

**Network Access > Policy Sets**). The typical best practice is to dedicate a policy set for remote access policies, instead of blending them with a wired or wireless policy set. It makes it easier when troubleshooting, and avoids confusion when designing the policies.

[Figure 19-25](#) shows an example policy set for VPN devices, with a generic authorization rule that sends a RADIUS Access-Accept if the user is a member of the Employees group in Active Directory.

**Note** Always check with your company's security requirements, because a generic authorization rule might not be adequate in some cases. Many companies use an external identity store to authenticate against a two-factor authentication server.

The screenshot shows the ASA Policy Sets configuration interface. On the left, there is a sidebar with options like 'Summary of Policies', 'Global Exceptions', and several mode policies ('ATW-VPN', 'VPN Policy Set', 'Wireless', 'Monitor Mode', 'Low-Impact Mode', 'Closed Mode', 'Default'). The 'ATW-VPN' policy is selected. The main pane displays the configuration for the 'ATW-VPN' policy set:

Status	Name	Description	Conditions
<input checked="" type="checkbox"/>	ATW-VPN	VPN Policy Set	DEVICE:Device Type STARTS WITH Device Type#All Device Types#VPN

**Authentication Policy**

Default Rule (If no match)		Allow Protocols	and use
<input checked="" type="checkbox"/>	Allow Network Access	: Default Network Access	: All_User_ID_Stores

**Authorization Policy**

Exceptions (0)

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Employee-Permit	if AD-Employees	then PermitAccess
<input checked="" type="checkbox"/>	Default	If no matches, then	DenyAccess

**Figure 19-25** Sample Basic RA-VPN Policy Set

This very simple policy is all you need to get the VPN authentication and authorization to work. Of course, the policy can be tuned and made much more specific to the needs of your organization. For instance, you can add posture assessment to the policy, as described later in the chapter.

## Testing the Configuration

To test your configuration, the first test you should perform is a basic AAA test from the ASA to ISE, to ensure you have everything configured correctly for authentication and authorization. After that, you will log in to the portal on the ASA to download and install AnyConnect. Lastly, you will connect to the VPN and verify that you have full connectivity.

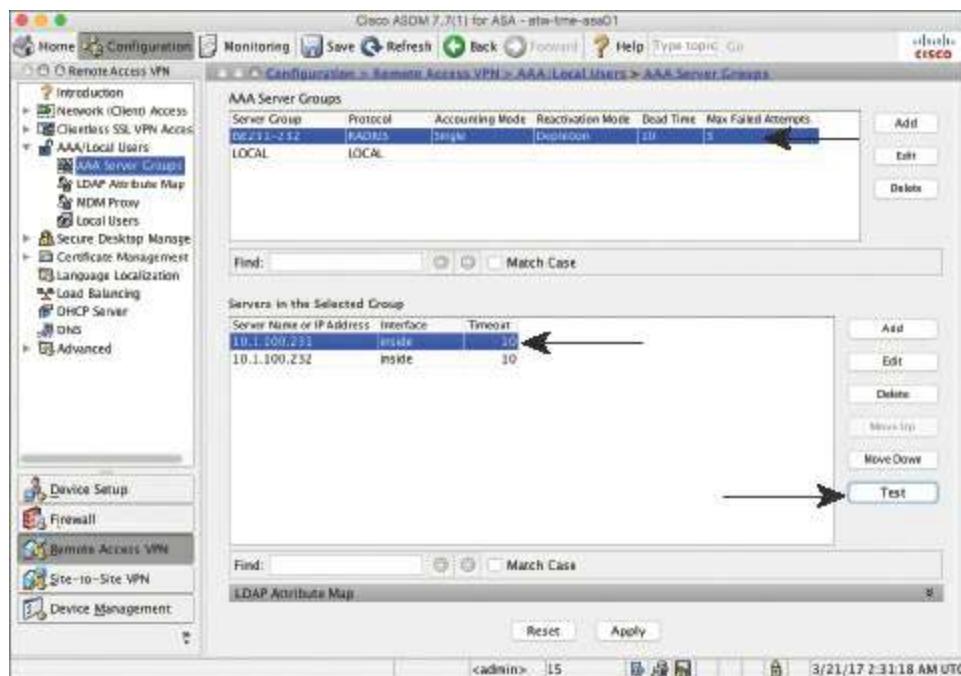
### Perform a Basic AAA Test

The first test is to perform a basic AAA test. From the ASDM GUI:

**Step 1.** Navigate to Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups.

**Step 2.** Select the server group you configured earlier in the chapter.

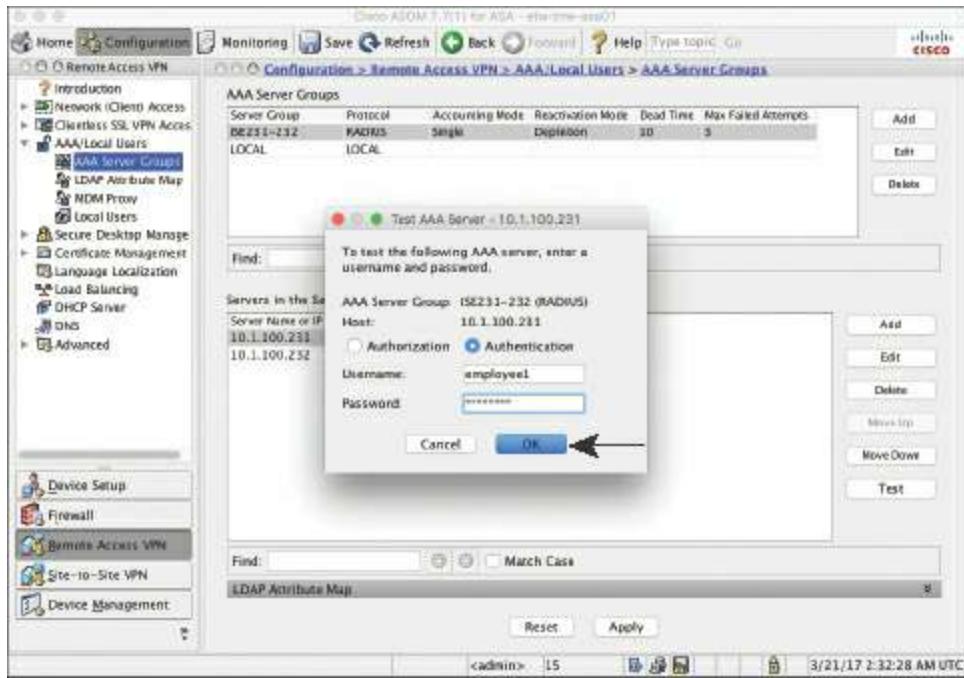
**Step 3.** Select one of the PSNs you added to the AAA Server Group, as shown in [Figure 19-26](#).



**Figure 19-26** Testing from the AAA Server Groups Window

**Step 4.** Click Test.

**Step 5.** In the Test AAA Server dialog box, shown in [Figure 19-27](#), choose **Authentication**, which actually tests both authentication and authorization because RADIUS performs both within a single transaction.



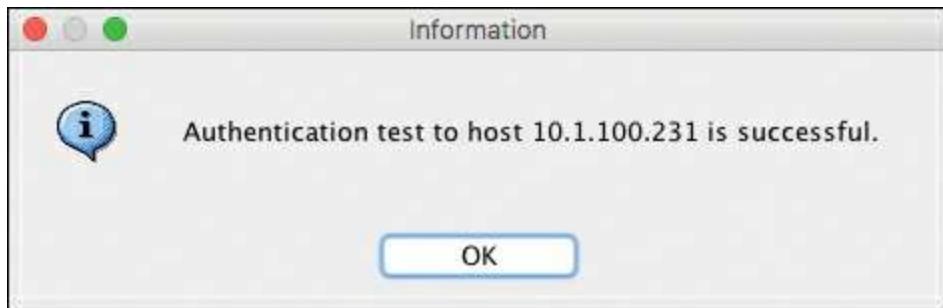
**Figure 19-27** Test AAA Server Window

**Step 6.** In the Username field, enter the username from Active Directory of the user who should receive an Access-Accept.

**Step 7.** Enter the user's password.

**Step 8.** Click **OK** to perform the test.

**Step 9.** If all is configured correctly, you see a success message such as the one shown in [Figure 19-28](#).



**Figure 19-28** Successful Test

## Log In to the ASA Web Portal

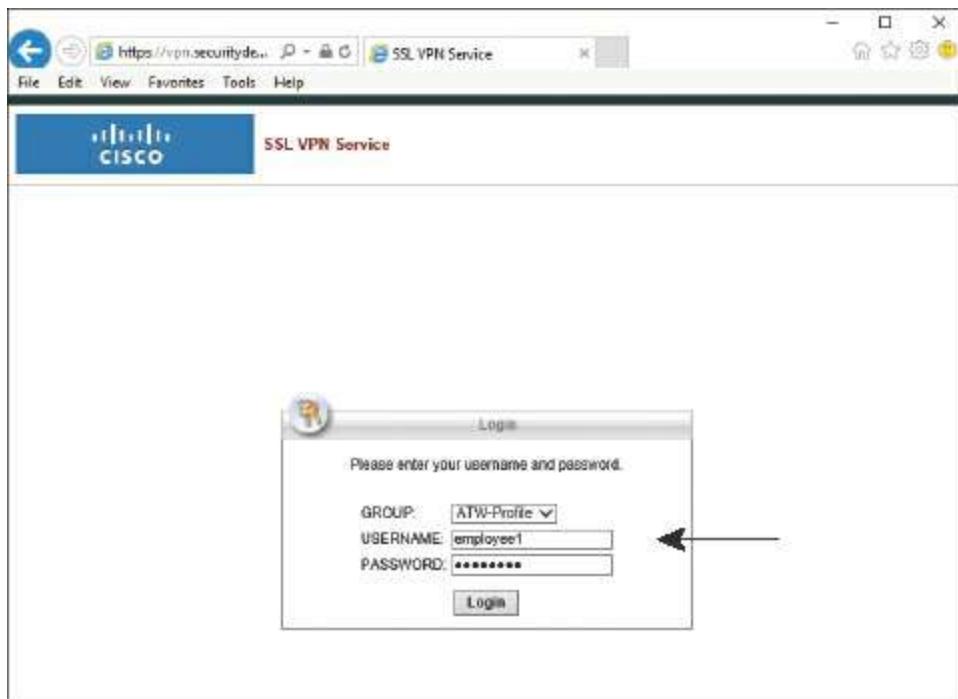
After confirming the AAA configuration in the ASA and in ISE is all correct, the next test is to log in to the web portal, where you can download and install AnyConnect. From an endpoint that can access the outside of your ASA:

**Step 1.** Open a web browser and navigate to the outside IP address of your ASA using HTTPS. For example: <https://vpn.securitydemo.net/>.

The URL automatically changes to /+CSCOE+/logon.html#.

**Step 2.** In the portal, log in with a username and password, as shown in [Figure 19-29](#).

The username and password are sent to ISE via a RADIUS Access-Request.



**Figure 19-29** ASA Web Portal

**Step 3.** Logging in to the portal automatically launches an ActiveX applet (Windows) or a Java applet (non-Windows) that installs AnyConnect.

- If the applet fails to launch, you can download the manual installer directly from the portal.
- If the endpoint already has AnyConnect installed, the applet connects the VPN using the credentials entered into the portal.

**Step 4.** After AnyConnect installs or launches, you are logged in to the VPN with the tunnel established, as shown in [Figure 19-30](#).



**Figure 19-30** AnyConnect Established VPN

Also, don't forget to check the ISE RADIUS Live Logs to see the AAA from ISE's perspective, as illustrated in [Figure 19-31](#).

Live Logs									
Misconfigured Supplicants		Misconfigured Network Devices		RADIUS Drops		Client Stopped Responding		Repeat	
0		0		0		0		0	
<input type="checkbox"/> Refresh	<input checked="" type="radio"/> Reset Repeat Counts	<input type="button" value="Export To"/>							
Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	Network Device
x			Identity	Endpoint ID	Endpoint Prof	Authentication	Authorization	Authorization	Network Device
<span style="color: blue;">●</span>	<span style="color: blue;">○</span>	0	employee1	00:0C:29:D6:91:69	Workstation	ATW-VPN >...	ATW-VPN >...	PermitAccess	
<span style="color: green;">●</span>	<span style="color: green;">○</span>		employee1	00:0C:29:D6:91:69	Workstation	ATW-VPN >...	ATW-VPN >...	PermitAccess	ATW-TME-5515
<span style="color: red;">●</span>	<span style="color: red;">○</span>		employee1	00:0C:29:D6:91:69		ATW-VPN >...			ATW-TME-5515
<span style="color: blue;">●</span>	<span style="color: blue;">○</span>	0	employee1	10.117.118.215		ATW-VPN >...	ATW-VPN >...	PermitAccess	
<span style="color: green;">●</span>	<span style="color: green;">○</span>		employee1	10.117.118.215		ATW-VPN >...	ATW-VPN >...	PermitAccess	ATW-TME-5515
<span style="color: green;">●</span>	<span style="color: green;">○</span>		employee1	10.117.118.215		ATW-VPN >...	ATW-VPN >...	PermitAccess	ATW-TME-5515
<span style="color: green;">●</span>	<span style="color: green;">○</span>		employee1			ATW-VPN >...	ATW-VPN >...	PermitAccess	ATW-TME-5515

**Figure 19-31** Live Log

## Connect to the VPN via AnyConnect

The third and final test is to connect to the VPN directly from AnyConnect. From the endpoint that can access the outside of your ASA, which now has AnyConnect

installed:

**Step 1.** Launch the AnyConnect Secure Mobility Client.

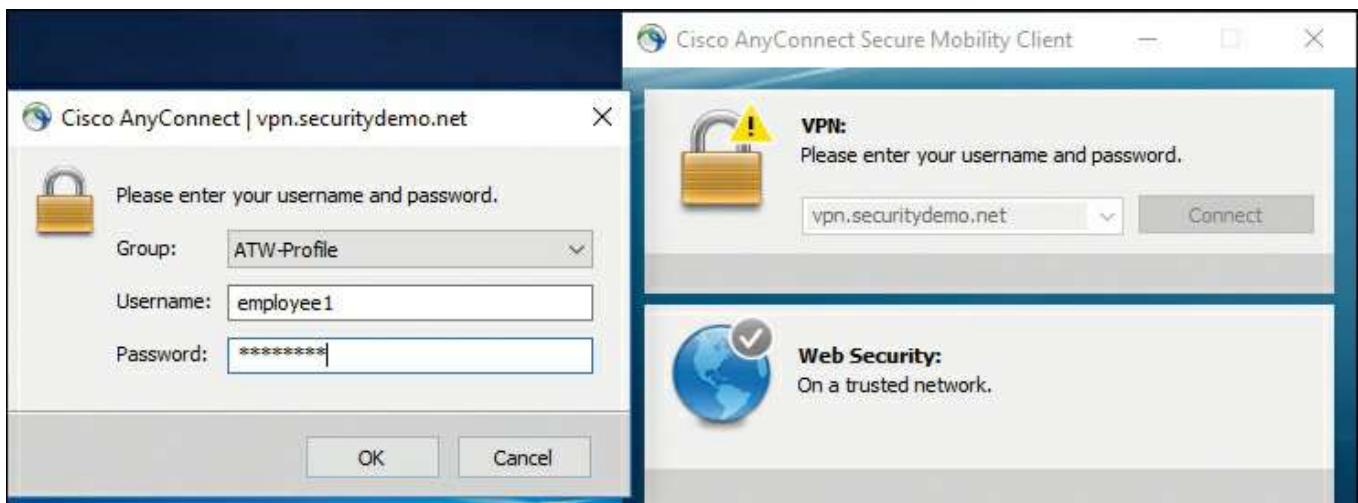
**Step 2.** Enter the FQDN of the ASA's outside interface or the IP address itself into the VPN connection field, as shown in [Figure 19-32](#).



**Figure 19-32** Ready to Connect

**Step 3.** Click Connect.

**Step 4.** Enter your username and password in the popup window, as shown in [Figure 19-33](#).



**Figure 19-33** Enter Your Username and Password

**Step 5.** Click OK.

The VPN establishes and AnyConnect minimizes itself by default.

**Step 6.** Click the AnyConnect icon in the system tray to bring the client user interface back up.

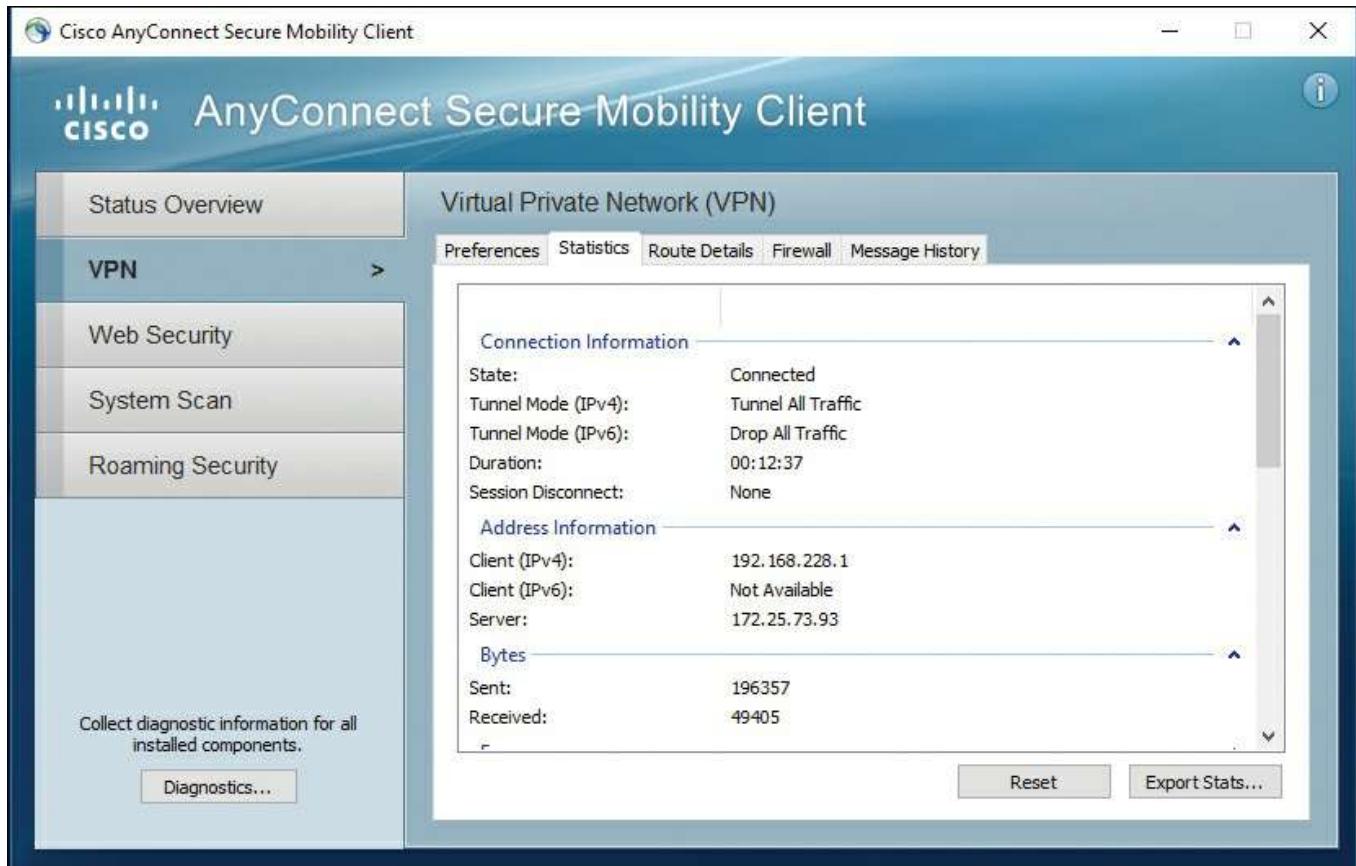
**Step 7.** Click the gear icon in the bottom-left corner of the AnyConnect client to bring up the status window, as shown in [Figure 19-34](#).



**Figure 19-34** Status Overview

You can see in [Figure 19-34](#) that AnyConnect was assigned an IPv4 address from the client pool configured earlier (192.168.228.1).

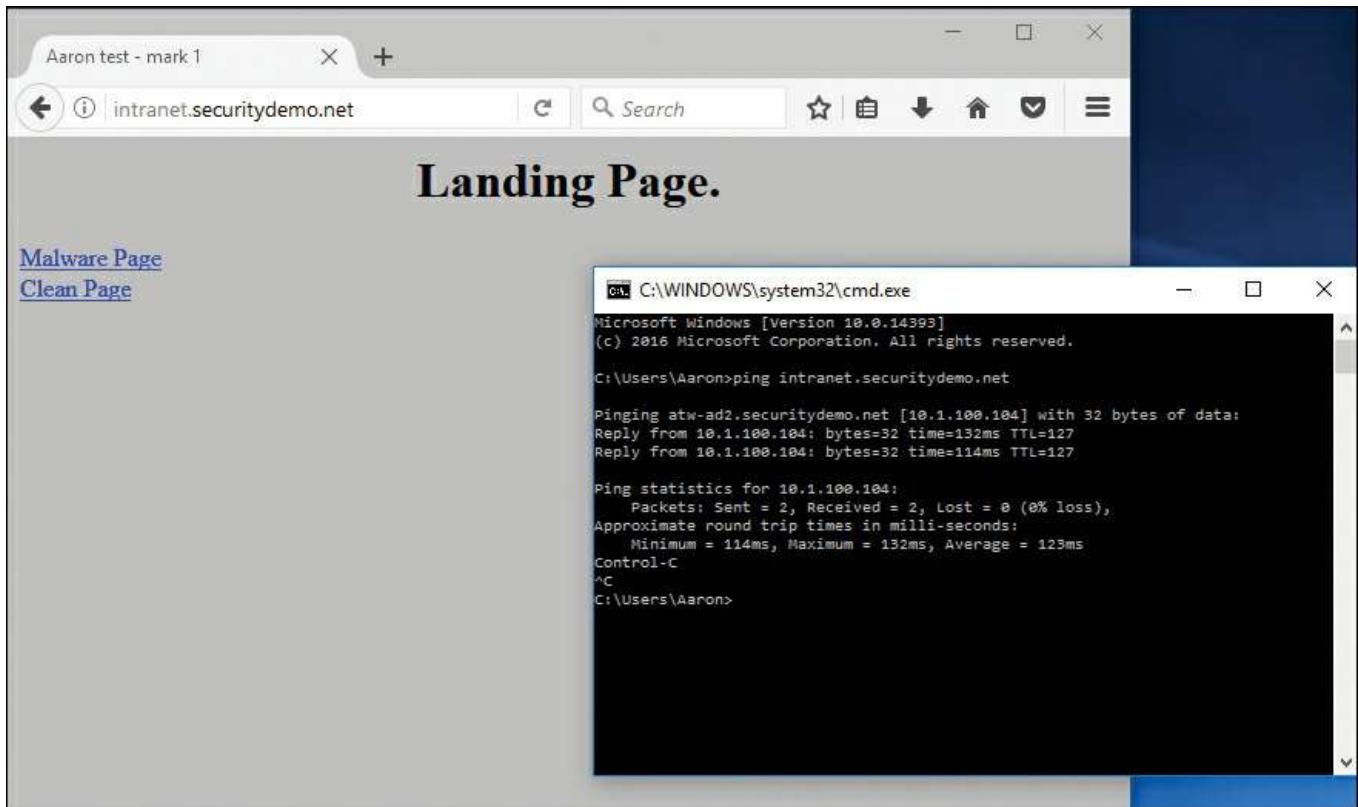
**Step 8.** Choose **VPN > Statistics** to see more connection information about the VPN, as shown in [Figure 19-35](#).



**Figure 19-35** VPN Statistics

Finally, it's time to verify connectivity by trying to connect to a server in the corporate network.

**Step 9.** Using the web browser, connect to a server, as shown in [Figure 19-36](#).



**Figure 19-36** Successful Connectivity to an Internal Server

As you can see by the successful ping and successful web browsing to an internal server, the VPN connection is successful, and return traffic is also flowing back to the client.

## Remote Access VPN and Posture

Thus far, we have focused on the ASA for remote access purposes only. However, as you well know, this is an ISE book! There is a lot more to network access nowadays than just basic authentication and authorization and the passing of traffic.

As you read in [Chapter 15, “Client Posture Assessment,”](#) ISE posture assessment helps ensure that your endpoints are in compliance with your organization’s host security policy. Posture assessment allows you to check the security “health” of your PC and Mac clients. This includes checking for the installation, running state, and last update for security software such as antivirus, antimalware, and personal firewall. With the ASA, there are two ways to perform this health check.

First, the ASA can use a function called HostScan, which is also available in the AnyConnect client as the VPN Posture (HostScan) module. This module performs the function of examining the endpoint software and patch installations, reporting the results back to the ASA. In this instance, the ASA is the policy server and the HostScan results are run through the Dynamic Access Policy (DAP), which will make changes to the endpoint’s level of access. Examples of the changes are to apply ACLs, change settings

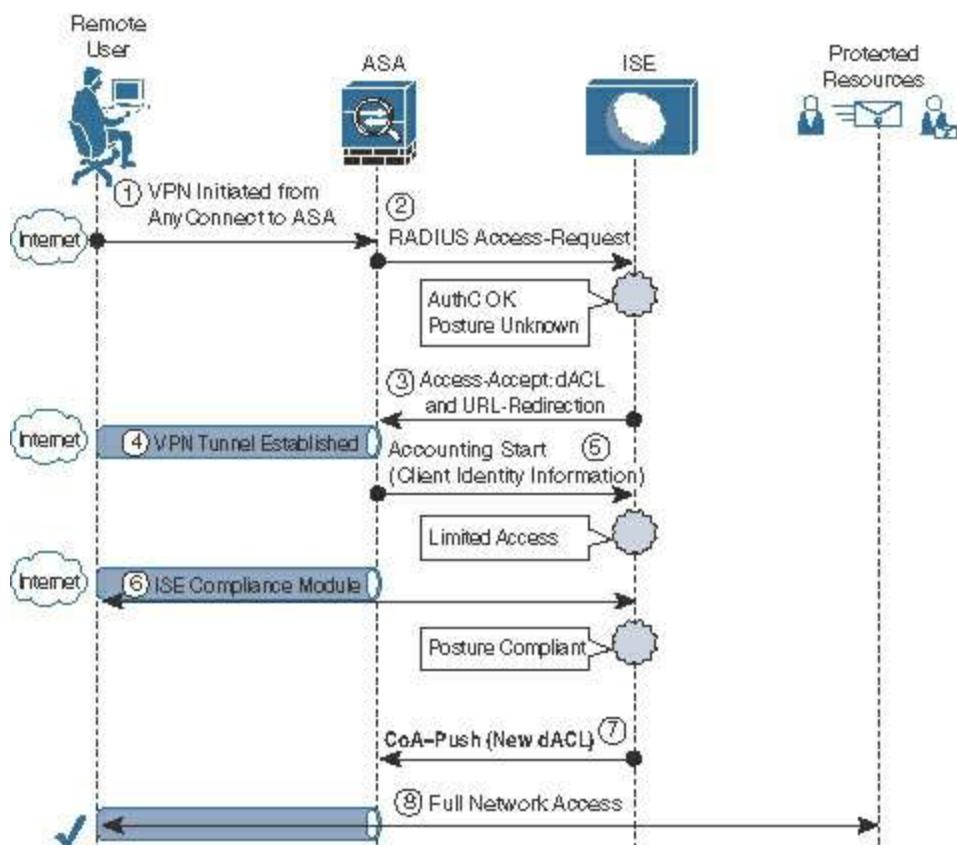
in the web portal (clientless VPN), and quarantine the endpoint, among many other choices. However, all that fun you can have with DAP does nothing to tie into a single pane of glass for policy, or leverage the centralized control that you spent so much time creating throughout the many chapters of this book and beyond.

Therefore, the focus of this section is entirely on the other method to provide posture with the ASA: using the ISE compliance module in AnyConnect, also known as the System Scan module. This module is exactly the same as what you used in [Chapter 15](#) to communicate with ISE and provide the security or “health” of the PC or Mac.

## RA-VPN with Posture Flows

When using the AnyConnect ISE compliance module, the posture data is sent directly to ISE. This means the VPN tunnel must be established already; otherwise, the posture communication would never occur. Revisit [Chapter 15](#) for more information on the posture discovery process; the focus here is on the basic flows as they relate to the RA-VPN.

[Figure 19-37](#) shows the basic RA-VPN flows and their tie-in with posture.



**Figure 19-37** Basic RA-VPN Flows with Posture

Let's examine the steps that are in the flow:

1. The VPN is initiated from the AnyConnect VPN module to the ASA headend.

Encryption is negotiated and then credentials are passed.

2. The ASA sends the user credentials to ISE within a RADIUS Access-Request packet. ISE processes the credentials and runs through the authorization policy. Assuming the user is allowed to connect, then Step 3 occurs and the user's session in ISE has the posture compliance value set to unknown.
3. ISE responds to the ASA with a RADIUS Access-Accept packet that includes the AV pairs for a URL redirection and a dACL. The dACL is applied to the user's session, limiting their access, and the redirection is for the ISE compliance module to be redirected to the ISE PSN.
4. The VPN tunnel is fully established and an IP address is assigned to the endpoint. At this point, the endpoint has limited access.
5. The ASA sends a RADIUS Accounting packet to the ISE PSN, which informs ISE of the assigned IP address.
6. With the access limited, and traffic redirected to the PSN, the ISE compliance module is able to communicate to the active ISE PSN and share the posture elements with ISE. ISE processes that posture data against the posture policy and updates the user's session in ISE with the posture compliance value set to compliant.
7. The change in posture compliance of the session triggers the CoA-Push. Unlike a CoA-ReAuth, where the authentication occurs again, running through the entire policy set, a CoA-Push sends down the new authorization (new dACL, no URL redirection) as part of the CoA itself, not a RADIUS Access-Accept.
8. The user has full network access.

This section reviewed the flow with the ASA and posture assessment. In the next section, you configure ISE to make this flow happen.

## **Adding the Access Control Lists to ISE and the ASA**

ISE needs downloadable Access Control Lists (dACLs) that will be sent to the ASA at different stages of the user's session. Additionally, it needs an access list that defines what traffic to redirect to ISE and what traffic not to redirect.

First, create the dACLs that will be used. Start with the final dACL that will provide full access after the endpoint is found posture compliant.

From the ISE GUI, follow these steps:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Elements > Results > Downloadable ACLS.**

**Step 2.** Click **Add.**

**Step 3.** Name the ACL **VPN-PostureCompliant**.

**Step 4.** Provide a description.

**Step 5.** Enter **permit ip any any** in the dACL Content field, or provide a more restrictive ACL if it suits your organizational needs.

**Step 6.** Click **Check DACL Syntax** to ensure there were not any typos.

**Step 7.** Click **Submit**.

[Figure 19-38](#) shows the complete VPN-PostureCompliant dACL.

The screenshot shows the ASA's configuration interface for creating a new Downloadable ACL. The 'Name' field is set to 'VPN-PostureCompliant'. The 'Description' field contains the text 'dACL to use for VPN when posture is compliant'. The 'DACL Content' section shows a single rule: '1 permit ip any any'. Below this, a 'Check DACL Syntax' button is visible, and the status message 'DACL is valid' is displayed.

**Figure 19-38** VPN-PostureCompliant dACL

Next, you need another dACL that limits traffic through the ASA for the endpoints that are posture-unknown or posture-noncompliant. This dACL should be set up to permit traffic destined to ISE nodes, the DNS server, and other critical infrastructure, just as you did in [Chapter 15](#). It should permit access to the remediation server, and deny all other traffic.

**Step 8.** Click **Add**.

**Step 9.** Name the ACL **VPN-PostureNotCompliant**.

**Step 10.** Provide a description.

**Step 11.** In the dACL Content field, type **permit ip any host ISE\_PSN**.

**Step 12.** Repeat Step 11 for each ISE PSN.

- Step 13.** Type **permit ip any host DNS\_server**.
- Step 14.** Type **permit ip any host remediation\_server**.
- Step 15.** Type **permit ip any internal network**.
- Step 16.** Type **deny ip any any**, or provide a more restrictive ACL if it suits your organizational needs.
- Step 17.** Click **Check DACL Syntax** to ensure there were not any typos.
- Step 18.** Click **Submit**.

[Figure 19-39](#) shows the complete VPN-PostureNotCompliant dACL.

The screenshot shows the ASA's configuration interface for a 'Downloadable ACL'. The 'Name' is set to 'VPN-PostureNotCompliant'. The 'Description' is 'dACL to use for VPN when posture is not compliant'. The 'DACL Content' section lists the following rules:

- 1 permit ip any host 10.1.100.231
- 2 permit ip any host 10.1.100.232
- 3 permit ip any host 10.1.100.244
- 4 permit ip any host 10.1.100.103
- 5 permit ip any host 10.1.100.104
- 6 deny ip any any
- 7
- 8
- 9
- 10

Below the ACL content is a 'Check DACL Syntax' button. A message below the button states 'DACL is valid'.

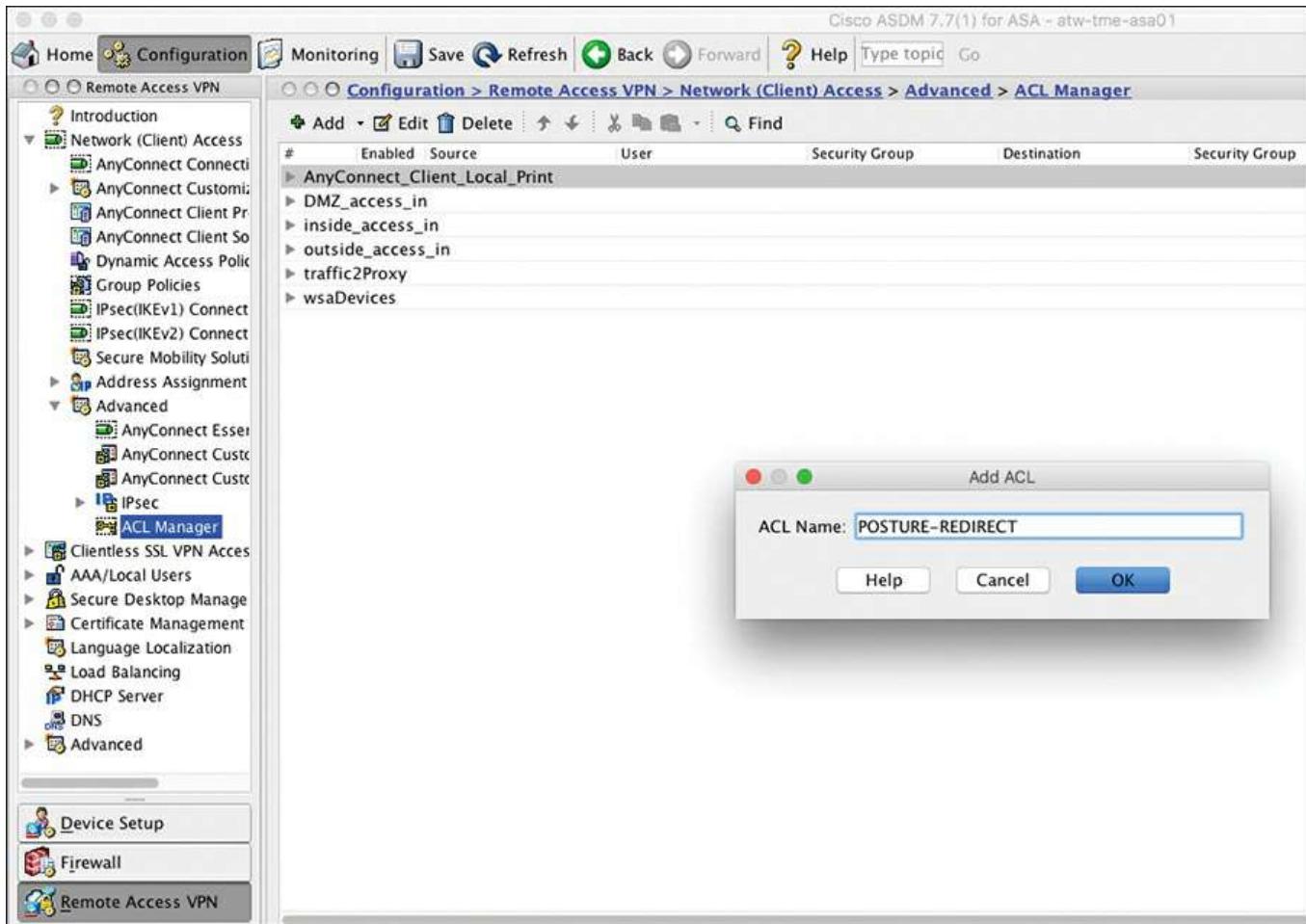
**Figure 19-39** VPN-PostureNotCompliant dACL

The redirection ACL is configured locally on the ASA, not in ISE. It needs to be configured to deny any traffic that shouldn't be redirected, and permit any traffic that should be redirected.

- Step 19.** From ASDM, navigate to **Configuration > Network (Client) Access > Advanced > ACL Manager**.

- Step 20.** Click **Add > ACL**.

- Step 21.** Name the ACL **POSTURE-REDIRECT**, as shown in [Figure 19-40](#).



**Figure 19-40** Adding a New ACL

**Step 22.** Click **OK**.

**Step 23.** With the newly created POSTURE-REDIRECT ACL selected, click **Add > ACE**.

**Step 24.** Add an ACE configured to deny traffic from any source to TCP port 8905 for posture discovery.

**Step 25.** Add an ACE configured to deny traffic from any source to UDP port 8905 for posture discovery.

**Step 26.** Add an ACE that denies traffic from any source to UDP port 53 for DNS.

**Step 27.** Add an ACE that denies traffic from any source to the remediation server.

**Step 28.** Add an ACE that permits traffic from any source to HTTP and HTTPS, to cause redirection.

**Step 29.** Add an ACE that denies all other traffic, which will not redirect any of the traffic that is not explicitly denied in the preceding steps.

[Figure 19-41](#) shows the complete POSTURE-REDIRECT ACL.

#	Enabled	Source	User	Security Group	Destination	Security Group	Service	Action	Log...	T...	Description
> AnyConnect_Client_Local_Print											
> DMZ_access_in											
> inside_access_in											
> outside_access_in											
> POSTURE-REDIRECT											
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> 8905	<input checked="" type="checkbox"/> Deny			posture discovery
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> 8905	<input checked="" type="checkbox"/> Deny			posture discovery
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> domain	<input checked="" type="checkbox"/> Deny			DNS
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> 10.1.100.104	<input checked="" type="checkbox"/> 10.1.100.104	<input checked="" type="checkbox"/> ip	<input checked="" type="checkbox"/> Deny			Remediation Server
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> http	<input checked="" type="checkbox"/> Permit			Redirect Web
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> any	<input checked="" type="checkbox"/> any		<input checked="" type="checkbox"/> https				Do not redirect the rest of the ..
> traffic2Proxy							<input checked="" type="checkbox"/> ip	<input checked="" type="checkbox"/> Deny			
> wsaDevices											

**Figure 19-41** POSTURE-REDIRECT ACL

**Step 30.** Click **Apply**.

**Step 31.** Click **Save**.

## Adding Posture Policies to the VPN Policy Set

You created posture checks, requirements, remediations, and policies in [Chapter 15](#).

Those same policies are used in this section, but are extended to the VPN policy set.

What remains in ISE is to create the authorization profiles that will use the dACLs you created previously, and then finally to create the authorization rules.

## Create the Authorization Profiles

First, create the pre-posture authorization result. From the ISE GUI:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Elements > Results > Authorization Profiles**.

**Step 2.** Click **Add**.

**Step 3.** Name the profile **VPN-Posture-Redirect**.

**Step 4.** Provide a description.

**Step 5.** Ensure that the **Access Type** field is set to **ACCESS\_ACCEPT**.

**Step 6.** Under Common Tasks, check the **DACL Name** check box and choose the **VPN-PostureNonCompliant** dACL from the drop-down list.

**Step 7.** Check the **Web Redirection** check box and choose **Client Provisioning (Posture)**.

**Step 8.** For the ACL, type **POSTURE-REDIRECT**, which is the ACL you configured locally on the ASA.

**Step 9.** From the Value drop-down list, choose **Client Provisioning Portal**.

[Figure 19-42](#) shows the complete VPN-Posture-Redirect authorization profile.

The screenshot shows the 'Authorization Profile > New Authorization Profile' screen. The profile is named 'VPN-Posture-Redirect' with a description of 'Redirect traffic for posture assessment.' The 'Access Type' is set to 'ACCESS\_ACCEPT'. In the 'Common Tasks' section, the 'DACL Name' is chosen as 'VPN-PostureNotCompliant'. Under 'Web Redirection (CWA, MDM, NSP, CPP)', 'Client Provisioning (Posture)' is selected with 'ACL' set to 'POSTURE-REDIRECT' and 'Value' set to 'Enter Provisioning Portal (default)'. The 'Attributes Details' section shows the access type and the selected DACL. The 'Submit' button is at the bottom.

**Figure 19-42** VPN-Posture-Redirect Authorization Profile

### Step 10. Click Submit.

Now, create the post-posture authorization result to be used after the endpoint is compliant.

From the ISE GUI:

### Step 11. Click Add.

### Step 12. Name the profile **VPN-Full-Access**.

### Step 13. Provide a description.

### Step 14. Ensure that Access Type field is set to **ACCESS\_ACCEPT**.

### Step 15. Under Common Tasks, check the **DACL Name** check box and choose the **VPN-PostureCompliant** dACL from the drop-down list.

### Step 16. Click Submit.

## Create the Authorization Policies

The authorization profiles are created, so now it's time to create the authorization policies.

Navigate to **Work Centers > Network Access > Policy Sets**. Choose the VPN Policy Set, and insert a rule at the top that looks for endpoints where Session:PostureStatus NOT\_EQUALS Compliant, and set the authorization result to be the **VPN-Posture-Redirect** profile, which limits access and redirects the posture traffic.

You also need to insert a rule below that one that looks for a condition where

Session:PostureStatus EQUALS Compliant, and set the authorization result to be the **VPN-Full-Access** profile, which removes the redirection and replaces the traffic-limiting dACL with the less-restrictive dACL.

[Figure 19-43](#) shows an example policy set leveraging a rule that redirects the endpoint to get posture, and another rule that permits full access.

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Status	Name	Description	Conditions
<input checked="" type="checkbox"/>	ATW-VPN	VPN Policy Set	DEVICE:Device Type STARTS WITH Device Type#All Device Types#VPN

**▼ Authentication Policy**

<input checked="" type="checkbox"/> Default Rule (If no match)	: Allow Protocols : Default Network Access	and use : All_User_ID_Stores
--	--	------------------------------

**▼ Authorization Policy**

▶ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Employee-PostureRedirect	if (AD-Employees AND Session:PostureStatus NOT_EQUALS Compliant )	then VPN-Posture-Redirect
<input checked="" type="checkbox"/>	Employee-Permit	if (AD-Employees AND Session:PostureStatus EQUALS Compliant )	then VPN-Full-Access
<input checked="" type="checkbox"/>	Default	if no matches, then DenyAccess	

**Figure 19-43** Example Modified VPN Policy Set

## Watching It Work

To see the fruits of your labor, connect to the VPN from an endpoint. Watching the AnyConnect client, the System Scan module should inform the end user about the posture checks occurring, as shown in [Figure 19-44](#).



**Figure 19-44** AnyConnect System Scan Module in Progress

From the ISE user interface, you can immediately focus on “old faithful,” the ISE Live Log. As you can see in [Figure 19-45](#), the Live Log allows you to watch the endpoint join the network, and watch all the activity that is happening related to the posture and CoA.

Status	Details	Identity	Endpoint ID	Endpoint Profile	Authentication P...	Authorization Policy	Authorization Profiles	Posture Status
5	Initial Endpoint Connection...	Employee	192.168.1.11	Employee Profile	Employee Authentication	Employee Authorization	Employee Profile	Pending
4	Employee	Employee	192.168.1.11	Employee Profile	Employee Authentication	Employee Authorization	Employee Profile	Completed
3	Initial Endpoint Connection...	Employee	192.168.1.11	Employee Profile	Employee Authentication	Employee Authorization	Employee Profile	Completed
2	Employee	Employee	192.168.1.11	Employee Profile	Employee Authentication	Employee Authorization	Employee Profile	Completed
1	Initial Endpoint Connection...	Employee	192.168.1.11	Employee Profile	Employee Authentication	Employee Authorization	Employee Profile	Pending

**Figure 19-45** Example Live Log

[Figure 19-45](#) shows an example policy set leveraging a rule that redirects the endpoint to get posture, and another rule that permits full access.

Let’s examine what transpired in the Live Log snapshot in [Figure 19-45](#):

1. The initial authentication and authorization. The posture was not known, and listed in Live Log as Pending, and therefore the resulting authorization rule is Employee-PostureRedirect.
2. The dACL was sent from ISE to the ASA, and the ASA has acknowledged the success. Click the Details icon for this entry to see the detailed report. [Figure 19-46](#) shows a snippet of the details report of this Live Log entry. Notice in [Figure 19-46](#) each line of the dACL is shown along with the success messages.

Result	
State	ReauthSession:0a0165fe0001a00058d29b10
Class	CACS:0a0165fe0001a00058d29b10:atw-ise244/279568865/18
cisco-av-pair	ip:inac1#1=permit ip any host 10.1.100.231
cisco-av-pair	ip:inac1#2=permit ip any host 10.1.100.232
cisco-av-pair	ip:inac1#3=permit ip any host 10.1.100.244
cisco-av-pair	ip:inac1#4=permit ip any host 10.1.100.103
cisco-av-pair	ip:inac1#5=permit ip any host 10.1.100.104
cisco-av-pair	ip:inac1#6=deny ip any any

Session Events	
2017-03-22 08:41:38.044	DACL Download Succeeded
2017-03-22 08:41:38.043	Dynamic Authorization succeeded
2017-03-22 08:41:04.669	DACL Download Succeeded
2017-03-22 08:41:04.667	Authentication succeeded

**Figure 19-46** Report Snippet for dACL Download

3. The i in the Status column for this entry identifies it as an informational event, showing that the endpoint's posture status is now compliant.
4. This entry is the CoA initializing from ISE to the ASA.
5. This final entry is the success of the dACL. Click the Details icon for this entry to see the detailed report. [Figure 19-47](#) shows a portion of the details report, where the session settled into its final state.

Authentication Details	
Event	5232 DACL Download Succeeded
Username	#ACS/ACL#-IP-VPN-PostureCompliant-5d1b405
Audit Session Id	0a0163fe0001a00058d29b10
Other Attributes	
RADIUS Username	#ACS/ACL#-IP-VPN-PostureCompliant-5d1b405
Device IP Address	10.1.101.254
CiscoAVPair	audit-session-id=dat165fe0001a00058d29b10, acs-service=vpn, acs-event=dac-download, cos-pwsh=true
Result	
State	ReauthSession:0a0163fe0001a00058d29b10
Class	CACS:0a0163fe0001a00058d29b10:awx-iae244/279568865/19
cisco-av-pair	{permit ip any any}

**Figure 19-47 Report Snippet for the Final dACL of the Session**

Finally, you can always look at the session from the ASA's perspective. You can use either the command-line interface or one of the graphical interfaces, such as ASDM. The CLI tends to be easier to view and understand in this context, so we'll switch to that to view the session.

The CLI command to view the session is **show vpn-sessiondb detail anyconnect**.

Examples 19-1 and 19-2 show the output of the command in two different stages of the session. [Example 19-1](#) shows the output of the command when the endpoint posture is unknown and the session is set to redirect traffic to ISE.

### Example 19-1 show vpn-sessiondb detail anyconnect Command Output

[Click here to view code image](#)

```
atw-tme-5515# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username      : employee1          Index      : 26
Assigned IP   : 192.168.228.2      Public IP   : 10.117.118.215
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-
```

```
256 DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none   SSL-Tunnel:
(1)SHA384    DTLS-Tunnel: (1)     SHA1
Bytes Tx      : 24431                  Bytes Rx      : 13670
Pkts Tx       : 33                   Pkts Rx       : 67
Pkts Tx Drop : 0                   Pkts Rx Drop : 0
Group Policy  : GroupPolicy1
ConnectionProfile
Tunnel Group  : ATW-
Login Time    : 15:41:04 UTC Wed Mar 22 2017
Duration      : 0h:00m:09s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN          : none
Audt Sess ID  : 0a0165fe0001a00058d29b10
Security Grp  : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

< output removed for space >

SSL-Tunnel:

```
Tunnel ID      : 26.2
Assigned IP    : 192.168.228.2          Public IP      : 10.117.118.215
Encryption     : AES-GCM-256           Hashing        : SHA384
Ciphersuite   : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2                TCP Src Port : 58163
TCP Dst Port  : 443                  Auth Mode     : userPassword
Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
Client OS      : Windows
Client Type    : SSL VPN Client
Client Ver     : Cisco AnyConnect VPN Agent for Windows 4.4.01054
Bytes Tx       : 7354                  Bytes Rx      : 816
Pkts Tx        : 5                   Pkts Rx       : 12
Pkts Tx Drop  : 0                   Pkts Rx Drop : 0
Filter Name   : #ACSACL#-IP-VPN-PostureNotCompliant-58d1c6f2
```

< output removed for space >

```
ISE Posture:  
  Redirect URL : https://atw-ise244.securitydemo.net:8443/portal/gateway?sessionId=0a0165fe0001a00058d29b10&portal=4cb1...  
  Redirect ACL : POSTURE-REDIRECT
```

```
atw-tme-5515#
```

[Example 19-2](#) shows the output of the command when the endpoint posture is known to be compliant and the session is given full access.

## Example 19-2 show vpn-sessiondb detail anyconnect Command Output

[Click here to view code image](#)

```
atw-tme-5515# show vpn-sessiondb detail anyconnect  
  
Session Type: AnyConnect Detailed  
  
Username : employee1 Index : 25  
Assigned IP : 192.168.228.2 Public IP : 10.117.118.215  
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License : AnyConnect Premium  
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-  
256 DTLS-Tunnel: (1)AES256  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel:  
(1)SHA384 DTLS-Tunnel: (1) SHA1  
Bytes Tx : 101366 Bytes Rx : 92634  
Pkts Tx : 204 Pkts Rx : 511  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : GroupPolicy1 Tunnel Group : ATW-  
ConnectionProfile  
Login Time : 15:31:17 UTC Wed Mar 22 2017  
Duration : 0h:05m:29s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audit Sess ID : 0a0165fe0001900058d298c5  
Security Grp : none  
AnyConnect-Parent Tunnels: 1
```

```

SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

< output removed for space >

SSL-Tunnel:
  Tunnel ID      : 25.2
  Assigned IP    : 192.168.228.2          Public IP      : 10.117.118.215
  Encryption     : AES-GCM-256          Hashing       : SHA384

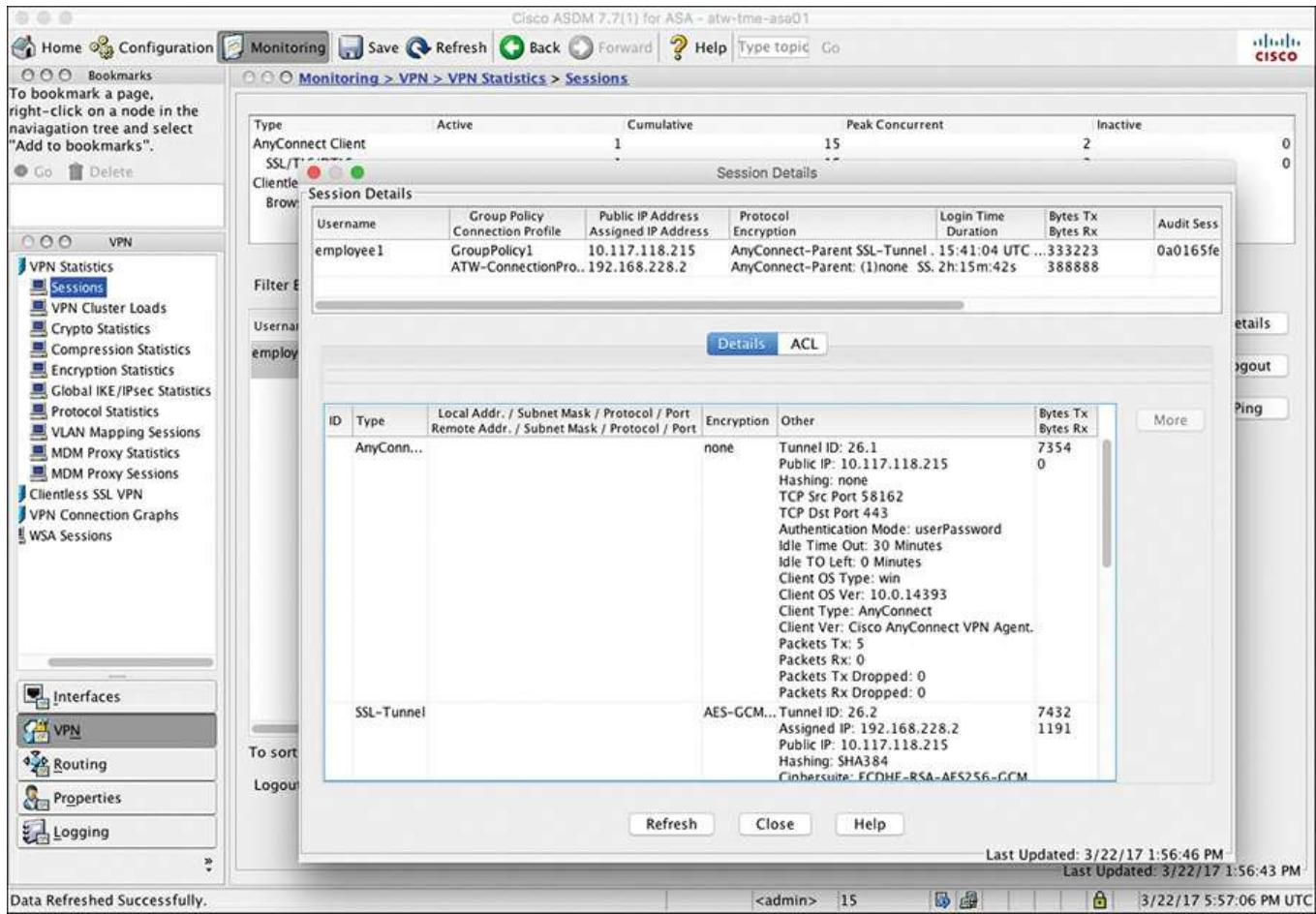
Ciphersuite   : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2                  TCP Src Port : 57916
TCP Dst Port : 443                      Auth Mode    : userPassword
Idle Time Out: 30 Minutes                Idle TO Left : 24 Minutes
Client OS     : Windows
Client Type   : SSL VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.4.01054
Bytes Tx      : 7354                     Bytes Rx     : 216
Pkts Tx       : 5                        Pkts Rx      : 4
Pkts Tx Drop : 0                        Pkts Rx Drop : 0
Filter Name   : #ACSACL#-IP-VPN-PostureCompliant-58d18405

< output removed for space >

atw-tme-5515#

```

For completeness, [Figure 19-48](#) shows a screenshot of viewing the same information within ASDM. To view it in ASDM, navigate to **Monitoring > VPN > VPN Statistics > Sessions**. Then, ensure that you are viewing remote access sessions, by selecting All Remote Access from the **Filter By** dropdown. [Figure 19-48](#) shows an example of the filtered results.



**Figure 19-48 Session Details in ASDM**

## Extending the ASA Remote Access VPN Capabilities

One very interesting feature of the ASA is its ability to perform a double authentication (not to be confused with dual-factor authentication, which is a single authentication using two factors). The ASA can also authenticate VPNs using certificate-based authentication, in addition to using username and password authentications.

Additionally, the ASA can help provision certificates to AnyConnect clients for VPN purposes, leveraging an external certificate authority such as ISE. These topics are covered in this section.

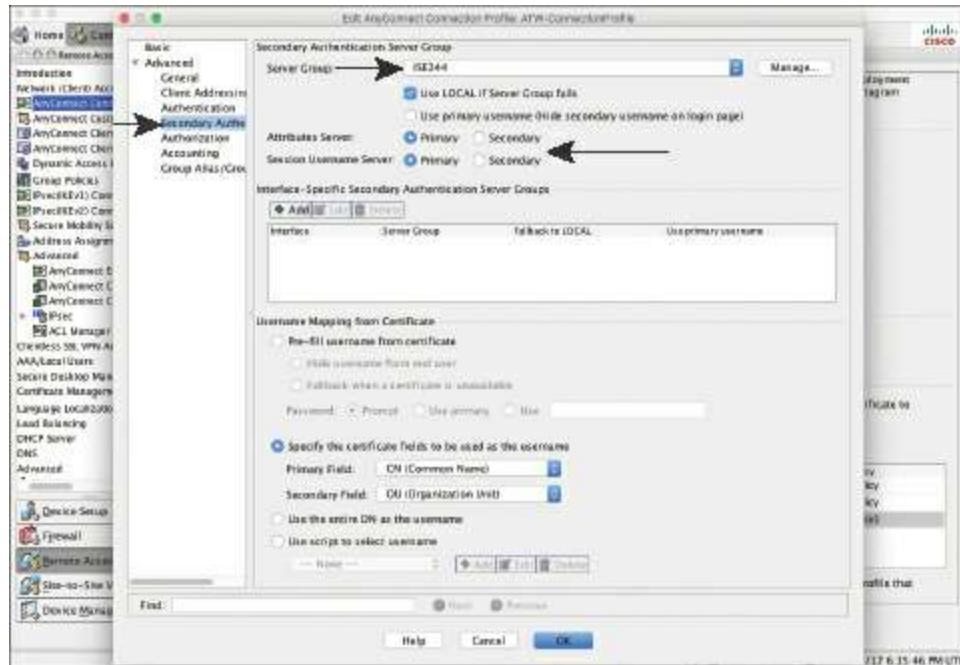
## Double Authentication

As you might have noticed earlier in the chapter when configuring the AnyConnect connection profile, the navigation pane on the left also has an Advanced section. Click **Advanced**, and you see an option called Secondary Authentication, which is commonly referred to colloquially as double authentication. Whichever term is used, it refers to authenticating two completely different sets of credentials. Often, this is used to authenticate a machine certificate followed by the username and password, or a one-time password (OTP) followed by an Active Directory authentication. Only after

passing both authentications is the end user authorized by the ASA to establish the full tunnel.

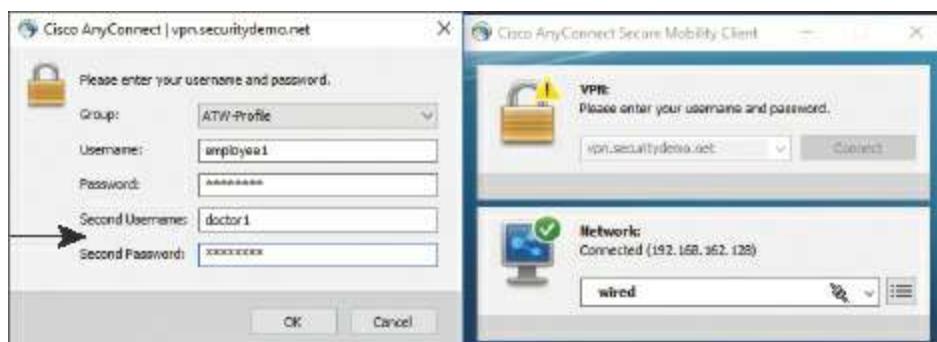
**Note** At the time of writing, the ASA does not support doing a certificate-based authentication for both primary and secondary authentication.

[Figure 19-49](#) shows the setting in ASDM. You select the AAA server group to use for the secondary authentication, and then configure some other options.



**Figure 19-49** AnyConnect Connection Profile: Secondary Authentication

[Figure 19-49](#) shows the ASA configuration screen, but what does double authentication look like to the end user? [Figure 19-50](#) shows the AnyConnect user interface when double authentication is configured for two username/password-based authentications.



**Figure 19-50** Live Log of Double Authentication

Where this becomes really interesting is how it looks when both authentications are sent to the same ISE PSN. You see both authentications and both authorizations, but only the

second authorization is maintained as an active session. [Figure 19-51](#) shows the Live Log, with the Identity column showing that both employee1 and doctor1 have entries. Click over to the Live Sessions screen, as shown in [Figure 19-52](#), and you can see that only doctor1 has a session.

Status	Details	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorization Policy	Authorized...	Posture St...
Green	employee1	ISEC64CL8-IP-NY...		Endpoint ID	Endpoint Prof...	Authenticator	Authentication Policy	Authorized by...
Blue	doctor1	00:0C:29:D6:91:69	WindowsP...	ATM-VPN x...	ATW-VPN >> Employee-PortalAndRetail...	ATW-VPN >> Employee-PortalAndRetail...	VPN Postur...	Pending
Green	doctor1	00:0C:29:D6:91:69	WindowsP...	ATM-VPN x...	ATW-VPN >> Employee-PortalAndRetail...	ATW-VPN >> Employee-PortalAndRetail...	VPN Postur...	Pending
Green	employee1	180C:29:D6:91:69	WindowsP...	ATM-VPN x...	ATW-VPN >> Employee-PortalAndRetail...	ATW-VPN >> Employee-PortalAndRetail...	VPN Postur...	Pending

**Figure 19-51** Live Log of Double Authentication

Live Log								
Updated	Session Status	Action	Endpoint ID	Identity	IP Address	Endpoint Profile	Posture Status	St...
Mar 27, 2017 11:38:33:170 AM	Authenticated	Block CoA, Allow	00:0C:29:D6:91:69	doctor1		WindowsP...-Mortyman	Pending	

**Figure 19-52** Live Session Log of Double Authentication

Double authentication makes sense when you are not using an intelligent centralized policy server, which ISE most certainly is. However, it also makes sense when you are performing two different types of authentications, such as a certificate-based authentication followed by a username/password-based authentication.

## Certificate-Based Authentication

Now that your interest is fully piqued about certificate-based authentications, this section examines those certificate-based authentications with ASA RA-VPNs.

### Provisioning Certificates

Before you can authenticate using a certificate, you have to be in possession of said certificate. So, we start our dive into this topic by looking at the function within AnyConnect and the ASA to provision certificates using Simple Certificate Enrollment Protocol (SCEP) from ISE's internal CA to the AnyConnect clients.

**Note** For more details on ISE's internal CA, revisit [Chapter 17, “BYOD: Self Service Onboarding and Registration,”](#) but also take some time to read Appendix D, “The ISE CA and How Cert Based Auth Works.”

The ASA can act as an SCEP proxy, taking the SCEP request from the AnyConnect client and passing it along to an external CA, such as ISE. ISE allows SCEP only from devices that are listed as NADs in the ISE configuration, so the ASA is perfect because it is

already listed as a NAD for RA-VPN.

You first need to download the ISE CA certificates to be installed in the ASA as a trusted CA. From the ISE GUI:

**Step 1.** Navigate to **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**, as shown [Figure 19-53](#).

friendly_name	Status	Trusted For	Serial Number	Issued To	Issued By
Certificate Services Root CA - ise-isec244#00001	Enabled	Infrastructure,Endpoints	64 26 83 5A BE 6D 4E 9C 91 FB FE 3A 44 CD 1D 1D PE	Certificate Services Root CA - ise-isec244	Certificate Services Root CA - ise-isec244
Certificate Services Node CA - ise-isec244#00002	Enabled	Infrastructure,Endpoints	66 33 C3 8B C1 F7 40 90 A6 8E 3B A7 0E 97 D6 8F	Certificate Services Node CA - ise-isec244	Certificate Services Root CA - ise-isec244
Certificate Services Endpoint Sub CA - ise-isec244#00003	Enabled	Infrastructure,Endpoints	59 F9 47 E7 AD A5 40 78 85 12 F8 48 3A F5 B0 17	Certificate Services Endpoint Sub CA - ise-isec244	Certificate Services Node CA - ise-isec244
Certificate Services OCSP Responder - ise-isec244#00004	Enabled	Infrastructure,Endpoints	9E A2 74 E1 J4 10 4C 49 F4 P5 B1 EF 20 B0 F8 C9	Certificate Services OCSP Responder - ise-isec244	Certificate Services Node CA - ise-isec244

**Figure 19-53** Certificate Authority Certificates

**Step 2.** Download the Root CA, all the Node CA, and all the Sub CA certificates by selecting them one at a time and clicking **Export**.

**Step 3.** Save the downloaded files in a location where you can readily retrieve them later.

Now that you have the certificates from ISE, create an AnyConnect connection profile for the SCEP enrollment. From ASDM:

**Step 4.** Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

**Step 5.** Add a new connection profile named **Enroll**.

**Step 6.** From the Method drop-down list under Authentication, choose **AAA and Certificate**.

**Step 7.** From the AAA Server Group drop-down list, choose the ISE server group used previously (ISE244 in the example).

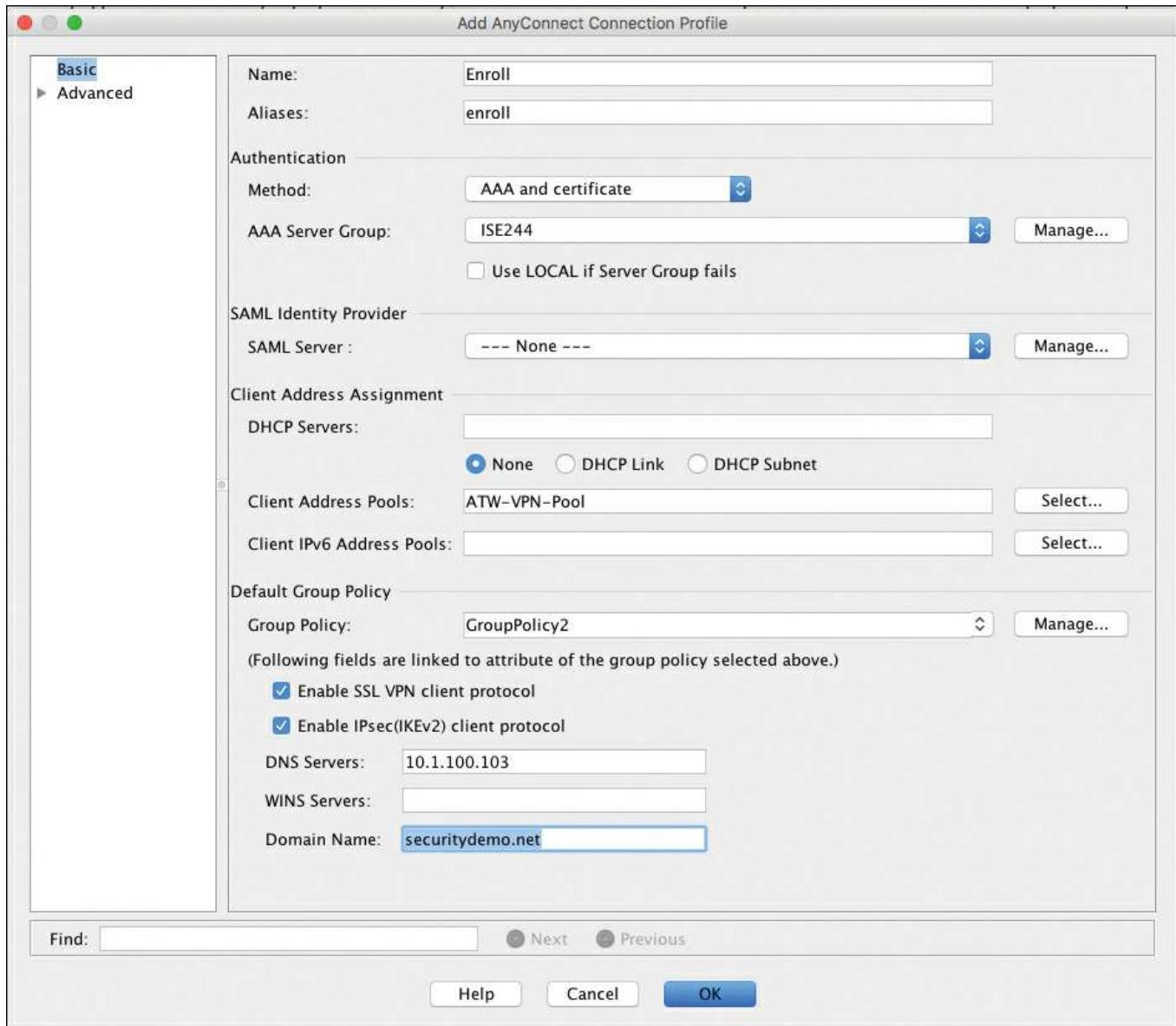
**Step 8.** Click the **Select** button to the right of the Client Address Pools field and choose a client address pool.

**Step 9.** Leave the Group Policy setting alone for now.

**Step 10.** Enable the SSL VPN and IPsec client protocols by checking the corresponding check boxes.

**Step 11.** Fill in the DNS Servers and Domain Name fields.

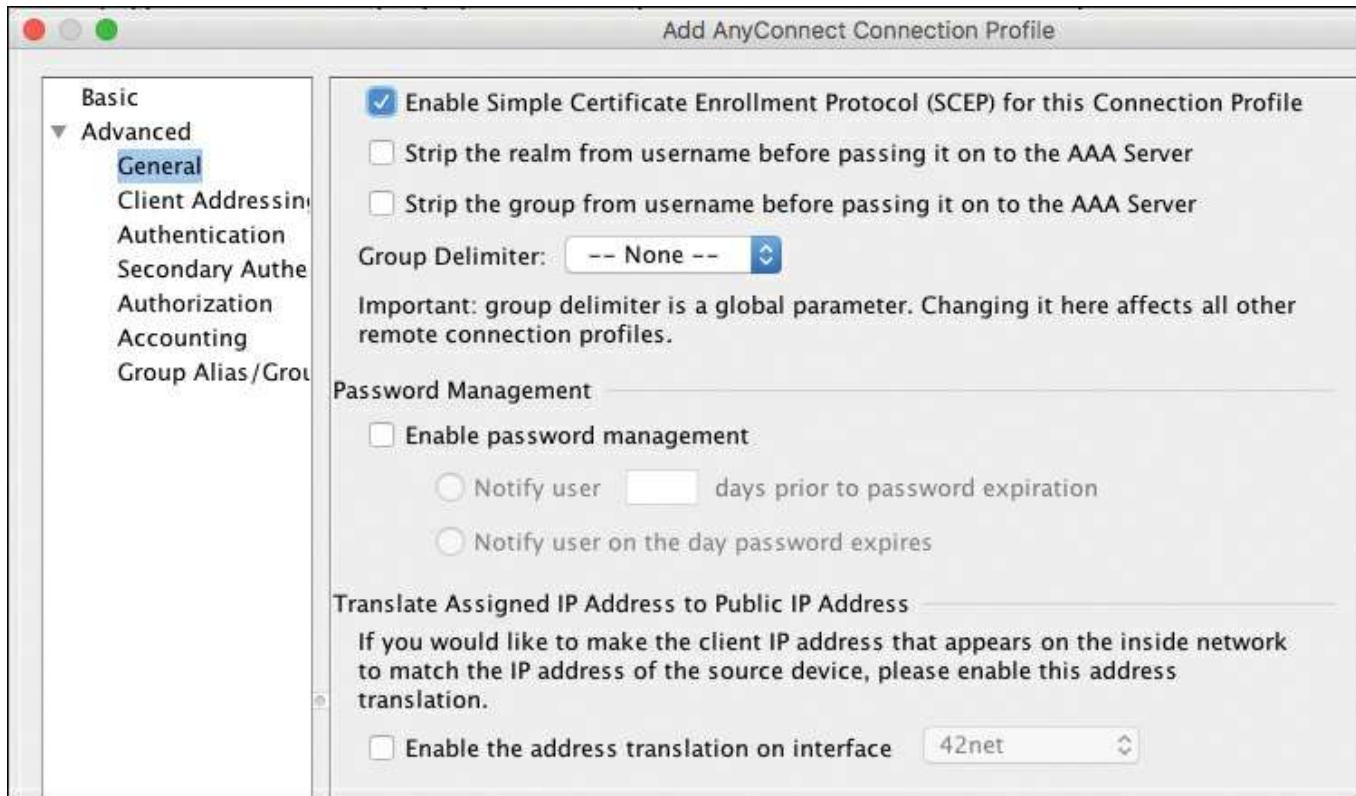
[Figure 19-54](#) shows the configuration of the Enroll connection profile thus far.



**Figure 19-54** Enroll Connection Profile: Basic Configuration

**Step 12.** From the navigation pane on the left, choose **Advanced > General**.

**Step 13.** Check the **Enable Simple Certificate Enrollment Protocol (SCEP) for this Connection Profile** check box, as shown in [Figure 19-55](#).



**Figure 19-55** Enroll Connection Profile: General Configuration

**Step 14.** Click OK.

**Step 15.** Edit the newly created Enroll profile.

**Step 16.** Manage the Group Policy assigned to this profile.

**Step 17.** Set the SCEP Forwarding URL field to

**http://<ISE>:9090/auth/caservice/pkiclient.exe.**

[\*\*Figure 19-56\*\*](#) shows the group policy with the SCEP forwarding URL configured.



**Figure 19-56** Group Policy: General Configuration

The connection profile and group policy now exist, which takes care of the ASA configuration for SCEP proxy. However, you still need to configure AnyConnect for SCEP, because the client must initiate the signing request. To accomplish that task, you need to create an AnyConnect client profile that will pass the configuration to AnyConnect after the client successfully connects to the ASA.

**Step 18.** Select **Network (Client) Access > AnyConnect Client Profile**.

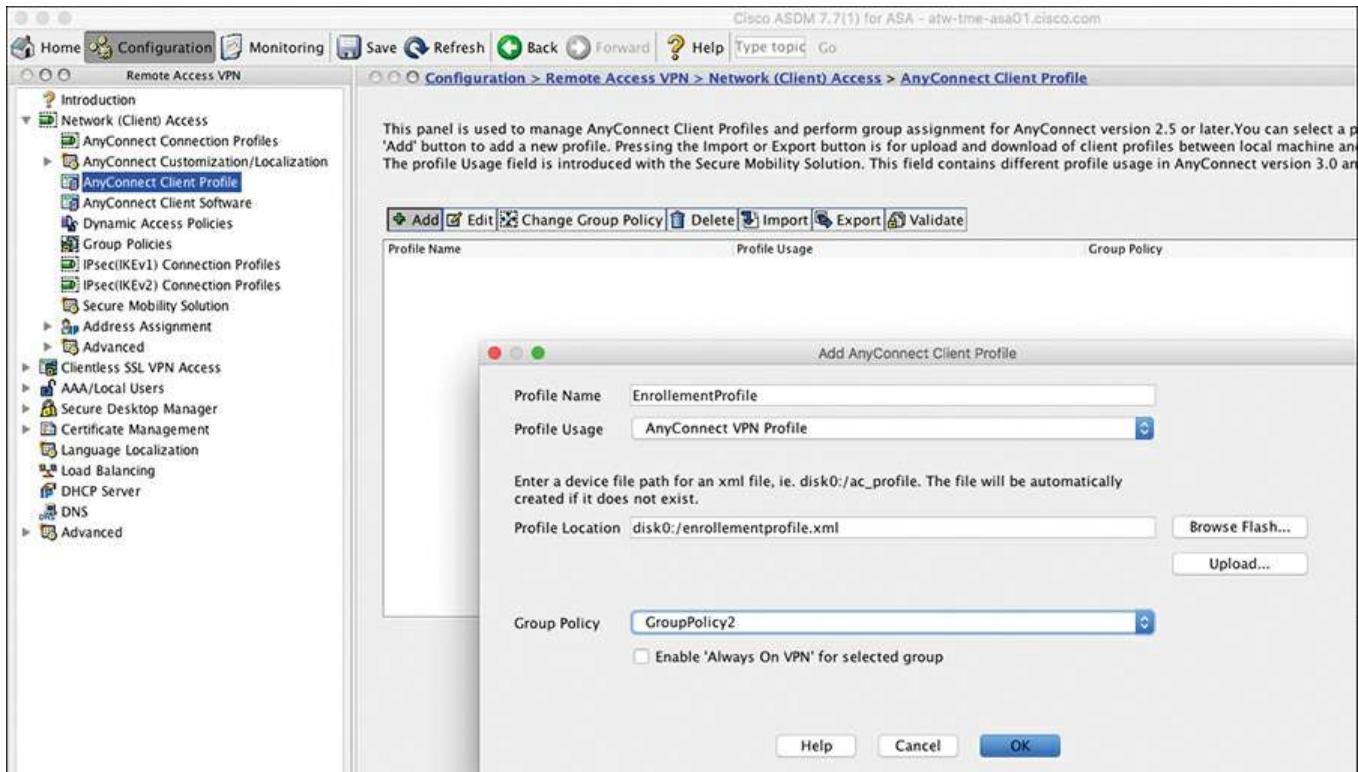
**Step 19.** Click **Add**.

**Step 20.** Name the client profile **EnrollmentProfile**.

**Step 21.** From the Profile Usage drop-down list, choose **AnyConnect VPN Profile**.

**Step 22.** Ensure that the Group Policy field matches the group policy assigned to the connection profile that you edited in Step 16.

[Figure 19-57](#) shows the addition of the client profile named EnrollmentProfile.



**Figure 19-57** Adding the EnrollmentProfile Client Profile

**Step 23.** Click **OK**.

**Step 24.** Edit the newly created EnrollmentProfile client profile.

**Step 25.** Select **Certificate Enrollment** in the navigation pane on the left side.

**Step 26.** Check the **Certificate Enrollment** check box.

**Step 27.** Set the Certificate Expiration Threshold to **30** days.

**Step 28.** In the Automatic SCEP Host field, enter an FQDN for the SCEP host. From the

Certificate Import drop-down list, choose **All**.

**Step 29.** In the CA URL field, enter **http://<ISE>:9090/auth/caservice/pkiclient.exe**.

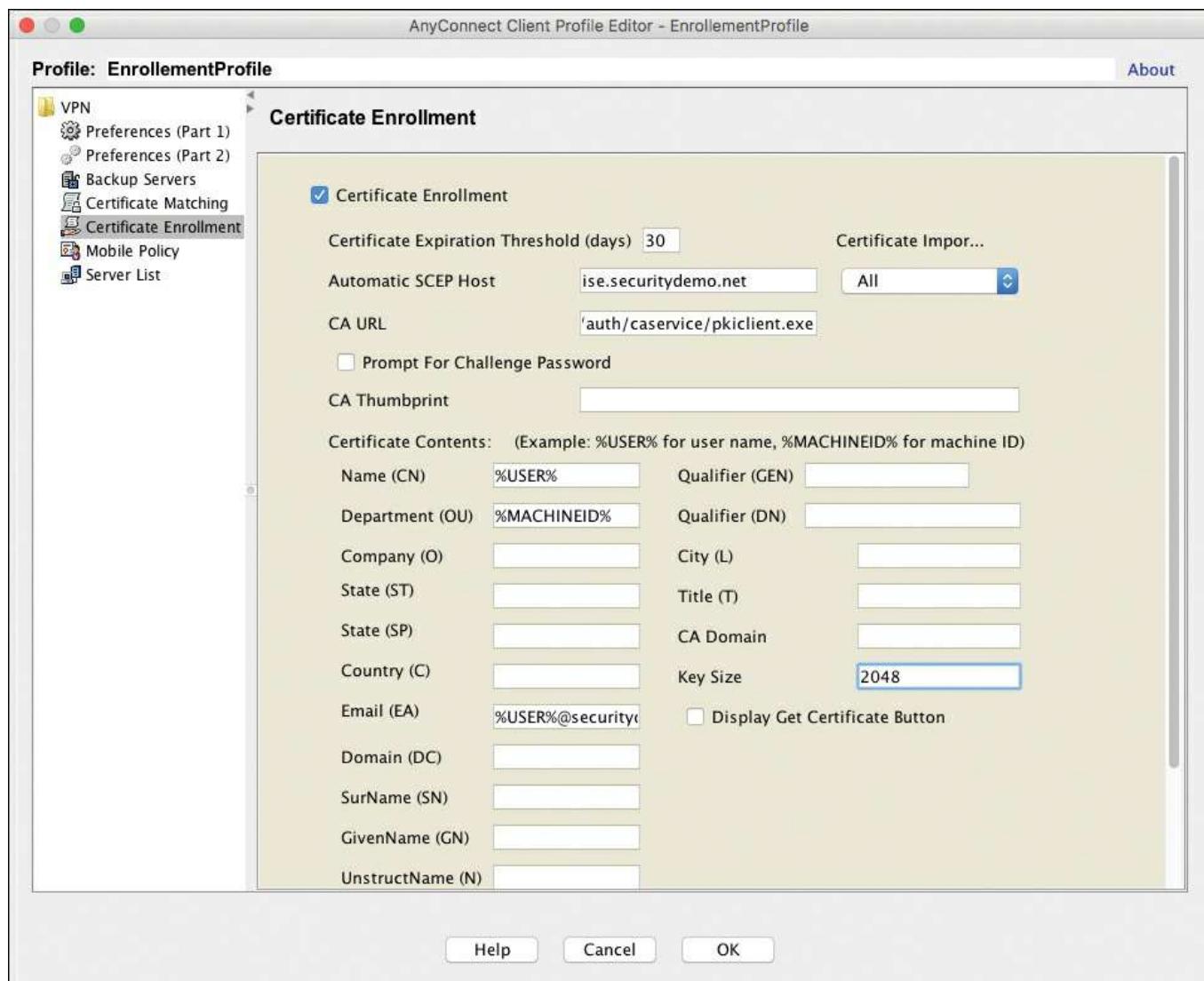
**Step 30.** Type **%USER%** in the Name (CN) field.

**Step 31.** Type **%MACHINEID%** in the Department (OU) field.

**Step 32.** Set the Key Size field to **2048**.

**Step 33.** Type **%USER%@<your domain>** in the Email (EA) field.

[Figure 19-58](#) shows the Certificate Enrollment page of the EnrollmentProfile client profile.



**Figure 19-58** Certificate Enrollment Page

**Step 34.** Click **OK** to save the changes to the XML client profile.

Now that the ASA is configured for SCEP proxy and the AnyConnect client profile is configured to have the client initiate the certificate signing request, the ASA needs to be configured to trust certificates signed by the ISE CA.

**Step 35.** Navigate to Network (Client) Access > Certificate Management > CA Certificates.

**Step 36.** Click Add to import one of the ISE CA certificates that you exported and downloaded from ISE previously in Steps 1, 2, and 3.

**Step 37.** Repeat Step 36 for each of the CA certificates. [Figure 19-59](#) shows the certificates added to the ASA for trust.

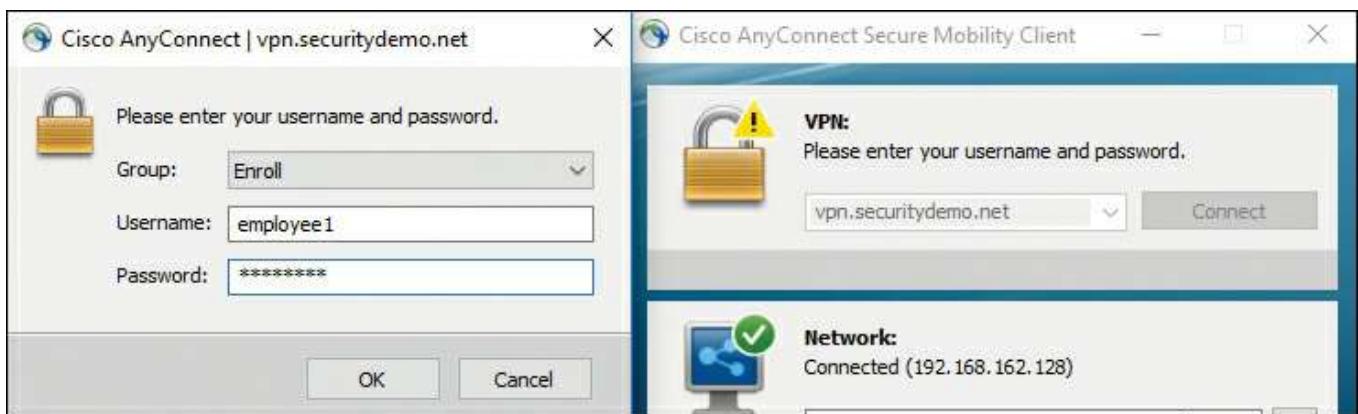
The screenshot shows the Cisco ASDM 7.7(1) interface for ASA atw-tme-asa01. The left sidebar navigation tree is expanded under 'Network (Client) Access' and 'Certificate Management'. The 'CA Certificates' option is selected. The main pane displays a table titled 'Configuration > Remote Access VPN > Certificate Management > CA Certificates'. The table lists various certificates with columns for 'Issued To', 'Issued By', 'Expiry Date', and 'Associated Trustpoints'. One row is highlighted in blue, showing 'Certificate Services Endpoint' issued by 'cn=Certificate Services Node...' with an expiry date of 19:06:34 UTC Jan 26 2022 and associated with 'ISE244-EndpointCA'. Other entries include 'AddTrust External CA Root', 'SSL.com DV CA', and 'USERTrust RSA Certificate'.

Issued To	Issued By	Expiry Date	Associated Trustpoints
AddTrust External CA Root	cn=AddTrust External C...	10:48:38 UTC May 30 2020	AddTrust_TrustPoint
Certificate Services Endpo...	cn=Certificate Services N...	19:06:34 UTC Jan 26 2022	ISE244-EndpointCA
Certificate Services Node ...	cn=Certificate Services R...	19:06:34 UTC Jan 26 2022	ISE244-NodeCA
Certificate Services Root ...	cn=Certificate Services R...	19:06:26 UTC Jan 26 2027	ISE244-root
SSL.com DV CA	cn=USERTrust RSA Certific...	23:59:59 UTC Jul 3 2024	SSLdotCom_TrustPoint
USERTrust RSA Certificati...	cn=AddTrust External C...	10:48:38 UTC May 30 2020	UserTrust_TrustPoint
VeriSign Class 3 Secure S...	cn=VeriSign Class 3 Publi...	23:59:59 UTC Feb 7 2020	_SmartCallHome_ServerCA

**Figure 19-59** CA Certificates

That's it. You are all set and ready to connect to the ASA VPN and receive certificates. When you connect to the Enroll profile, which is configured for AAA and certificate authentication, AnyConnect will look for the certificate, and when it doesn't find one, it will prompt for AAA authentication and perform the SCEP process to the ASA.

[Figure 19-60](#) shows the user connecting the VPN headend.

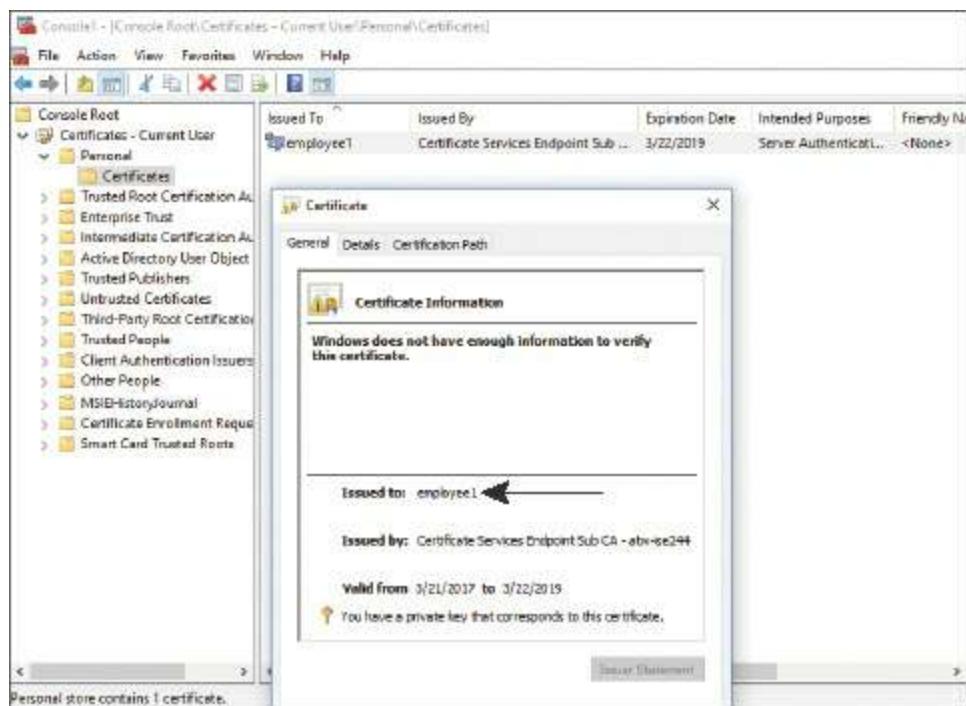


**Figure 19-60** Connecting to the Enroll Profile

[Figure 19-61](#) shows AnyConnect after it has already processed the SCEP and is now storing the certificate. [Figure 19-62](#) shows the Windows Certificates store with the employee1 certificate there.



**Figure 19-61** Storing the Certificate



**Figure 19-62** Windows Certificates Store

Now that the user and computer have a certificate, you can focus on the configuration of an AnyConnect connection profile that uses certificates for authentication.

## Authenticating the VPN with Certificates

When authenticating a VPN with certificates, the ASA performs the certificate validation. This is in contrast to the way certificate-based authentication works with 802.1X on the wired and wireless LAN. When performing 802.1X with certificates, ISE receives the certificate and performs the authentication.

The ASA is handling the authentication, but it can still leverage ISE for the authorization process. This means configuring an AAA server group that is set up for authorize-only, configuring an AnyConnect connection profile set up for certificate-only authentication,

and performing authorization against the AAA server group. It also means configuring some very different types of policies on the ISE side, because ISE would normally expect an authentication before processing an authorization.

To create an AnyConnect connection profile for the certificate-based authentication, from ASDM:

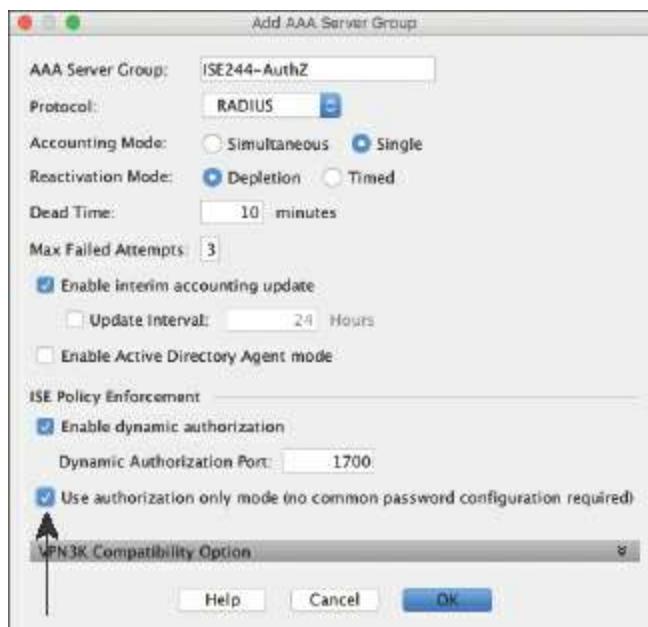
**Step 1.** Navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**.

**Step 2.** Add a new connection profile named **CertProfile**.

**Step 3.** From the method drop-down list, choose **Certificate Only**.

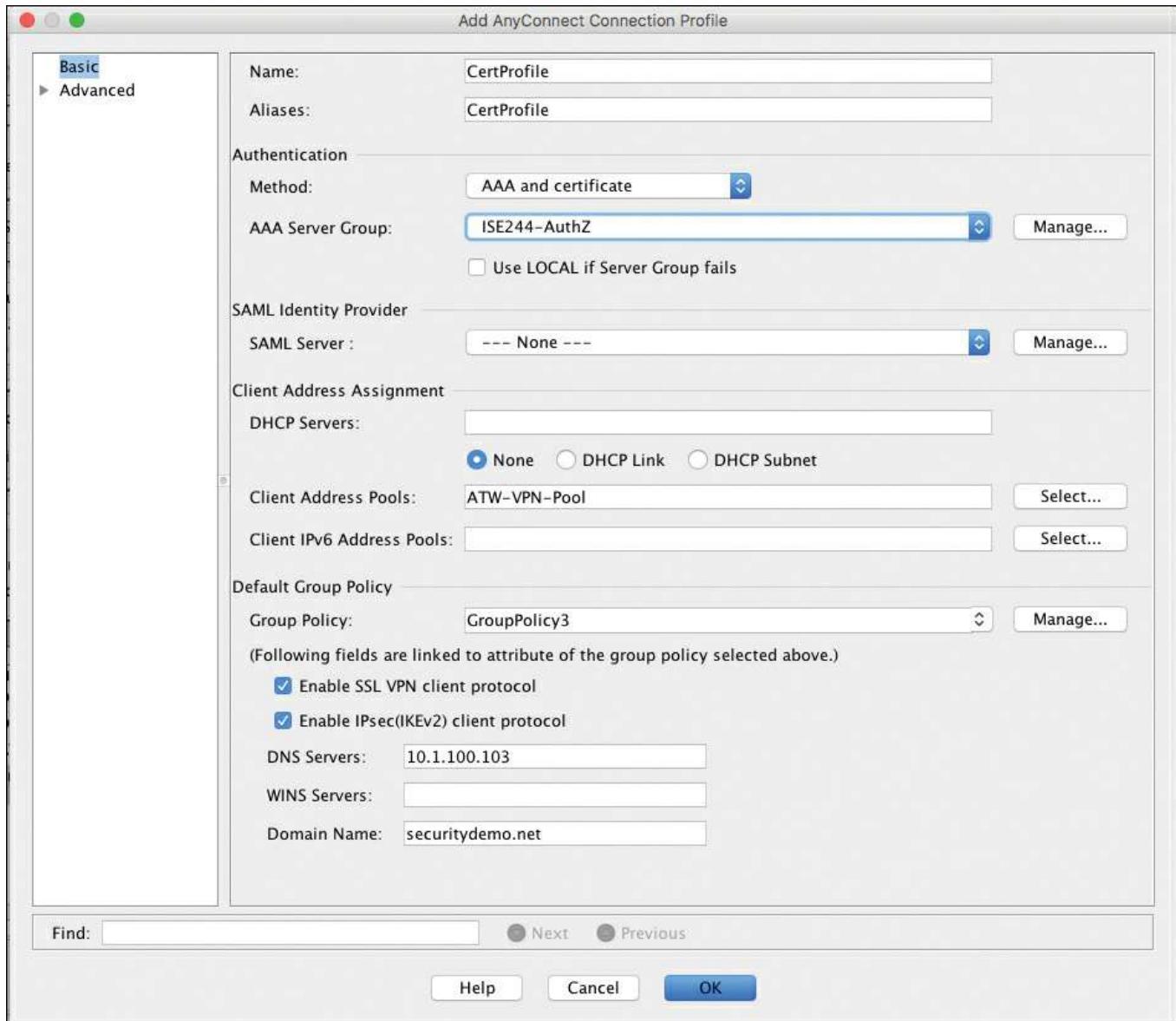
**Step 4.** To the right of the AAA Server Group field, click **Manage**.

**Step 5.** Add a new AAA server group configured normally, but check the **Use Authorization Only Mode** check box, as shown in [Figure 19-63](#).



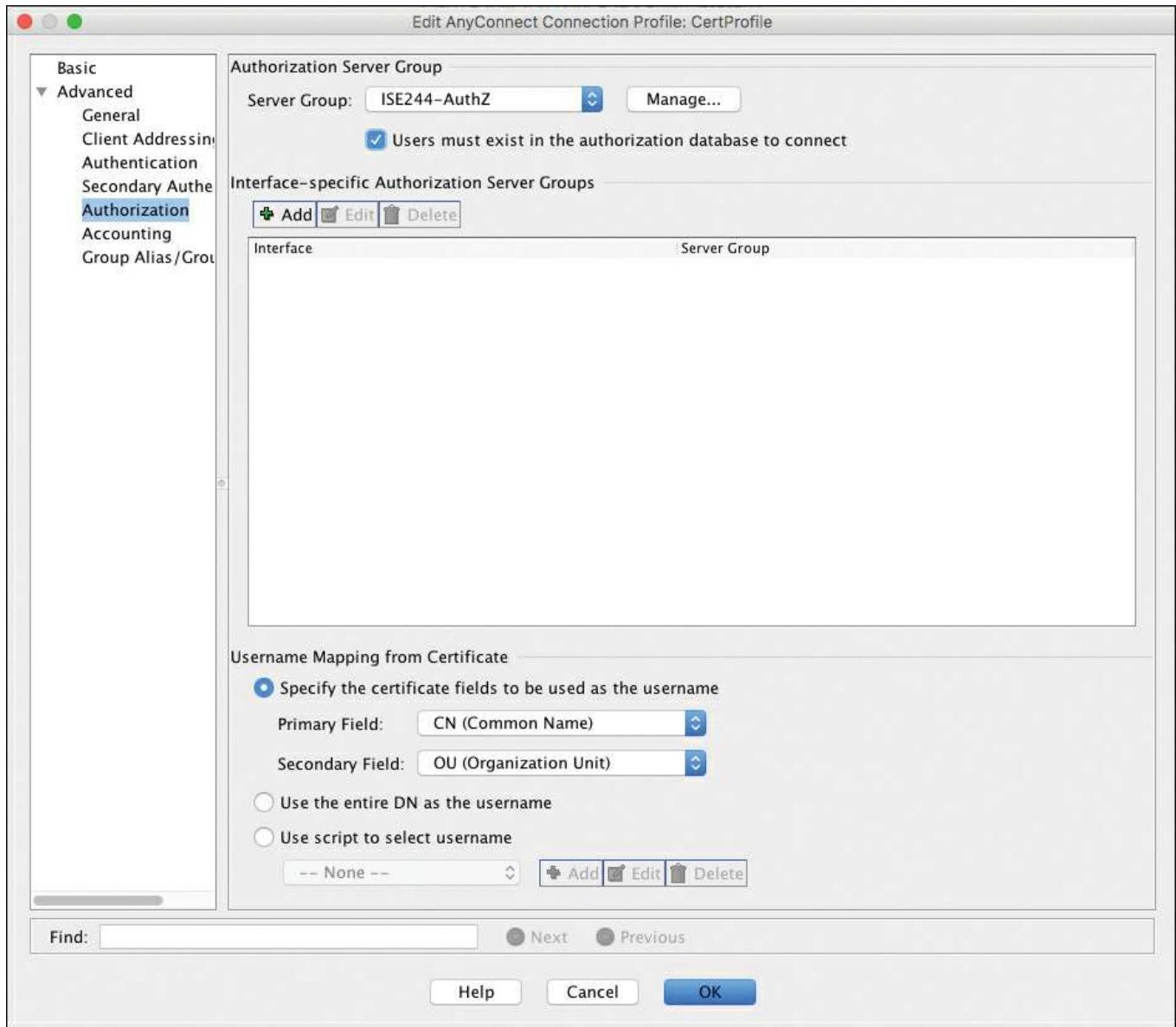
**Figure 19-63** AAA Server Group for Authorization Only

**Step 6.** Complete the remaining portions of the connection profile, as shown in [Figure 19-64](#).



**Figure 19-64** CertProfile: Basic Configuration

**Step 7.** Navigate to the **Advanced > Authorization** page of the connection profile, and select the AAA server group, as shown in [Figure 19-65](#).



**Figure 19-65 CertProfile: Authorization**

**Step 8.** Check the **Users Must Exist in the Authorization Database to Connect** check box.

**Step 9.** Click **OK**.

The ASA configuration is complete. Ensure that you save the configuration before exiting ASDM. There is one last step, which is to configure ISE to allow the ASA to perform the authorizations.

In the ISE policy set for VPN, insert a new authorization rule with a condition of **RADIUS:Service-Type EQUALS Authorize Only**, and to use the **ALL\_AD\_Join\_Points** identity source sequence. Ensure that the If Authentication Failed option is set to **Continue**.

You have created a special authentication rule that looks for authorize-only RADIUS

requests. It is configured as a separate authentication rule, because the If Authentication Failed option is set to Continue. In theory, with this setting configured, you could inadvertently allow malicious users to gain access to the network, so it needs to be restricted as much as possible.

[Figure 19-66](#) shows the VPN policy set with the new authentication rule configured.

The screenshot shows the Cisco ASA Policy Set configuration interface. At the top, it says "Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page".

**ATW-VPN Policy Set**

Status	Name	Description	Conditions	Actions
<input checked="" type="checkbox"/>	ATW-VPN	VPN Policy Set	DEVICE:Device Type STARTS WITH Device Type#All Device Types#VPN	<a href="#">Edit</a>

**Authentication Policy**

- AuthZOnly : If Radius:Service-Type EQUALS Authorize Only Allow Protocols : Default Network Access and [Edit](#)
- Default : use All\_AD\_Join\_Points
- Default Rule (If no match) : Allow Protocols : Default Network Access and use : All\_User\_ID\_Stores [Edit](#)

**Authorization Policy**

**Exceptions (0)**

**Standard**

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	Actions
<input checked="" type="checkbox"/>	Employee-PostureRedirect	If (AD-Employees AND Session:PostureStatus NOT_EQUALS Compliant)	then VPN-Posture-Redirect	<a href="#">Edit</a>
<input checked="" type="checkbox"/>	Employee-Permit	If (AD-Employees AND Session:PostureStatus EQUALS Compliant)	then VPN-Full-Access	<a href="#">Edit</a>
<input checked="" type="checkbox"/>	Default	If no matches, then DenyAccess		<a href="#">Edit</a>

**Figure 19-66** VPN Policy Set with Authorize-Only Authentication Rule

## Connecting to the VPN via CertProfile

When connecting to the VPN through the new CertProfile connection profile, the user is not prompted for their username and password; instead, the connection occurs automatically using the certificate.

[Figure 19-67](#) shows a connection attempt where the user chooses the CertProfile connection profile. Normally, you would not have the end user select their profile. All of this should happen in the background and be seamless to the end user.



**Figure 19-67** Connecting to the VPN via CertProfile

[Figure 19-68](#) shows the Live Log, where you can see the connection establish, and the posture change from Pending to Compliant, all while the AuthZOnly authentication rule is being used. Whether certificate-based authentication or username/password-based authentication is being used doesn't matter; ISE is still able to perform its functions, such as performing the posture assessment.

Status	Details	Identity	Endpoint ID	Endpoint P...	Authentication Policy	Authorization Policy	Authorizati...	Posture St...
x	▼	Identity	Endpoint ID	Endpoint Prof...	Authentication Policy	Authorization Policy	Authorization	Posture Status
✓	o	#ACSAACL#-IP-VP...						a
✓	o		10.117.118.215				VPN-Full-Acc...	Compliant
●	o	employee1	00:0C:29:D6:91:69	Windows7-...	ATW-VPN >> AuthZOnly	ATW-VPN >> Employee-PostureRedirect	VPN-Postur...	Compliant
✓	o	#ACSAACL#-IP-VP...						a
✓	o	employee1	00:0C:29:D6:91:69	Windows7-...	ATW-VPN >> AuthZOnly	ATW-VPN >> Employee-PostureRedirect	VPN-Postur...	Pending

**Figure 19-68** Live Log: Posture Compliance with Certificate-based Authentication

## Summary

Congratulations! You made it! This was a long chapter with a lot of configuration steps and technologies.

In this chapter, you learned about the different types of VPNs. The two types of remote access VPN are clientless and client-based, the latter of which was the focus of this chapter because it is relevant to ISE. Cisco AnyConnect is the VPN client used for the RA-VPN and the ASA, but it is also a very powerful endpoint client that has many different security modules, including HostScan, which is used for ASA-based posture assessment, and System Scan, which is used for ISE-based posture assessment.

You learned about the differences between the ASA and other NADs, especially with regard to the way CoA is used. The ASA uses CoA-Push, instead of CoA-Reauth. You also learned that the ASA has a lot of capabilities related to RA-VPNs, including double authentication. You discovered how to use the ASA as an SCEP proxy from AnyConnect to the ISE CA, for issuing certificates to AnyConnect that can then be used to perform certificate-based authentications.

You also examined how the certificate-based authentications leverage an authorize-only form of RADIUS request to ISE, and ISE never performs an authentication at all.

Keep in mind that the ASA VPN is capable of much more than we covered in this chapter. For more detailed information and knowledge, check out Cisco ASA: All-in-One Next-Generation Firewall, IPS, and VPN Services, Third Edition (Cisco Press, 2014).

# Chapter 20 Deployment Phases

This chapter covers the following topics:

- Reasons to use a phased approach
- Monitor Mode
- Low-Impact Mode
- Closed Mode
- Transitioning from Monitor Mode to your end state
- Wireless networks

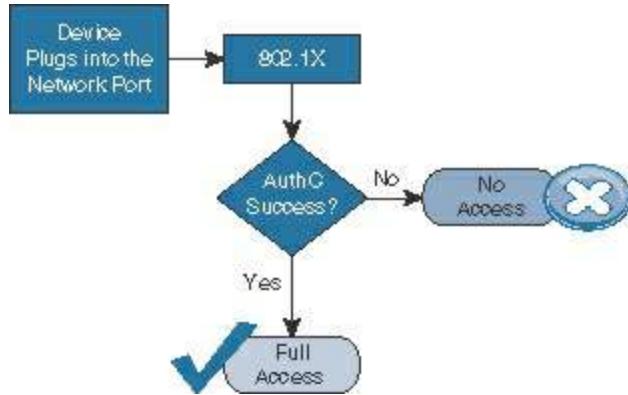
This book has already examined quite a bit of configuration detail about ISE and the network access devices. It has covered the technical merit of policy creation, guest lifecycle management, posture assessment, and much more. There is obviously a great deal to consider when you deploy a system such as this one. It is not something you should just enable overnight with the “flip of a switch.”

This chapter focuses on the recommended approach to deploying the Secure Access system. It reviews some of the challenges that were encountered in the past, and why certain technologies were enhanced to provide a more prescriptive approach to deployment.

## Why Use a Phased Approach?

Back in the early 2000s, a new technology was emerging that would revolutionize networking as we knew it. This technology was IEEE 802.1X, which enabled authentication of a network access port prior to allowing devices onto the network. The concept was simple, and some predicted that within 5 years there would not be any “hot ports” in the world that wouldn’t first authenticate the user, and that unauthorized users would no longer be able to access networks.

802.1X was originally created to be very binary in nature. A device either is authenticated and gets access or fails authentication and is denied. [Figure 20-1](#) graphically represents the logical process of 802.1X authentication.



**Figure 20-1** 802.1X Intended Behavior

However, as you already know from reading the previous chapters in this book, this authentication process has many different moving parts that must all be aligned properly if you want to avoid causing denial of service (DoS) on your own user population. This can be accomplished with the following:

- Suplicants must be configured on devices.
- Lists of MAC addresses must be created in order to properly MAB devices.
- Profiling probes must be enabled and have the ability to collect data regarding endpoints to help build that list of MAC addresses.
- Certificates must be trusted.
- Guest accounts must be created.

If you were to just “flip the switch” and enable 802.1X on all access-layer switch ports all at once, you would most likely have a swarm of angry users converging on the IT department threatening to terminate their jobs. That is called a “career-limiting event,” or CLE for short.

We’re reminded of one implementation at a financial organization with 2000 switch ports in its campus building. Due to an audit requirement, the organization had to enable network authentication by a certain date to avoid being subject to fines. The mandate came down from management, the project received its funding, and away we went. We lab tested everything and proved it all would work using our Cisco Catalyst 6513 Switches and the native Windows XP (Service Pack 3) supplicant configured for EAP-TLS machine authentication with the Active Directory–issued machine certificate.

It was beautiful. Everything was working perfectly on our test systems in the lab, and the desktop team assured us that the Group Policy Object (GPO) was sent out properly and all the Windows XP systems were ready to authenticate. All we had to do was turn on the authentication on the switch ports (theoretically).

Our advice was still to deploy in Monitor Mode first, and then change over to Closed Mode (the end state). This meant that the **authentication open** command needed to be

applied to the switch port, but Monitor Mode would allow us to validate that authentications would all be successful before we truly enforced access to the network. The security oversight committee nixed the idea immediately, because the word “open” was in the command. We were simply not allowed to use it—ever. Never mind that all 2000 ports were currently wide open and that using the command would not make matters worse at all. We simply were not allowed to use that command.

So, the big day arrived. At 10 p.m. on a Sunday night, we had our change-control window to run our scripts and enable Closed Mode authentication across 2000 switch ports in a matter of minutes. Of those 2000 ports, only 10 were authenticating successfully, and we had accomplished exactly what I feared: a denial of service for all other systems.

Why did this occur? The policies were all correct. The certificates had all been pushed out to the desktops. The supplicants were configured. However, no one had realized that the supplicant configuration would not take effect prior to rebooting the Windows systems! We did not figure that out until the next afternoon, after the desktop team had researched the issue further; meanwhile, we had created a DoS problem for all the users that morning.

The story has a happy ending. After the desktop team pushed out a job to reboot all the systems, we re-enabled authentication at the next change-control window and were able to get 99 percent of the systems to authenticate successfully.

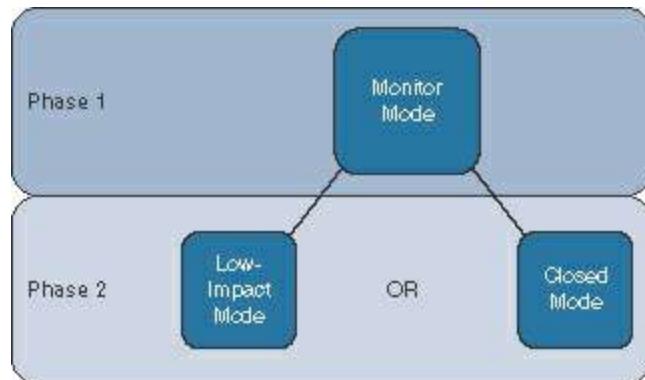
However, not all deployments are that lucky, or that well planned out in advance. This is why a phased approach to deploying identity solutions is always a good idea.

## A Phased Approach

Using a phased deployment approach, you start off in Monitor Mode and gradually transition into your end state of either Low-Impact Mode or Closed Mode. By doing so, you can avoid DoS scenarios such as the one described in the previous section. With a monitoring phase, you have time to build your list of endpoints with profiling. You can manually import the MAC addresses that will be MAB’d without profiling and ensure that you know exactly what will happen, before it happens.

Then, you can gradually move into a final state of enforcement. [Figure 20-2](#) shows how you logically start with Monitor Mode in Phase 1 and then move to either Low-Impact Mode or Closed Mode.

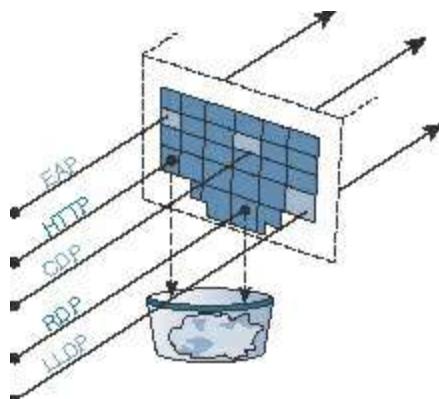
**Note** The end state of your deployment does not necessarily need to be either Low-Impact Mode or Closed Mode; you can blend the two. We have worked with a number of customers who use Low-Impact Mode in campus environments, and Closed Mode in their branches. It is up to you to determine what works best for your environment, and then deploy accordingly.



**Figure 20-2** Phased Deployments

## Authentication Open Versus Standard 802.1X

As previously described, a port that is protected with 802.1X will not allow network traffic to flow without a successful authentication. [Figure 20-3](#) illustrates that an 802.1X-controlled port normally only allows Extensible Authentication Protocol (EAP), Cisco Discovery Protocol (CDP), and Link Layer Discovery Protocol (LLDP) traffic to enter the port (all three are Layer 2 protocols) and denies all other traffic. When 802.1X is enabled on a port, the port is said to be a supplicant authenticator. That is a fancy way of stating that the port will communicate with EAP at Layer 2; the switch will broker that authentication to the RADIUS server.

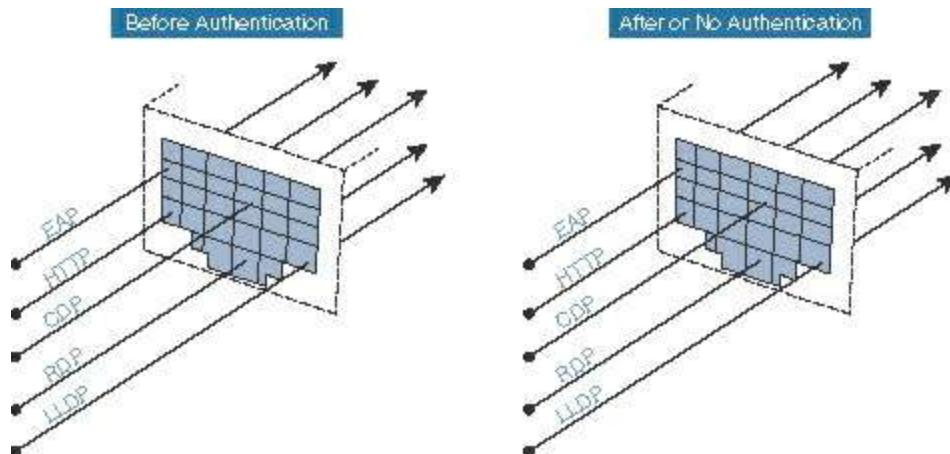


**Figure 20-3** Default Port Behavior with 802.1X

Cisco created an enhancement to standard 802.1X ports that allows the port to be a supplicant authenticator. However, it permits all traffic to flow normally through the

switch port even without an authentication occurring. This allows the supplicant to authenticate correctly if it is configured, but if the device does not have a supplicant configured or the switch receives an Access-Reject message from the RADIUS server, the Reject message is ignored.

[Figure 20-4](#) illustrates that, regardless of authentication, the switch port allows all traffic to flow, but it also authenticates the supplicant and performs MAB just like a standard 802.1X-enabled switch port.



**Figure 20-4** Port Behavior with Open Authentication

It is the creation of this authenticator enhancement that truly made Monitor Mode possible. It is, of course, not the only necessary component of Monitor Mode, but it is certainly the catalyst (pardon the pun).

## Monitor Mode

Monitor Mode is a process, not just a command on a switch. The process is to enable authentication (with **authentication open**) to see exactly which devices fail and which ones succeed.

[Figure 20-5](#) shows a high-level flow diagram describing Monitor Mode.



**Figure 20-5** Monitor Mode Operational Flow

One key point to understand about Monitor Mode is that it is applicable to wired

environments only. If you have ever configured a device to connect to a wireless network, you are familiar with the concept of a service set identifier (SSID). When using Wi-Fi, configuring a client (supplicant) is expected behavior. You must tell the Wi-Fi-capable endpoint which network to connect to by identifying its SSID, and then you provide credentials for that network. It's common, it's expected, and it's well known.

A wired network, however, does not have the concept of an SSID, so there is no popup window on the endpoint asking which network you would like to connect with. It's just assumed that your device is physically connected and therefore you are attached to the correct network. With wireless, if you don't have a supplicant, you cannot connect. Wired environments are expected to always work, supplicant or not. The wired port must be able to handle the following:

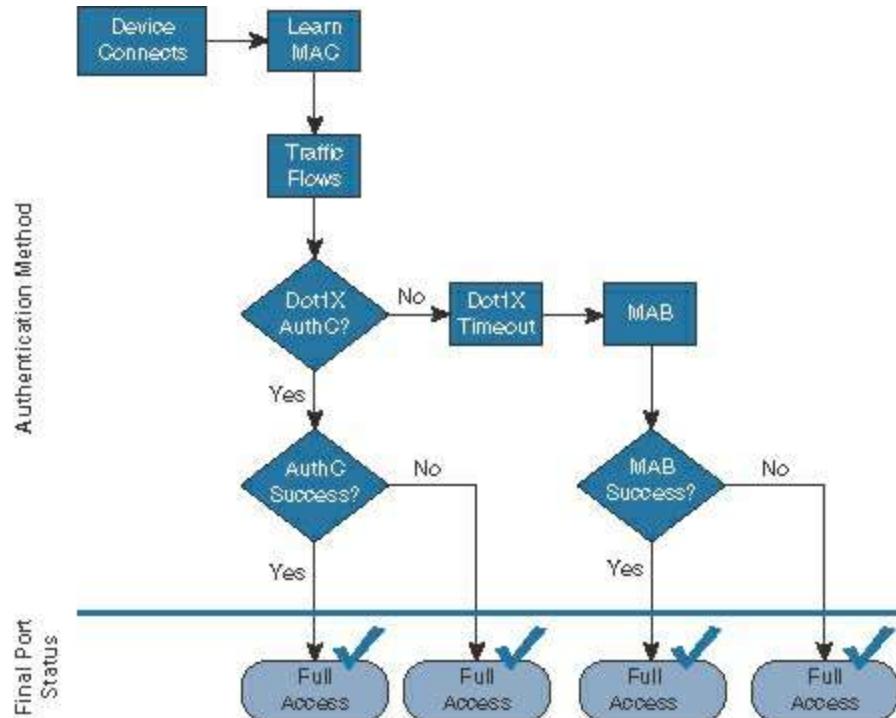
- A device that has a supplicant (802.1X)
- A corporate device that doesn't have a supplicant but belongs on the network (such as an IP phone or printer)
- Guest users

So, there is quite a bit to audit when in Monitor Mode.

Another very important thing to understand about Monitor Mode is that authorization results from the RADIUS server will absolutely be honored (Access-Reject is the only command that is ignored). So, if your authorization result from ISE includes dynamic VLAN (dVLAN) assignment or downloadable ACLs (dACL), those will absolutely be honored and applied to the port.

For a phased deployment approach, it is highly recommended to use Network Device Groups (NDG) in ISE. Using these NDGs, you can build specific policies that only send the basic authorization results (Access-Accept and Access-Reject) to switches that are part of a Monitor Mode NDG.

[Figure 20-6](#) shows a high-level flow diagram describing Monitor Mode.



**Figure 20-6** Monitor Mode Flow Diagram

## Prepare ISE for a Staged Deployment

One of the primary ways to differentiate modes within your ISE policies is to use NDGs. In this section, you will configure the NDGs to have a top-level group of Stage, and then subgroups for Monitor Mode, Low-Impact Mode, and Closed Mode. With these NDGs, the authorization policies may look for the particular stage of deployment. For purposes of keeping the policies nice and clean, use separate policy sets for each stage of deployment.

**Note** The following exercises assume that policy sets have been enabled already under **Administration > System > Settings > Policy Sets**.

## Create the Network Device Groups

A Network Device Group may be a top-level group, such as Location or Type. The NDG may also be created as a child (aka subgroup) of an existing top-level group, such as Switch (which would be a subgroup of the Type NDG). The following steps guide you through the creation of both a new top-level group, named Stage, and subgroups.

From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Work Centers > Network Access > Network Resources > Device Groups**.

**Step 2.** Click Add.

**Step 3.** In the Name field, name the Network Device Group **Stage**, as shown in [Figure 20-7](#).

The screenshot shows a modal dialog titled "Add Group". It has three input fields: "Name" with a red asterisk containing the value "Stage", "Description" which is empty, and "Parent Group" with a red asterisk containing the value "Select Group or Add as root group". Below these is a dropdown menu with a downward arrow. At the bottom right are two buttons: "Cancel" and "Save", with "Save" being green and "Cancel" being grey.

**Figure 20-7** Add a Stage NDG

**Step 4.** Leave the Parent Group alone, so that Stage becomes a new root group.

**Step 5.** Click Save.

**Step 6.** Click Add to add another group named Monitor Mode, with Stage selected as the parent group.

**Step 7.** Repeat Step 6 and create a group for Low Impact Mode and Closed Mode.

[Figure 20-8](#) shows the final NDG configuration.

Network Device Groups	
All Groups	Choose group ▾
<span>⟳ Refresh</span> <span>+ Add</span> <span>Duplicate</span> <span>✎ Edit</span> <span>trash</span> Trash <span>👁 Show group members</span> <span>Import</span>	
<input type="checkbox"/> Name	Description
<input type="checkbox"/> All Device Types	All Device Types
<input type="checkbox"/> All Locations	All Locations
<input type="checkbox"/> Is IPSEC Device	Is this a RADIUS over IPSEC Device
<input type="checkbox"/> Stage	
<input type="checkbox"/> Closed Mode	
<input type="checkbox"/> Low Impact Mode	
<input type="checkbox"/> Monitor Mode	

**Figure 20-8** Final Stage Network Device Groups

## Create the Policy Sets

Now that you have the NDGs configured for the different stages of the deployment, you can move on to creating the policies themselves. From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Work Centers > Network Access > Policy Sets**.

**Step 2.** Ensure that your default policy is selected on the left side (as shown in [Figure 20-9](#)) and click the + icon in the upper-left corner.



**Figure 20-9** Default Policy Set Selected

**Step 3.** Choose **Create Above**.

**Step 4.** Name the new policy set **Monitor Mode**, as shown in [Figure 20-10](#).

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order. For Policy Export go to <a href="#">Administration &gt; System &gt; Backup &amp; Restore &gt; Policy Export Page</a>			
Status	Name	Description	Conditions
 	Monitor Mode		DEVICE:Stage EQUALS Stage#Monitor Mode

**Figure 20-10** Monitor Mode Policy Set

**Step 5.** Add a new condition of **DEVICE:Stage EQUALS Monitor Mode**.

**Step 6.** Click **Done**.

At this point, any network device that is a member of the NDG named Monitor Mode will use this policy set. All authentications and authorizations occur with this set of policies.

It is up to you, the administrator of ISE policies, to ensure that any authorization results for Monitor Mode switches are only Access-Accept and Access-Reject. Always remember that other authorization results will be accepted and applied to the switch port, so you must ensure that web authentication, ACLs, and VLAN assignments do not occur for these switches.

## Low-Impact Mode

As described previously in this chapter, Low-Impact Mode is one of the end-state choices for your deployment. Closed Mode is the other final stage. There is no specific best practice for which mode is better to deploy; it is entirely dependent on the organization and its needs.

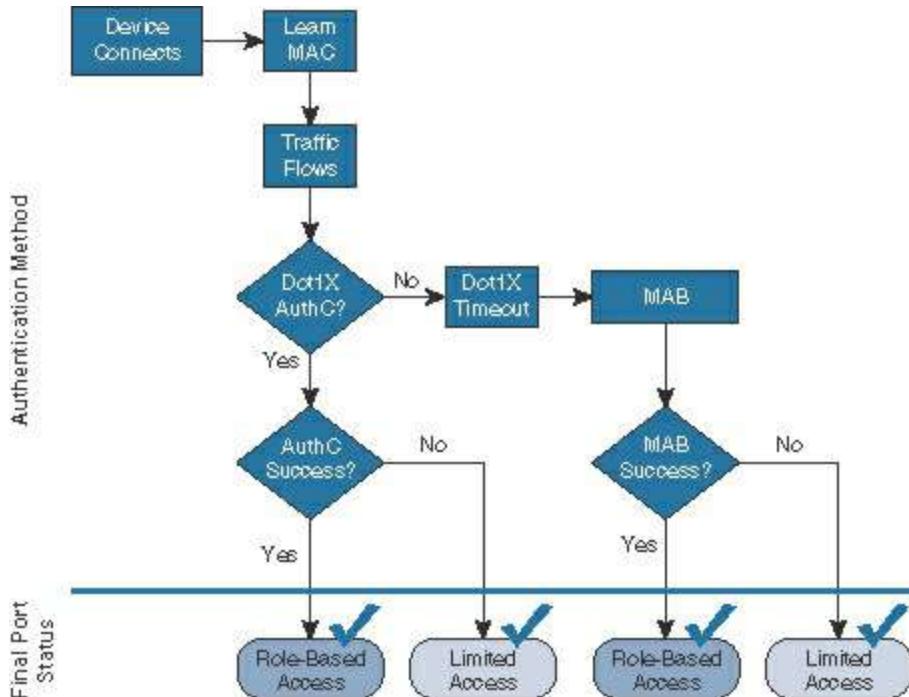
For example, we have worked with a number of large organizations that use a variety of technologies to reimagine desktop systems that make use of the Preboot Execution Environment (PXE) to boot into a pseudo OS and then connect to an imaging server that reimages the company desktop. Those PXEs were time sensitive and had no ability to authenticate to the network infrastructure. Yet they had to seamlessly be able to boot, connect to the reimaging server, and update the desktop to the latest corporate image, and do so without any additional user interaction. Low-Impact Mode was the only way to make this work feasibly in those environments.

Another example is a retail organization that uses thin clients in its retail stores. These thin clients must be able to boot using PXE, gain limited access to the network, download their OS from the local store server, and have that access before their local DHCP timers expire. Once that OS is loaded into memory and takes the system over, its supplicant sends an EAPoL-Start message into the network and authenticates with 802.1X. Low-Impact Mode allows the thin client to boot automatically and have the appropriate levels of access to the store server to download the OS.

Low-Impact Mode adds security on top of the framework that was built in Monitor Mode. It continues to use the **authentication open** capabilities of the switch port, which allows traffic to enter the switch prior to an authorization result. This permits the DHCP clients to be assigned an IP address before their DHCP timers run out (for example).

With Low-Impact Mode, you are adding security right from the start by putting a port-based ACL (pACL) on the switch port interface. This is a traffic-filtering ACL that gets applied to the port as part of the switch configuration and is then overridden by the dACL sent down from ISE.

[Figure 20-11](#) shows the operational flow intended for Low-Impact Mode. As one of the two possible end states (Closed Mode being the second), it provides very specific access per user, per device, or other condition that you wish to use in the ISE authorization policies. Remember, the goal of Low-Impact Mode is to administer very limited network access to devices without authentication, and then provide very specific access to those that have been authorized. As with any other security solution, tuning the authorization results is something that can take a lot of operational man-hours. So, it is always recommended that you deploy authorization results in stages. For example, begin with a policy that permits full access to any device that has authenticated successfully. Ensure that the environment is fully functional, and then begin to “ratchet down” the security. Make the dACLs more specific, and so on.



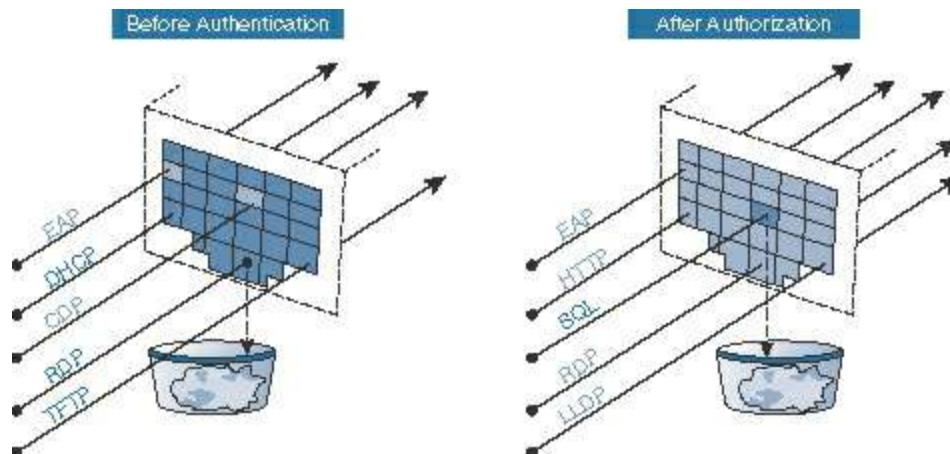
**Figure 20-11** Low-Impact Mode Operational Flow

[Figure 20-12](#) shows that the pACL is applied prior to authentication, which only allows specific traffic into the port. Once the authentication occurs, the authorization needs to include a dACL that selectively permits or denies traffic. Other authorization results

may also be applied at the port, such as:

- URL redirection
- VLAN assignment
- Media Access Control Security (MACsec) encryption
- Security Group Tags

**Note** VLAN assignment should be used only on devices that use supplicants. Without a supplicant, the device will most likely not be able to identify the VLAN change, and may end up with the wrong IP address for its final VLAN assignment.



**Figure 20-12** Low-Impact Mode Port Behavior

## Closed Mode

Closed Mode is similar to the default behavior of 802.1X. As shown earlier in [Figure 20-3](#), the port does not allow any traffic before the authentication (except for EAP, CDP, and LLDP), and then the port will be assigned to specific authorization results after the authentication.

**Note** Closed Mode was once called High-Security Mode. It was renamed to discourage the perception that it is more secure than Low-Impact Mode. In truth, both modes are equally protected. The security level of either end state is truly dependent on the configuration of the devices and the policies on ISE, not the mode of operation. In other words, an administrator can make Closed Mode very insecure or very secure, depending on their implementation.

As shown in [Figure 20-1](#) earlier in the chapter, the operational model of 802.1X was always designed to deny access to any device that does not authenticate successfully.

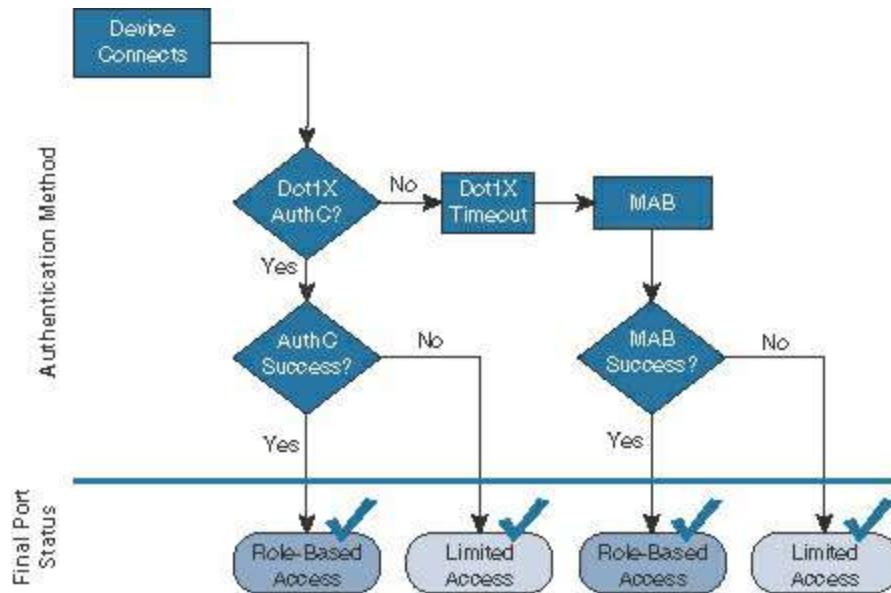
This is a perfectly understandable model for wireless network access, where a human is required to interact with the device and configure a wireless client (supplicant) to connect to a specific SSID with specific credentials.

However, in a wired world, there are many devices that require network access without any user interaction, such as IP cameras, IP phones, printers, fax machines, badge readers, and so much more. So, MAB had to be added to the process flow.

The concept of completely denying access to the network if authentication fails, or if a supplicant is not configured, proved to have operational difficulties. Some level of access was needed. Originally, the switch itself would have a “Failed Authentication VLAN,” where the switch makes a local decision to authorize access to a specific VLAN when a device failed authentication. Additionally, if authentication were to time out (meaning there was no supplicant on the endpoint), then it would authorize access to a locally configured guest VLAN.

One of the problems with that original logic was the lack of centralized knowledge and control. As far as the policy server was concerned, the access was denied. Yet the device was still on the network because the NAD made a local decision in spite of what the policy server said.

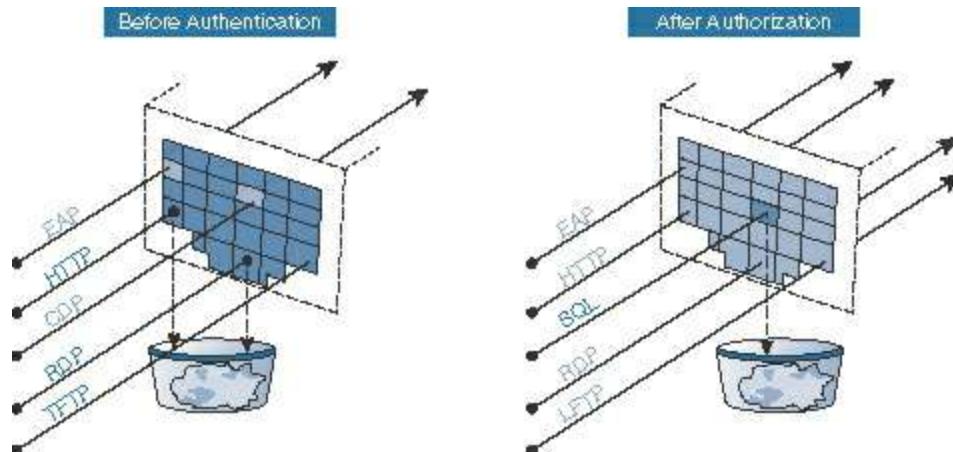
[Figure 20-13](#) shows the operational flow of Closed Mode. Notice that it is nearly exactly the same as Low-Impact Mode. All the same authorization results are available for use, but Closed Mode does not allow any of the PXE-type traffic into the port prior to the authorization result, unlike Low-Impact Mode.



**Figure 20-13** Closed Mode Flow

[Figure 20-14](#) shows the port behavior in Closed Mode. Virtually zero traffic is allowed into the port before the authentication. Once the session is authorized, very specific authorization results may be applied to the port, such as:

- VLAN assignment
- dACL
- URL redirection
- MACSec encryption
- Security Group Tags



**Figure 20-14** Closed Mode Port Behavior

## Transitioning from Monitor Mode to Your End State

The key to using a phased deployment approach successfully is to understand how to transition from Monitor Mode to the end state chosen (Low-Impact Mode or Closed Mode). This is why you built out NDGs and policy sets previously in this chapter.

With Monitor Mode, you must ensure that only Access-Accept and Access-Reject authorizations are used. With Low-Impact Mode and Closed Mode, you are able to send the other authorization results, such as sending a URL redirection for Centralized Web Authentication (CWA).

The purpose of Monitor Mode is to ensure that the endpoints are all authenticating correctly, either via 802.1X with their supplicants or via MAB with profiling or even statically. You could get the first pilot switch ready, prepare all the devices for authentication, and, seeing that everything looks good, flip the switch and change the default authorization policy to send a CWA result instead of just the basic accept or reject message. That first switch will be fine, all the devices will work correctly, and life will look easy.

However, you wouldn't want to push the CWA result to the switch port if you have not fully prepared the supplicants and educated the users on a possible change of experience when logging in to the network. That would be another career-limiting event.

That is why you use NDGs. You ensure with the NAD's membership of the "Stage" NDG that you are sending the correct results to the correct network devices.

Imagine rolling out ISE to thousands of branch locations. You prepare a branch by putting it into Monitor Mode. When you are certain that that branch is fully ready and all the devices are recognized and authenticating successfully, you then can simply move the switch from the Monitor Mode NDG to the end-state NDG, and make a few command modifications to the switches.

## Wireless Networks

Wireless networks behave differently than wired networks. With the creation of a WLAN, you must define the security for that WLAN. When using 802.1X, set the security to use WPA+WPA2 for key management. This setting cannot be mixed with an open authentication, and there are no “fallback” options.

For a guest authentication, the guest needs to connect to a different SSID. This is fundamentally a much different model from that used for a wired network.

Even though wireless behaves differently, the authorization results in ISE may be configured to send the responses to wired devices and wireless devices, providing a unified access strategy. This permits wireless networks to be managed as part of your Low-Impact Mode or Closed Mode deployments.

## Summary

This chapter provided an overview of the phased deployment approach to deploying ISE and 802.1X. It covered the importance of Monitor Mode for wired environments, with an emphasis on using only basic authorization results while in Monitor Mode.

This chapter showed you how to configure policy sets differently for NADs based on their “Stage” NDG membership. It also discussed methods for how to use those NDG memberships to transition one switch at a time from Monitor Mode to the end-state mode of your choice.

## **Part V Advanced Secure Access Features**

[Chapter 21 Advanced Profiling Configuration](#)

[Chapter 22 Cisco TrustSec AKA Security Group Access](#)

[Chapter 23 Passive Identities, ISE-PIC, and EasyConnect](#)

[Chapter 24 ISE Ecosystems: The Platform eXchange Grid \(pxGrid\)](#)

# Chapter 21 Advanced Profiling Configuration

This chapter covers the following topics:

- Profiler Work Center
- Creating custom profiles for unknown endpoints
- Advanced NetFlow probe configuration
- Profiler CoA and exceptions
- Profile monitoring and reporting

This chapter explores the intricacies of the Identity Services Engine profiling service. The profiling service is designed to help corporations correctly identify the various device types that are attaching to their network. [Chapter 6, “Quick Setup of an ISE Proof of Concept.”](#) described how to quickly set up the ISE profiling service via the Visibility Setup Wizard, and [Chapter 10, “Profiling Basics and Visibility.”](#) explained the basic configuration of the ISE profiling service and its different profiling probes. This chapter explains how to create basic and complex profiler policies, how to configure custom profiler rules, and how to use profiler data in authorization policies. By the end of this chapter, you will have a firm grasp of the advanced capabilities and configuration of the Cisco ISE profiling service.

## Profiler Work Center

The Profiler Work Center was created to provide you with all of the steps necessary to configure profiling in ISE. [Figure 21-1](#) shows an overview of the steps required, broken down into three sections: Prepare, Define, and Go Live & Monitor.

The screenshot shows the Cisco ISE Profiler Work Center interface. At the top, there is a navigation bar with links like Overview, Ext Id Sources, Network Devices, Endpoint Classification, Node Config, Feeds, Manual Scans, Policy Elements, Profiling Policies, Policy Sets, and Troubleshoot. Below the navigation bar, the title "Profiler Overview" is displayed. The main content area is divided into three horizontal sections:

- Prepare (Section 1):**
  - Network Preparation:** Configure the network devices that you will be using for profiling.
  - Active Directory:** Configure your active directory identity stores to help with operating system identification.
  - Profiling Configuration:** Check the *Enable Profiling Service* option and specify the profiling configuration for each node in your deployment that will be profiling endpoints.
  - Feed Service:** Configure the feed service to automatically or manually update your profiling policies.
  - Settings:** Check the defaults for profiler configuration settings such as change of authorization to make sure they are acceptable.
  - Network Devices:** Configure your network devices to send probe data to ISE.
- Define (Section 2):**
  - Logical Endpoint Groups:** Review and customize logical profiles that enable you to organize endpoints into groups that make sense for your organization.
  - Profiling Policies:** Create custom profiling policies for devices unique to your organization.
  - NMAP Scan Actions:** Customize NMAP scan actions to maximize profiler accuracy.
  - Endpoint Access:** Add profile and logical profile conditions to your authorization policy.
- Go Live & Monitor (Section 3):**
  - Auditing:** Examine the endpoint classification to see how endpoints are profiled and customize the displayed information to meet your needs.
  - Endpoint Profile Changes:** Examine the Endpoint Profile Changes and other profiler reports to verify endpoints are profiled correctly and view information about them.
  - Troubleshooting:** Troubleshoot issues using diagnostic tools.

**Figure 21-1** Profiler Work Center

Each of the steps in the three sections also aligns with one of the categories listed at the top of the Profiler Work Center. This menu bar remains visible as you step through the workflows, thus making it easy for you to navigate. By following the steps in the Work Center and using the Work Center as a go-to starting point for any profiling needs, you can quickly configure, operate, and troubleshoot the profiling service.

## Creating Custom Profiles for Unknown Endpoints

Cisco ISE Profiler includes hundreds of device profiles out of the box. However, given the thousands of network device types available, it is inevitable that you will need to create a few custom profiles for your environment. When ISE cannot identify a device, it marks it as unknown and adds it to the Unknown Device Identity Group. ISE also saves all the attributes and their values it has collected on the device's behavior. You can then use these values to assist in creating your custom profile for this device type.

The key to creating a reliable custom device profile is to find profiler probe values that are unique to your custom device. If the values are too generic, you will have false-positive results matching your new device profile. Therefore, it is imperative that you choose unique profiler probe values or combination of values that become unique when combined into a profiler rule set. Refer to [Chapter 10](#) for more information on the ISE profiling probes.

## Identifying Unique Values for an Unknown Device

To identify the values that the ISE Profiler has collected on a device, go to **Context Visibility > Endpoints**. Filter under the Endpoint Profile column using the keyword **Unknown**, as shown in [Figure 21-2](#). You can then use the other filter options to find your device.

MAC Address	Status	IPv4 Address	Username	Hostname	Location	Endpoint Profile
00:30:44:17:C5:62	Up	10.40.132.18	00-30-44-17-...	SJC ➔ SJC19	Unknown	unknown
00:D0:2D:3A:87:9C	Up	10.0.0.186	00-d0-2d-3a-...	OEAP	Unknown	
00:D0:2D:40:AC:C6	Up	10.0.0.73	00-d0-2d-40-...	OEAP	Unknown	
00:0F:E5:01:7D:9A		173.39.21.15	000fe5017d9a	bgl16-access...	IND ➔ BLR-B...	Unknown
00:17:C3:7A:C7:92			0017c37ac792		OEAP	Unknown
00:21:CC:CB:51:16		10.127.6.12	0021ccb5116		IND ➔ BLR-B...	Unknown

**Figure 21-2** Unknown Profile Endpoints in ISE

Once you find your unknown device, click its MAC address. You are shown a list of all the attributes and their values that ISE has recognized from that device so far. Hopefully, this list is populated with enough unique information that you can now create your custom device profile. If this is not the case, you can do three things to gather more information:

- Create more traffic from this device
- Run a manual NMAP scan of the host
- Enable additional ISE profiler probes to capture more information types from this device

If all else fails, you could run an NMAP scan every time the device connects. This should be used with caution, however, because it drains ISE resources and performance.

By nature of the way profiling is used, make sure that the types of attributes and their values you use to create your device profile are

- Sent from the device every time it connects to the network
- Happen very, very early after the device is connected to the network

[Figure 21-3](#) and [Figure 21-4](#) depict an example device showing a manual NMAP scan and the host's various attributes/values that ISE has collected. You could then use any of

these in the creation of your new custom device profile. To see the manual NMAP scan results, click on the link of the same name shown in [Figure 21-3](#). You will be presented with data similar to that shown in [Figure 21-4](#).

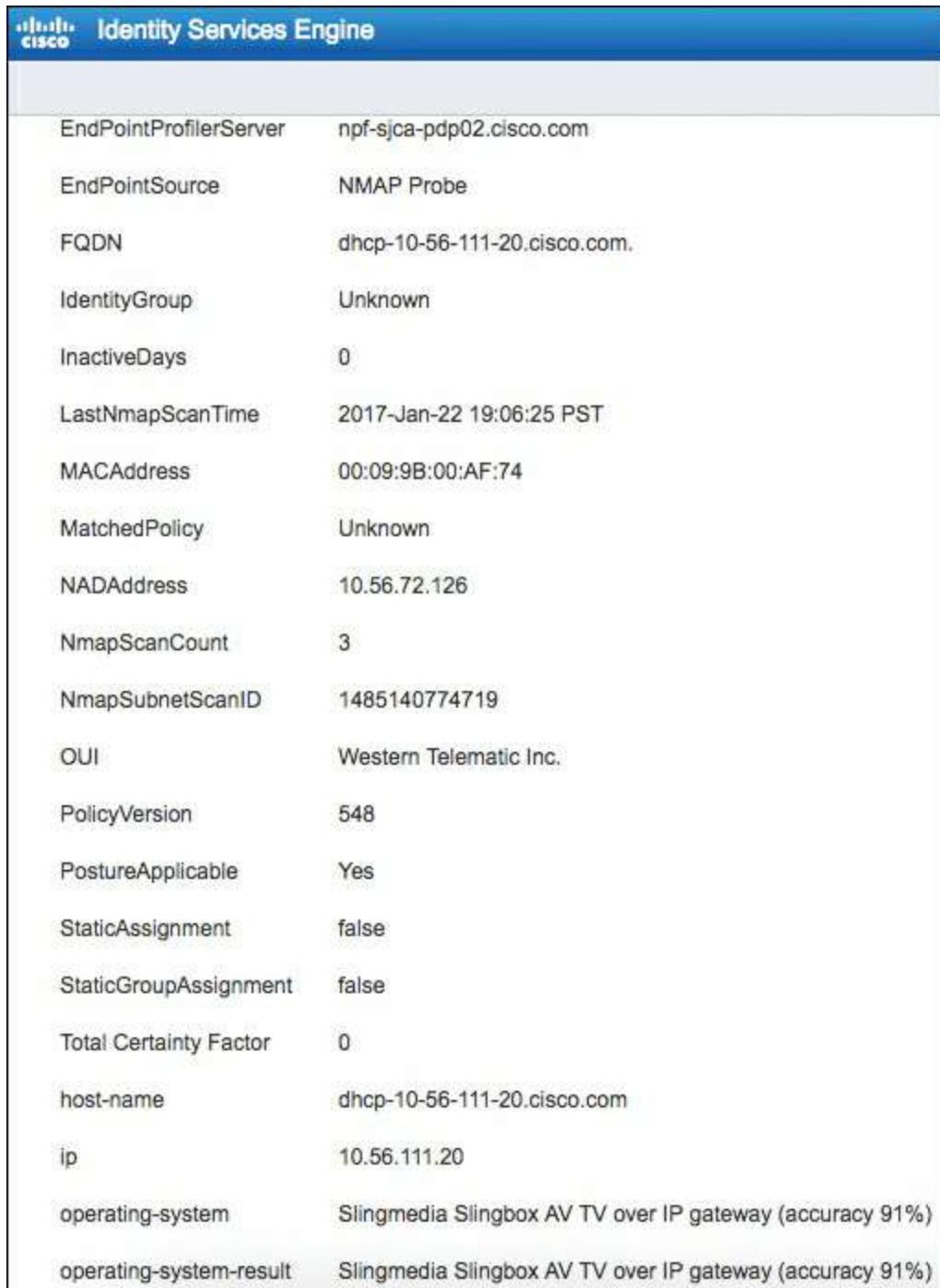
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, and PassiveID. Below the navigation is a secondary menu with links for Overview, Ext Id Sources, Network Devices, Endpoint Classification, Node Config, Feeds, Manual Scans (which is highlighted), Policy Elements, Profiling Policies, Policy Sets, Troubleshoot, and Reports.

The main content area is titled "Run Manual NMAP Scan". It contains the following fields:

- Node:** npf-sjca-pdp02
- Manual Scan Subnet:** 10.56.111.20 / 32
- Scan Options:**
  - Specify scan options
  - Select an existing NMAP scan action
- Scan Options (checkboxes):**
  - OS
  - SNMP Port
  - Common ports
  - Custom ports
  - Run SMB Discovery script
  - Skip NMAP Host Discovery (Only applies to manually run scans)
  - Include service version information

Below the scan options is a "Reset to Default Scan Options" button. At the bottom of the form are three buttons: "Run Scan", "Cancel Scan", and "Save As Scan Action...". A status message "Manual scan in progress..." is displayed at the bottom.

**Figure 21-3** Manual NMAP Scan



The screenshot shows the Cisco Identity Services Engine interface with a blue header bar containing the Cisco logo and the text "Identity Services Engine". Below the header is a table with various endpoint attributes listed in two columns.

EndPointProfilerServer	npf-sjca-pdp02.cisco.com
EndPointSource	NMAP Probe
FQDN	dhcp-10-56-111-20.cisco.com.
IdentityGroup	Unknown
InactiveDays	0
LastNmapScanTime	2017-Jan-22 19:06:25 PST
MACAddress	00:09:9B:00:AF:74
MatchedPolicy	Unknown
NADAddress	10.56.72.126
NmapScanCount	3
NmapSubnetScanID	1485140774719
OUI	Western Telematic Inc.
PolicyVersion	548
PostureApplicable	Yes
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	0
host-name	dhcp-10-56-111-20.cisco.com
ip	10.56.111.20
operating-system	Slingmedia Slingbox AV TV over IP gateway (accuracy 91%)
operating-system-result	Slingmedia Slingbox AV TV over IP gateway (accuracy 91%)

**Figure 21-4** Sample Endpoint Attributes

Because not all attributes can be obtained from an NMAP scan, other attributes are typically gathered from multiple sources (such as DHCP helpers, NetFlow, and web redirects). In general, the more useful attributes to look for when creating custom device profilers include the following (shown with attributes from the example):

- **User-Agent:** Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
- **dhcp-class-identifier:** MSFT 5.0
- **host-name:** dhcp-10-56-111.20.cisco.com

- **ip:** 10.56.111.20
- **OUI:** Western Telematic Inc.
- **operating-system:** Slingmedia Slingbox AV TV over IP gateway

The User-Agent string is populated with information gathered from packets sent from a web browser. All web browsers send a User-Agent string in the HTML requests and responses to identify the type of browser and operating system being used.

The dhcp-class-identifier is populated either by the manufacturer of the device or by the operating system that is running on the device. In the case of embedded systems, it is almost always populated by the manufacturer and thus can be a helpful profiling attribute.

The host-name attribute can come in handy as a supporting attribute. For example, if the hostname contains a string such as “iPad,” you can use that as part of a larger profiler policy with other rules. The other rules might be OUI vendor equaling “apple” and User-Agent string containing “iPad.” Each rule adds something to the certainty value of the policy when matched. But alone, neither could add enough certainty to cause a match of the whole device profile policy. This helps to cut down on false positives with your custom profile policies.

## Collecting Information for Custom Profiles

[Table 21-1](#) depicts an example worksheet you could create to collect the information needed for your custom ISE device profiles.

Device Type	Attribute Type	Attribute Name	Condition Operator	Attribute Value	Collection Method
MRI Scanner	DHCP	host-name	Contains	TS34D	DHCP SPAN of corp. DHCP server ports
	MAC	OUI	Equals	Drier-ACME	Radius authentication
A/C Unit	DHCP	Vendor Class	Contains	GE	DHCP SPAN
	DHCP	host-name	Contains	GE	DHCP SPAN

**Table 21-1** Device Profile Information Worksheet

ISE now includes hundreds of medical device profiles out of the box. Seeing as there are so many network-connected medical devices these days, let’s walk through creating a theoretical profile policy to identify a medical device.

Here are the high-level steps:

- Step 1.** (Optional) Create one or more profiler conditions using attributes and values collected by ISE.
- Step 2.** Create an endpoint profiler policy using the conditions created.
- Step 3.** (Optional) Create a logical profiler policy to group similar profiling policies under a single logical name. For example, IP Phones would include all IP Phone-related profiler policies.

## Creating Custom Profiler Conditions

Creating a profiler condition is not a required step, but it is definitely a common one. Instead of creating a condition, you could just create the conditions within the profile policy ruleset. In most cases, though, you will want to create a condition for anything that you may use again, use in multiple policies, or have to change the value for periodically. Here are the steps to creating a profiler condition:

- Step 1.** Connect the new device to your ISE Profiler-monitored network. Try to log on to the network with this device and then perform any typical startup activities that this device or operator would normally complete. This allows ISE to collect information about the device.
- Step 2.** Look up the MAC address of your test device in the ISE endpoint classification list. Examine what was captured and look for values that either are unique by themselves or would be unique when combined. Write these down.
- Step 3.** (Optional) Run a manual NMAP scan against the device. Note any useful findings of the scan.
- Step 4.** Create a set of profiler conditions using the unique values that were captured. Go to **Policy > Policy Elements > Conditions > Profiling**. You should see a screen like [Figure 21-5](#).

Profiler Check Name	System Type	Expression	Description
Android-Amazon-Kindle-Rule3-Check1	Cisco Provided	host-name CONTAINS kindle	Condition for Android-Amazon-Kindle , based on DHCP-H
Android-Amazon-Kindle-Rule4-Check1	Cisco Provided	host-name CONTAINS kindle-	Condition for Android-Amazon-Kindle , based on DHCP-H
Android-Amazon-Phone-Rule1-Check1	Cisco Provided	User-Agent CONTAINS SD49	User-Agent CONTAINS SD49
Android-Amazon-TV-Rule1-Check1	Cisco Provided	User-Agent CONTAINS AFT	User-Agent CONTAINS AFT
Android-Asus-Rule1-Check1	Cisco Provided	OUI CONTAINS ASUSTek	OUI CONTAINS ASUSTek
Android-Generic-DHCP-PRL-Check1	Cisco Provided	dhcp-parameter-request-list EQUALS 1, 12...	Custom condition for generic Android device based on D
Android-Generic-DHCP-PRL-Check2	Cisco Provided	dhcp-parameter-request-list EQUALS 1, 3, ...	Custom condition for generic Android device based on D
Android-Generic-DHCP-PRL-Check3	Cisco Provided	dhcp-parameter-request-list EQUALS 1, 12...	Custom condition for generic Android device based on D
Android-Generic-DHCP-PRL-Check4	Cisco Provided	dhcp-parameter-request-list EQUALS 1, 12...	Custom condition for generic Android device based on D
Android-Google-Class-B-1-Check1	Cisco Provided	User-Agent CONTAINS Glass	User-Agent CONTAINS Glass

**Figure 21-5** Profiler Conditions List

- Step 5.** To create a new condition, click **Add**.

**Tip** Each condition can only contain a single attribute and value. This makes it critical that your naming of the condition be descriptive not only of the device type but also the type of condition it is checking. Names are case sensitive and should usually start with a capital letter. A good name would be something like “Biomed-scanner-dhcp.” The condition name communicates that it is a biomedical device of type scanner that is keying off a DHCP attribute.

**Step 6.** Create your condition using the attributes and values you obtained from the endpoint’s attributes list. [Figure 21-6](#) depicts an example profiler condition for an MRI scanner.

Profiler Condition List > [New Profiler Condition](#)

Profiler Condition	
* Name	MRI_DeviceIP_OS
Description	Faux MRI device
* Type	IP
* Attribute Name	operating-system-result
* Operator	CONTAINS
* Attribute Value	MRI-Linuxv10
System Type	Administrator Created
<a href="#">Submit</a> <a href="#">Cancel</a>	

**Figure 21-6** Example Profiler Condition

**Step 7.** Create as many additional profiler conditions as required for your device.

## Creating Custom Profiler Policies

Even though ISE ships with hundreds of predefined profiler policies, it is inevitable that you will have a device on your network that isn’t in the list. When that happens, follow these steps to create a custom profiler policy:

**Step 1.** Go to **Policy > Profiling > Profiling Policies**. Click **Add**.

**Step 2.** Fill in the policy information with a descriptive name and description.

**Step 3.** Fill in the Minimum Certainty Factor value for the policy; leave everything else at their default values.

**Tip** It is a best practice to start with a Minimum Certainty Factor value of at least 1,000 for all custom profiler policies. This ensures that they will not be undermined by current or future Cisco-provided policies.

If multiple profiler policies match a device, the one with the highest certainty value is used. Ties are handled through first alphabetical match of the policy name.

**Step 4.** Add your rules. Insert a rule for each condition that you built previously for this device, as shown in the example in [Figure 21-7](#). Ensure that when you add up your certainty values, they equal or exceed the minimum certainty value you set for the device policy.

The screenshot shows the configuration of a new Profiler Policy named "Biomed-scanner". The policy is described as an "MRI Scanner". It is enabled and has a minimum certainty factor of 1,000. There are no exception or NMAP actions. An identity group is being created for this policy. The parent policy is set to none, and the associated CoA type is global settings. Two rules are defined: one for "Biomed-scanner-dhcp" with a certainty increase of 700, and another for "Biomed-scanner-out" with a certainty increase of 300. The "Submit" button is highlighted.

**Figure 21-7** Example Profiler Policy

**Step 5.** Click **Submit** when complete.

**Step 6.** The Profiler now reprofiles all devices. Any matches to your new profile policy will take effect immediately.

Using these simple steps, you can create all sorts of custom profiles. You also might choose to group some of your policies into logical policies (see [Chapter 10](#) for details). Some custom policies may be very simple; others might be extremely complex. Be sure to use a consistent naming scheme and always fill in the Description field on conditions and policies.

## Advanced NetFlow Probe Configuration

Cisco NetFlow data for profiling comes in handy when the other ISE probes are not able to capture enough unique data from a device to be used in a custom device policy. In most cases, you will not need to enable the NetFlow probe. But if you do, this section provides some of the best practices for setting it up.

**Note** The NetFlow probe should be used with caution, given its ability to overwhelm an ISE Policy Service Node (PSN) with millions of NetFlow records if not properly deployed.

Cisco NetFlow captures IP session data for network traffic flows. A NetFlow record can contain lots of useful information, but at a minimum, it contains the source/destination (SRC/DST) IP address and port/protocol of a flow. NetFlow is supported on all Cisco router platforms and some Cisco switching and wireless platforms. NetFlow is collected from NetFlow-capable Cisco devices that export the flow data to an ISE PSN. The default port that Cisco ISE listens on for NetFlow is 9996.

NetFlow is a Cisco-proprietary messaging protocol that comes in several versions. The only version that is useful to ISE is NetFlow v9. Don't bother sending ISE the other versions; it's just not worth it. The following is a partial list of Cisco devices that support NetFlow:

- Cisco 7.4+ WLC
- Cisco ISR Router
- Cisco ISR G2
- Cisco 4500 Sup 8
- Cisco ASR1000
- Cisco ASR9000
- Cisco 3750X and 3560X
- Cisco 4500 and 4500X with Sup 7
- Cisco 6500 with SUP2T
- Cisco 6500 with Sup 32 and Sup 720
- Cisco 7600
- Cisco C3650/3850
- Cisco UCS Servers
- Cisco XR12000/12000 Series Routers
- Cisco CRS-1

- Cisco Nexus 7000
- Cisco Nexus 1000V

In addition to the NetFlow probe's ability to match a device to a device type based on its traffic flow characteristics, it can also identify a device that is sending anomalous traffic. Here is an example: A certain biomed device should only ever talk to two IP addresses and only on two TCP ports, 5454 and 4533. If NetFlow recognizes traffic other than that, the ISE Profiler can issue a Change of Authorization (CoA) or start an NMAP scan of the device to see if the device type for that MAC address has changed. Perhaps someone is trying to spoof the MAC address of a known device with his or her own device. Or perhaps the device itself has been compromised with malware and is being used as part of a botnet. Whatever the case might be for the anomalous traffic, NetFlow can detect it, and the ISE Profiler can take additional action because of it.

## Commonly Used NetFlow Attributes

Cisco NetFlow offers a multitude of field types, called attributes by ISE. However, only a handful are commonly used for developing ISE device profiles. Here is a list and description of the most favored ISE NetFlow attributes:

- **IPv4\_SRC\_ADDR:** Source IP address of the flow
- **IPv4\_DST\_ADDR:** Destination IP address of the flow
- **L4\_SRC\_PORT:** TCP/UDP source port
- **L4\_DST\_PORT:** TCP/UDP destination port
- **DIRECTION:** Flow direction (0 - ingress flow, 1 - egress flow)

## Example Profiler Policy Using NetFlow

Typically, NetFlow attributes would be used with other ISE probe data, such as OUI and DHCP rules. [Figure 21-8](#) depicts a sample profiler policy that is just pure NetFlow rules.

Profiler Policy List > Door-Entry-Pad

### Profiler Policy

\* Name: Door-Entry-Pad      Description: door security entry swipe pad

Policy Enabled:

\* Minimum Certainty Factor: 1,000 (Valid Range 1 to 65535)

\* Exception Action: NONE

\* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy:  Yes, create matching Identity Group  
 No, use existing Identity Group hierarchy

\* Parent Policy: NONE

\* Associated CoA Type: Global Settings

System Type: Administrator Created

**Rules**

If Condition	NETFLOW_IPV4_SRC_ADDR_CONTAINS_1...	Then	Certainty Factor Increases	1000
			AND	
Condition Name	Expression			
NETFLOW:IPV4_SRC	CONTAINS	192.168.45	AND	
NETFLOW:IPV4_DST	EQUALS	192.168.45.10	AND	
NETFLOW:L4_DST_P	EQUALS	443		

**Figure 21-8** NetFlow-Based Profiler Policy

The policy shown in [Figure 21-8](#) has one rule, but that rule is made up of three conditions that all must be true, as indicated by the AND operator between them:

- IPv4 source address contains 192.168.45. This effectively means the SRC addr needs to be in the 192.168.45.0/21 subnet.
- IPv4 destination address must be 192.168.45.10. The source must be talking to this destination.
- Layer 4 destination UDP/TCP port must equal 443.

Also notice that the policy does not use defined conditions but instead creates new conditions within the policy itself. To create new conditions, click the **Create New Condition** button, as show in [Figure 21-9](#).

Profiler Policy List > New Profiler Policy

### Profiler Policy

* Name	heart-pump	Description
Policy Enabled	<input checked="" type="checkbox"/>	
* Minimum Certainty Factor	1,000	(Valid Range 1 to 65535)
* Exception Action	NONE	
* Network Scan (NMAP) Action	NONE	
Create an Identity Group for the policy	<input checked="" type="radio"/> Yes, create matching Identity Group <input type="radio"/> No, use existing Identity Group hierarchy	
* Parent Policy	NONE	
* Associated CoA Type	Global Settings	
System Type		
<b>Rules</b>		
If Condition	Conditions	Then Certainty Factor Increases 10
<input type="button" value="Submit"/> <input type="button" value="Cancel"/> <input type="button" value="Select Existing Condition from Library"/> or <input type="button" value="Create New Condition (Advance Option)"/>		

**Figure 21-9** NetFlow-Based Profiler Policy: Creating New Conditions

## Designing for Efficient Collection of NetFlow Data

As stated earlier, the collection of NetFlow data, if not done properly, can saturate ISE, causing a sort of denial-of-service condition. By using some best practices, you can alleviate much of that risk. Consider the following best practices in your deployment:

- Export an IP flow only once and from a single direction (ingress or egress) to ISE profiler.
- Use a dedicated ISE network interface for NetFlow collection. It will have its own IP address.
- Export flows to ISE only from parts of the network that are needed in ISE device profile policies.
- Position your PSNs as close to the NetFlow collectors as is practical. Avoid collection over a long-distance or low-speed WAN link.
- Use flexible NetFlow to reduce the amount of data that is exported to the ISE PSN profiler.
- Implement a third-party NetFlow collector and forwarder that allows you to filter the exported NetFlow data to the bare minimum required for your ISE NetFlow

policies.

- Regularly monitor the health of your PSNs to ensure that NetFlow is not causing a problem.

## Configuration of NetFlow on Cisco Devices

There are many ways to configure NetFlow on the various Cisco devices. This section focuses on the best practices and tips for configuring NetFlow to work properly with ISE. There are four steps to configuring flexible NetFlow v9 on a Cisco device:

**Step 1.** Create customized flow records. These records define which attributes you want to store for the flow. Keep these to the minimum needed for your profiler policies.

**Step 2.** Configure a flow exporter. The exporter destination is the closest ISE PSN running the Profiler. Remember to export to a dedicated IP/interface on the ISE PSN. This interface is created using the ISE CLI.

**Step 3.** Configure a flow monitor. A flow monitor defines the records, exporters, and cache to use. The flow monitor is assigned to interfaces for flow collection.

**Step 4.** Apply a flow monitor to one or more interfaces. This starts the flexible NetFlow process. You're done!

[Example 21-1](#) through 21-4 outline some of the best practice configurations for each step.

### Example 21-1 Flexible NetFlow Record Configuration

[Click here to view code image](#)

