Cisco ISE Compliance
How To Upgrade and Deploy the AnyConnect and NAC Agents with ISE

Author: Imran Bashir

Table of Contents

Introduction 4

What Is the Cisco TrustSec System? 4

About the TrustSec How-To Guides 4

Sample Topology used to write this guide 5

Lab IP Addresses and VLANs 6

Internal IP Addresses 6

Internal VLANs and IP Subnets 6

Introduction to ISE Endpoint Compliance Services and Configuration Workflow 7

Exercise Description 7

Configure and Deploy Client Provisioning Services 9

Exercise Description 9

Exercise Objective 9

Lab Exercise Steps 9

Define Authorization Policy for Client Provisioning and Posture Compliance 15

Exercise Description 15

Exercise Objective 15

Lab Exercise Steps 16

Test and Monitor Client Provisioning Services for NAC Web Agent 24

Exercise Description 24

Exercise Objective 24

Lab Exercise Steps 24

Test and Monitor Client Provisioning Services for AnyConnect Unified Agent 29

Exercise Description 29

Exercise Objective 29

Lab Exercise Steps 29

Configure an Anti-Virus Posture Policy 35

Exercise Description 35

Exercise Objective 35

Lab Exercise Steps 36

OPTIONAL: Configure a Secure Screen Saver Posture Policy 40

Exercise Description 40

Exercise Objective 40

Lab Exercise Steps 40

Test Posture Assessment and Posture Policies using AnyConnect Unified Agent 45

Exercise Description 45

Exercise Objective 45

Lab Exercise Steps......45
Test Posture Assessment and Posture Policies using NAC Web Agent......54
Exercise Description......54
Exercise Objective......54
Lab Exercise Steps......54
Monitor and Report on Posture Services......61
Exercise Description......61
Exercise Objective......61
Lab Exercise Steps......61

Introduction

What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into whom and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

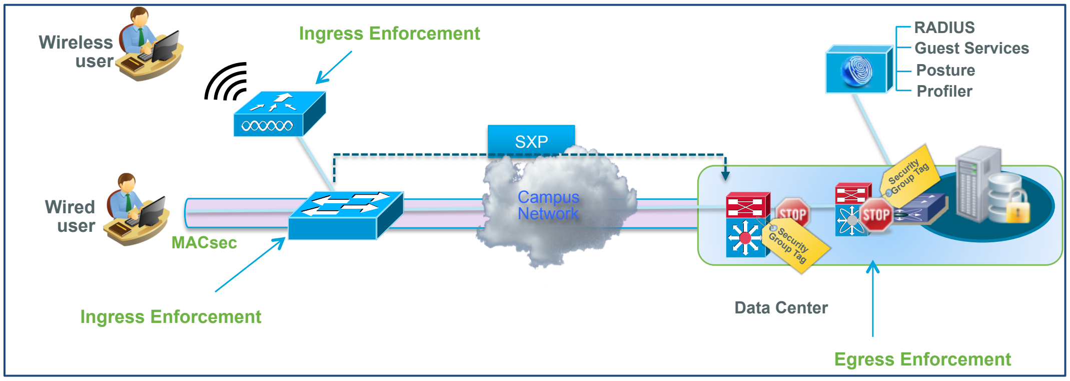
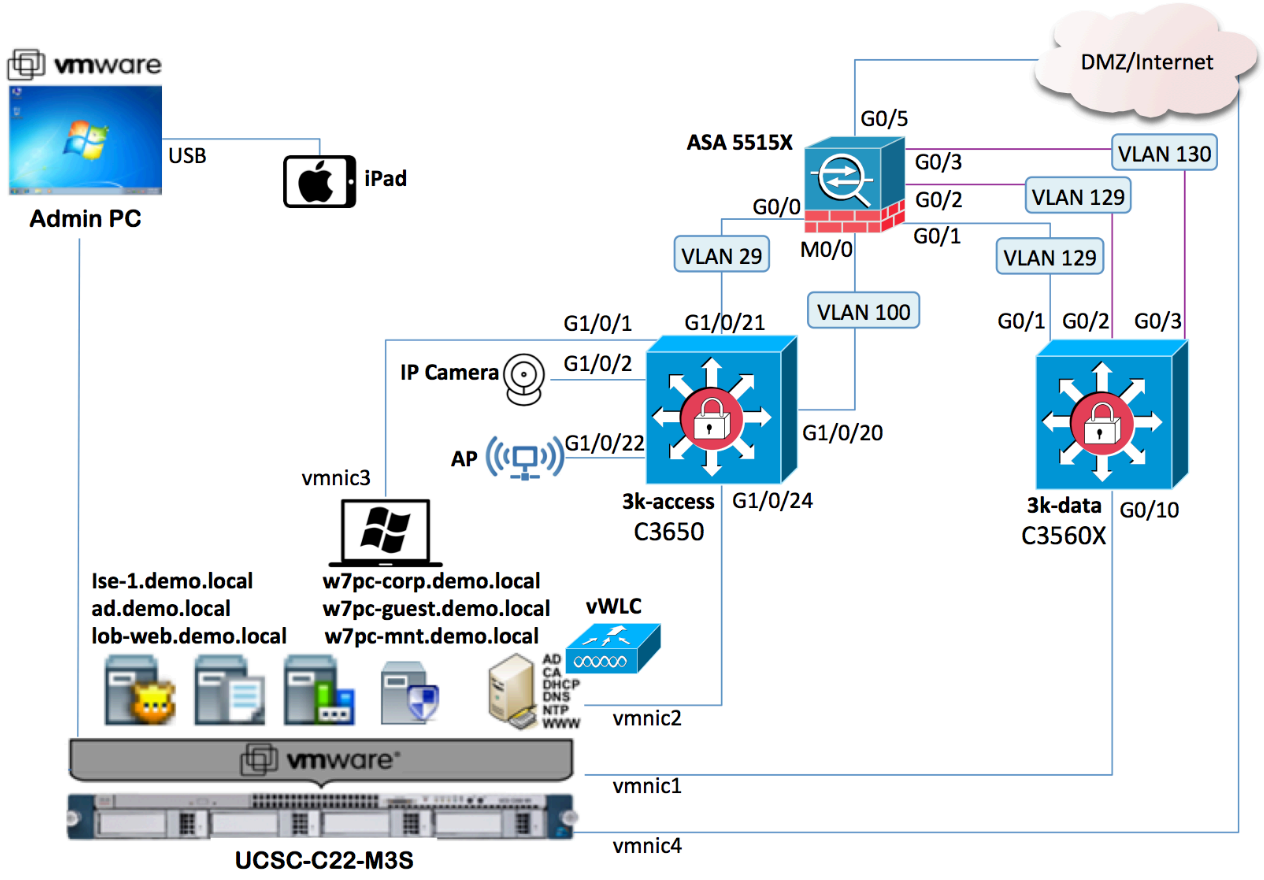


