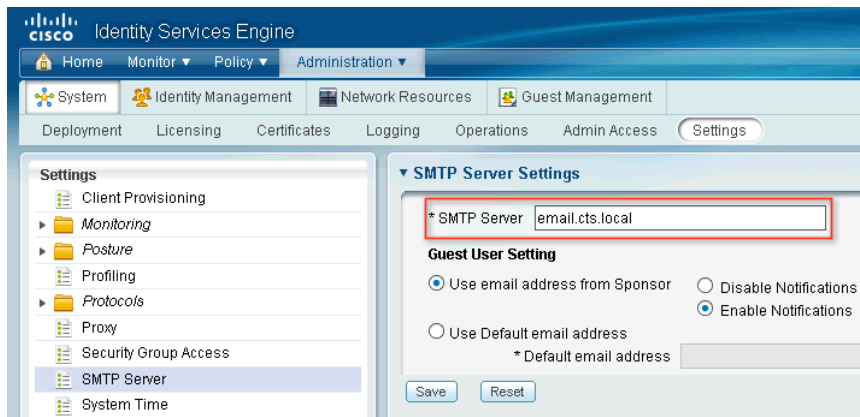
Step 2 Verify the HTTP and HTTPS ports used for portal access as required for the guest and sponsor portal.

Step 3 The default ports are 8080 and 8443 for HTTP and HTTPS, respectively.



Step 4 Navigate to Administration → System → Settings → SMTP Server Settings.

Step 5 Enter your mail server and configure notification settings as required.

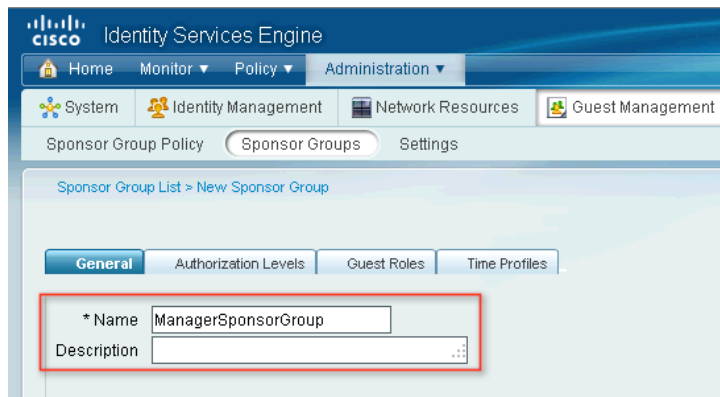


Procedure 2 Configure Sponsor Groups.

Guest sponsor groups contain the permissions and settings for the sponsor user.

Step 1 Navigate to Administration → Guest Management → Sponsor Groups.

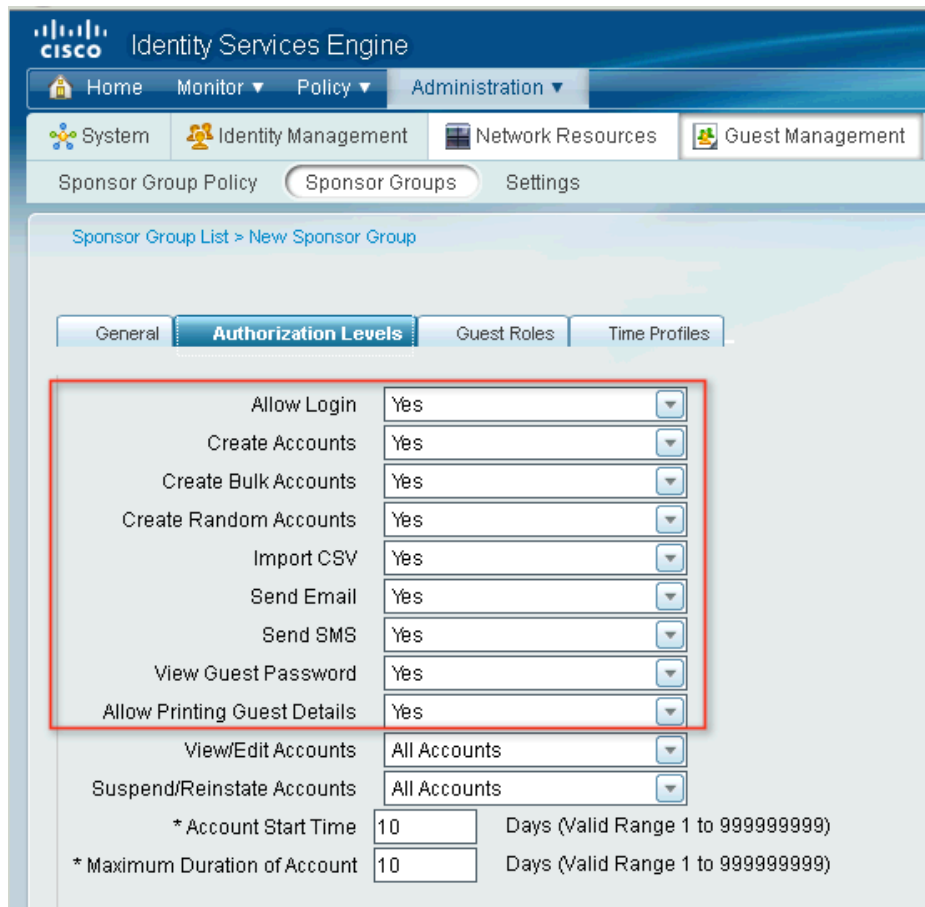
Step 2 Click **Add** or **Edit** to create or edit a sponsor group.



The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation bar includes Home, Monitor, Policy, and Administration. The main menu has System, Identity Management, Network Resources, and Guest Management. The sub-menu shows Sponsor Group Policy, Sponsor Groups, and Settings. The 'Sponsor Group List > New Sponsor Group' page is displayed. The 'General' tab is selected, and the 'Name' field is highlighted with a red box, containing the text 'ManagerSponsorGroup'.

Step 3 Under the **General** tab enter a name and description.

Step 4 Under the **Authorization Levels** tab set permissions as necessary.



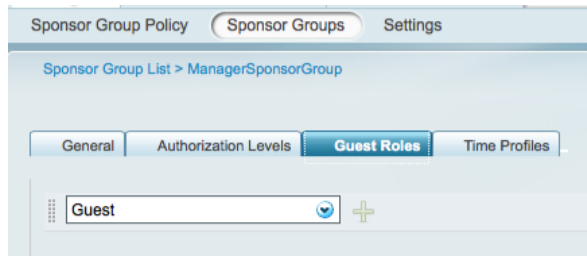
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation bar includes Home, Monitor, Policy, and Administration. The main menu has System, Identity Management, Network Resources, and Guest Management. The sub-menu shows Sponsor Group Policy, Sponsor Groups, and Settings. The 'Sponsor Group List > New Sponsor Group' page is displayed. The 'Authorization Levels' tab is selected, and the permissions section is highlighted with a red box.

Permission	Value
Allow Login	Yes
Create Accounts	Yes
Create Bulk Accounts	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	Yes
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	10 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	10 Days (Valid Range 1 to 999999999)

Step 5 Choose appropriate choices for View/Edit Accounts, Suspend/Reinstate Accounts, Account Start Time, and Maximum Duration of Account settings.

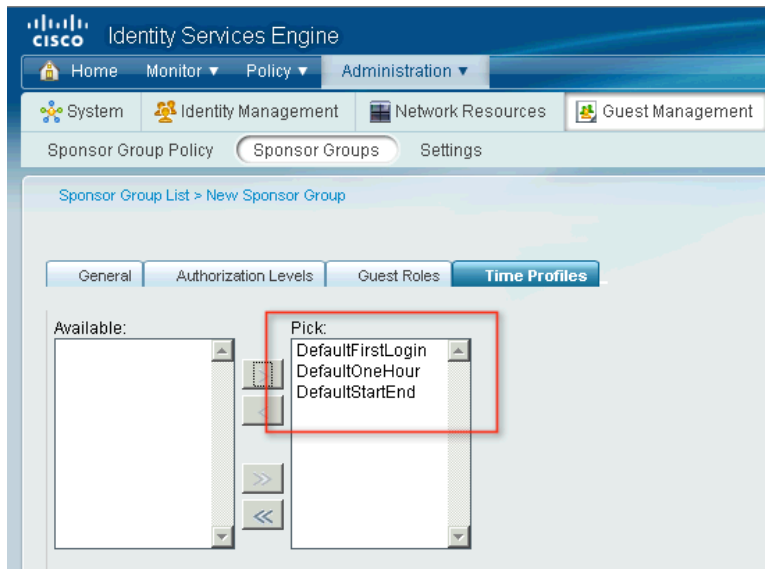
Note: Please see the Cisco ISE User Guide for more detailed options surrounding Guest account provisioning.

Step 6 From the **Guest Roles** tab choose the guest roles that the sponsor group user would be allowed to assign to the guest user.



Note: These roles are used in the authorization policies to relate guest user accounts to identity groups.

Step 7 Under the **Time Profiles** tab choose time profiles that the sponsor group user would be able to assign to guest accounts.



Step 8 Click **Submit** to save the configuration.

Procedure 3 Configure Identity Source Sequences (optional).

Identity source sequences define the order in which Cisco ISE will look for user credentials in the different databases. We created one called ALL_ID_STORES in the "Create an Identity Sequence" procedure. This one will normally be sufficient for most installations.

Step 1 Navigate to Administration → Identity Management → Identity Source Sequences.

Step 2 Click **Add** to add an identity source sequence. You can check the check box or click **Edit** or **Duplicate** accordingly.

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is: Administration > Identity Management > Identity Source Sequences. The page title is 'Identity Source Sequence'. The 'Name' field is 'Sponsor_Portal_Sequence' and the 'Description' is 'A Built-in Identity Sequence For The Sponsor Portal'. Under the 'Certificate Based Authentication' section, the 'Select Certificate Authentication Profile' checkbox is unchecked. Under the 'Authentication Search List' section, there is a description: 'A set of identity sources that will be accessed in sequence until first authentication succeeds'. Below this, there are two columns: 'Available' and 'Selected'. The 'Available' column contains 'Internal Endpoints' and the 'Selected' column contains 'Internal Users'. A red box highlights the 'Available' and 'Selected' columns.

Step 3 In the Authentication Search List area, select the appropriate method if you want Cisco ISE to stop the search if the user is not found in the first identity store.

Note: Ensure that you have the identity sources in the Selected list in the order you want Cisco ISE to search the identity sources.

Procedure 4 Configure Authentication Sources.

To allow a sponsor to log into the sponsor portal, you have to choose an identity store sequence. This sequence is used with the login credentials of the sponsor to authenticate and authorize the sponsor for access to the sponsor portal.

Step 1 Navigate to Administration → Guest Management → Settings → Sponsor → Authentication Source.

Step 2 From the **Identity Store Sequence** drop-down list, choose the sequence to be used for the sponsor authentication (ALL_ID_STORES).

The screenshot shows the Cisco ISE Administration console. The breadcrumb trail is: Administration > Guest Management > Settings > Sponsor > Authentication Source. The page title is 'Sponsor Authentication Servers'. The 'Identity Store Sequence' dropdown menu is set to 'ALL_ID_STORES'. There are 'Save' and 'Reset' buttons at the bottom.

Step 3 Click **Save**.

Note: When the primary node with Administration persona is down, Sponsor administrators cannot create new guest user accounts.

Procedure 5 Configure a New Sponsor User (optional).

For the majority of installs, Active Directory will be the identity source chosen to authenticate sponsors to. However, it is possible to create local sponsor users on Cisco ISE. This procedure details the creation of that local sponsor user.

Step 1 Navigate to Administration → Identity Management → Identities → Users.

Step 2 Click **Add** to create a new network access user. The Network access user page is displayed.

Step 3 Enter values as appropriate to configure the sponsor user.

Step 4 Associate the sponsor of the appropriate sponsor user group.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The breadcrumb navigation at the top reads: Administration > Identity Management > Identities > Users. The left sidebar shows a search bar and a 'No Data Available' message. The main content area is titled 'Network Access Users > New Network Access User'. It contains several sections: 'Network Access User' with fields for 'Name' (Sponsor1) and 'Status' (Enabled); 'Password' with fields for '* Password' and '* Re-Enter Password'; 'User Information' with fields for 'First Name' and 'Last Name'; 'Account Options' with a 'Description' field and a 'Password Change' checkbox; and 'User Groups' with a dropdown menu showing 'SponsorAllAccounts'. The 'Name' and 'User Groups' fields are highlighted with red boxes. At the bottom are 'Submit' and 'Cancel' buttons.

Step 5 Click **Submit** to add the user to the Cisco ISE database.

Procedure 6 Configure Sponsor Group Policies.

Sponsor Group Policies are more like Identity Mapping policies. These Policies map Identity Groups (Active Directory or Local groups) to a Directory or Local groups) to a Sponsor Group. Each Sponsor group may have different settings (such as the ManagerSponsor group created in the “

Configure Sponsor Groups" procedure.

Step 1 Navigate to Administration → Guest Management → Sponsor Group Policy.

Step 2 Click **Actions** to insert a new rule above the existing rules.

Step 3 Name the Rule ManagerSponsors.

Step 4 Leave the Identity Groups at the default of **Any**.

Step 5 Under conditions, choose Create a New Condition (Advanced Option).

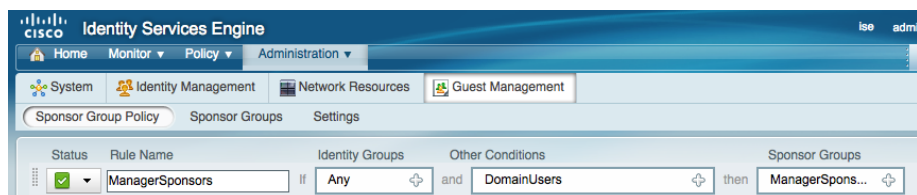
Step 6 Within expression, choose: AD1 → ExternalGroups → Sponsors_Full.

Note: Sponsors_Full is a group that we have preconfigured in Active Directory. Many organizations create a special group for Sponsors, and others will allow any member of "Domain Users" to create Guest Accounts.

Step 7 Under **Other Conditions**, you may configure any number of conditions and statements as per network requirements. These conditions will be used to match users as they authenticate to the Guest Service Sponsor portal.

For the Sponsor Group, choose ManagerSponsors created in the "

Step 8 Configure Sponsor Groups” procedure.



Step 9 Click **Save** to save the configuration.

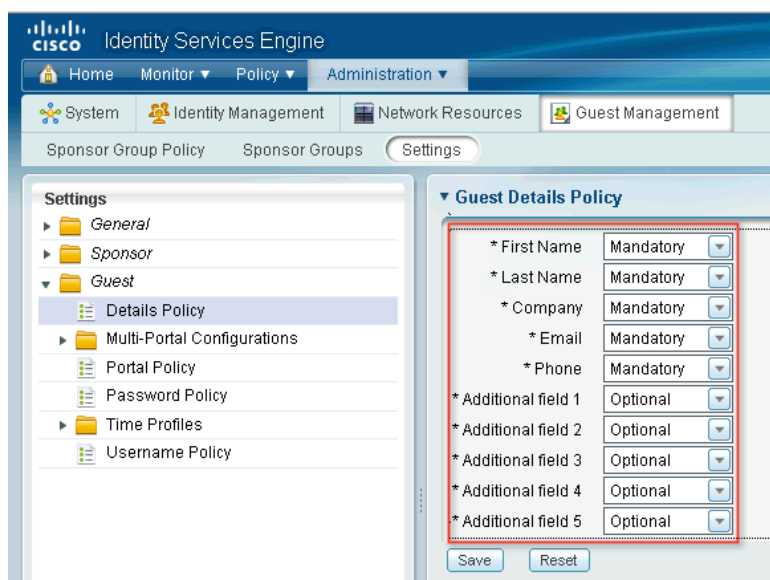
Procedure 7 Configure the Guest Details Policy.

The details policy determines the data that the sponsor needs to enter when creating a guest account. The Cisco ISE administrator must define the fields that should appear on the Sponsor Guest User create and edit pages and in the Guest User Self-Registration page.

Step 1 Navigate to Administration → Guest Management → Settings → Guest → Details Policy.

Step 2 Enter fields such as First Name, Last Name, Company, Email, Phone, as required.

Step 3 Specify any of the three settings for each field: **Mandatory**, **Optional**, or **Unused**.



There are five additional fields that can be customized to require sponsors to fill out when creating guest accounts.

Step 4 Click Submit.

Procedure 8 Configure the Guest Username Policy.

The Guest Portal policy specifies how the usernames will be created for the guest accounts. It contains username requirements for guest services, such as allowed characters and the username format. Username policy configuration can be done in two ways – General or Random.

To configure general guest username policy, complete the following steps:

- Step 1 Navigate to Administration → Guest Management → Settings → Guest → Username Policy.
- Step 2 Choose one of the username policy options – from an email address or from first and last names.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The left sidebar displays the 'Settings' menu with 'Username Policy' selected. The main content area shows the 'General' tab of the Username Policy configuration. The 'Create username from first name and last name' option is selected. The 'Minimum Username Length' is set to 8. The 'Random' tab is also visible, showing options for including alphabetic, numeric, and special characters in the username.

Step 3 Enter minimum username length as required.

Step 4 Click **Submit**.

Procedure 9 Configure the Password Policy.

The Guest Portal policy specifies the characters that may be used for password generation as well as the number of each type for all guest accounts.

Step 1 Navigate to Administration → Guest Management → Settings → Guest → Password Policy.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The left sidebar displays the 'Settings' menu with 'Password Policy' selected. The main content area shows the 'Password Policy' configuration page. The 'Minimum number to include' for alphabetic, numeric, and special characters is set to 4, 4, and 1 respectively.

Step 2 Enter appropriate details according to your guest password policy requirements.

Step 3 Click Submit.

Procedure 10 Configure the Guest Portal Policy.

The Guest Portal policy identifies functional items such as guest login attempts, password expiration, etc.

Step 1 Navigate to Administration → Guest Management → Settings → Guest → Portal Policy.

Step 2 Configure the following options as required:

- Self-Registration Guest Role
- Self-Registration Time Profile
- Maximum Login Failures

- Device Registration Portal Limit
- Guest Password Expiration

Guest Portal Policy

* Self Registration Guest Role: Guest

* Self Registration Time Profile: DefaultFirstLogin

* Maximum Login Failures: 5 (Valid Range 1 to 9)

* Device Registration Portal Limit: 5 (Valid Range 1 to 20)

* Guest Password Expiration (Days): 1 (Valid Range 1 to 999)

NOTE: Guest Password Expiration must be enabled in the Portal Configuration

Save Reset

Step 3 Click **Save** to save configuration.

Universal Guest Configuration – Multi-Portal Guest User Configuration

A predefined DefaultGuestPortal is available under Multi-Portal Configurations. This portal has the default Cisco design and you cannot customize it. To create a customized portal, you must first begin by adding a new portal.

Procedure 1 Configure the Multi-Portal.

Note: This procedure is crucial to more than just Guest Access. It is critical that this portal be configured correctly for all Web Authentication needs.

Step 1 Navigate to Administration → Guest Management → Settings → Guest → Multi-Portal Configuration.

Step 2 Select the DefaultGuestPortal.

Multi-Portal Configuration List > DefaultGuestPortal

General Authentication

* Name: DefaultGuestPortal

Description: default portal

Guest Portal Policy Configuration

☒ Allow guest users to change password

☐ Require guest and internal users to change password at expiration

☒ Guest users should download the posture client

☐ Guest users should be allowed to do self service

☐ Guest users should be allowed to do device registration

☐ Vlan Dhcp Release (Note: Release should occur prior to the CoA. Renew should be set to occur after the CoA occurs).

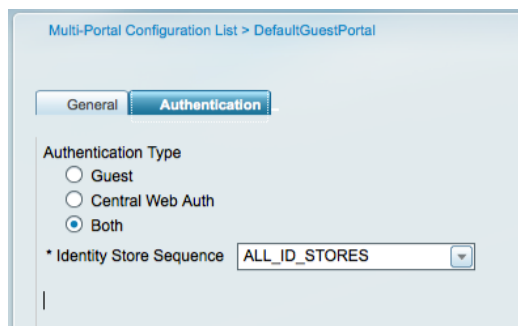
Delay to Release: 1 seconds (Valid Range 1 to 200)

Delay to CoA: 0 seconds (Allow enough delay before CoA for the control to download from the server.)

Save Reset

Step 3 Make any changes to these settings as needed by your organization.

Step 4 Click Authentication.



The screenshot shows a web interface for configuring a guest portal. At the top, it says "Multi-Portal Configuration List > DefaultGuestPortal". Below this, there are two tabs: "General" and "Authentication". The "Authentication" tab is selected. Under the "Authentication Type" section, there are three radio buttons: "Guest", "Central Web Auth", and "Both". The "Both" radio button is selected. Below this, there is a label "* Identity Store Sequence" followed by a dropdown menu that currently displays "ALL_ID_STORES".

Step 5 Choose "Both" for the type of users who will be authenticated during the guest login.

Step 6 Select the ALL_ID_STORES identity store.

Step 7 Click Save.

Supplicant Configuration

Cisco AnyConnect Network Access Manager

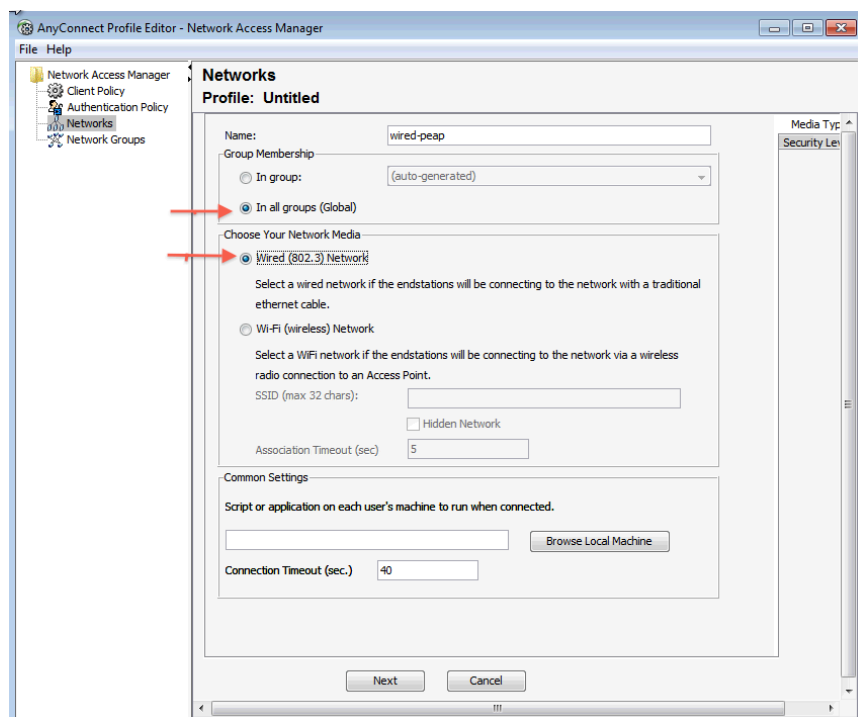
Cisco AnyConnect Network Access Manager (NAM) is a module of the Cisco AnyConnect Client for Windows 3.0 and provides a fully configurable and very powerful supplicant option instead of the native supplicant of the Windows Operating System. NAM is licensed with no charge, and more information may be found here: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/data_sheet_c78-527494.html.

Cisco AnyConnect NAM Configuration Using the Standalone Profile Editor

Procedure 1 Configure NAM with the Standalone Profile Editor

Step 1 Select Networks, click Add, and enter “Wired-PEAP”.

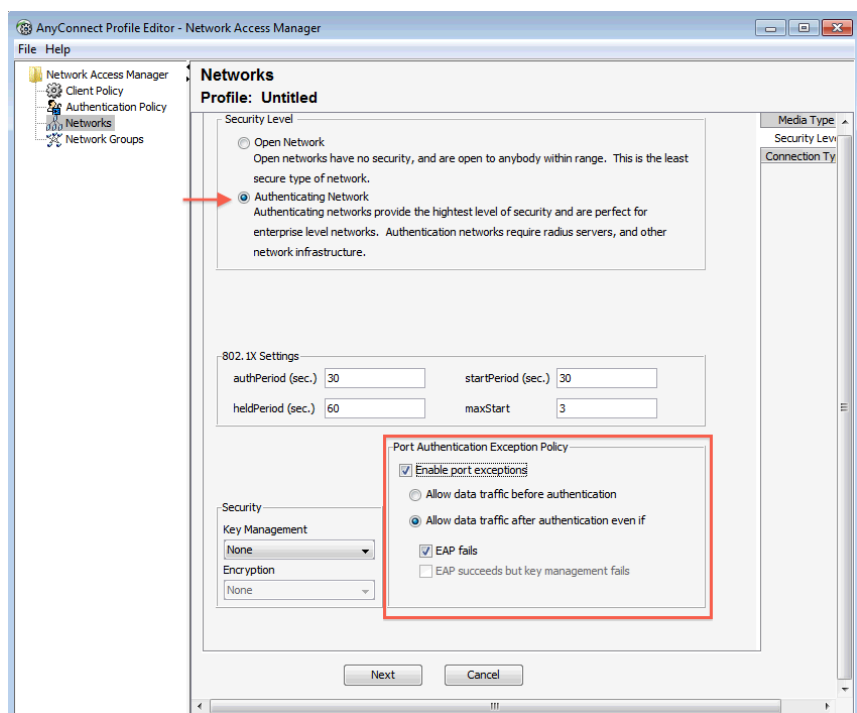
Step 2 Follow the configuration settings in the screen shot that follows:



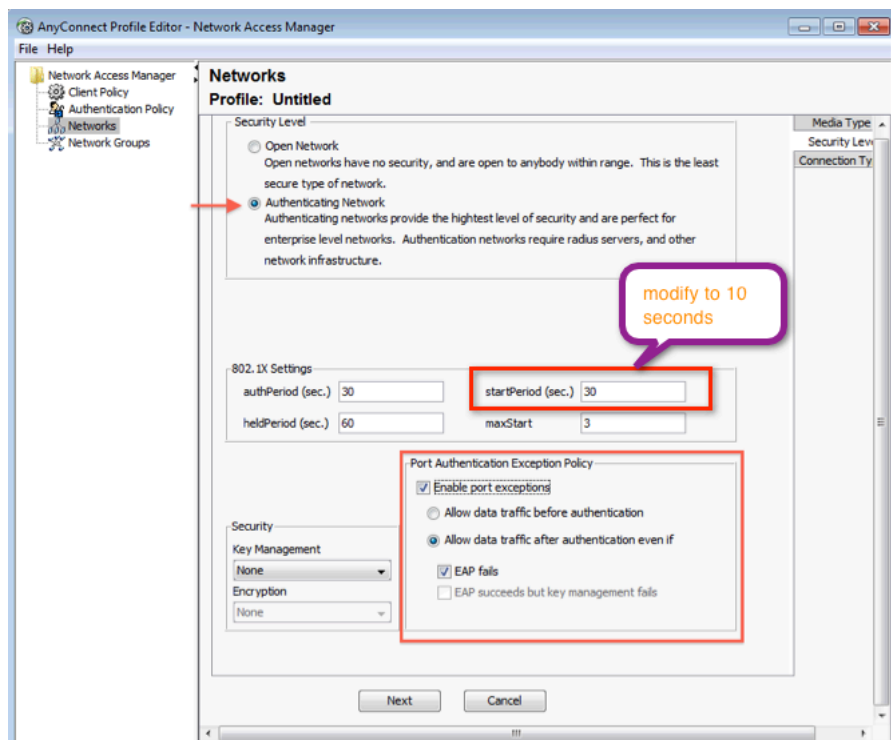
Step 3 Click Next.

Step 4 Select “Authenticating Network” and check “EAP fails” under the Port Authentication Exception Policy.

Note: Since the switchport is configured for open mode, step 4 configures NAM to allow traffic to flow as well. Otherwise NAM, per IEEE 802.1X specifications, will fail the connection if EAP authentication fails.



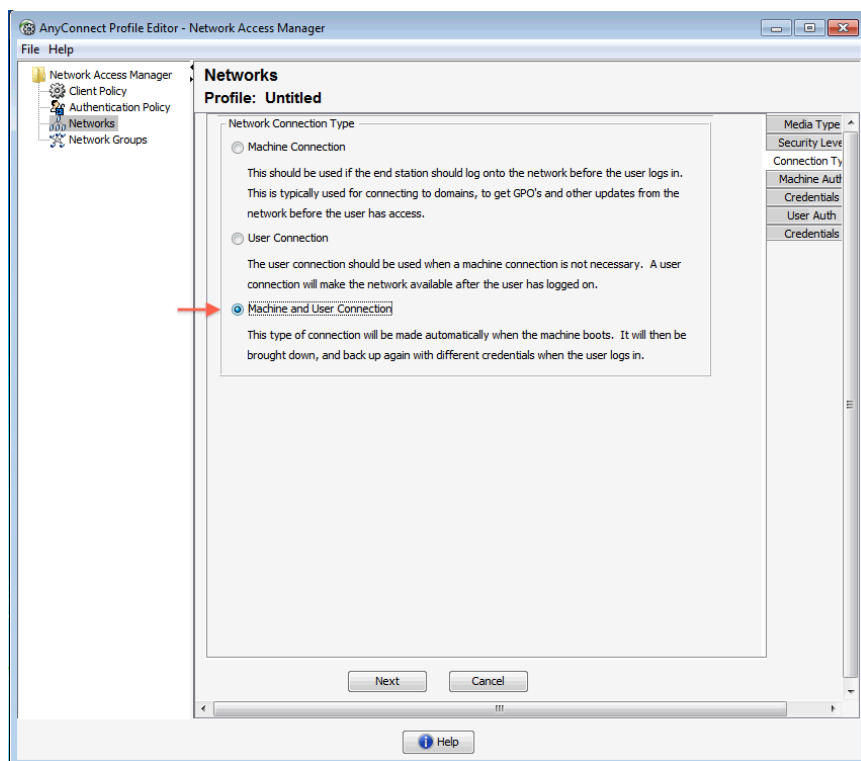
Step 5 Change the **startperiod** to 10 seconds.



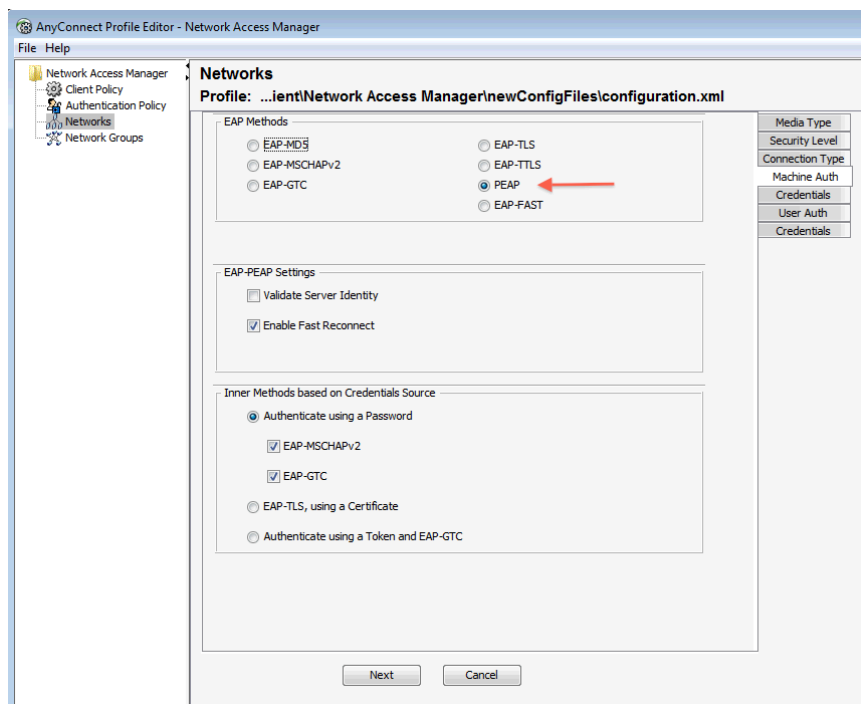
Note: the startperiod is equivalent to tx-period on the switchport. Because it is best practice to set the tx-period to 10 seconds, the NAM startperiod value must also reflect the same value (refer to the section "Authentication Settings – Timers").

Step 6 Click Next.

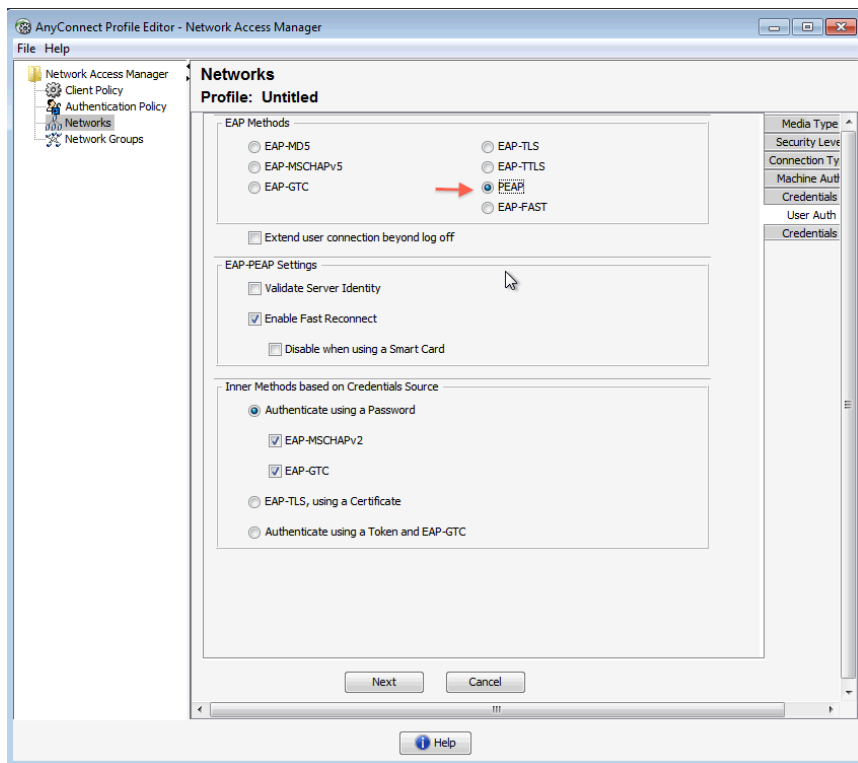
Step 7 Select “Machine and User Connection”.



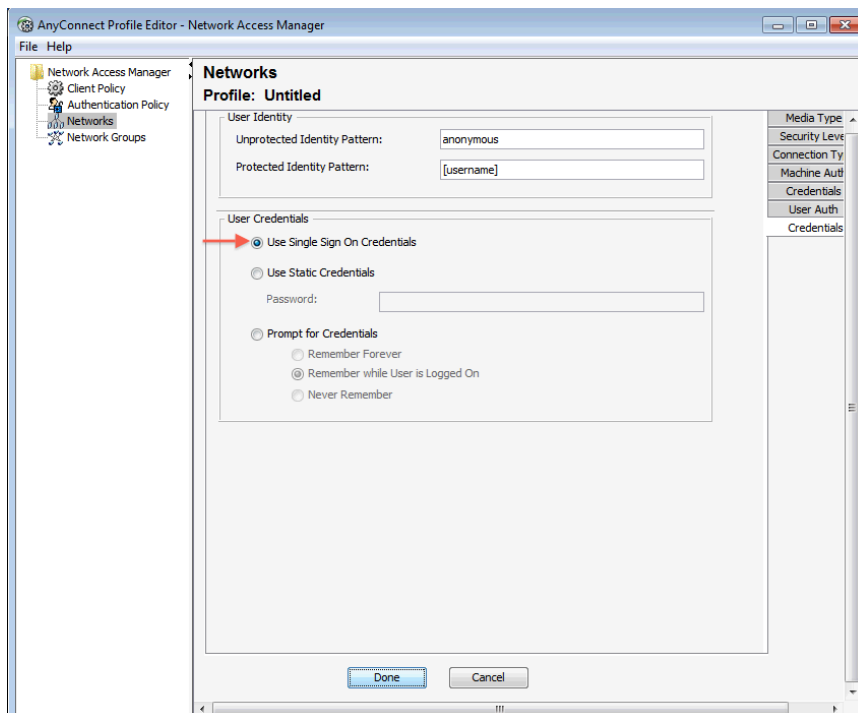
Step 8 In the Upper Right, select “Machine Auth”. Set “PEAP” as the EAP Method.



Step 9 On the upper right, select the “User Auth” tab. Set the EAP Methods to “PEAP”.



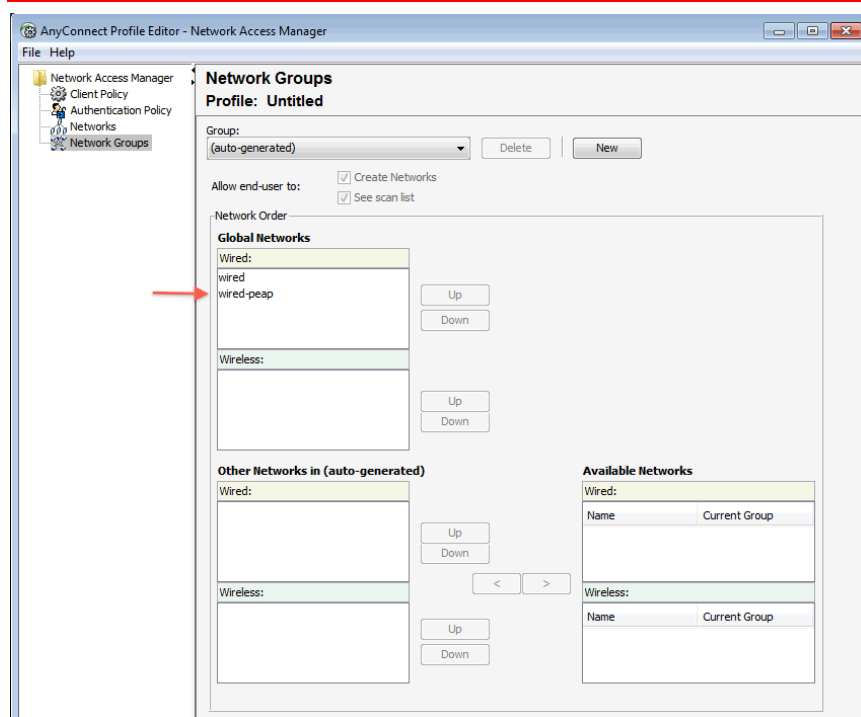
Step 10 On the upper right, select the “Credentials” tab. Note that Single Sign On is checked.




Step 11 Click Done.

Step 12 Select Network Groups. Move the wired-peap connection to the top of the Network Order.

Note: By moving the “wired-peap” connection to the top, NAM will attempt this connection first.

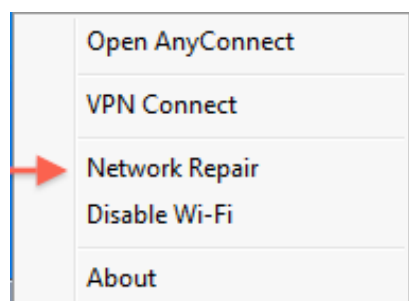


Step 13 From the menu, click File and then Save As to save the configuration with the filename **configuration.xml** (**Note: This file name is required**) in the “\ProgramData\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\newConfigFiles” directory.

Step 14 To apply this new configuration, go to the AnyConnect icon  in the system tray.

Step 15 Right click to view the options

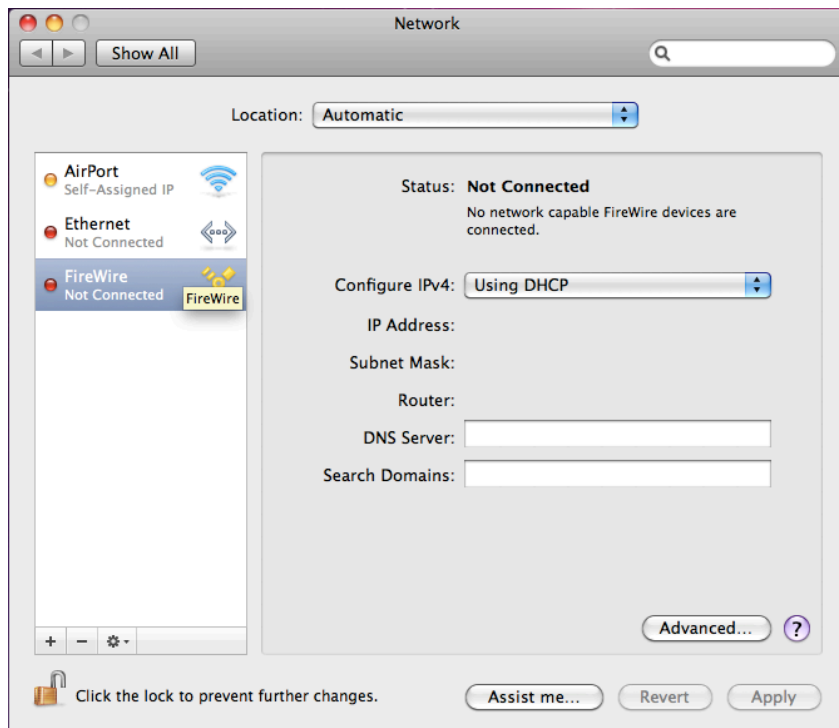
Step 16 Select “Network Repair”. This step forces the Cisco AnyConnect NAM to restart its services. A service restart causes NAM to search the newConfigFiles directory for a “configuration.xml” file.



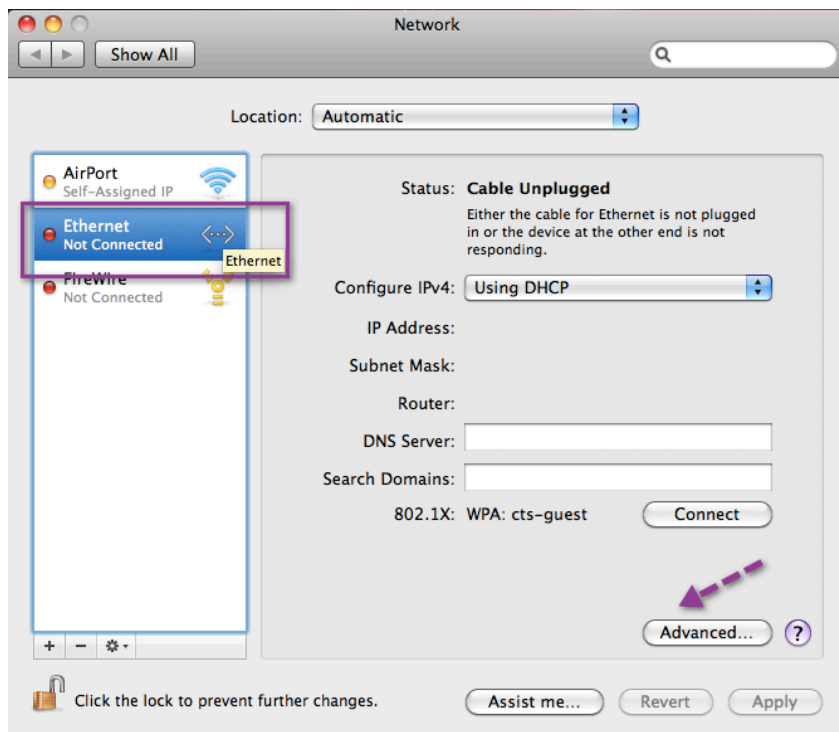
Configuration Apple Mac OS X 10.6

Note: For Apple Mac OS X 10.7, please follow this link. <http://support.apple.com/kb/HT4772>.

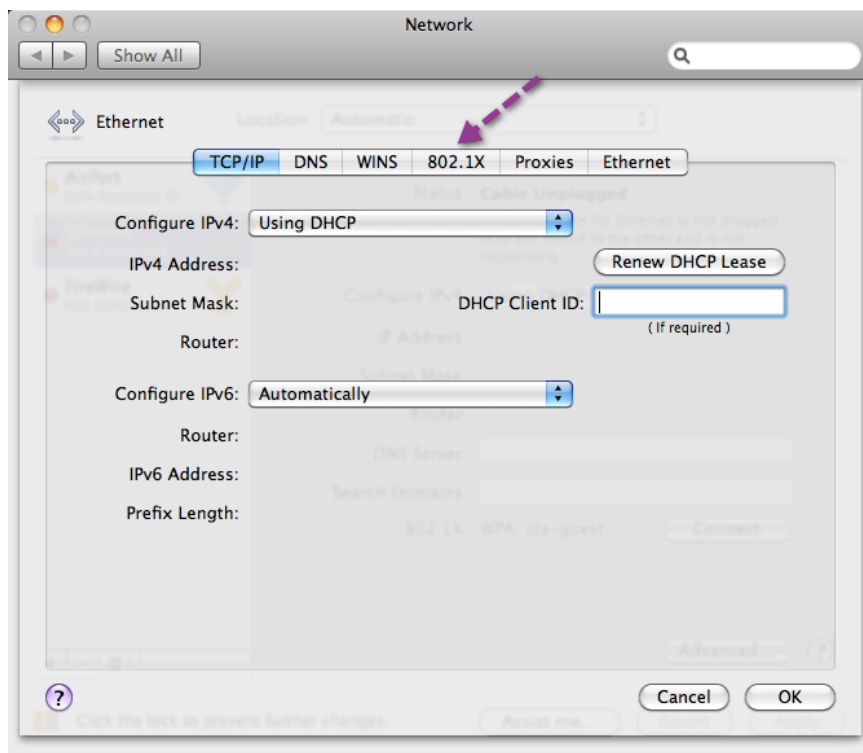
Step 1 Click "System Preferences" and select "Network" under "Internet and Network".



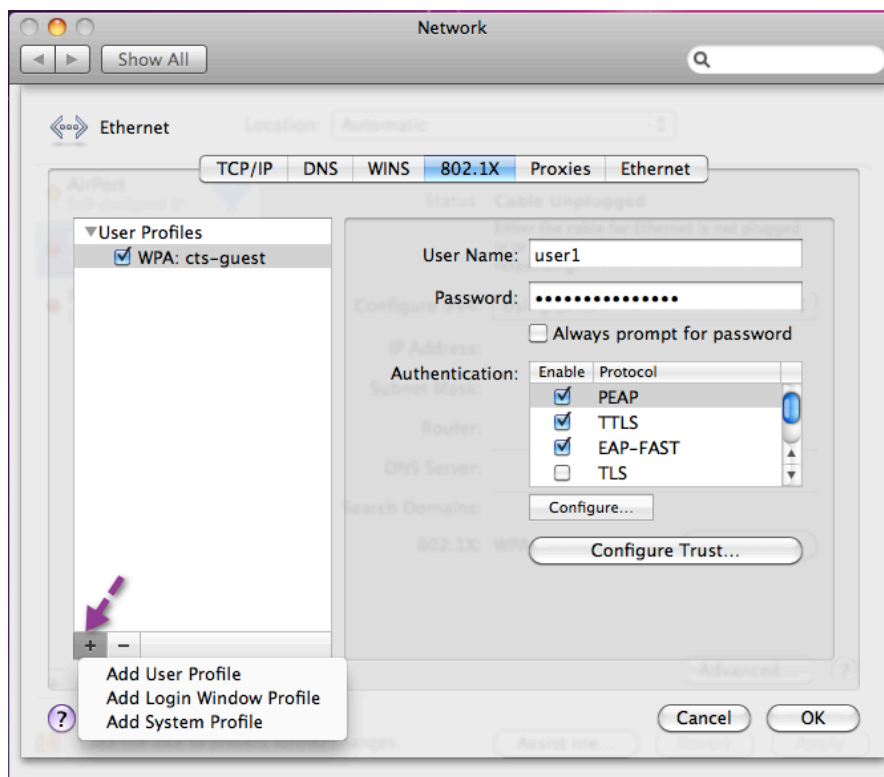
Step 2 Highlight the Ethernet Connection and click "Advanced".



Step 3 In the resulting window, select the “802.1X” tab.



Step 4 At the bottom left corner, click the “+”.



Step 5 Select the appropriate profile.