```
flow record ise-flows
description export only flows needed by ise
match datalink mac source-address
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport tcp flags
Cswitch# show flow record
flow record ise-flows:
  Description:          export only flows needed by ise
  No. of users:         0
  Total field space:   20 bytes
  Fields:
    match datalink mac source-address
    match ipv4 protocol
      match ipv4 source address
      match ipv4 destination address
      match transport source-port
      match transport destination-port
      match transport tcp flags
```

## Example 21-2 Flexible NetFlow Exporter Configuration

[Click here to view code image](#)

```
flow exporter ISE
description Export to ISE PSN1
destination 10.1.103.4
source TenGigabitEthernet1/1/1
transport udp 9996
Cswitch# show flow exporter
Flow Exporter ISE:
  Description:          Export to ISE PSN1
  Export protocol:      NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.1.103.4
    Source IP address:      10.1.48.2
    Source Interface:       TenGigabitEthernet1/1/1
    Transport Protocol:     UDP
    Destination Port:       9996
    Source Port:            49736
    DSCP:                  0x0
    TTL:                   255
    Output Features:        Not Used
```

### Example 21-3 Flexible NetFlow Monitor Configuration

[Click here to view code image](#)

```
flow monitor ISE-Flows
description Used for ISE Profiler
record ise-flows
exporter ISE
cache timeout active 60
```

```
Cswitch# show flow monitor
```

Flow Monitor ISE-Flows:

```
Description:      Used for ISE Profiler
Flow Record:    ise-flows
Flow Exporter:   ISE
```

Cache:

```
Type:          normal
Status:        not allocated
Size:          128 entries / 0 bytes
```

Cache:

```
Type:          normal (Platform cache)
Status:        not allocated
Size:          Unknown
```

Timers:

	Local	Global
Inactive Timeout:	15 secs	
Active Timeout:	60 secs	1800 secs
Update Timeout:	1800 secs	

## Example 21-4 Flexible NetFlow Interface Configuration

[Click here to view code image](#)

```
interface TenGigabitEthernet1/1/1
description Cat6K Ten1/5
no switchport
ip flow monitor ISE-Flows input
ip address 10.1.48.2 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP
load-interval 60
```

```
Cswitch# show flow interface tel/1/1
Interface TenGigabitEthernet1/1/1
  FNF:  monitor:          ISE-Flows
        direction:         Input
        traffic(ip):      on
```

## Profiler CoA and Exceptions

If you want the ISE Profiler to take a more proactive action based on a device profile rule match or network activity, use the Profiler Change of Authorization (CoA) and exception rules. By default, the Profiler is passive and doesn't perform CoA actions. You may want to change this default behavior globally and/or based on certain profiler conditions and exceptions. A profiler policy-based CoA action overrides the global CoA settings for the Profiler.

Here are some of the conditions for which the ISE Profiler issues a CoA request to a NAD:

- An endpoint is deleted from the Endpoints page.
- A profile policy exception is triggered.
- An endpoint is profiled for the first time.
- There is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:
  - The endpoint identity group changes for endpoints when they are dynamically profiled.
  - The endpoint identity group changes when the static assignment flag is set to true for a dynamic endpoint.

- An endpoint profiler policy has changed, and the policy is used in an authorization policy.
- A profiler policy triggers a re-authentication based on anomalous device behavior.
- A device changes to a new profile that would result in a change to the endpoint's access rights. These access rights are defined in the authorization policies that use device identity groups.

It is also important to know which conditions do not produce a CoA event. Here are many of them:

- An endpoint disconnects from the network.
- A wired endpoint that is EAP capable connects to the network. For example, an 802.1X supplicant-enabled client.
- Multiple hosts are connected to a single port. A CoA with reauthorization will be issued even if you have configured port bounce (as described in the following section).
- For wireless clients, a packet-of-disconnect is sent to the WLC instead of a port bounce.
- CoA is disabled for any device going through the Guest Device Registration portal/flow.
- If the global profiler CoA setting in ISE is set to No CoA, all profiler policy CoA actions are ignored. In effect, a global No CoA setting disables the ability of ISE profiler to issue any CoA.

## Types of CoA

There are three types of CoA:

- No CoA (default)
- Port Bounce
- Reauth

To use CoA inside the Profiler, you have to enable it globally. Go to **Administration > System > Settings > Profiling**. In most cases, you will select the Reauth option, as shown in [Figure 21-10](#). Best practice is to use Port Bounce for non-802.1X endpoints and Reauth for 802.1X endpoints.

**Profiler Configuration**

\* CoA Type:

Current custom SNMP community strings:

Change custom SNMP community strings:

Confirm changed custom SNMP community strings:

EndPoint Attribute Filter:  Enabled (i)

Enable Anomalous Behaviour Detection:  Enabled (i)

Enable Anomalous Behaviour Enforcement:  Enabled

**Figure 21-10** Global Profiler CoA Setting

## Creating Exception Actions

A custom exception action does two things:

- Forces a CoA or prevents a CoA from happening
- Statically assigns the device to a profiler policy

To create an exception action, go to **Policy > Policy Elements > Results > Profiling > Exception Actions**. The CoA option either forces a CoA if checked or prevents a CoA if unchecked. See [Figure 21-11](#) for an example.

Profiler Exception Action List > [New Profiler Exception Action](#)

**Profiler Exception Action**

\* Name  Description

COA Action  Force COA

\* Policy Assignment

System Type Administrator Created

**Figure 21-11** Exception Action

The action shown in [Figure 21-11](#) forces a CoA and assigns the Unknown profile to the device.

## Configuring CoA and Exceptions in Profiler Policies

After you have created a few exception actions, you can use them in your profiler

policies. It is also in the profile policy that you can change the CoA action from the global default. Changing the CoA action, known as the Associated CoA Type in the GUI, is trivial. As shown in [Figure 21-12](#), use the Associated CoA Type drop-down list to select the type you want to use for this profiler profile.

Profiler Policy List > Door-Entry-Pad

**Profiler Policy**

\* Name: Door-Entry-Pad      Description: door security entry swipe pad

Policy Enabled:

\* Minimum Certainty Factor: 1,000 (Valid Range 1 to 65535)

\* Exception Action: Force\_COA\_Unknown

\* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy:  Yes, create matching Identity Group  
 No, use existing Identity Group hierarchy

\* Parent Policy: NONE

\* Associated CoA Type: Port Bounce

System Type: No CoA  
 Port Bounce  
 Reauth  
 Global Settings

Rules

If Condition: NETFLOW\_IPV4\_SRC\_ADDR\_CONTAINS\_1... Then: Certainty Factor Increases 1000

Save    Reset

**Figure 21-12 Per-Profiler Policy CoA Action**

To configure an exception rule, you need to define which condition triggers an exception action. In [Figure 21-13](#), the exception condition defined is this: If device communicates with any IP destination address except for 192.168.45.10, then issue the exception action.

Profiler Policy List > Door-Entry-Pad

**Profiler Policy**

\* Name: Door-Entry-Pad      Description: door security entry swipe pad

Policy Enabled:

\* Minimum Certainty Factor: 1,000 (Valid Range 1 to 65535)

\* Exception Action: Force\_COA\_Unknown

\* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy:  Yes, create matching Identity Group  
 No, use existing Identity Group hierarchy

\* Parent Policy: NONE

\* Associated CoA Type: Port Bounce

System Type: Administrator Created

Rules

If Condition: NETFLOW\_IPV4\_SRC\_ADDR\_CONTAINS\_1... Then: Certainty Factor Increases 1000

If Condition: NETFLOW\_IPV4\_DST\_ADDR\_NOTEQUALS\_... Then: Take Exception Action

Condition Name	Expression
NETFLOW:IPV4_DST	NOTEQUALS 192.168.45.10

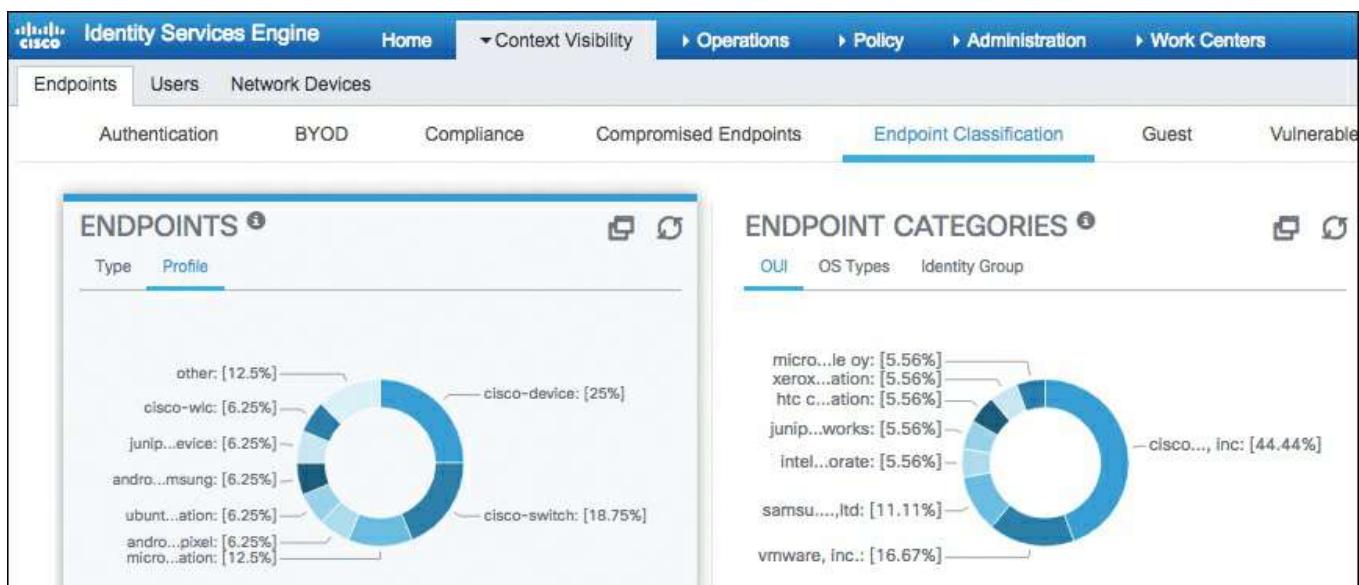
Save    Reset

**Figure 21-13** Exception Profiler Policy Rule

## Profiler Monitoring and Reporting

Cisco ISE includes several reports that deal specifically with the Profiler function. These reports can be used to audit which devices are on your network, provide you with a device inventory, help you troubleshoot Profiler issues, and so on. This section covers the most useful reports and monitoring tools available in ISE.

The first place you can quickly see Profiler results is Context Visibility > Endpoints > Endpoint Classification. [Figure 21-14](#) shows a snippet of the dashboard.



**Figure 21-14** Endpoint Classification Dashboard

This dashboard provides you with a live snapshot of the profiled endpoints on the network and a detailed view of profiled endpoints.

A useful troubleshooting tool for device profiling is the Live Log screen, shown in [Figure 21-15](#). You can find it by choosing **Operations > RADIUS Livelog**.

Status	Details	Identity	Endpoint ID	Endpoint Profile	Authentication Policy
x		Identity	Endpoint ID	Endpoint Profile	Authentication Policy
✓	radius-test				ATS >> Default >> Default
✓	radius-test				ATS >> Default >> Default
✓	radius-test				ATS >> Default >> Default
●	student1	A8:06:00:C5:9C:1D	Android-Samsung-Galaxy...	Android-Samsung-Galaxy...	ATS >> Dot1X >> Default
✓	student1	A8:06:00:C5:9C:1D	Android-Samsung-Galaxy...	Android-Samsung-Galaxy...	ATS >> Dot1X >> Default

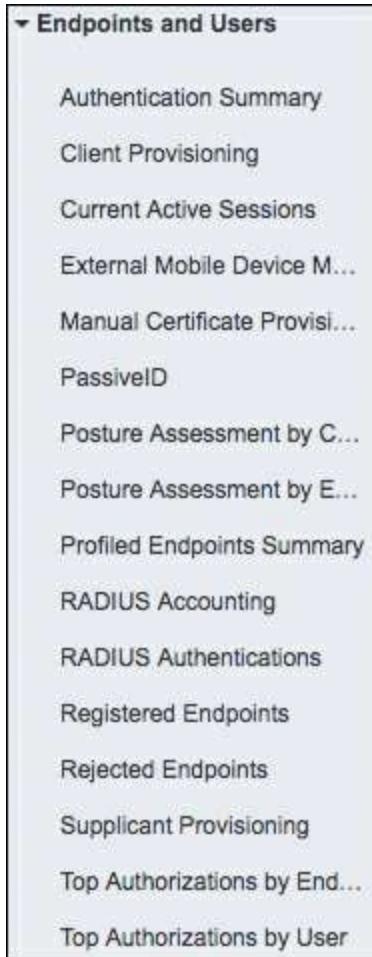
**Figure 21-15** Live Log Screen

The Endpoint Profile column shows the profile group that the device matched. This value doesn't necessarily match the exact profile policy that was a match. It shows the closest identity group that is part of the profile policy hierarchy. To see the actual match profile for the device, click the **Details** icon in the row of the device. This opens the Details screen. As shown in [Figure 21-16](#), if you scroll down you see the EndPoint Matched Policy attribute with a value. This value shows the exact profile policy matched.

Profiler Detail	
Logged At	2017-02-04 21:47:45.041
Server	atw-lse231
Endpoint MacAddress	D0:87:E2:12:B2:04
Day	
Endpoint Static Assignment	SNMPQuery Probe
Endpoint OUI	Samsung Electronics Co.,Ltd
Matched Rule	
Certainty Metric	70
Endpoint Matched Policy	Android-Samsung
Matched Rule	
Endpoint Identity Group	Android
Event	Profiler EndPoint profiling event occurred
Profiler History	
Day	Endpoint Profile
2017-02-04 21:47:45.041	Android-Samsung
2017-02-04 09:46:26.776	Android-Samsung

**Figure 21-16** Live Auth Details

Under **Operations > Reports > Endpoints and Users** , you see several profiler reports. [Figure 21-17](#) shows a list of them.



**Figure 21-17 Profiler Reports**

Two of the most helpful reports are

- **Posture Assessment by Condition:** This report shows endpoints that have changed from one profile match to a different profile match.
- **Profiled Endpoints Summary Report:** Clicking Details next to a device provides you all sorts of useful information for reporting and troubleshooting the Profiler. This screen also shows you the profile history of a particular device over time, as shown in [Figure 21-18](#).

Profiler Detail	
Logged At	2017-02-04 21:47:45.041
Server	atw-lse231
Endpoint MacAddress	D0:87:E2:12:B2:04
Day	
Endpoint Static Assignment	SNMPQuery Probe
Endpoint OUI	Samsung Electronics Co.,Ltd
Matched Rule	
Certainty Metric	70
Endpoint Matched Policy	Android-Samsung
Matched Rule	
Endpoint Identity Group	Android
Event	Profiler EndPoint profiling event occurred
Profiler History	
Day	Endpoint Profile
2017-02-04 21:47:45.041	Android-Samsung
2017-02-04 09:46:26 776	Android-Samsung

**Figure 21-18 Profiler History**

## Summary

This chapter covered several advanced profiler concepts, configurations, and best practices. These included creating custom profiles, advanced NetFlow, Change of Authorization (CoA), profiler exceptions, and profiler monitoring and reports. This chapter discussed that, when implemented correctly, NetFlow can be used as an effective profiler probe. It also discussed how to create your own custom and complex profile conditions and policies. Using the skills presented in this chapter, you will be able to correctly identify all of the devices on your network. As mentioned in the chapter introduction, the ISE Visibility Setup Wizard enables you to set up the Profiler very quickly. See [Chapter 10](#) for details.

# Chapter 22 Cisco TrustSec AKA Security Group Access

This chapter covers the following topics:

- Ingress access control challenges
- What Is TrustSec?
- Transport: Security Group Tag (SGT) eXchange Protocol (SXP)
- Transport: Platform eXchange Grid (pxGrid)
- Transport: native tagging
- Enforcement

Throughout this book, you have been exposed to many different ways of controlling network access based on the context of a user and device. There is VLAN assignment, in which Layer 2 segments are created and access is controlled at the Layer 3 edge, or by isolating that VLAN into a segmented virtual network (VRF). Additionally, there is ACL assignment, which can be a local ACL, called into action by a RADIUS attribute, or a downloadable ACL (dACL). These ACLs are applied ingress at the switch port or virtual port in the case of the Wireless LAN Controller (WLC).

These are all good access control methods, but regulating passage only at the point of network ingress can leave room for a more desirable and scalable solution. This chapter discusses one such Cisco enhancement to make access control more scalable and powerful: TrustSec (formerly known as Security Group Access [SGA]).

With TrustSec, controls are defined simply using endpoint roles, not IP addresses. By classifying systems using human-friendly logical groups, security rules can be defined using these groups, which are more flexible and much easier to manage than using IP address-based controls.

IP addresses do not indicate the role of a system, the type of application a server hosts, the purpose of an Internet of Things (IoT) device, or the threat state of a system, but a TrustSec security group can denote any of these roles. These security groups can be used to simplify firewall rules, web security appliance policies, and the access control lists (ACL) used in switches, WLAN controllers, and routers.

## Ingress Access Control Challenges

VLAN assignment and dACLs are fantastic and classic ways of controlling access to a network; however, when a network grows, so do the challenges of keeping up with the ingress access controls. Let's look at each one of these standard use cases individually and discuss the challenges.

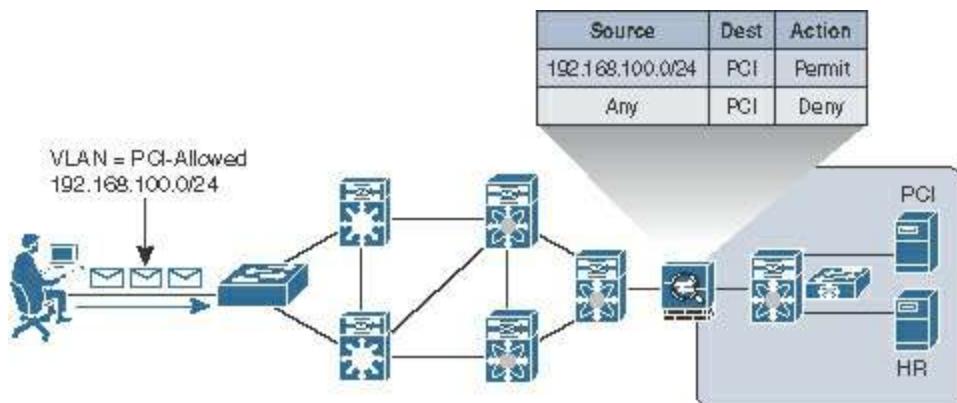
## VLAN Assignment

VLAN assignment based on the context of a user or device is a common way to control access to the network. Let's use a hypothetical scenario of controlling access to servers that contain credit-card data, which falls under Payment Card Industry Data Security Standard (PCI DSS) compliance.

1. A user is a member of the Retail-Managers group in Active Directory.
2. The posture of the system is compliant.
3. Therefore, ISE assigns the user into the PCI-Allowed VLAN on the switch or WLC.

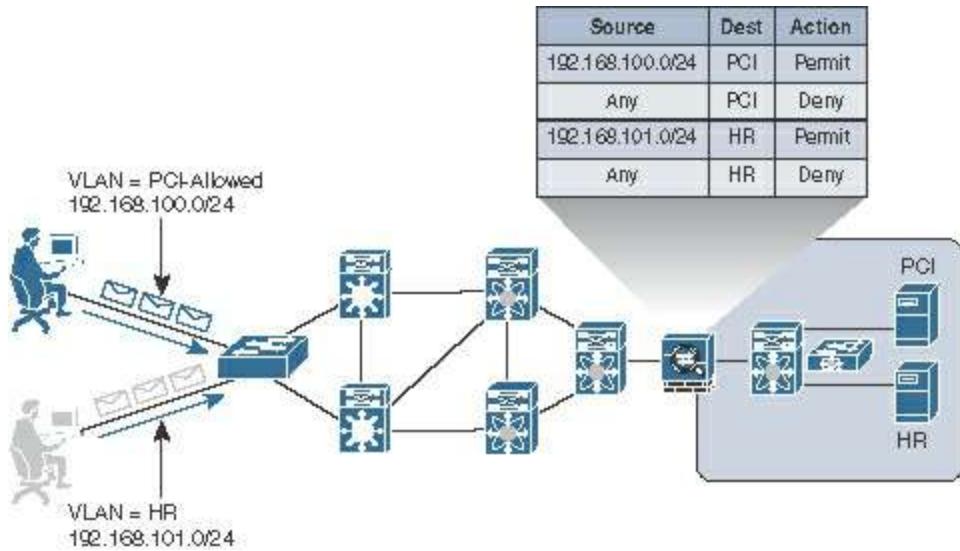
Now, to use that VLAN assignment to control access to the servers that house that PCI data, an ACL must be applied somewhere. Let's assume the ACL is applied at a firewall between the campus/branch networks and the data center.

4. The ACL on the data center firewall must be updated to include the entire source IP address range of PCI-Allowed VLANs throughout the entire network infrastructure, as shown in [Figure 22-1](#).



**Figure 22-1** Controlling Access with VLANs on Single Switch

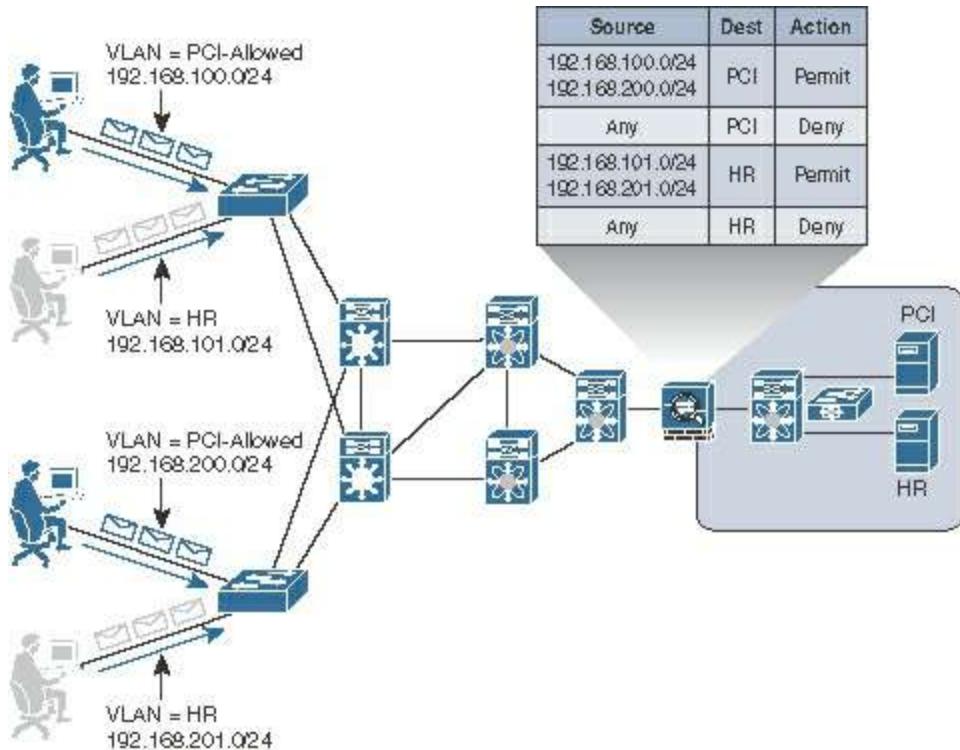
Next, the company decided to control access to the HR server, so that only members of the HR department may talk to HR servers. Another set of rules must be built that assign the HR VLAN, and another set of entries in the access list, as shown in [Figure 22-2](#).



**Figure 22-2** Controlling Access with Two VLANs on Single Switch

Now, consider how this can scale as you continue to add VLANs and switches and WLCs to the equation. One of your large customers has over 50,000 switches in its access layer. That is a tremendous number of VLANs to create and addresses to maintain in an access list on a firewall. That same customer has 15 full-time employees managing the firewall rules. This customer needs to find some better mechanism to control access that would lower its operating expense (OPEX) tremendously.

What if you had 100 remote sites? That is 100 new IP subnets, which can easily modify your existing route summarization strategy. When that is the case, the route summarization alone can cause a network redesign, which will add even more operational cost, as shown in [Figure 22-3](#).



**Figure 22-3 VLAN Control Can Be Operationally Expensive**

There is a formula to determine the number of access control entries (ACE) in an access control list (ACL). The formula takes the number of sources multiplied by the number of destinations multiplied by the permissions of the ACL:

$$(\# \text{ of sources}) \times (\# \text{ of destinations}) \times \text{permissions} = \# \text{ of ACEs}$$

With the environment depicted in [Figure 22-3](#), with only 4 sources  $\times$  2 destinations  $\times$  4 permissions, you would need 32 ACEs. We often refer to this as ACE explosion. This is obviously just a small example. This is examined more in the following sections.

## Ingress Access Control Lists

Another way to control access is to use ACLs applied at ingress (inbound) at the port (or virtual port) that the user or device is using to access the network. This could be locally defined ACLs that are called by using the filter-ID RADIUS attribute, or they could be dACLs, where the entire ACL is defined on ISE and downloaded to the port.

Obviously, dACLs provide a better operational model, because there is only one place to update an ACL when a change needs to be made. Additionally, the number of ACEs required is lower when applying the ACL to a switch port than it would be to apply the ACL to a centralized location. Because the ACL is being applied at the point of ingress, there would only be a single source IP address (theoretically). Cisco switches perform source substitution on these ACLs to make it even easier. With source substitution, the **any** keyword in the source field of an ACL is replaced with the actual IP address of the host on the switch port.

Using the same formula for six destinations and four permissions, you would have

$$1 \text{ source} \times 6 \text{ destinations} \times 4 \text{ permissions} = 24 \text{ ACEs}$$

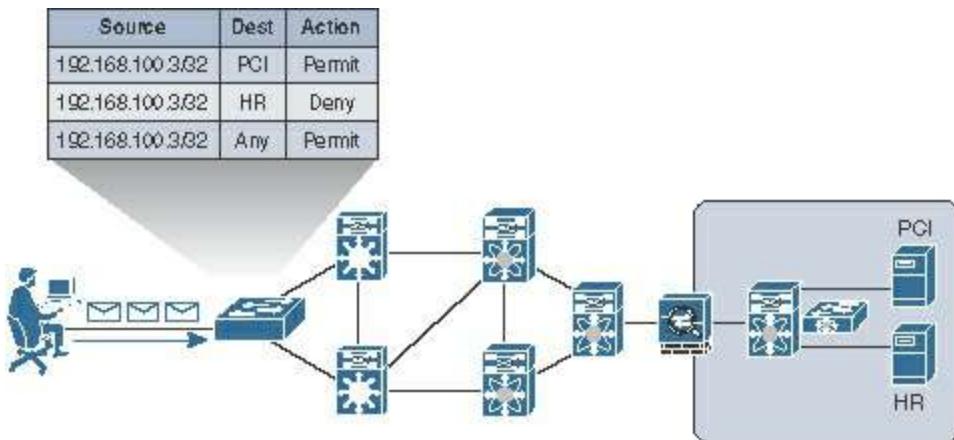
However, there are a few complications with using ACLs on access layer devices. Two major drawbacks that exist are the regular maintenance of the ACLs and the size of the ACLs.

If ACLs are being used to explicitly defend hosts, they must be updated regularly for all new destinations that get added to the network. This can cause an exorbitant amount of OPEX maintaining the lists and ensuring they get updated correctly. Additionally, there is a limited number of ACEs that a switch will be able to apply.

ACLs get loaded into and executed from Ternary Content Addressable Memory (TCAM). Access layer switches have a limited amount of TCAM, which is usually assigned per ASIC. Therefore, the number of ACEs that can be loaded depends on various factors, such as the number of hosts per ASIC and the amount of free TCAM space.

Because of that limited amount of TCAM, ACLs cannot be overly large, especially when the access layer may be a mixture of different switches, each switch having a different level of TCAM per ASIC. The best practice recommendation is to keep the ACEs less than 64 per dACL. This may need to be adjusted for your specific environment, but it is a good place to start.

[Figure 22-4](#) shows ingress ACLs in the network.



**Figure 22-4** Ingress ACLs

## What Is TrustSec?

TrustSec is a next-generation access control enforcement that was created to address the growing operational expenses with maintaining firewall rules and ACLs. TrustSec is a complementary enforcement technology that removes the concerns of TCAM space and ACE explosion.

The ultimate goal of TrustSec is to assign a tag (known as a Security Group Tag, or

SGT) to the user/device's traffic at ingress (inbound into the network), and then enforce the access elsewhere in the infrastructure (in the data center, for example). So, TrustSec assigns an SGT at login and enforces that SGT elsewhere in the network (egress enforcement).

The SGT should be representative of some overarching roles within the company. For instance, an SGT may be assigned to a GUEST user, so that GUEST traffic may be isolated from non-GUEST traffic throughout the infrastructure. Here is a list of some common security groups:

- **Network Infrastructure:** This SGT gets assigned to all the switches, routers, WLCs, and firewalls within the organization.
- **Network Services:** This SGT is assigned to the servers providing common services that most everyone should be able to reach (DNS, DHCP, NTP, and so on).
- **Executive:** Many organizations may classify their executives into their own SGT, simply to ensure that executives will never be denied access to anything.
- **Sales:** This SGT would signify a member of the sales organization.
- **Finance:** This SGT would signify a member of the finance organization.
- **HR:** Used to signify a member of the Human Resources department.
- **Line-of-Business-1:** SGTs are used often when an umbrella company has many different lines of business, and those lines of business cannot have access to each other's data.
- **Line-of-Business-2:** See previous.

The trick with SGTs is to use them for bulk access control, and do your fine-grain access control within the application security itself. Additionally, each end user or end device may only be assigned a single SGT. You do not want to create too many roles, or you will spend too much operational time mapping users to the correct tags.

## So, What Is a Security Group Tag?

A Security Group Tag (SGT) is a 16-bit value that ISE assigns to the user's or endpoint's session upon login. The network infrastructure views the SGT as another attribute to assign to the session, and inserts the Layer 2 tag into all traffic from that session. The SGT can represent the context of the user and device. Let's look at an example.

This is one of our favorite examples from a client that we worked with directly. It is a retail organization, and therefore, it accepts credit cards from customers, which places it under the domain of PCI DSS compliance. Access to any server housing credit-card data must be protected as strictly as any technology will allow.

In this client's case, we defined a rule in ISE that looked for machine and user authentication (EAP chaining) and verified the user was a member of a PCI group in Active Directory and the machine's posture was compliant. If the user and machine met all these conditions, an SGT named PCI was assigned. No access was granted to PCI servers without the PCI SGT.

So, as you can see, SGTs can be applied based on the full context of the authentication or simply based on a single condition, such as Guest.

**Note** The endpoint itself is not aware of the SGT. It is known in the network infrastructure. [Figure 22-5](#) illustrates the SGT being assigned to an authentication session.

```
C3750X#sho authentication 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: xACSAACLx-IP-Employee-ACL-
  SGT: 0002-0 ←
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A01300200000022DC6C328F
  Acct Session ID: 0x00000033
  Handle: 0xCC000022

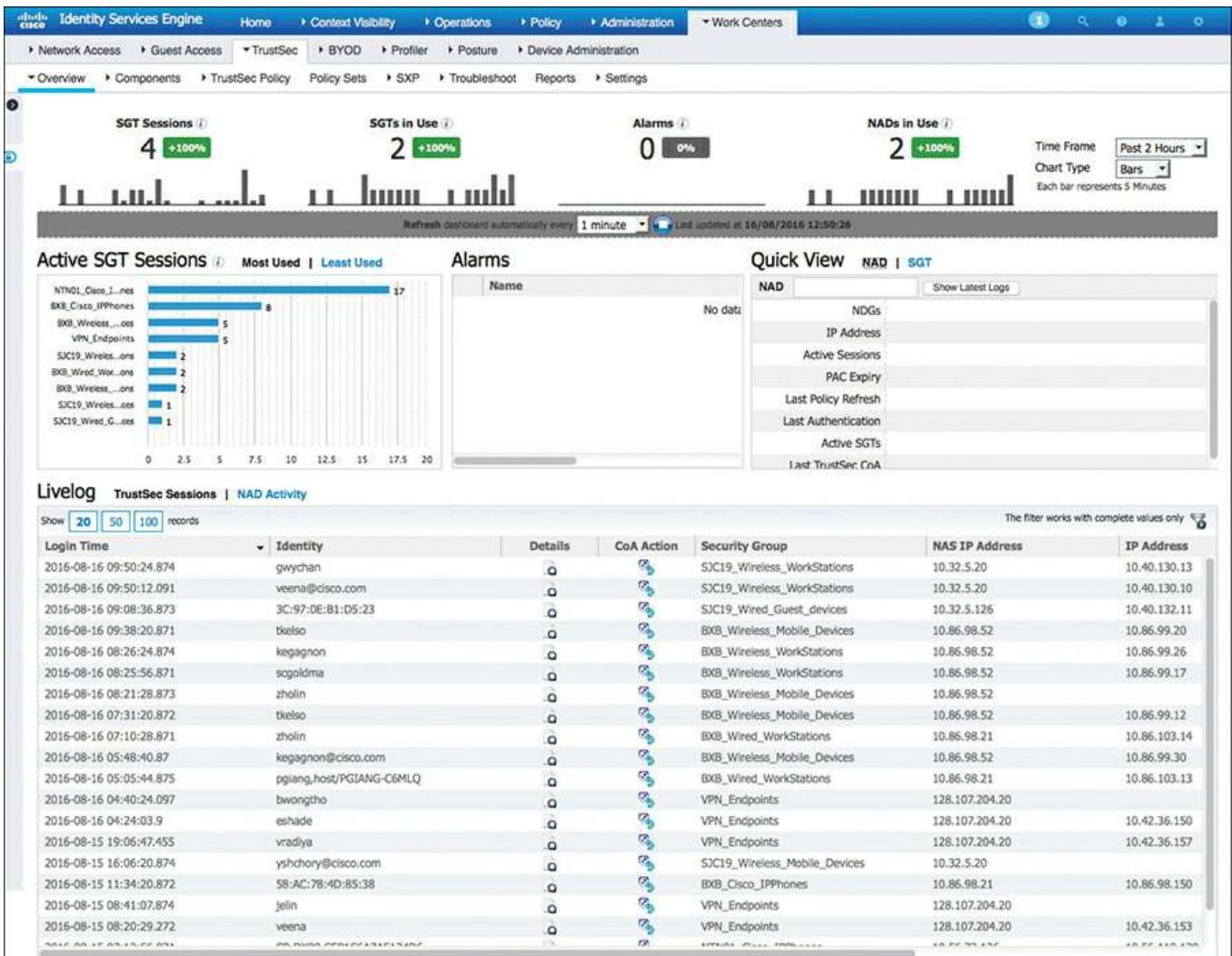
  Runnable methods list:
    Method      State
      dot1x     Authc Success
```

**Figure 22-5** SGT Applied to Session

## Defining the SGTs

One could say that ISE wears many hats. ISE serves as a TrustSec controller of sorts. In fact, there is even a dedicated TrustSec Work Center in ISE, and ISE can accurately be viewed as the single source of truth for what SGTs exist.

To view the TrustSec Work Center, navigate to **Work Centers > TrustSec**. [Figure 22-6](#) shows an example TrustSec dashboard within the Work Center.



**Figure 22-6** TrustSec Dashboard

ISE considers an SGT a policy result. Therefore, create one SGT result for each SGT you want to define in the environment. To help customers understand usages of SGTS, ISE also comes with a large number of preexisting SGTS with assigned icons, as shown in [Figure 22-7](#).

Security Groups				
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page				
	Icon	Name	▲ SGT (Dec / Hex)	Description
<input type="checkbox"/>		Auditors	9/0009	Auditor Security Group
<input type="checkbox"/>		BYOD	15/000F	BYOD Security Group
<input type="checkbox"/>		Contractors	5/0005	Contractor Security Group
<input type="checkbox"/>		Developers	8/0008	Developer Security Group
<input type="checkbox"/>		Development_Servers	12/000C	Development Servers Security Group
<input type="checkbox"/>		Employees	4/0004	Employee Security Group
<input type="checkbox"/>		Guests	6/0006	Guest Security Group
<input type="checkbox"/>		Network_Services	3/0003	Network Services Security Group
<input type="checkbox"/>		PCI_Servers	14/000E	PCI Servers Security Group
<input type="checkbox"/>		Point_of_Sale_Systems	10/000A	Point of Sale Security Group
<input type="checkbox"/>		Production_Servers	11/000B	Production Servers Security Group
<input type="checkbox"/>		Production_Users	7/0007	Production User Security Group
<input type="checkbox"/>		Quarantined_Systems	255/00FF	Quarantine Security Group
<input type="checkbox"/>		Test_Servers	13/000D	Test Servers Security Group
<input type="checkbox"/>		TrustSec_Devices	2/0002	TrustSec Devices Security Group
<input type="checkbox"/>		Unknown	0/0000	Unknown Security Group

**Figure 22-7 Security Groups**

To view the preexisting SGTs or to create new ones within the ISE GUI, navigate to **Work Centers > TrustSec > Components > Security Groups**.

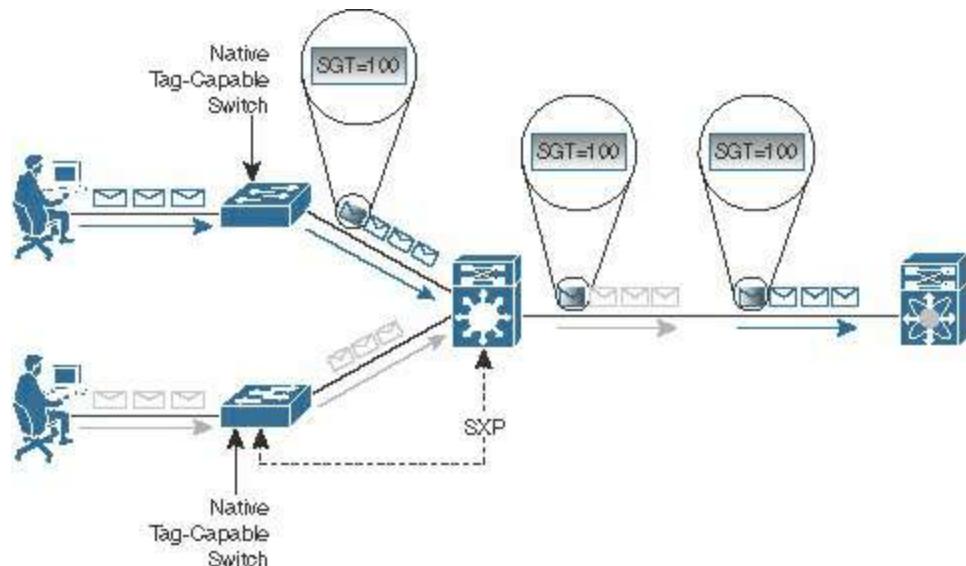
Notice in the last row of [Figure 22-7](#) the default SGT of 0, Unknown. This SGT will be used if traffic arrives that is untagged. In other words, even the lack of an SGT can be used in the security policy.

## Classification

This should not come as a surprise to you, but to use SGTs within your infrastructure, your devices should support SGTs. All supported Cisco switches and wireless controllers do support the assignment of the SGT. This is defined as classification. The process of communicating that assigned SGT upstream into the network can either occur via native tagging or via a peering protocol, and this process is defined as transport.

[Figure 22-8](#) shows an example of one access switch that has native tagging, and the packets get tagged on the uplink port and through the infrastructure. It also shows a non-native-tagging capable switch, which uses a peering protocol to update the upstream switch. In both cases, the upstream switch continues to tag the traffic throughout the

infrastructure.



**Figure 22-8** Security Group Tagging

To use the Security Group Tag, the tag needs to be assigned, which can happen in one of three ways: the SGT can be assigned dynamically, and be downloaded as the result of an ISE authorization; it can be assigned manually at the port level; or it can be mapped to IP addresses and downloaded to SGT-capable devices.

**Note** For network devices that do not support SGT classification, ISE itself may still assign the tag as part of the authorization result. The network session within ISE's session directory will be updated and the IP address-to-SGT mapping may be shared via SXP or pxGrid for enforcement elsewhere.

## Dynamically Assigning an SGT via 802.1X

Assigning an SGT is as simple as adding it as another permission or result of an authorization in an authorization policy. ISE comes with a few preconfigured examples of the TAG assignment, as highlighted in [Figure 22-9](#). You can see these by navigating to **Work Centers > Network Access > Policy Sets > Default > Authorization**. The examples in [Figure 22-9](#) show three different SGTs being assigned: BYOD, Employees, and Guests.

Wireless_Block_List_Default	If Blocklist AND Wireless_Access	then Blackhole_Wireless_Access
Profiled_Cisco_IP_Phones	If Cisco-IP-Phone	then Cisco_IP_Phones
Profiled_Non_Cisco_IP_Phones	If Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
Compliant_Device_Access	If Network_Access_Authentication_Passed AND Compliant_Devices	then PermitAccess
Emp_TLS_MDM_OnBoard	If Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_In_SAN AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:MDMServerReachable EQUALS Reachable AND MDM:MDMServerReachable EQUALS Reachable	then MerakiOnboard AND BYOD
Emp_TLS_MDM_Compliant	If Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_In_SAN AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:MDMServerReachable EQUALS Reachable AND MDM:DeviceCompliantStatus EQUALS Compliant	then PermitAccess AND BYOD
EAP_Chaining	If Network_Access_EapChainingResult EQUALS User and machine both succeeded AND AD-SecurityDemo-ExternalGroups EQUALS securitydemo.net/Users/Employee	then PermitAccess AND Employee
Employee_EAP-TLS	If Wireless_802.1X AND BYOD_Is_Registered AND EAP-TLS AND MAC_In_SAN	then PermitAccess AND BYOD
Employee_Onboarding	If Wireless_802.1X AND EAP-MSCHAPv2	then NSP_Onboard AND BYOD
Wi-Fi_Guest_Access	If Guest_Flow AND Wireless_MAB	then PermitAccess AND Guests
Wi-Fi_Redirect_to_Guest_Login	If Wireless_MAB	then Cisco_WebAuth
Basic_Authenticated_Access	If Network_Access_Authentication_Passed	then PermitAccess
Default	If NO matches, then	DenyAccess

**Figure 22-9 Default Authorization Rules Showing SGT Assignment**

To add a Security Group Tag as an authorization result, perform the following steps:

**Step 1.** Click **Edit** to edit your existing authorization rule.

**Step 2.** Click the + sign under Permissions.

**Step 3.** Click the + sign next to the authorization profile.

**Step 4.** Choose **Security Group**.

**Step 5.** Select the appropriate Security Group to apply.

## Manually Assigning an SGT at the Port

In most cases, 802.1X is not used in the data center. Servers are not usually required to authenticate themselves to the data center switch, as the DC is normally considered physically secure, and there is no network access control applied there. However, the servers themselves will be the destination of traffic coming from the campus and from within the data center itself.

Because 802.1X is not typically used in the data center, you need a manual way to apply the SGT. This is configured at the interface level of the Nexus configuration and is manually applied to the port itself:

[Click here to view code image](#)

```
NX7K-DIST(config)# int eth1/3
NX7K-DIST(config-if)# cts manual
NX7K-DIST(config-if-cts-manual)# policy static sgt 0x3
```

This has manually assigned the SGT 3 to the port on the Nexus 7000. This is also available on the Nexus 5000 and 1000v.

## Manually Binding IP Addresses to SGTs

As an alternative to assigning the SGT to the port itself, ISE added the capability to centrally configure a database of IP addresses and their corresponding SGTs. This is accomplished under **Work Centers > TrustSec > Components > IP SGT Static Mapping**. Then, SGT-capable devices may download that list from ISE, as shown in [Figure 22-10](#) and [Figure 22-11](#).

IP SGT static mapping > New

IP address(es)

Add to a mapping group  
 Map to SGT individually

SGT \*

Send to SXP Domain

Deploy to devices

Cancel Save

**Figure 22-10** Mapping an SGT to an IP Address in ISE

Now that the mappings exist on ISE, you can download them to the other devices, such as a Nexus 7000 data center switch, or even a Cisco Firepower or Check Point firewall. [Figure 22-11](#) shows multiple static mappings in the ISE GUI.

IP address/Host	SGT	Mapping group	Deploy via	Deploy to
10.1.100.253	PCI_Servers (14/000E)		default	All TrustSec Devices
10.1.100.254	TrustSec_Devices (2/0002)		default	All TrustSec Devices

**Figure 22-11** IP SGT Static Mapping

## Access Layer Devices That Do Not Support SGTs

Because it isn't a perfect world, and not all the equipment on the network will be the latest and greatest, you need another way to classify the endpoint traffic. For example, you may still be using an older Cisco Wireless LAN Controller (like the 4400) that does not support version 7.2 or newer code and therefore cannot accept the SGT classification from ISE nor send the update via SXP.

Additionally, this could be a VPN Concentrator, or some third-party equipment that found its way into the deployment. Although that gear may not support the classification and transport natively, you may still use TrustSec in those environments. You can leverage ISE to maintain the list of bindings and share those via SXP or pxGrid; or that network device may be capable of assigning different VLANs or IP addresses per authorization result.

With the Catalyst 6500, you can map subnets and VLANs and assign all source IP addresses from the subnet or VLAN to a specific tag.

### Mapping a Subnet to an SGT

Use the **cts role-based sgt-map [ipv4-subnet | ipv6-subnet] sgt tag-value** command to enable this binding. When used, the device-tracking feature in the Catalyst 6500 Supervisor 2T will be used to identify matches and assign the SGT. Here is an example of this mapping.

```
C6K-DIST(config)# cts role-based sgt-map 192.168.26.0/24 sgt 4
```

### Mapping a VLAN to an SGT

Use the **cts role-based sgt-map vlan-list vlans sgt tag-value** command to enable this binding. When used, the device-tracking feature in the Catalyst 6500 Supervisor 2T will be used to identify matches and assign the SGT. Here is an example of this mapping.

```
C6K-DIST(config)# cts role-based sgt-map vlan-list 40 sgt 4
```

## Transport: SGT eXchange Protocol (SXP)

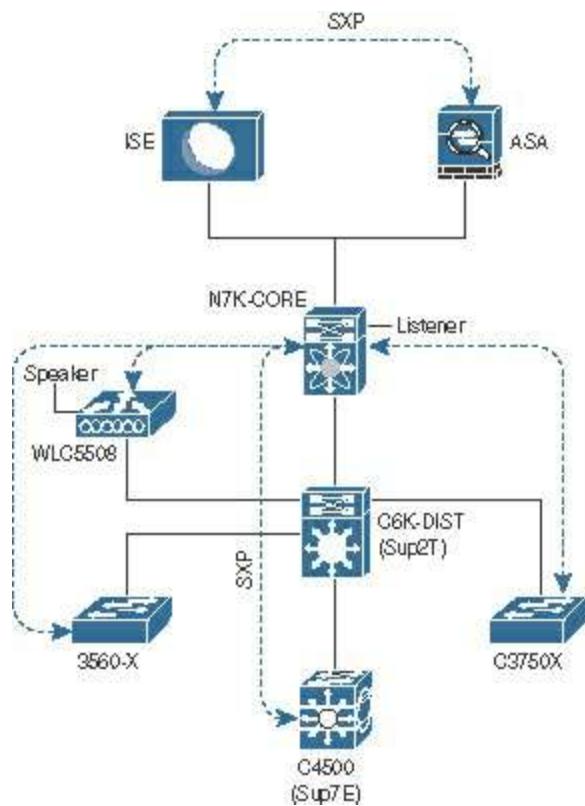
In a perfect world, all of your access layer devices would support tagging the users' traffic natively. Yet in the world we live in, the reality is that not all devices support native tagging.

Cisco developed a peering protocol (similar to Border Gateway Protocol [BGP]) to allow devices to communicate their database of IP-address-to-SGT mappings to one another. This peering protocol is called SGT eXchange Protocol (SXP). Because this is a peering protocol, it is possible to be specific and deterministic as to which devices send updates and which ones receive updates.

An SXP peer may be defined as a speaker or as a listener. The definition of a speaker is a device that sends the IP-address-to-SGT bindings. The definition of a listener is a device that receives the IP-address-to-SGT bindings.

## SXP Design

Because SXP uses TCP as its transport, the peer may be Layer 2 adjacent or multiple hops away. A network device may peer directly to the enforcement device (the data center switch or security group firewall). [Figure 22-12](#) shows a rudimentary design to illustrate the point.

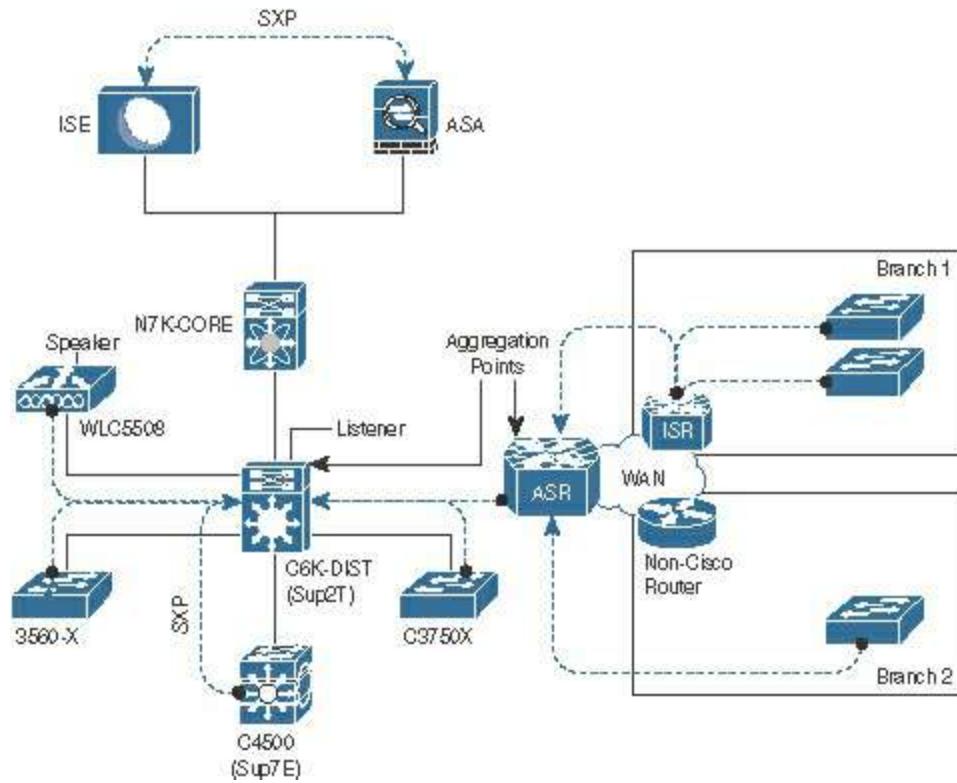


**Figure 22-12** SXP Peering

[Figure 22-12](#) shows some network access switches and a WLC. All of these NADs receive IP-address-to-SGT bindings as part of the user's authorization session. When users authenticate through these NADs, ISE authorizes them and sends back an SGT as part of the result (classification). The NAD in turn acts as an SXP speaker and updates any configured listeners. In [Figure 22-12](#), each NAD is configured to send the updates to the Nexus 7000 in the data center, which is multiple hops away. Additionally, [Figure 22-12](#) illustrates ISE updating a Cisco Adaptive Security Appliance (ASA) of all the bindings via SXP. The ASA could also peer directly to the Nexus 7000, or any of the NADs if that was your chosen design.

Remember that routing protocols have a limitation for the number of neighbors they can scale to, and so does SXP. Because of the limitations of scale for the number of peers,

SXP design may be architected to be multihop, which allows for aggregation points, as shown in [Figure 22-13](#). Devices like the Catalyst 6500 with a Supervisor 2T engine or the Aggregation Services Router (ASR) are solid choices for SXP aggregation.



**Figure 22-13** SXP Multihop

[Figure 22-13](#) shows a design where multiple branch locations may have one or more switches, which aggregate their IP-address-to-SGT bindings at the gateway Integrated Services Router (ISR). Each gateway ISR sends those aggregated bindings to the WAN head-end, represented by an ASR, which in turn aggregates all those branch peers. The ASR sends the aggregated bindings to the Catalyst 6000 for further aggregation with all the other bindings from the campus access layer.

There are numerous benefits to this design. Mainly it provides a deterministic and scalable design; however, it also does not require SXP-aware infrastructure along every hop in the network path, because SXP peers do not need to be directly connected. For example, the switch in Branch 2 of [Figure 22-13](#) bypasses the non-Cisco gateway router and is peering directly to the ASR.

## Configuring SXP on IOS Devices

The following steps walk you through the SXP configuration on Cisco IOS-based devices.

From global configuration mode, perform the following steps:

## **Step 1.** Enter **cts xp enable**.

This turns SXP on globally. Each peer needs to be added individually, and a global default SXP password needs to be set.

## **Step 2.** Enter **cts xp connection peer peer-ip-address password [default | none] mode [local | peer] [listener | speaker]**.

This command is used to define the SXP peer. The options are as follows:

- **password default:** States to use the password defined globally for all SXP connections. At the current time, it is not possible to have different SXP passwords per peer.
- **password none:** Do not use a password with this SXP peer.
- **mode local:** States that the following SXP argument is defining the local side of the connection.
- **mode peer:** States that the following SXP argument is defining the peer's side of the connection.
- **listener:** Defines that the specified device (local or peer) will receive SXP updates through this connection.
- **speaker:** Defines that the specified device (local or peer) will send SXP updates through this connection.

## **Step 3.** (Optional) Enter **cts xp default password** password.

This is an optional step for when your connections will use the globally defined password, instead of no password.

[Example 22-1](#) and [Example 22-2](#) display the steps for setting up the SXP connection between a Catalyst 4500 (access layer device that does not support native tagging) and a Catalyst 6500 with a Supervisor 2T (distribution layer device that supports native tagging) as previously shown in [Figure 22-13](#).

### **Example 22-1** Enabling SXP on the Catalyst 4500

[Click here to view code image](#)

```
4503(config)# cts xp enable
4503(config)#
*Aug  9 06:51:04.000: %CTS-5-SXP_STATE_CHANGE: CTS SXP enabled
4503(config)# cts xp connection peer 10.1.40.1 password default mode
peer listener
4503(config)#
*Aug 10 09:15:15.564: %CTS-6-SXP_TIMER_START: Connection <0.0.0.0,
0.0.0.0> retry open timer started.
*Aug 10 09:15:15.565: %CTS-6-SXP_CONN_STATE_CHG: Connection
<10.1.40.1, 10.1.40.2>-1 state changed from Off to Pending_On.
4503(config)#
*Aug 10 09:15:15.566: %CTS-3-SXP_CONN_STATE_CHG_OFF: Connection
<10.1.40.1, 10.1.40.2>-1 state changed from Pending_On to Off.
4503(config)# cts xp default password TrustSec123
4503(config)#
*Aug 10 09:17:20.936: %CTS-5-SXP_DFT_PASSWORD_CHANGE: CTS SXP password
changed.
```

## Example 22-2 Enabling SXP on the Catalyst 6500

[Click here to view code image](#)

```
C6K-DIST(config)# cts xp enable
C6K-DIST(config)#
Aug 10 16:16:25.719: %CTS-6-SXP_TIMER_START: Connection <0.0.0.0,
0.0.0.0> retry open timer started.
C6K-DIST(config)# cts xp default password TrustSec123
C6K-DIST(config)# cts xp connection peer 10.1.40.2 password default
mode peer speaker
C6K-DIST(config)#
Aug 10 16:17:26.687: %CTS-6-SXP_CONN_STATE_CHG: Connection <10.1.40.2,
10.1.40.1>-1 state changed from Off to Pending_On.
Aug 10 16:17:26.687: %CTS-6-SXP_CONN_STATE_CHG: Connection <10.1.40.2,
10.1.40.1>-1 state changed from Pending_On to On.
```

## Configuring SXP on Wireless LAN Controllers

The Cisco WLC added support for SGT classification and SXP transport in the 7.2 release.

From the WLC user interface, perform the following steps:

**Step 1.** Using the top-menu navigation, select **Security**.

**Step 2.** Along the left side, choose **TrustSec SXP**, as shown in [Figure 22-14](#).

The screenshot shows the Cisco WLC interface with the following details:

- Top Navigation:** MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (highlighted).
- Left Sidebar (Security Category):**
  - AAA
    - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
    - DNS
    - Downloaded AVP
  - TACACS+
    - LDAP
    - Local Net Users
    - MAC Filtering
  - Disabled Clients
    - User Login Policies
    - AP Policies
    - Password Policies
  - Local EAP
    - Advanced EAP
    - Priority Order
    - Certificate
    - Access Control Lists
    - Wireless Protection Policies
    - Web Auth
  - TrustSec SXP (selected)
  - Local Policies
- SXP Configuration Panel:**
  - Total SXP Connections: 1
  - SXP State: Enabled (dropdown menu)
  - SXP Mode: Speaker
  - Default Password: ..... (text input field)
  - Default Source IP: 10.1.60.2
  - Retry Period: 120 (text input field)
- Peer Table:**

Peer IP Address	Source IP Address	Connection Status	Action
10.1.101.254	10.1.60.2	On	▼

**Figure 22-14** SXP Connection on WLC

**Step 3.** From the SXP State drop-down list, choose **Enabled**.

**Step 4.** In the Default Password field, enter the same default password you configured on the switches. All passwords in the SXP domain need to be the same.

This has turned SXP on globally. Each peer must be added individually. To add a new SXP peer (a listener), follow these steps:

**Step 5.** Click **New** (in the upper-right corner).

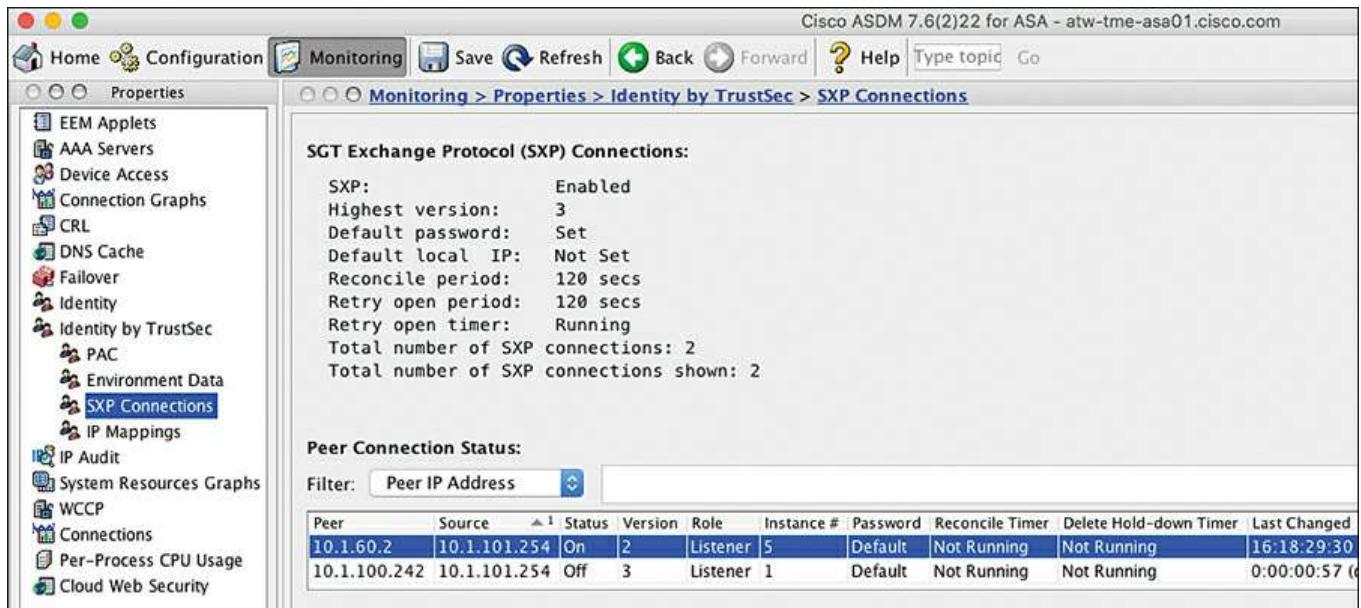
**Step 6.** Enter the IP address of the listener peer.

**Step 7.** Click **Apply** (upper-right corner).

The added peers are displayed on the TrustSec SXP page. Their status is listed next to

their IP address. Once the peer is configured on the other side, the status changes from **Off** to **On**, as shown in [Figure 22-14](#).

It is also possible to verify the SXP connection from the other side, as shown in [Figure 22-15](#) and demonstrated in Example 22-3.



**Figure 22-15** SXP Connections on Cisco ASA

### Example 22-3 Verifying the Connection Between the WLC and Catalyst 6500

[Click here to view code image](#)

```
C6K-DIST# sho cts sxp connections brief
SXP : Enabled
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
-----
-----
Peer_IP      Source_IP      Conn_Status      Duration
-----
10.1.40.2    10.1.40.1     On               4:06:36:24
(dd:hr:mm:sec)
10.1.60.2    10.1.60.1     On               0:00:03:31
(dd:hr:mm:sec)
Total num of SXP Connections = 2
```

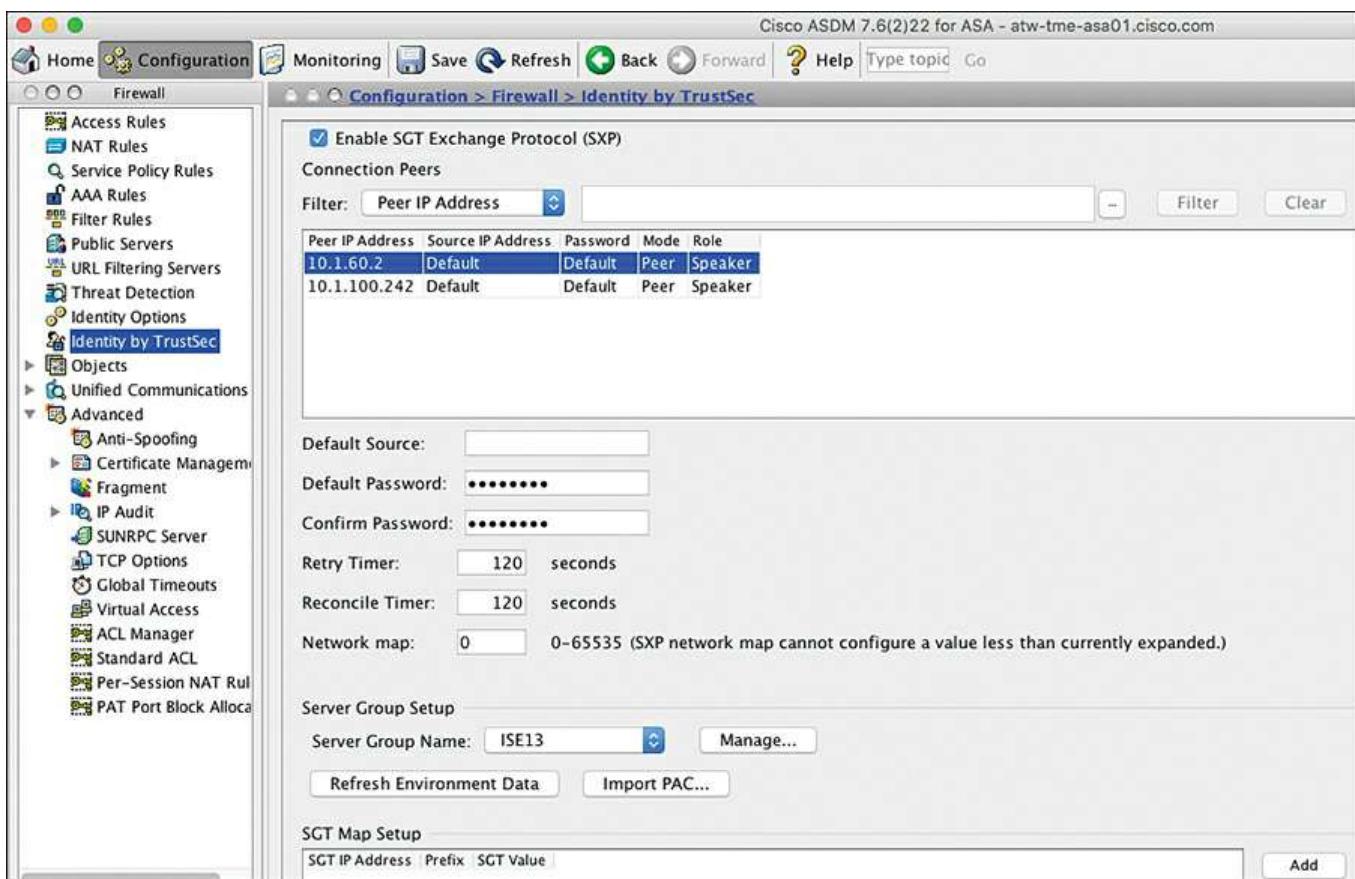
## Configuring SXP on Cisco ASA

Cisco ASA includes support for SGT enforcement (known commonly as SG-Firewall). Certain ASA models do support native tagging, and all ASA models support SXP for the transport of IP-address-to-SGT bindings.

It is important to note that the ASA has multiple functions. These functions include deep packet inspection firewalling and remote-access VPN (among many others). So, the ASA will enforce SGTs (enforcement) and receive SGTs (transport), as well as assign SGTs (classification) to Remote-Access VPN users.

From the ASA Device Manager (ASDM), perform the following steps:

**Step 1.** Navigate to **Configuration > Firewall > Identity by TrustSec**, as shown in [Figure 22-16](#).



**Figure 22-16** ASDM Identity by TrustSec

**Step 2.** Globally enable SXP by checking the **Enable SGT Exchange Protocol (SXP)** check box in the upper left.

**Step 3.** Click **Add** to add a new SXP peer.

**Step 4.** In the Add Connection Peer popup window, add the IP address of the remote peer.

**Step 5.** Choose **Default** for the Password (unless you will not be using passwords).

**Step 6.** Set the mode to **Peer**.

**Step 7.** Set the role to **Speaker**.

**Step 8.** Click **OK**.

After clicking OK, you are returned to the main Identity by TrustSec page. At this point, you have SXP enabled and a single peer defined, but no default password yet.

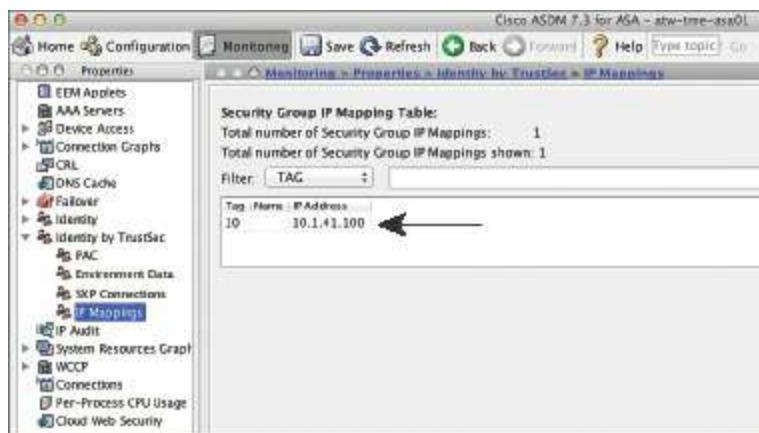
**Step 9.** (Optional) If you will be specifying the source IP address of the ASA, you may configure that source in the Default Source field.

**Step 10.** In the Default Password field and Confirm Password field, enter the default password for your entire SXP deployment.

[Figure 22-16](#) shows the Global Identity by TrustSec page in ASDM.

**Step 11.** To verify the SXP connection in ASDM, navigate to **Monitoring > Properties > Identity by TrustSec > SXP Connections** to see the configured peers and their status, as shown previously in [Figure 22-15](#).

**Step 12.** Click **IP Mappings** to see any IP-address-to-SGT mappings that the ASA has learned about, as shown in [Figure 22-17](#).



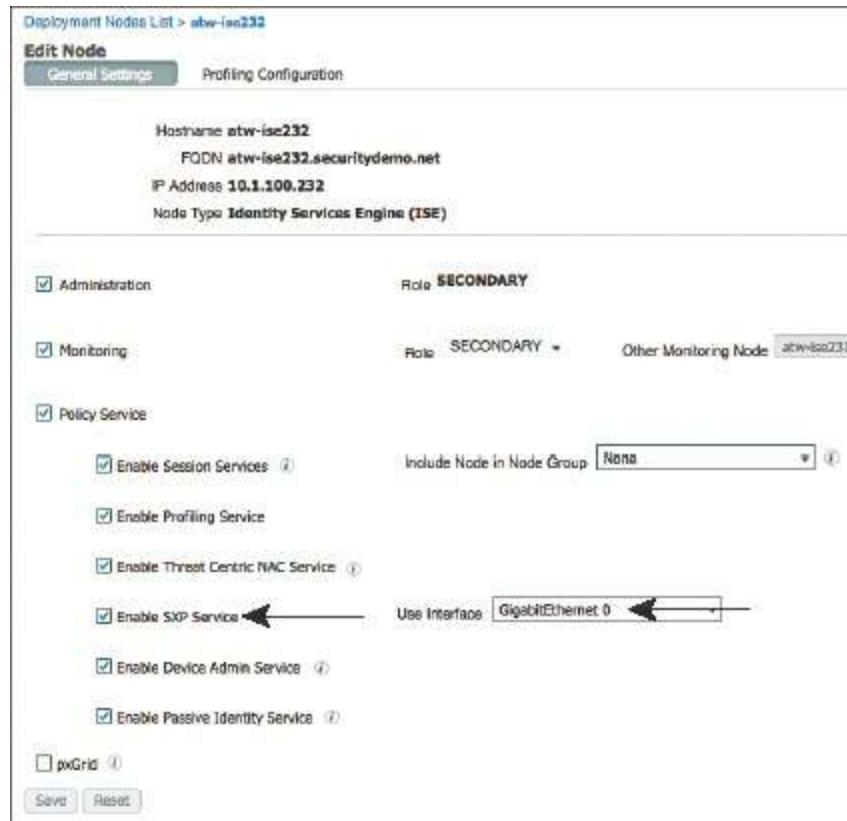
**Figure 22-17** ASDM Security Group IP Mapping Table

## Configuring SXP on ISE

As previously described, ISE acts as the TrustSec controller. So it only makes sense for ISE to be able to speak directly to enforcement devices, such as firewalls, and therefore SXP was added natively to ISE. This was illustrated previously in [Figures 22-12](#) and [22-13](#).

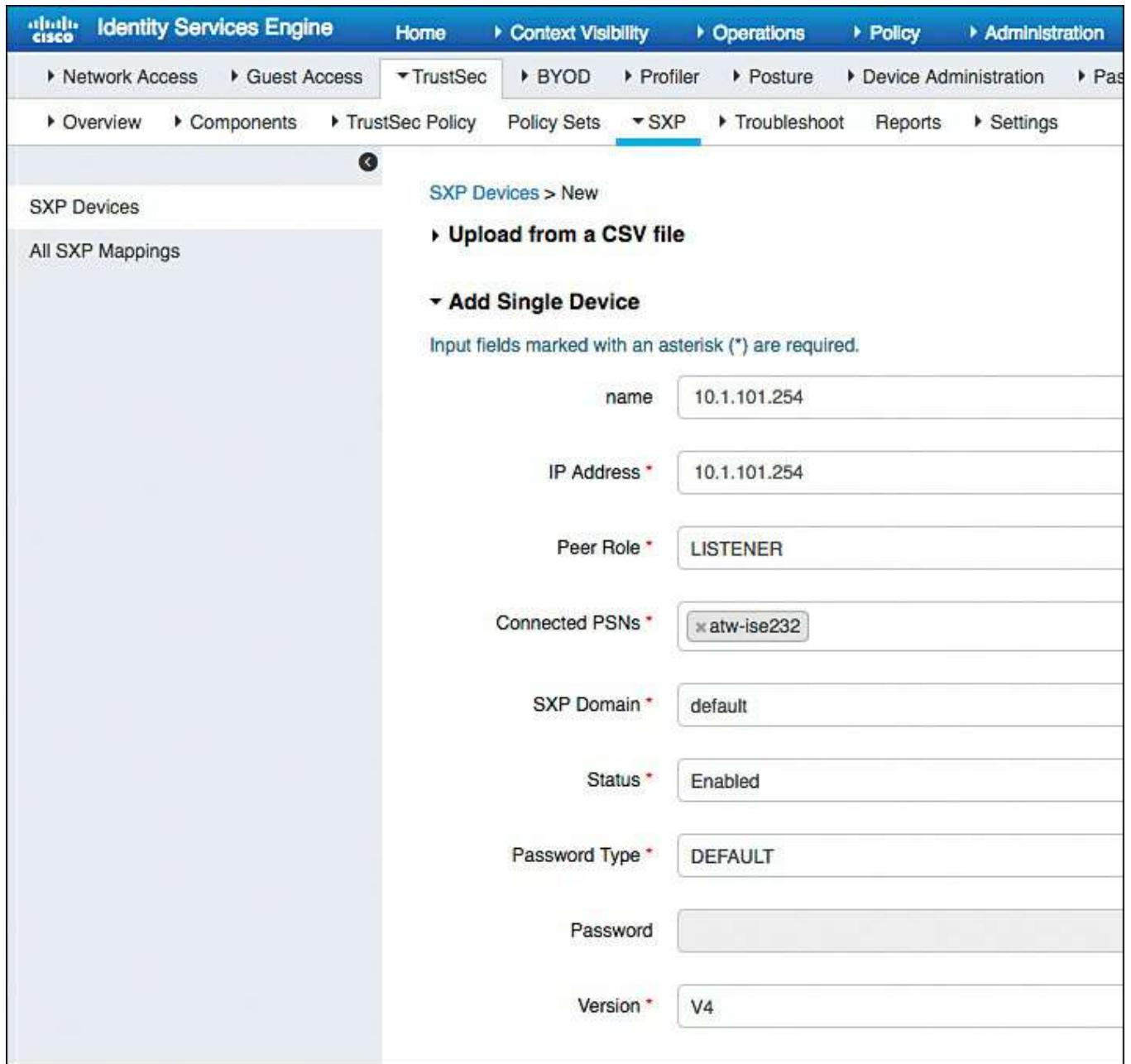
You must enable SXP on at least one of the PSNs in the ISE cube. It is a simple matter of checking the **Enable SXP Service** check box at **Administration > System >**

**Deployment**, as shown in [Figure 22-18](#). After checking the check box, you must also specify the interface for SXP to operate on. The default is the GigabitEthernet 0 interface.



**Figure 22-18** Enabling SXP in the PSN Deployment Configuration

After enabling SXP on one or more PSNs, navigate to **Work Centers > TrustSec > SXP > SXP Devices**, as shown in [Figure 22-19](#). Here you configure the peers with which to share IP address-to-SGT bindings, as well as learn from. That's right, ISE can act as both a speaker and a listener.



**Figure 22-19** Adding an SXP Peer within the ISE GUI

Click **Add** to add an SXP peer. [Figure 22-19](#) shows the ISE configuration of the ASA as a peer. ISE can operate with SXP versions 1 through 4, and will negotiate with the peer automatically.

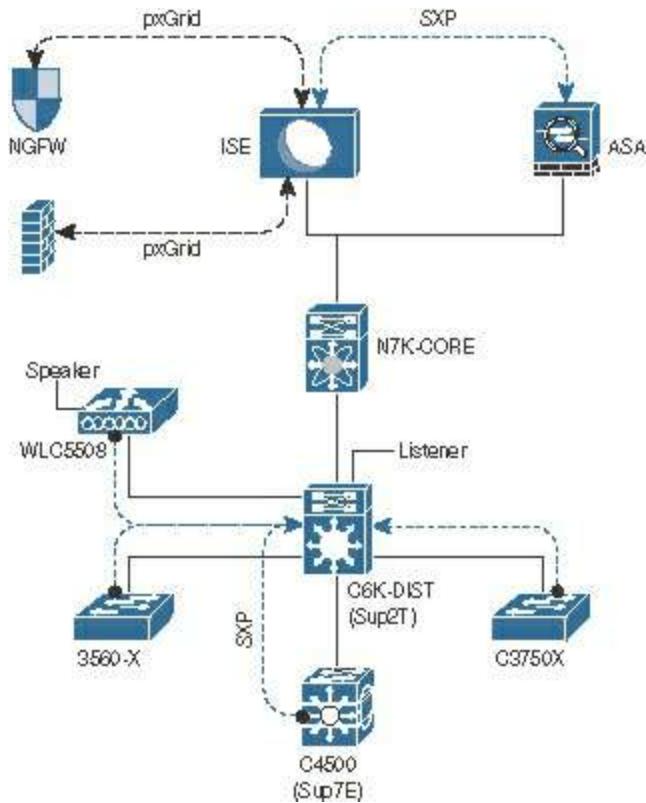
## Transport: pxGrid

SXP is not the only way that ISE can communicate the IP-address-to-SGT bindings. There are a number of devices that are also able to receive information via Cisco Platform Exchange Grid (pxGrid). pxGrid is a communication bus that is designed to share dynamic information at very large scale, and has a large number of security devices that use it to learn contextual information from ISE.

For example, the Cisco Firepower Next-Generation Firewall (NGFW) uses pxGrid to learn identities and SGT information from ISE, as does the Cisco Web Security Appliance (WSA) and Check Point firewalls.

pxGrid will be covered in more detail in [Chapter 24, “ISE Ecosystems: The Platform Exchange Grid.”](#)

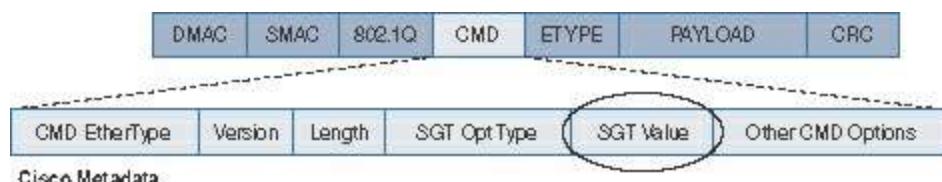
[Figure 22-20](#) illustrates adding pxGrid receivers in addition to the SXP design.



**Figure 22-20** SXP Design and pxGrid Consumers

## Transport: Native Tagging

Native tagging is the ultimate goal. With this approach, the access layer is capable of applying the SGT to the Layer 2 frame as it is sent across the wire to the upstream host. The upstream host continues that and ensures the SGT is applied. So, the SGT is always present throughout the entire infrastructure, as shown in [Figure 22-21](#).

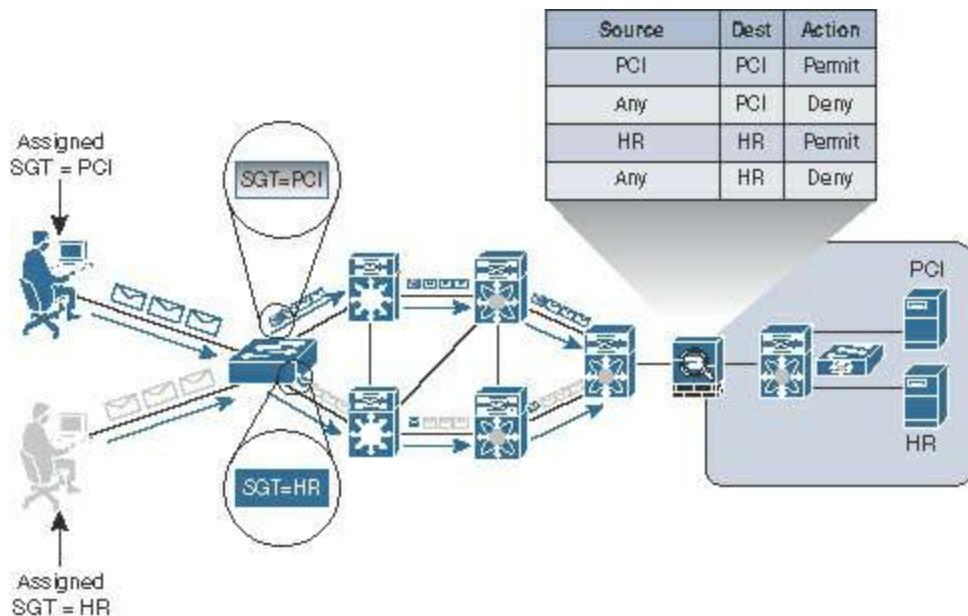


**Figure 22-21** Layer 2 Frame Format with SGT

Native tagging allows the technology to scale virtually endlessly, and it remains

completely independent of any Layer 3 protocol. In other words, architecturally speaking: If the traffic is IPv4 or IPv6, it does not matter. The SGT is completely independent.

As shown in [Figure 22-22](#), when native tags are supported pervasively within the infrastructure, the SGT is communicated hop-by-hop. This provides for end-to-end segmentation and tremendous scale. With the SGT being applied to the traffic at every Layer 2 link, we are able to enforce policy at any point in the infrastructure, and there are no limitations to the size of an IP-address-to-SGT mapping database, because the database is not being used at all.

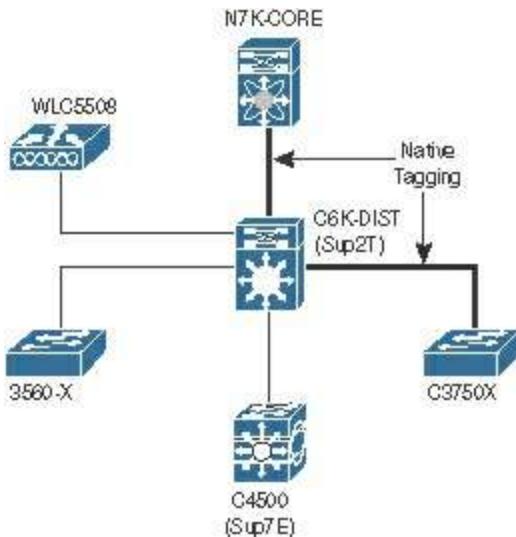


**Figure 22-22** Pervasive Tagging

For added security, the SGT may be encrypted with MACsec or IPsec, and the network infrastructure may be authenticated prior to sending or receiving tags, which is a solution known as Network Device Admission Control (NDAC).

## Configuring Native SGT Propagation (Tagging)

The next few configuration exercises show the enabling of native security group tagging on three different types of switches: a Cisco Catalyst 3000 series access layer switch, a Cisco Catalyst 6500 series distribution layer switch, and Nexus 7000 data center switches. [Figure 22-23](#) shows the logical network layout used in the configuration examples to follow.



**Figure 22-23** SGTs from Access to Distribution and Distribution to Data Center

## Configuring SGT Propagation on Cisco IOS Switches

This section discusses the configuration of SGT propagation on access layer switches, such as the Cisco Catalyst 3560-X and Cisco Catalyst 3750-X, that have the ability to use native tags. The Catalyst 6500 and Nexus series switches are covered in subsequent sections.

When it comes to inserting the SGT into Layer 2 traffic, there is a fundamental choice to make: to use encryption or not to use encryption. For simplicity, this chapter focuses on the easy one: without encryption.

From global configuration mode, perform the following steps:

**Step 1.** Enter **cts role-based enforcement**. This globally enables the tagging of SGTs. It also enables the ability to enforce Security Group ACLs (as discussed later, in the section “Traffic Enforcement with SGACLs”). However, without this command in the global configuration mode, the switch will not tag the Layer 2 traffic.

**Step 2.** Enter into interface configuration mode of the tagging-capable port by typing **interface interface-name**.

**Step 3.** Enter **cts manual**.

You are using **cts manual** because you are not utilizing NDAC at this point. The **cts manual** mode of operation allows you to apply the tag to the Layer 2 frame without having to negotiate encryption or requiring a fully trusted domain of Cisco switches (as you would need with NDAC).

**Step 4.** Enter **policy static sgt sgt-value trusted**.

ISE has default security groups defined out of the box. One of those SGTs is a

special group for network access devices named TrustSec\_Devices, and the value of that group is 2 (0x02). That is the value you are applying here with this **policy static sgt 2 trusted** command. The **trusted** keyword in this command ensures that no changes are made to the incoming tags, as they are from a trusted source.

[Example 22-4](#) displays the configuration to enable tagging, while [Example 22-5](#) shows the monitoring output.

### Example 22-4 Enabling Tagging on a 3750-X Series Access Switch

[Click here to view code image](#)

```
C3750X(config)# cts role-based enforcement
C3750X(config)# interface Ten 1/1/1
C3750X(config-if)# cts manual
C3750X(config-if-cts-manual)# policy static sgt 2 trusted
```

### Example 22-5 Verifying Tagging on a 3750-X Series Access Switch

[Click here to view code image](#)

```
C3750X# sho cts interface Ten 1/1/1
Global Dot1x feature is Enabled
Interface TenGigabitEthernet1/1/1:
    CTS is enabled, mode:      MANUAL
        IFC state:          OPEN
        Authentication Status: NOT APPLICABLE
            Peer identity:      "unknown"
            Peer's advertised capabilities: ""
        Authorization Status: SUCCEEDED
    Peer SGT:          2
    Peer SGT assignment: Trusted
    SAP Status:        NOT APPLICABLE
        Configured pairwise ciphers:
            gcm-encrypt
            null
        Replay protection:     enabled
        Replay protection mode: STRICT
        Selected cipher:
    Propagate SGT:       Enabled
```