Figure 1.

About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy, or simply pick the single use-case that meets your specific need.

Sample Topology used to write this guide



Lab IP Addresses and VLANs

Internal IP Addresses

Device	Name/Hostname	IP Address
Access Switch (3650)	3k-access.demo.local	10.1.100.1
Data Center Switch (3560X)	3k-data.demo.local	10.1.129.3
Wireless LAN Controller (virtual)	wlc.demo.local	10.1.100.61
Wireless Access Point (2602i)	ap.demo.local	10.1.90.x/24 (DHCP)
ASA (5515-X)	asa.demo.local	10.1.100.2
ISE Appliance	ise-1.demo.local	10.1.100.21
AD (AD/CS/DNS/DHCP)	ad.demo.local	10.1.100.10
Mail	mail.demo.local	10.1.100.40
NTP Server	ntp.demo.local	128.107.212.175
Tools	tools.demo.local	128.107.210.137
LOB Web	lob-web.demo.local	10.1.129.12
Admin (Management) Client (also FTP Server)	admin.demo.local ftp.demo.local	10.1.100.6
Windows 7 Client PC	w7pc-guest.demo.local	10.1.50.x/24 (DHCP)

Internal VLANs and IP Subnets

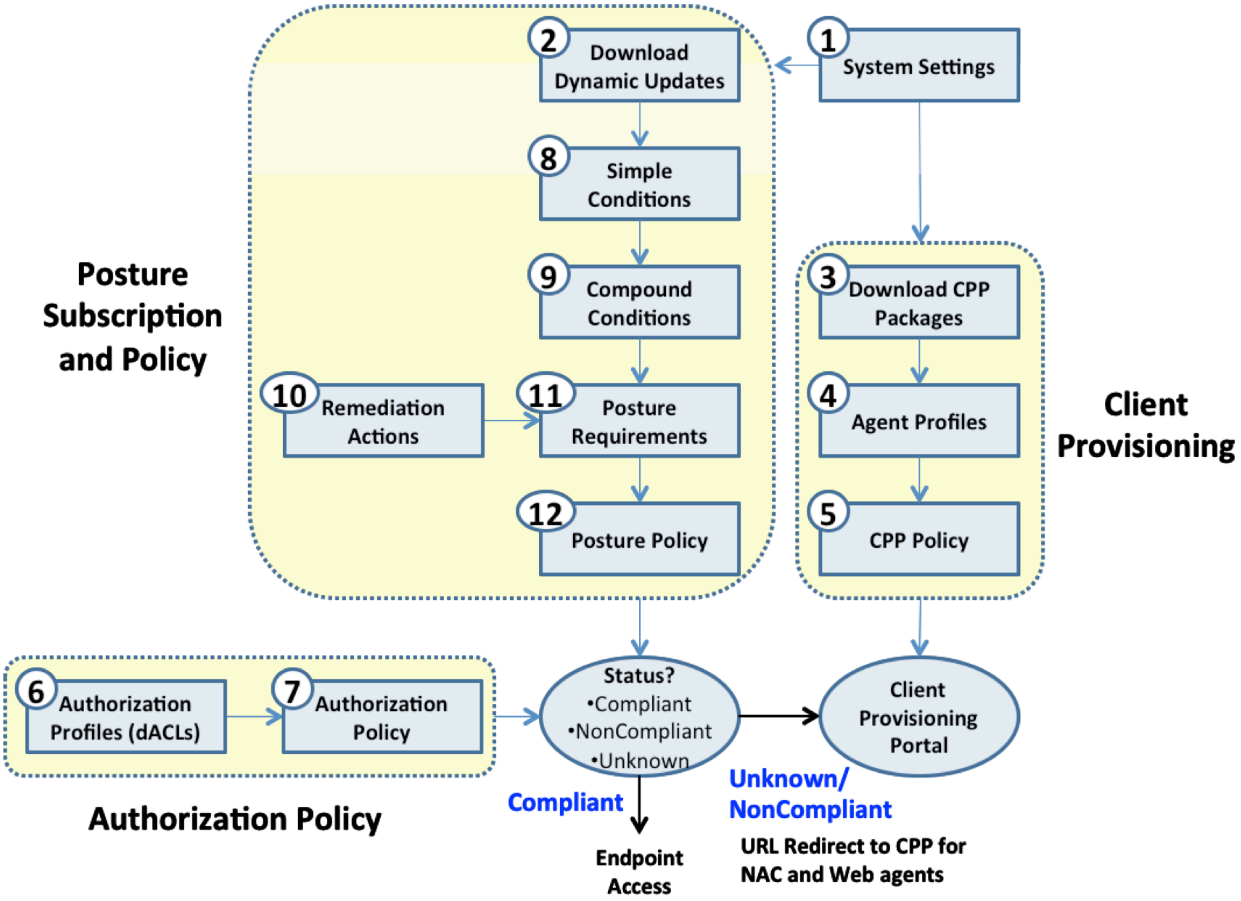
VLAN	VLAN Name	IP Subnet	Description
10	ACCESS	10.1.10.0/24	Authenticated users or access network using ACLs
20	MACHINE	10.1.20.0/24	Microsoft machine-authenticated devices (L3 segmentation)
(29)		10.1.29.0/24	Interconnect subnet between ASA and Access switch
30	QUARANTINE	10.1.30.0/24	Unauthenticated or non-compliant devices (L3 segmentation)
40	VOICE	10.1.40.0/24	Voice VLAN
50	GUEST	10.1.50.0/24	Network for authenticated and compliant guest users
90	AP	10.1.90.0/24	Wireless AP VLAN
98	ISE.LOCAL	10.1.98.0/24	AD domain – ise.local
99	LAB.LOCAL	10.1.99.0/24	AD domain – lab.local and sam.lab.local
100	Management	10.1.100.0/24	Network services (AAA, AD, DNS, DHCP, etc.)
129	WEB	10.1.129.0/24	Line-of-business Web servers
130	DB	10.1.130.0/24	Line-of-business Database servers

Introduction to ISE Endpoint Compliance Services and Configuration Workflow

Exercise Description

In this section we will review the overall workflow for configuring ISE Endpoint Compliance Services including Client Provisioning, Posture Policy, and Authorization Policy for posture compliant access.

Step 1 Review the diagram below which outlines the main steps in configuring ISE Posture Services.



Step 2 Note that the Posture Services workflow is comprised of three main configuration sections:

1. Client Provisioning
2. Posture Subscription and Policy
3. Authorization Policy

The diagram depicts the logical grouping of configuration tasks under each section.

Note: The numbers in the diagram indicate the order in which you will complete the tasks in this lab. Although in practice an administrator may choose to complete the Posture Policy section before configuring the Authorization Policy, in this lab we will first validate Client Provisioning without any specific posture policies configured before configuring and applying specific posture requirements. Also, since the download of posture updates (pre-built checks and rules for assessment including Windows and AV/AS) may take a while to download, that step is moved to the beginning of the lab to ensure the required files are present at the start of the Posture Policy lab exercise.