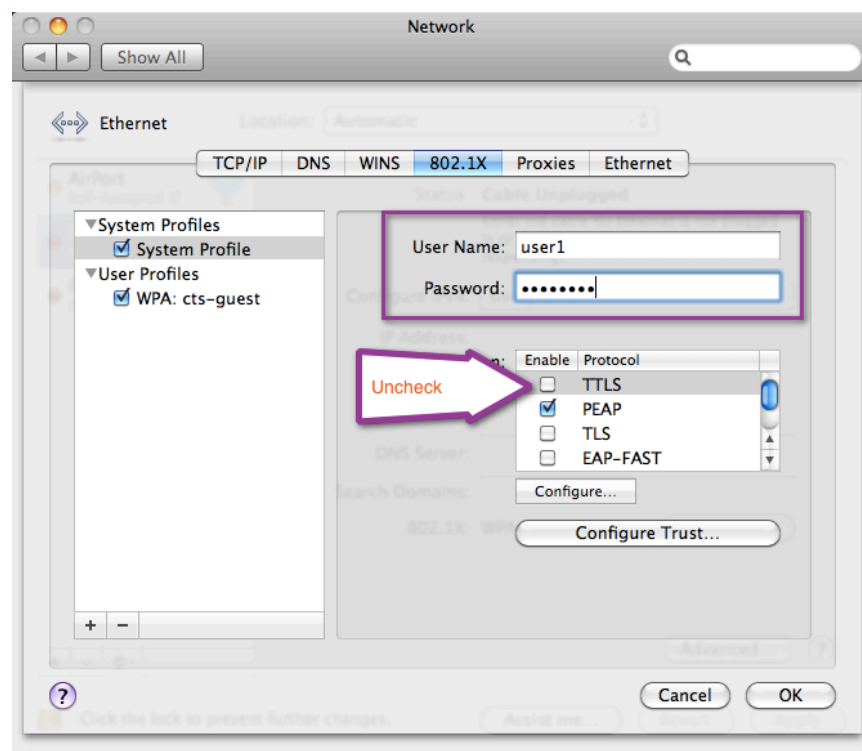
“Login Window Profile”- Use this profile if multiple users use the machine.

or

“System Profile” – Use this profile to authenticate to the network automatically. The computer will authenticate to the network even when no one is logged in, regardless of which user account logs in afterward.

Note: There can be only one system profile.

Step 6 In the resulting profile window, enter your credentials, uncheck TTLS, and click “OK”.



Notes:

Cisco ISE does not support TTLS.

When system profile is used, the user is not prompted for authentication. Instead the account that was saved (in step 7) is used. If the account entered is used to authenticate the system (not an actual user), then the account must be maintained as user in Active Directory or use a different database.

When you use Login Window Profile, you will not get prompted as long as you are logged into the system with account user credential.


To connect to a non-802.1X-enabled wired port, uncheck “System Profile” prior to plugging in.

Step 7 Click “OK” and then Apply. You will need to reboot the computer to have the settings take effect.

Note: For additional supplicant-specific information, please refer to:

http://images.apple.com/support/security/guides/docs/SnowLeopard_Security_Config_v10.6.pdf.

Procedure 1 Configure the iOS supplicant.

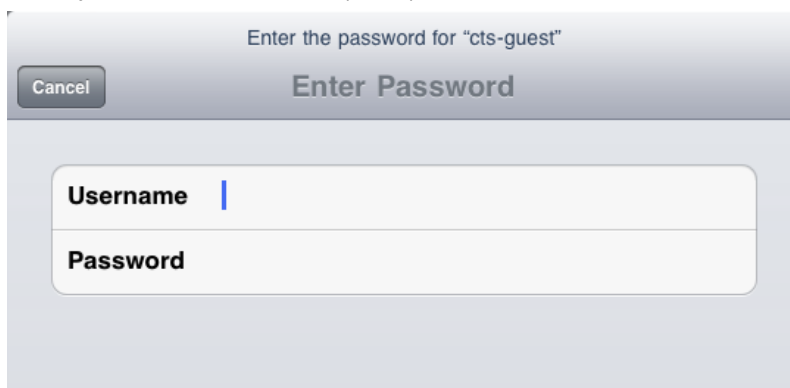
Step 1 From the home screen, tap the “Settings”  icon.

Step 2 Enable Wi-Fi. Use the slider to turn Wi-Fi on. Wait for the available networks to appear.

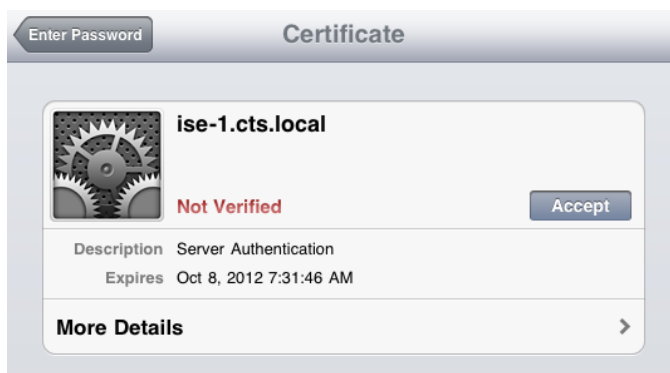


Step 3 Choose the network with which to connect. (cts-guest or cts-corp).

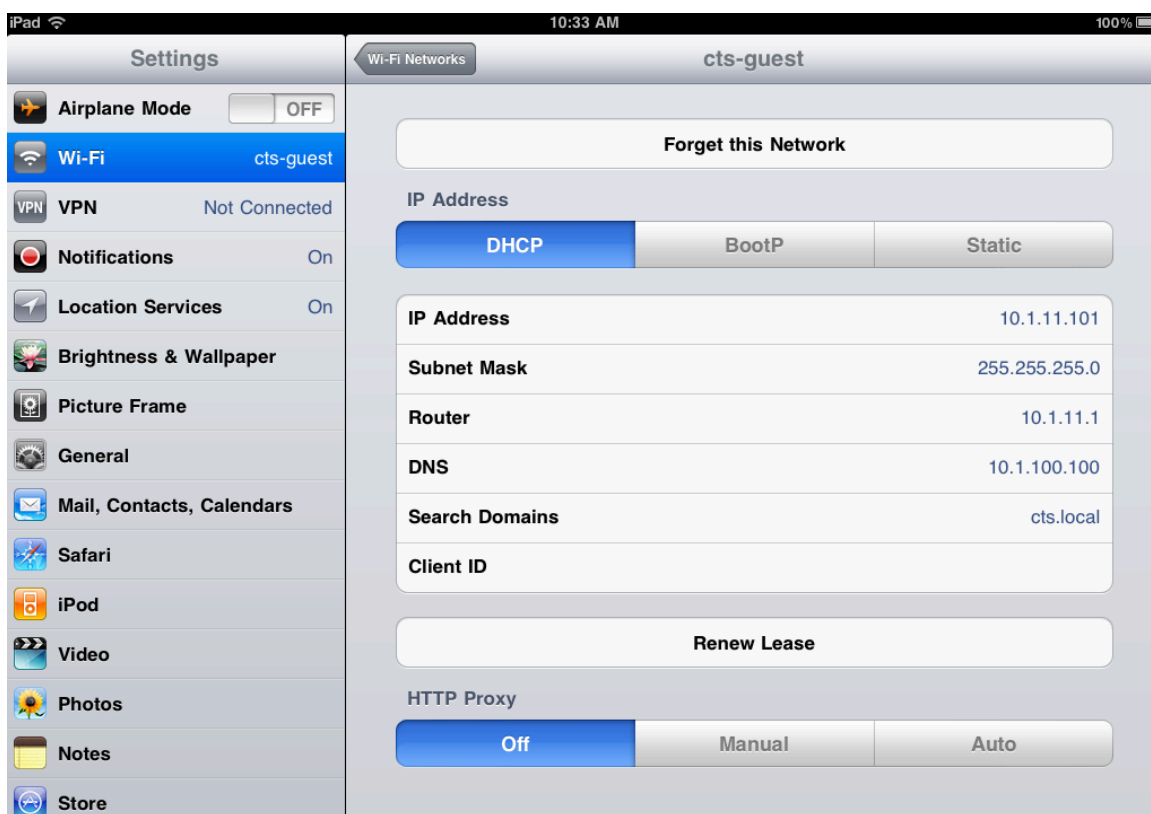
Step 4 Enter your credentials when prompted



Step 5 Accept the certificate notification.



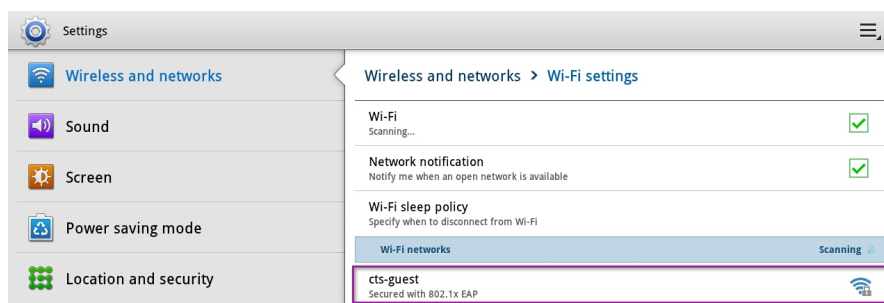
Step 6 You are now connected.



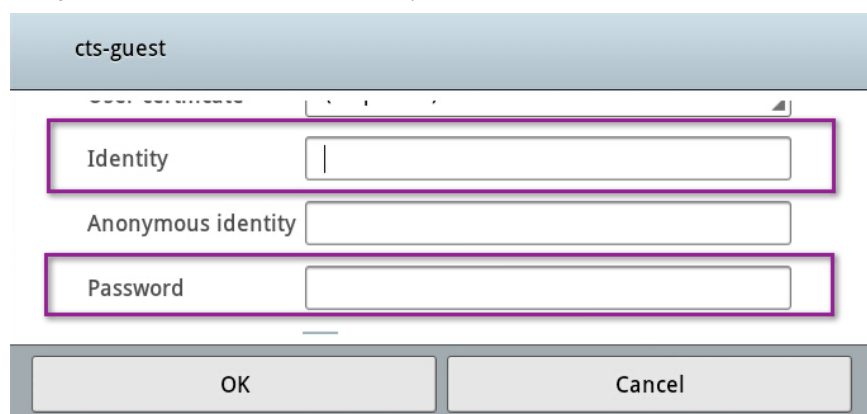
Android Honeycomb 3.1 Configuration

Step 1 From the Settings screen, select “Wireless and networks->Wi-Fi Settings”.

Step 2 From the list of available Wi-Fi networks, choose the network to which you want to connect (cts-guest or cts-corp).

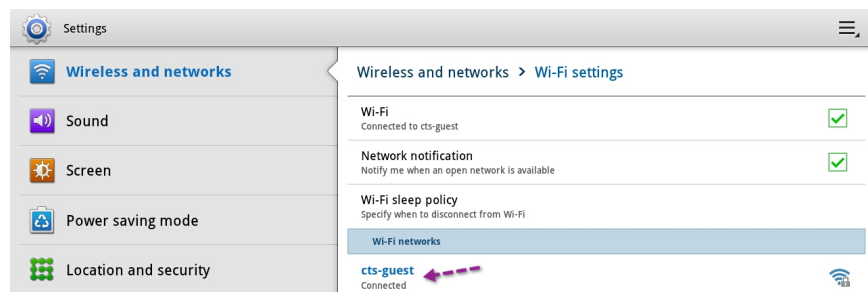


Step 3 A pop-up window should appear that requests credential and connection information. Scroll to the bottom of this window to enter credentials into the Identity and Password fields. (These are the only fields in which you need to enter information.)



Step 4 Click OK.

Step 5 You are now connected.



Step 6 To determine what the assigned IP address is, tap the “cts-guest” connection entry.



IP Phones

Within this deployment Guide, we will initially rely on endpoint profiling and MAB for Cisco IP Phones, and configure the phone supplicants in a later section. Endpoint profiling allows an organization to become more familiar with the operations of a network enabled with Cisco TrustSec security before having to fully understand the Certificate Authority Proxy Functions of an IP Phone.

Please see the section titled “[Cisco IP Phones](#)” for more information.

Switches – Universal Global Configuration Commands

The following section describes the universal switch configuration. These recommended configurations are compiled as a best practice to be used for all deployments, and remain consistent through the different stages of deployment as well as the different deployment types chosen.

Best Practice: It is recommended to use Network Configuration Management solutions, such as CiscoWorks LAN Management Solution (LMS) to manage the configurations enterprisewide. However, it was not part of the Cisco TrustSec 2.0 test lab, and therefore cannot be part of this document. It will be part of a future version.

Switch Configuration – Global Settings

Within the Cisco TrustSec 2.0 system, the switch performs the URL redirection for web authentication as well as redirecting the discovery traffic from the posture agent (Cisco NAC Agent) to the Cisco ISE Server.

Performing URL redirection at the Layer 2 access (edge) device is a vast improvement over previous NAC solutions that require an appliance to capture web traffic and perform redirection to a web authentication page, simplifying the deployment for both web authentication and the posture agent discovery process.

Note: Prerequisite configuration: This guide assumes that the switches have the fundamental basics preconfigured on them. For example, correct date and time settings by using Network Time Protocol (NTP) are considered best practice, but will not be covered in any section.

Best Practice: Always ensure that the Switch can communicate with the client subnets, to ensure that HTTP Redirection works properly. For Security Best Practices, use an Access Class to limit what addresses may manage the switch. This topic is beyond the scope of this document.

Procedure 1 Configure the HTTP Server on the Switch.

Step 1 Set the DNS Domain Name on the switch.

Cisco IOS Software does not allow for certificates, or even self-generated keys to be created and installed without first defining a DNS domain name on the device.

```
C3750X(config)#ip domain-name domain_name
```

Step 2 Generate Keys to be used for HTTPS.

```
C3750X(config)#crypto key generate rsa general-keys mod 2048
```

Note: It is recommended to use a certificate that is issued by your trusted Certificate Authority instead of a local certificate to avoid possible certificate mismatch errors during web redirection. An enterprise CA was not part of the test bed in Cisco TrustSec 2.0, and therefore is not part of this document.

Step 3 Enable the HTTP Servers on the switch.

The HTTP Server must be enabled on the switch to perform the HTTP / HTTPS capture and redirection.

```
C3750X(config)#ip http server
C3750X(config)#ip http secure-server
```

Note: Do not run the `ip http secure-server` command prior to generating the keys in step 2. If you perform the commands out of order, the switch will automatically generate a certificate with a smaller key size. This certificate can cause undesirable behavior when redirecting HTTPS traffic.

Procedure 2 Configure the Global AAA Commands.

Step 1 Enable Authentication, Authorization and Accounting on the access switch(es).

By default, the AAA "subsystem" of the Cisco switch is disabled. Prior to enabling the AAA subsystem, none of the required commands will be available in the configuration.

```
C3750X(config)#aaa new-model
```

Step 2 Create an authentication method for 802.1X.

An authentication method is required to instruct the switch on which group of RADIUS servers to use for 802.1X authentication requests.

```
C3750X(config)#aaa authentication dot1x default group radius
```

Step 3 Create an authorization method for 802.1X.

The method created in step 2 will enable the user/device Identity (username/password or certificate) to be validated by the RADIUS Server. However, simply having valid credentials is not enough. There must be an authorization as well. The authorization is what defines that the user or device is actually allowed to access the network, and what level of access is actually permitted.

```
C3750X(config)#aaa authorization network default group radius
```

Step 4 Create an Accounting method for 802.1X.

RADIUS accounting packets are extremely useful, and in many cases are required. These types of packets will help ensure that the RADIUS server (Cisco ISE) knows the exact state of the switchport and endpoint. Without the accounting packets, Cisco ISE would have knowledge only of the authentication and authorization communication. Accounting packets provide information on length of the authorized session, as well as local decisions made by the switch (such as AuthFail VLAN assignment, etc.)

```
C3750X(config)#aaa accounting dot1x default start-stop group radius
```

Procedure 3 Configure the Global RADIUS Commands.

We configure a proactive method to check the availability of the RADIUS server. With this practice, the switch will send periodic test authentication messages to the RADIUS server (Cisco ISE). It is looking for a RADIUS response from the server. A success message is not necessary – a failed authentication will suffice, because it shows that the server is alive.

Best Practice Tip: It is not possible to filter these authentications from the logging server in Cisco ISE 1.0(377). Filtering will skew the authentication success versus failures that display on the Cisco ISE dashboard, so it is recommended to use an account where authentication will succeed but authorization will deny access.

Step 1 Within global configuration mode, add a username and password for the RADIUS keepalive.

The username we are creating here will be added to the local user database in Cisco ISE at a later step. This account will be used in a later step where we define the RADIUS server.

```
C3750X(config)#username radius-test password password
```

Step 2 Add the Cisco ISE servers to the RADIUS group.

In this step we will add each Cisco ISE Policy Decision Point (PDP) to the switch configuration, using the test account we created previously. Repeat for each PDP.

```
C3750X(config)#radius-server host ise_ip_address auth-port 1812 acct-port 1813 test
username radius-test key shared_secret
```

Note: The server will proactively be checked for responses 1 time per hour, in addition to any authentications or authorizations occurring through normal processes.

Step 3 Set the dead criteria.

The switch has been configured to proactively check the Cisco ISE server for RADIUS responses. Now configure the counters on the switch to determine if the server is alive or dead. Our settings will be to wait 5 seconds for a response from the RADIUS server and attempt the test 3 times before marking the server dead. If a Cisco ISE server doesn't have a valid response within 15 seconds, it will be marked as dead.

```
C3750X(config)#radius-server dead-criteria time 5 tries 3
```

Note: We will discuss high availability in more detail in the deployment mode sections.

Step 4 Enable Change of Authorization (CoA).

Previously we defined the IP address of a RADIUS server that the switch will send RADIUS messages to. However, we define the servers that are allowed to perform Change of Authorization (RFC 3576) operations in a different listing, also within global configuration mode.

```
C3750X(config)#aaa server radius dynamic-author
C3750X(config-locsvr-da-radius)#client ise_ip_address server-key shared_secret
```

Step 5 Configure the switch to use the Cisco vendor-specific attributes.

Here we configure the switch to send any defined Vendor-Specific Attributes (VSA) to Cisco ISE PDPs during authentication requests and accounting updates.

```
C3750X(config)#radius-server vsa send authentication
C3750X(config)#radius-server vsa send accounting
```

Step 6 Next, we will enable the Vendor-Specific Attributes (VSAs).

```
C3750X(config)#radius-server attribute 6 on-for-login-auth
C3750X(config)#radius-server attribute 8 include-in-access-req
C3750X(config)#radius-server attribute 25 access-request include
```

Step 7 Ensure the Switch always sends traffic from the correct interface.

Switches may often have multiple IP Addresses associated to them. Therefore, it is a best practice to always force any management communications to occur through a specific interface. This interface IP Address must match the IP Address defined in the Cisco ISE Network Device object.

Network Management Best Practice: Use a loopback adapter for all management communication, and advertise that loopback interface into the internal routing protocol.

```
C3750X(config)#ip radius source-interface interface_name
C3750X(config)#snmp-server trap-source interface_name
C3750X(config)#snmp-server source-interface informs interface_name
```

Procedure 4 Configure the Switch to allow Profiling to / from Cisco ISE.

Identity Services Engine (Cisco ISE) 1.0 will use SNMP to query the switch for certain attributes to help identify the devices connected to the switch. As such, we will configure SNMP communities for Cisco ISE to query, as well as SNMP traps to be sent to Cisco ISE.

Step 1 Configure a read-only SNMP community.

In Cisco TrustSec 2.0, Cisco ISE needs only “read-only” SNMP commands. Ensure this community string matches the one configured in the network device object in Cisco ISE.

Security Best Practice: It is considered a best practice for security to limit the SNMP access to switches with an access class. SNMP configuration was not part of the testbed for Cisco TrustSec 2.0, and therefore will not be part of this document.

```
C3750X(config)#snmp-server community community_string RO
```

Step 2 Configure the switch to send traps.

We will now enable an SNMP trap to be sent with changes to the MAC address table. A trap that includes the device MAC address and interface identifier is sent to Cisco ISE whenever a new address is inserted, removed, or moved in the address table.

```
C3750X(config)#snmp-server enable traps mac-notification change move threshold
```

Step 3 Add Cisco ISE as an SNMP trap receiver.

Here, a server is added as a trap receiver for the configured MAC notification.

```
C3750X(config)#snmp-server host ise_ip_address version 2c community_string mac-
notification
```

Step 4 Configure DHCP snooping trusted ports.

DHCP snooping is not required for Cisco TrustSec 2.0, but it is considered a best practice. Not only does it enable better availability by denying rogue DHCP servers, but it also prepares the switch for other security tools such as Dynamic ARP Inspection, as well as preparing the switch for some future functions coming in later releases of Cisco TrustSec technology.

Before configuring DHCP snooping, be sure to note the location of your trusted DHCP servers. When configuring DHCP snooping, the switch will deny DHCP server replies from any port not configured as "trusted". Enter interface configuration mode for the uplink interface and configure it as a trusted port.

Note: This step is required only if the uplink port is a switchport or trunk, not a Layer 3 interface. This fact explains why the **ip dhcp snooping trust** command is missing from the example configuration at the end of this section.

```
C3750X(config)#interface interface_name
C3750X(config-if)#ip dhcp snooping trust
```

Step 5 Enable DHCP snooping.

DHCP Snooping is enabled at global configuration mode. After enabling DHCP snooping, you must then configure the VLANs it should work with.

```
C3750X(config)#ip dhcp snooping
C3750X(config)#ip dhcp snooping vlan vlan_id_or_vlan_range
```

Procedure 5 Configure Local Access Control Lists.

Certain functions on the switch require the use of locally configured Access Control Lists (ACLs), such as URL redirection. Some of these ACLs created will be used immediately, and some may not be used until a much later phase of your deployment. The goal of this section is to prepare the switches for all possible deployment models at one time, and limit the operational expense of repeated switch configuration.

Note: More explanation of where and when these ACLs will be used will follow.

Step 1 Add the following ACL to be used on switchports in Monitor Mode:

```
C3750X(config)#ip access-list ext ACL-ALLOW
C3750X(config-ext-nacl)#permit ip any any
```

Step 2 Add the following ACL to be used on switchports in Authentication and Enforcement Modes:

```
C3750X(config)#ip access-list ext ACL-DEFAULT
C3750X(config-ext-nacl)#remark DHCP
C3750X(config-ext-nacl)#permit udp any eq bootpc any eq bootps
C3750X(config-ext-nacl)#remark DNS
C3750X(config-ext-nacl)#permit udp any any eq domain
C3750X(config-ext-nacl)#remark Ping
C3750X(config-ext-nacl)#permit icmp any any
C3750X(config-ext-nacl)#remark PXE / TFTP
C3750X(config-ext-nacl)#permit udp any any eq tftp
C3750X(config-ext-nacl)#remark Drop all the rest
C3750X(config-ext-nacl)#deny ip any any log
```

Step 3 Add the following ACL to be used for URL redirection with Web Authentication:

```
C3750X(config)#ip access-list ext ACL-WEBAUTH-REDIRECT
C3750X(config-ext-nacl)#remark explicitly deny DNS from being redirected to address a bug
C3750X(config-ext-nacl)#deny udp any any eq 53
C3750X(config-ext-nacl)#remark redirect all applicable traffic to the ISE Server
C3750X(config-ext-nacl)#permit tcp any any eq 80
C3750X(config-ext-nacl)#permit tcp any any eq 443
C3750X(config-ext-nacl)#remark all other traffic will be implicitly denied from the redirection
```

Step 4 Add the following ACL to be used for URL redirection with the posture agent:

```
C3750X(config)#ip access-list ext ACL-AGENT-REDIRECT
C3750X(config-ext-nacl)#remark explicitly deny DNS from being redirected to address a bug
C3750X(config-ext-nacl)#deny udp any any eq 53
C3750X(config-ext-nacl)#remark redirect HTTP traffic only
C3750X(config-ext-nacl)#permit tcp any any eq 80
C3750X(config-ext-nacl)#remark all other traffic will be implicitly denied from the redirection
```

Procedure 6 Configure the Global 802.1X Commands.

Step 1 Enable 802.1X globally on the switch.

Enabling 802.1X globally on the switch does not actually enable authentication on any of the switchports. Authentication will be configured, but not enabled until the later sections where we configure monitor mode.

```
C3750X(config)#dot1x system-auth-control
```

Step 2 Enable Downloadable ACLs to function.

Downloadable Access Control Lists (DACLS) are a very common enforcement mechanism in a Cisco TrustSec deployment. In order for DACLS to function properly on a switch, IP device tracking must be enabled globally.

```
C3750X(config)#ip device tracking
```

Note: There are some uncommon cases with Windows 7 and devices that do not respond to ARPs where it may be required to use the command **ip device tracking use SVI**. See CSCtn27420, CSCti94012, and CSCtr26069 for more details.

Step 3 Enable Syslog on the Switch.

Syslog may be generated on Cisco IOS Software in many events. Some of the syslog message can be sent to Cisco ISE to be used in troubleshooting purposes. To ensure Cisco ISE is able to compile appropriate syslog messages from the switch, use the following commands.

Note: The logs should be sent to the Cisco ISE node with the Monitor persona.

```
C3750X(config)#logging monitor informational
C3750X(config)#logging origin-id ip
C3750X(config)#logging source-interface <interface_id>
C3750X(config)#logging host <ISE_MNT_PERSONA_IP_Address_x> transport udp port 20514
```

Set up standard logging functions on the switch to support possible troubleshooting / recording for Cisco ISE functions. EPM is a part of the Cisco IOS Software module responsible for features such as Web Authentication and Downloadable ACL. Enabling EPM Logging generates a syslog related to Downloadable ACL authorization, and part of the log can be correlated inside Cisco ISE when such logs are sent to Cisco ISE.

```
C3750X(config)#epm logging
```

Only the following NAD syslog messages are actually collected and used by Cisco ISE:

- AP-6-AUTH_PROXY_AUDIT_START
- AP-6-AUTH_PROXY_AUDIT_STOP
- AP-1-AUTH_PROXY_DOS_ATTACK
- AP-1-AUTH_PROXY_RETRIES_EXCEEDED
- AP-1-AUTH_PROXY_FALLBACK_REQ
- AP-1-AUTH_PROXY_AAA_DOWN
- AUTHMGR-5-MACMOVE
- AUTHMGR-5-MACREPLACE
- MKA-5-SESSION_START
- MKA-5-SESSION_STOP
- MKA-5-SESSION_REAUTH
- MKA-5-SESSION_UNSECURED
- MKA-5-SESSION_SECURED
- MKA-5-KEEPALIVE_TIMEOUT
- DOT1X-5-SUCCESS / FAIL
- MAB-5-SUCCESS / FAIL
- AUTHMGR-5-START / SUCCESS / FAIL
- AUTHMGR-SP-5-VLANASSIGN / VLANASSIGNERR
- EPM-6-POLICY_REQ
- EPM-6-POLICY_APP_SUCCESS / FAILURE
- EPM-6-IPEVENT:
- DOT1X_SWITCH-5-ERR_VLAN_NOT_FOUND
- RADIUS-4-RADIUS_DEAD

Example Global Configuration:

```
hostname C3750X
username radius-test password 0 Cisco123
!
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
  client 10.1.100.3 server-key Cisco123
!
ip dhcp snooping vlan 10-13
ip dhcp snooping
ip domain-name cts.local
ip device tracking
!
dot1x system-auth-control
!
ip http server
ip http secure-server
!
ip access-list extended ACL-AGENT-REDIRECT
  remark explicitly prevent DNS from being redirected to address a bug
  deny  udp any any eq domain
  remark redirect HTTP traffic only
  permit tcp any any eq www
  remark all other traffic will be implicitly denied from the redirection
ip access-list extended ACL-ALLOW
  permit ip any any
ip access-list extended ACL-DEFAULT
  remark DHCP
  permit udp any eq bootpc any eq bootps
  remark DNS
  permit udp any any eq domain
  remark Ping
  permit icmp any any
  remark PXE / TFTP
  permit udp any any eq tftp
  remark Drop all the rest
  deny  ip any any log
ip access-list extended ACL-WEBAUTH-REDIRECT
  remark explicitly prevent DNS from being redirected to accommodate certain switches
  deny  udp any any eq domain
  remark redirect all applicable traffic to the ISE Server
  permit tcp any any eq www
  permit tcp any any eq 443
  remark all other traffic will be implicitly denied from the redirection
!
ip radius source-interface Loopback0
snmp-server community Cisco123 RO
snmp-server trap-source Loopback0
snmp-server source-interface informs Loopback0
snmp-server enable traps mac-notification change move threshold
snmp-server host 10.1.100.3 version 2c Cisco123 mac-notification
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server dead-criteria time 5 tries 3
radius-server host 10.1.100.3 auth-port 1812 acct-port 1813 test username radius-test key
Cisco123
radius-server vsa send accounting
radius-server vsa send authentication
logging monitor informational
epm logging
logging origin-id ip
logging source-interface Loopback0
logging host 10.1.100.3 transport udp port 20514
```

Switches: Universal Switchport Configuration

In the previous section we defined the universal commands for the Global Configuration settings of the access layer switches, including RADIUS, SNMP, Profiling, and AAA methods.

This section focuses on building a single port configuration that can be used across your entire Cisco TrustSec deployment, regardless of switch type or deployment model you use.

Configure All Access Ports to Have the Golden Configuration

One of the first things to do before configuring any of the authentication settings on the switchport is to ensure the switchport is configured as a Layer 2 port, not a Layer 3 port. This command is a simple, one-word command that we will run, and from that point the other commands we run will all take effect.

Note: If you are using a bulk configuration tool, such as Cisco LAN Management Solution (LMS) 4.1, you may need to ensure this command is run prior to any of the commands that follow.

Procedure 1 Set up basic switchport configurations.

Step 1 Enter interface configuration mode for the switchport range.

```
C3750X(config)#interface range first_interface - last_interface
```

Step 2 Ensure the ports are Layer 2 switchports.

```
C3750X(config-if-range)#switchport
```

Step 3 Configure the port for Layer 2 Edge, using the host macro.

The host macro will automatically run three commands for you. It will configure the port to be an access port (nontrunk), disable channel groups, and configure spanning tree to be in portfast mode.

```
C3750X(config-if-range)#switchport host  
! - Switch Output:  
switchport mode will be set to access  
spanning-tree portfast will be enabled  
channel group will be disabled
```

Procedure 2 Authentication Settings – Flexible Authentication and High Availability

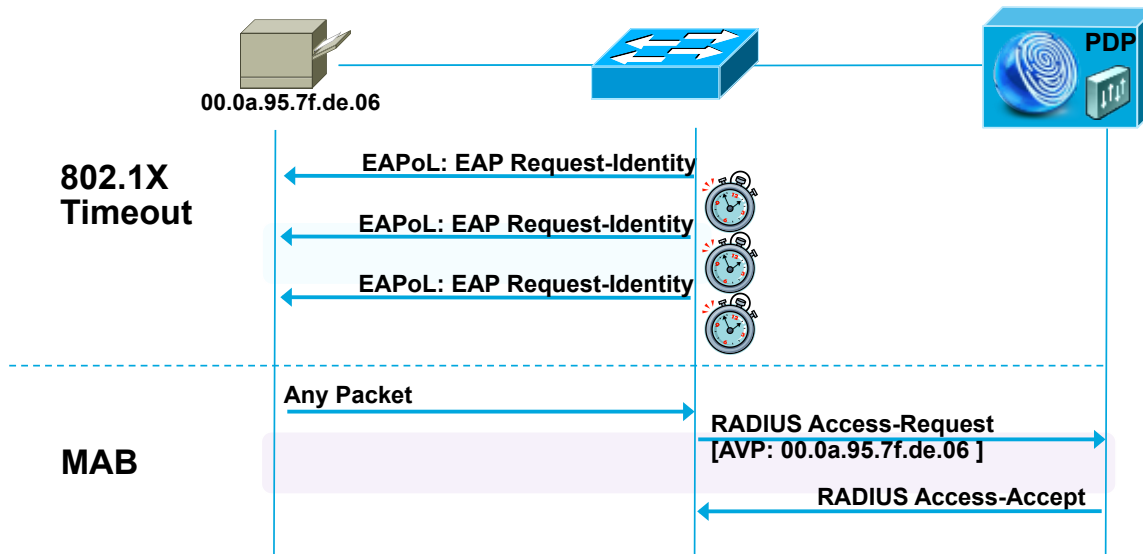
The default behavior of 802.1X is to deny access to the network when an authentication fails. This behavior was discovered to be an undesirable behavior in many customer deployments, because it does not allow for guest access, nor does it allow employees to remediate their computer systems and gain full network access. The next phase in handling 802.1X authentication failures was to provide an “Auth-Fail VLAN” to allow a device/user that failed authentication to be granted access to a VLAN that provided limited resources.

This step was a step in the right direction, but was still missing some practicality, especially in environments that must use MAC authentication bypass for all the printers and other nonauthenticating devices. With the default behavior of 802.1X, an administrator would have to configure ports for printers and other devices that do not have supplicants differently from the ports where they planned to do authentication.

Therefore, Cisco created Flexible Authentication (Flex-Auth). Flex-Auth allows a network administrator to set an authentication order and priority on the switchport, thereby allowing the port to attempt 802.1X, MAC authentication bypass, and then WebAuth in order. All of these functions are provided while maintaining the same configuration on all access ports, thereby providing a much simpler operational model for customers than traditional 802.1X deployments.

As mentioned previously, there are multiple methods of authentication on a switchport: 802.1X (dot1x), MAC Authentication Bypass (MAB), and Web-based Authentication (WebAuth). With 802.1X authentication, the switch sends an identity request (EAP-Identity-Request) periodically after the link state has changed to “up” (see the “Authentication Settings – Timers” section for recommended timer changes). Additionally, the endpoint supplicant should send a periodic EAP over LAN Start (EAPoL-Start) message into the switchport to speed up authentication. If a device is not able to authenticate, it merely has to wait until the dot1x timeout occurs, and MAC Authentication Bypass (MAB) will occur. Assuming the device MAC address is in the correct database, it will then be authorized to access the network (Figure 6).

Figure 6: Flexible Authentication



The following steps will walk you through the configuration of Flex-Auth and the configurable actions for Authentication High Availability.

Step 1 Configure the authentication method priority on the switchports.

The best practice is to always prefer the stronger authentication method (dot1x). The dot1x method is also the default of all Cisco Switches.

```
C3750X(config-if-range) #authentication priority dot1x mab
```

Step 2 Configure the authentication method order on the switchports.

There are certain deployment methods where MAC-Authentication Bypass (MAB) should occur before 802.1X authentication. For those corner cases, Cisco switches do allow for a network administrator to set a user-definable authentication order. However, the best practice is to maintain the order of dot1x and then MAB.

```
C3750X(config-if-range) #authentication order dot1x mab
```

Step 3 Configure the port to use Flex-Auth.

```
C3750X(config-if-range) #authentication event fail action next-method
```

Step 4 Configure the port to use a local VLAN when the RADIUS server is "dead".

In the "Configure the Global RADIUS Commands" procedure, we configured the RADIUS server entry to use a test account that will proactively alert the switch when Cisco ISE has stopped responding to RADIUS requests. Now we will configure the switchport to locally authorize the port when that server is found to be "dead", and re-initialize authentication when the server becomes "alive" again.

```
C3750X(config-if-range) #authentication event server dead action authorize vlan vlan-id  
C3750X(config-if-range) #authentication event server alive action reinitialize
```

Step 5 Configure the port to use a local VLAN when the RADIUS server is "dead", and allow existing and new hosts.

This feature was introduced to resolve problems with multiple authentication hosts on single port when a portion of them already authenticate while the RADIUS server is operational, and others (new hosts) are trying to authenticate when the RADIUS server is down.

Before introducing this new feature, all authenticated hosts (when the RADIUS server is **up**) get full access to network and the others (the new hosts) do not get access to the network. With this new feature/CLI, when new hosts try to access to the network and the RADIUS server is down, that port is reinitialized immediately and all hosts (in this port) get the same VLAN.

```
C3750X(config-if-range) #authentication event server dead action reinitialize vlan vlan-id
```

Step 6 Set the host mode of the port.

The default behavior of an 802.1X-enabled port is to authorize only a single MAC address per port. There are other options, most notably Multi-Domain Authentication (MDA) and Multiple Authentication (Multi-Auth) modes. During the initial phases of any Cisco TrustSec deployment, it is best practice to use Multi-Auth mode to ensure that there is no denial of service while deploying 802.1X.

Note: Port Security is not recommended in a Cisco TrustSec deployment, because 802.1X handles this function natively.

Multi-Auth mode will allow virtually unlimited MAC addresses per switchport, and require an authenticated session for every MAC address. When the deployment moves into the late stages of the authenticated phase, or into the enforcement phase, it is then recommended to use Multi-Domain mode. Multi-Domain Authentication will allow a single MAC address in the DATA Domain and a single MAC address in the Voice domain per port.

```
C3750X(config-if-range) #authentication host-mode multi-auth
```

Step 7 Configure the violation action.

When an authentication violation occurs, such as more MAC addresses than are allowed on the port, the default action is to put the port into an err-disabled state. Although this behavior may seem to be a nice, secure behavior, it can create an accidental denial of service, especially during the initial phases of deployment. Therefore we will set the action to be "restrict". This mode of operation will allow the first authenticated device to continue with its authorization, and deny any additional devices.

```
C3750X(config-if-range) #authentication violation restrict
```

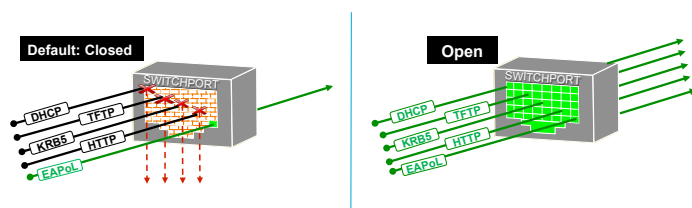
Procedure 3 Authentication Settings – Open Authentication and Additional Steps

802.1X is designed to be binary by default. Successful authentication means the user is authorized to access the network. Unsuccessful authentication means the user has no access to the network. This paradigm does not lend itself very well to a modern organization. Most organizations need to do workstation imaging with Pre-Execution Environments (PXE), or may have some thin clients that have to boot with DHCP and don't have any way to run a supplicant.

Additionally, when early adopters of 802.1X would deploy authentication companywide, there were repercussions. Many supplicants were misconfigured; there were unknown devices that could not authenticate because of a lack of supplicant, and other reasons.

Cisco created open authentication to aid with deployments. Open authentication will allow all traffic to flow through the switchport, even without the port being authorized. This feature will allow authentication to be configured across the entire organization, but not deny access to any device.

Figure 7: Default Mode vs. Open Mode



Step 1 Set the port for open authentication.

```
C3750X(config-if-range) #authentication open
```

Step 2 Enable MAC Authentication Bypass on the port.

```
C3750X(config-if-range) #mab
```

Step 3 Enable the port to do IEEE 802.1X Authentication.

```
C3750X(config-if-range) #dot1x pae authenticator
```

Procedure 4 Authentication Settings – Timers

Many timers can be modified as needed in a deployment. Unless you are experiencing a specific problem where adjusting the timer may correct unwanted behavior, it is recommended to leave all timers at their default values except for the 802.1X Transmit timer (tx-period).

The tx-period timer defaults to a value of 30 seconds. Leaving this value at 30 seconds provides a default wait of 90 seconds (3 x TX-Period) before a switchport will begin the next method of authentication, and begin the MAB process for non-authenticating devices.

Best Practice Tip: Based on numerous deployments, the best-practice recommendation is to set the tx-period value to 10 seconds to provide the most optimal time for MAB devices. Setting the value below 10 seconds may result in unwanted behavior.

Step 1 Configure the tx-period timer.

```
C3750X(config-if-range) #dot1x timeout tx-period 10
```

Procedure 5 Apply the initial ACL on the Port and enable authentication.

This step will prepare the port for Monitor Mode: Applying a default ACL on the port without denying any traffic.

Step 1 Apply the initial ACL (ACL-ALLOW).

```
C3750X(config-if-range) #ip access-group ACL-ALLOW in
```

Step 2 Turn Authentication "on".

```
C3750X(config-if-range) #authentication port-control auto
```

Note: This command is required to enable authentication (802.1X, MAB, WebAuth). Without this command, everything will appear to be working, but no authentications will be sent to the RADIUS server.

Wireless – Universal Configuration

The following section describes the “universal configuration” for Wireless LAN Controllers (WLC). These recommended configurations are compiled as a best practice to be used for all deployments, and they remain consistent through the different stages of deployment, as well as the different deployment types chosen.

Wireless LAN Controllers – Configuration

Procedure 1 Bootstrap the Wireless LAN Controller.

Step 1 Connect to the console port of the WLC. Refer to the following settings to bootstrap the WLC.

```
(Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup

Would you like to terminate autoinstall? [yes]:yes
AUTO-INSTALL: process terminated -- no configuration loaded

System Name [Cisco_91:e2:64] (31 characters max):
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): *****
Re-enter Administrative Password                : *****

Service Interface IP Address Configuration [static][DHCP]:dhcp

Enable Link Aggregation (LAG) [yes][NO]: no

Management Interface IP Address: 10.1.60.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.1.60.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.1.100.100

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: cts.local

Network Name (SSID): CTS-CORP

Configure DHCP Bridging Mode [yes][NO]: no

Allow Static IP Addresses [YES][no]: no

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:us

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: yes
Enter the NTP server's IP address: 10.1.100.100
Enter a polling interval between 3600 and 604800 secs: 3600

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

Best Practice: It has been discovered that with the WLC Virtual Gateway address 1.1.1.1, users may get certificate mismatches. Therefore the Best Practice recommendation is to use a routable IP Address that is also in the DNS, and issue a valid Certificate for the WLC for this IP Address from your internal CA.

An enterprise CA was not part of the Cisco TrustSec 2.0 Testing environment, and therefore cannot be included in this Design and Implementation Guide. It will be added to a future Cisco TrustSec release.

Step 2 Configure the Switchport for the port connected to the WLC.