```
Cache Info:  
    Cache applied to link : NONE  
Statistics:  
    authc success:          0  
    authc reject:           0  
    authc failure:          0  
    authc no response:      0  
    authc logoff:           0  
  
    sap success:            0  
    sap fail:               0  
    authz success:          3  
    authz fail:              0  
    port auth fail:         0  
L3 IPM:    disabled.
```

## Configuring SGT Propagation on a Catalyst 6500

The Catalyst 6500 is a special case. This switch is sometimes used in the access layer, but it's most often used in the distribution layer or even in the data center. There are also a tremendous number of line cards possible for this chassis-based switch, some of which can support native tagging and others that cannot. Because of the possibility of multiple locations and multiple line-card possibilities, the Catalyst 6500 requires the administrator to set whether the switch should be used for egress (receiving the tag from other devices) or ingress (placing it at the access layer). These modes are referred to as reflector modes.

**Note** This switch is unable to be configured for both ingress and egress mode simultaneously.

Ingress reflector mode should only be used in the access layer. This mode allows the use of non-TrustSec-capable line cards along with a TrustSec-capable supervisor. (An example of this would be a Catalyst 6504-E chassis populated with a Supervisor 2T and a 6148 series line card.) With this mode, all packet forwarding occurs on the Supervisor 2T PFC. Line cards that use distributed forwarding are not supported in

ingress reflector mode (such as the 6748-GE-TX).

With this mode of operation, ISE is able to assign an SGT to a device entering the access layer via any supported line card, but that tag is only applied to network traffic leaving one of the ports physically on the Supervisor 2T. In other words, the switch applies the tag on an uplink port, but not on any of the downlink ports. Additionally, the switch cannot read the incoming tag on any ports except the ones physically on the Supervisor 2T module itself.

**Note** Using a Supervisor 2T in the access layer is not normally recommended and is not part of Secure Access systems testing.

Egress reflector mode is normally associated with the Catalyst 6500 being deployed in the distribution layer or data center. With this mode, TrustSec propagation and encryption (MACsec) may be enabled on the Supervisor 2T and 6900 series line cards. These are the models of line card most often seen in the distribution layer, and as such, this provides for a nice TrustSec aggregation design. The switch can read all incoming SGT tagged packets and apply that tag to the traffic leaving the switch as well. This is the model of SGT that one normally thinks of when discussing the topic. Additionally, if the Catalyst 6500 is an SXP peer, it is capable of applying the SGT to Layer 2 traffic based on the IP-address-to-SGT bindings learned via SXP.

From global configuration mode on the Catalyst 6500, perform the following steps:

**Step 1.** Choose the CTS reflector mode by typing **platform cts [egress | ingress]**.

Because this is a distribution layer deployment of the Catalyst 6500, choose egress mode. If this were an access layer deployment, where end users would be authenticated, you would choose ingress mode.

**Step 2.** Enter **cts role-based enforcement**.

This globally enables the tagging of SGTs. It also has the capability to enforce SGACLs (discussed later in the section “Traffic Enforcement with SGACLs”). However, without this command in the global configuration mode, the switch will not tag the Layer 2 traffic.

**Step 3.** Enter into interface configuration mode of the tagging-capable port by typing **interface interface-name**.

**Step 4.** Enter **cts manual**.

You are using **cts manual** because you are not utilizing NDAC at this point. The **cts manual** mode of operation allows you to apply the tag to the Layer 2 frame without having to negotiate encryption or require a fully trusted domain of Cisco switches (as would be necessary with NDAC).

## **Step 5. Enter `policy static sgt sgt-value trusted`.**

ISE has default security groups defined out of the box. One of those SGTs is a special group for network access devices named TrustSec\_Devices, and the value of that group is 2 (0x02). That is the value you are applying here with this **policy static sgt 2 trusted** command. The **trusted** keyword in this command ensures that no changes are made to the incoming tags, because they are from a trusted source.

Examples 22-6 and 22-7 display the enabling and verifying of tagging with the Catalyst 6500 Supervisor 2T.

### **Example 22-6 Enabling Tagging on Catalyst 6500 Supervisor 2T**

[Click here to view code image](#)

```
C6K-DIST(config)# platform cts egress
C6K-DIST(config)# cts role-based enforcement
C6K-DIST(config)# interface Ten1/5
C6K-DIST(config-if)# cts manual
C6K-DIST(config-if-cts-manual)# policy static sgt 2 trusted
```

### **Example 22-7 Verifying Tagging on the Catalyst 6500 Supervisor 2T**

[Click here to view code image](#)

```
C6K-DIST# show cts interface Ten1/5
Global Dot1x feature is Enabled
Interface TenGigabitEthernet1/5:
    CTS is enabled, mode:      MANUAL
        IFC state:              OPEN
        Authentication Status:   NOT APPLICABLE
            Peer identity:       "unknown"
            Peer's advertised capabilities: ""
        Authorization Status:    SUCCEEDED
            Peer SGT:             2
            Peer SGT assignment: Trusted
        SAP Status:             NOT APPLICABLE
        Configured pairwise ciphers:
            gcm-encrypt
            null
        Replay protection:       enabled
        Replay protection mode: STRICT
        Selected cipher:
            Propagate SGT:        Enabled
        Cache Info:
            Cache applied to link : NONE
        Statistics:
            authc success:         0
            authc reject:          0
            authc failure:         0
            authc no response:     0
            authc logoff:          0
            sap success:           0
            sap fail:              0
            authz success:          1
            authz fail:             0
            port auth fail:        0
        L3 IPM:      disabled.
```

## Configuring SGT Propagation on a Nexus Series Switch

The following steps guide you through the configuration of SGT propagation on the

Nexus Series switch.

From global configuration mode on the Nexus Series switch, perform the following steps:

**Step 1.** Type **feature dot1x** at global configuration mode.

The Nexus Series requires the feature **dot1x** to be enabled before enabling CTS features.

**Step 2.** Type **cts enable** at global configuration mode.

This command enables TrustSec, MACsec, and NDAC features to be enabled and configured.

**Step 3.** Enter **cts role-based enforcement**.

This globally enables the tagging of SGTs. It also provides the capability to enforce SGACLs (discussed later in the section, “Traffic Enforcement with SGACLs”). Without this command in the global configuration mode, however, the switch will not tag the Layer 2 traffic.

**Step 4.** Enter into interface configuration mode of the tagging-capable port by typing **interface interface-name**.

**Step 5.** Enter **cts manual**.

You are using **cts manual** because you are not utilizing NDAC at this point. The **cts manual** mode of operation allows you to apply the tag to the Layer 2 frame without having to negotiate encryption or requiring a fully trusted domain of Cisco switches (such as you would need with NDAC).

**Step 6.** Enter **policy static sgt sgt-value trusted**.

ISE has default security groups defined out of the box. One of those SGTs is a special group for network access devices named **TrustSec\_Devices**, and the value of that group is 2 (0x02). That is the value you are applying here with the **policy static sgt 2 trusted** command. The **trusted** keyword in this command ensures that no changes are made to the incoming tags, because they are from a trusted source.

[Example 22-8](#) walks through the enabling of tagging on a Nexus 7000 series switch.

**Example 22-8** Enabling Tagging on Nexus 7000

[Click here to view code image](#)

```
NX7K-CORE(config)# feature dot1x
NX7K-CORE(config)# cts enable
NX7K-CORE(config)# cts role-based enforcement
NX7K-CORE(config)# int eth1/26
NX7K-CORE(config-if)# cts manual
NX7K-CORE(config-if-cts-manual)# policy static sgt 0x2 trusted
```

## Enforcement

Now that you have security groups being assigned (classification) and they are being transmitted across the network (transport), it is time to focus on the third staple of TrustSec: enforcement.

There are multiple ways to enforce traffic based on the tag, but they can ultimately be summarized into two major types:

- Enforcement on a switch (SGACL)
- Enforcement on a firewall (SG-FW)

## Traffic Enforcement with SGACLs

Historically, enforcement with SGACLs was the only option available. It started with the Nexus 7000 Series and has expanded to the Nexus 5000 Series, Catalyst 6500 (Supervisor 2T), and the 3000-X Series switches. A major benefit to SGACL usage is the consolidation of ACEs and the operational savings involved with maintenance of those traditional ACLs.

An SGACL can be visualized in a format similar to a spreadsheet. It is always based on a source tag to a destination tag. [Figure 22-24](#) shows an example SGACL policy on ISE, which represents the SGACLs in a columns and rows presentation, like a simple spreadsheet. The simple policy in [Figure 22-24](#) shows that traffic from BYOD devices will be denied when attempting to communicate to PCI\_Servers. It also shows that Developers will be permitted to contact Development\_Servers, but those Development\_Servers cannot communicate to each other.

Production Matrix      Populated cells: 0

Source ▾	Contractors 5/0005	Developers 8/0008	Development_Ser... 12/000C	Network_Service... 3/0003	PCI_Servers 14/000E
Destination ▾	Contractors 5/0005	Developers 8/0008	Development_Ser... 12/000C	Network_Service... 3/0003	PCI_Servers 14/000E
BYOD 15/000F	Permit IP			NetServicesOnly	Deny IP
Contractors 5/0005				Permit IP	Deny IP
Developers 8/0008			Permit IP		Deny IP
Development_Ser... 12/000C		Permit IP	Deny IP		

**Figure 22-24 SGACL Egress Policy: Matrix View**

In addition to blanket permit or deny SGACLS like Permit IP or Deny IP, an SGACL may be specific about the destination protocols and ports to permit or deny. NetServicesOnly is a more restrictive SGACL that is applied when BYOD devices attempt to reach Network\_Services.

As you can see in [Figure 22-25](#), the resulting ACL would be to permit only specific traffic and deny all the rest. This traffic is applied at egress of the switch where the SGACL is configured. In this case, it is applied at the Nexus 7000 in the data center, as traffic attempts to reach any Network\_Services tagged devices.

**Figure 22-25** NetServicesOnly SGACL Contents

This form of traffic enforcement can provide a tremendous savings on the complexity and number of ACEs to maintain. There is a general formula to see the savings:

$$(\# \text{ of sources}) \times (\# \text{ of destinations}) \times \text{permissions} = \# \text{ of ACEs}$$

With a traditional ACL on a firewall:

$$4 \text{ VLANs (src)} \times 30 \text{ (dst)} \times 4 \text{ permission} = 480 \text{ ACEs}$$

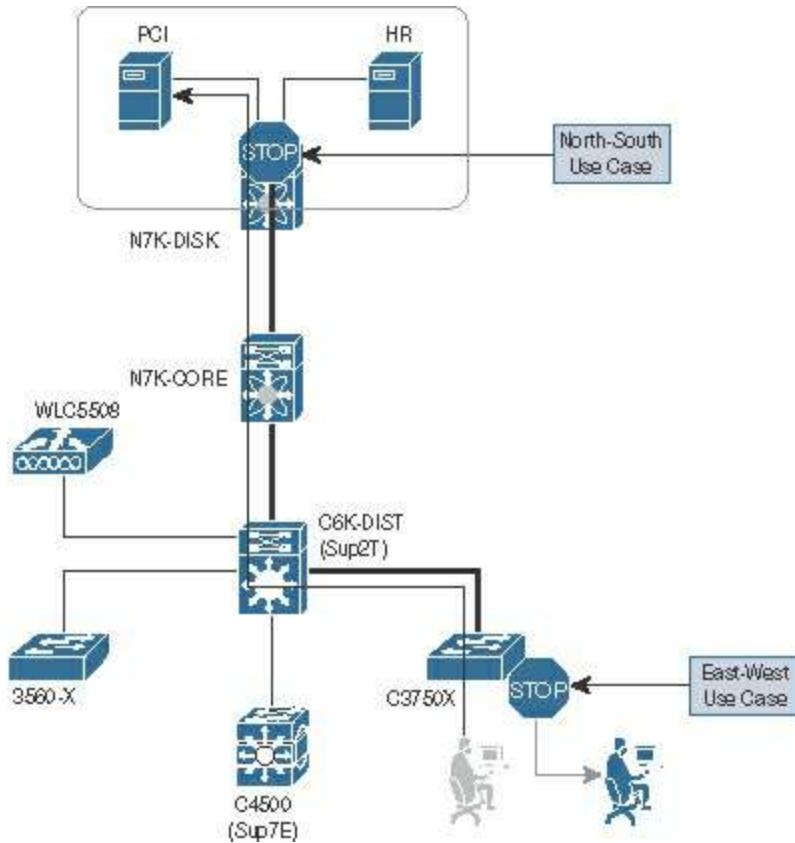
Per source IP on a port using dACL:

$$1 \text{ group (source)} \times 30 \text{ (dst)} \times 4 \text{ permission} = 120 \text{ ACEs}$$

With SGACLs, the number of ACEs is a magnitude smaller:

$$4 \text{ SGT (src)} \times 3 \text{ SGT (dst)} \times 4 \text{ permission} = 48 \text{ ACEs}$$

There are two main ways to deploy SGACLs: North-South and East-West, as shown in [Figure 22-26](#). North-South refers to the use case of a user or device being classified at the access layer, but enforcement with the SGACL occurring at the data center. For example, a guest entering the access layer is assigned a GUEST SGT. Traffic with a GUEST SGT is dropped if it tries to reach a server with financial data.



**Figure 22-26 North-South Versus East-West Visually Explained**

East-West refers to the use case of an SGACL protecting resources that exist on the same switch. For example, in a scenario with a development server and a production server on the same Nexus 5000 Series switch in the data center, an SGACL may be deployed to prevent the development server from ever communicating with the production server. Another East-West example is a guest and an employee both using the same access layer switch. Traffic may be filtered between these two devices so the guest cannot communicate to the employee who is in the same VLAN on the same switch.

## Creating TrustSec Matrices in ISE

ISE provides three different views to create TrustSec policies and SGACLS: two tree views (Source Tree and Destination Tree), and a Matrix View. The Matrix View is the one that looks and acts more like a spreadsheet. Additionally, ISE allows you to have multiple matrices, so that you can test policy changes in limited environments before pushing those changes to production. The Matrix View is the view we focus on in this book.

From the ISE Administration GUI, perform the following steps:

**Step 1.** Navigate to **Work Centers > TrustSec > TrustSec Policy > Matrix.**

**Step 2.** Click the square that represents the intersection of a source SGT and a destination SGT.

## Traffic Enforcement with Security Group Firewalls

Some organizations prefer to do the traffic enforcement on the switching infrastructure, on a device that was purpose-built to do traffic filtering: a firewall. Cisco has added the capability to enforce traffic on firewalls by including the source SGT and/or destination SGT in the firewall policy itself.

This section focuses on the Cisco ASA. The Cisco Firepower solution may also use source SGTs in its access policies, but that requires the use of pxGrid for context sharing and is part of the coverage in [Chapter 24](#).

### Security Group Firewall on the ASA

Beginning with ASA version 9.0, the ASA firewall gains SG-FW functionality. ASDM supports the full configuration, and therefore the ASA is the only SG-FW that has a GUI (as of this writing).

The SG-FW in the ASA is a simple concept. The powerful firewall policy in the firewall has been expanded to include source and destination security groups into the decision. As you can see in [Figure 22-27](#), there is a new Security Group column in the Source Criteria and Destination Criteria sections.

Configuration > Firewall > Access Rules													
#	Enabled	Source Criteria:			Action	Service	Destination Criteria:						
		Source	User	Security Group			Destination	Security Group					
<b>outside (1 incoming rule)</b>													
1	<input checked="" type="checkbox"/>		any			1044		Permit		ip		any	
<b>Global (4 rules)</b>													
1	<input checked="" type="checkbox"/>		any		PCI		Permit		ip		DataCenter		PCI
2	<input checked="" type="checkbox"/>		any		ALL-Em...		Permit		ip		any		HR
3	<input checked="" type="checkbox"/>		any		ANY		Deny		ip		DataCenter		PCI
4			any				Deny		ip		any		

Figure 22-27 ASDM Firewall Policy

### Security Group Firewall on the ISR and ASR

The ASA is not the only security group firewall on the market. Both the Cisco Integrated Services Router Generation 2 (ISR G2) and the Cisco Aggregation Services Router

(ASR) have a powerful ZBF capability.

The Cisco ISR Gen2 (c3900, c3900e, c2900, c2901, c1941, c890) began support of SG-FW as of version 15.2(2)T. The Cisco ASR 1000 added support of the SG-FW as of IOS-XE version 3.4.

## Summary

This chapter explained TrustSec, and at this point, you should be able to articulate why it is so valuable and how much OPEX it can save your organization.

You learned that there are three foundational pillars of security group access: classification, transport, and enforcement. Where classification is the ability to accept the tag for a particular network authentication session, transport is the ability to send that assigned tag to upstream neighbors either via native tagging, Security group eXchange Protocol (SXP), or the Platform eXchange Grid (pxGrid); and that enforcement may be on switches using Security Group ACLs (SGACL) or on a Security Group Firewall (SG-FW).

# Chapter 23 Passive Identities, ISE-PIC, and EasyConnect

This chapter covers the following topics:

- Passive authentication
- Identity sharing
- ISE Passive Identity Connector (ISE-PIC)
- EasyConnect

One of the most common functions of secure network access is to identify who is attempting to access the network before granting them access. Throughout this book, you have learned about technologies such as supplicants, authenticators, authentication servers, 802.1X, WebAuth, MAB, and even Active Directory integration.

Up until this point, the identities have been presented directly to ISE, meaning the endpoint's supplicant was configured to pass the user's credentials inside of an EAP packet to ISE itself (802.1X) or the user's credentials were entered directly into a web page hosted on ISE (WebAuth). However, ISE isn't the only server or service on the network performing authentications day in and day out. The vast majority of organizations are using Microsoft Active Directory, so wouldn't it be neat if we could piggy-back off that for network access, even if only temporarily as 802.1X is being deployed across the organization?

The function of learning about identities that have been authenticated by another server or service is known as passive authentication, and the identities that have been learned are referred to as passive identities.

Most of this book is dedicated to the active authentication use cases. Conversely, this chapter remains focused on passive authentications.

## Passive Authentication

Many security products on the market today use passive authentication to learn user identities and which IP addresses are assigned to those users. For example, most modern firewall and NGFW solutions use user identities within their firewall policies instead of constructing the policies with source IP addresses.

The Cisco ASA has used a solution known as Cisco Context Directory Agent (CDA) for years. The Cisco Sourcefire Firepower solution leveraged an Active Directory agent named Source Fire User Agent (SFUA). Both solutions would integrate with Active Directory using Windows Management Instrumentation (WMI) to learn about user authentications and their corresponding IP addresses, and then leverage that information within the firewall policies.

An active authentication learns the identity directly from the user, and a firewall usually

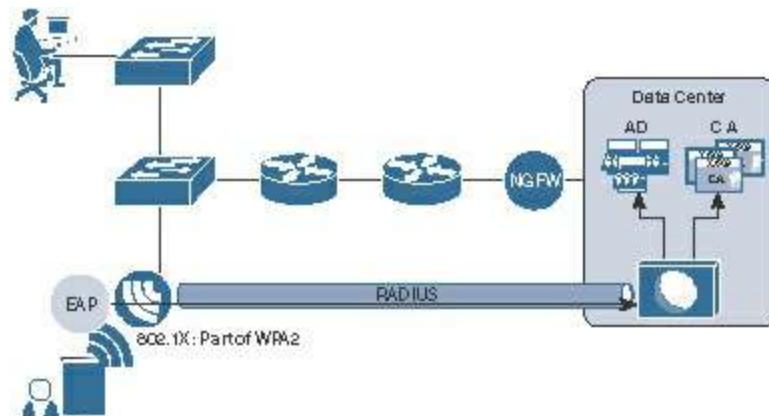
only does this by sending the user through a web authentication process. By leveraging passive authentications, the firewall is able to transparently authenticate the user's IP address and apply the correct firewall rule to the traffic traversing the firewall.

For comparison, [Figure 23-1](#) illustrates an active authentication and [Figure 23-2](#) illustrates a passive authentication.

When it comes to ISE, identities could be used for its own policies and authorizing of network access. Of course, that is the main purpose of ISE, isn't it? Well the other major use case for ISE is sharing this information to other products. [Chapter 24, “ISE Ecosystems: The Platform Exchange Grid \(pxGrid\),”](#) is dedicated to this use case.

[Figure 23-1](#) shows an EAP packet from the endpoint traversing the RADIUS connection to ISE. The following steps explain the active authentication process shown in [Figure 23-1](#):

1. The identity is contained within the EAP packet and is sent from the supplicant to the network, which passes the packet to ISE within the RADIUS connection.

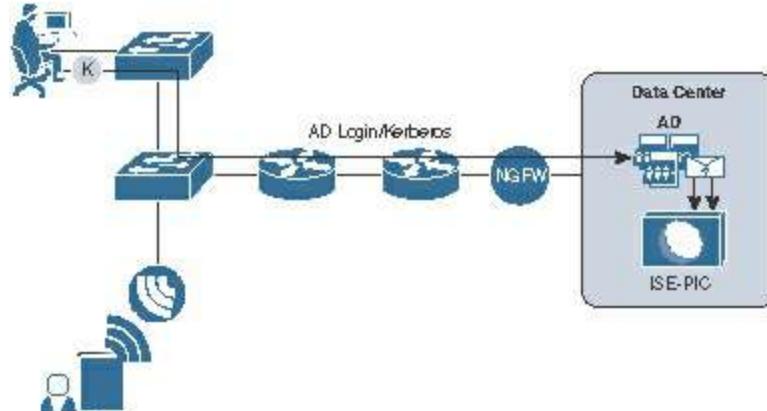


**Figure 23-1** Active Authentication Using 802.1X

2. ISE validates the credentials against the correct ID store, ensuring the identity is valid. The identity may be in the form of a username and password, a certificate, or other credential.
3. As part of the authorization process, ISE learns the group membership and other attributes of the user's identity and adds this to ISE's session directory.
4. ISE provides the end result back to the network, authorizing the user to have the assigned level of access.
5. The session directory information can be shared with ecosystem partners, such as firewalls and web security appliances.

[Figure 23-2](#) illustrates ISE learning about a user with a Windows workstation authenticating to Active Directory, which leverages Kerberos. The following steps explain the passive authentication process shown in [Figure 23-2](#):

1. The identity is part of the Kerberos authentication that occurs as part of the normal Active Directory processes.



**Figure 23-2** Passive Authentication Using WMI

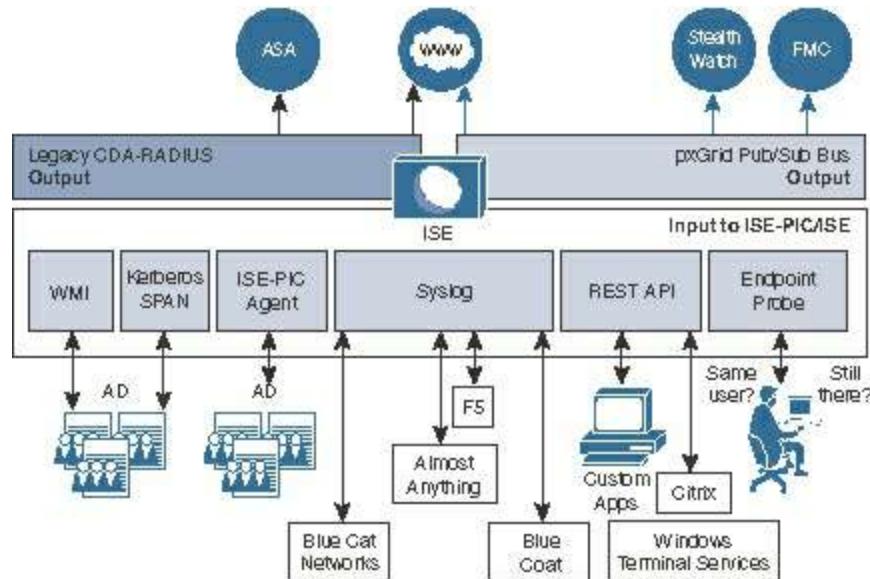
2. The AD authentication triggers a notification through WMI.
3. ISE is subscribed to those WMI messages and learns about the authentication event, the user ID, and the source IP address of that authentication.
4. ISE performs an AD lookup and learns the user's group membership, adding the information to the session directory.
5. The session directory information can be shared with ecosystem partners, such as firewalls and web security appliances.

Most of this book is dedicated to the active authentication use cases. However, this chapter remains focused on passive authentications and the uses of that information for network access and for identity sharing.

## Identity Sharing

Identity sharing is a key function of ISE. There are many solutions on the market that have their own identity sharing capabilities, designed for their firewall or for their web security appliance. ISE is architected to be the center of information sharing in a multivendor security ecosystem, including identities.

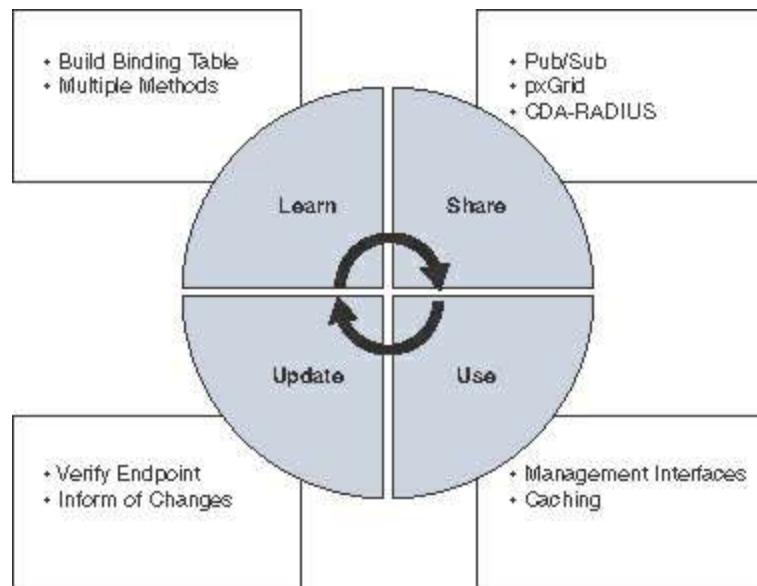
The vision for ISE is to provide these identities to all Cisco security products and more, through whichever means necessary. ISE version 2.2 moves the solution forward in a big way, but does not solve the entire problem yet. Because this book will most likely be referenced for many versions past version 2.2, [Figure 23-3](#) illustrates ISE with some features that are not available in version 2.2. Specifically, it shows the CDA-RADIUS interface, which is not available at the time of writing.



**Figure 23-3** ISE ID Sharing Inputs and Outputs

Don't worry too much about [Figure 23-3](#) just yet. We will dive into the different pieces of this design and solution throughout this chapter. For now, it's important that you understand a fundamental concept: identity sharing is a system with many moving parts, functions, and needs. To try and explain it, we will break all of it down to the four main pillars or tenets of a complete solution, as illustrated in [Figure 23-4](#):

- Learn
- Share
- Use
- Update



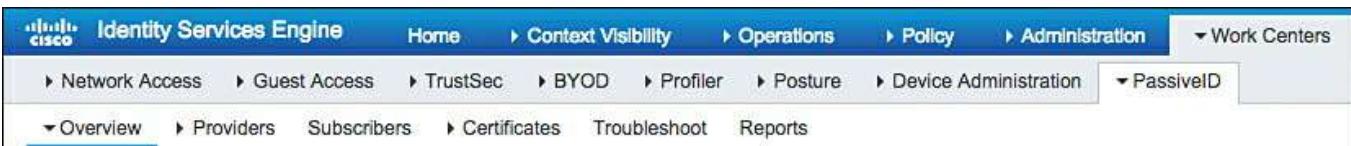
**Figure 23-4** Four Tenets of Identity Sharing

The graphical user interface of ISE is organized in a way that also aligns well with

these tenets. In ISE 2.2, passive identity functions have been consolidated into the PassiveID Work Center to make configuration and administration easier. Let's examine the PassiveID Work Center. Navigate to **Work Centers > PassiveID**.

As shown in [Figure 23-5](#), the Work Center is organized into the following sections:

- **Overview:** This section includes a dashboard focused on passive identity functions, and the live sessions log.
- **Providers:** This section is focused on the sources of passive identity information such as Active Directory, syslog, and SPAN.
- **Subscribers:** This is where pxGrid and its related configuration exists, where the products and solutions that need to receive the username and IP bindings are configured in ISE.
- **Certificates:** There are a lot of certificate functions needed when leveraging pxGrid, and those configuration objects are in this section of the Work Center.
- **Troubleshoot:** In ISE 2.2, this section contains the TCP Dump tool. Expect more in future versions of ISE.
- **Reports:** Rather self-explanatory. This section provides the relevant reports for passive identity functions.



**Figure 23-5** PassiveID Work Center

Now let's drill into those four tenets illustrated in [Figure 23-4](#) and look at the configuration in the ISE GUI.

## Tenet 1: Learn

The mission statement assigned to the Learn tenet is for the solution (ISE in our case) to build the bindings of the users on the network and their current IP addresses. The methods available to learn of these users and their addresses will vary depending on the source of the information.

Although all four of the tenets are critical to a complete and working solution, the Learn tenet is most likely the one that truly separates the men from the boys when comparing passive identity solutions. The number of sources, the flexibility, and the ease of integration to those sources all play a big role in the solution.

The next few sections drill into each of the different identity sources: Active Directory, syslog, and REST.

## Active Directory

Active Directory is the main source of passive identities today. ISE can learn about the AD authentications through three main methods:

- **Windows Management Instrumentation (WMI):** WMI is a publish/subscribe (pub/sub) messaging system within AD. ISE may remotely communicate with AD using WMI and subscribe to certain security events, like logins. When those events occur, ISE is notified by AD.

**Note** At the time of writing, with ISE version 2.2, WMI is the only passive identity source that can be used with EasyConnect (covered in more detail later in this chapter).

- **ISE-PIC agent:** The ISE Passive Identity Connector (ISE-PIC) agent is a native Windows application that can be loaded on an AD domain controller or an AD member server. The agent leverages native Windows APIs for WMI to learn about the authentications and sends the data to ISE over a secure channel.
- **SPAN session:** You can leverage Cisco Switched Port Analyzer (SPAN) technology to allow ISE to examine Kerberos traffic to learn of the authentications by “sniffing the traffic on the wire” without having to install any agents or configure WMI.

## Windows Management Instrumentation

As described previously, WMI is a core Windows management technology that allows you to manage Windows servers or workstations locally or remotely.

ISE can remotely communicate with AD using WMI and subscribe to certain security events, like logins. When those events occur, ISE is notified by AD.

The main benefit to using this WMI method to learn about the passive authentication is that it does not require installation of an agent on a domain controller or a member server. Before WMI can be used, connectivity requirements for successful WMI connections must be met. The good news is that the Config WMI function from the ISE GUI will perform that configuration for you, as demonstrated a bit later in this section.

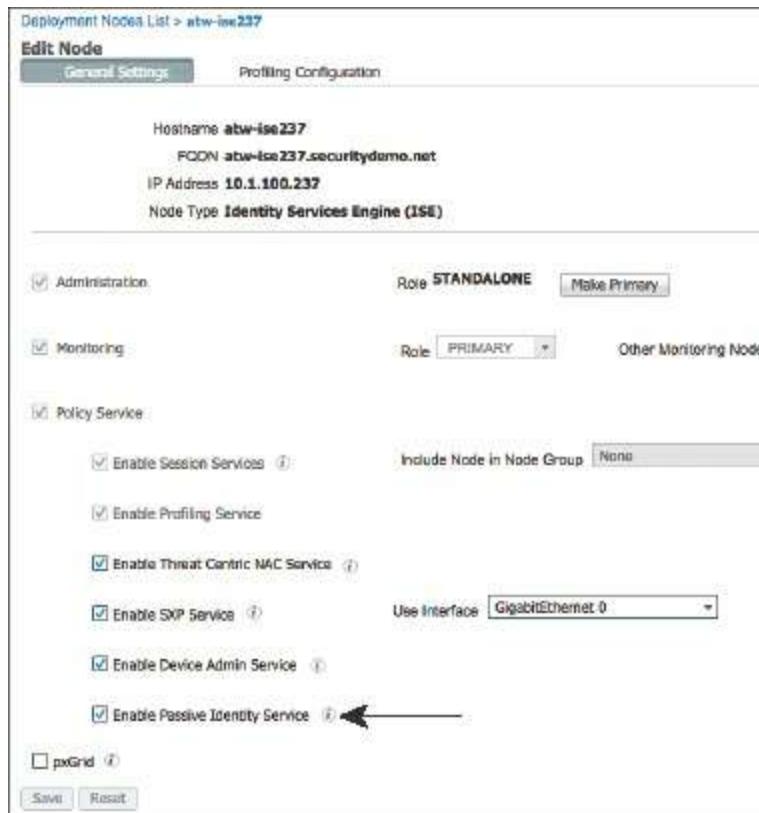
This type of connection to AD has been around for a very long time. Cisco Context Directory Agent (CDA) used it, and it's been a part of ISE since version 1.3. In ISE, it was previously referred to as “pxGrid Identity Mapping” and was designed to bring the passive identity functionality of CDA into ISE for sharing with pxGrid subscribers.

This functionality was then extended to create the EasyConnect deployment method in ISE version 2.1 and then given a tremendous boost in capability and ease of use in ISE version 2.2.

The WMI connection allows ISE to remotely communicate to an AD domain controller as a subscriber of WMI security events. Specifically, ISE looks for new Kerberos tickets that are granted and when those tickets are renewed. The granting of a ticket shows that a new Windows authentication session has occurred; it could be a user or a machine authentication, but that is for ISE to sort through after it is notified. The renewing of Kerberos tickets shows that the session is still active and should not be timed out or purged.

**Configuring WMI** To integrate ISE with Active Directory via WMI, from the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Administration > System > Deployment**. Ensure that at least one Policy Service Node (PSN) has the Passive Identity Service enabled, as shown in [Figure 23-6](#).

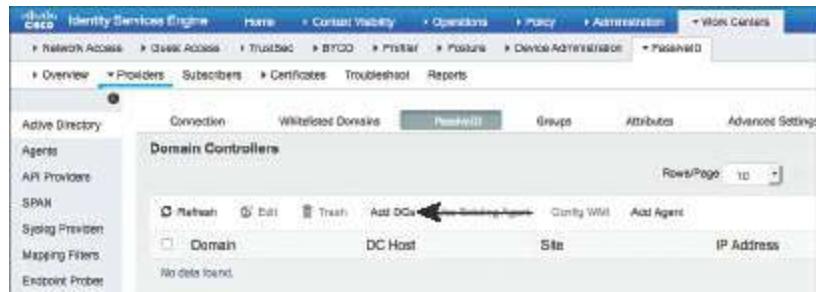


**Figure 23-6** Passive Identity Service

**Step 2.** Navigate to **Work Centers > PassiveID > Providers > Active Directory**.

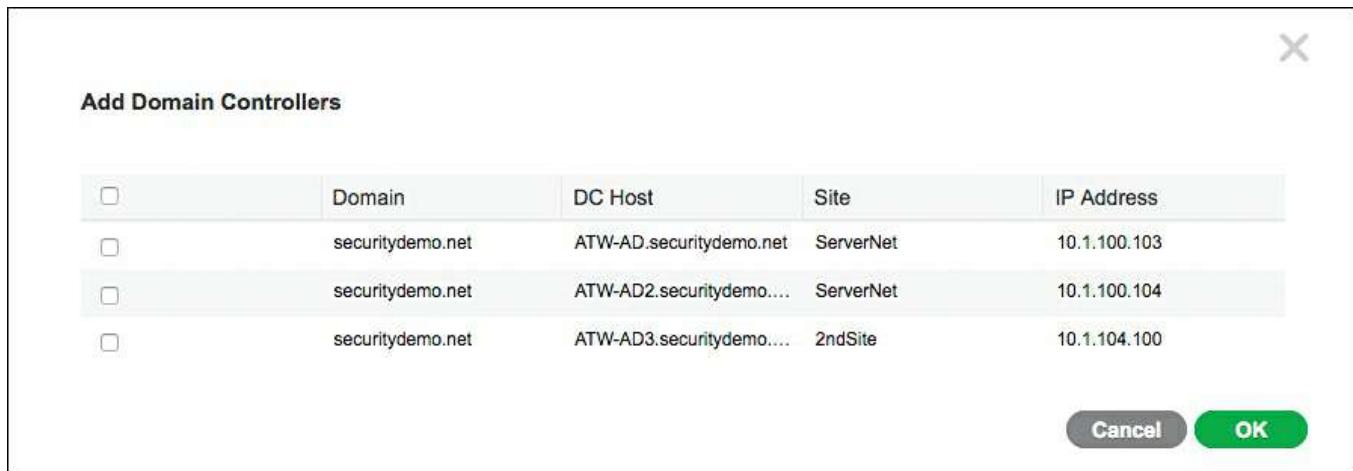
**Step 3.** Select your Active Directory join point. In the example used in this book, it is named AD-SecurityDemo.

**Step 4.** Click the **PassiveID** tab, as shown in [Figure 23-7](#).



**Figure 23-7** PassiveID Tab

**Step 5.** Click **Add DCs**. The list of domain controllers is displayed, as shown in [Figure 23-8](#).



**Figure 23-8** Add Domain Controllers

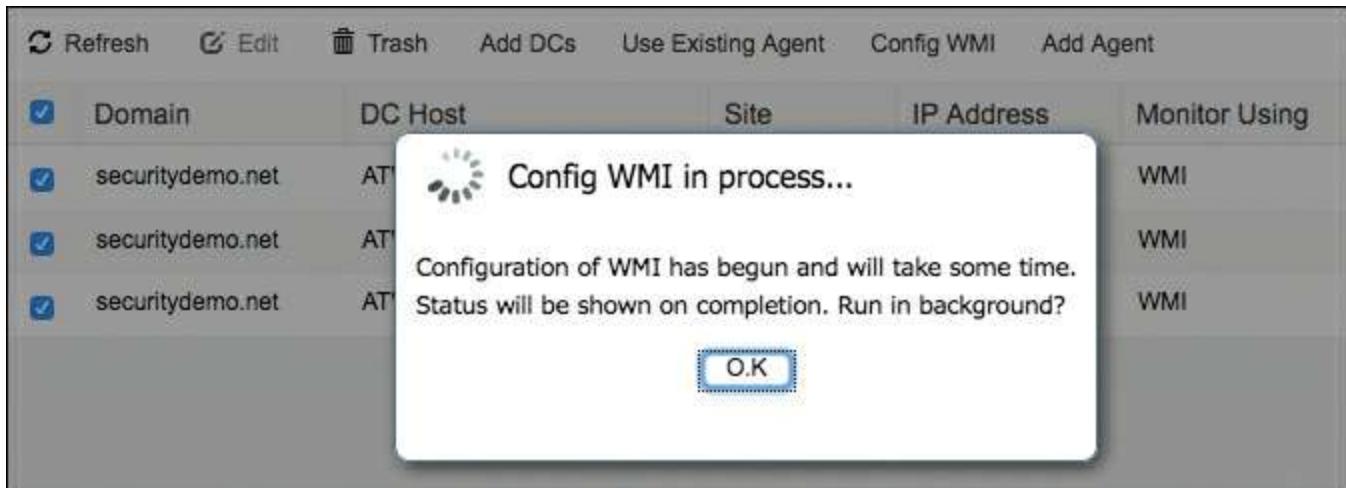
**Step 6.** Choose the domain controller(s) that you wish to monitor and click **OK**.

**Step 7.** The domain controllers are added to the list of PassiveID Domain Controllers. Select the DCs and click **Config WMI**, as highlighted in [Figure 23-9](#).



**Figure 23-9** Config WMI on Selected DCs

**Step 8.** The Config WMI in Progress message is displayed, as shown in [Figure 23-10](#).



**Figure 23-10** Config WMI in Progress

**Step 9.** When the configuration process is complete, a success message is displayed, such as the one shown in [Figure 23-11](#). The process performed by the Config WMI function is quite extensive and detailed after these configuration steps.



**Figure 23-11** Successfully Configured DCs

**Step 10.** ISE is now configured to subscribe to the WMI security events, and the AD controllers are configured to send those events to ISE. When AD authentications occur, those sessions are displayed in the Live Sessions screen, as shown in [Figure 23-12](#).

Initiated	Updated	Session Status	Action	Endpoint ID	Identity	IP Address
Dec 13, 2016 10:12:17.936 PM	Dec 13, 2016 10:12:17.936 PM	Authenticated	Show Actions	2.1.4.250	FakeUser-2-4-250	2.1.4.250
Dec 13, 2016 10:12:17.936 PM	Dec 13, 2016 10:12:17.936 PM	Authenticated	Show Actions	2.1.4.249	FakeUser-2-4-249	2.1.4.249
Dec 13, 2016 10:12:17.936 PM	Dec 13, 2016 10:12:17.936 PM	Authenticated	Show Actions	2.1.4.248	FakeUser-2-4-248	2.1.4.248
Dec 13, 2016 10:12:17.936 PM	Dec 13, 2016 10:12:17.936 PM	Authenticated	Show Actions	2.1.4.247	FakeUser-2-4-247	2.1.4.247
Dec 13, 2016 10:12:17.936 PM	Dec 13, 2016 10:12:17.936 PM	Authenticated	Show Actions	2.1.4.246	FakeUser-2-4-246	2.1.4.246
Dec 13, 2016 10:12:17.935 PM	Dec 13, 2016 10:12:17.935 PM	Authenticated	Show Actions	2.1.4.245	FakeUser-2-4-245	2.1.4.245
Dec 13, 2016 10:12:17.935 PM	Dec 13, 2016 10:12:17.935 PM	Authenticated	Show Actions	2.1.4.244	FakeUser-2-4-244	2.1.4.244

**Figure 23-12** Live Sessions

**What Does that Config WMI Button Do?** The Config WMI process performs an awful lot in the background. Prior to ISE version 2.2, everything detailed in this section needed to be performed manually. To see more of the painful process of the past, check out the Cisco Identity Services Engine Administrator Guide for ISE version 1.3 or 1.4 and its instructions for setting up the pxGrid Identity Mapping function.

There are five main things that Config WMI completes for you:

- **Registry changes:** ISE creates two registry keys that add the ID of the WMI client used by ISE. The key name is 76A64158-CB41-11D1-8B02-00600806D9B6 and it must be added in two locations:
  - HKEY\_CLASSES\_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
  - HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- **Permissions to use DCOM:** ISE communicates to the domain controllers using a Windows account, which needs to have local and remote access to DCOM. The **dcomcnfg** command could be used to configure DCOM permissions manually.
- **Permissions to use WMI remotely:** By default, AD users do not have the Execute Methods and Remote Enable permissions by default. These can be granted manually by using the **wmimgmt.msc** command.
- **Access to read the security event log of the AD domain controller:** To allow the AD user to read the security event log of the DC, the user must be added to two different security groups:
  - Event Log Readers group
  - Distributed COM Users group
- **Configure the Windows firewall to allow traffic to and from ISE:** By default, the Windows firewall on the domain controller would block the communication, so a rule must be added to allow ISE to remotely access the server for DCOM/WMI.

## ISE-PIC Agent

WMI is a very nice and popular option that is tried and true; however, not all organizations are keen on the idea of a non-Windows device like ISE remotely connecting and using DCOM. Those organizations prefer an agent-based approach, where software is installed on a Windows domain controller or a member server instead of connecting to an external system like ISE.

With ISE version 2.2 and newer, that option is a reality. The software that installs on an AD DC or on an AD Member server is named the ISE Passive Identity Connector Agent (aka the ISE-PIC agent).

The ISE-PIC agent comes preinstalled with ISE 2.2, but newer versions of the agent may be downloaded from [Cisco.com](https://Cisco.com) and uploaded to ISE. The agent is a native 32-bit Windows application that you can install manually or, a much cooler option, have ISE push the install to the server! That's right, you can install the agent remotely, with the click of a button in ISE's user interface.

The ISE-PIC agent is located under **Work Centers > PassiveID > Providers > Agents**. From this screen, shown in [Figure 23-13](#), you can manually register an agent, you can download the agent from ISE, you can upload a newer agent to ISE, and you can push the install of an agent to a server in the AD domain.

Name	Host	Monitoring
No data found.		

**Figure 23-13** ISE-PIC Agent Screen

**Deploying the Agent from ISE** Even though there is an Agents page in the ISE GUI for managing the existing agents and installing new ones, our experience has shown that it is a better experience to initiate the remote installation from the PassiveID tab within ISE's AD configuration itself. This way the configuration for the agent will be prepopulated and working immediately, not requiring you to log into the Windows server and add the list of domain controllers to be monitored.

To install the agent onto a Windows server remotely following this experience-based best practice:

**Step 1.** Navigate to **Work Centers > Passive ID > Providers > Active Directory > [join point] > PassiveID** tab.

**Step 2.** Select the Domain Controllers that you want to monitor.

**Step 3.** Click **Add Agent** , as shown in [Figure 23-14](#).

PassiveID Domain Controllers					
	DC Host	Site	IP Address	Monitor Using	
1 Selected	ATW-AD1.securitydemo.net	SemesterNet	10.1.190.103	WMI	
	ATW-AD2.securitydemo.net	SemesterNet	10.1.190.104	WMI	
	ATW-AD3.securitydemo.net	2ndSite	10.1.190.108	WMI	

**Figure 23-14** PassiveID Tab, Servers Selected to Be Monitored

**Step 4.** In the Agents dialog box, click the **Deploy New Agent** radio button and enter a name for the agent. A good practice is to name the agent for the server that it will be installed on; however, keep in mind that a single agent may be installed on a single server but monitor many domain controllers.

**Step 5.** (Optional) Enter a description, which is a good idea to remind you later why this agent exists.

**Step 6.** In the Host text box, enter the fully qualified domain name (FQDN) for the domain controller or member server to install the agent onto.

**Step 7.** Provide an AD username and password (not stored) for an account that has enough permissions to install the software onto the server. A Domain Admin account is preferable, to avoid chasing down odd permission issues. [Figure 23-15](#) shows a completed new agent screen.

The screenshot shows the 'Agents' dialog box with the following fields filled out:

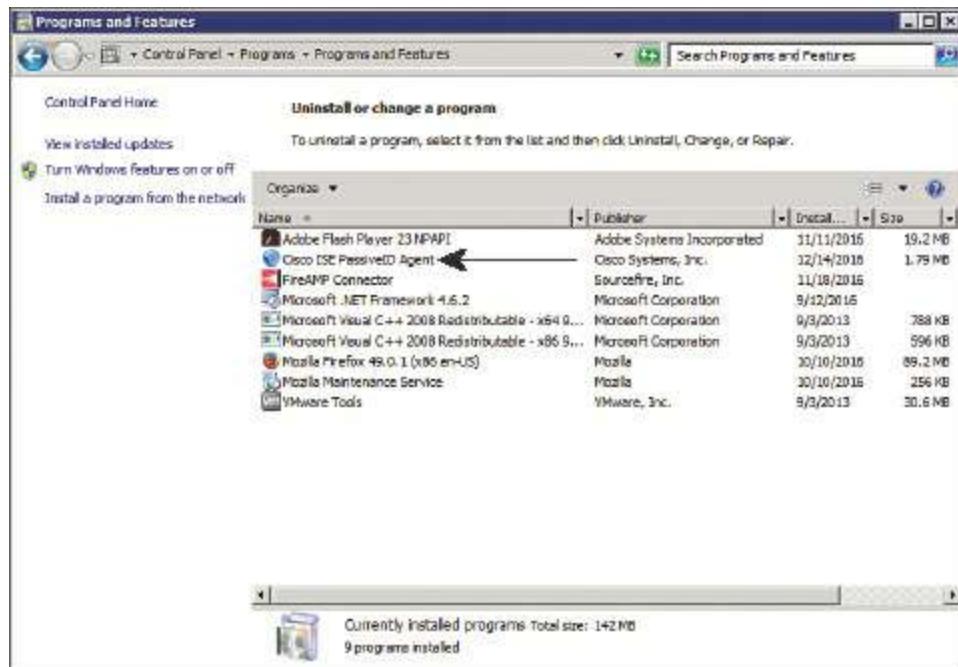
- Deploy New Agent** radio button is selected.
- Name**: ATW Member Server Agent
- Description**: Agent installed on atw-2k8-member that is monitoring all three domain controllers.
- Host**: atw-2k8-member.securitydemo.net
- User Name**: administrator
- Password**: (redacted)

At the bottom right are two buttons: **Cancel** and **Deploy**.

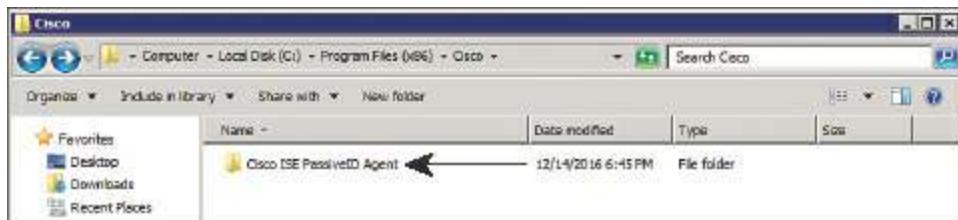
**Figure 23-15** Completed New Agent Screen

**Step 8.** Click Deploy.

At this point ISE logs in remotely to the server, copies the files to a temporary location, and installs the MSI package. All of this happens behind the scenes, without any interaction. To see if the installation completed successfully, leverage the Windows Programs and Features Control Panel applet, as shown in [Figure 23-16](#). You can also see that the application is installed under the C:\Program Files (x86)\Cisco\Cisco ISE PassiveID Agent\ directory, as shown in [Figure 23-17](#).

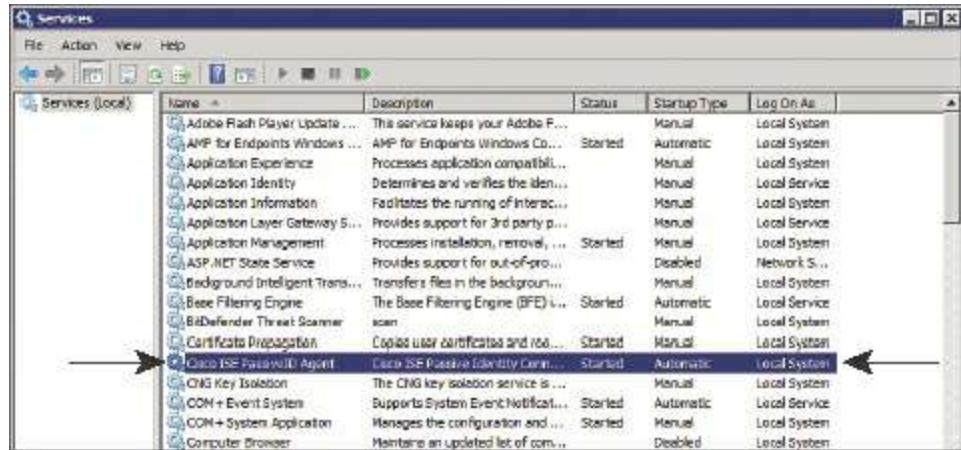


**Figure 23-16** Programs and Features: Cisco ISE PassiveID Agent Is Installed



**Figure 23-17** Program Files on the Windows Server Hard Drive

Additionally, you can view that the service was installed correctly and is running within the Services Control Panel applet. As shown in [Figure 23-18](#), the service is named Cisco ISE Passive Identity Agent; it should be started and configured to start automatically.



**Figure 23-18 Windows Services**

Back in the ISE GUI, the list of domain controllers will have changed from using WMI to using the recently added agent, as shown in [Figure 23-19](#).

Connection	Whitelisted Domains	PassiveID	Groups	Attributes	Advanced Settings
<b>PassiveID Domain Controllers</b>					
3 Selected				Rows/Page: 3	1 / 1
<input type="checkbox"/> Refresh	<input type="checkbox"/> Edit	<input type="checkbox"/> Trash	Add DCs	Use Existing Agent	Config WMI
<input checked="" type="checkbox"/> Domain	DC Host	Site	IP Address	Monitor Using	
<input checked="" type="checkbox"/> securitydemo.net	ATW-AD.securitydemo.net	ServerNet	10.1.100.103	ATW Member Server Agent	
<input checked="" type="checkbox"/> securitydemo.net	ATW-AD2.securitydemo.net	ServerNet	10.1.100.104	ATW Member Server Agent	
<input checked="" type="checkbox"/> securitydemo.net	ATW-AD3.securitydemo.net	2ndSite	10.1.104.100	ATW Member Server Agent	

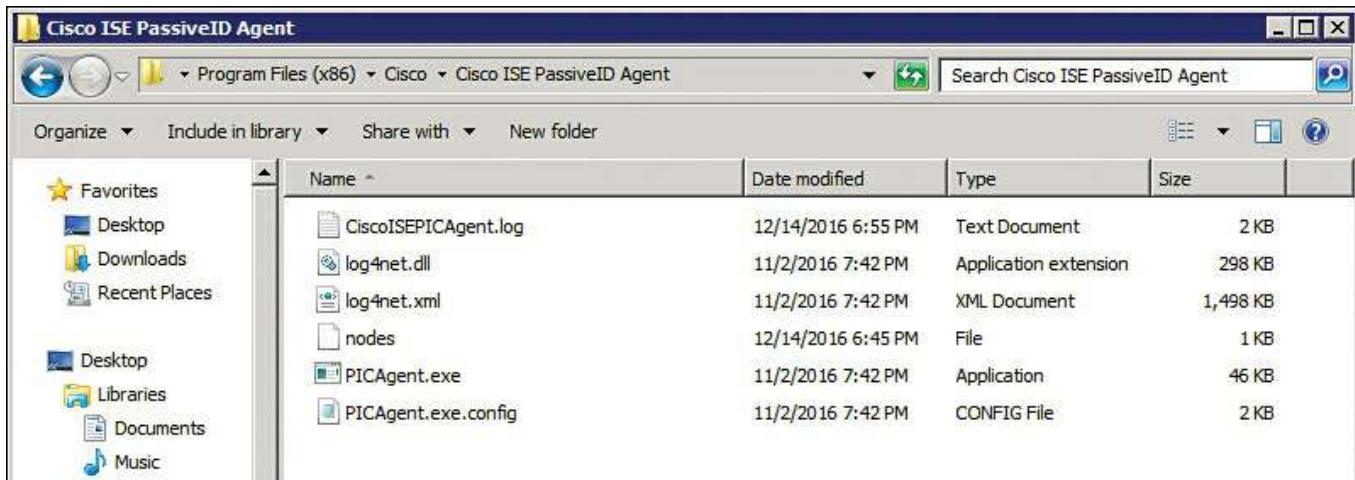
**Figure 23-19 PassiveID Tab, Servers Monitored by Agent**

There are some questions that must be burning in your mind right now: Is there a performance benefit to using the agent instead of WMI? Which method is better? Which approach should I use?

There is a bit of a performance benefit to using the native Windows application. Because it is a native process, running directly on the Windows server and leveraging local APIs for the WMI events, it does retrieve and consume those events more rapidly. However, at the time of writing, there are no official performance numbers to back up that statement.

Truthfully, there is no “better” solution; it is all a matter of preference and matching the needs of your environment. While the agent is very attractive, it does have one downside: EasyConnect only works with WMI in ISE version 2.2. So, any design leveraging the ISE-PIC agent with ISE version 2.2 will lose out on the capability to tie those passive identities into EasyConnect.

**Nodes File** [Figure 23-20](#) shows the contents of the agent’s program files directory. There are a few files to pay attention to, starting with the nodes file.



**Figure 23-20** Contents of the Cisco ISE Passive ID Agent Directory

The nodes file is a text file that lists all the ISE nodes it could be sending data to. The agent processes the list one line at a time, and if the communication generates an error, it moves to the next line in the list. Put another way, the agent sends updates to only one ISE node, and it uses this list to provide backup nodes.

[Example 23-1](#) shows the contents of a nodes file. You can see that it is simply a list of secure URLs, including the port (9095) that the agent uses to communicate to the ISE node.

### Example 23-1 Nodes File

[Click here to view code image](#)

```
https://atw-ise237.securitydemo.net:9095
https://atw-ise231.securitydemo.net:9095
https://atw-ise232.securitydemo.net:9095
https://atw-ise233.securitydemo.net:9095
```

When the agent starts, it picks up the list of nodes from this file. Any changes to the nodes file will not be noticed until the next time the service starts. So if you make any changes, restart the service to have those changes picked up.

The communication is always from the agent to ISE, in a typical client-server architecture. The agent reaches out to the ISE node every 10 seconds. This 10-second polling interval acts as a keepalive, informing ISE that the agent is still alive and well. The agent configuration will be provided from ISE during that same polling interval.

The agent reports the status of its connection to the monitored domain controllers once per minute. However, when the agent learns of a new mapping, that information is sent immediately to the ISE node.

**Note** When you deploy the agent from ISE as demonstrated previously in this chapter, the nodes file is preconfigured with the ISE nodes that have PassiveID enabled on them. However, if you perform a manual installation of the agent, you need to manually edit this nodes file and add the URLs for the applicable ISE nodes.

**Agent Configuration File** The PICAgent.exe.config file defines the logging level for the agent, which is set to INFO by default. It defines the name and location of the log file and the configuration of its maximum size, and the rollover setting for when the log file reaches that maximum size.

[Example 23-2](#) shows the default configuration of the agent.

**Example 23-2** PICAgent.exe.config

[Click here to view code image](#)

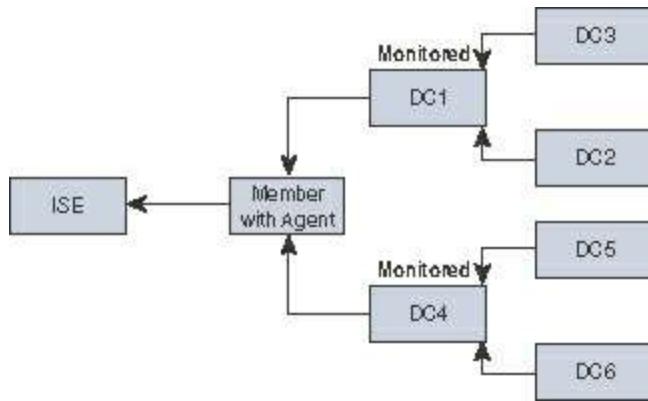
```
<configuration>
  <configSections>
    <section name="log4net"
      type="log4net.Config.Log4NetConfigurationSectionHandler, log4net"/>
  </configSections>

  <log4net>
    <root>
      <level value="INFO" />      <!-- Logging Levels: OFF, FATAL,
      ERROR, WARN, INFO, DEBUG, ALL -->
      <appender-ref ref="RollingFileAppender" />
    </root>
    <appender name="RollingFileAppender"
      type="log4net.Appender.RollingFileAppender">
      <file value="CiscoISEPICAgent.log" />
      <appendToFile value="true" />
      <rollingStyle value="Size" />
      <maxSizeRollBackups value="5" />
      <maximumFileSize value="10MB" />
      <staticLogFileName value="true" />
      <layout type="log4net.Layout.PatternLayout">
        <conversionPattern value="%date %level - %message%newline" />
      </layout>
    </appender>
  </log4net>

  <startup>
    <supportedRuntime version="v4.0"/>
    <supportedRuntime version="v2.0.50727"/>
  </startup>
</configSections>
```

**Design Fun** ISE version 2.2 supports monitoring events on 100 domain controllers. That is true of both WMI and the ISE-PIC agent. However, you should remember that a single agent can monitor more than one domain controller. This allows for a bit of fun when designing your passive identity deployment. Additionally, AD servers can be configured to forward event logs from one server to another, allowing consolidation. [Figure 23-21](#)

provides a crude sketch to illustrate this concept.



**Figure 23-21** Scaling Passive ID with Log Forwarding and Consolidation

For more on log forwarding, see the TechNet article at

<https://blogs.technet.microsoft.com/wincat/2008/08/11/quick-and-dirty-large-scale-eventing-for-windows/>.

## Kerberos Sniffing via SPAN

The WMI approach is pretty darn cool. It's tried and true, and certainly works like a charm. The ISE-PIC agent is a very nice enhancement that comes with ISE 2.2 and will certainly help with certain customers who don't want to allow remote WMI from ISE to their Windows devices. However, both of these options require the help of your Active Directory team to set up. That fact makes doing a quick test or proof of concept a bit more challenging. That is why ISE added a SPAN option to learn about the passive identities. It allows for a quick and easy installation and very fast time to value.

Cisco SPAN is a technology that is sometimes referred to as port mirroring or port monitoring. It takes network traffic being transmitted through a switch port and sends a duplicate copy of that traffic to a configured destination port so that packet analyzing solutions such as intrusion prevention systems (IPS) and network monitors may examine that traffic.

Simply configure the SPAN on the switch to copy the AD traffic going to the domain controller (the source) and send that over to the configured SPAN port on ISE (the destination). This could result in an awful lot of traffic being sent over to ISE, and it only needs to see Kerberos traffic. A trick of the trade is to use a VLAN ACL (VACL) to filter the traffic that is being sent to the destination SPAN port so that it only receives Kerberos traffic to analyze.

Configuring the SPAN interface on the ISE node is fairly straightforward. Navigate to **Work Centers > PassiveID > Providers > SPAN**. Enable the SPAN provider, and then select the ISE node(s) that SPAN should be enabled for. Once you select the node, the list of possible interfaces is displayed and you must select one. Then click **Save** and

you're done (on the ISE side).

[Figure 23-22](#) shows the SPAN configuration in ISE.

The screenshot shows the ISE interface with the 'Providers' tab selected. On the left, a sidebar lists Active Directory, Agents, API Providers, SPAN, Syslog Providers, Mapping Filters, and Endpoint Probes. The 'SPAN' section is currently active. In the main pane, there is a configuration form for a SPAN session:

- Description:** Sniff that Kerberos Traffic!
- Status:** Enabled
- Interface NIC:** atw-ise237 (selected)
  - GigabitEthernet 0
  - GigabitEthernet 1
  - GigabitEthernet 2** (selected)
  - GigabitEthernet 3

At the bottom right are 'Reset' and 'Save' buttons.

**Figure 23-22** SPAN Configuration

Both SPAN and VACL configuration are covered in [Chapter 10, “Profiling Basics and Visibility.”](#) For more detailed guidance on SPAN or VACLs, please check out the configuration guide for your Cisco switch at [Cisco.com](#).

## Syslog Sources

While Active Directory is the primary source for passive identities in the modern enterprise, AD and its use of Kerberos authentication for AD members is most certainly not the only game in town. There are many other authentications that can and do occur in a modern network. There could be other AAA servers, such as Cisco Secure Access Control System (ACS) or even FreeRADIUS, that are used to authenticate and authorize users accessing the network. Maybe VPN solutions are being used, such as Cisco ASA or F5 VPNs. Thinking more broadly, authentication could be occurring via web security appliances or web proxies that authenticate users through a web page or web prompt before allowing them to access the Internet.

Why not allow ISE to leverage the information from those systems to learn about users and their corresponding IP addresses, for the purposes of sharing that information? That is where syslog comes in. You can configure those products to send their logs to

ISE so ISE can learn about those users and add their information to the session directory for sharing. Beginning with ISE version 2.2, ISE has a generic syslog parser with some preconfigured templates for a variety of solutions on the market today.

It's not only user identities that can be learned through the ingestion of syslog. IP address management (IPAM) products such as Infoblox, BlueCat, and even Microsoft's DHCP server may provide very useful data that ISE can use to ensure the validity of the data in the session directory. When one of these solutions issues an IP address to a DHCP client, it logs the MAC address of the endpoint and the IP address that was assigned.

Those logs provide Layer 2 to Layer 3 bindings, so ISE can learn the MAC addresses that correspond to the IP addresses learned via passive ID methods. For instance, if the DHCP server assigns the IP address to a different MAC address, then ISE knows to invalidate the current passive authentication session.

## Configuring a Syslog Provider

This section covers the ISE side of the configuration. Don't forget, you need to configure your individual product to send its syslog messages to ISE on UDP port 40514 or TCP port 11468.

From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Work Centers > PassiveID > Providers > Syslog Providers**.

**Step 2.** Click **Add**.

**Step 3.** Enter a name for the provider.

**Step 4.** (Optional) Provide a description of what you expect to get from this provider.

**Step 5.** From the Status drop-down list, choose **Enabled**.

**Step 6.** In the Host text box, enter the FQDN or IP address that the provider will source the logs from.

**Note** This is a very important step. ISE uses reverse DNS to determine what hosts to allow through ISE's firewall to send the log messages. If there is a mismatch, the traffic will be dropped.

**Step 7.** From the Connection Type drop-down list, choose **UDP** or **TCP**.

**Step 8.** From the Template drop-down list, choose a syslog parsing template.

**Step 9.** (Optional) Provide a default AD domain to map the identities to. This is used when the domain cannot be identified within the syslog message.

[Figure 23-23](#) shows a completed example syslog provider.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, Overview, Providers, Subscribers, Certificates, Troubleshoot, and Reports. The 'Providers' link is currently selected.

The main content area is titled 'Syslog Providers > New'. On the left, a sidebar lists Active Directory, Agents, API Providers, SPAN, Syslog Providers (which is selected and highlighted in blue), Mapping Filters, and Endpoint Probes. The 'Syslog Providers' section contains the following fields:

- Name: ATW-ACS
- Description: ACS 5.8 node used for legacy dot1x deployment
- Status: Enabled
- Host: atw-ac.s.cisco.com
- Connection Type: UDP - Port 40514
- Template: ACS (with Edit and New buttons)
- Default Domain: securitydemo.net

At the bottom right are 'Cancel' and 'Submit' buttons.

**Figure 23-23** Example Syslog Provider

The template is critical to the success of your syslog provider. The template defines the regular expressions needed to identify the usernames and IP addresses from the log messages. You can edit or create a new template as needed. [Figure 23-24](#) shows an example of a template for a Blue Coat gateway that is preconfigured during a default install of ISE 2.2. The template UI even provides a location on the right side to paste a raw syslog message and allow the UI to show you the identified information, as a way to test the template.

Syslog Template

Name *	BlueCoat Proxy SG	
<b>Mapping Operations</b>		<b>Test Template</b>
New Mapping *	(\-lsPROXIED){1}	Paste one line of syslog
Removed Mapping		
<b>User Data</b>		<b>Data Identified</b>
IP Address *	\s((?:([0-9]{1,3})\.){3}[0-9]{1,3}) (\?:([a-zA-Z0-9]{1,4})\{1,2\}{1,7}[a-zA-Z0-9]{1,3})	User name
User Name	\s[0-9]{1,3}\.([0-9]{1,3})\.[0-9]{1,3}\.[0-9]{1,3}\s([a-zA-Z0-9\_]+)\s\-	IP Address
Domain		Domain
MAC address		MAC Address
		<b>Cancel</b> <b>Save</b>

**Figure 23-24** Example Blue Coat Template

## More Tidbits on Syslog Providers

The syslog parsing service matches the hostname from the message to that which the administrator previously defined in the GUI in order to identify the correct client template. Therefore, you should always ensure you have configured reverse lookup from the syslog client's IP address to hostname for the relevant DNS server(s).

To achieve high availability with syslog providers, you need to set up redundancy. In other words, configure the source to send syslog to two different ISE nodes. However, that means double the logs and a lot of added noise, not to mention duplication of information. Another option is to use Anycast or a load-balancer to provide that redundancy.

For more on Anycast, take a look at an example solution designed by E. Peter Karelis and detailed on Aaron Woland's blog:

<http://www.networkworld.com/article/3074954/security/how-to-use-anycast-to-provide-high-availability-to-a-radius-server.html>.

## REST API Sources

The final identity source to discuss is the representational state transfer (REST) API that ISE implements to allow custom-built applications to update ISE with usernames and IP

addresses. A simple use case might be a custom Guest solution in an enterprise. When a visitor arrives, she checks in with security and receives a visitor's badge and possibly guest credentials to access the Internet. When that guest user authenticates to that guest system, the user ID and IP address can be inserted into ISE's session directory via this REST API.

A more specific use case for the REST API is the Cisco Terminal Services (TS) Agent. This is a kernel-level agent that gets installed onto Microsoft or Citrix terminal servers and assigns each user a unique port range for all that user's network traffic. So now that allows a solution that normally has multiple users with the same IP address to have the users uniquely identified on the network. The TS Agent can be used directly with Cisco Firepower Management Center (FMC) or ISE, but obviously, FMC is out of scope for this book.

## Learning More Is Critical

A major function of the Learn tenet is to get more than just the information included in the syslog or the WMI message, because that raw information might only include a simple username that hasn't been normalized in a way that every consumer requires to consume the data equally. It also does not include other pertinent information that is needed for the subscriber to apply the correct policy to the user. For example, most subscriber products such as firewalls and web security appliances want to use the group membership of a user within their policy constructs. The groups would not be included in the passive identity messaging (WMI, Kerberos, syslog). Therefore, ISE must take the learned identity and retrieve the user's applicable groups from Active Directory and add that information to the session directory to be shared to the subscribers. In addition to the group membership, ISE also retrieves the following attributes from AD for username normalization:

- **User principle name (UPN):** user@domain
- **Distinguished name (DN):**  
CN=Administrator,CN=Users,DC=securitydemo,DC=net

Remember, the goal of an identity sharing solution is to become the source of truth for its subscribers. Those products shouldn't have to connect to AD separately to learn the groups of the user. If they did have to maintain that connection and do those lookups, then the identity sharing solution would be doing only partial work.

## Tenet 2: Share

All that power of learning which users are on the network and which addresses correspond to them is all for naught if that information can't be used. EasyConnect is an

example of ISE using the learned identity mappings within its own product. Yet, this is not about EasyConnect, it's about identity sharing! There are a lot of products that require the knowledge of those identities to make using their solution easier and better. Firewalls, web proxies, behavioral analysis systems—you name it—can all use this information. Why should each product be required to code its own version of this capability?

Let's take Cisco's security portfolio as an example. It includes many different products, and each one may have a different identity solution with completely different capabilities. The long-term goal and vision is to consolidate those solutions into a single solution, all using ISE.

For ISE, there can be two mechanisms to share that data to the products that subscribe to the information. The main method is through the Cisco Platform Exchange Grid (pxGrid). However, there was an older solution called Cisco Context Directory Agent (CDA) that used a modified RADIUS interface, and a few Cisco products communicate with CDA leveraging that modified RADIUS interface already.

## pxGrid

pxGrid is Cisco's premier publish/subscribe (pub/sub) communication bus that was designed from the ground up to be a scalable and secure data sharing system. pxGrid is covered in more detail in [Chapter 24](#), so we won't look at how to configure it in this chapter.

pxGrid is the primary mechanism that ISE uses to share identities and other contextual data to those products and solutions that subscribe to that data. For convenience and completeness, Cisco has added the relevant pxGrid configuration UI to the PassiveID Work Center, as shown in [Figure 23-25](#).

The screenshot shows the Cisco Identity Services Engine (ISE) PassiveID Work Center. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under Work Centers, there are links for Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, and PassiveID. The PassiveID link is highlighted. Below this, there are links for Overview, Providers, Subscribers (which is selected), Certificates, Troubleshoot, and Reports. The main content area is titled 'Clients' and includes tabs for Capabilities, Live Log, Settings, and Certificates. A toolbar at the top of the client list includes buttons for Enable, Disable, Approve, Group, Decline, Delete, Refresh, and Total Pending Approval(0). The client list table has columns for Client Name, Client Description, Capabilities, and Status. Two clients are listed: 'ise-admin-atw-ise237' and 'ise-mnt-atw-ise237'. Both clients are online and have specific capability counts listed under 'Capabilities'.

Client Name	Client Description	Capabilities	Status
ise-admin-atw-ise237		Capabilities(6 Pub, 2 Sub)	Online
ise-mnt-atw-ise237		Capabilities(2 Pub, 1 Sub)	Online

**Figure 23-25** pxGrid Configuration Interface

**Note** If you do not have pxGrid enabled yet, the UI will not display. You will need to come back to this part after performing the configuration in [Chapter 24](#), or enable pxGrid on the desired ISE nodes under **Administration > System > Deployment**.

When a product such as Cisco Stealthwatch connects to ISE with pxGrid, it subscribes to the topics that it needs. A topic could be the session topic, where the shared information from ISE's session directory is published for consumption by the subscribed products and applications. The product or application joins pxGrid and subscribes to the session topic, and then the pxGrid controller (ISE) authorizes and directs the subscriber to download the bulk session data from the MnT node (the publisher). When new information is discovered, it is published to the session directory and sent to the subscribers of that topic. This is a very elegant way to share such dynamic data at large scale while being proactive about notifying the interested parties of interesting data.

ISE uses pxGrid to share those identities and the list of interesting groups that the identity is a member of. It's designed to be a one-stop shop for identity, providing all the possible tenets. Unlike the older CDA product, a product that uses ISE for identity sharing should not ever have to leverage its own connection to the source of identity truth (like AD). ISE should be able to provide all the information instead. Keep in mind that although this is how ISE is designed, it is not always how the integrated products are designed to integrate; and each integration may have different levels of integration. You will see that more clearly in the "Tenet 3: Use" section.

## CDA-RADIUS

As previously mentioned, Cisco Context Directory Agent is an older solution that is used to provide passive identities to Cisco ASA, Cisco WSA, and a few other products. For ISE to be a drop-in replacement for CDA, ISE will have to support the same communication protocol used by CDA. CDA did not support pxGrid. Instead, CDA used a modified RADIUS interface, and any product that supported CDA would use that modified RADIUS protocol to pull the list of users and their IP addresses from the CDA appliance.

The CDA-RADIUS interface wasn't ready for release with ISE version 2.2, but is expected to be in the follow-on release. Since this book will not receive a third revision before that release is out, it is best to describe the CDA-RADIUS interface here.

Unlike ISE, when a product uses CDA for identity sharing, it must still have its own connection to the identity source to perform the additional lookups about the username that was shared. This means CDA will provide the username and IP address but won't

have group membership (for example).

### Tenet 3: Use

A product, such as a firewall or even a software-defined networking (SDN) controller, needs to know more than just which users exist on the network and which IP addresses they have assigned. That product needs a way to configure what level of access should be assigned to those users, and that policy creation must happen before users attempt to access the network.

Each product has some construct that permits this policy authoring. Perhaps it uses LDAP to query AD for which groups and users exist, and then builds the policy from that data. Then, once the information is received from pxGrid or CDA-RADIUS, the product can determine which level of access to assign through the firewall or the web gateway.

If an identity sharing product is to replace that integration, and prevent that product from having to have its own AD integration, then the identity sharing product requires APIs to provide that information. You may hear this type of API referred to as a management API or a metadata AP or even a policy authoring API. In this book, we refer to it as the metadata API.

ISE is able to provide that metadata API for AD user accounts and internal ISE accounts, including guest users. This information is provided through the External RESTful Services (ERS) set of APIs provided by ISE. ERS is enabled via

**Administration > System > Settings > ERS Settings**, as shown in [Figure 23-26](#). If you have more interest in understanding what is available with ERS, perhaps for your own custom integrations with ISE, the SDK is located on the ISE node itself, once you enable ERS itself, and is available at the following URL:

[https://\[ISE\\_IPAddress\]:9060/ers/sdk](https://[ISE_IPAddress]:9060/ers/sdk).

The screenshot shows the Cisco Identity Services Engine (ISE) administration interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, Threat C, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, Admin Access, and Settings. The 'Settings' link is currently selected. On the left, a sidebar menu lists Client Provisioning, FIPS Mode, Alarm Settings, Posture, Profiling, Protocols, Proxy, SMTP Server, SMS Gateway, System Time, Policy Sets, ERS Settings (selected), Smart Call Home, and DHCP & DNS Services. The main content area is titled 'ERS Settings' and contains a 'General' section with a note about the ERS service being disabled by default and requiring specific group assignments. It also includes an 'ERS Setting for Administration Node' section with a radio button for enabling ERS for Read/Write access. At the bottom are 'Save' and 'Reset' buttons.

**Figure 23-26** Enabling the ERS APIs

There are two key functions in this Use tenet: to get the information to build the policy, and to have ability to compare and match the information received from ISE via pxGrid or the CDA-RADIUS mechanisms with the information in their policies. In other words, they have to be able to bind the information received from the different sources to make it actionable. This might include the need to reach out to AD and get the list of groups that the user belongs to.

## Integration Details

This section reviews some of the key identity consumers (AKA subscribers) and the way in which they integrate.

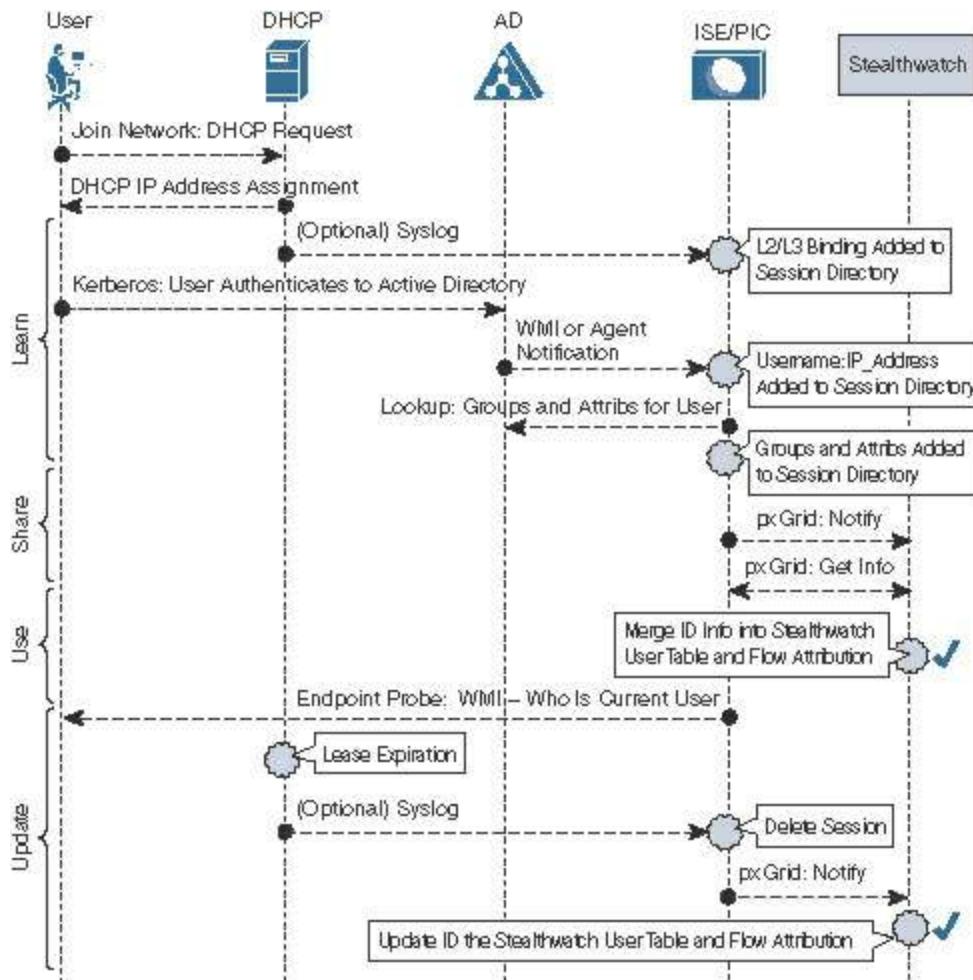
### Stealthwatch

Stealthwatch has been a long-time partner of ISE, long before Cisco acquired its developer, Lancope. The initial integration only used pxGrid to initiate endpoint quarantine. The identities were gathered by parsing syslog messages from ISE and learning about the active authentications that ISE authorized for network access. Lancope also had its own identity appliance prior to Cisco's acquisition of the company. Beginning with Stealthwatch 6.9, ISE becomes the single source of identity. It

could be either ISE or the ISE-PIC form factor, leveraging pxGrid as the communication mechanism.

When identities are sent to Stealthwatch, the session data is added to the user table and flow attribution. In other words, the identities are merged with all the identified network flows to provide usernames and context to those flows. Since Stealthwatch is a macro-analytical tool providing analysis of what has transpired and not a real-time traffic-regulating device like a firewall, there is no current need to have the metadata API for building policies prior to merging the live user data.

[Figure 23-27](#) illustrates the passive identity flow with Stealthwatch, leveraging pxGrid. Configuration steps for integrating Stealthwatch and ISE are covered in [Chapter 24](#).



**Figure 23-27 Day in the Life of Passive ID: Cisco Stealthwatch**

## Firepower Management Center

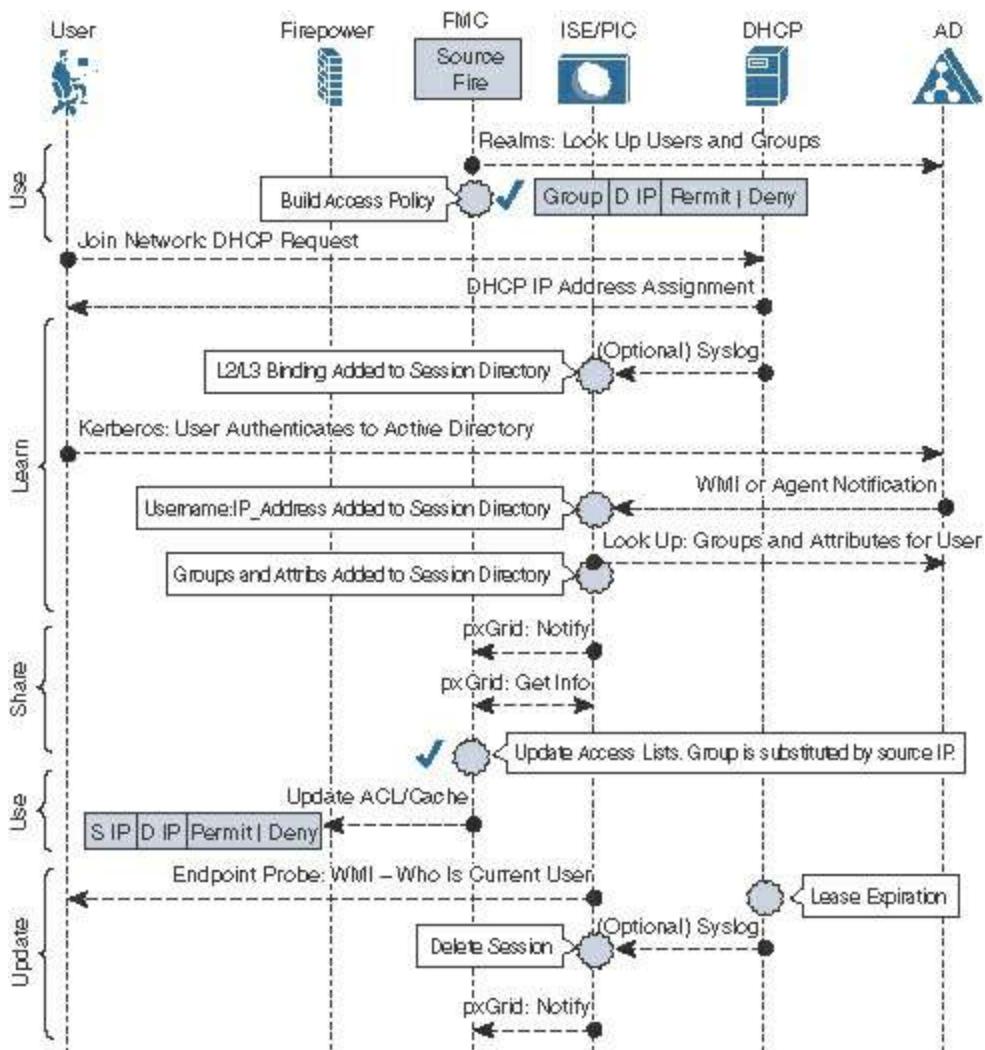
Firepower is an interesting solution when it comes to identity. There could probably be an entire chapter dedicated just to Firepower, because it had a fully functional identity sharing solution prior to the integration to ISE. That Active Directory identity sharing solution was named the Source Fire User Agent (SFUA).

Firepower Management Center (FMC) uses realms to provide the metadata for policy authoring. A realm configured for AD leverages LDAP to query for users, groups, and attributes. The policies are constructed using this data, and the passive identity and IP address bindings are sent from the SFUA to FMC, where the information gets added to the identity cache and sent to the Firepower appliances.

That was the old way. Starting with FMC version 6.2, the new way is to use ISE or the ISE-PIC form factor to replace the SFUA function.

The ISE integration is happening in phases. The first phase was to replace SFUA to provide the passive identities. However, the metadata is still coming from the realm configuration. At the time of writing, that is the state-of-the-art for ISE integration, and replacing the metadata API is a roadmapped item.

[Figure 23-28](#) illustrates the passive identity flow with FMC, leveraging realms and pxGrid. Configuration steps for integrating Stealthwatch and ISE are covered in [Chapter 24](#).



**Figure 23-28** Day in the Life of Passive ID: Firepower Management Center

## Web Security Appliance

The Web Security Appliance is an interesting consumer of identity. What makes it really intriguing is that it has support for both pxGrid and CDA-RADIUS, but as of WSA version 9.1.2, the capabilities are not equal.

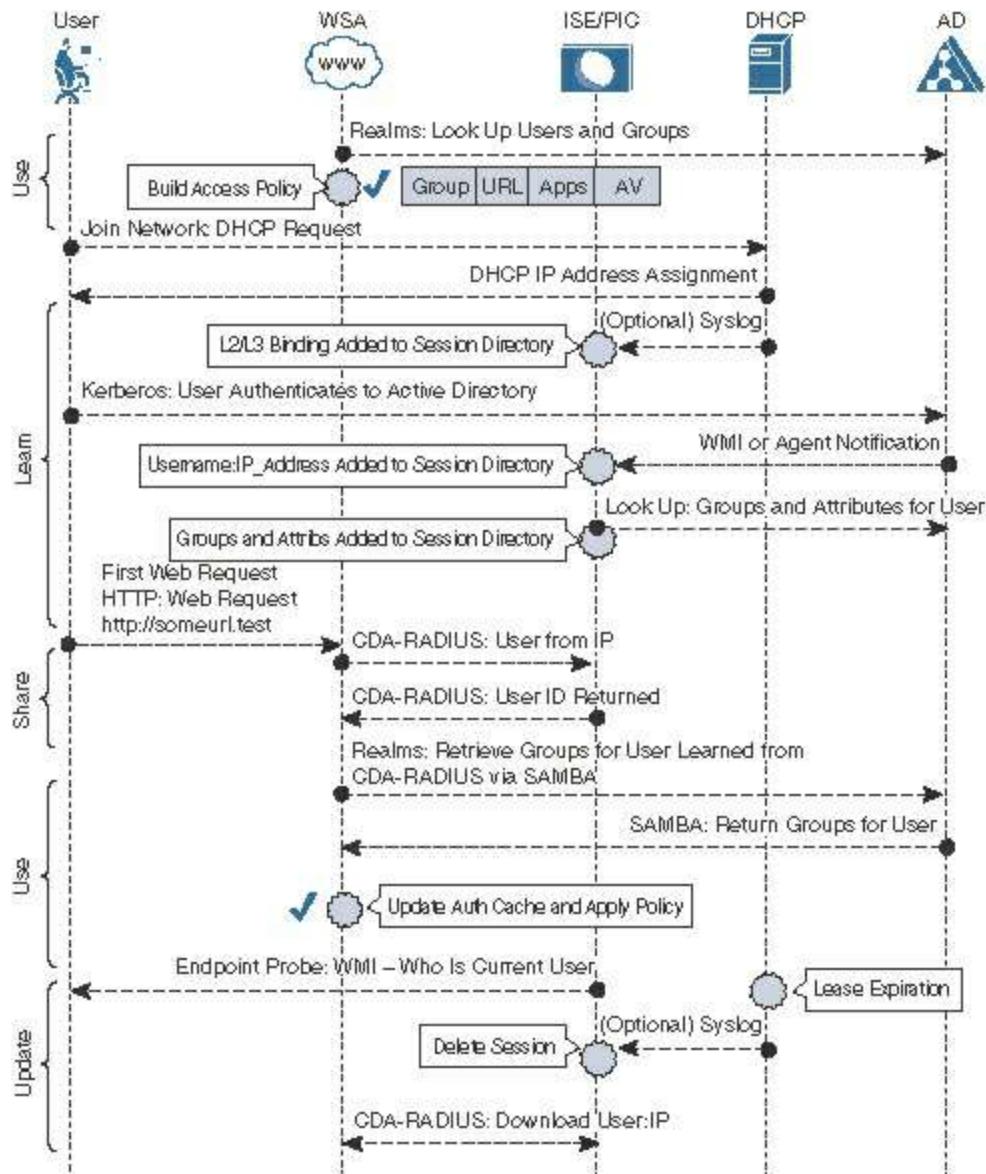
The WSA can leverage CDA. In fact, CDA was the main option for passive identity. Similar to the way Firepower works, the metadata comes from the realm configuration, but the passive identity and IP address bindings come from CDA. The user identities are stored in the Auth Cache on the WSA.

Interestingly enough, the WSA can also leverage pxGrid, but not for passive identity. The WSA's pxGrid integration with ISE does not leverage AD groups at all. Instead, it is a TrustSec integration only, leveraging the assigned Security Group Tag (SGT) for the user session only. If the session does not have an SGT, it cannot be used with the WSA. The exception to this rule is when the WSA's policy uses individual user accounts instead of AD groups or SGTs.

The TrustSec integration makes life simple, clean, and easy. However, the ISE-PIC form factor doesn't have any authorization support, including TrustSec, and therefore cannot be used with the WSA. Full ISE does have TrustSec authorizations and therefore would work perfectly with the WSA for this type of integration.

When ISE releases the CDA-RADIUS interface, you should be able to drop in an ISE node to replace CDA without worry. The WSA would still use the realms for metadata used in policy authoring, and use the CDA-RADIUS interface for the real-time binding.

[Figure 23-29](#) illustrates the passive identity flow with WSA, leveraging realms and CDA-RADIUS. The configuration steps for integrating the WSA using pxGrid with ISE are covered in [Chapter 24](#).



**Figure 23-29 Day in the Life of Passive ID: WSA**

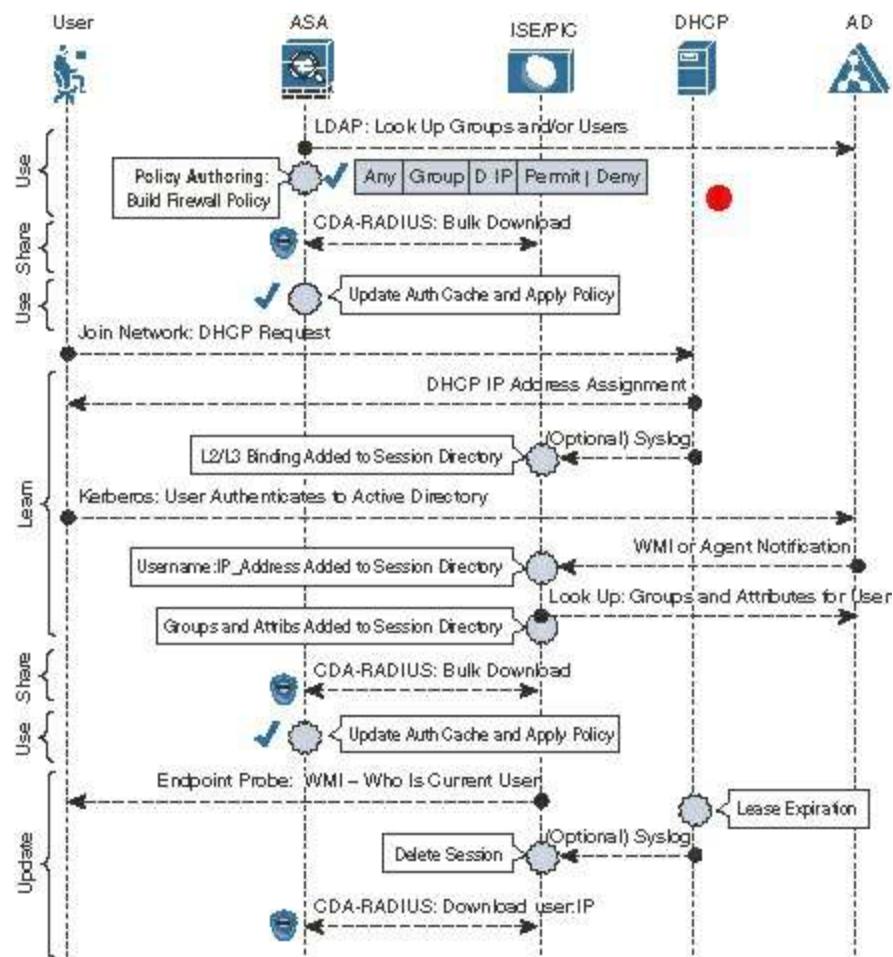
## Adaptive Security Appliance

The ASA is another interesting use case, particularly because it is entering another stage in its evolution. Most recently, the ASA is evolving into a Next-Generation Firewall platform, in the form of Firepower Threat Defense (FTD). So, the number of “classic ASA” being deployed has dropped off significantly.

If the ASA is an FTD appliance, the passive identity is integrated using Firepower Management Center, previously introduced. When the appliance is a classic ASA, then it requires the CDA-RADIUS interface.

The ASA is very similar to the WSA in how it integrates with an identity sharing solution. The ASA can and does leverage CDA. Similar to the way Firepower works, the metadata comes from an LDAP configuration, but the passive identity and IP address bindings come from CDA.

TrustSec integration is another option, but unlike FMC and WSA, the ASA does not learn about SGTs via pxGrid. The ASA can learn about TrustSec tags natively on the wire (in the Layer 2 frame) or through the Security group eXchange Protocol (SXP). Leveraging a tag is not passive identity and therefore is out of scope for this use case. For passive identity sharing, the ASA requires the CDA-RADIUS interface. [Figure 23-30](#) illustrates the passive identity flow with ASA, leveraging LDAP and CDA-RADIUS.



**Figure 23-30** Day in the Life of Passive ID: ASA

## Integration Summary

Stealthwatch, Firepower Management Center, WSA, and ASA are only four examples of integration. There are so many more that are expected within Cisco's product portfolio. Additionally, similar integrations exist within Cisco's security partner ecosystem, such as the integration between ISE and Infoblox, or ISE and Splunk.

## Tenet 4: Update

This tenet is meant to keep the data up to date and as valid as possible. You wouldn't want a firewall working off stale information and allowing the wrong user through. One

method to keep sessions up to date is to monitor the syslog messages from a DHCP server and see when the endpoint's lease expires or the IP address is assigned to a different MAC address. You saw this in the “Syslog Sources” section earlier in the chapter. Several other events and tools can be used to update the session data, including logoff detection, WMI updates, and session timeouts, all three of which are discussed in this section.

## Logoff Detection with the Endpoint Probe

Users do not always log off from their computers before leaving the network. Often, they just close the lid on their laptop and pack up for the day. ISE 2.2 introduces an endpoint probe to aid with logoff detection. The probe is designed to answer the burning questions: Is the endpoint still there? If so, is the same user logged in?

The endpoint probe uses WMI to remotely communicate with the endpoint and check if the user is still there. If the endpoint is on the network but WMI is not responding, ISE tries to remotely log into the endpoint using the saved Domain Admin credentials and enable WMI. If you chose to not save the credential when joining AD, then the endpoint probe will not function. If the endpoint is not there or if a different user is logged in, the session will be cleared.

Keep in mind that the endpoint probe relies on reverse-DNS to map IP addresses to hostnames, and the probe runs every four hours. If the endpoint is online but is not responding to WMI, then ISE remotely logs in with the saved Domain Admin credentials and enables WMI. This behavior is not configurable—if it is not desirable for your organization, the only option is to disable the endpoint probe.

ISE also allows you to map subnets to PSNs for the endpoint probe. This way you can design and plan which PSN is responsible for specific areas of your network. If a subnet does not exist in the list, then the endpoint probe will not operate in that subnet.

To add a subnet to PSN mapping, from the ISE GUI:

**Step 1.** Navigate to **Work Centers > PassiveID > Providers > Endpoint Probes**.

**Step 2.** Click **Add**.

**Step 3.** Name the endpoint probe and (optional) add a description.

**Step 4.** From the Status drop-down list, choose **Enabled**.

**Step 5.** From the Host Name drop-down list, choose the PSN.

**Step 6.** In the Subnets text box, enter the subnets in Classless Interdomain Routing (CIDR) notation (x.x.x.x/y), with a comma separating multiple networks.

**Step 7.** Click **Submit**.

[Figure 23-31](#) shows the creation of an endpoint probe, while [Figure 23-32](#) shows a

completed list of multiple probes assigned to their respective PSN.

The screenshot shows the ISE web interface under the 'Providers' section. On the left sidebar, 'Endpoint Probes' is selected. The main form is titled 'Endpoint Probes > New'. It contains the following fields:

- Name: 10\_1\_41-43\_Nets
- Description: The 10.1.41.0 - 43.0 Networks
- Status: Enabled
- Host Name: atw-ise243
- Subnets: 10.1.41.0/24, 10.1.42.0/24, 10.1.43.0/24

At the bottom right are 'Cancel' and 'Submit' buttons.

Figure 23-31 Creating an Endpoint Probe

The screenshot shows the ISE web interface displaying a list of endpoint probes. The table has the following columns: Name, Description, Status, PSN, and Number Of Subnets. The data is as follows:

<input type="checkbox"/>	Name	Description	Status	PSN	Number Of Subnets
<input type="checkbox"/>	172_16_Nets	The 172.16.0.0/16 Networks	Enabled	atw-ise237	1
<input type="checkbox"/>	10_1_40_net	The 10.1.40.0/24 Network	Enabled	atw-ise242	1
<input type="checkbox"/>	10_1_41-43_Nets	The 10.1.41.0 - 43.0 Networks	Enabled	atw-ise243	3

Figure 23-32 List of Endpoint Probes

**Note** The PSN to subnet mapping is only available with a full ISE install. When using the ISE-PIC form factor, configuration of the endpoint probe is limited to enabling and disabling only, as shown [Figure 23-33](#). The ISE-PIC GUI shown in [Figure 23-33](#) is discussed in the next section.

The screenshot shows the Cisco ISE Passive Identity Connector interface. The top navigation bar includes links for Home, Live Sessions, Providers, Subscribers, Certs, Active Directory, Agents, API Providers, SPAN, Syslog Providers, Mapping Filters, and Endpoint Probes. The 'Endpoint Probes' tab is selected. Below the tabs, the title 'Endpoint Probes' is displayed. A note states: 'Endpoint probes check if learned logged-in users are still present on their respective endpoints. The service is enabled by default.' There are two radio buttons: 'Enabled' (selected) and 'Disabled'. At the bottom are 'Reset' and 'Save' buttons.

Figure 23-33 Endpoint Probe in the ISE-PIC User Interface

## WMI Update Events

As described previously, Kerberos ticket renewals generate WMI events and keep the session alive. Other WMI events can also renew the session, show an actual user logoff, and expire the session when that logoff occurs.

## Session Timeouts

All entries in the session directory will expire and be purged at a configured interval between 1 and 24 hours. If no qualifying events or activity has been seen, then ISE removes those inactive sessions. The session timeout is configurable under the Advanced Settings tab of your AD join point, as shown in [Figure 23-34](#). The purge timer is called User Session Aging Time.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The 'Administration' tab is selected. The left sidebar lists Active Directory, Agents, API Providers, SPAN, Syslog Providers, Mapping Filters, and Endpoint Probes. The main pane shows the 'PassiveID' tab. Under 'PassiveID Settings', there are fields for 'History Interval' (set to 10 minutes) and 'User session aging time' (set to 24 hours). A note below says 'Note: Changes apply only for new connections'. At the bottom are 'Save' and 'Reset' buttons.

Figure 23-34 User Session Aging Time

## ISE Passive Identity Connector

ISE version 2.2 introduces a new form factor to the world that is designed for passive identity sharing only. It's known as a form factor and not a persona because it's a standalone model known as the ISE Passive Identity Connector (ISE-PIC).

Cisco created ISE-PIC to provide a low-cost offering of the passive identity sharing capabilities within ISE for Cisco products to consume. Yes, it is still ISE, but the low-cost PIC license disables most of what comes with ISE, leaving only the services required for passive identity sharing enabled. Not only does it limit the services that run, it wraps this all up into a nice, simple, lightweight installation package and user interface. [Figure 23-35](#) shows the ISE-PIC user interface.

The screenshot displays the ISE Passive Identity Connector (ISE-PIC) user interface. At the top, there is a navigation bar with links for Home, Live Sessions, Providers, Subscribers, Certificates, Troubleshoot, Reports, Administration, Settings, and License Warning. The main content area is titled "PASSIVE IDENTITY METRICS" and includes four summary cards: Sessions (1004), Providers (3), Agents (0), and Subscribers (4). Below these cards are two tables: "PROVIDERS" and "SUBSCRIBERS". The "PROVIDERS" table lists three entries: ATW-AD.security..., ATW-AD2.security..., and ATW-AD3.security... under the columns Name, Domain, and Type. The "SUBSCRIBERS" table lists four entries: ise-admin-atw-ise233, ise-admin-atw-ise234, ise-mnt-atw-ise233, and ise-mnt-atw-ise234 under the columns Name, Status, and Description. To the right of these tables is a section titled "TOTAL COMPROMISE" which is currently empty. Further down the page are sections for "OS TYPES", "ALARMS", and "ENDPOINT CATEGORIES". The "OS TYPES" section shows two entries: "cisco identity services engine" and "windows server 2008 r2 enterprise". The "ALARMS" section shows two active alarms: "Configuration Changed" (Severity: Informational, Occurred: 12 times, Last Occurred: 8 mins ago) and "CA Server Is down" (Severity: Critical, Occurred: 1 time, Last Occurred: 16 mins ago). The "ENDPOINT CATEGORIES" section has tabs for "Identity Group", "Policy Service Node", and "OS Types", with "Identity Group" currently selected.

Figure 23-35 ISE-PIC User Interface

As you can see in [Figure 23-35](#), the UI is basically just the PassiveID Work Center brought to the top level of the ISE menu system. Remember, ISE-PIC is a standalone deployment. It doesn't get added to an ISE cube. All the functions already exist in ISE and are enabled on a per-node basis. However, ISE-PIC does provide for redundancy by allowing for a secondary node to be added. Unlike a full ISE install, because there are so few options available to the administrator, the registration process is simplified even more. There is no need to import each node's certificates into the trusted certificate store like you must with full ISE. Instead, when joining the second node, the UI prompts you to accept the untrusted certificate, just like when you try to go to a new HTTPS website.

[Figure 23-36](#) shows the deployment screen and the fields for adding a secondary node, but none of the options for selecting services are there because it is ISE-PIC. [Figure 23-37](#) shows the UI prompting the admin to accept the secondary node's certificate.

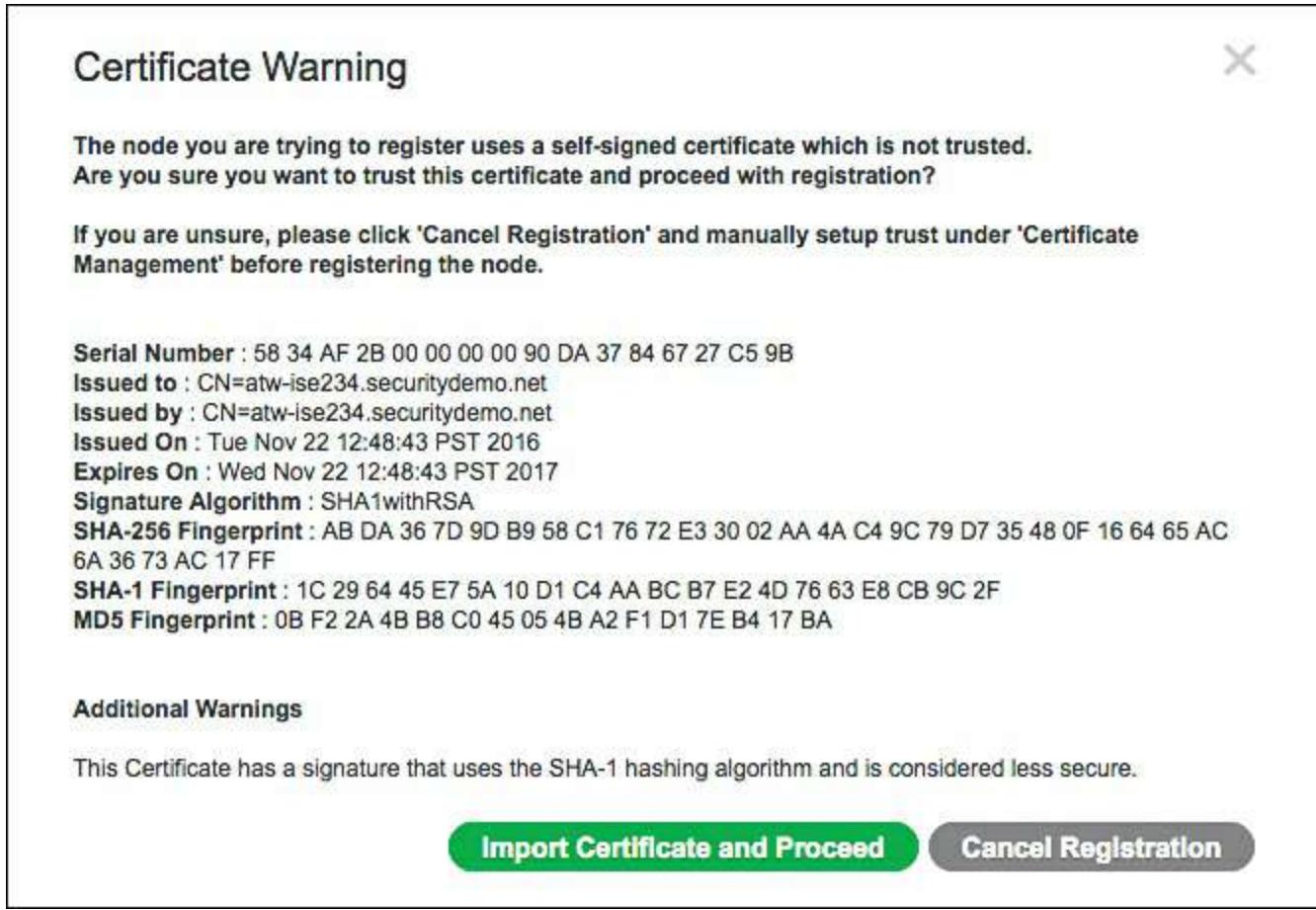
The screenshot shows the Cisco ISE Passive Identity Connector interface. The top navigation bar includes links for Home, Live Sessions, Providers, Subscribers, and Certificates. Below the navigation is a breadcrumb trail: Deployment > Licensing > Logging > Maintenance > Admin Access. A section titled "This Node" displays the current node's configuration: Role (Standalone), IP Address (10.1.100.233), and FQDN (atw-ise233.securitydemo.net). Below this, a "Add Secondary Node" section contains three input fields: FQDN (atw-ise234.securitydemo.net), User Name (admin), and Password (\*\*\*\*\*). At the bottom right are "Cancel" and "Save" buttons.

Role	Standalone
IP Address	10.1.100.233
FQDN	atw-ise233.securitydemo.net

**Add Secondary Node**

FQDN *	atw-ise234.securitydemo.net
User Name *	admin
Password *	*****

**Figure 23-36** Adding a Second ISE-PIC Node



**Figure 23-37** Accepting a Certificate

It's important to understand that, under the covers, ISE-PIC is still just ISE. Remember, it is a simpler and smaller install of ISE with only what is required for passive identity sharing enabled. It has no authentication, authorization, access control, device administration, or TrustSec. It still includes pxGrid, because it is required for sharing the identities. However, it only works for Cisco subscribers such as Stealthwatch and Firepower. Non-Cisco subscribers such as Splunk or Check Point would require Plus licenses to subscribe and integrate with pxGrid, which means you need a full ISE install.

Some good news: because ISE-PIC is still ISE under the covers, it is a simple license install to upgrade an ISE-PIC node to a full ISE node. Install the right license(s) and you can join a full ISE cube, separate out the functions and spread them across multiple nodes for scale and design elegance, and perform identity and context sharing with any pxGrid subscriber.

ISE-PIC has a separate installation ISO or Open Virtual Appliance (OVA), which exists to enable better tracking of downloads and usage for Cisco.

## EasyConnect

EasyConnect extends the concepts of passive identity and by providing network

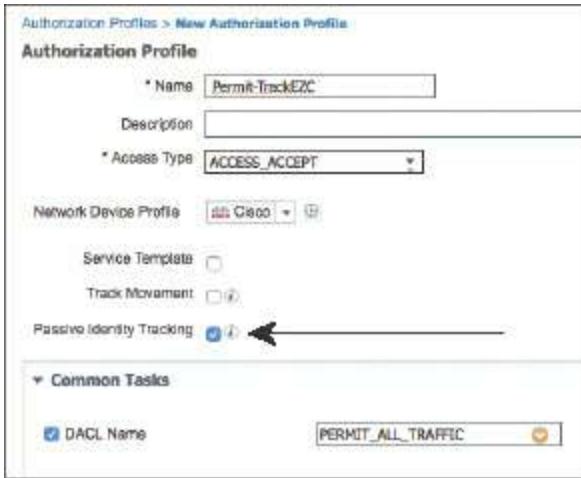
authorization without requiring 802.1X on the endpoints. Active Directory logins are used to map user information to network connections, which is then used for authorizing users on the network even when ISE is not involved in the user authentication process. EasyConnect can be used as a backup authentication method or way to add a second level of identity.

Some customers use EasyConnect as a stepping stone toward a full 802.1X environment. They use EasyConnect in some locations to provide network access control before the supplicant is fully deployed on all endpoints. The deployment is capable of mixed authorizations, so as the desktop team rolls out the supplicant configuration to the managed endpoints, both dot1x-capable systems and non-dot1x-capable systems can coexist.

The following are some basic concepts about EasyConnect (EZC):

- EZC requires a network authentication, usually MAB.
- EZC is for Microsoft AD joined computers—Windows only.
- EZC identity is based on AD user login, not AD machine login.
- It is possible to combine authentications:
  - Combine MAB identity (endpoint MAC address) with EZC—this is the most common use of EZC.
  - Combine 802.1X machine authentication with EZC user information for a dual-factor authentication.
- EZC requires an AD login event to be processed from the endpoint to AD. If access to the domain controllers is not permitted at time of user login, EZC will fail.
- The network access devices (NADs) are not configured any differently:
  - They must still process network authentications (MAB and 802.1X).
  - ISE must still be configured as the RADIUS server.

When a machine joins the network, a MAB is processed. The authorization result must include the Passive Identity Tracking option, such as shown in [Figure 23-38](#).

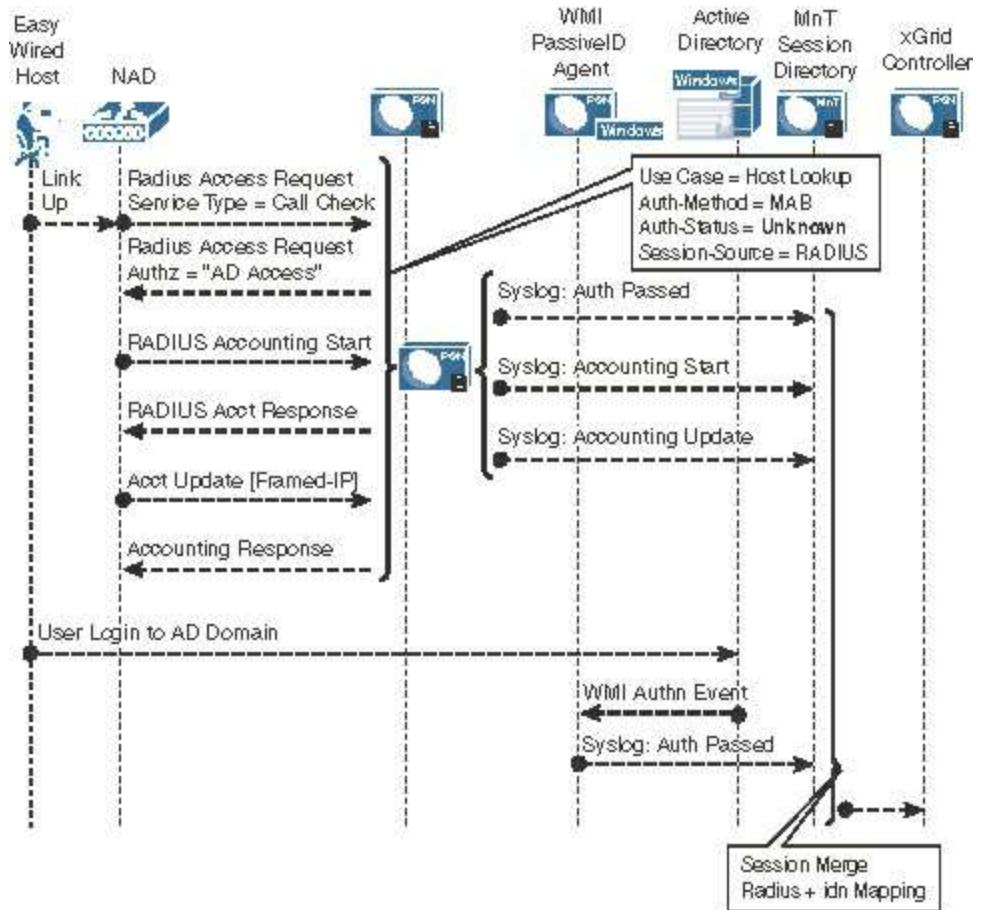


**Figure 23-38** Authorization Profile with Passive Identity Tracking Enabled

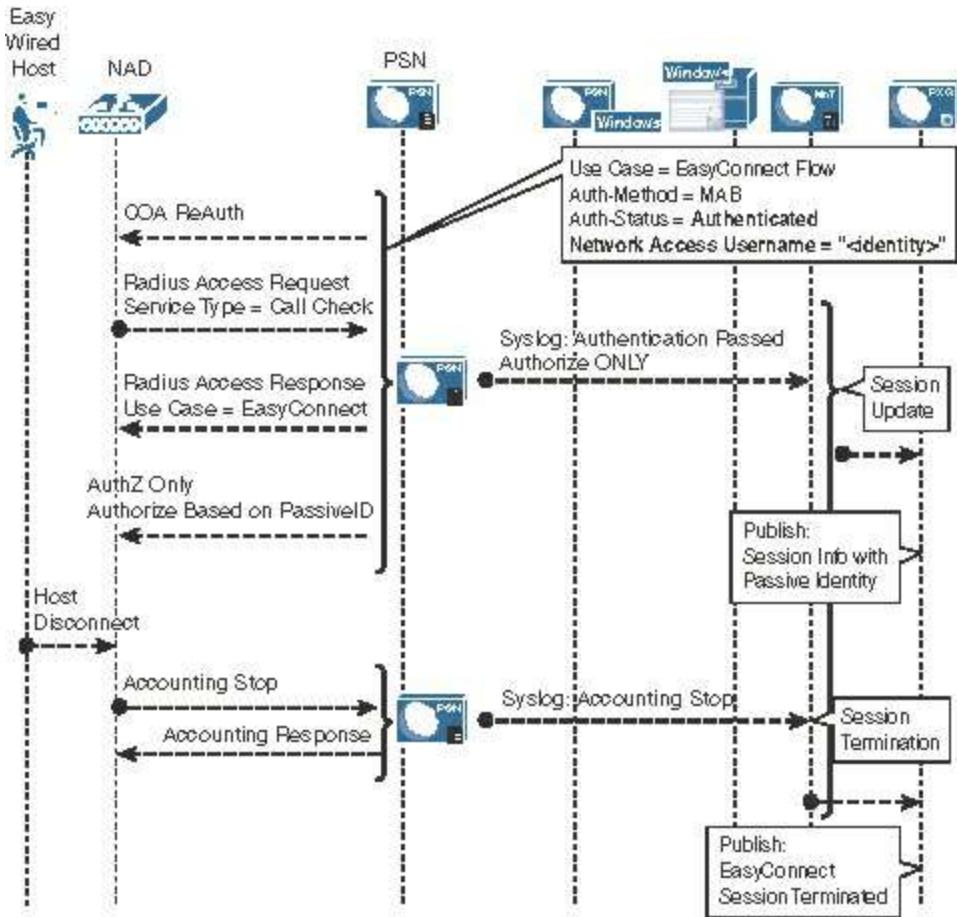
When a network session is authorized with this flag, ISE monitors the session and looks for WMI events that leverage the same endpoint ID (MAC address), to stitch the passive identity together with the network session.

After the WMI event for that endpoint is stitched together, a CoA-Reauth is sent to the NAD and a new authorization result may be applied that is based on the combined authentication (MAB + EZC).

[Figures 23-39](#) and [23-40](#) show the EasyConnect flow leveraging MAB for the network session.



**Figure 23-39** EasyConnect Flow with MAB



**Figure 23-40** EasyConnect Flow with MAB (Continued)

## Summary

In this chapter, you learned all about the importance of identity sharing and the difference between active and passive identities. You learned about all four tenets of a complete identity sharing solution: Learn, Share, Use, and Update.

You examined ISE's Active Directory integration with WMI and the ISE-PIC agent, saw how easy it is to configure WMI on the domain controllers from the ISE GUI, and how to push the agent installation to domain controllers and member servers.

You were introduced to EasyConnect as an alternative method of providing network access control and as a new method to provide dual-factor authentication.

You examined the basic premise of pxGrid for identity sharing and compared it to the legacy CDA-RADIUS methods. The next chapter dives much deeper into pxGrid, context sharing, and using ISE as the center of a security ecosystem.

# Chapter 24 ISE Ecosystems: The Platform eXchange Grid (pxGrid)

This chapter covers the following topics:

- The many integration types of the ecosystem
- pxGrid in action

Because Cisco ISE is positioned to know exactly who and what is on the network at any given time, as well as assign different levels of access and context assignments with Security Group Tags (SGT), it is the perfect security tool to be at the center of a security ecosystem.

There are many tools that exist within your “security toolkit”: firewalls, next-generation firewalls (NGFW), intrusion prevention systems (IPS), NG-IPSSs, security information and event management (SIEM) systems, secure web gateways, threat defense tools, vulnerability assessment scanners, mobile device managers, and more.

Most of these tools do not know the identity of the user, only the identity of the endpoint. These other tools can be made even more valuable by integrating into a full security ecosystem with ISE. Wouldn’t the reporting in the SIEM be more valuable if it showed which user was involved in the security event, instead of only the IP or MAC address? What about when your intrusion prevention tools or threat defense solutions identify malicious activity on the network? Wouldn’t it be great if they could trigger something that would change the way the endpoint was treated on the network? With a single “trigger,” the endpoint’s level of network access can be changed, the endpoint’s traffic can be inspected deeper as it passes through a Cisco Adaptive Security Appliance (ASA), the Cisco Web Security Appliance (WSA) can apply a different SSL decryption policy, and so much more.

You’ve already read about ISE integrating with mobile device managers (MDM), and how ISE can provide passive identities to ecosystem partners; it can also provide the single point of policy control for threat containment and context setting.

## The Many Integration Types of the Ecosystem

An integration of ISE can take multiple forms, where data (referred to as context) may be received into ISE or shared out of ISE. Generally, the integrations can be classified in one of three ways:

- **Context Sharing:** The endpoint and user attributes known to ISE are shared outbound to partner applications to consume.
- **Context In:** ISE is learning new attributes about users and endpoints used to further enhance ISE’s own authorization capabilities.

- **Context Brokering:** ISE is being used as a transport medium to communicate security data from one system to another system.

## MDM Integration

In [Chapter 17](#), “[BYOD: Self-Service Onboarding and Registration](#),” you read all about BYOD and the integration between ISE and mobile device managers. That integration is two-fold. ISE provides the redirection to the MDM service for onboarding, but the MDM is also able to provide “context in” to ISE. In other words, the MDM tells ISE about the mobile endpoints, its compliance with the policies for the endpoint, the status of encryption or pin lock, and more.

This integration uses a specific bidirectional application programming interface (API) between ISE and the MDM (cloud service or appliance). This API is unique, and created just for MDM integration.

For more on MDM integration, refer to [Chapter 17](#).

## Rapid Threat Containment

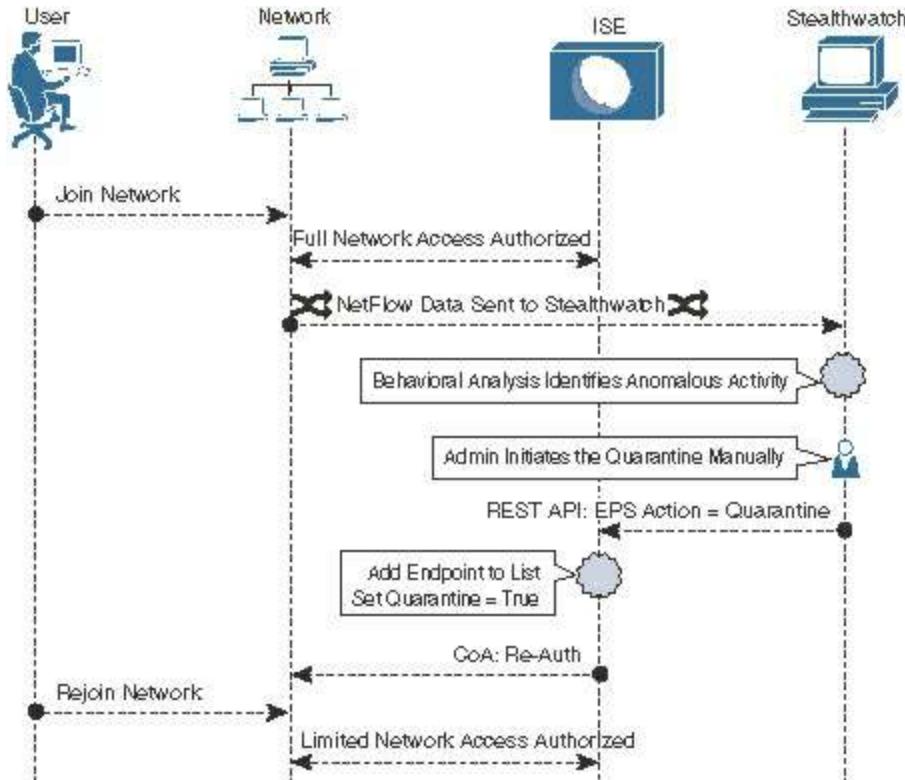
MDM integration is one of the first and most common integration types for ISE. In true Cisco marketing fashion, Cisco Rapid Threat Containment has gone through many different names and marketing initiatives. This section describes the evolution of Rapid Threat Containment.

The roots of Rapid Threat Containment begin back in ISE 1.1, with the addition of a new feature called Endpoint Protection Services (EPS). EPS provided an API allowing other applications to initiate three actions against an endpoint based on IP address or MAC address:

- **Quarantine:** Set the binary flag on the endpoint record to “true,” added the endpoint to a list of quarantined endpoints, and allowed the administrator to create authorization policies that used that assignment to assign a different level of network access.
- **Unquarantine:** Removed the endpoint from the list of quarantined endpoints and cleared the binary flag.
- **Shutdown:** Was supposed to send a CoA Terminate to the network and shut down the port on the network switch. Note: This option existed in the API, but it is not exposed to the policy and is therefore not usable.

Many of the first integrations with ISE used EPS, including the original integration with Lancope StealthWatch (now Cisco’s Stealthwatch)—where an endpoint is quarantined from the StealthWatch user interface.

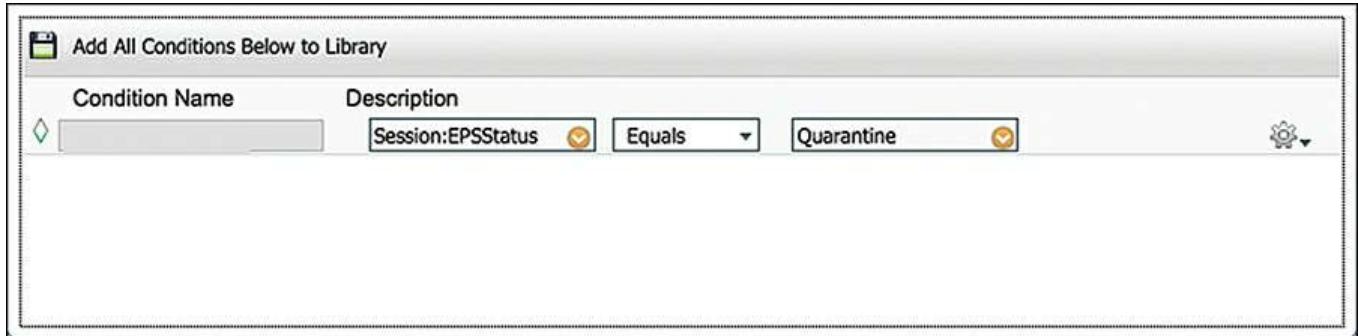
[Figure 24-1](#) illustrates a flow with Stealthwatch initiating an EPS quarantine.



**Figure 24-1** Stealthwatch to ISE—EPS Quarantine

The flow illustrated in [Figure 24-1](#) shows an endpoint being admitted to the network with full access. The Stealthwatch admin initiates a quarantine, and Stealthwatch connects to ISE using the EPS REST API, telling ISE to quarantine the endpoint with the specific IP address. ISE then adds the endpoint to the EPS list and sets the flag on the endpoint object, and sends a CoA to the network.

When the new access request comes in, a rule created with the EPSStatus condition will be matched. [Figure 24-2](#) shows that condition.



**Figure 24-2** EPSStatus Authorization Condition

The resulting network authorization may provide for limited access, or even set a new SGT that can be acted upon differently at miscellaneous points in the network, such as the WSA.

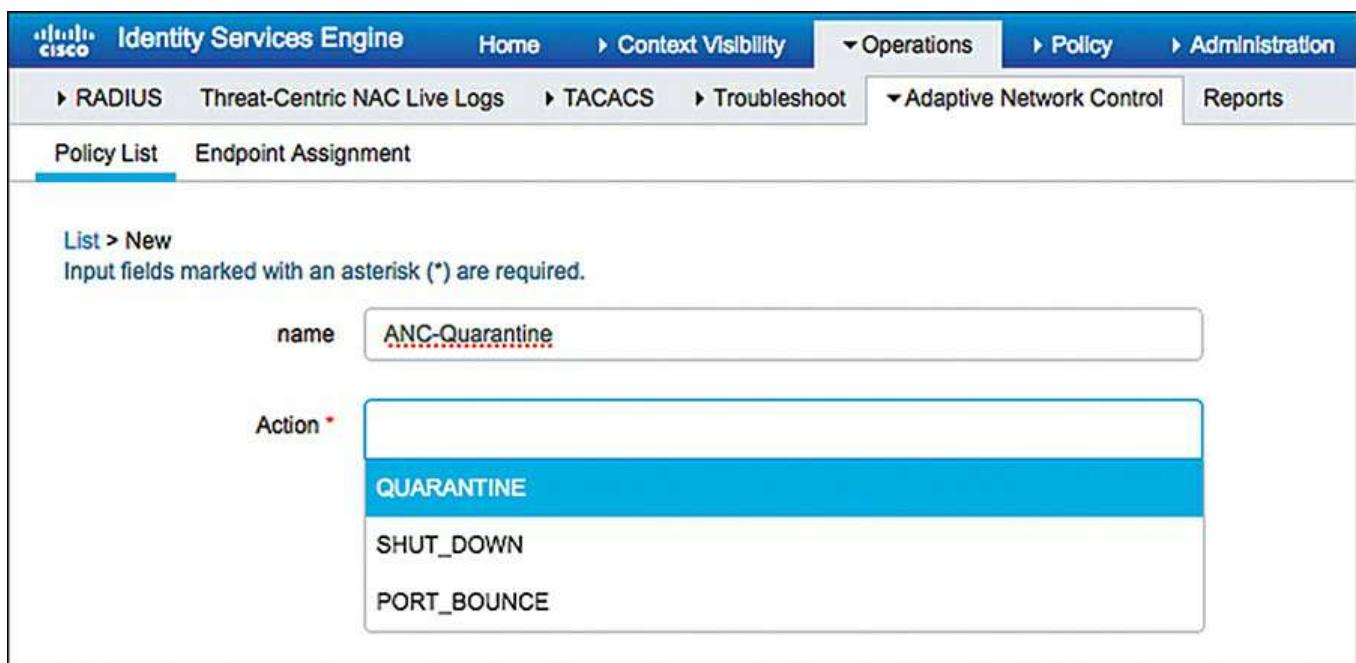
Well, ultimately EPS was just too rigid. It only provided for a single actionable

classification (quarantine). More flexibility was needed, not only to provide many different options, but also to integrate into the new-fangled context-sharing technology that Cisco was creating named the Platform eXchange Grid (pxGrid). So, EPS needed to evolve into EPS 2.0 or something like it.

In response, in ISE 1.3, Cisco introduced something new named Adaptive Network Control (ANC). A huge step forward? Alas, it amounted to simply renaming EPS to ANC. ISE 1.3 didn't improve anything.

ISE 1.4 actually added new functionality to ANC. It still supported the old EPS API calls for backward-compatibility purposes, but it also added a new API with different classifications available, including the ability to create your own classification. With ANC, each classification can correspond to a different action. Although you can add many different classifications, there are really only three choices for classification types: Quarantine, Shut Down, and Port Bounce.

To create an ANC policy (AKA classification), navigate to **Operations > Adaptive Network Control > Policy List**, and click **Add**, which opens the options shown in [Figure 24-3](#).



**Figure 24-3** Adding an ANC Policy

You can create multiple ANC policies, and each policy can contain one or more actions. Each ANC policy can be associated to a different authorization. For example, you can end up with ANC policies such as

- Investigate
- Black Hole

- Eradicate
- Nuke from Orbit

In addition to a much more flexible approach to classification, or as Cisco's legendary Paul Forbes would call it, "flexible name spaces," ANC also integrates tightly with pxGrid, enabling pxGrid subscribers to trigger the ANC action within the pxGrid connection, not through the point API of the past.

So, Endpoint Protection Services was renamed to Adaptive Network Control. Then ANC got new functionality in ISE 1.4. Then Cisco security marketing got involved and came up with a new naming convention to refer to the entire integrated security system where any Cisco security product takes action through another Cisco security product. That name is Rapid Threat Containment. You now have solutions such as Rapid Threat Containment with Cisco Stealthwatch and the Identity Services Engine and Rapid Threat Containment with Cisco Firepower Management Center and Identity Services Engine.

Crystal clear, right?

## Platform Exchange Grid

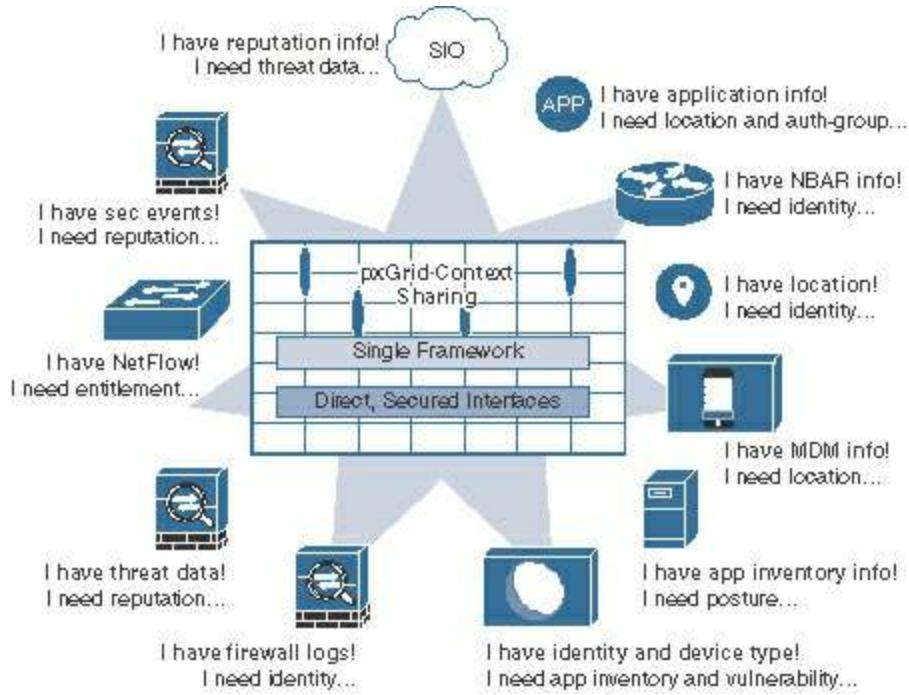
pxGrid is Cisco's premier publish and subscribe (pub/sub) communication bus that was designed from the ground up to be a scalable and secure data sharing system.

Like most other next-generation AAA solutions, ISE originally started sharing information through the use of APIs. It was quickly recognized that point APIs would not scale to the level of data that needed to be shared and the scale at which it was requested.

Cisco went down the path of a pub/sub bus, similar to the way Call Manager and Jabber work. There is a controller that keeps track of all the topics that exist. A topic is a list of information that is available. A topic might be session data of who and what is on the network, for example, or it might be a list of vulnerable endpoints and the list of those vulnerabilities.

pxGrid participants can subscribe to any topic of interest, after which they are notified when there is data for that topic to be retrieved. Those participants are known as subscribers. The true source of the data can be any other pxGrid participant, collectively known as publishers. A publisher registers the topic with the controller, who performs the authorization for each subscriber to retrieve the data from the many possible publishers.

[Figure 24-4](#) shows the standard Cisco illustration that is often used to explain pxGrid. You can see the many different types of products, each one of which has different information to publish and needs information from one of the other products.



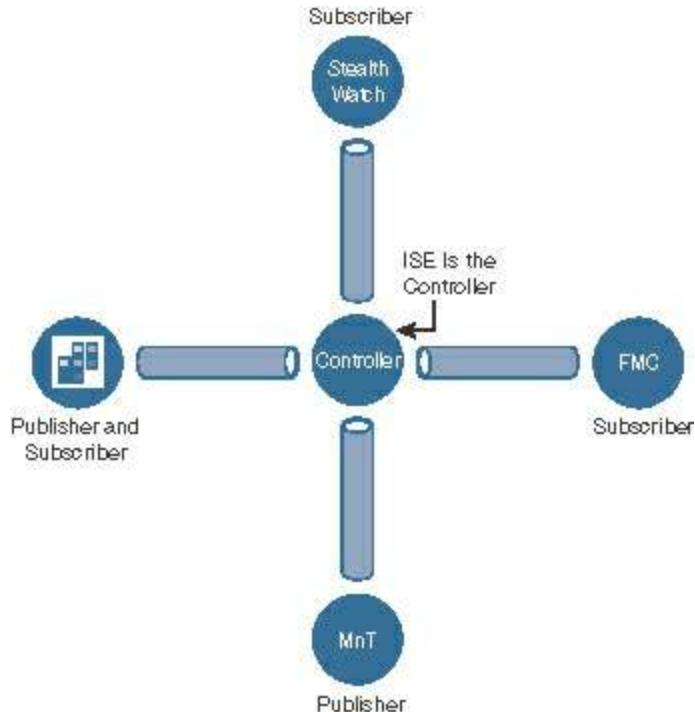
**Figure 24-4** Standard Cisco pxGrid Illustration

pxGrid was initially added to ISE in version 1.3, so it's been around for a while now and has an ecosystem of partner applications that continues to grow at a very rapid pace.

ISE 2.2 makes great strides in enhancing pxGrid. Most of the pxGrid-related enhancements support ease of use, making it even easier to configure and maintain. ISE 2.2 also adds more information into ISE's pxGrid topics for consumption by the subscribers. It includes data such as the list of groups that each user is a member of, all shared within the same topics that were used in the past, which enables smooth backward compatibility.

pxGrid was designed by extending the Extensible Messaging and Presence Protocol (XMPP), which is also the communication protocol used by Jabber. In fact, the pxGrid controller is a modified Extensible Communication Platform (XCP). For more on XMPP, see <https://www.xmpp.org>.

**Figure 24-5** depicts an example showing the three main components of pxGrid: a controller, publishers, and subscribers.



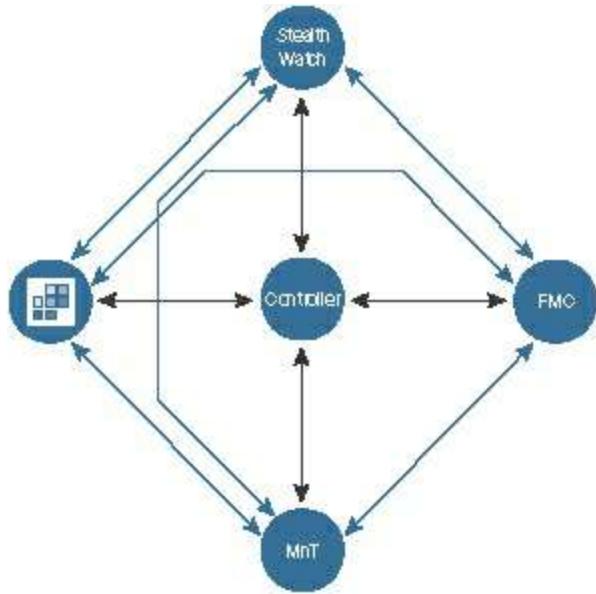
**Figure 24-5** Sample pxGrid Illustration

## pxGrid in Action

pxGrid uses secure communication between the participants, and therefore certificates are of great importance to the success and ease of your deployment. Every participant must trust the controller, and the controller must trust each of the participants.

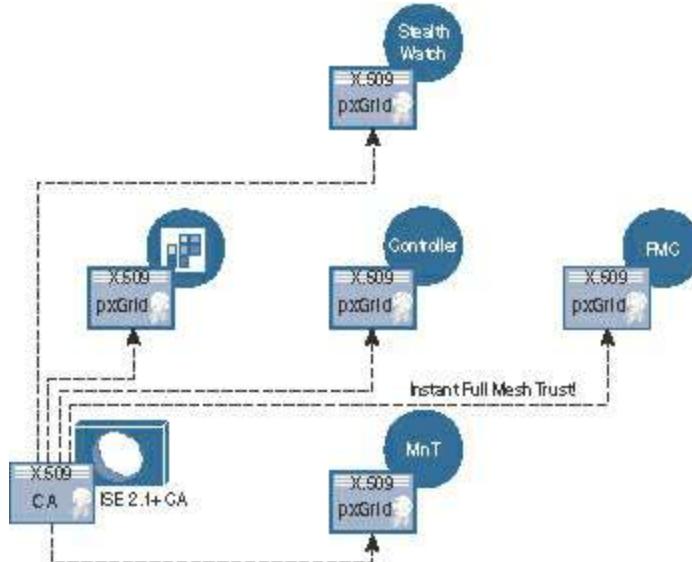
Examining [Figure 24-5](#) again, FMC needs to speak to the pxGrid controller to learn which topics exist, but then also needs to speak directly to the MnT node to perform bulk downloads of the published session data. If FMC were to trust the controllers' certificate but not the MnT's certificate, then the communication would ultimately fail.

[Figure 24-6](#) illustrates this concept. You end up needing a full mesh of trust between pxGrid participants. Each participant must trust the controller as well as each other participant.



**Figure 24-6** Full Mesh of Trust

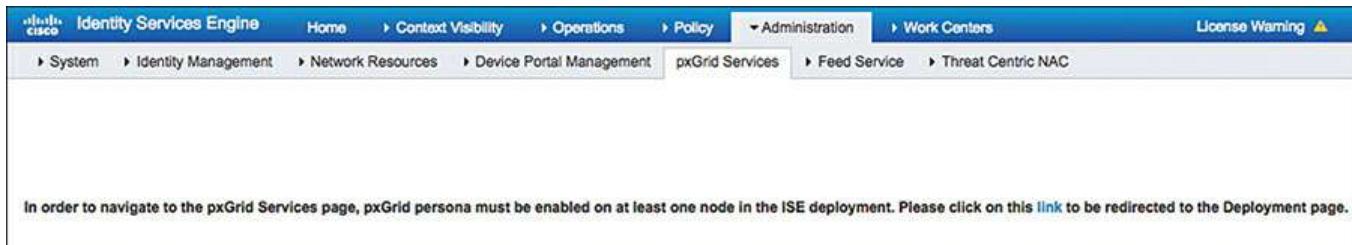
Based on a lot of deployment experience, the resulting best practice is to always use the same certificate authority (CA) to issue the pxGrid certificates for each of the participants. To make that even easier, ISE's built-in CA was enhanced to issue pxGrid certificates in addition to endpoint certificates beginning with ISE version 2.1. [Figure 24-7](#) illustrates a single CA issuing the certificates to all the participants.



**Figure 24-7** ISE CA Issuing the pxGrid Certificates to All Participants

## Configuring ISE for pxGrid

The pxGrid user interface is located under **Administration > pxGrid Services**. Those services will not be enabled by default on any ISE node, as shown in [Figure 24-8](#).



**Figure 24-8** pxGrid Services User Interface

Before enabling pxGrid on any of the ISE nodes in the deployment, it's best to ensure that each node in the ISE cube has a pxGrid certificate signed by the same certificate authority.

Beginning in ISE 2.2, each node's pxGrid certificate will be signed automatically by the internal CA. Naturally, you can replace that certificate with one from an external CA of your choosing, but the default certificate will use the internal CA in an attempt to simplify the setup and follow best practices.

To check that each node has a pxGrid certificate signed by the same CA:

**Step 1.** Navigate to **Administration > System > Certificates**.

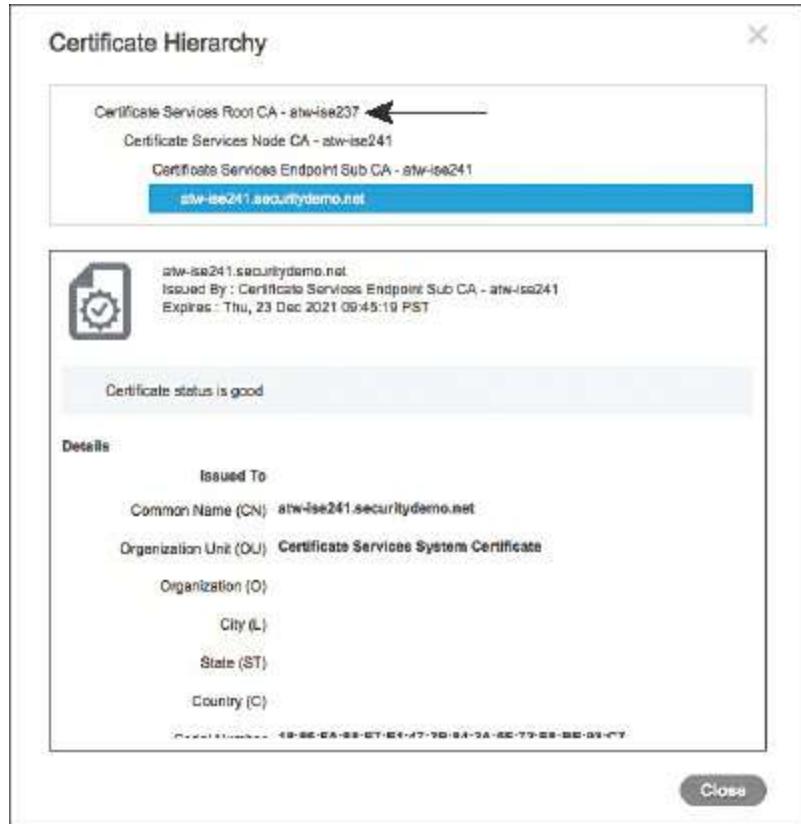
**Step 2.** Select the pxGrid certificate of one of the nodes, as shown in [Figure 24-9](#).



**Figure 24-9** Viewing System Certificates

**Step 3.** Click **View**.

**Step 4.** Check that the root signer of the certificate is the primary Policy Administration Node (PAN) of the ISE cube (the root CA), as shown in [Figure 24-10](#).



**Figure 24-10** Certificate Hierarchy

Once you're sure the certificates in use are all issued by the same public key infrastructure (PKI), then it's time to enable them. It is an experienced-based recommendation to have a pxGrid certificate on every single node in the ISE deployment, even if the node will not run the pxGrid controller function.

**Note** Beginning in ISE version 2.2, all pxGrid communications occur within the secure pxGrid channel; in other words, all communication occurs leveraging the pxGrid certificate of the ISE node. In prior versions, all bulk downloads from the MnT node occurred using the Admin Certificate, not the pxGrid certificate. This caused many TAC cases and confusion, and needed to change. If you are implementing pxGrid on any ISE version prior to ISE 2.2, you must ensure the participant trusts the admin certificate issuing CA as well as the pxGrid certificate.

To enable the pxGrid controller function:

**Step 1.** Navigate to **Administration > System > Deployment**.

**Step 2.** The pxGrid controller function must run on a Policy Service Node (PSN).

Select one of the PSNs from the list.

**Step 3.** Check the **pxGrid** check box, as shown in [Figure 24-11](#).

## Step 4. Click Save.



**Figure 24-11** Enabling the pxGrid Controller Function

This enables the pxGrid controller function on the PSN. You may have up to two pxGrid controllers per ISE cube to provide redundancy.

Once the pxGrid services are all up and running, the PAN and MnT nodes automatically register and publish their respective topics into the grid, as shown in [Figure 24-12](#). By default, only ISE nodes are registered; all others require approval, or require that you enable auto-registration.

A screenshot of the 'pxGrid Services' section of the Identity Services Engine interface. The top navigation bar includes 'Identity Management', 'Network Resources', 'Device Portal Management', 'pxGrid Services', 'Feed Services', and 'Threat Centric NAC'. The main content area is titled 'Clients' and shows a list of clients with their capabilities and status. One client, 'se-admin-awt-ise237', is expanded to show its capability details. The 'Capability Detail' table lists the following information:

Capability Name	Capability Version	Messaging Role
GridControllerAdminService	1.0	Sub
AdaptiveNetworkControl	1.0	Pub
Core	1.0	Sub
EndpointProfileMetaData	1.0	Pub
EndpointProtectionService	1.0	Pub
IdentityGroup	1.0	Pub
SessionDirectory	1.1	Pub

An arrow points to the 'Pub' role in the last row of the table. A message at the bottom left says 'Connected to pxGrid awt-ise237.securitydemo.net'.

**Figure 24-12** pxGrid Capability (AKA Topic) Detail

Notice in [Figure 24-12](#) that the topics are listed under the pxGrid participant, as well as the role that node plays with the topic (Pub or Sub).

## Configuring pxGrid Participants

Many different subscribers and publishers can participate in the ecosystem with pxGrid. Each one uses the information in its own way, and the integration UI is bound to be unique per product, but the basic requirements and configuration steps will always remain the same:

1. Trust the ISE certificate authority.
2. Install a pxGrid certificate for its own identity.
3. Configure the IP or FQDN of the pxGrid controller.

For the most part, that is all you need to do on each participant. Some will make things easier than others. Let's take a look configuring some of the main pxGrid participants: Cisco Firepower Management Center, Cisco Stealthwatch, and Cisco Web Security Appliance.

## Configuring Firepower Management Center for pxGrid

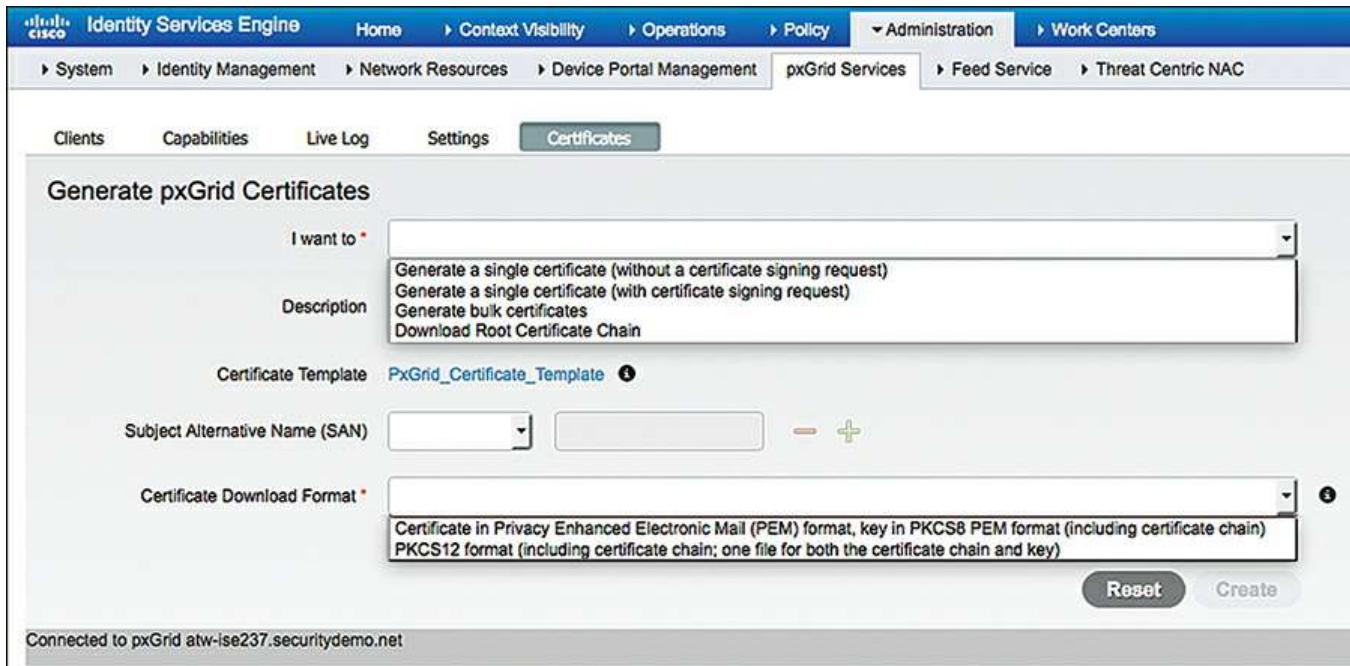
Cisco FMC is the ultimate device manager and security monitoring tool for Cisco Firepower Threat Defense (FTD) NGFW, Firepower NGFW, and Firepower NGIPS devices.

FMC has had pxGrid integration for a while, but version 6.2 adds an even better integration, with the ability to use the TrustSec data independent of user identities. FMC can use context information provided by pxGrid, such as endpoint profiles, TrustSec tags, and both passive and active user identities.

Before configuring pxGrid on FMC, generate a pxGrid certificate for FMC to use. In versions past, you had to configure a certificate provisioning portal in ISE, but in ISE 2.2 you can generate certificates directly from the pxGrid services user interface.

To generate a pxGrid certificate for FMC:

**Step 1.** Navigate to **Administration > pxGrid Services > Certificates** , as shown in [Figure 24-13.](#)



**Figure 24-13** Generating pxGrid Certificates

Examining [Figure 24-13](#), from this screen you can generate a single certificate, sign a certificate signing request (CSR), generate bulk certificates from a CSV file, or download the certificate authority chain for import into the trust store of the pxGrid participant. For FMC, you need to generate a certificate-key pair.

**Step 2.** From the I Want To drop-down list, choose **Generate a Single Certificate (Without a Certificate Signing Request)**.

**Step 3.** In the Common Name (CN) text box, enter a common name for the subject of your certificate.

The CN is normally the FQDN of the host (that is, atw-fmc.securitydemo.net); however, a common practice is to add a prefix to your CN, such as pxGrid- (as shown in [Figure 24-14](#)), which will help you avoid installation errors that can sometimes occur when you try to install more than one certificate with the same FQDN.

**Step 4.** (Optional) In the Subject Alternative Name (SAN) field, add a SAN, if needed.

If you use anything other than the true FQDN for the device, then you need to complete this field. Per the RFC, anytime you use a SAN, it must also contain the CN. Add an entry for the FQDN of the host. Adding a SAN for the IP address is helpful, just in case one of the pxGrid peers is sent to the host via the IP address instead of the FQDN.

**Step 5.** From the Certificate Download Format drop-down list, choose **Certificate in Privacy Enhanced Electronic Mail (PEM) Format, Key in PKCS8 PEM Format**.

All options include the internal CA's certificates, for the entire PKI hierarchy. There is also an option to download it as a PKCS12 chain file, where the public certificate + private key + signing chain are all in a single file. For FMC, the download format needs to be separate PEM files, not the PKCS12 chain.

**Step 6.** Add a password for the private key.

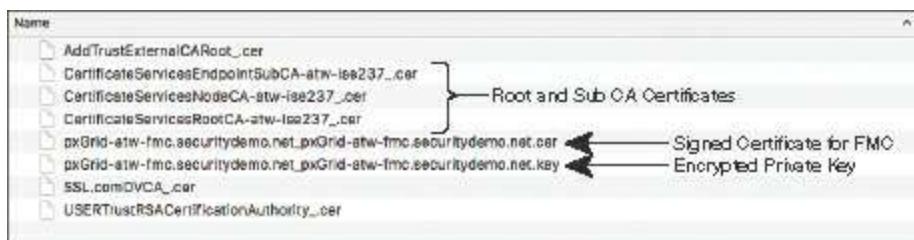
ISE will never issue private keys without a password to encrypt the key.

**Step 7.** Click **Create** and download the resulting ZIP file.

[Figure 24-14](#) shows the completed certificate form, and [Figure 24-15](#) shows the contents of the ZIP file.

The screenshot shows the 'Generate pxGrid Certificates' page in the Cisco ISE Administration section. The 'Certificates' tab is selected. The 'Common Name (CN)' field is set to 'pxGrid-atw-fmc.securitydemo.net'. The 'Certificate Template' is 'PxGrid\_Certificate\_Template'. Under 'Subject Alternative Name (SAN)', there are three entries: 'FQDN' with value 'pxGrid-atw-fmc.securitydemo.net', 'FQDN' with value 'atw-fmc.securitydemo.net', and 'IP address' with value '10.1.100.13'. The 'Certificate Download Format' is set to 'Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)'. The 'Certificate Password' and 'Confirm Password' fields both contain '\*\*\*\*\*'. At the bottom right are 'Reset' and 'Create' buttons. A status message at the bottom left says 'Connected to pxGrid atw-ise237.securitydemo.net'.

**Figure 24-14** Completed Certificate Form



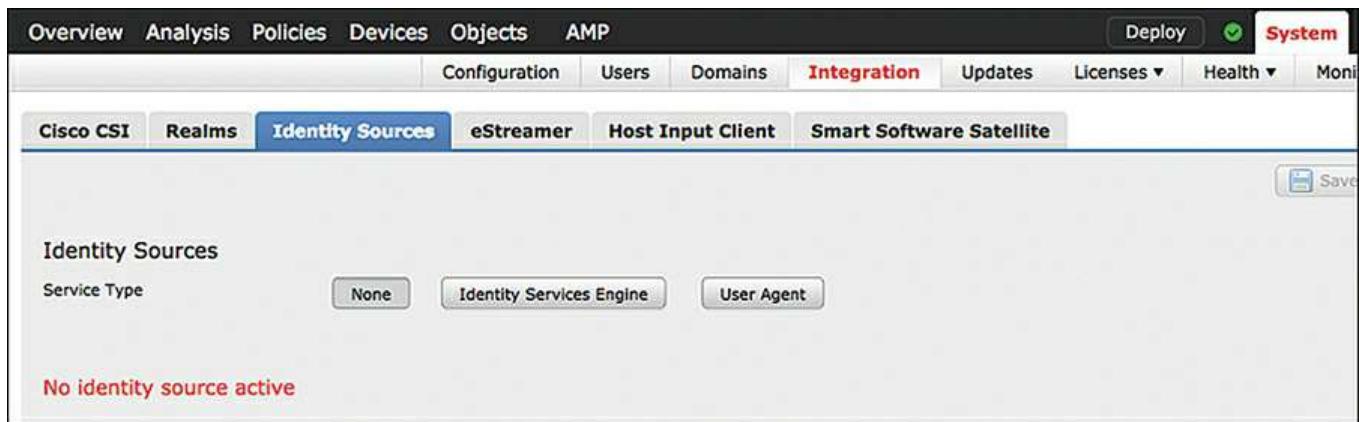
**Figure 24-15** Contents of the Resulting ZIP File

Examining [Figure 24-15](#), the ZIP file contains the signed certificate, the encrypted

private key, and all the signing certificates in the PKI hierarchy for the issued certificate. Additionally, the signing certificates in the PKI hierarchy for the admin certificate are also included for good measure. Beginning with ISE 2.2, they should not be required.

Now you have all the required certificates and the private key for FMC. To configure pxGrid on FMC:

**Step 1.** Navigate to **System > Integration > Identity Sources**, as shown in [Figure 24-16](#).



**Figure 24-16** Identity Sources

**Step 2.** Click **Identity Services Engine**.

Figure 24-19, shown later in this process, shows the completed Identity Services Engine form.

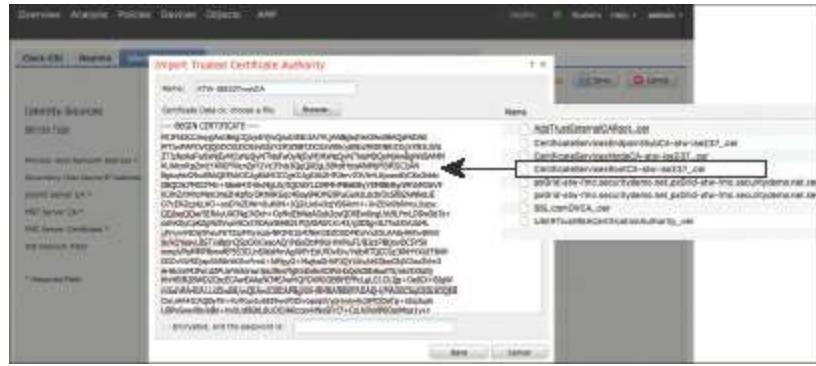
**Step 3.** In the Primary Host Name/IP Address text box, enter the FQDN or IP address of the primary pxGrid controller.

**Step 4.** If there is a secondary controller, add its FQDN or IP address in the Secondary Host Name/IP Address text box.

**Step 5.** To add the ISE root CA certificate, click the green and white plus button to the right of the pxGrid Server CA field to open the Imported Trusted Certificate Authority dialog box.

This step adds the root CA certificate to the list of trusted CAs in FMC. In the Name text box, give the certificate a name that makes sense to you, similar to what you see in [Figure 24-17](#).

**Step 6.** Click **Browse** and select the root CA certificate from the expanded ZIP file you downloaded earlier, as shown in [Figure 24-17](#).



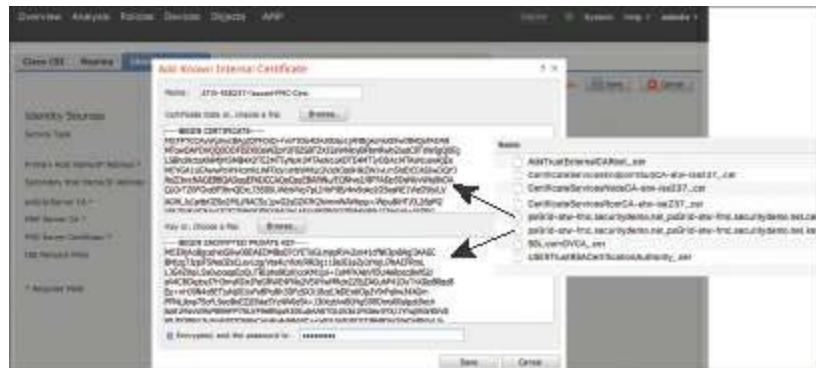
**Figure 24-17 Import Trusted Certificate Authority: ISE Root CA**

**Step 7.** Click Save.

**Step 8.** Ensure that the newly imported root CA certificate is selected for both the pxGrid Server CA and the MNT Server CA fields, as shown later in [Figure 24-19](#).

**Step 9.** To add the signed certificate and private key for FMC, click the green and white plus button to the right of the FMC Server Certificate field to open the Add Known Internal Certificate dialog box.

This step adds the PEM encoded certificate that was signed by ISE's endpoint CA and the encrypted private key to FMC. In the Name text box, give the internal certificate a name that makes sense to you, similar to what you see in [Figure 24-18](#).



**Figure 24-18 Adding the Internal Certificate**

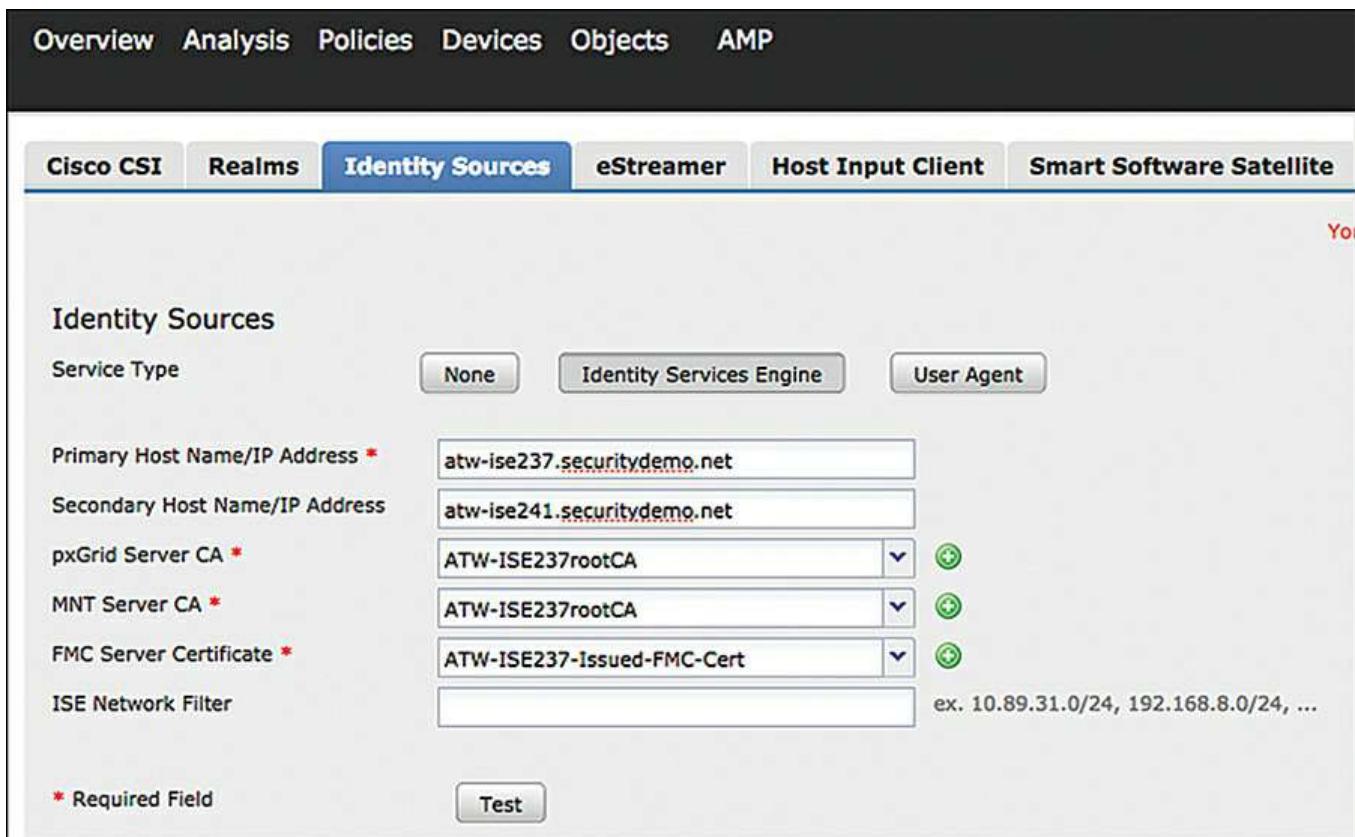
**Step 10.** Click Browse to the right of Certificate Data and select the PEM certificate from the expanded ZIP file you downloaded earlier, as shown in [Figure 24-18](#).

**Step 11.** Click Browse to the right of Key and select the PKCS8 key file from the expanded ZIP file you downloaded earlier, as shown in [Figure 24-18](#).

**Step 12.** Check the Encrypted, and the Password Is check box.

**Step 13.** Enter the password used to encrypt the key file from the ISE certificate authority. Click Save.

**Step 14.** Click **Save** in the upper-right corner of the screen. [Figure 24-19](#) shows the completed form.



The screenshot shows the 'Identity Sources' configuration page in the Cisco ISE GUI. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, AMP, Cisco CSI, Realms, Identity Sources (which is selected and highlighted in blue), eStreamer, Host Input Client, and Smart Software Satellite. The main section is titled 'Identity Sources' and contains the following fields:

Service Type	<input type="button" value="None"/> <input type="button" value="Identity Services Engine"/> <input type="button" value="User Agent"/>
Primary Host Name/IP Address *	atw-ise237.securitydemo.net
Secondary Host Name/IP Address	atw-ise241.securitydemo.net
pxGrid Server CA *	ATW-ISE237rootCA
MNT Server CA *	ATW-ISE237rootCA
FMC Server Certificate *	ATW-ISE237-Issued-FMC-Cert
ISE Network Filter	<input type="text" value="ex. 10.89.31.0/24, 192.168.8.0/24, ..."/>

At the bottom left is a note: \* Required Field. At the bottom right is a **Test** button.

**Figure 24-19** Completed ISE Identity Source Form

**Step 15.** Click **Test** to verify a successful connection.

The test will most likely fail the first time you try. Why? Because ISE is not configured to automatically approve new participants.

**Step 16.** In the ISE GUI, navigate to **Administration > pxGrid Services > Clients**.

**Step 17.** Check the box to the left of the iseagent client for FMC, as shown in [Figure 24-20](#), and click **Approve**.



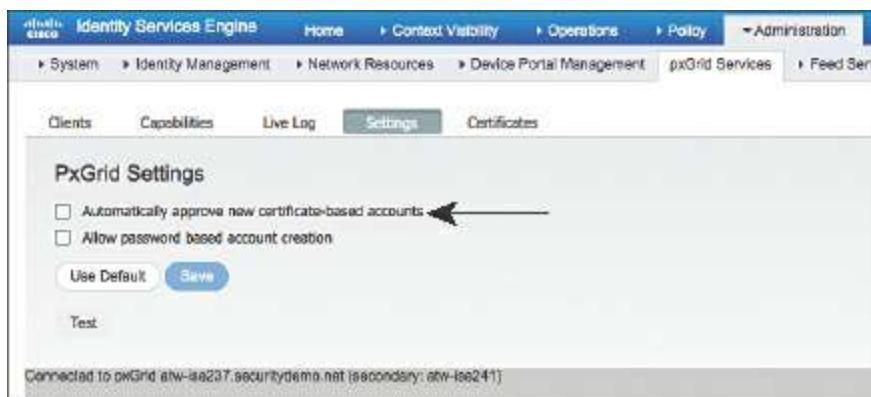
The screenshot shows the 'Clients' table in the pxGrid Services section of the ISE GUI. The table has columns for Client Name, Client Description, Capabilities, Status, and Client Group(s). A checkbox column is present on the far left. One row is selected, indicated by a blue highlight. The table shows the following data:

Client Name	Client Description	Capabilities	Status	Client Group(s)
ise-admin-ise-ise237		Capabilties(3 Pub, 1 Sub)	Online	Administrator
ise-admin-ise-ise241		Capabilties(3 Pub, 1 Sub)	Online	Administrator
ise-admin-ise-ise241		Capabilties(3 Pub, 2 Sub)	Online	Administrator
ise-admin-ise-ise241		Capabilties(3 Pub, 1 Sub)	Online	Administrator
ise-admin-ise-ise241		Capabilties(3 Pub, 1 Sub)	Online	Administrator
ise-admin-ise-ise241		Capabilties(3 Pub, 1 Sub)	Online	Administrator
iseagent-sourcefiresecurity		Capabilties(2 Pub, 0 Sub)	Pending	ANCEPSI

**Figure 24-20** pxGrid Clients

**Step 18.** Check the box to the left of the firesightisetest client and click **Approve**.

**Step 19.** Return to the FMC UI and attempt the test again. This test should be successful. Manually approving each and every pxGrid participant and their test accounts can be time consuming and somewhat confusing. Alternatively, you may enable the automatic approval of certificate-based accounts in the pxGrid settings, as shown in [Figure 24-21](#). Just remember to disable it again after you are finished.



**Figure 24-21** pxGrid Settings

**Note** In the pxGrid settings is an option to allow password-based account creation. This is an alternative to the certificate-based accounts that you are seeing in this chapter, where a password is leveraged instead and then tokens are assigned for authorization. At the time of writing, there are not any pxGrid client applications leveraging this account method. Also in the settings screen is a Test button to verify that pxGrid is working as expected within ISE. It is very useful for checking that ISE trusts its own certificates.

## Configuring the Web Security Appliance for pxGrid

Cisco WSA was one of the first pxGrid partner applications in the security ecosystem. The WSA may use pxGrid to ascertain both passive and active user identities, as well as TrustSec tags. However, at the time of writing, the WSA (version 9.1.2) is unable to combine Active Directory group membership with the identity information gathered from pxGrid, which means that TrustSec tagging is realistically the only scalable approach when using pxGrid.

Create a certificate for the WSA using the same procedure that you used for FMC, as shown in [Figure 24-22](#).

Connected to pxGrid atw-ise237.securitydemo.net (secondary: atw-ise241)

**Figure 24-22** Completed Certificate Form: WSA

To configure pxGrid on the WSA:

- Step 1.** Navigate to Network > Identification Services > Identity Services Engine.
- Step 2.** Click Enable and Edit Settings , as shown in [Figure 24-23](#).



**Figure 24-23** Editing the Identity Services Engine Configuration on the WSA

- Step 3.** Enter the FQDN for the primary pxGrid controller, as shown in [Figure 24-24](#).



**Figure 24-24** Primary ISE pxGrid Node

**Step 4.** Click **Upload File** to upload the ISE root CA certificate, as shown in [Figure 24-24](#).

**Step 5.** Enter the FQDN for the optional secondary pxGrid controller.

**Step 6.** Upload the ISE root CA certificate.

**Note** The WSA provides a location to upload the admin certificate for the primary and secondary Monitoring (MnT) nodes. This is left over from the days before ISE 2.2, when the admin certificate was used for the bulk downloads from the MnT nodes to the pxGrid subscribers. With ISE version 2.2 and newer, the same root CA certificate should be used.

**Step 7.** Click **Browse** to the right of Certificate and select the PEM certificate from the expanded ZIP file you downloaded earlier, as shown in [Figure 24-25](#).



**Figure 24-25** WSA Client Certificate

**Step 8.** Click **Browse** to the right of Key and select the PKCS8 key file from the expanded ZIP file you downloaded earlier, as shown in [Figure 24-25](#).

**Step 9.** Check the **Key in Encrypted** check box. In the Password text box, enter the password to decrypt the key.

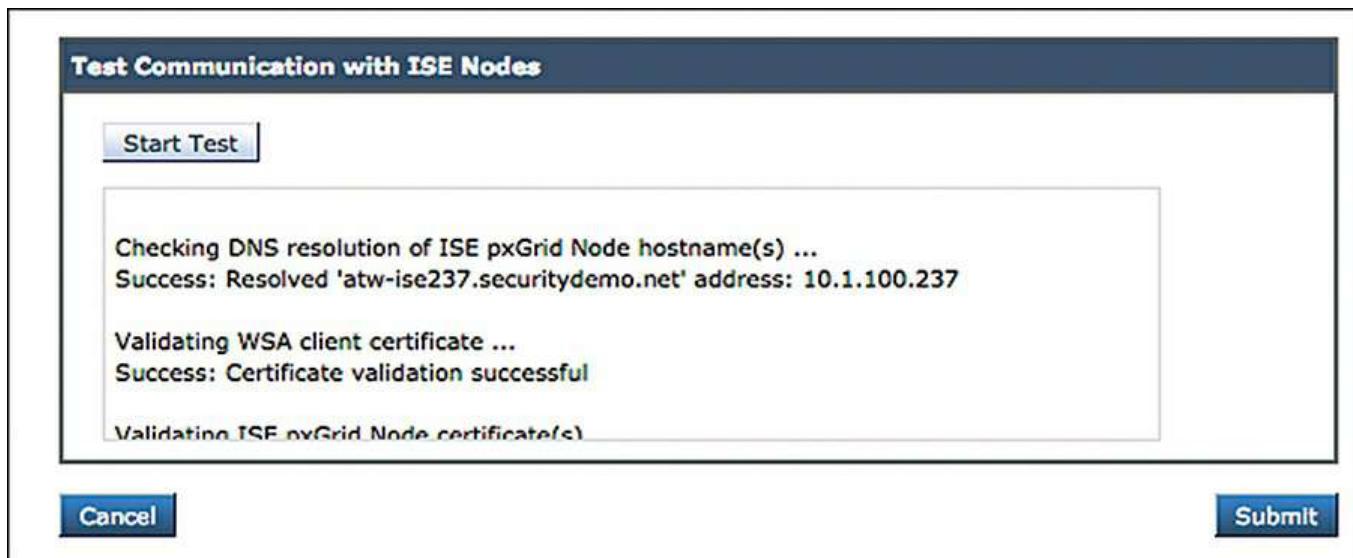
**Step 10.** Click **Upload Files**.

**Step 11.** Click **Submit** to complete the configuration.

**Step 12.** Click **Commit Changes** twice.

**Step 13.** To test the connection, click **Edit Settings**.

**Step 14.** Click **Start Test** at the bottom of the screen, as shown in [Figure 24-26](#). If auto approval is enabled, then the test should be successful. If it is not enabled, the test will fail without manually approving the two WSA accounts on the pxGrid controller.



**Figure 24-26** Test Communication with ISE Nodes

[Example 24-1](#) demonstrates an example of the test output.

**Example 24-1** Test Execution on WSA

[Click here to view code image](#)