Step 3 Understanding Posture Services:

Client Provisioning: In order to perform posture assessment and determine the compliance state of an endpoint, it is necessary to provision a client, or agent, to the endpoint. ISE Agents can be persistent whereby the agent is installed and is automatically loaded each time a user logs in. ISE Agents can also be temporal whereby a Web-based agent is dynamically downloaded to the user upon each new session and then removed following the posture assessment process. AnyConnect agent is also responsible for facilitating remediation and providing an optional Acceptable Use Policy (AUP) to the end user. Therefore, one of the first steps in the workflow is to retrieve the agent files from the Cisco website and to create policies that determine agent and configuration files downloaded to endpoints based on their attributes, for example, user identity and client OS type.

Posture Policy: Defines the set of requirements for an endpoint to be deemed "Compliant" based on file, registry, process, application, Windows, and AV/AS checks and rules. Posture policy is applied to endpoints based on defined set of conditions such as user identity and client OS type. An endpoint's compliance (posture) status can be one of the following:

Step 4 Unknown (no data collected to determine posture state)

Step 5 NonCompliant (posture assessment performed and one or more requirements failed)

Step 6 Compliant (compliant with all mandatory requirements)

Step 7 Posture requirements are based on a configurable set of one or more conditions. Simple Conditions include a single assessment check. Compound Conditions include a logical grouping of one or more Simple Conditions. Each requirement is associated with a remediation action that assists endpoint to satisfy the requirement, for example, an AV signature update.

Step 8 **Authorization Policy:** Defines the levels of network access and optional services to be delivered to an endpoint based on posture status. Endpoints that are deemed "not compliant" with Posture Policy may be optionally quarantined until the endpoint becomes compliant. During this phase, a typical Authorization Policy may limit a user's network access to posture and remediation resources only. If remediation by the agent or end user is successful, then the Authorization Policy can grant privileged network access to the user. Policy is often enforced using downloadable ACLs (dACLs) or dynamic VLAN assignment. This lab uses dACLs for endpoint access enforcement.