```
interface GigabitEthernet2/46
description WLC-5500 connection
ip address 10.1.60.1 255.255.255.0
end
```

Procedure 2 Configure SNMP on the WLC.

Step 1 Navigate to **Management → SNMP → General** and ensure that SNMPv2 is enabled for profiling.

The screenshot shows the Cisco WLC Management interface. The left sidebar has a 'Management' section with a tree view. 'SNMP' is expanded, and 'General' is selected, indicated by red arrows. The main content area is titled 'SNMP System Summary'. It contains several fields: 'Name' (Cisco_91:e2:64), 'Location' (empty), 'Contact' (empty), 'System Description' (Cisco Controller), 'System Object ID' (1.3.6.1.4.1.9.1.1069), 'SNMP Port Number' (161), 'Trap Port Number' (162), 'SNMP v1 Mode' (Disable), 'SNMP v2c Mode' (Enable), and 'SNMP v3 Mode' (Enable). A red arrow points to the 'SNMP v2c Mode' dropdown menu.

Step 2 Click Communities and create a new community using the values in Table 9. Click **Apply** when done.

Table 9: Values for Creating New Community

Attribute	Value
Community Name	ciscoro
IP Address	10.1.100.0
IP Mask	255.255.255.0
Access Mode	Read Only
Status	Enable

Procedure 3 Configure the WLC to use Cisco ISE as a RADIUS server.

Step 1 Access the WLC GUI and navigate to Security → RADIUS → Authentication.

Step 2 Set the Call Station ID type to System MAC address.



Step 3 Click Apply.

Note: This setting is not required for 802.1X authentication, but may be useful in Cisco ISE profiling of wireless devices, even when they connect to non-1X networks configured for RADIUS NAC. By sending the MAC address of the endpoint versus IP address, RADIUS packets sent to a Cisco ISE Policy Service node configured for Profiling Services will be able to discover this MAC address and collect attributes for classification purposes.

Note: Full Profiling Services are **not** currently supported for non-1X WLANs because CoA is not supported on these networks. However, profiling information can be collected for endpoints while connected to a non-1X WLAN. This information can then be used for inventory purposes. It can also be used for new wireless connections that rely on 802.1X or wireless MAC Filtering via RADIUS lookup for authentication and authorization.

Step 4 Click **New...** on the top right corner, to add a new RADIUS Authentication server (Table 10).

Table 10: RADIUS Authentication Server Settings

Attribute	Value
Server Index (Priority)	1
Server IP Address	10.1.100.3
Shared Secret Format	ASCII
Shared Secret	Cisco123
Key Wrap	(Not checked)
Port Number	1812
Server Status	Enabled (checked)
Support for RFC 3576	Enabled (checked)
Server Timeout	2 seconds
Network User	Enabled (checked)
Management	Enabled (checked)
IPSec	(Not checked)

Step 5 Click **Accounting** and **New...** to add RADIUS accounting servers (Table 11).

Table 11: RADIUS accounting Servers Settings

Attribute	Value
Server Index (Priority)	1
Server IP Address	10.1.100.3
Shared Secret Format	ASCII
Shared Secret	Cisco123
Port Number	1813
Server Status	Enabled (checked)
Server Timeout	30 seconds
Network User	Enabled (checked)
IPSec	(Not checked)

Step 6 Click Apply and Save Configuration.

Procedure 4 Create a wACL for Posture Assessment.

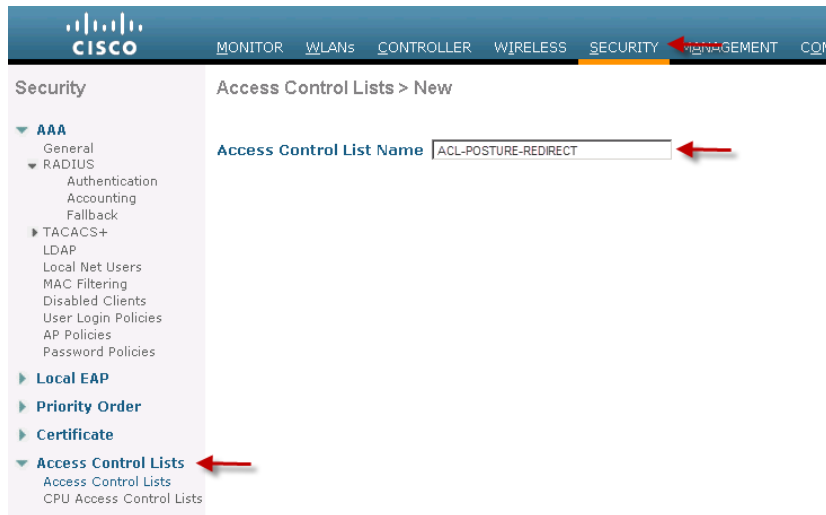
When a user connects to a network, the user is initially put into a quarantine state. During this stage, we allow only DNS and traffic from the NAC agent to go to Cisco ISE. When Cisco ISE determines the user to be using a posture-compliant device, RADIUS CoA is used to reauthenticate the user and provide the user with access appropriate to the user's role. Because the WLCs support only named ACLs today, we need to predefine ACLs on the WLC.

Although we are defining this ACL for posture redirection at this stage, it will not be utilized until we move in to the Enforcement mode with posture enabled.

Note: ACLs on the Wireless LAN Controller enforce policies at Layer 3 and Layer 4. wACLs support up to 64 rules and can be applied on a per-interface or per-user basis.

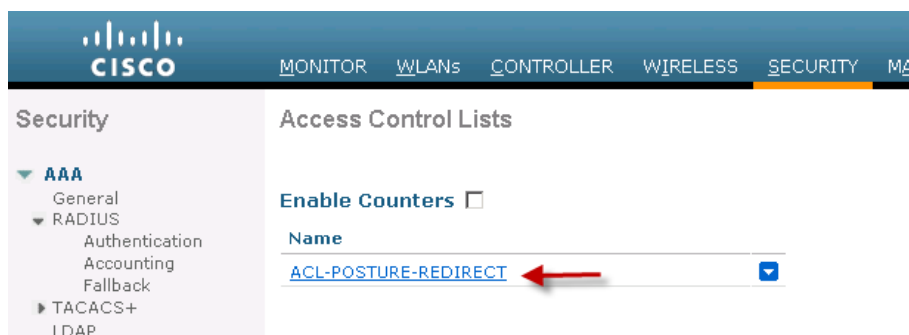
Step 1 From the WLC, navigate to Security → Access Control Lists. Click New.

Step 2 Use **ACL-POSTURE-REDIRECT** as the ACL name.



Note: The ACL to be applied to a user session has to be predefined on the WLC. The name used in the Cisco ISE authorization profile should exactly match the ACL name on the WLC.

Step 3 Click **ACL-POSTURE-REDIRECT** ACL.



Step 4 Click **Add New Rule**. Use the values listed in Table 12 for each sequence.

Step 5 Click **Apply** after each set of values and select to **Add New Rule** for the next rule.

Table 12: ACL-POSTURE-REDIRECT for Wireless LAN Controller

ACL-POSTURE-REDIRECT				
Sequence	1	2	3	4
Source	Any	IP address 10.1.100.3 255.255.255.255	Any	Any
Destination	IP address 10.1.100.3 255.255.255.255	Any	Any	Any
Protocol	Any	Any	UDP	UDP
Source Port	Not Applicable	Not Applicable	DNS	Any
Destination Port	Not Applicable	Not Applicable	Any	DNS
Action	Permit	Permit	Permit	Permit

The screenshot shows the Cisco Wireless LAN Controller configuration interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted), MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the configuration tree with Security > AAA > General selected. The main content area is titled 'Access Control Lists > Edit' and shows the configuration for the 'ACL-POSTURE-REDIRECT' access list. The 'General' tab is active, displaying the 'Access List Name' as 'ACL-POSTURE-REDIRECT' and 'Deny Counters' as '0'. Below this is a table with columns: Seq, Action, Source IP/Mask, Destination IP/Mask, Protocol, Source Port, Dest Port, DSCP, Direction, and Number of Hits. The table is currently empty. At the top right of the configuration area, there are buttons for '< Back' and 'Add New Rule'.

Step 6 Confirm the ACL is configured correctly.

Final ACL

Access List Name: ACL-POSTURE-REDIRECT
Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.1.100.3 / 255.255.255.255	Any	Any	Any	Any	Any	0
2	Permit	10.1.100.3 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0

Note: When a client is in the Pre-Posture state (*POSTURE_REQ* – as defined in the WLC), the default Behavior of the WLC is to Block All traffic except DHCP/DNS. The PRE-POSTURE ACL (which is called in the url-redirect-acl AV Pair received for Cisco ISE) is applied to the client, and it can reach only resources specifically allowed in the ACL.

Procedure 5 Add a wACL to permit all traffic.

Step 1 Follow the steps in the section “Create a wACL for Posture Assessment” to create an ACL :

Sequence	1
Source	Any
Destination	Any
Protocol	Any
DSCP	Any
Direction	Any
Action	Permit

Step 2 Create dynamic interfaces for the Employee and Guest VLANs.

Step 3 From the WLC GUI, navigate to **Controller → Interfaces** and click **New**.

Controller

Interfaces

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
management	untagged	10.1.60.2	Static	Enabled
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

Step 4 Use the values listed in below and click **Apply**.

Attribute	Value
Interface Name	Employee
VLAN id	10

Step 5 Enter the values listed below for the **Employee Interface**.

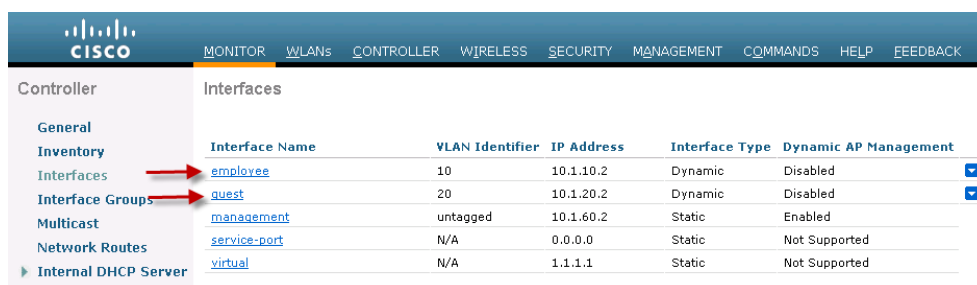
Attribute	Value
Port Number	1
VLAN Identifier	10
IP Address	10.1.10.2
Netmask	255.255.255.0
Gateway	10.1.10.1
DHCP	10.1.100.100

Step 6 Repeat the steps to create a dynamic interface for Guests :

Attribute	Value
Interface Name	Guest
VLAN id	20

Attribute	Value
Port Number	1
VLAN Identifier	20
IP Address	10.1.20.2
Netmask	255.255.255.0
Gateway	10.1.20.1
DHCP	10.1.100.100

Step 7 Save the configuration.

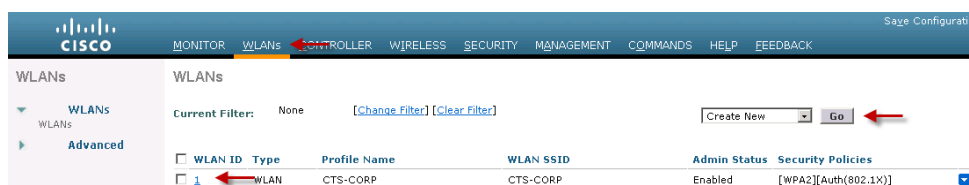


The screenshot shows the Cisco WLC configuration page. The left sidebar has a menu with 'Controller' selected. Under 'Controller', 'Interfaces' is highlighted with a red arrow. The main area shows a table of interfaces. The 'employee' and 'guest' interfaces are highlighted with red arrows. The 'employee' interface is a dynamic interface with IP address 10.1.10.2 and VLAN 10. The 'guest' interface is a dynamic interface with IP address 10.1.20.2 and VLAN 20. Other interfaces shown are 'management' (static, IP 10.1.60.2, VLAN untagged), 'service-port' (static, IP 0.0.0.0, VLAN N/A), and 'virtual' (static, IP 1.1.1.1, VLAN N/A).

Interface Name	VLAN Identifier	IP Address	Interface Type	Dynamic AP Management
employee	10	10.1.10.2	Dynamic	Disabled
guest	20	10.1.20.2	Dynamic	Disabled
management	untagged	10.1.60.2	Static	Enabled
service-port	N/A	0.0.0.0	Static	Not Supported
virtual	N/A	1.1.1.1	Static	Not Supported

Procedure 6 Add an 802.1X WLAN for Employees

Step 1 From the WLC, navigate to **WLANs** → **WLAN ID** to modify the SSID defined at bootstrap. If you want to define a new SSID, click **WLANs** → **Create New** → **Go**.



The screenshot shows the Cisco WLC 'WLANs' configuration page. The left sidebar has 'WLANs' selected. The main area shows a table of WLANs. The 'WLAN ID' column has a value of '1' highlighted with a red arrow. The 'Profile Name' is 'CTS-CORP', the 'WLAN SSID' is 'CTS-CORP', and the 'Admin Status' is 'Enabled'. The 'Security Policies' column shows '[WPA2][Auth(802.1X)]'. A red arrow points to the 'Go' button in the top right corner.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	CTS-CORP	CTS-CORP	Enabled	[WPA2][Auth(802.1X)]

Step 2 Set the values for the **General** tab of the WLAN settings.

WLANs > Edit 'CTS-CORP'

The screenshot shows the 'General' tab of the WLAN configuration interface. The tabs at the top are 'General', 'Security', 'QoS', and 'Advanced'. The 'General' tab is selected. The configuration fields are as follows:

Profile Name	CTS-CORP
Type	WLAN
SSID	CTS-CORP
Status	<input checked="" type="checkbox"/> Enabled
Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
Radio Policy	All
Interface/Interface Group(G)	employee
Multicast Vlan Feature	<input type="checkbox"/> Enabled
Broadcast SSID	<input checked="" type="checkbox"/> Enabled

A red callout bubble points to the 'Interface/Interface Group(G)' dropdown menu with the text: "Map the SSID to the Employee VLAN".

Step 3 Set the values listed for the **Security** → **Layer 2** tab.

WLANs > Edit 'CTS-CORP'

The screenshot shows the 'Security' tab of the WLAN configuration interface, specifically the 'Layer 2' sub-tab. The tabs at the top are 'General', 'Security', 'QoS', and 'Advanced'. The 'Security' tab is selected, and the 'Layer 2' sub-tab is also selected. The configuration fields are as follows:

Layer 2 Security	WPA+WPA2
MAC Filtering	<input type="checkbox"/> 10 MAC Filtering
WPA+WPA2 Parameters	
WPA Policy	<input type="checkbox"/>
WPA2 Policy	<input checked="" type="checkbox"/>
WPA2 Encryption	<input checked="" type="checkbox"/> AES <input type="checkbox"/> TKIP
Auth Key Mgmt	802.1X

Step 4 Set the values listed for the **Security** → **AAA servers** tab.

WLANs > Edit 'CTS-CORP'

Step 5 Set the values for the **Advanced** tab.

WLANs > Edit 'CTS-CORP'

Note: The RADIUS NAC setting is required for CoA enforcement. Although we define it at this stage, it will not have any effect until Cisco ISE is configured to send the redirect VSA to the WLC to invoke the pre-posture assessment ACL.

Step 6 Click **Apply** to save the WLAN settings.

Procedure 7 Add an open WLAN for Guests

Step 1 From the WLC GUI, navigate to **WLANs** → **Create New** → **Go**.

Step 2 Enter the values below and click **Apply**.

Attribute	Value
Profile Name	CTS-GUEST
SSID	CTS-GUEST

Step 3 Set the values in the **General** tab of the WLAN settings.

WLANs > Edit 'CTS-GUEST'

The screenshot shows the 'General' tab of the WLAN settings for 'CTS-GUEST'. The 'Security' tab is highlighted with a red arrow. The 'Interface/Interface Group(G)' is set to 'guest', which is highlighted with a red callout bubble saying 'Map the SSID to the Guest VLAN'. Other settings include Profile Name: CTS-GUEST, Type: WLAN, SSID: CTS_GUEST, Status: Enabled, Security Policies: [WPA2][Auth(802.1X)], Radio Policy: All, Multicast Vlan Feature: Disabled, and Broadcast SSID: Enabled.

Step 4 Set the values in **Layer 2** tab under **Security**.

WLANs > Edit 'CTS-GUEST'

The screenshot shows the 'Layer 2' tab under the 'Security' section. The 'Security' tab is highlighted with a red arrow. The 'Layer 2 Security' is set to 'None'. The 'MAC Filtering' checkbox is unchecked.

Step 5 Set the values for **Layer 3** tab under **Security**.

Note: The URL must point to a Policy Service Node. Our example uses a single-node deployment, but in a distributed deployment of Cisco ISE, the Policy Service Nodes will host the portal.

WLANs > Edit 'CTS-GUEST'

The screenshot shows the 'Layer 3' tab under the 'Security' section. The 'Security' tab is highlighted with a red arrow. The 'Layer 3 Security' is set to 'None'. The 'Web Policy' checkbox is checked, and the 'Authentication' radio button is selected. The 'Preauthentication ACL' is set to 'ACL-POSTURE-REDIRECT'. The 'Over-ride Global Config' checkbox is checked. The 'Web Auth type' is set to 'External(Re-direct to external server)', and the 'URL' is set to 'https://10.1.100.3:8443/guestportal/Login.action'. A red callout bubble points to the URL field with the text 'Point to ISE Guest Portal'.

Step 6 Set the values for the **Advanced** tab.

WLANs > Edit 'CTS-GUEST'

The screenshot shows the 'Advanced' tab of the Cisco ISE configuration interface for a WLAN named 'CTS-GUEST'. The 'General' tab is also visible. The 'Advanced' tab contains the following settings:

Setting	Value
Allow AAA Override	<input checked="" type="checkbox"/> Enabled
Coverage Hole Detection	<input checked="" type="checkbox"/> Enabled
Enable Session Timeout	<input checked="" type="checkbox"/> 1800 Session Timeout (secs)
Aironet IE	<input checked="" type="checkbox"/> Enabled
Diagnostic Channel	<input type="checkbox"/> Enabled
IPv6 Enable	<input type="checkbox"/>
Override Interface ACL	None
P2P Blocking Action	Disabled

Note: It is important to enable AAA Override to allow attributes from the AAA server to be applied.

Step 7 Save the WLC Configuration

Procedure 8 Configure Cisco ISE to accept Wireless authentication requests.

Step 1 From Cisco ISE, navigate to Policy → Authentication.

Step 2 Expand the If conditions for the Dot1X rule and choose to Add Condition from Library.

The screenshot shows the Cisco ISE Policy configuration page. The 'Policy Type' is set to 'Rule-Based'. The 'Rule Based' section shows a list of conditions: 'MAB', 'Dot1X', and 'Default Rule (If no match)'. The 'Dot1X' condition is expanded, showing a list of conditions: 'Wired_802.1X', 'Wireless_802.1X', 'Switch_Local_Web_Authentication', and 'WLC_Web_Authentication'. The 'Add Condition from Library' dialog is open, showing the 'Condition Name' as 'Wired_802.1X' and the 'Expression' as 'AND'. The 'Add Condition from Library' button is highlighted.

Step 3 From the Select Condition drop-down menu go to Compound Condition → Wireless_802.1X.

The screenshot shows the Cisco ISE Policy configuration page. The 'Policy Type' is set to 'Rule-Based'. The 'Rule Based' section shows a list of conditions: 'MAB', 'Dot1X', and 'Default Rule (If no match)'. The 'Dot1X' condition is expanded, showing a list of conditions: 'Wired_802.1X', 'Wireless_802.1X', 'Switch_Local_Web_Authentication', and 'WLC_Web_Authentication'. The 'Wireless_802.1X' condition is selected. The 'Select Condition' button is highlighted.

Step 4 Save the settings.

Cisco ISE is now ready to accept RADIUS requests originating from wireless networks. When it receives a RADIUS request from a wireless source, it will check to see if the authentication protocol is permitted or not. Typically, the **default networks options** allows all authentications protocols supported by Cisco ISE. The next step for Cisco ISE is to query the specified identity store to validate the credentials received.

Base-Identity Use Cases

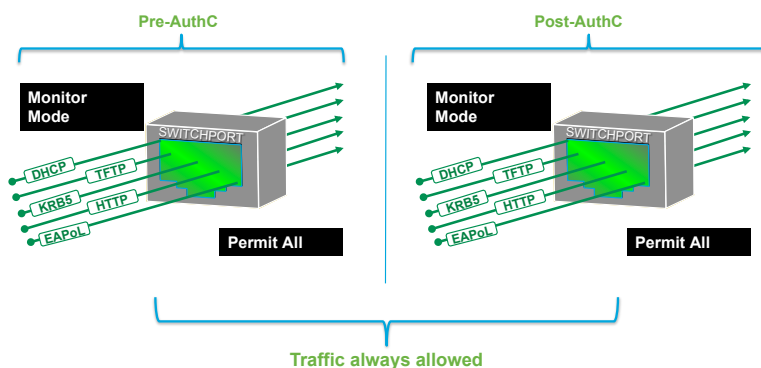
Introduction

Throughout the remainder of the document, we will be discussing the recommended way to deploy Cisco TrustSec with little-to-no effect on the end users. At this stage of deployment we are focusing on the use-cases of Authenticating and Authorizing at the Access Layer (wired and wireless) with Access-Layer enforcement (VLAN assignment and downloadable ACLs). Other use cases will be examined in the later sections of the document.

This document will guide you through a phased approach.

Phase 1: Monitor Mode

Figure 8: Monitor Mode Port Behavior



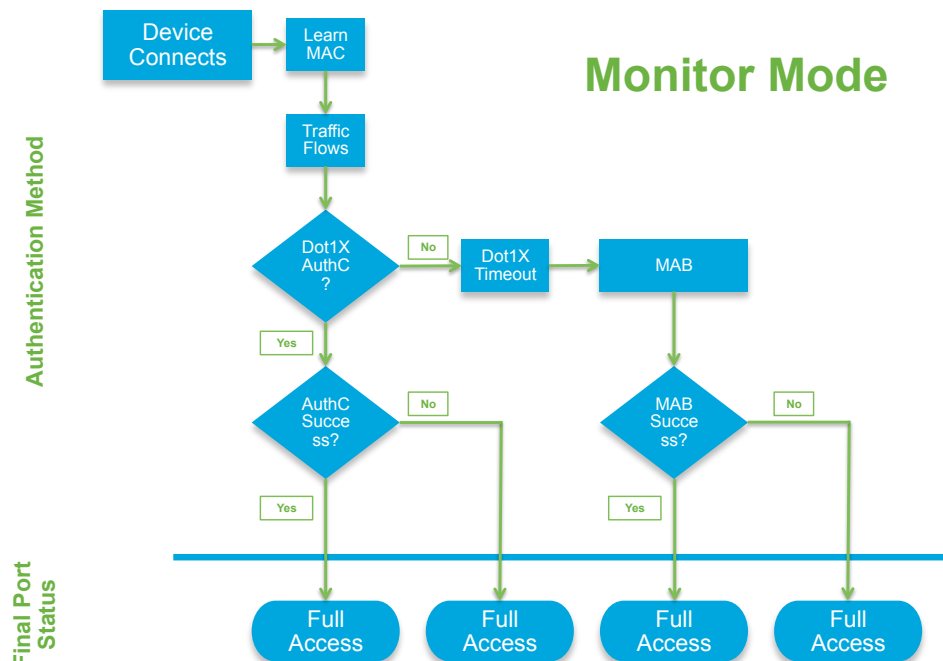
Monitor Mode will allow your organization to enable authentication across your wired and wireless infrastructure, without affecting your wired users or devices. It can be thought of as an “audit mode”. Administrators will use this mode to ensure all devices are authenticating correctly, either with 802.1X or MAB. If a device is misconfigured or is missing an 802.1X supplicant, access will not be denied. When deploying Monitor Mode, most organizations are surprised at what devices they find connected to the network that they were unaware of previously.

Wireless environments with 802.1X are binary (just like 802.1X was designed to be), so when users are unable to authenticate, they simply do not get access to the wireless network. Most users can accept this behavior and are willing to find a location with a physical network connection (wire) instead. Although end users are mostly willing to accept an inability to join a wireless environment, they are much less understanding when faced with a lack of access to a wired network port.

Monitor mode is a process, not just a command on a switch. The process will use a combination of RADIUS Accounting, Open Authentication, and Multi-Auth Features on your Cisco infrastructure, as well as Device Profiling to grant visibility to the Administrator of who and what is connecting to the network, and from where. If a device should be Authenticating, but cannot because of a misconfiguration of sorts, the Administrator will know and can correct it without denying network access to the user.

Note: It is not possible to implement Monitor Mode with wireless networks. Therefore, we will introduce wireless in the Authenticated Mode phase.

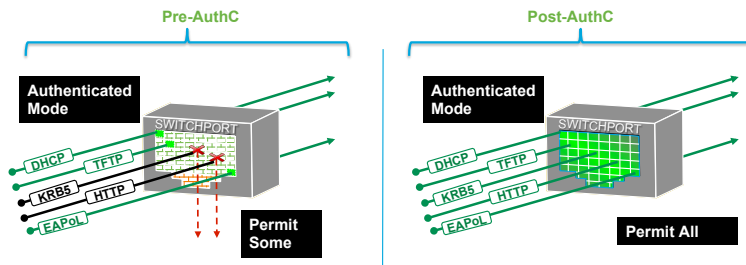
Figure 9: Monitor Mode Flow Chart



Phase 2: Authenticated Mode

When looking at previous Cisco documentation, you will notice there used to be a mode known as “Low-Impact” mode. We have divided Low-Impact mode into two distinctly different modes: “Authenticated Mode” and “Enforcement Mode”. The biggest difference between the two new modes is the level of enforcement used. Authenticated mode will provide full network access to any authenticated user or device, whereas Enforcement Mode shall provide Role-Specific Access Control for those users and devices (Figure 10).

Figure 10: Authenticated Mode Port Behavior



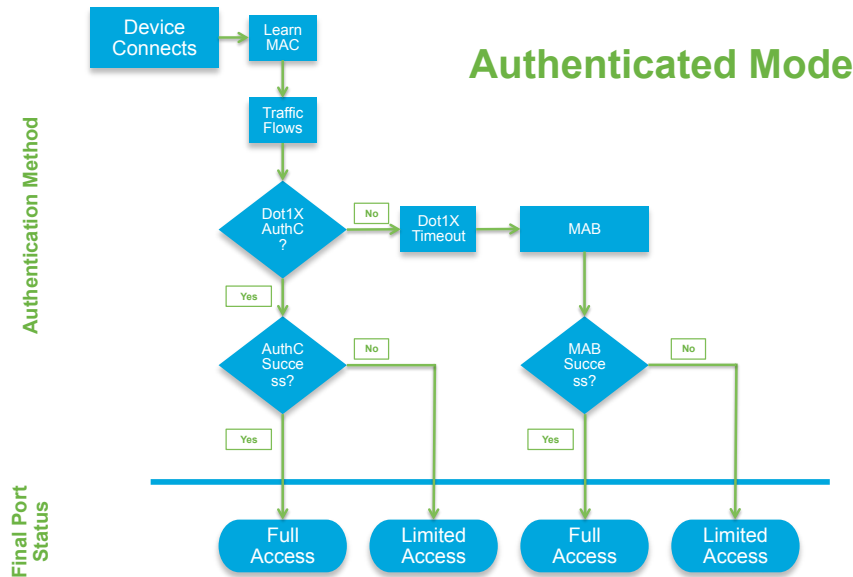
In the Authenticated Phase we will add security on top of the framework that we built in Monitor Mode by applying an Access Control List (ACL) to the switchport that allows very limited network access prior to authentication. After users or devices have successfully authenticated, they will be granted full network access.

An example of how this feature may be used is giving any host attaching to the network the ability to use DHCP and DNS and perhaps get to the Internet, all while blocking access to internal resources. When a device connected to that same switchport passes authentication, a downloadable ACL (DACL) is applied that will permit all traffic.

This phase continues to use “open authentication” on the switchports, while providing very strong levels of security for non-authenticated devices. However, because a limited set of traffic will always flow regardless of the authentication state of the device, this mode becomes ideal and pragmatic for today’s enterprises by allowing the regular IT operational activities to occur such as the re-imaging of workstations with Pre Executable Environment (PXE) type solutions.

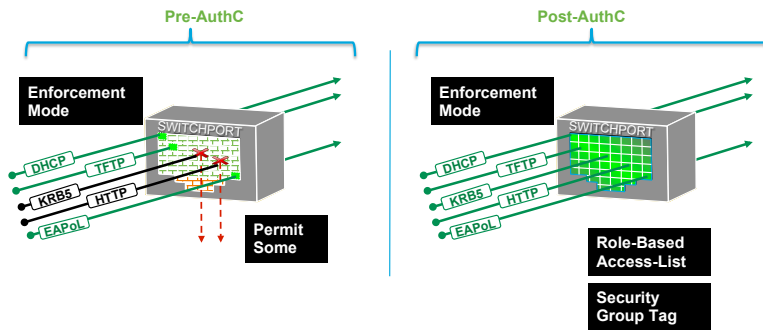
When considering Wireless Access, we will follow a very similar flow. A user or device authenticating to wireless with valid credentials will be authorized for full network access. Access should be tightened down with additional security and specific access based on the role of the user or device (Figure 11).

Figure 11: Authenticated Mode Flow Chart



Phase 3: Enforcement Mode

Figure 12: Enforcement Mode Port Behavior

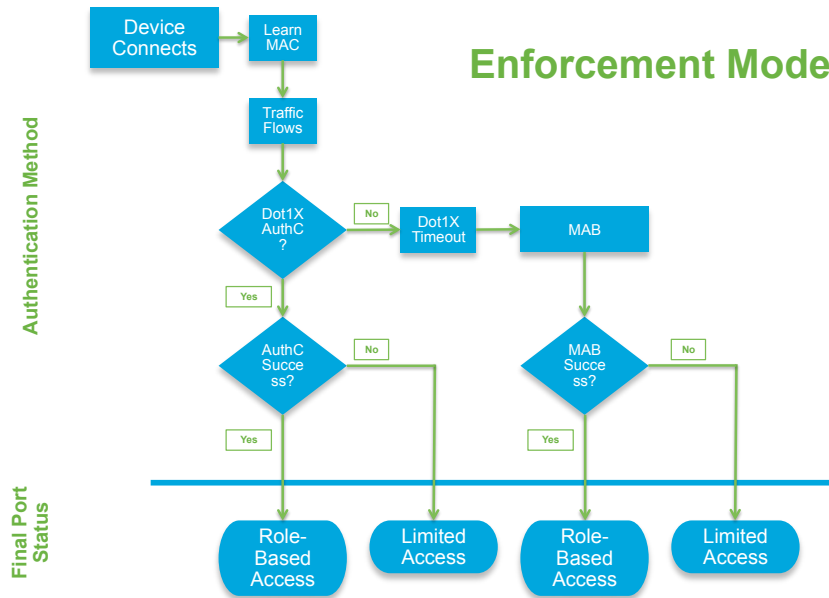


Building on the previous two modes, Enforcement mode will add more granular security and differentiated access to the Network. In the previous mode, any successful authentication will be granted full access. This process is a great way to provide security to the network, but it doesn't provide differentiated access based on the user's role – normally one of the goals of any identity project.

Within the Enforcement Mode phase, we replace the DACL or Wireless ACL (wACL) that permits all traffic with a more specific DACL / wACL that is assigned based on the user's group membership or other attributes of the user's context (Figure 13).

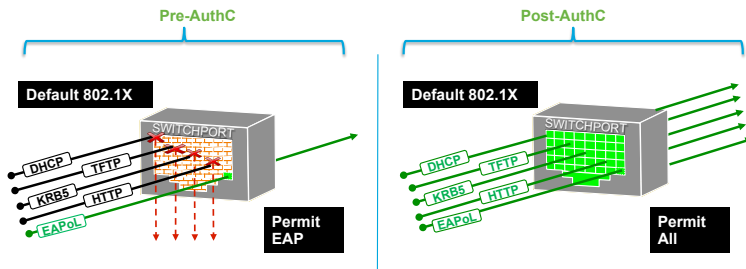
Note: the previous terms of "Low Impact Mode" and "High-Security Modes" are no longer used. Low Impact mode was broken up into two parts: Authenticated Mode and Enforcement Mode. High-Security Mode was another name for the default behavior of 802.1X – which is very difficult to deploy and operationalize, and therefore not recommended for the majority of customer environments. That mode is now being referred to as "Closed Mode".

Figure 13: Enforcement Mode Flow Chart



Closed Mode (formerly High-Security Mode)

Figure 14 - Default 802.1X Port Behavior (Closed Mode)



As mentioned previously in this section: the default 802.1X mode was previously called "High-Security Mode", and will now be referred to as "Closed Mode". This type of deployment is recommended only for environments that are experienced with 802.1X deployments and have considered all the nuances that go along with it. Think of this mode as a "deploy with caution" mode, and it is beyond the scope of this version of the Cisco TrustSec Design and Implementation Guide.

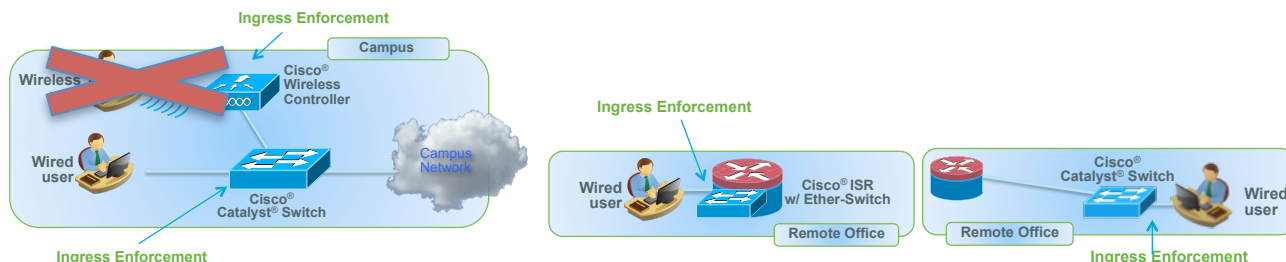
By default, wireless follows this same closed mode logic, but instead of permitting all traffic after authentication, it is recommended to add the Authenticated and Enforcement mode logic of using a wACL or DVLAN with the wireless connection. However, there is no capability equivalent of "authentication open" on a wireless device.

Phase 1: Monitor Mode

This section will cover wired access, both in a campus and in a remote office. The solution test includes the use of the Cisco EtherSwitch® module in the Integrated Services Router (ISR) for remote office locations.

Note: As discussed previously, there is no concept of Monitor Mode with wireless access. Therefore, wireless access will not be introduced until the Authenticated Mode phase of deployment.

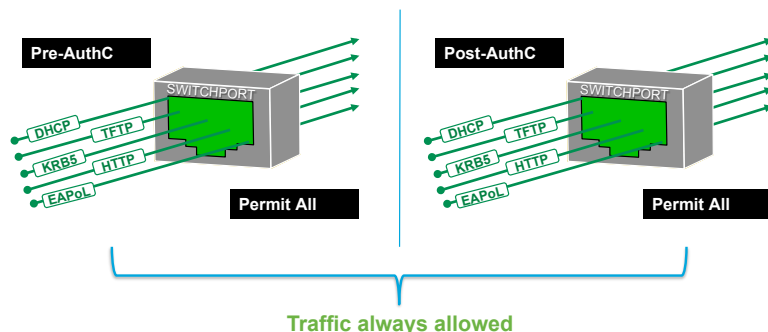
Figure 15: Wired Scenarios in the Campus and Remote Office



As discussed in the introduction of this section, monitor mode is a deployment strategy that will provide full access regardless of authentication state. This state is where authentication may be configured on all applicable devices, and Cisco ISE will provide visibility into which devices are authenticating successfully as well as which ones are not.

It is usually not required, but because of some corner cases it is considered a best practice to apply the ACL-ALLOW Access List that we created in the “[Configure Local Access Control Lists](#)” section to all switchports in this phase.

Figure 16: Monitor Mode



Configure Monitor Mode

Before examining the Cisco ISE default configuration or configuring anything new in Cisco ISE, it is critical that you have a solid understanding of the functions of network access and the flow.

RADIUS-controlled network access follows a traditional Authentication, Authorization, and Accounting (AAA) model.

An authentication is, simply put, verifying valid credentials. That's all. An authentication could be verifying a client's certificate validity, or checking for a valid username/password combination. However, Authentication does not provide any access by itself.

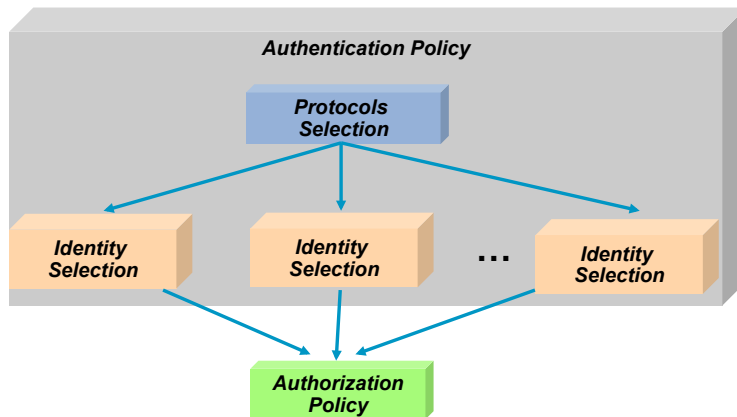
Authorization is where one defines the access to provide an authenticated user or device. It is where the bulk of the work occurs for controlling network access.

The Cisco ISE Graphical User-Interface logic separates out the Authentication and Authorization Policies. The Authentication Policy will dictate what Identity Store to check based on the incoming authentication request. For example, an authentication request coming from a VPN may be configured to check a One-Time-Password (OTP) server to validate credentials.

Meanwhile, using the same Cisco ISE installation, an authentication request from a Wireless LAN Controller will result in validating the credentials with Active Directory. Cisco ISE provides a very powerful and flexible Authentication policy.

The Authentication Policy will compare the incoming protocol to the configured rules, select the assigned Identity Store, and then the Authorization Policy takes over from there (Figure 17).

Figure 17 Authentication Policy



Configure Authentication

Procedure 1 Examine the Default Cisco ISE Authentication Policy.

Step 1 Navigate to Policy → Authentication.

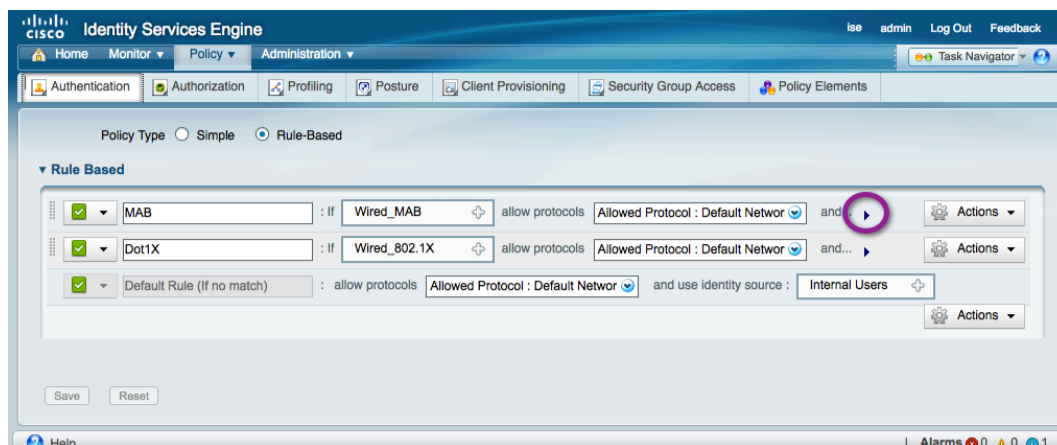
There are two preconfigured rules in the Authentication Policy, and the “default rule”. The Policy Rule table behaves like an access-list – where it is processed from the top down, and the first match is the rule that is used.

The way an authentication request is matched to a rule line is based on the conditions. To explain this concept further, we will examine the first preconfigured rule, named “MAB”. This rule is for MAC Authentication Bypass from switches.

Cisco ISE Policy constructs are built in a very logical “IF – THEN” format. Notice the “If” just before the “picker” that says “Wired_MAB”. This line is stating: “If RADIUS request is Wired_MAB, then allow the Default Network Protocols to be used”.

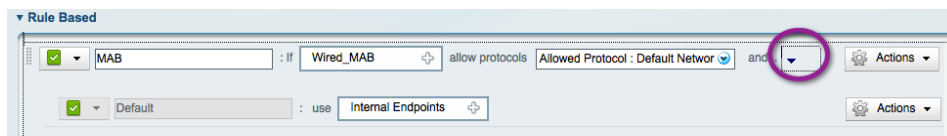
```

IF Wired_MAB
THEN Allow the default protocols
ELSE Move to next Line in Authentication Policy Table
    