```
Checking DNS resolution of ISE pxGrid Node hostname(s) ...
Success: Resolved 'atw-ise237.securitydemo.net' address: 10.1.100.237

Validating WSA client certificate ...
Success: Certificate validation successful

Validating ISE pxGrid Node certificate(s) ...
Success: Certificate validation successful

Validating ISE Monitortng Node Admin certificate(s) ...
Success: Certificate validation successful

Checking connection to ISE pxGrid Node(s) ...
Success: Connection to ISE pxGrid Node was successful.
Retrieved 17 SGTs from: atw-ise237.securitydemo.net

Checking connection to ISE Monitortng Node (REST server(s)) ...
Success: Connection to ISE Monitortng Node was successful.
REST Host contacted: atw-ise237.securitydemo.net

Test completed successfully.
```

## Configuring Stealthwatch for pxGrid

Beginning with version 6.9, Cisco's Stealthwatch uses ISE as the primary source for learning passive and active user identities to merge into the flow records used for behavioral analysis. The mechanisms used are exactly the same, whether it is full ISE or the ISE Passive Identity Connector (ISE-PIC), which provides only passive identities (see [Chapter 23, “Passive Identities, ISE PIC, and EZ Connect,”](#) for more information on ISE-PIC).

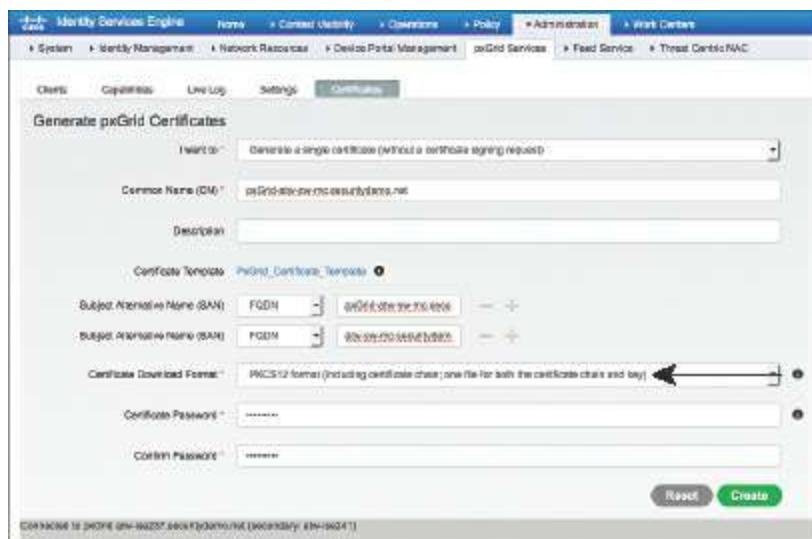
Unlike FMC and the WSA, Stealthwatch uses the PKCS12 chain files instead of individual certificates. To generate the chain for Stealthwatch:

**Step 1.** Navigate to **Administration > pxGrid Services > Certificates**.

**Step 2.** From the I Want To drop-down list, choose **Generate a Single Certificate**

**(Without a Certificate Signing Request ).**

**Step 3.** From the Certificate Download Format drop-down list, choose **PKCS12 Format** , as shown in [Figure 24-27](#).



The screenshot shows a configuration interface for generating pxGrid certificates. The 'Generate pxGrid Certificates' section has the following settings:

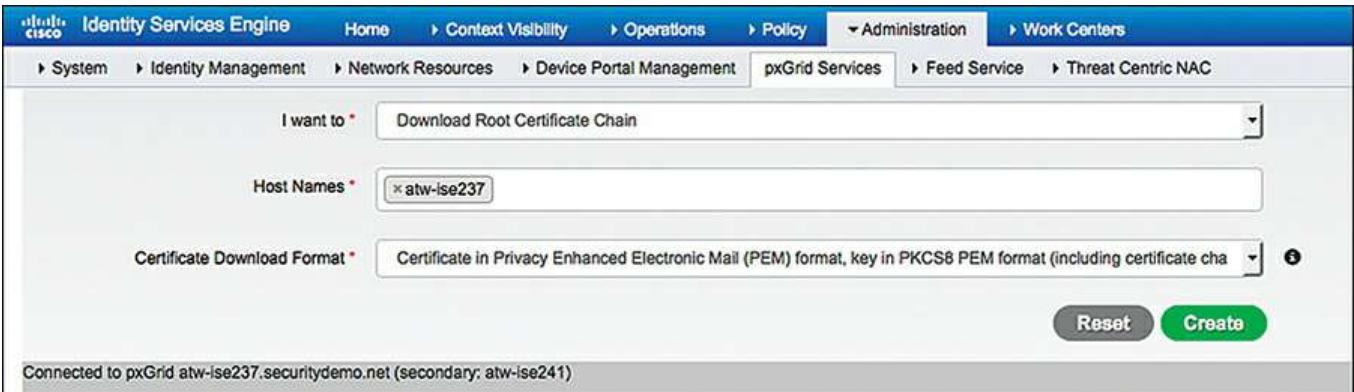
- I want to: Generate a single certificate (Without a certificate signing request)
- Commerce Name (CN): pxGrid-stealthwatch.securitydemo.net
- Description: (empty)
- Certificate Template: pxGrid\_Certificate\_Template
- Subject Alternative Name (SAN): FQDN: 192.168.100.1000
- Subject Alternative Name (SAN): FQDN: 192.168.100.1000
- Certificate Download Format: PKCS12 format (including certificate chain; one file for both the certificate chain and key)
- Certificate Password: (empty)
- Confirm Password: (empty)

At the bottom are 'Reset' and 'Create' buttons. A status message at the bottom left says: Connected to pxGrid atw-ise237.securitydemo.net (secondary: atw-ise241).

**Figure 24-27** Completed Certificate Form: Stealthwatch

**Step 4.** Click **Create** to download the certificate chain.

Next, download the root certificates in PEM format, as shown in [Figure 24-28](#).



The screenshot shows a configuration interface for downloading root certificates. The 'Download Root Certificate Chain' section has the following settings:

- I want to: Download Root Certificate Chain
- Host Names: atw-ise237
- Certificate Download Format: Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)

At the bottom are 'Reset' and 'Create' buttons. A status message at the bottom left says: Connected to pxGrid atw-ise237.securitydemo.net (secondary: atw-ise241).

**Figure 24-28** Completed Certificate Form: Downloading the Root Chain

**Step 5.** From the I Want To drop-down list, choose **Download Root Certificate Chain**.

**Step 6.** From the Certificate Download Format drop-down list, choose **Certificate in Privacy Enhanced Electronic Mail (PEM) Format, Key in PKCS8 PEM Format**.

To configure Stealthwatch for pxGrid, first add the root certificate to the main list of trusted certificate authorities, as shown in [Figure 24-29](#):

**Step 1.** Navigate to **Administer Appliance > Configuration > Certificate Authority Certificates**.

Certificate Authority Certificates

Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	<input type="checkbox"/>
lancope	2036-01-01 05:10:10	Lancope	Lancope	<input type="checkbox"/>

**Delete**

Select SSL certificate to add

Browse... CertificateServicesRootCA-atw-ise237\_.cer

Name:  
ATW-ISE237-Root

**Add Certificate**

**Figure 24-29** Add Trusted Certificate Authority

**Step 2.** Scroll down to **Select SSL Certificate to Add**.

**Step 3.** Click **Browse** and select the ISE root CA PEM file previously downloaded.

**Step 4.** Click **Add Certificate**.

Next, add the PKCS12 chain file, as shown in [Figure 24-30](#).

**Step 5.** Navigate to **Configuration > SSL Certificate**.

Upload a PKCS12 Bundle

Friendly Name:

PKCS12 Bundle Password:

PKCS12 Bundle:  
 pxGrid-atw-sw-mc.securitydemo.net\_pxGrid-atw-sw-mc.securitydemo.net.p12

**Figure 24-30** Upload Bundle

**Step 6.** Scroll down to **Upload a PKCS12 Bundle**.

**Step 7.** Provide a friendly name, such as **pxGrid Certificate**.

**Step 8.** Enter the password for the encrypted PKCS12 file.

**Step 9.** Click **Browse** and select the .p12 file previously downloaded.

**Step 10.** Click **Upload Bundle**.

The uploaded certificate identity is displayed in the SSL Client Identities section, as shown in [Figure 24-31](#).

## SSL Client Identities

Use this section to upload certificates that the appliance will present when performing client certificate authentication.

Friendly Name	Issued To	Issued By	Expiration Date	Delete
pxGrid Certificate	pxGrid-atw-sw-mc.securitydemo.net	Certificate Services Endpoint Sub CA - atw-ise237	12-28-2018	<input type="checkbox"/>

**Delete**

**Figure 24-31 SSL Client Identities**

Now that the CA is trusted, and the pxGrid identity has been installed into Stealthwatch, it is time to configure the ISE integration.

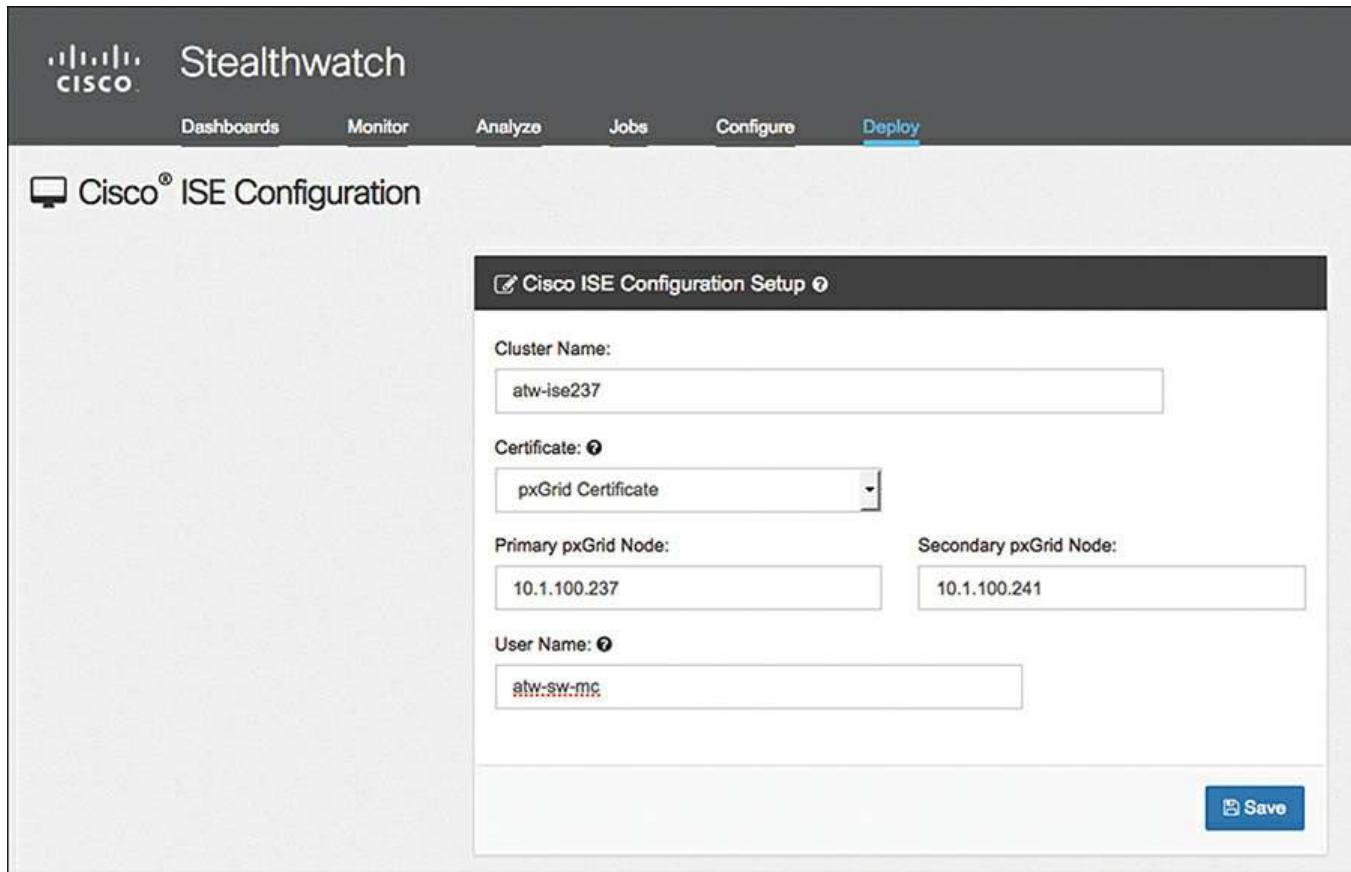
On the main Stealthwatch screen, navigate to **Deploy > Cisco ISE Configuration**, as shown in [Figure 24-32](#), and proceed through the steps that follow:



**Figure 24-32 Deploying Cisco ISE Configuration**

- Step 1.** In the Cluster Name text box, enter a friendly name for the ISE cube.
- Step 2.** From the Certificate drop-down list, choose **pxGrid Certificate**.
- Step 3.** Enter the IP addresses for the primary and secondary pxGrid controllers.
- Step 4.** Create a username to uniquely identify Stealthwatch in the ISE pxGrid UI.

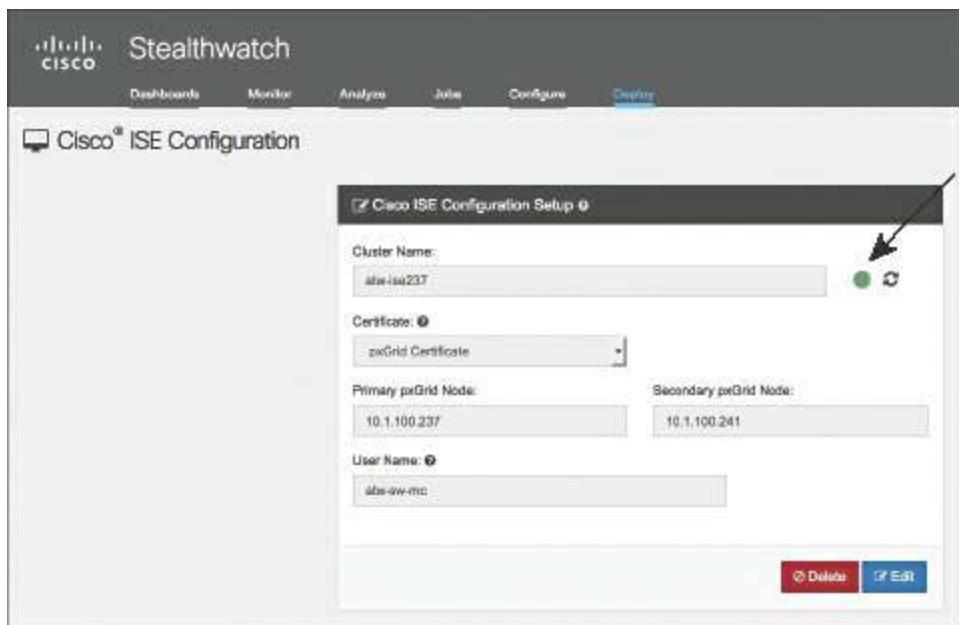
[Figure 24-33](#) shows the completed Cisco ISE Configuration form.



**Figure 24-33** Cisco ISE Configuration

### Step 5. Click Save.

After saving the connection details, Stealthwatch will join the pxGrid connection and refresh the screen with the current connection status, as shown in [Figure 24-34](#).



**Figure 24-34** Successful Connection

[Figure 24-35](#) shows the final pxGrid Clients screen, where you can see the FMC, WSA, and the Stealthwatch clients in the list.

Clients					
	Client Name	Client Description	Capabilities	Status	Client Group(s)
<input type="checkbox"/>	► ise-mnt-atw-ise237		Capabilities(2 Pub, 1 Sub)	Online	Administrator
<input type="checkbox"/>	► ise-admin-atw-ise243		Capabilities(2 Pub, 1 Sub)	Online	Administrator
<input type="checkbox"/>	► ise-admin-atw-ise237		Capabilities(6 Pub, 2 Sub)	Online	Administrator
<input type="checkbox"/>	► ise-admin-atw-ise242		Capabilities(2 Pub, 1 Sub)	Online	Administrator
<input type="checkbox"/>	► ise-mnt-atw-ise241		Capabilities(2 Pub, 1 Sub)	Online	Administrator
<input type="checkbox"/>	► ise-admin-atw-ise241		Capabilities(3 Pub, 1 Sub)	Online	Administrator
<input type="checkbox"/>	► atw-tme-wsa.cisco.com-pxgrid_cl...	pxGrid Connection from WSA	Capabilities(0 Pub, 2 Sub)	Online	Session
<input type="checkbox"/>	► iseagent-sourcefire3d.securityde...		Capabilities(0 Pub, 6 Sub)	Online	ANC,EPS
<input type="checkbox"/>	► atw-sw-mc		Capabilities(0 Pub, 3 Sub)	Online	EPS
<input type="checkbox"/>	► ise_internal_test		Capabilities(0 Pub, 0 Sub)	Offline	Session
<input type="checkbox"/>	► atw-tme-wsa.cisco.com-test_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session
<input type="checkbox"/>	► firesightisetest-sourcefire3d.secur...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS

**Figure 24-35** Final pxGrid Clients Screen

## Summary

In this chapter, you examined the many facets of the ISE ecosystem. Integration types can be ISE accepting “context-in,” where information received by ISE is used within policy, or “context-out,” where information that ISE possesses is shared to consumers (AKA subscribers).

You learned about the Cisco Platform Exchange Grid (pxGrid) and how it is Cisco’s premier pub/sub communication bus designed from the ground up to be a scalable and secure data sharing system. You saw first-hand how tightly coupled pxGrid is with certificate-based communication and how to configure three of the main pxGrid participant products.

In the next chapter, you will learn about the monitoring and alerting functions within ISE.

# **Part VI Monitoring, Maintenance, and Troubleshooting for Network Access AAA**

[Chapter 25 Understanding Monitoring, Reporting, and Alerting](#)

[Chapter 26 Troubleshooting](#)

[Chapter 27 Upgrading ISE](#)

# Chapter 25 Understanding Monitoring, Reporting, and Alerting

This chapter covers the following topics:

- ISE monitoring
- ISE reporting
- ISE alarms

This chapter introduces you to the monitoring, reporting, and alerting functions of Cisco ISE.

Monitoring provides you with real-time or close-to-real-time data depicting the various activities, functions, and processes that ISE performs. Monitoring gives you an important operational tool for the daily usage of ISE and is key to the long-term success of an ISE deployment.

Reporting provides you with non-real-time information that is typically based on either a time frame or number of events. Examples of reports are top-client authentication, all authentications yesterday, administrator changes last month, and so on. The catalog of reports that ISE provides is meant to assist with analyzing trends, performance, and activities over time. Reports can also be run periodically or scheduled and then emailed and/or stored on completion.

ISE-alerting functions are handled by alarms. ISE alarms notify you when critical events occur or thresholds are met/crossed. Alarms are also sent when ISE completes some system functions, such as database purge, so you know they have been completed. ISE alarms are divided into multiple categories and are sent real-time when an alert is triggered.

## ISE Monitoring

As discussed in [Chapter 4, “The Building Blocks in an Identity Services Engine Design.”](#) the monitoring functions of ISE are separated into their own Monitoring persona. In a standalone ISE deployment, one node takes on the Administration, Monitoring, and Policy Service personas, but in a distributed deployment, you have a dedicated high availability (HA) pair of Monitoring nodes. Also recall that all of the monitoring data is viewed from the Admin node and never directly from the Monitoring node. A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from all the Administration and Policy Service Nodes as well as from all the network access devices (NAD) in your network.

ISE displays monitoring information in many places:

- Cisco ISE Home page
- Context Visibility views
- RADIUS Live Logs and Live Sessions
- Global search
- Threat-Centric NAC Live Logs
- TACACS Live Logs

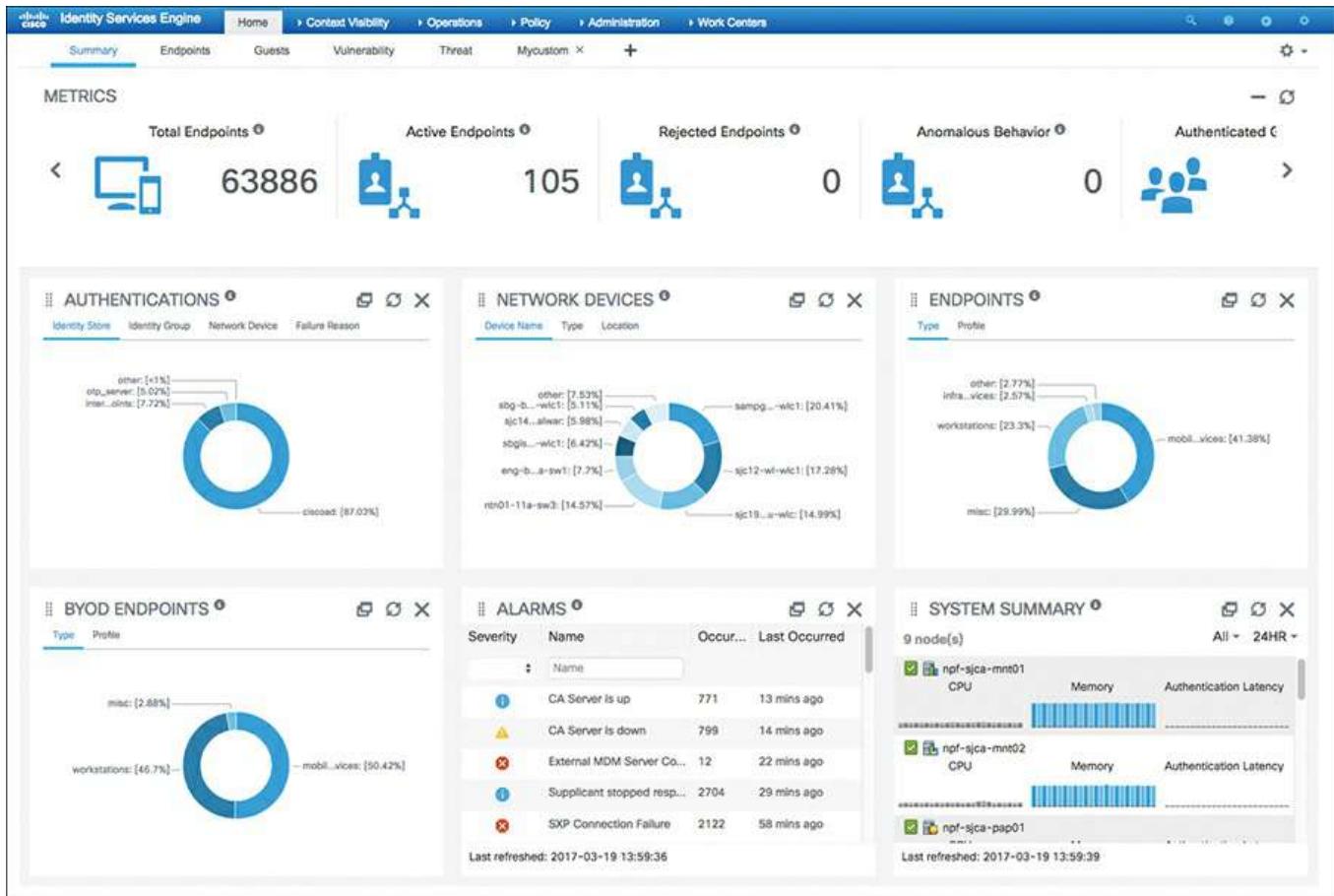
Most of these monitoring tools are explored in this chapter. TC-NAC and TACACS logs are beyond the scope of this book. Check the Cisco website for more information: [www.cisco.com/go/ise](http://www.cisco.com/go/ise).

## Cisco ISE Home Page

The most prominent of the monitoring tools in ISE is the ISE Home page, which in the GUI is labeled Home. It includes multiple dashboards that display real-time consolidated and statistically correlated data that is most essential for effective ISE monitoring. ISE provides multiple dashboards by default (listed next) and allows you to create your own custom dashboards. Unless otherwise noted, the information shown in a dashboard is for a 24-hour period. Each dashboard is made up of several individual dashlets that you can manipulate.

Here is a description of the five default dashboards in ISE:

- **Summary:** This dashboard, shown in [Figure 25-1](#), has a linear Metrics dashlet at the top to display noteworthy real-time ISE metrics, pie chart dashlets, and list dashlets. All but the Metrics dashlet are configurable.



**Figure 25-1 ISE Summary Dashboard**

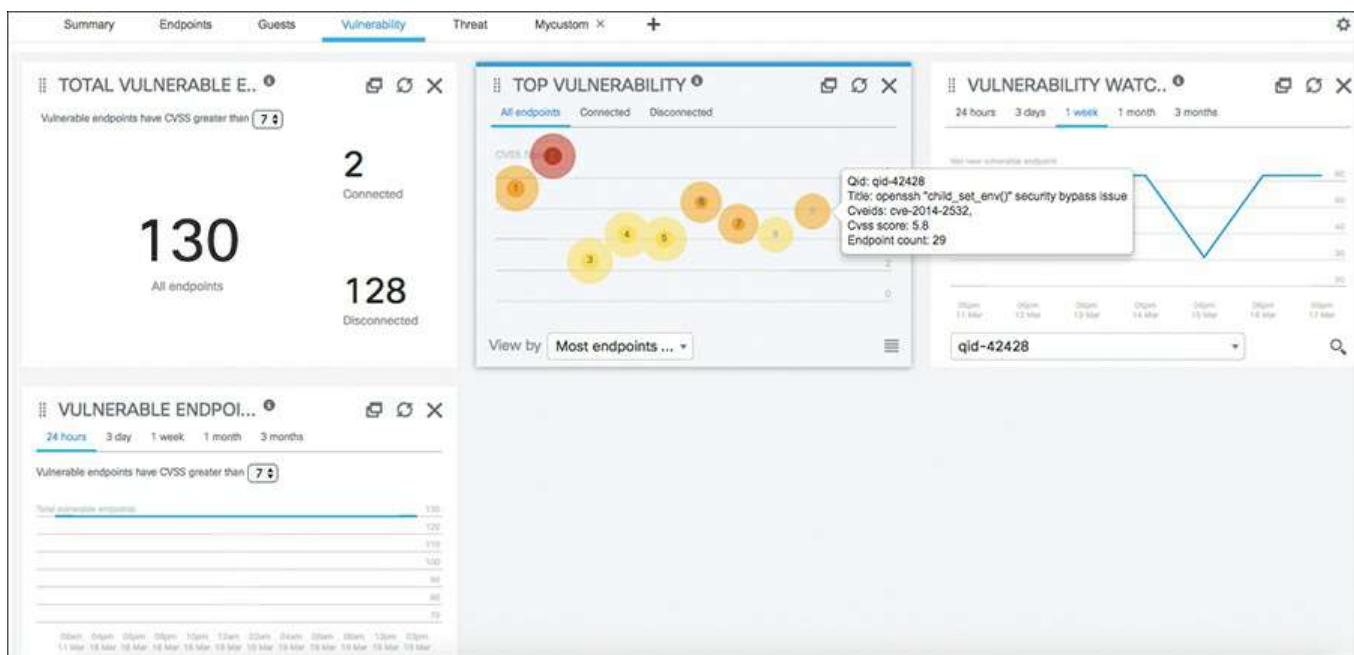
- **Endpoints:** Includes dashlets named Status, Endpoints, Endpoint Categories, and Network Devices.
- **Guests:** Displays information such as guest user type, logon failures, and location.
- **Vulnerability:** Displays information reported to ISE by vulnerability servers.
- **Threat:** Displays information reported to ISE by threat servers.

For more information on a dashlet, hover your mouse over it. Additionally, many of the elements are clickable and provide you with a drill-down view. You should explore the drill-down views of the dashboard elements and become familiar with them. [Table 25-1](#) provides a description for each dashlet in the Summary dashboard.

Name	Description
Metrics	Summarizes the most important live information on the state of ISE.
Authentications	Passed/failed auths and a distribution of auths by type.
Network Devices	Authentications per network device.
Endpoints	Endpoint types recognized by ISE.
BYOD Endpoints	Endpoints profiled by network function.
Alarms	List of current alarms. Click each for more detail and a description of the alarm.
System Summary	Provides system-health information for each ISE node.

**Table 25-1** ISE Summary Dashboard Dashlets

[Figure 25-2](#) shows the Vulnerability dashboard in ISE. This dashboard is useful to quickly understand the number and severity of software vulnerabilities on your endpoints. This data comes from ISE’s integration with external vulnerability scanner data. Vulnerabilities are classified by Common Vulnerability Scoring System (CVSS) score. CVSS uses the ratings shown in [Table 25-2](#). You can quickly sort based on the CVSS score in many of the dashlets.



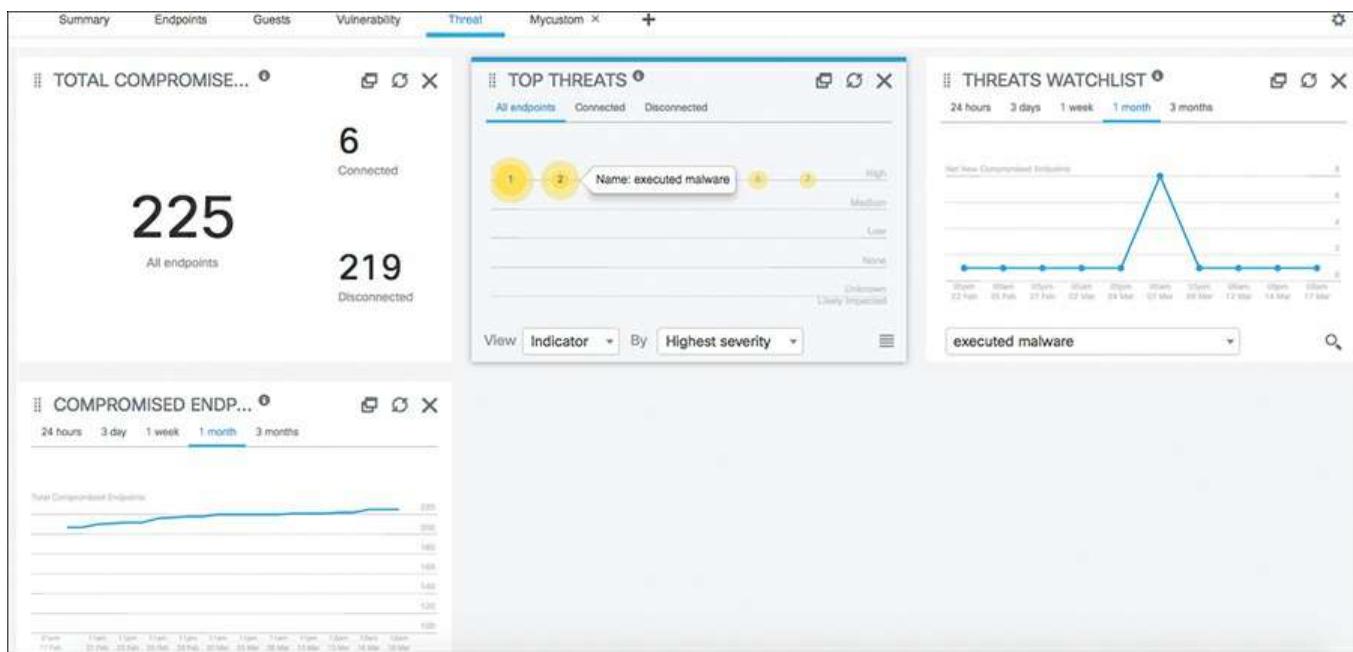
**Figure 25-2** ISE Vulnerability Dashboard

Rating	CVSS Score
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10.0

**Table 25-2 CVSS Scoring**

The Vulnerability Watchlist dashlet enables you to track specific vulnerabilities. [Figure 25-2](#) shows qid-42428 being tracked. Qid stands for Qualys ID; other vulnerability scanners have their own tracking IDs.

[Figure 25-3](#) shows the Threat dashboard. This dashboard is useful for quickly seeing how many hosts are actively compromised and what indicators of compromise behaviors they are exhibiting. This data comes from ISE’s integration with Cisco Advanced Malware Protection (AMP) for Endpoints and Cisco Cognitive Threat Analysis (CTA) software.



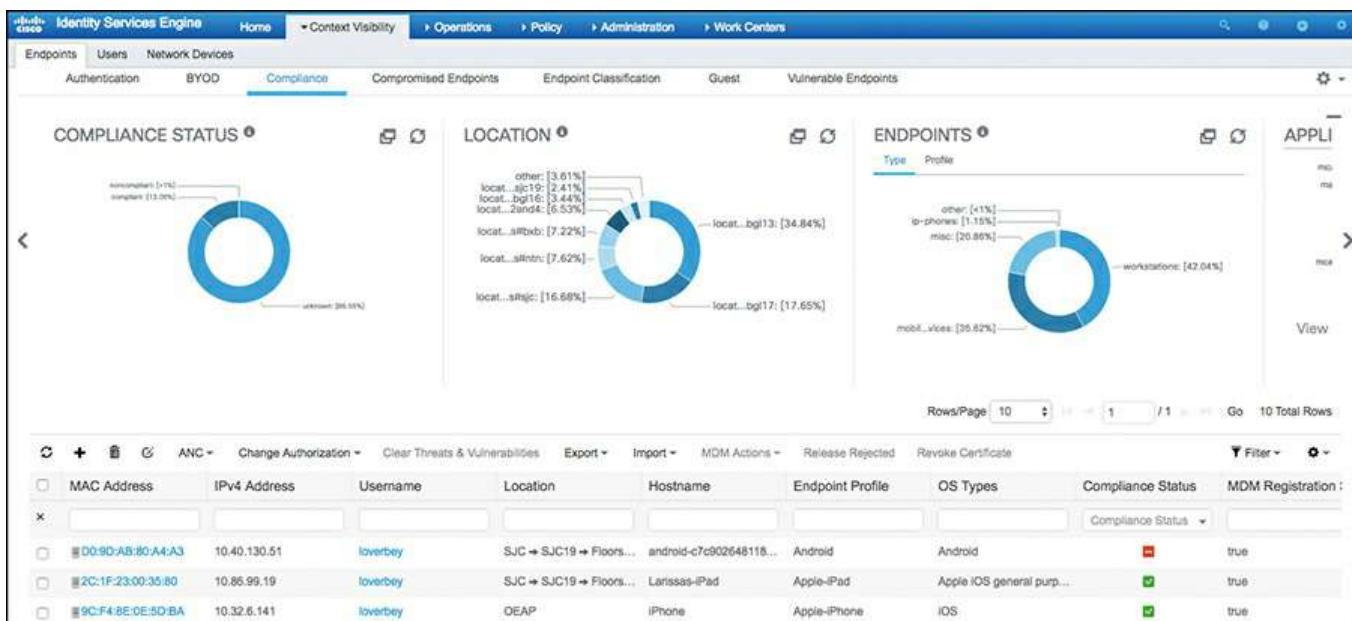
**Figure 25-3** ISE Threat Dashboard

## Context Visibility Views

Context Visibility views are a lot like dashboards except they are more customizable and provide you with a detailed results table that is actionable. There are three views available: Endpoints, Users, and Network Devices. Each view has multiple subviews to choose from. Context Visibility views are very useful when you need to get a live snapshot of what is happening, especially when you need the details. The most useful

section of the views is the results table at the bottom of the page.

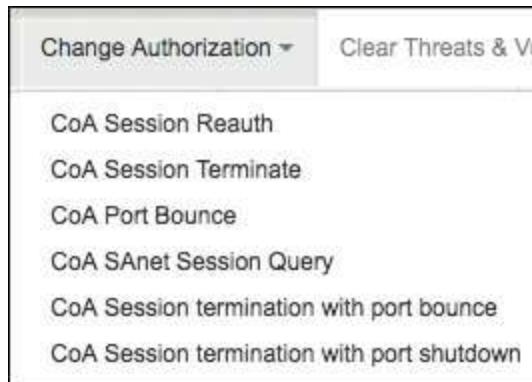
[Figure 25-4](#) shows the Endpoints view with the Compliance subview. It shows you the state of posture compliance for your endpoints.



**Figure 25-4** Context Visibility Views: Endpoints

The table at the bottom of [Figure 25-4](#) is searchable, sortable, and allows you to take immediate actions on endpoints when needed. There are two drop-down menus available above the table to take an action on an endpoint:

- **ANC (Adaptive Network Control):** Enables you to shut down, port bounce, or quarantine a host
- **Change Authorization:** Enables you to select the CoA options shown in [Figure 25-5](#)



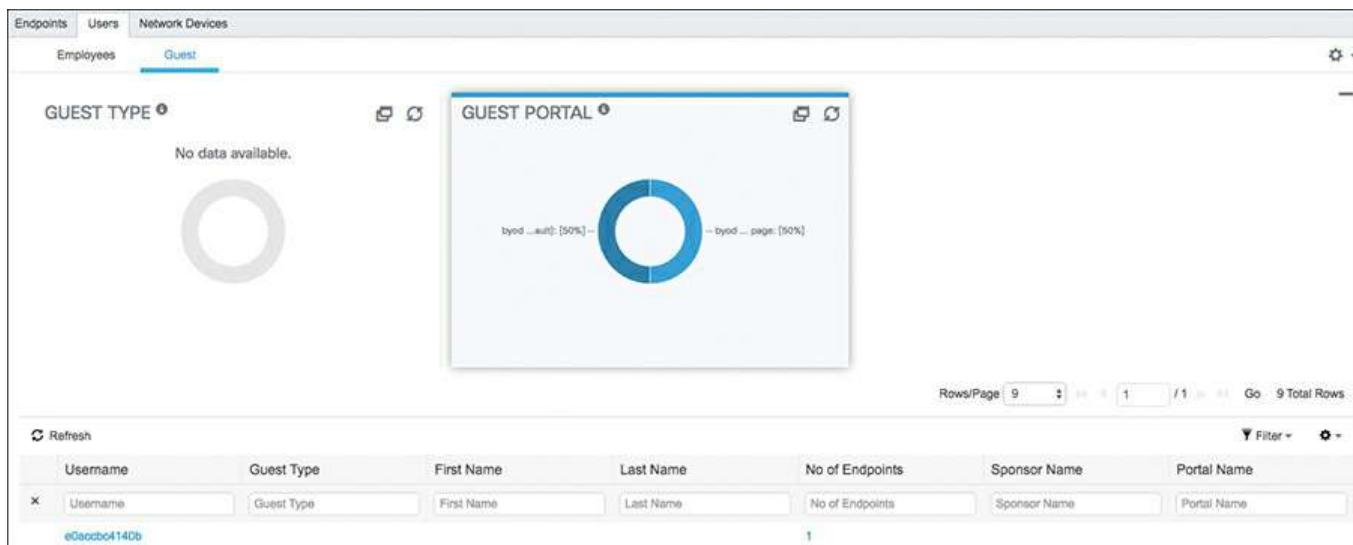
**Figure 25-5** Context Visibility Views: CoA Menu

If ISE is connected to your mobile device management (MDM) system, you can take MDM actions from here as well, via the MDM Actions menu (grayed out as unavailable)

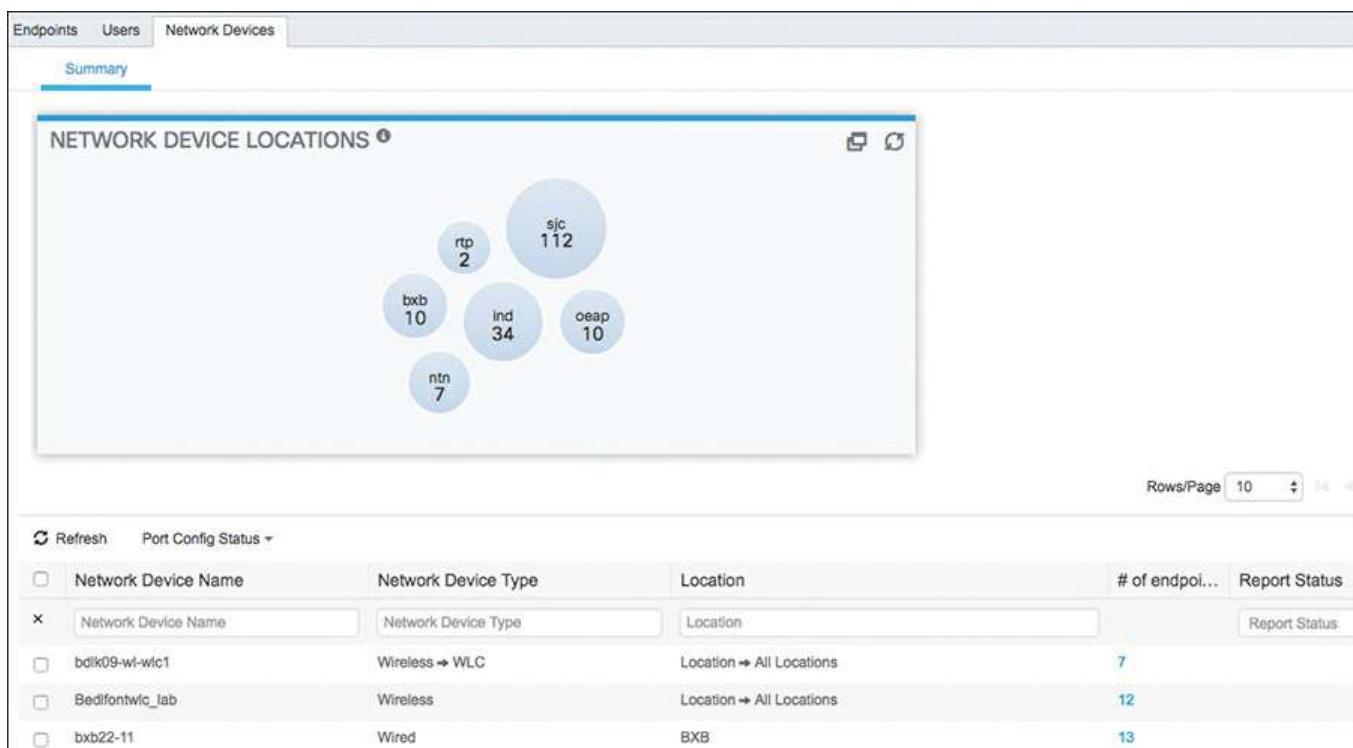
in [Figure 25-4](#)). ISE provides four actions it can send to your MDM vendor for execution: Corporate Wipe, Full Wipe, Pin Lock, and Refresh MDM Partner Endpoint. Next, from this view you can also revoke a certificate from the endpoint if it was given a certificate from the built-in ISE CA.

Finally, from here you can clear threats and vulnerabilities, export and import the table data, and release rejected hosts.

The other Context Visibility views, Users and Network Devices, are shown in [Figure 25-6](#) and [Figure 25-7](#), respectively.



**Figure 25-6** Context Visibility Views: Users



**Figure 25-7** Context Visibility Views: Network Devices

## RADIUS Live Logs and Live Sessions

The RADIUS Live Logs and Live Sessions views are perhaps the most useful monitoring and troubleshooting tools that ISE offers. These views are most useful for troubleshooting, which is covered in detail in [Chapter 26, “Troubleshooting.”](#) This section covers just the monitoring aspects of the Live Logs page. To bring up a live log, go to **Operations > RADIUS > Live Logs.** [Figure 25-8](#) displays the live log for RADIUS authentications, while [Figure 25-9](#) shows the Live Sessions page. The sessions page only shows you hosts that have a live and fully established session with ISE. Hosts in other stages of authentication or in error states do not appear here but appear in Live Logs.

This screenshot shows the RADIUS Live Logs page in the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under the Context Visibility tab, the RADIUS section is selected. Below the navigation, there are five summary metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (2), Client Stopped Responding (809), and Repeat Counter (0). A filter bar at the top right allows setting refresh intervals (Never, Every 1 minute, etc.) and showing latest records (Latest 20 records, Last 3 hours, etc.). The main table lists two entries, both from March 20, 2017, at 11:15:41.474 PM, showing successful RADIUS authentication (Status: OK) for endpoints with MAC addresses E0:D1:73:E0:2C:EF, connected to Cisco-IP-Phone-9971 and Cisco-IP-Phone-9962 respectively, with IP addresses 10.32.216.15 and 10.32.216.15, and assigned to Building\_SJC\_1.

**Figure 25-8** RADIUS Live Logs

This screenshot shows the RADIUS Live Sessions page in the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under the Context Visibility tab, the RADIUS section is selected. Below the navigation, there are five summary metrics: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (2), Client Stopped Responding (809), and Repeat Counter (0). A filter bar at the top right allows setting refresh intervals (Never, Every 1 minute, etc.) and showing latest records (Latest 20 records, Last 24 hours, etc.). The main table lists two entries, both from February 13, 2017, at 02:05:17.513 AM, showing sessions started (Action: Started) for endpoints with MAC addresses E0:D1:73:E0:2C:EF and D4:A0:2A:89:78:12, connected to Cisco-IP-Phone-9971 and Cisco-IP-Phone-9962 respectively, with IP addresses 10.32.216.15 and 10.32.216.15, and assigned to Building\_SJC\_1. An 'Actions' button is visible next to the endpoint ID column for each row.

**Figure 25-9** RADIUS Live Sessions

Both the Live Logs and Live Sessions views have extensive filtering options. A filter box appears at the top of each column. This filter box allows for complete or partial matches but not compound conditions. For example, you could input 00:13 in the Endpoint ID column filter, and it shows you all devices with 00:13 anywhere in their MAC address. You can also sort by time or status by clicking the column headers. In the top right, notice a few additional fields you can change: refresh rate, show number of records, and within a timeframe. You can also export any of these tables from ISE.

The RADIUS Live Sessions page also allows you to take actions such as CoA or

endpoint debugging, as shown in [Figure 25-9](#). For both of these pages, the filtering feature is your friend and makes finding what you want easier.

## Global Search

The global search box, positioned at the top of the ISE GUI, enables you to find endpoints. Here is a list of search criteria you can enter into the global search box:

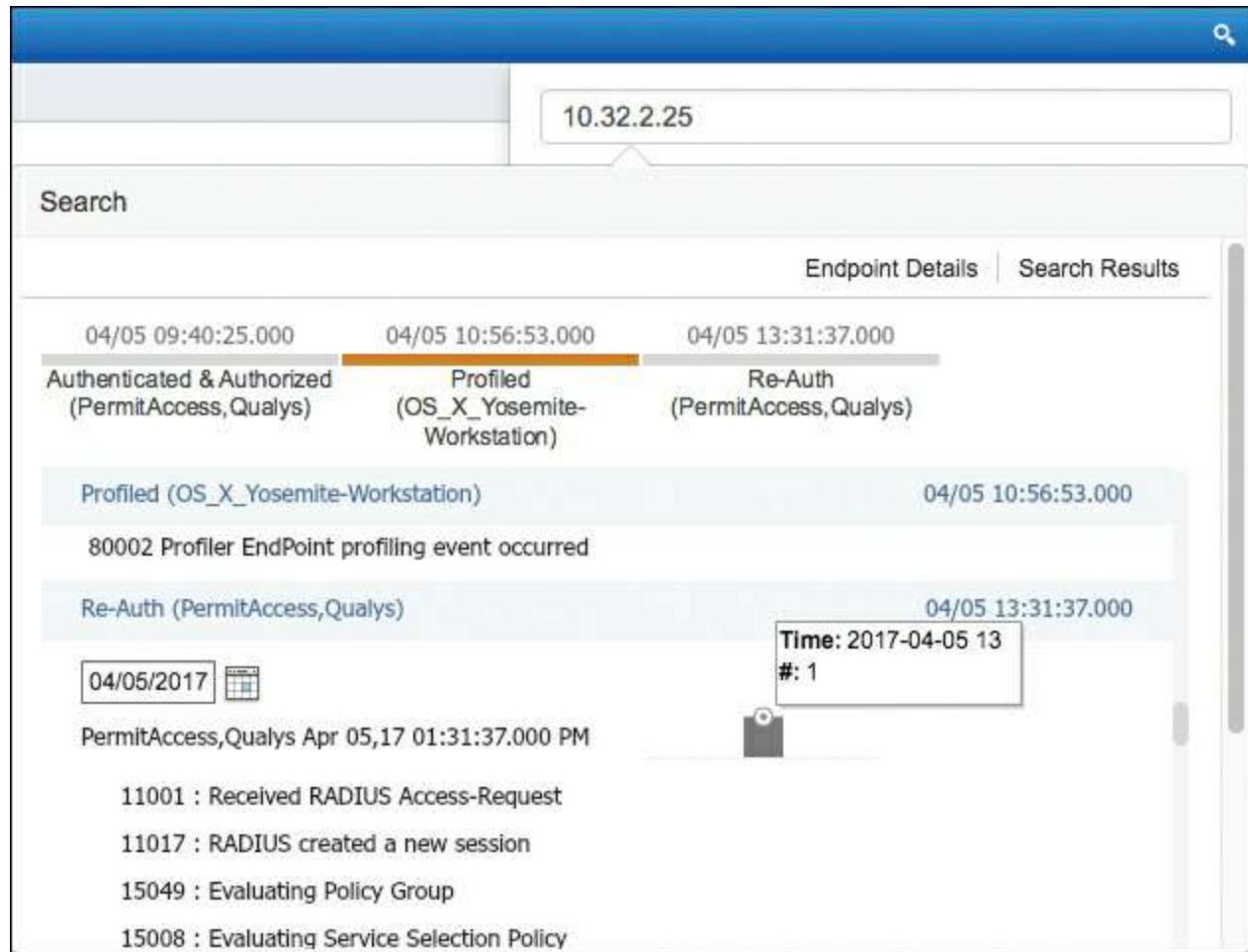
- Username
- MAC address
- IP address
- Authorization profile
- Endpoint profile
- Failure reason
- Identity group
- Identity store
- Network device name
- Network device type
- Operating system
- Posture status
- Location
- Security group
- User type

With global search, the most popular search criteria are username, device name, IP address, and failure reason. After the RADIUS Live log and Live Sessions views, global search is perhaps the most useful tool for helpdesk personnel when troubleshooting an issue with a user. Just enter the user's IP or username and the search query quickly finds the user's session and status. [Figure 25-10](#) shows the results of searching for an IP address.

The screenshot shows the Cisco Identity Services Engine (ISE) Global Search interface. At the top, there is a search bar containing the IP address "10.32.2.25". Below the search bar, a "Search" button is visible. A summary bar indicates "1 Connected | 0 Failed | 3 Disconnected | 4 Total". On the left, a sidebar titled "Distribution" lists various categories with their counts: Authorization Profile (1), Endpoint Profile (3), Identity Group (1), Identity Store (1), Location (1), Network Device (1), and Network Device Type (1). The main pane displays a list of endpoints ordered by recent activity. The first endpoint listed is "OS\_X\_Yosemite-Workstation", which is connected (indicated by a green checkmark) and has a location of "All Locations#SJC#S..." and device type "All Device Types#Wi...". It also has a "PermitAccess" status. The second endpoint is "Microsoft-Workstation", which is connected and has a location of "All Locations#SJC#S...", device type "All Device Types#Wi...", and "PermitAccess" status. The third endpoint is "Windows7-Workstation", which is connected and has a location of "All Locations#SJC#S...", device type "All Device Types#Wi...", and "PermitAccess" status. The fourth endpoint is another "Windows7-Workstation", which is connected and has a location of "All Locations#SJC#S...", device type "All Device Types#Wi...", and "PermitAccess" status.

Figure 25-10 ISE Global Search

The search result shows a detailed current status of the device. At the top, notice live statistics on connection status. Clicking the arrows icon by a device shows you the latest session trace page, as shown in [Figure 25-11](#). From there, click the **Endpoint Details** button or go back to the search results by clicking the **Search Results** button. Clicking Endpoint Details displays a wealth of information on the selected device, including authentication, accounting, posture, and profiler data. [Figure 25-12](#) presents an example of authentication data. Notice that there are several other tabs (Result, Other Attributes, and Steps) to see more info. All this data can be exported too, using the export button at the bottom (not shown in [Figure 25-12](#)).



**Figure 25-11** ISE Global Search: Session Trace

The screenshot shows a search results page for an endpoint. At the top, there's a search bar and a header with the IP address 10.32.2.25. Below the header, there are tabs for Session Trace and Search Results. Underneath, there are three buttons: Authentication (highlighted), Accounting, and Profiler. Below these buttons are four links: Details, Result, Other Attributes, and Steps. The main content is a table with two columns: Name and Value.

Name	Value
Source Timestamp	2017-04-05 13:31:34.773
Received Timestamp	2017-04-05 13:31:37.487
Policy Server	np odp02
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	pl ya
User Type	
Endpoint Id	A0:99:9B:08:86:29

**Figure 25-12** ISE Global Search: Endpoint Details

## Monitoring Node in a Distributed Deployment

In larger deployments, it is required to set up a dedicated ISE Monitoring node. A Cisco ISE node with this persona functions as the log collector and stores log messages from all the ISE Administration and Policy Service Nodes in your network. At least one node in your distributed setup must assume the Monitoring persona. It is a best practice to not have the Monitoring and Policy Service personas enabled on the same Cisco ISE node. It is recommended that, in a larger ISE deployment, you dedicate a pair of nodes to be Monitoring nodes.

## Device Configuration for Monitoring

For ISE to properly monitor your system, it must receive the appropriate information from network access devices. This requires that the NADs be configured properly. This section provides some examples of proper NAD configuration.

Cisco ISE monitoring requires that the logging source interface of a NAD be the same as the network access server (NAS) IP address configured in ISE. This allows ISE to correctly associate log messages with the proper NAD source. To accomplish this, configure the **source-interface** command on the NAD devices. The value of **source-**

**interface** should be the same as the NAS IP address configured in ISE. The NAD CLI command **logging source-interface** should match the NAD CLI command **ip radius source-interface** and/or **ip tacacs source-interface**. Here is the command syntax for IOS:

[Click here to view code image](#)