Step 9 Understanding Lab Configuration Workflow:

Step 10 In this lab, you will download both persistent (AnyConnect (AC) Unified Agent) and temporal (Web Agent) agent files to ISE and define client provisioning policies that require Employees to download the AC Unified Agent and Guest users to download the Web Agent. Note: Employees will be authenticated using 802.1X; Guest users will be authenticated using Central Web Authentication (CWA).

Step 11 Before configuring posture assessment policies and requirements, we will update the Authorization policy to apply Authorization Profiles to Employees and Guests that are flagged "not compliant". The Authorization Profile will use a new dACL that we create to limit access to posture and remediation resources. Employees and Guest users flagged "compliant" will be allowed regular network access. Once configured, we can test client provisioning services. Since no Posture Policy has been configured, these users should be allowed access once the agent successfully loads and sends its report to ISE.

Step 12 Once Client Provisioning services have been verified, posture requirements will be configured to check for Antivirus being installed and signatures up to date. Another requirement will be configured based on registry checks to verify the client has a screen saver enabled and is set to require a password to access a desktop once activated.

Step 13 Testing will be conducted using both AC Unified Agents for Employees and Web Agents for Guest Users.

Configure and Deploy Client Provisioning Services

Exercise Description

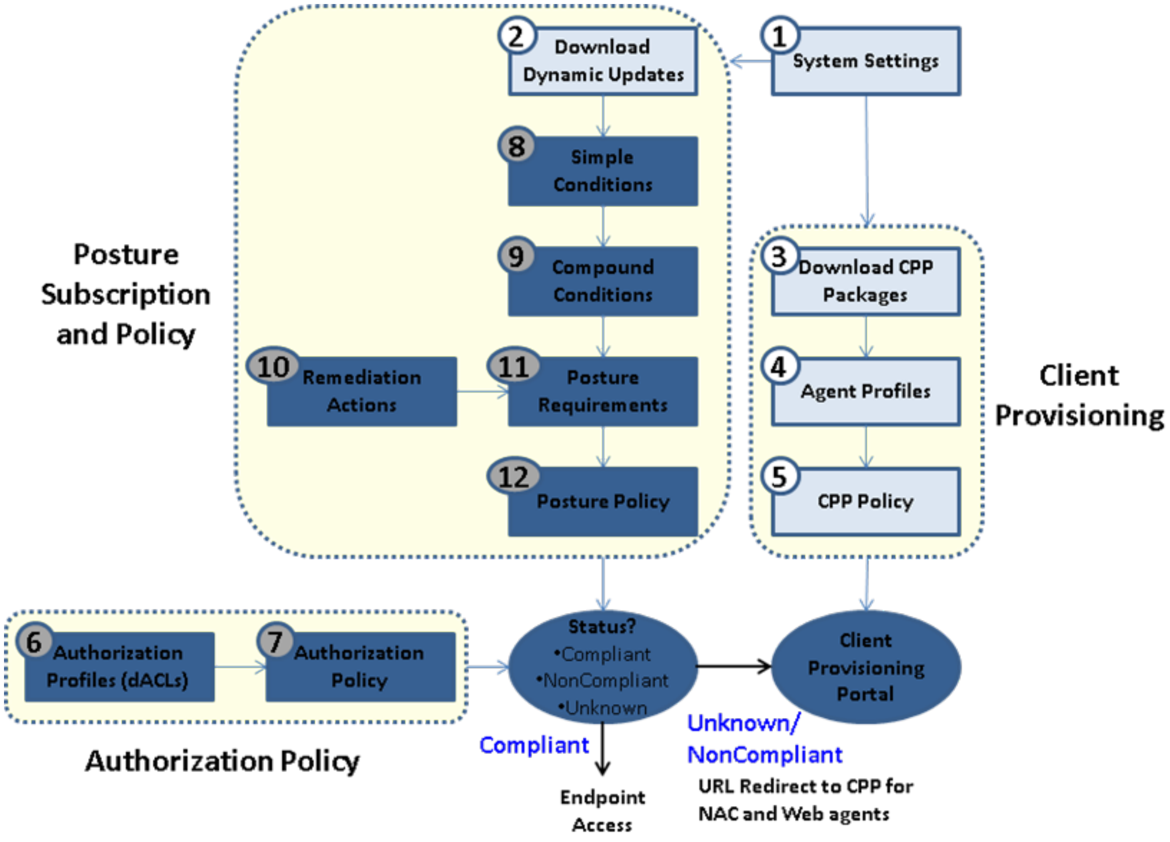
Client provisioning allows ISE administrators to centrally configure and deploy client software to network users such as posture agents and configuration files. This lab exercise covers how to download client software from Cisco to the ISE appliance and how to configure policies to automatically deploy the AnyConnect Unified Agent and Web Agent. Creation and deployment of an AnyConnect ISE Posture profile is also addressed in this exercise.