```



Step 2 Now, notice the “and” after the allowed protocols section. Next to the word “and” is a black drop-down triangle. Click the **down triangle**.

Each rule in the Authentication Policy table has a second part to it. It is the line where the credential store is chosen. By default, this preconfigured rule for MAC Authentication Bypass is configured to use the “Internal Endpoints” data store. The Internal Endpoints data store is the database of known devices internal to Cisco ISE. This database may be populated manually or dynamically.



Note: An example of manual population: The admin exports a list of known Cisco IP Phone MAC Addresses from the Cisco Unified Communications Manager interface, and imports that list into Cisco ISE.

An example of dynamic population: Cisco ISE profiling discovered this device through one or more of the Profiling Probes, and created the device entry in the Internal Endpoints data store.

So, the IF-THEN statement looks like this:

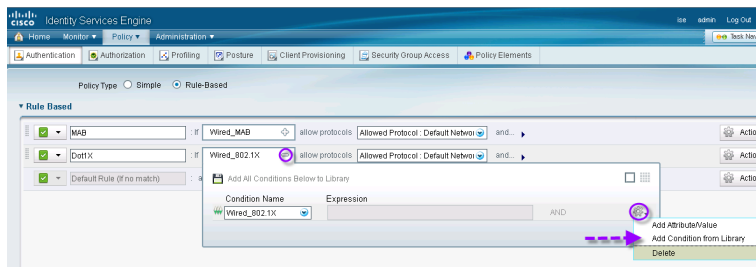
```
IF Wired_MAB
THEN Allow the default protocols
AND Check Credentials with the Internal Endpoints Data Store
ELSE Move to next Line in Authentication Policy Table
```

Note: "Wired_MAB" is a prebuilt condition to match RADIUS attributes: service-type = call-check, and nas-port-type = ethernet.

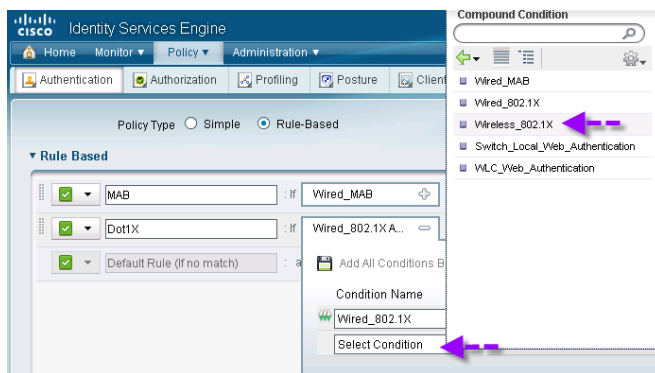
Procedure 2 Enable Wireless Authentication.

Step 1 Navigate to Policy → Authentication.

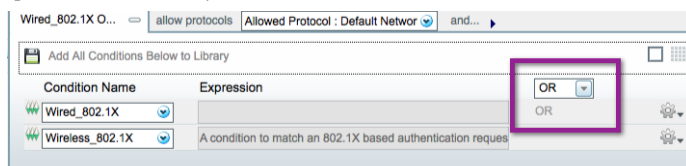
Step 2 Expand the If conditions for the Dot1X rule and choose Add Condition from Library.



Step 3 From the Select Condition drop-down menu, go to Compound Condition → Wireless_802.1X.



Step 4 Ensure the operator is "OR" not "AND".



Step 5 Save the Settings

Procedure 3 Change the identity stores.

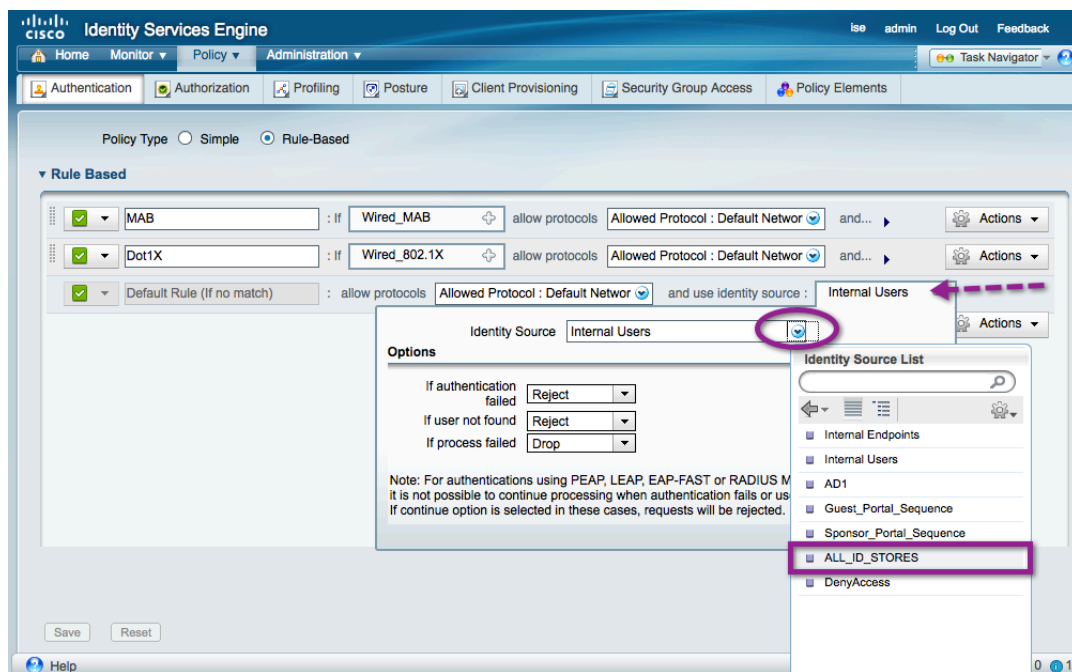
With the preconfigured rules, MAB will use the internal endpoints store to look for the MAC addresses of known devices. If the incoming authentication request is an 802.1X authentication, Cisco ISE will use the “internal users” data store to check for username and password validity.

If the authentication is of another type (say WebAuth, for example), it will not match either of the preconfigured lines and it will end up with the Default Rule. The default rule is preconfigured to check the internal users’ data store.

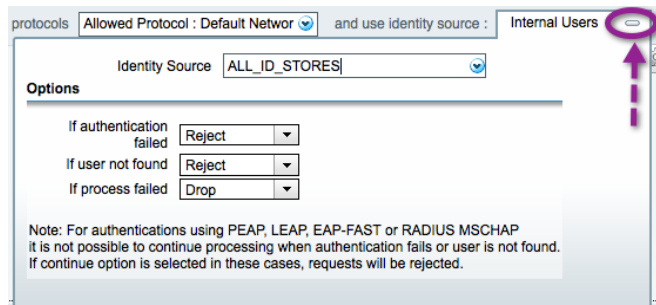
Most organizations will not want to use the default, local data stores for user accounts. The vast majority of organizations use Active Directory for their main source of user identity. Therefore, we will change both the Dot1X and the default Rules to include Active Directory in their user credential lookups.

Step 1 In the Default Rule, Click the “+” sign next to “Internal Users” to open the Identity Source “picker”.

Click the Identity Source drop-down list, and select the “All_ID_STORES” Identity sequence that was built in the “Create an Identity Sequence” procedure.



Step 2 Click the “-” sign to close the Identity Source picker.



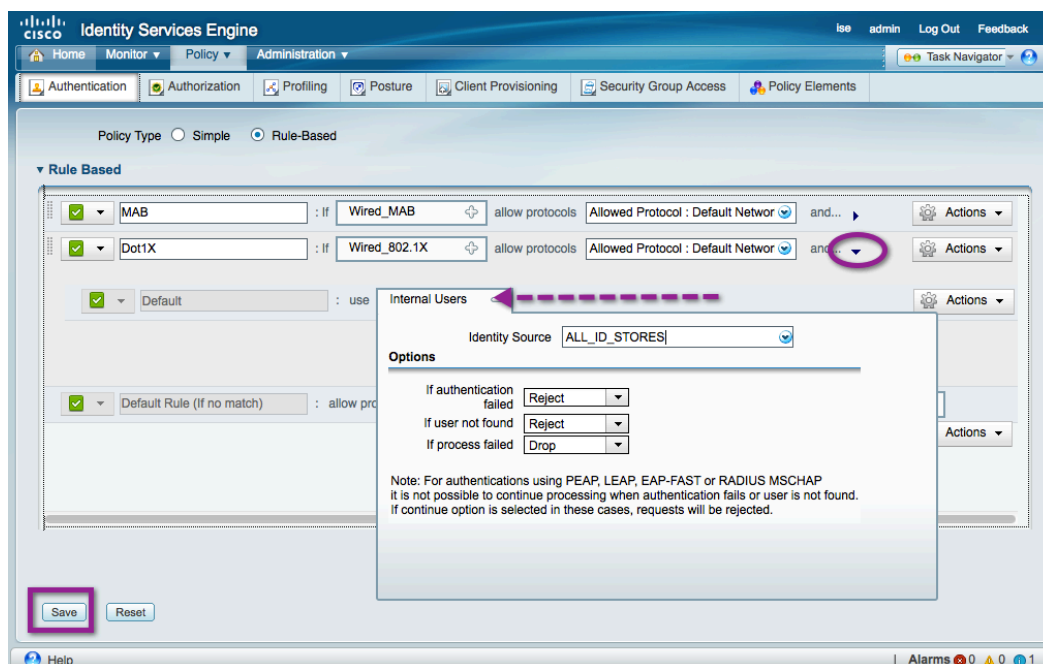
Step 3 Make note of the options below the Identity source.

The actions for each option are **Reject**, **Drop**, or **Continue**. These three options and their respective choices are available with every Authentication Policy rule, as well as the default rule.

Option	Description
Authentication Failed	Received explicit response that authentication has failed such as bad credentials, disabled user, and so on. The default course of action is reject.
User not found	No such user was found in any of the identity databases. The default course of action is reject.
Process failed	Unable to access the identity database or databases. The default course of action is drop.

Action	Description
Reject	Sends a RADIUS ACCESS-REJECT response to the NAD.
Drop	Drops the ACCESS-REQUEST, without sending a response.
Continue	Proceed to the authorization policy.

Step 4 Expand the Dot1X line, and repeat Steps 1 and 2 to change the identity source to be All_ID_Stores.



Step 5 Click **Save**.

Note: There is a lot of customization that may occur per authentication rule. We are using the default network access as our allowed protocols. This use of the defaults allows the vast majority of authentication types, but it does not restrict access to a certain type of EAP-Method.

To configure a customized set of authentication protocols (such as EAP-TLS only), go to **Policy → Policy Elements → Results → Authentication → Allowed Protocols**.

Begin Authorization Configuration

Procedure 1 Examine the Default Cisco ISE Authorization Policy.

As discussed previously, Authentication is simply the validation of user credentials. All the enforcement and access control occurs within the Authorization phase of network access.

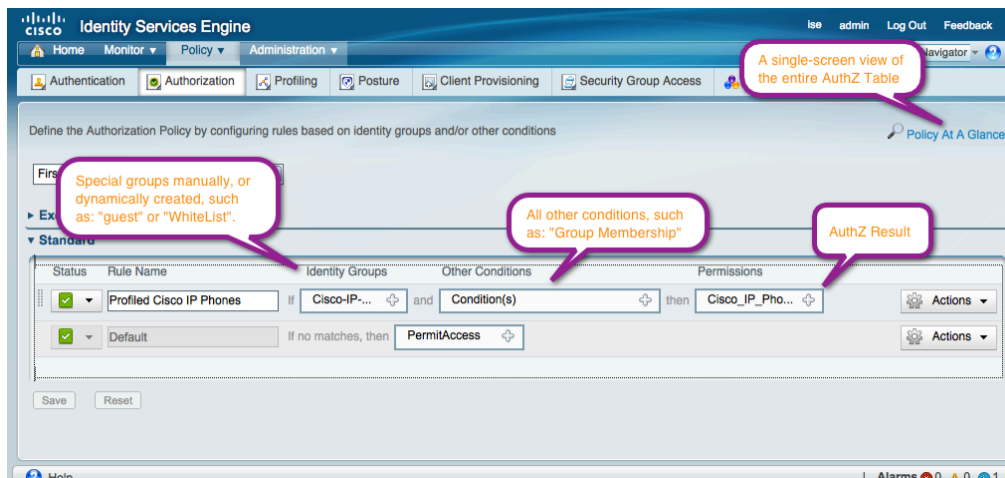
Step 1 Navigate to Policy → Authorization.

There is one preconfigured rule in the Authorization Policy, plus the “default rule”. Just like the Authentication Policy, the Authorization Rule table behaves like an access list by default– where it is processed from the top down, and the first match is the rule that is used.

Note: The Authorization Table can match multiple rules, allowing for **very** complex authorization results. This topic is considered out of scope for this document.

Best Practice: Use the default of “First Matched Rule Applies”.

Just like the authentication policy, the manner in which an authorization request is matched to a rule line is based on the conditions. To explain this concept further, we will examine the preconfigured rule, named “Profiled Cisco IP Phones”. As the name implies, this rule is used to authorize Cisco IP Phones that were identified in the Profiling process.

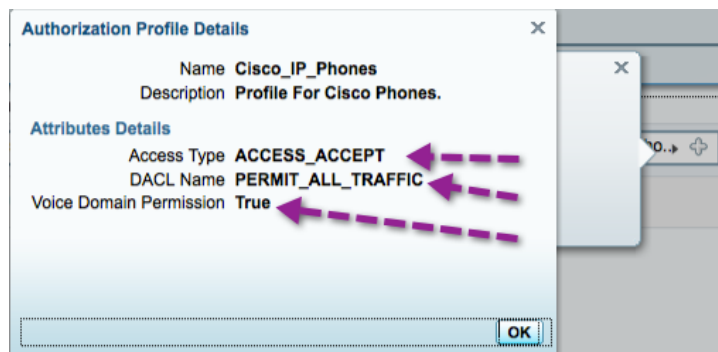


Cisco ISE Policy constructs are built in a very logical “IF – THEN” format. Examining this rule, we see that:

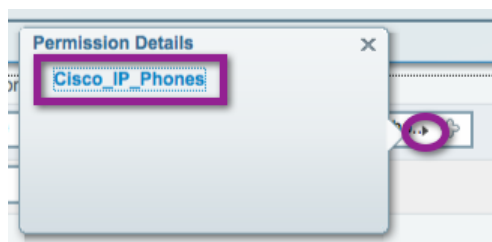
```
IF Device is memberOf ISE ID Group = Cisco-IP-Phone
AND (no other conditions in this line)
THEN Assign the Cisco_IP_Phone Authorization Profile
ELSE Move to next Line in Authentication Policy Table
```

Step 2 View the details of the Cisco_IP_Phone Authorization Profile.

To see the details of the Cisco_IP_Phone Authorization Profile, hover the mouse cursor over the Permissions Picker and the “Permission Details” pop-up appears. Click the link for **Cisco_IP_Phones**.

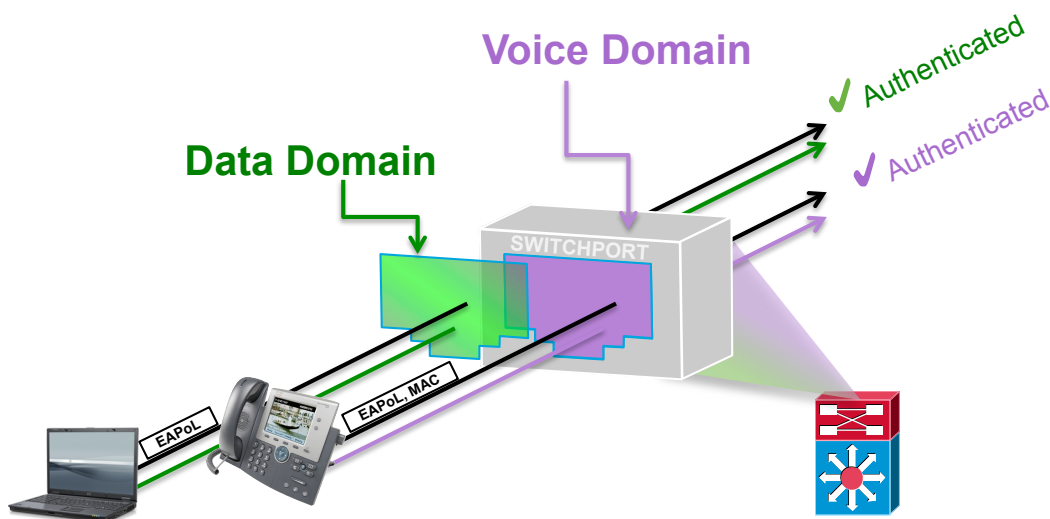


Examining the Authorization Profile Details pictured above right: Cisco_IP_Phones sends a RADIUS Access-Accept message, sends a downloadable ACL (DACL) named "PERMIT_ALL_TRAFFIC", and allows the device to join the Voice Domain (voice VLAN).



Voice Domain: an IP Phone requires a special RADIUS attribute to be sent in the Authorization result, which grants the device permission to join the Voice VLAN. See the "IP Phones" section for more information.

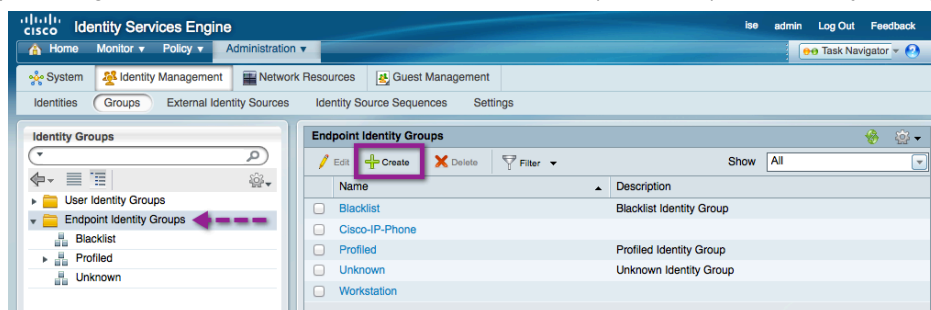
Figure 18: Multi-Domain Authentication (MDA)



Procedure 2 Create a Whitelist for Endpoints.

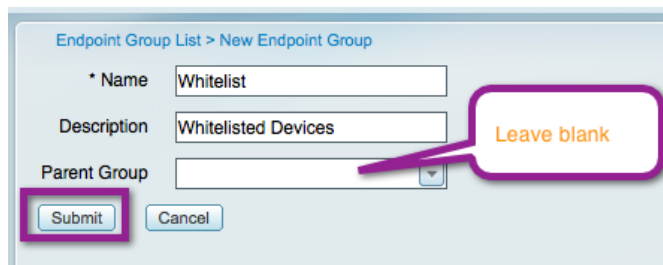
We will manually create a Whitelist identity group. This group is a group that an administrator may add a device to, in order to permit it full access to the network. This permission is recommended only for special cases.

Step 1 Navigate to Administration → Identities → Groups → Endpoint Identity Groups.



Step 3 Click Create.

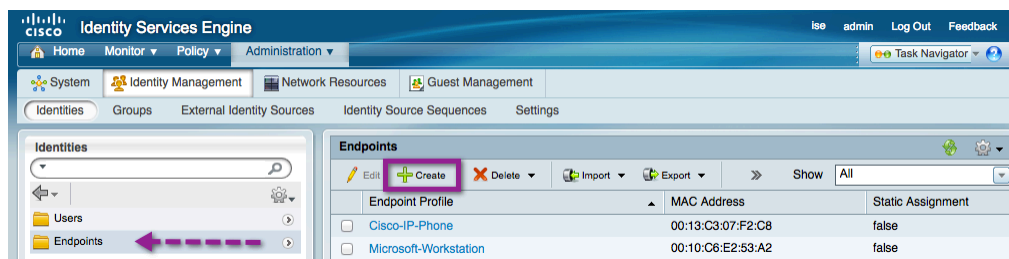
Step 4 Name the new group **"Whitelist"**. Leave the Parent Group drop-down field blank.



Step 5 Click Submit.

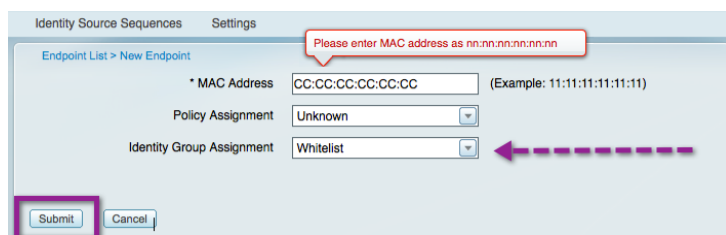
When troubleshooting or for special circumstances, a device may be added to this list, and it will be permitted access to the network.

Step 6 To add a device to the Whitelist group: **Administration** → **Identities** → **Endpoints**. Click **Create**.



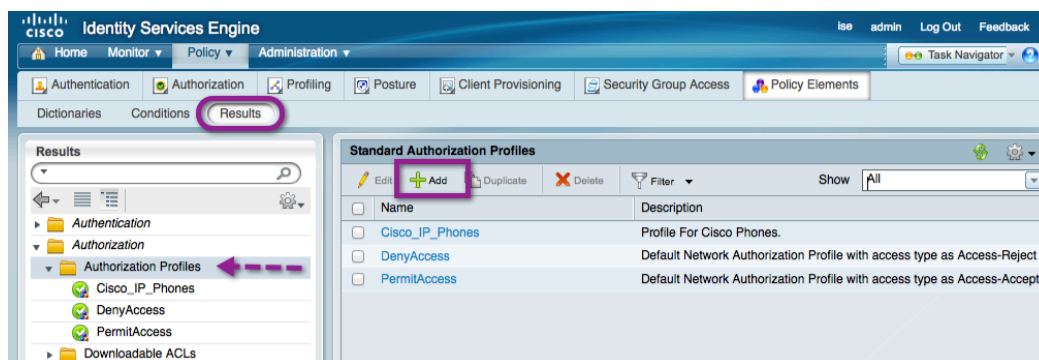
Step 7 Add the device MAC Address in format nn:nn:nn:nn:nn:nn, and choose **"Whitelist"** from the Identity Group Assignment drop-down menu.

Note: If the device type is known (for example, Android), it may be selected from the Policy Assignment drop-down menu.



Procedure 3 Create an Authorization Profile for Whitelisted devices.

Step 1 Navigate to **Policy** → **Policy Elements** → **Results** → **Authorization** → **Authorization Profiles**.



Step 2 Click **Add**.

Step 3 Configure the new Authorization profile as described:

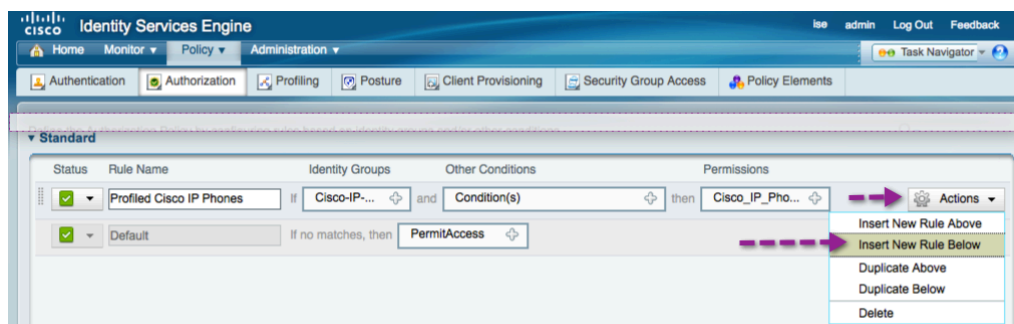
Name = Whitelist
Description = Authorization Profile for Whitelist
Access-Type = ACCESS_ACCEPT
-- **Common Tasks**
☒ **DACL Name** = PERMIT_ALL_TRAFFIC

Step 4 Click Submit.

Procedure 4 Create an Authorization Rule for Whitelisted devices.

Step 1 Navigate to Policy → Authorization.

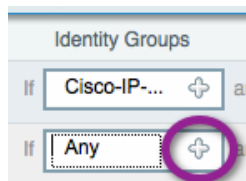
Step 2 Click **Actions** at the end of the IP-Phone Authorization rule.



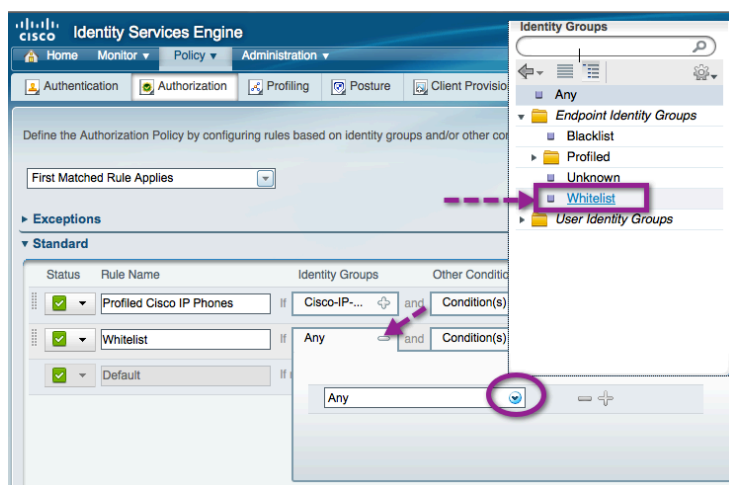
Step 3 Select Insert New Rule Below.

Step 4 Name the new rule **Whitelist**.

Step 5 Click the “+” sign next to “Any” in the Identity Group column.



Step 6 Select the new Whitelist Identity Group from the Picker.



Step 7 Do not change the **Other Conditions** column.

Step 8 Click the “+” sign under the permission column.

Step 9 Select the Authorization profile named **Whitelist**.

Status	Rule Name	Identity Groups	Other Conditions	Permissions
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	If Cisco-IP-...	and Condition(s)	then Cisco_IP_Pho...
<input checked="" type="checkbox"/>	Whitelist	If Whitelist	and Condition(s)	then Whitelist
<input checked="" type="checkbox"/>	Default	If no matches, then	PermitAccess	

Step 10 Click **Save**.

Monitoring in Monitor Mode

At this point in the monitor mode configuration, all devices are still permitted to access the network, regardless of whether or not the device successfully authenticated. This way there is no effect on the end users. However, all during this phase the switchports are attempting to authenticate the devices that are connected. The port will cycle through attempts to authenticate with EAP (802.1X) and to bypass authentication with MAB.

During this phase, we will use the Monitoring and Reporting engine within Cisco ISE to see all failed authentications, and use this time to correct any misconfigurations in the network infrastructure, or even within the supplicant provisioning process for managed assets.

This document will cover one example of a misconfiguration, and the corrective actions taken to fix this misconfiguration.

Monitor Misconfigurations and Errors

Procedure 1 View the Live Authentications Log.

Step 1 Navigate to Monitor → Authentications.

Step 2 Click the Details button for one of the errors.

Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Prof
Sep 21, 11:25:25.709 PM	✗	Details						
Sep 21, 11:25:20.773 PM	✗							
Sep 21, 11:25:15.727 PM	✗							
Sep 21, 11:25:11.094 PM	✗							
Sep 21, 11:24:26.493 PM	✗							
Sep 21, 11:24:21.317 PM	✗							
Sep 21, 11:24:16.410 PM	✗							
Sep 21, 11:24:11.100 PM	✗							
Sep 21, 11:23:25.086 PM	✗							
Sep 21, 11:23:20.418 PM	✗							
Sep 21, 11:23:15.724 PM	✗							
Sep 21, 11:23:11.099 PM	✗							
Sep 21, 11:22:26.323 PM	✗							

Step 3 The **RADIUS Authentication Detail** report opens in a new tab, or pop-up window.

In most cases the errors will be highlighted in Red Text.

Authentication Summary	
Logged At:	September 21, 2011 11:17:25.652 PM
RADIUS Status:	RADIUS Request dropped : 11007 Could not locate Network Device or AAA Client
NAS Failure:	
Username:	
MAC/IP Address:	
Network Device:	: 192.168.254.1 :
Allowed Protocol:	
Identity Store:	
Authorization Profiles:	
SGA Security Group:	
Authentication Protocol :	

Look at the screen capture; Cisco ISE has dropped the requested RADIUS request because it is sourced from an unknown AAA Client (Network Access Device), meaning the device with IP Address 192.168.254.1 was not added correctly in the Network Devices section of Cisco ISE.

Step 4 Navigate to Administration → Network Devices.

That IP Address is the loopback address for the SJC18-SW-1. Looking at the details of that device, we see that it was added to Cisco ISE with the wrong IP Address.

Network Devices List > SJC18-sw-1

* Name: SJC18-sw-1

Description: Access-Layer Switch i

* IP Address: 192.168.252.1 / 32

Step 5 Correct the mistake.

Network Devices List > SJC18-sw-1

* Name: SJC18-sw-1

Description: Access-Layer Switch i

* IP Address: 192.168.254.1 / 32

Step 6 Save.

Procedure 2 Review Failed Authentications.

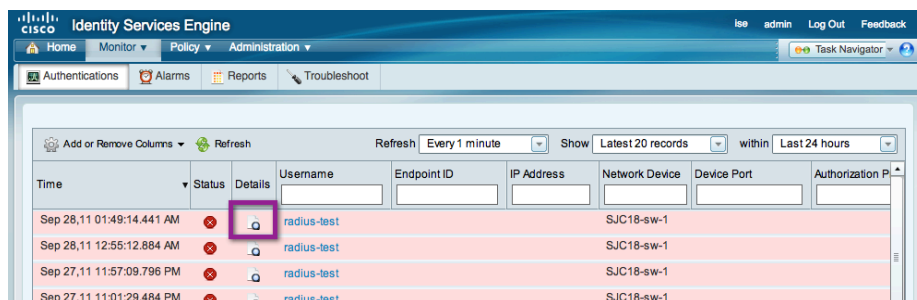
Now that the Network Device is properly registered with Cisco ISE, we see new errors. These errors are a failed authentication. The authentications that are failing are from the “Authentication Settings – Flexible Authentication and High Availability” procedure, where we configured the switch to proactively check for the Cisco ISE server to be “alive” or “dead” by sending periodic test authentications to Cisco ISE. We configured the switch to use an account named “radius-test”, which is not defined in Active Directory or in the Cisco ISE internal hosts.

The switch will receive a RADIUS Access-Reject message back, because the username does not exist in any of the configured identity stores. The switch is not looking for a successful authentication, only a response from the RADIUS server. So an Access-Accept or an Access-Reject will suffice.

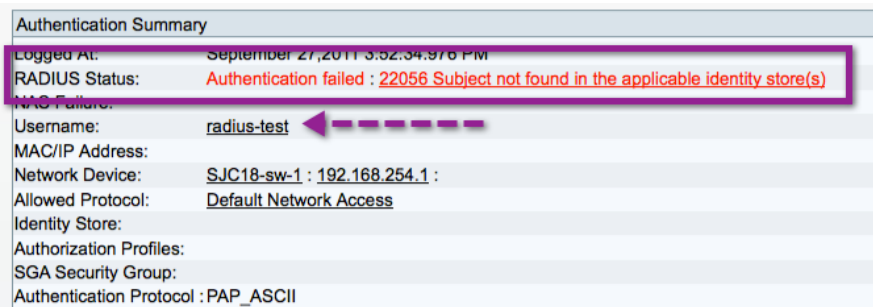
It is recommended that you create an Authorization Rule to allow these authentication requests otherwise they will skew the dashboard and reporting statistics by showing more failed authentications than are truly occurring. We will fix this inconvenience in this next procedure.

Note: ACS has the ability to filter these types of events from reaching the logs, thereby preventing these test accounts from skewing the trend reports and dashboards. Cisco ISE 1.0 does not have this ability today. It should appear in a future release of Cisco ISE.

Step 1 Navigate to Monitor → Authentication.

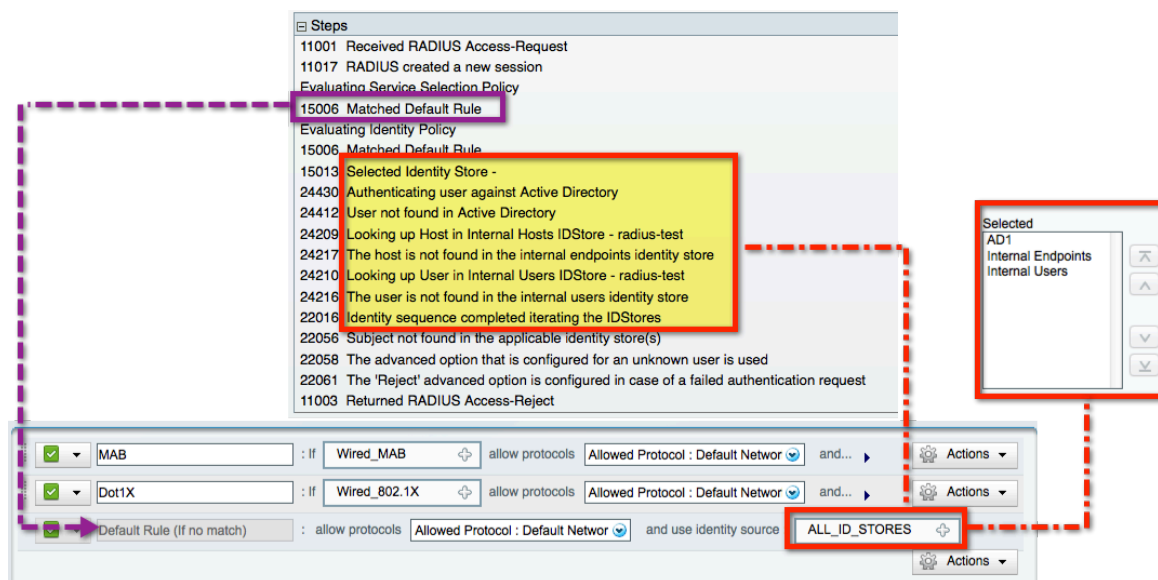


Step 2 Click the Details icon for one of the failed authentications of radius-test.



Step 3 Scroll down to the **Steps** Section of the report.

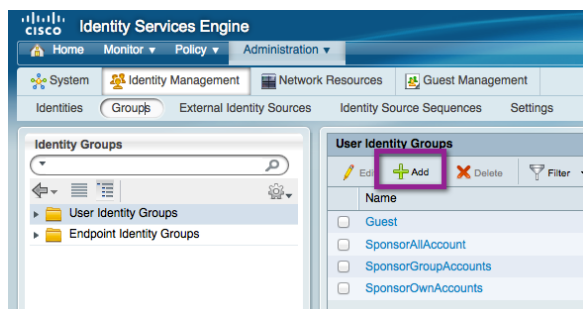
Here we can see that the Access-Request is received, and it matched the default Authentication Rule. That rule uses the All_ID_STORES identity sequence, which checks Active Directory, Internal Endpoints, and then Internal Users. We can see all these items in the Steps section of the report, but have expanded the Authentication Policy table and Identity Sequences details as follows for illustration purposes.



Procedure 3 Remediate the failed authentication (optional).

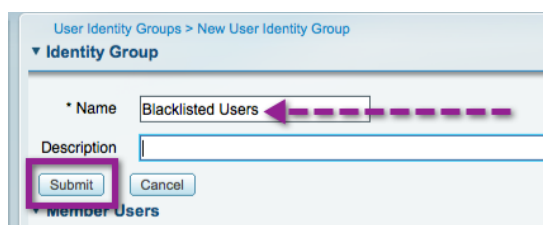
In order to clean up the dashboard and reporting, we will add that user to the Cisco ISE Internal Users identity store. However, we do not want to open any back-door vulnerabilities for a malicious user to gain network access using that account. So, we will add the radius-test user to a blacklist Identity Group that is denied network access through the Authorization policy.

Step 1 Navigate to Administration → Identity Management → Groups → User Identity Groups.

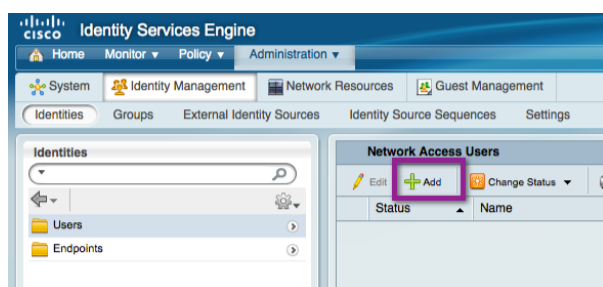


Step 2 Click **Add**.

Step 3 Name the group **Blacklisted Users**, and click **Submit**.



Step 4 Navigate to Administration → Identity Management → Identities → Users.



Step 5 Click **Add**.

Network Access Users > New Network Access User

Network Access User

* Name Status ☒ Enabled

Email

Password

* Password Must match what was configured in the switches (Cisco123)

* Re-Enter Password

User Information

First Name

Last Name

Account Options

Description

Password Change ☐ Change password on next login

User Groups

☒

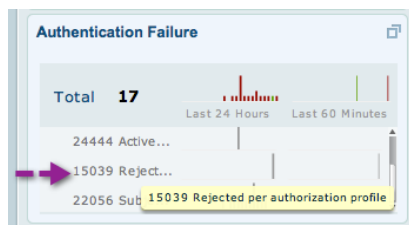
Step 6 Navigate to Policy → Authorization.

Step 7 Insert a rule above the IP Phone rule, named **Blacklisted**. Choose the **Blacklisted Users** Identity Group, and set the Permissions to **Standard → DenyAccess**.

Status	Rule Name	Identity Groups	Other Conditions	Permissions
<div><div></div><div>✔</div></div>	<div>Blacklisted</div>	<div>If</div> <div><div>Blackliste...</div><div></div></div> <div>and</div>	<div><div>Condition(s)</div><div></div></div> <div>then</div>	<div><div>DenyAccess</div><div></div></div>
<div><div></div><div>✔</div></div>	<div>Profiled Cisco IP Phones</div>	<div>If</div> <div><div>Cisco-IP-...</div><div></div></div> <div>and</div>	<div><div>Condition(s)</div><div></div></div> <div>then</div>	<div><div>Cisco_IP_Pho...</div><div></div></div>

Step 8 Click **Save**.

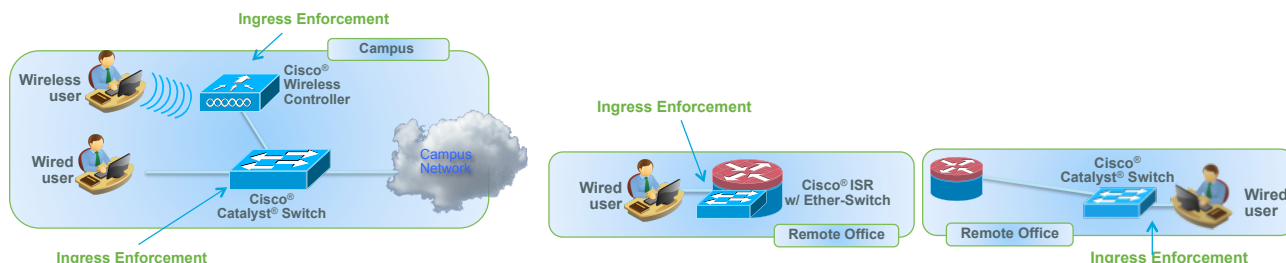
Now the user will still show as a failed authentication, but the reason will be "rejected per authorization profile".



Phase 2: Authenticated Mode

As with Phase 1: Monitor Mode, this section will cover wired access, in both a campus and a remote office. The solution test includes the use of the Cisco EtherSwitch module in the Integrated Services Router (ISR) for remote-office locations. However, now that authentication is being added, we are also able to introduce Wireless Access to the network.

Figure 19: Typical Authenticated Access Scenarios



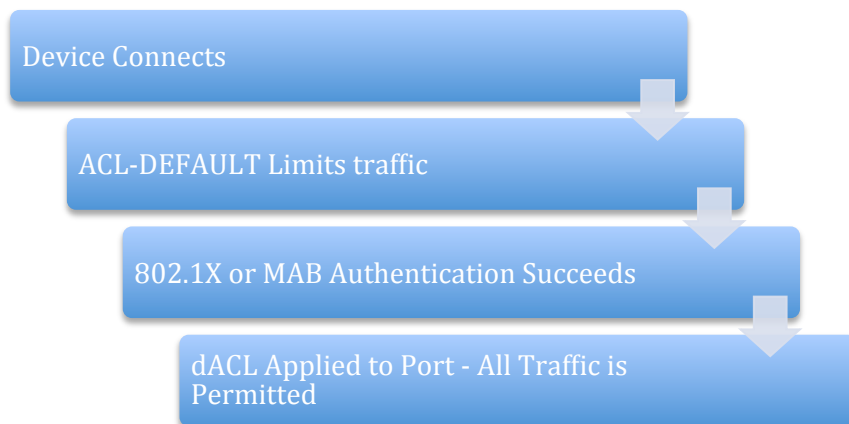
Wired Access

At this stage there should be no wired devices that are not authenticating by either 802.1X or MAB. Therefore it is now time to instill some additional security to limit traffic from devices that have not authenticated, and introduce the topics of Web Authentication and Guest Access.

As discussed in the “Introduction” section, authenticated mode is a deployment strategy that adds security on top of the framework that we built in monitor mode by applying an Access Control List (ACL) to the switchport that allows very limited network access prior to authentication. We will refer to that ACL as the “default ACL” or “port ACL”. We configured this in the “Switches – Universal Global Configuration Commands” section, and it was named ACL-DEFAULT. The purpose of this ACL is to allow critical traffic to flow prior to an authentication. It may be necessary to open additional traffic depending on your environment.

After users or devices successfully authenticate, they are granted full network access with a downloadable ACL (DACL) that permits all traffic. This component is a critical component of this phase of Cisco TrustSec deployment. The DACL overrides the default port ACL for the specific device that authenticated (handled per session). Without the DACL, a device would still be subjected to the ACL-DEFAULT that is assigned to the port (Figure 20).

Figure 20: Process for Authentication Mode



Create an Authorization Rule for Other Network Devices – Cisco Wireless Access Points

Cisco IP Phones and Wireless Access Points are among two of the more common endpoints that may need access to the network. Both have configurable supplicants, and may require special access. As we saw previously, IP Phones will require access to the Voice Domain.

Wireless Access Points will typically need limited access to the network. They require DNS, TFTP, DHCP, CAPWAP, and LWAP protocols at a minimum. For this reason, we will create a separate Authorization rule for Access Points that permits all traffic at this stage (Authenticated Mode).

Note: In the final phase (Enforcement), we will strengthen the Authorization enforcement to lock down access points further.

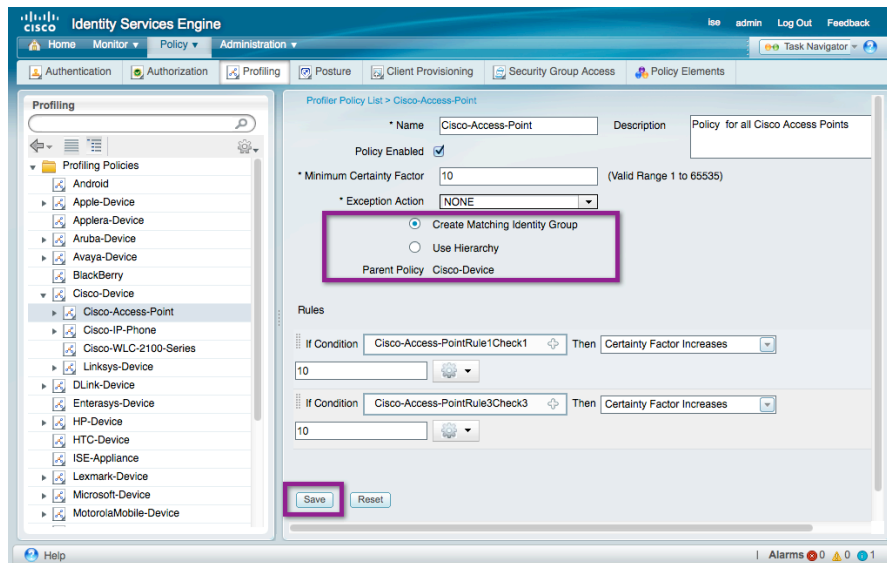
Procedure 1 Create an Identity Group based on Profiling Policies.

Step 1 Navigate to Policy → Profiling.

Step 2 Expand the **Profiling Policies** container. Expand **Cisco-Devices**.

Step 3 Highlight Cisco-Access-Point.

Step 4 Select Create Matching Identity Group.



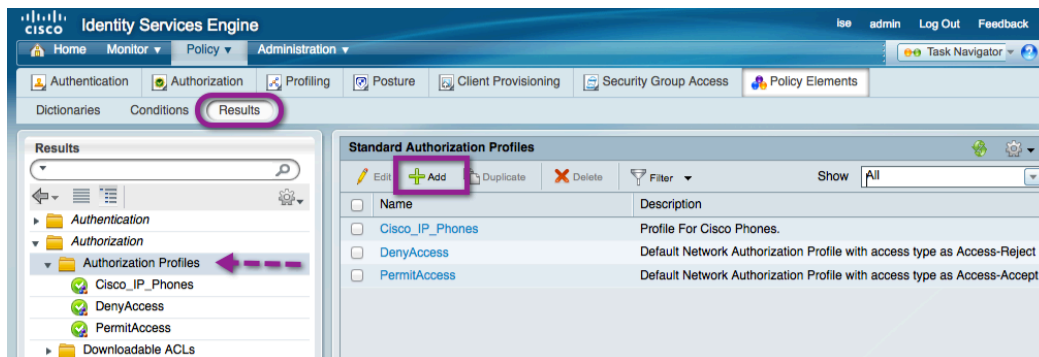
Step 5 Click **Save**.

Note: We have just created an Identity group, similar to the Whitelist identity group created in the "Create a Whitelist for Endpoints" procedure. The difference is we are building that identity group from a device profile instead of manually.

Procedure 2 Create a new Authorization Profile.

Note: The Authorization profile will be exactly the same as the prebuilt "Permit-Access". The purpose of creating a new Authorization Profile is to have a unique Authorization profile that may be changed during the Authenticated or Enforcement phases of deployment.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.



Step 2 Click **Add**.

Step 3 Configure the new Authorization profile as described:

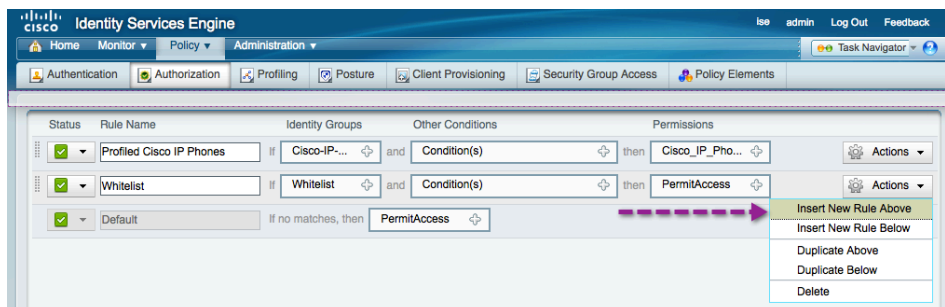
```
Name = Access-Points
Description = Authorization Profile for Access-Points.
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☒ DACL Name = PERMIT_ALL_TRAFFIC
☒ Wireless LAN Controller (WLC) = PERMIT_ALL_TRAFFIC
```

Step 4 Click Submit.

Procedure 3 Add a Rule to the Authorization Policy for Access Points.

Step 1 Navigate to Policy → Authorization.

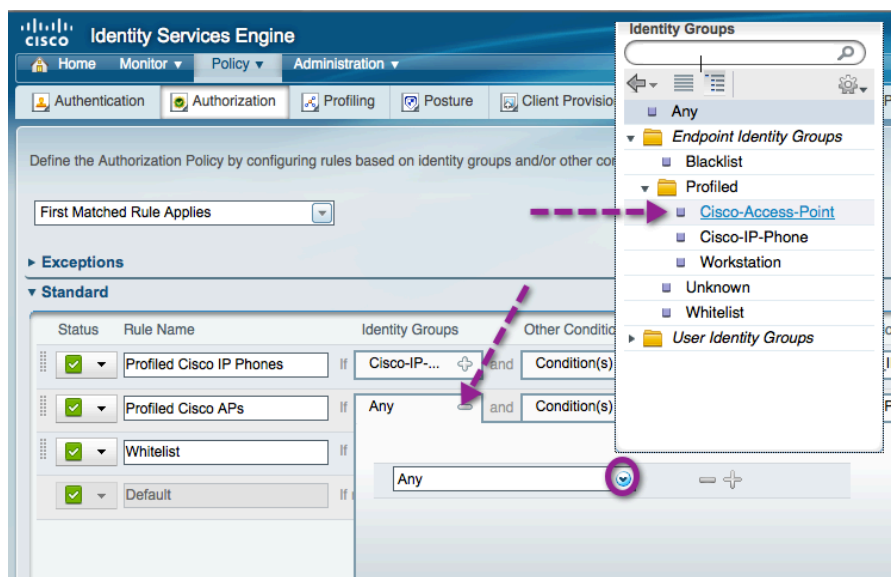
Step 2 Click **Actions** at the end of the Whitelist Authorization rule. Select **Insert New Rule Above**.



Step 3 Name the new rule: **Profiled Cisco APs**.

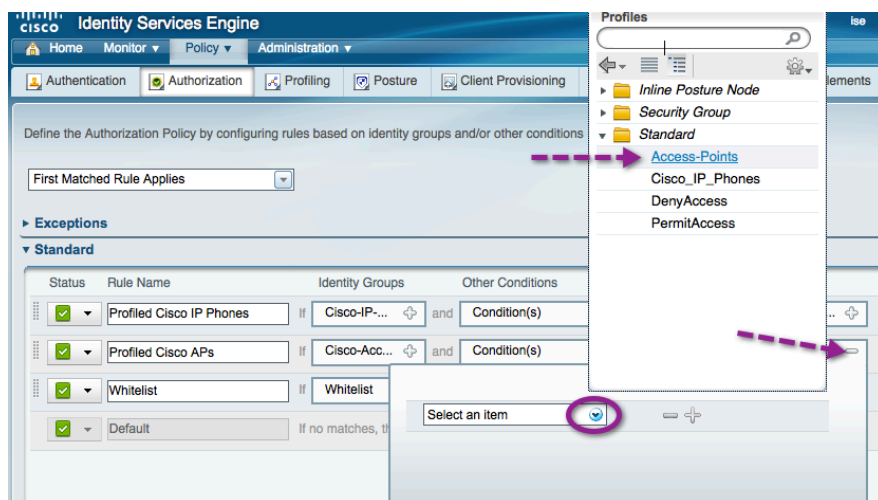
Step 4 Click the "+" sign under the Identity Groups column.

Step 5 Select Endpoint Identity Groups → Profiled → Cisco-Access-Point (created in Procedure 1).



Step 6 Click the “+” sign in the Permissions column.

Step 7 Select Standard → Access-Points (created in Procedure 1).



Step 8 Click **Save**.

Create an Authorization Rule for Windows Machine Authentication

Windows machine authentication is used to allow Windows-based computers to communicate to the Active Directory domain for group policy and other updates **before** the user logs in. This rule is being created to better suit enterprise environments, where machines may be powered on without an interactive user being logged in.

Note: It is not currently possible to enforce a dual authentication of both Machine and User-Auth in a feasible way. There is an enhancement underway in the Standards body and within Cisco for EAP-Chaining within EAP-FASTv2. EAP-Chaining will allow a single Authentication to include Machine and User credentials.

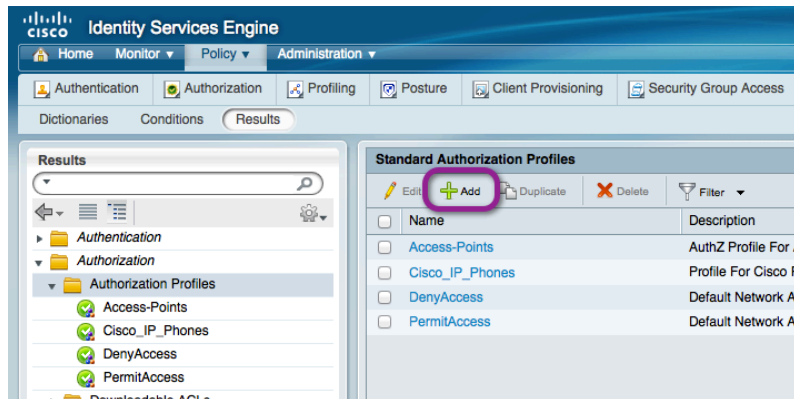
There are multiple ways to accomplish machine authentication. It is possible for machine authentication to occur with the use of a certificate (such as EAP-TLS). However, when using a non-certificate-based EAP method, such as PEAP-MSCHAPv2, Windows supplicants also have the ability to send the computer name as the credential. Cisco ISE can be configured to verify the computer exists in Active Directory, and if so, provide connectivity.

Because this phase is part of the Monitor Mode phase of deployment, we will configure the Authorization rule to permit full access to the computer.

Note: When the user logs in to a machine-authenticated Windows endpoint, the supplicant will start a new Authentication by sending an EAPoL-Start message into the switchport. After the new Authentication completes, a new Authorization result may be sent to the switchport to update the authorization profile, if desired.

Procedure 1 Create an Authorization Profile for Domain Computers.

Step 1 Navigate to Policy → Policy Elements → Results.

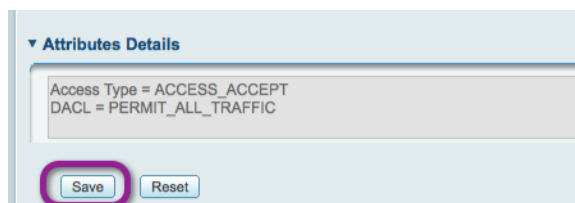


Step 2 Click **Add**.

Step 3 Configure the new Authorization profile as described:

```
Name = AD_Machine_Access
Description = Authorization Profile for Windows Machine Auth.
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☒ DACL Name = PERMIT_ALL_TRAFFIC
```

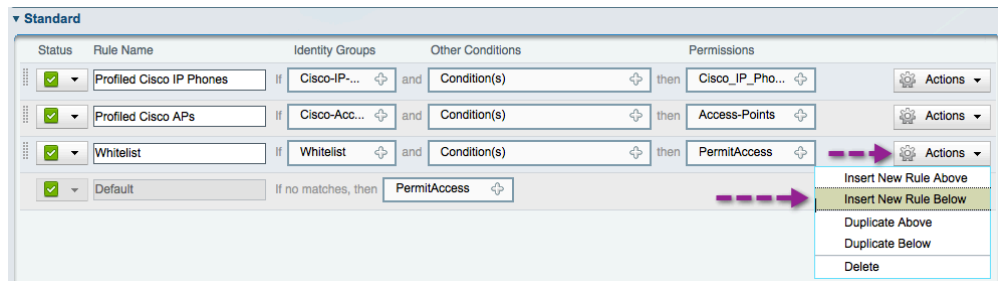
Step 4 Scroll to the bottom, and click **Save**.



Procedure 2 Create the Domain Computer Authorization rule.

Step 1 Navigate to Policy → Authorization.

Step 2 Click the **Action** button next to the **Whitelist Rule**, and select **Insert New Rule** Below.

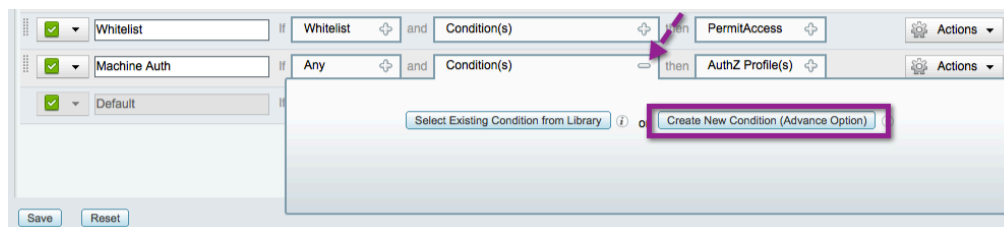


Step 3 Name the rule **Machine Auth**.

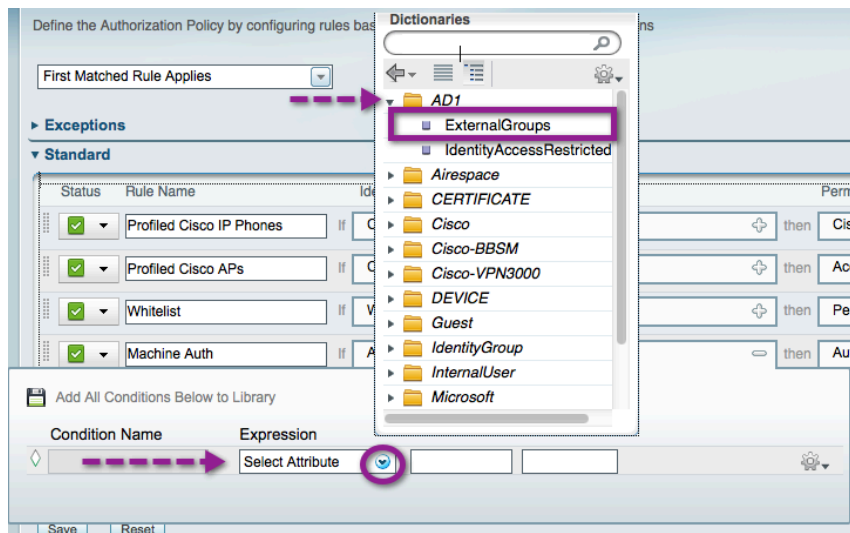
Step 4 Do not change the Identity Group; leave it as **Any**.

Step 5 Click the “+” sign to choose conditions.

Step 6 Click Create New Condition.

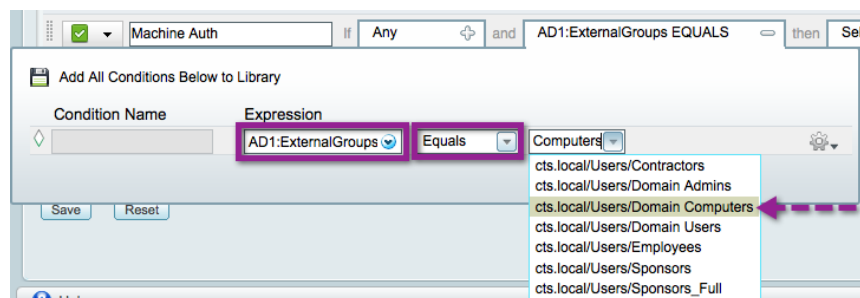


Step 7 Use the Expression drop-down menu to choose the attribute: **AD1 → ExternalGroups**



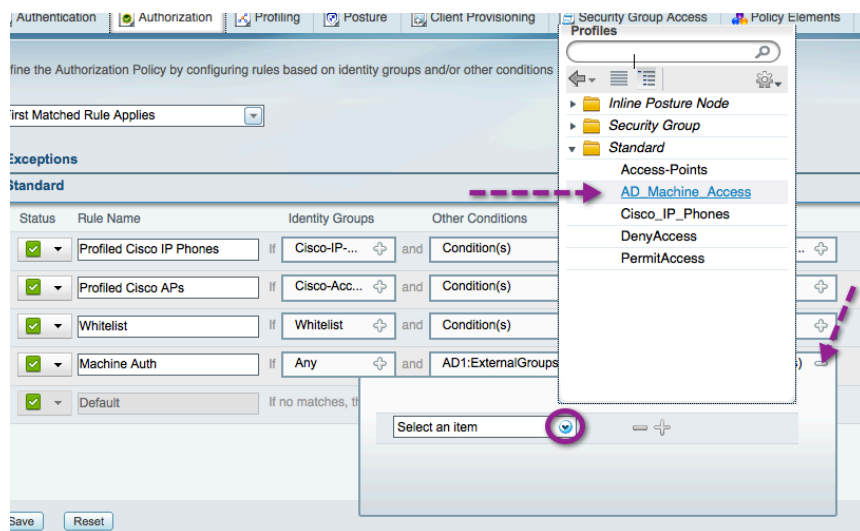
Step 8 Select **Equals**.

Step 9 Select the Domain Computers.



Note: if Domain Computers is not in the drop-down menu, revisit the Active Directory Integration section.

Step 10 For the Permissions column, click the drop-down menu and choose **Standard** → **AD_Machine_Access**.



Step 11 Click **Save**.

Create an Authorization Rule for Authenticated Users

One big difference between Monitor mode and Authenticated mode is that a user or device must successfully authenticate to the network in order to gain access. Therefore, we need to have a specific authorization rule for each user or device type. To accomplish this requirement, we will create a new Authorization rule that permits full access to any member of the Domain Users Active Directory group.

Note: When reaching the Enforcement mode phase of deployment, it is highly recommended to create an Authorization rule for each main group in AD, and to discontinue the use of this Domain Users rule.

Procedure 1 Create the Domain Users Authorization Profile.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 2 Click **Add**.

Step 3 Configure the new Authorization profile as described. Click **Save**.

Name = Domain_Users

Description = Authorization Profile to provide full-access to Users (Authenticated Mode).

Access-Type = ACCESS_ACCEPT

-- Common Tasks

☒ **DACL Name** = PERMIT_ALL_TRAFFIC

Procedure 2 Create the Domain Users Authorization Rule.

Step 1 Navigate to Policy → Authorization.

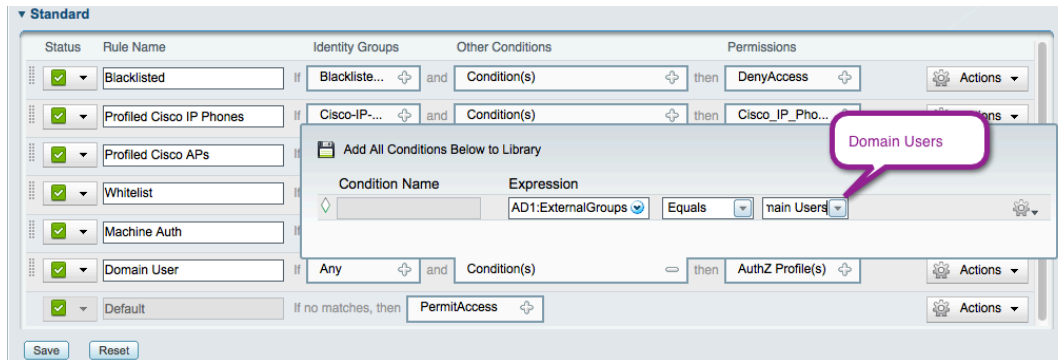
Step 2 Insert a new rule below Machine Auth.

Step 3 Name the new rule “Domain Users”.

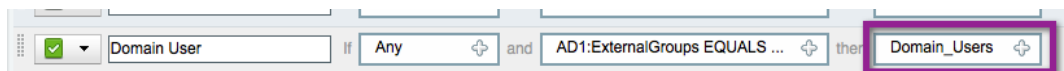
Step 4 Leave Identity Groups as “Any”.

Step 5 Create a new condition. Choose AD1 → External Groups.

Step 6 Set the condition to equals. Select Domain Users.



Step 7 Set the Permission to Domain_Users.



Step 8 Click Save.

Wireless Access

Introduction

Over the past couple of years, wireless networks have transitioned from being an optional medium of connectivity to being the primary medium used by most people. The advances in wireless technology and the proliferation of Wi-Fi-capable devices such as laptops, mobile phones, and tablets have made wireless security one of the biggest challenges for IT administrators. Not only do the IT administrators have to identify users connecting to the wireless network, they also need to be able to differentiate between users using corporate assets as opposed to users using personal assets on the corporate networks.

There are three main policy models around wireless network access:

1. Complete access to corporate resources over wireless networks – Once users successfully authenticate via 802.1X, they are given unrestricted access to all corporate resources, irrespective of the device being used. Although this model is easy to maintain, there are very high risks associated with it.
2. No access to corporate resources over wireless networks - Although this model may have worked in the earlier days when Wi-Fi was still in its early stages, it is definitely not an option today. For obvious reasons, this model requires very low maintenance and is a very low associated risk.
3. Differentiated Access to corporate resources – This model requires IT administrators to define policies around multiple factors such as a user's role in the organization, the type of device being used to access the network, etc. Traditionally, this model has been a very high maintenance, low risk model.

Cisco TrustSec takes advantage of technologies such as IEEE 802.1X authentication and profiling to allow IT administrators to provide differentiated access on wireless networks in a scalable and easily manageable manner. Cisco TrustSec uses Cisco ISE as a central policy-management server to help provide secure wireless networks and enables organization to allow their users to bring their own devices (BYOD).

This document will walk you through the steps of configuring Cisco ISE and the WLC to enable differentiated access on wireless networks to allow BYOD. We will also highlight how Cisco TrustSec allows you to provide Guests with wireless access.

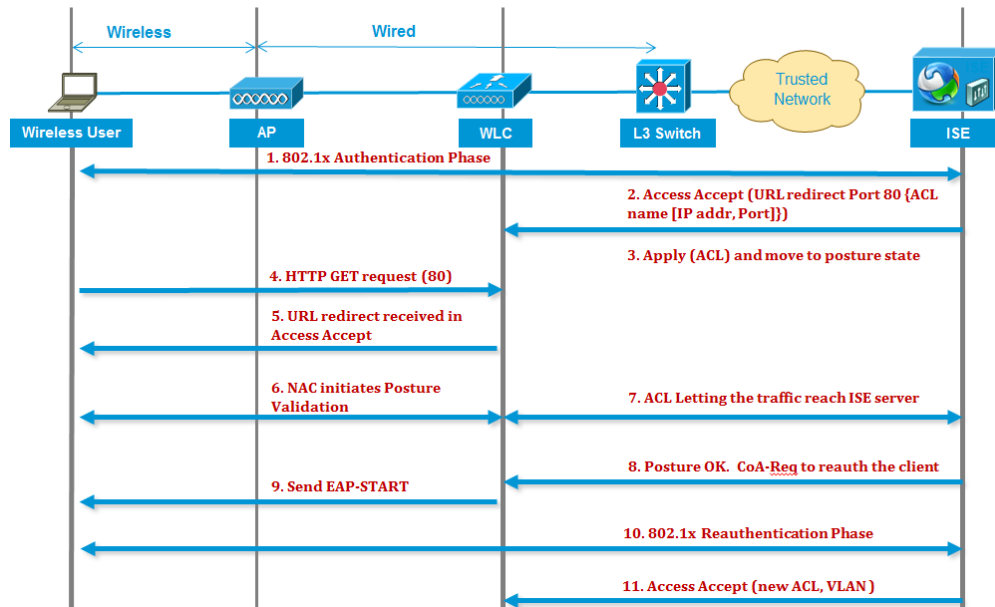
The use cases we will cover are:

1. Employees + Corp device (laptop / tablet : EAP-TLS) + Posture compliant = Full access (VLAN + No ACL)
2. Employee + Personal device (PEAP) = Internet-only access (Same VLAN + Named ACL restricting access)
3. Guest = Internet-Only Access (enforced using ACL)

Elaboration on Wireless Access

With the ability of Cisco ISE to enforce policy across wired and wireless access, it is easy for IT administrators to provide users with a similar network access experience across both access mediums. Cisco ISE allows us to perform user authentication, device profiling, and posture assessment on a wireless network configured for IEEE 802.1X authentication. The authentication and authorization flow for wireless users is explained below.

Figure 21: Wireless 802.1X Authentication Flow



1. Client successfully authenticates using dot1x authentication.
2. RADIUS Access Accept carries redirected URL for port 80 and pre-auth ACLs that includes allowing IP addresses and ports or quarantine VLAN.
3. Client will be redirected to the URL provided in access accept and put into Posture_Req until posture validation is complete.
4. NAC agent on client initiates posture validation (traffic to port 80): Agent sends HTTP discovery request to port 80, which the controller redirects to a URL provided in access accept. Cisco ISE knows that client trying to reach it and responds directly to the client. This way the client learns about Cisco ISE server IP and from now on, the client talks directly with Cisco ISE server.
5. WLC allows this traffic because we have configured ACL to allow it. In the case of VLAN override, we simply bridge the traffic so that it reaches the Cisco ISE server.
6. When the Cisco ISE client completes assessment, a RADIUS CoA-Req with reauth service is sent to WLC, which initiates re-authentication of the client (by sending EAP-START). When re-authentication succeeds, Cisco ISE sends Access Accept with a new ACL (if any) and no URL redirect or access VLAN.
7. WLC supports CoA-Req and Disconnect-Req as per RFC 3576. WLC needs to support CoA-Req for reauth service, which is as per RFC 5176.
8. Instead of downloadable ACLs, we need to use preconfigured ACLs on the WLC, and the Cisco ISE server just sends ACL name, which is already configured in the controller.
9. This design should work for both VLAN and ACL cases. In the case of VLAN override, we just redirect the port 80 and allow (bridge) rest of the traffic on the quarantined VLAN. For ACL, we will just apply the pre-auth ACL we got in access accept.

Wireless in Branch Offices

In a typical wireless deployment, all traffic from an access point is tunneled back to a wireless LAN controller from where it is introduced on the network. This tunneling is known as the Split-MAC architecture for wireless networks. Because all the traffic is switched centrally at the WLC, Cisco ISE pushes the policy down to the WLC.

Although the Split-MAC architecture works well for campus WLAN deployments, it is not recommended for remote-site deployments. Access points installed at remote sites would typically communicate with the WLAN located in a data center. Using the Split-MAC architecture will require all user traffic to be first over the WAN to the WLC before it is switched. This results in an additional load on WAN links. Cisco hence recommends using the Hybrid Remote Access Point (H-REAP) or Local MAC architecture. The H-REAP model forwards only the control traffic to the WLC over the WAN link and all user data is switched locally at the remote site (Table 13).

Table 13: Cisco TrustSec Features

Cisco TrustSec Features	Cisco 5508 Wireless Controller and Cisco Wireless Services Module 2 (WiSM-2)		Cisco 7500 Wireless Controller	
	Central Switching	Local Switching	Central Switching	Local Switching
Basic AAA Functions	Yes	Yes	N/A	Yes
Profiling	Yes	No	N/A	No
Posturing	Yes	No	N/A	No
VLAN Override	Yes	No	N/A	No
ACL Override	Yes	No	N/A	No
Guest Provisioning	No	No	No	No

Web Authentication

Configuration of Web Authentication is a critical step when moving transparently from the Monitor Mode phase into the Authenticated phase of deployment. Until this point, the “default” rule (the rule of last resort) in the authorization policy was set to **PermitAccess**, meaning that if a device does not meet any of the more specific criteria mentioned previously, we will just allow it full access to the network.

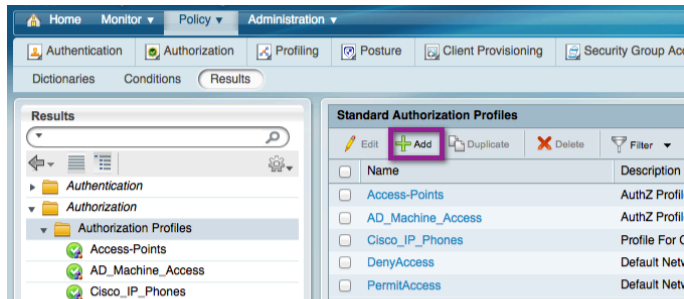
By implementing Web Authentication, we will provide a different Authorization rule of last resort. If you are not Authorized by one of the more specific rules, then the user/device will be forced into an Authorization state where traffic is extremely limited and the switch / WLC will redirect all web traffic to the Web Authentication captive portal. This redirection provides a webpage for users (guests and employees alike) to authenticate to the network and receive an Authorization result.

There are two different Web Authentication types. There is Local WebAuth, where the webpages and the authentication transaction occur locally to a switch or WLC. Then there is a more advanced Centralized Web Authentication method where the switch or WLC redirects web traffic to a centralized Captive Portal, and the authentication transaction occurs at the Captive Portal instead of locally.

Note: Cisco TrustSec 2.0 uses the Centralized Web Authentication (CWA) method.

Procedure 1 Create WEBAUTH Authorization Profile.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.



Step 2 Name the Authorization Profile “WEBAUTH”.

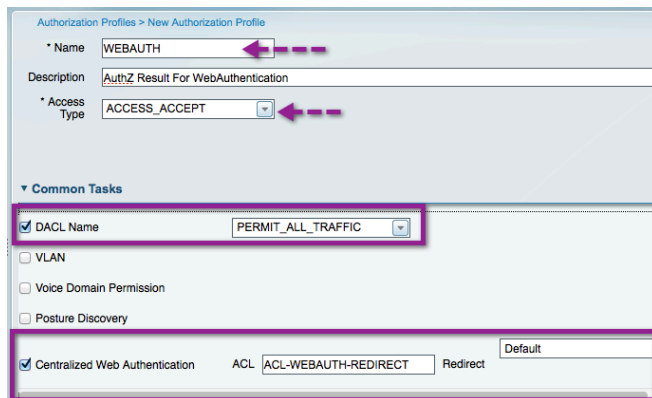
Step 3 Leave the Access Type as ACCESS_ACCEPT.

Step 4 Set the DACL to PERMIT_ALL_TRAFFIC.

Step 5 Enable Centralized Web Authentication, and enter ACL-WEBAUTH-REDIRECT as the ACL.

The ACL-WEBAUTH-REDIRECT ACL was built on the switch and the WLC during the “Configure Local Access Control Lists” procedure of this deployment guide. This ACL is the ACL that identifies the “interesting traffic”. Traffic matching that ACL will be redirected to the Centralized Web Authentication Portal. This ACL is distinctly different from a Downloadable ACL that limits traffic through the port.

Step 6 Leave the Redirect as Default.



Step 7 Scroll to the bottom of and validate that the Attributes Detail looks like the one that follows.



Step 8 Click **Save**.

GUEST Access

We have just configured Web Authentication that may be used for employees and also for Guests. Even though the lifecycle is known as Guest Lifecycle management, it can refer to any user needing network access. Cisco ISE provides mechanisms to create multiple Guest Types and control which sponsor groups are able to create each Guest Type.

For the purposes of this document, we will have only a single Guest-Type, and a single Authorization rule will need to be created for that Guest Type.

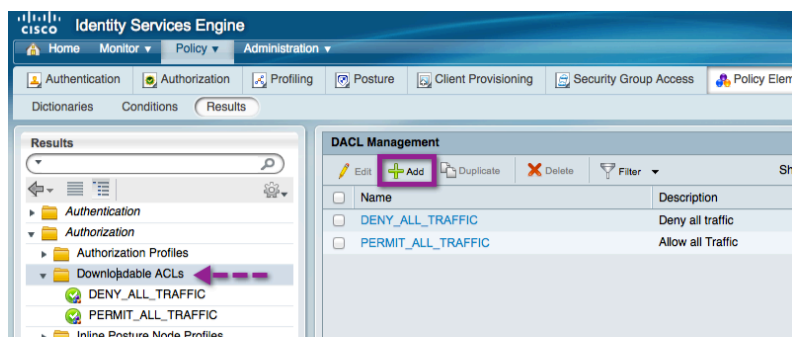
Cisco ISE Configuration – Configure the Guest Authorization

Authorization for Guest users is a topic that could take up an entire design guide, by itself. For the purposes of this design guide, we will authorize the Guest Users into the Guest VLAN, and provide a downloadable ACL that permits all traffic ingress at the switch.

This type of Authorization is commonly used, and assumes the network infrastructure is providing the isolation of the Guest user from the remainder of the corporate network. This type of isolation is often accomplished using network virtualization (VRF instances) or even simply access lists at the Layer 3 edge.

Procedure 1 Create a GUEST Downloadable ACL.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Downloadable ACLs.



Step 2 Click **Add**.

Step 3 Configure the new DACL as described:

Name = GUEST

Description = dACL for GUEST users (Authentication Mode).

DACL Content = permit ip any any

Warning: There is no syntax checking in Cisco ISE. If the DACL syntax is incorrect, it will not apply to the session.

Step 4 Click Submit.

Procedure 2 Create a GUEST Authorization Profile.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 2 Click **Add**.

Step 3 Configure the new Authorization Profile as described:

Name = GUEST

Description = Authorization Profile for GUEST role (Authentication Mode)

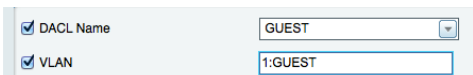
Access-Type = ACCESS_ACCEPT

-- Common Tasks

☒ **DACL Name** = GUEST

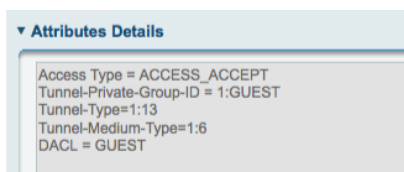
☒ **VLAN** = GUEST

Note: Cisco ISE 1.0 will automatically put a “1:” in front of the VLAN name. This notation is part of the RADIUS standard, and should be ignored.



DACL Name: GUEST
VLAN: 1:GUEST

Step 4 Scroll to the bottom, ensure the Attribute Details look like the following, and click **Submit**.



Attributes Details
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:GUEST
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DACL = GUEST

Note: The switchport host mode is extremely important when using VLAN assignment. VLAN Assignment is not recommended when using Multi-Auth, or Multi-Host modes. Only one VLAN may be assigned to the Data Domain, and another VLAN for the Voice Domain. Multi-Auth and Multi-Host modes allow for more than one device in the Data Domain, and therefore the first VLAN assigned to the port will take effect for all switchports.

Procedure 3 Create a GUEST Authorization Policy Rule.

Step 1 Navigate to Policy → Authorization.

Step 2 Insert a new Rule above the Default rule (bottom of the Policy table).

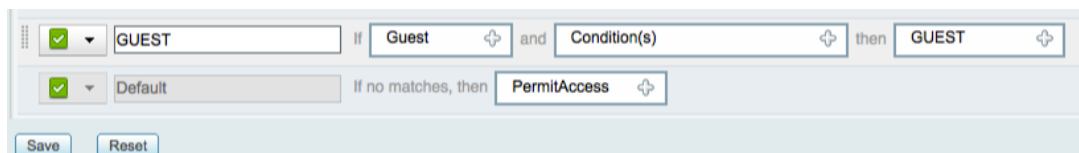
Step 3 Name the new Rule **GUEST**.

Step 4 Under Identity Groups, Click the “+” sign on the picker.

Step 5 Choose User Identity Groups → GUEST.

Step 6 Leave Other Conditions alone.

Step 7 For Permissions, click the “+” sign and select **Standard → GUEST**.



Policy configuration interface showing a rule named 'GUEST' with conditions 'Guest' and 'Condition(s)', and a permission of 'GUEST'. Below it, the 'Default' rule is shown with a permission of 'PermitAccess'.

Step 8 Click **Save**.

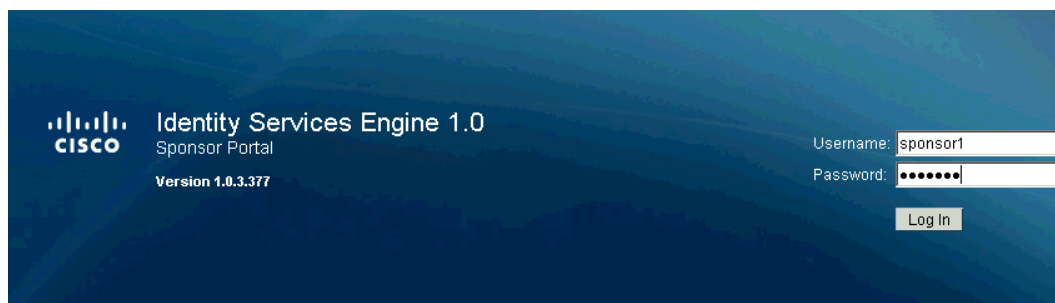
Cisco ISE Configuration – Guest Account Creation

Procedure 1 Configure Guest User in the Sponsor Portal.

Step 1 From your web browser, navigate to the sponsor portal at:

https://<portal_host_or_IP_address>:8443/sponsorportal.

Step 2 Log in to the portal using the sponsor user’s credentials.



Identity Services Engine 1.0
Sponsor Portal
Version 1.0.3.377
Username: sponsor1
Password:
Log In

Step 3 Navigate to Create Guest Account.

Step 4 Configure at a minimum the required fields.

The screenshot shows the Cisco Sponsor Portal interface. On the left is a navigation menu with 'Sponsor' and 'Account Management' sections. The 'Account Management' section is expanded, showing options like 'View Guest Accounts', 'Create Multiple Accounts', 'Create Random Accounts', and 'Import Accounts'. The main content area is titled 'Create Guest Account' and contains a form with the following fields: First Name (John), Last Name (Doe), Email Address (jdoe@acme.com), Phone Number (123456), Company (Acme Corp), and five Optional Data fields. Below these are dropdown menus for Group Role (Guest) and Time Profile (DefaultOneHour). A Timezone dropdown is set to UTC. A legend indicates that orange asterisks mark required fields. At the bottom are 'Submit' and 'Cancel' buttons.

Step 5 Click Submit.

Change Default Authorization to WebAuth and Test

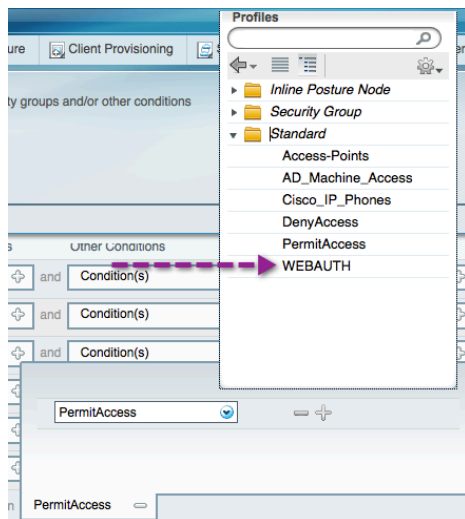
Procedure 1 Change the Default Authorization Rule to WebAuth.

Warning: Before completing this step, ensure you are ready for Authenticated mode. After this procedure, any device that does not have a specific authorization rule will be put into the WEBAUTH Authorization state.

Step 1 Navigate to Policy → Authorization.

Step 2 Scroll to the bottom, and click the “+” sign in the picker, next to “if no matches, then”.

Step 3 Select Standard → WEBAUTH. Click Save.



Procedure 2 Test Web Authentication.

Now that the “authorization of last resort” has been set to WebAuth, it is time to verify that WebAuth is working correctly.

Step 1 Connect to the network with a Windows or Mac device that does not have a configured supplicant.

Step 2 On the switch, verify the authorization result.

```
C3750X#show authentication session interface <interface_name>
```

```
C3750X#show authentication session int gig1/0/2
  Interface: GigabitEthernet1/0/2
  MAC Address: 0050.5687.0004
  IP Address: 10.1.10.50
  User-Name: 00-50-56-87-00-04
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Group: N/A
  ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-4dc4ad0d
  URL Redirect ACL: ACL-WEBAUTH-REDIRECT
  URL Redirect:
https://ise.cts.local:8443/guestportal/gateway?sessionId=0A0130020000000F2703ACFF&action=cwa
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A0130020000000F2703ACFF
  Acct Session ID: 0x00000012
  Handle: 0x7E00000F

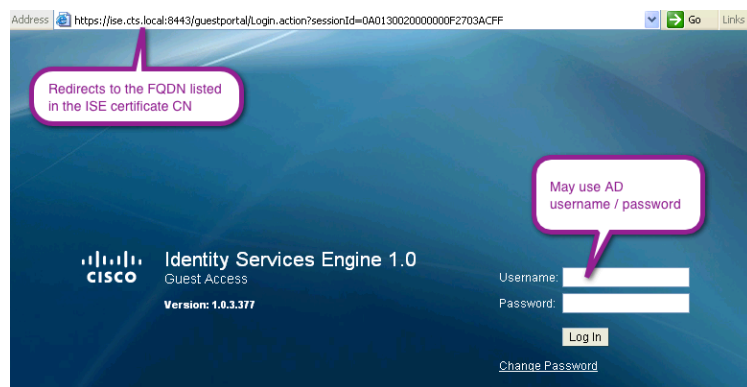
Runnable methods list:

  Method  State
  dot1x   Failed over
  mab     Authc Success
```

Step 3 View the Cisco ISE Live Authentications Log for the session.

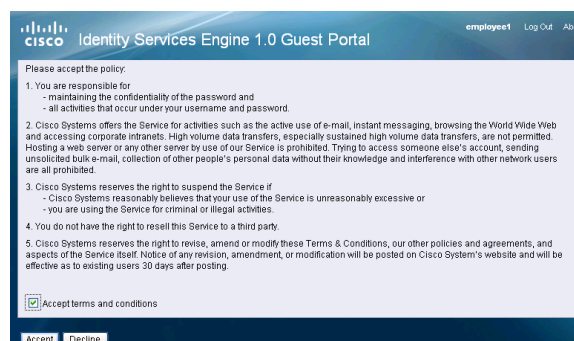
Oct 05,11 09:05:00.365 AM	✓		00:50:56:87:00:04	00:50:56:87:00:04	10.1.10.50	SJC18-sw-1	GigabitEthernet1/0/2	WEBAUTH
Authentication Summary								
Logged At:		October 5,2011 9:05:00.365 AM						
RADIUS Status:		Authentication succeeded						
NAS Failure:								
Username:		00:50:56:87:00:04						
MAC/IP Address:		00:50:56:87:00:04						
Network Device:		SJC18-sw-1 : 192.168.254.1 : GigabitEthernet1/0/2						
Allowed Protocol:		Default Network Access						
Identity Store:		Internal Endpoints						
Authorization Profiles:		WEBAUTH						
SGA Security Group:								
Authentication Protocol :		Lookup						

Step 4 On the Client, open a web browser. Traffic will be automatically redirected to Cisco ISE.



Common issue: If Cisco ISE is not in DNS, this redirection will fail. Ensure that all Cisco ISE nodes are listed correctly in the DNS.
We entered "employee1", which is a valid AD user Account.

Step 5 The Acceptable Use policy will display, and Employee1 accepts it.



Step 6 A New Authorization occurs. View the results on the switch and the Live Authentications Log:

C3750X#show authentication session interface <interface_name>

```
C3750X#show authen sess int g1/0/2
  Interface: GigabitEthernet1/0/2
  MAC Address: 0050.5687.0004
  IP Address: 10.1.10.50
  User-Name: employee1
  Status: Authz Success
  Domain: DATA
  Security Policy: Should Secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Group: N/A
  ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-4dc4ad0d
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A0130020000001127DC1A50
  Acct Session ID: 0x00000014
  Handle: 0x53000011

Runnable methods list:
  Method   State
  dot1x    Failed over
  mab      Authc Success
```

Note: Notice the changes in the output. The URL redirection is no longer there, and the username is known.

Oct 05,11 09:05:50.949 AM	✓	employee1	00:50:56:87:00:04	10.1.10.50	SJC18-sw-1	GigabitEthernet1/0/2	PermitAccess
Authentication Summary							
Logged At:	October 5,2011 9:05:50.949 AM						
RADIUS Status:	Authorize-Only succeeded						
NAS Failure:							
Username:	employee1						
MAC/IP Address:	00:50:56:87:00:04						
Network Device:	SJC18-sw-1 : 192.168.254.1 : GigabitEthernet1/0/2						
Allowed Protocol:	Default Network Access						
Identity Store:	AD1						
Authorization Profiles:	PermitAccess						
SGA Security Group:							
Authentication Protocol :							

Configure Cisco ISE for Wireless Guest Access

Organizations will typically have an open SSID to provide Guest Access. When the Guest user is connected to the SSID, the guest will be redirected to the Cisco ISE guest portal. Here the guest can use the Guest credentials (created by a sponsor) and get access to the network.

Note: The WLC uses Local Web-Auth for Guest Access. It does not support Central Web-Auth. In LWA, the access device intercepts the login credentials via the web authentication process and then submits them to Cisco ISE via RADIUS for authentication and authorization.

Note: The WLC also does not support RADIUS CoA on Open SSIDs. As a result, Guests cannot be assigned to VLANs dynamically. Guests can be restricted to VLANs by mapping the SSID to a dynamic interface. wACLs can be applied to Guests as an enforcement method.

Note: Using anchor controllers located in a DMZ to completely isolate Guest traffic from corporate traffic is a recommended best practice. However, it was not part of the Cisco TrustSec Systems Test, and therefore cannot be part of this documentation. Even so, please be warned that because Cisco ISE would typically be located within a data center, it is difficult to allow a client whose traffic is going through an Anchor WLC located in a DMZ to send traffic back to the data center. This concern will be addressed in a future release of Cisco ISE.

Procedure 3 Define the Guest ACL on the WLC.

Step 1 Refer to the section “Create a wACL for Posture Assessment” for information on adding a wACL

Step 2 Add rules for the Guest wACL (Table 14)

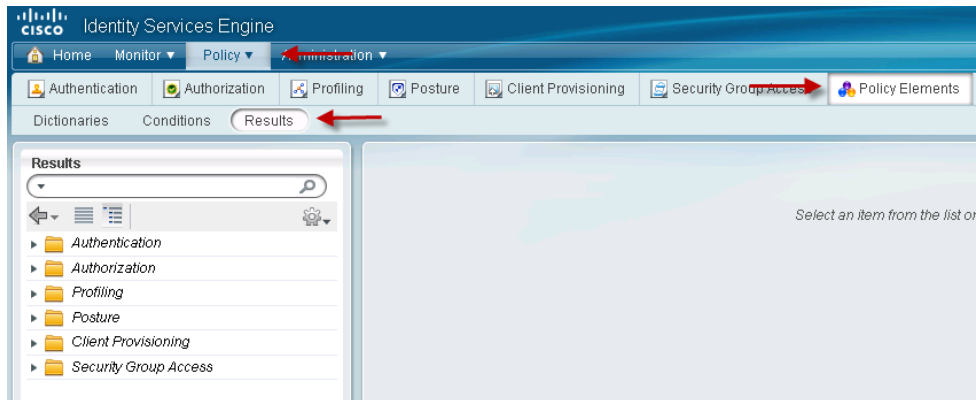
Table 14: Guest wACL

Guest wACL			
Sequence	1	2	3
Source	Any	Any	Any
Destination	IP address 10.1.20.1 255.255.255.255	IP address 10.1.0.0 255.255.0.0	Any
Protocol	Any	Any	Any
DSCP	Any	Any	Any
Direction	Any	Any	Any
Action	Permit	Deny	Permit

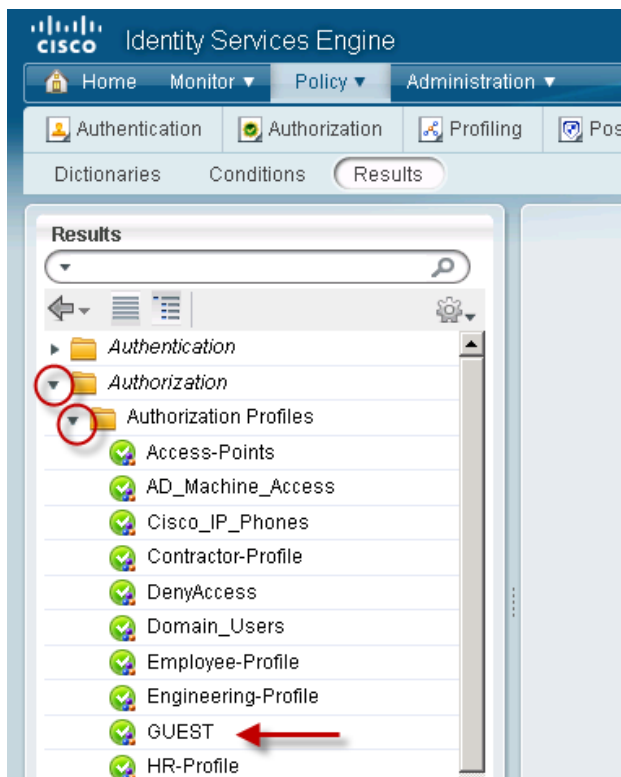
Note: DNS is permitted by default for pre-authenticated endpoints.

Procedure 4 Add the wACL to the Guest Authorization profile on Cisco ISE.

Step 1 On Cisco ISE, navigate to Policy → Policy Elements → Results.



Step 2 Select Authorization → Authorization Profiles → GUEST.



Step 3 Add the wACL value under the Common Tasks section.

Authorization Profiles > GUEST

* Name: GUEST

Description: AuthZ Profile For GUEST Role (Authentication Mode)

* Access Type: ACCESS_ACCEPT

▼ Common Tasks

- ☐ Reauthentication
- ☐ MACSec Policy
- ☐ NEAT
- ☐ Web Authentication (Local Web Auth)
- ☒ Wireless LAN Controller (WLC) GUEST-ACL
- ☐ ASA VPN

Committing to Authenticated Mode

At this stage the Cisco ISE policies are all created to allow all authenticated devices to have full access to the network; Web Authentication has been configured; and Sponsored Guest Access and Guest Account creation is operational. However, the default port ACL on the switches still allows all traffic.

To fully commit to the Authenticated Mode phase of deployment, we must change the default port ACL to one that restricts access. The level of restriction is entirely up to the deployment plan. We will examine a few default ACLs that have been used in the field, and discuss what complications may exist in your deployment, and how to adjust the default ACL appropriately.

Following are two suggested default ACLs. We configured the first one during the “Apply the initial ACL on the Port and enable authentication” stage of this deployment guide.

ACL-DEFAULT (the recommended, secure Default ACL):

```
ip access-list extended ACL-DEFAULT
remark DHCP
permit udp any eq bootpc any eq bootps
remark DNS
permit udp any any eq domain
remark Ping
permit icmp any any
remark PXE / TFTP
permit udp any any eq tftp
remark Drop all the rest
deny ip any any log
```

The second suggested default port ACL opens a lot of Microsoft ports to allow devices to communicate with Active Directory before login in order to improve login times. Opening Microsoft-specific ports may also be accomplished with the Machine Authentication we accomplished in the “Create an Authorization Profile for Domain Computers” procedure.

ACL-DFLT-LESS-RESTRICT:

```
ip access-list extended ACL-DFLT-LESS-RESTRICT
remark DHCP, DNS, ICMP
permit udp any eq bootpc any eq bootps    !DHCP
permit udp any any eq domain              !DNS
permit icmp any any                       !ICMP Ping
remark Allow Microsoft Ports (used for better login performance)
permit tcp any host 10.1.100.10 eq 88      !Kerberos
permit udp any host 10.1.100.10 eq 88      !Kerberos
permit udp any host 10.1.100.10 eq 123     !NTP
permit tcp any host 10.1.100.10 eq 135     !RPC
permit udp any host 10.1.100.10 eq 137     !NetBIOS-Nameservice
permit tcp any host 10.1.100.10 eq 139     !NetBIOS-SSN
permit tcp any host 10.1.100.10 eq 389     !LDAP
permit udp any host 10.1.100.10 eq 389     !LDAP
permit tcp any host 10.1.100.10 eq 445     !MS-DC/SMB
permit tcp any host 10.1.100.10 eq 636     !LDAP w/ SSL
permit udp any host 10.1.100.10 eq 636     !LDAP w/ SSL
permit tcp any host 10.1.100.10 eq 1025    !non-standard RPC
permit tcp any host 10.1.100.10 eq 1026    !non-standard RPC
remark PXE / TFTP
permit udp any any eq tftp
remark Drop all the rest
deny ip any any log
```

Slow Logins

If a slow login is still being detected, it is possible that another application is causing the slowness. Today's enterprise environments tend to have a lot of corporate applications installed on them. Some are very "chatty" and will relentlessly try to communicate with their management servers. Following are some suggested methods to identify the application that is causing the slow login:

- Option1: Use a network packet sniffer application to identify all traffic attempts prior to login.
- Option2: Implement a similar access list on a Cisco ASA Adaptive Security Appliance Firewall to log all attempts and all drops. Leave the default port ACL as ACL-ALLOW (permit ip any any).

Change the Default Port ACL

Procedure 1 Replace ACL-ALLOW with ACL-DEFAULT.

Step 1 Apply the initial ACL (ACL-ALLOW).

```
C3750X(config-if-range)#ip access-group ACL-DEFAULT in
```

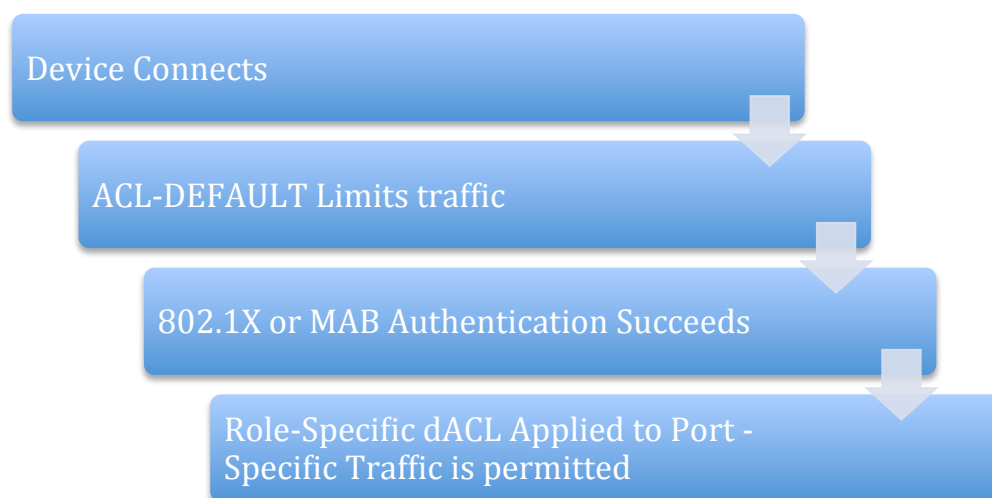
Phase 3: Enforcement Mode

Wired Access

At this stage there should be no wired devices that are not authenticating either by 802.1X or MAB. When a device (wired or wireless) authenticates, it is given full access to the network. It is now time to secure the network even more by differentiating the access that is granted per user. Full Access after an authentication may be enough security for some deployments, but is not secure enough for most companies.

As discussed in the “Introduction” section, Enforcement Mode is a deployment strategy that tightens the security framework that we built in monitor mode and authenticated mode by applying a specific downloadable Access Control List (DACL) to the session of the user or device. This component is a critical one of this phase of Cisco TrustSec deployment. The DACL overrides the default port ACL for the specific device that authenticated (handled per session). Without the DACL, a device would still be subjected to the ACL-DEFAULT that is assigned to the port. The big difference between this phase and the previous one is the specific Authorization result that will be issued per user or device based on the role of that user (Figure 22).

Figure 22: Enforcement Mode Process



Examining Additional User Information

Until this point, if a user was a member of the Domain Users group, that user received full network access. To improve security, we will look at additional groups, and provide differentiated access to each group. Please reference the table of Active Directory users and group membership.

Procedure 1 Add additional groups to the Active Directory connector.

Step 1 Navigate to Administration → External Identity Sources → Active Directory.

Step 2 Click the **Groups** tab.

Step 3 Click Add → Select Groups from Active Directory.

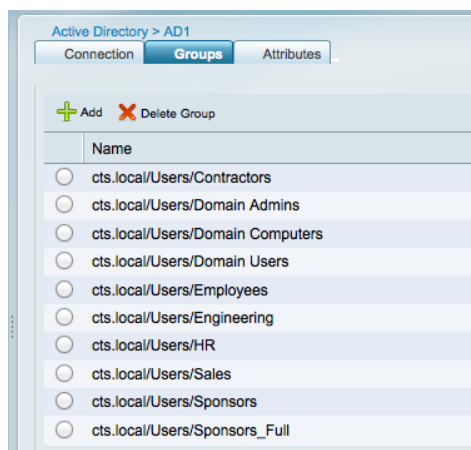
Step 4 Click Retrieve Groups.

Note: When AD has more than 100 groups, use the filter options to find the specific group you are looking for.

Step 5 Select the additional groups.

In our example, we will be selecting the **Engineering**, **Sales**, and **HR** groups.

Step 6 Click **OK**. A screenshot of our final Group selection follows:



Step 7 Scroll to the bottom and click **Save Configuration**.

Note: it is a common mistake to forget this step. Without saving the configuration, the additional groups will not be retrieved from Active Directory during Authorization.

Cisco ISE Configuration – Continue Configuration for Enforcement Mode

Procedure 1 Create additional downloadable ACLs for each main role.

This procedure should be repeated for each role that will have a different Authorization. For the purposes of documentation, we will step through the creation of the HR dACL, and then show the final screen with all the DACLS defined.

Best Practice: Keep all DACLS small. DACL support on a switch is related to the amount of available Ternary Content Addressable Memory (TCAM) space. Each ASIC in a switch has its own TCAM, and the number of ASICs per port will vary between switch models. The amount of TCAM assigned to each ASIC also varies between switch models (i.e., there is more TCAM on a Cisco Catalyst 3750 than on a Cisco Catalyst 2960).

The limit of DACL support for Cisco Switches is 64 ACEs (64 lines). The best practice is to keep all DACLS to just a few lines.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Downloadable ACLs.

Step 2 Click **Add**.

Name = HR-ACL

Description = dACL for HR users (Enforcement Mode).

DACL Content =

```
Deny ip any <ip_address_range_of_engineering_servers>
permit ip any any
```

Warning: There is no syntax checking in Cisco ISE. If the DACL syntax is incorrect, it will not apply to the session.

Step 3 Click **Submit**.

Step 4 Repeat the entire procedure for each distinct role type.

Following is a screen shot of the final DACL list used in our example:



Procedure 2 Create wireless ACLs (wACLs) for each main role.

This procedure should be repeated for each role that will have a different Authorization. The wACL for an HR user is shown for reference.

Best Practice: For consistency, all wACLs should use the same name as the DACLs defined for wired access.

Step 1 Refer to the section “Create a wACL for Posture Assessment”.

Table 15: Rules for HR wACL

HR-ACL						
Sequence	Source	Destination	Protocol	DSCP	Direction	Action
1	Any	IP address 10.1.100.87 255.255.255.255	Any	Any	Any	Deny
2	Any	Any	Any	Any	Any	Permit

Procedure 3 Create additional Authorization Profiles for each main role.

This procedure should be repeated for each role that will have a different Authorization. For the purposes of documentation, we will step through the creation of the HR Authorization Profile, and then show the final screen with all the Authorization Profiles defined.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 2 Click **Add**.

Step 3 Complete the Authorization Profile with the following information:

```
Name = HR-Profile
Description = Authorization Profile for HR role (Enforcement Mode).
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☒ DACL Name = HR-ACL
☒ Wireless LAN Controller (WLC) = HR-ACL
```

Note: The Wireless LAN Controller (WLC) field is used to apply a Wireless ACL (wACL) that is locally defined on the WLC. WLCs do not support DACLs today. You configured the wACLs on the WLC in the “Create wireless ACLs (wACLs) for each main role. procedure.

Step 4 Click Submit.

Step 5 Repeat the entire procedure for each distinct role type.

Procedure 4 Create another Authorization Profile for Employees.

We have singled out this specific Authorization Profile to replace the current “Domain Users” Authorization Rule. This Authorization Profile and its associated rule will be used as a “catch all” for all employees who may not have been authorized by a more specific role.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.






Step 2 Click **Add**.

Step 3 Complete the Authorization Profile with the following information:

```
Name = Employee-Profile
Description = Authorization Profile for Employees (Enforcement Mode).
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☒ DACL Name = Employee-ACL
☒ Wireless LAN Controller (WLC) = Employee-ACL
```

Step 4 Click Submit.

Following is a screenshot of the final Authorization Profile list used in our example:

Standard Authorization Profiles		
		
		
<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Access-Points	AuthZ Profile For Access-Points. Permit All Traffic
<input type="checkbox"/>	AD_Machine_Access	AuthZ Profile For Windows Machine Auth.
<input type="checkbox"/>	Cisco_IP_Phones	Profile For Cisco Phones.
<input type="checkbox"/>	Contractor-Profile	AuthZ Profile For Contractor Access
<input type="checkbox"/>	DenyAccess	Default Network Authorization Profile with access type as Access-Reject
<input type="checkbox"/>	Domain_Users	AuthZ Profile To Provide Full-access To Any Domain User (Authenticated
<input type="checkbox"/>	Employee-Profile	AuthZ Profile For Employee's That Were Not AuthZ By More Specific Ru
<input type="checkbox"/>	Engineering-Profile	AuthZ Profile For Engineering Role (Enforcement Mode)
<input type="checkbox"/>	GUEST	AuthZ Profile For GUEST Role (Authentication Mode)
<input type="checkbox"/>	HR-Profile	AuthZ Profile For HR Role (Enforcement Mode)
<input type="checkbox"/>	PermitAccess	Default Network Authorization Profile with access type as Access-Accept
<input type="checkbox"/>	Sales-Profile	AuthZ Profile For Sales Role (enforcement Mode)
<input type="checkbox"/>	WEBAUTH	AuthZ Result For WebAuthentication
<input type="checkbox"/>	Whitelist	AuthZ Profile For Whitelisted Devices (Authenticated Mode)

Procedure 5 Adjust the Domain Computer Authorization.

In the Authenticated Mode phase of deployment, we created a Domain Computers Authorization Profile. At that point it permitted all traffic by using the PERMIT_ALL_TRAFFIC dACL, but in Enforcement Mode it should be locked down to only the required ports for those Windows Domain Members to communicate with Active Directory.

Step 1 Navigate to Policy → Policy Elements → Results → Authorization → Downloadable ACLs.

Step 2 Click **Add**.

Step 3 Complete the new DACL as follows:

Name = AD-Machine-ACL

Description = dACL used to permit Windows to communicate to AD for Machine Auth (Enforcement Mode).

DACL Content =

```

permit udp any eq bootpc any eq bootps !DHCP
permit udp any any eq domain !DNS
permit icmp any any !ICMP Ping
permit tcp any host 10.1.100.10 eq 88 !Kerberos
permit udp any host 10.1.100.10 eq 88 !Kerberos
permit udp any host 10.1.100.10 eq 123 !NTP
permit tcp any host 10.1.100.10 eq 135 !RPC
permit udp any host 10.1.100.10 eq 137 !NetBIOS-Nameservice
permit tcp any host 10.1.100.10 eq 139 !NetBIOS-SSN
permit tcp any host 10.1.100.10 eq 389 !LDAP
permit udp any host 10.1.100.10 eq 389 !LDAP
permit tcp any host 10.1.100.10 eq 445 !MS-DC/SMB
permit tcp any host 10.1.100.10 eq 636 !LDAP w/ SSL
permit udp any host 10.1.100.10 eq 636 !LDAP w/ SSL
permit tcp any host 10.1.100.10 eq 1025 !non-standard RPC
permit tcp any host 10.1.100.10 eq 1026 !non-standard RPC

```

Step 4 Create this same ACL on the WLC.

Step 5 Navigate to Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 6 Click AD_Machine_Access.

Step 7 Modify the Authorization Profile as follows:

```
Name = AD_Machine_Access
Description = Authorization Profile For Windows Machine Auth.
Access-Type = ACCESS_ACCEPT
-- Common Tasks
☒ DACL Name = AD-Machine-ACL
☒ Wireless LAN Controller (WLC) = AD-Machine-ACL
```

Procedure 6 Create additional Authorization Policy rules for each main role.

This procedure should be repeated for each role that will have a different Authorization. For the purposes of documentation, we will step through the creation of the HR Authorization, and then show the final screen with all the Authorization Policy rules defined.

Step 1 Navigate to Policy → Authorization.

Step 2 Insert a new Policy rule below the Whitelist rule.

Step 3 Name the rule HR-Rule.

Step 4 Leave Identity Group as **Any**.

Step 5 In the Other Conditions, choose: AD1:External Groups → Equals → HR.

Step 6 For the permissions, choose: **Standard** → HR-Profile.


Step 7 Click **Save**.

Step 8 Repeat the entire procedure for each distinct role type.

Procedure 7 Disable the Domain Users rule.

Step 1 Navigate to Policy → Authorization.

Step 2 Click the Green Arrow under Status, for the Domain Users Rule.

Step 3 Change to “ Disabled”.

Step 4 Click **Save**.

Step 5 The Final Rule table should be similar to the table below:

Table 16: Final Rule Table

Status	Rule Name		Identity Groups		Other Conditions		Permissions
<input checked="" type="checkbox"/>	Blacklisted	if	Blacklisted	and	Condition(s)	then	DenyAccess
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if	Cisco-IP-Phone	and	Condition(s)	then	Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Cisco APs	if	Cisco-Access-Point	and	Condition(s)	then	Access-Points
<input checked="" type="checkbox"/>	Whitelist	if	Whitelist	and	Condition(s)	then	Whitelist
<input checked="" type="checkbox"/>	HR Rule	if	Any	and	AD1:ExternalGroups EQUALS HR	then	HR-Profile
<input checked="" type="checkbox"/>	Engineering Rule	if	Any	and	AD1:ExternalGroups EQUALS Engineering	then	Engineering-Profile

Status	Rule Name		Identity Groups		Other Conditions		Permissions
<input checked="" type="checkbox"/>	Sales Rule	if	Any	and	AD1:ExternalGroups EQUALS Sales	then	Sales-Profile
<input checked="" type="checkbox"/>	Employee rule	if	Any	and	AD1:ExternalGroups EQUALS Employees	then	Employee-Profile
<input checked="" type="checkbox"/>	Contractor rule	if	Any	and	AD1:ExternalGroups EQUALS Contractors	then	Contractor-Profile
<input checked="" type="checkbox"/>	Machine Auth	if	Any	and	AD1:ExternalGroups EQUALS Domain Computers	then	AD_Machine_Access
x	Domain User	if	Any	and	AD1:ExternalGroups EQUALS Domain Users	then	Domain_Users
<input checked="" type="checkbox"/>	GUEST	if	GUEST	and	Condition(s)	then	GUEST
<input checked="" type="checkbox"/>	Default	if no matches, then			WEBAUTH		

Procedure 8 Consider moving to Multi-Domain Authentication (MDA) Mode.

As discussed in the “Authentication Settings – Flexible Authentication and High Availability” procedure, we configured the use of Multi-Auth. Multi-Auth mode will allow a virtually unlimited number of MAC addresses per switchport, and require an authenticated session for every MAC address. Multi-Auth is used to help prevent an accidental denial of service to users with unauthorized hubs in their cubical or other anomalies.

Now that the deployment has moved into the enforcement phase, it is recommended to use Multi-Domain mode because it is the most secure and provides the most value from a security perspective. Multi-Domain Authentication will allow a single MAC address in the DATA Domain and a single MAC address in the Voice domain per port.

Note: Future functions, such as MACsec (Layer 2 encryption between the endpoint and the switchport) requires Multi-Domain (MDA) or Single-Auth mode, and will not function in Multi-Auth mode.

Wireless: Bring Your Own Device

Configure Cisco ISE to Enable “Bring Your Own Device”

The advances in wireless technology and the proliferation of Wi-Fi-capable devices such as laptops, mobile phones, and tablets have made wireless security one of the biggest challenges for IT administrators. Not only do the IT administrators have to identify users connecting to the wireless network, they also need to be able to differentiate between users using corporate assets as opposed to users using personal assets on the corporate networks. Cisco TrustSec takes advantage of technologies such as IEEE 802.1X authentication and profiling to allow IT administrators to provide differentiated access on wireless networks in a scalable and operationally efficient manner. Cisco TrustSec uses Cisco ISE as a central policy-management server to help provide secure wireless networks and enables organizations to allow their users to bring their own devices (BYOD).

Organizations enabling BYOD, take one of 2 approaches:

1. Complete access to corporate resources over wireless networks – When users successfully authenticate via 802.1X, they are given access to all corporate resources. There are no checks to identify whether the device is a corporate-owned device or a personal device. Although this model is easy to maintain, there are very high risks associated with it.
2. Differentiated Access to corporate resources – Organizations implementing this model allow users restricted access to corporate resources on personal assets. If users are using a corporate-owned asset, they are given full access to corporate resources. Although this approach is a more secure one, it requires a high level of maintenance.

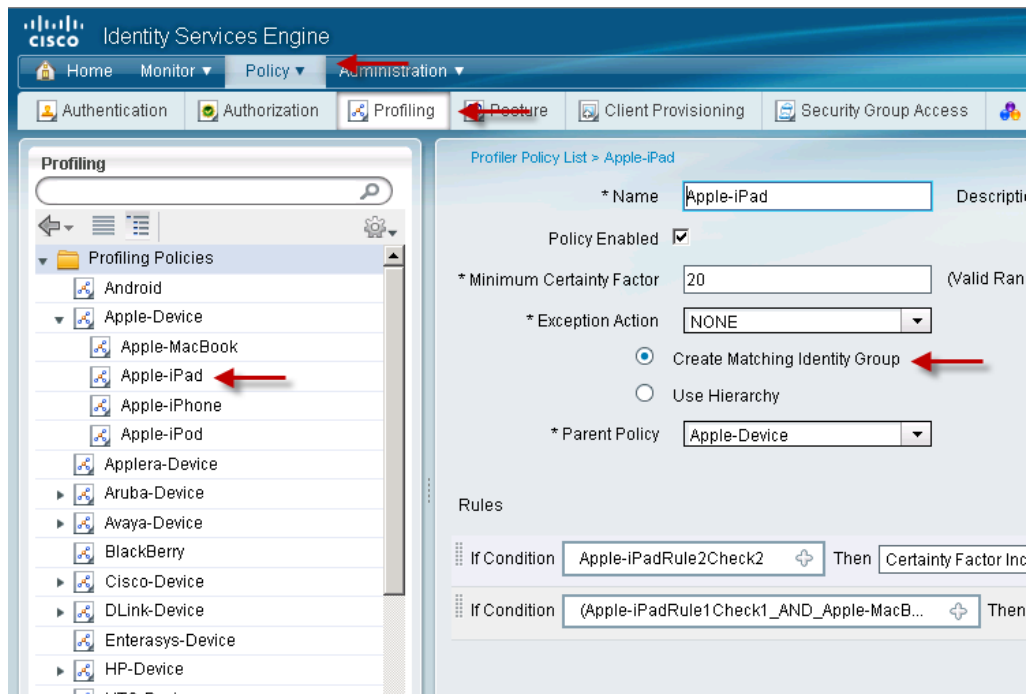
In the following section, we will walk through the steps of defining policies to provide employees with restricted access to corporate resources when they are using personal devices. For this demo, we will implement the following policy:

- Employees using corporate devices will get assigned to the Employee Authorization rule.
- Employees using personal devices will get guest access only. They will not be able to access corporate resources on personal devices.

To enforce the policy described, we will add all corporate devices to the whitelist group. The BYOD rule will specifically require employees to authenticate and be identified as domain users; in addition, they need to identify the devices they used, and they need to be a part of the whitelist. If both these rules are met, the users are assigned the employee Authorization rules. Personal devices will be identified using profiling and will be assigned to Guest access.

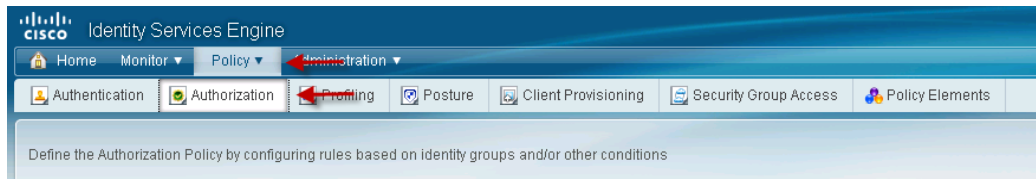
Procedure 1 Enable endpoint identity groups for profiled devices.

Step 1 Refer to the section on [creating Identity Groups based on profiling services](#) and enable id groups for Apple iPads, iPhones, iPods, Android devices, Blackberry phones, etc.

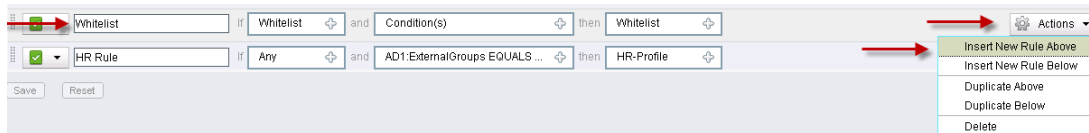


Procedure 2 Create new Authorization rules for BYOD policies.

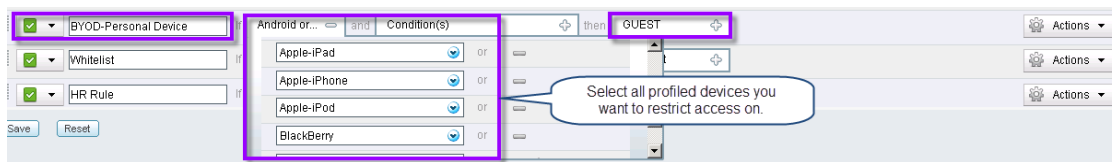
Step 1 Navigate to Policy → Authorization.



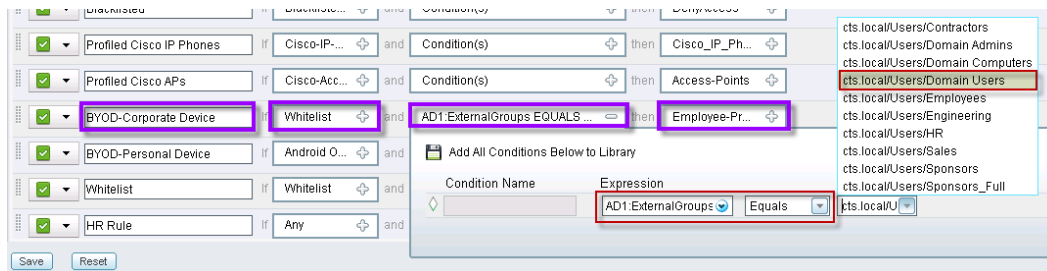
Step 2 Add a new rule above the Whitelist rule.



Step 3 Create the following rule for personal devices on the network:



Step 4 Add the BYOD-Corporate Device rule given previously regarding the BYOD-Personal Device for employees using corporate devices.



Step 5 Save the Changes.

Note: Using certificates to differentiate corporate devices from personal devices will be covered in the Cisco TrustSec 2.1 release.

Cisco IP Phones

Out of the box, Cisco IP Phones are capable of 802.1X, but they are not enabled for 802.1X. This decision was made to preserve backward compatibility with older releases of code. Although Cisco IP Phones can be enabled for 802.1X manually using the phone keypad, this process is not scalable when deploying large numbers of phones.

For scalability and ease of deployment, phones should be enabled for 802.1X via the network. Starting with Cisco Unified Communications Manager 7.1.2, it is possible to enable 802.1X on phones by enabling 802.1X in the phone configuration file or via the Bulk Administration Tool on the Cisco Unified Communications Manager. The next time the phone resets and downloads its configuration file, 802.1X will be enabled for all supported EAP methods.

Cisco IP Phones may use password-based (EAP-MD5) or certificate-based (EAP-TLS or EAP-FAST) authentication. Certificates are the recommended authentication method with either EAP-TLS or EAP-FAST.

Note: Phones Have Long User Names.

IP phones have usernames that are usually 24 characters long. Some AAA servers and back-end directory servers (including Active Directory) have trouble with usernames that exceed 20 characters. Be sure that your AAA server can support the length of the hardcoded IP Phone name.

Cisco ISE 1.0 supports usernames up to 25 characters. Some IP Phones may have a username that is longer than the 25 characters supported by Cisco ISE 1.0. (Example: CP-7961G-GE-SEP001AA163AF AE). For this and other reasons, EAP-MD5 is not recommended for production deployments of Cisco TrustSec 1.0.

Best Practice Tip: Configure Cisco ISE to Request the Preferred EAP Method.

There is no way to disable individual EAP methods on a Cisco IP Phone. Therefore, the phone will accept any EAP method that the Cisco ISE requests. So, for example, if Cisco ISE requests EAP-MD5, the phone will accept that method, even if a password has not been configured. If a password was not configured, the phone will fail EAP-MD5 authentication, even if the phone has a valid certificate and is capable of EAP-FAST or EAP-TLS. To avoid this situation, configure Cisco ISE to request only the preferred and most secure EAP method when authenticating a phone.

Certificates

Cisco IP Phones are shipped with a certificate preinstalled during the manufacturing process. This certificate is known as a Manufacturing Installed Certificate (MIC). This certificate is an X.509 certificate that has been signed by the Cisco Manufacturing Certificate Authority. This certificate is normally used to secure the signaling and voice path used for IP Telephony, but these same certificates may be used for 802.1X.

The MIC may be used for authentication with 802.1X. A phone that presents a valid MIC can be assumed to be a valid Cisco phone. However, the MIC by itself cannot be used to determine if this phone is a corporate asset or a rogue Cisco phone. For that, you need a Locally Significant Certificate (LSC). Unlike the MIC, the LSC is signed by the Certificate Authority Proxy Function (CAPF) of the Cisco Unified Communications Manager – which is the central call control and configuration engine for Cisco IP Telephony.

Note: Self-signed CAPF vs. CA-signed CAPF:

Cisco Unified Communications Manager can sign LSCs using two different types of CAPF: self-signed CAPF or CA-signed CAPF. A self-signed CAPF acts as a standalone CA, signing the LSCs with its own self-signed certificate. A CA-signed CAPF, on the other hand, is signed by an external Certificate Authority. A CA-signed CAPF signs the LSCs with the externally signed certificate in a subordinate-like manner.

Self-signed CAPF CAs have a lifetime of 5 years. Therefore, if you use a self-signed CAPF, the CAPF certificate must be renewed after 5 years and all the LSCs will have to be reissued. Cisco ISE will not allow the phones network access if the LSCs have expired.

The lifetime of the CA-signed CAPF is determined by the CA when it issues the certificate to Cisco Unified Communications Manager. Whatever lifetime you choose, be sure to renew the CAPF certificate and reissue the LSCs prior to expiration.

Because the LSC has been issued by your own Cisco Unified Communications Manager Certificate Authority, you can be certain that a phone presenting a valid LSC is, in fact, a corporate-owned and -managed asset.

Best Practice: Use the MIC to allow new phones limited access to the network. This limited access will allow a new phone to reach the Cisco Unified Communications Manager, where an LSC may be issued to the phone. When the phone has an LSC, it will be granted full network access.

Note: To deploy LSCs, Cisco Unified Communications Manager first must be enabled for Certificate Authority Proxy Functions (CAPF). Configuring CAPF is a multistep process that is not covered in this document. For full details on how to deploy CAPF, see the Cisco Unified Communications Security Guide.

Configure 802.1X on Cisco IP Phones

Cisco ISE is responsible for validating the certificate provided by the phone. To do this, Cisco ISE must have a copy of the root CA certificate that signed the phone certificate. The root certificates for both Locally Significant Certificates (LSCs) and Manufacturing Installed Certificates (MICs) can be exported from the Cisco Unified Communications Manager Operating System Administration interface and imported into your AAA server.

When the certificate is validated, Cisco ISE server may be able to authorize the phone based simply on attributes in the certificate. This way is the recommended way to authorize phones with certificates, because it enables you to authenticate and authorize phones with a single global policy and avoids the need to enter individual phones in a database. Cisco ACS supports this type of authorization, but not all AAA servers do.

Best Practice Recommendation: Use Certificate Attributes for Phone Authorization.

Using certificate attributes to authorize phones avoids the need to enter individual phones in a database, thus significantly reducing the effort needed to deploy 802.1X for phones. Cisco ISE supports certificate attribute-based authorization for EAP-TLS.

Note: Only the attributes of the certificate subject can be used in an authorization policy. The issuer's attributes cannot be used.

Procedure 1 Generate the CAPF Certificate Signing Request (CSR).

To use a certificate from your enterprise CA, instead of the self-signed certificates from Cisco Unified Communications Manager, you must obtain both the signed CAPF certificate and the CA root certificate from the CA. These procedures will show an example using a Windows 2008 Certificate Authority. For other CAs, please locate instructions from the documentation for that CA.

CAPF Certificate Signing Requests (CSRs) include extensions that you must include in your request for an application certificate from the CA. If your CA does not support the ExtensionRequest mechanism, you must enable the X.509 extensions that are listed on the final page of the CSR generation process.

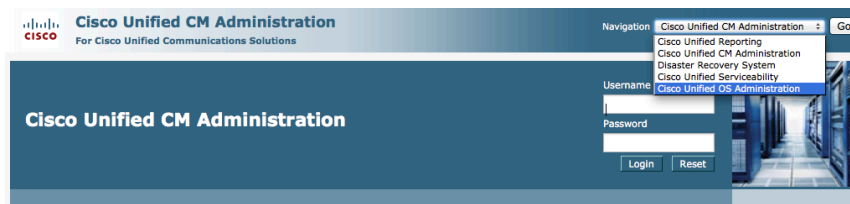
Note: For CAPF, it is required to obtain and upload a CA root certificate and an application certificate only on the first Cisco Unified Communications Manager node.

CAPF and Cisco Unified Communications Manager CSRs include extensions that you must include in your request for an application certificate from the CA. If your CA does not support the ExtensionRequest mechanism, you must enable the X.509 extensions as follows:

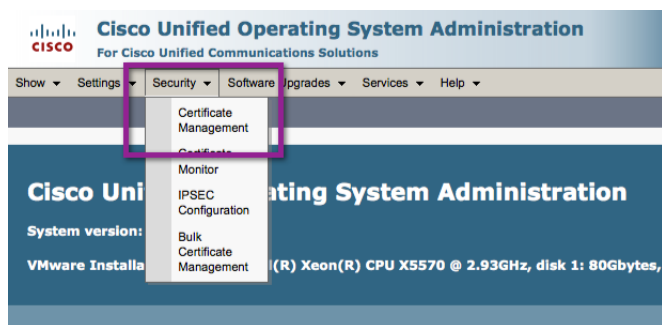
The CAPF CSR uses the following extensions:

- X509v3 extensions:
- X509v3 Key Usage:
- Digital Signature, Certificate Sign
- X509v3 Extended Key Usage:
- TLS Web Server Authentication, IPsec End System

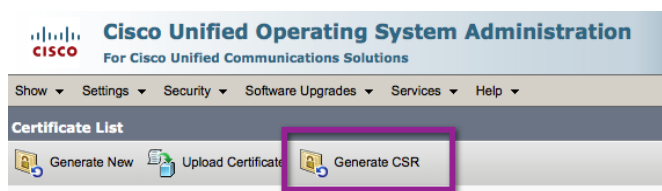
Note: There are multiple GUIs for Cisco Unified Communications Manager. You must log into the Cisco Unified Communications Manager "Operating System Administration" GUI.



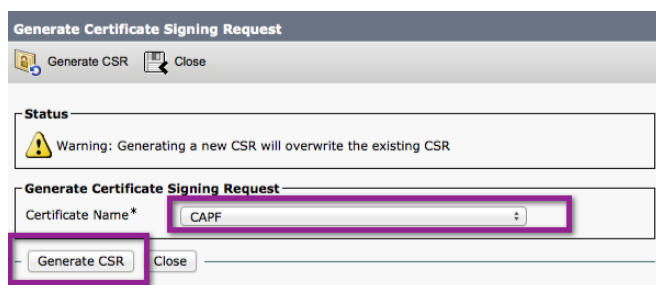
Step 1 In the Cisco Unified Communications Manager Administration GUI: choose **Security** → **Certificate Management**.



Step 2 Click the “Generate CSR” button.



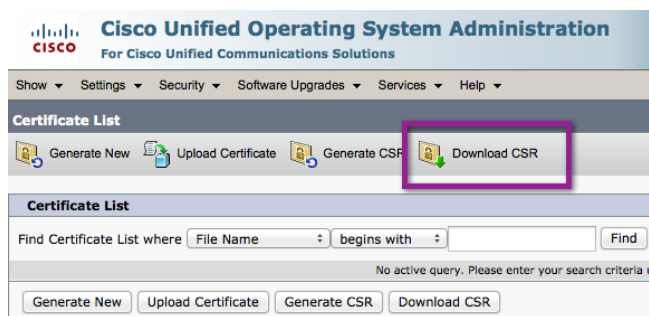
Step 3 The Generate Certificate Signing Request pop-up window should appear. In the Certificate Name drop-down menu, select “CAPF”.



Step 4 Click the **Generate CSR** button.

Step 5 Click **Close**.

Step 6 Click the **Download CSR** button.



Step 7 Ensure CAPF is selected in the drop-down menu, and click the **Download CSR** Button in the resulting pop-up window.



Step 8 Save the resulting .csr file to an easily accessible location.

Procedure 2 Obtain a Certificate from the CA.

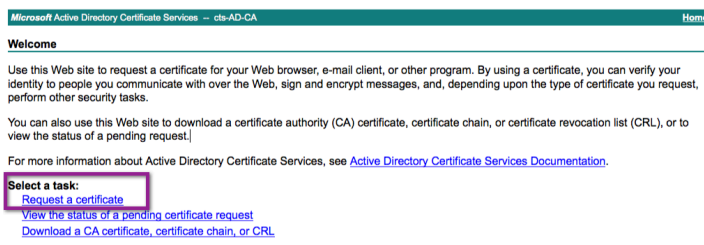
In this section, we will submit the CSR to the Certificate Authority, and download the resulting Certificate.

Step 1 Open the .csr file with a text-editing application.

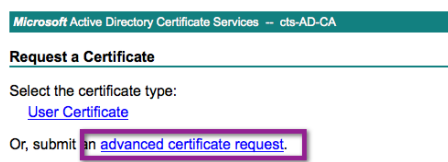
```
-----BEGIN CERTIFICATE REQUEST-----
MIIB2zCCAUCQAQAwKjEwMBQGA1UEAwN0Q0R111NzMhMTA0NzEMMAoGA1UECwwD
YZx0MQ4wDQYDVQQKDAVjaXNjb2ZEMMAoGA1UEBwwDBGFlMQswCQYDVQQIDAJ0QzEL
MAkGA1UEBhMCVWwmgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAIBSWNzAHWDF
zsnPvatrKqMlZ5M4evrraFqudyvNvzTfJTCF1caf08T0ZEsuQapDvJFSUCo9KyeWm
aMdlGjGZ+mVnA6gkjpMbQ675gCarHvrj3ShxFTmoQ0L1hZLPHf6dPpd1nuB+Kg
heHGPKJZkU48TD4oKUpDnK9hXLQXkmnAgMBAAGgPTA78gkqkqkL69w0BCQ4xLjAs
MASGA1UdDwQEAwIChDAdBgNVHSUEfjAUBgggrBgEFBQcDAQYTKwY8QUHAWUdQYJ
KoZIhvcNAQEFBQADgYEAZP/RDe3CwopRbudpuoj6Ym19XxkS9zkk/6cBjGgjsD0z
suW+tbRlK+4Cjxo2rU7HZROhAgvqV3VX311UZi8JxBS1aoZfd31Oqc/SX7fQKbDF
SPp0Mm/Sc/zWcSt+OVNbkIPDSJHFg7Bx0rra/sjnp2Ao/6twzCwE2kZ5u9M1X4=
-----END CERTIFICATE REQUEST-----
```

Step 2 Copy all the text to your clipboard.

Step 3 On the CA webpage, choose **Request a Certificate**.



Step 4 Select "advanced certificate request".



Step 5 Paste the contents of the CSR file into the “Saved Request” section. Select “**Web Server**” from the Certificate Template drop-down menu.

Microsoft Active Directory Certificate Services -- cts-AD-CA

Submit a Certificate Request or Renewal Request

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

Saved Request:

```
heHGPKJ2xU40ID4oKUrDnK9hXLQXkmnAgMBAAGg:
MasGA1UdDwQEAwICDAdBgNVHSUEFjAUBgggrBgEF:
certificate request KoZlthvcNAQEFBQADgYEAZP/RDe3CowpRbudpuoj6:
(CMC or suW+LbRIK+4Cjxo2rU7H2R0hAGyqV3VX311UZi8J:
PKCS #10 or SPp0Mmn/Sc/zWcST+OVNbkIPD5JHFg7Bx0rra/sj:
PKCS #7): -----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes: X509v3 extensions: X509v3 Key Usage:

Submit >

Step 6 Paste the following into the Additional Attributes field:

```
X509v3 extensions:
X509v3 Key Usage:
Digital Signature, Certificate Sign
X509v3 Extended Key Usage:
TLS Web Server Authentication, IPSec End System
```

Step 7 Click Submit.

Step 8 Click Download certificate.

Microsoft Active Directory Certificate Services -- cts-AD-CA

Certificate Issued

The certificate you requested was issued to you.

☒ DER encoded or ☐ Base 64 encoded

[Download certificate](#)

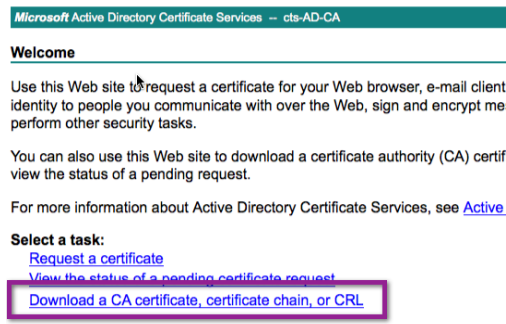
[Download certificate chain](#)

Step 9 Save the resulting .cer file somewhere to an easily accessible location.

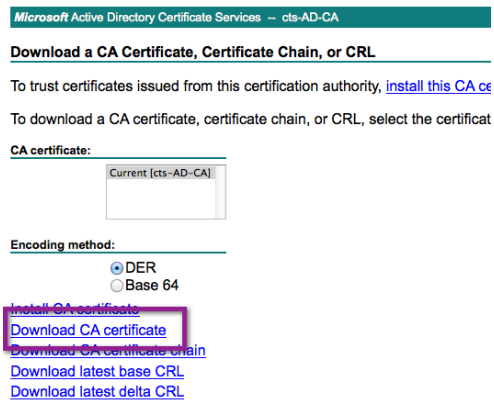
Procedure 3 Download and install the Root CA Certificate.

In this section, we will download the Certificate-Authority Root Certificate. We will then import the certificate to Cisco Unified Communications Manager, as the CAPF-Trust Certificate.

Step 1 From the Microsoft CA Home Screen, select Download a CA certificate, certificate chain, or CRL.

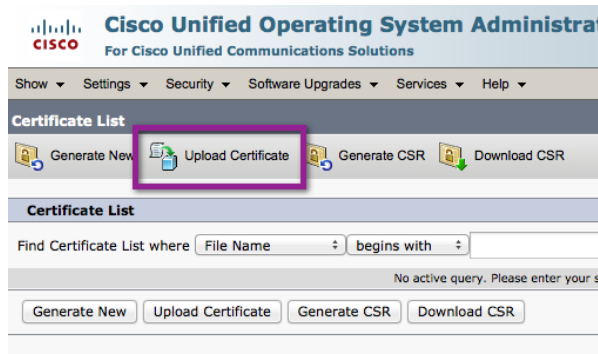


Step 2 Select Download CA certificate.



Step 3 Save the CA certificate somewhere easily accessible.

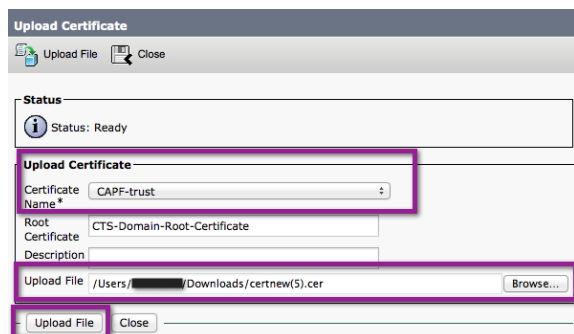
Step 4 From the Cisco Unified Communications Manager Certificate Management Screen, click the **Upload Certificate** button.



Step 5 In the Certificate Name drop-down menu, choose **CAPF-trust**.

Step 6 Click Browse.

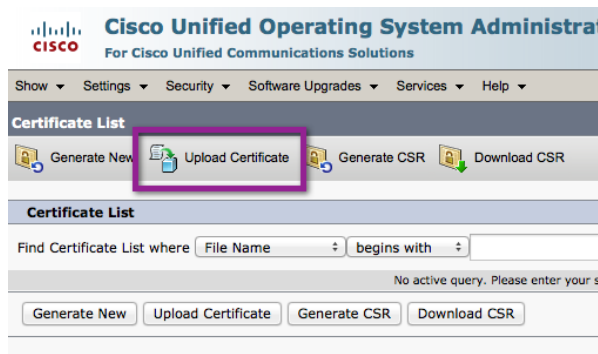
Step 7 Select the .cer file downloaded in Step 2.



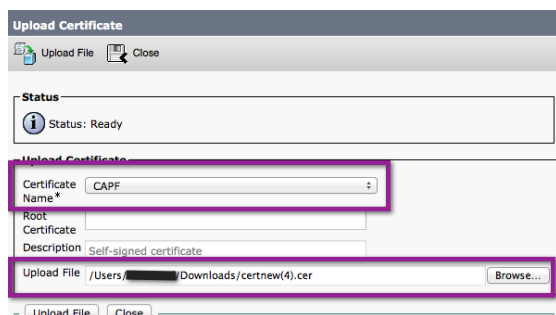
Step 8 Click Upload File.

Procedure 4 Import the CAPF application certificate into Cisco Unified Communications Manager.

Step 1 Click Upload Certificate.



Step 2 In the Certificate Name drop-down menu, select **CAPF**.



Step 3 Click **Browse**.

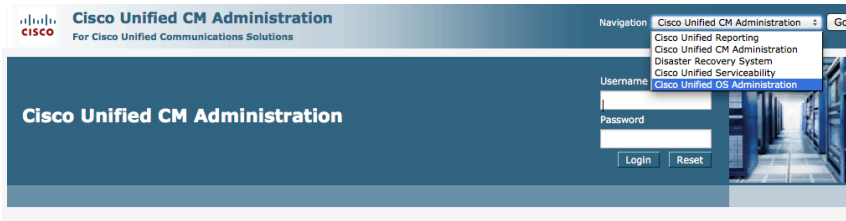
Step 4 Select the .cer file that was issued by the CA for CAPF.

Step 5 Click Upload File.

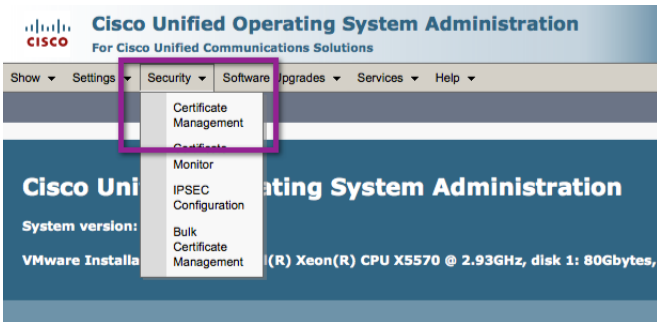
Procedure 5 Export Certificates from Cisco Unified Communications Manager.

In this section, root Certificate Authority Certificates are exported from Cisco Unified Communications Manager (to be imported into Cisco ISE in the next section).

Note: There are multiple GUIs for Cisco Unified Communications Manager. You must log into the Cisco Unified Communications Manager “Operating System Administration” GUI.



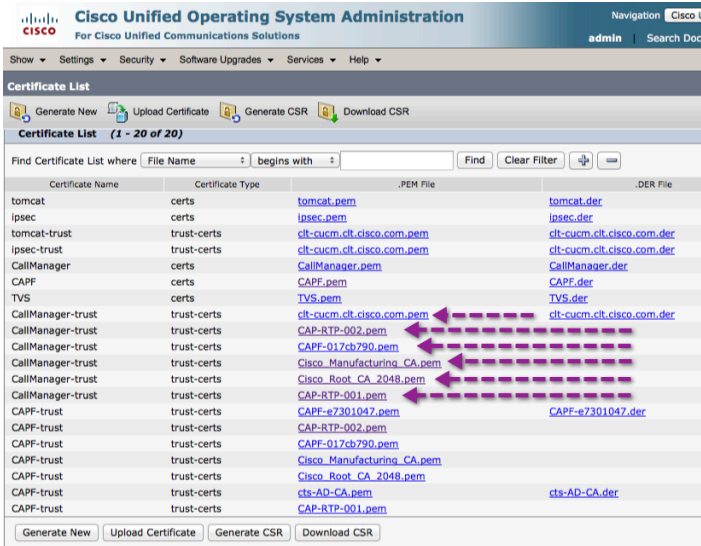
Step 1 In the Cisco Unified Communications Manager Administration GUI, choose **Security** → **Certificate Management**.



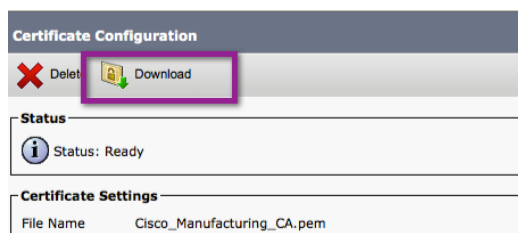
Step 2 Click **Find**.

Step 3 Download each of the certificates trusted by Cisco Unified Communications Manager.

They will be labeled “CallManager-trust” in the Certificate Name column. For each required certificate, select the name of the certificate in .PEM format and save them somewhere easily accessible.



Step 4 When the certificate configuration window displays, click **Download**. When prompted, save the certificate.



Step 5 Repeat for each required certificate.

Note: If authenticating phones using MICs, the required certificates may include: Cisco_Root_CA_2048, Cisco_Manufacturing_CA, CAP-RTP-001, and CAP-RTP-002. If authenticating using LSCs, the required certificates will depend on your CAPF deployment. The CAPF CA in the previous example is "CAPF-e7301047.pem". The actual name of your CAPF CA will vary.

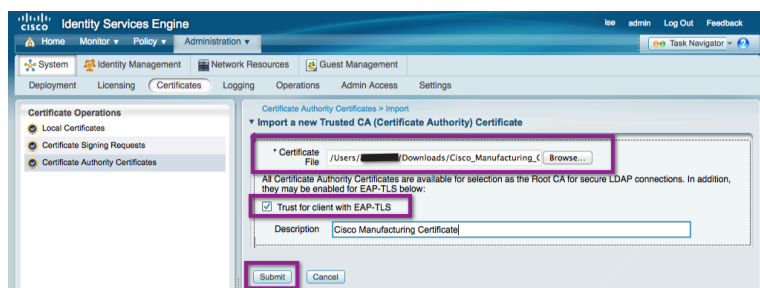
Procedure 6 Import Certificates into Cisco ISE.

Similar to what we accomplished in the "General Settings – Certificates and Certificate Authorities" section, we will import the Cisco Unified Communications Manager root Certificates into Cisco ISE as trusted root certificates.

Step 1 In the Cisco ISE Administration GUI, navigate to Administration → System → Certificates → Certificate Authority Certificates.

Step 2 Click **Add**.

Browse for one of the certificates saved in the previous "Export Certificates from Cisco Unified Communications Manager." procedure.



Step 3 Select Trust for client with **EAP-TLS**.

Step 4 Click Submit.

Repeat this procedure for each of the certificates downloaded in the previous "Export Certificates from CUCM" procedure.

Procedure 7 Enable 802.1X per Device.

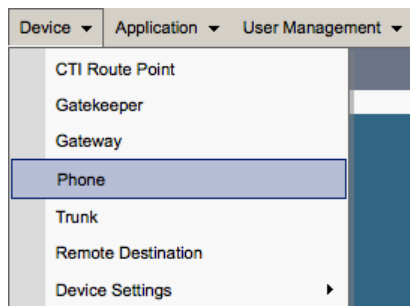
Follow the steps in this procedure if you are configuring a single phone or only a few phones. For multiple phones at once, it is recommended to use the Bulk Administration Tool (BAT). The table below lists the Cisco IP Phones and their firmware versions to support 802.1X with certificates.

Table 17: Cisco IP Phones That Support 802.1X Certificates

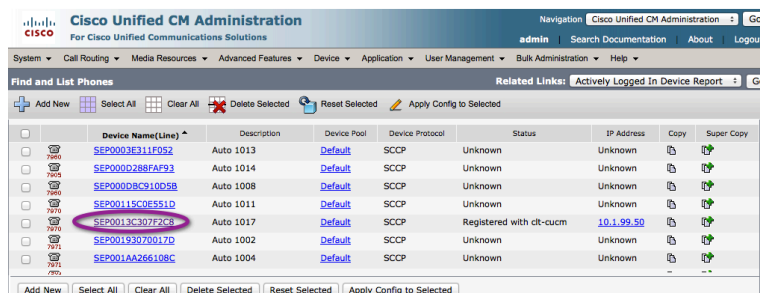
Cisco IP Phone Model	Minimum Firmware for X.509 Certificate-Based 802.1X Using EAP-TLS or EAP-FAST	Recommended Firmware for 802.1X
7906, 7911	8.5(2)	9.0(3)
7931, 7937	8.5(2)	9.0(3)
7941, 7942-G, 7945-G	8.5(2)	9.0(3)
7961, 7962-G, 7965-G	8.5(2)	9.0(3)
7970, 7971, 7975-G	8.5(2)	9.0(3)
All newer Cisco IP Phones should support X.509 Certificated-based 802.1X		

Note: There are multiple GUIs for Cisco Unified Communications Manager. You must log into the Cisco Unified "CM Administration" GUI.

Step 1 In the Cisco Unified Communications Manager Administration UI, choose **Device** → **Phone**.



Step 2 The Find and List Phone window displays. Find and select the phone you wish to enable for 802.1X.



Step 3 The Phone Configuration window appears.

Step 4 Scroll down to the line titled “802.1X Authentication.” From the drop-down menu, select **Enabled**.

The screenshot shows the 'Phone Configuration' window in the Cisco Unified CM Administration interface. The '802.1X Authentication' dropdown menu is set to 'Enabled' and is highlighted with a red box. Below it, the 'Detect Unified CM Configuration Failure' dropdown is set to 'Normal'. Other settings include 'Cisco Discovery Protocol (CDP): PC Port' (Enabled), 'Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port' (Enabled), 'Link Layer Discovery Protocol (LLDP): PC Port' (Enabled), 'LLDP Asset ID' (Unknown), 'IPv6 Load Server' (Unknown), 'IPv6 Log Server' (Unknown), 'Minimum Ring Volume' (0-Silent), 'Headset Sidetone Level' (Use Phone Default), 'HTTPS Server' (http and https Enabled), 'Enbloc Dialing' (Enabled), 'Switch Port Remote Configuration' (Disabled), 'PC Port Remote Configuration' (Disabled), and 'Automatic Port Synchronization' (Disabled). The 'Save' button at the bottom left and the 'Apply Config' button at the bottom center are also highlighted with red boxes.

Step 5 Click **Save** and then **Apply Config**.

Procedure 8 Deploying Locally Significant Certificates.

In this section, the Cisco Unified Communications Manager administrative interface is used to install an LSC on an IP Phone. This section is required only when using 802.1X-capable Cisco IP Phones.

Note: To deploy LSCs, Cisco Unified Communications Manager first must be enabled for Certificate Authority Proxy Functions (CAPF). Configuring CAPF is a multistep process that is not covered in this document. For full details on how to deploy CAPF, see the Cisco Unified Communications Security Guide.

Step 1 In the Cisco Unified Communications Manager Administration user interface, choose **Device** → **Phone**.

Step 2 The Find and List Phone window displays. Find and select the phone to which a certificate should be deployed.

Step 3 The Phone Configuration window appears.

Step 4 Scroll down to the section entitled Certificate Authority Proxy Function (CAPF) Information.

The screenshot shows the 'Certification Authority Proxy Function (CAPF) Information' window. The 'Certificate Operation' dropdown is set to 'Install/Upgrade'. The 'Authentication Mode' dropdown is set to 'By Existing Certificate (precedence to LSC)'. The 'Authentication String' field is empty. The 'Key Size (Bits)' is set to 1024. The 'Operation Completes By' date and time are set to 2011 9 29 12 (YYYY:MM:DD:HH). The 'Certificate Operation Status' is 'Operation Pending'. The 'Note' at the bottom states: 'Security Profile Contains Addition CAPF Settings.'

Step 5 Under Certificate Operation, select Install/Upgrade.

Step 6 Under Authentication Mode, select By Existing Certificate (precedence to LSC).

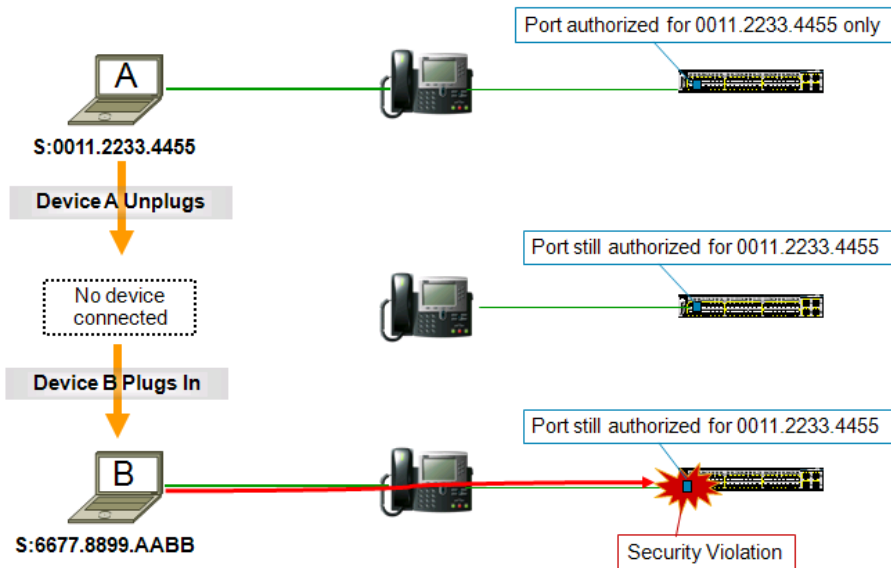
Step 7 Under Operation Completes By, enter the date and time the certificate should be deployed.

Step 8 Click Save and then Apply Config to begin the process of enrolling a certificate for the phone.

Device Behind Phone Disconnects: The Link State Problem

If the device unplugs from behind the phone, the switch cannot rely on link state to know when to clear the session. Dangling sessions can lead to security violations and security holes. Consider the situation illustrated in Figure 23.

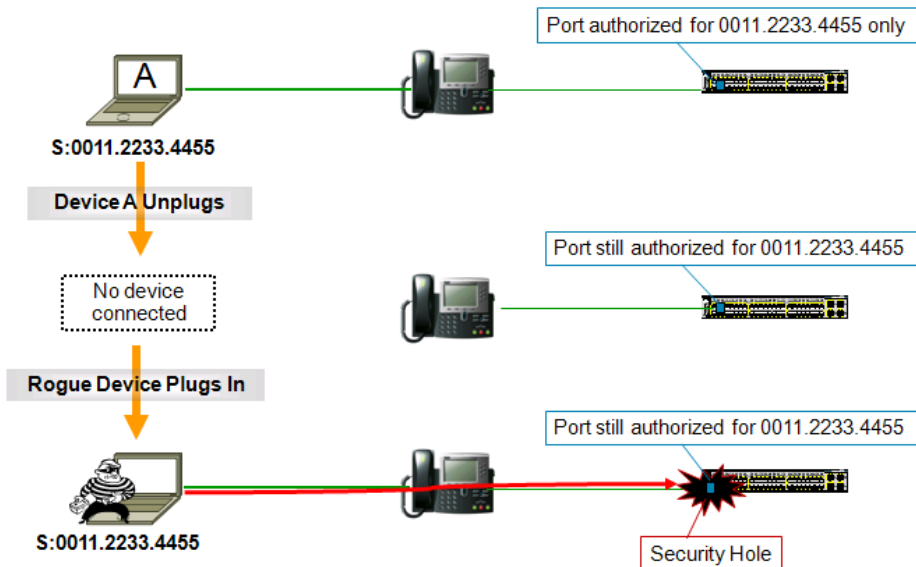
Figure 23 Link State Problem 1: Authorized User B Triggers Security Violation



In the figure, Device A has previously authenticated behind the IP Phone. Device A unplugs, but the switch, not knowing A has left, keeps the port authorized for the Device A MAC address only. Sometime later, Device B plugs in and sends traffic. Because there is still an existing session for Device A, the switch does not attempt to authenticate Device B. From the perspective of the switch, Device B is an unauthorized device that may be trying to piggyback on the authenticated session of device A. Therefore, the switch immediately triggers a security violation.

Another consequence of not removing an authenticated session when the data device disconnects from behind the phone is a security hole that could be exploited by a rogue user. This security hole is illustrated in Figure 24.

Figure 24: Link State Problem 2: Rogue User Spoofs Authenticated User's Session



In the figure, Device A has previously authenticated behind the IP Phone. Device A unplugs, but the switch, not knowing A has left, keeps the port authorized for the MAC address of device A. Sometime later, a rogue user

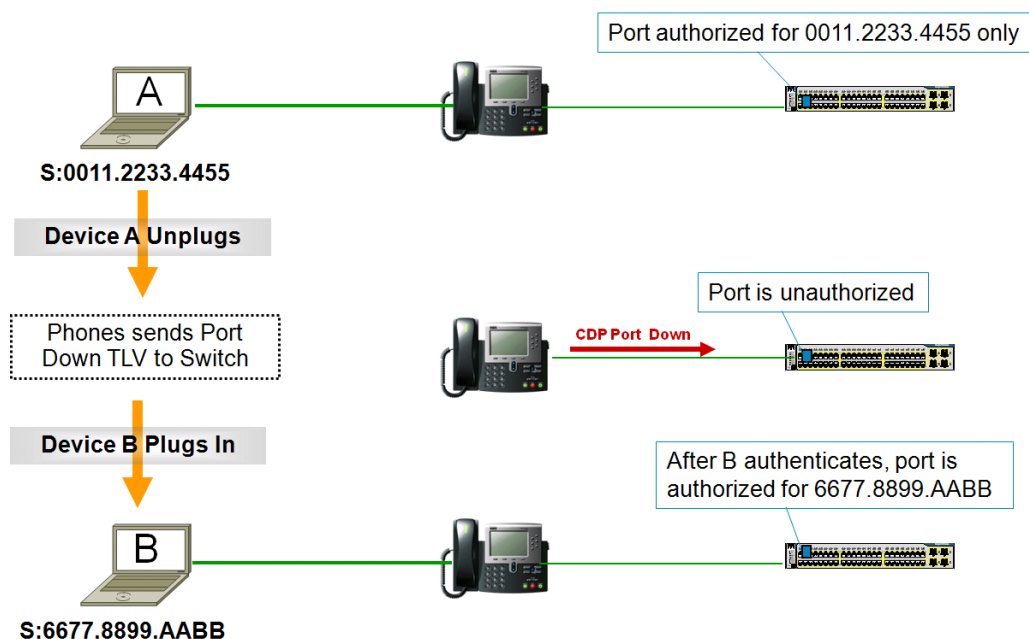
plugs in and spoofs the MAC address of device A. Because there is still an existing session for Device A, the switch allows all traffic from the rogue device without forcing the rogue device to authenticate.

To avoid security violations and security holes, some method must be used to clear the session for the data domain. This section discusses three possible solutions, in order of preference. One or more of these methods must be operational to ensure smooth integration of IP Telephony and 802.1X.

Cisco Discovery Protocol Enhancement for Second Port Disconnect

The best solution for the lack of direct link state awareness is to address the root cause. The switch does not know the link state of the phone data port ("the second port"), but the phone does. Therefore, if the phone could communicate link state to the switch, then the switch could immediately clear the session. This communication is exactly what the Cisco Discovery Protocol Enhancement for Second Port Disconnect (aka "Host Movement Detection") does. Cisco IP Phones can send a Cisco Discovery Protocol message to the switch indicating that the link state for the data device port is down, allowing the switch to immediately clear the session of the data device (Figure 25).

Figure 25: Recommended Link State Solution: Cisco Discovery Protocol Enhancement for Second Port Disconnect



Cisco IP Phones and Cisco Catalyst switches with the appropriate releases of code automatically perform Cisco Discovery Protocol Enhancement for Second Port Disconnect. It works for all authentication methods (802.1X, MAB, Web-Auth), and no configuration is required.

Best Practice Recommendation: Use Cisco Discovery Protocol Enhancement for Second Port Disconnect

This feature works for all authentication methods, takes effect as soon as the device disconnects, and requires no configuration. If you are using Cisco IP Phones and Cisco Catalyst switches with the appropriate release of code, this solution is the simplest and most effective one. No other method works as well to address the inability of the switch to detect link state for devices connected behind IP Phones.

Expanded Services

Introduction to Security Group Access

Security Group Access architecture provides security group-based access control using security group-based tags (SGTs). The previous sections described how users and devices successfully authenticate to the network using 802.1X and gain network access via authorization options such as VLANs and downloadable ACLs. These methods are *ingress* access control methods.

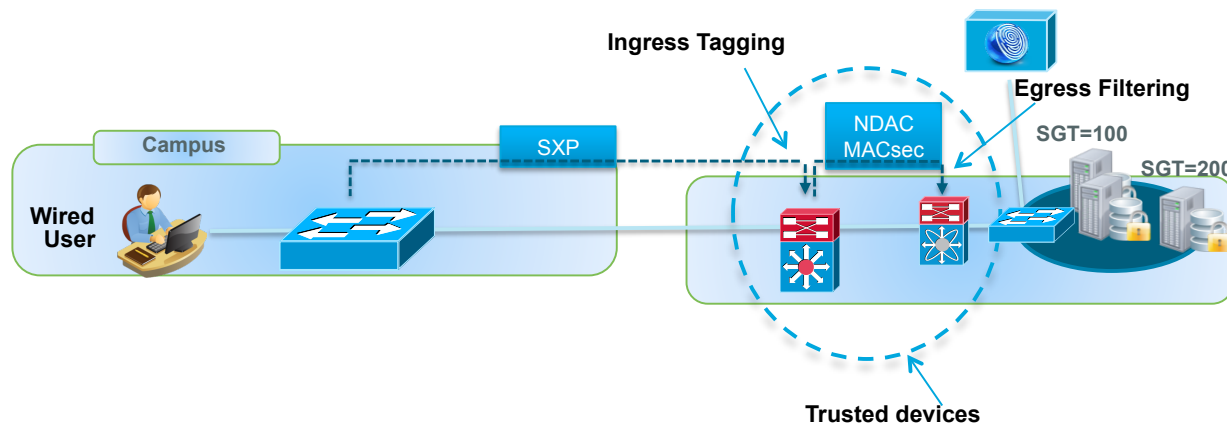
Alternatively, by using security group tags (SGTs) to tag user traffic with role information, identity information may be carried throughout the network and used by devices deeper in the network for policy control rather than gating access entirely at the entry point to the network.

SGTs allow enterprises to build simple role-based access policies that are topology independent and provide operational flexibility compared to VLANs and downloadable ACLs. Additionally, specific resources that are being accessed can in turn be grouped into security groups to simplify operations.

SGA architecture builds a trusted network infrastructure. The basic idea is to have the devices authenticate each other to prevent any rogue entity from joining the network. The authentication process between devices is called Network Device Admission Control (NDAC). It creates a circle of trusted devices by allowing only authenticated switches entry into the network. NDAC uses EAP-FAST to authenticate these switches to Cisco ISE so they can obtain SGT and other identity information.

SGA architecture also secures the network by providing encryption at Layer 2 via MACsec (802.1AE). Traffic is encrypted from switch to switch or, in other words, hop by hop. This means that packets are encrypted on egress for transmission then decrypted on ingress where they can be inspected within the switch. (Figure 26).

Figure 26: SGA with MACsec Provides Hop-By-Hop Encryption



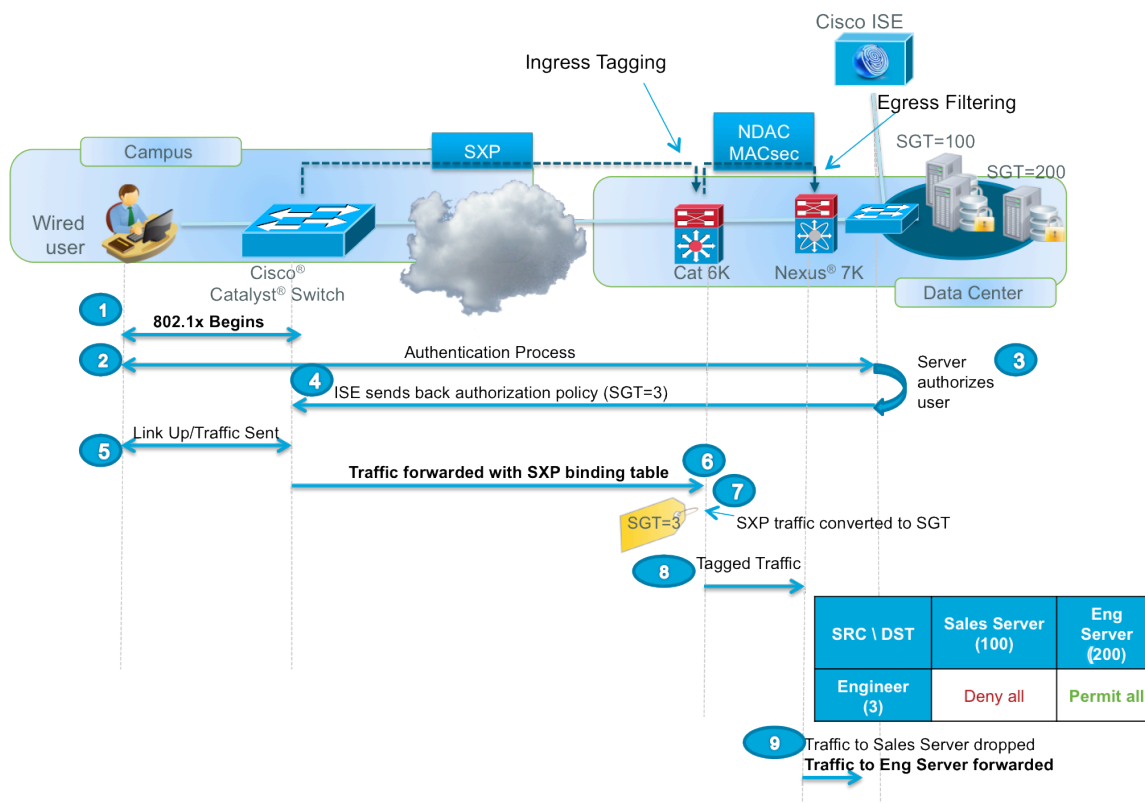
How Security Group Access works in conjunction with existing infrastructure and identity deployments, common use cases, and the configuration of these use cases is shown in the following sections.