```
logging source-interface type number
!sets the IP address associated with fastethernet 0/1 as the syslog message
source.
logging source-interface fastethernet 0/1
```

The next command you want to have on your Cisco access switches is the global command **epm logging**. EPM is short for Enforcement Policy Module. EPM logging messages are displayed during the following switch events:

- **POLICY\_APP\_SUCCESS:** Policy application success events on named ACLs, proxy ACLs, service policies, and URL redirect policies
- **POLICY\_APP\_FAILURE:** Policy application failure conditions similar to unconfigured policies, wrong policies, download request failures, and download failures from AAA
- **IPEVENT:** IP assignment, IP release, and IP wait events for clients
- **AAA:** AAA events (similar to download requests or download successes from AAA)

Finally, you need to send switch syslog messages over to the ISE Monitoring node. Again, the source interface must be the ISE NAS IP. This configuration is straightforward:

[Click here to view code image](#)

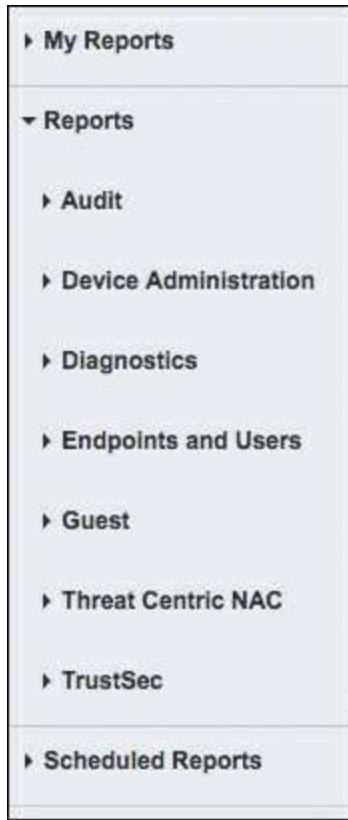
```
logging monitor informational
logging origin-id ip
logging source-interface interface_id
logging host ISE Monitoring Node IP transport udp port 20514
```

For a complete list of the NAD syslogs that ISE collects, see the ISE user guide on [cisco.com/go/ise](http://cisco.com/go/ise).

## ISE Reporting

The log data that ISE collects is organized and available in reports. The reports aggregate the data in useful ways so that you can get a longer-term view of ISE's operations. ISE provides a set of reports for you to use. Customization is possible in these reports. To see the ISE reports, go to **Operations > Reports**. As shown in [Figure 25-13](#), the ISE reports are grouped into categories. Each category has several reports

available. The My Reports category at the top of the list is where you save reports you customize or create. All reports are exportable, can be scheduled, and can be emailed.



**Figure 25-13** ISE Report Categories

Click any report to run it. You then use the report-specific filters to customize the contents of the report. [Figure 25-14](#) shows an example report.

RADIUS Authentications <small>?</small>					
From 2017-03-14 00:00:00.0 to 2017-03-21 01:29:30.150					
<small>Filter ▾ Refresh ⏪ Schedule ⏪</small>					
Logged At	RADIUS Status	Details	Identity	Endpoint ID	Endpoint Profile
Last 7 Days	>Last 7 Days	Details	Identity	Endpoint ID	Endpoint Profile
2017-03-21 00:28:49.475	✓	smrt	smtt	9C:F4:8E:D5:64:F7	Apple-iPhone
2017-03-21 00:28:45.818	✓	smrt	smtt	9C:F4:8E:D5:64:F7	Apple-iPhone
2017-03-21 00:28:41.476	✓	smrt	smtt	9C:F4:8E:D5:64:F7	Apple-iPhone
2017-03-21 00:28:41.016	✓	smrt	smtt	9C:F4:8E:D5:64:F7	Apple-iPhone
2017-03-21 00:28:25.474	✗	smrt	CP-7971G-GE-SEP0019E84FDAEB	00:19:E8:4F:DA:EB	

**Figure 25-14** ISE Example Report

In the upper right of the report screen, you see a few options:

- **My Reports:** Click to put this report into your My Reports folder.
- **Export To:** Click to export a version of the currently run report.
- **Schedule:** Click to display any scheduled reports in the left category pane under

Scheduled Reports, as shown in [Figure 25-13](#).

## Data Repository Setup

A data repository is a storage location that ISE can use to store non-system data such as reports, images, backup files, and so forth. If you don't already have a data repository set up or need to set up a new one, go to **Administration > System > Maintenance > Repository**. Click **Add**. [Figure 25-15](#) shows the repository setup.



**Figure 25-15** Creating a Data Repository

As you can see, there are many protocols you can use for data storage. Be careful when using DISK, as you may quickly run out of disk space on your ISE nodes. Any local repositories created on the Admin node are replicated to all other nodes. For more details on repositories, see [Chapter 27, “Upgrading ISE.”](#)

## ISE Alarms

ISE uses alarms to alert you to critical events or important system events. To create new alarms or customize alarms, go to **Administration > System > Settings > Alarm Settings**. Some alarms allow more customization than others, but all alarms allow you to enable or disable them. Alarms can send syslog and email messages. To customize an alarm, select the alarm and click **Edit**. [Figure 25-16](#) shows the Alarm Settings screen.

The screenshot shows the Cisco ISE GUI with the 'Administration' tab selected. Under 'Work Centers', 'Settings' is highlighted. On the left, a sidebar lists 'Client Provisioning', 'FIPS Mode', 'Alarm Settings', 'Posture', 'Profiling', 'Protocols', 'Proxy', and 'SMTP Server'. The main area is titled 'Alarm Settings' with tabs for 'Alarm Configuration' (selected) and 'Alarm Notification'. Below is a table with columns: 'Alarm Name', 'Category', 'Severity', 'Status', 'User Defined', and 'Conditions'. The table contains several rows of alarm configurations.

Alarm Name	Category	Severity	Status	User Defined	Conditions
AD Connector had to be restarted.	ISE Services	⚠️	✓	✗	
AD: ISE account password update failed	ISE Services	⚠️	✓	✗	
AD: ISE machine account does not have the required privileges to fetch..	ISE Services	⚠️	✓	✗	
AD: Machine TGT refresh failed.	ISE Services	⚠️	✓	✗	
Active Directory forest is unavailable	ISE Services	✗	✓	✗	

**Figure 25-16** Configuring ISE Alarms

When an alarm fires, it shows up in a couple places in the ISE GUI. The first place is on the Summary dashboard's Alarms dashlet. Clicking an alarm brings up the alarm details. Click **Acknowledge** to remove the alarm from the active alarms. At any given point in time, only the latest 15,000 alarms are retained. If you want to send alarms to an email address or to a syslog server, you must configure these services first. For syslog setup, go to **Administration > System > Logging > Remote Logging Targets** and click **Add**. For email, go to **Administration > System > Settings > SMTP Server** and fill in the email server details.

## Summary

This chapter explored the various monitoring, reporting, and alerting that ISE offers. It discussed key monitoring features, such as the ISE dashboards, dashlets, and the useful Live Log and Live Sessions views. Key reporting and alarm configuration settings and their usage were also reviewed. A firm understanding of the features and their operations will help ensure the successful operation of your ISE deployment.

# Chapter 26 Troubleshooting

This chapter covers the following topics:

- Diagnostic tools
- Troubleshooting methodology

Troubleshooting a product can sometimes get fairly complex. Troubleshooting a solution made up of multiple products is bound to get down-right difficult. The biggest tip we can give you is this: always stay calm, take your time, and think through the flows. Once you are comfortable with the Secure Access solution and how the parts work together, troubleshooting it really is not bad at all.

This chapter attempts to provide you with a strong foundation by introducing proven troubleshooting methodologies for the Secure Access solution and examining some of the built-in tools and tricks that have assisted us in the field.

With each version of ISE, there are new serviceability enhancements and tools created to ease the administrative burden that comes with troubleshooting. Tools are created and updated to make your life easier, based on direct feedback from customers, partners, and Cisco TAC.

Regardless of the version of ISE that you are using, and which tools are available, the methodology for troubleshooting shall remain the same. Let's repeat that statement: the methodology for troubleshooting remains the same, regardless of the version of ISE that you are using; it is only some of the tooling that might be different.

We'll start off by introducing some of the tools that are provided within ISE.

## Diagnostic Tools

Cisco ISE provides the following built-in tools to aid in your troubleshooting efforts:

- RADIUS Authentication Troubleshooting
- Evaluate Configuration Validator
- TCP Dump
- Endpoint Debug
- Session Trace

We'll look at each in turn.

## RADIUS Authentication Troubleshooting

The RADIUS Authentication Troubleshooting tool examines different aspects of a session and provides some additional details that may not have been available in the detailed authentication report. It also provides some suggestions for items to check next.

To use this tool, follow these steps from the ISE GUI:

**Step 1.** Navigate to **Operations > Troubleshoot > Diagnostic Tools > General Tools > RADIUS Authentication Troubleshooting**, as shown in [Figure 26-1](#).

Search and Select a RADIUS Authentication for troubleshooting.

Username:	<input type="text"/>	<input type="button" value="Select"/>	<input type="button" value="Clear"/>
MAC Address:	<input type="text"/>	<input type="button" value="Select"/>	<input type="button" value="Clear"/>
Audit Session ID:	<input type="text"/>	<input type="button" value="Clear"/>	
NAS IP:	<input type="text"/>	<input type="button" value="Select"/>	<input type="button" value="Clear"/>
NAS Port:	<input type="text"/>	<input type="button" value="Select"/>	<input type="button" value="Clear"/>
Authentication Status:	<input type="button" value="Fail"/>		
Failure Reason:	<input type="text"/>	<input type="button" value="Select"/>	<input type="button" value="Clear"/>
Time Range:	<input type="button" value="Today"/>		
Start Date-Time:	<input type="text"/> (mm/dd/yyyy) <input type="button" value="00:00"/>	hours	
End Date-Time:	<input type="text"/> (mm/dd/yyyy) <input type="button" value="24:00"/>	hours	
Fetch Number of Records:	<input type="button" value="100"/>		
<input type="button" value="Search"/>			

**Search Result**

Time	Status	Username	MAC Address	Audit Session ID	Network Device IP	Failure Reason
2013-01-14 14:48:18,119	x	[REDACTED]	00:1C:58:CD:3A:E9	ab462383000128ec50f40e09	171.70.35.131	24408 User authentication against
2013-01-14 14:48:13,809	x	[REDACTED]	00:22:90:FD:CC:C2	ab46238300012c2550f48407	171.70.35.131	24408 User authentication against
2013-01-14 14:48:08,184	x	[REDACTED]	00:1C:58:CD:3A:E9	ab462383000128ec50f40e09	171.70.35.131	24408 User authentication against
2013-01-14 14:48:03,751	x	[REDACTED]	00:22:90:FD:CC:C2	ab46238300012c2550f48407	171.70.35.131	24408 User authentication against
2013-01-14 14:47:58,156	x	[REDACTED]	00:1C:58:CD:3A:E9	ab462383000128ec50f40e09	171.70.35.131	24408 User authentication against
2013-01-14 14:47:53,923	x	[REDACTED]	00:22:90:FD:CC:C2	ab46238300012c2550f48407	171.70.35.131	24408 User authentication against

**Figure 26-1** RADIUS Authentication Troubleshooting Tool

**Step 2.** From here you may select any number of specifics to limit your search, such as a specific username, failed or passed authentication status, and more. Click **Search**.

**Step 3.** Select one of the entries presented as the result of the search, scroll to the bottom, and click **Troubleshoot**.

ISE examines aspects of the session details, looks for possible causes of an issue, and offers suggestions on possible fixes, as shown in [Figure 26-2](#).

**Diagnosis and Resolution**

**Diagnosis**  
User authentication against Active Directory failed since user has entered the wrong password

**Resolution**  
Check the user password credentials. If the RADIUS request is using PAP for authentication, also check the Shared Secret configured for the Network Device

**Troubleshooting Summary**

Investigated authentication record with details:

Details	
Timestamp	2013-01-14 14:48:18.119
ISEServer	npf-sjc14-pdp01
Username	[REDACTED]
MAC Address	00:1C:58:CD:3A:E9
Status	Failed
Failure Reason	24408 User authentication against Active Directory failed since user has entered the wrong password
Network Device Name	WNBU-sjc14-00a-homeap1
Network Device IP	171.70.35.131
Identity Store	CiscoAD
Identity Group	
NAS Port ID	
Audit Session ID	ab462383000128ec50f40e09
Authentication Method	dot1x

Investigated failure code: 24408 User authentication against Active Directory failed since user has entered the wrong password

[Show Progress Details](#) [Done](#)

**Figure 26-2 RADIUS Authentication Troubleshooting Tool (Continued)**

In this simple example, either the user has mistyped their password or the shared secret is incorrect between the network access device (NAD) and ISE. Differentiating which is truly the cause is impossible because the shared secret is used to encrypt the password between the endpoint and the RADIUS server, and the result of a mismatched shared secret is the same as the result of an incorrect password.

## Evaluate Configuration Validator

This is a great tool...with a terrible name. This tool connects to a switch via Telnet, Secure Shell (SSH), or even through a console server. It examines the configuration, compares it to a “template” configuration built into ISE, and then reports any differences between the configurations. At the time of writing, the tool was overdue for an update, as explained next, but it still may provide a lot of value.

The following list explains why Evaluate Configuration Validator may misdiagnose as missing or incorrect a few of the common configurations:

- Evaluate Configuration Validator does not currently understand Device Sensor, and expects the use of SNMP for the SNMP probe(s).
- Evaluate Configuration Validator does not recognize the active test options when defining a RADIUS server, and therefore may think the RADIUS server definition is incorrect.

- WebAuth is Local WebAuth only, and the tool does not recognize that MAC Authentication Bypass (MAB) is used for Centralized WebAuth instead.

Even with the limitations listed, this tool is still recognized by Cisco Technical Assistance Center (TAC) as being useful for quickly identifying a high number of misconfigurations, and in many cases would have prevented a customer from opening the TAC case.

The following steps show you how to run the Evaluate Configuration Validator tool from the ISE GUI:

**Step 1.** Navigate to **Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator** to access the tool, shown in [Figure 26-3](#).

The screenshot shows the 'Evaluate Configuration Validator' window. At the top, there is a field labeled 'Network Device IP:' containing '192.168.254.60' with a 'Clear' button next to it. Below this, a message says 'Select the configuration items below that you want to compare against the recommended template.' A list of configuration items follows, each with a checkbox:

Configuration Item	Status
AAA:	<input checked="" type="checkbox"/>
RADIUS:	<input checked="" type="checkbox"/>
Device Discovery:	<input checked="" type="checkbox"/>
Logging:	<input checked="" type="checkbox"/>
Web Authentication:	<input type="checkbox"/>
Profiler Configuration:	<input checked="" type="checkbox"/>
CTS:	<input type="checkbox"/>
802.1X	<input checked="" type="checkbox"/>
Open Mode:	<input checked="" type="radio"/>
Low Impact Mode (Open Mode + ACL):	<input type="radio"/>
High Security Mode (Closed Mode):	<input type="radio"/>

At the bottom left is a 'Run' button.

**Figure 26-3** Evaluate Configuration Validator

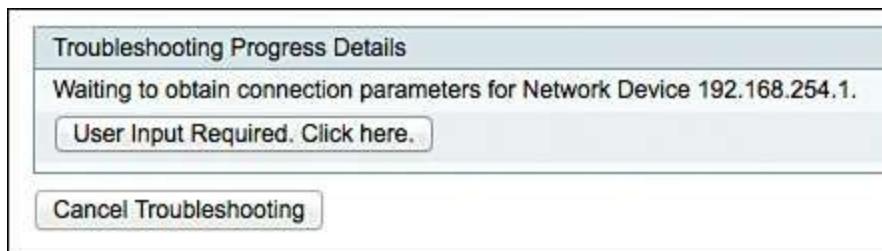
**Step 2.** Enter the IP address of the NAD, and choose which options you would like the tool to examine.

In [Figure 26-3](#), the check box for Web Authentication is unchecked because the tool is hard-coded to look for Local WebAuth (LWA), and not Centralized WebAuth (CWA).

**Step 3.** Click **Run** to begin the evaluation.

**Step 4.** ISE connects to the switch, and prompts for your interaction if the switch asks

for user authentication or other interactive prompts, as shown in [Figure 26-4](#). If prompted, click the **User Input Required** button, enter your credentials in the dialog box shown in [Figure 26-5](#), and then click **Submit**.



**Figure 26-4** User Input Required

Specify Connection Parameters for Network Device 192.168.254.1:  
(Available parameters are prepopulated.)

Username:

Password:  .....

Protocol:  Telnet

Port:  23

Enable Password:

Same as login password.

Use Console Server:

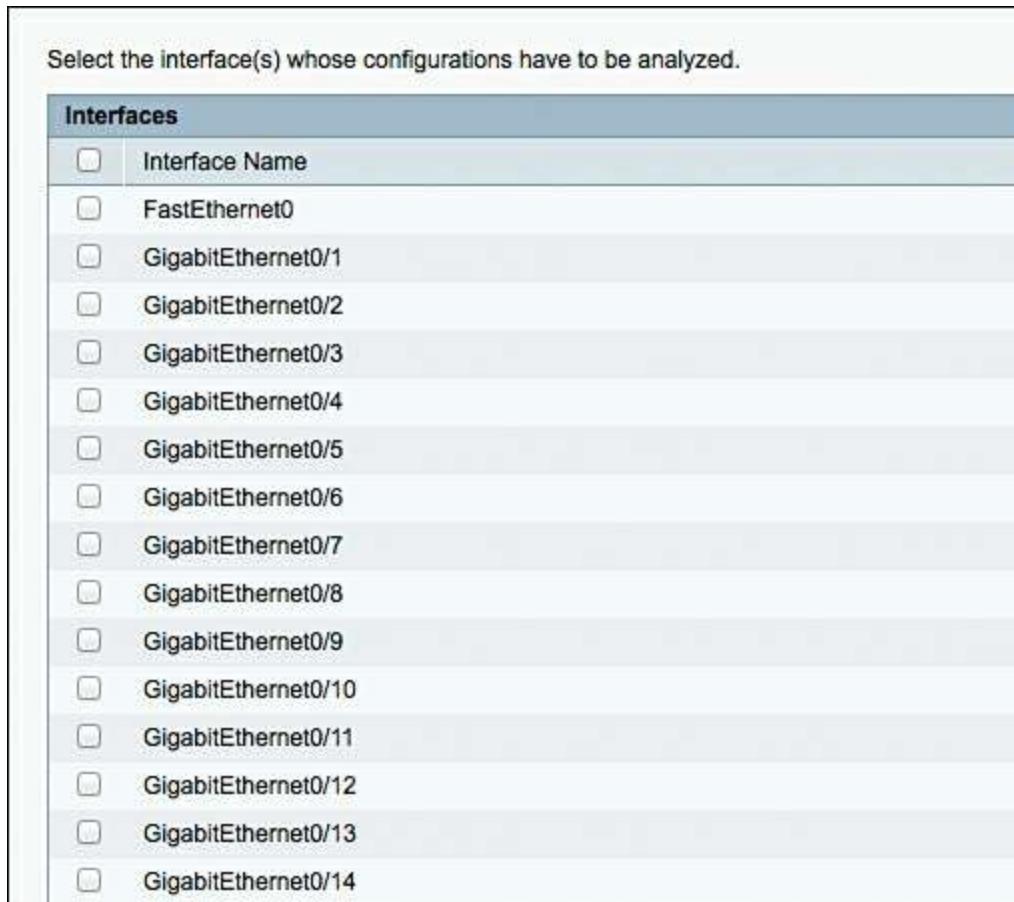
Console IP Address:

(Enter console port in the above "Port" input field, when "Use Console Server" option is selected.)

► Advanced (Use these if you see a 'Expect timeout error' or you know that the device has non-standard prompt strings)

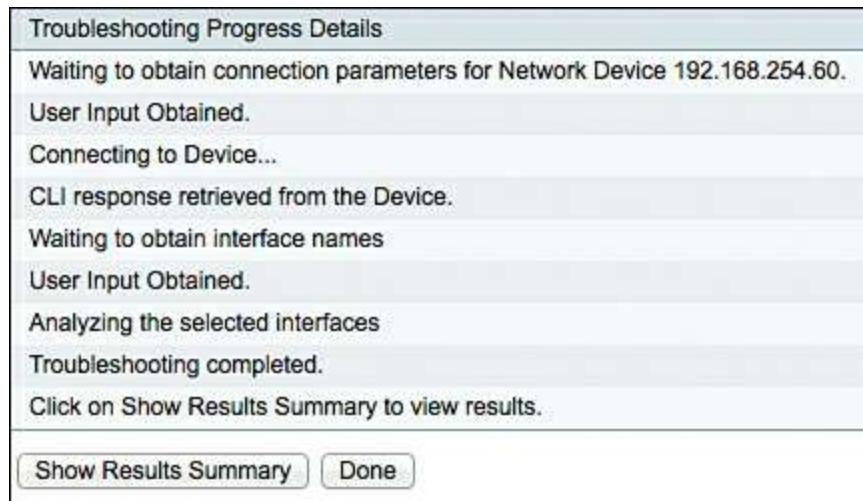
**Figure 26-5** Entering Credentials

**Step 5.** You should be prompted to select which interfaces you want to compare, as shown in [Figure 26-6](#). If you have followed the guidelines set forth in this book, nearly every interface will have the exact same configuration, so you should only select one interface to compare, and then scroll to the bottom and click **Submit**.



**Figure 26-6** Select an Interface

**Step 6.** After the comparison is completed, click **Show Results Summary** to see the results, as shown in [Figure 26-7](#).



**Figure 26-7** Comparison Complete

The report will be broken down into sections, as shown in [Figure 26-8](#), and anything found to be missing or incorrect will be displayed in red. At this point, it is up to you to be familiar with your own deployment. For instance, you should know whether you truly

need the SNMP community strings or are using Device Sensor instead.

✓	Running Configuration		
✓	AAA Configuration (Global)		
✓	RADIUS Configuration (Global)		
✗	Device Discovery Configuration (Global)		
	Details		
Mandatory	Expected	Configuration Found On Device	
✗	ip dhcp snooping vlan <Vlan_ID_for_DHCP_Snooping>	Missing	
✗	no ip dhcp snooping information option	Missing	
✗	ip dhcp snooping	ip dhcp snooping	
✗	ip device tracking	ip device tracking	
✓	Logging Configuration (Global)		
✗	Profiler Configuration (Global)		
	Details		
Mandatory	Expected	Configuration Found On Device	
✗	snmp-server community <snmp_ro_string> RO	snmp-server community <b>CiscoPressRO</b> RO	
✗	snmp-server community <snmp_ro_string> RW	Missing	
✗	snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart	Missing	
✗	snmp-server host <snmp_host1> public	Missing	
✗	snmp-server host <snmp_host1> mac-notification snmp	Missing	
✗	mac address-table notification change	mac address-table notification change	
✗	mac address-table notification change interval 0	Missing	
✗	Interface GigabitEthernet0/2		
	Details		
802.1x Commands	Mandatory	Expected	Configuration Found On Device

**Figure 26-8 Results Summary**

## TCP Dump

When troubleshooting 802.1X, in order to get a better understanding of what is transpiring, it is often necessary to go deeper than the GUI and Live Logs would normally allow you to do. This is where packet captures come in very handy. We have personally used Wireshark more times than we can count to get a deep view of what is transpiring, such as whether ISE is even receiving the RADIUS message; what the certificate signing request (CSR) of the client actually looks like; and much more.

Cisco includes TCP Dump in ISE and even provides a fantastic way to grab TCP Dumps from any ISE node on the deployment, right from the main Admin GUI! TCP Dump also enables you to filter the capture, such as by specifying **ip host 10.1.40.60** (as shown in [Figure 26-9](#)). We use this filter all the time so that we can limit the traffic to just the NAD that we are troubleshooting with.

## TCP Dump

Monitor the packet headers on the network and save to a file (up to 500,000 packets)

Status - Stopped Start

Host Name atw-cp-ise04 ▼

Network Interface GigabitEthernet 0 ▼

Promiscuous Mode  On  Off

Filter ip host 10.1.40.60

Example: 'ip host helios and not iceburg'

Format Raw Packet Data ▼

---

### Dump File

Last created on Tue Jan 22 22:19:56 UTC 2013

File size: 24 bytes

Format: Raw Packet Data

Host Name: atw-cp-ise04

Network Interface: GigabitEthernet 0

Promiscuous Mode: On

Filter: ip host 192.168.40.60

Download

Delete

**Figure 26-9** TCP Dump

To set a TCP Dump capture, perform the following steps:

**Step 1.** Navigate to **Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump.**

**Step 2.** From the Host Name drop-down list, choose which ISE node to grab the TCP Dump from.

**Step 3.** From the Network Interface drop-down list, choose which interface on that ISE node should be used.

**Step 4.** Click the **On** radio button for Promiscuous Mode if you want to grab all traffic seen on the interface, even if it's not destined for ISE. So, if you have a Switched

Port Analyzer (SPAN) set up for one of the ISE interfaces, you could capture all traffic seen on that SPAN interface.

**Step 5.** In the Filter field, you can accept any standard TCP Dump filter, and limit the traffic captured.

Here is a link for TCP Dump filters: <http://bit.ly/Va243S>.

**Step 6.** From the Format drop-down list, choose the file format:

**Human Readable:** Choosing this option will format the file as XML, which can be used when a sniffer tool (such as Wireshark) is unavailable. **Raw Packet Data:** This will save the file as a pcap (common packet capture format) and can be opened in the sniffer tool of your choice.

**Step 7.** Click **Start** to begin the capture.

**Step 8.** Click **Stop** to end the capture.

**Step 9.** Click **Download** to initiate a download of the pcap file.

**Step 10.** Click **Delete** if you want to delete the pcap file from ISE. Only one capture may be stored at a time, and starting a new capture will automatically overwrite the existing one.

## Endpoint Debug

ISE can be quite large and distributed in nature. Even with a single ISE node, there are many different components within ISE that might be in use for any network session. These components include, among many others, Guest for all web portal traffic as well as guest account creation and sponsorship; Posture for checking the compliance of an endpoint; Profiler to help identify what type of endpoint it is; and RADIUS run times for the processing of incoming access requests.

As you go through the troubleshooting methodology within this chapter, there might come a time when you have to set the logging level of a particular component to debug and examine those debug logs within ISE. As you are likely to discover, there are so many logs and so many logging categories within ISE that searching through all those separate logs to find the entries that pertain to the endpoint, user, or session in question is often quite burdensome.

This is where Endpoint Debug comes into play. It was designed by Aaron Woland and a leader within Cisco TAC named Jesse Dubois. The purpose of this tool is to enable you, the ISE administrator, to easily and effectively troubleshoot an endpoint's activity with ISE in its entirety.

The Endpoint Debug tool provides a single debug file for all components of a specific endpoint across its entire session—across the entire deployment!

So, if an endpoint is getting profiled in the East-Coast Data Center and the West-Coast

Data Center at the same time, all of that information will still show up in the single, consolidated debug file. It disburdens you from having to enable debug on the components themselves for all endpoints, and it focuses the debug on the specific endpoint and its related session activity instead. This is incredibly elegant, and it helps advanced admins and TAC engineers to greatly reduce time to resolution when experiencing an issue.

There are two ways to launch the Endpoint Debug tool. The first method (and the most cumbersome) is as follows:

**Step 1.** Navigate directly to **Operations > Troubleshoot > Diagnostic Tools > EndPoint Debug**.

**Step 2.** Click either the **MAC Address** radio button or **IP** radio button.

**Step 3.** Enter the endpoint's address.

**Step 4.** Click **Start**.

[Figure 26-10](#) shows the Endpoint Debug screen.

The screenshot shows the 'Endpoint Debug' configuration screen. At the top, there is a status indicator showing 'Status: Stopped' with a red 'Stop' button and a blue 'Start' button. Below this, there are two radio buttons: 'MAC Address' (selected) and 'IP'. An input field contains the MAC address '28:CF:E9:1B:A7:B7'. To the right of the input field is an 'Info' icon. Below the radio buttons is a checked checkbox for 'Automatic disable after' followed by a '10' input field and a 'Minutes' label, with an 'Info' icon next to it. At the bottom of the screen, there is a table listing files. The table has columns for 'File Name', 'Host Name', 'Modified Date', and 'Size (Bytes)'. The table shows the following data:

File Name	Host Name	Modified Date	Size (Bytes)
28-cf-e9-1b-a7-b7	npf-sjca-pap02	Nov 18 13:33	736
28-cf-e9-1b-a7-b7.cert	npf-sjca-pdp01	Nov 18 13:29	1866
28-cf-e9-1b-a7-b7	npf-sjca-pdp01	Nov 18 13:35	1189260
2c-1f-23-00-35-80	npf-sjca-pap01	Oct 10 13:23	2590
2c-1f-23-00-35-80.cert	npf-sjca-pdp01	Nov 10 14:36	1866
2c-1f-23-00-35-80	npf-sjca-pdp01	Nov 10 14:37	845054

**Figure 26-10** Endpoint Debug

The second (and easiest) method to launch Endpoint Debug is to navigate to **Operations > RADIUS > Live Logs**, click the Actions target icon for the endpoint you want to debug, and click **Endpoint Debug** from the list of available options, as shown in [Figure 26-11](#).



**Figure 26-11** Endpoint Debug from Live Logs

When you use the option to launch Endpoint Debug from Live Logs, the tool automatically launches in a new window with the address for the endpoint displayed.

When you run Endpoint Debug, it creates a single file for the endpoint on each ISE node where that endpoint was active. All files are listed in the single GUI, as you can see in [Figure 26-10](#). To view one of the files, click the filename and you will be prompted to download just the single file or to combine all the files from all the nodes into a single file for download and easier consumption.

If a certificate was used in the authentication, that captured certificate is listed with the same filename and a .cert extension. The certificate will be downloaded in Privacy Enhanced Electronic Mail (PEM) format so you can more easily examine it. [Figure 26-10](#) also shows two examples of .cert files in the list.

## Session Trace

The Session Trace tool is brand new for ISE 2.2, and is comparable to Packet Tracer, a feature in the ASA firewall and ASDM GUI that enables an administrator to test what the firewall would be expected to do with a packet matching certain traits. Session Trace is that tool for ISE.

The tool was designed by Aaron Woland, Jesse Dubois, and Vivek Santuka from TAC, along with a slew of developers at Cisco including Douglas Gash and Eyal Keren, among others. This is a tool that administrators, partners, and technical marketing engineers (TMEs) have been begging for since ISE 1.0, and it's so exciting to have it in the product now.

Just like the Endpoint Debug tool, there are two ways to launch Session Trace. You can navigate directly via **Operations > Troubleshoot > Diagnostic Tools > Session Trace Tests**. Much like using this method to launch the Endpoint Debug tool, you then have to create your test from scratch.

The easier option is to start with an existing session. You can launch the Session Trace tool, with the test prepopulated with all the attributes of an existing session, right from the Live Logs screen, as shown in [Figure 26-12](#).

Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticated...	Authorized...
				Endpoint ID	Endpoint Prof...	Authenticator	Authorization
●	○	○	○	AC:37:43:A1:54:3D	HTC-Device	Default >> D...	Default >> E...
●	○	○	○	AC:37:43:A1:54:3D	Default	Default >> D...	Default >> E...
●	○	○	○	00:50:56:8B:B1:C7	Microsoft-W...	Default >> M...	Default >> B...
●	○	○	○	00:50:56:8B:B1:C7	Microsoft-W...	Default >> M...	Default >> B...
●	○	○	○	00:50:56:A1:3D:5A	Microsoft-W...	Default >> M...	Default >> B...
●	○	○	○	00:50:56:A1:3D:5A	Microsoft-W...	Default >> M...	Default >> B...
●	○	○	○	00:50:56:A1:3D:5A	Microsoft-W...	Default >> M...	Default >> B...
●	○	○	○	00:50:56:A1:3D:5A	Microsoft-W...	Default >> M...	Default >> B...

**Figure 26-12** Launching Session Trace Test from Live Logs Screen

The Session Trace tool opens with the Test Setup tab displayed, as shown in [Figure 26-13](#). The box labeled 1 is prepopulated with the attributes of the session you chose from Live Logs. You can add other attributes by using the Custom Attributes drop-down lists (identified as 2). The box labeled 3 is the summary of all attributes.

Session Trace Test Cases > New

**Session Trace Test Case**

Test Setup Run Test Previous Runs

Name \* Employee1-GooglePIXEL

Description This was pre-populated from Live Log

Predefined Test Select type (optional) ②

Custom Attributes ①

- Radius.Calling-Station-ID=ac-37-43-a1-54-3d
- Radius.User-Name=employee1
- Radius.Service-Type=Framed
- Radius.NAS-IP-Address=10.1.60.2
- Radius.NAS-Port-Type=Wireless - IEEE 802.11
- Network Access.NetworkDeviceName=WLC02
- Network Access.Protocol=RADIUS
- Radius.NAS-Port=2

Summary of all attributes ③

- Radius.Calling-Station-ID=ac-37-43-a1-54-3d
- Radius.User-Name=employee1
- Radius.Service-Type=Framed
- Radius.NAS-IP-Address=10.1.60.2
- Radius.NAS-Port-Type=Wireless - IEEE 802.11
- Network Access.NetworkDeviceName=WLC02
- Network Access.Protocol=RADIUS
- Radius.NAS-Port=2
- Radius.Framed-MTU=1300
- Radius.State=37CPMSessionID=0a013c02000004a585c8a26:34SessionID=altw-ise237/271579291/938;
- Radius.Acct-Session-Id=585c8a26/ac:37:43:a1:54:3d/75

Cancel Submit

**Figure 26-13** Test Setup

The Test Setup tab enables you to modify any of the attributes. For example, you could try a different username, or try changing the endpoint profile. This allows you to play with “what-if” scenarios to see what authentication and authorization rules would be

used, in which policy sets, and what the end result would be.

Clicking **Submit** brings you to the Run Test tab of the tool, where you can select which ISE node to run the test against, as shown in [Figure 26-14](#).

The screenshot shows a web-based application titled "Session Trace Test Cases > New". The main title is "Session Trace Test Case". Below it, there are three tabs: "Test Setup", "Run Test" (which is highlighted in blue), and "Previous Runs".  
  
The "Test Name" field contains "Employee1-GooglePIXEL".  
The "ISE Node" dropdown menu is set to "atw-ise237.securitydemo.net".  
  
A large green "Run" button is prominently displayed.  
  
At the bottom left, there is a link labeled "User Groups & Attributes".

**Figure 26-14** Run Test

Click **Run** to execute the test, and the results are displayed right on the same page, as shown in [Figure 26-15](#).

Session Trace Test Cases > New

### Session Trace Test Case

Test Setup Run Test Previous Runs

Test Name: Employee1-GooglePIXEL

ISE Node: atw-ise237.securitydemo.net

**Run**

Policy Stage	Matching Rule	Result Object(s)
Policy Set		Default
Authentication Policy (Allowed Protocols)	Dot1X	Default Network Access
Authentication Policy (Identity Selection)	Default	All_User_ID_Stores
Authorization policy	Basic_Authenticated_Access	PermitAccess

User Groups & Attributes

**Figure 26-15 Executed Test Results**

The executed test is saved in the Previous Runs tab, as shown in [Figure 26-16](#).

Session Trace Test Cases > New

### Session Trace Test Case

Test Setup Run Test Previous Runs

View/Compare Trash

	Time	Authentication Policy ...	Allowed Protocol	Authorization Profile
<input type="checkbox"/>	12/22/16 6:28...	Dot1X	Default Network Access	PermitAccess

**Figure 26-16 Previous Runs**

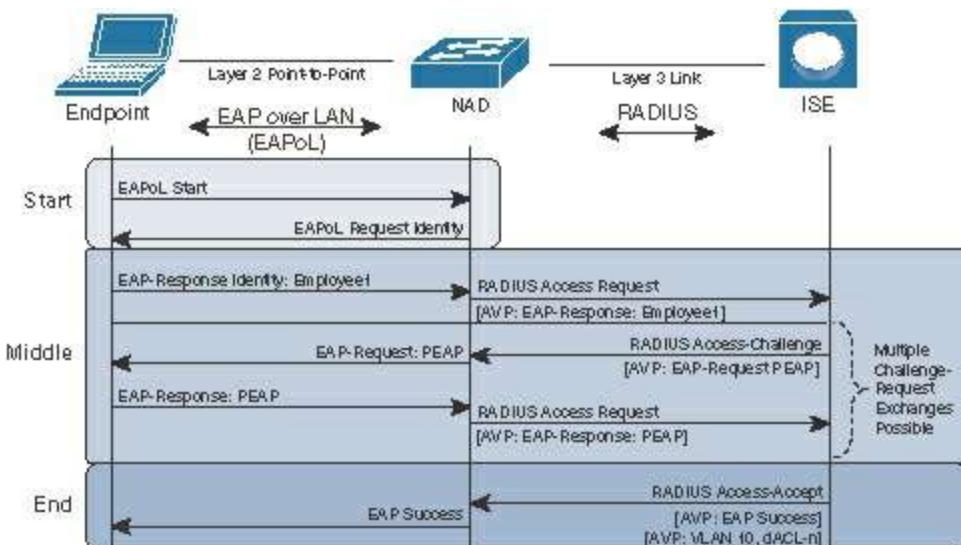
## Troubleshooting Methodology

As you read this section, keep in mind the tip from the beginning of the chapter: always stay calm, take your time, and think through the flows. Taking your time may sound counterproductive, but when you rush to fix a problem, you often end up taking much longer. There have been many situations where we were asked to help when “it just isn’t working,” and by staying calm, taking our time, and thinking through the flows, we came to the solution very quickly.

This section examines some common troubleshooting exercises and how to resolve the problems.

## Troubleshooting Authentication and Authorization

This section offers some possible options and solutions to a common complaint that a help desk or IT administrator may hear: “I plugged into the network, but my system is not granted access.” As you read this section, your focus should be on understanding the methodology and the secure access flow. Always keep the authentication and authorization flows in mind, as shown in [Figure 26-17](#).



**Figure 26-17 Basic Authentication and Authorization Flows**

## Log Deduplication

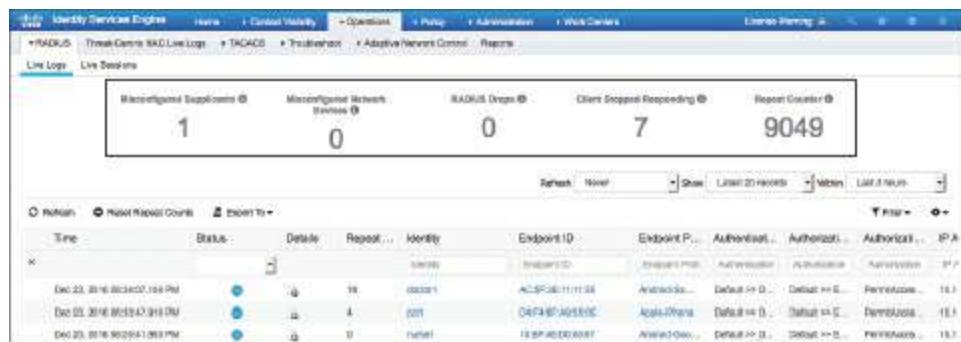
Prior to ISE 1.2, every authentication request created a 12-KB log record that was then stored. In a scenario where bad endpoint behavior was causing millions of failed authentications a day, a lot of log data was stored.

Beginning in ISE 1.2, ISE suppresses anomalous clients by default, only storing a single

record and then logging each time that same exact record is received. This saves a tremendous amount of processing and log storage and provides for higher scale.

The deduplication feature is a very nice and welcome change, but it did leave a few gaps to be addressed. Live Logs is the first screen that you would use when troubleshooting a login problem; however, if the entries are not showing up in Live Logs because they are being suppressed, it leaves the admin in a very bad position with no visibility into what's going on.

So, ISE added key counters at the top of the Live Logs screen to help provide visibility. You can see those counters in [Figure 26-18](#).

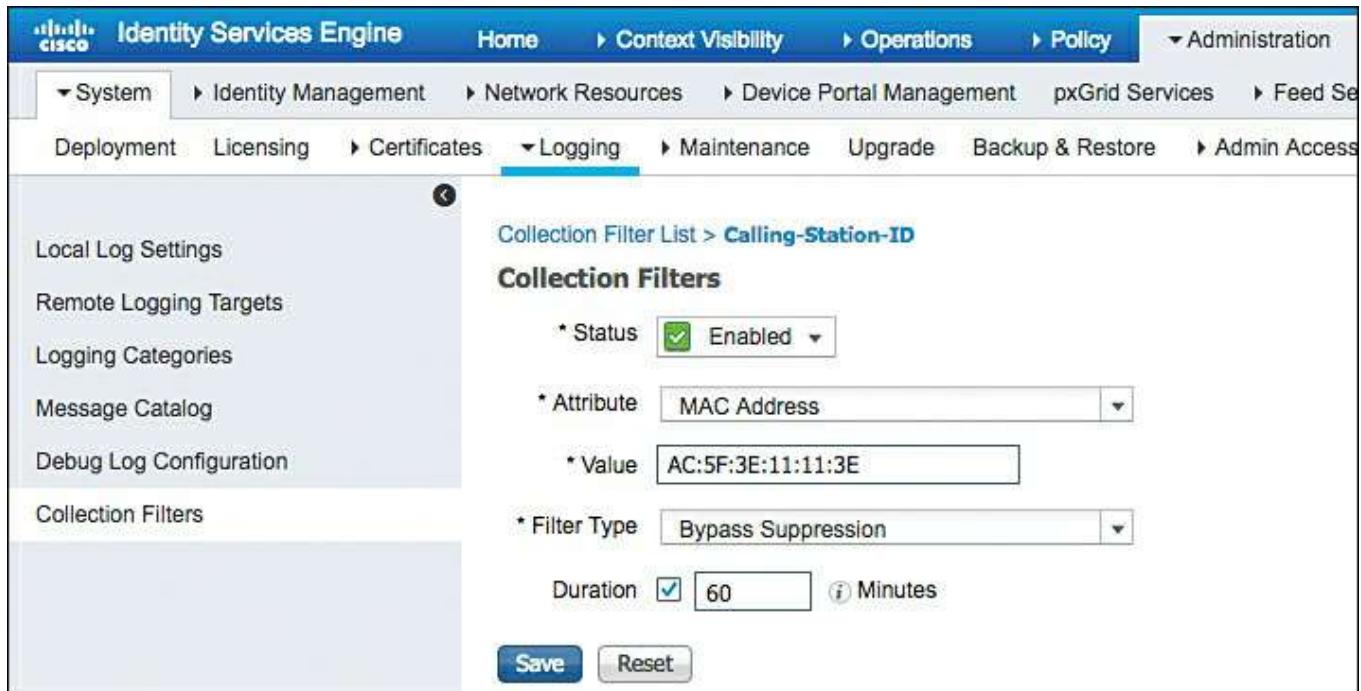


**Figure 26-18** Counters in Live Logs

Although the counters improve quick visibility from the Live Logs screen, troubleshooting is still quite difficult when the log entries are not appearing in the tool. There are two main ways to disable deduplication so that the log entries appear in Live Logs and you can be more effective in troubleshooting. The main way is to click the **Actions** target icon from Live Logs and choose **Bypass Suppression Filtering for 1 Hour**, as shown in [Figure 26-19](#). This automatically sets a collection filter for the endpoint that bypasses the deduplication for 60 minutes. After that hour, suppression is reenabled for that endpoint. Also shown in [Figure 26-19](#) is the option **Modify Collection Filters**, which opens a screen that allows you to change an existing filter to extend the duration of time the filter is disabled (and more), as shown in [Figure 26-20](#).



**Figure 26-19** Bypass Suppression Filtering for 1 Hour



**Figure 26-20** Collection Filters

The deduplication is a global setting that can be disabled; however, we do not recommend disabling the suppression in production networks without direction from Cisco TAC. The setting is found under **Administration > System > Settings > Protocols > RADIUS**, as shown in [Figure 26-21](#).

**RADIUS Settings**

Suppression & Reports	UDP Ports	DTLS
<b>SUPPRESS REPEATED FAILED CLIENTS</b>		
<input checked="" type="checkbox"/> Suppress repeated failed clients <small>i</small>		
Detect two failures within	5	minutes (1 - 30)
Report failures once every	15	minutes (15 – 60)
<input checked="" type="checkbox"/> Reject RADIUS requests from clients with repeated failures <small>i</small>		
Failures prior to automatic rejection	5	(2-100)
Continue rejecting requests for	60	minutes (5 – 180)
Ignore repeated accounting updates within	5	seconds (1 - 86,400)
<b>SUPPRESS SUCCESSFUL REPORTS</b>		
<input checked="" type="checkbox"/> Suppress repeated successful authentications <small>i</small>		
<b>AUTHENTICATION DETAILS</b>		
Highlight steps longer than	1,000	milliseconds (500 - 10,000)

**Figure 26-21 RADIUS Settings**

Examining [Figure 26-21](#) further, there are numerous settings:

- **Suppress repeated failed clients:** Globally enables or disables the suppression of logs from clients who repeatedly fail authentication.
- **Detect Two Failures Within interval Minutes:** Flags misbehaving supplicants when they fail authentication more than once per interval.
- **Report Failures Once Every interval Minutes:** Sends the alarm from the PSN to the MnT at the designated interval.
- **Reject RADIUS Requests from Clients With Repeated Failures:** Stops sending logs for repeat authentication failures for the same endpoint during the rejection interval set in the subfields (suppresses the logs).

**Note** A successful authentication clears all flags.

Next, you will notice the ability to deduplicate successful authentications with the Suppress Repeated Successful Authentications settings. This applies the deduplication and suppresses the logs from MnT.

Finally, there is a setting to Highlight Steps Longer Than Interval Milliseconds. This relates to the step latency that is visible in the Authentication Detail report, to point out areas of possible trouble.

## Active Troubleshooting

Now that you know about the deduplication feature and how to bypass it for troubleshooting, it is time to get into that troubleshooting methodology for when you hear the complaint: “I plugged into the network, but my system is not granted access.” Remember as you troubleshoot to always keep the authentication and authorization flows in mind, as previously illustrated in [Figure 26-17](#).

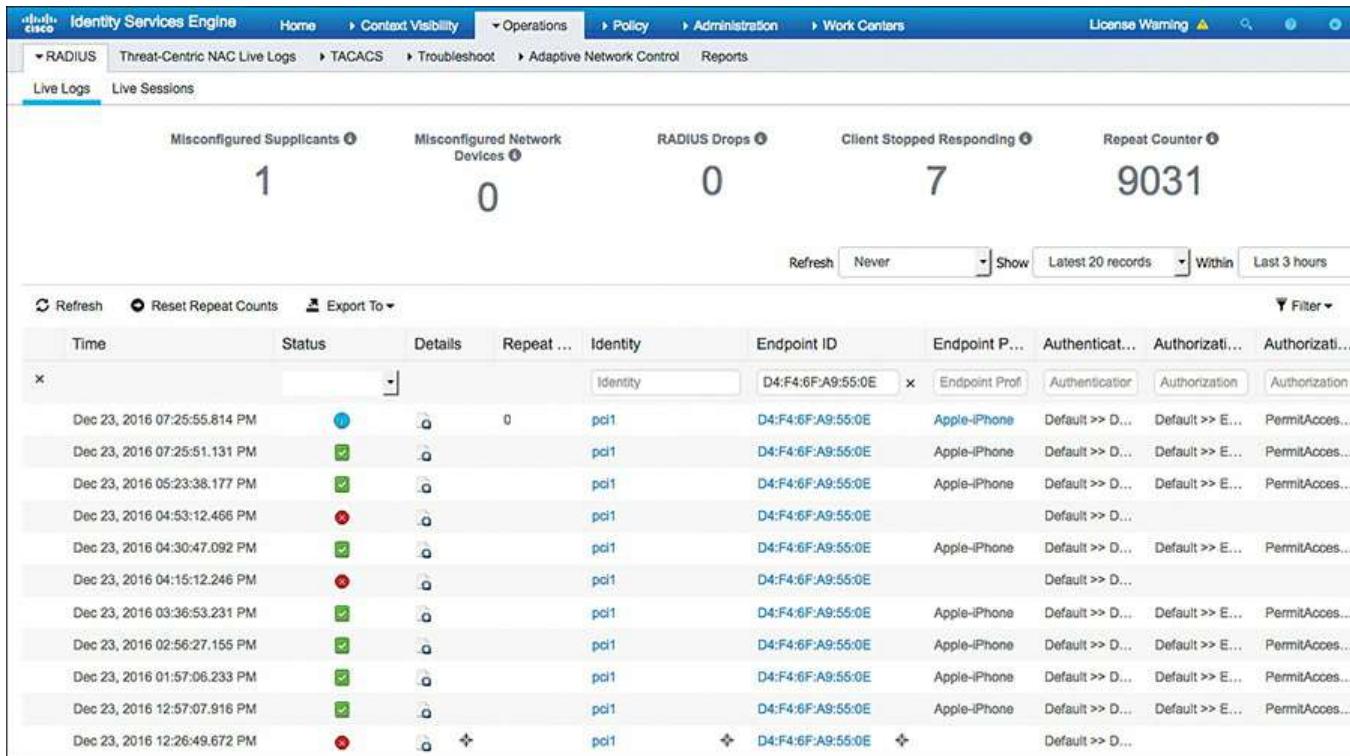
The first action you should take after being contacted with this kind of problem is to gather as much data as you can about the client machine and then examine the Live Logs on ISE, as described in the following steps:

**Step 1.** Collect as many of the following data points about the client machine as you can, if not all of them:

- Username (good)
- Machine name (good)
- Switch or Wireless LAN Controller name (better)
- Switch interface (even better)
- MAC address of the machine (best)

**Step 2.** Go to the Live Logs by navigating to **Operations > RADIUS > Live Logs**.

**Step 3.** Filter the log using the data that you gathered, until you find the attempted authentication. [Figure 26-22](#) shows the Live Logs being filtered by Endpoint ID (MAC address).



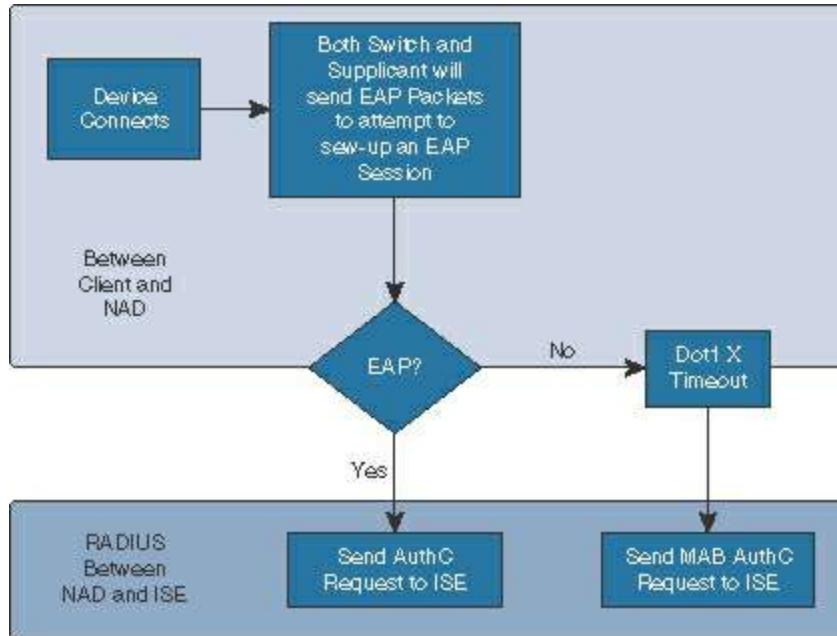
**Figure 26-22** Live Logs Filtered by MAC Address

**Step 4.** Your next action depends on what you find in the Live Logs:

- If the log contains no entry at all for that MAC address, then you must determine whether ISE is even receiving an authentication request, as described in the following section.
- If the log contains an entry for the MAC address, proceed as described in the subsequent section, “Option 2: An Entry Exists in the Live Logs.”

### Option 1: No Live Logs Entry Exists

If there is no entry at all in the Live Logs, you need to examine the communication between the NAD and ISE. Always keep the flows in mind, as shown in [Figure 26-23](#).



**Figure 26-23** Authentication Flow

Remember that there must be an EAP communication occurring locally between the NAD and the endpoint first, which gets “wrapped” inside of RADIUS from the NAD to ISE. If EAP is not present (that is, no supplicant is present), then there should be a MAB request from the switch to ISE.

At this point, you need to verify that ISE is receiving the authentication requests. There are a few ways to accomplish this. Normally, either one of these methods would suffice, but for the purposes of completeness in this chapter, you will be shown both options in the steps that follow:

**Step 1.** From the dashboard in ISE, check the Alarms section for any “Unknown NAD” alarms, as shown in [Figure 26-24](#). If you see this alarm, there are two possible reasons:

- a. ISE does not have the switch configured as a network device.
- b. The switch is sending the request from an IP address that is not defined in the Network Device object within ISE.

Severity	Name	Occurrences
!	RADIUS Request Dropped	160
!	Supplicant stopped responding	2
!	Misconfigured Supplicant Detected	3
!	Health Status Unavailable	5
!	Configuration Changed	125
!	CA Server is down	4
!	Log Collection Error	104
!	Active Directory not joined	49
!	Unknown NAD	274
!	Inufficient Virtual Machine Resources	1

**Figure 26-24 Alarms**

**Step 2.** Ensure that the request is reaching ISE. Run the TCP Dump utility with a filter of **ip host ip-address-of-nad**.

In this case, you will see that the issue is actually Step 1b. The **ip radius source-interface** command is missing on the switch. How we made the determination that it was Step 1b is described next.

The two alarms of interest in [Figure 26-24](#) are RADIUS Request Dropped and Unknown NAD. Double-click the first alarm to drill into it, and you see the source of these alarms is 10.1.40.60, as shown in [Figure 26-25](#).

## ⚠ Alarms: Unknown NAD

### Description

The ISE Policy Service nodes are receiving Authentication requests from a Network Device that is not configured in ISE

### Suggested Actions

Check if the Network Device is a genuine request and add it to the configuration. Ensure the secret matches.

<input type="checkbox"/>	Time Stamp	Description	Details
<input type="checkbox"/>	Dec 23 2016 10:08:56.250 AM	Unknown NAD : Server=atw-ise241 NAS IP Address=192.168.254.60	
<input type="checkbox"/>	Dec 23 2016 10:08:56.241 AM	Unknown NAD : Server=atw-ise237 NAS IP Address=10.1.60.2	
<input type="checkbox"/>	Dec 23 2016 10:08:56.198 AM	Unknown NAD : Server=atw-ise243 NAS IP Address=10.1.60.2	
<input type="checkbox"/>	Dec 22 2016 16:29:23.059 PM	Unknown NAD : Server=atw-ise241 NAS IP Address=192.168.254.60	
<input type="checkbox"/>	Dec 22 2016 16:18:43.059 PM	Unknown NAD : Server=atw-ise237 NAS IP Address=10.1.60.2	
<input type="checkbox"/>	Dec 22 2016 16:15:23.059 PM	Unknown NAD : Server=atw-ise243 NAS IP Address=10.1.60.2	
<input type="checkbox"/>	Dec 22 2016 15:14:23.059 PM	Unknown NAD : Server=atw-ise241 NAS IP Address=192.168.254.60	
<input type="checkbox"/>	Dec 22 2016 15:03:13.060 PM	Unknown NAD : Server=atw-ise237 NAS IP Address=10.1.60.2	
<input type="checkbox"/>	Dec 22 2016 15:03:03.059 PM	Unknown NAD : Server=atw-ise243 NAS IP Address=10.1.60.2	
<input type="checkbox"/>	Dec 22 2016 13:59:23.059 PM	Unknown NAD : Server=atw-ise241 NAS IP Address=192.168.254.60	

**Figure 26-25** Alarm Details

The device with the IP address of 10.1.40.60 is the 3560-X switch, and you connect to it via SSH or the console. Upon doing so, notice immediately that authentication-related failures exist, as displayed in Example 26-1.

### Example 26-1 Failures Shown in the Switch Logs

#### [Click here to view code image](#)

```
*Sep 13 19:26:39.634: %MAB-5-FAIL: Authentication failed for client  
(0050.5687.0039) on Interface Gi0/1 AuditSessionID  
0A01283C0000001517B7584B  
  
*Sep 13 19:26:39.634: %AUTHMGR-7-RESULT: Authentication result  
'server dead' from 'mab' for client (0050.5687.0039) on Interface  
Gi0/1 AuditSessionID 0A01283C0000001517B7584B  
  
*Sep 13 19:26:39.634: %AUTHMGR-5-FAIL: Authorization failed for  
client (0050.5687.0039) on Interface Gi0/1 AuditSessionID  
0A01283C0000001517B7584B
```

To see more details, issue the **show authentication session interface** interface-name command. This is one of the most commonly used commands when troubleshooting authentication with Cisco IOS Software. The output of this command shows that the switch is trying to do both MAB and 802.1X, and neither is successful. [Example 26-2](#) displays that output.

### Example 26-2 Output of the **show authentication session interface** Command

[Click here to view code image](#)

```
3560-X# sho authen sess int g0/1

    Interface: GigabitEthernet0/1
    MAC Address: 0050.5687.0039
    IP Address: 10.1.41.102
    User-Name: 005056870039
    Status: Running
    Domain: UNKNOWN
    Security Policy: Should Secure
    Security Status: Unsecure
    Oper host mode: multi-auth
    Oper control dir: both
    Session timeout: N/A
    Idle timeout: N/A
    Common Session ID: 0A01283C00000018F595EC0B
    Acct Session ID: 0x00000049
                  Handle: 0x41000018

    Runnable methods list:
        Method      State
          mab       Failed over
          dot1x     Running
```

To verify which IP addresses the switch may be sending the RADIUS messages from, issue the **show ip interface brief** command, with the **| include up** option to limit your display, as shown in Example 26-3.

### Example 26-3 Output of the **show ip int brief | include up** Command

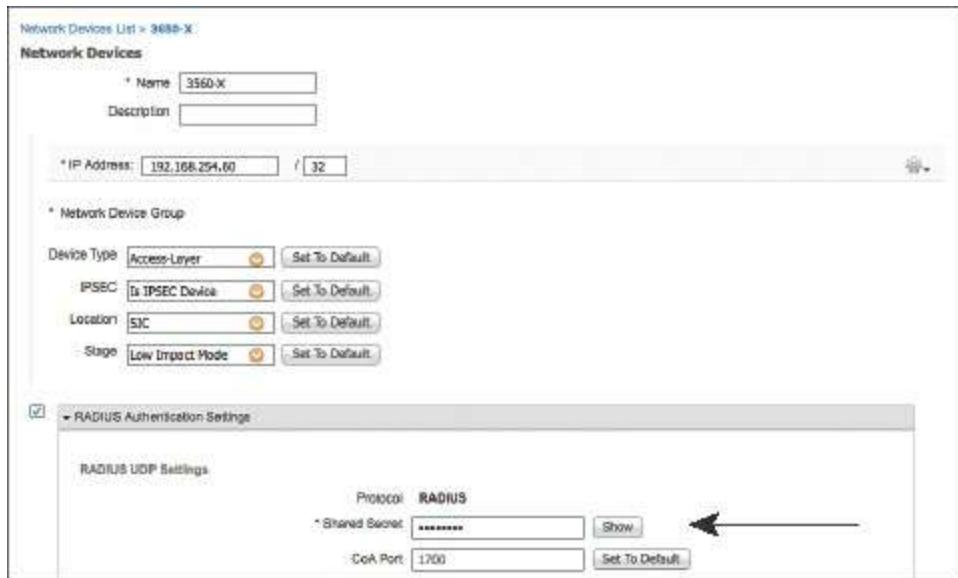
[Click here to view code image](#)

```
3560-X# sho ip int brief | include up
```

Vlan1	unassigned	YES	NVRAM	up	up
Vlan40	10.1.40.60	YES	NVRAM	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/24	unassigned	YES	unset	up	up
Loopback0	192.168.254.60	YES	NVRAM	up	up

```
3560-X#
```

Next, verify the NAD definition in ISE by navigating to **Administration > Network Resources > Network Devices** and then editing the 3560-X object, as shown in [Figure 26-26](#). Within this object, notice that the expected IP address is 192.168.254.60, which is the loopback interface.



**Figure 26-26** NAD Object Definition

To correct this, add the **ip radius source-interface** interface-name command into the configuration, as shown in Example 26-4.

This should have been part of your configuration already, but obviously something must have happened. This occurs quite often in customer environments; an admin might not fully know what the command was used for and could have removed it from the configuration, or the switch might have been added without the appropriate command. The reason behind the interface not being set is not the purpose of this exercise; the

purpose is to enable the users to authenticate again.

#### Example 26-4 Output of the **ip radius source-interface** Command

[Click here to view code image](#)

```
3560-X(config)# ip radius source-interface Loopback0  
3560-X(config)#{
```

Verify that everything works now by reissuing the **show authentication session interface** interface-name command, or by checking the Live Logs on ISE.

[Example 26-5](#) shows the working authentication on the switch, which happens to be a Centralized Web Authentication result.

#### Example 26-5 Output of the **show authentication session interface** Command

[Click here to view code image](#)

```
3560-X# sho authen sess int g0/1

      Interface: GigabitEthernet0/1
      MAC Address: 0050.5687.0039
      IP Address: 10.1.41.102
      User-Name: 00-50-56-87-00-39
      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: xACSAACLx-IP-Pre-Auth-ACL-50fc97ba
      URL Redirect ACL: ACL-WEBAUTH-REDIRECT
      URL Redirect: https://atw-cp-  
ise04.ise.local:8443/questportal/gateway?  
sessionId=0A01283C0000001AF59D671A&action=cwa
```

```
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 0A01283C0000001AF59D671A
      Acct Session ID: 0x0000004B
      Handle: 0xAC00001A
```

Runnable methods list:

Method	State
mab	Authc Success
dot1x	Not run

```
3560-X#
```

## Option 2: An Entry Exists in the Live Logs

If there is an entry for the MAC address in the Live Logs, you are in luck, because you can troubleshoot this almost entirely from the ISE GUI, as described in the following

steps:

**Step 1.** Starting with the Live Logs, as shown in [Figure 26-27](#), in the Details column, click the icon (which looks like a magnifying glass on a piece of paper) to view the details of the failure. [Figure 26-27](#) shows an older Live Logs screen, but the activity is the same regardless of the ISE version.

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Authentication Protocol	Auth Method	Identity Group
Jan 25,13 09:29:41.399 AM	✓	<input type="checkbox"/> #ACSAACL#-IP-P..			3750-X						
Jan 25,13 09:29:41.386 AM	✓	<input type="checkbox"/> 00:13:C3:07:F2:C8	employee1	00:13:C3:07:F2:C8	10.1.99.50	3750-X	GigabitEthernet1/0/1	Cisco_IP_Phones	Lookup	mab	Cisco-IP-Phone
Jan 25,13 09:29:38.369 AM	✓	<input type="checkbox"/> employee1	employee1	00:50:56:87:00:39	10.1.41.102	3560-X	GigabitEthernet0/1	NSP	EAP-FAST (EAP-MSCHA..)	dot1x	Profiled
Jan 25,13 09:29:26.248 AM	✓	<input type="checkbox"/> #CTSRQUEST#				Cat6K					
Jan 25,13 09:29:14.461 AM	✗	<input type="checkbox"/> employee2	employee2	00:50:56:87:00:39	10.1.41.102	3560-X	GigabitEthernet0/1		PEAP (EAP-MSCHAv2)	dot1x	
Jan 25,13 09:29:06.609 AM	✓	<input type="checkbox"/> #ACSAACL#-IP-P..			3750-X						
Jan 25,13 09:29:06.566 AM	✓	<input type="checkbox"/> 00:13:C3:07:F2:C8		00:13:C3:07:F2:C8	10.1.99.50	3750-X	GigabitEthernet1/0/1	Cisco_IP_Phones	Lookup	mab	Cisco-IP-Phone
Jan 25,13 09:28:31.737 AM	✓	<input type="checkbox"/> #ACSAACL#-IP-P..			3750-X						

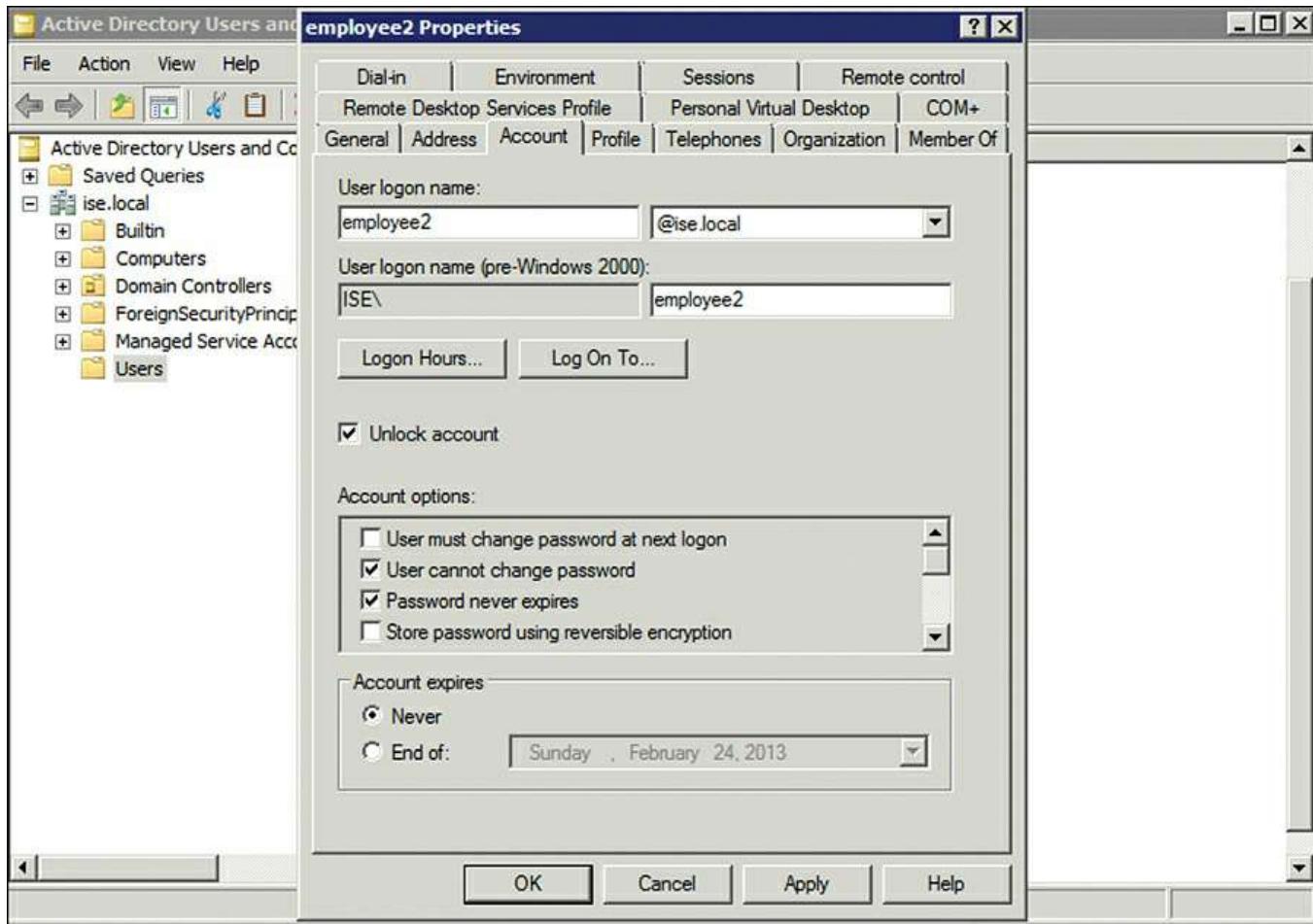
**Figure 26-27** Live Logs with a Failure

**Step 2.** Review the Authentication Details that open in the new window (shown in [Figure 26-28](#)), and you can see almost instantly that the authentication failed because the user's AD account is disabled.

Authentication Details	
Source Timestamp	2013-01-25 09:29:14.457
Received Timestamp	2013-01-25 09:29:14.461
Policy Server	atw-cp-ise04
Event	5400 Authentication failed
Username	employee2
User Type	
Endpoint Id	00:50:56:87:00:39
IP Address	10.1.41.102
Identity Store	AD1
Identity Group	
Audit Session Id	0A01283C0000001AF59D671A
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	3560-X
Device Type	Switches#Access-Layer
Location	NorthAmerica#SJC
NAS IP Address	192.168.254.60
NAS Port Id	GigabitEthernet0/1
Authorization Profile	
Posture Status	
Security Group	
Failure Reason	24409 User authentication against Active Directory failed since the user's account is disabled

**Figure 26-28** Authentication Details

**Step 3.** Access your Active Directory management console and check the account; reenable the account if it really is disabled by checking the **Unlock Account** check box, as displayed in [Figure 26-29](#).



**Figure 26-29** Unlocking the Disabled Account

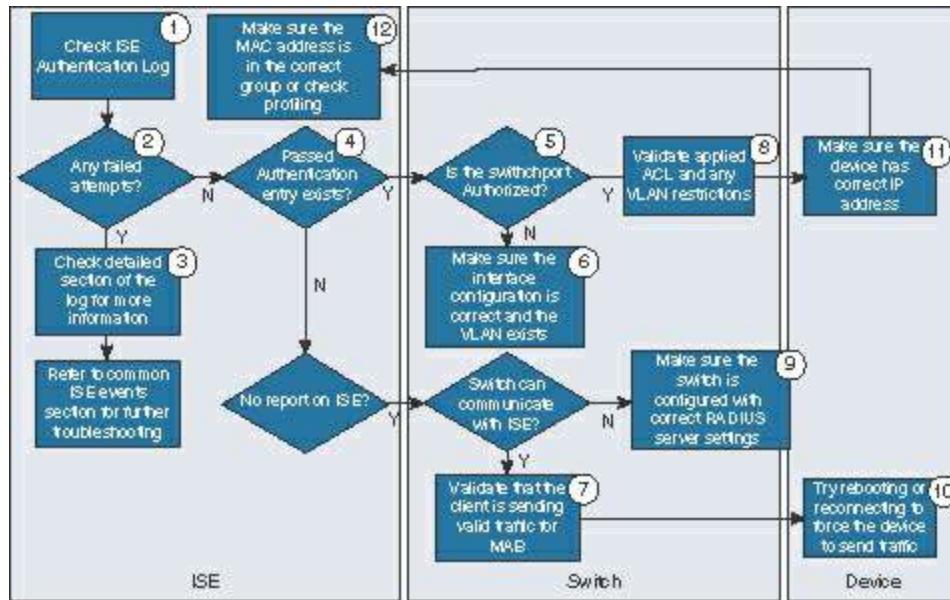
Now, the authentications are succeeding for Employee2, as shown in [Figure 26-30](#).

Cisco Identity Services Engine										
Authentications										
Operations   Policy   Administration										
atw-cp-ise04   admin   Logout   Feedback   <a href="#">P</a>										
Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Authentication Protocol	Auth Method
Jan 25,13 09:51:39.932 AM	<span style="color: green;">✓</span>	<span style="color: green;">○</span>	employee2	00:50:56:87:00:39	10.1.41.102	3560-X	GigabitEthernet0/1	NSP	PEAP (EAP-MSCHAPv2)	dot1x
Jan 25,13 09:40:22.222 AM	<span style="color: red;">✗</span>	<span style="color: red;">○</span>	employee2	00:50:56:87:00:39	10.1.41.102	3560-X	GigabitEthernet0/1		PEAP (EAP-MSCHAPv2)	dot1x
Jan 25,13 09:40:14.972 AM	<span style="color: red;">✗</span>	<span style="color: red;">○</span>	employee2	00:50:56:87:00:39	10.1.41.102	3560-X	GigabitEthernet0/1		PEAP (EAP-MSCHAPv2)	dot1x
Jan 25,13 09:29:38.369 AM	<span style="color: green;">✓</span>	<span style="color: green;">○</span>	employee1	00:50:56:87:00:39	10.1.41.102	3560-X	GigabitEthernet0/1	NSP	EAP-FAST (EAP-MSCHA...)	dot1x
Jan 25,13 09:29:14.461 AM	<span style="color: red;">✗</span>	<span style="color: red;">○</span>	employee2	00:50:56:87:00:39	10.1.41.102	3560-X	GigabitEthernet0/1		PEAP (EAP-MSCHAPv2)	dot1x
Jan 25,13 09:28:04.639 AM	<span style="color: green;">✓</span>	<span style="color: green;">○</span>	employee1	00:50:56:87:00:39	10.1.41.102	3560-X	GigabitEthernet0/1	NSP	EAP-FAST (EAP-MSCHA...)	dot1x
Jan 24,13 10:25:19.850 AM	<span style="color: green;">✓</span>	<span style="color: green;">○</span>	employee1	BC-B1-F3:B1:CC:82		WLC-02		NSP	PEAP (EAP-MSCHAPv2)	dot1x

**Figure 26-30** Success

## General High-Level Troubleshooting Flowchart

One of our colleagues, Hosuk Won, put together the flowchart shown in [Figure 26-31](#) to aid in the troubleshooting of the Secure Access system. This is an excellent flowchart to follow for general high-level troubleshooting.



**Figure 26-31** High-Level Troubleshooting Flowchart

## Troubleshooting WebAuth and URL Redirection

The URL redirection employed by CWA—as well as by both BYOD and MDM onboarding—is one of those things that can be confusing to folks who are new to it. One of the most common troubleshooting exercises that our team(s) will get involved in is helping someone when they report “WebAuth isn’t working.” Of course, they will also report “nothing was missed” and “nothing has changed.” You know, the normal cliché statements that you hear from someone who is asking for assistance. Ninety-nine times out of a hundred, staying calm and remembering to always “follow the flows” is what enabled us to solve their problem.

The following is an example series of steps to follow:

**Step 1.** Check the Live Logs. Ensure that the authorization result includes the URL redirection, as displayed in [Figure 26-32](#). If so, make note of the url-redirect-acl name.

```

▼ Attributes Details
Access Type = ACCESS_ACCEPT
DACL = Pre-Auth-ACL
cisco-av-pair = url-redirect-acl=ACL-WEBAUTH-REDIRECT
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

```

**Figure 26-32** Attribute Details from the Authorization Result

**Step 2.** Gather information about the client session.

- For wired URL redirection, execute the **show authentication session interface interface-name** command:

[Click here to view code image](#)

```

3560-X# sho authen sess int g0/1

      Interface: GigabitEthernet0/1
      MAC Address: 0050.5687.0039
      IP Address: 10.1.41.102
      User-Name: 005056870039
          Status: Running
          Domain: UNKNOWN
      Security Policy: Should Secure
      Security Status: Unsecure
      Oper host mode: multi-auth
      Oper control dir: both
      Session timeout: N/A
      Idle timeout: N/A
      Common Session ID: 0A01283C00000018F595EC0B
      Acct Session ID: 0x00000049
          Handle: 0x41000018

Runnable methods list:
      Method      State
      dot1x      Running
      mab        Failed over

```

The preceding output highlights the most important fields for this exercise. The ACS-ACL field is displaying the downloadable ACL (dACL) name that was downloaded from ISE and applied to the sessions' IP traffic. This ACL is examined further in Step 4.

The URL Redirect ACL describes the name of a local ACL that must preexist on the switch for it to be used. That ACL determines which traffic is redirected and which is not. This ACL is examined further in Step 4.

Finally, the session ID from ISE will be present in the URL Redirect field, and it must match the Common Session ID displayed below it. If by chance these IDs do not match, you should open a TAC case to receive further assistance.

- b.** For wireless URL redirection, choose **Monitor > Clients**, as shown in [Figure 26-33](#).

Clients > Detail	
<a href="#">General</a> <b>AVC Statistics</b>	
<b>Security Information</b>	
Security Policy	No
Completed	No
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	SUPPLICANT_PROVISIONING
CTS Security Group Tag	Not Applicable
AAA Override ACL Name	Android-Marketplace
AAA Override ACL Applied Status	Yes
AAA Override Flex ACL none	
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	<a href="https://atw-cp-ise04.ise.local:8443/guestportal/gate">https://atw-cp-ise04.ise.local:8443/guestportal/gate</a>
IPv4 ACL Name	none
IPv4 ACL Applied Status	Unavailable
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable
mDNS Profile Name	default-mdns-profile
mDNS Service Advertisement Count	0

**Figure 26-33** Client > Details Showing the AAA Override and Redirect URL

[Figure 26-33](#) points out the most important fields for this exercise. If the Radius NAC State field shows RUN, then the RADIUS NAC setting was never enabled on the WLAN. This is a pretty common oversight. The fix is to enable RADIUS NAC in the controller.

The AAA Override ACL Name field must list the exact name that was noted in Step 1 and [Figure 26-32](#).

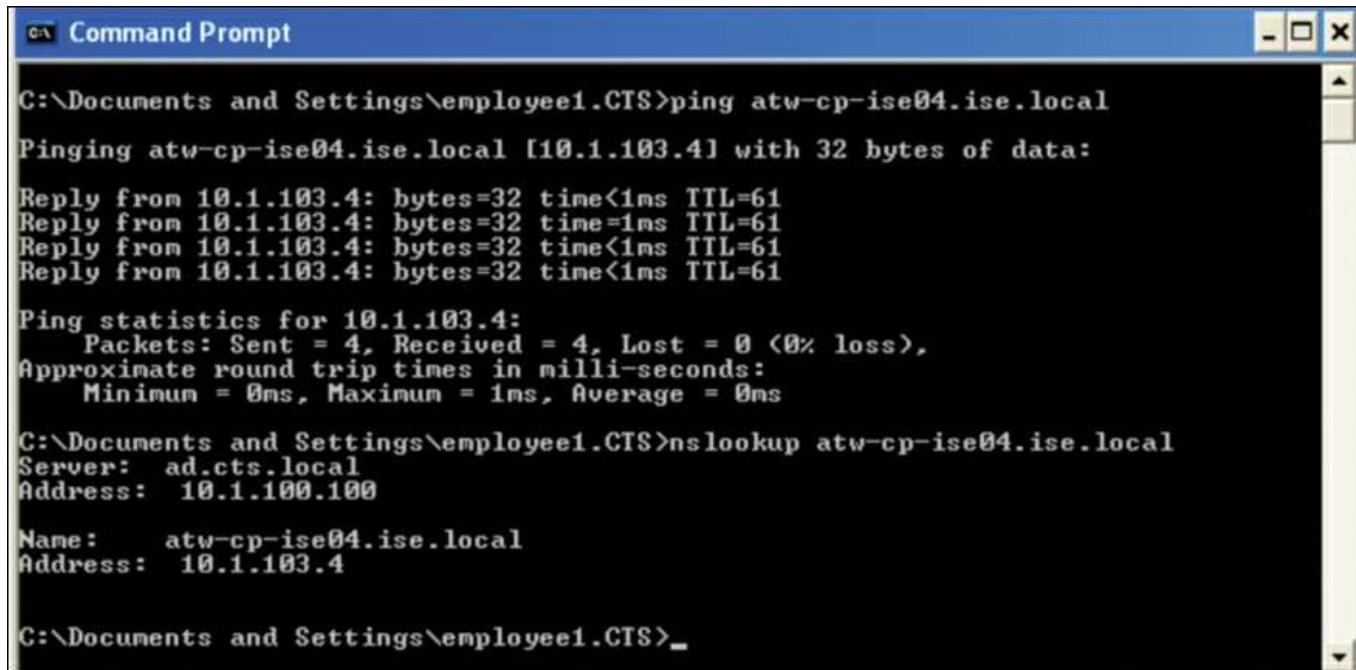
The Redirect URL field should contain the URL pointing to ISE. Make note of the hostname.

### Step 3. Verify that DNS resolution is working from the client.

The URL redirect is automatically sent to the fully qualified domain name as configured in ADE-OS, such as <https://atw-cp-ise04.ise.local>—which is visible in [Figure 26-32](#) and [Figure 26-33](#), as well as in the output in Step 2a. The client must be able to resolve this name with DNS. This is another common error, and easily correctable.

Sometimes, the issue may be that the entry was never made on the DNS server that the client is using, or that the ACL is not permitting DNS traffic. The ACLs are examined in Step 4.

To verify DNS from the client, you would normally use **ping** or **nslookup**, as shown in [Figure 26-34](#). The **ping** may fail, depending on the ACL. However, you are looking for DNS resolution, not successful ICMP. [Figure 26-34](#) demonstrates a successful DNS lookup, using both **ping** and **nslookup**.



```
C:\Documents and Settings\employee1.CTS>ping atw-cp-ise04.ise.local
Pinging atw-cp-ise04.ise.local [10.1.103.4] with 32 bytes of data:
Reply from 10.1.103.4: bytes=32 time<1ms TTL=61
Reply from 10.1.103.4: bytes=32 time=1ms TTL=61
Reply from 10.1.103.4: bytes=32 time<1ms TTL=61
Reply from 10.1.103.4: bytes=32 time<1ms TTL=61

Ping statistics for 10.1.103.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\employee1.CTS>nslookup atw-cp-ise04.ise.local
Server:  ad.cts.local
Address: 10.1.100.100

Name:  atw-cp-ise04.ise.local
Address: 10.1.103.4

C:\Documents and Settings\employee1.CTS>_
```

Figure 26-34 Verifying DNS from the Client

**Step 4.** Examine the ACLs.

- a. For wired devices, execute the **show ip access-list interface** interface-name command:

```
3560-X# sho ip access-list int g0/1
```

```
permit udp host 10.1.41.102 any eq bootps
permit udp host 10.1.41.102 any eq domain (4 matches)
permit icmp host 10.1.41.102 any
permit tcp host 10.1.41.102 host 10.1.100.232 eq 8443
permit tcp host 10.1.41.102 host 10.1.100.232 eq 8905
permit tcp host 10.1.41.102 host 10.1.100.232 eq 8909
permit udp host 10.1.41.102 host 10.1.100.232 range 8905 8906
permit udp host 10.1.41.102 host 10.1.100.232 eq 8909
```

As you see, the output of this **show** command displays the effective ACL that is applied to the interface, after applying the downloadable ACL.

- b. Also for wired devices, you have to ensure that the redirection ACL is correct with the **show ip access-list** access-list-name command, as shown in the output that follows. This ACL will redirect only traffic that is permitted. Any traffic that is denied will bypass redirection.

```
3560-X# sho ip access-list ACL-WEBAUTH-REDIRECT
```

Extended IP access list ACL-WEBAUTH-REDIRECT

```

10 deny udp any any eq domain (58523 matches)
20 permit tcp any any eq www (7978448 matches)
30 permit tcp any any eq 443 (416 matches)

```

Ensure that traffic is being redirected by looking for the matches for TCP ports 80 and 443.

- c. With wireless access, only a single ACL is in effect. To examine the contents of the ACL and ensure it is named correctly, choose **Security > Access-Control-Lists**.

Ensure the name matches exactly what is sent in the authorization result noted in Step 1. If it does, edit the ACL to examine the individual rules, as shown in [Figure 26-35](#).

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCH	Direction	Number of Hits
1	Permit	0.0.0.0 0.0.0.0	/ 0.0.0.0 0.0.0.0	/ Any	Any	Any	Any	Outbound	27462 <input checked="" type="checkbox"/>
2	Permit	0.0.0.0 0.0.0.0	/ 10.130.1.0 255.255.255.0	/ Any	Any	Any	Any	Inbound	3095 <input checked="" type="checkbox"/>
3	Permit	0.0.0.0 0.0.0.0	/ 74.125.0.0 255.255.0.0	/ Any	Any	Any	Any	Inbound	323 <input checked="" type="checkbox"/>
4	Permit	0.0.0.0 0.0.0.0	/ 173.194.0.0 255.255.0.0	/ Any	Any	Any	Any	Inbound	21316 <input checked="" type="checkbox"/>
5	Permit	0.0.0.0 0.0.0.0	/ 173.227.0.0 255.255.0.0	/ Any	Any	Any	Any	Inbound	0 <input checked="" type="checkbox"/>
6	Permit	0.0.0.0 0.0.0.0	/ 206.111.0.0 255.255.0.0	/ Any	Any	Any	Any	Inbound	0 <input checked="" type="checkbox"/>
7	Permit	0.0.0.0 0.0.0.0	/ 12.150.127.0 255.255.255.0	/ Any	Any	Any	Any	Inbound	0 <input checked="" type="checkbox"/>
8	Deny	0.0.0.0 0.0.0.0	/ 0.0.0.0 0.0.0.0	TCP	Any	Any	Any	Inbound	3990 <input checked="" type="checkbox"/>

**Figure 26-35** Verifying Airespace ACL

## Debug Situations: ISE Logs

If you are unable to isolate a root cause via the ISE GUI, it may be necessary to look into the log files. ISE maintains very detailed logging, and enables you to set the logging levels. If it becomes necessary to start debugging, perform the following steps:

- Step 1.** Navigate to **Administration > System > Logging > Debug Log Configuration**.
- Step 2.** Choose the appropriate ISE Policy Service Node (PSN).
- Step 3.** Set the appropriate logs to debug level.
- Step 4.** Reproduce the problem and gather relevant seed information to aid in searching

the logs, such as MAC Address, IP Address, sessionID, and so forth.

**Step 5.** Navigate to **Operations > Troubleshoot > Download Logs** and choose the appropriate ISE node.

**Step 6.** On the Debug Logs tab, download the logs.

**Step 7.** Use an intelligent editor such as Notepad++ (Windows) or TextWrangler (Mac) to parse the log files.

**Step 8.** Once the issue has been isolated, return the log levels to their default levels.

## The Support Bundle

Cisco TAC may ask for the support bundle, which contains the full ISE configuration and all logs. You can think of it as an equivalent of the **show tech-support** command on a Cisco IOS device. It allows the support engineer to re-create the environment in a lab, if necessary.

The bundle will save as a simple tar.gpg (GPG encrypted) file. The support bundle is automatically named with the date and time stamps in the following format: ise-support-bundle\_ise-support-bundle-mm-dd-yyyy-hh-mm.tar.gpg.

You have the option to choose which logs you want to be part of your support bundle. For example, you can configure logs from a particular service to be part of your bundle. The logs that you can download are categorized as follows:

- **Full configuration database:** If you choose this category, the ISE configuration database is saved into the support bundle and allows TAC to import this database configuration in another ISE node to re-create the scenario.
- **Debug logs:** This category captures bootstrap, application configuration, run-time, deployment, monitoring and reporting, and Public Key Infrastructure (PKI) information.
- **Local logs:** This category contains log messages from the various processes that run but are not collected by the MnT node.
- **Core files:** This category contains critical information that would help identify the cause of a crash. These logs are created if the application crashed and includes core dumps.
- **Monitoring and reporting logs:** This category contains information about the alarms and reports from the MnT node.
- **System logs:** This category contains the underlying OS (Application Deployment Engine [ADE-OS]) logs. These logs are not directly part of the ISE application itself.

There are two ways to create and download the support bundle: from the ISE GUI and from the command-line interface (CLI).

From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Operations > Troubleshoot > Download Logs**.

**Step 2.** Select the ISE node in the left pane.

**Step 3.** Choose which categories of logs you want to include, which were described in the previous list.

**Step 4.** Enter a password to use for encrypting the bundle, or select to use **Public Key Encryption**. The Public Key Encryption option uses Cisco's PKI to encrypt the bundle where only Cisco can decrypt it, and helps with TAC case automation tooling.

**Step 5.** Click **Create Support Bundle**, such as what is displayed in [Figure 26-36](#).

**Support Bundle**      **Debug Logs**

Include full configuration database [i](#)

Include debug logs [i](#)

Include local logs [i](#)

Include core files [i](#)

Include monitoring and reporting logs [i](#)

Include system logs [i](#)

Include policy configuration [i](#)

From Date  
 [Calendar icon](#) (mm/dd/yyyy)

To Date  
 [Calendar icon](#) (mm/dd/yyyy)

\* Note: Output from the 'show tech-support' CLI command will be included along with the selected entries.

**▼ Support Bundle - Encryption**

Public Key Encryption [i](#)

Shared Key Encryption [i](#)

\* Encryption key  [i](#)

\* Re-Enter Encryption key

\* Note: Log bundle may contain sensitive data. Ensure it is only distributed to authorized personnel.

**Create Support Bundle**

**Figure 26-36** Creating a Support Bundle from the GUI

## Summary

If you have gained nothing else from this chapter, you should at least take away the following lesson: when troubleshooting, always stay calm, take your time, and follow the flows.

If you can do that, you will be an expert troubleshooter in no time, and your understanding of the solution will grow exponentially. Cisco has also provided you with a number of tools to help solve common problems, so don't hesitate to use those tools.

For more on serviceability in ISE and troubleshooting, take a look at Aaron Woland's

blog: <http://www.networkworld.com/article/3053669/security/troubleshooting-ciscos-ise-without-tac.html>

# Chapter 27 Upgrading ISE

This chapter covers the following topics:

- The upgrade process
- Repositories
- Performing the upgrade
- Command-line upgrade

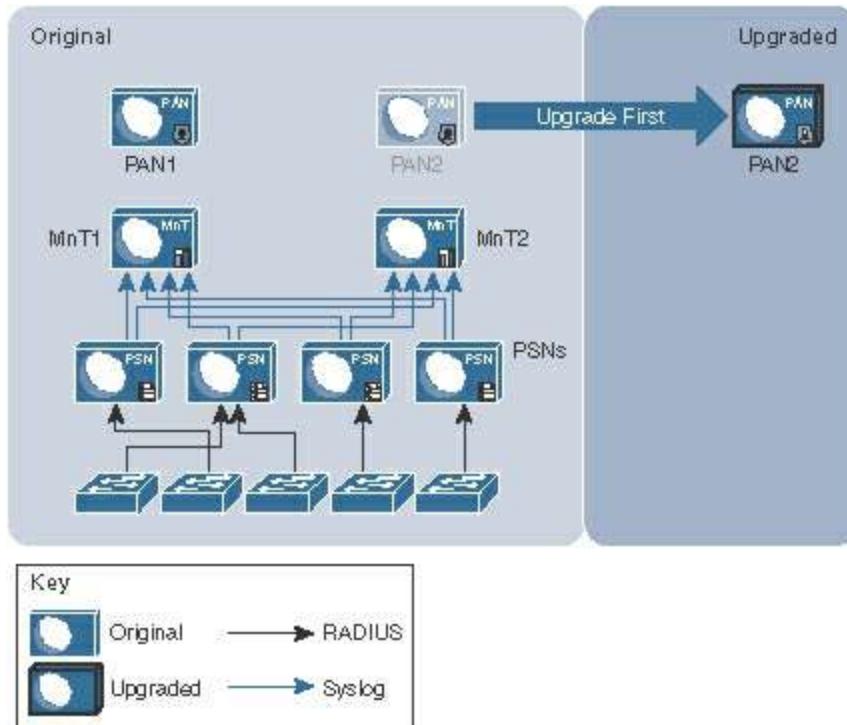
As with many feature and functions in ISE, upgrades have improved with each release as ISE has evolved over the years. Prior to version 1.2, you had to make every ISE node a standalone before upgrading it. Beginning in version 1.2, the process improved by eliminating the requirement to remove each node from the deployment and make it standalone. It also removed a number of erroneous reboots, speeding the process up even more.

## The Upgrade Process

If you are going to upgrade a multinode ISE cube, the upgrade model is known as the Secondary PAN First (SPF) flow. This means that you should upgrade the Secondary PAN First and then upgrade all other nodes sequentially or in parallel. This section provides an overview of the upgrade process. The specific steps that you follow to perform the upgrade are presented later in the chapter, both for a GUI-based upgrade for a command-line upgrade.

The Secondary PAN First flow works in this manner:

1. The upgrade always starts with the Secondary PAN (S-PAN). When the upgrade begins on the Secondary PAN, it automatically becomes the Primary PAN for the upgraded deployment. The PANs no longer sync with one another, because their versioning is different, as shown in [Figure 27-1](#).



**Figure 27-1** Upgrading the Secondary PAN First

Because this newly upgraded PAN is the first node in the new deployment, it is automatically configured to run both the Admin and Monitoring personas, and to be the primary role for those personas.

After the S-PAN has been successfully upgraded, you can upgrade the PSNs and MnT nodes one at a time or a few simultaneously. Always leave enough PSNs active to handle the authentication load of the entire deployment.

2. Upgrade one of the MnT nodes, so that a full logging target exists in the new deployment.
3. Ensure that each PSN is taken out of service before beginning the upgrade process on that node.

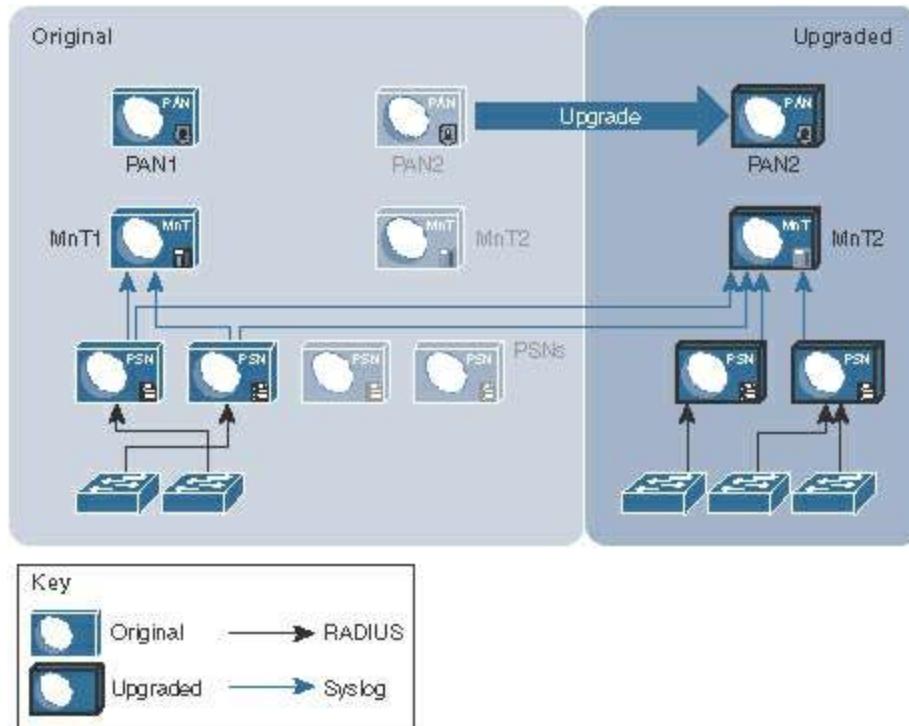
If your deployment is using a load balancer, all you need to do is mark the server as down to remove it from the virtual IP (VIP). If the NADs are pointing directly to the PSNs, you must go into the NAD configuration and remove the server from the configuration, or leverage a network ACL to stop RADIUS traffic from reaching the out-of-service PSN that is going through the upgrade.

Why? The PSNs will go through a number of changes and restarts. The entire database gets wiped out. During that process, the RADIUS runtime (the RADIUS engine) goes up and down, and possibly responds to RADIUS requests with an invalid configuration, which can cause an accidental denial of service (DoS).

4. When each of the PSNs is finished upgrading, it automatically joins the new PAN, which synchronizes its database to the PSN. This saves a tremendous amount of

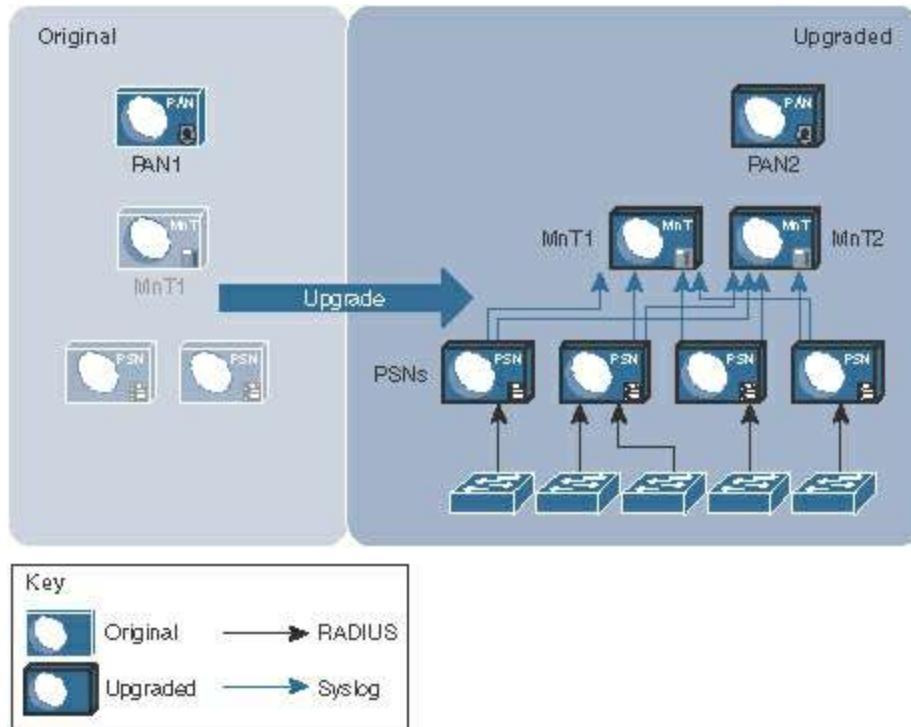
time per PSN, because it does not need to upgrade the entire database, like the process for the PAN. The MnT nodes take the longest amount of time, followed by the PAN, and the PSNs are fastest.

5. All logging is sent to the configured MnT node(s) of the new deployment, as shown in [Figure 27-2](#), and the PSN is ready to be reinstated to active duty once it's fully in sync with the PAN.



**Figure 27-2** Staged Upgrade

6. Remember to take the PSNs out of service before upgrading them to ensure that you have limited the risk of end-user downtime, as shown in [Figure 27-3](#).



**Figure 27-3 Staged Upgrade: Primary PAN Is Last**

7. The last node to be upgraded should be the original Primary PAN. It also receives a complete database dump from the Secondary PAN.

If you want the original primary PAN to be primary in the upgraded model, you need to manually promote it back to the primary role.

In all ISE versions prior to 2.0, this is a very manual process to be performed by you, the ISE administrator, through the CLI of each node in the ISE cube.

Beginning with ISE 2.0, the product took a major step forward with regard to usability of upgrades and making it much easier for the ISE admin. The big change in version 2.0 is a graphical tool to automate most of the upgrade process, following the Secondary PAN First (SPF) approach. We review that tool in detail later in this chapter.

## Repositories

The upgrade cannot occur without one or more repositories available. Simply put, a repository is a location to store files. The repository may be local to ISE or positioned on a remote server. You may have more than one configured, but you certainly need at least one before you can perform upgrade procedures. The repository stores all application upgrade bundles, support bundles, and system backups. It is recommended that you have a repository of at least 10 GB for small deployments (less than 100 endpoints), 100 GB for medium deployments, and 200 GB for large deployments.

## Configuring a Repository

You add repositories via the Maintenance tab of the System Properties of ISE. Technically, you can add a repository within the CLI, but all repositories are always overwritten by the ones added within the ISE GUI.

To add a repository, perform the following steps from the ISE GUI:

**Step 1.** Navigate to **Administration > System > Maintenance**.

**Step 2.** Choose **Repository** on the left side.

**Step 3.** Click **Add** to add a new repository.

**Step 4.** Give the repository a name and choose the type.

## Repository Types and Configuration

Multiple types of repositories are available. When adding a repository in the GUI, the GUI automatically displays the necessary fields. For example, you need to enter a username and password for an FTP repository, but not for a CD-ROM. Repository types include

- Disk
- FTP
- SFTP
- TFTP
- NFS
- CDROM
- HTTP
- HTTPS

The disk repository type is used to provide a repository on the local hard disk. This type of repository is not used often, but sometimes, it can be helpful when Cisco TAC needs to export a support bundle quickly or for other reactive needs. This type of repository needs a name and a path (such as /tac/helpme/), as shown in [Figure 27-4](#).

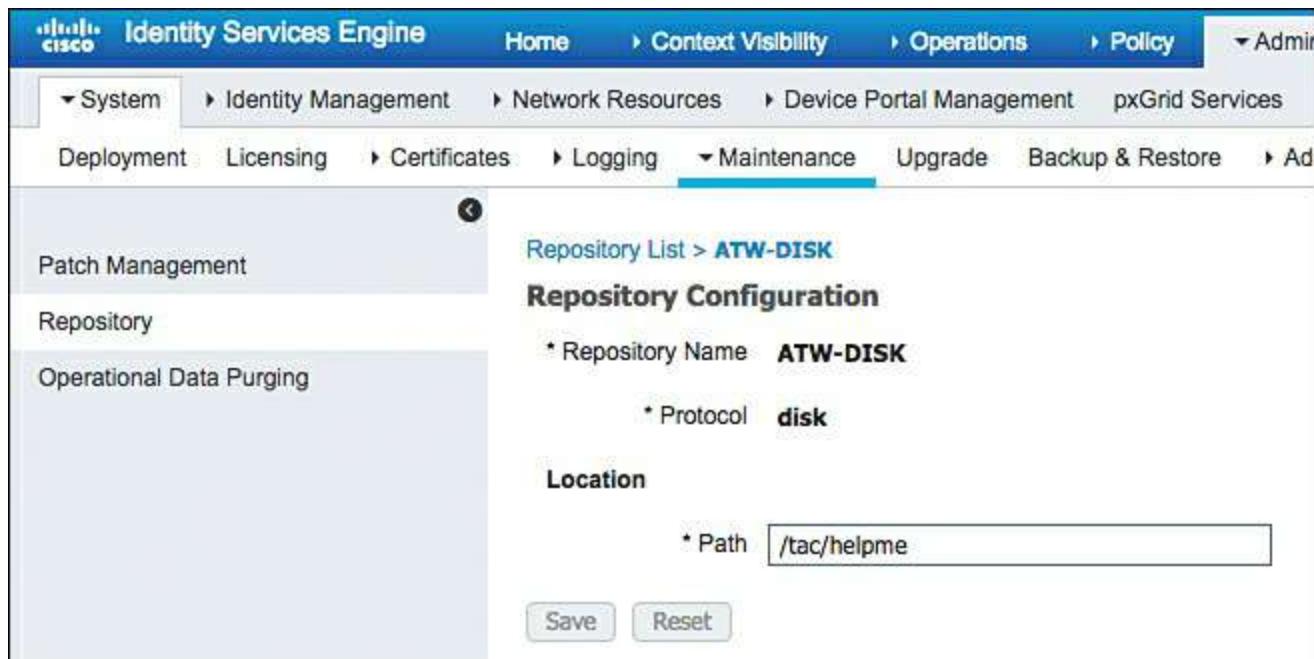


Figure 27-4 Disk Repository

FTP is the most common repository type. It uses File Transfer Protocol (FTP) and requires a server address or DNS name, along with the path, username, and password, as shown in [Figure 27-5](#).



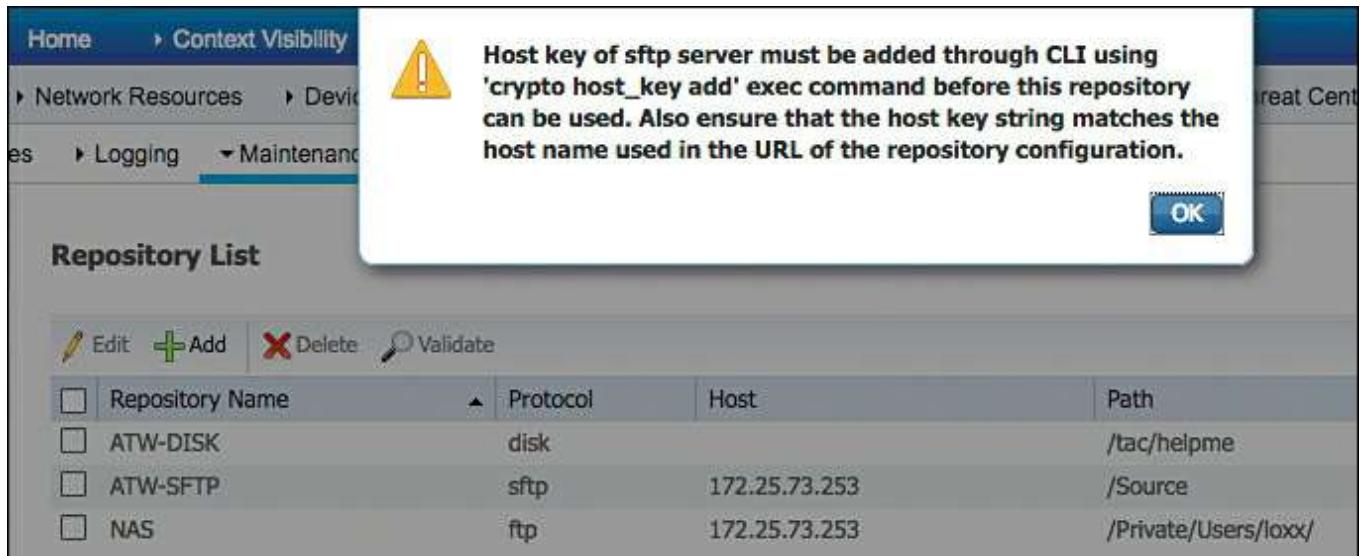
**Figure 27-5** FTP Repository

The SFTP repository uses Secure File Transfer Protocol (SFTP). It also requires a server address or DNS name along with the path, username, and password, as shown in [Figure 27-6](#).

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, and Administration. Below the navigation is a secondary menu with System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Deployment, Licensing, Certificates, Logging, Maintenance (which is selected), Upgrade, Backup & Restore, and Admin. On the left, a sidebar lists Patch Management, Repository (selected), and Operational Data Purging. The main content area is titled "Repository List > Add Repository" and "Repository Configuration". It contains fields for Repository Name (ATW-SFTP), Protocol (SFTP), Server Name (172.25.73.253), Path (/Source), User Name (admin), and Password (\*\*\*\*\*). At the bottom are "Submit" and "Cancel" buttons.

**Figure 27-6** SFTP Repository

**Note** Before this type of repository works, you must trust the certificate of the SFTP server with the **host-key** command, as shown in [Figure 27-7](#).



**Figure 27-7 Host-Key Required Popup**

[Example 27-1](#) shows truncated output of a **show running-config** command. As shown in the example, the repository was created and contains the URL as well as credentials.

### Example 27-1 Repository Output from **show running-config**

[Click here to view code image](#)

```
atw-cp-ise02/admin# show run
! - Displaying only necessary information
repository ATW-SFTP
  url sftp://172.25.73.252/array1/FTPROOT/
  user admin password hash b5558b4ef1742747cc50723474f842818642df47
```

Next, to support SFTP, you need to enter repository configuration mode to add the host key to the repository, as shown in Example 27-2.

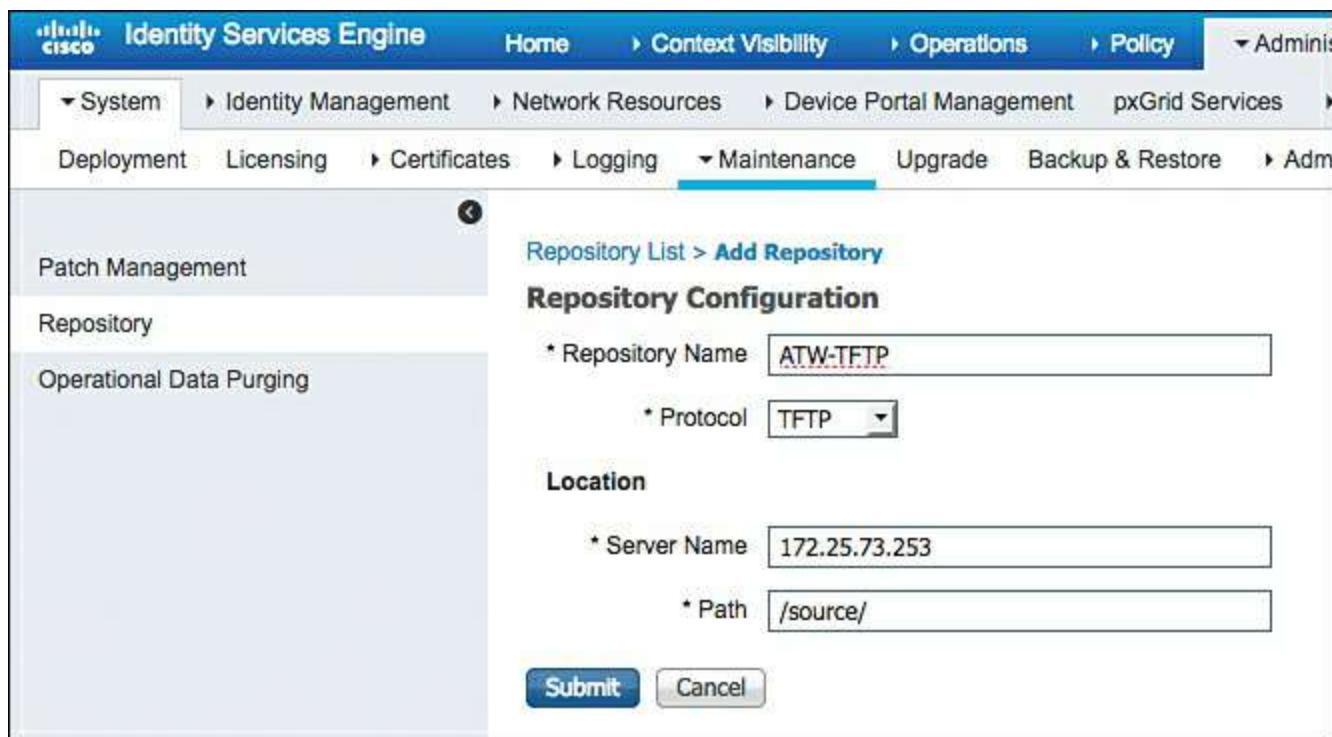
### Example 27-2 Adding the Host Key to the Repository

[Click here to view code image](#)

```
atw-cp-ise02/admin# conf t
atw-cp-ise02/admin(config)# repository ATW-SFTP
% Warning: Host key of the server must be added using 'crypto host_key
add' exec command before sftp repository can be used.
atw-cp-ise02/admin(config-Repository)# exit
atw-ise245/admin# crypto host_key add host 172.25.73.253
host key fingerprint added
# Host 172.25.73.253 found: line 1 type RSA
2048 fa:0c:a4:b4:28:78:fd:0f:b7:91:1a:a5:8f:72:4a:1c 172.25.73.253
(RSA)
```

TFTP is not a common repository type for ISE. TFTP servers often have drawbacks related to file sizes, and ISE packages usually exceed those file-size limitations. No credentials are necessary because TFTP is connectionless and does not use authentication credentials, as shown in [Figure 27-8](#).

**Note** TFTP is significantly slower than FTP because it uses 512-byte packets, and each packet must be acknowledged (ACK'd). Therefore, on high-latency links, TFTP can be hundreds of times slower. Even on low-latency links, TFTP is much slower than FTP.



**Figure 27-8** TFTP Repository

The Network File System (NFS) repository is fairly common, especially in environments with a network-attached storage (NAS) system. NFS is usually a responsive and reliable transport mechanism for storage. This repository requires the NFS server, IP address or FQDN, and path and credentials, as shown in [Figure 27-9](#).

**Identity Services Engine**

Home > Context Visibility > Operations > Policy > Admin

System Identity Management Network Resources Device Portal Management pxGrid Services

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin

Patch Management

Repository

Operational Data Purging

**Repository List > Add Repository**

**Repository Configuration**

\* Repository Name

\* Protocol

**Location**

\* Server Name

\* Path

**Credentials**

\* User Name

\* Password

**Submit** **Cancel**

The screenshot shows the 'Add Repository' configuration page for an NFS repository. The 'Repository Name' is set to 'ATW-NFS'. The 'Protocol' is selected as 'NFS'. In the 'Location' section, the 'Server Name' is '172.25.73.253' and the 'Path' is '/mnt/array1/source'. Under 'Credentials', the 'User Name' is 'admin' and the 'Password' is masked as '\*\*\*\*\*'. At the bottom are 'Submit' and 'Cancel' buttons.

**Figure 27-9** NFS Repository

CD-ROM is a repository that is used with the physical CD-ROM/DVD-ROM drive of the Cisco SNS 3315, 3355, and 3395 appliances (SNS 3415, 3495, 3515, and 3595 appliances have no drive) or the virtual CD drive with VMware, as shown in [Figure 27-10](#).

The screenshot shows the Cisco Identity Services Engine interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Admin, System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade, Backup & Restore, and Administration. The Maintenance link is highlighted. On the left, a sidebar lists Patch Management, Repository (which is selected and highlighted in blue), and Operational Data Purging. The main content area is titled "Repository List > Add Repository" and "Repository Configuration". It contains fields for "Repository Name" (set to "ATW-CDROM"), "Protocol" (set to "CDROM"), and "Location" with a "Path" field containing a single slash (/). At the bottom are "Submit" and "Cancel" buttons.

**Figure 27-10** CD-ROM Repository

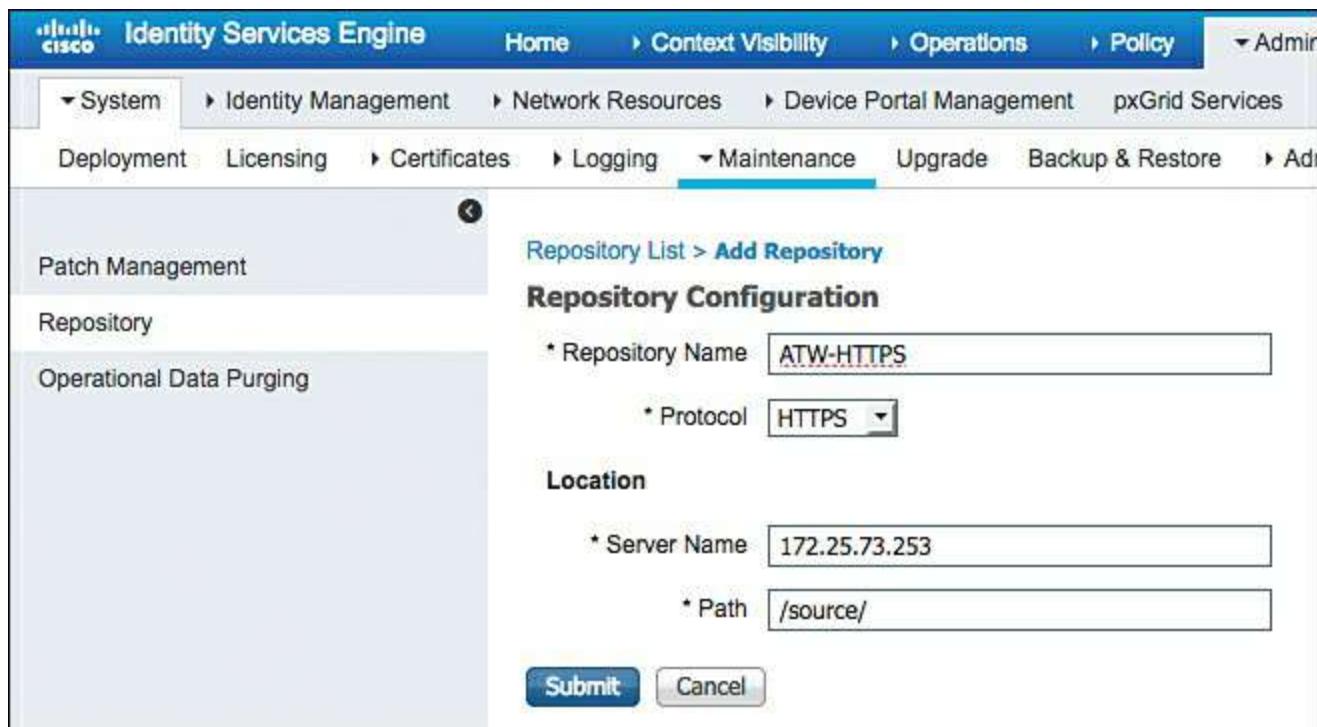
HTTP is used for Hypertext Transfer Protocol (HTTP) file storage. This repository does not support authentication credentials, just the path, as shown in [Figure 27-11](#). Yes, an HTTP repository without the capability to authenticate is fairly useless, so don't expect this one to get much usage today unless it is only to download files.

This screenshot is identical to Figure 27-10, showing the configuration for an "ATW-HTTP" repository using the HTTP protocol. The "Path" field is set to "/source/".

**Figure 27-11** HTTP Repository

HTTPS is used for HTTP Secure file storage. This repository does not provide authentication credentials, just the path, as shown in [Figure 27-12](#). Yes, an HTTPS-

encrypted repository type that does not provide enough security to authenticate the user is again pretty useless. So, don't expect this one to get too much usage today, either.



**Figure 27-12** HTTPS Repository

You may validate the repository at any time from the command line by using the **show repository repository-name** command, as shown in Example 27-3.

### Example 27-3 Output of **show repository** Command

[Click here to view code image](#)

```
atw-cp-ise02/admin# show repository ATW-CDROM
FILE NAME                                SIZE   MODIFIED TIME
=====
.discinfo                               102 Bytes Tue Nov 13 18:38:10
2012
Server                                  72 KB   Mon Nov 19 02:26:26
2012
TRANS.TBL                               1 KB    Mon Nov 19 02:26:26
2012
images                                   2 KB    Mon Nov 19 02:25:36
2012
isolinux                                 2 KB    Mon Nov 19 02:25:36
2012
ks.cfg                                    24 KB   Mon Nov 19 02:25:36
2012
```

## Performing the Upgrade

As mentioned earlier in the chapter, ISE 2.0 adds a graphical tool to automate the upgrade process and the tool follows the SPF approach.

To perform the upgrade:

**Step 1.** Navigate to **Administration > System > Upgrade**, as shown in [Figure 27-13](#).

The Overview tab is displayed, showing all the nodes within the ISE cube and their role.

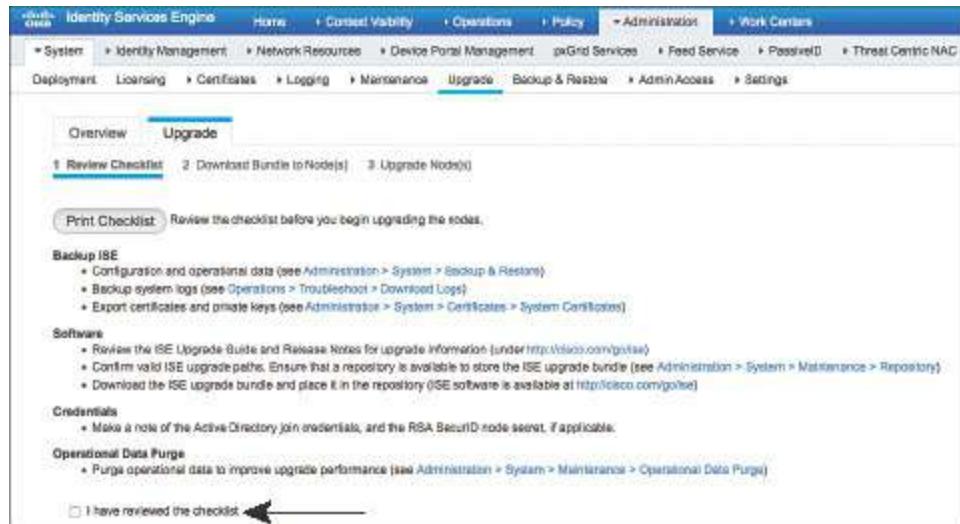
The screenshot shows the Cisco Identity Services Engine (ISE) Administration interface. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, PassiveID, Threat Centric NAC, Deployment, Licensing, Certificates, Logging, Maintenance, Upgrade (which is highlighted), Backup & Restore, Admin Access, and Settings. Below the navigation bar, there are two tabs: Overview and Upgrade. The Overview tab is currently selected. A note below the tabs states: "Read only mode. Click the Upgrade tab to proceed." A table below the note lists four nodes with their details: Node Group - Host Name, Persona, Version - Repository, and Status. The nodes are: atw-ise244.securitydemo.net (Admin SECONDARY Monitor SECONDARY, 2.1.0.474 nodelist.version.label.patch, Active); DataCenter1PSNs - atw-ise247.securityde... (Policy service, 2.1.0.474 nodelist.version.label.patch, Active); DataCenter1PSNs - atw-ise246.securityde... (Policy service, 2.1.0.474 nodelist.version.label.patch, Active); and atw-ise245.securitydemo.net (Admin PRIMARY Monitor PRIMARY, 2.1.0.474 nodelist.version.label.patch, Active). Each node entry has a red vertical bar on its left side.

Node Group - Host Name	Persona	Version - Repository	Status
atw-ise244.securitydemo.net	Admin SECONDARY Monitor SECONDARY	2.1.0.474 nodelist.version.label.patch	● Active
DataCenter1PSNs - atw-ise247.securityde...	Policy service	2.1.0.474 nodelist.version.label.patch	● Active
DataCenter1PSNs - atw-ise246.securityde...	Policy service	2.1.0.474 nodelist.version.label.patch	● Active
atw-ise245.securitydemo.net	Admin PRIMARY Monitor PRIMARY	2.1.0.474 nodelist.version.label.patch	● Active

**Figure 27-13 Upgrade Overview**

**Step 2.** Click the **Upgrade** tab.

As you can see in [Figure 27-14](#), you are presented with a checklist that you must acknowledge before proceeding with the upgrade.



**Figure 27-14 Upgrade Checklist**

**Step 3.** Review and perform the items in the checklist prior to upgrading, check the **I Have Reviewed the Checklist** check box, and click **Continue**.

**Step 4.** Check the check boxes on the left to select the first nodes to download the bundle to.

Step 2 in the tool is to download the upgrade bundle from a repository to each node in the cube, as shown in [Figure 27-15](#). You are selecting nodes that will use the same repository. For instance, if there are two data centers, select the nodes that are all in the same data center together.

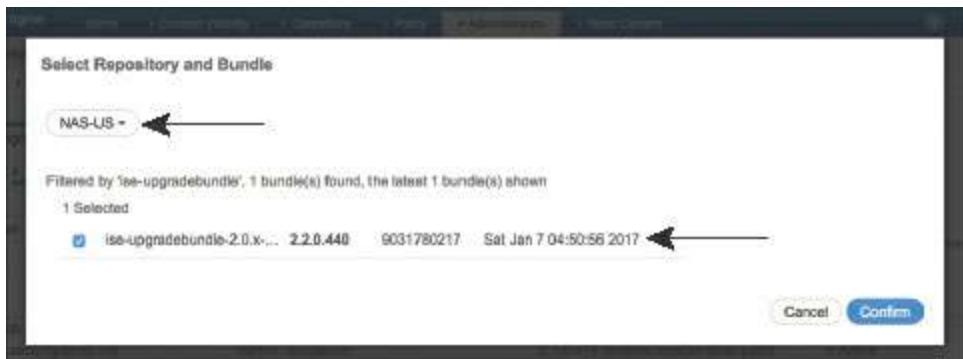
	Node Group - Host Name	Persona	Version - Repository	Status
<input checked="" type="checkbox"/>	atw-ise244.securitydemo.net	Admin <small>SECONDARY</small> Monitor <small>SECONDARY</small>	2.1.0.474 nodelist.version.label.patch	<span style="color: green;">Active</span>
<input type="checkbox"/>	DataCenter1PSNs - atw-ise247.securityde...	Policy service	2.1.0.474 nodelist.version.label.patch	<span style="color: green;">Active</span>
<input checked="" type="checkbox"/>	DataCenter1PSNs - atw-ise246.securityde...	Policy service	2.1.0.474 nodelist.version.label.patch	<span style="color: green;">Active</span>
<input type="checkbox"/>	atw-ise245.securitydemo.net	Admin <small>PRIMARY</small> Monitor <small>PRIMARY</small>	2.1.0.474 nodelist.version.label.patch	<span style="color: green;">Active</span>

**Figure 27-15 Selecting First Nodes**

**Step 5. Click Download.**

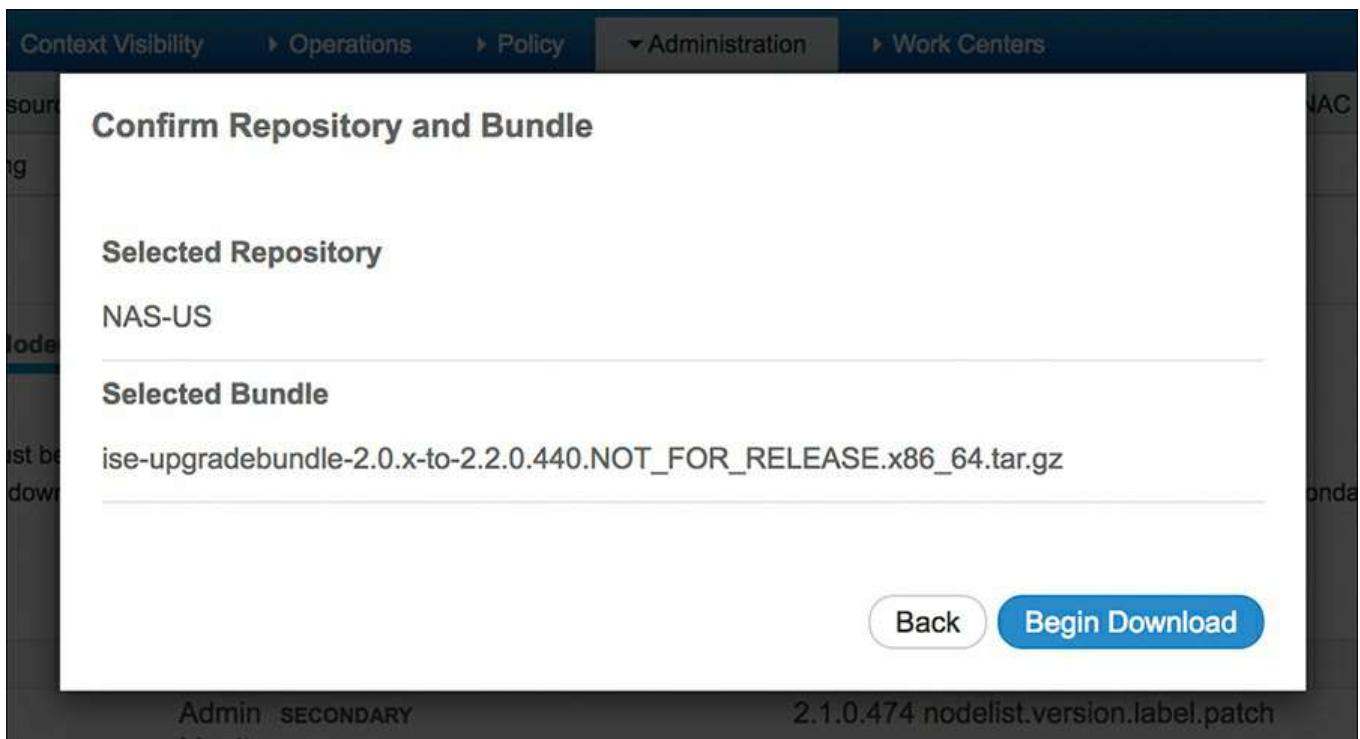
**Step 6. Select the repository from the drop-down list.**

Any properly named upgrade bundles that exist in that repository are listed in the UI automatically, as shown in [Figure 27-16](#). Select the correct upgrade bundle.



**Figure 27-16** Choosing a Repository for Nodes

**Step 7. Click Confirm.** Another confirmation box appears, as shown in [Figure 27-17](#).



**Figure 27-17** Confirming Your Confirmation

**Step 8. Click Begin Download.**

The selected nodes start downloading the bundle from the repository and a progress bar for the download is displayed, as shown in [Figure 27-18](#).

2 Selected				
	Node Group - Host Name	Persona	Version - Repository	Status
<input type="checkbox"/>	atw-ise244.securitydemo.net	Admin <small>SECONDARY</small> Monitor <small>SECONDARY</small>	2.1.0.474 nodelist.version.label.patch <small>...</small>	57%  Downloading... <small>?</small>
<input type="checkbox"/>	DataCenter1PSNs - atw-ise247.securityde...	Policy service	2.1.0.474 nodelist.version.label.patch	Active
<input checked="" type="checkbox"/>	DataCenter1PSNs - atw-ise246.securityde...	Policy service	2.1.0.474 nodelist.version.label.patch <small>...</small>	52%  Downloading... <small>?</small>
<input type="checkbox"/>	atw-ise245.securitydemo.net	Admin <small>PRIMARY</small> Monitor <small>PRIMARY</small>	2.1.0.474 nodelist.version.label.patch	Active

**Figure 27-18** Download Progress

**Step 9.** Repeat Steps 4 through 8 for the rest of the nodes, grouping the nodes by repository.

**Note** There is no limit to the number of nodes that can use a single repository, nor is there a limit to the number of nodes you can download to at a time. The separating of nodes and grouping by repository is simply recommended for downloading the files from the closest and most performant repository with respect to that node.

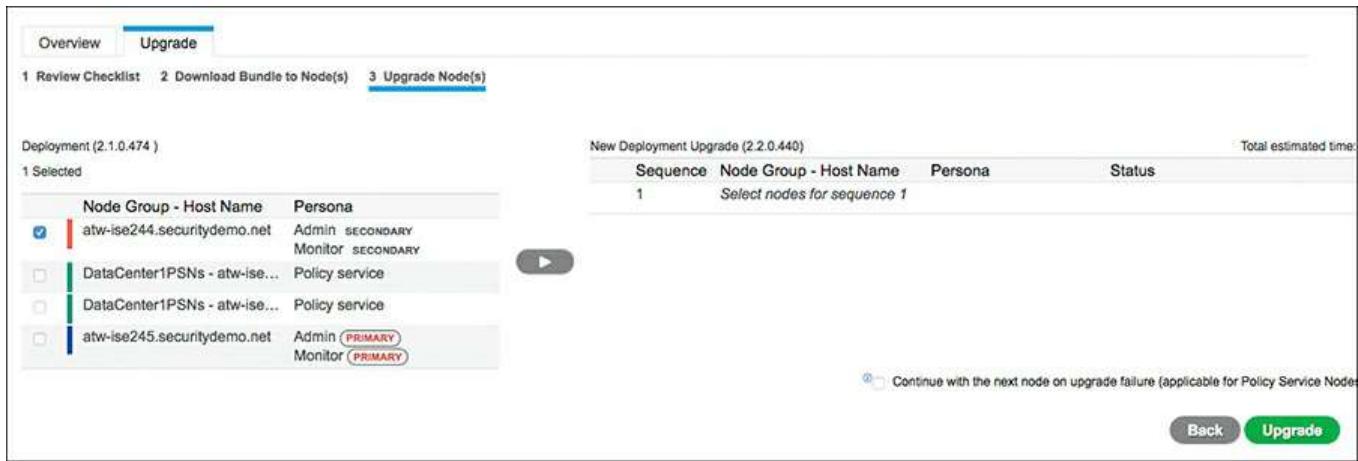
After all the nodes have the upgrade bundle downloaded, it is unbundled onto the local disk. After that succeeds, the node status changes to Ready for Upgrade and the **Continue** button enables itself, as shown in [Figure 27-19](#).

<a href="#">Overview</a> <a href="#">Upgrade</a>				
<a href="#">1 Review Checklist</a> <a href="#">2 Download Bundle to Node(s)</a> <a href="#">3 Upgrade Node(s)</a>				
<a href="#">Download</a> <a href="#">Abort</a>				
<small>Note: The bundle must be present in the repository. From the repository, download the bundle to one or more nodes simultaneously. To proceed with upgrade, download the bundle to the Secondary Administration and Primary Monitor nodes.</small>				
	Node Group - Host Name	Persona	Version - Repository	Status
<input type="checkbox"/>	atw-ise244.securitydemo.net	Admin <small>SECONDARY</small> Monitor <small>SECONDARY</small>	2.1.0.474 nodelist.version.label.patch <small>...</small>	Ready for upgrade <small>?</small>
<input type="checkbox"/>	DataCenter1PSNs - atw-ise247.securityde...	Policy service	2.1.0.474 nodelist.version.label.patch <small>...</small>	Ready for upgrade <small>?</small>
<input type="checkbox"/>	DataCenter1PSNs - atw-ise246.securityde...	Policy service	2.1.0.474 nodelist.version.label.patch <small>...</small>	Ready for upgrade <small>?</small>
<input type="checkbox"/>	atw-ise245.securitydemo.net	Admin <small>PRIMARY</small> Monitor <small>PRIMARY</small>	2.1.0.474 nodelist.version.label.patch <small>...</small>	Ready for upgrade <small>?</small>

**Figure 27-19** Ready for Upgrade

**Step 10.** Click **Continue**.

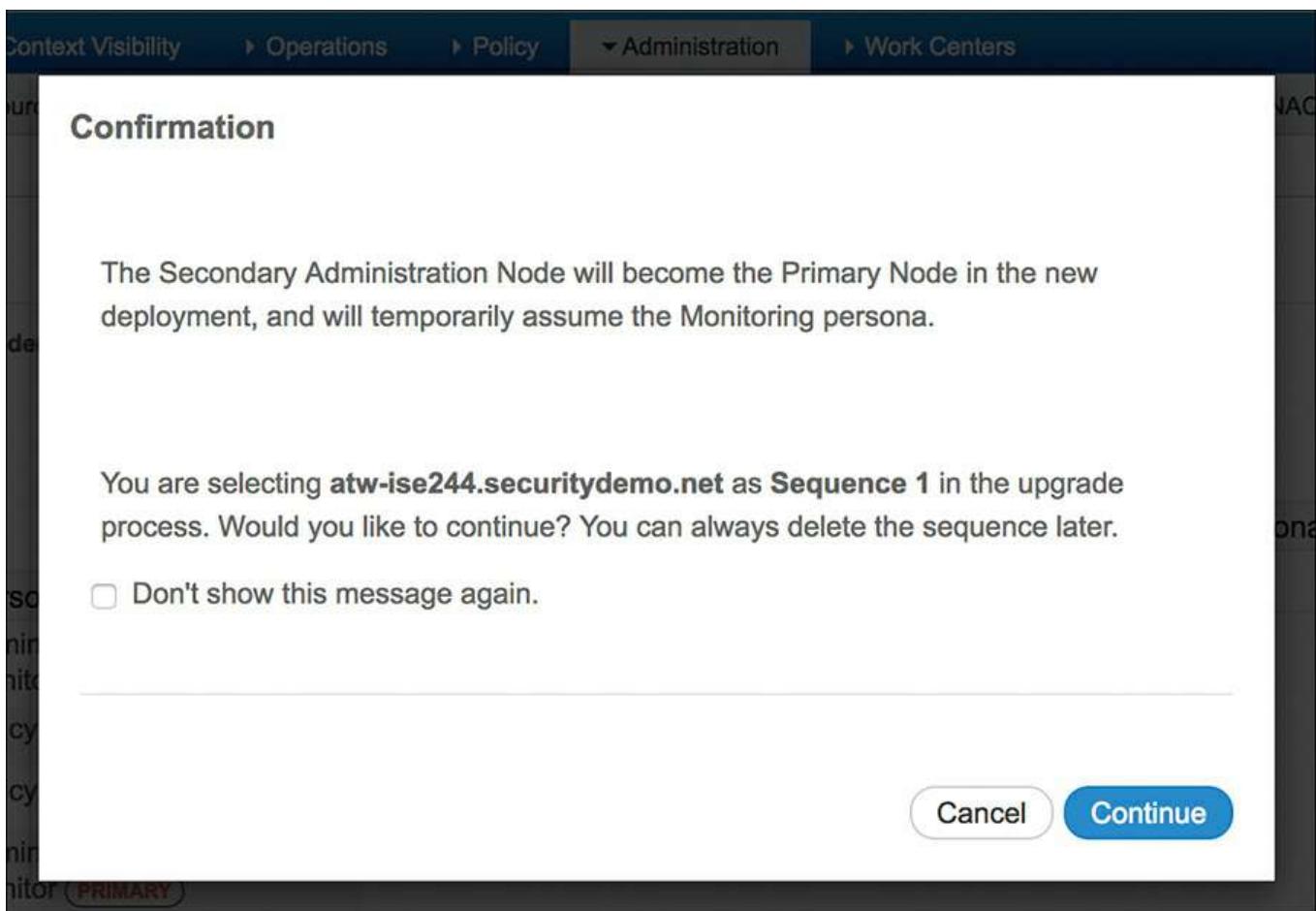
Now you are presented with a screen where you can choose the upgrade order of the nodes, as shown in [Figure 27-20](#).



**Figure 27-20** Upgrade Nodes Screen

**Step 11.** Select the secondary admin node and click the arrow icon to move it from the left to the right.

**Step 12.** Click **Continue**, as seen in [Figure 27-21](#).



**Figure 27-21** Confirming Your Choice

**Step 13.** Select the other node(s) and assign them to the correct order.

It's recommended that you never upgrade more than two nodes simultaneously.

In smaller deployments, never upgrade more than one at a time, in order to be cautious.

**Step 14.** After all the nodes are selected in the correct order, click **Upgrade**.

[Figure 27-22](#) shows the final upgrade sequence being assigned, and [Figure 27-23](#) shows the nodes all being queued for upgrade.

The screenshot shows the 'Upgrade' step of a deployment wizard. At the top, there are three tabs: 'cklist' (selected), '2 Download Bundle to Node(s)', and '3 Upgrade Node(s)'. On the left, a list of nodes is shown with their group names and host names. On the right, a table titled 'New Deployment Upgrade (2.2.0.440)' lists the upgrade sequence, node group, host name, persona, and status for each node. The total estimated time is 960 mins. The sequence is as follows:

Sequence	Node Group - Host Name	Persona	Status
1	atw-ise244.securitydemo.net	Admin <span style="border: 1px solid red; padding: 2px;">PRIMARY</span> Monitor <span style="border: 1px solid red; padding: 2px;">SECONDARY</span>	300 min. est. time
2	atw-ise247.securitydemo.net	Policy service	180 min. est. time
3	atw-ise246.securitydemo.net	Policy service	180 min. est. time
4	atw-ise245.securitydemo.net	Admin <span style="border: 1px solid red; padding: 2px;">SECONDARY</span> Monitor <span style="border: 1px solid red; padding: 2px;">PRIMARY</span>	300 min. est. time
5	Select nodes for sequence 5		

At the bottom, there is a checkbox for 'Continue with the next node on upgrade failure (applicable for Policy Service Nodes only)' and two buttons: 'Back' and 'Upgrade'.

**Figure 27-22** Upgrade Sequence Assigned

The screenshot shows the 'Upgrade' step of a deployment wizard, similar to Figure 27-22 but with a different visual style. The table is titled 'New Deployment Upgrade (2.2.0.440)' and shows the same sequence of nodes. The status column now indicates that all nodes are 'Upgrade queued'. The total estimated time is 960 mins. The sequence is as follows:

Sequence	Node Group - Host Name	Persona	Status
1	atw-ise244.securitydemo.net	Admin <span style="border: 1px solid red; padding: 2px;">PRIMARY</span> Monitor <span style="border: 1px solid red; padding: 2px;">SECONDARY</span>	Upgrade queued
2	atw-ise247.securitydemo.net	Policy service	Upgrade queued
3	atw-ise246.securitydemo.net	Policy service	Upgrade queued
4	atw-ise245.securitydemo.net	Admin <span style="border: 1px solid red; padding: 2px;">SECONDARY</span> Monitor <span style="border: 1px solid red; padding: 2px;">PRIMARY</span>	Upgrade queued
5	Select nodes for sequence 5		

At the bottom, there is a checkbox for 'Continue with the next node on upgrade failure (applicable for Policy Service Nodes only)' and two buttons: 'Back' and 'Upgrade'.

**Figure 27-23** Upgrade Queued

## Command-Line Upgrade

For smaller deployments, such as standalone systems, the Secondary PAN First graphical upgrade process does not hold as much of a purpose. For those types of deployments, or if you just want more control of the process in a larger deployment, you can choose the CLI option.

The command is **application upgrade**, and it has a few options. Begin with the

**application upgrade prepare** command, as shown in Example 27-4. This downloads the upgrade bundle to the local disk, unpacks the bundle, and verifies it is valid and usable.

The node waits for the ISE administrator to continue or cancel the upgrade, so the admin can choose when the upgrade occurs, such as during a change control window.

#### Example 27-4 Output of **application upgrade prepare** Command

[Click here to view code image](#)

```
atw-ise245/admin# application upgrade prepare ise-upgradebundle-2.0.x-
to-2.2.0.440.NOT_FOR_RELEASE.x86_64.tar.gz NAS-US
Getting bundle to local machine...
Unbundling Application Package...
Verifying Application Signature...
Application upgrade preparation successful
```

If you need to cancel the upgrade, use the **application upgrade cleanup** command, as shown in Example 27-5. This deletes all the unpacked upgrade files created during the prepare phase.

#### Example 27-5 Output of **application upgrade cleanup** Command

[Click here to view code image](#)

```
atw-ise245/admin# application upgrade cleanup
Application upgrade preparation directory cleanup successful
```

To continue the upgrade, use the **application upgrade proceed** command, as shown in Example 27-6. This begins the upgrade process. If it's a multinode deployment, remember to do the Secondary PAN First.

#### Example 27-6 Output of **application upgrade proceed** Command

[Click here to view code image](#)

```
atw-ise244/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until
upgrade completes.
-Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
```

```
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: De-registering node from current deployment...
STEP 5: Taking backup of the configuration data...
- Running db sanity check to fix index corruption, if any...
- Auto Upgrading Schema for UPS Model...
- Upgrading Schema completed for UPS Model.

ISE database schema upgrade completed.

STEP 7: Running ISE configuration data upgrade...
- Data upgrade step 1/48, NSFUpgradeService(2.1.101.145) ... Done in 33 seconds.
- Data upgrade step 2/48, ProfilerUpgradeService(2.1.101.145) ... Done in 1 seconds.
<SNIP>

- Data upgrade step 48/48, GuestAccessUpgradeService(2.2.0.440) ...
Done in 5 seconds.

STEP 8: Running ISE configuration data upgrade for node specific data...

STEP 9: Making this node PRIMARY of the new deployment. When other nodes are upgraded it will be added to this deployment.

STEP 10: Running ISE M&T database upgrade...
ISE M&T Log Processor is not running
ISE database M&T schema upgrade completed.
% Warning: Some warnings encountered during MNT sanity check
Gathering Config schema(CEPM) stats .....
Gathering Operational schema(MNT) stats .....
% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes successfully.