Exercise Objective

In this exercise, your goal is to complete the following tasks:

- Complete general system settings to support Client Provisioning and Posture Services
- Download AV/AS support files for use in posture assessment and policies
- Download client agent software to deploy to the lab client
- Create an AnyConnect ISE Posture profile to deploy to the lab client
- Define a Client Provisioning Policy to deploy agents based on user identity and client OS

The diagram highlights the key tasks covered in this exercise including System Settings, Download of Dynamic Updates and CPP Packages, Agent Profiles and CPP Policy:



Lab Exercise Steps

Step 14 Access ISE admin web interface

Step 15 Launch the Mozilla Firefox web browser on the admin client PC and enter the address https://ise-1.demo.local

Step 16 Login with username **admin** and password **ISEisC00L**

Step 17 (Accept/Confirm any browser certificate warnings if present)

Step 18 The ISE Home Dashboard page should display. Navigate the interface using the multi-level menus.

Step 19 Download pre-built posture checks for AV/AS and Microsoft Windows.

Step 20 Navigate to Administration > System > Settings

Step 21 Click the ▸ icon to the left of **Posture** in the left-hand pane to expand the contents of the Posture settings, and then click **Updates**. The Update Information in the bottom right-hand pane displays the last time Posture updates took place.

Step 22 Review and add a check mark to Automatically Check for updates starting from initial delay as shown below:

⦿ Web	
Update Feed URL:	https://www.cisco.com/web/secure/pmbu/posture-update.xml
Proxy Address:	
Proxy Port:	
☑ Automatically check for updates starting from initial delay … every **24** hours	

Step 23 Click the **Save** button.

Step 24 Click **Update Now** to run it immediate.

Note: You may proceed to next steps while the update is running.

Step 25 Configure general settings for agent behavior:

Step 26 Select **General Settings** from the left-hand pane under the **Posture** settings. Review the default values for Remediation Timer, Network Transition Delay, and Default Posture Status.

Step 27 **Check** (enable) the checkbox ☑ to "**Automatically Close Login Success Screen After**" and set time to **5** seconds. *This option does not apply to AnyConnect ISE Posture Module*.

Step 28 **Posture Lease** is new in ISE 1.3. It controls posture assessment at re-authentications. For example, a user needs not posture again after disconnecting from network in the office and then reconnecting in the conference room.

Step 29 For this lab, we are **NOT** enabling the posture lease in order to exercise variations of posture policy.

Posture General Settings

Remediation Timer	4	Minutes
Network Transition Delay	3	Seconds
Default Posture Status	Compliant	
☑ Automatically Close Login Success Screen After	**5**	Seconds

Posture Lease

⦿ Perform posture assessment every time a user connects to the network

[ ] Perform posture assessment every 1 Days

Step 30 Click **Save**.

Note: The posture agent profiles may be used to override these global settings.

Step 31 Configure an Acceptable Use Policy for ISE Posture.
Step 32 Select **Acceptable Use Policy** from the left-hand pane under the **Posture** settings.
Step 33 Click **Add**. Enter the following values for the new AUP policy:

* Configuration Name	**aupAnyUser**
Configuration Description	**Simple Acceptable Use Policy**
Show AUP to Agent Users	[☑
(●)	Use URL for AUP message
( )	Use file for AUP message
AUP URL / AUP File	**http://updates.demo.local/AUP.html** (Case Sensitive)
* Select User Identity Groups	**Any**

Step 34 Click **[Submit]** when finished.
Step 35 ISE Offline Upload AnyConnect and NAC Web Agent files.
Step 36 Open a new tab in Firefox to http://tools.demo.local/cp/ and download the following files by right-click and *Save Link As…* to the **Downloads** folder.
Step 37 anyconnect-win-4.0.00048-k9.pkg
Step 38 anyconnect-win-compliance-3.6.9492.2.pkg
Step 39 anyconnect-VPN-disable.xml
Step 40 anyconnect-NAM-EAP-FAST.xml
Step 41 webagent-4.9.5.2-isebundle.zip
Step 42
Step 43 Back to ISE admin web UI, go to **Policy > Policy Elements > Results** and click the ▸ icon to left of **Client Provisioning** to expand its contents.
Step 44 Select **Resources** in the left-hand pane.
Step 45 For each of the following files:
Step 46 anyconnect-win-4.0.00048-k9.pkg
Step 47 anyconnect-win-compliance-3.6.9492.2.pkg
Step 48 webagent-4.9.5.2-isebundle.zip
Step 49
Step 50 From the right-hand pane, click **Add** then click **Agent Resources from local Disk** from the drop-down list. Select ***Cisco Provided Packages*** from Category drop-down.
Step 51 **Browse...** to C:\Users\admin\Downloads\, select the file to **Open**, **Submit**, and **Confirm** the checksum for.
Step 52
Step 53 CLIENT PROVISIONING FILE REFERENCE:
Step 54 **AnyConnectDesktopWindows**: AnyConnect ISE Posture module for Windows.
Step 55 **AnyConnectDesktopOSX**: AnyConnect ISE Posture module for OSX.
Step 56 **Compliance Module(s)**: AnyConnectComplianceModuleOSX, AnyConnectComplianceModuleWindows are compliance modules that provide updates to AV/AS vendor support for AC ISE Posture Module.
Step 57 **AnyConnect ISE Posture Profiles**: Configuration files for AnyConnect ISE Posture Module.