SGA Use Cases

Access Layer to Data Center

This use is the most common use of SGTs and SGACLs. In this case, different users log in to the network to access resources in the data center. SGA is used to classify traffic from a specific user role dynamically assigned via user authentication by tagging. This tagged traffic is going to be filtered at the egress port of the switch in the Data center. Because the SGT assignment is done at ingress and filtering is done at egress, SGA technology can be used with any authenticated and identity deployment method. Figure 27 shows how this use is possible.

Figure 27: SGA's Ingress Tag Assignment and Egress Enforcement



Step 1 The supplicant sends an EAPOL-start that initiates EAP-ID exchange.

Step 2 Here the user's credentials are sent to Cisco ISE.

Step 3 Cisco ISE authenticates the user and assigns an authorization policy based upon user context.

Step 4 The Authorization policy contains the SGT assigned and may also include a DACL or VLAN.

Step 5 User's traffic is forwarded.

Step 6 The IP-to-SGT (end user's IP mapped to SGT=3) binding table is forwarded from the access switch to the distribution switch; in this case it is the Cisco Catalyst 6500 switch with Supervisor Engine 2T, via SXP.

Step 7 The Cisco Catalyst 6500 switch with Supervisor Engine 2T takes the IP-SGT mapping, takes the user's incoming packets based on source IP address, and then inserts the SGT to propagate to the next hop.

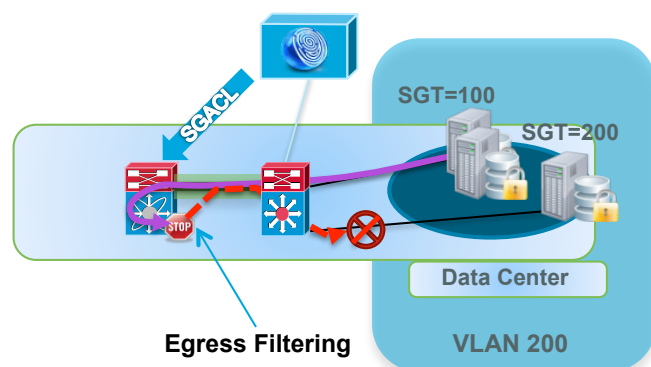
Step 8 The Cisco Catalyst 6500 switch forwards the tagged packets (SGT=3) out the supervisor uplink port to the Cisco Nexus 7000 switch.

Step 9 The Cisco Nexus 7000 switch filters traffic based upon SGACLs.

Intra-Data Center Enforcement

Security Group Access allows you to dynamically control server-to-server communication without defining a static access list on the switch. In the following example, there are multiple servers in the data center. We are going to use SGTs to tag each server and to use SGACLs to enforce traffic between them. Security Group Access allows you to dynamically control server-to-server communication without defining a static access list on the switch. So regardless of whether the servers are on the same subnet or different subnets, SGACLs can be used to filter traffic between them (Figure 28).

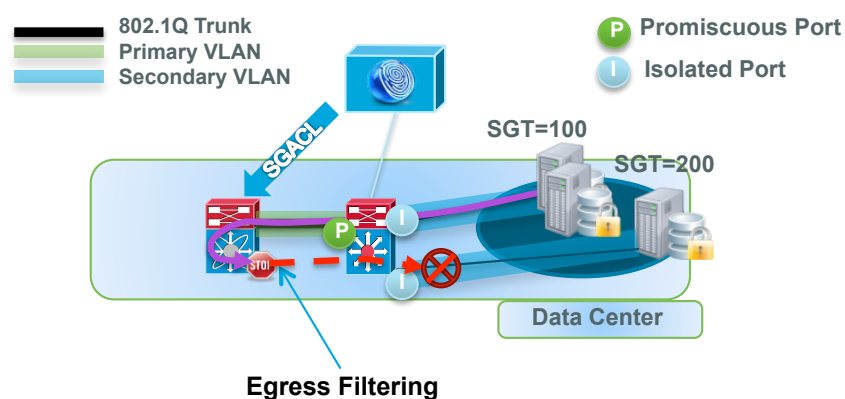
Figure 28: Egress Filtering



Data Center Use Case Configuration

Previously there were two use cases shown. We are going to first set up the data center use case because the server SGTs will also be used for the campus to data center use cases. A more detailed diagram of the traffic flow is shown in Figure 29.

Figure 29: SGA Egress Filtering

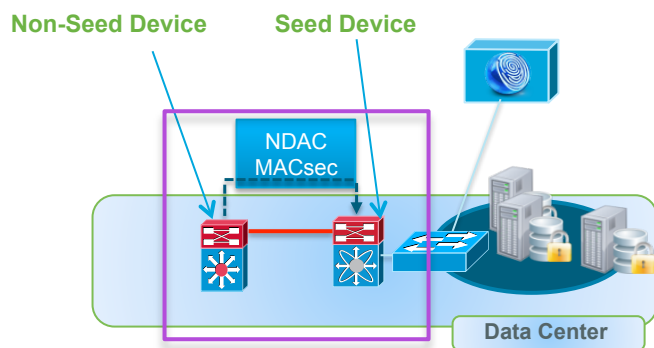


There are two server groups, Sales and Engineering, that are in the same VLAN. The goal is to control traffic between these server groups with SGACLs instead of static ACLs. Although these servers are connected to a Cisco Catalyst 4948 series switch that does not support SGACL enforcement currently, SGACL enforcement is still possible via the Cisco Nexus 7000 switch. This enforcement is accomplished by initially defining a private VLAN so that server traffic is sent to the promiscuous port so that the Cisco Nexus 7000 switch can filter the traffic.

Note: Please reference the appendix for private-vlan and interface-vlan configuration. Step-by-step instructions are not covered in this guide.

Configuring Network Devices to Enable SGA

Figure 30: Network Device Authentication (NDAC) with SGA



NDAC requires a device to behave as an 802.1X supplicant to gain access to the Cisco TrustSec network. After admission, the device is able to act as an authenticator, in turn admitting other supplicants devices into the trusted network circle. However, there has to be at least one device, which we refer to as the Seed Device, that is configured with knowledge of at least one Cisco ISE. After the seed device authenticates with the authentication server to begin the SGA domain, each new device, called the Non-Seed Device, added to the domain is authenticated by its peer devices already within the domain. The peers act as intermediaries for the domain authentication server. Each newly authenticated device is categorized by the authentication server and assigned a security group number based on its identity, role, and security posture.

Procedure 1 Define Device SGT

As a part of the policy acquisition phase (authorization), a Cisco TrustSec capable device receives an SGT called a Device SGT. This Device SGT represents the security group to which the device itself belongs and is exchanged with a neighbor device as a token of trusted devices. This Device SGT is configured on Cisco ISE prior to the seed device NDAC process.

A device SGT can be uniquely assigned to every Cisco TrustSec capable device.

Best Practice: It is recommended to use single SGT value for all Cisco TrustSec capable devices unless there is a specific need to separate a security group for a certain set of devices.

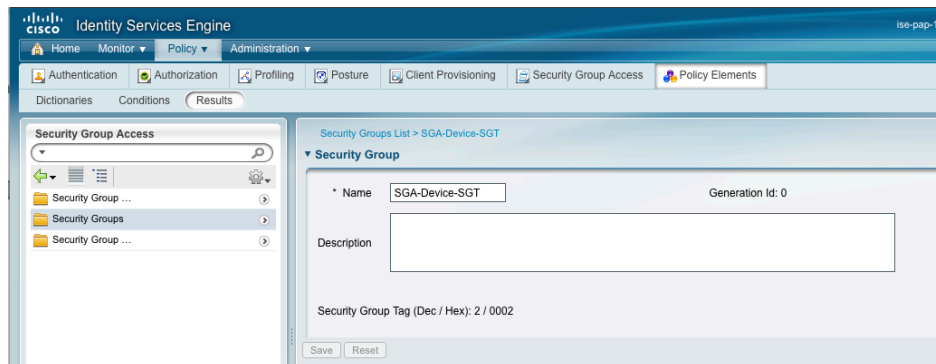
In the next step you will configure Device SGT and create a policy that tags devices as they get added to Cisco ISE with the same tag.

Step 1 Navigate to Policy → Policy Elements → Results → Security Group Access → Security Groups.

Step 2 Click **Add**.

Step 3 Provide a name (e.g., SGA-Device-SGT). Add a description if you wish.

Step 4 Click **Submit** when you are done.

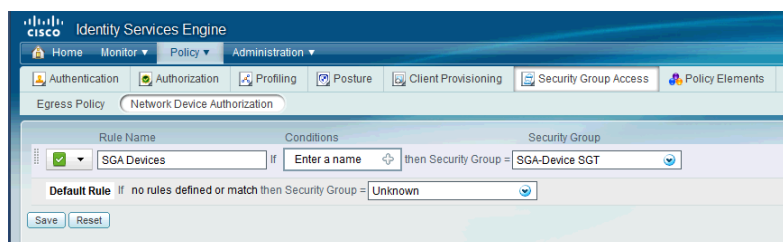


Step 5 Navigate to Policy → Security Group Access → Network Device Authorization.

Step 6 On the far right, click the  Actions button, and choose Insert new row above.

Step 7 Create an NDAC Policy :

Rule Name	Conditions	Security Group
SGA Devices	Device:Device Type = SGA –Device-SGT	SGA Device SGT



Step 8 Click **Save**.

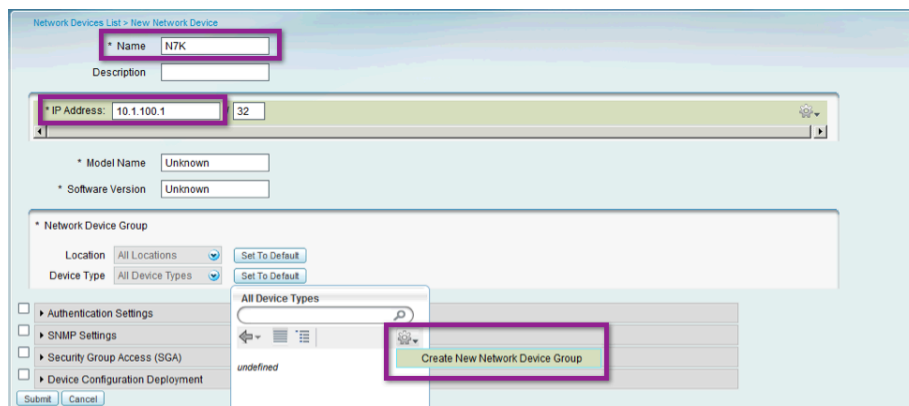
Procedure 2 Define AAA Client.

Step 1 Within Cisco ISE, navigate to Administration → Network Resources → Network Devices.

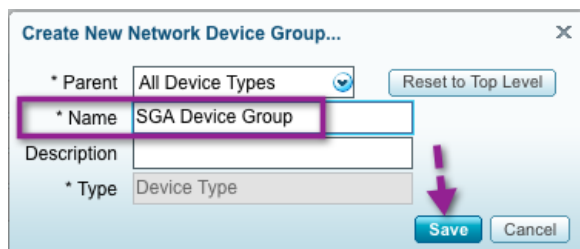
Step 2 Click Add.

Step 3 Enter the name N7K and an IP address of 10.1.100.1.

Step 4 Under Network Device Group, click the gear icon to create a new device group.



Step 5 Type SGA Device Group for group name and then click Save.



Step 6 Now that the SGA Device Group has been created, select it as the Device Type.

Network Device Group

Location: All Locations [Set To Default]

Device Type: All Device Types [Set To Default]

All Device Types

- Authentication Settings
- SNMP Settings
- Security Group Access (SGA)
- Device Configuration Deployment

SGA Device Group

Step 7 Scroll down and check the box for **Authentication Settings**. Configure the secret as "Cisco123".

Authentication Settings

Enable Authentication Settings

Protocol: RADIUS

* Shared Secret: cisco123

Step 8 Scroll down and check the box for **Security Group Access (SGA)**. Fill in the resulting fields and check boxes per the following screenshot.

Security Group Access (SGA)

Use Device ID for SGA Identification: ☒

Device Id: N7K

* Password: trustsec123

* Download environment data every (Valid Range: 1 to 24850): 1 Days

* Download peer authorization policy every (Valid Range: 1 to 24850): 1 Days

* Reauthentication every (Valid Range: 1 to 24850): 1 Days

* Download SGACL lists every (Valid Range: 1 to 24850): 1 Days

Other SGA devices to trust this device: ☒

Include this device when deploying Security Group Tag Mapping Updates: ☒

Step 9 Scroll down and check the box for **Device Configuration Deployment**. Fill in the exec mode username and password.

Device Configuration Deployment

Device Interface Credentials

* Exec Mode Username: admin

* Exec Mode Password: [masked] [Show]

Enable Mode Password: [empty] [Show]

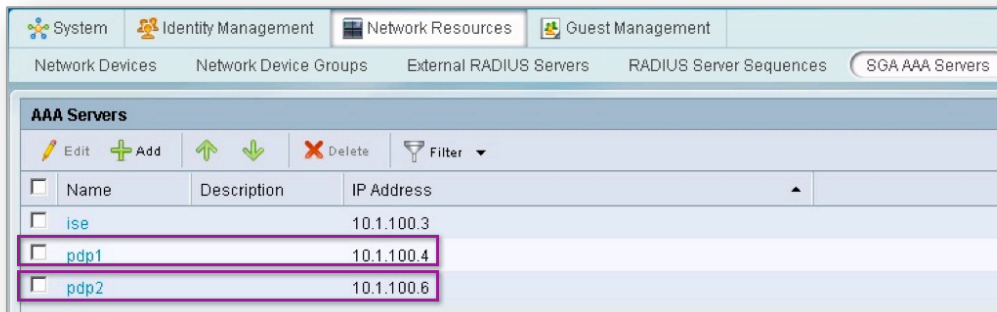
Note: This step is necessary for deploying the IP/hostname to SGT mapping later on.

Step 10 Click Submit.

Procedure 3 Configure Private Server List

Best Practice: In a multiple PDP environment, configure the seed device with the list of fall-back PDPs.

Step 1 Navigate to Administration → Network Resources → SGA AAA Servers.



Note: Multiple PDP servers are not discussed in this guide. They are noted here just for best practice methods.

Procedure 4 Modify the A-ID description

Best Practice: Modify the Authority ID description. This modification is useful when troubleshooting PAC-related problems.

Step 1 Navigate to Administration → Settings → Protocols → EAP-FAST → EAP-FAST Settings.

Step 2 Change “Authority Identity Info Description” to a unique identifier.

For example, <ise-hostname>

Step 3 Click **Save**.

Procedure 5 Configure Cisco Nexus 7000 Switch

Step 1 Connect to the Cisco Nexus 7000 switch and enter configuration mode.

Step 2 Go into configuration mode and enable 802.1X and SGA features.

```
N7K# conf t
Enter configuration commands, one per line. End with CNTL/Z.
N7K(config)# feature dot1x
N7K(config)# feature cts
N7K(config)# show dot1x
Sysauthcontrol Enabled
Dot1x Protocol Version 2
```

Step 3 Verify 802.1x and SGA were enabled by the following commands:

```
N7K(config)# show cts
CTS Global Configuration
=====
CTS support : enabled
CTS device identity : not configured
SGT : 0
CTS caching support : disabled
Number of CTS interfaces in
DOT1X mode : 0
Manual mode : 0
```

Step 4 Next configure the device to join the Cisco TrustSec domain.

```
N7K(config)# cts device-id N7K password trustsec123
```

Note: The device ID should match the name entry in Cisco ISE. To verify the ID has been configured, use the following command:

```

N7K(config)# show cts
CTS Global Configuration
=====
CTS support          : enabled
CTS device identity  : N7K
SGT                  : 0
CTS caching support  : disabled
Number of CTS interfaces in
DOT1X mode          : 0
Manual mode          : 0

```

Step 5 Next configure the AAA commands that are required for 802.1x authentication with Cisco ISE.

Note: The “pac” keyword is used to request a per-server Protected Access Credential key for this switch. This pac keyword is required for the seed device. The resulting PAC file will be used to secure the RADIUS exchanges with Cisco ISE.

```

N7K(config)# radius-server host 10.1.100.3 key Cisco123 pac
N7K(config)# aaa group server radius ise-radius
N7K(config-radius)# server 10.1.100.3
N7K(config-radius)# use-vrf default

```

Step 6 Next configure AAA configuration that is needed to talk to Cisco ISE and for 802.1x authentication.

```

N7K(config)# aaa authentication dot1x default group ise-radius
N7K(config)# aaa accounting dot1x default group ise-radius
N7K(config)# aaa authorization cts default group ise-radius

```

Step 7 Enter the following command again on the Cisco Nexus 7000 switch:

```

N7K(config)# cts device-id N7K password trustsec123

```

Note: This command will invoke device registration with Cisco ISE and to force a PAC download.

Step 8 Next verify that the Cisco Nexus 7000 switch has successfully communicated with Cisco ISE to download the PAC data.

Note: The “AID Info” output will match the string that you entered

```

N7K# show cts pac
PAC Info :
=====
PAC Type          : Trustsec
AID                : 05dbd5b84f65f0deb436c517e07672bc
I-ID              : N7K
AID Info          : <ISE-hostname>
Credential Lifetime : Tue May  3 07:39:14 2011
PAC Opaque        : 000200a8000300010004001005dbd5b84f65f0deb436c517e07672bc
0006008c000301005ff2563d5242b3f00eaf7b64c5560f39000000134d43a8f700093a80eac7c503
a3f64f572632ce7503aa93190533c47e958daf0e61f7cc0a1267a66fcc790bcc92354476d30a12f0
2f5e9156f8c9905c91cd0dfb999f02555e1bc5ff7bfe07b1ac7a09c63aad6f742ecd1f78c9154fca
4a02ca4b5075faa58c170a7ada1132b2890f306ccd4a5e8a

```

```

N7K# show cts environment-data
CTS Environment Data
=====
Current State      : CTS_ENV_DNLD_ST_ENV_DOWNLOAD_DONE
Last Status        : CTS_ENV_SUCCESS
Local Device SGT    : 0x0002
Transport Type      : CTS_ENV_TRANSPORT_DIRECT
Data loaded from cache : FALSE
Env Data Lifetime   : 86400 seconds after last update
Last Update Time    : Wed Feb  2 12:36:07 2011
Server List         : CTSServerList1
AID:05dbd5b84f65f0deb436c517e07672bc IP:10.1.100.21 Port:1812

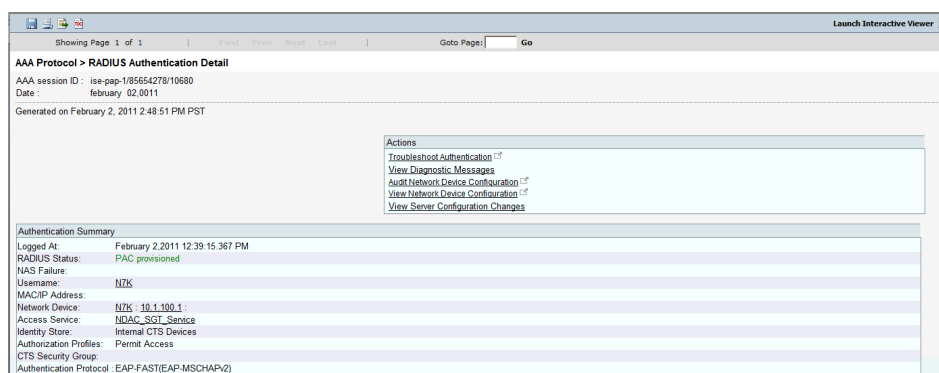
```

Step 9 On Cisco ISE, go to Monitor → Authentications.



Time	Status	Details	Username	Calling Station ID	IP Address	NAD	Session ID	NAS Port ID	Event	Authorization Profiles
Feb 02, 11 12:39:20.004 PM	✓	⏏	#CTSREQUEST#			N7K			CTS Data Download Succeeded	
Feb 02, 11 12:39:19.989 PM	✓	⏏	#CTSREQUEST#			N7K			CTS Data Download Succeeded	
Feb 02, 11 12:39:19.953 PM	✓	⏏	#CTSREQUEST#			N7K			CTS Data Download Succeeded	
Feb 02, 11 12:39:19.947 PM	✓	⏏	#CTSREQUEST#			N7K			CTS Data Download Succeeded	
Feb 02, 11 12:39:15.367 PM	✓	⏏	N7K			N7K			PAC provisioned	Permit Access

Step 10 To see detailed logs on PAC provisioning, click  within the Cisco Nexus 7000 entry.



AAA Protocol > RADIUS Authentication Detail	
AAA session ID :	iss-pap-185554278/10680
Date :	February 02, 2011
Generated on February 2, 2011 2:48:51 PM PST	
<div> <div>Actions</div> <div> Troubleshoot Authentication View Diagnostic Messages Audit Network Device Configuration View Network Device Configuration View Server Configuration Changes </div> </div>	
Authentication Summary Logged At: February 2, 2011 12:39:15.367 PM RADIUS Status: PAC provisioned NAS Failure: Username: N7K MAC/IP Address: Network Device: N7K - 10.1.190.1 Access Service: NDAC_SCT_Service Identity Store: Internal CTS Devices Authorization Profiles: Permit Access CTS Security Group: Authentication Protocol: EAP-FAST(EAP-MSCHAPv2)	

NDAC and Non-Seed Device Configuration

A non-seed device does not have a config to locate the AAA server for NDAC. Instead, it receives the AAA server list from the Seed device after completing NDAC (and receiving environment data).

Procedure 1 Configure Cisco ISE

Step 1 Navigate to Administration-> Network Resources-> Network Devices. On this screen, add the seed device per instructions from Steps 1-4.

Step 2 Scroll down and check the box for **Security Group Access (SGA)**. Fill in the "Password" field. Leave the other options as they are.

Step 3 Scroll down and check the box for **Device Configuration Deployment**. Fill in the exec mode username and password.

Step 4 Click **Save**.

Procedure 2 Configure NDAC on Cisco Catalyst 6500.

The Cisco Catalyst 6500 switch Supervisor Engine 2T is supported in Cisco TrustSec 2.0. The Supervisor Engine 2T supports both Cisco TrustSec Capable and Cisco TrustSec Non-Capable switching modules.

Table 18: TrustSec-Compatible Hardware

Type	Description	Module
Cisco TrustSec capable	Hardware supports insertion and propagation of SGT	WS-X6908-10G WS-6904-40G
Cisco TrustSec aware	Hardware does not support insertion of propagation of SGT, but hardware can perform a lookup to determine the source and destination SGT for a packet	WS-X6816-10G-2T WS-X6816-10T-2T
Cisco TrustSec incapable	Hardware does not support insertion and propagation of SGT and cannot determine the SGT by a hardware lookup	WS-X6748-SFP WS-X6748-GETX WS-X6724-SFP WS-6704-10G WS-X6148-series

In this guide, the Cisco Catalyst 6500 Supervisor Engine and a line card that is not Cisco TrustSec capable are used. Therefore the Cisco TrustSec reflector feature must be enabled to accommodate the Cisco TrustSec incapable switching modules within the same switch. Available in Cisco IOS Software Release 12.2(50)SY and later releases, the Cisco TrustSec reflector uses SPAN to reflect traffic from a Cisco TrustSec incapable switching module to the supervisor engine for SGT assignment and insertion.

The Cisco TrustSec reflector operates in two mutually exclusive modes, ingress and egress.

Table 19: Ingress and Egress Reflector Types

Reflector Type	Description
Ingress Reflector	<p>The following conditions must be met before the Cisco TrustSec ingress reflector configuration is accepted.</p> <ul style="list-style-type: none">• The supervisor engine must be Cisco TrustSec capable.• Any Cisco TrustSec incapable DFCs must be powered down.• A Cisco TrustSec egress reflector must not be configured on the switch.• Before disabling the Cisco TrustSec ingress reflector, you must remove power from the Cisco TrustSec incapable switching module.
Egress Reflector	<p>The following conditions must be met before the Cisco TrustSec egress reflector configuration is accepted:</p> <ul style="list-style-type: none">• The supervisor engine or DFC switching module must be Cisco TrustSec capable.• Cisco TrustSec must not be enabled on non-routed interfaces on the supervisor engine uplink ports or on the Cisco TrustSec capable DFC switching modules.• Before disabling the Cisco TrustSec egress reflector, you must remove power from the Cisco TrustSec incapable switching modules.• A Cisco TrustSec ingress reflector must not be configured on the switch.

Note: For the topology used in this guide, the egress reflector should be enabled.

Step 1 Use the following command to enable Egress Reflector mode.

```
C6K-DIST(config)#platform cts egress
CTS Egress reflector will be active only on next system reboot.
Please reboot the system for CTS Egress reflector to be active.
```

Step 2 Reboot the system.

Step 3 Verify whether the Cisco Catalyst 6500 switch is in egress mode.

```
C6K-DIST#show platform cts
CTS Egress mode enabled
```

Procedure 3 Configure Non-Seed Device.

Step 1 Connect to the Cisco Catalyst 6500 switch and enter configuration mode.

Step 2 Configure the Cisco Catalyst 6500 switch to communicate with Cisco ISE for SGA.

```
C6K-DIST(config)#aaa new-model
C6K-DIST(config)#dot1x system-auth-control
C6K-DIST(config)#exit
```

Step 3 Enable 802.1x on the uplink interface to the Cisco Nexus 7000 switch.

```
C6K-DIST(config)#int g1/1
C6K-DIST(config-if)#cts dot1x
C6K-DIST(config-if)# no shut
```

Step 4 Verify that the Cisco Catalyst 6500 has successfully downloaded the PAC from Cisco ISE.

```
C6K-DIST#show cts pac
AID: 6A593707323253D0ACB126E82EEB7BB0
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: 6A593707323253D0ACB126E82EEB7BB0
  I-ID: C6K-DIST
  A-ID-Info: ise-10
  Credential Lifetime: 00:49:19 UTC Dec 24 2011
PAC-Opaque:
000200B000030001000400106A593707323253D0ACB126E82EEB7BB0000060094000301008B01F0EE0F1485C66
0E9BF638B522704000000134E75FF0300093A80A5C12334C13B45E5F19D066BCF7DBA138ABFB8CDAEB2E32525
2C78A2A4F19E94FAB8C375485F82FABAC9D2F48C41C3493EC7D9230BD14F9A5997C416EAD4548DF10E6CCDEDC
A5614994AEDD035F64F70A742BC44D7AE8E5F4B5CA8B71674B0D3631B9F46E9A432B8B436187BA190043BA3B2
01E7
Refresh timer is set for 12w0d
```

Step 5 Verify that the Cisco Catalyst 6500 switch successfully downloaded the environment data.

```
C6K-DIST#show cts env
CTS Environment Data
=====
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 2-00
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
  *Server: 10.1.100.3, port 1812, A-ID 6A593707323253D0ACB126E82EEB7BB0
    Status = ALIVE
    auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
  0001-17 :
    2-98 : 80 -> SGA
    unicast-unknown-98 : 80 -> Unknown
    Any : 80 -> ANY
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 17:17:25 UTC Mon Sep 26 2011
Env-data expires in 0:17:19:52 (dd:hr:mm:sec)
Env-data refreshes in 0:17:19:52 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

Step 6 To see the transaction on Cisco ISE, go to **Monitor->Authentications**.

Step 7 The communication with Cisco ISE should look similar to this:

Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status
Sep 26,11 08:14:43.437 AM	Success	#CTSREQUEST#				C6K-DIST				
Sep 26,11 08:14:43.436 AM	Success	#CTSREQUEST#				C6K-DIST				
Sep 26,11 08:13:43.782 AM	Success	C6K-DIST		C8:4C:75:BF:4A:00		C6K-DIST				

Note: By default the Cisco Catalyst 6500 series switch proactively checks whether Cisco ISE is “alive” or “dead” by sending test authentications every 60 minutes. These authentications display as authentication failures because the predefined user “CTS-Test-Server” does not exist in any configured identity store.

CTS-Test-Server	C6K-DIST	Authentication f... 22056 Subject not found in the applicable identity store(s)
CTS-Test-Server	C6K-DIST	Authentication f... 22056 Subject not found in the applicable identity store(s)
CTS-Test-Server	C6K-DIST	Authentication f... 22056 Subject not found in the applicable identity store(s)
CTS-Test-Server	C6K-DIST	Authentication f... 22056 Subject not found in the applicable identity store(s)

There is no functional effect on Cisco ISE if these tests continue. However, the dashboard and any trend reports for authentication will be skewed. To fix this inconvenience, please refer to the [“Remediate the failed authentication”](#) procedure.

Enforcing Access Policy for Servers Using SGACLs

Step 1 Create SGT

Step 1 Navigate to Policy → Policy Elements → Results → Security Group Access → Security Groups.

Step 2 Click **ADD**.

Step 3 Create the SGT values

Name	SGT (Dec/Hex)	Description
Sales Servers	3/0003	SGT for Sales Servers
Engineering Servers	4/0004	SGT for Engineering Servers

Note: The tag values are generated by Cisco ISE. The ability to specify the tag value for management purposes will come in a future Cisco ISE release.

The next step is to associate these SGTs with the proper data center servers.

Step 4 Go to Policy → Policy Elements → Results → Security Group Access → Security Group Mappings.

Step 5 Add the IP-to-SGT mappings

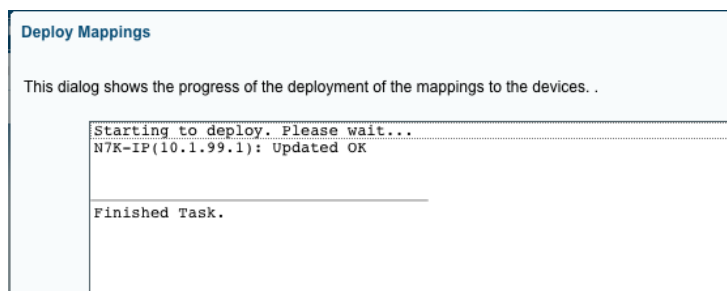
Security Group Mappings			
Edit Add Reassign Groups Deploy Check Status Delete Filter			
<input type="checkbox"/>	Security Group	Hostname	IP Address
<input type="checkbox"/>	Engineering_Servers	db2	10.1.200.20
<input type="checkbox"/>	Sales_Servers	db1	10.1.200.10

Step 6 Now click the **Check Status** icon.

Cisco ISE will compare its SGT mapping to what is configured on the Cisco Nexus 7000 switch. Currently, there is no configuration on the Cisco Nexus 7000 switch, so the result will be “Not up to date”.

Step 7 Click **Deploy** to push the SGT mappings to the Cisco Nexus 7000 switch. Following are the two methods to verify that deployment is successful.

On Cisco ISE:



On the Cisco Nexus 7000 switch:

```
NX7K-DIST# show cts role-based sgt-map
IP ADDRESS          SGT          VRF/VLAN          SGT CONFIGURATION
10.1.200.10         3            vrf:1             CLI Configured
10.1.200.20         4            vrf:1             CLI Configured
```

Note: There are conditions when a packet fails to get tagged:

- Endpoint authentication failure
- Endpoint authorized to locally significant VLAN (Failed-Auth-VLAN, Guest VLAN, or Critical VLAN)
- When SXP connection is down and listener receives packet from unknown source IP Address
- When there is no static IP-to-SGT binding associated to traffic received
- When access device does not support SXP

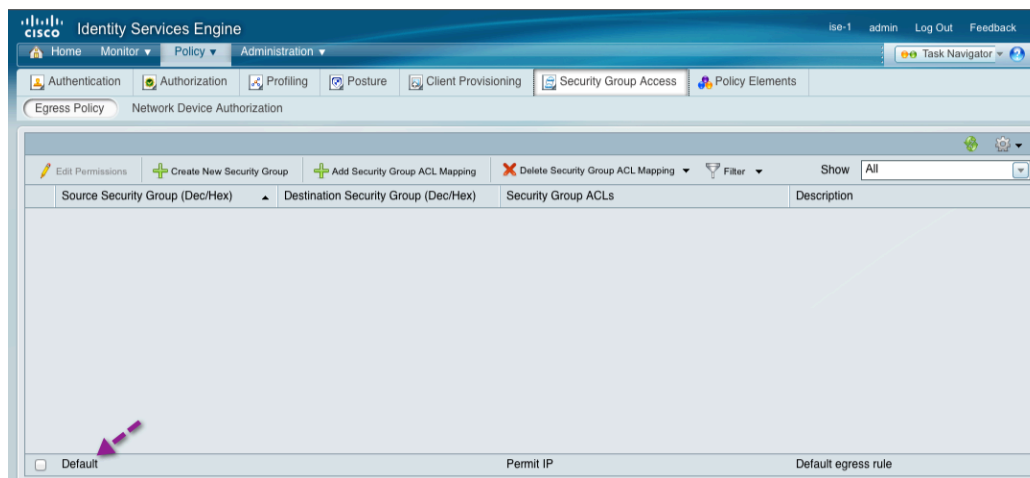
In these conditions, the SGT value is zero (SGT = 0). Default egress policy is to permit all traffic that is not defined in the egress policy. Therefore, traffic with an unknown tag (SGT = 0) is not filtered.

Best Practice: Focus on creating enforcement policies to secure business-critical servers and leave the default policy untouched (default is permit).

Procedure 4 Create SGACL.

Step 1 Navigate to Policy → Security Group Access → Egress Policy.

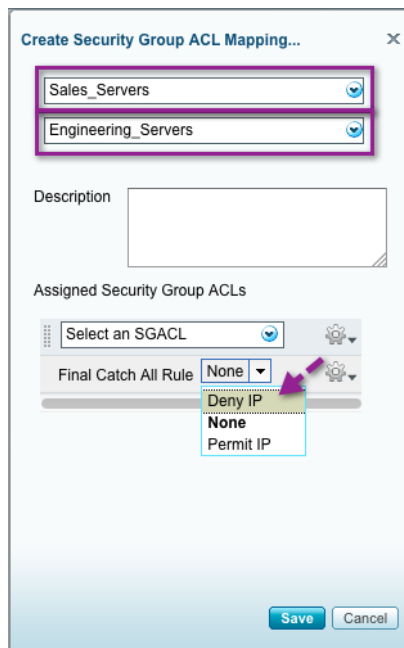
Currently the only table entry will be the default “permit” policy at the bottom of the screen.



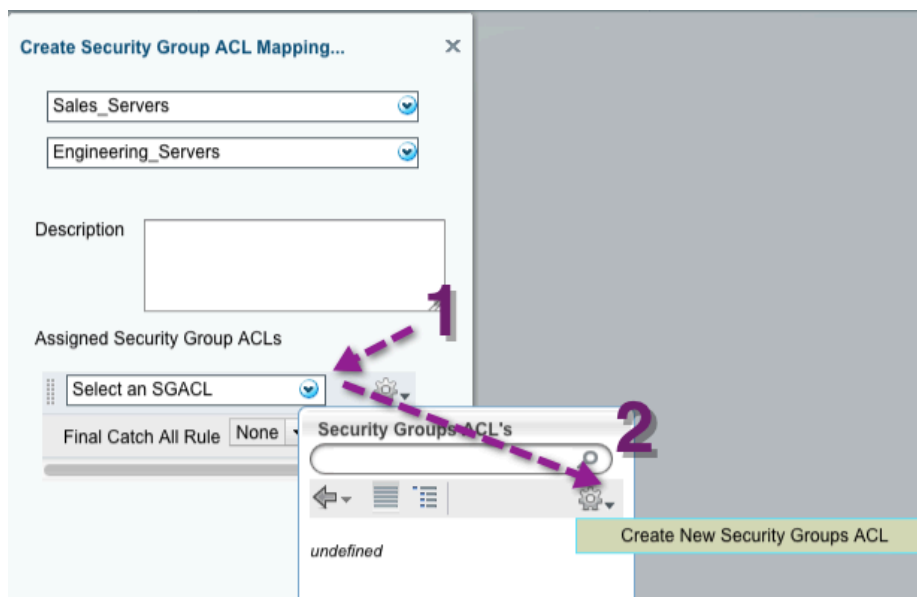
Step 2 Click “Add Security Group ACL Mapping”.

Step 3 Choose the “Source Security Group” and “Destination Security Group” as “Sales” and “Engineering”.

Step 4 Select the predefined “deny ip” because the goal is to prevent communication between the sales and engineering servers,



or create specific traffic rules :



Use following syntax to create content of the SGACL:

```
deny icmp
deny igmp
deny ip
deny tcp [{dest|src} {{eq | gt | lt | neq} port-number | range port-number1 portnumber 2}}
deny udp [{dest|src} {{eq | gt | lt | neq} port-number | range port-number1 portnumber 2}}
permit icmp
permit igmp
permit ip
```

```
permit tcp [{dest|src} {{eq | gt | lt | neq} port-number | range port-number1 portnumber 2}}
permit udp [{dest|src} {{eq | gt | lt | neq} port-number | range port-number1 portnumber 2}}
```

Note: The closing ACL (Permit IP or Deny IP) can be used to set the default filter for any unmatched traffic at the end of the ACL. The Cisco Nexus 7000 Series does not support the download of multiple SGACLs in a single authorization message. Therefore, as shown in the example, the closing ACL is included within the SGACL definition.

Step 5 Click “Save”.

Procedure 5 Enforce SGACL.

Step 1 On the Cisco Nexus 7000 switch, download the policy created previously using **cts refresh role-based policy**.

```
N7K# cts refresh role-based-policy
N7K# show cts role-based policy

sgt:3
dgt:4   rbacl:Deny IP <--Deny IP traffic from SGT=3 to SGT=4
        deny ip

sgt:any
dgt:any rbacl:Permit IP

N7K# show cts role-based access-list
rbacl:Deny IP
        deny ip
rbacl:Permit IP
        permit ip
```

Step 2 To validate whether traffic is hitting the RBACL, type “show cts role-based counters”.

```
N7K# show cts role-based counters
```

```
RBACL policy counters enabled
Counters last cleared: 10/01/2011 at 01:14:33 PM
```

```
sgt:3 dgt:4      [4]  <--Indicates # of packets dropped from SGT=3 to SGT=4
rbacl:Deny IP
      deny ip [4]

sgt:any dgt:any [6]
rbacl:Permit IP
      permit ip      [6]
```

Campus-to-Data Center Use Case Configuration

Additional Security Group Access Information

Currently the Cisco Nexus 7000 switch and the Cisco Catalyst 6500 switch with Supervisor Engine 2T are the only fully SGA-capable devices because ASIC support is necessary for 802.1AE encryption. Such support requires hardware changes. Therefore, the SXP protocol was introduced. SXP stands for SGT Exchange Protocol over TCP, or SXPoTCP.

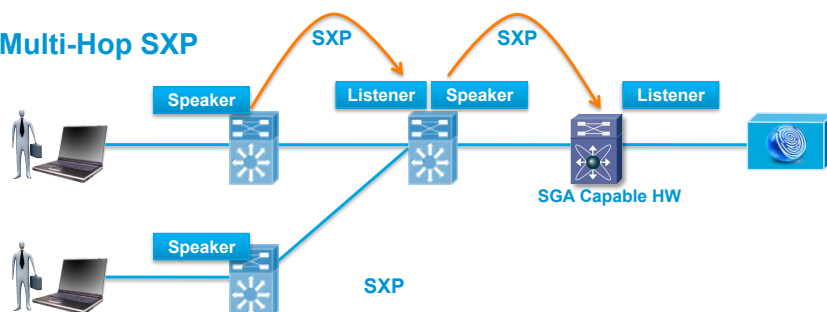
SXP is a peer-to-peer protocol used to exchange IP-to-SGT bindings from a non-SGA capable device. The SXP peer that sends IP-to-SGT bindings is called a “speaker”. The IP-to-SGT binding receiver is called a “listener”. SXP connections can be single hop or multi-hop as shown below.

Figure 31: Single-Hop vs. Multi-Hop SXP Connections

Single-Hop SXP



Multi-Hop SXP



Whether single-hop or multihop, SXP configuration varies per deployment. The table below gives scaling numbers for guidance.

Table 20: Scaling Numbers

Device	Max # of IP to SGT Bindings	Max # of SXP Connections (Associated with max # of IP-SGT bindings)
Cisco ASR 1000 RP1 (4GB RAM) / ESP10	128,000	2,000
Cisco ASR 1000 RP2 / ESP20	256,000	2,000
Cisco Catalyst 6500 Switch	16,000	500
Cisco Nexus 7000 Switch	300	900

In the data center use case shown previously, IP-to-SGT assignment was done manually. In this use case, dynamic SGT assignment is used. Assignment is dynamically done through the authorization process after successful authentication. Additionally, because access layer switches do not support SGT imposition, these switches must be configured to use SXP.

Procedure 6 Configure SXP

Step 1 On the Cisco Catalyst 6500 switch configure SXP commands to make the switch an SXP listener.

```
nexus-1-ts2-lab7-pod1(config)# cts sxp enable
nexus-1-ts2-lab7-pod1(config)# cts sxp connection peer 10.1.251.2 source 10.1.251.1
password required cisco123 mode speaker
nexus-1-ts2-lab7-pod1(config)# cts sxp connection peer 10.1.250.2 source 10.1.250.1
password required cisco123 mode speaker
```

Step 2 Configure the Cisco Catalyst 3560-X switch for SXP commands as an SXP speaker.

```
3560X(config)#cts sxp enable
3560X(config)#cts sxp default password cisco123
3560X(config)#cts sxp connection peer 10.1.48.1 source 10.1.48.2 password default mode
peer listener
```

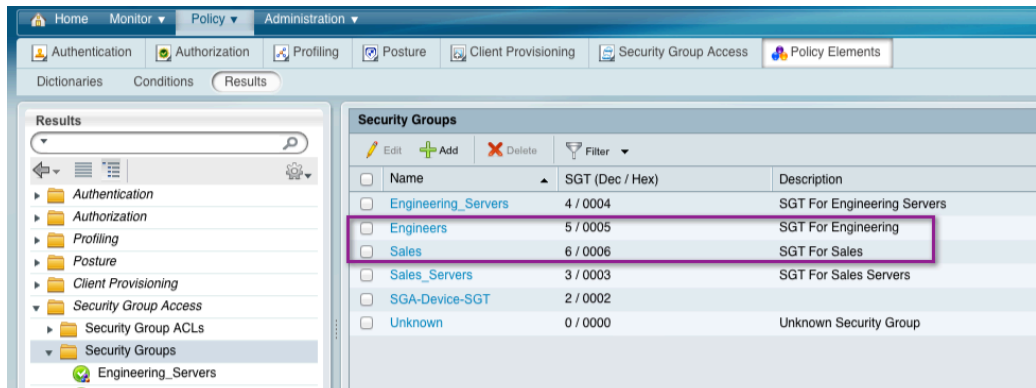
Step 3 Use the following CLI command to verify the SXP connection establishment:

```
3560X#show cts sxp connection
SXP                : Enabled
Default Password   : Set
Default Source IP  : Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
-----
Peer IP            : 10.1.48.1
Source IP          : 10.1.48.2
Conn status        : Off
Local mode         : SXP Speaker
Connection inst#    : 1
TCP conn fd        : -1
TCP conn password: default SXP password
Duration since last state change: 8:16:02:29 (dd:hr:mm:sec)
```

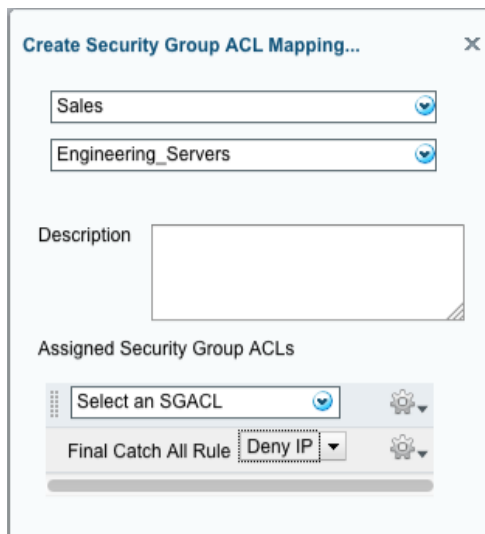
Procedure 7 Assign Dynamic SGT

An SGT is dynamically assigned via Cisco ISE to the endpoint upon successful authorization.

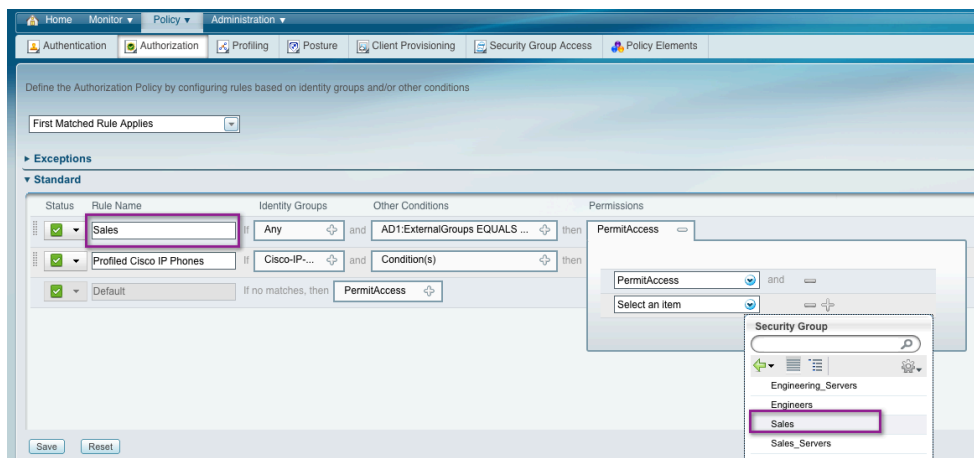
Step 1 Associate SGT values to user roles.



Step 2 Create a SGACL policy for user roles.



Step 3 Associate SGT with authorization policy.



Step 4 You are ready to connect.

Step 5 Use the following commands to verify the connection is successful:

To show the SGT is assigned to the user's connection on the Cisco Catalyst 3000:

```
3560X#show auth session int g0/1
      Interface: GigabitEthernet0/1
      MAC Address: 0010.1864.e3de
      IP Address: 10.1.10.100
      User-Name: sales1
      Status: Authz Success
      Domain: DATA
      Security Policy: Should Secure
      Security Status: Unsecure
      Oper host mode: multi-domain
      Oper control dir: both
      Authorized By: Authentication Server
      Vlan Group: N/A
      SGT: 0006-0 ← SGT=6 (Sales)
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 0A013002000000038873C0496
      Acct Session ID: 0x00000044
      Handle: 0xC3000038
```

```
Runnable methods list:
      Method      State
      dot1x       Authc Success
      mab          Not run
```

On the Cisco Catalyst 6500 switch:

To show that the IP to SGT binding was forwarded to the 6K from the 3K:

```
C6K-DIST#show cts sxp sgt-map
```

IP-SGT Mappings as follows:

```
IPv4,SGT: <10.1.10.100 , 6> <- 10.1.10.100 is associated with SGT=6
source   : SXP;
Peer IP   : 10.1.48.2;
Ins Num   : 1;
Status    : Active;
Seq Num   : 1
Total number of IP-SGT Mappings: 1
```

An alternate view of the IP to SGT mapping follows:

```
C6K-DIST#show cts role-based sgt-map all
```

Active IP-SGT Bindings Information

IP Address	SGT	Source
10.1.10.100	6	SXP
10.1.48.1	2	INTERNAL

IP-SGT Active Bindings Summary

```
=====
Total number of SXP      bindings = 1
Total number of INTERNAL bindings = 1
Total number of active   bindings = 2
```

On the Cisco Nexus 7000 switch:

The Cisco Nexus 7000 switch is the enforcement point. Therefore the tagged packets (SGT = 6) from the Cisco Catalyst 6500 switch are subject to the SGACLs configured previously.