<SNIP>

% This application Install or Upgrade requires reboot, rebooting now...
Broadcast message from root@atw-ise244 (pts/1) (Sat Jan  7 18:12:13 2017):
The system is going down for reboot NOW
```

## **Summary**

This chapter discussed the importance of repositories and the types of repositories available. It reviewed the Secondary PAN First upgrade process, and stepped through examples of using the GUI-based upgrade tool and the command-line upgrade commands.

## **Part VII Device Administration**

[Chapter 28 Device Administration Fundamentals](#)

[Chapter 29 Configuring Device Admin AAA with Cisco IOS](#)

[Chapter 30 Configuring Device Admin AAA with Cisco WLC](#)

[Chapter 31 Configuring Device Admin AAA with Cisco Nexus Switches](#)

# Chapter 28 Device Administration Fundamentals

This chapter covers the following topics:

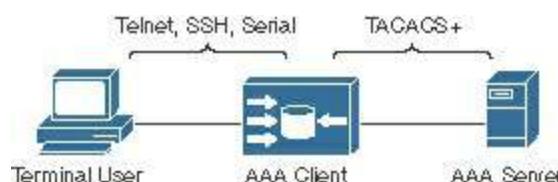
- Device administration in ISE
- Enabling TACACS+ in ISE
- Network devices

In [Chapter 2](#), “[Fundamentals of AAA](#),” you were introduced to the concepts of network access AAA and device administration AAA. Although both are focused on identifying “who” is allowed to perform “what” action, they are vastly different in their ultimate purpose. The purposes are so different, in fact, that a few years ago Aaron Woland wrote an article for Network World about why both types shouldn’t be in ISE; that ISE should stick to network access AAA and leave device admin AAA for Cisco Access Control Server (ACS) to handle. You can read that opinion piece here:

<http://www.networkworld.com/article/2838882/radius-versus-tacacs.html>.

As described in [Chapter 2](#), device administration AAA exists to control access to network device consoles, Telnet sessions, Secure Shell (SSH) sessions, or other method of gaining administrative control over a network device. The purpose is not only to control the access, but also to provide centralized visibility of all those actions. For example, if an administrator makes a change that causes a network outage, then the organization will need an audit trail (proof) of who caused it and what they did.

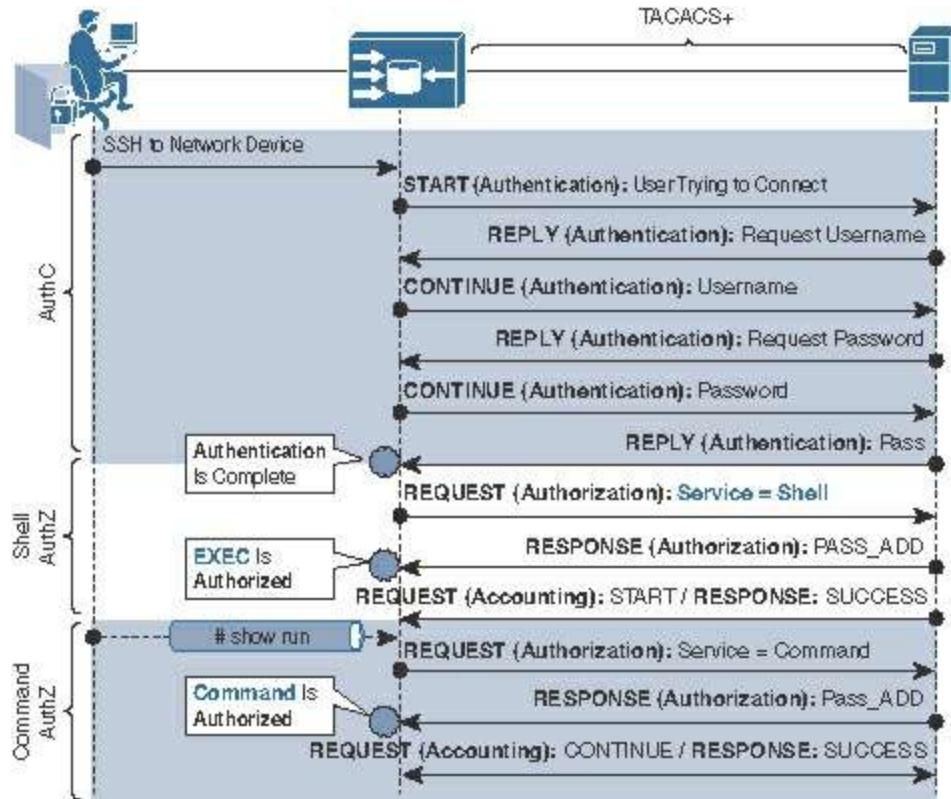
[Figure 28-1](#) illustrates device administration graphically.



**Figure 28-1** Device Administration AAA

Device administration AAA is very interactive in nature, or at least it can be. An administrator could write a policy that authorizes the user’s entire CLI session, or a policy that requires authorization of each and every command the user enters (authenticate once, authorize many). Due to the extremely interactive nature of command authorization, TACACS+ lends itself to be the perfect AAA protocol for device administration.

[Figure 28-2](#) illustrates how TACACS+ can perform the authenticate once, authorize many. This is key for device administration. Think about it: You can authenticate the user, then authorize them to access the CLI of a router, but you may still have to authorize each of the commands entered from that CLI for granular control.



**Figure 28-2** Authenticate Once, Authorize Many

Please review [Chapter 2](#) for more information on what device administration AAA is and for a detailed look at TACACS+.

## Device Administration in ISE

When it comes to the Identity Services Engine, device administration is synonymous with TACACS+. Everything to do with TACACS+ exists within the Device Administration Work Center. In fact, to enable TACACS+, there is a single license, named Device Admin, as shown in [Figure 28-3](#). Unlike Base, Plus, and Apex licenses, the Device Admin license does not have a per-device count. It's a single license that applies for the entire ISE cube, and is valid for the maximum number of network devices. This differs a bit from what you may be used to with the predecessor to ISE, Cisco ACS, which had a base license and a large deployment license. ISE only has the latter.



**Figure 28-3** Device Admin License Enabled

If the device admin license is not enabled, the corresponding Work Center is not

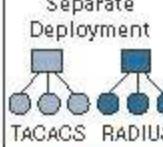
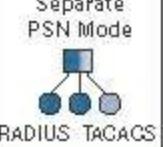
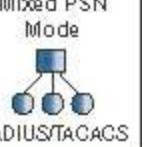
displayed.

There are a few schools of thought when it comes to designing ISE for device administration. As previously mentioned, Aaron Woland has publically stated his belief that device administration AAA has no business being in a network access AAA product. There is too much disparity in the uses of the two AAA types, their traffic patterns, and the load level they put on the AAA and monitoring servers.

There are a few different design options:

- Separate ISE cubes, with one for RADIUS and another for TACACS+. Provides dedicated PSNs and dedicated MnT nodes for each function.
- Mixed ISE cube with separate PSNs, which provides dedicated PSNs for each AAA protocol but shares a single MnT node for logging and reporting.
- Mixed ISE cube where the PSNs are not dedicated to any protocol.

[Figure 28-4](#) presents a table created by the father of TACACS+ at Cisco, Douglas Gash. Doug is the brilliant chief architect of TACACS+ for ACS and ISE at Cisco, as well as a major contributor to the TACACS+ standard within the IETF. This table helps you to decide which deployment model to follow, based on what is most important to your organization. Is it scale of TACACS+ and RADIUS services? Are the audit trail and log retention most important? Perhaps it is a political separation of duties within your organization?

Priorities According to Policy		Separate Deployment	Separate PSN Mode	Mixed PSN Mode
TACACS	RADIUS			
Separation of Configuration	Yes: Specialization for TACACS+ No: Avoid Duplication of Shared Items Avoid Cost of Duplicate PAN/PSN	✓		✓
Separation of Logging Store	Yes: Optimize Log Retention VM No: Centralized Monitoring	✓	✓	✓
Independent Scaling of Services	Yes: Scale as Needed Avoid NAC/Device Admin Load No: Avoid Underutilized PSNs	✓	✓	✓

**Figure 28-4** Doug Gash's Options for Deploying Device Admin

For simplicity, in this chapter we separate the deployment recommendations into categories based on deployment size: large, medium, and small.

## Large Deployments

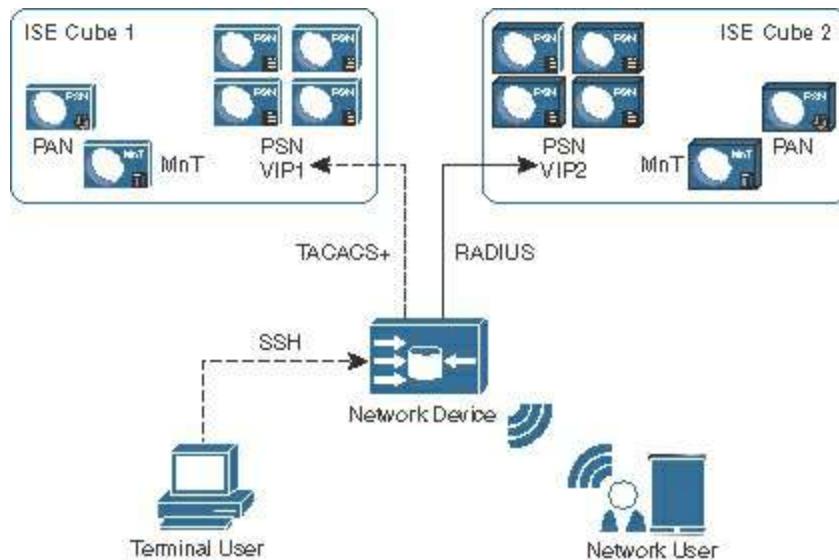
For a large deployment, it is best to have separate ISE cubes for network access and device administration. That ensures one will never affect the other. After all, you would

never want to accidentally prevent your CEO from getting on the wireless network, just because a script was actively making a lot of changes across your network infrastructure. Nor would you want the audit logs for network device changes to be kept for less time because the limited MnT disk space was shared between network access and device admin.

MnT is one of the key items of concern. The MnT node plays a key role with network access functions beyond just logging and reporting. As of ISE 2.2, MnT is still the holder of critical functions such as the centralized session directory; the pxGrid topic publishing for session data; merging of passiveID and active authentication data into the session directory; and much more.

If the MnT node must also process tremendous amounts of logging for all the command authorization accounting—logging entries for every single command entered on every single network device in the entire organization—you can begin to see why this becomes a point of concern.

[Figure 28-5](#) illustrates two different ISE cubes. Cube 1 is dedicated to TACACS+ and Cube 2 is dedicated to RADIUS. Therefore, the PAN and MnT nodes are also dedicated, not just the PSNs. Although the illustration does include a virtual IP (VIP) for the PSNs, a load balancer is not required. It's only illustrated this way to show a common practice.



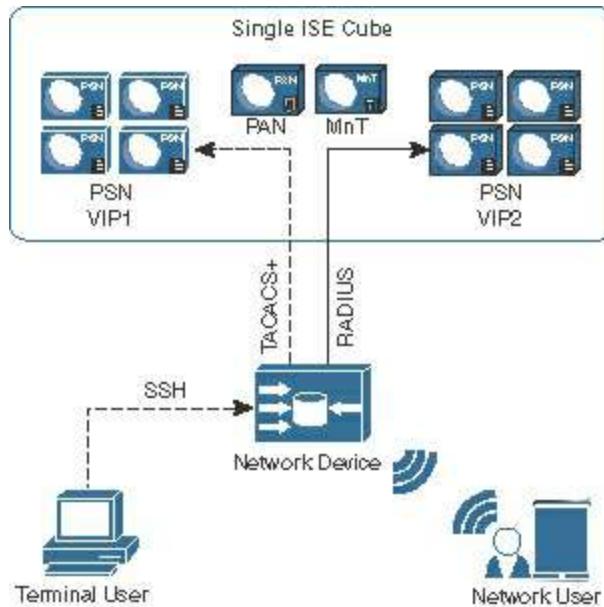
**Figure 28-5** Large Deployments: Separate ISE Cubes for TACACS+ and RADIUS

## Medium Deployments

With medium-size deployments, you may want to have a single ISE cube, but it is best to have separate PSNs for network access and device administration. That ensures one will never affect the other, without having to maintain separate cubes.

One set of PSNs would primarily be responsible for all the RADIUS traffic, while another set of PSNs would be primarily responsible for the TACACS+ traffic. For redundancy, you may choose to send the RADIUS traffic to the TACACS+ PSNs, but only in the case of a disaster. The primary purpose of the PSNs is still dedicated to either RADIUS or TACACS+.

[Figure 28-6](#) illustrates a single ISE cube, with dedicated PSNs per function. As with a large deployment, although the illustration shows a VIP for the PSNs, a load balancer is not required. It's only illustrated this way to show a common practice.

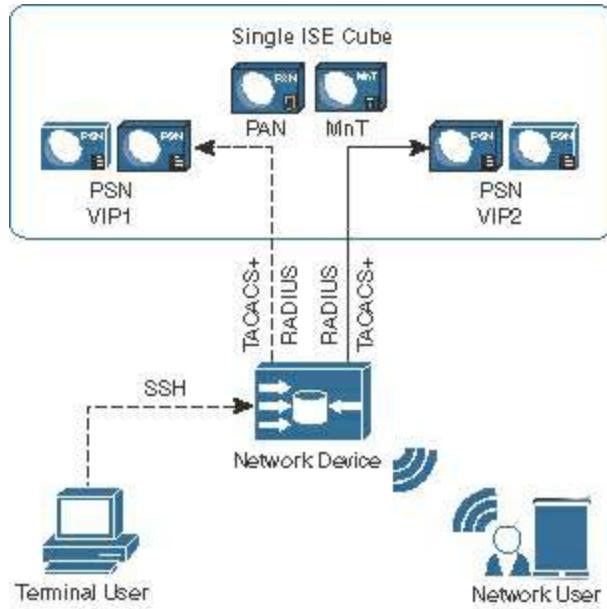


**Figure 28-6** Medium Deployments: One ISE Cube, Separate PSNs for TACACS+ and RADIUS

## Small Deployments

A small deployment could certainly be just a single ISE cube, or even a standalone ISE node that is performing all functions. In these instances, there are no dedicated nodes—all PSNs handle equal amounts of TACACS+ and RADIUS traffic.

[Figure 28-7](#) illustrates a single ISE cube with dedicated PSNs per function. Again, the illustration shows a VIP for the PSNs, but a load balancer is not required. It's only illustrated this way to show a common practice.



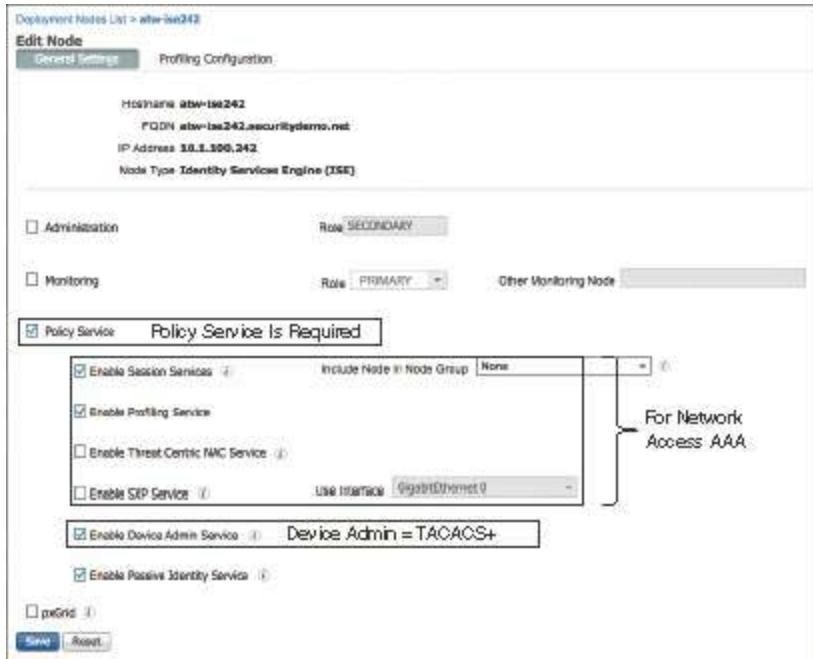
**Figure 28-7** Small Deployments: One ISE Cube, No Separation of TACACS+ and RADIUS

## Enabling TACACS+ in ISE

Installing the Device Admin license is not enough to start accepting TACACS+ communications. You also must enable it in the Deployment settings:

- Step 1.** Navigate to **Administration > System > Deployment**.
- Step 2.** Select the PSN where you wish to enable TACACS+.
- Step 3.** Check the **Enable Device Admin Service** check box.
- Step 4.** Click **Save**.

[Figure 28-8](#) shows the deployment screen for a PSN.



**Figure 28-8 Deployment Screen**

Know your intended design before enabling the TACACS+ functionality, and only enable the Device Admin service on the PSNs that will handle TACACS+; leave it disabled on any PSNs that are supposed to be dedicated for RADIUS, and vice versa. Keep the remainder of the session services disabled on the dedicated TACACS+ PSNs.

A more practical and easier-to-use method for enabling the TACACS+ run time on an ISE PSN is shown later in the chapter, in the section “Device Administration Work Center.”

## Network Devices

We can design ISE cubes and TACACS+ or RADIUS PSNs all day long. Yet, none of it will matter if the network access device (NAD) is not set up correctly. Just like RADIUS, the NAD object within ISE must be configured with the TACACS+ shared secret, and the connection type.

The same Network Device Group (NDG) guidelines for network access apply for device administration as well. The more applicable the NDG design is for your organization, the more it aids in your policy creation. Device type, location, and line of business are all very useful types of NAD groupings.

[Figure 28-9](#) shows the TACACS+ portion of the NAD definition in the ISE UI.

\* Network Device Group

Device Type	Cisco	<input checked="" type="checkbox"/>	Set To Default
IPSEC	Is IPSEC Device	<input checked="" type="checkbox"/>	Set To Default
Location	SJC	<input checked="" type="checkbox"/>	Set To Default
Stage	Stage	<input checked="" type="checkbox"/>	Set To Default

▶ RADIUS Authentication Settings

▾ TACACS Authentication Settings

Shared Secret	*****	Show	Retire	i
Enable Single Connect Mode	<input type="checkbox"/>			
<input checked="" type="radio"/> Legacy Cisco Device <input type="radio"/> TACACS Draft Compliance Single Connect Support				

**Figure 28-9** NAD TACACS+ and NDG Configuration

In [Figure 28-9](#) you can see the NDG assignments, such as Device Type. In this instance, the Device Type assignment is leveraged to identify this switch as a Cisco access layer switch, so we effectively use that assignment to point the TACACS+ requests to a policy set that is created for IOS devices.

[Figure 28-9](#) also shows how the TACACS+ shared secret gets configured, just like with RADIUS. That shared secret is the password used between the NAD and ISE to validate the source of the TACACS+ communication and to provide a seed value for the encryption.

There is also an option to Enable Single Connect Mode. The normal communication mode for TACACS+ is to open a new TCP session for each and every TACACS communication, which means each authentication request, each authorization request, and each accounting request. Enabling this setting allows the NAD to maintain a single open connection between itself and the TACACS+ service on ISE. This type of connection is more efficient because it allows the service to handle a higher number of TACACS operations, but it does require the NAD to also be configured for Single Connect.

Next, note the **Retire** button. This allows the administrator to retire the existing shared secret and configure a new one. During the retirement period, ISE accepts both the old and new shared secrets for the device, allowing the administrator some buffer time, making the updating of shared secrets more operationally feasible. The retirement time leverages the timer configured under **Work Centers > Device Administration > Settings > Connection Settings**, as shown in [Figure 28-10](#) in the next section.

## Device Administration Global Settings

The retire option for shared secrets is just one of the many global settings for TACACS+ within ISE. To see the globally applicable settings, navigate to **Work Centers > Device Administration > Settings**, as shown in [Figure 28-10](#).

The screenshot shows the 'Device Admin Policy Sets' section of the 'Settings' tab. The 'Connection Settings' tab is selected. Configuration options include:

- Protocol Session Timeout: 5 Minutes (Range 1-9999)
- Connection Timeout: 10 Minutes (Range 1-9999)
- Maximum Packet Size: 32768 kb (Range 4096-65536)
- Single Connect Support: checked
- Username Prompt: Username: [text input field]
- Password Prompt: Password: [text input field]
- Default Shared Secret Retirement Period: 7 Days (Range 1-99)

At the bottom right are 'Reset' and 'Save' buttons.

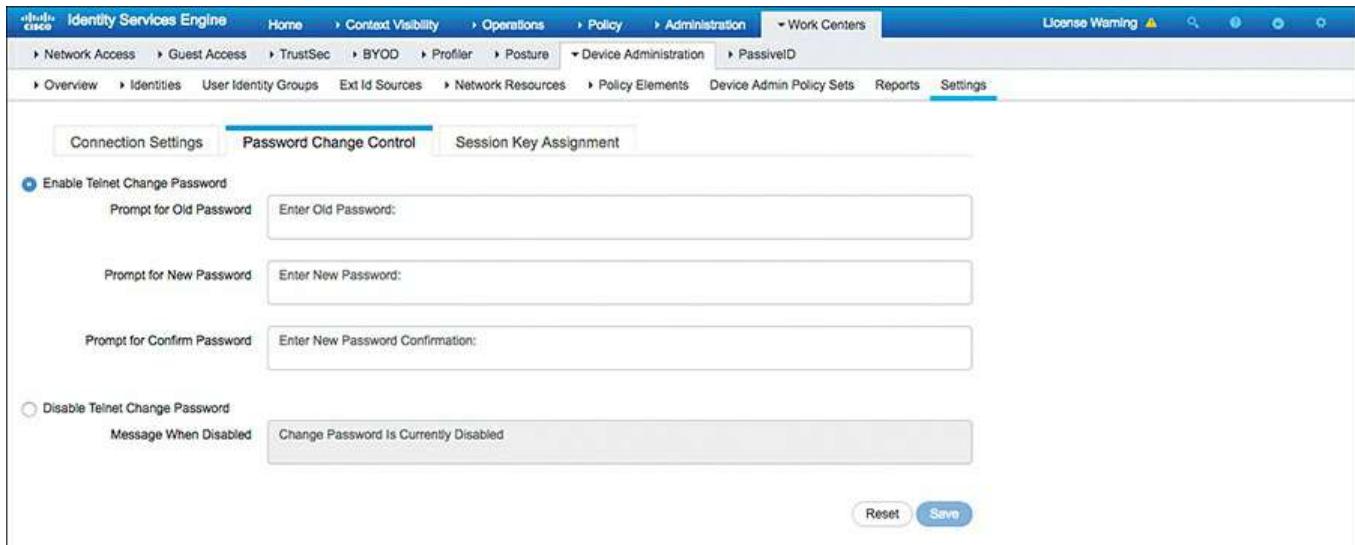
**Figure 28-10** Device Administration Work Center Settings

## Connection Settings

[Figure 28-10](#) shows that the tab displayed by default is Connection Settings. The shared secret retirement period is configured on this tab, and can range from 1 to 99 days. The connection and session timers are also configured on this tab, as well as the string used for username and password prompts and a check box for indicating whether Single Connect Mode should be enabled.

## Password Change Control

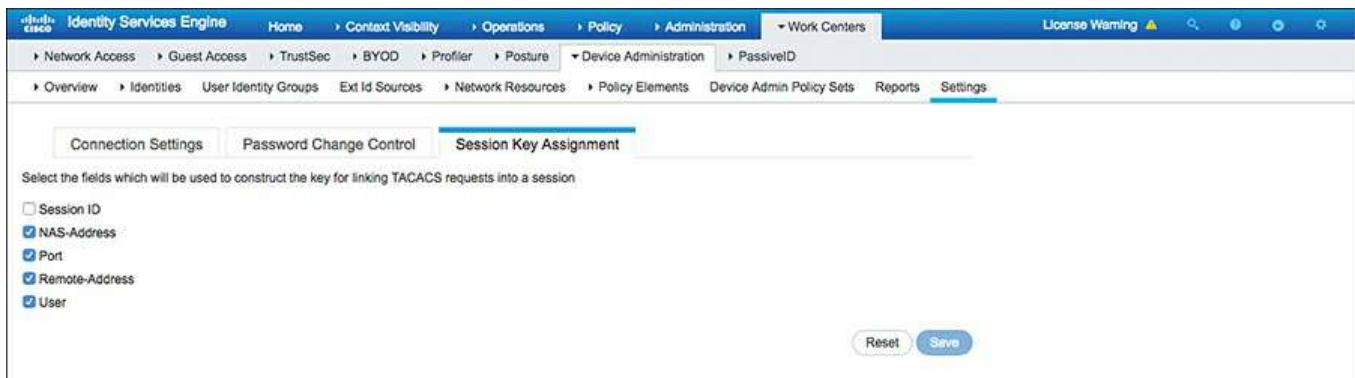
Click the **Password Change Control** tab, shown in [Figure 28-11](#), where you can globally enable or disable the ability to change passwords through the TACACS+ session, and enter the strings to be used in the prompts.



**Figure 28-11** Password Change Control Tab

## Session Key Assignment

Click the **Session Key Assignment** tab, shown in [Figure 28-12](#), to access the remaining global settings. On this tab, you see the different values from the TACACS packets that are available for use in identifying when the packets are part of the same session. This enables ISE to track the full session throughout the single authentication and multiple authorization and accounting requests that may come in. There is rarely a need to change anything on this tab, unless directed by TAC. The real purpose of this setting is to help determine the number of sessions when you configure a limit for the maximum sessions allowed.



**Figure 28-12** Session Key Assignment Tab

## Device Administration Work Center

Now that you have been introduced to the Settings screen of the Device Administration Work Center, this section walks you through the remaining eight screens. As with the other Work Centers in ISE, Device Administration is designed to provide you with access to just about everything you need to accomplish a complete set of tasks, in this

case the administrative tasks associated with device administration AAA. Also, as is the user experience typical of ISE Work Centers, the flow when starting from no configuration is to go from left to right, starting with the Overview screen.

## Overview

[Figure 28-13](#) shows the ISE GUI navigation for the Overview screen of the Device Administration Work Center.

The screenshot shows the ISE Device Administration Work Center. The top navigation bar includes links for Home, Context Visibility, Operations, Policy, Administration, Work Centers, Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, PassiveID, Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets, Reports, and Settings. The left sidebar has links for Introduction, TACACS Livelog, and Deployment. The main content area is titled "Device Administration Overview". It is divided into three sections: "Prepare" (1), "Define" (2), and "Go Live & Monitor" (3). The "Prepare" section contains links for "Authorization Roles", "Migrating from ACS (5.5 - 5.8 & 5.8.1)", and "Enable Deployment for TACACS". The "Define" section contains links for "Configure Devices", "Device Administrators", "Policy", and "Settings". The "Go Live & Monitor" section contains links for "Real-time Monitoring" and "Auditing".

**Figure 28-13** Navigation UI and Introduction Page

You first see the standard Work Center Introduction page, which provides a very broad review of the activities within the Work Center, as well as some helpful links. In this particular introduction page, there is a link to the ACS-to-ISE migration tool.

Next in the Overview navigation menu on the left is TACACS Livelog, a dedicated, near-real-time log screen, but for TACACS only. Much the same as the original Live Log (renamed to RADIUS Live Log), this will become your go-to page when looking for an overview of operations and for troubleshooting. We will come back to this page in the next few chapters.

Finally in the Overview navigation menu is the Deployment page (designed by Aaron

Woland and Doug Gash), shown in [Figure 28-14](#). It is a TACACS deployment page designed to allow you to quickly enable TACACS+ on any number of PSNs from a single screen, instead of having to enable it on each PSN one at a time, as demonstrated previously in [Figure 28-8](#).

The screenshot shows the 'Device Administration Deployment' section of the TACACS deployment page. On the left, there's a sidebar with links: Overview (selected), Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Introduction, TACACS Livelog, and Deployment. The Deployment link is highlighted. The main area has a title 'Device Administration Deployment' and a sub-section 'Activate ISE Nodes for Device Administration'. It includes three radio button options: 'None', 'All Policy Service Nodes', and 'Specific Nodes', with 'Specific Nodes' selected. Below this is a list of ISE nodes with checkboxes: 'ISE Nodes' (unchecked), 'atw-ise237.securitydemo.net' (checked), 'atw-ise241.securitydemo.net' (unchecked), 'atw-ise242.securitydemo.net' (unchecked), and 'atw-ise243.securitydemo.net' (unchecked). A note at the bottom says 'Only ISE Nodes with Policy Service are displayed.' At the bottom are fields for 'TACACS Ports \*' containing '49', a help icon, and buttons for 'Save' and 'Reset'.

**Figure 28-14** TACACS Deployment Page

Examining [Figure 28-14](#), you have three options to enable TACACS: on None of the PSNs, on All of the PSNs, or on Specific Nodes. This page alone saves countless amounts of time and aggravation when setting up ISE for device administration.

Finally, this is the page where you configure the TCP port(s) for TACACS+. By default, only port 49 is leveraged for TACACS. You can add more ports by separating the values with a comma.

## Identities

Moving to the right through the Device Administration Work Center navigation, the next three screens are related to user identities: Identities, User Identity Groups, and Ext Id Sources. However, these user identities are not unique to the Device Administration Work Center at all. In fact, they are the same as the identities you find in the other Work Centers. The Identities screen (see [Figure 28-15](#)) houses the internal users created within ISE's internal user database. The Users page is titled Network Access Users, but that is simply a legacy name, as these user accounts can be leveraged for device administration as well.

The screenshot shows the 'Network Access Users' screen. At the top, there is a navigation bar with links: Overview, Identities (which is highlighted), User Identity Groups, Ext Id Sources, Network Resources, and Policy Elements. Below the navigation bar, there is a toolbar with buttons for Edit, Add, Change Status, Import, Export, Delete, and Duplicate. A table below the toolbar displays user information. The columns are: Status, Name, User Identity Groups, and Description. One row is visible, showing 'Enabled' status, the name 'Internal-Employee', and the description 'Employee'. The 'Status' column has a checkbox icon, and the 'Name' column has a user icon.

**Figure 28-15** User Identities

Remember, internal users can be configured to leverage internal passwords, or they can be local accounts with the same names as AD user accounts and leverage the AD passwords. This is commonly used with device administration as an additional authorization condition—in other words, not only leverage an account or group membership from AD, but also rely on the need for the TACACS+ administrator to create that local account within ISE.

Just as the Identities screen is simply a shortcut of sorts to the existing users, so too are the User Identity Groups screen, shown in [Figure 28-16](#), and the Ext Id Sources screen, shown in [Figure 28-17](#). These are exactly the same as the other areas of the ISE GUI, and are simply shortcuts to those configuration areas to make the Work Center easier to use and more complete.

Name	Description
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
Employee	Default Employee User Group
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
GuestType_Contractor (default)	Identity group mirroring the guest type
GuestType_Daily (default)	Identity group mirroring the guest type
GuestType_Weekly (default)	Identity group mirroring the guest type
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

**Figure 28-16 User Identity Groups**

ISE Node	ISE Node Role	Status	Domain Controller	Site
atw-ise237.securitydemo.net	PRIMARY	Operational	ATW-AD.securitydemo.net	ServerNet
atw-ise241.securitydemo.net	SECONDARY	Operational	ATW-AD.securitydemo.net	ServerNet
atw-ise242.securitydemo.net	SECONDARY	Operational	ATW-AD.securitydemo.net	ServerNet
atw-ise243.securitydemo.net	SECONDARY	Operational	ATW-AD.securitydemo.net	ServerNet

**Figure 28-17 Ext Id Sources**

## Network Resources

Again, similar to the three screens to its left, the Network Resources screen of the Device Administration Work Center is a shortcut to the same network resources available all throughout the ISE GUI and within other Work Centers. A very noticeable difference is the inclusion of TACACS External Servers and TACACS Server Sequence pages, as shown in [Figure 28-18](#).

Overview	Identities	User Identity Groups	Ext Id Sources	Network Resources	Policy Elements	Device Admin Policy Sets
Network Devices	TACACS External Servers					
Network Device Groups	0 Selected					
Default Devices	Rows/Page					
TACACS External Servers	Refresh	Add	Duplicate	Trash	Edit	
TACACS Server Sequence	<input type="checkbox"/>	Name	Description	Host IP	Connec...	Single ...
	<input type="checkbox"/>	Ext-Tplus-Server1	ACS 5.8 node	10.1.100.122	49	Enable 20
	<input type="checkbox"/>	Ext-Tplus-Server2	ACS 5.8 node	10.1.100.123	49	Enable 20

**Figure 28-18 Network Resources**

Just like with external RADIUS servers and RADIUS server sequences, there are many reasons why you may need to forward TACACS+ requests to other servers. It could be a requirement for proof of concept or a phase in migrating away from another solution. The external TACACS servers that you add are then added to one or more TACACS Server Sequences, which are leveraged in a proxy sequence instead of a standard authentication within the policy set.

## Policy Elements

The Policy Elements screen of the Work Center is a shortcut to the conditions and results. Let's focus on the results. The two main results that are used with device administration are TACACS command sets and TACACS profiles.

### TACACS Command Sets

You will dive deeper into command sets in the following chapter when you actually configure device administration with TACACS+. The purpose is to limit which commands a user can or cannot use, and to assign those permissions to a session as one of the authorization results.

Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets**, as shown in [Figure 28-19](#).

Name	Description
DenyAllCommands	Default Command Set

**Figure 28-19** TACACS Command Sets

The command sets are groups of commands that should be permitted, commands that should be denied, or any combination thereof. The command set provides you with the ability to use simple or complex combinations of permit and deny statements.

Click **Add** to see the available choices with a command set, as shown in [Figure 28-20](#).

Grant	Command	Arguments
Deny Always	configure	*

**Figure 28-20** A Look at a Command Set

[Figure 28-20](#) keeps things very simple to illustrate a point about command sets. This particular command set has the check box for Permit Any Command That Is Not Listed Below checked, with **configure** the only command listed below, set to Deny Always.

The choices per command are Permit, Deny, or Deny Always. The difference between Deny and Deny Always has to do with stacking command sets—in other words, combining multiple command sets together in an authorization result. A Permit always trumps a Deny, but a Deny Always wins every time.

You will work more with command sets in the following chapters as you configure device administration with TACACS+.

## TACACS Profiles

TACACS profiles are most aptly compared to authorization profiles with network access (RADIUS). They are the basic form of authorization result for device administration, similar to allowing access or denying access—a result that is more bulk and uniform than the granular command sets that you looked at previously.

TACACS profiles are located under **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**, as shown in [Figure 28-21](#). There are some predefined profiles out of the box, and there are different profile types: Shell (IOS), WLC, Nexus, and Generic. Those types are provided to help make it even easier to work with well-known devices.

Name	Type	Description
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR
Deny All Shell Profile	Shell	Deny All Shell Profile
Default Shell Profile	Shell	Default Shell Profile

**Figure 28-21** Default TACACS Profiles

[Figure 28-22](#) shows an example TACACS profile for the type of Shell, in other words for an IOS device. [Figure 28-23](#) shows the exact same profile, but it shows the Raw View tab, which is live. You can make changes in either the Task Attribute View tab or the Raw View tab. The Task Attribute View tab is just a friendly view of the raw data.

TACACS Profiles > IOS NetAmin

### TACACS Profile

Name

Description Network Administrator Profile, Priv 15, Short Timeout

Task Attribute View

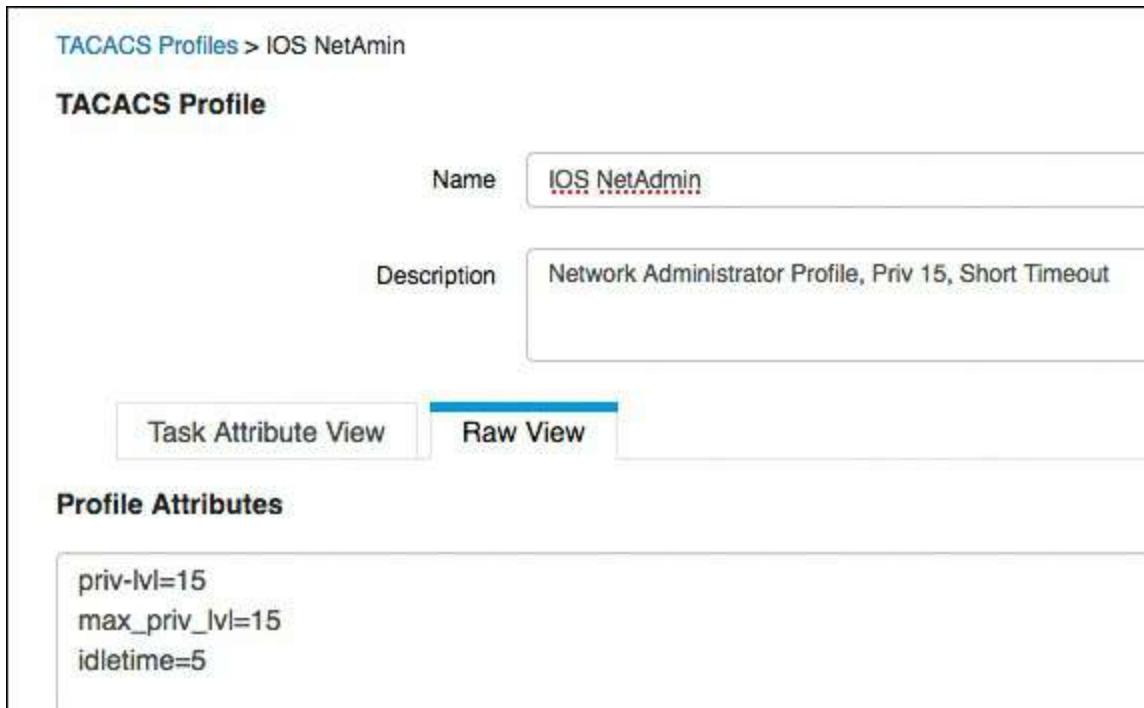
Raw View

### Common Tasks

Common Task Type

<input checked="" type="checkbox"/> Default Privilege	<input type="text" value="15"/>	<input checked="" type="checkbox"/>	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	<input type="text" value="15"/>	<input checked="" type="checkbox"/>	(Select 0 to 15)
<input type="checkbox"/> Access Control List		<input checked="" type="checkbox"/>	
<input type="checkbox"/> Auto Command		<input checked="" type="checkbox"/>	
<input type="checkbox"/> No Escape		<input checked="" type="checkbox"/>	(Select true or false)
<input type="checkbox"/> Timeout		<input checked="" type="checkbox"/>	Minutes (0-9999)
<input checked="" type="checkbox"/> Idle Time	<input type="text" value="5"/>	<input checked="" type="checkbox"/>	Minutes (0-9999)

Figure 28-22 TACACS Profile: Shell, Task Attribute View



**Figure 28-23** TACACS Profile: Shell, Raw View

You will see the different profile types in the subsequent chapters when you configure TACACS+ for Cisco Catalyst Switches (IOS), Cisco Wireless LAN Controller (WLC), and Cisco Nexus Switches (NX-OS).

## Device Admin Policy Sets

As my old guitar instructor, Jamie Hoover, used to say: we are now at the “crux of the biscuit.” In more familiar terms, it means we are at the heart of the matter, or the most important part.

As described in [Chapter 13](#), “[Authentication and Authorization Policies](#),” policy sets for network access policies should have been included in the first version of ISE. Instead, they weren’t added to ISE until version 1.2, and are not on by default (yet). That is different for Device Administration Policies, which have policy sets turned on by default, and that’s a great thing.

You can and should create policy sets that work with your organization’s need: perhaps based on location, job role, or even line of business.

For the purposes of this chapter and the device administration chapters that follow, we will walk through the configuration of three policy sets, one per device type that we will work with in the following chapters: Cisco Catalyst Switches (IOS), Cisco Wireless LAN Controller (WLC), and Cisco Nexus Switches (NX-OS).

To create the Catalyst policy set:

**Step 1.** Navigate to **Work Centers > Device Administration > Device Admin Policy**

## Sets.

**Step 2.** Click the **Default** policy set, as shown in [Figure 28-24](#).



**Figure 28-24** Default Device Admin Policy Set

**Step 3.** Click the plus symbol, and choose **Create Above**, as highlighted in [Figure 28-24](#).

**Step 4.** Name the policy set **Catalyst Switches** and provide a description.

**Step 5.** Choose the condition for the policy set: **DEVICE:Device Type STARTS WITH All Device Types#Switches#Access-Layer#Cisco**, as shown in [Figure 28-25](#).



**Figure 28-25** Catalyst Switches Policy Set

**Note** The policy sets in the figures are using the NDGs created in the earlier chapters.

**Step 6.** Click **Submit**

Next, create the WLC policy set:

**Step 1.** Navigate to **Work Centers > Device Administration > Device Admin Policy Sets**.

**Step 2.** Click the **Default** policy set, as shown in [Figure 28-24](#).

**Step 3.** Click the plus symbol, and choose **Create Above**, as highlighted in [Figure 28-](#)

24.

**Step 4.** Name the policy set **Wireless Controllers** and provide a description.

**Step 5.** Choose the condition for the policy set: **DEVICE:Device Type STARTS WITH Device Type#All Device Types#WiFi#Cisco**, as shown in [Figure 28-26](#) (the resulting summary of policies).

The screenshot shows the 'Device Admin Policy Sets' page. On the left, there's a sidebar titled 'Policy Sets' with a search bar and icons for creating, deleting, and saving. It lists several policy sets: 'Summary of Policies', 'Global Exceptions', 'Nexus Switches', 'Wireless Controllers' (which is selected), 'Catalyst Switches', and 'Default'. Below these are 'Save Order' and 'Reset Order' buttons. The main area is titled 'Device Admin Policy Sets' and shows a table of defined policy sets. The table has columns for Status, Name, Description, and Conditions. There are four rows:

Status	Name	Description	Conditions
✓	Nexus Switches	Policy Set for NX-OS	DEVICE:Device Type EQUALS Device Type#All Device Types#Switches#DC
✓	Wireless Controllers	Policy Set for Cisco WLCs	DEVICE:Device Type STARTS WITH Device Type#All Device Types#WiFi#Cisco
✓	Catalyst Switches	Policy Set for Cisco Catalyst Switches	DEVICE:Device Type STARTS WITH Device Type#All Device Types#Switches#Access-Layer#Cisco
✓	Default	Tacacs_Default	

**Figure 28-26** Summary of Policies

**Step 6.** Click Submit.

Next, create the Nexus policy set:

**Step 1.** Navigate to **Work Centers > Device Administration > Device Admin Policy Sets**.

**Step 2.** Click the **Default** policy set, as shown in [Figure 28-24](#).

**Step 3.** Click the plus symbol, and choose **Create Above**, as highlighted in [Figure 28-24](#).

**Step 4.** Name the policy set **Nexus Switches** and provide a description.

**Step 5.** Choose the condition for the policy set: **DEVICE:Device Type EQUALS Device Type#All Device Types#Switches#DC**, as shown in [Figure 28-26](#) (the resulting summary of policies).

**Step 6.** Click Submit.

The policy sets are now ready for Chapters 29 through 31, where you will configure device administration policies.

It is important to note that TACACS+ is not the only protocol that could be used for device administration. Some devices may use RADIUS, even though RADIUS is better suited for network access AAA. If you need a device administration AAA policy set for RADIUS, that set cannot exist within the Device Administration Work Center; you would need to create it in the Network Access Work Center, because ISE logically

separates them based on the AAA protocol.

## Reports

The reports related to device administration are packaged up quite neatly within the Device Administration Work Center, so that you don't have to leave the Work Center. Navigating to **Work Centers > Device Administration > Reports** will show you the four default reports: TACACS Accounting, TACACS Authentication, TACACS Authorization, and TACACS Command Accounting—as seen in [Figure 28-27](#).

The screenshot shows the Device Administration Work Center interface. The top navigation bar includes links for Overview, Identities, User Identity Groups, Ext Id Sources, Network Resources, Policy Elements, Device Admin Policy Sets, Reports (which is underlined in blue), and Settings. On the left, a sidebar menu has sections for My Reports, Reports (selected), and Device Administration Reports (which is expanded, showing TACACS Accounting, TACACS Authentication, TACACS Authorization, and TACACS Command Account...). The main content area is titled "TACACS Accounting" with a small info icon. It displays a timestamp from "From 2016-12-24 00:00:00.0 to 2016-12-31 17:47:23.694". Below this is a table header with columns: Logged Time, Status, Details, Username, and Action. A dropdown menu next to "Logged Time" is set to "Last 7 Days". To the right of the table are search fields for "Username" and "Action", and a "Rows/Page" dropdown set to 0. A message at the bottom states "No data found."

**Figure 28-27** Reports

## Summary

This chapter reviewed the purpose of device administration AAA and how it fits into the ISE administrative user experience. You learned about ISE cube design with separate cubes, or cubes that mix RADIUS and TACACS+ together.

You walked through the entire Device Administration Work Center, and created policy sets for use in the next three chapters where you will dive deeper into configuring device admin for IOS, WLC, and NX-OS.

# Chapter 29 Configuring Device Admin AAA with Cisco IOS

This chapter covers the following topics:

- Preparing ISE for incoming AAA requests
- Time to test

Much of what you are about to read and do in this chapter should feel rather familiar. There is quite a bit of overlap and similarity between configuring IOS for network access AAA and configuring IOS for device administration AAA. Because the features are so similar, you will certainly see overlap with [Chapter 11, “Bootstrapping Network Devices.”](#)

## Preparing ISE for Incoming AAA Requests

Before configuring the Cisco IOS device, you should ensure that the AAA server (ISE) is ready for the incoming authentication and authorization requests. If the network device is configured to authenticate users before granting them access to the IOS shell, and the AAA server is not responding with an authorization, you could create an accidental denial of service (DoS) incident.

You need to prepare the TACACS profiles and TACACS command sets that will be used as authorization results. You also need to ensure that the Network Device object in ISE is configured for TACACS and is in the correct Network Device Groups (NDG).

## Preparing the Policy Results

For the purposes of this chapter, we will design the policies to support the following groups of people who require command-line access to the organization’s Catalyst switches:

- **NetAdmin:** Network administrators who receive full control of the network device.
- **NetOps:** Network operators who receive full control of the network device but are not permitted to erase the configuration.
- **SecAdmin:** Security administrators who receive read-only access to view the configuration but not change anything.
- **Helpdesk:** Personnel who need to be able to see the status of certain **show** commands, to aid in their assistance of employees and guests.

In this section, you will create a TACACS profile and a command set for each of the four role types. It is best to preface each result object with its type: IOS for the Catalyst switches, WLC for the wireless controllers, and NXOS for the Nexus switches. This

will help you greatly when creating policies and will ensure that you don't get confused when building the policies later.

## Create the Authorization Results for Network Administrators

First create the TACACS profile:

**Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**.

**Step 2.** Click **Add**.

**Step 3.** Name the profile **IOS NetAdmin**, as shown in [Figure 29-1](#).

The screenshot shows the 'TACACS Profile' configuration page. At the top, the path 'TACACS Profiles > IOS NetAdmin' is displayed. Below it, the title 'TACACS Profile' is followed by a form with two fields: 'Name' containing 'IOS NetAdmin' and 'Description' containing 'Network Administrator Profile, Priv 15, Short Timeout'. Below the form are two tabs: 'Task Attribute View' (selected) and 'Raw View'. Under 'Common Tasks', a dropdown menu shows 'Common Task Type' set to 'Shell'. A table lists seven configuration items with checkboxes and input fields:

<input checked="" type="checkbox"/> Default Privilege	15	<input checked="" type="radio"/>	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	15	<input checked="" type="radio"/>	(Select 0 to 15)
<input type="checkbox"/> Access Control List		<input checked="" type="radio"/>	
<input type="checkbox"/> Auto Command		<input checked="" type="radio"/>	
<input type="checkbox"/> No Escape		<input checked="" type="radio"/>	(Select true or false)
<input type="checkbox"/> Timeout		<input checked="" type="radio"/>	Minutes (0-9999)
<input checked="" type="checkbox"/> Idle Time	5	<input checked="" type="radio"/>	Minutes (0-9999)

**Figure 29-1** IOS NetAdmin TACACS Profile

**Step 4.** Leave the Common Task Type field at its default value, **Shell**.

## **Step 5.** Check the **Default Privilege** check box and set the value to **15**.

Cisco IOS offers 16 different levels of access to the shell, level 0 through 15, with 15 being the highest level of access, known as privileged EXEC mode.

Because the network administrator must receive full control of the device, set the privilege level to 15.

**Note** When using the Task Attribute View tab to set the timeout values and the privilege levels, you can select the predefined options from the drop-down, or you can use an attribute or value that was stored in Active Directory.

## **Step 6.** Check the **Maximum Privilege** check box and set the value to **15**.

The default privilege is the assigned privilege level provided to the logged-in user. Although it is the assigned privilege, it is not the maximum privilege that a user could use within IOS. By typing the **enable** command, the user could use a second authorization to gain escalated privilege. The Maximum Privilege setting provides that limit.

## **Step 7.** Check the **Idle Time** check box and set the value to **5** minutes.

Because this user has elevated privilege, you may want to provide a relatively short timeout to the EXEC session, kind of like an automatic lock on your laptop screen or mobile device.

## **Step 8.** Click **Submit**.

[Figure 29-1](#) shows the final configuration of the TACACS profile.

After the TACACS profile is complete, create the TACACS command set for network administrators:

## **Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets**.

### **Step 2.** Click **Add**.

### **Step 3.** Name the profile **IOS NetAdmin Command Set**.

### **Step 4.** Provide a description.

### **Step 5.** Check the box for **Permit Any Command That Is Not Listed Below**.

### **Step 6.** Click **Submit**.

You have just created a command set that permits all commands, no exceptions. [Figure 29-2](#) shows the final configuration of the TACACS command set.

TACACS Command Sets > IOS NetAdmin

**Command Set**

Name	IOS NetAdmin Command Set
Description	Permit all commands.

**Commands**

Permit any command that is not listed below

Grant	Command	Arguments
No data found.		

**Actions:** + Add, Trash, Edit, Move Up, Move Down, Settings

**Buttons:** Cancel, Save

**Figure 29-2** IOS NetAdmin TACACS Command Set

## Create the Authorization Results for Network Operators

First create the TACACS profile:

**Step 1.** Navigate to Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles.

**Step 2.** Click Add.

**Step 3.** Name the profile **IOS NetOps**.

**Step 4.** Leave the Common Task Type field at its default value, **Shell**.

**Step 5.** Check the **Default Privilege** check box and set the value to **7**.

**Step 6.** Check the **Maximum Privilege** check box and set the value to **15**.

**Step 7.** Click Submit.

[Figure 29-3](#) shows the final configuration of the TACACS profile.

TACACS Profiles > IOS NetOps

**TACACS Profile**

Name	IOS NetOps
Description	For Network Operators. Limited Access.

Task Attribute View    Raw View

**Common Tasks**

Common Task Type: Shell

<input checked="" type="checkbox"/> Default Privilege	7	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	15	(Select 0 to 15)
<input type="checkbox"/> Access Control List		
<input type="checkbox"/> Auto Command		
<input type="checkbox"/> No Escape		(Select true or false)
<input type="checkbox"/> Timeout		Minutes (0-9999)
<input type="checkbox"/> Idle Time		Minutes (0-9999)

**Figure 29-3 IOS NetOps TACACS Profile**

Create the TACACS command set for network operators:

**Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets.**

**Step 2.** Click **Add**.

**Step 3.** Name the profile **IOS NetOps Command Set**.

**Step 4.** Provide a description.

**Step 5.** Check the box for **Permit Any Command That Is Not Listed Below**.

**Step 6.** In the Commands section, click **Add**.

**Step 7.** Set to **DENY\_ALWAYS** the **reload** and **shutdown** commands, as shown in [\*\*Figure 29-4\*\*](#).

TACACS Command Sets > IOS NetOps Command Set

**Command Set**

Name	IOS NetOps Command Set
Description	Network Operators Command Set

**Commands**

Permit any command that is not listed below

<input type="checkbox"/> Grant	Command	Arguments	<input type="checkbox"/> <input type="button" value="Delete"/> +
<input type="checkbox"/> DENY_ALWAYS	shutdown	*	<input type="checkbox"/> <input type="button" value="Delete"/> +
<input type="checkbox"/> DENY_ALWAYS	reload	*	<input type="checkbox"/> <input type="button" value="Delete"/> +

**Cancel** **Save**

**Figure 29-4** IOS NetOps TACACS Command Set

### Step 8. Click Submit.

You have just created a command set that permits all commands, except **reload** and **shutdown**.

### Create the Authorization Results for Security Administrators

First create the TACACS profile:

**Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**.

**Step 2.** Click **Add**.

**Step 3.** Name the profile **IOS SecAdmin**.

**Step 4.** Leave the Common Task Type drop-down at its default value, **Shell**.

**Step 5.** Check the **Default Privilege** check box and set the value to **15**.

**Step 6.** Check the **Maximum Privilege** check box and set the value to **15**.

**Step 7.** Check the **Timeout** check box and set the value to **5** minutes.

**Step 8.** Check the **Idle Time** check box and set the value to **5** minutes.

## Step 9. Click Submit.

Figure 29-5 shows the final configuration of the TACACS profile.

TACACS Profiles > New

**TACACS Profile**

Name: **IOS SecAdmin**

Description: Security Administrators Profile, Priv 15 - limited by the Command Set

Task Attribute View Raw View

**Common Tasks**

Common Task Type: Shell

<input checked="" type="checkbox"/> Default Privilege	15	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	15	(Select 0 to 15)
<input type="checkbox"/> Access Control List		
<input type="checkbox"/> Auto Command		
<input type="checkbox"/> No Escape		(Select true or false)
<input checked="" type="checkbox"/> Timeout	5	Minutes (0-9999)
<input checked="" type="checkbox"/> Idle Time	5	Minutes (0-9999)

Figure 29-5 IOS SecAdmin TACACS Profile

Create the TACACS command set for security administrators:

**Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets**.

**Step 2.** Click **Add**.

**Step 3.** Name the profile **IOS SecAdmin Command Set**.

**Step 4.** Provide a description.

**Step 5.** Check the box for **Permit Any Command That Is Not Listed Below**.

**Step 6.** In the Commands section, click **Add**.

**Step 7.** Set to **DENY\_ALWAYS** the **configure** command, as shown in [Figure 29-6](#).

The screenshot shows the 'TACACS Command Sets > IOS SecAdmin Command Set' configuration page. The 'Command Set' section includes fields for 'Name' (set to 'IOS SecAdmin Command Set') and 'Description' (set to 'Permits everything except configuring'). Under the 'Commands' section, there is a table with two rows. The first row has a checkbox labeled 'Grant' and a column for 'Command' (empty) and 'Arguments' (empty). The second row has a checkbox labeled 'DENY\_ALWAYS' and a column for 'Command' (set to 'configure') and 'Arguments' (set to '\*'). The table includes standard UI controls like 'Add', 'Edit', 'Move Up', 'Move Down', and 'Delete'. At the bottom are 'Cancel' and 'Save' buttons.

**Figure 29-6** IOS SecAdmin TACACS Command Set

**Step 8.** Click **Submit**.

You have just created a command set that permits all commands, except **configure**.

### Create the Authorization Results for the Helpdesk

First, create the TACACS profile:

**Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**.

**Step 2.** Click **Add**.

**Step 3.** Name the profile **IOS Helpdesk**.

**Step 4.** Leave the Common Task Type field at its default value, **Shell**.

**Step 5.** Check the **Default Privilege** check box and set the value to **2**.

**Step 6.** Check the **Maximum Privilege** check box and set the value to **2**.

**Step 7.** Click **Submit**.

[Figure 29-7](#) shows the final configuration of the TACACS profile.

TACACS Profiles > New

**TACACS Profile**

Name	IOS Helpdesk
Description	Permit them to login, but that's about it.

Task Attribute View    Raw View

**Common Tasks**

Common Task Type: Shell

<input checked="" type="checkbox"/> Default Privilege	2	(Select 0 to 15)
<input checked="" type="checkbox"/> Maximum Privilege	2	(Select 0 to 15)
<input type="checkbox"/> Access Control List		
<input type="checkbox"/> Auto Command		
<input type="checkbox"/> No Escape		(Select true or false)
<input type="checkbox"/> Timeout		Minutes (0-9999)
<input type="checkbox"/> Idle Time		Minutes (0-9999)

**Figure 29-7** IOS Helpdesk TACACS Profile

Create the TACACS command set for the helpdesk users:

**Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets.**

**Step 2.** Click **Add**.

**Step 3.** Name the profile **IOS Helpdesk Command Set**.

**Step 4.** Provide a description.

**Step 5.** In the Commands section, click **Add**.

**Step 6.** Set to **PERMIT** the **show**, **exit**, and **quit** commands, as shown in [Figure 29-8](#).

TACACS Command Sets > IOS Helpdesk Command Set

**Command Set**

Name	IOS Helpdesk Command Set
Description	Command Set that only allows them to access to show commands

**Commands**

Permit any command that is not listed below

**Add** **Trash** **Edit** **Move Up** **Move Down**

Grant	Command	Arguments
<input type="checkbox"/> PERMIT	quit	*
<input type="checkbox"/> PERMIT	exit	*
<input type="checkbox"/> PERMIT	show	*

**Figure 29-8** IOS Helpdesk TACACS Command Set

### Step 7. Click Submit.

You have just created a command set that only allows **show** commands, and the ability to type **exit** and **quit**.

## Preparing the Policy Set

Now it's time to use the policy sets that you prepared in [Chapter 28](#). Navigate to **Work Centers > Device Administration > Device Admin Policy Sets**. Here you'll see the three policy sets you created along with the Default set. Choose the **Catalyst Switches** policy set.

[Figure 29-9](#) shows the policy set that you created for IOS-based Catalyst switches. There is a default authentication rule with a result of **All\_User\_ID\_Stores**, just like in the network access policies. This identity sequence attempts to authenticate incoming TACACS+ requests against all the internal and external identity stores in order.

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Status	Name	Description	Conditions	Edit
<input checked="" type="checkbox"/>	Catalyst Switches	Policy Set for Cisco Catalyst Switches	DEVICE:Device Type STARTS WITH Device Type#All Device Types#Switches#Access-Layer#Cisco	<a href="#">Edit</a>

Regular  Proxy Sequence

▼ **Authentication Policy**

<input checked="" type="checkbox"/>	Default Rule (If no match)	:	Allow Protocols : Default Device Admin	and use : All_User_ID_Stores	<a href="#">Edit</a>   ▾
-------------------------------------	----------------------------	---	--	------------------------------	--------------------------

▼ **Authorization Policy**

► **Exceptions (0)**

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles	Edit
<input checked="" type="checkbox"/>	Tacacs_Default	If no matches, then <a href="#">Select Profile(s)</a> Deny All Shell Profile			<a href="#">Edit</a>   ▾

**Figure 29-9 Catalyst Switches Policy Set**

There is also a default authorization rule at the end of the policy set, named Tacacs\_Default. This rule is a last resort in a top-down, first-match policy set. It has a special authorization result, the Deny All Shell Profile, which will send a TACACS+ fail result even though the authentication passed. In other words, if you are not authorized, you will be denied access.

I know this probably seems silly to point out, because that is how authorization is supposed to work. However, in ISE 2.0 there was no way to do this, and the Deny All Shell Profile was added into ISE in version 2.1.

It's your job to ensure that valid traffic never meets this default rule and suffers the ultimate fate of service denial. So, let's begin creating the authorization rules, shall we?

Add the authorization rule for network administrators:

**Step 1.** Insert a rule above the Tacacs\_Default rule.

**Step 2.** Name the rule **NetAdmin IOS**.

**Step 3.** Set the condition to be an external group from AD, like you see in [Figure 29-10](#).

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.  
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description	Conditions
<input checked="" type="checkbox"/>	Catalyst Switches	Policy Set for Cisco Catalyst Switches	DEVICE:Device Type STARTS WITH Device Type#All Device Types#Switches#Access-Layer#Cisco

Regular  Proxy Sequence

▼ Authentication Policy

<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Device Admin	and use : All_User_ID_Stores
-------------------------------------	----------------------------	--	------------------------------

▼ Authorization Policy

► Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	NetAdmin IOS	If AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/NetAdmins	then IOS NetAdmin Command Set	AND IOS NetAdmin
<input checked="" type="checkbox"/>	Tacacs_Default	If no matches, then Select Profile(s)	Deny All Shell Profile	

**Figure 29-10** NetAdmin IOS Authorization Rule

**Step 4.** For the command set, select **IOS NetAmin Command Set**.

**Step 5.** For the shell profile, select **NetAdmin IOS**.

**Step 6.** Click Done.

**Step 7.** Click Save.

[Figure 29-10](#) shows the completed NetAdmin IOS authorization rule.

Add the authorization rule for network operators:

**Step 1.** Insert a rule above the Tacacs \_Default rule.

**Step 2.** Name the rule **NetOps IOS**.

**Step 3.** Set the condition to be an external group from AD, like you see in [Figure 29-11](#).

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.  
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Status	Name	Description	Conditions
<input checked="" type="checkbox"/>	Catalyst Switches	Policy Set for Cisco Catalyst Switches	DEVICE:Device Type STARTS WITH Device Type#All Device Types#Switches#Access-Layer#Cisco

Regular  Proxy Sequence

▼ Authentication Policy

<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Device Admin	and use : All_User_ID_Stores
-------------------------------------	----------------------------	--	------------------------------

▼ Authorization Policy

► Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	NetAdmin IOS	If AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/NetAdmins	then IOS NetAdmin Command Set	AND iOS NetAdmin
<input checked="" type="checkbox"/>	NetOps IOS	If AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/NetOps	then IOS NetOps Command Set	AND iOS NetOps
<input checked="" type="checkbox"/>	SecAdmin IOS	If AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/SecAdmin	then IOS SecAdmin Command Set	AND iOS SecAdmin
<input checked="" type="checkbox"/>	Helpdesk IOS	If AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/Helpdesk	then IOS Helpdesk Command Set	AND iOS Helpdesk
<input checked="" type="checkbox"/>	Tacacs_Default	If no matches, then Select Profile(s)	Deny All Shell Profile	

**Figure 29-11** Finished Catalyst Switches Policy Set

**Step 4.** For the command set, select **IOS NetOps Command Set**.

**Step 5.** For the shell profile, select **IOS NetOps**.

Add the authorization rule for security administrators:

**Step 1.** Insert a rule above the Tacacs\_Default rule.

**Step 2.** Name the rule **SecAdmin IOS**.

**Step 3.** Set the condition to be an external group from AD, like you see in [Figure 29-11](#).

**Step 4.** For the command set, select **IOS SecAdmin Command Set**.

**Step 5.** For the shell profile, select **IOS SecAdmin**.

Finally, add the authorization rule for helpdesk users:

**Step 1.** Insert a rule above the Tacacs\_Default rule.

**Step 2.** Name the rule **Helpdesk IOS**.

**Step 3.** Set the condition to be an external group from AD, like you see in [Figure 29-11](#).

**Step 4.** For the command set, select **IOS Helpdesk Command Set**.

**Step 5.** For the shell profile, select **IOS Helpdesk**.

[Figure 29-11](#) shows the completed Catalyst Switches policy set.

# Configuring the Network Access Device

Now that the policy set is ready, it's time to start configuring the network devices to authenticate the interactive logins and authorize the commands executed in their shell:

## 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. You likely have configured this already, back in [Chapter 11](#), but if not, here is the command:

```
3750-X(config) # aaa new-model
```

## Step 2. Define the TACACS+ servers.

Just as with RADIUS in [Chapter 11](#), you have to define the TACACS AAA servers:

```
3750-X(config) # tacacs server atw-ise237
3750-X(config-server-tacacs) # address ipv4 10.1.100.237
3750-X(config-server-tacacs) # key Cisco123
3750-X(config) # tacacs server atw-ise241
3750-X(config-server-tacacs) # address ipv4 10.1.100.241
3750-X(config-server-tacacs) # key Cisco123
```

## Step 3. Create a TACACS+ server group, named ISE-Group, and add the AAA servers to the group:

```
3750-X(config) # aaa group server tacacs+ ISE-Group
3750-X(config-sg-tacacs+) # server name atw-ise237
3750-X(config-sg-tacacs+) # server name atw-ise241
```

## Step 4. Just like you did for RADIUS traffic, configure all TACACS+ communication to be sourced from the loopback interface that matches what is configured in the ISE NAD object:

```
3750-X(config) # ip tacacs source-interface Loopback0
```

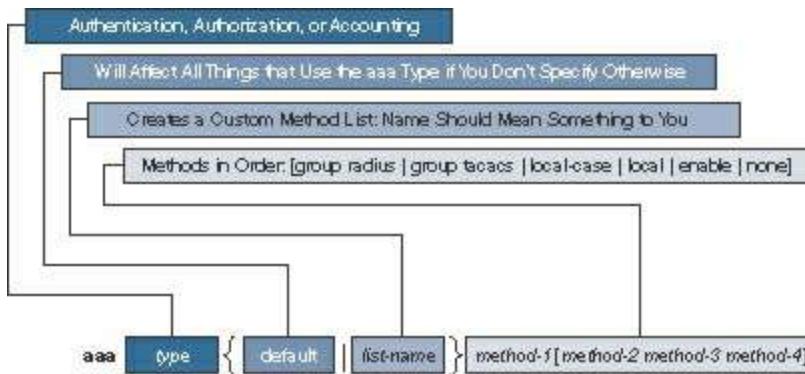
## Step 5. Create an AAA method that disables authentication, and apply it to the console during your configuration.

This action helps to ensure that you do not accidentally lock yourself out of the switch while you are creating the authentication and authorization methods. You will come back and apply the correct authentication to the console after you are certain the authentications and authorizations are built correctly. Here is the command:

```
3750-X(config) # aaa authentication login failsafe none
```

The word failsafe is the name of the method you just created. It could be called anything, but it's always a good practice to name the method something that helps describe what it does. The **none** keyword in the method configures it to not perform any authentication.

Method lists are used to define an order for IOS to leverage for AAA. At this point, you should be very familiar with these, but [Figure 29-12](#) illustrates the method lists and a breakdown of each portion.



**Figure 29-12** Method Lists Breakdown

**Step 6.** Apply the new failsafe authentication method to the console:

```
3750-X(config)# line con 0
3750-X(config-line)# login authentication failsafe
```

Assuming you are configuring the switch through the console port, you have now protected yourself during this configuration, ensuring that you cannot accidentally lock yourself out of the switch. It's a trick many of us used in the CCIE lab to ensure seamless configuration, and we have brought that practice forward into the field.

**Step 7.** Create an authentication method using the TACACS+ server group you created in Step 3.

Field deployment experience dictates that we should always create a local user or two for an additional failsafe in case the TACACS+ servers are unavailable.

```
3750-X(config)# aaa authentication login ISE-TAC+ group ISE-Group local
```

**Note** If you do not have a local user created with the **username** global-configuration command, then the fallback option of using local users will certainly not help you.

**Step 8.** Create authorization methods using the same TACACS+ server group.

Hopefully at this point, you understand that authentication alone does nothing.

You must configure authorizations to provide or restrict access. There are different locations within the shell to enforce authorization. Here you create methods for the shell itself (exec), configuration mode, and commands at four different levels (0, 1, 7 and 15):

```
3750-X(config) # aaa authorization exec ISE-TAC+ group ISE-Group local
3750-X(config) # aaa authorization config-commands
3750-X(config) # aaa authorization commands 0 ISE-TAC+ group ISE-Group local
3750-X(config) # aaa authorization commands 1 ISE-TAC+ group ISE-Group local
3750-X(config) # aaa authorization commands 7 ISE-TAC+ group ISE-Group local
3750-X(config) # aaa authorization commands 15 ISE-TAC+ group ISE-Group local
```

**Note** Without the **aaa authorization config-commands** option, the IOS device will only authorize commands in the exec mode, and not in configuration mode. In other words, no configuration changes will be authorized.

#### Step 9. Create accounting methods using the same TACACS+ server group.

At this point the IOS device is ready to authenticate users and authorize their activity. Now it is important to set up accounting, so you have an audit trail of the activities:

```
3750-X(config) # aaa accounting exec default start-stop group ISE-Group
3750-X(config) # aaa accounting commands 0 default start-stop
               group ISE-Group
3750-X(config) # aaa accounting commands 1 default start-stop
               group ISE-Group
3750-X(config) # aaa accounting commands 7 default start-stop
               group ISE-Group
3750-X(config) # aaa accounting commands 15 default start-stop
               group ISE-Group
```

#### Step 10. Apply the methods to the lines for Telnet and SSH.

Now that all the methods are defined, it's time to apply the methods to the access type (Telnet, SSH, HTTP, etc.). Remember, your console is currently exempt from authentication, until you're certain everything is working.

```
3750-X(config) # line vty 0 4
3750-X(config-line) # login authentication ISE-TAC+
3750-X(config-line) # authorization exec ISE-TAC+
```

```

3750-X(config-line)# authorization commands 0 ISE-TAC+
3750-X(config-line)# authorization commands 1 ISE-TAC+
3750-X(config-line)# authorization commands 7 ISE-TAC+
3750-X(config-line)# authorization commands 15 ISE-TAC+

```

## Time to Test

You have configured policy sets, authorization results, network devices, and all the authentication and authorization methods in the switch, applying those methods to the virtual terminal lines for Telnet, SSH, and HTTP. Now we'll ensure that it all works.

From the command-line interface:

**Step 1.** Issue the **test aaa** command to ensure the NAD is communicating successfully with ISE:

```

3750-X# test aaa group tacacs+ employee1 xxxxxxxx legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User authentication request was rejected by server.

```

The authentication request was rejected by the server? Don't worry, we did this on purpose—to show you the default Deny All Shell Profile, and how it appears to fail authentication.

**Step 2.** Examine the TACACS Live Log at **Work Centers > Device Administration > Overview > TACACS Live Log**, as shown in [Figure 29-13](#).

Status	Details	Username	Type	Authentication Policy	Authorization Policy
Failed		employee1	Authentication	Catalyst Switches >> Default	>> Default

**Figure 29-13** Live Log: Failed Test Authentication

Notice in [Figure 29-13](#) that the authentication policy is **Catalyst Switches >> Default >> Default**. This shows us the policy set selection worked. But why did the authentication fail? I'm certain that I put in the correct username and password.

**Step 3.** To find out, click the icon under **Details**, as highlighted in [Figure 29-13](#), which opens another window with the details report. The details report contains a tremendous amount of detail. However, the Overview section in the upper-left portion of the report contains everything you need to understand why this attempt failed. [Figure 29-14](#) shows the Overview section of the report.

## Overview

Request Type	Authentication
Status	Fail
Session Key	atw-ise237/271890916/5283
Message Text	Failed-Attempt: Authentication failed
Username	employee1
Authentication Policy	Catalyst Switches >> Default >> Default
Selected Authorization Profile	Deny All Shell Profile

**Figure 29-14** Live Log: Failed Test Authentication Details Overview

In the Overview section, you see the message text of “**Failed-Attempt: Authentication failed**”, and that the Selected Authorization Profile is “**Deny All Shell Profile**”. Wait a second...if it failed authentication, then how did it land on a shell profile at all? Shell profiles are part of authorization, and a failed authentication would mean the request should have dropped before getting to the authorization portion of the policy set!

The answer is right there in the details report, but may not be obvious. Take a look at the right side of the report, where all the steps are listed. You will see an Authentication Passed step, shown in [Figure 29-15](#), which is showing you that the username and password were good. You did have a successful authentication.

```
24343 RPC Logon request succeeded - Employee1@securitydemo.net
24402 User authentication against Active Directory succeeded - All_AD_Join_Points
22037 Authentication Passed
15036 Evaluating Authorization Policy
24432 Looking up user in Active Directory
24325 Resolving identity
24313 Search for matching accounts at join point
24319 Single matching account found in forest
24323 Identity resolution detected single matching account
24355 LDAP fetch succeeded
24416 User's Groups retrieval from Active Directory succeeded
15048 Queried PIP - AD-SecurityDemo.ExternalGroups
13036 Selected Shell Profile is DenyAccess
13015 Returned TACACS+ Authentication Reply
```

**Figure 29-15** Live Log: Failed Test Authentication Details Steps

Because of the way that TACACS+ works, with the separation of authentication and authorization, ISE has to take a “peek” at the authorization policy before sending the authentication request. It has to look ahead and be sure the authorization is not going to be rejected before sending the authentication pass message back to the NAD.

Examining [Figure 29-15](#), you see the successful authentication followed by a selected shell profile of Deny Access, and a returned authentication message. ISE cannot send the authentication success to the NAD if the user will end up being denied access to the shell. This is exactly what was wrong in ISE 2.0, before the Deny All Shell Profile was created. Any successful authentication resulted in access, regardless of the authorization.

**Step 1.** Test again, but with an account that should receive access to the IOS exec:

```
3750-X# test aaa group tacacs+ netadmin1 xxxxxxxx legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

This time the result was successful. [Figure 29-16](#) shows the TACACS Live Log showing the successful authentication attempt.

**Figure 29-16** Live Log: Successful Test

**Step 2.** SSH or Telnet into the switch to verify the authentication and authorization aspects.

We have just proven that the communication between the NAD and ISE is working correctly using TACACS+. Now it's time to try to log in remotely to the CLI of the device and test all aspects of the device administration configuration:

```
loxx@atw-ubuntu:~$ telnet 10.1.48.2
Trying 10.1.48.2...
Connected to 10.1.48.2.
Escape character is '^]'.
Username:netadmin1
Password:
3750-X# show privilege
Current privilege level is 15
3750-X# exit
Connection closed by foreign host.
```

We just used **telnet** to remotely log in as a user named **netadmin1** to the switch via one of its IP addresses. The login was successful, and the **show privilege** command shows us that we were assigned privilege level 15 (privileged EXEC).

**Step 3.** Examine the TACACS Live Log at **Work Centers > Device Administration > Overview > TACACS Live Log**, as shown in [Figure 29-17](#).

## Figure 29-17 Live Log: netadmin1 Successes

Notice the four highlighted lines in [Figure 29-17](#):

1. The successful authentication
2. Successful authorization to the shell, with IOS NetAdmin as the shell profile
3. Successful authorization of the **show privilege** command
4. Successful authorization of the **exit** command

**Step 4.** Log in as a user from the SecAdmin group:

```
loxx@atw-ubuntu:~$ telnet 10.1.48.2
Trying 10.1.48.2...
Connected to 10.1.48.2.
Escape character is '^]'.
Username:secadmin1
Password:
3750-X# show privilege
Current privilege level is 15
3750-X# show run
Building configuration...
<SNIP>
3750-X# conf t
Command authorization failed.
3750-X#
*
*
* Line timeout expired
*
*
3750-X#Connection closed by foreign host.
loxx@atw-ubuntu:~$
```

We just used **telnet** to remotely log in as a user named **secadmin1** to the switch via one of its IP addresses. The login was successful, and the **show privilege** command showed us that we were assigned privilege level 15 (privileged EXEC).

However, we were denied the ability to enter into configuration mode, which was expected. Also, remember from [Figure 29-5](#), we configured a timeout. You just saw that timeout occur.

**Step 5.** Examine the TACACS Live Log, as shown in [Figure 29-18](#).

The screenshot shows a table of log entries. The columns include Status, Details, Username, Type, Authentication Policy, Authorization Policy, Watched Elements, Shell Profile, and a timestamp. Five rows are highlighted with red numbers 1 through 5, indicating specific events:

- Row 1: Authentication success for secadmin1.
- Row 2: Authorization to shell (privilege level) via SecAdmin profile.
- Row 3: Authorization of the 'show privilege' command.
- Row 4: Authorization of the 'show run' command.
- Row 5: Failed authorization of the 'conf t' command.

**Figure 29-18** Live Log: secadmin1 Successes

Notice the five highlighted lines in [Figure 29-18](#):

1. The successful authentication
2. Successful authorization to the shell, with IOS SecAdmin as the shell profile
3. Successful authorization of the **show privilege** command
4. Successful authorization of the **show run** command
5. Failed authorization of the **conf t** command

**Step 6.** Navigate to **Work Centers > Device Administration > Reports > Device Administration Reports > TACACS Command Accounting**, as shown in [Figure 29-19](#).

The screenshot shows the TACACS Command Accounting report page. The left sidebar has sections for My Reports, Reports (Device Administration Reports), and Scheduled Reports. The main area displays a table of command history from December 27, 2016, to January 3, 2017. The table columns are Logged Time, Details, Username, Command, and Command Arguments. The data shows various commands like show, exit, configure, and write being typed by users secadmin1 and netadmin1.

Logged Time	Details	Username	Command	Command Arguments
2017-01-03 14:01:05.097	Last 7 Days	secadmin1	show	running-config
2017-01-03 14:01:00.278		secadmin1	show	privilege
2017-01-03 13:55:16.472		secadmin1	exit	
2017-01-03 13:55:13.624		secadmin1	configure	terminal
2017-01-03 13:55:08.611		secadmin1	exit	
2017-01-03 13:55:02.267		secadmin1	configure	terminal
2017-01-03 13:54:54.514		secadmin1	show	running-config
2017-01-03 13:54:52.061		secadmin1	show	privilege
2017-01-03 13:35:56.415		netadmin1	exit	
2017-01-03 13:35:09.423		netadmin1	show	privilege
2017-01-03 13:34:27.046		netadmin1	show	ip interface brief
2017-01-03 13:34:08.084		netadmin1	show	running-config
2017-01-03 13:28:02.092		netadmin1	test	aaa group tacacs+ netadmin1 Cisco123 !...
2017-01-03 11:52:43.111		netadmin1	test	aaa group tacacs+ employee1 Cisco123 !...
2017-01-03 11:44:20.839		netadmin1	write	

**Figure 29-19** TACACS Command Accounting Report

The TACACS Command Accounting report provides the detailed command-level audit trail of who typed what and when. It's incredibly useful when you need to

identify who it was that broke a configuration of sorts, and auditors will truly love the details of this report. However, think about all the interactive communication between all the devices on your network and ISE, and then all those logs going from the PSNs to the MnT node of your ISE cube. If your organization uses scripts or other automation tools to make configuration changes, there could be a tremendous amount of activity that ISE has to maintain records of. This brings us back to the design discussion earlier in [Chapter 28](#), and why some of us still prefer to maintain separate ISE cubes for device administration.

**Step 7.** Before you move on, don't forget to set the authentication on the console. Remember, we currently have it disabled to ensure we don't get locked out.

```
3750-X(config)# line con 0
3750-X(config-line)# login authentication ISE-TAC+
3750-X(config-line)# authorization exec ISE-TAC+
3750-X(config-line)# authorization commands 0 ISE-TAC+
3750-X(config-line)# authorization commands 1 ISE-TAC+
3750-X(config-line)# authorization commands 7 ISE-TAC+
3750-X(config-line)# authorization commands 15 ISE-TAC+
```

## Summary

Cisco IOS is a very powerful operating system that controls Cisco's routers and switches. While there are many approaches to providing device administration, such as moving certain commands to lower privilege levels, those approaches rely on local configurations of the switch.

By leveraging AAA servers, such as ISE, you can centralize all that power and control. TACACS profiles provide the shell access, while TACACS command sets limit which commands are available to the applicable users. All of this is configured centrally and therefore allows for a single configuration on ISE to be applicable to your global Cisco network.

This chapter focused on Cisco IOS devices, specifically Catalyst switches. In the next chapter, you will focus on Cisco Wireless LAN Controllers.

# Chapter 30 Configuring Device Admin AAA with Cisco WLC

This chapter covers the following topics:

- Overview of WLC device admin AAA
- Configuring ISE and the WLC for device admin AAA
- Testing and troubleshooting

In [Chapter 29, “Configuring Device Admin AAA with Cisco IOS,”](#) you focused on a network device that has very granular control all the way down to individual commands. Keep in mind that not all network devices have the capability to control access at a per-command level. Many provide a more broad-stroke access control, such as the assignment of roles.

The Cisco Wireless LAN Controller (WLC) provides a broad-level approach to role-based access control by controlling access at a menu level.

## Overview of WLC Device Admin AAA

The WLC provides role-based access control (RBAC) on a per-menu basis. However, the WLC does not prevent access to those sections of the GUI, but instead prevents changes from being saved when inside a menu section that is not authorized.

[Figure 30-1](#) shows the WLC user interface. The top-level menus are where the RBAC occurs.



**Figure 30-1** Cisco WLC Top-Level Menus

The WLC expects the authorization results from ISE to include a list of the menus that the user is authorized to make changes within. The WLC refers to those results as roles. The AAA server can send back a single role, or multiple roles that will be additive, as long as each role is designated with a unique role#. For example, to allow a user to make changes only within the WLANs, Wireless, and Security menus, the TACACS+ authorization result should include the following text: role1=WLANS

role2=SECURITY role3=WIRELESS. The good news is that the order does not matter. There are six different roles that exist that correspond directly to the menu system in the WLC user interface:

- **WLAN**: Permits write access to the WLAN menu structure.
- **CONTROLLER**: Permits write access to the CONTROLLER menu structure.
- **WIRELESS**: Permits write access to the WIRELESS menu structure.
- **SECURITY**: Permits write access to the SECURITY menu structure.
- **MANAGEMENT**: Permits write access to the MANAGEMENT menu structure.
- **COMMANDS**: Permits write access to the COMMANDS menu structure.

Additionally, there are three special roles that cannot be mixed with any other roles:

- **LOBBY**: Permits access to the Lobby Ambassador functions, which remain from when the WLC performed its own guest lifecycle management. Lobby Ambassador on the WLC has since been superseded by the Guest capabilities in ISE.
- **MONITOR**: Provides a read-only style of access to the WLC. All pages are visible to the user, but no changes are authorized.
- **ALL**: Just like it sounds, it permits access to all menus.

## Configuring ISE and the WLC for Device Admin AAA

The requisite steps for configuring device administration AAA are very similar regardless of what the actual network device is. You perform some configuration on ISE, to ensure that ISE is ready to receive the TACACS+ requests from the network access device (NAD), and then you configure the NAD to send those TACACS+ requests to ISE.

## Preparing ISE for WLC Device Admin AAA

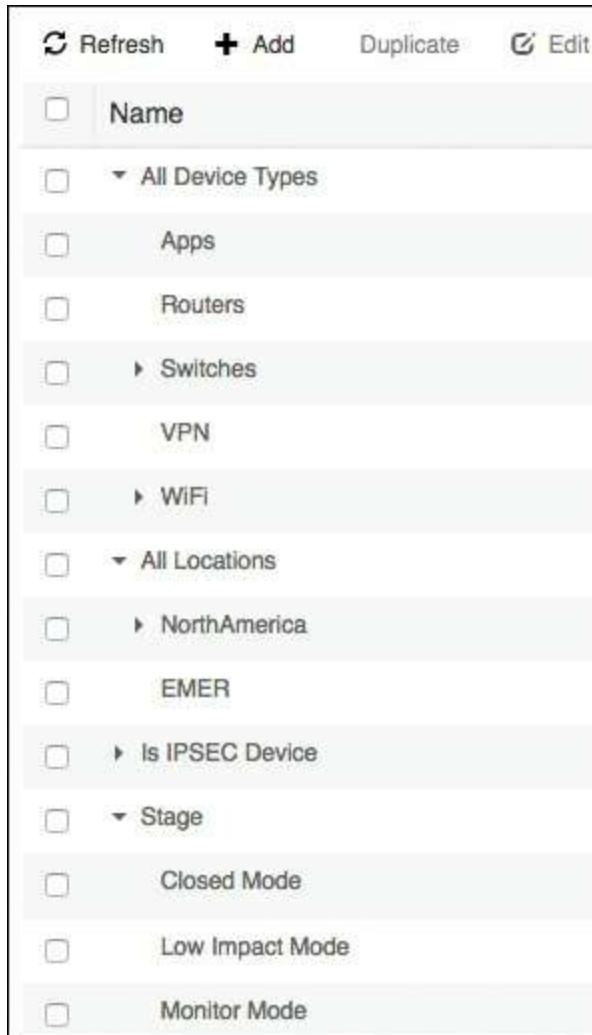
Within the ISE GUI, you need to ensure that the Network Device object is configured correctly and assigned to appropriate Network Device Groups (NDG). Then you create the authorization results and configure the Wireless LAN Controllers policy set that you created in [Chapter 28](#).

### Prepare the Network Device

In the ISE GUI, navigate to **Work Centers > Device Administration > Network Resources > Network Device Groups**.

You should already have a detailed set of hierarchical NDGs, similar to what you see in [Figure 30-2](#). Ensure that you have the appropriate groups to go along with the policies

you want to create.



**Figure 30-2** Example NDG Hierarchy

At the very least, ensure that these Cisco WLCs have their own group for a device type. With that group, you can ensure that a device administration policy set is built just for these devices and their unique way of doing device administration.

Next, you should ensure that your Cisco WLC itself has a Network Device object in ISE with the TACACS+ shared secret configured:

**Step 1.** Navigate to **Work Centers > Device Administration > Network Resources > Network Devices.**

**Step 2.** Click the WLC or click **Add** to create a new object.

**Step 3.** Ensure that the NDGs are assigned properly and the TACACS+ shared secret is configured correctly. [Figure 30-3](#) shows the NAD settings.

Network Devices List > **WLC02**

### Network Devices

* Name	<input type="text" value="WLC02"/>
Description	<input type="text"/>
* IP Address:	<input type="text" value="10.1.60.2"/> / <input type="text" value="32"/>
* IP Address:	<input type="text" value="10.1.42.2"/> / <input type="text" value="32"/>
* IP Address:	<input type="text" value="10.1.41.2"/> / <input type="text" value="32"/>
* Device Profile <input type="button" value="Cisco"/> <input type="button" value=""/>	
* Network Device Group	
Device Type	<input type="text" value="Cisco"/> <input type="button" value=""/>
IPSEC	<input type="text" value="Is IPSEC Device"/> <input type="button" value=""/>
Location	<input type="text" value="SJC"/> <input type="button" value=""/>
Stage	<input type="text" value="Closed Mode"/> <input type="button" value=""/>

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device  
 TACACS Draft Compliance Single Connect Support

**Figure 30-3** WLC Network Device Object

## Prepare the Policy Results

Device administration AAA is ready on ISE, but you have no policies and no authorizations to send down to the WLC yet. Now you’re going to add one TACACS profile for each role that you plan to use with the WLC.

Following suit with [Chapter 29](#), you will create three different roles for the WLC: NetAdmin, SecAdmin, and Helpdesk. Finally, you will create a LobbyAmbassador result to apply for any other employee who attempts to log in.

Navigate to **Work Centers > Device Administration > Policy Elements > Results >**

**TACACS Profiles.** Notice the predefined TACACS profiles, WLC ALL and WLC MONITOR, as shown in [Figure 30-4](#).

The screenshot shows a table titled "TACACS Profiles" with the following data:

Name	Type	Description
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR
Deny All Shell Profile	Shell	Deny All Shell Profile
Default Shell Profile	Shell	Default Shell Profile
IOS NetAdmin	Shell	Network Administrator Profile, Priv 15, Short Timeout
IOS NetOps	Shell	For Network Operators, Limited Access
IOS SecAdmin	Shell	Security Administrators Profile, Priv 15 - limited by the Command Set
IOS Helpdesk	Shell	Permit them to login, but that is about it.

**Figure 30-4** Predefined TACACS Profiles for the WLC

## Create the NetAdmin Profile

To create the NetAdmin profile, from the TACACS Profiles screen:

**Step 1.** Click Add.

**Step 2.** Name the profile **WLC NetAdmin**.

It is always best to prefix the profile name on the device that will use it, such as WLC [role type]. That makes it easy to know which result is for the WLC and which result is for IOS devices.

**Step 3.** From the Common Task Type drop-down list, choose **WLC**.

Notice the UI changes to one that aligns with the UI of the WLC menu structure. You have a choice to select from the three special roles (All, Monitor, Lobby) or to select the individual menus. Thank you Doug Gash for this very cool UI enhancement, making the experience of configuring the WLC TACACS profiles intuitive to anyone who is familiar with the WLC!

**Step 4.** Click the **All** radio button.

Notice in [Figure 30-5](#) the text “The configured options give a mgmtRole Debug value of: **0xffffffff8**.” This is calling out a mgmtRole field that will appear in debug logs on the WLC, to help you troubleshoot if and when the time arises. Again, this is another wonderful user experience that we can thank Doug Gash for thinking of.



**Figure 30-5** Completed NetAdmin TACACS Profile

**Step 5.** Click Submit.

[Figure 30-5](#) shows the completed WLC NetAdmin profile.

### Create the SecAdmin Profile

From the TACACS Profiles screen, create the profile for the SecAdmin users:

**Step 1.** Click Add.

**Step 2.** Name the profile **WLC SecAdmin**.

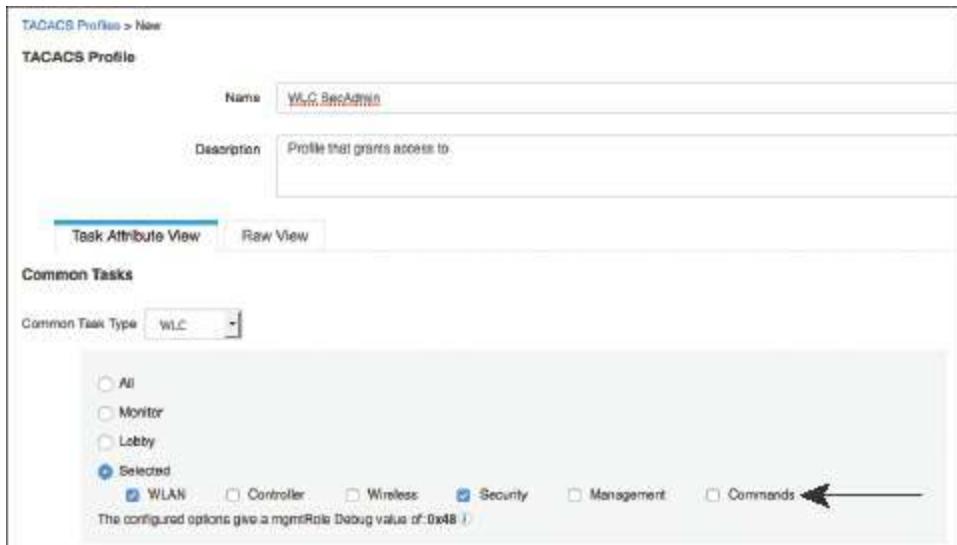
**Step 3.** From the Common Task Type drop-down list, choose **WLC**.

**Step 4.** Click the **Selected** radio button and check the **WLAN** check box.

**Step 5.** Check the **Security** check box.

**Step 6.** Click Submit.

[Figure 30-6](#) shows the completed WLC SecAdmin profile.



**Figure 30-6** Completed SecAdmin TACACS Profile

## Create the Helpdesk Profile

From the TACACS Profiles screen, create the profile for the helpdesk users:

**Step 1.** Click Add.

**Step 2.** Name the profile **WLC Helpdesk**.

**Step 3.** From the Common Task Type drop-down list, choose **WLC**.

**Step 4.** Click the **Monitor** radio button.

**Step 5.** Click Submit.

[Figure 30-7](#) shows the completed WLC Helpdesk profile.

The screenshot shows the 'TACACS Profiles > New' screen. The profile is named 'WLC Helpdesk' and has a description 'Permit access only to the monitor screen.' The 'Task Attribute View' tab is selected. In the 'Common Tasks' section, the 'Common Task Type' dropdown is set to 'WLC'. The 'All' radio button is selected, and under 'Selected', 'WLAN' is checked. A note at the bottom states: 'The configured options give a mgmtRole Debug value of: 0xffffffff8'.

**Figure 30-7** Completed Helpdesk TACACS Profile

## Create the Employee Profile

The last profile to create is for the rest of the employees. From the TACACS Profiles screen:

**Step 1.** Click Add.

**Step 2.** Name the profile **WLC Employees**.

**Step 3.** From the Common Task Type drop-down list, choose **WLC**.

**Step 4.** Click the **Lobby** radio button.

**Step 5.** Click Submit.

[Figure 30-8](#) shows the completed WLC Employees profile.

TACACS Profiles > WLC Helpdesk

**TACACS Profile**

Name: WLC Helpdesk

Description: Permit access only to the monitor screen.

Task Attribute View Raw View

**Common Tasks**

Common Task Type: WLC

All  
 Monitor  
 Lobby  
 Selected  
 WLAN  
 Controller  
 Wireless  
 Security  
 Management  
 Commands

The configured options give a mgmtRole Debug value of: 0x0

**Figure 30-8** Completed Employees TACACS Profile

## Configure the Policy Set

Now that you have all the role types that you need, it's time to configure the device administration policy set for the WLCs.

Add the authorization rule for network administrators:

**Step 1.** Navigate to **Work Centers > Device Administration > Device Admin Policy Sets**.

**Step 2.** Click the previously created **Wireless Controllers** policy set.

**Step 3.** Insert a new authorization rule above the **Tacacs\_Default** rule.

**Step 4.** Name the rule **NetAdmin WLC**.

**Step 5.** Set the condition to be an external group from AD, like you see in [Figure 30-9](#).

**Step 6.** There are no command sets for the WLC, so you can ignore that option.

**Step 7.** For the shell profile, select **WLC NetAdmin**.

**Step 8.** Click **Done**.

**Step 9.** Click **Save**.

[Figure 30-9](#) shows the completed NetAdmin WLC authorization rule.

Authorization Policy						
Exceptions (0)						
Standard						
Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles		
<input checked="" type="checkbox"/>	NetAdmin WLC	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/NetAdmins	then Select Profile(s)	WLC NetAdmin		
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then Select Profile(s)	Deny All Shell Profile			

**Figure 30-9** NetAdmin WLC Authorization Rule

Add the authorization rule for the security administrators:

**Step 1.** Insert a rule above the Tacacs\_Default rule.

**Step 2.** Name the rule **SecAdmin WLC**.

**Step 3.** Set the condition to be an external group from AD, like you see in [Figure 30-10](#).

**Step 4.** For the shell profile, select **WLC SecAdmin**.

Add the authorization rule for the helpdesk:

**Step 1.** Insert a rule above the Tacacs\_Default rule.

**Step 2.** Name the rule **Helpdesk WLC**.

**Step 3.** Set the condition to be an external group from AD, like you see in [Figure 30-10](#).

Authorization Policy						
Exceptions (0)						
Standard						
Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles		
<input checked="" type="checkbox"/>	NetAdmin WLC	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/NetAdmins	then Select Profile(s)	WLC NetAdmin		
<input checked="" type="checkbox"/>	SecAdmin WLC	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/SecAdmin	then Select Profile(s)	WLC SecAdmin		
<input checked="" type="checkbox"/>	Helpdesk WLC	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/Helpdesk	then Select Profile(s)	WLC Helpdesk		
<input checked="" type="checkbox"/>	Employee WLC	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/Employees	then Select Profile(s)	WLC Employees		
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then Select Profile(s)	Deny All Shell Profile			

**Figure 30-10** Complete Wireless Controllers Policy Set

**Step 4.** For the shell profile, select **WLC Helpdesk**.

Add the authorization rule for the rest of the employees to get LobbyAmbassador access:

**Step 1.** Insert a rule above the Tacacs\_Default rule.

**Step 2.** Name the rule **Employees WLC**.

**Step 3.** Set the condition to be an external group from AD, like you see in [Figure 30-10](#).

**Step 4.** For the shell profile, select **WLC Employees**.

**Step 5.** Click **Done**.

**Step 6.** Click **Save**.

[Figure 30-10](#) shows the completed Wireless Controllers policy set.

## Adding ISE to the WLC TACACS+ Servers

Now that the policy set is ready, it's time to start configuring the WLC to authenticate and authorize interactive users. ISE needs to be added to the WLC as a TACACS+ Authentication Server, an Authorization Server, and an Accounting Server.

Configure the TACACS+ servers from the WLC GUI as follows:

**Step 1.** Navigate to **Security > AAA > TACACS+ > Authentication**.

**Step 2.** Click **New**.

**Step 3.** Complete the Server IP Address and Shared Secret/Confirm Shared Secret text boxes, as shown in [Figure 30-11](#).

Setting	Value
Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	10.1.100.237
Shared Secret Format	ASCII
Shared Secret	.....
Confirm Shared Secret	.....
Port Number	49
Server Status	Enabled
Server Timeout	5 seconds

**Figure 30-11** Authentication Server Entry

**Step 4.** Click **Apply**.

**Step 5.** Navigate to **Security > AAA > TACACS+ > Accounting**.

**Step 6.** Click **New**.

**Step 7.** Complete the Server IP Address and Shared Secret/Confirm Shared Secret text boxes, as shown in [Figure 30-12](#).



The screenshot shows the Cisco Wireless LAN Controller (WLC) interface. The top navigation bar includes MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (which is highlighted in orange), and MANAGEMENT. On the left, a sidebar under the Security heading has expanded AAA, showing General, RADIUS, and TACACS+. Under TACACS+, Authentication, Accounting, Authorization, Fallback, DNS, LDAP, Local Net Users, MAC Filtering, Disabled Clients, and User Login Policies are listed. The main content area is titled "TACACS+ Accounting Servers > New". It contains the following fields:

Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	10.1.100.237
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Port Number	49
Server Status	Enabled
Server Timeout	5 seconds

**Figure 30-12** Accounting Server Entry

**Step 8.** Click **Apply**.

**Step 9.** Navigate to **Security > AAA > TACACS+ > Authorization**.

**Step 10.** Click **New**.

**Step 11.** Complete the Server IP Address and Shared Secret/Confirm Shared Secret text boxes, as shown in [Figure 30-13](#).



The screenshot shows the Cisco WLC interface, similar to Figure 30-12 but for Authorization. The top navigation bar and sidebar are identical. The main content area is titled "TACACS+ Authorization Servers > New". It contains the same set of fields as Figure 30-12:

Server Index (Priority)	1
Server IP Address(Ipv4/Ipv6)	10.1.100.237
Shared Secret Format	ASCII
Shared Secret	*****
Confirm Shared Secret	*****
Port Number	49
Server Status	Enabled
Server Timeout	5 seconds

**Figure 30-13** Authorization Server Entry

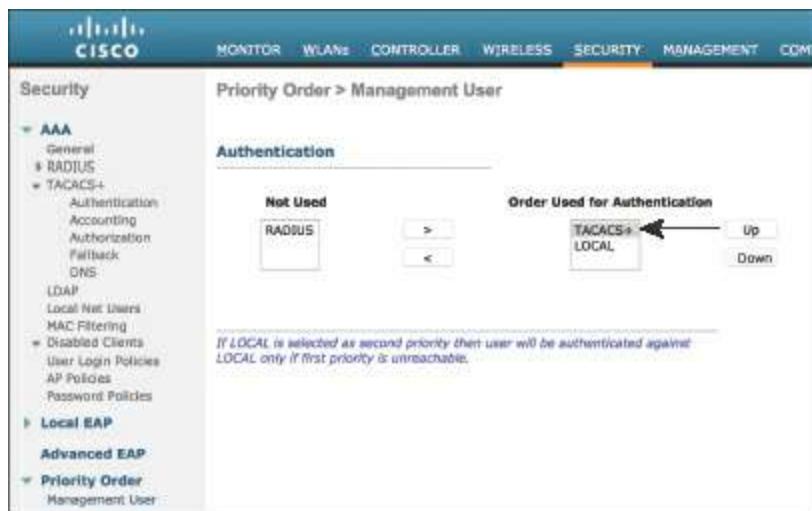
## Step 12. Click Apply.

Repeat this process for each of the ISE PSNs running TACACS+.

Now that you have added the ISE PSN(s) to the WLC for use with TACACS+, built the authorization policy, and defined the TACACS+ servers in the WLC, the next step is to configure the WLC to use TACACS+ for administrative access.

## Step 13. Navigate to Security > Priority Order > Management User.

**Step 14.** Ensure that TACACS+ is at the top of the Order Used for Authentication list, as shown in [Figure 30-14](#).



**Figure 30-14** Management Order

## Step 15. Click Apply.

By putting TACACS+ at the top of the list, and leaving LOCAL below it, you are providing yourself with a failsafe mechanism. The WLC will use the local accounts (such as the built-in admin account) in the case that the TACACS+ servers are not reachable.

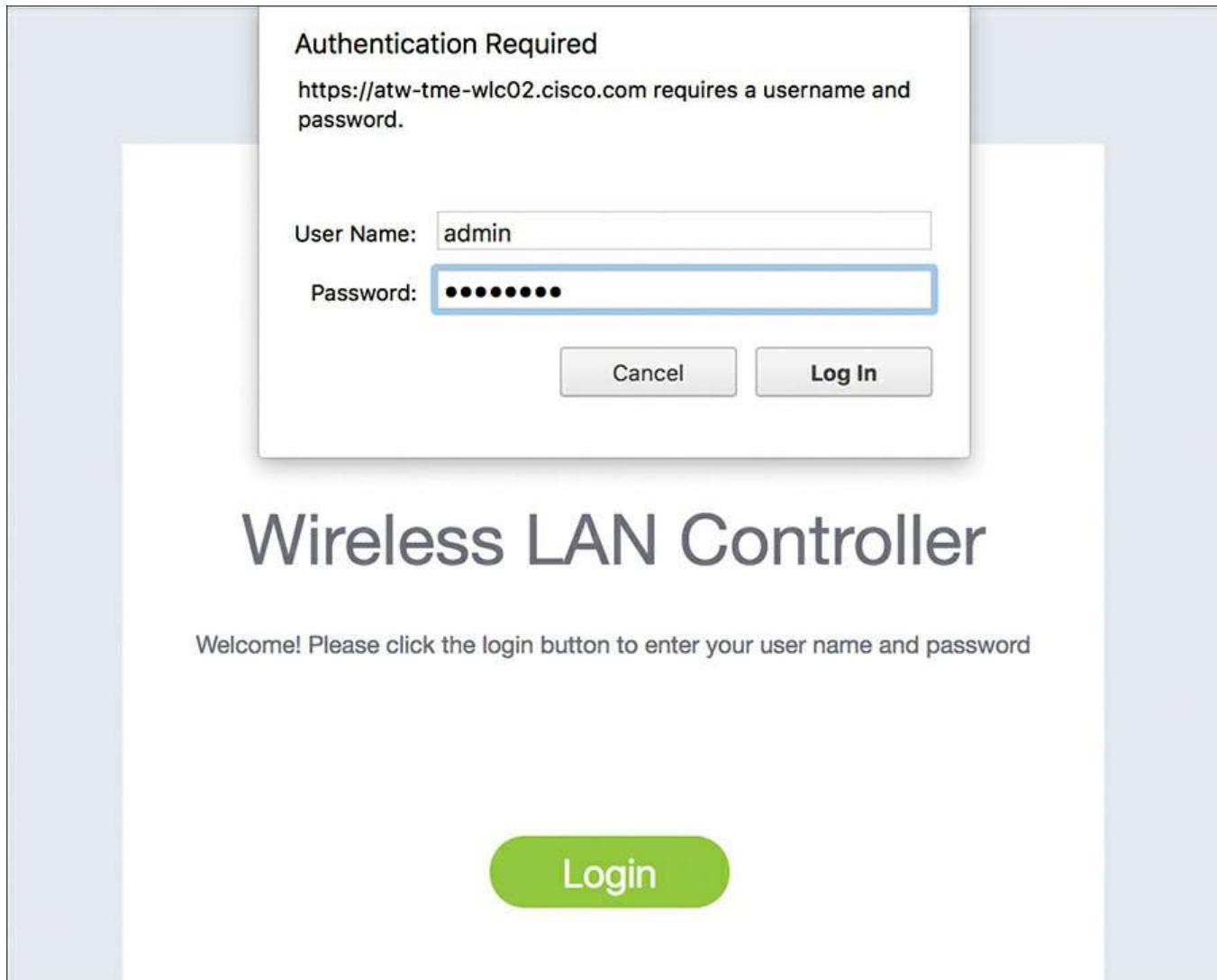
The WLC is now configured to use TACACS+ for its logins. Let's test it.

## Testing and Troubleshooting

It should be very easy to test the logins from the WLC—just try to log in from a browser.

### Step 1. Log in as **admin**.

[Figure 30-15](#) shows an attempted login using the same admin account that was used to configure the WLC up to this point.



**Figure 30-15** Logging In to the WLC

The authentication fails. So, where do you look first to identify why an authentication has failed? That's right, the TACACS Live Log.

**Step 2.** Navigate to **Work Centers > Device Administration > Overview > TACACS Live Log**.

[Figure 30-16](#) shows the failed admin login.

TACACS Live Log						
Status	Details	Username	Type	Authentication Policy	Authorization Policy	Shell Profile
x		Username		Authentication Policy	Authorization Policy	Shell Profile
✗	✗	admin	Authentication	Wireless Controllers >> Default >> D...		
✗	✗	admin	Authentication	Wireless Controllers >> Default >> D...		

Last Updated: Thu Jan 05 2017 00:08:36 GMT-0500 (EST)

### Figure 30-16 TACACS Live Log: Failed admin Login

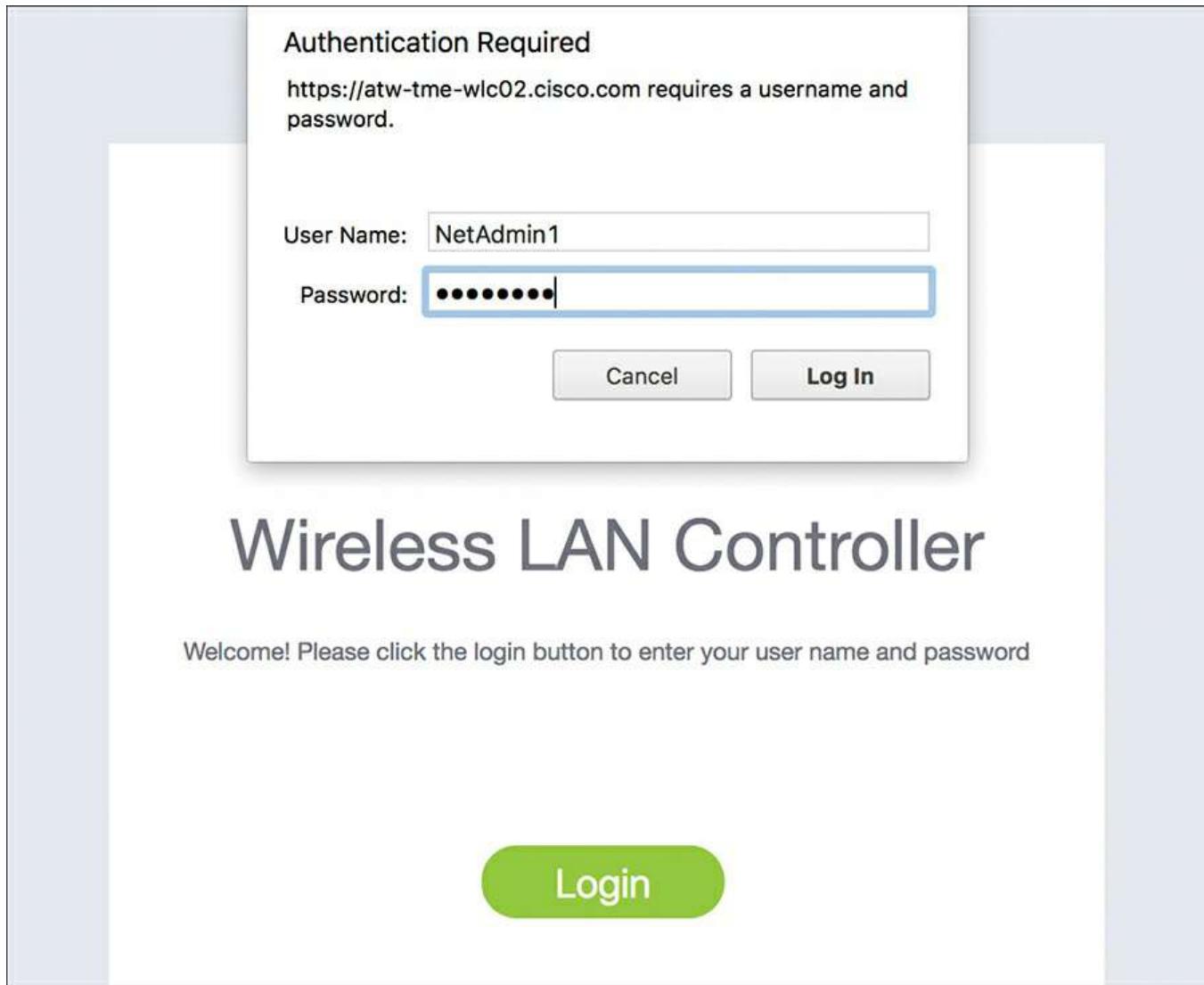
Click the icon under Details to view the authentication details report, which explains the failure reason as **22056 Subject not found in the applicable identity store(s)**, as shown in [Figure 30-17](#).

Authentication Details	
Generated Time	2017-01-04 21:06:35.432000 -08:00
Logged Time	2017-01-04 21:06:35.432
ISE Node	abw-ise237
Message Text	Failed-Attempt: Authentication failed
Failure Reason	22056! Subject not found in the applicable identity store(s) 

### Figure 30-17 Failure Reason

This makes sense. ISE is configured to check with the backend identity stores, such as its own internal user database and Active Directory. The admin account is a local account that only exists on the WLC. The WLC will not attempt to authenticate local accounts while the TACACS+ server responds.

**Step 3.** Log in again, but this time as the **NetAdmin1** user, as shown in [Figure 30-18](#).



**Figure 30-18** Logging In as NetAdmin1

This time the authentication succeeds.

**Step 4.** Examine the Live Log, as shown in [Figure 30-19](#).

Live Log						
Status		Details		Authentication Policy		Authorization Policy
		Username	Type	Authentication Policy	Authorization Policy	Shell Profile
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	NetAdmin1	Authorization	Wireless Controllers >> NetAdmin WLC	WLC NetAdmin	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	NetAdmin1	Authentication	Wireless Controllers >> Default >> D...		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	admin	Authentication	Wireless Controllers >> Default >> D...		
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	admin	Authentication	Wireless Controllers >> Default >> D...		

**Figure 30-19** Successful Login, NetAdmin WLC Result

As you can see in [Figure 30-19](#), the authentication succeeds, as does the

subsequent authorization where the NetAdmin WLC authorization result is applied. Test making a configuration change.

**Step 5.** Navigate to a WLC menu that the other roles do not have access to, such as **CONTROLLER**.

**Step 6.** Make a change to that configuration page, such as adding a DNS server, like what you see in [Figure 30-20](#).

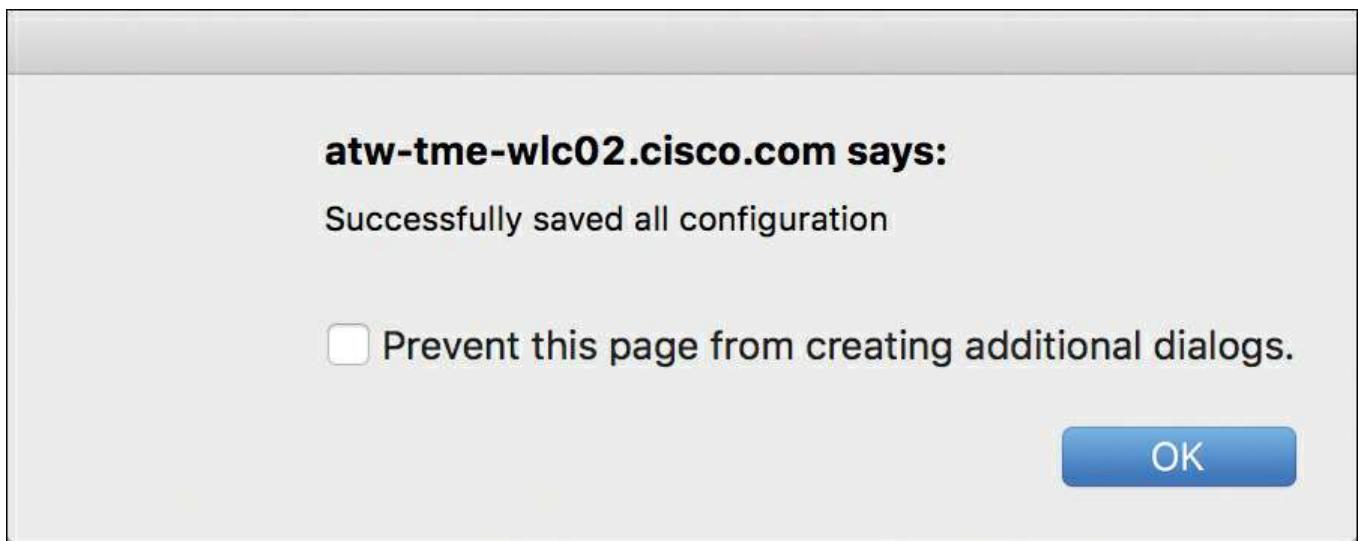


**Figure 30-20** Controller > General Settings

**Step 7.** Click **Apply**.

**Step 8.** Click **Save Configuration**.

As you can see in [Figure 30-21](#), the change is applied successfully, and the configuration is saved successfully.



**Figure 30-21** Successful Configuration Save

**Step 9.** SSH into the WLC.

**Step 10.** Log in as **admin**, and it will fail.

**Step 11.** Log in as **NetAdmin1**, and it will succeed.

Now you can see that the CLI is being controlled by the same RBAC as the GUI. [Figure 30-22](#) shows the login attempts from the CLI.

**Figure 30-22** CLI Login Attempts in Live Log

**Step 12.** In the WLC CLI, type **debug aaa tacacs enable**.

### **Step 13. Log out of the GUI.**

#### **Step 14. Log in to the GUI as SecAdmin1.**

The login as SecAdmin1 succeeds. [Figure 30-23](#) shows the success and the assigned SecAdmin WLC profile in Live Log. Additionally, in the CLI there is a tremendous amount of debug activity happening. One of the messages in the debug reads **User has the following mgmtRole 48**. That number matches the value shown in the ISE GUI for the SecAdmin WLC TACACS profile.

User Accounts						
Status	Details	Username	Type	Authentication Policy	Authorization Policy	Shell Profile
<span style="color: green;">OK</span>	<a href="#">Details</a>	SeoAdmin1	Administrator	<a href="#">Authentication Policy</a>	<a href="#">Authorization Policy</a>	<a href="#">Shell Profile</a>
<span style="color: green;">OK</span>	<a href="#">Details</a>	SeoAdmin2	Administrator	Wireless Controllers == SeoAdmin W...	Wireless Controllers == SeoAdmin W...	WLC SeAdmin
<span style="color: green;">OK</span>	<a href="#">Details</a>	NakAdmin1	Administrator	<a href="#">Authentication Policy</a>	<a href="#">Authorization Policy</a>	<a href="#">Shell Profile</a>
<span style="color: green;">OK</span>	<a href="#">Details</a>	NakAdmin2	Administrator	Wireless Controllers == Default == D...	Wireless Controllers == NakAdmin W...	WLC NakAdmin

**Figure 30-23** SecAdmin1 Login Shown in Live Log

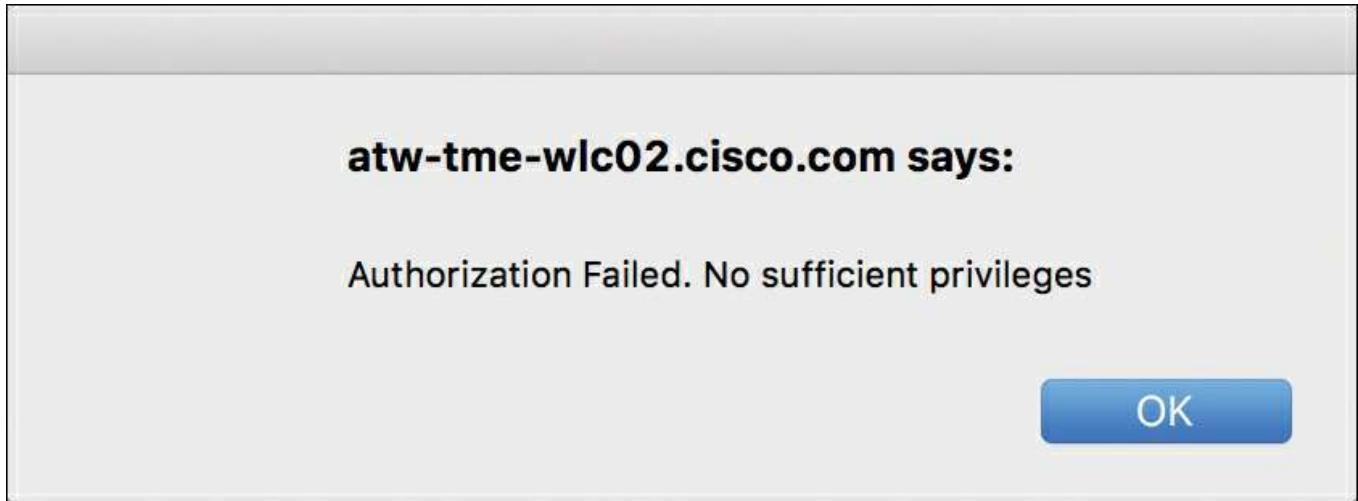
Test by making a configuration change.

**Step 15.** Navigate to a menu that the SecAdmin role should not have access to, such as **CONTROLLER**.

**Step 16.** Make a change to that configuration page, such as adding a DNS server. The change is accepted.

### **Step 17. Click Apply.**

As you can see in [Figure 30-24](#), the user's attempt to apply the change fails due to insufficient privileges.



**Figure 30-24** Authorization Failed

This is more proof of how RBAC works with the WLC. The menus are available to everyone, but only authorized changes will be applied.

**Step 18.** Navigate to a menu that the SecAdmin role does have access to, such as **SECURITY**.

**Step 19.** Make a change to that configuration page, such as adding a new ACL. The change is accepted.

**Step 20.** Click **Apply**.

**Step 21.** Click **Save Configuration**.

The change is applied successfully, and the configuration is saved successfully.

**Step 22.** Log out of the GUI.

**Step 23.** Log in to the GUI as **Helpdesk1**.

**Step 24.** The login as Helpdesk1 succeeds.

All of the UI pages are available, but no changes will be applied. The Helpdesk users are assigned the MONITOR role, which is basically equivalent to “read everything, write nothing.”

**Step 25.** Log out of the GUI.

**Step 26.** Log in to the GUI as **Employee1**.

**Step 27.** The login as Employee1 succeeds.

As you see in [Figure 30-25](#), it’s a different GUI. The LOBBY role that is assigned to any employee not matching one of the more specific groups in the configuration provides access to a guest management user interface only.

The screenshot shows the 'Guest Management' section of the 'Lobby Ambassador Guest Management' interface. At the top right are links for 'Logout | Refresh | Help'. Below the header, a 'Guest Users List' is displayed with a 'New...' button. A status bar at the bottom indicates 'Items 0 to 0 of 0'. A header row defines columns for 'User Name', 'WLAN SSID', 'Account Remaining Time', and 'Description'.

**Figure 30-25** Lobby Ambassador UI

## Summary

In this chapter you saw how a Cisco Wireless LAN Controller is designed to handle role-based access control (RBAC) with device administration AAA. Unlike Cisco IOS-based systems, which provide granular command-level controls, the WLC provides a more broad-stroke role-based approach.

The roles are tied to top-level menu items. While most users will see all menu items and configuration pages, they cannot apply changes in any page where they are not authorized by their role.

ISE has a very easy-to-use WLC-specific shell profile, which is even organized just like the actual WLC user interface to make things even easier.

The next chapter looks at another role-based device administration model with the Nexus NX-OS platforms.

# Chapter 31 Configuring Device Admin AAA with Cisco Nexus Switches

This chapter covers the following topics:

- Overview of NX-OS device admin AAA
- Configuring ISE and the Nexus switch for device admin AAA

In [Chapter 29, “Configuring Device Admin AAA with Cisco IOS,”](#) you focused on a network device that has very granular control all the way down to individual commands. In [Chapter 30, “Configuring Device Admin AAA with Cisco WLC,”](#) you saw how the WLC provides a broad-level approach to role-based access control by controlling access at a menu level.

The NX-OS provides a combination of the granular command-level approach and the easier-to-use role-based approach.

## Overview of NX-OS Device Admin AAA

The Cisco NX-OS software leverages user roles. Each role contains one or more rules, and each user can have more than one role. The roles are additive in nature, to allow this.

NX-OS provides two default user roles:

- **network-admin (superuser):** Full read/write access to entire switch
- **network-operator:** Complete read access to entire switch

Additionally, for the NX-OS platforms that support virtual device contexts (VDC), there are two more default user roles:

- **vdc-admin (superuser):** Full access to the management VDC that is used to create individual VDCs
- **vdc-operator:** Read-only access to the management VDC

NX-OS also provides built-in roles for each of the privilege levels, but assigns all the features and commands to Priv-1 and Priv-15, to behave similarly to IOS.

A role is made up of rules, which are the most basic element of the role. They state which operation the user role is allowed to perform. Each rule has parameters:

- **Command:** Command or group of commands defined with regular expressions (regex)
- **Feature:** Commands that apply to a function of the NX-OS switch (**show role feature command**)

- **Feature group:** Default or user-defined group of features (**show role feature-group** command)

For the purposes of this chapter, we will stick with the built-in network-admin and network-operator roles.

## Configuring ISE and the Nexus for Device Admin AAA

The requisite steps for configuring device administration AAA are very similar regardless of what the actual network device is. You perform some configuration on ISE, to ensure ISE is ready to receive the TACACS+ requests from the network access device (NAD), and then you configure the NAD to send those TACACS+ requests to ISE.

## Preparing ISE for Nexus Device Admin AAA

Before configuring the Nexus switch, you should ensure that the AAA server (ISE) is ready for the incoming TACACS+ requests. If the network device is configured to authenticate users before granting them access to the IOS shell, and the AAA server is not responding with an authorization, you could create an accidental denial of service (DoS) incident.

You need to prepare the TACACS profiles that will be used as authorization results. There are no command sets needed with NX-OS. You also need to ensure that the Network Device object in ISE is configured for TACACS and is in the correct Network Device Groups (NDG).

### Prepare the Network Device

Ensure the Nexus switch has a Network Device object in ISE with the TACACS+ shared secret configured. From the ISE GUI:

**Step 1.** Navigate to **Work Centers > Device Administration > Network Resources > Network Devices**.

**Step 2.** Click the Nexus or click **Add** to create a new object.

**Step 3.** Ensure that the NDGs are assigned properly and the TACACS+ shared secret is configured correctly. [Figure 31-1](#) shows the NAD settings.

Network Devices List > **NSK**

**Network Devices**

\* Name

\* IP Address:  /

\* Device Profile:

\* Network Device Group

Device Type

IPSEC

Location

Stage

▶ RADIUS Authentication Settings

▶ TACACS Authentication Settings

Shared Secret

Enable Single Connect Mode

Legacy Cisco Device  
 TACACS Draft Compliance Single Connect Support

▶ SNMP Settings

▶ Advanced TrustSec Settings

**Figure 31-1** Nexus Network Device Object

## Prepare the Policy Results

For the purposes of this chapter, we will design the policies to support the following groups of people who each require command-line access to the organization's Nexus switches:

- **NetAdmin:** Network administrators who receive full read-write access to the switch.
- **NetOps:** Network operators who receive read-only access to the switch.
- **SecAdmin:** Security administrators who receive read-only access to the switch.
- **Helpdesk:** Personnel who receive read-only access to the switch.

In this section, you will create a TACACS profile for each of the four role types. It is best to preface each result object with its type: IOS for the Catalyst switches, WLC for the wireless controllers, and NXOS for the Nexus switches. This will help you greatly when creating policies and will ensure that you don't get confused when building the policies later.

## Create the NetAdmin Profile

The steps to create the NetAdmin profile are as follows:

**Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**.

**Step 2.** Click **Add**.

**Step 3.** Name the profile **NXOS NetAdmin**.

**Step 4.** From the Common Task Type drop-down list, choose **Nexus**.

The UI immediately changes to allow you to configure the Network role and VDC role directly, as shown in [Figure 31-2](#).

TACACS Profiles > New

**TACACS Profile**

Name	NXOS NetAdmin
Description	Read Write for the Network and the VDC role.

Task Attribute View      Raw View

**Common Tasks**

Common Task Type Nexus

Set attributes as Optional i

**Network role**

None  
 Operator (Read Only)  
 Administrator (Read Write)

**VDC role**

None  
 Operator (Read Only)  
 Administrator (Read Write)

The screenshot shows the 'TACACS Profiles > New' screen. A 'TACACS Profile' is being created with the name 'NXOS NetAdmin'. The description is 'Read Write for the Network and the VDC role.' Below the profile details, there are two tabs: 'Task Attribute View' (selected) and 'Raw View'. Under 'Common Tasks', the 'Common Task Type' is set to 'Nexus'. The 'Set attributes as' dropdown is set to 'Optional' with an information icon ('i'). In the 'Network role' section, the 'Administrator (Read Write)' option is selected. In the 'VDC role' section, the 'Administrator (Read Write)' option is also selected. The background of the interface is light gray, and the main content area has a white background.

**Figure 31-2** NXOS NetAdmin TACACS Profile

**Step 5.** Set the Network role to **Administrator (Read Write)**.

**Step 6.** Set the VDC role to **Administrator (Read Write)**.

**Step 7.** Click **Submit**.

[Figure 31-2](#) shows the final configuration of the TACACS profile.

## Create the NetOps Profile

The steps to create the NetOps profile are as follows:

**Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**.

**Step 2.** Click **Add**.

**Step 3.** Name the profile **NXOS NetOps**.

**Step 4.** From the Common Task Type drop-down list, choose **Nexus**.

**Step 5.** Set the Network role to **Operator (Read Only)**.

**Step 6.** Set the VDC role to **Operator (Read Only)**.

**Step 7.** Click **Submit**.

[Figure 31-3](#) shows the final configuration of the TACACS profile.

TACACS Profiles > New

## TACACS Profile

Name

NXOS NetOps

Description

Task Attribute View

Raw View

## Common Tasks

Common Task Type

Nexus

Set attributes as

Optional



### Network role

None

Operator (Read Only)

Administrator (Read Write)

### VDC role

None

Operator (Read Only)

Administrator (Read Write)

Figure 31-3 NXOS NetOps TACACS Profile

## Create the SecAdmin Profile

The steps to create the SecAdmin profile are as follows:

**Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**.

**Step 2.** Click **Add**.

**Step 3.** Name the profile **NXOS SecAdmin**.

**Step 4.** From the Common Task Type drop-down list, choose **Nexus**.

**Step 5.** Set the Network role to **Operator (Read Only)**.

**Step 6.** Set the VDC role to **Operator (Read Only)**.

**Step 7.** Click **Submit**.

## Create the Helpdesk Profile

The steps to create the Helpdesk profile are as follows:

**Step 1.** Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**.

**Step 2.** Click **Add**.

**Step 3.** Name the profile **NXOS SecAdmin**.

**Step 4.** From the Common Task Type drop-down list, choose **Nexus**.

**Step 5.** Set the Network role to **Operator (Read Only)**.

**Step 6.** Set the VDC role to **Operator (Read Only)**.

**Step 7.** Click **Submit**.

## Configure the Policy Set

Now that you have all the role types that you need, it's time to configure the device administration policy set for the Nexus switches.

**Step 1.** Navigate to **Work Centers > Device Administration > Device Admin Policy Sets**.

**Step 2.** Click the previously created **Nexus Switches** policy set.

**Step 3.** Insert a new authorization rule above the **Tacacs\_Default** rule.

**Step 4.** Name the rule **NetAdmin NXOS**.

**Step 5.** Set the condition to be an external group from AD, like you see in [Figure 31-4](#).

**Step 6.** There are no command sets for the NXOS device, so you can ignore that option.

**Step 7.** For the shell profile, select **NXOS NetAdmin**.

**Step 8.** Click **Done**.

**Step 9.** Click **Save**.

[Figure 31-4](#) shows the completed NetAdmin NXOS authorization rule.

Authorization Policy					
Exceptions (0)					
Standard					
Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles	
<input checked="" type="checkbox"/>	NetAdmin NXOS	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/NetAdmins	then Select Profile(s)	NXOS NetAdmin	
<input checked="" type="checkbox"/>	Tacacs_Default	If no matches, then Select Profile(s)	Deny All Shell Profile		

**Figure 31-4** NetAdmin NXOS Authorization Rule

Add the authorization rule for the network operators:

**Step 1.** Insert a rule above the Tacacs\_Default rule.

**Step 2.** Name the rule **NetOps NXOS**.

**Step 3.** Set the condition to be an external group from AD, like you see in [Figure 31-5](#).

**Step 4.** For the shell profile, select **NXOS NetOps**.

Add the authorization rule for the security administrators:

**Step 1.** Insert a rule above the Tacacs\_Default rule.

**Step 2.** Name the rule **SecAdmin NXOS**.

**Step 3.** Set the condition to be an external group from AD, like you see in [Figure 31-5](#).

**Step 4.** For the shell profile, select **NXOS SecAdmin**.

Add the authorization rule for the helpdesk personnel:

**Step 1.** Insert a rule above the Tacacs\_Default rule.

**Step 2.** Name the rule **Helpdesk NXOS**.

**Step 3.** Set the condition to be an external group from AD, like you see in [Figure 31-5](#).

**Step 4.** For the shell profile, select **NXOS Helpdesk**.

**Step 5.** Click **Done**.

**Step 6.** Click **Save**.

[Figure 31-5](#) shows the completed Nexus Switches policy set.