Step 58 Create an AnyConnect posture profile for Windows clients.

Step 59 From the right-hand pane, click **Add** then select [**NAC or AnyConnect Posture Profile**] from the drop-down list.

Step 60 In ISE Posture Agent Profile Settings > New Profile, click on drop down arrow for Select a Category and then select AnyConnect

Step 61 Enter the following values for the new Agent profile. When finished, click **Submit**.

Step 62

ISE Posture Agent Profile Settings

*The defaults should work for most cases. Changed items are **highlighted**. See ISE User Guide, Release 1.3 for more info on Agent Profile Parameters and Applicable Values.*

AnyConnect	
* Name:	**acPostureWinProfile**
Description:	**AnyConnect ISE Posture Profile for Windows clients**

Agent Behavior

Parameter	Value	Notes	Description
Enable debug log	No		Enables the debug log on the agent
Operate on non-802.1X wireless	No		Enables the agent to operate on non-802.1X wireless networks.
Enable signature check	No	OSX: N/A	Enables signature checking of executables before the agent will run them.
Log file size	5 MB		The maximum agent log file size
Remediation timer	4 mins	The default is empty which means use the global setting. The default of global setting is 4.	The time the user has for remediation before they will be tagged as non-compliant

IP Address Change

Parameter	Value	Notes	Description
Enable agent IP refresh	Yes	Enables VLAN change detection	Sets the Vlan change detection flag on the server, to transmit the configured dhcp release delay, and the dhcp renew delay values from the server to the client.
VLAN detection interval	0 secs	0 means VLAN detection is disabled	The interval at which the agent will check for a VLAN change
Ping or ARP	Ping		Ping timeout.
Maximum timeout for ping	1 secs		
DHCP renew delay	1 secs		
DHCP release delay	4 secs		
Network transition delay	3 secs	The default is empty which means uses the global setting. The default of global setting is 3.	The period for which the agent suspends network monitoring so it can wait for a planned IP change to happen

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Discovery host	**biz.demo.local**		The server that the agent should connect to
* Server name rules	*	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com

Note: **Discovery host** set to biz.demo.local shows that it can be any site that may trigger URL redirect to ISE by the redirect ACL so needs not be an ISE node.

Step 63 Configure an AnyConnect VPN profile to **hide** the VPN tile in AnyConnect GUI.

Note: We need a VPN profile in order **not** to show AnyConnect VPN module tile on the client machine.
Ref: **CSCur22131**: Discrepancy with VPN module appearing on client when it is de-selected

Step 64 Click **Add** then **Agent** **from local Disk** drop-down list. click **Resources** from the

Category	**Customer Created Packages**
Type	**AnyConnect Profile**
Name	***acVPNdisableProfile***
Description	Disable/hide VPN tile.

Step 65

Step 66

Step 67

Step 68

Step 69 Browse to C:\Users\admin\Downloads\

Step 70 Select anyconnect-VPN-disable.xml

Step 71 Click **Submit** to save changes. **Confirm** when prompted for *SHA1 hash match***.**

Step 72 Upload NAM profile to ISE.

Step 73 Click Add then Agent Resources from local Disk from the drop-down list.

Category	**Customer Created Packages**
Type	**AnyConnect Profile**
Name	***acNAMProfile***
Description	Configure AnyConnect NAM for EAP-FAST.

Step 74 Browse to C:\Users\Admin\Downloads\

Step 75 Select anyconnect-NAM-EAP-FAST.xml

Step 76 Click **Submit** to save changes. **Confirm** when prompted for *SHA1 hash match***.**

Step 77 Create an AnyConnect configuration profile for Windows clients.

Step 78 From the right-hand pane, click **Add** then select **AnyConnect Configuration** from the drop-down list.

Step 79 Under AnyConnect Package, click on drop down arrow for Choose a Package and then select AnyConnectDesktopWindows 4.0.48.0

Step 80 Enter the following values for the new Agent Configuration. When finished, click **Submit** to save the changes.

* AnyConnect Package:	**AnyConnectDesktopWindows 4.0.48.0**
* Configuration Name:	***acConfigWin***
Description:	AnyConnect agent configuration for Windows
* Compliance Module	**Anyconnect-win-compliance-3.6.9492.2**

AnyConnect Module Selection

ISE Posture	☑
VPN	□
Network Access Manager	☑
Web Security	□
ASA Posture	□
Start Before Logon	□
Diagnostic and Reporting Tool	☑

Profile Selection

ISE Posture	**acPostureWinProfile**
VPN	**acVPNdisableProfile**
	acNAMProfile

Network Access Manager -

-

Web Security

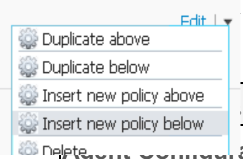
Customer Feedback

Step 81 Define Client Provisioning Policy for Employees and Guest users

Step 82 Go to Policy → Client Provisioning.

Step 83 Add two new Client Provisioning rules per the following table values, and then [**Save**].

Step 84 To add a new policy, point to the right and select the **Edit** drop do **New Policy below**.