```
N7K# show cts role-based counters
```

```
RBACL policy counters enabled  
Counters last cleared:
```

```
sgt:3 dgt:4      [0]  
rbacl:Deny IP  
      deny ip [0]
```

```
sgt:5 dgt:3      [0]  
rbacl:Deny IP  
      deny ip [0]
```

```
sgt:6 dgt:4      [4] <- 4 packets sent from Sales to Engineering Server  
rbacl:Deny IP  
      deny ip [4]<- 4 packets denied access
```

```
sgt:any dgt:any [358]  
rbacl:Permit IP  
      permit ip      [358]
```

Table 21: Cisco Nexus 7000 Switch Commands Compared with Cisco Catalyst 6500 Switch Commands

Cisco Nexus 7000 Switch	Cisco Catalyst 6500 Switch
show cts role-based policy	show cts role-based permissions
show cts role-based access-list	show cts rbac1
cts refresh role-based policy	cts refresh policy
aaa authorization CTS default group <radius group-name>	cts authorization list <authorization-list-name>
aaa group server radius <group name>	aaa authorization network <authorization-list-name> group radius

Posture Assessment

Introduction

Cisco ISE can assess the posture of all endpoints that are connecting to the Cisco ISE enabled network with your corporate security policies for compliance before endpoints access protected areas of your network. This section will go over basic posture configuration available on Cisco ISE.

The Network Admission Control (NAC) agents that are installed on the endpoint clients interact with the Cisco ISE posture service to enforce security policies on all endpoints that gain access to your protected network. At the same time, the NAC agents enforce security policies on noncompliant endpoints by preventing access to the protected network.

The Cisco ISE posture service checks the state of the clients for compliance while the Client provisioning service helps ensure that the clients have the appropriate agents installed to assess posture and perform the remediation.

Client Provisioning

In order to perform posture assessment and determine the compliance state of an endpoint, it is necessary to provision a client, or agent, to the endpoint. Cisco ISE Agents can be persistent whereby the agent is installed and is automatically loaded each time a user logs in. Cisco ISE Agents can also be temporal whereby a Web-based agent is dynamically downloaded to the user upon each new session and then removed following the posture assessment process. NAC Agents are also responsible for facilitating remediation and providing an optional Acceptable Use Policy (AUP) to the end user. Therefore, one of the first steps in the workflow is to retrieve the agent files from the Cisco website and to create policies that determine agent and configuration files downloaded to endpoints based on their attributes, for example, user identity and client OS type.

Posture Policy

The posture policy defines the set of requirements for an endpoint to be deemed "Compliant" based on file, registry, process, application, Windows, and AV/AS checks and rules. Posture policy is applied to endpoints based on a defined set of conditions such as user identity and client OS type.

Compliance (posture) status of an endpoint can be one of the following:

- Compliant (compliant with all mandatory requirements)
- Noncompliant (posture assessment performed and one or more requirements failed)
- Unknown (no data collected to determine posture state)

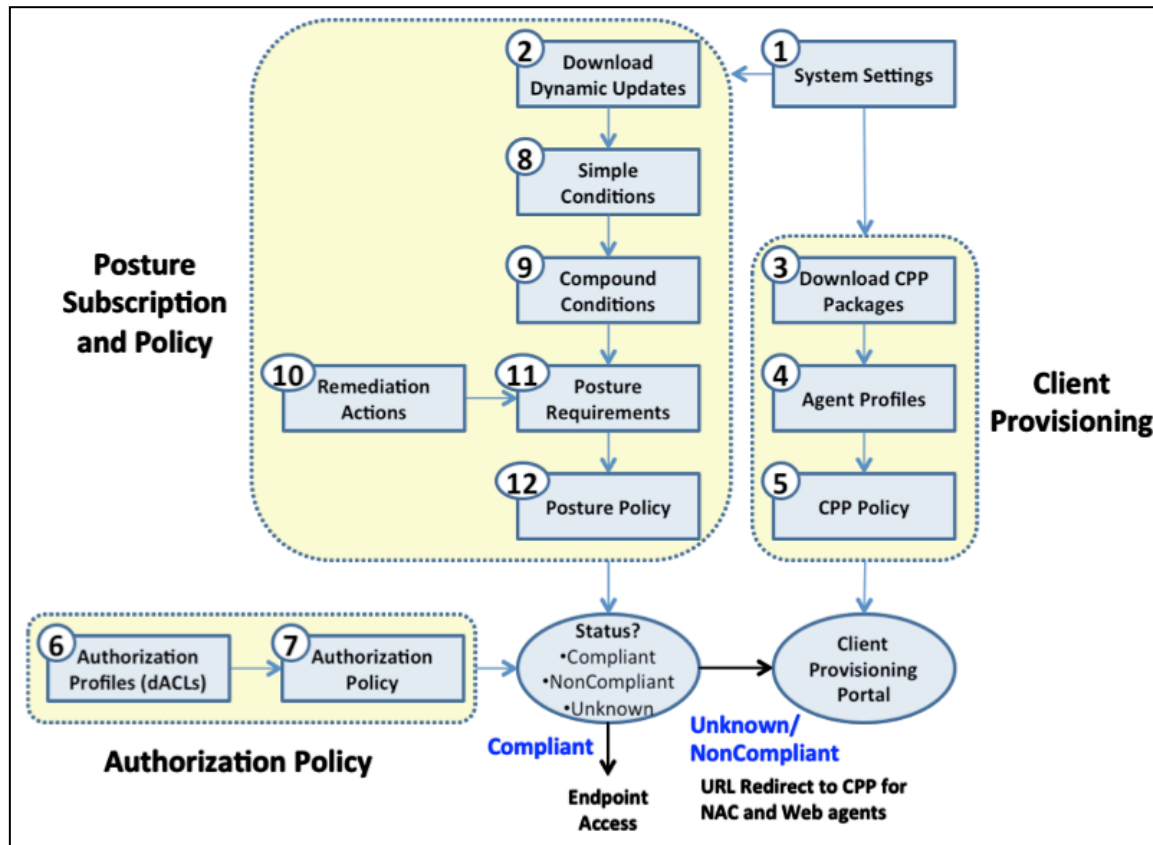
Posture requirements are based on a configurable set of one or more conditions. Simple Conditions include a single assessment check. Compound Conditions include a logical grouping of one or more Simple Conditions. Each requirement is associated with a remediation action that assists endpoint to satisfy the requirement; for example, an AV signature update.

Authorization Policy

An authorization policy defines the levels of network access and optional services to be delivered to an endpoint based on posture status. Endpoints that are deemed "not compliant" with Posture Policy may be optionally quarantined until the endpoint becomes compliant. During this phase, a typical Authorization Policy may limit a user's network access to posture and remediation resources only. If remediation by the agent or end user is successful, then the Authorization Policy can grant privileged network access to the user. Policy is often enforced using downloadable ACLs (DACLS) or dynamic VLAN assignment.

The main steps in configuring posture services follow (Figure 34).

Figure 32: Posture Service Configuration Overview



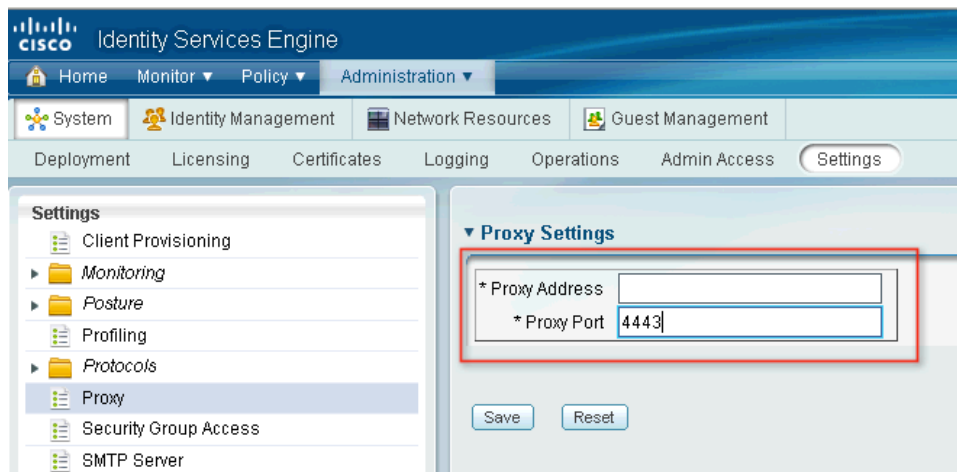
The diagram depicts the logical grouping of configuration tasks. In some cases tasks may be applicable to both sponsor and guest configuration.

Posture Configuration – Configure Cisco ISE for Client Provisioning

Procedure 1 Configure System Settings.

If your existing network topology requires you to use a proxy for Cisco ISE to access external resources, configure the proxy details as needed.

Step 1 Navigate to Administration → System → Settings → Proxy → Policy Services.

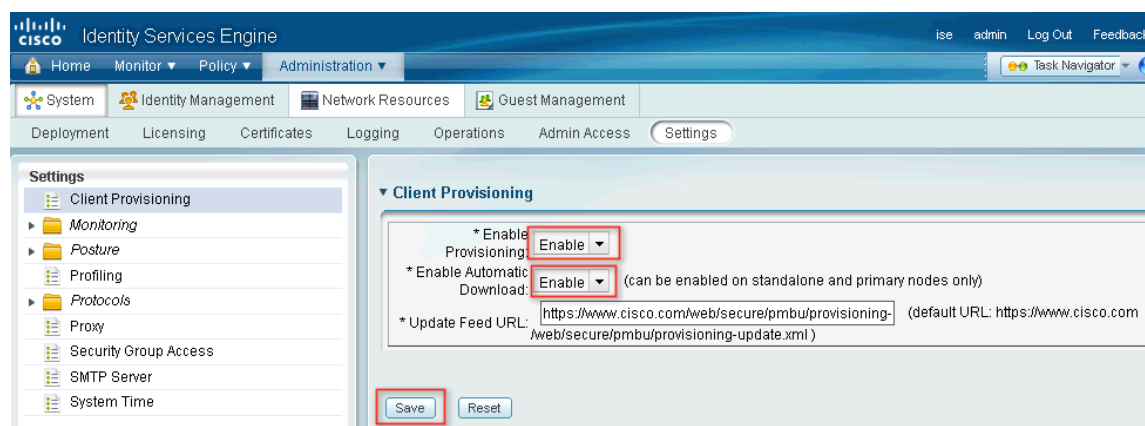


Step 2 Enter the proxy IP address or DNS resolvable host name in the **Proxy Address** field. Specify the appropriate port in the **Proxy Port** field.

Step 3 Click **Save**.

Step 4 Navigate to Administration → System → Settings → Client Provisioning.

Step 5 Click the Enable Provisioning drop-down menu and choose **Enable**.



Step 6 On the Enable Automatic Download option, click **Enable**.

Step 7 When enabling automatic downloads, be sure to specify the URL where Cisco ISE searches for system updates.

The default URL for downloading client-provisioning resources is shown on the GUI.

Step 8 Click **Save**.

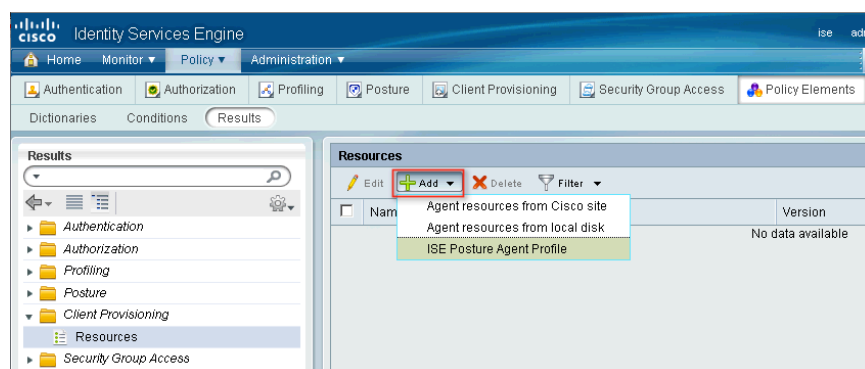
Cisco ISE automatically checks for updated resources every 24 hours, based on the time Cisco ISE was first installed.

Procedure 2 Configure Cisco ISE Posture Agent Profile.

Cisco recommends configuring agent profiles to control remediation timers, network transition delay timers, and the timer to control the login success screens on client machines.

Step 1 Navigate to Policy → Policy Elements → Results → Client Provisioning → Resources.

Step 2 Click Add and then ISE Posture Agent Profile.



Step 3 Specify a name for the Windows agent profile.

Step 4 Specify values for parameters, and specify whether these settings should merge with or overwrite existing profile settings as necessary based on the Windows client agent behavior.

Parameter Description	Parameter Value	Mode	Notes
VLAN detect interval in secs (<i>VlanDetectInterval</i>): (0-900):	5	overwrite	For OSX, if <i>EnableAgentIpRefresh</i> parameter is enabled, set this value to 5 or greater
Enable VLAN detect without UI? (<i>EnableVlanDetectWithoutUi</i>):	yes	overwrite	OSX: N/A
Disable Agent exit? (<i>DisableExit</i>):	no	merge	OSX: N/A
Allow CRL checks? (<i>AllowCRLChecks</i>):	yes	overwrite	OSX: N/A
Accessibility mode? (<i>AccessibilityMode</i>):	no	merge	OSX: N/A
Check signature? (<i>SignatureCheck</i>):	no	overwrite	OSX: N/A
Bypass summary screen? (<i>BypassSummaryScreen</i>):	yes	merge	OSX: N/A
MAC exception list (<i>ExceptionMACList</i>):		merge	OSX: N/A
Discovery host (<i>DiscoveryHost</i>):	ise.cts.local	overwrite	
Discovery host editable? (<i>DiscoveryHostEditable</i>):	yes	overwrite	OSX: N/A

Step 5 Click **Submit** to save the agent profile to Cisco ISE.

Procedure 3 Configure the Client Provisioning Policy.

Client provisioning resource policies determine which users receive which version of resources (agent, agent compliance modules, or agent customization packages/profiles) from Cisco ISE upon login and user session initiation.

Step 1 Navigate to Policy → Client Provisioning.

Step 2 Select from **Enable**, **Disable**, or **Monitor** from the behavior drop-down menu on the left of the policy rule.

Step 3 Enter a name for the new resource policy in the **Rule Name** field.

Step 4 Specify one or more **Identity Groups** to which a user who logs into Cisco ISE might belong.

Step 5 You can choose to specify any identity group type, or choose one or more groups from a list of existing Identity Groups previously configured.

Step 6 Use the **Operating System** field to specify one or more operating systems that might be running on the client machines.

Step 7 You can choose to specify one [e.g., Mac OS X] or an umbrella [e.g., Windows 7 (ALL)].

Step 8 In the **Other Conditions** portion of the client provisioning resource policy, specify a new expression you want to create for this particular resource policy.

Step 9 Specify agent type, compliance module, customization package, and profile to provision the client machine based on categories defined earlier.

Step 10 Click **Save**.

Procedure 4 Configure the Authorization Policy for Client Provisioning and Posture Compliance.

The authorization policy sets the types of access and services to be granted to endpoints based on their attributes such as identity, access method, and compliance with posture policies.

Step 1 First configure a DACL for the authorization policy.

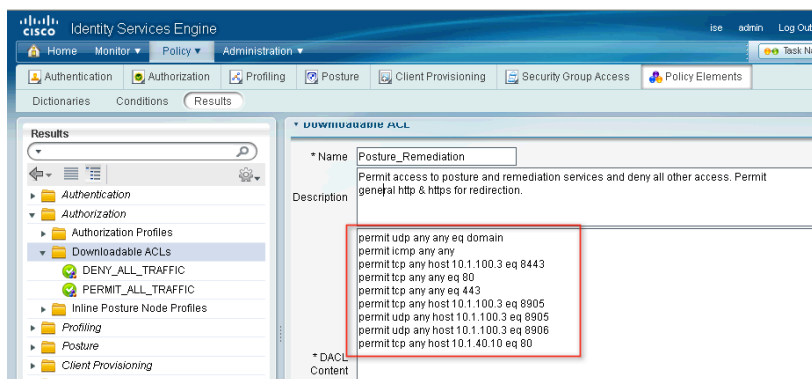
Step 2 Navigate to Policy → Policy Elements → Results and double-click Authorization.

Step 3 Select **Downloadable ACLs** from the left pane.

Step 4 Click **Add** from the right pane under DACL Management, configure a name and description for the dACL, and enter the values required by your network policy.

Example:

```
permit udp any any eq domain
permit icmp any any
permit tcp any host 10.1.100.3 eq 8443
permit tcp any any eq 80
permit tcp any any eq 443
permit tcp any host 10.1.100.3 eq 8905
permit udp any host 10.1.100.3 eq 8905
permit udp any host 10.1.100.3 eq 8906
permit tcp any host 10.1.40.10 eq 80
```



Step 5 Click **Submit** to save the configuration changes for the DACL.

Step 6 On the access switch, a URL redirect ACL must be created.

Example:

```
3k-access# conf t
3k-access(config)# ip access-list extended ACL-POSTURE-REDIRECT
3k-access(config-ext-nacl)# deny udp any any eq domain
3k-access(config-ext-nacl)# deny udp any host 10.1.100.3 eq 8905
3k-access(config-ext-nacl)# deny udp any host 10.1.100.3 eq 8906
3k-access(config-ext-nacl)# deny tcp any host 10.1.100.3 eq 8443
3k-access(config-ext-nacl)# deny tcp any host 10.1.100.3 eq 8905
3k-access(config-ext-nacl)# deny udp any host 10.1.40.10 eq www
3k-access(config-ext-nacl)# permit ip any any
```

This ACL will be called by the Authorization Profile and work in conjunction with the accompanying DACL applied to the switchport interface.

Step 7 Navigate to Policy → Policy Elements → Results → Authorization.

Step 8 Click **Add** and enter the values for the authorization profile as required.

The screenshot shows the Cisco TrustSec Policy Elements configuration interface. The 'Results' tab is selected, and the 'Authorization' section is expanded. The 'Common Tasks' section shows 'DACL Name' set to 'Posture_Remediation' and 'Posture Discovery' checked with 'ACL' set to 'ACL-POSTURE-REDIRECT'. The 'Attributes Details' section shows 'Access Type = ACCESS_ACCEPT', 'DACL = Posture_Remediation', and two 'cisco-av-pair' attributes for URL redirection.

The values configured for the dACL name and Posture Discovery fields should match with the previously configured DACL and redirect ACL.

Step 9 Click Submit.

Procedure 5 Define a new Authorization Profile for web-authenticated/Web Agent users named CWA_Posture_Remediation.

Step 1 Navigate to Authorization Profiles under Policy → Policy Elements → Results → Authorization.

Step 2 Click **Add** from the right pane and enter values for the authorization profile.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The left pane displays the navigation tree with 'Authorization Profiles' selected. The main pane shows the configuration for the 'CWA_Posture_Remediation' profile. The 'Name' field is 'CWA_Posture_Remediation', the 'Description' is 'Permit Access To Posture And Remediation Services; Redirect Traffic To Central Web Auth Services', and the 'Access Type' is 'ACCESS_ACCEPT'. Under 'Common Tasks', 'DACL Name' is set to 'Posture_Remediation', 'VLAN' is unchecked, 'Voice Domain Permission' is unchecked, 'Posture Discovery' is unchecked, 'Centralized Web Authentication' is checked with 'ACL' set to 'ACL-POSTURE-REDIRECT' and 'Redirect' set to 'Default', and 'Auto Smart Port' is unchecked.

The attribute details would be similar to the following output:

The screenshot shows the 'Attributes Details' section of the configuration. The attributes are listed as follows:

```
Access Type = ACCESS_ACCEPT
DACL = Posture_Remediation
cisco-av-pair = url-redirect-acl=ACL-POSTURE-REDIRECT
cisco-av-pair = url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionIdValue&
action=cwa
```

Step 3 Click **Submit** to apply your changes.

Note: The difference between the two profiles is the URL Redirect cisco-av-pair attribute. Users that need to be authenticated using CWA will be initially redirected to the guest portal for web authentication (cwa) and then automatically redirected to the Client Provisioning Portal (cpp) as needed. Users authenticating through 802.1X will be redirected directly to the Client Provisioning Portal.

Step 4 Update the authorization policy to support posture compliance. Navigate to **Policy → Authorization**.

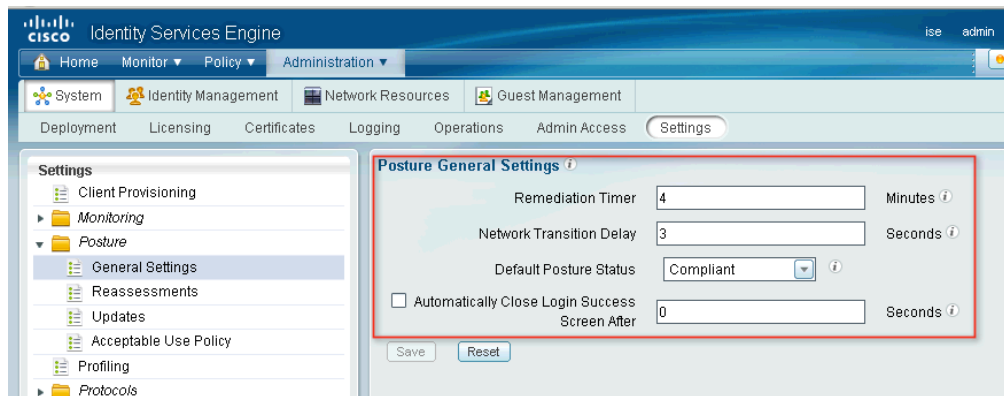
Step 5 Configure authorization policies for compliant and noncompliant network users.

Step 6 Click **Save** to apply your changes.

Procedure 6 Configure the Posture Subscription and Policy.

The posture general settings for agents on Windows and Macintosh clients can be configured in client provisioning resources. You can configure the Remediation Timer, Network Transition Delay, Default posture status, and timeout for the Successful Login Screen.

Step 1 Navigate to Administration → System → Settings → Posture → General Settings.

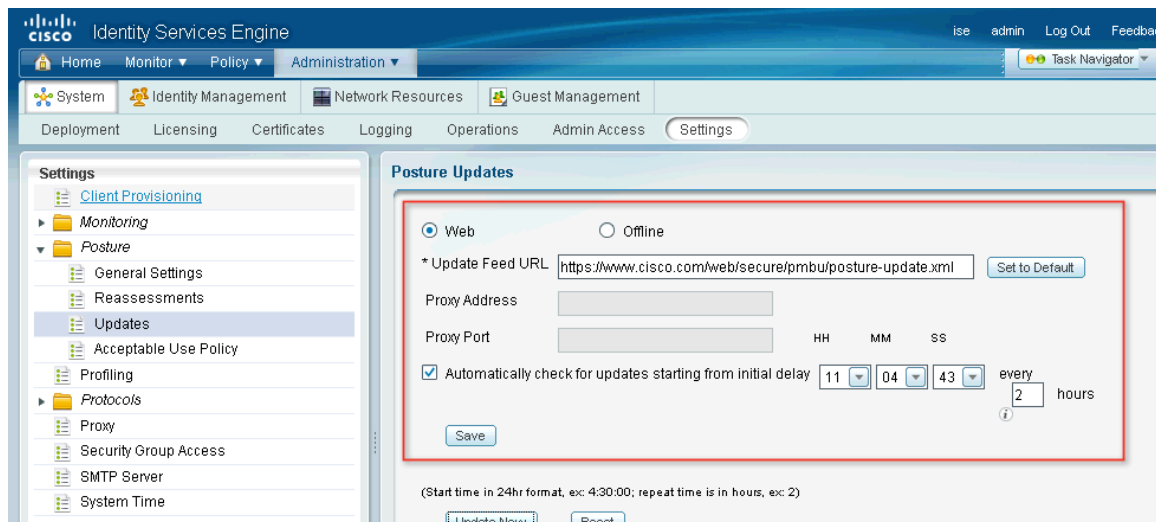


Step 2 Click **Save** to save your settings.

Procedure 7 Configure Dynamic Updates.

Updates for posture include a set of predefined checks, rules, antivirus, and antispyware support charts. You can download posture updates from Cisco to your Cisco ISE deployment through the web dynamically, as well as configure updates to occur automatically.

Step 1 Navigate to Administration → System → Settings → Posture → Updates.



Step 2 Choose the **Web** option to download updates dynamically.

Step 3 Modify the values on the posture update page based on network requirements. For example, configure proxy settings if necessary.

Step 4 Click the **Update Now** button to download the update from Cisco. Then click Ok.

Note: Downloading updates from the web may take a few minutes for the first time to update the Cisco ISE server. While the updates progress, you can leave the updates page to continue to other tasks in Cisco ISE. A warning is displayed if an update is already in progress.

Procedure 8 Configure an Acceptable Use Policy (AUP).

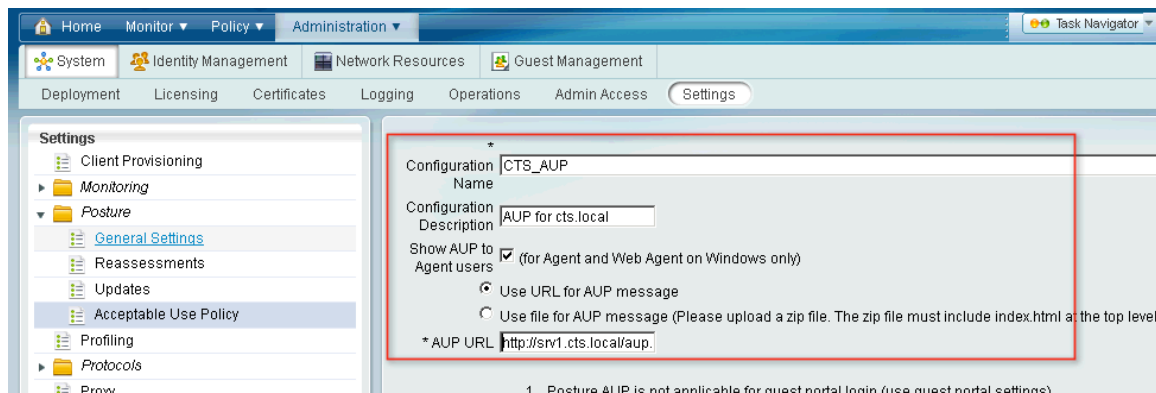
After login and successful posture assessment of clients, the NAC agents and Web agents display a temporary network access screen. The link presented there redirects end users to the AUP page, where you define your network usage terms and conditions that the end users must read and accept.

To create an acceptable use policy, complete the following:

Step 1 Navigate to Administration → System → Settings → Posture → Acceptable Use Policy.

Step 2 Click **Add**.

Step 3 Modify the values on the Acceptable use policy configuration as per requirements.



Step 4 Click **Submit** to create an AUP configuration.

Procedure 9 Create a simple condition.

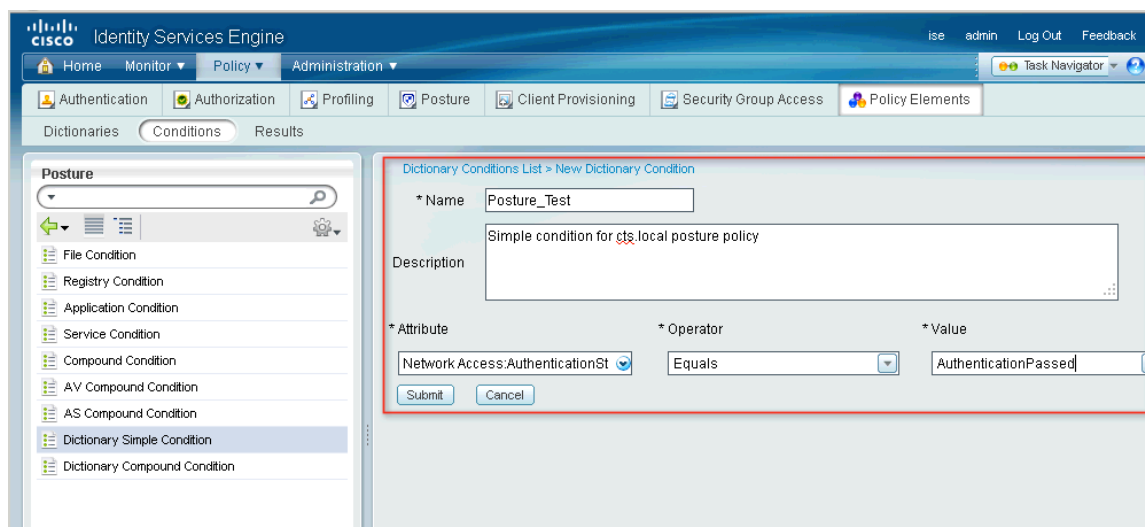
You can create a dictionary simple condition for use with a client posture policy.

Step 1 Navigate to Policy → Policy Elements → Conditions → Posture.

Step 2 From the posture menu, choose **Dictionary Simple Condition**.

Step 3 Click **Add**. Then click **Submit**.

Modify the values of the new dictionary condition based on network requirements:



Procedure 10 Configure a client Posture Policy.

You can create a dictionary simple condition for use with a client posture policy.

Step 1 Navigate to Policy → Posture.

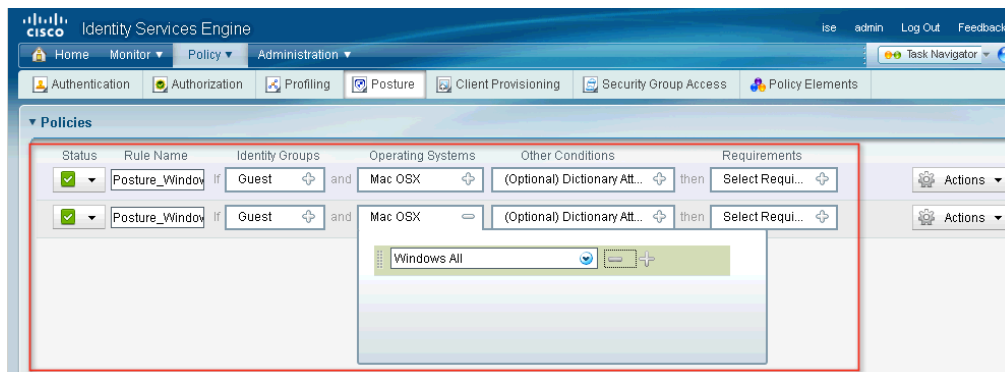
Step 2 Select the **Actions** menu and select **Insert New Policy**.

Step 3 Configure a **Name** for the policy and then select an **Identity Group**, **Operating System**, **Condition**, and then **Requirement** for the policy.

Step 4 From the posture menu, choose **Dictionary Simple Condition**.

Step 5 Click **Add**.

Modify the values of the new dictionary condition based on network requirements:



Step 6 Click **Save** to save the posture policy.

Cisco NAC Agent 4.9.0 Discovery Process

In Cisco NAC Agent 4.9.0, the discovery loop has the following flow:

1. http discovery probe on port 80 to discovery host (ISE with HTTP Redirect)
2. https discovery probe on port 8905 to discovery host (if configured)(ISE & NAC Appliance)
3. http discovery probe on port 80 to default gateway(ISE with HTTP Redirect)
4. https discovery probe on port 8905 to default gateway (NAC Appliance)
5. L2 UDP Swiss discovery probe port 8905 to default gateway (NAC Appliance)
6. L3 UDP Swiss discovery probe port 8906 to discovery host (if configured)(NAC Appliance)
7. https reconnect probe on port 8905 to previously contacted FQDN: ISE PSN or NAC Server (ISE & NAC Appliance)
8. GoTo 1

The agent discovery process specific to Cisco ISE only follows:

1. http discovery probe on port 80 to discovery host, if configured (via HTTP Redirect)
2. https discovery probe on port 8905 to discovery host, if configured
3. http discovery probe on port 80 to default gateway (via HTTP Redirect)
4. https reconnect probe on port 8905 to previously contacted Cisco ISE Policy Services node
5. GoTo 1

Lesson Learned: If there is a Windows Client that has two NICs enabled, where Windows has an equal administrative distance for both NICs (i.e.: both NICs connected at 100 Mbps): The routes from the Windows stack might collide and cause posture to happen on one NIC, and the user traffic may get redirected via the other NIC.

This is not a problem for OSX, because the Network Preferences in OSX defines the order of preferred connections.

If the Windows Client uses Cisco AnyConnect Network Access Module (NAM), this problem does not exist because Cisco AnyConnect NAM does not allow multiple NICs to be connected at the same time.

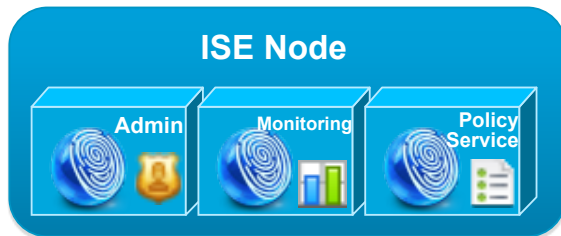
Appendix A: Cisco ISE Design Notes

The number of possible endpoints is the single most important aspect of Cisco ISE design. There are multiple deployment models:

Standalone:

All services are run on a single Cisco ISE node. It supports up to 2000 endpoints (Figure A1).

Figure A1 Standalone ISE Node



Basic 2-Node Deployment:

Both Cisco ISE Nodes run all services for redundancy. They support up to 2000 endpoints (Figure A2).

Figure A2 A Simple, 2-Node Distributed ISE Deployment for Redundancy

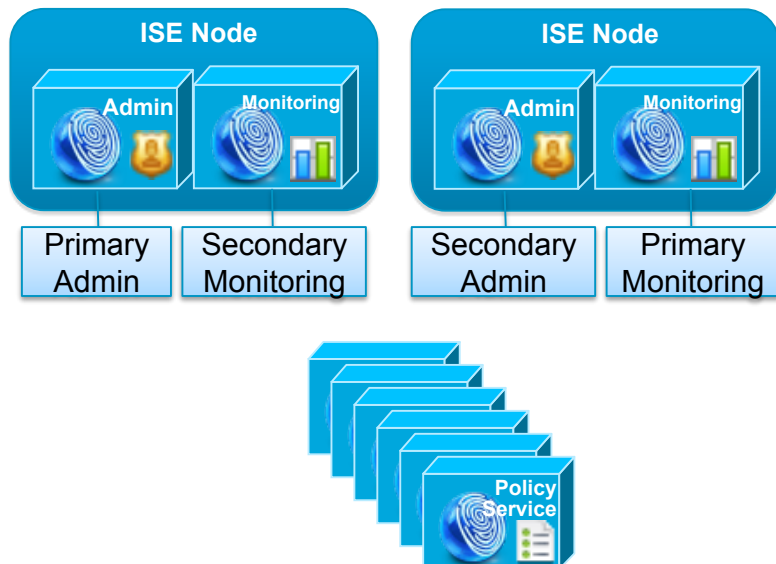


Distributed Deployment, Up to 10,000 Endpoints

“Administrative” personas are shared. The Dedicated Policy Service Nodes follow (Figure A3):

- Two Cisco ISE Nodes for Admin + Monitoring functions
- Up to Five Policy Service Nodes

Figure A3 A Distributed ISE Deployment for Scaling



Distributed Deployment, Up to 100,000 Endpoints

Dedicated Cisco ISE nodes for each persona follow:

- Two Admin nodes
- Two Monitoring Nodes
- Up to 40 Policy Service Nodes

Figure A4 Maximum ISE 1.0 Distributed Deployment



Figure A5 Policy Service Sizing and Performance

	Platform	Max Endpoints	Max Profiler Events
Physical	3315	3,000	500/sec
	3355	6,000	500/sec
	3395	10,000	1200/sec
Virtual	VM	10,000 *	TBD

* Sizing guidance based on matching/exceeding specification of the physical appliance.

Figure A6 Policy Service Node Performance (authentications/second)

PAP/ASCII	1431
EAP-MD5	600
EAP-TLS	335 internal, 124 LDAP
LEAP	455
MSCHAPv1	1064 internal, 361 AD
MSCHAPv2	1316 internal, 277 AD
PEAP-MSCHAPv2	181
PEAP-GTC	196 AD, 188 LDAP
FAST-MSCHAPv2	192
FAST-GTC	222
Guest (web auth)	17
Posture (3315)	70
Posture (3355)	70
Posture (3395)	110

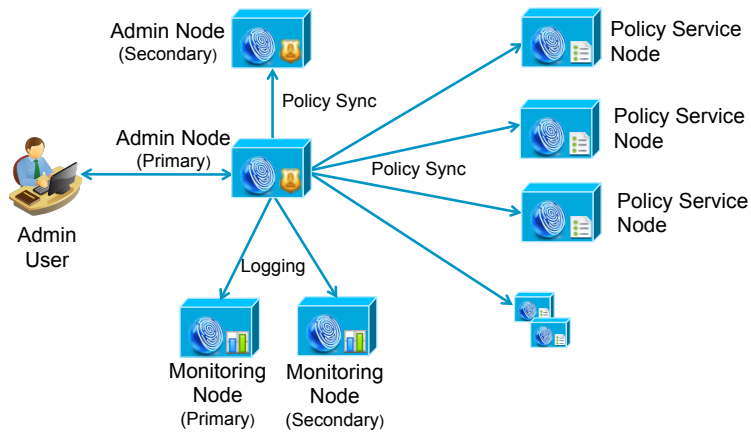
Figure A7 Monitoring Node Performance

Max syslogs (3395)	1000/sec
Max sessions per day	2 million
Authentications per day	2 million
Max stored alarms	5000

Figure A8 Bandwidth Requirements

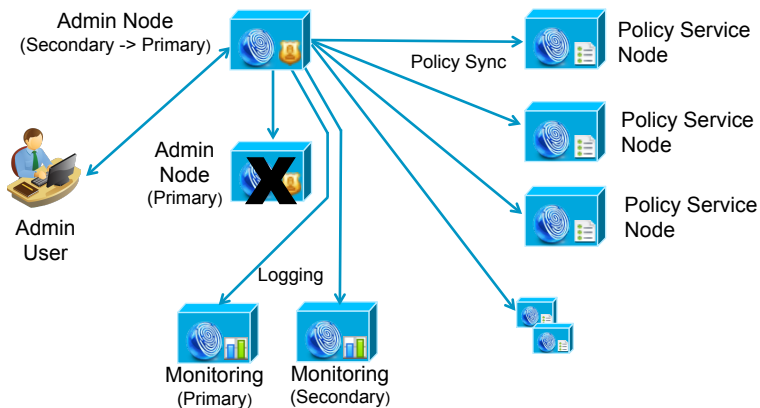
Connection Between:	Minimum Bandwidth
Administration and Monitoring	256Kbps
Redundant Monitoring pair	256Kbps
Policy Services and Administration	256Kbps
Policy Services and Monitoring	1 Mbps
Endpoint and Policy Services (posture)	125bps per endpoint

Figure A9 Administration HA and Synchronization I



Changes made via the Primary administration node are automatically synchronized to the Secondary administration node and all ISE policy service nodes (PSNs).

Figure A10 Administration HA and Synchronization II



Upon failure of the Primary administration node, the admin user can connect to the Secondary administration node; all changes via backup administration node are automatically synchronized to all policy service nodes (PSNs).

The Secondary administration node must be manually promoted to Primary.

Figure A11 Monitoring – Distributed Log Collection

- ISE supports distributed log collection across all nodes to optimize local data collection , aggregation, and centralized correlation and storage.
- Each ISE node collects logs locally from itself; Policy Service nodes running Profiler Services may also collect log (profile) data from NADs.
- Each node buffers and transports collected data to each Monitoring node as Syslog
- NADs may also send Syslog directly to Monitoring node on UDP/20514 for activity logging, diagnostics, and troubleshooting.

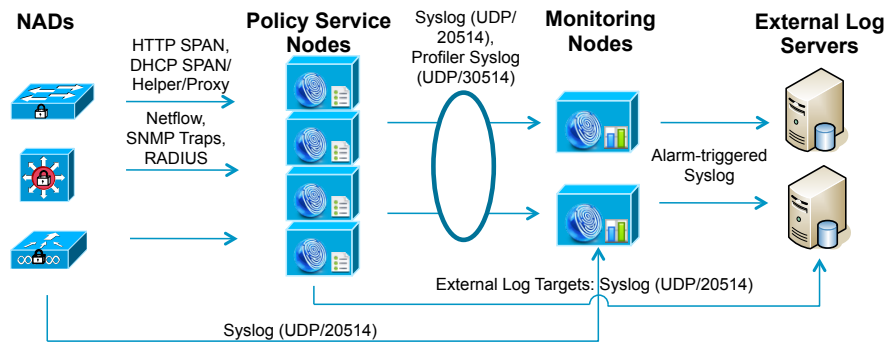


Figure A12 Policy Service Node (PSN) Scaling and Redundancy

- NADs can be configured with redundant RADIUS servers (Policy Service nodes).
- Policy Service nodes can also be configured in a cluster, or “node group”, behind a load balancer. NADs send requests to LB virtual IP for Policy Services.
- Policy Service nodes in node group maintain heartbeat to verify member health.

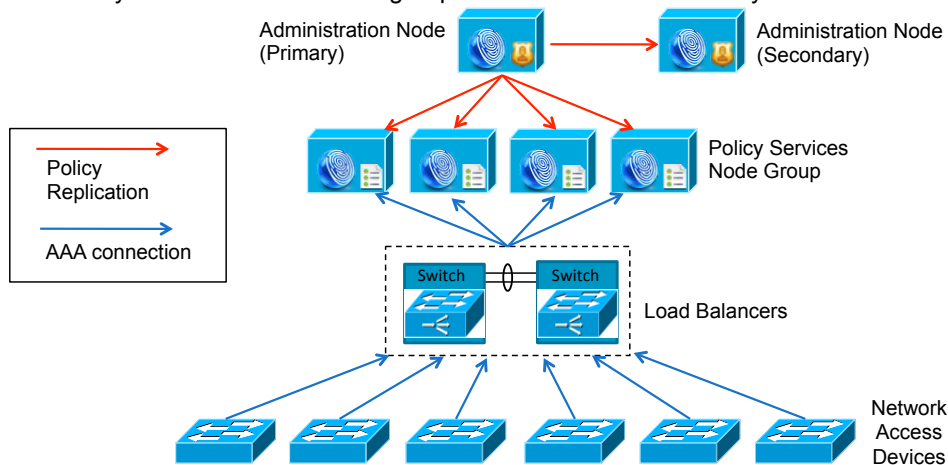


Figure A13 Typical SMB-sized ISE Deployment (> 2,000 Endpoints)

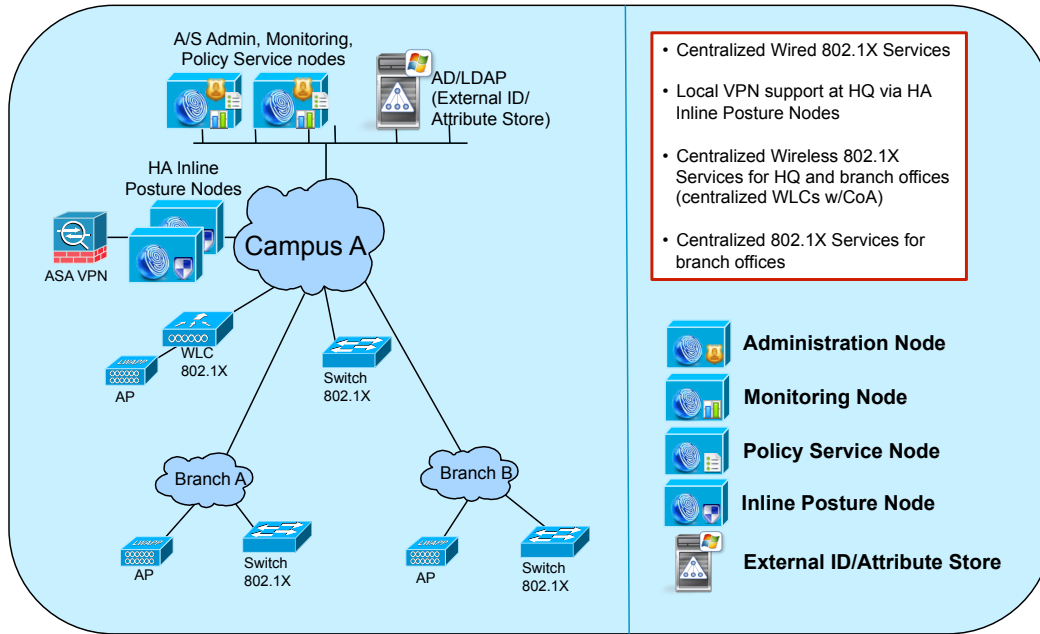


Figure A14 Typical Medium-sized ISE Deployment (< 10,000 Endpoints)

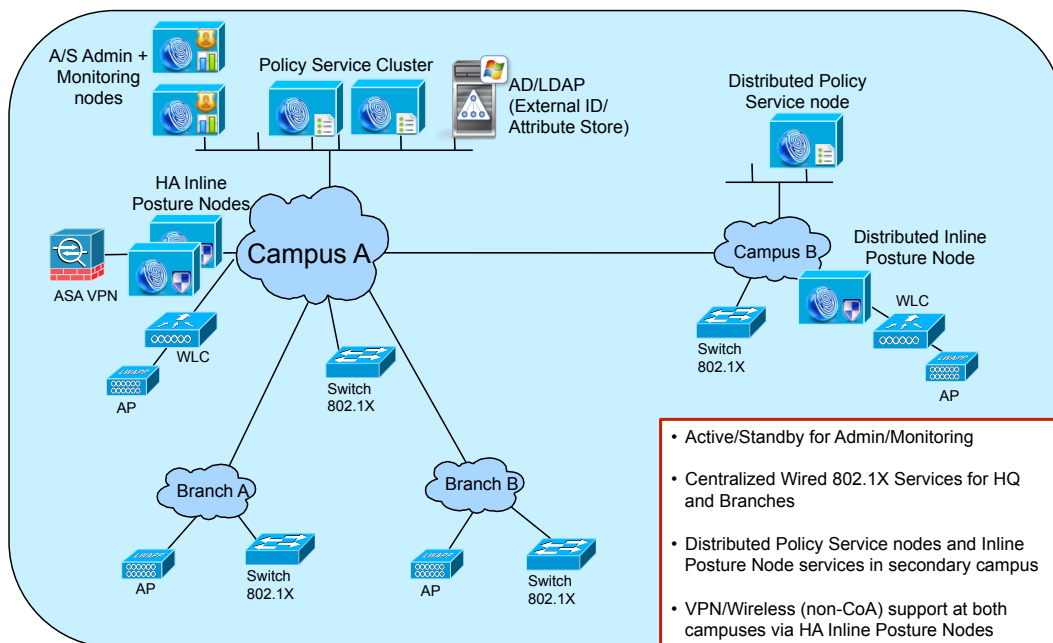
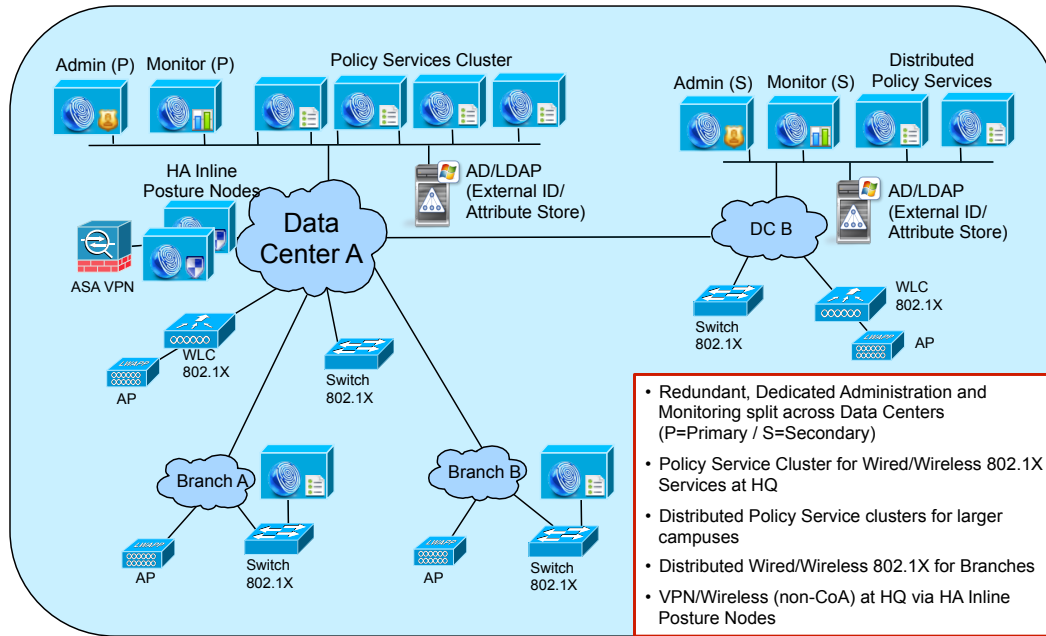


Figure A15 Typical Enterprise-sized ISE Deployment (> 10,000 Endpoints)



Appendix B: References

- Cisco Unified Communications Manager 8 Security Configuration Guide:
http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/cucos/8_0_1/cucos/iptpch6.html#wp1055278
- Cisco ISE 1.0 User Guide:
http://www.cisco.com/en/US/docs/security/ise/1.0.4/user_guide/ise104_user_guide.html

Switch Configuration Guides:

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html
- For Cisco Wireless LAN Controllers:
http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html