Authorization Policy						
Exceptions (0)						
Standard						
	Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles	
■	<input checked="" type="checkbox"/>	NetAdmin NXOS	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/NetAdmins	then Select Profile(s)	NXOS NetAdmin	
■	<input checked="" type="checkbox"/>	NetOps NXOS	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/NetOps	then Select Profile(s)	NXOS NetOps	
■	<input checked="" type="checkbox"/>	SecAdmin NXOS	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/SecAdmin	then Select Profile(s)	NXOS SecAdmin	
■	<input checked="" type="checkbox"/>	Helpdesk NXOS	if AD-SecurityDemo:ExternalGroups EQUALS securitydemo.net/Users/Helpdesk	then Select Profile(s)	NXOS Helpdesk	
		Tacacs_Default	if no matches, then Select Profile(s)	Deny All Shell Profile		

**Figure 31-5 Complete Nexus Switches Policy Set**

## Preparing the Nexus Switch for TACACS+ with ISE

Now that the policy set is ready, it's time to start configuring the Nexus switch to authenticate and authorize interactive users. You need to add ISE to the Nexus switch as a TACACS+ Authentication Server, configure a shared secret, and add the authentication method.

### Enable TACACS+ and Add ISE to NX-OS

To configure the network devices to authenticate the interactive logins and authorize the commands executed in their shell, follow these steps.

#### Step 1. Enable TACACS+ on the switch.

By default, the tacacs+ feature of the Nexus switch is disabled. Enable TACACS+ with the **feature** command:

```
n5k(config)# feature tacacs+
```

#### Step 2. Define the TACACS+ AAA servers in the configuration:

```
n5k(config)# tacacs-server host 10.1.100.237 key xxxxxxxx
n5k(config)# tacacs-server host 10.1.100.241 key xxxxxxxx
```

#### Step 3. Configure the automated tester for the TACACS servers:

```
n5k(config)# tacacs-server host 10.1.100.237 test username tacacs-test
  password xxxxxxxx idle-time 5
n5k(config)# tacacs-server host 10.1.100.241 test username tacacs-test
  password xxxxxxxx idle-time 5
n5k(config)# tacacs-server timeout 5
```

#### Step 4. Create a TACACS+ server group, named ISE-TAC+, and add the PSNs to the

group:

```
n5k(config)# aaa group server tacacs+ ISE-TAC+
n5k(config-tacacs+)# server 10.1.100.237
n5k(config-tacacs+)# deadtime 5
n5k(config-tacacs+)# server 10.1.100.241
n5k(config-tacacs+)# deadtime 5
```

**Step 5.** Enable TACACS with the **directed-request** command:

```
n5k(config)# tacacs-server directed-request
```

**Step 6.** Set the AAA authentication and accounting methods to use the ISE-TAC+ group:

```
n5k(config)# aaa authentication login default group ISE-TAC+
n5k(config)# aaa accounting default group ISE-TAC+
```

## Summary

There are a few ways to provide device administration AAA and role-based access control. IOS provides a very granular control all the way down to individual commands. The Cisco WLC provides a broad-level approach to role-based access control by controlling access at a menu level. The NX-OS provides a combination of the granular command-level approach and the easier-to-use role-based approach. There are two main role types out of the box: networkadmin, which gives administrators read-write access, and network-operator, which gives operators read-only access.

## **Part VIII Appendixes**

[Appendix A Sample User Community Deployment Messaging Material](#)

[Appendix B Sample ISE Deployment Questionnaire](#)

[Appendix C Sample Switch Configurations](#)

[Appendix D The ISE CA and How Cert-Based Auth Works](#)

# Appendix A Sample User Community Deployment Messaging Material

This appendix provides sample messaging for you to use to inform your user population about what Identity Services Engine is, how to use it, and where to get help. This messaging is primarily tailored for the education environment but can be easily tailored for use in other environments. This appendix contains the following information and materials:

- Sample Identity Services Engine requirement change notification email
- Sample Identity Services Engine notice for a bulletin board or poster
- Sample Identity Services Engine letter to students

Feel free to modify and adapt these samples to your needs.

## Sample Identity Services Engine Requirement Change Notification Email

The following email sample is meant to be sent out to the user community prior to the enforcement of a new posture assessment requirement or check in ISE. It is recommended that you first roll out all new requirements as Audit only, so that you can review the possible impact on your organization without actually causing any outage in the production environment. Then, after a set amount of time, make the new requirement Optional. The sending of this email should coincide with the implementation of the Optional requirement, to provide ample warning to the user community prior to the Mandatory enforcement date. It should then be sent again immediately prior to the requirement being made Mandatory.

To: Students and Faculty

From: ITD

Subject: NEW PC security updates required

Faculty and Students,

Starting tomorrow, September 23rd, there will be two new security requirements for all **Windows** PCs connected to the residential network. You may see the NAC Agent prompt you to install these new security updates on your PC. Please follow the instructions given to install these updates. You have a two-week discretionary period within which to install the new updates before enforcement begins.

In order to ensure uninterrupted network access, it is **strongly recommended** that you install the new updates during this discretionary period. Please keep in mind that these updates can take from 5 to 30 minutes to install depending on the

performance of your PC.

**Starting October 8th**, the NAC system will initiate the enforcement of the new security updates. Once enforcement begins, any PC not running the required security updates will be forced to install them before being allowed full network access.

If you have any questions or need technical assistance, please go to the ITD ISE support page at [www.univ.com/nac/support](http://www.univ.com/nac/support) or call the help desk at x4000.

## **Sample Identity Services Engine Notice for a Bulletin Board or Poster**

The following announcement can be posted on internal websites, posted on bulletin boards, or handed out as a flyer. Your implementation may differ, so please use this only as a guideline. The objectives of this announcement are as follows:

- To inform the user community that the ISE solution is in place, and to explain why
- To inform users how to employ the system
- To set expectations on its use
- To give references for obtaining more information

## **Connecting to the Campus Network**

In an effort to reduce the threat posed by viruses and worms to the campus network, the University has implemented the Cisco Identity Services Engine network admission control solution.

### **Here's what students need to know:**

- All students living in the residence halls will be required to go through the new network policy controls to gain access to any campus network.
- Students with Windows PCs and Mac computers are required to install the Cisco NAC Agent and Cisco AnyConnect security software. This will be delivered to you automatically through the student web portal page.
- Students are required to authenticate to the network using their campus username and password.
- The PC being used will be checked to make sure it has the necessary security software and system patches installed before being allowed onto the network.
- Any PC that does not meet the security requirements will dynamically be placed into network quarantine and provided the necessary instructions and security software. Once the PC is certified, full network access will be restored.
- The Cisco Identity Services Engine solution does NOT access your personal files, block any applications, or monitor your network traffic.

## **Why is Cisco Identity Services Engine necessary?**

Nearly all network outages or brown-outs experienced on the campus network are the result of virus-infected or severely compromised student PCs accessing the network. As a result, it has become necessary for the University to implement a network security system in order to minimize the risk posed by students who connect infected PCs to the campus network. This security solution will keep your computers much more secure, allowing them to resist the infection of viruses that may destroy your documents or render your PC unusable.

### **How to obtain the Cisco NAC Agent:**

- 1.** Plug in to the campus network.
- 2.** Open your web browser of choice. You will be redirected to the University login page.
- 3.** Log in using your campus username and password.
- 4.** You will be directed to install the Cisco NAC Agent and Cisco AnyConnect software.
- 5.** Click the **Download** button and follow the installation wizard's instructions to install the software. Installation may require a reboot.

### **How to log in to the network:**

- 1.** Login is done using the Cisco AnyConnect Agent.
- 2.** The agent login will happen automatically whenever your computer attempts to access the campus network.
- 3.** If required, enter your username and password and click **Login**.
- 4.** Follow the instructions given to remediate any failed security checks on your PC.
- 5.** Once your PC is compliant, you will gain full network access.

### **Who to contact for help:**

- Help desk at x4000
- [www.university.com/nac/support](http://www.university.com/nac/support)
- Email: [Support@university.com](mailto:Support@university.com)

Additional information can be found at [www.university.com/nac/support](http://www.university.com/nac/support).

### **Sample Identity Services Engine Letter to Students**

The following sample letter is intended to be added to the university's student handbook, which is typically sent to students before the beginning of the new school year. The letter serves two purposes: to inform students about the ISE solution, and to instruct students on how to obtain the NAC Agent prior to arriving on campus.

Dear Student,

This letter is to inform you that the university's campus network is protected using a system called Cisco Identity Services Engine. This security solution was put in place in an effort to decrease the threat posed by viruses and worms on the university's network. The vast majority of previous network outages or slowness could be attributed directly to the outbreak of a computer virus or worm. These outbreaks also resulted in the widespread damage or loss of data on student PCs. An effective method of combating these outbreaks is to ensure that every PC connecting to the network is running an up-to-date antivirus software package and also has all of the latest Windows security patches installed. The Cisco Identity Services Engine security solution provides this capability to the University.

In order to be ready for the school year, you will need to download and install the NAC Agent on your Windows or Mac-based computer. Please make every effort to install the agent prior to arriving on campus. This will help make your arrival go that much smoother. The agent download can be found at [www.university.com/agent](http://www.university.com/agent). Just follow the instructions provided to complete the simple install. Should you have any questions or need technical assistance, please call the University help desk at 800-333-3333.

Thank you,

The ITD Staff

# Appendix B Sample ISE Deployment Questionnaire

This appendix provides a series of questions meant to help you determine the scope of your proposed ISE deployment. Most of this content comes from the Cisco ISE High-level Design Guide that is used by the Cisco ISE Certified Partners. Once you have answered the questions in each given table, you can then proceed to determine your Bill of Materials for Cisco ISE and your approximate project scope to plan for.

## State Your Business Goals for ISE

Services	Wire (Yes or No)	Wireless (Yes or No)
Guest Services		
Device Profiling		
Host Posture Assessment		
TC-NAC		
BYOD		

## Estimated Timelines

Phase	Number of Endpoints	Begin	End	Comments
Lab testing and qualification				
Final Design Review call with Cisco SME	—			
Production phase 1 (pilot)				
Production phase 2				
Production phase 3				

## Customer Environment Summary

Deployment Summary	Response
Use cases in scope for design	
Wired?	
Wireless?	
VPN?	
Guest?	
<b>Endpoint count</b>	
Total endpoint count for entire deployment (endpoint count equals the sum of user and non-user devices)	
Total user endpoints (laptops, PCs, mobile devices, etc.)	
Total non-user endpoints that support 802.1X (i.e., IP phones, printers, BioMed, etc.)	
Total non-user endpoints that do not support 802.1X (i.e., IP cameras, badge readers, etc.)	
<b>Concurrent endpoint count</b>	
Max. number of endpoints online with ISE at any given time	
<i>*ISE is licensed based on max. concurrent online users and devices.</i>	
<b>Total physical locations</b>	
How many physical buildings/locations will you protect with ISE?	
Is your deployment geographically disperse?	
How many ISE Policy Service Node locations do you anticipate?	
<b>Total number of network infrastructure devices</b>	
Switches	
Wireless controllers	
VPN gateways	
Wireless Access Points	
IP phones (do they support dot1x?)	
Routers	
Other	
<b>Topology Specifics</b>	

Required Information	Response
<b>Network Access Devices</b>	
<p>Provide the general switch/controller model numbers/ platforms deployed and Cisco IOS Software versions to be deployed to support ISE design.</p>	
<b>Client OS and Suplicant Types</b>	
<p>List all non-mobile client OS types and versions that will be used by non-guest users.</p>	
<p>Which 802.1X supplicant is used (native OS, AnyConnect NAM, other)?</p>	
<p>Number (general count for each type)?</p>	
<p><i>*Please provide service pack details for Windows and OS types for Mac OS X.</i></p>	
<b>Mobile Devices (smartphones, tablets)</b>	
<p>List all vendor types and mobile OS versions deployed by non-guest users.</p>	
<p>Are mobile devices corporate- or employee-owned assets?</p>	
<p>Will you use a mobile device management system?</p>	
<p>If so, list the details.</p>	
<b>802.1X Authentication</b>	
<p>Will you be deploying 802.1X for wired, wireless, or both?</p>	
<p>Will you be using machine authentication, user authentication, or both?</p>	
<p>What percentage of your devices will not support 802.1X?</p>	
<b>Extensible Authentication Protocol (EAP) Types</b>	
<p>EAP types for users</p>	
<p>EAP types for machines</p>	
<p>Examples:</p>	
<p>PEAP (Username/password-based auth.)</p>	
<p>EAP-TLS (Certificate-based auth.)</p>	
<p>EAP-FAST</p>	

## ID Stores

[EAP and ID Store Compatibility Reference]

*List the ID store to be used by each Auth. Type:*

802.1X machine auth.

802.1X user auth.

802.1X cert-based auth.

---

## MAB

Web Authentication/Guests

*For Active Directory:*

Are there multiple domains?

Are there multiple forests?

---

## Authorization

Which enforcement types will be used?

List wired/wireless.

## VLANs

Downloadable ACLs

Security Group Tags (SGTs/SGACLs)

SmartPort macros

---

## Posture

Will you be using host posture assessment?

If so, which operating systems are in scope?

---

## Profiling

List the primary device types to be profiled.

Which probes will be deployed to collect the required data?

If RSPAN or NetFlow is to be used, is there sufficient bandwidth between source SPAN/NetFlow exporter and ISE Policy Service Node used for profiling?

Is profiling for visibility only or for use in Authorization Policy?

---

## ISE Nodes/Personas

Will high availability be deployed for ISE?

Number and type of each ISE appliance (node).

Define the personas assigned to each node  
(e.g., Administration, Monitoring, Policy Service, Inline Posture).

---



# Appendix C Sample Switch Configurations

This appendix includes some full sample configurations of various device types with multiple Cisco IOS versions, all designed to follow the guidelines and practices laid out in [Chapter 11, “Bootstrapping Network Access Devices.”](#)

## Catalyst 3000 Series, 12.2(55)SE

[Click here to view code image](#)

```
3560-X# sho run
Building configuration...
Current configuration : 22928 bytes
!
version 12.2
hostname 3560-X
logging monitor informational
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 10.1.103.231 server-key Cisco123
client 10.1.103.4 server-key Cisco123
!
aaa session-id common
authentication mac-move permit
ip routing
!
ip domain-name cts.local
ip name-server 10.1.100.100
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-4076357888
enrollment selfsigned
```

```
subject-name cn=IOS-Self-Signed-Certificate-4076357888
revocation-check none
rsakeypair TP-self-signed-4076357888
!
!
crypto pki certificate chain TP-self-signed-4076357888
certificate self-signed 01
quit
!
dot1x system-auth-control
!
interface Loopback0
ip address 192.168.254.60 255.255.255.255
!
interface <ALL EDGE PORTS>
switchport access vlan 41
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 41
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
!
interface Vlan1
no ip address
!
interface Vlan40
ip address 10.1.40.60 255.255.255.0
!
!
```

```
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
logging origin-id ip
logging source-interface Loopback0
logging host 10.1.103.4 transport udp port 20514
!
snmp-server community CiscoPressRO RO
snmp-server trap-source Loopback0
snmp-server source-interface informs Loopback0
snmp-server host 10.1.103.231 version 2c CiscoPressRO
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 10.1.103.231 auth-port 1812 acct-port 1813 key Cisco123
radius-server host 10.1.103.4 auth-port 1812 acct-port 1813 key Cisco123
radius-server vsa send accounting
radius-server vsa send authentication
!
end
```

## Catalyst 3000 Series, 15.0(2)SE

[Click here to view code image](#)

```
C3750X# sho run brief
Building configuration...
Current configuration : 18936 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C3750X
!
boot-start-marker
boot-end-marker
!
logging monitor informational
!
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 10.1.103.231 server-key Cisco123
client 10.1.103.4 server-key Cisco123
!
```

```
aaa session-id common
clock timezone EDT -1 0
authentication mac-move permit
ip routing
!
!
ip dhcp snooping vlan 10-13
ip dhcp snooping
ip domain-name cts.local
ip device tracking
!
!
device-sensor filter-list cdp list my_cdp_list
tlv name device-name
tlv name platform-type
!
device-sensor filter-list lldp list my_lldp_list
tlv name port-id
tlv name system-name
tlv name system-description
!
device-sensor filter-list dhcp list my_dhcp_list
option name host-name
option name class-identifier
option name client-identifier
device-sensor filter-spec dhcp include list my_dhcp_list
device-sensor filter-spec lldp include list my_lldp_list
device-sensor filter-spec cdp include list my_cdp_list
device-sensor accounting
device-sensor notify all-changes
!
epm logging
!
crypto pki trustpoint TP-self-signed-254914560
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-254914560
revocation-check none
rsakeypair TP-self-signed-254914560
!
!
crypto pki certificate chain TP-self-signed-254914560
```

```
certificate self-signed 01
cts role-based enforcement
!
dot1x system-auth-control
!
interface Loopback0
ip address 192.168.254.1 255.255.255.255
!
interface <ALL EDGE PORTS>
switchport access vlan 10
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 10
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
ip dhcp snooping information option allow-untrusted
!
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
ip address 10.1.10.1 255.255.255.0
!
interface Vlan20
ip address 10.1.20.1 255.255.255.0
!
interface Vlan30
```

```
ip address 10.1.30.1 255.255.255.0
!
interface Vlan99
ip address 10.1.99.1 255.255.255.0
!
!
ip http server
ip http secure-server
!
!
ip access-list extended ACL-AGENT-REDIRECT
remark explicitly prevent DNS from being redirected
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 address
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 access-list extended AGENT-REDIRECT
remark explicitly prevent DNS from being redirected to address
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 radius source-interface Loopback0
ip sla enable reaction-alerts
logging origin-id ip
logging source-interface Loopback0
logging host 10.1.103.4 transport udp port 20514
!
snmp-server community Cisco123 RO
snmp-server community TrustSecRO RO
snmp-server trap-source Loopback0
snmp-server source-interface informs Loopback0
snmp-server host 10.1.103.4 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 vsa send accounting
radius-server vsa send authentication
!
radius server CP-VIP
address ipv4 10.1.103.231 auth-port 1812 acct-port 1813
automate-tester username radius-test
key Cisco123
!
radius server CP-04
address ipv4 10.1.103.4 auth-port 1812 acct-port 1813
automate-tester username radius-test
key Cisco123
!
end

```

## Catalyst 4500 Series, IOS-XE 3.3.0 / 15.1(1)SG

[Click here to view code image](#)

```

4503# show run brief
Building configuration...
Current configuration : 35699 bytes
!
!
version 15.1

```

```
!
hostname 4503
!
!
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 10.1.103.231 server-key Cisco123
client 10.1.103.4 server-key Cisco123
!
aaa session-id common
clock timezone EDT -1 0
!
ip domain-name cts.local
!
ip device tracking
!
device-sensor filter-list cdp list my_cdp_list
tlv name device-name
tlv name platform-type
!
device-sensor filter-list lldp list my_lldp_list
tlv name port-id
tlv name system-name
tlv name system-description
!
device-sensor filter-list dhcp list my_dhcp_list
option name host-name
option name class-identifier
option name client-identifier
device-sensor filter-spec dhcp include list my_dhcp_list
device-sensor filter-spec lldp include list my_lldp_list
device-sensor filter-spec cdp include list my_cdp_list
device-sensor accounting
```

```
device-sensor notify all-changes
epm logging
!
!
crypto pki trustpoint CISCO_IDEVID_SUDI
revocation-check none
rsakeypair CISCO_IDEVID_SUDI
!
crypto pki trustpoint CISCO_IDEVID_SUDIO
revocation-check none
!
!
crypto pki certificate chain CISCO_IDEVID_SUDI
certificate 238FC0E90000002BFCA1
certificate ca 6A6967B3000000000003
crypto pki certificate chain CISCO_IDEVID_SUDIO
certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
!
dot1x system-auth-control
!
!
vlan 40
name jump
!
vlan 41
name data
!
vlan 99
name voice
!
interface <ALL EDGE PORTS>
switchport access vlan 41
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 41
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication open
```

```
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
ip dhcp snooping information option allow-untrusted
!
interface Vlan1
no ip address
!
interface Vlan40
ip address 10.1.40.2 255.255.255.0
!
ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.1.40.1
!
ip access-list extended ACL-AGENT-REDIRECT
remark explicitly prevent DNS from being redirected to address
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 address
```

```

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
!
logging 10.1.103.4
!
snmp-server community Cisco123 RO
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 10.1.103.231 auth-port 1812 acct-port 1813 test username
radiustest
key Cisco123
radius-server host 10.1.103.4 auth-port 1812 acct-port 1813 test username
radiustest
key Cisco123
radius-server vsa send accounting
radius-server vsa send authentication
!
end

```

## Catalyst 6500 Series, 12.2(33)SXJ

[Click here to view code image](#)

```

hostname 6503
logging monitor informational
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 10.1.103.231 server-key Cisco123
client 10.1.103.4 server-key Cisco123

```

```
!
aaa session-id common
authentication mac-move permit
ip routing
!
ip domain-name cts.local
ip name-server 10.1.100.100
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-4076357888
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-4076357888
revocation-check none
rsakeypair TP-self-signed-4076357888
!
!
crypto pki certificate chain TP-self-signed-4076357888
certificate self-signed 01
quit
!
dot1x system-auth-control
!
interface Loopback0
ip address 192.168.254.1 255.255.255.255
!
interface <ALL EDGE PORTS>
switchport access vlan 10
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 10
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
```

```
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
!
interface Vlan1
no ip address
!
interface Vlan40
ip address 10.1.40.1 255.255.255.0
!
!
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
deny ip any any
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
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
deny ip any any
```

```
!
ip radius source-interface Loopback0
logging origin-id ip
logging source-interface Loopback0
logging host 10.1.103.4 transport udp port 20514
!
snmp-server community CiscoPressRO RO
snmp-server trap-source Loopback0
snmp-server source-interface informs Loopback0
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 10.1.103.231 auth-port 1812 acct-port 1813 key Cisco123
radius-server host 10.1.103.4 auth-port 1812 acct-port 1813 key Cisco123
radius-server vsa send accounting
radius-server vsa send authentication
!
end
```

# Appendix D The ISE CA and How Cert-Based Auth Works

This appendix provides a primer on certificate-based authentications as described by Aaron Woland.

I find a few universal truths when mentioning certificates to IT professionals. Almost without fail, most people I speak with consider certificates and public key cryptography (PKI) to be a very secure concept. However, upon mentioning to someone that I want to talk about certificates or PKI, that person's face turns a slightly lighter shade, their eyes get a bit wider, and they have this immediate fight-or-flight instinct kick in.

This is a subject that does not have to be scary; there are just a few misunderstandings. One example of a common misunderstanding is the notion that a certificate is the same as two-factor authentication. Another common misconception is: "Since the certificate was issued by Active Directory's certificate authority, then authenticating that certificate is the same as an Active Directory authentication." I realize how and why that assumption is made. It does get awfully confusing to try to separate out Active Directory from a certificate authority (CA) when they are so tightly integrated. However, let me assure you, standard certificate-based authentication is the same regardless of which vendor has created the CA you are using.

Before moving on, a quick shout out to Max Pritkin. Max is one of the unsung heroes working behind the scenes in the standards bodies, like the IETF, to build standards around PKI and other technologies. Max is a flat-out, uncontested genius with PKI and yet can somehow still explain it in simple terms. I call him out because he has taught me so much about PKI that I can no longer remember what it was like working with PKI without the knowledge he bestowed upon me. I now transfer a portion of that wisdom to you.

## Certificate-Based Authentication

Let's take some time and review how certificate-based authentications actually work. When presented with a certificate, an authentication server checks the following (at a minimum):

1. Has the digital certificate been issued (signed) by a trusted CA?
2. Is the certificate expired? This check examines both the start and end dates.
3. Has the certificate been revoked? Revocation could be identified using the Online Certificate Status Protocol (OCSP) or a certificate revocation list CRL to verify.
4. Has the client provided proof of possession?

Let's examine these four items one at a time.

## Has the Digital Certificate Been Signed by a Trusted CA?

This first check is something you are most likely very familiar with, whether you know it or not. To describe it, let's focus on a hypothetical real-world situation.

Suppose you are a bartender and have to check the ID of a patron who is asking for an alcoholic beverage. That person hands you a napkin with the name Bob Smith written on it, a date of birth over 21 years ago written below the name, and has signed that napkin. Would you trust that it is a valid ID? Of course not! In the same situation, if Bob Smith hands you a state-issued driver's license, that would be much more trustworthy, right? In this hypothetical scenario, the state is the authority that signed the credential (the driver's license). A digital certificate works the same way. A trustworthy authority must sign the certificate.

The signing of the certificate has two parts. First, the certificate must be signed correctly (following the correct format, etc.). If it is not, it will be discarded immediately. Second, the signing CA's public key must be in a Trusted Certificates store, and that certificate must be trusted for purposes of authentication. Using Cisco ISE as an example, the trusted certificate needs to have the "Trust for client authentication" use case selected, as shown in [Figures D-1](#) and [D-2](#). [Figure D-1](#) shows a certificate that is trusted by ISE, while [Figure D-2](#) shows a certificate trusted on an Apple Mac device.

The screenshot shows the 'Edit Certificate' page in Cisco ISE. The top section is titled 'Issuer' and contains the following details:

- \* Friendly Name: Certificate Services Endpoint Sub CA - woland-ise#00003
- Status: Enabled
- Description: Auto import of trust certificate from CA server
- Subject: CN=Certificate Services Endpoint Sub CA - woland-ise
- Issuer: CN=Certificate Services Node CA - woland-ise
- Valid From: Tue, 10 Jan 2017 12:42:01 UTC
- Valid To (Expiration): Tue, 11 Jan 2022 12:41:59 UTC
- Serial Number: 25 F2 46 B9 0E FE 41 9A 9F E2 7F C6 DF 9C 4F 12
- Signature Algorithm: SHA256WITHRSA
- Key Length: 4096

The bottom section is titled 'Usage' and contains the 'Trusted For:' configuration:

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for authentication of Cisco Services

**Figure D-1** Cisco ISE Trusting a Certificate

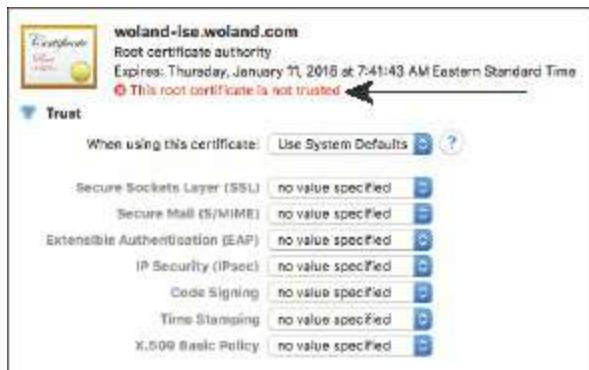


**Figure D-2** Apple Mac OS Trusting a Certificate

So not only does ISE trust certificates that have been signed by this CA, it trusts those for a specific use-case (client authentication). If a client presents a certificate, and that certificate has not been signed by a CA that is trusted for client authentication, the authentication will fail. It's exactly like someone entering in the wrong password.

With the Apple example in [Figure D-2](#), that system has even more purposes or uses to trust the certificate for, including Secure Sockets Layer (SSL), Secure Mail (S/MIME), and Extensible Authentication (EAP), among others.

Figure D-3 shows a certificate that is not signed by a trusted CA and therefore is not trusted for any particular service.



**Figure D-3** Untrusted Certificate

If you take away nothing else from this section, take away the knowledge that certificates are signed by certificate authorities. Authenticators are configured to trust certain authorities. If the certificate is signed by a trusted certificate authority, it is considered a valid certificate, and the authenticator will proceed to the next check: has the certificate expired?

## Has the Certificate Expired?

Just like a driver's license or a passport, a certificate has two dates listed in it: the date

issued, and the date it is valid until (when it expires).

To relate that back to a driver's license, let's examine a fun and very true story. I was in Las Vegas for a conference. I was out on the town with my girlfriend (now wife) and a few friends and we went into the ICE bar at Mandalay Bay to sample some very cold vodka in a unique setting. When we presented our IDs, my North Carolina Department of Motor Vehicles (DMV)-issued driver's license was expired by one day. The picture was still a valid picture of me, the name was still mine, and my birth date showed that I was of legal drinking age and it was (in fact) the day after my birthday—yet I was refused service because the license expired and was therefore no longer a valid source of identity. In RADIUS terms: Access-Reject.

An authenticator does the same sort of check. Is the certificate valid for the date and time that the authentication request comes in? This is one reason why Network Time Protocol (NTP) is so important when working with certificates. Many of us have seen problems where time was out of sync. For example, a certificate was presented on January 10, 2014 at 11:11 a.m., but its "valid-from" value started on January 10, 2014 at 11:30 a.m. This discrepancy occurred because of a time sync issue that caused the CA to think it was 20 minutes later than the authentication server, and the brand-new certificate was not valid yet! This is so common you would laugh, or maybe even cry.

Notice in [Figure D-4](#) that the certificate has a Valid From attribute and a Valid To (Expiration) attribute.

The screenshot shows the 'Edit Certificate' interface with the 'Issuer' tab selected. The 'Friendly Name' field contains 'USERTrust RSA Certification Authority#AddTrust External CA Root#0000'. The 'Status' dropdown is set to 'Enabled'. The 'Description' field is empty. The 'Subject' field shows 'CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,BT>New Jersey,C=US'. The 'Issuer' field shows 'CN=AddTrust External CA Root,OU=AddTrust External TTP Network,O=AddTrust AB,C=SE'. Two arrows point from the text 'Is it valid yet?' and 'Is it still valid?' to the 'Valid From' and 'Valid To (Expiration)' fields respectively. The 'Valid From' field is set to 'Tue, 30 May 2000 10:48:38 UTC' and the 'Valid To (Expiration)' field is set to 'Sat, 30 May 2020 10:48:38 UTC'. Other visible fields include 'Serial Number: 13 EA 2B 70 5B F4 EC ED CC 35 83 09 80 81 43 38', 'Signature Algorithm: SHA256WITHRSA', and 'Key Length: 4096'.

**Figure D-4** Validity Period

## Has the Certificate Been Revoked?

Let's examine another hypothetical real-world situation. You are driving down the road, and are pulled over by a police officer. The officer asks for your driver's license and proof of insurance. You hand your driver's license to the officer, who immediately checks for evidence of authenticity; that is, does it look like a valid driver's license or a forgery? The officer determines that it's not fake. Check. Next, the officer inspects the

expiration: it is not expired. Check. Now the officer asks you to wait while he goes back to his squad car.

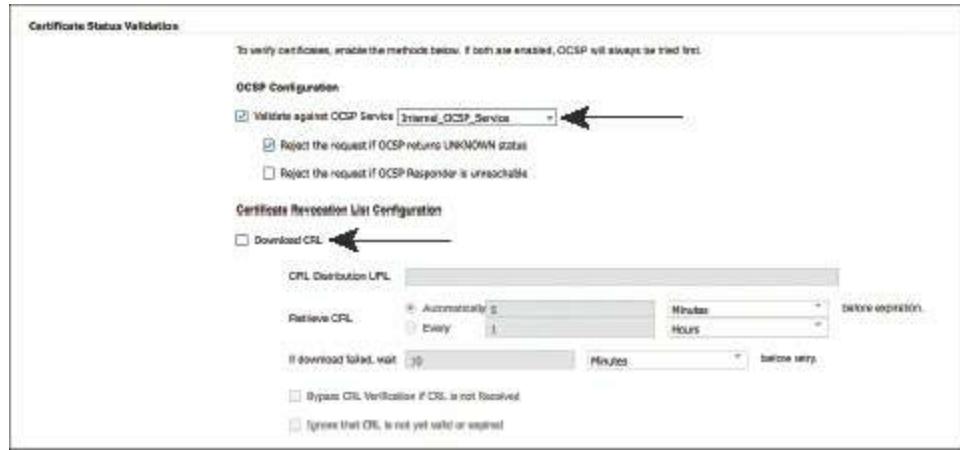
While in the squad car, the officer performs some authorization checks (whether you are a registered owner of the car you are driving, etc.). Those are not important for this hypothetical situation, though. What is important is that the police officer must make sure your valid driver's license has not been revoked by the DMV. A quick lookup on the computer into the DMV records shows that your driver's license was revoked for too many unpaid speeding tickets. The cold steel of the handcuffs and the rough shove into the back seat of the squad car as you are hauled off to jail make you re-evaluate your life choices.

Certificate authentication has the same capability. No, not the handcuffs. It has the same capability to perform a lookup to verify the revocation status. Every certificate authority should also have a service to publish a list of certificates that have been revoked. There are two main ways to do this today:

- **Certificate revocation list (CRL):** This is basically a signed list that the CA publishes on a website that can be read by authentication servers. The file is periodically downloaded and stored locally on the authentication server, and when a certificate is being authenticated, the server examines the CRL to see if the client's certificate was revoked already. A CRL could be compared to the police officer having a printed list of suspended driver's licenses in his squad car.
- **Online Certificate Status Protocol (OCSP):** This is the preferred method for revocation checks in most environments today, because it provides near-real-time updates. OCSP allows the authentication server to send a real-time request (similar to an HTTP web request) to the service running on the CA or another device to check the status of the certificate in near real time. OCSP could be compared to the police officer using the computer in the squad car to search the DMV's database.

If the certificate has been revoked, then access is denied. Enjoy the lights and sirens on the way to jail.

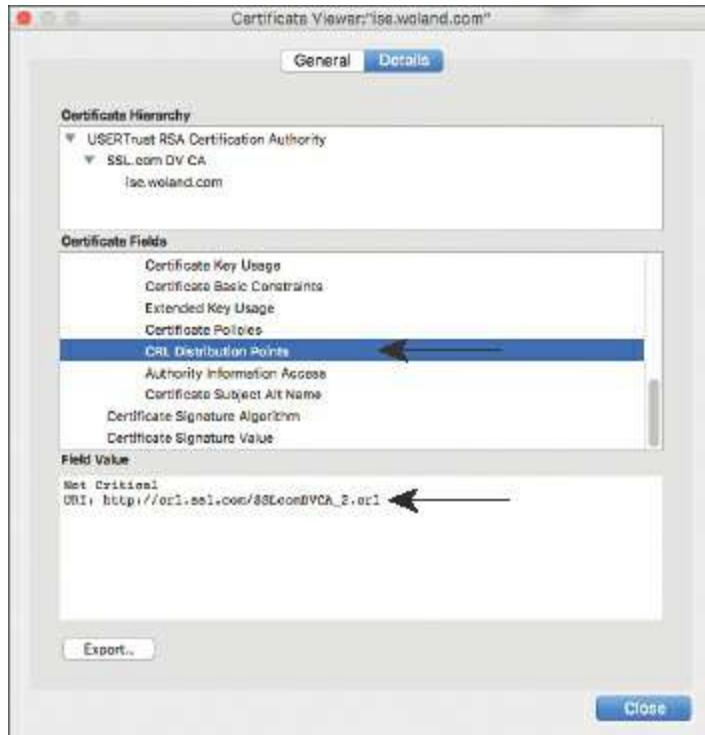
Figure D-5 shows an example of the configuration screen for a trusted certificate authority in Cisco ISE. You have options to configure where to check for OCSP and/or the CRL, when a certificate is signed by this particular root (or its subordinates).



**Figure D-5** Revocation Checking Settings

It is very important for you to understand that checking for certificate revocation is an option. When you initially trust a certificate, neither CRL nor OCSP is on by default; they require the administrator to configure the URL or the service location. It is also critical to understand what behavior will happen if the service is not available or the status of the certificate is unknown. This determines how the authentication policy will handle exceptions. It could be configured to fail-open or fail-closed.

The client's certificate itself will have a field (known as an extension) named CRL Distribution Points, which can be populated with the URI where the authentication server may locate the CRL. [Figure D-6](#) shows an example of the CRL Distribution Points extension in a certificate and the defined URI.



**Figure D-6** CRL Distribution Points Certificate Extension

Here is another interesting piece of trivia about managing revocation lists that may help you win a bet someday: In the earlier discussion of certificate expiration, [Figure D-4](#) displayed the Valid From and Valid To fields in the certificate. These fields form the validity period, the time range during which the signing CA will warrant that it will maintain revocation information regarding that certificate. This helps keep CRL and OCSP lists at manageable sizes. In other words, an expired certificate should be no less valid than one that has not expired, except for the fact that the issuing CA will no longer guarantee the revocation list for that certificate. That's all.

## Has the Client Provided Proof of Possession?

Proof of possession is a way for an authentication server to be sure the client truly owns the certificate and private key pair, and isn't just presenting someone else's public certificate. Returning to our scenario, you are pulled over by a police officer for speeding and you hand your driver's license to the police officer, who confirms the following:

- It is a valid driver's license, issued by a trusted root (the state DMV).
- It has not expired yet.
- The DMV has not revoked the driver's license.

All of the checks have passed, but the picture on the driver's license is of a woman with long flowing brown hair and hazel eyes, whereas you are a bald elderly man. Oops! This "valid" driver's license was not issued to you—the proof of possession has failed! Again, proceed directly to jail!

Certificate authentications do something similar. There will be some throwaway piece of data that must be encrypted and decrypted. Successfully encrypting and decrypting that data ensures that the client has both the public and private keys, and therefore it is the proof of possession. This ensures that someone did not just grab the client's public key and try to present that as being their own. If the client cannot provide proof of possession, then the authentication will fail: Access-Reject.

## So, What Does Any of This Have to Do with Active Directory?

What can often confuse people with regard to AAA is the difference between authentication and authorization. They often blend so much. A certificate issued by Active Directory Certificate Services (the CA built into AD) is still just an X.509 digital certificate. It will go through all the authentication validation discussed in this appendix regardless of the fact that the CA is integrated into AD.

What is possible with certificates and Active Directory is to examine a field of the certificate and then do a separate lookup into AD based on that field during the authorization phase. For example, a certificate with a subject of Aaron is sent to the

authentication server using EAP-TLS. The certificate is validated through the four functions described previously and it passed. So the authentication was successful. Now it's time for the authorization. The RADIUS server (ISE) will take the certificate subject (Aaron) and do a lookup into AD for that username. This is where group membership and other policy conditions will be examined, and the specific authorization result will be issued.

Cisco ISE uses something called a certificate authentication profile (CAP) to examine a specific field and map it to a username for authorization. [Figure D-7](#) shows an example CAP.

**Note** Cisco ISE will also do a courtesy check to validate whether the machine or account has been disabled in AD. If the account has been disabled in AD, then the authorization will be to deny access.

The screenshot shows the 'Certificate Authentication Profiles List > Preloaded\_Certificate\_Profile' section of the Cisco ISE interface. The profile name is 'Preloaded\_Certificate\_Profile'. The 'Description' field contains 'Precreated Certificate Authorization Profile.' The 'Identity Store' dropdown is set to '[not applicable]'. Under 'Use Identity From', the radio button for 'Certificate Attribute' is selected, with 'Subject - Common Name' chosen from the dropdown. Below this, there are three options for matching client certificates against identity store certificates: 'Never' (selected), 'Only to resolve identity ambiguity', and 'Always perform binary comparison'. At the bottom are 'Save' and 'Reset' buttons.

**Figure D-7** Certificate Authentication Profile (CAP)

This is a very different process than an Active Directory authentication, which uses Kerberos, and therefore AD logs will be recorded differently. As covered in [Chapter 24](#), there are solutions on the market that examine AD log files and use that information to help tie together usernames and IP addresses for single sign-on to web proxy servers, identity-enabled firewalls, and other services.

If the authentication was a certificate-based authentication (EAP-TLS) but the user was authorized from an AD lookup, that process will not provide the right types of logging for those identity-enabled firewalls, web proxies, and so forth.

## **ISE's Internal Certificate Authority**

Now that you are an emergent expert on certificate-based authentication, let's review the internal CA added to ISE beginning in version 1.3.

### **Why Put a CA into ISE?**

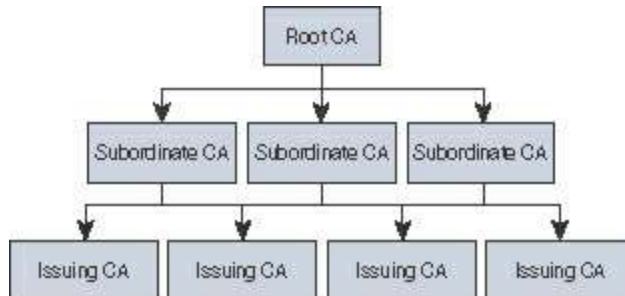
The first edition of this book, which covered ISE version 1.2, included an appendix covering the configuration of the Microsoft CA and another appendix for using the Cisco IOS CA. These appendixes were included because ISE did not have its own CA in version 1.2, and CAs are a key function of any complete BYOD solution. At that time, the most common CA in a BYOD deployment, and the only CA fully tested by the ISE quality assurance team, was the Microsoft enterprise CA. That presented many challenges: organizational, political, financial, and sometimes technical. One team could be controlling Active Directory while another team controlled the Microsoft CA, and the two teams (network and AD) did not necessarily communicate or collaborate well. Perhaps the organization didn't need to pay for the Enterprise version of Windows Server, yet the functionality required for that CA was only available in the Enterprise edition. (Once upon a time, I created a 54-slide step-by-step PowerPoint on configuring the Microsoft CA for use in the BYOD solution.)

So, Cisco needed to simplify the ISE BYOD deployment, and integrating an internal certificate authority simplifies BYOD exponentially. Among others, Avinash Kumar, Victor Ashe, Mohammad Zayed, and Rajesh Thattakath deserve major kudos for truly developing a rock-solid CA.

You no longer need to rely on integrating ISE to your existing PKI, providing ISE with a closed-loop BYOD solution—although you can absolutely make ISE's CA a subordinate CA to an existing PKI if you choose.

### **ISE CA PKI Hierarchy**

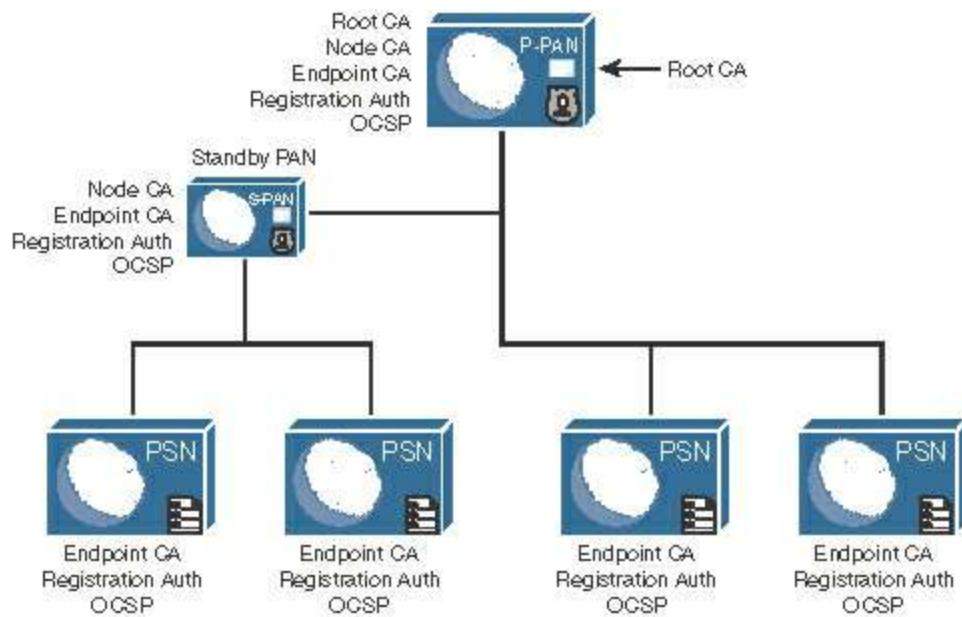
While ISE can join an existing PKI, it is a PKI hierarchy unto itself. Every ISE cube from version 1.3 on has a root CA (on the initial Primary PAN by default), as well as subordinate CAs and other roles within a PKI. [Figure D-8](#) illustrates a basic PKI hierarchy. There is a single root CA, and there can be numerous subordinate CAs that are allowed to sign certificates on behalf of that root CA. As shown, there can be additional layers of CAs that are authorized to sign on behalf of their parent CA in the tree.



**Figure D-8** Generic PKI Hierarchy

PKI design is quite basic. The root is only used to sign the certificates of its subordinate CAs, and then it sits idle. In fact, the best practice for PKI is to take the root offline and only bring it back online whenever a new subordinate CA needs to be added. As an example of that behavior, the certificates for the common root CAs on the public Internet are kept locked up in safes and an actual key ceremony occurs for the extraction of those keys from the safe for the signing of a new subordinate CA. Google the term “key ceremony” for more information. If you are a geek, like me, it is a fun thing to watch when it happens.

Figure D-9 illustrates the basic PKI hierarchy of a distributed ISE cube. You can see that the Primary PAN (P-PAN) is also the Root CA. Each PSN is a subordinate CA, and also has additional functionalities related to PKI.

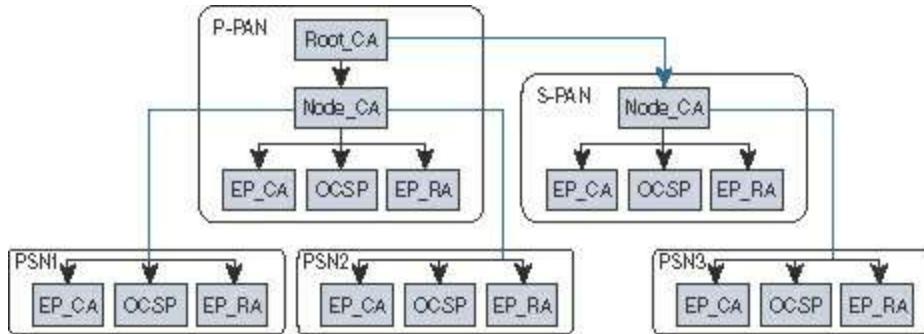


**Figure D-9** Basic ISE PKI Hierarchy

The important thing to understand is that the first PAN in an ISE cube, the P-PAN, is always the root of an ISE PKI, and the PSNs are automatically joined to that root without any intervention from you, the ISE administrator.

The actual PKI design of ISE is a little more complicated than the simple one displayed in [Figure D-9](#). [Figure D-10](#) illustrates the complete PKI tree for an ISE cube, with the

roles called out explicitly.



**Figure D-10** Detailed ISE PKI Hierarchy

Let's dive into those detailed PKI roles:

- **Root CA:** The root of the PKI tree. There can be only one, and it is always the first PAN in the ISE cube: the P-PAN. Promoting the secondary PAN (S-PAN) to primary will not change the root, as the S-PAN does not have the root certificate.

**Note** The root CA is only used to sign the node CA certificates. Once that is completed, the root certificate has no active function.

- **Node CA:** This tier of CA exists on both administrative nodes, and is used to sign the endpoint CA of each node in the ISE cube.
- **Endpoint CA:** The final tier in the PKI tree. This is the CA function that performs the signing of the endpoint certificates themselves. Both PANs and all PSNs have the endpoint CA function.
- **Endpoint registration authority (RA):** The function used to broker certificate requests from the endpoint to external CAs. Both PANs and all PSNs have the RA function.
- **Online Certificate Status Protocol (OCSP):** The function used for certificate revocation checking. All nodes in the ISE cube maintain a copy of the certificate database, and the OCSP service runs on both PANs and all PSNs to allow the checking of those certificates.

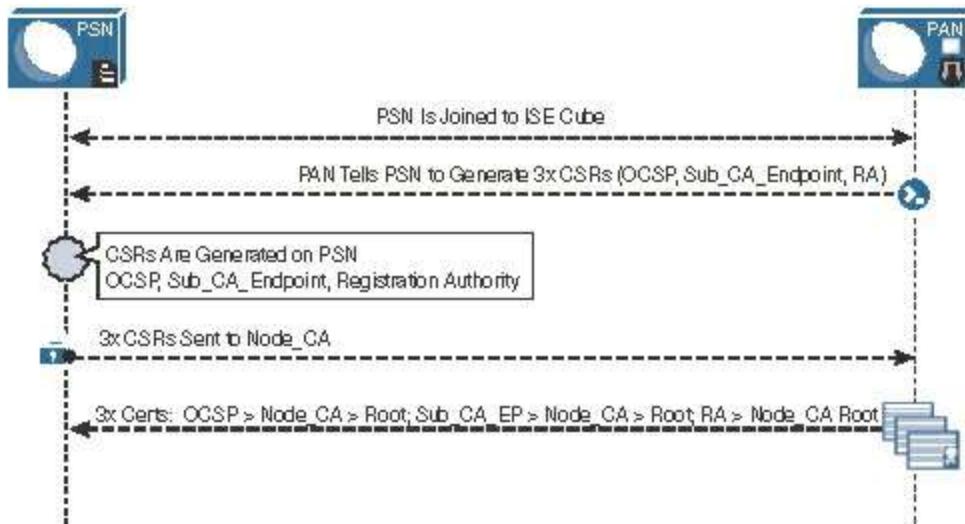
Each function in the PKI has a corresponding certificate to go along with it, used to uniquely identify the node and the individual function in the PKI tree. [Figure D-11](#) shows an example list of certificates for the internal CA of a distributed ISE cube, located under **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**.

CA Certificates						
	Edit	Import	Export	Delete	View	Refresh
Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From
<b>▼ atw-ise237</b>						
Certificate Services Root CA - atw-ise237#00001	<input checked="" type="checkbox"/> Enabled	Endpoints, Infrastructure	39 54 DA F9 A3 E6 48 5C BE F0 3C 60 0F FF 7D AB	Certificate Services Root CA - atw-ise237	Certificate Services Root CA - atw-ise237	Mon, 12 Dec 2016
Certificate Services Endpoint Sub CA - atw-ise237#00003	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	5B 7F 94 B8 5E C6 4C BC 8B 33 9A 29 7E BB F8 D2	Certificate Services Endpoint Sub CA - atw-ise237	Certificate Services Node CA - atw-ise237	Mon, 12 Dec 2016
Certificate Services OCSP Responder - atw-ise237#00004	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	3D OC EA A2 22 11 42 9A 93 3E 9B 5D C2 5B E6 64	Certificate Services OCSP Responder - atw-ise237	Certificate Services Node CA - atw-ise237	Mon, 12 Dec 2016
Certificate Services Node CA - atw-ise237#00002	<input checked="" type="checkbox"/> Enabled	Endpoints, Infrastructure	5D 62 EA A5 BB 05 47 2D BF 88 81 82 73 90 D7 FE	Certificate Services Node CA - atw-ise237	Certificate Services Root CA - atw-ise237	Mon, 12 Dec 2016
Certificate Services Root CA - atw-ise237#00018	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	21 CA 5B 62 3B 6F 42 CB 8E 8B 90 75 B4 0E FD D6	Certificate Services Root CA - atw-ise237	Certificate Services Root CA - atw-ise237	Thu, 22 Dec 2016
Certificate Services Node CA - atw-ise237#00019	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	4E 3E FA DA CC D0 4A 1F BF DA AE 22 04 F3 8F 56	Certificate Services Node CA - atw-ise237	Certificate Services Root CA - atw-ise237	Thu, 22 Dec 2016
Certificate Services Endpoint Sub CA - atw-ise237#00020	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	20 90 3E 3A BB C9 4F 08 A0 C4 D0 23 28 4C 0E 8B	Certificate Services Endpoint Sub CA - atw-ise237	Certificate Services Node CA - atw-ise237	Thu, 22 Dec 2016
Certificate Services OCSP Responder - atw-ise237#00021	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	09 DD EF B3 18 10 45 56 94 13 13 D9 89 44 0B CF	Certificate Services OCSP Responder - atw-ise237	Certificate Services Node CA - atw-ise237	Thu, 22 Dec 2016
<b>▼ atw-ise241</b>						
Certificate Services Node CA - atw-ise241#00015	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	6B 64 39 D7 AB B5 4D A3 9B 8D 8F 73 87 F1 E9 C4	Certificate Services Node CA - atw-ise241	Certificate Services Root CA - atw-ise237	Sun, 18 Dec 2016
Certificate Services Endpoint Sub CA - atw-ise241#00016	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	3B 02 D0 23 9E 7F 41 23 A9 39 09 52 82 8E 3F 5C	Certificate Services Endpoint Sub CA - atw-ise241	Certificate Services Node CA - atw-ise241	Sun, 18 Dec 2016
Certificate Services OCSP Responder - atw-ise241#00017	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	2F C8 45 B2 40 0A 4B 23 B4 46 A6 BC 09 43 00 CE	Certificate Services OCSP Responder - atw-ise241	Certificate Services Node CA - atw-ise241	Sun, 18 Dec 2016
Certificate Services Node CA - atw-ise241#00026	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	09 45 E7 79 DD 82 4D B5 99 9B 0C A7 FD C6 FC 59	Certificate Services Node CA - atw-ise241	Certificate Services Root CA - atw-ise237	Thu, 22 Dec 2016
Certificate Services Endpoint Sub CA - atw-ise241#00027	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	49 1E F8 39 A2 A0 48 F6 89 B2 A9 F7 DD 80 8A C2	Certificate Services Endpoint Sub CA - atw-ise241	Certificate Services Node CA - atw-ise241	Thu, 22 Dec 2016
Certificate Services OCSP Responder - atw-ise241#00028	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	56 84 49 02 BF 5F 47 49 A8 C5 89 D0 F6 26 4C 7F	Certificate Services OCSP Responder - atw-ise241	Certificate Services Node CA - atw-ise241	Thu, 22 Dec 2016
<b>▼ atw-ise242</b>						
Certificate Services OCSP Responder - atw-ise242#00024	<input checked="" type="checkbox"/> Enabled	Infrastructure, Endpoints	37 60 3A FF 07 2D 45 A3 90 C5 CA 98 60 32 A6 FA	Certificate Services OCSP Responder - atw-ise242	Certificate Services Node CA - atw-ise237	Thu, 22 Dec 2016

**Figure D-11 Example Certificate Authority Certificates**

## The Endpoint CA

When a PSN joins the ISE cube, the PAN instructs the PSN to generate three certificate signing requests (CSR). The PSN is requesting the node CA to sign a certificate for the endpoint CA, another certificate for the OCSP function, and a third certificate for the RA role. There is no administrative action needed; it all happens automatically, unless you have disabled the internal CA. [Figure D-12](#) illustrates this behavior.



**Figure D-12 Example Certificate Authority Certificates**

## Reissuing CA Certificates

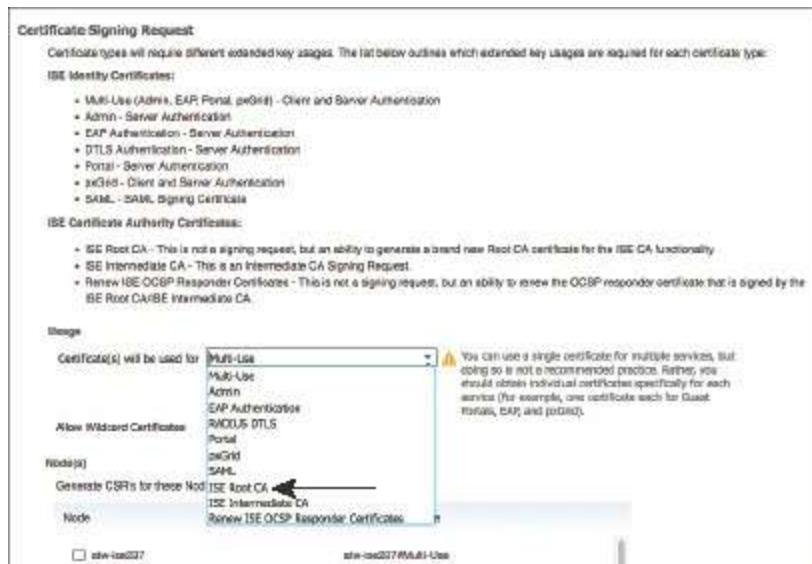
There may come a time when you have to start over with your certificate authority's certificates. Perhaps you didn't back things up (securely) and you lost the original root CA certificate. There could be a number of reasons.

Reissuing CA certificates is fairly easy to do (some consider it too easy, considering the importance of the task). From the ISE GUI, perform the following steps:

**Step 1.** Navigate to **Administration > System > Certificates > Certificate Management > Certificate Signing Requests**.

**Step 2.** Click **Generate Certificate Signing Requests (CSR)**.

**Step 3.** From the Usage drop-down list, choose **ISE Root CA**, as shown in [Figure D-13](#).



**Figure D-13** Certificate Signing Request

**Step 4.** Click Replace ISE Root CA Certificate chain , as shown in [Figure D-14](#).



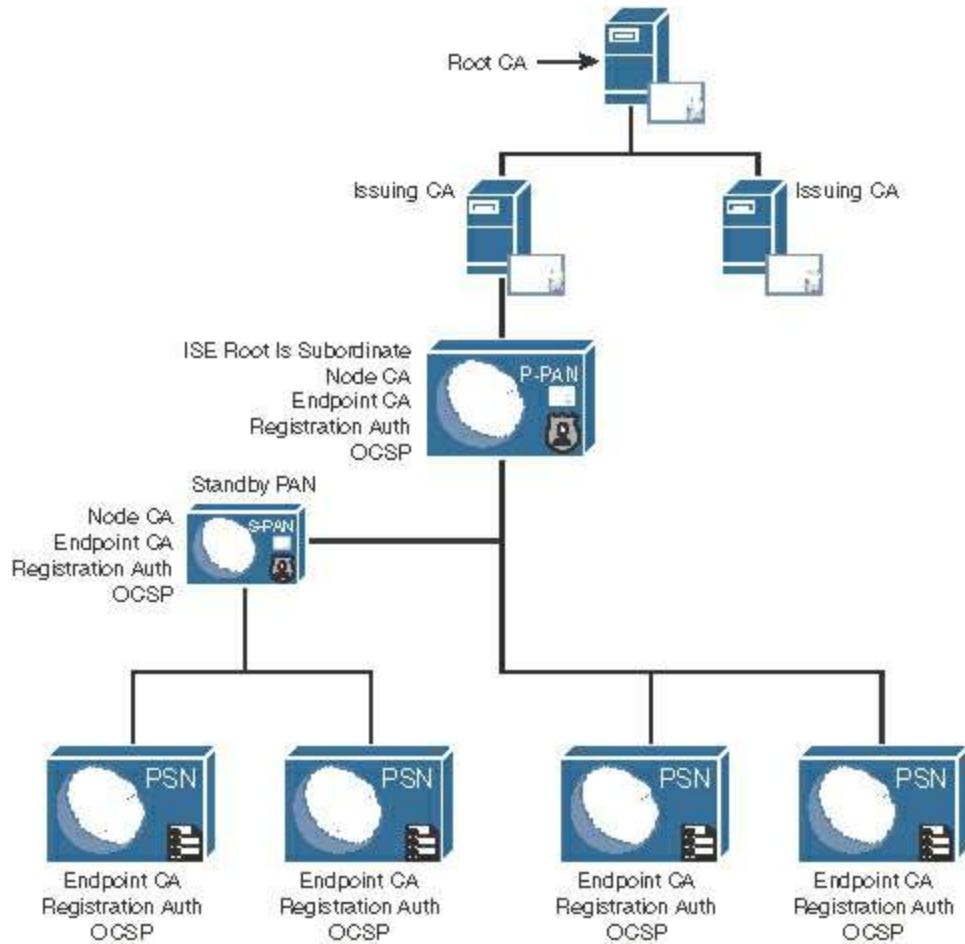
**Figure D-14** Replace ISE Root CA Certificate Chain

That's it. You've just replaced all the CA certificates on all the ISE nodes. Don't worry, you did not invalidate all the existing endpoints that have already gotten certificates. Those certificates are still in the database and still warranted by the CA until their expiration date. ISE still trusts any certificate that was signed by the older PKI chain, as the old and new certificates are now listed in **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates**. You also continue to have the power to revoke any certificates that were previously issued.

**Warning** Do not ever delete the certificates from **Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates** , unless you are certain and directed by Cisco TAC. Doing so will result in the CA revoking every certificate issued under that PKI chain, and could result in your denying access to all those endpoints. There is no way to undo this action.

## Configuring ISE to be a Subordinate CA to an Existing PKI

ISE's internal certificate authority does not need to be a standalone PKI. You also have the option to "join" it to an existing hierarchy. [Figure D-15](#) illustrates this concept, where the root CA is a Microsoft CA, and the ISE P-PAN is subordinate to one of the Microsoft issuing CAs.

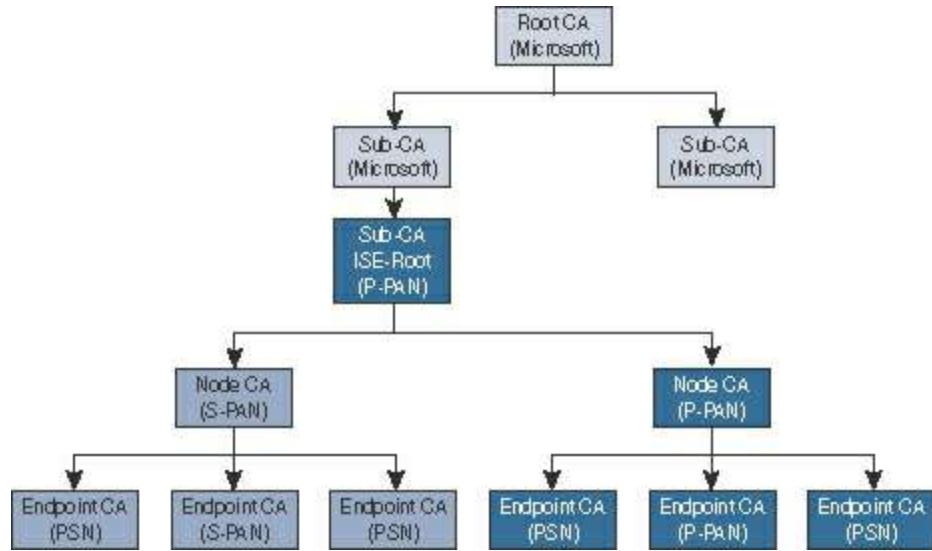


**Figure D-15 ISE CA as Subordinate to Existing PKI**

In the illustration shown in [Figure D-15](#), it is possible that the endpoint CA that issues the certificate to the BYOD endpoints is actually five levels deep in the PKI hierarchy. Note that this is not a best practice, just an illustration.

When considering the depths of a PKI tree (also known as branches), you must remember that ISE's CA by itself is three branches deep on its own. Many enterprise CAs allow the administrator to limit the depth of the PKI tree, so an adjustment to the policy may be required before you can sign ISE's certificate with the existing PKI.

To help illustrate the tree depth, [Figure D-16](#) shows the logical tree of the illustration in D-15.



**Figure D-16 PKI Hierarchy Illustrated**

Notice in [Figure D-16](#) that the P-PAN may be a single physical ISE node, but it acts as three separate CAs: root, node, and endpoint CA. The secondary PAN is a single physical node, but it acts as two separate CAs: node and endpoint. All nodes descend from a single root of the PKI tree.

Although the PKI design may look complex, ISE truly simplifies the configuration. To configure ISE to be a subordinate CA to an existing PKI, follow these steps:

**Step 1.** Navigate to **Administration > System > Certificates > Certificate Management > Certificate Signing Requests.**

**Step 2.** Click **Generate Certificate Signing Requests (CSR).**

**Step 3.** From the Usage drop-down list, choose **ISE Intermediate CA**, as shown in [Figure D-17](#).

The screenshot shows the 'Certificate Signing Request' dialog box. The 'Usage' dropdown menu is open, showing the option 'ISE Intermediate CA' selected. Other options listed include 'ISE Root CA', 'ISE Intermediate CA', and 'Renew ISE OCSP Responder Certificate'. The dialog also contains sections for 'ISE Identity Certificates' and 'ISE Certificate Authority Certificates'.

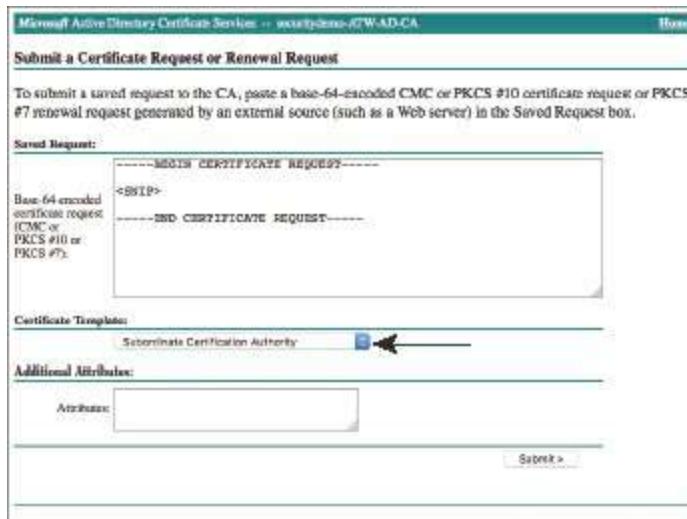
**Figure D-17 Generating the Intermediate CA Certificate Signing Request**

**Step 4. Click Generate.**

The CSR that is generated is requesting a certificate with permissions to sign

certificates (a CA certificate), not an end-entity certificate like the BYOD. You will take the CSR to whichever CA you wish to become subordinate to. If the example in [Figure D-17](#) were real, you would take the CSR to the certificate portal on the subordinate Microsoft CA, not the root. It all depends on what level of the existing PKI tree you want the ISE branch to start at.

Figure D-18 shows an example certificate portal on a Microsoft CA signing the intermediate CA CSR that was exported from ISE.



**Figure D-18** Signing the Intermediate CA Certificate Signing Request

Now that you know how to make ISE subordinate to an existing PKI, ask yourself: “Why do I want to?” One reason is that any client that already trusts the root certificate authority of the existing PKI will now trust the certificates signed by one of its subordinates. Therefore, ISE issued certificates are automatically trusted. However, as you read in [Chapter 17](#), that is not how it works with trust chains for EAP. The network client on the endpoint has to explicitly trust the certificates of the EAP servers before an EAP exchange will occur, unless that list of trusted certificates was provided by an MDM or similar management solution.

Being part of the same PKI hierarchy does not mean that the CAs share their issued certificate databases, or revocation status. The ISE database will remain separate from the Microsoft one, and any Microsoft CRL or OCSP databases will not get the list of certificates that ISE has issued or revoked. There are no APIs in existence today to make CAs of different vendors share the data.

Due to the separate certificate databases and because the ISE CA is very specific to BYOD, network authentication, and pxGrid, it is a more common practice to leave the ISE PKI hierarchy as standalone, and not join it to the existing PKI.

## Backing Up the Certificates

Backing up certificates is a very controversial topic in the PKI community. The general security guideline would frown on any situation where a private key is exposed. Public certificates are designed to be passed around, and it shouldn't matter who has a copy of them, but the private key must remain private.

Within the certificate authority, the signing keys should always be stored in an encrypted database, perhaps even within a hardware security module (HSM). The use of HSMs is deemed the ultimate method of securing your private keys, and HSMs are used for the Internet roots as well as many enterprises. An HSM is a piece of hardware that stores digital keys in a nonreversible encrypted storage.

Although the ISE CA stores the private keys within a key storage database that leverages very strong encryption, it does not yet make use of HSMs. Therefore, it is not possible to simply detach the HSM housing the root key and store it in a safe.

The keys used by the ISE CA to sign certificates are not backed up as part of the normal ISE backup process. What ISE does provide is a separate mechanism to extract the certificate and private key pairs for the CA in an encrypted bundle, which can then be imported back into a restored ISE node.

It is up to you, the administrator, to ensure those private keys remain secure once they are outside of ISE's secured storage. One idea is to use an encrypted USB drive that is locked away in a physical vault.

To back up the certificate authority key pairs:

**Step 1.** Connect to the ISE console, or SSH to the ISE node.

**Step 2.** Issue the **application configure ise** command.

**Step 3.** Choose **[7]Export Internal CA Store**.

**Step 4.** Type the name of the ISE repository to export the encrypted bundle to.

**Step 5.** Provide an encryption key (passphrase) for encrypting and decrypting the bundle.

[Example D-1](#) shows the exporting of keys from an ISE node.

### **Example D-1 Exporting Keys from an ISE Node**

[Click here to view code image](#)

```
woland-ise/admin# application configure ise
```

```
Selection ISE configuration option
```

- [1]Reset M&T Session Database
- [2]Rebuild M&T Unusable Indexes
- [3]Purge M&T Operational Data

```
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Exit
```

## 7

```
Export Repository Name: Synology
Enter encryption-key for export: [redacted]
log4j:WARN No appenders could be found for logger
(org.springframework.core.env.StandardEnvironment).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig
for more info.

Integritycheck Openssl digest output from verification with Swims
release key: Verified OK

Integritycheck Output: Verified signature of integritycheck program
with Swims release key

Integritycheck Output: Verified signature of integritycheck.sums file
with Swims release key
```

```
Integritycheck PASSED
Inside Session facade init
node-config.rc has been modified - rebuilding active properties file
PlatformProperties whoami: root

PlatformProperties show inventory: Process Output:
```

```
Getting profile properties for profile 'ibmLarge' and persona
'standalone'
```

```
In the init method of PDPFacade  
Time taken for NSFAdminServiceFactory to load4158  
Export in progress...
```

The following 5 CA key pairs were exported to repository 'Synology' at 'ise\_ca\_key\_pairs\_of\_woland-ise':

```
Subject:CN=Certificate Services Root CA - woland-ise  
Issuer:CN=Certificate Services Root CA - woland-ise  
Serial#:0x769a465c-342c4a7b-a529bf09-f3e5720c
```

```
Subject:CN=Certificate Services Node CA - woland-ise  
Issuer:CN=Certificate Services Root CA - woland-ise  
Serial#:0x4bfc93d9-e0b147a7-a1955f9e-e2041967
```

```
Subject:CN=Certificate Services Endpoint Sub CA - woland-ise  
Issuer:CN=Certificate Services Node CA - woland-ise  
Serial#:0x25f246b9-0efe419a-9fe27fc6-df9c4f12
```

```
Subject:CN=Certificate Services Endpoint RA - woland-ise  
Issuer:CN=Certificate Services Endpoint Sub CA - woland-ise  
Serial#:0x6e1d8208-3c2647fa-9fdbcb4-2f732ba0
```

```
Subject:CN=Certificate Services OCSP Responder - woland-ise  
Issuer:CN=Certificate Services Node CA - woland-ise  
Serial#:0x2f5ba187-4eb4452f-8a35c3b7-fa6d9548
```

ISE CA keys export completed successfully

```
Selection ISE configuration option  
[1]Reset M&T Session Database  
[2]Rebuild M&T Unusable Indexes  
[3]Purge M&T Operational Data  
[4]Reset M&T Database  
[5]Refresh Database Statistics  
[6]Display Profiler Statistics  
[7]Export Internal CA Store  
[8]Import Internal CA Store
```

```
[9]Create Missing Config Indexes  
[10]Create Missing M&T Indexes  
[11]Enable/Disable ACS Migration  
[12]Generate Daily KPM Stats  
[13]Generate KPM Stats for last 8 Weeks  
[14]Enable/Disable Counter Attribute Collection  
[15]View Admin Users  
[16]Get all Endpoints  
[17]Exit
```

17

```
woland-ise/admin#
```

**Note** The keys exported and backed up through this process are the CA key pairs, not the certificates that have been signed and issued to endpoints. Those public certificates are backed up as part of the normal ISE backup process.

## Issuing Certificates from the ISE CA

As you saw in [Chapter 17](#), the ISE CA is capable of delivering certificates directly to the BYOD endpoints during the onboarding phase. In fact, there are default out-of-the-box rules and certificate templates within ISE that leverage the internal CA without your having to configure much of anything.

You saw in [Chapter 25](#) that the ISE CA is also capable of providing certificates to pxGrid participants using the pxGrid user interface, as shown in [Figure D-19](#). ISE also automatically issues those pxGrid certificates to ISE nodes in the cube.

Connected to pxGrid atw-ise241.securitydemo.net (secondary: atw-ise237)

**Figure D-19** Issuing pxGrid Certificates from the pxGrid Admin UI

In addition to the methods already listed, ISE is also able to provide certificates through a web-based portal, for those devices that cannot participate in the BYOD onboarding flows (such as Windows Mobile and IoT devices).

The portal can be configured for any network user to provision themselves a certificate, or for an ISE SuperAdmin to provision certificates for anyone at all. To configure the portal:

**Step 1.** Navigate to **Administration > Device Portal Management > Certificate Provisioning.**

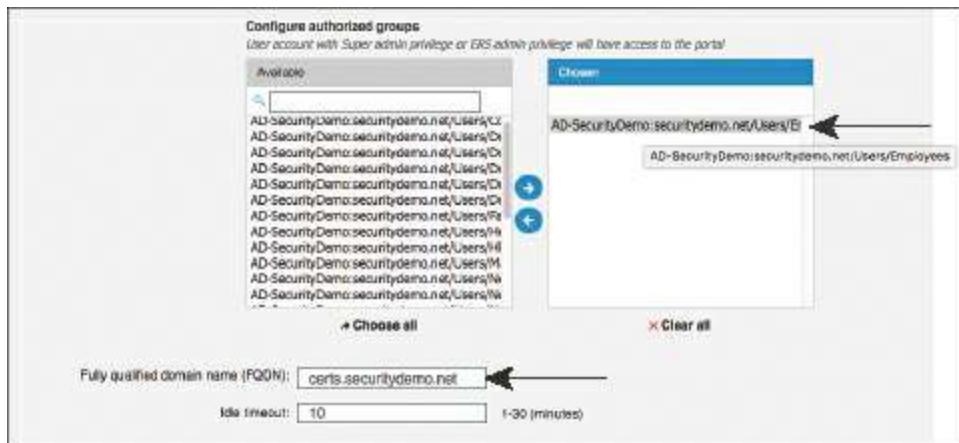
**Step 2.** Edit the **Certificate Provisioning Portal (default)** or create a new one.

The Certificate Provisioning Portal leverages the same portal framework as all the other client-facing portals within ISE. Therefore, it is fully customizable. The port, interfaces, and certificate used are all configurable. You can change out the look and feel to brand the portal as you wish for your organization.

By default, there are no groups permitted to access the portal.

**Step 3.** Within the Portal Settings section, under Configure Authorized Groups, select from the list on the left each group that should be able to access this portal, and move that group to the right side of the widget by clicking the right-facing arrow,

as shown in [Figure D-20](#).



**Figure D-20** Authorizing Groups to Access the Portal

**Step 4.** Provide a friendly name for the FQDN, also shown in [Figure D-20](#), which is required to access the portal.

**Step 5.** Expand the Certificate Portal Settings section, and select one or more certificate templates to allow users of this portal to issue certificates for, as shown in [Figure D-21](#).

For example, perhaps this portal is for pxGrid certificates only, or this portal was added for endpoint certificates only.

The screenshot shows the 'Portal & Page Settings' section of the 'Certificate Provisioning' tab. At the top, there are two sections: 'Guest Experience Settings' for the first portal and 'Guest Experience Settings' for the second portal. Below these, the 'Portal & Page Settings' section has several expandable categories: 'Portal Settings', 'Login Page Settings', 'Acceptable Use Policy (AUP) Page Settings', 'Post-Login Banner Page Settings', 'Change Password Settings', and 'Certificate Portal Settings'. Under 'Certificate Portal Settings', the 'Certificate Templates:' dropdown is expanded, showing two options: 'pxGrid\_Certificate\_Template' and 'EAP\_Authentication\_Certificate\_Template'. The 'pxGrid\_Certificate\_Template' option is currently selected and highlighted with a blue background.

## **Figure D-21** Selecting the Certificate Templates for the Portal

### **Step 6. Click Save.**

To issue or sign certificates from the portal:

### **Step 7.** Navigate to the friendly FQDN that you defined previously in Step 4.

### **Step 8.** Log in to the portal.

### **Step 9.** Select the action you wish to pursue.

The portal allows you to create a single certificate with and without a CSR, or to generate bulk certificates using a CSV file. If you choose to create a certificate without a CSR, then ISE must also generate the private key and have the portal user download the resulting public/private key pair.

### **Step 10.** Provide a Common Name (CN) for the certificate. This is a mandatory field.

### **Step 11.** Provide the endpoint MAC address. This is also a mandatory field, as the MAC address is required for all endpoint certificates, and will be entered into the SAN of the certificate.

### **Step 12.** Choose the certificate template to leverage for the certificate creation.

### **Step 13.** Pick your download format.

Different endpoints will be able to work with different formats. The ISE CA tries to be as flexible as possible.

### **Step 14.** Because this request will include a private key, a password to use for the encryption is required. Enter the password in the Password field.

### **Step 15. Click Generate.**

Figure D-22 illustrates the portal login screen, and [Figure D-23](#) shows an example portal being filled out.

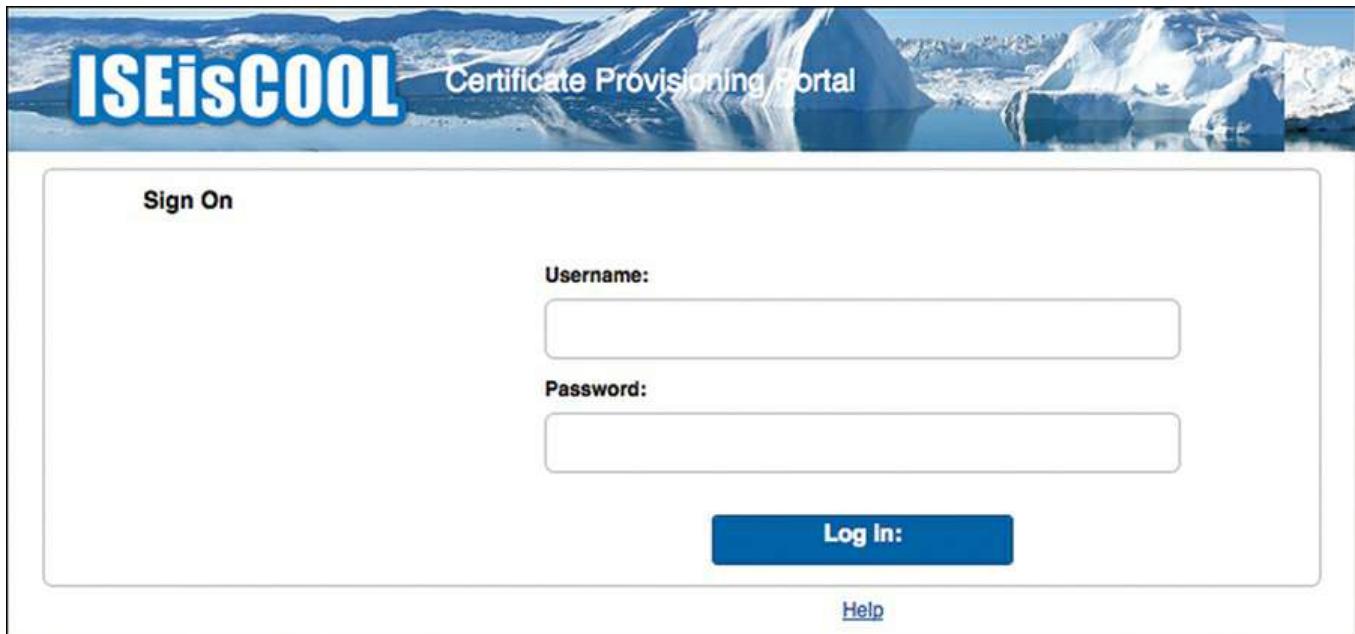


Figure D-22 Portal Login Screen

This screenshot shows the 'Certificate Provisioning' configuration page. The 'I want to:' dropdown is set to 'Generate a single certificate (without a certificate chain)'. The 'Common Name (CN)' field contains 'ATW-Win10Mobile'. The 'MAC Address:' field contains 'E4:98:D1:AB:4F:10'. The 'Choose Certificate Template:' dropdown is set to 'EAP\_Authentication\_Certificate\_Template'. The 'Description:' field contains 'Windows Mobile Cannot do SCEP'. The 'Certificate Download Format:' dropdown has a tooltip explaining four options: 'PKCS12 format, including certificate chain ...', 'PKCS12 format, including certificate chain (One file for both Certificate Chain and Key)', 'PKCS12 format (One file for both Certificate and Key)', and 'Certificates in PEM format, Key in PKCS8 PEM format, including certificate chain'. The 'Confirm Password:' field contains a redacted password. At the bottom are 'Generate' and 'Reset' buttons, and a 'Help' link.

Figure D-23 Selecting the Certificate Templates for the Portal



# Index

## Numbers

**802.1X**, [5](#), [31](#), [36](#)

agents, [42–43](#)

configuration

on C3PL switches, [220–221](#)

on Classic IOS/IOS 15.x switches, [204](#)

global commands

for C3PL switches, [220–221](#)

for Classic IOS/IOS 15.x switches, [204](#)

phased deployment, [524–525](#)

supplicants

choosing, [366–367](#)

Cisco AnyConnect Secure Mobility Client NAM, [377–381](#)

comparison of popular supplicants, [366–367](#)

configuration, [365–366](#)

definition of, [32](#), [42–43](#), [524](#)

Mac OS X 10.8.2 native supplicant, [367–369](#)

native supplicant provisioning, [365](#)

Windows 7, 8/8.1, and 10 native supplicants, [373–377](#)

Windows GPO configuration for wired supplicant, [369–373](#)

## A

**AAA (authentication, authorization, and accounting)**, [4](#), [9–10](#), [28](#). See also [auditing policy](#); [authentication](#); [authorization](#); [device administration](#)

AAA tests, [488–490](#)

AV (attribute-value) pairs, [20](#)

configuration on switches, [198–199](#)

credentials, [10](#)

global commands, [198–199](#)

network access, [12](#)

RADIUS, [17–20](#), [32](#)

AV (attribute-value) pairs, [20](#)

C3PL switch configuration, [217–219](#)

Classic IOS switch configuration, [199–201](#)

CoA (Change of Authorization), [20–21](#)  
compared to TACACS+[21](#)  
global commands, [199–203](#), [217–220](#)  
IOS 15.x switch configuration, [201–202](#)  
Live Logs, [666–667](#), [686–696](#)  
Live Sessions views, [666–667](#)  
messages, [18–20](#)  
RADIUS probe, [74](#)  
RADIUS probes, [142–143](#)  
service types, [18](#)  
use cases, [17–18](#)  
WLC (Wireless LAN Controller) configuration, [226–229](#)

TACACS+[13–21](#)  
command sets, [733–734](#)  
enabling, [726–727](#)  
profiles, [734–736](#)  
troubleshooting, [685](#)  
active troubleshooting, [688–696](#)  
high-level troubleshooting flowchart, [697](#)  
ISE logs, [701–703](#)  
log deduplication, [686–688](#)  
WebAuth and URL redirection, [697–701](#)

**aaa authorization config-commands command**, [751](#)

**AAA message**, [670](#)

**ACCEPT packet**, [14](#)

**acceptable use policy (AUP)**, [89–90](#)

**access control**, [27](#)

**access control entries (ACE)**, [251–253](#)

**access control lists.** See [ACLs \(access control lists\)](#)

**Access Control Server (ACS)**, [13](#)

**Access Registrar**, [13](#)

**Access Type field (authorization profiles)**, [254](#)

**Access-Accept messages**, [18](#)

**Access-Challenge messages**, [19](#)

**Access-Reject messages**, [19](#)

## **Access-Request messages, [18](#)**

accounting, [128–129](#). See also [AAA \(authentication, authorization, and accounting\)](#)  
accounting messages, [15–17](#), [19](#)  
importance of, [117–118](#)  
user accounting, [131–132](#)

## **Accounting-Request messages, [19](#)**

## **Accounting-Response messages, [20](#)**

### **accounts**

administrator accounts, [126–127](#)  
guest accounts  
    creating, [320](#)  
    managing, [320–321](#)

## **ACE (access control entries), [251–253](#)**

### **ACLs (access control lists), [7](#)**

    ACL bypass, [231–232](#)  
    Airespace ACLs, [229–232](#)  
    BYOD onboarding, [390–391](#)  
    creating  
        for C3PL switches, [219–220](#)  
        for Classic IOS/IOS 15.x switches, [202–203](#)

    dACLs (downloadable access control lists), [18](#), [36](#)

        configuration, [251–253](#)  
        creating, [496–499](#)  
        syntax checker, [253](#)  
        for wired guests, [310–311](#)

    ingress ACLs, [560–561](#)

    RA-VPN with posture flows, [496–499](#)

    SGACLs, traffic enforcement with, [588–591](#)

    VLAN ACL capture configuration, [157](#)

## **ACS (Access Control Server), [13](#)**

**active authentication.** See [authentication](#)

**Active Directory.** See [AD \(Active Directory\)](#)

## **Active Directory Run Time (ADRT) connector, [149](#)**

### **active troubleshooting**

    existing entry in Live Logs, [694–696](#)

no Live Log entries exist, [689–694](#)

steps for, [686–689](#)

## AD (Active Directory)

identity stores, [304–305](#)

multi-forest Active Directory support, [29](#)

passive identities, learning about, [598–599](#)

ISE-PIC (Passive Identity Connector), [603–610](#)

Kerberos sniffing via SPAN, [610–611](#)

WMI (Windows Management Instrumentation), [599–603](#)

probes, [149–150](#)

## Adapter Status report, [115](#)

## Adaptive Network Control (ANC), [634–635, 664](#)

## Adaptive Security Appliance (ASA), [32, 467, 621–622](#)

addresses (MAC). See [MAC addresses](#)

AD-Host-Exists attribute, [149](#)

AD-Join-Point attribute, [149](#)

Admin nodes, [55](#)

administration. See [device administration](#)

Administration persona, [43](#)

administrator accounts, creating, [126–127](#)

Administrator Change Configuration Audit report, [130](#)

AD-Operating-System attribute, [150](#)

AD-OS-Version attribute, [150](#)

ADRT (Active Directory Run Time) connector, [149](#)

AD-Service-Pack attribute, [150](#)

Advanced Malware Protection (AMP), [6, 663](#)

agent configuration file (ISE-PIC), [609](#)

agents, [42–43](#)

AireOS features (WLCs), [225–226](#)

Airespace ACLs, [229–232](#)

alarms, [672](#). See also [monitoring tools](#)

ALL role, [760](#)

ALL\_ACCOUNTS group, [308](#)

AMP (Advanced Malware Protection), [6, 663](#)

AMP Enabler module, [469](#)

**ANC (Adaptive Network Control), [634–635, 664](#)**

**Android**

BYOD onboarding, [401–408](#)

onboarding flow, [425–428](#)

**Anycast HA (high availability), [456–459, 614](#)**

**AnyConnect**

AnyConnect Agent with ISE Compliance Module, [339](#)

client provisioning policy, [343](#)

configuration file creation, [341–342](#)

Apex license, [45–46](#)

Compliance Module, [43](#)

connection profiles, [473–478](#)

Headend packages, [469–470](#)

Posture Agent, [91–95](#)

Secure Mobility Client NAM, [377–381](#)

**Apex license, [45–46](#)**

**Apple iOS onboarding, [394–401](#)**

application upgrade cleanup command, [719](#)

application upgrade prepare command, [719](#)

application upgrade proceed command, [719–720](#)

**architecture (ISE), [23](#). See also [deployment](#); [ISE-enabled network design](#)**

authorization rules, [33–34](#)

centralized policy control operation, [23–26](#)

endpoint components, [42–43](#)

features and benefits, [3–5, 26–30](#)

infrastructure components

feature-to-functionality mapping, [37](#)

functionality of, [36–37](#)

recommended components, [41](#)

role of, [35–36](#)

supported components, list of, [37–41](#)

ISE personas, [43–45](#)

licensing, [45–46](#)

node types, [43–45](#)

performance, [47–48](#)

platform support and compatibility, [30](#)

policy components, [42](#)

policy construct, [30–33](#)

policy-based structure, [48–49](#)

requirements, [46–47](#)

## **ASA (Adaptive Security Appliance), [32](#), [467](#), [621–622](#)**

### **assigning**

SGTs (Security Group Tags), [566–568](#)

VLANs, [558–560](#)

### **attributes**

for access control entries (ACE), [251–253](#)

AD-Host-Exists, [149](#)

AD-Join-Point, [149](#)

AD-Operating-System, [150](#)

AD-OS-Version, [150](#)

AD-Service-Pack, [150](#)

endpoint attributes, filtering, [182–183](#)

EndPointPolicy, [187](#)

MDM (mobile device management), [430–431](#)

NetFlow probes, [546](#)

saving for reuse, [295–297](#)

### **attribute-value (AV) pairs, [253](#)**

### **auditing policy**

audit logs

collection of, [128–129](#)

ensuring integrity and confidentiality of, [129](#)

logging categories, [128](#)

regular audit data review, [129](#)

remote logging targets, [129](#)

importance of, [117–118](#)

PCI DSS (Payment Card Industry Data Security Standard), [118–126](#)

simplification of, [25](#)

unique username and password enforcement, [126–128](#)

user accounting, [128–129](#)

### **AUP (acceptable use policy), [89–90](#), [338](#)**

### **authenticated guest access, [33](#)**

**authentication**, [4](#), [9–10](#), [28](#), [258–261](#). See also [AAA \(authentication, authorization, and accounting\)](#); [passive authentication](#); [suplicants](#)

authenticated guest access, [33](#)

authentication servers, [32](#)

authenticators, [32](#)

AV (attribute-value) pairs, [20](#)

certificate-based

authenticating VPN with certificates, [515–518](#)

connecting to VPN via CertProfile, [518–519](#)

provisioning certificates, [509–515](#)

compared to authorization, [257–258](#)

configuration on switches, [211–213](#)

credentials, [10](#)

definition of, [10](#)

device administration, [11](#), [28](#)

double authentication, [507–508](#)

Flex-Auth (Flexible Authentication), [208–211](#)

network access, [12](#)

open authentication, [524–525](#)

policies, [310](#)

allowed protocols, [266–271](#)

alternative ID stores based on EAP type, [278–280](#)

conditions, [263–266](#)

definition of, [78](#)

goals of, [261–262](#)

guest post-authentication, [312](#)

guest pre-authentication, [310–312](#)

identity store, [271–272](#)

policy sets, [258–260](#)

processing of, [262–263](#)

RA-VPN example, [277](#)

wireless SSID example, [272–276](#)

troubleshooting, [685](#)

active troubleshooting, [688–696](#)

high-level troubleshooting flowchart, [697](#)

ISE logs, [701–703](#)

log deduplication, [686–688](#)  
WebAuth and URL redirection, [697–701](#)

VPNs (virtual private networks), [5](#)  
web authentication, [32](#), [36](#)

**authentication display legacy command**, [213](#)

**authentication messages**, [14–15](#)

**authentication open command**, [523](#), [526](#), [530](#)

**authentication servers**, [32](#)

**Authentications Summary report**, [131](#)

**authenticators**, [32](#). See also [supplicants](#)

**authorization**. See also [AAA \(authentication, authorization, and accounting\)](#); [CoA \(Change of Authorization\)](#)

- authorization profiles
  - configuration, [253–255](#)
  - RA-VPN with posture flows, [499–500](#)
- Authorization Results, [251–255](#)
  - compared to authentication, [257–258](#)
  - definition of, [10](#)
- device admin AAA with Cisco IOS
  - Helpdesk profile, [745–746](#)
  - NetAdmin profile, [740–742](#)
  - NetOps profile, [742–743](#)
  - policy sets, [747–749](#)
- policies, [78](#), [247–251](#), [310](#)
  - authorization based on posture compliance, [360–361](#)
  - authorization profiles, [253–255](#)
  - Authorization Results, [251](#)
  - BYOD onboarding, [422–423](#)
  - conditions, [249–250](#)
  - dACLs (downloadable access control lists), [251–253](#)
  - employee and corporate machine full-access rule, [286–288](#)
  - employee limited access rule, [292–295](#)
  - goals of, [280](#)
  - guest post-authentication, [312](#)
  - guest pre-authentication, [310–312](#)
  - Internet only for mobile devices, [288–292](#)

policy rules, [247–251](#)  
policy sets, [247–248](#)  
posture client provisioning, [359–360](#)  
processing of, [280–286](#)  
profiles in, [183–187](#)  
RA-VPN with posture flows, [501](#)  
rules, [286](#)  
saving attributes for reuse, [295–297](#)  
profiles, [421–422](#)  
roles, [111](#)  
rules, [33–34, 87–89](#)  
TACACS+ messages, [15–17](#)  
troubleshooting, [685](#)  
    active troubleshooting, [688–696](#)  
    high-level troubleshooting flowchart, [697](#)  
    ISE logs, [701–703](#)  
    log deduplication, [686–688](#)  
    WebAuth and URL redirection, [697–701](#)

## **Authorization Results, [251](#)**

    authorization profiles, [253–255](#)  
    dACLs (downloadable access control lists), [251–253](#)

## **auto PAN (Policy Administration Node) failover, [449–450](#)**

## **AV (attribute-value) pairs, [20, 253](#)**

## **B**

### **backups, [462](#)**

### **bandwidth**

    centralized deployment, [54](#)  
    distributed deployment, [56–57](#)

### **Base license, [45–46](#)**

### **benefits of Cisco ISE (Identity Services Engine), [3–5, 26–30](#)**

### **Blacklist Identity Group, [185–186](#)**

### **bootstrapping. See [configuration](#)**

### **Bring Your Own Device (BYOD) Wizard, [67–69](#)**

### **business-based access, [25](#)**

### **business-policy enforcement, [26](#)**

## **BYOD onboarding, 27, 386**

accelerating, 25

Android onboarding flow, 425–428

dual SSID, 387

end-user experience, 393–394

  dual-SSID onboarding with Android, 401–408

  single-SSID onboarding with Apple iOS, 394–401

iOS onboarding flow, 423–425

ISE configuration, 392–393

  authorization policy rules, 422–423

  authorization profiles, 421–422

  certificate template, 411–413

  client provisioning policy, 413–415

  default unavailable client provisioning policy action, 420–421

  native supplicant profile, 408–411

  WebAuth portals, 415–420

NADs (network access devices)

  required ACLs (access control lists), 390–391

  URLs, adding to ACL\_WEAUTH\_REDIRECT, 392

  WLC (Wireless LAN Controller) configuration, 388–390

single SSID, 387–388

Windows and Mac OS onboarding flow, 428–429

## **BYOD Wizard, 67–69**

# C

## **C3PL switch configuration, 196, 213–215**

ACLs (access control lists), 219–220

certificates, 216–217

differentiated authentication, 214

global 802.X commands, 220–221

global RADIUS commands, 217–219

local service templates, 219–220

policies, 222–224

## **CA (certificate authority), 4, 28, 439, 638**

## **capabilities of Cisco ISE (Identity Services Engine), 3–5, 23–26**

**Catalyst switches.** See [switches](#)

**CDA (Context Directory Agent), [594](#), [616](#)**

**CDA-RADIUS, [617](#)**

**CD-ROM repositories, [712](#)**

**Central Web Authentication. See [CWA \(Central Web Authentication\)](#)**

**centralized deployment**

bandwidth guidance, [54](#)

considerations for, [53](#)

diagram of, [52–53](#)

**centralized management, [26](#)**

**centralized policy**

advantages of, [6–7](#)

Cisco ISE operation, [23–26](#)

**certificate authority. See [CA \(certificate authority\)](#)**

**certificates**

certificate-based authentication

authenticating VPN with certificates, [515–518](#)

connecting to VPN via CertProfile, [518–519](#)

provisioning certificates, [509–515](#)

configuration

for C3PL switches, [216–217](#)

on Classic IOS/IOS 15.x switches, [196–197](#)

importing, [440](#)

provisioning, [509–515](#)

renewing for EAP-TLS, [271](#)

templates, [411–413](#)

**certifications, [30](#)**

**CertProfile, [518–519](#)**

**chaining (EAP), [436–437](#)**

**Challenge Handshake Authentication Protocol (CHAP), [12](#)**

**Change Configuration Audit report, [162](#)**

**Change of Authorization. See [CoA \(Change of Authorization\)](#)**

**CHAP (Challenge Handshake Authentication Protocol), [12](#), [268](#)**

**Cisco Access Registrar, [13](#)**

**Cisco Adaptive Security Appliance. See [ASA \(Adaptive Security Appliance\)](#)**

**Cisco Advanced Malware Protection. See [AMP \(Advanced Malware Protection\)](#)**

**Cisco AnyConnect.** See [AnyConnect](#)

**Cisco Catalyst switches.** See [switches](#)

**Cisco Context Directory Agent (CDA),** [594](#), [616](#)

**Cisco Firepower Management Center (FMC).** See [FMS \(Firepower Management Center\)](#)

**Cisco Firepower Threat Defense (FTD),** [467](#)

**Cisco IOS.** See [IOS \(Cisco\)](#)

**Cisco ISE (Identity Services Engine).** See [ISE-enabled network design](#)

**Cisco NAC Appliance,** [24](#)

**Cisco NGFW,** [6](#)

**Cisco Platform Exchange Grid.** See [pxGrid \(Platform Exchange Grid\)](#)

**Cisco Rapid Threat Containment,** [29](#), [632–635](#)

**Cisco Secure Access Control Server (ACS),** [13](#)

**Cisco Stealthwatch.** See [Stealthwatch](#)

**Cisco Terminal Services (TS) Agent,** [615](#)

**Cisco TrustSec.** See [TrustSec](#)

**Cisco Wireless LAN Controller.** See [WLCs \(Wireless LAN Controllers\)](#)

**classes, control,** [222–223](#)

**Classic IOS switch configuration,** [196](#)

- ACLs (access control lists), [202–203](#)
- authentication settings, [211–212](#)
- authentication timers, [212](#)
- certificates, [196–197](#)
- Flex-Auth (Flexible Authentication), [208–211](#)
- global 802.X commands, [204](#)
- global AAA commands, [198–199](#)
- global logging commands, [204–205](#)
- global profiling commands, [205–207](#)
- global RADIUS commands, [199–202](#)
- HTTP/HTTPS server, [197](#)
- Monitor Mode, [213](#)
- native SGT propagation, [582–584](#)
- switch port interfaces, [208](#)

**classification of SGTs (Security Group Tags),** [565–566](#)

**client address pools, assigning,** [481–484](#)

**client posture assessment.** See [posture assessment](#)

**client provisioning policy**

configuration, [413–415](#)

default unavailable client provisioning policy action, [420–421](#)

**client provisioning portal,** [343–344](#)

**client supplicants.** See [supplicants](#)

**client-based remote access VPNs**

configuration

AnyConnect connection profiles, [473–478](#)

AnyConnect Headend packages, [469–470](#)

client address pool, [481–484](#)

configuration tools, [469–470](#)

Headend preparation, [471–473](#)

ISE configuration, [487–488](#)

network reachability tasks, [484–487](#)

PSNs (Policy Service Nodes), [478–481](#)

security services modules, [468–469](#)

connecting to, [490–491](#)

overview of, [467–468](#)

testing

AAA test, [488–490](#)

connecting to VPN, [492–494](#)

logging in to web portal, [490–491](#)

**clientless remote access VPNs,** [466–467](#)

**Closed Mode,** [532–534](#)

**CoA (Change of Authorization),** [20–21, 36, 179–180](#)

COA Events report, [115](#)

CoA menu, [663–665](#)

CoA-Push, [477, 496](#)

CoA-ReAuth, [477](#)

conditions producing, [550–551](#)

configuration, [552–553](#)

exceptions, [552](#)

global CoA, [180–181](#)

per-profile CoA, [181](#)

types of, [551–552](#)

**Cognitive Threat Analysis (CTA),** [663](#)

**CollectData SGT (Security Group Tag),** [194](#)

**command sets,** [21](#), [733–734](#)

**commands**

802.1X commands, [204](#), [220–221](#)

aaa authorization config-commands, [751](#)

AAA commands, [198–199](#)

application upgrade cleanup, [719](#)

application upgrade prepare, [719](#)

application upgrade proceed, [719–720](#)

authentication display legacy, [213](#)

authentication open, [523](#), [526](#), [530](#)

cts role-based sgt-map, [569](#)

cts role-based sgt-map vlan-list, [569](#)

epm logging, [669](#)

interface range, [208](#)

ip dhcp relay ISE\_PSN\_address, [75](#)

ip domain-name, [197](#)

ip helper-address, [153–156](#)

ip helper-address ISE\_PSN\_address, [74](#)

ip http secure-server, [197](#)

ip http server, [197](#)

ip radius source-interface, [669](#), [690](#), [693](#)

ip tacacs source-interface, [669](#)

logging commands, [204–205](#)

logging source-interface, [669](#)

monitor session, [156](#)

nslookup, [700](#)

ping, [700](#)

profiling commands, [205–207](#)

RADIUS commands, [199–203](#), [217–220](#)

radius-server load-balance, [459](#)

service-policy, [224](#)

show aaa server, [459](#)

show application status ise, [441–442](#)

show authentication session interface, [691–692](#), [693–694](#), [698](#)

show device-sensor, [191](#)  
show ip access-list interface, [700](#)  
show ip interface brief, [692](#)  
show privilege, [756](#)  
show repository, [713](#)  
show role feature, [778](#)  
show role feature-group, [778](#)  
show running-config, [710–711](#)  
show tech-support, [702](#)  
show vpn-sessiondb detail anyconnect, [503–506](#)  
source-interface, [669](#)  
switchport, [208](#)  
test aaa, [752](#)  
username, [751](#)

## **COMMANDS role, [760](#)**

### **committees (NASP), [79–81](#)**

**Common Classification Policy Language switches.** See [C3PL switch configuration](#)

### **Common Criteria, [30](#)**

### **Common Ports scan (NMAP), [146](#)**

### **Common Vulnerability Scoring System (CVSS), [111, 662](#)**

### **compliance, simplification of, [25](#)**

### **compound conditions, [249](#)**

### **conditions**

authentication policy, [263–266](#)  
authorization policy, [249–250](#)  
ISE profiler, [108–109](#)  
posture conditions, [345–349](#)

### **confidentiality of audit logs, [129](#)**

**configuration.** See also [NASP \(network access security policy\); onboarding; profiling](#)

802.1X supplicants, [365–366](#)

Cisco AnyConnect Secure Mobility Client NAM, [377–381](#)  
comparison of popular supplicants, [366–367](#)  
Mac OS X C10.8.2 native supplicant, [367–369](#)  
Windows 7, 8/8.1, and 10 native supplicants, [373–377](#)

Windows GPO configuration for wired supplicant, [369–373](#)  
alarms, [672](#)  
authorization policy, [247](#)  
    authorization profiles, [253–255](#)  
    Authorization Results, [251](#)  
    conditions, [249–250](#)  
    dACLs (downloadable access control lists), [251–253](#)  
    policy rules, [247–251](#)  
    policy sets, [247–248](#)  
authorization profiles, [253–255](#)  
auto PAN (Policy Administration Node) failover, [449–450](#)  
C3PL switches, [213–215](#)  
    ACLs (access control lists), [219–220](#)  
    certificates, [216–217](#)  
    differentiated authentication, [214](#)  
    global 802.X commands, [220–221](#)  
    global RADIUS commands, [217–219](#)  
    local service templates, [219–220](#)  
    policies, [222–224](#)  
Classic IOS/IOS 15.x switches  
    ACLs (access control lists), [202–203](#)  
    authentication settings, [211–212](#)  
    authentication timers, [212](#)  
    certificates, [196–197](#)  
    Flex-Auth (Flexible Authentication), [208–211](#)  
    global 802.X commands, [204](#)  
    global AAA commands, [198–199](#)  
    global logging commands, [204–205](#)  
    global profiling commands, [205–207](#)  
    global RADIUS commands, [199–202](#)  
    HTTP/HTTPS server, [197](#)  
    Monitor Mode, [213](#)  
    switch port interfaces, [208](#)  
client-based remote access VPNs  
    AnyConnect connection profiles, [473–478](#)  
    AnyConnect Headend packages, downloading, [469–470](#)

client address pool, [481–484](#)  
configuration tools, [469–470](#)  
Headend preparation, [471–473](#)  
ISE configuration, [487–488](#)  
network reachability tasks, [484–487](#)  
PSNs (Policy Service Nodes), [478–481](#)  
security services modules, [468–469](#)  
testing, [488–494](#)

CoA (Change of Authorization), [552–553](#)  
dACLs (downloadable access control lists), [251–253](#)  
device admin AAA with Cisco IOS  
    Helpdesk profile, [745–746](#)  
    NAD (network access device) configuration, [749–752](#)  
    NetAdmin profile, [740–742](#)  
    NetOps profile, [742–743](#)  
    overview of, [739](#)  
    policy sets, [747–749](#)  
    testing and troubleshooting, [752–758](#)  
    user roles, [739–740](#)

device admin AAA with Cisco Nexus switches, [777](#)  
    Helpdesk profile, [781–782](#)  
    NetAdmin profile, [779–780](#)  
    NetOps profile, [780–781](#)  
    network device preparation, [778–779](#)  
    policy sets, [782–783](#)  
    SecAdmin profile, [781](#)  
    TACACS+, enabling, [783–784](#)  
    user roles, [777–778](#)

device admin AAA with Cisco WLC  
    Employee profile, [765–766](#)  
    Helpdesk profile, [765](#)  
    NetAdmin profile, [763–764](#)  
    network device preparation, [761–762](#)  
    overview of, [759–760](#)  
    policy sets, [766–768](#)  
    SecAdmin profile, [764](#)

TACACS+, enabling, [768–770](#)  
testing and troubleshooting, [770–775](#)

Device Administration Work Center, [728–729](#)  
    Connection settings, [729](#)  
    Device Admin Policy Sets, [736–738](#)  
    Ext ID Sources, [732](#)  
    Identities, [731–732](#)  
    navigation UI, [730–731](#)  
    Network Resources, [733](#)  
    Password Change Control settings, [729](#)  
    Policy Elements, [733–736](#)  
    Reports, [738](#)  
    Session Key Assignment settings, [729–730](#)  
    User Identity Groups, [731–732](#)

device configuration for monitoring, [669–670](#)

guest services  
    guest accounts, [320–321](#)  
    guest post-authentication authorization policy, [312](#)  
    guest pre-authentication authorization policy, [310–312](#)  
    hotspot guest portals, [302–303](#)  
    sponsored guest portals, [302–318](#)

ISE for wireless, [59–60](#)  
    BYOD (Bring Your Own Device) Wizard, [67–69](#)  
    Guest Self-Registration Wizard, [61–65](#)  
    Secure Access Wizard, [65–67](#)  
    Wireless Setup Wizard home page, [59–60](#)

ISE nodes in distributed environment, [439–440](#)  
    node personas and roles, [445](#)  
    node registration, [442–445](#)  
    primary PANs, [440–442](#)

ISE to gain visibility, [69](#)  
    DHCP probe, [74–75](#)  
    RADIUS probe, [74](#)  
    SNMPQUERY probe, [73–74](#)  
    Visibility Setup Wizard, [69–73](#)

NetFlow probes, [548–550](#)

Network Device Groups, [528–529](#)

node groups, [451–453](#)

policy sets, [529–530](#), [736–738](#)

posture assessment

AnyConnect Agent with ISE Compliance Module, [339–343](#)

AUP (acceptable use policy) enforcement, [338](#)

authorization policies, [359–361](#)

client provisioning portal, [343–344](#)

enabling in network, [362–363](#)

host application visibility and context collection, [357–358](#)

posture client provisioning global setup, [331–335](#)

posture conditions, [345–349](#)

posture elements, [345](#)

posture general settings, [335–336](#)

posture policy, [355–357](#)

posture reassessments, [336–337](#)

posture remediations, [349–353](#)

posture requirements, [353–355](#)

posture updates, [337](#)

probes, [138–139](#)

AD (Active Directory) probes, [149–150](#)

DHCP and DHCPSPAN probes, [141–142](#)

HTTP probes, [151](#)

NMAP probes, [144–147](#)

RADIUS probes, [142–143](#)

SNMPQUERY probe, [148–149](#)

SNMPTRAP probes, [148–149](#)

pxGrid (Platform Exchange Grid)

ISE, [639–642](#)

Stealthwatch, [652–657](#)

WSA (Web Security Appliance), [649–652](#)

remote logging targets, [129](#)

repositories, [671–672](#), [708–713](#)

SGTs (Security Group Tags)

native tagging on Catalyst 6500, [584–586](#)

native tagging on Cisco IOS switches, [582–584](#)

native tagging on Nexus series switch, [586–587](#)

SXP (SGT Exchange Protocol)

- on Cisco ASA, [576–577](#)
- on IOS devices, [572–573](#)
- on ISE, [578–579](#)
- on wireless LAN controllers, [573–575](#)

Syslog providers, [612–614](#)

TACACS+[726–727](#)

triggered NetFlow, [191–194](#)

WLCs (Wireless LAN Controllers), [225](#)

- AireOS features, [225–226](#)
- Airespace ACLs, [229–232](#)
- Corporate SSID, [240–245](#)
- dynamic interfaces for client VLANs, [233–235](#)
- Guest WLAN, [236–240](#)
- RADIUS accounting servers, [227–228](#)
- RADIUS authentication servers, [226–227](#)
- RADIUS fallback, [229](#)

WMI (Windows Management Instrumentation), [599–603](#)

**configuration files, AnyConnect Agent**, [341–342](#)

**Configure WMI process**, [599–603](#)

**Connection Settings (Device Administration)**, [729](#)

**context**

- context collection, [357–358](#)
- context visibility
  - Context Visibility views, [663–665](#)
  - device profiling, [107–108, 169–178](#)
  - verification of, [190–191](#)
- context-based access, [25](#)
- contextual information, [6](#)
  - definition of, [31](#)

**Context Directory Agent (CDA)**, [594, 616](#)

**Context In integration**, [632](#)

**Context Sharing integration**, [632](#)

**CONTINUE packet**, [14–16](#)

**control classes**, [222–223](#)

## **control policies**

applying to interfaces, [224](#)  
configuration, [223–224](#)

## **CONTROLLER role, [760](#)**

**controllers, pxGrid (Platform Exchange Grid), [635](#)**

**Corporate SSID, [240–245](#)**

**corporate system identification, [436–437](#)**

**credentials, [10](#)**

**Critical MAB, [214](#)**

**CTA (Cognitive Threat Analysis), [663](#)**

**cts role-based sgt-map command, [569](#)**

**cts role-based sgt-map vlan-list command, [569](#)**

**Custom Ports scan (NMAP), [146](#)**

**customization. See [configuration](#)**

**CVSS (Common Vulnerability Scoring System), [111, 662](#)**

**CWA (Central Web Authentication), [299–301, 321–325](#)**

## **D**

**dACLs (downloadable access control lists), [18, 36](#)**

configuration, [251–253](#)  
creating, [496–499](#)  
syntax checker, [253](#)  
for wired guests, [310–311](#)

## **dashboards**

Summary, [660–661](#)  
Threat, [663](#)  
verification of profiles, [189–190](#)  
Vulnerability, [662](#)

**Data Access permissions, [127](#)**

**data repositories. See [repositories](#)**

**data sources for device profiling, [110–111](#)**

**Datagram Transport Layer Security (DTLS), [467](#)**

**debugging. See [troubleshooting](#)**

**decision matrix (NASP), [84–85](#)**

**deduplication of logs, [686–688](#)**

**Default Rule policies**, [249](#)

**deny statement**, [230](#)

**deployment**

centralized

- bandwidth guidance, [54](#)

- considerations for, [53](#)

- diagram of, [52–53](#)

device administration

- large deployments, [724–725](#)

- medium deployments, [725](#)

- small deployments, [726](#)

distributed, [55–57](#), [439](#)

- Anycast HA, [456–459](#)

- backup and restore, [462](#)

- bandwidth requirements, [56–57](#)

- Cisco IOS load balancing, [459](#)

- HA (high-availability) options, [446–453](#)

- ISE node configuration in, [439–445](#)

- load balancers, [453–455](#)

- maintaining, [460–462](#)

- Monitoring nodes in, [669](#)

- patches, [460–462](#)

- sample model, [55–56](#)

- when to use, [55](#)

host security posture assessment rules, [101](#)

ISE-PIC (Passive Identity Connector) Agent, [604–607](#)

phased approach, [521](#)

- 802.1X, [524–525](#)

- advantages of, [521–523](#)

- Closed Mode, [532–534](#)

- deployment process, [523–524](#)

- Low-Impact Mode, [530–532](#)

- Monitor Mode, [526–527](#)

- open authentication, [524–525](#)

- preparation for, [527–530](#)

- transition from Monitor Mode to end state, [534–535](#)

wireless networks, [535](#)

**Description field (authorization profiles)**, [254](#)

**design**. See [ISE-enabled network design](#)

device admin license, [723](#)

**Device Admin Policy Sets (Device Administration)**, [736–738](#)

device administration, [11](#), [28](#), [721–724](#). See also [device profiling](#)

device admin AAA with Cisco IOS

Helpdesk profile, [745–746](#)

NAD (network access device) configuration, [749–752](#)

NetAdmin profile, [740–742](#)

NetOps profile, [742–743](#)

overview of, [739](#)

policy sets, [747–749](#)

testing and troubleshooting, [752–758](#)

user roles, [739–740](#)

device admin AAA with Cisco Nexus switches, [777](#)

Helpdesk profile, [781–782](#)

NetAdmin profile, [779–780](#)

NetOps profile, [780–781](#)

network device preparation, [778–779](#)

policy sets, [782–783](#)

SecAdmin profile, [781](#)

TACACS+, enabling, [783–784](#)

user roles, [777–778](#)

device admin AAA with Cisco WLC

Employee profile, [765–766](#)

Helpdesk profile, [765](#)

NetAdmin profile, [763–764](#)

network device preparation, [761–762](#)

overview of, [759–760](#)

policy sets, [766–768](#)

SecAdmin profile, [764](#)

TACACS+, enabling, [768–770](#)

testing and troubleshooting, [770–775](#)

device admin license, [723](#)

device onboarding, [27](#)

device-profile feed service, [29](#)  
large deployments, [724–725](#)  
medium deployments, [725](#)  
monitoring, [669–670](#)  
NADs (network access devices), [727–728](#)  
security policy, [107](#)  
small deployments, [726](#)  
TACACS+, enabling, [726–727](#)  
TC-NAC (Threat-Centric Network Access Control)  
    authorization conditions, [112–113](#)  
    in incident response process, [113–116](#)  
    reports, [115–116](#)  
    software support, [111–112](#)  
Work Center, [728–729](#)  
    Connection settings, [729](#)  
    Device Admin Policy Sets, [736–738](#)  
    Ext ID Sources, [732](#)  
    Identities, [731–732](#)  
    navigation UI, [730–731](#)  
    Network Resources, [733](#)  
    Password Change Control settings, [729](#)  
    Policy Elements, [733–736](#)  
    Reports, [738](#)  
    Session Key Assignment settings, [729–730](#)  
    User Identity Groups, [732](#)  
**Device Administration license**, [45–46](#)  
**Device Logical Profiles**, [110](#)  
device posture, [6](#)  
**Device Profile Information worksheet**, [541](#)  
**device profiling**, [28](#)  
    authorization policy based on, [135–136](#), [183](#)  
    endpoint Identity Groups, [183–186](#)  
    EndPointPolicy, [187](#)  
    in authorization roles, [111](#)  
CoA (Change of Authorization), [179–180](#)  
    global CoA, [180–181](#)

per-profile CoA, [181](#)  
context visibility, [107–108](#)  
data sources, [110–111](#)  
evolution of, [136](#)  
global profiler settings  
    endpoint attribute filtering, [182–183](#)  
    NMAP Scan Subnet Exclusions, [183](#)  
    SNMP settings for probes, [182](#)  
how it works, [134–135](#)  
HTTP profiling without probes, [152](#)  
importance of, [133–134](#)  
importing profiles, [187–188](#)  
infrastructure configuration, [153](#)  
    device sensor, [157–159](#)  
    DHCP helper, [153–156](#)  
    ip helper-address commands, [153–156](#)  
    SPAN, [156](#)  
    VLAN ACL captures, [157](#)  
    VMware Promiscuous Mode vSwitch setting, [159](#)  
least-privilege strategy, [136](#)  
logical profiles, [110, 178–179](#)  
policies, [109–110, 160](#)  
    context visibility, [169–178](#)  
    definition of, [78](#)  
    endpoint profile policies, [167–169](#)  
    logical profiles, [178–179](#)  
    profiler feed service, [160–166](#)  
probes  
    AD (Active Directory) probes, [149–150](#)  
    configuration, [138–139](#)  
    definition of, [137](#)  
    DHCP probes, [140–142](#)  
    DHCPSPAN probes, [140–142](#)  
    DNS probes, [147](#)  
    HTTP probes, [150–152](#)  
    NetFlow probes, [152–153](#)

NMAP probes, [142–143](#)  
RADIUS probes, [142–143](#)  
SNMPQUERY probes, [148–149](#)  
SNMPTRAP probes, [148–149](#)  
profiler conditions, [108–109](#)  
profiler feed service  
    configuration, [160–161](#)  
    offline manual update, [164–166](#)  
    verification, [162–163](#)  
Profiler Work Center, [137](#)  
triggered NetFlow, [191–194](#)  
verification of profiles, [189](#)  
    context visibility, [190–191](#)  
    dashboard, [189–190](#)  
    device sensor show commands, [191](#)  
**device sensor, 205–207**  
    configuration, [157–159](#)  
    show commands, [191](#)  
**device-profile feed service, 29**  
**DHCP (Dynamic Host Configuration Protocol)**  
    DHCP probes, [74–75](#)  
        Cisco WLC considerations, [141](#)  
        configuration, [141–142](#)  
        overview of, [140](#)  
    DHCPSPAN probes  
        Cisco WLC considerations, [141](#)  
        configuration, [141–142](#)  
        overview of, [140–141](#)  
    infrastructure configuration, [153–156](#)  
**diagnostic tools, 674**  
    Endpoint Debug, [680–682](#)  
    Evaluate Configuration Validator, [675–678](#)  
    RADIUS Authentication Troubleshooting, [674–675](#)  
    Session Trace, [682–685](#)  
    TCP Dump, [678–680](#)  
**DIAMETER, 12**

**dictionaries**, [249–250](#)

**differentiated authentication**, [214](#)

**DIRECTION attribute**, [546](#)

**disk repositories**, [709](#)

**disk space requirements (ISE)**, [47](#)

**distinguished name (DN)**, [615](#)

**distributed deployment**

- Anycast HA, [456–459](#)
- backup and restore, [462](#)
- bandwidth guidance, [56–57](#)
- Cisco IOS load balancing, [459](#)
- HA (high-availability) options, [446](#)
  - MnT (Monitoring & Troubleshooting) nodes, [446–447](#)
  - node groups, [451–453](#)
  - PANs (Policy Administration Nodes), [446–447](#)
  - PSNs (Policy Service Nodes), [450–451](#)
- ISE node configuration, [439–440](#)
  - node personas and roles, [445](#)
  - node registration, [442–445](#)
  - primary PANs, [440–442](#)
- load balancers, [453–455](#)
- maintaining, [460–462](#)
- Monitoring nodes in, [669](#)
- patches, [460–462](#)
- sample model, [55–56](#)
- when to use, [55](#)

**DN (distinguished name)**, [615](#)

**DNS (Domain Name System) probes**, [147](#)

**DNS probes**, [147](#)

**documentation, posture requirements for**, [96–97](#)

**domains, security**, [85–87](#)

**double authentication**, [507–508](#)

**downloadable access control lists**. See [dACLs \(downloadable access control lists\)](#)

**downloading**

- AnyConnect Headend packages, [469–470](#)

ISE logs, [702–703](#)

**DTLS (Datagram Transport Layer Security), [467](#)**

**dual-SSID onboarding**

with Android, [401–408](#)

overview of, [387](#)

**Dubois, Jesse, [680, 682](#)**

**dynamic network access privileges, [102](#)**

## E

**EAP (Extensible Authentication Protocol), [12, 268](#)**

alternative ID stores based on EAP type, [278–280](#)

EAP chaining, [436–437](#)

EAP-FAST, [269](#)

EAP-FASTv2, [436–437](#)

EAP-MD5, [268](#)

EAP-TLS, [268–269, 271](#)

EAP-TTLS, [269](#)

PEAP (Protected EAP), [269](#)

**EAPoL (Extensible Authentication Protocol over LAN), [42–43](#)**

**Easy Connect, [5, 27](#)**

**ECC (elliptic curve cryptography), [412](#)**

**ecosystems. See [ISE ecosystems](#)**

**elliptic curve cryptography (ECC), [412](#)**

**EMM (enterprise mobility management)**

partners, [25](#)

triggered NetFlow, [192–194](#)

**employee and corporate machine full-access rule, [286–288](#)**

**employee authorization rule, [104–105](#)**

**employee dynamic interface, [233–234](#)**

**employee limited access rule, [292–295](#)**

**Employee profile, [765–766](#)**

**Endpoint Classification page (Visibility Setup Wizard), [72](#)**

**Endpoint Debug, [680–682](#)**

**Endpoint Protection Services (EPS), [632](#)**

**EndPointPolicy attribute, [187](#)**

## endpoints

Advanced Malware Protection (AMP) for Endpoints, [663](#)  
components, [42–43](#)  
context visibility, [169–178](#)  
custom profiles for, [538](#)  
    collecting information for, [541–542](#)  
    profiler conditions, [542–543](#)  
    profiler policies, [543–544](#)  
    unique values for unknown devices, [539–541](#)  
endpoint attribute filtering, [182–183](#)  
Endpoint Debug, [680–682](#)  
endpoint probe, [623–624](#)  
EndPointPolicy, [187](#)  
Endpoints view, [663–664](#)  
finding, [667–669](#)  
Identity Groups, [183–186](#)  
posture service, [29](#)  
profile policies, [167–169](#)

## Endpoints view, [663–664](#)

## end-user experience, [393–394](#)

dual-SSID onboarding with Android, [401–408](#)  
single-SSID onboarding with Apple iOS, [394–401](#)

## enforcement

AUP (acceptable use policy), [338](#)  
host security posture assessment rules, [98–101](#)  
NASP (network access security policy), [102–103](#)  
TrustSec, [587–588](#)  
    with security group firewalls, [591–592](#)  
    with SGACLs, [588–591](#)  
unique usernames and passwords, [126–128](#)

## Enforcement Policy Module (EPM), [669](#)

## enterprise mobility

accelerating, [25](#)  
EMM (enterprise mobility management), [25](#)

## EPM (Enforcement Policy Module), [669](#)

## epm logging command, [669](#)

**EPS (Endpoint Protection Services),** [632](#)  
**ERROR packet,** [14](#), [16](#)  
**Evaluate Configuration Validator,** [675–678](#)  
**Exception policies,** [248](#)  
**exceptions for CoA (Change of Authorization),** [552](#)  
**Ext ID Sources screen (Device Administration),** [732](#)  
**Extensible Authentication Protocol.** See [EAP \(Extensible Authentication Protocol\)](#)  
**Extensible Authentication Protocol over LAN (EAPoL),** [42–43](#)  
**Extensible Communication Platform (XCP),** [636](#)  
**Extensible Messaging and Presence Protocol (XMPP),** [636](#)  
**EZ Connect,** [628–630](#)

## F

**FAIL packet,** [16](#)  
**failover,** [449–450](#)  
**features of Cisco ISE (Identity Services Engine),** [26–30](#)  
**Federal Information Processing Standard (FIPS) 2,** [30](#), [140](#)  
**feed service (profiler),** [160](#)  
    configuration, [160–161](#)  
    offline manual update, [164–166](#)  
    verification, [162–163](#)  
**fields for authorization profiles,** [254–255](#)  
**File Transfer Protocol repositories,** [709](#)  
**files**  
    AnyConnect Agent configuration files, [341–342](#)  
    audit logs  
        collection of, [128–129](#)  
        ensuring integrity and confidentiality of, [129](#)  
        logging categories, [128](#)  
        regular audit data review, [129](#)  
        remote logging targets, [129](#)  
    ISE-PIC (Passive Identity Connector) Agent  
        agent configuration, [609](#)  
        nodes, [608](#)  
**filtering**

endpoint attributes, [182–183](#)  
Live Logs, [666](#)

**finding endpoints**, [667–669](#)

**FIPS (Federal Information Processing Standard)** [140–2](#), [30](#)

**Firepower Management Center**. See [FMC \(Firepower Management Center\)](#)

**Firepower Threat Defense (FTD)**, [467](#)

**firewalls**

- IDFW (identity firewalling), [32](#)
- traffic enforcement with, [591–592](#)

**Flex-Auth (Flexible Authentication)**, [208–211](#)

**FlexConnect**, [41](#)

**flow diagrams**

- Closed Mode, [533](#)
- high-level troubleshooting flowchart, [697](#)
- Low-Impact Mode, [531](#)
- Monitor Mode, [526](#), [527](#)
- phased deployment, [524](#)