Edit
Duplicate above
Duplicate below
Insert new policy above
Insert new policy below
Delete

Step 85

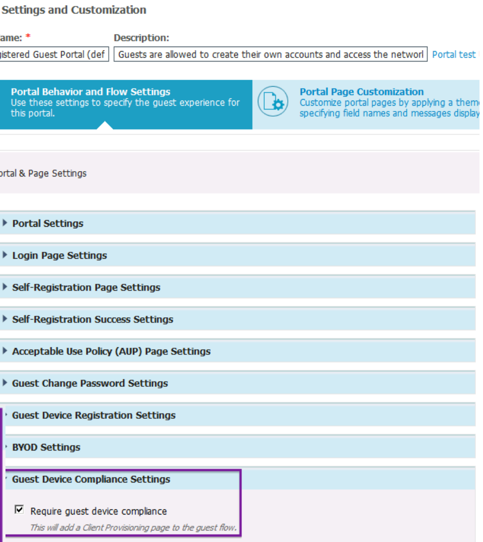
Rule Name	ID Groups	OS	Conditions	
Employee WinAll	Any	Windows All	demoAD.local:ExternalGroups **EQUALS** demo.local/HCC/Groups/Employees	**Agent Configuration** Agent: acConfigWin
Guest WinAll	Any	Windows All	Network Access:UseCase **EQUALS** Guest Flow	**Agent Configuration** Agent: WebAgent 4.9.5.2

Note: Be sure to **Save** Client Provisioning Policy!

Step 86 Configure Guest Portal to go through posture checks

Step 87 Go to Guest Access → Configure → Guest Portals and click on Self-Registered Guest Portal (default) hyperlink.

Note: If Error code WAP00008 is received, refresh the web page and click on the portal links again. -- CSCuq43931



Portals Settings and Customization

Portal Name: * Self-Registered Guest Portal (def

Description: Guests are allowed to create their own accounts and access the networl

Portal test

Portal Behavior and Flow Settings
Use these settings to specify the guest experience for this portal.

Portal Page Customization
Customize portal pages by applying a them specifying field names and messages display

Portal & Page Settings

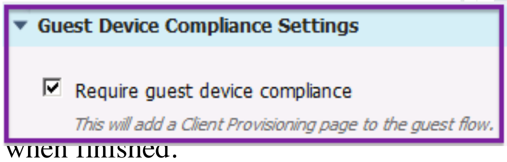
- Portal Settings
- Login Page Settings
- Self-Registration Page Settings
- Self-Registration Success Settings
- Acceptable Use Policy (AUP) Page Settings
- Guest Change Password Settings
- Guest Device Registration Settings
- BYOD Settings
- Guest Device Compliance Settings

☑ Require guest device compliance
This will add a Client Provisioning page to the guest flow.

Step 88 Scroll down to **Guest Device Compliance Settings.** Check [☑ Require guest device compliance] as shown.

Step 89

Step 90



Guest Device Compliance Settings

☑ Require guest device compliance
This will add a Client Provisioning page to the guest flow.

Step 91

Step 92

Step 93

Step 94 Click **Save** when finished.

Step 95 Configure Retry URL for timing-out at Guest / Client Provisioning Portals

Step 96 Go to Administration → Device Portal Management → Settings

Step 97 Expand on **Retry URL**

Step 98 Set the value as below:

Retry URL for onboarding: **http://www.cisco.com**

Step 99 [**Save**] once done.

Step 100

Step 101

Define Authorization Policy for Client Provisioning and Posture Compliance

Exercise Description

The Authorization Policy sets the types of access and services to be granted to endpoints based on their attributes such as identity, access method, and compliance with posture policies. This exercise includes modifications to an existing Authorization Policy to ensure that endpoints that are not posture compliant are quarantined (granted limited access sufficient to provision agent software and to remediate failed requirements), and that only posture compliant endpoints are granted privileged network access.