**FMC (Firepower Management Center)**, [619–620](#), [642–648](#)

**FMS (Firepower Management Center)**, [615](#), [619–620](#)

**FOLLOW packet**, [16](#)

**forwarding logs**, [610](#)

**FQDN (fully qualified domain name)**, [147](#), [454](#)

**FTD (Firepower Threat Defense)**, [467](#)

**FTP (File Transfer Protocol) repositories**, [709](#)

**fully qualified domain name (FQDN)**, [147](#), [454](#)

## G

**Gash, Douglas**, [682](#), [723–724](#)

**global CoA (Change of Authorization)**, [180–181](#)

**global search**, [667–669](#)

**global settings**

- Device Administration Work Center, [728–729](#)
  - Connection settings, [729](#)
  - Device Admin Policy Sets, [736–738](#)
  - Ext ID Sources, [732](#)

Identities, [731–732](#)  
navigation UI, [730–731](#)  
Network Resources, [733](#)  
Password Change Control settings, [729](#)  
Policy Elements, [733–736](#)  
Reports, [738](#)  
Session Key Assignment settings, [729–730](#)  
User Identity Groups, [731–732](#)

**posture assessment**

- posture client provisioning global setup, [331–335](#)
- posture general settings, [335–336](#)
- posture reassessments, [336–337](#)
- posture updates, [337](#)

**profiler**

- endpoint attribute filtering, [182–183](#)
- NMAP Scan Subnet Exclusions, [183](#)
- SNMP settings for probes, [182](#)

**Go Live button (Guest Self-Registration Wizard), 65**

**Google Play app store, 391**

**Google URLs, adding for ACL bypass, 231–232**

**government certifications, 30**

**GPOs (Group Policy Objects)**

- phased deployment, [523](#)
- Windows GPO configuration for wired supplicant, [369–373](#)

**GROUP\_ACCOUNTS group, 308**

**groups**

- guest sponsor groups, [307–309](#)
- Identity Groups, [183–186](#)
- NDGs (Network Device Groups)
  - creating, [528–529](#)
  - phased deployment, [527](#)
- node groups, [451–453](#)

**guest accounts**

- creating, [320](#)
- managing, [320–321](#)

**guest authorization rule, 105**

## **Guest domain, [86](#)**

### **guest portals**

hotspot guest portals, [302–303](#)

sponsored guest portals, [313](#)

    Active Directory identity stores, [304–305](#)

    guest sponsor groups, [307–309](#)

    guest types, [305–307](#)

    multiple guest portals, [318](#)

    overview of, [304](#)

    portal page customization, [315](#)

    sponsor portal behavior and flow settings, [313–314](#)

## **Guest Self-Registration Wizard, [61–65](#)**

### **Guest Server, [33](#)**

### **guest services, [5, 33, 299–302](#)**

CWA (Central Web Authentication)

    compared to LWA (Local Web Authorization), [299–301](#)

    wired switches, [321–322](#)

    WLCs (Wireless LAN Controllers), [322–325](#)

dynamic interface, [234–235](#)

guest accounts

    creating, [320](#)

    managing, [320–321](#)

guest experience, [25](#)

guest sponsors, [299, 307–309](#)

guest types, [305–307](#)

hotspot guest portal configuration, [302–303](#)

lifecycle management, [27](#)

LWA (Local Web Authorization), [299–301](#)

policies, [310](#)

    guest post-authentication authorization policy, [312](#)

    guest pre-authentication authorization policy, [310–312](#)

sponsored guest portals, [313](#)

    Active Directory identity stores, [304–305](#)

    guest sponsor groups, [307–309](#)

    guest types, [305–307](#)

    layout, [319](#)

multiple guest portals, [318](#)  
overview of, [304](#)  
portal page customization, [315](#)  
sponsor portal behavior and flow settings, [313–314](#)

## **Guest WLAN, creating, [236–240](#)**

# **H**

## **HA (high-availability) options, [43, 446](#)**

Anycast HA, [456–459](#)  
configuration on Classic IOS/IOS 15.x switches, [208–211](#)  
MnT (Monitoring & Troubleshooting) nodes, [446–447](#)  
node groups, [451–453](#)  
PANs (Policy Administration Nodes)  
    auto PAN failover, [449–450](#)  
    HA (high-availability) options, [446–447](#)  
    promoting, [448](#)  
PSNs (Policy Service Nodes), [450–453](#)  
RADIUS fallback, [227–228](#)

**hardware addresses.** See [\*\*MAC addresses\*\*](#)

## **Headend packages**

downloading, [469–470, 471–473](#)  
preparing, [471–473](#)

## **Helpdesk profile**

device admin AAA with Cisco IOS, [745–746, 747–752](#)  
device admin AAA with Cisco Nexus switches, [781–782](#)  
device admin AAA with Cisco WLC, [765](#)

**high-availability options.** See [\*\*HA \(high-availability\) options\*\*](#)

**high-level goals (NASP), [81–84](#)**

**high-level troubleshooting flowchart, [697](#)**

**High-Security Mode.** See [\*\*Closed Mode\*\*](#)

**Holla, Hariprasad, [222](#)**

**host application visibility, [357–358](#)**

**host keys, adding to SFTP repository, [710–711](#)**

**host security posture assessment rules**

    adding, [98–101](#)

common checks, rules, and requirements, [97](#)  
definition of, [78](#)  
deployment, [98–101](#)  
determining validity of, [99–100](#)  
documentation of posture requirements, [96–97](#)  
enforcement, [98–101](#)  
examples of, [89–90](#)  
posture assessment options, [93–94](#), [95](#)

## **HostScan, [494](#)**

**hotspot guest portal configuration, [302–303](#)**

**“How To: Cisco and F5 Deployment Guide-ISE Load Balancing Using BIG-IP” (Hyps), [454](#)**

**HREAP (Hybrid Remote Edge Access Point) mode, [41](#)**

## **HTTP/HTTPS**

enabling on Classic IOS/IOS 15.x switches, [197](#)

probes

    HTTP probes, [150–152](#)

    HTTP profiling without probes, [152](#)

repositories, [712–713](#),

**Hybrid Remote Edge Access Point (HREAP) mode, [41](#)**

**Hypertext Transfer Protocol. See [HTTP/HTTPS](#)**

**Hyper-Threading Technology, [46](#)**

**Hyps, Craig, [153](#), [188](#), [454](#)**

## **I**

**Identities screen (Device Administration), [731–732](#)**

### **identity awareness**

    contextual information, [6](#)

    definition of, [5](#)

### **identity consumers**

    ASA (Adaptive Security Appliance), [621–622](#)

    FMS (Firepower Management Center), [619–620](#)

    Stealthwatch, [618–619](#)

    Web Security Appliance, [620–621](#)

**identity firewalling (IDFW), [32](#)**

**identity gathering**, [31–33](#)

**Identity Groups**, [183–186](#)

**Identity Services Engine**. See [ISE-enabled network design](#)

**identity sharing**

Active Directory identities, learning about, [598–599](#)

ISE-PIC (Passive Identity Connector), [603–610](#)

Kerberos sniffing via SPAN, [610–611](#)

WMI (Windows Management Instrumentation), [599–603](#)

Active Directory identity stores, [304–305](#)

ASA (Adaptive Security Appliance), [621–622](#)

CDA-RADIUS, [617](#)

EZ Connect, [628–630](#)

FMS (Firepower Management Center), [619–620](#)

ISE-PIC (Passive Identity Connector), [603–604](#), [626–628](#)

logoff detection with endpoint probe, [623–624](#)

metadata API, [617–618](#)

pxGrid (Platform Exchange Grid), [616–617](#)

session timeouts, [625](#)

Stealthwatch, [618–619](#)

Syslog sources, [611–615](#)

Web Security Appliance, [620–621](#)

**identity store**, [271–272](#)

Active Directory identity stores, [304–305](#)

alternative ID stores based on EAP type, [278–280](#)

**IDFW (identity firewalling)**, [32](#)

**IETF RFC 2196**, [82](#)

**IKE (Internet Key Exchange)**, [468](#)

**importing profiles**, [187–188](#)

**Incident Response policy**, [113–116](#)

**Include Service Version Information scan (NMAP)**, [147](#)

**infrastructure components**

feature-to-functionality mapping, [37](#)

functionality of, [36–37](#)

recommended components, [41](#)

role of, [35–36](#)

supported components, list of, [37–41](#)

**infrastructure configuration.** See [configuration](#)

**ingress access control challenges,** [558–561](#)

**Inline Posture Node,** [44](#)

**integration**

- identity sharing
  - ASA (Adaptive Security Appliance), [621–622](#)
  - FMS (Firepower Management Center), [619–620](#)
  - metadata API, [617–618](#)
  - Stealthwatch, [618–619](#)
  - Web Security Appliance, [620–621](#)
- integration types, [632](#)
  - MDM (mobile device management), [632](#)
    - integration configuration, [431–433](#)
    - integration points, [430–431](#)
    - Rapid Threat Containment, [632–635](#)
- integrity of audit logs, ensuring,** [129](#)
- Intel Hyper-Threading Technology,** [46](#)
- interface range command,** [208](#)
- Interface SNMPQUERY probe,** [148](#)
- interfaces**
  - configuration on Classic IOS/IOS 15.x switches, [208](#)
  - dynamic interfaces for client VLANs, [233–235](#)
- Internal Administrator Summary report,** [130](#)
- internal CA (certificate authority),** [28](#)
- Internet Access domain,** [86](#)
- Internet Key Exchange (IKE),** [468](#)
- Internet of Things (IoT),** [2](#)
- Internet only for mobile devices authorization rule,** [288–292](#)
- Internet service providers (ISPs),** [12](#)
- iOS (Apple), onboarding,** [394–401](#)
- IOS (Cisco)**
  - BYOD onboarding, [394–401](#)
  - Classic IOS switches, [196](#)
  - ACLs (access control lists), [202–203](#)

authentication settings, [211–212](#)  
authentication timers, [212](#)  
certificates, [196–197](#)  
Flex-Auth (Flexible Authentication), [208–211](#)  
global 802.X commands, [204](#)  
global AAA commands, [198–199](#)  
global logging commands, [204–205](#)  
global profiling commands, [205–207](#)  
global RADIUS commands, [199–202](#)  
HTTP/HTTPS server, [197](#)  
Monitor Mode, [213](#)  
native SGT propagation, [582–584](#)  
switch port interfaces, [208](#)

device admin AAA  
    Helpdesk profile, [745–746](#)  
    NAD (network access device) configuration, [749–752](#)  
    NetAdmin profile, [740–742](#)  
    NetOps profile, [742–743](#)  
    overview of, [739](#)  
    policy sets, [747–749](#)  
    testing and troubleshooting, [752–758](#)  
    user roles, [739–740](#)

Device Sensor, [37](#)

IOS 15.x switches  
    ACLs (access control lists), [202–203](#)  
    authentication settings, [211–212](#)  
    authentication timers, [212](#)  
    certificates, [196–197](#)  
    characteristics of, [196](#)  
    Flex-Auth (Flexible Authentication), [208–211](#)  
    global 802.X commands, [204](#)  
    global AAA commands, [198–199](#)  
    global logging commands, [204–205](#)  
    global profiling commands, [205–207](#)  
    global RADIUS commands, [199–202](#)  
    HTTP/HTTPS server, [197](#)

Monitor Mode, [213](#)  
native SGT propagation, [582–584](#)  
switch port interfaces, [208](#)

load balancing, [459](#)  
onboarding flow, [423–425](#)  
SXP (SGT Exchange Protocol) configuration, [572–573](#)

**IoT (Internet of Things), [2](#)**

**IP address management (IPAM), [612](#)**

**IP addresses, binding to SGTs, [568](#)**

**ip dhcp relay ISE\_PSN\_address command, [75](#)**

**ip domain-name command, [197](#)**

**ip helper-address commands, [153–156](#)**

**ip helper-address ISE\_PSN\_address command, [74](#)**

**ip http secure-server command, [197](#)**

**ip http server command, [197](#)**

**ip radius source-interface command, [669, 690, 693](#)**

**IP service-level agreement (IPSLA), [456](#)**

**ip tacacs source-interface command, [669](#)**

**IPAM (IP address management), [612](#)**

**IPEVENT message, [670](#)**

**IPSLA (IP service-level agreement), [456](#)**

**IPv4\_DST\_ADDR attribute, [546](#)**

**IPv4\_SRC\_ADDR attribute, [546](#)**

**IR (Incident Response) policy, TC-NAC in, [113–116](#)**

**ISE ecosystems**

- integration types, [632](#)
- MDM integration, [632](#)
- overview of, [631](#)

pxGrid (Platform Exchange Grid)

- CA (certificate authority), [638](#)
- controllers, [635](#)

FMC (Firepower Management Center) configuration, [642–648](#)

full mesh of trust, [637–638](#)

ISE configuration for, [639–642](#)

overview of, [635–637](#)

publishers, [635](#)

Stealthwatch configuration, [652–657](#)

subscribers, [635](#)

WSA (Web Security Appliance) configuration, [649–652](#)

Rapid Threat Containment, [632–635](#)

**ISE Home Page**, [660–663](#)

**ISE Posture module**, [469](#)

**ISE-enabled network design**, [23](#). See also [security policy](#); [upgrades \(ISE\)](#)

authorization rules, [33–34](#)

centralized policy control operation, [23–26](#)

deployment

    centralized, [52–54](#)

    distributed, [55–57](#)

endpoint components, [42–43](#)

features and benefits, [3–5](#), [26–30](#)

infrastructure components

    feature-to-functionality mapping, [37](#)

    functionality of, [36–37](#)

    recommended components, [41](#)

    role of, [35–36](#)

    supported components, list of, [37–41](#)

ISE for wireless, [59–60](#)

    BYOD (Bring Your Own Device) Wizard, [67–69](#)

    Guest Self-Registration Wizard, [61–65](#)

    Secure Access Wizard, [65–67](#)

    Wireless Setup Wizard home page, [59–60](#)

ISE personas, [43–45](#)

ISE to gain visibility, [69](#)

    DHCP probe, [74–75](#)

    RADIUS probe, [74](#)

    SNMPQUERY probe, [73–74](#)

    Visibility Setup Wizard, [69–73](#)

licensing, [45–46](#)

node types, [43–45](#)

performance, [47–48](#)

platform support and compatibility, [30](#)

policy components, [42](#)  
policy construct, [30–33](#)  
policy-based structure, [48–49](#)  
requirements, [46–47](#)

## ISE-PIC (Passive Identity Connector) Agent, [603–604](#), [626–628](#)

agent configuration file, [609](#)  
Agent screen, [603–604](#)  
deploying, [604–607](#)  
design options, [610](#)  
log forwarding, [610](#)  
nodes file, [608](#)

## ISO 27001, [30](#)

## ISPs (Internet service providers), [12](#)

## J–K

Jobs, Steve, [383](#)  
Karelis, E. Pete, [456](#), [614](#)  
Kerberos sniffing, [610–611](#)  
Keren, Eyal, [682](#)  
**keywords.** See also [commands](#)  
    log, [252](#)  
    smartlog, [252](#)

## L

**L4\_DST\_PORT attribute**, [546](#)  
**L4\_SRC\_PORT attribute**, [546](#)  
**large deployments**, [724–725](#)  
**layout of sponsored guest portals**, [319](#)  
**Learn tenet (passive identification)**, [598](#), [615](#)  
**least-privilege strategy**, [136](#)  
**licensing**  
    device admin license, [723](#)  
    ISE (Identity Services Engine), [45–46](#)  
**listeners**, [569](#)  
**Live Logs**, [666–667](#)

filtering, [666](#)

troubleshooting

- existing entry in Live Logs, [694–696](#)

- no Live Log entries exist, [689–694](#)

- steps for, [686–689](#)

**Live Sessions views, [666–667](#)**

**load balancing**

- Cisco IOS load balancing, [459](#)

- failure scenarios, [455](#)

- general guidelines, [454–455](#)

- load balancers, [453–455](#)

**LOBBY role, [760](#)**

**local service templates, [219–220](#)**

**Local Web Authentication (LWA), [36](#)**

**log deduplication, [686–688](#)**

**log keyword, [252](#)**

**logging source-interface command, [669](#)**

**logical profiles, [110, 178–179](#)**

**logoff detection with endpoint probe, [623–624](#)**

**logs**

- audit logs

- collection of, [128–129](#)

- ensuring integrity and confidentiality of, [129](#)

- logging categories, [128](#)

- regular audit data review, [129](#)

- remote logging targets, [129](#)

- configuration on Classic IOS/IOS 15.x switches, [204–205](#)

- deduplication, [686–688](#)

- forwarding, [610](#)

- global logging commands, [204–205](#)

- ISE logs, [701–703](#)

- Live Logs, [666–667](#)

- filtering, [666](#)

- troubleshooting, [688–696](#)

- MnT (Monitoring & Troubleshooting) nodes, [446–447](#)

support bundle, [702–703](#)

TACACS+660

TC-NAC, [660](#)

## **Low-Impact Mode, [530–532](#)**

**LWA (Local Web Authentication), [36](#), [299–301](#)**

# **M**

**MAB (MAC Authentication Bypass), [5](#), [36](#), [134](#), [214](#)**

**MAC addresses**

MAB (MAC Authentication Bypass), [5](#), [32](#), [36](#), [134](#), [214](#)

MAM (MAC address management) model, [185](#)

**Mac OS onboarding flow, [428–429](#)**

**Mac OS X C10.8.2 native supplicants, [367–369](#)**

**maintenance of distributed deployments, [460–462](#)**

**MAM (MAC address management) model, [185](#)**

**management API, [617–618](#)**

**MANAGEMENT role, [760](#)**

**MDA (Multi-Domain Authentication), [210](#)**

**MDM (mobile device management) onboarding, [429](#)**

  attributes, [430–431](#)

  integration, [632](#)

  integration configuration, [431–433](#)

  integration points, [430–431](#)

  policies, [433–435](#)

**medium deployments, [725](#)**

**Menu Access permissions, [127–128](#)**

**messages**

  AAA, [670](#)

  IPEVENT, [670](#)

  POLICY\_APP\_FAILURE, [670](#)

  POLICY\_APP\_SUCCESS, [670](#)

  RADIUS, [18–20](#)

  TACACS+

    accounting messages, [15–17](#)

    authentication messages, [14–15](#)

authorization messages, [15–17](#)

**metadata API**, [617–618](#)

**Metasploit**, [99](#)

**Microsoft CHAP (MS-CHAP)**, [12](#)

**Microsoft Security Bulletin**, [98](#)

**Microsoft TechNet Security Center**, [98](#)

**MnT (Monitoring & Troubleshooting) nodes**, [43–44](#), [117](#)

- HA (high-availability) options, [446–447](#)
- in large deployments, [724](#)
- upgrading, [705–708](#)

**mobile device management**. See [\*\*MDM \(mobile device management\) onboarding\*\*](#)

**Monitor Mode**

- configuration on Classic IOS/IOS 15.x switches, [213](#)
- operational flow, [526–527](#)
- transition to end state, [534–535](#)

**MONITOR role**, [760](#)

**monitor session command**, [156](#)

**Monitoring & Troubleshooting nodes**. See [\*\*MnT \(Monitoring & Troubleshooting\) nodes\*\*](#)

**Monitoring nodes**, [55](#), [669](#)

**Monitoring persona**, [43–44](#)

**monitoring tools**, [30](#), [659–660](#). See also [\*\*profiling\*\*](#)

- Context Visibility views, [663–665](#)
- data repository setup, [671–672](#)
- device configuration for monitoring, [669–670](#)
- global search, [667–669](#)
- ISE alarms, [672](#)
- ISE Home Page, [660–663](#)
- ISE reporting, [670–671](#)
- Monitoring nodes, [669](#)
- RADIUS Live Logs and Live Sessions views, [666–667](#)

**MS-CHAP (Microsoft CHAP)**, [12](#)

**Multi-Auth (Multiple Authentication)**, [210](#)

**Multi-Domain Authentication (MDA)**, [210](#)

**multi-forest Active Directory support**, [29](#)

**multiple guest portals, creating, 318**

## N

**NAC (Network Access Control), 23–24, 112–116**

**NADs (network access devices), 12, 51, 99.** See also [device administration](#)

BYOD onboarding

ACLs (access control lists), [390–391](#)

URLs, adding to ACL\_WEBAUTH\_REDIRECT, [392](#)

WLC (Wireless LAN Controller) configuration, [388–390](#)

C3PL switch configuration, [196, 213–215](#)

ACLs (access control lists), [219–220](#)

certificates, [216–217](#)

differentiated authentication, [214](#)

global 802.X commands, [220–221](#)

global RADIUS commands, [217–219](#)

local service templates, [219–220](#)

policies, [222–224](#)

Classic IOS/IOS 15.x switch configuration, [195–196](#)

ACLs (access control lists), [202–203](#)

authentication settings,

[211–212](#)

authentication timers, [212](#)

certificates, [196–197](#)

Flex-Auth (Flexible Authentication), [208–211](#)

global 802.X commands, [204](#)

global AAA commands, [198–199](#)

global logging commands, [204–205](#)

global profiling commands, [205–207](#)

global RADIUS commands, [199–202](#)

HTTP/HTTPS server, [197](#)

Monitor Mode, [213](#)

switch port interfaces, [208](#)

WLC (Wireless LAN Controller) configuration, [225](#)

AireOS features, [225–226](#)

Airespace ACLs, [229–232](#)

Corporate SSID, [240–245](#)

dynamic interfaces for client VLANs, [233–235](#)  
Guest WLAN, [236–240](#)  
RADIUS accounting servers, [227–228](#)  
RADIUS authentication servers, [226–227](#)  
RADIUS fallback, [229](#)

**NAM (Network Access Manager)**, [377–381, 469](#)

**Name field (authorization profiles)**, [254](#)

**NAS (network access server)**, [17](#)

**NASP (network access security policy)**. See also [policy sets](#)

- AnyConnect client provisioning policy, [343](#)
- auditing policy
  - audit log collection, [128–129](#)
  - audit log integrity and confidentiality, [129](#)
  - PCI DSS (Payment Card Industry Data Security Standard), [118–126](#)
  - regular audit data review, [129](#)
  - unique usernames and passwords, [126–128](#)
  - user accounting, [131–132](#)
- AUP (acceptable use policy), [89–90, 338](#)
- authentication policies
  - allowed protocols, [266–271](#)
  - alternative ID stores based on EAP type, [278–280](#)
  - conditions, [263–266](#)
  - goals, [261–262](#)
  - identity store, [271–272](#)
  - processing of, [262–263](#)
  - RA-VPN example, [277](#)
  - wireless SSID example, [272–276](#)
- authorization policies
  - authorization based on posture compliance, [360–361](#)
  - BYOD onboarding, [422–423](#)
  - employee and corporate machine full-access rule, [286–288](#)
  - employee limited access rule, [292–295](#)
  - goals of, [280](#)
  - Internet only for mobile devices, [288–292](#)
  - posture client provisioning, [359–360](#)
  - processing of, [280–286](#)

profiles in, [183–187](#)  
RA-VPN with posture flows, [501](#)  
rules, [286](#)  
saving attributes for reuse, [295–297](#)

authorization policy, [247](#)  
  authorization profiles, [253–255](#)  
  Authorization Results, [251](#)  
  conditions, [249–250](#)  
  dACLs (downloadable access control lists), [251–253](#)  
  policy rules, [247–251](#)  
  policy sets, [247–248](#)  
authorization rules, [87–89](#)  
centralized policy  
  advantages of, [6–7](#)  
  Cisco ISE operation, [23–26](#)  
checklist, [79](#)  
client provisioning policy  
  configuration, [413–415](#)  
  default unavailable client provisioning policy action, [420–421](#)  
commonly used policies, [103–105](#)  
components of, [78–79](#)  
configuration on C3PL switches, [222–224](#)  
control policies  
  applying to interfaces, [224](#)  
  configuration, [223–224](#)  
custom policies, [543–544](#)  
decision matrix, [84–85](#)  
definition of, [77](#)  
device profiling policy, [160](#)  
  context visibility, [169–178](#)  
  endpoint profile policies, [167–169](#)  
  logical profiles, [178–179](#)  
  profiler feed service, [160–166](#)  
device security policy, [107](#)  
  device profiling, [107–111](#)  
TC-NAC (Threat-Centric Network Access Control), [111–116](#)

dynamic network access privileges, [102](#)  
enforcement, [102–103](#)  
guest policies, [310](#)  
    guest post-authentication authorization policy, [312](#)  
    guest pre-authentication authorization policy, [310–312](#)  
high-level goals for, [81–84](#)  
host security posture assessment rules, [91–101](#)  
    adding, [98–101](#)  
    common checks, rules, and requirements, [97](#)  
    deployment, [98–101](#)  
    determining validity of, [99–100](#)  
    documentation of posture requirements, [96–97](#)  
    enforcement, [98–101](#)  
    examples of, [89–90](#)  
    posture assessment options, [93–94](#)  
    posture remediation options, [95](#)  
IR (Incident Response) policy, [113–116](#)  
MDM onboarding policies, [433–435](#)  
NASP committees, [79–81](#)  
policy components, [42](#)  
policy construct, [30–33](#)  
policy sets, [48, 247–248](#)  
    creating, [529–530, 736–738](#)  
    device admin AAA with Cisco IOS, [747–749](#)  
    device admin AAA with Cisco WLC, [766–768](#)  
    enabling, [258–261](#)  
    ISE for Nexus device admin AAA, [782–783](#)  
policy-based structure, [48–49](#)  
posture policy, [355–357](#)  
security domains, [85–87](#)  
software-defined segmentation policy, [25](#)  
**NAT (Network Address Translation), [454](#)**  
**National Cyber Awareness System, [99](#)**  
**National Vulnerability Database, [99](#)**  
**native supplicants**  
    comparison of popular supplicants, [366–367](#)

configuration

Mac OS X C10.8.2 native supplicant, [367–369](#)

Windows 7, 8/8.1, and 10 native supplicants, [373–377](#)

profiles, configuring for onboarding, [408–423](#)

provisioning, [365](#)

## **native tagging, [580–581](#)**

**navigation UI (Device Administration), [730–731](#)**

## **NDGs (Network Device Groups)**

creating, [528–529](#)

device administration, [727–728](#)

phased deployment, [527](#)

## **NetAdmin profile**

device admin AAA with Cisco IOS, [740–742](#)

device admin AAA with Cisco Nexus switches, [779–780](#)

device admin AAA with Cisco WLC, [763–764](#)

## **NetFlow**

probes, [152–153, 544–545](#)

attributes, [546](#)

configuration, [548–550](#)

efficient data collection, [547–548](#)

example profile policy using, [546–547](#)

triggered NetFlow, [191–194](#)

## **NetOps profile**

device admin AAA with Cisco IOS, [742–743](#)

device admin AAA with Cisco Nexus switches, [780–781](#)

## **Network Access Control (NAC), [23–24](#)**

**network access devices. See [NADs \(network access devices\)](#)**

**Network Access Manager (NAM) module, [469](#)**

**network access security policy. See [NASP \(network access security policy\)](#)**

**network access server (NAS), [17](#)**

**Network Address Translation (NAT), [454](#)**

**network authorization policy, [247](#)**

authorization profiles, [253–255](#)

Authorization Results, [251](#)

conditions, [249–250](#)

dACLs (downloadable access control lists), [251–253](#)  
policy rules, [247–251](#)  
policy sets, [247–248](#)

**network design.** See [ISE-enabled network design](#)

**Network Device Groups (NDGs)**

creating, [528–529](#)  
device administration, [727–728](#)  
phased deployment, [527](#)

**Network Devices view**, [665](#)

**network reachability tasks**, [484–487](#)

**Network Resources screen (Device Administration)**, [733](#)

**Network Scan probes.** See [NMAP probes](#)

**network visibility, gaining**, [25](#)  
**network-admin user role**, [777](#)  
**network-operator user role**, [777](#)  
**next-generation firewalls (NGFW)**, [4](#), [467](#)

**Nexus switches**

configuring device admin AAA with, [777](#)  
Helpdesk profile, [781–782](#)  
NetAdmin profile, [779–780](#)  
NetOps profile, [780–781](#)  
network device preparation, [778–779](#)  
policy sets, [782–783](#)  
SecAdmin profile, [781](#)  
TACACS+, enabling, [783–784](#)  
user roles, [777–778](#)  
native SGT propagation for, [586–587](#)

**NFS (Network File System) repositories**, [712](#)

**NGFW (next-generation firewalls)**, [4](#), [6](#), [467](#)

**NMAP probes**

configuration, [144–147](#)  
considerations for, [144](#)  
NMAP Scan Subnet Exclusions, [183](#)  
overview of, [143–144](#)

**No CoA setting**, [180](#)

**node types (ISE),** [43–45](#)

**nodes.** See also [PANs \(Policy Administration Nodes\)](#)

Admin, [55](#)

configuration in distributed environment, [439–440](#)

node personas and roles, [445](#)

node registration, [442–445](#)

primary PANs, [440–442](#)

MnT (Monitoring & Troubleshooting), [117](#)

in large deployments, [724](#)

upgrading, [705–708](#)

Monitoring, [55, 669](#)

node groups, [451–453](#)

personas, verifying, [445](#)

PSNs (Policy Service Nodes), [51–52](#)

adding to AAA server group, [478–481](#)

upgrading, [705–708](#)

registering to deployment, [442–445](#)

**nodes files,** [608](#)

**nslookup command,** [700](#)

**NX-OS device admin AAA,** [777](#)

Helpdesk profile, [781–782](#)

NetAdmin profile, [779–780](#)

NetOps profile, [780–781](#)

network device preparation, [778–779](#)

policy sets, [782–783](#)

SecAdmin profile, [781](#)

TACACS+, enabling, [783–784](#)

user roles, [777–778](#)

## O

**offline manual update (profiler feed service),** [164–166](#)

**onboarding.** See [BYOD onboarding](#); [MDM \(mobile device management\) onboarding](#)

**one-time password (OTP),** [507](#)

**OOB Management domain,** [86](#)

**Open Authentication,** [211](#)

**open authentication**, [524–525](#)  
**OS scan (NMAP)**, [146](#)  
**OTA (Over the Air) provisioning**, [391](#)  
**OTP (one-time password)**, [507](#)  
**OWN\_ACCOUNTS group**, [308](#)

## P

**PANs (Policy Administration Nodes)**, [55](#), [128–129](#)  
auto PAN failover, [449–450](#)  
configuring as primary devices, [440–442](#)  
HA (high-availability) options, [446–447](#)  
promoting, [448](#)  
S-PAN (Secondary PAN), [705–708](#)  
**PAP (Password Authentication Protocol)**, [12](#), [268](#)  
**PASS\_ADD packet**, [16](#)  
**PASS REPL packet**, [16](#)  
**passive authentication**  
compared to active authentication, [594–595](#)  
definition of, [593](#)  
EZ Connect, [628–630](#)  
identity sharing  
Active Directory identities, [598–599](#)  
ASA (Adaptive Security Appliance), [621–622](#)  
CDA-RADIUS, [617](#)  
FMS (Firepower Management Center), [619–620](#)  
input and outputs, [596](#)  
logoff detection with endpoint probe, [623–624](#)  
metadata API, [617–618](#)  
pxGrid (Platform Exchange Grid), [616–617](#)  
REST (representational state transfer) API sources, [614–615](#)  
session timeouts, [625](#)  
Stealthwatch, [618–619](#)  
Syslog sources, [611–614](#)  
Web Security Appliance, [620–621](#)  
**ISE-PIC (Passive Identity Connector)**, [603–604](#), [626–628](#)  
**PassiveID Work Center**, [596–597](#)

tenets of, [596–597](#)

Learn, [598, 615](#)

Share, [615–616](#)

Update, [623](#)

Use, [617–618](#)

## passive identities

Active Directory identities, learning about, [598–599](#)

ISE-PIC (Passive Identity Connector), [603–610](#)

Kerberos sniffing via SPAN, [610–611](#)

WMI (Windows Management Instrumentation), [599–603](#)

ASA (Adaptive Security Appliance), [621–622](#)

CDA-RADIUS, [617](#)

definition of, [593](#)

EZ Connect, [628–630](#)

FMS (Firepower Management Center), [619–620](#)

ISE-PIC (Passive Identity Connector), [603–604, 626–628](#)

logoff detection with endpoint probe, [623–624](#)

metadata API, [617–618](#)

pxGrid (Platform Exchange Grid), [616–617](#)

REST (representational state transfer) API sources, [614–615](#)

session timeouts, [625](#)

Stealthwatch, [618–619](#)

Syslog sources, [611–614](#)

Web Security Appliance, [620–621](#)

**Passive Identity Connector (PIC)**, [603–604, 626–628](#)

**Passive Identity Tracking field (authorization profiles)**, [255](#)

**PassiveID Work Center**, [596–597](#)

**Password Authentication Protocol (PAP)**, [12, 268](#)

**Password Change Control (Device Administration)**, [729](#)

**password enforcement**, [126–128](#)

**patches**, [460–462](#)

**PCI-DSS (Payment Card Industry Data Security Standard)**, [1, 118–126, 558](#)

**PEAP (Protected EAP)**, [269](#)

**Perfigo, acquisition by Cisco**, [24](#)

**performance of ISE (Identity Services Engine)**, [47–48](#)

**permissions, administrator**, [127](#)

**permit statement**, [230](#)

**per-profile CoA (Change of Authorization)**, [181](#)

**personas**, [43–45](#), [445](#)

**phased deployment**, [521](#)

  802.1X, [524–525](#)

  advantages of, [521–523](#)

  Closed Mode, [532–534](#)

  deployment process, [523–524](#)

  Low-Impact Mode, [530–532](#)

  Monitor Mode, [526–527](#)

  open authentication, [524–525](#)

  preparation for

    Network Device Groups, [528–529](#)

    policy sets, [529–530](#)

    transition from Monitor Mode to end state, [534–535](#)

    wireless networks, [535](#)

**physical addresses**. See [MAC addresses](#)

**PIC (Passive Identity Connector)**, [603–604](#), [626–628](#)

**PICAgent.exe.config file**, [609](#)

**ping command**, [700](#)

**plain old telephone service (POTS)**, [12](#)

**Platform Exchange Grid (pxGrid)**, [4](#), [25](#), [44](#), [579–580](#), [616–617](#)

**platform support and compatibility**, [30](#)

**Plus license**, [45–46](#)

**Point-to-Point Protocol (PPP)**, [17](#)

**policies**. See [NASP \(network access security policy\)](#)

**Policy Administration Nodes**. See [PANs \(Policy Administration Nodes\)](#)

**policy authoring API**, [617–618](#)

**Policy Elements screen (Device Administration)**, [733–736](#)

  TACACS+ command sets, [733–734](#)

  TACACS+ profiles, [734–736](#)

**Policy Service Nodes**. See [PSNs \(Policy Service Nodes\)](#)

**Policy Service persona**, [43](#)

**policy sets**, [48](#), [247–248](#)

creating, [529–530](#), [736–738](#)  
device admin AAA with Cisco IOS, [747–749](#)  
device admin AAA with Cisco WLC, [766–768](#)  
enabling, [258–261](#)  
ISE for Nexus device admin AAA, [782–783](#)

**POLICY\_APP\_FAILURE message**, [670](#)  
**POLICY\_APP\_SUCCESS message**, [670](#)  
**policy-based structure**, [48–49](#)  
**Port Bounce CoA (Change of Authorization)**, [180–181](#)  
**Portal Behavior and Flow Settings page**, [313–314](#)  
**Portal Customization (Guest Self-Registration Wizard)**, [63](#)  
**Portal Notifications (Guest Self-Registration Wizard)**, [63](#)  
**Portal Page Customization page**, [315](#)  
**Portal Pages (Guest Self-Registration Wizard)**, [63](#)  
portals. See [client provisioning portal](#); [sponsored guest portals](#)  
ports. See also [802.1X](#); [suplicants](#)

Closed Mode, [532–534](#)  
configuration on Classic IOS/IOS 15.x switches, [208](#)  
Low-Impact Mode, [530–532](#)

**posture assessment**. See also [posture flows](#)

configuration

AnyConnect Agent with ISE Compliance Module, [339–343](#)  
AUP (acceptable use policy) enforcement, [338](#)  
authorization policies, [359–361](#)  
client provisioning portal, [343–344](#)  
host application visibility and context collection, [357–358](#)  
posture client provisioning global setup, [331–335](#)  
posture conditions, [345–349](#)  
posture elements, [345](#)  
posture general settings, [335–336](#)  
posture policy, [355–357](#)  
posture reassessments, [336–337](#)  
posture remediations, [349–353](#)  
posture requirements, [353–355](#)  
posture updates, [337](#)

enabling in network, [362–363](#)  
overview of, [327–329](#)  
Posture Assessment Work Center, [328–329](#)  
reports, [361–362](#)  
rules  
    adding, [98–101](#)  
    common checks, rules, and requirements, [97](#)  
    deployment, [98–101](#)  
    determining validity of, [99–100](#)  
    documentation of posture requirements, [96–97](#)  
    enforcement, [98–101](#)  
    examples of, [89–90](#)  
    posture assessment options, [93–94](#)  
    posture remediation options, [95](#)  
troubleshooting, [361–362](#)

**Posture Assessment by Condition report**, [556](#)

**Posture Assessment Work Center**, [328–329](#)

## posture flows

overview of, [329–331](#)  
RA-VPNs with, [495–496](#)  
    ACLs (access control lists), [496–499](#)  
    authorization policies, [501](#)  
    authorization profiles, [499–500](#)  
    sample session, [501–506](#)

**POTS (plain old telephone service)**, [12](#)

**PPP (Point-to-Point Protocol)**, [17](#)

**Preboot Execution Environment (PXE)**, [211](#), [530](#)

**Pre-Deploy mode**, [469](#)

## primary nodes

MnT (Monitoring & Troubleshooting) nodes, [446–447](#)  
PANs (Policy Administration Nodes), [448–450](#)

**primary PANs (Policy Administration Nodes)**, [440–442](#)

## privileges

administrator accounts, [126–127](#)  
dynamic network access privileges, [102](#)

## probes

AD (Active Directory) probes, [149–150](#)

configuration, [138–139](#)

definition of, [137](#)

DHCP, [74–75](#)

Cisco WLC considerations, [141](#)

configuration, [141–142](#)

overview of, [140](#)

DHCPSpan

Cisco WLC considerations, [141](#)

configuration, [141–142](#)

overview of, [140–141](#)

DNS, [147](#)

endpoint probe, logoff detection with, [623–624](#)

HTTP, [150–152](#)

NetFlow, [152–153](#), [544–545](#)

attributes, [546](#)

configuration, [548–550](#)

efficient data collection, [547–548](#)

example profile policy using, [546–547](#)

NMAP

configuration, [144–147](#)

considerations for, [144](#)

overview of, [143–144](#)

RADIUS, [74](#), [142–143](#)

SNMPQUERY, [73–74](#), [148–149](#)

SNMPTRAP, [148–149](#)

## Profiled Endpoints Summary Report report, [556](#)

### profiler. See also [profiling](#)

CoA (Change of Authorization), [179–180](#)

global CoA, [180–181](#)

per-profile CoA, [181](#)

custom conditions, [542–543](#)

custom policies, [543–544](#)

feed service, [160](#)

configuration, [160–161](#)

offline manual update, [164–166](#)  
verification, [162–163](#)  
global profiler settings  
  endpoint attribute filtering, [182–183](#)  
  NMAP Scan Subnet Exclusions, [183](#)  
  SNMP settings for probes, [182](#)  
monitoring, [553–556](#)  
reports, [553–556](#)

## Profiler Work Center, [137](#), [537–538](#)

### profiling, [28](#). See also [profiler](#)

AnyConnect connection profiles, [473–478](#)  
authorization policy based on, [135–136](#), [183](#)  
  endpoint Identity Groups, [183–186](#)  
  EndPointPolicy, [187](#)  
authorization profiles  
  BYOD onboarding, [421–422](#)  
  configuration, [253–255](#)  
  RA-VPN with posture flows, [499–500](#)  
  in authorization roles, [111](#)  
  on Classic IOS/IOS 15.x switches, [205–207](#)  
CoA (Change of Authorization), [179–180](#)  
  conditions producing, [550–551](#)  
  configuration, [552–553](#)  
  exceptions, [552](#)  
  global CoA, [180–181](#)  
  per-profile CoA, [181](#)  
  types of, [551–552](#)  
context visibility, [107–108](#)  
custom profiles, [538](#)  
  collecting information for, [541–542](#)  
  profiler conditions, [542–543](#)  
  profiler policies, [543–544](#)  
  unique values for unknown devices, [539–541](#)  
data sources, [110–111](#)  
Employee profile, [765–766](#)  
evolution of, [136](#)

global commands, [205–207](#)

global profiler settings

- endpoint attribute filtering, [182–183](#)

- NMAP Scan Subnet Exclusions, [183](#)

- SNMP settings for probes, [182](#)

Helpdesk profile

- device admin AAA with Cisco IOS, [745–746](#)

- device admin AAA with Cisco Nexus switches, [781–782](#)

- device admin AAA with Cisco WLC, [765](#)

how it works, [134–135](#)

HTTP profiling without probes, [152](#)

importance of, [133–134](#)

importing profiles, [187–188](#)

infrastructure configuration, [153](#)

- device sensor, [157–159](#)

- DHCP helper, [153–156](#)

- ip helper-address commands, [153–156](#)

- SPAN, [156](#)

- VLAN ACL captures, [157](#)

- VMware Promiscuous Mode vSwitch setting, [159](#)

least-privilege strategy, [136](#)

logical profiles, [110, 178–179](#)

monitoring, [553–556](#)

native supplicant profiles, [408–423](#)

NetAdmin profile

- device admin AAA with Cisco IOS, [740–742](#)

- device admin AAA with Cisco Nexus switches, [779–780](#)

- device admin AAA with Cisco WLC, [763–764](#)

NetOps profile

- device admin AAA with Cisco IOS, [742–743](#)

- device admin AAA with Cisco Nexus switches, [780–781](#)

policies, [109–110, 160](#)

- context visibility, [169–178](#)

- endpoint profile policies, [167–169](#)

- logical profiles, [178–179](#)

- profiler feed service, [160–166](#)

probes

AD (Active Directory) probes, [149–150](#)

configuration, [138–139](#)

definition of, [137](#)

DHCP probes, [140–142](#)

DHCPSpan probes, [140–142](#)

DNS probes, [147](#)

HTTP probes, [150–152](#)

NetFlow probes, [152–153](#), [544–545](#)

NMAP probes, [143–147](#)

RADIUS probes, [142–143](#)

SNMPQUERY probes, [148–149](#)

SNMPTRAP probes, [148–149](#)

profiling infrastructure, [153](#)

device sensor, [157–159](#)

DHCP helper, [153–156](#)

feed service, [160–166](#)

ip helper-address commands, [153–156](#)

SPAN, [156](#)

VLAN ACL captures, [157](#)

VMware Promiscuous Mode vSwitch setting, [159](#)

pxGrid (Platform Exchange Grid), [642–648](#)

reports, [553–556](#)

SecAdmin profile

device admin AAA with Cisco Nexus switches, [781](#)

device admin AAA with Cisco WLC, [764](#)

TACACS+ profiles, [734–736](#)

triggered NetFlow, [191–194](#)

verification of, [189](#)

context visibility, [190–191](#)

dashboard, [189–190](#)

device sensor show commands, [191](#)

**Profiling Configuration tab (Visibility Setup Wizard), [73](#)**

**Promiscuous Mode, [159](#)**

**promoting PANs (Policy Administration Nodes), [448](#)**

**proof of concept**

ISE for wireless, [59–60](#)

BYOD (Bring Your Own Device) Wizard, [67–69](#)

Guest Self-Registration Wizard, [61–65](#)

Secure Access Wizard, [65–67](#)

Wireless Setup Wizard home page, [59–60](#)

ISE to gain visibility, [69](#)

DHCP probe, [74–75](#)

RADIUS probe, [74](#)

SNMPQUERY probe, [73–74](#)

Visibility Setup Wizard, [69–73](#)

**Protected EAP (PEAP), [269](#)**

**providers (Syslog), [612–614](#)**

**provisioning certificates, [509–515](#)**

**provisioning policy**

configuration, [413–415](#)

default unavailable client provisioning policy action, [420–421](#)

**proxy server, profiler feed service setting, [163](#)**

**PSNs (Policy Service Nodes), [43, 51–52, 117](#)**

adding to AAA server group, [478–481](#)

Anycast HA, [456–459](#)

HA (high-availability) options, [450–451](#)

node groups, [451–453](#)

upgrading, [705–708](#)

**publishers, [635](#)**

**PXE (Preboot Execution Environment), [211, 530](#)**

**PXE (Preboot Execution Environments), [579–580](#)**

**pxGrid (Platform Exchange Grid), [4, 25, 44, 616–617, 733–734](#)**

CA (certificate authority), [638](#)

controllers, [635](#)

FMC (Firepower Management Center) configuration, [642–648](#)

full mesh of trust, [637–638](#)

ISE configuration for, [639–642](#)

overview of, [635–637](#)

publishers, [635](#)

Stealthwatch configuration, [652–657](#)

subscribers, [635](#)

WSA (Web Security Appliance) configuration, [649–652](#)

## Q–R

**quarantine action**, [632](#)

**RADIUS (Remote Authentication Dial-In User Service)**, [17–20](#), [32](#)

AV (attribute-value) pairs, [20](#)

C3PL switch configuration, [217–219](#)

CDA-RADIUS, [617](#)

Classic IOS switch configuration, [199–201](#)

CoA (Change of Authorization), [20–21](#)

compared to TACACS+21

global commands

for C3PL switches, [217–220](#)

for Classic IOS/IOS 15.x switches, [199–203](#)

IOS 15.x switch configuration, [201–202](#)

Live Logs, [666–667](#), [686–696](#)

Live Sessions views, [666–667](#)

messages, [18–20](#)

RADIUS probe, [74](#), [142–143](#)

service types, [18](#)

use cases, [17–18](#)

**WLC (Wireless LAN Controller) configuration**

RADIUS accounting servers, [227–228](#)

RADIUS authentication servers, [226–227](#)

RADIUS fallback, [229](#)

**RADIUS Authentication Troubleshooting tool**, [674–675](#)

**radius-server load-balance command**, [459](#)

**Rapid Threat Containment**, [29](#), [632–635](#)

**RA-VPNs (remote access VPNs)**

authentication policy, [277](#)

client-based RA-VPN configuration

AnyConnect connection profiles, [473–478](#)

AnyConnect Headend packages, downloading, [469–470](#)

client address pool, [481–484](#)

configuration tools, [469–470](#)

Headend preparation, [471–473](#)  
ISE configuration, [487–488](#)  
network reachability tasks, [484–487](#)  
PSNs (Policy Service Nodes), [478–481](#)  
security services modules, [468–469](#)  
testing, [488–494](#)  
connecting to, [490–491](#)  
overview of, [466–467](#)  
with posture flows, [495–496](#)

ACLs (access control lists), [496–499](#)  
authorization policies, [501](#)  
authorization profiles, [499–500](#)  
sample session, [501–506](#)

**RBAC (role-based access control)**, [759](#)

**realms**, [619](#)

**reassessments, posture**, [336–337](#)

**Reauth CoA (Change of Authorization)**, [181](#)

**recommended infrastructure components**, [41](#)

**redirect to web portal**, [5](#)

**redundancy, syslog providers**, [614](#)

**registering nodes to deployment**, [442–445](#)

**REJECT packet**, [14](#)

**remediation, posture**, [95, 349–353](#)

**Remote Access domain**, [86](#)

**remote access VPNs**. See [RA-VPNs \(remote access VPNs\)](#)

**Remote Authentication Dial-In User Service**. See [RADIUS \(Remote Authentication Dial-In User Service\)](#)

**remote logging targets**, [129](#)

**REPLY packet**, [14](#)

**reports**, [670–671](#)

- Adapter Status**, [115](#)
- Administrator Change Configuration Audit**, [130](#)
- Authentications Summary**, [131](#)
- Change Configuration Audit**, [162](#)
- COA Events**, [115](#)

Device Administration, [738](#)  
Internal Administrator Summary, [130](#)  
posture assessment, [361–362](#)  
Posture Assessment by Condition, [556](#)  
Profiled Endpoints Summary, [556](#)  
profiler, [553–556](#)  
Scheduled Admin Change Configuration, [131](#)  
Threat Events, [115](#)  
Top Authorizations by User, [132](#)  
Vulnerability Assessment, [116](#)

**repositories**, [708](#)  
CD-ROM, [712](#)  
configuration, [708–713](#)  
creating, [671–672](#)  
disk, [709](#)  
FTP, [709](#)  
HTTP, [712–713](#)  
HTTPS, [713](#)  
NFS, [712](#)  
SFTP, [710–711](#)  
TFTP, [711](#)  
validation, [713](#)

**REQUEST packet**, [15–16](#)

researching host security posture assessment rules, [98–99](#)

**RESPONSE packet**, [16](#)

**REST (representational state transfer) API**, [614–615](#)

**restore**, [462](#)

**results**  
Authorization Results, [251](#)  
authorization profiles, [253–255](#)  
dACLs (downloadable access control lists), [251–253](#)  
definition of, [251](#)

**reviewing audit data**, [129](#)

**role-based access control (RBAC)**, [759](#)

**roles (WLC)**, [760](#)

## **rules**

authorization, [87–89](#), [286](#)  
host security posture assessment rules  
    adding, [98–101](#)  
    common checks, rules, and requirements, [97](#)  
    deployment, [98–101](#)  
    determining validity of, [99–100](#)  
    documentation of posture requirements, [96–97](#)  
    enforcement, [98–101](#)  
    examples of, [89–90](#)  
    posture assessment options, [93–94](#)  
    posture remediation options, [95](#)  
    network authorization policy, [247](#)

## **Run SMB Discovery Script scan (NMAP), [147](#)**

## **S**

**SAN (Subject Alternative Names), [454](#)**  
**SANS policy site, [90](#)**  
**Santuka, Vivek, [191](#), [682](#)**  
**saving attributes for reuse, [295–297](#)**  
**scans, NMAP (network scan) probes, [143–147](#)**  
**SCEP (Simple Certificate Enrollment Protocol), [509–515](#)**  
**Scheduled Admin Change Configuration report, [131](#)**  
**searching, [667–669](#)**  
**SecAdmin profile**  
    device admin AAA with Cisco Nexus switches, [781](#)  
    device admin AAA with Cisco WLC, [764](#)  
**SecLists.Org mailing lists, [98](#)**  
**secondary nodes**  
    MnT (Monitoring & Troubleshooting) nodes, [446–447](#)  
    PANs (Policy Administration Nodes), [448–450](#)  
**Secondary PAN First (SPF) flow, [705–708](#)**  
**Secure Access, definition of, [23](#)**  
**Secure Access Wizard, [65–67](#)**  
**Secure File Transfer Protocol repositories, [710–711](#)**

Secure Sockets Layer (SSL), [467](#)  
security domains, [85–87](#)  
Security Group Access. See [TrustSec](#)  
Security Group Tags. See [SGTs \(Security Group Tags\)](#)  
security information and event manager (SIEM), [447](#)  
security policy. See [NASP \(network access security policy\)](#)  
security risks, [2–3](#)  
SECURITY role, [760](#)  
security services modules, [468–469](#)  
SecurityFocus, [98](#)  
segmentation policy, software-defined, [25](#)  
self-registration, [61–65](#)  
self-service onboarding. See [onboarding](#)  
self-signed certificates, importing, [440](#)  
servers  
    authentication servers, [32](#)  
    Guest Server, [33](#)  
    HTTP/HTTPS servers, [197](#)  
    RADIUS accounting servers, [227–228](#)  
    RADIUS authentication servers, [226–229](#)  
service set identifier (SSID), [5, 526](#)  
Service Template field (authorization profiles), [255](#)  
service templates, [219–220](#)  
service types, [18](#)  
service-policy command, [224](#)  
services of Cisco ISE (Identity Services Engine), [3–5](#)  
Session Key Assignment (Device Administration), [729–730](#)  
session timeouts, [625](#)  
Session Trace, [682–685](#)  
SFTP (Secure File Transfer Protocol) repositories, [710–711](#)  
SFUA (Source Fire User Agent), [594, 619](#)  
SGA (Security Group Access). See [TrustSec](#)  
SGACLS, traffic enforcement with, [588–591](#)  
SGTs (Security Group Tags), [7, 18, 33, 37, 562–563](#). See also [SXP \(SGT Exchange Protocol\)](#)

assigning, [566–568](#)  
binding IP addresses to, [568](#)  
classification, [565–566](#)  
CollectData, [194](#)  
defining, [564–565](#)  
mapping subnets to, [569](#)  
mapping VLANs to, [569](#)  
native tagging  
    on Catalyst 6500, [584–586](#)  
    on Cisco IOS switches, [582–584](#)  
    on Nexus series switch, [586–587](#)

**Share tenet (passive identification)**, [615–616](#)

**sharing identity**. See [identity sharing](#)

**show aaa server command**, [459](#)

**show application status ise command**, [441–442](#)

**show authentication session interface command**, [691–692](#), [693–694](#), [698](#)

**show device-sensor commands**, [191](#)

**show ip access-list interface command**, [700](#)

**show ip interface brief command**, [692](#)

**show privilege command**, [756](#)

**show repository command**, [713](#)

**show role feature command**, [778](#)

**show role feature-group command**, [778](#)

**show run command**, [16](#)

**show running-config command**, [710–711](#)

**show tech-support command**, [702](#)

**show vpn-sessiondb detail anyconnect command**, [503–506](#)

**SIEM (security information and event manager)**, [447](#)

**Simple Certificate Enrollment Protocol (SCEP)**, [509–515](#)

**simple conditions**, [249](#)

**Simple Network Management Protocol (SNMP)**, [24](#)

**single-SSID onboarding**  
    with Apple iOS, [394–401](#)  
    overview of, [387–388](#)

**site-to-site VPNs (virtual private networks)**, [465–466](#)

**Skip NMAP Host Discover scan (NMAP), [147](#)**

small deployments, [726](#)

smartlog keyword, [252](#)

SNAT (source NAT), [455](#)

sniffing, [610–611](#)

**SNMP (Simple Network Management Protocol), [24](#)**

global profiler settings, [182](#)

SNMP Port scan, [146](#)

SNMPQUERY probe, [74](#)

SNMPQUERY probes, [148–149](#)

SNMPTRAP probes, [148–149](#)

**software-defined segmentation policy, [25](#)**

**solution components (ISE)**

endpoint components, [42–43](#)

infrastructure components

feature-to-functionality mapping, [37](#)

functionality of, [36–37](#)

recommended components, [41](#)

role of, [35–36](#)

supported components, list of, [37–41](#)

policy components, [42](#)

**Source Fire User Agent (SFUA), [594, 619](#)**

**source NAT (SNAT), [455](#)**

**source-interface command, [669](#)**

**S-PAN (Secondary PAN), [705–708](#)**

**SPAN (Switched Port Analyzer)**

configuration, [156](#)

Kerberos sniffing via, [610–611](#)

**SPF (Secondary PAN First) flow, [705–708](#)**

**sponsored guest portals, [313](#)**

Active Directory identity stores, [304–305](#)

guest sponsor groups, [307–309](#)

guest types, [305–307](#)

layout, [319](#)

multiple guest portals, [318](#)

overview of, [304](#)  
portal page customization, [315](#)  
sponsor portal behavior and flow settings, [313–314](#)

**SSID (service set identifier), [5, 526](#)**  
Corporate SSIDs, creating, [240–245](#)  
dual-SSID onboarding, [387, 401–408](#)  
single-SSID onboarding, [387–388, 394–401](#)

**SSL (Secure Sockets Layer), [467](#)**  
staged deployment. See [phased deployment](#)

**Standard policies, [249](#)**

**START packet, [14–16](#)**

**statements**  
deny, [230](#)  
permit, [230](#)

**Stealthwatch, [6, 618–619, 652–657](#)**

**STOP packet, [16](#)**

**Subject Alternative Names (SAN), [454](#)**

**subnets**  
mapping to SGTs, [569](#)  
NMAP Scan Subnet Exclusions, [183](#)

**subscribers, [635](#)**

**SUCCESS packet, [16](#)**

**Summary dashboard, [660–661](#)**

**super administrator accounts, [126–127](#)**

**supplicant-less network access, [27](#)**

**supplicants**  
choosing, [366–367](#)  
comparison of, [366–367](#)  
configuration, [365–366](#)  
Cisco AnyConnect Secure Mobility Client NAM, [377–381](#)  
Mac OS X C10.8.2 native supplicant, [367–369](#)  
Windows 7, [8/8.1, and 10](#) native supplicants, [373–377](#)  
Windows GPO configuration for wired supplicant, [369–373](#)  
definition of, [32, 42–43](#)  
native supplicants, [365, 408–423](#)

**support bundle**, [702–703](#)

**supported infrastructure components**, list of, [41](#)

**Switched Port Analyzer**. See [SPAN \(Switched Port Analyzer\)](#)

**switches**. See also [device administration](#)

C3PL switch configuration, [196, 213–215](#)

ACLs (access control lists), [219–220](#)

certificates, [216–217](#)

differentiated authentication, [214](#)

global 802.X commands, [220–221](#)

global RADIUS commands, [217–219](#)

local service templates, [219–220](#)

policies, [222–224](#)

Classic IOS/IOS 15.x switch configuration, [195–196](#)

ACLs (access control lists), [202–203](#)

authentication settings, [211–212](#)

authentication timers, [212](#)

certificates, [196–197](#)

Flex-Auth (Flexible Authentication), [208–211](#)

global 802.X commands, [204](#)

global AAA commands, [198–199](#)

global logging commands, [204–205](#)

global profiling commands, [205–207](#)

global RADIUS commands, [199–202](#)

HTTP/HTTPS server, [197](#)

Monitor Mode, [213](#)

switch port interfaces, [208](#)

configuring device admin AAA with, [777](#)

Helpdesk profile, [781–782](#)

NetAdmin profile, [779–780](#)

NetOps profile, [780–781](#)

network device preparation, [778–779](#)

policy sets, [782–783](#)

SecAdmin profile, [781](#)

TACACS+, enabling, [783–784](#)

user roles, [777–778](#)

device admin AAA with Cisco Nexus switches, [777](#)

Helpdesk profile, [781–782](#)  
NetAdmin profile, [779–780](#)  
NetOps profile, [780–781](#)  
network device preparation, [778–779](#)  
policy sets, [782–783](#)  
SecAdmin profile, [781](#)  
TACACS+, enabling, [783–784](#)  
user roles, [777–778](#)

guest CWA (Central Web Authentication), [321–322](#)

native SGT propagation

- Catalyst 6500, [584–586](#)
- Classic IOS/IOS 15.x switches, [582–584](#)
- Nexus series, [586–587](#)

**switchport command**, [208](#)

**SXP (SGT Exchange Protocol)**, [569](#)

- configuration
  - on Cisco ASA, [576–577](#)
  - on IOS devices, [572–573](#)
  - on ISE, [578–579](#)
  - on wireless LAN controllers, [573–575](#)
- design, [570–572](#)
- support for, [27](#)

**Syslog**

- passive identities, [611–615](#)
- providers, [612–614](#)

**System SNMPQUERY probe**, [148](#)

## T

### TACACS+

- accounting messages, [15–17](#)
- authentication messages, [14–15](#)
- authorization messages, [15–17](#)
- client-server communication, [13–14](#)
- command sets, [733–734](#)
- compared to RADIUS, [21](#)
- enabling, [726–727](#)

device admin AAA with Cisco WLC, [768–770](#)

ISE for Nexus device admin AAA, [783–784](#)

logs, [660](#)

profiles, [734–736](#)

support for, [26](#)

## **TC-NAC (Threat-Centric Network Access Control)**

authorization conditions, [112–113](#)

in incident response process, [113–116](#)

logs, [660](#)

reports, [115–116](#)

software support, [111–112](#)

## **TCP Dump, [678–680](#)**

### **templates**

certificate templates, [411–413](#)

service templates, [219–220](#)

## **tenets of passive identification, [596–597](#)**

Learn, [598, 615](#)

Share, [615–616](#)

Update, [623](#)

Use, [617–618](#)

## **Terminal Access Controller Access-Control System. See [TACACS+](#)**

## **Terminal Services (TS) Agent, [615](#)**

### **test aaa command, [752](#)**

### **testing. See also [troubleshooting](#)**

client-based remote access VPNs

AAA test, [488–490](#)

connecting to VPN, [490–491](#)

logging in to web portal, [490–491](#)

device admin AAA with Cisco IOS, [752–758](#)

device admin AAA with Cisco WLC, [770–775](#)

## **TFTP repositories, [711](#)**

## **Threat dashboard, [663](#)**

## **Threat Events report, [115](#)**

## **Threat-Centric Network Access Control. See [TC-NAC \(Threat-Centric Network Access Control\)](#)**

## **threats, 2–3**

Cisco Rapid Threat Containment, [29](#)

CVSS (Common Vulnerability Scoring System), [111](#)

TC-NAC (Threat-Centric Network Access Control)

    authorization conditions, [112–113](#)

    in incident response process, [113–116](#)

    software support, [111–112](#)

Threat dashboard, [663](#)

## **timeouts, session, 625**

## **timers, 212**

## **TLS (Transport Layer Security), 440, 467**

## **tools. See also [commands](#)**

    diagnostic tools, [674](#)

        Endpoint Debug, [680–682](#)

        Evaluate Configuration Validator, [675–678](#)

        RADIUS Authentication Troubleshooting, [674–675](#)

        Session Trace, [682–685](#)

        TCP Dump, [678–680](#)

    monitoring tools

        Context Visibility views, [663–665](#)

        data repository setup, [671–672](#)

        device configuration for monitoring, [669–670](#)

        global search, [667–669](#)

        ISE alarms, [672](#)

        ISE Home Page, [660–663](#)

        ISE reporting, [670–671](#)

        Monitoring nodes, [669](#)

        RADIUS Live Logs and Live Sessions views, [666–667](#)

## **Top Authorizations by User report, 132**

## **Track Movement field (authorization profiles), 255**

## **transition from Monitor Mode to end state, 534–535**

## **Transport Layer Security (TLS), 440, 467**

## **triggered NetFlow, 191–194**

## **Triple-A. See [AAA \(authentication, authorization, and accounting\)](#)**

## **troubleshooting, 30, 673**

authentication and authorization, [685](#)  
active troubleshooting, [688–696](#)

high-level troubleshooting flowchart, [697](#)

ISE logs, [701–703](#)

log deduplication, [686–688](#)

WebAuth and URL redirection, [697–701](#)

device admin AAA with Cisco IOS, [752–758](#)

device admin AAA with Cisco WLC, [770–775](#)

diagnostic tools, [674](#)

Endpoint Debug, [680–682](#)

Evaluate Configuration Validator, [675–678](#)

RADIUS Authentication Troubleshooting, [674–675](#)

Session Trace, [682–685](#)

TCP Dump, [678–680](#)

posture assessment, [361–362](#)

**trust, pxGrid (Platform Exchange Grid) and, [637–638](#)**

**TrustSec, [4, 557–558](#)**

definition of, [562](#)

enforcement, [587–588](#)

with security group firewalls, [591–592](#)

with SGACLs, [588–591](#)

ingress access control challenges, [558–561](#)

pxGrid (Platform Exchange Grid), [579–580](#)

Security Group Tags (SGTs), [33](#)

SGTs (Security Group Tags), [562–563](#)

assigning, [566–568](#)

binding IP addresses to, [568](#)

classification, [565–566](#)

defining, [564–565](#)

mapping subnets to, [569](#)

mapping VLANs to, [569](#)

native tagging, [580–587](#)

SXP (SGT Exchange Protocol), [569](#)

configuration on Cisco ASA, [576–577](#)

configuration on IOS devices, [572–573](#)

configuration on ISE, [578–579](#)

configuration on wireless LAN controllers, [573–575](#)

design, [570–572](#)

**TS (Terminal Services) Agent**, [615](#)

tunneled EAP, [269–270](#)

## U

**Umbrella Roaming module**, [469](#)

unauthenticated guest access, [33](#)

unavailable client provisioning policy action, [420–421](#)

**Unified Capabilities Approved Product List**, [30](#)

unique usernames and passwords, enforcing, [126–128](#)

unknown endpoints, custom profiles for, [538](#)

  collecting information for, [541–542](#)

  profiler conditions, [542–543](#)

  profiler policies, [543–544](#)

  unique values for unknown devices, [539–541](#)

**unquarantine action**, [632](#)

**untrusted certificates, importing**, [440](#)

**Update Report Page link (profiler feed service)**, [162](#)

**Update tenet (passive identification)**, [623](#)

**updates, posture**, [337](#)

**upgrades (ISE)**

  command-line upgrade, [718–720](#)

  GUI upgrade tool, [714–718](#)

  repositories, [708–713](#)

  Secondary PAN First (SPF) flow, [705–708](#)

  upgrade process, [705–708](#)

**UPN (user principle name)**, [615](#)

**URLs**

  adding for ACL bypass, [231–232](#)

  adding to ACL\_WEBAUTH\_REDIRECT, [392](#)

  redirection, [697–701](#)

**U.S. Computer readiness team**, [99](#)

**Use tenet (passive identification)**, [617–618](#)

**user accounting**, [131–132](#)

**User Identity Groups screen (Device Administration), [731–732](#)**

**user principle name (UPN), [615](#)**

**username command, [751](#)**

**usernames, unique, [126–128](#)**

**Users view, [665](#)**

## V

**VACL (VLAN ACL), [157, 610](#)**

**validating repositories, [713](#)**

**validity of posture rules, [99–100](#)**

**vdc-admin user role, [777](#)**

**vdc-operator user role, [777](#)**

**verification of profiles, [189](#)**

    context visibility, [190–191](#)

    dashboard, [189–190](#)

    device sensor show commands, [191](#)

    profiler feed service, [162–163](#)

## views

    Context Visibility, [663–665](#)

    Live Sessions, [666–667](#)

**VIP (virtual IP), [155](#)**

**virtual private networks. See [VPNs \(virtual private networks\)](#)**

## visibility

    context visibility, [169–178, 190–191](#)

    ISE deployment, [69](#)

        DHCP probe, [74–75](#)

        RADIUS probe, [74](#)

        SNMPQUERY probe, [73–74](#)

    Visibility Setup Wizard, [69–73](#)

**Visibility Setup Wizard, [69–73](#)**

    DHCP probe, [74–75](#)

    RADIUS probe, [74](#)

    SNMPQUERY probe, [73–74](#)

**VLAN ACL (VACL), [157, 610](#)**

**VLANs**

assignment, [558–560](#)

dynamic interfaces for, [233–235](#)

mapping to SGTs, [569](#)

wireless LANs

Corporate SSID, [240–245](#)

Guest WLAN, [236–240](#)

## **VMware Promiscuous Mode, [159](#)**

### **VPNs (virtual private networks)**

authentication, [5, 32](#)

certificate-based authentication

authenticating VPN with certificates, [515–518](#)

connecting to VPN via CertProfile, [518–519](#)

provisioning certificates, [509–515](#)

client-based RA-VPN configuration

AnyConnect connection profiles, [473–478](#)

AnyConnect Headend packages, downloading, [469–470](#)

client address pool, [481–484](#)

configuration tools, [469–470](#)

Headend preparation, [471–473](#)

ISE configuration, [487–488](#)

network reachability tasks, [484–487](#)

PSNs (Policy Service Nodes), [478–481](#)

security services modules, [468–469](#)

testing, [488–494](#)

clientless remote access VPNs, [466–467](#)

connecting to, [490–491](#)

double authentication, [507–508](#)

overview of, [465–468](#)

RA-VPN with posture flows, [495–496](#)

ACLs (access control lists), [496–499](#)

authorization policies, [501](#)

authorization profiles, [499–500](#)

sample session, [501–506](#)

## **vSwitch Promiscuous Mode, [159](#)**

## **Vulnerability Assessment report, [116](#)**

## **Vulnerability dashboard, [662](#)**

# **W**

**web authentication**, [32](#), [36](#), [415–420](#). See also [\*\*CWA \(Central Web Authentication\)\*\*](#)

**Web Authentication Redirection ACL**, [230–231](#)

**web portals**

logging in to, [490–491](#)

redirect to, [5](#)

**Web Security Appliance**. See [\*\*WSA \(Web Security Appliance\)\*\*](#)

**WebAuth**

portals, [415–420](#)

troubleshooting, [697–701](#)

**Web-Deploy mode**, [469](#)

**Windows 7 supplicants**

native supplicant configuration, [373–377](#)

Windows GPO configuration for wired supplicant, [373–377](#)

**Windows 8/8.1 supplicants**

native supplicant configuration, [373–377](#)

Windows GPO configuration for wired supplicant, [373–377](#)

**Windows 10 supplicants**

native supplicant configuration, [373–377](#)

Windows GPO configuration for wired supplicant, [373–377](#)

**Windows GPO**, [369–373](#)

**Windows Management Instrumentation**. See [\*\*WMI \(Windows Management Instrumentation\)\*\*](#)

**Windows onboarding**, [428–429](#)

**Wired domain**, [86](#)

wired supplicants, Windows GPO configuration for, [369–373](#)

wired switches, guest CWA (Central Web Authentication) for, [321–322](#)

**Wireless domain**, [87](#)

**Wireless LAN Controller**. See [\*\*WLCs \(Wireless LAN Controllers\)\*\*](#)

**wireless networks**. See also [\*\*WLCs \(Wireless LAN Controllers\)\*\*](#)

Corporate SSID, [240–245](#)

Guest WLAN, [236–240](#)

ISE deployment, [59–60](#)

BYOD (Bring Your Own Device) Wizard, [67–69](#)

Guest Self-Registration Wizard, [61–65](#)

Secure Access Wizard, [65–67](#)

Wireless Setup Wizard home page, [59–60](#)

phased deployment, [535](#)

## **WIRELESS role, [760](#)**

### **Wireless Setup Wizard**

BYOD (Bring Your Own Device) Wizard, [67–69](#)

Guest Self-Registration Wizard, [61–65](#)

home page, [60–61](#)

Secure Access Wizard, [65–67](#)

startup, [59–60](#)

### **wireless SSID, [272–276](#)**

### **wizards**

Visibility Setup Wizard, [69–73](#)

DHCP probe, [74–75](#)

RADIUS probe, [74](#)

SNMPQUERY probe, [73–74](#)

### **Wireless Setup Wizard**

BYOD (Bring Your Own Device) Wizard, [67–69](#)

Guest Self-Registration Wizard, [61–65](#)

home page, [60–61](#)

Secure Access Wizard, [65–67](#)

startup, [60–61](#)

## **WLAN role, [760](#)**

### **WLCs (Wireless LAN Controllers), [59](#)**

AireOS features, [225–226](#)

BYOD onboarding, [388–390](#)

configuration, [225](#)

Airespace ACLs, [229–232](#)

Corporate SSID, [240–245](#)

dynamic interfaces for client VLANs, [233–235](#)

Guest WLAN, [236–240](#)

RADIUS accounting servers, [227–228](#)

RADIUS authentication servers, [226–227](#)

RADIUS fallback, [229](#)

roles, [760](#)

SXP (SGT Exchange Protocol) configuration, [573–575](#)

## device admin AAA

- Employee profile, [765–766](#)
  - Helpdesk profile, [765](#)
  - NetAdmin profile, [763–764](#)
  - network device preparation, [761–762](#)
  - overview of, [759–760](#)
  - policy sets, [766–768](#)
  - SecAdmin profile, [764](#)
  - TACACS+, enabling, [768–770](#)
  - testing and troubleshooting, [770–775](#)
- DHCP probe considerations, [141](#)
- guest CWA (Central Web Authentication), [322–325](#)

## WMI (Windows Management Instrumentation)

- benefits of, [599](#)
- configuration, [599–603](#)

## Work Centers

- Device Administration Work Center, [728–729](#)
  - Connection settings, [729](#)
  - Device Admin Policy Sets, [736–738](#)
  - Ext ID Sources, [731–732](#)
  - Identities, [731–732](#)
  - navigation UI, [730–731](#)
  - Network Resources, [733](#)
  - Password Change Control settings, [729](#)
  - Policy Elements, [733–736](#)
  - Reports, [738](#)
  - Session Key Assignment settings, [729–730](#)
  - User Identity Groups, [731–732](#)
- PassiveID Work Center, [596–597](#)
- Posture Assessment Work Center, [328–329](#)
- Profiler Work Center, [137, 537–538](#)

## WSA (Web Security Appliance), [649–652](#)

## X–Y–Z

### XCP (Extensible Communication Platform), [636](#)

### XMPP (Extensible Messaging and Presence Protocol), [636](#)





# The Cisco Learning Network

The IT Community that helps you get Cisco Certified.



Be a Part of the  
Community



Prepare for  
Success



Interact with  
Professionals



Mentor, Share,  
Achieve

Join over 1 Million Members on the Cisco Learning Network, featuring powerful study resources like IT Training Videos, Study Groups and Certification Exam Topics.

Connect with us on social media at:  
[cs.co/LearningatCisco-About](http://cs.co/LearningatCisco-About)



[ciscolearningnetwork.com](http://ciscolearningnetwork.com)





**REGISTER YOUR PRODUCT** at [CiscoPress.com/register](http://CiscoPress.com/register)  
Access Additional Benefits and SAVE 35% on Your Next Purchase

- Download available product updates.
- Access bonus material when applicable.
- Receive exclusive offers on new editions and related products.  
(Just check the box to hear from us when setting up your account.)
- Get a coupon for 35% for your next purchase, valid for 30 days.  
Your code will be available in your Cisco Press cart. (You will also find it in the Manage Codes section of your account page.)

Registration benefits vary by product. Benefits will be listed on your account page under Registered Products.

---

CiscoPress.com – Learning Solutions for Self-Paced Study, Enterprise, and the Classroom  
Cisco Press is the Cisco Systems authorized book publisher of Cisco networking technology, Cisco certification self-study, and Cisco Networking Academy Program materials.

At [CiscoPress.com](http://CiscoPress.com) you can

- Shop our books, eBooks, software, and video training.
- Take advantage of our special offers and promotions ([ciscopress.com/promotions](http://ciscopress.com/promotions)).
- Sign up for special offers and content newsletters ([ciscopress.com/newsletters](http://ciscopress.com/newsletters)).
- Read free articles, exam profiles, and blogs by information technology experts.
- Access thousands of free chapters and video lessons.

Connect with Cisco Press – Visit [CiscoPress.com/community](http://CiscoPress.com/community)  
Learn about Cisco Press community events and programs.



**Cisco Press**



# Code Snippets

Many titles include programming code or configuration examples. To optimize the presentation of these elements, view the eBook in single-column, landscape mode and adjust the font size to the smallest setting. In addition to presenting code and configurations in the reflowable text format, we have included images of the code that mimic the presentation found in the print book; therefore, where the reflowable format may compromise the presentation of the code listing, you will see a “Click here to view code image” link. Click the link to view the print-fidelity code image. To return to the previous page viewed, click the Back button on your device or app.

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
ip radius source-interface <Interface>
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 host <ISE_PSN_Address> auth-port 1812 acct-port 1813 key xxx
radius-server vsa send accounting
radius-server vsa send authentication
```

```
<line #> Permit|Deny <protocol> from <device(s) | network(s)> to <device(s) |  
network(s)> equaling | not equaling port(s) <list of port numbers or names>  
Description: <explanation of rule>
```

10 Deny IP from any to any internal network

Description: Block IP traffic from anyone to any internal subnet or device.

20 Permit tcp from guest authorization rule to any equaling ports 53,80 & 443

Description: Allow web traffic from clients in the guest authorization rule to the internet

30 Deny IP from guest authorization rule to any

Description: Block everything else

Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_11) AppleWebKit/601.1.27 (KHTML, like Gecko)

Version/8.1 Safari/601.1.27

Mozilla/5.0Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko

```
DC-4948(config)# monitor session [1-4] source [interface | vlan] [rx | tx]
DC-4948(config)# monitor session [1-4] destination interface [interface name]
```

```
3750-X# show device-sensor cache all
```

```
Device: 0050.5687.0004 on port GigabitEthernet1/0/2
```

Proto	Type:Name	Len	Value
dhcp	43:vendor-encapsulated-optio	5	2B 03 DC 01 00
dhcp	55:parameter-request-list	14	37 0C 01 0F 03 06 2C 2E 2F 1F 21 F9 2B FC
dhcp	60:class-identifier	10	3C 08 4D 53 46 54 20 35 2E 30
dhcp	12:host-name	12	0C 0A 58 59 5A 2D 42 69 6F 4D 65 64
dhcp	61:client-identifier	9	3D 07 01 00 50 56 87 00 04
dhcp	77:user-class-id	13	4D 0B 73 79 6D 75 6E 75 73 2D 62 69 6F

```
event manager applet CaptureData
  event syslog pattern "Authorization succeeded for client"
  action 1.0 regexp "Interface (.*) AuditSessionID" "$_syslog_msg" match intname
  action 1.1 cli command "enable"
  action 1.2 cli command "show auth sess int $intname | i SGT"
  action 1.3 set sgttag "0000-0"
  action 1.4 regexp "000C-0" "$sgttag"
  action 1.5 regexp "SGT:  (.*)" "$_cli_result" match sgttag
  action 1.6 regexp "000C-0" "$sgttag"
  action 1.7 if $_regexp_result eq "1"
  action 1.8  cli command "conf t"
  action 1.9  cli command "int $intname"
  action 2.0  cli command "ip flow ingress"
  action 2.1 else
  action 2.2  cli command "conf t"
  action 2.3  cli command "int $intname"
  action 2.4  cli command "no ip flow ingress"
  action 2.5 end
```

```
flow record ise-flows
description export only flows needed by ise
match datalink mac source-address
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport tcp flags
!
flow exporter ISE
description Export to ISE PSN1
destination 10.1.100.234
source TenGigabitEthernet1/1/1
transport udp 9996
!
flow exporter ISE-flows
!
flow monitor ISE-Flows
description Used for ISE Profiler
record ise-flows
exporter ISE
```

```
cache timeout active 60
!
flow monitor CaptureData
  record ise-flows
!
flow monitor test
```

```
C3560X(config)# radius-server host ise_ip_address auth-port 1812  
acct-port 1813 test username radius-test key shared_secret
```

```
C3560X(config)# radius-server dead-criteria time 5 tries 3  
C3560X(config)# radius-server deadtime 15
```

```
C3560X(config)# aaa server radius dynamic-author
C3560X(config-locsvr-da-radius)# client ise_ip_address server-key
shared_secret
```

```
C3560X(config)# radius-server vsa send authentication  
C3560X(config)# radius-server vsa send accounting
```

```
C3560X(config)# radius-server attribute 6 on-for-login-auth  
C3560X(config)# radius-server attribute 8 include-in-access-req  
C3560X(config)# radius-server attribute 25 access-request include
```

```
C3560X(config)# ip radius source-interface interface_name
C3560X(config)# snmp-server trap-source interface_name
C3560X(config)# snmp-server source-interface informs interface_name
```

```
Cat4503(config)# username radius-test password password
```

```
Cat4503 (config)# radius server server-name
Cat4503 (config-radius-server)# address ipv4 address auth-port 1812
    acct-port 1813
Cat4503 (config-radius-server)# key Shared-Secret
Cat4503 (config-radius-server)# automate-tester username radius-test
    probe-on
```

```
Cat4503(config)# radius-server dead-criteria time 5 tries 3
Cat4503(config)# radius-server deadtime 15
```

```
Cat4503(config)# aaa server radius dynamic-author
Cat4503(config-locsvr-da-radius)# client ise_ip_address server-key
shared_secret
```

```
Cat4503(config)# radius-server vsa send authentication  
Cat4503(config)# radius-server vsa send accounting
```

```
Cat4503 (config)# radius-server attribute 6 on-for-login-auth
Cat4503 (config)# radius-server attribute 8 include-in-access-req
Cat4503 (config)# radius-server attribute 25 access-request include
```

```
Cat4503(config)# ip radius source-interface interface_name
Cat4503(config)# snmp-server trap-source interface_name
Cat4503(config)# snmp-server source-interface informs interface_name
```

```
C3560X(config)# ip access-list extended ACL-ALLOW
C3560X(config-ext-nacl)# permit ip any any
```

```
C3560X(config)# ip access-list ext ACL-DEFAULT
C3560X(config-ext-nacl)# remark DHCP
C3560X(config-ext-nacl)# permit udp any eq bootpc any eq bootps
C3560X(config-ext-nacl)# remark DNS
C3560X(config-ext-nacl)# permit udp any any eq domain
C3560X(config-ext-nacl)# remark Ping
C3560X(config-ext-nacl)# permit icmp any any
C3560X(config-ext-nacl)# remark PXE / TFTP
C3560X(config-ext-nacl)# permit udp any any eq tftp
C3560X(config-ext-nacl)# remark Drop all the rest
C3560X(config-ext-nacl)# deny ip any any log
```

```
C3560X(config)# ip access-list extended ACL-WEBAUTH-REDIRECT
C3560X(config-ext-nacl)# remark explicitly deny DNS from being
    redirected to address a bug
C3560X(config-ext-nacl)# deny udp any any eq 53
C3560X(config-ext-nacl)# remark redirect all applicable traffic to the
    ISE Server
C3560X(config-ext-nacl)# permit tcp any any eq 80
C3560X(config-ext-nacl)# permit tcp any any eq 443
C3560X(config-ext-nacl)# remark all other traffic will be implicitly
    denied from the redirection
```

```
C3560X(config)# ip access-list extended ACL-AGENT-REDIRECT
C3560X(config-ext-nacl)# remark explicitly deny DNS and DHCP from being
    redirected
C3560X(config-ext-nacl)# deny udp any any eq 53 bootps
C3560X(config-ext-nacl)# remark redirect HTTP traffic only
C3560X(config-ext-nacl)# permit tcp any any eq 80
C3560X(config-ext-nacl)# remark all other traffic will be implicitly
    denied from the redirection
```

```
C3560X(config)# logging monitor informational
C3560X(config)# logging origin-id ip
C3560X(config)# logging source-interface interface_id
C3560X(config)# logging host ISE_MNT_PERSONA_IP_Address_x transport udp
port 20514
```

```
C3560X(config)# device-sensor filter-list dhcp list dhcp_list_name
C3560X(config-sensor-dhcplist)# option name host-name
C3560X(config-sensor-dhcplist)# option name class-identifier
C3560X(config-sensor-dhcplist)# option name client-identifier
```

```
C3560X(config)# device-sensor filter-list cdp list cdp_list_name
C3560X(config-sensor-cdplist)# tlv name device-name
C3560X(config-sensor-cdplist)# tlv name platform-type
```

```
C3560X(config)# device-sensor filter-list lldp list lldp_list_name
C3560X(config-sensor-lldplist)# tlv name port-id
C3560X(config-sensor-lldplist)# tlv name system-name
C3560X(config-sensor-lldplist)# tlv name system-description
```

```
C3560X(config)# device-sensor filter-spec dhcp include list  
      dhcp_list_name  
C3560X(config)# device-sensor filter-spec cdp include list cdp_list_name  
C3560X(config)# device-sensor filter-spec lldp include list lldp_list_name
```

```
C3560X(config)# device-sensor accounting  
C3560X(config)# device-sensor notify all-changes
```

```
C3560X(config-if-range)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
```

```
C3560X(config-if-range)# authentication event server dead action
    authorize vlan vlan-id
C3560X(config-if-range)# authentication event server dead action
    authorize voice
C3560X(config-if-range)# authentication event server alive action
    reinitialize
```

```
C3850(config)# radius server server-name
C3850(config-radius-server)# address ipv4 address auth-port 1812
    acct-port 1813
C3850(config-radius-server)# key Shared-Secret
C3850(config-radius-server)# automate-tester username radius-test probe-on
```

```
C3850(config)# radius-server dead-criteria time 5 tries 3
C3850(config)# radius-server deadtime 15
```

```
C3850(config)# aaa server radius dynamic-author
C3850(config-locsvr-da-radius)# client ise_ip_address server-key
    shared secret
```

```
C3850(config)# radius-server vsa send authentication  
C3850(config)# radius-server vsa send accounting
```

```
C3850(config)# radius-server attribute 6 on-for-login-auth
C3850(config)# radius-server attribute 8 include-in-access-req
C3850(config)# radius-server attribute 25 access-request include
C3850(config)# radius-server attribute 31 mac format ietf upper-case
C3850(config)# radius-server attribute 31 send nas-port-detail mac-only
```

```
Cat4503(config)# ip radius source-interface interface_name
Cat4503(config)# snmp-server trap-source interface_name
Cat4503(config)# snmp-server source-interface informs interface_name
```

```
C3850(config)# ip access-list extended ACL-ALLOW
C3850(config-ext-nacl)# permit ip any any
```

```
C3850(config)# ip access-list extended ACL-DEFAULT
C3850(config-ext-nacl)# remark DHCP
C3850(config-ext-nacl)# permit udp any eq bootpc any eq bootps
C3850(config-ext-nacl)# remark DNS
C3850(config-ext-nacl)# permit udp any any eq domain
C3850(config-ext-nacl)# remark Ping
C3850(config-ext-nacl)# permit icmp any any
C3850(config-ext-nacl)# remark PXE / TFTP
C3850(config-ext-nacl)# permit udp any any eq tftp
C3850(config-ext-nacl)# remark Drop all the rest
C3850(config-ext-nacl)# deny ip any any log
```

```
C3850(config)# ip access-list extended ACL-WEBAUTH-REDIRECT
C3850(config-ext-nacl)# remark explicitly deny DNS from being
    redirected to address a bug
C3850(config-ext-nacl)# deny udp any any eq 53
C3850(config-ext-nacl)# remark redirect all applicable traffic to the
    ISE Server
C3850(config-ext-nacl)# permit tcp any any eq 80
C3850(config-ext-nacl)# permit tcp any any eq 443
C3850(config-ext-nacl)# remark all other traffic will be implicitly
    denied from the redirection
```

```
C3850(config)# ip access-list extended ACL-AGENT-REDIRECT
C3850(config-ext-nacl)# remark explicitly deny DNS and DHCP from being
    redirected
C3850(config-ext-nacl)# deny udp any any eq 53 bootps
C3850(config-ext-nacl)# remark redirect HTTP traffic only
C3850(config-ext-nacl)# permit tcp any any eq 80
C3850(config-ext-nacl)# remark all other traffic will be implicitly
    denied from the redirection
```

```
C3850(config)# service-template CRITICAL
C3850(config-service-template)# description Apply for Critical Auth
C3850(config-service-template)# access-group ACL-ALLOW
```

```
C3850(config)# class-map type control subscriber match-any AAA-DOWN  
C3850(config-filter-control-classmap)# match result-type aaa-timeout
```

```
C3850(config)# class-map type control subscriber match-all DOT1X-FAILED
C3850(config-filter-control-classmap)# match method dot1x
C3850(config-filter-control-classmap)# match result-type method dot1x
    authoritative
```

```
C3850(config-event-control-policymap)# event session-started match-all
C3850(config-class-control-policymap)# 10 class always do-all
C3850(config-action-control-policymap)# 10 authenticate using dot1x
  priority 10
C3850(config-action-control-policymap)# 20 authenticate using mab
  priority 20
```

```
C3850(config-action-control-policymap)# event violation match-all
C3850(config-class-control-policymap)# 10 class always do-all
C3850(config-action-control-policymap)# 10 restrict
```

```
C3850(config-action-control-policymap)# event agent-found match-all  
C3850(config-class-control-policymap)# 10 class always do-all  
C3850(config-action-control-policymap)# 10 authenticate using dot1x
```

```
C3850(config-action-control-policymap)# event authentication-failure  
      match-all  
C3850(config-class-control-policymap)# 10 class AAA-DOWN do-all  
C3850(config-action-control-policymap)# 10 authorize  
C3850(config-action-control-policymap)# 20 activate service-template  
      CRITICAL  
C3850(config-action-control-policymap)# 30 terminate dot1x  
C3850(config-action-control-policymap)# 40 terminate mab  
C3850(config-action-control-policymap)# 20 class DOT1X-FAILED do-all  
C3850(config-action-control-policymap)# 10 authenticate using mab
```

```
C3850(config)# interface range GigabitEthernet 1/0/1 - 24
C3850(config-if-range)# description Dot1X Enabled Ports
C3850(config-if-range)# switchport host
C3850(config-if-range)# service-policy type control subscriber
    DOT1X-DEFAULT
```

```
C3850(config-if-range)# authentication periodic
C3850(config-if-range)# authentication timer reauthenticate server
C3850(config-if-range)# mab
C3850(config-if-range)# ip access-group DEFAULT-ACL in
C3850(config-if-range)# access-session host-mode multi-auth
C3850(config-if-range)# no access-session closed
C3850(config-if-range)# dot1x timeout tx-period 10
C3850(config-if-range)# access-session port-control auto
C3850(config-if-range)# no shutdown
```

```
permit udp any any eq bootps
permit udp any any eq domain
permit tcp any any eq domain
remark ping for troubleshooting
permit icmp any any echo
permit icmp any any echo-reply
remark allow web traffic to the ISE PSN 10.1.100.232
permit tcp any 10.1.100.232 eq 80
permit tcp any 10.1.100.232 eq 443
remark allow internet-only web traffic to kick off redirect
deny tcp any <Internal networks> eq 80
deny tcp any <Internal networks> eq 443
permit tcp any any eq 80
permit tcp any any eq 443
remark 10.1.100.232 is the ISE PSN for Guest Portal
permit tcp any host 10.1.100.232 eq 8443
permit tcp any host 10.1.100.232 eq 8905
permit tcp any host 10.1.100.232 eq 8909
permit udp any host 10.1.100.232 range 8905 8906
permit udp any host 10.1.100.232 eq 8909
deny ip any any
```

```
ip access-list extended ACL-WEBAUTH-REDIRECT
    deny ip any host 10.1.100.232
    permit tcp any any eq www
    permit tcp any any eq 443
    permit tcp any any eq 8443
```

```
remark be sure to include any proxy ports you have enabled  
permit tcp any any eq 8080
```

```
ip access-list extended webauth
permit udp any any eq bootps
permit udp any any eq domain
permit tcp any any eq domain
remark ping for troubleshooting
permit icmp any any echo
permit icmp any any echo-reply
remark allow web traffic to kick off redirect
permit tcp any any eq www
permit tcp any any eq 443
remark 10.1.100.232 is the ISE PSN for Guest Portal
permit tcp any host 10.1.100.232 eq 8443
permit tcp any host 10.1.100.232 eq 8905
permit tcp any host 10.1.100.232 eq 8909
permit udp any host 10.1.100.232 range 8905 8906
permit udp any host 10.1.100.232 eq 8909
```

```
ip access-list extended ACL-WEBAUTH-REDIRECT
    deny ip any host 10.1.100.232
    permit tcp any any eq www
    permit tcp any any eq 443
    permit tcp any any eq 8443
    remark be sure to include any proxy ports you have enabled
    permit tcp any any eq 8080
```

```
ip http server
ip http secure-server
interface GigabitEthernet1/0/12
    description ISE1 - dot1x clients - UCS Eth0
    switchport access vlan 100
    switchport mode access
    ip access-group webauth in
    authentication order mab
    authentication priority mab
    authentication port-control auto
    mab
    spanning-tree portfast
```

```
remark Allow DHCP
permit udp any eq bootpc any eq bootps
remark Allow DNS
permit udp any any eq domain
remark Allow ping to ISE PSN and any other devices necessary
permit icmp any host <ISE PSN IP>
! This is for URL redirect
permit tcp any host <ISE PSN IP> eq 443
! This is for URL redirect
permit tcp any host <ISE PSN IP> eq www
! This is for guest portal
permit tcp any host <ISE PSN IP> eq 8443
! This is for posture
! Communication between NAC agent and ISE (SWISS ports)
permit tcp any host <ISE PSN IP> eq 8905
! This is for posture
! Communication between NAC agent and ISE (SWISS ports)
permit udp any host <ISE PSN IP> eq 8905
deny ip any any
```

```
atw-ise245/admin# show application status ise
```

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	5851
Database Server	running	75 PROCESSES
Application Server	initializing	
Profiler Database	running	6975
ISE Indexing Engine	running	1821
AD Connector	running	10338
M&T Session Database	running	1373
M&T Log Collector	running	2313
M&T Log Processor	running	2219
Certificate Authority Service	disabled	
EST Service	disabled	
SXP Engine Service	disabled	
TC-NAC Docker Service	disabled	
TC-NAC MongoDB Container	disabled	
TC-NAC RabbitMQ Container	disabled	
TC-NAC Core Engine Container	disabled	
VA Database	disabled	
VA Service	disabled	
pxGrid Infrastructure Service	disabled	
pxGrid Publisher Subscriber Service	disabled	
pxGrid Connection Manager	disabled	
pxGrid Controller	disabled	
PassiveID Service	disabled	
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	

```
atw-ise245/admin#
```

```
interface gig 0
    !Actual IP of Node
    ip address 1.1.1.163 255.255.255.0
interface gig 1
    !Anycast VIP assigned to all PSN nodes on G1
    ip address 2.2.2.2 255.255.255.255

ip default-gateway [Real Gateway for Gig0]
!note no static routes needed.
```

```
ip sla 1
!Test TCP to port 80 to the actual IP of the node.
!"control disable" is necessary, since you are connecting to an
actual host instead of an SLA responder

tcp-connect 1.1.1.163 80 control disable
! Consider the SLA as down if response takes longer than 1000msec

threshold 1000
! Timeout after 1000 msec.

timeout 1000
!Test every 5 Seconds:
frequency 5

ip sla schedule 1 life forever start-time now
track 1 ip sla 1
ip route 2.2.2.2 255.255.255.255 1.1.1.163 track 1
```

```
router eigrp [Autonomous-System-Number]
 redistribute static route-map STATIC-TO-EIGRP

route-map STATIC-TO-EIGRP permit 20
 match ip address prefix-list ISE_VIP
 !Set metrics correctly
 set metric 1000000 1 255 1 1500

ip prefix-list ISE_VIP seq 5 permit 2.2.2.2/32
```

```
3750-X# show aaa server | include host
RADIUS: id 4, priority 1, host 10.1.100.232, auth-port 1812, acct-port 1813
RADIUS: id 5, priority 2, host 10.1.100.233, auth-port 1812, acct-port 1813
RADIUS: id 6, priority 3, host 10.1.100.234, auth-port 1812, acct-port 1813
```

```
3750-X(config)# radius-server load-balance method least-outstanding  
batch-size 5
```

```
atw-tme-5515# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username      : employee1           Index      : 26
Assigned IP   : 192.168.228.2       Public IP   : 10.117.118.215
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 24431             Bytes Rx     : 13670
Pkts Tx       : 33                Pkts Rx     : 67
Pkts Tx Drop : 0                Pkts Rx Drop : 0
Group Policy  : GroupPolicy1      Tunnel Group : ATW-ConnectionProfile
Login Time    : 15:41:04 UTC Wed Mar 22 2017
Duration      : 0h:00m:09s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A              VLAN        : none
Audt Sess ID  : 0a0165fe0001a00058d29b10
Security Grp  : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

< output removed for space >

SSL-Tunnel:
Tunnel ID     : 26.2
Assigned IP   : 192.168.228.2       Public IP   : 10.117.118.215
Encryption    : AES-GCM-256          Hashing     : SHA384
Ciphersuite   : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2             TCP Src Port : 58163
TCP Dst Port : 443                Auth Mode   : userPassword
Idle Time Out: 30 Minutes         Idle TO Left : 29 Minutes
Client OS     : Windows
Client Type   : SSL VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.4.01054
Bytes Tx      : 7354               Bytes Rx     : 816
Pkts Tx       : 5                  Pkts Rx     : 12
Pkts Tx Drop : 0                Pkts Rx Drop : 0
Filter Name   : #ACSAACL#-IP-VPN-PostureNotCompliant-58d1c6f2
```

```
< output removed for space >

ISE Posture:
Redirect URL : https://atw-ise244.securitydemo.net:8443/portal/gateway?sessionId=0
                a0165fe0001a00058d29b10&portal=4cb1...
Redirect ACL : POSTURE-REDIRECT

atw-tme-5515#
```

```
atw-tme-5515# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

Username : employee1	Index : 25
Assigned IP : 192.168.228.2	Public IP : 10.117.118.215
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel	
License : AnyConnect Premium	
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES256	
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA1	
Bytes Tx : 101366	Bytes Rx : 92634
Pkts Tx : 204	Pkts Rx : 511
Pkts Tx Drop : 0	Pkts Rx Drop : 0
Group Policy : GroupPolicy1	Tunnel Group : ATW-ConnectionProfile
Login Time : 15:31:17 UTC Wed Mar 22 2017	
Duration : 0h:05m:29s	
Inactivity : 0h:00m:00s	
VLAN Mapping : N/A	VLAN : none
Audit Sess ID : 0a0165fe0001900058d298c5	
Security Grp : none	
AnyConnect-Parent Tunnels: 1	
SSL-Tunnel Tunnels: 1	
DTLS-Tunnel Tunnels: 1	
< output removed for space >	
SSL-Tunnel:	
Tunnel ID : 25.2	
Assigned IP : 192.168.228.2	Public IP : 10.117.118.215
Encryption : AES-GCM-256	Hashing : SHA384

```
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384
Encapsulation: TLSv1.2                               TCP Src Port : 57916
TCP Dst Port : 443                                 Auth Mode    : userPassword
Idle Time Out: 30 Minutes                          Idle TO Left : 24 Minutes
Client OS   : Windows
Client Type : SSL VPN Client
Client Ver  : Cisco AnyConnect VPN Agent for Windows 4.4.01054
Bytes Tx     : 7354                                Bytes Rx     : 216
Pkts Tx      : 5                                    Pkts Rx      : 4
Pkts Tx Drop : 0                                  Pkts Rx Drop : 0
Filter Name  : #ACSAACL#-IP-VPN-PostureCompliant-58d18405

< output removed for space >

atw-tme-5515#
```

```
flow record ise-flows
description export only flows needed by ise
match datalink mac source-address
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match transport tcp flags
```

```
Cswitch# show flow record
flow record ise-flows:
  Description:      export only flows needed by ise
  No. of users:    0
  Total field space: 20 bytes
  Fields:
    match datalink mac source-address
    match ipv4 protocol
```

```
match ipv4 source address  
match ipv4 destination address  
match transport source-port  
match transport destination-port  
match transport tcp flags
```

```
flow exporter ISE
description Export to ISE PSN1
destination 10.1.103.4
source TenGigabitEthernet1/1/1
transport udp 9996
```

```
Cswitch# show flow exporter
Flow Exporter ISE:
  Description:          Export to ISE PSN1
  Export protocol:      NetFlow Version 9
  Transport Configuration:
    Destination IP address: 10.1.103.4
    Source IP address:      10.1.48.2
    Source Interface:       TenGigabitEthernet1/1/1
    Transport Protocol:     UDP
    Destination Port:      9996
    Source Port:           49736
    DSCP:                  0x0
    TTL:                   255
    Output Features:       Not Used
```

```
flow monitor ISE-Flows
description Used for ISE Profiler
record ise-flows
exporter ISE
cache timeout active 60
```

```
Cswitch# show flow monitor
Flow Monitor ISE-Flows:
  Description:      Used for ISE Profiler
  Flow Record:      ise-flows
  Flow Exporter:    ISE
```

```
Cache:  
  Type:          normal  
  Status:        not allocated  
  Size:          128 entries / 0 bytes  
  
Cache:  
  Type:          normal (Platform cache)  
  Status:        not allocated  
  Size:          Unknown  
  
Timers:  
          Local      Global  
  Inactive Timeout: 15 secs  
  Active Timeout:   60 secs    1800 secs  
  Update Timeout:   1800 secs
```

```
interface TenGigabitEthernet1/1/1
description Cat6K Ten1/5
no switchport
ip flow monitor ISE-Flows input
ip address 10.1.48.2 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP
load-interval 60
```

```
Cswitch# show flow interface tel/1/1
```

```
Interface TenGigabitEthernet1/1/1
FNF: monitor: ISE-Flows
      direction: Input
      traffic(ip): on
```

```
NX7K-DIST(config)# int eth1/3
NX7K-DIST(config-if)# cts manual
NX7K-DIST(config-if-cts-manual)# policy static sgt 0x3
```

```
4503(config)# cts xp enable
4503(config)#
*Aug  9 06:51:04.000: %CTS-5-SXP_STATE_CHANGE: CTS SXP enabled
4503(config)# cts xp connection peer 10.1.40.1 password default mode peer listener
4503(config)#
*Aug 10 09:15:15.564: %CTS-6-SXP_TIMER_START: Connection <0.0.0.0, 0.0.0.0> retry
open timer started.
*Aug 10 09:15:15.565: %CTS-6-SXP_CONN_STATE_CHG: Connection <10.1.40.1, 10.1.40.2>-1
state changed from Off to Pending_On.
4503(config)#
*Aug 10 09:15:15.566: %CTS-3-SXP_CONN_STATE_CHG_OFF: Connection <10.1.40.1,
10.1.40.2>-1 state changed from Pending_On to Off.
4503(config)# cts xp default password TrustSec123
4503(config)#
*Aug 10 09:17:20.936: %CTS-5-SXP_DFT_PASSWORD_CHANGE: CTS SXP password changed.
```

```
C6K-DIST(config)# cts xp enable
C6K-DIST(config)#
Aug 10 16:16:25.719: %CTS-6-SXP_TIMER_START: Connection <0.0.0.0, 0.0.0.0> retry
open timer started.
C6K-DIST(config)# cts xp default password TrustSec123
C6K-DIST(config)# cts xp connection peer 10.1.40.2 password default mode peer speaker
C6K-DIST(config)#
Aug 10 16:17:26.687: %CTS-6-SXP_CONN_STATE_CHG: Connection <10.1.40.2, 10.1.40.1>-1
state changed from Off to Pending_On.
Aug 10 16:17:26.687: %CTS-6-SXP_CONN_STATE_CHG: Connection <10.1.40.2, 10.1.40.1>-1
state changed from Pending_On to On.
```

```
C6K-DIST# sho cts xp connections brief
SXP : Enabled
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
```

Peer_IP	Source_IP	Conn Status	Duration
10.1.40.2	10.1.40.1	On	4:06:36:24 (dd:hr:mm:sec)
10.1.60.2	10.1.60.1	On	0:00:03:31 (dd:hr:mm:sec)

```
Total num of SXP Connections = 2
```

```
C3750X(config)# cts role-based enforcement
C3750X(config)# interface Ten 1/1/1
C3750X(config-if)# cts manual
C3750X(config-if-cts-manual)# policy static sgt 2 trusted
```

```
C3750X# sho cts interface Ten 1/1/1
Global Dot1x feature is Enabled
Interface TenGigabitEthernet1/1/1:
    CTS is enabled, mode:      MANUAL
        IFC state:              OPEN
        Authentication Status:   NOT APPLICABLE
            Peer identity:       "unknown"
            Peer's advertised capabilities: ""
        Authorization Status:    SUCCEEDED
        Peer SGT:                2
        Peer SGT assignment:     Trusted
    SAP Status:                 NOT APPLICABLE
    Configured pairwise ciphers:
        gcm-encrypt
        null
    Replay protection:         enabled
    Replay protection mode:   STRICT
    Selected cipher:
        Propagate SGT:          Enabled
    Cache Info:
        Cache applied to link : NONE
    Statistics:
        authc success:           0
        authc reject:             0
        authc failure:            0
        authc no response:        0
        authc logoff:              0
```

sap success:	0
sap fail:	0
authz success:	3
authz fail:	0
port auth fail:	0
L3 IPM:	disabled.

```
C6K-DIST(config)# platform cts egress
C6K-DIST(config)# cts role-based enforcement
C6K-DIST(config)# interface Ten1/5
C6K-DIST(config-if)# cts manual
C6K-DIST(config-if-cts-manual)# policy static sgt 2 trusted
```

```
C6K-DIST# show cts interface Ten1/5
Global Dot1x feature is Enabled
Interface TenGigabitEthernet1/5:
    CTS is enabled, mode:      MANUAL
    IFC state:                OPEN
    Authentication Status:    NOT APPLICABLE
        Peer identity:        "unknown"
        Peer's advertised capabilities: ""
    Authorization Status:    SUCCEEDED
        Peer SGT:              2
        Peer SGT assignment: Trusted
    SAP Status:               NOT APPLICABLE
        Configured pairwise ciphers:
            gcm-encrypt
            null
        Replay protection:     enabled
        Replay protection mode: STRICT
        Selected cipher:
    Propagate SGT:           Enabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:          0
        authc reject:            0
        authc failure:           0
        authc no response:       0
        authc logoff:             0
        sap success:              0
        sap fail:                  0
        authz success:             1
        authz fail:                  0
        port auth fail:            0
    L3 IPM:      disabled.
```

```
NX7K-CORE(config)# feature dot1x
NX7K-CORE(config)# cts enable
NX7K-CORE(config)# cts role-based enforcement
NX7K-CORE(config)# int eth1/26
NX7K-CORE(config-if)# cts manual
NX7K-CORE(config-if-cts-manual)# policy static sgt 0x2 trusted
```

<https://atw-ise237.securitydemo.net:9095>  
<https://atw-ise231.securitydemo.net:9095>  
<https://atw-ise232.securitydemo.net:9095>  
<https://atw-ise233.securitydemo.net:9095>

```
<configuration>
    <configSections>
        <section name="log4net"
type="log4net.Config.Log4NetConfigurationSectionHandler, log4net"/>
    </configSections>

    <log4net>
        <root>
            <level value="INFO" />      <!-- Logging Levels: OFF, FATAL, ERROR, WARN,
INFO, DEBUG, ALL -->
            <appender-ref ref="RollingFileAppender" />
        </root>
        <appender name="RollingFileAppender"
type="log4net.Appender.RollingFileAppender">
            <file value="CiscoISEPICAgent.log" />
            <appendToFile value="true" />
            <rollingStyle value="Size" />
            <maxSizeRollBackups value="5" />
            <maximumFileSize value="10MB" />
            <staticLogFileName value="true" />
            <layout type="log4net.Layout.PatternLayout">
                <conversionPattern value="%date %level - %message%newline" />
            </layout>
        </appender>
    </log4net>

    <startup>
        <supportedRuntime version="v4.0"/>
        <supportedRuntime version="v2.0.50727"/>
    </startup>
    <configSections>
```

```
Checking DNS resolution of ISE pxGrid Node hostname(s) ...
Success: Resolved 'atw-ise237.securitydemo.net' address: 10.1.100.237

Validating WSA client certificate ...
Success: Certificate validation successful

Validating ISE pxGrid Node certificate(s) ...
Success: Certificate validation successful

Validating ISE Monitoruting Node Admin certificate(s) ...
Success: Certificate validation successful

Checking connection to ISE pxGrid Node(s) ...
Success: Connection to ISE pxGrid Node was successful.
Retrieved 17 SGTs from: atw-ise237.securitydemo.net

Checking connection to ISE Monitoruting Node (REST server(s)) ...
Success: Connection to ISE Monitoruting Node was successful.
REST Host contacted: atw-ise237.securitydemo.net

Test completed successfully.
```

```
logging source-interface type number
!sets the IP address associated with fastethernet 0/1 as the syslog message source.
logging source-interface fastethernet 0/1
```

```
logging monitor informational
logging origin-id ip
logging source-interface interface_id
logging host ISE Monitoring Node IP transport udp port 20514
```

```
*Sep 13 19:26:39.634: %MAB-5-FAIL: Authentication failed for client  
(0050.5687.0039) on Interface Gi0/1 AuditSessionID  
0A01283C0000001517B7584B
```

```
*Sep 13 19:26:39.634: %AUTHMGR-7-RESULT: Authentication result  
'server dead' from 'mab' for client (0050.5687.0039) on Interface  
Gi0/1 AuditSessionID 0A01283C0000001517B7584B
```

```
*Sep 13 19:26:39.634: %AUTHMGR-5-FAIL: Authorization failed for  
client (0050.5687.0039) on Interface Gi0/1 AuditSessionID  
0A01283C0000001517B7584B
```

```
3560-X# sho authen sess int g0/1

        Interface: GigabitEthernet0/1
        MAC Address: 0050.5687.0039
        IP Address: 10.1.41.102
        User-Name: 005056870039
        Status: Running
        Domain: UNKNOWN
        Security Policy: Should Secure
        Security Status: Unsecure
        Oper host mode: multi-auth
        Oper control dir: both
        Session timeout: N/A
        Idle timeout: N/A
        Common Session ID: 0A01283C00000018F595EC0B
        Acct Session ID: 0x000000049
        Handle: 0x41000018

Runnable methods list:
        Method      State
        mab        Failed over
        dot1x     Running
```

```
3560-X# sho ip int brief | include up
```

Vlan1	unassigned	YES	NVRAM	up	up
Vlan40	10.1.40.60	YES	NVRAM	up	up
GigabitEthernet0/1	unassigned	YES	unset	up	up
GigabitEthernet0/24	unassigned	YES	unset	up	up
Loopback0	192.168.254.60	YES	NVRAM	up	up

```
3560-X#
```

```
3560-X(config)# ip radius source-interface Loopback0  
3560-X(config)#
```

```
3560-X# sho authen sess int g0/1
```

```
    Interface: GigabitEthernet0/1
    MAC Address: 0050.5687.0039
    IP Address: 10.1.41.102
    User-Name: 00-50-56-87-00-39
    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: xACSAACLx-IP-Pre-Auth-ACL-50fc97ba
    URL Redirect ACL: ACL-WEBAUTH-REDIRECT
    URL Redirect: https://atw-cp-ise04.ise.local:8443/guestportal/gateway?
sessionId=0A01283C0000001AF59D671A&action=cwa
    Session timeout: N/A
    Idle timeout: N/A
    Common Session ID: 0A01283C0000001AF59D671A
    Acct Session ID: 0x0000004B
    Handle: 0xAC00001A
```

Runnable methods list:

Method	State
mab	Authc Success
dot1x	Not run

```
3560-X#
```

```
3560-X# sho authen sess int g0/1

        Interface: GigabitEthernet0/1
        MAC Address: 0050.5687.0039
        IP Address: 10.1.41.102
        User-Name: 00-50-56-87-00-39
        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: xACSAACLx-IP-Pre-Auth-ACL-50fc97ba
        URL Redirect ACL: ACL-WEBAUTH-REDIRECT
        URL Redirect: https://atw-cp-ise04.ise.local:8443/
guestportal/gateway?sessionId=0A01283C0000001D059317CE&action=cwa
        Session timeout: N/A
        Idle timeout: N/A
        Common Session ID: 0A01283C0000001D059317CE
        Acct Session ID: 0x00000055
        Handle: 0x7500001D

Runnable methods list:

        Method      State
        dot1x      Failed over
        mab       Authc Success
```

```
atw-cp-ise02/admin# show run
! -- Displaying only necessary information
repository ATW-SFTP
url sftp://172.25.73.252/array1/FTPROOT/
user admin password hash b5558b4ef1742747cc50723474E842818642df47
```

```
atw-cp-ise02/admin# conf t
atw-cp-ise02/admin(config)# repository ATW-SFTP
% Warning: Host key of the server must be added using 'crypto host_key add' exec
command before sftp repository can be used.
atw-cp-ise02/admin(config-Repository)# exit
atw-ise245/admin# crypto host_key add host 172.25.73.253
host key fingerprint added
# Host 172.25.73.253 found: line 1 type RSA
2048 fa:0c:a4:b4:28:78:fd:0f:b7:91:1a:a5:8f:72:4a:1c 172.25.73.253 (RSA)
```

```
atw-cp-ise02/admin# show repository ATW-CDROM
FILE NAME                      SIZE  MODIFIED TIME
=====
.discinfo                     102 Bytes Tue Nov 13 18:38:10 2012
Server                         72 KB   Mon Nov 19 02:26:26 2012
TRANS.TBL                      1 KB    Mon Nov 19 02:26:26 2012
images                          2 KB    Mon Nov 19 02:25:36 2012
isolinux                       2 KB    Mon Nov 19 02:25:36 2012
ks.cfg                          24 KB   Mon Nov 19 02:25:36 2012
```

```
atw-ise245/admin# application upgrade prepare ise-upgradebundle-2.0.x-to-2.2.0.440.  
NOT_FOR_RELEASE.x86_64.tar.gz NAS-US  
Getting bundle to local machine...  
Unbundling Application Package...  
Verifying Application Signature...  
Application upgrade preparation successful
```

```
atw-ise245/admin# application upgrade cleanup  
Application upgrade preparation directory cleanup successful
```

```
atw-ise244/admin# application upgrade proceed
Initiating Application Upgrade...
% Warning: Do not use Ctrl-C or close this terminal window until upgrade completes.
-Checking VM for minimum hardware requirements
STEP 1: Stopping ISE application...
STEP 2: Verifying files in bundle...
-Internal hash verification passed for bundle
STEP 3: Validating data before upgrade...
STEP 4: De-registering node from current deployment...
STEP 5: Taking backup of the configuration data...
- Running db sanity check to fix index corruption, if any...
- Auto Upgrading Schema for UPS Model...
- Upgrading Schema completed for UPS Model.

ISE database schema upgrade completed.
STEP 7: Running ISE configuration data upgrade...
- Data upgrade step 1/48, NSFUpgradeService(2.1.101.145)... Done in 33 seconds.
- Data upgrade step 2/48, ProfilerUpgradeService(2.1.101.145)... Done in 1 seconds.
<SNIP>
```

```
- Data upgrade step 48/48, GuestAccessUpgradeService(2.2.0.440)... Done in 5
seconds.

STEP 8: Running ISE configuration data upgrade for node specific data...

STEP 9: Making this node PRIMARY of the new deployment. When other nodes are
upgraded it will be added to this deployment.

STEP 10: Running ISE M&T database upgrade...

ISE M&T Log Processor is not running
ISE database M&T schema upgrade completed.

% Warning: Some warnings encountered during MNT sanity check
Gathering Config schema(CEPM) stats .....
Gathering Operational schema(MNT) stats .....

% NOTICE: Upgrading ADEOS. Appliance will be rebooted after upgrade completes
successfully.

<SNIP>

% This application Install or Upgrade requires reboot, rebooting now...
Broadcast message from root@atw-ise244 (pts/1) (Sat Jan  7 18:12:13 2017):
The system is going down for reboot NOW
```

```
3560-X# sho run
Building configuration...
Current configuration : 22928 bytes
!
version 12.2
hostname 3560-X
logging monitor informational
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 10.1.103.231 server-key Cisco123
client 10.1.103.4 server-key Cisco123
!
aaa session-id common
authentication mac-move permit
```

```
ip routing
!
ip domain-name cts.local
ip name-server 10.1.100.100
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-4076357888
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-4076357888
revocation-check none
rsakeypair TP-self-signed-4076357888
!
!
crypto pki certificate chain TP-self-signed-4076357888
certificate self-signed 01
quit
!
dot1x system-auth-control
!
interface Loopback0
ip address 192.168.254.60 255.255.255.255
!
interface <ALL EDGE PORTS>
switchport access vlan 41
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 41
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
!
interface Vlan1
```

```
no ip address
!
interface Vlan40
ip address 10.1.40.60 255.255.255.0
!
!
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
logging origin-id ip
logging source-interface Loopback0
logging host 10.1.103.4 transport udp port 20514
!
snmp-server community CiscoPressRO RO
snmp-server trap-source Loopback0
snmp-server source-interface informs Loopback0
```

```
snmp-server host 10.1.103.231 version 2c CiscoPressRO
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 10.1.103.231 auth-port 1812 acct-port 1813 key Cisco123
radius-server host 10.1.103.4 auth-port 1812 acct-port 1813 key Cisco123
radius-server vsa send accounting
radius-server vsa send authentication
!
end
```

```
C3750X# sho run brief
```

```
Building configuration...
```

```
Current configuration : 18936 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C3750X
!
boot-start-marker
boot-end-marker
!
logging monitor informational
!
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 10.1.103.231 server-key Cisco123
```

```
client 10.1.103.4 server-key Cisco123
!
aaa session-id common
clock timezone EDT -1 0
authentication mac-move permit
ip routing
!
!
ip dhcp snooping vlan 10-13
ip dhcp snooping
ip domain-name cts.local
ip device tracking
!
!
device-sensor filter-list cdp list my_cdp_list
tlv name device-name
tlv name platform-type
!
device-sensor filter-list lldp list my_lldp_list
tlv name port-id
tlv name system-name
tlv name system-description
!
device-sensor filter-list dhcp list my_dhcp_list
option name host-name
option name class-identifier
option name client-identifier
device-sensor filter-spec dhcp include list my_dhcp_list
device-sensor filter-spec lldp include list my_lldp_list
device-sensor filter-spec cdp include list my_cdp_list
device-sensor accounting
device-sensor notify all-changes
!
epm logging
!
crypto pki trustpoint TP-self-signed-254914560
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-254914560
revocation-check none
rsakeypair TP-self-signed-254914560
!
!
crypto pki certificate chain TP-self-signed-254914560
certificate self-signed 01
cts role-based enforcement
```

```
!
dot1x system-auth-control
!
interface Loopback0
ip address 192.168.254.1 255.255.255.255
!
interface <ALL EDGE PORTS>
switchport access vlan 10
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 10
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
ip dhcp snooping information option allow-untrusted
!
!
interface Vlan1
no ip address
shutdown
!
interface Vlan10
ip address 10.1.10.1 255.255.255.0
!
interface Vlan20
ip address 10.1.20.1 255.255.255.0
!
interface Vlan30
ip address 10.1.30.1 255.255.255.0
!
interface Vlan99
ip address 10.1.99.1 255.255.255.0
!
```

```
ip http server
ip http secure-server
!
!
ip access-list extended ACL-AGENT-REDIRECT
remark explicitly prevent DNS from being redirected
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 address
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 access-list extended AGENT-REDIRECT
remark explicitly prevent DNS from being redirected to address
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 radius source-interface Loopback0
ip sla enable reaction-alerts
logging origin-id ip
logging source-interface Loopback0
logging host 10.1.103.4 transport udp port 20514
!
snmp-server community Cisco123 RO
snmp-server community TrustSecRO RO
```

```
snmp-server trap-source Loopback0
snmp-server source-interface informs Loopback0
snmp-server host 10.1.103.4 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 vsa send accounting
radius-server vsa send authentication
!
radius server CP-VIP
address ipv4 10.1.103.231 auth-port 1812 acct-port 1813
automate-tester username radius-test
key Cisco123
!
radius server CP-04
address ipv4 10.1.103.4 auth-port 1812 acct-port 1813
automate-tester username radius-test
key Cisco123
!
end
```

```
4503# show run brief

Building configuration...
Current configuration : 35699 bytes
!
!
version 15.1
!
hostname 4503
!
!
username radius-test password 0 Ciscol23
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 10.1.103.231 server-key Cisco123
client 10.1.103.4 server-key Cisco123
!
aaa session-id common
clock timezone EDT -1 0
!
ip domain-name cts.local
!
ip device tracking
!
device-sensor filter-list cdp list my_cdp_list
  tlv name device-name
  tlv name platform-type
!
device-sensor filter-list lldp list my_lldp_list
  tlv name port-id
  tlv name system-name
  tlv name system-description
!
device-sensor filter-list dhcp list my_dhcp_list
  option name host-name
  option name class-identifier
  option name client-identifier
device-sensor filter-spec dhcp include list my_dhcp_list
device-sensor filter-spec lldp include list my_lldp_list
device-sensor filter-spec cdp include list my_cdp_list
device-sensor accounting
device-sensor notify all-changes
epm logging
!
!
crypto pki trustpoint CISCO_IDEVID_SUDI
  revocation-check none
  rsakeypair CISCO_IDEVID_SUDI
!
crypto pki trustpoint CISCO_IDEVID_SUDIO
  revocation-check none
!
!
crypto pki certificate chain CISCO_IDEVID_SUDI
  certificate 238FC0E90000002BFCA1
  certificate ca 6A6967B3000000000003
crypto pki certificate chain CISCO_IDEVID_SUDIO
```

```
certificate ca 5FF87B282B54DC8D42A315B568C9ADFF
!
dot1x system-auth-control
!
!
vlan 40
name jump
!
vlan 41
name data
!
vlan 99
name voice
!
interface <ALL EDGE PORTS>
switchport access vlan 41
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 41
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
ip dhcp snooping information option allow-untrusted
!
interface Vlan1
no ip address
!
interface Vlan40
ip address 10.1.40.2 255.255.255.0
!
ip http server
ip http secure-server
ip route 0.0.0.0 0.0.0.0 10.1.40.1
```

```
!
ip access-list extended ACL-AGENT-REDIRECT
remark explicitly prevent DNS from being redirected to address
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 address
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
!
logging 10.1.103.4
!
snmp-server community Cisco123 RO
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 10.1.103.231 auth-port 1812 acct-port 1813 test username radi-
ustest
key Cisco123
radius-server host 10.1.103.4 auth-port 1812 acct-port 1813 test username radiust-
est
key Cisco123
radius-server vsa send accounting
radius-server vsa send authentication
!
end
```

```
hostname 6503
logging monitor informational
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 10.1.103.231 server-key Cisco123
client 10.1.103.4 server-key Cisco123
!
aaa session-id common
authentication mac-move permit
ip routing
!
ip domain-name cts.local
ip name-server 10.1.100.100
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-4076357888
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-4076357888
revocation-check none
rsakeypair TP-self-signed-4076357888
!
!
crypto pki certificate chain TP-self-signed-4076357888
certificate self-signed 01
quit
!
dot1x system-auth-control
!
interface Loopback0
ip address 192.168.254.1 255.255.255.255
!
interface <ALL EDGE PORTS>
switchport access vlan 10
```

```
switchport mode access
switchport voice vlan 99
ip access-group ACL-ALLOW in
authentication event fail action next-method
authentication event server dead action authorize vlan 10
authentication event server alive action reinitialize
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication priority dot1x mab
authentication port-control auto
authentication violation restrict
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
!
interface Vlan1
no ip address
!
interface Vlan40
ip address 10.1.40.1 255.255.255.0
!
!
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
deny ip any any
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
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
deny ip any any
!
ip radius source-interface Loopback0
logging origin-id ip
logging source-interface Loopback0
logging host 10.1.103.4 transport udp port 20514
!
snmp-server community CiscoPressRO RO
snmp-server trap-source Loopback0
snmp-server source-interface informs Loopback0
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 10.1.103.231 auth-port 1812 acct-port 1813 key Cisco123
radius-server host 10.1.103.4 auth-port 1812 acct-port 1813 key Cisco123
radius-server vsa send accounting
radius-server vsa send authentication
!
end
```

```
woland-ise/admin# application configure ise

Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Exit
```

7

```
Export Repository Name: Synology
Enter encryption-key for export: [redacted]
log4j:WARN No appenders could be found for logger
  (org.springframework.core.env.StandardEnvironment).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
Integritycheck Openssl digest output from verification with Swims release key:
  Verified OK
Integritycheck Output: Verified signature of integritycheck program with Swims
  release key
Integritycheck Output: Verified signature of integritycheck.sums file with Swims
  release key
```

```
Integritycheck PASSED
Inside Session facade init
node-config.rc has been modified - rebuilding active properties file
PlatformProperties whoami: root

PlatformProperties show inventory: Process Output:

Getting profile properties for profile 'ibmLarge' and persona 'standalone'
In the init method of PDPFacade
Time taken for NSFAdminServiceFactory to load4158
Export in progress...
```

The following 5 CA key pairs were exported to repository 'Synology' at  
'ise\_ca\_key\_pairs\_of\_woland-ise':

```
Subject:CN=Certificate Services Root CA - woland-ise
Issuer:CN=Certificate Services Root CA - woland-ise
Serial#:0x769a465c-342c4a7b-a529bf09-f3e5720c
```

```
Subject:CN=Certificate Services Node CA - woland-ise
Issuer:CN=Certificate Services Root CA - woland-ise
Serial#:0x4bfc93d9-e0b147a7-a1955f9e-e2041967
```

```
Subject:CN=Certificate Services Endpoint Sub CA - woland-ise
Issuer:CN=Certificate Services Node CA - woland-ise
Serial#:0x25f246b9-0efe419a-9fe27fc6-df9c4f12
```

```
Subject:CN=Certificate Services Endpoint RA - woland-ise
Issuer:CN=Certificate Services Endpoint Sub CA - woland-ise
Serial#:0x6e1d8208-3c2647fa-9fdbcb4-2f732ba0
```

```
Subject:CN=Certificate Services OCSP Responder - woland-ise
Issuer:CN=Certificate Services Node CA - woland-ise
Serial#:0x2f5ba187-4eb4452f-8a35c3b7-fa6d9548
```

ISE CA keys export completed successfully

```
Selection ISE configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
```

[6]Display Profiler Statistics  
[7]Export Internal CA Store  
[8]Import Internal CA Store  
[9]Create Missing Config Indexes  
[10]Create Missing M&T Indexes  
[11]Enable/Disable ACS Migration  
[12]Generate Daily KPM Stats  
[13]Generate KPM Stats for last 8 Weeks  
[14]Enable/Disable Counter Attribute Collection  
[15]View Admin Users  
[16]Get all Endpoints  
[17]Exit

17

woland-ise/admin#