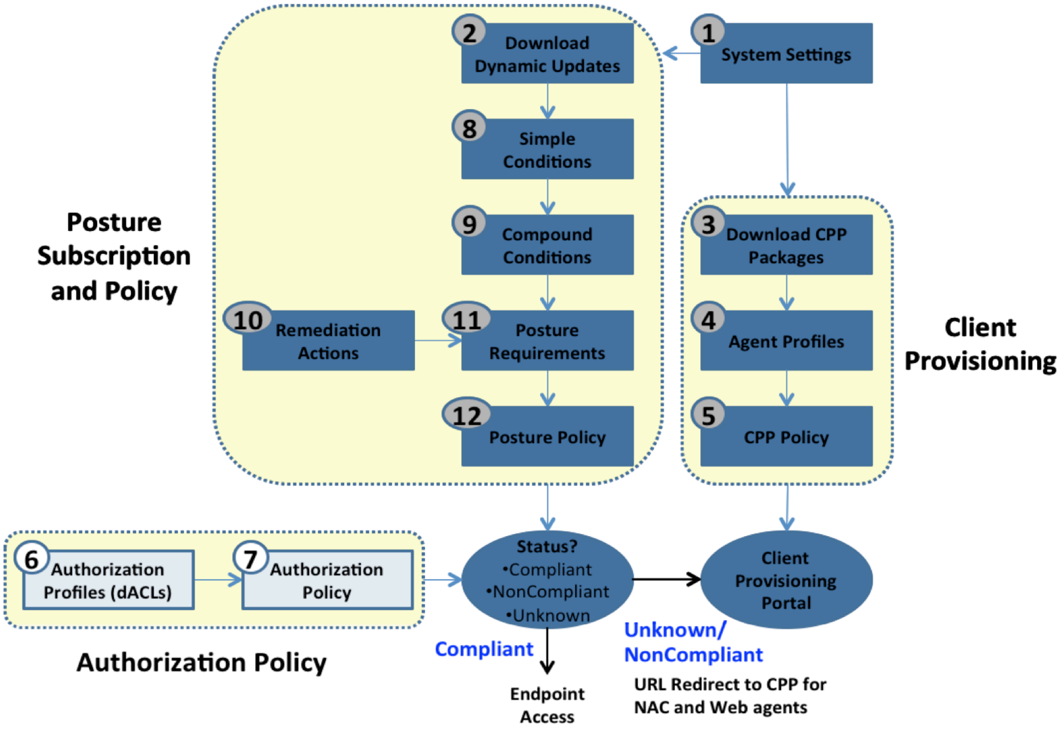
Exercise Objective

In this exercise, your goal is to complete the following tasks:

- Define a Downloadable ACL (dACL) that restricts network access for endpoints whose compliance state is either Unknown or NonCompliant.
- Define a new URL Redirect ACL on the access switch to ensure that general http/https traffic is redirected to the ISE Policy Service node while allowing access to remediation servers.
- Define new Authorization Profiles for 802.1X and web-authenticated users that apply the “quarantine” dACL and Redirect ACL to redirect endpoints to provisioning and posture services.
- Add new rules to the Authorization Policy that leverage the new Authorization Profiles to quarantine, assess posture, and remediate endpoints that are not posture compliant.
- Update existing Authorization Policy rules such that privileged network access is based on posture compliance.

The diagram highlights the key tasks covered in this exercise including Authorization Profiles, their component dACLs, and Authorization Policy:

-



Lab Exercise Steps

Step 102 Access the admin interface of the ISE Administrative node.
Step 103 Go to the Admin client PC and launch the Mozilla Firefox web browser. Enter the following URL in the address field:
Step 104 https://ise-1.demo.local
Step 105 Login with username **admin** and password **ISEisC00L**
Step 106 (Accept/Confirm any browser certificate warnings if present)
Step 107 Define a dACL that restricts network access for endpoints that are not posture compliant.
Step 108 Go to **Policy → Policy Elements → Results** and click ▸ icon to left of **Authorization** (or double-click **Authorization**) to expand its contents.
Step 109 Select **Downloadable ACLs** from the left-hand pane.
Step 110 Click **Add** from the right-hand pane under DACL Management and enter the following values for the new dACL:

Note: Copy-and-paste the DACL content from http://tools.demo.local/cp/DACL_POSTURE_REMEDIATION.txt

* Name	POSTURE_REMEDIATION
Description	Permit access to posture and remediation services and deny all other access. Permit general http and https for redirection only.
* DACL Content	permit udp any eq bootpc any eq bootps permit udp any any eq domain permit icmp any any permit tcp any host 10.1.100.21 eq 8443 permit tcp any host 10.1.100.21 eq 8905 permit udp any host 10.1.100.21 eq 8905 remark below for roadshow pods permit tcp any host 10.1.100.222 eq 80 remark below for GOLD pods permit tcp any host 10.1.129.8 eq 80

Step 111
Step 112 The following describes the purpose of individual access control entries (ACEs):

Downloadable ACE	Description
permit udp any any eq domain	Permit DNS for name resolution
permit icmp any any	Permit ICMP for initial troubleshooting
permit tcp any host 10.1.100.21 eq 8443	Permit CWA/CPP to ISE Policy Service node
permit tcp any host 10.1.100.21 eq 8905	Allow Agent discovery direct to Policy Service node
permit udp any host 10.1.100.21 eq 8905	Allow Agent discovery and keep-alives
permit tcp any host 10.1.129.8 eq 80	Explicit allow to remediation server

Step 113 Click **Submit** when completed.
Step 114
Step 115 Define dACL for AD Login Access
Step 116 Click **Add** from the right-hand pane under DACL Management and enter the following values for the new dACL:

Note: Copy-and-paste the DACL content from http://tools.demo.local/cp/DACL_AD_LOGIN_ACCESS.txt

* Name	AD_LOGIN_ACCESS

Description	Employee AD Access
* DACL Content	permit udp any eq bootpc any eq bootps permit udp any any eq domain permit icmp any any permit tcp any host 10.1.100.10 eq 88 permit udp any host 10.1.100.10 eq 88 permit udp any host 10.1.100.10 eq ntp permit tcp any host 10.1.100.10 eq 135 permit udp any host 10.1.100.10 eq netbios-ns permit tcp any host 10.1.100.10 eq 139 permit tcp any host 10.1.100.10 eq 389 permit udp any host 10.1.100.10 eq 389 permit tcp any host 10.1.100.10 eq 445 permit tcp any host 10.1.100.10 eq 636 permit udp any host 10.1.100.10 eq 636 permit tcp any host 10.1.100.10 eq 1025 permit tcp any host 10.1.100.10 eq 1026

Step 117

Step 118 Define dACL for Guest Access

Step 119 Click **Add** from the right-hand pane under DACL Management and enter the following values for the new dACL:

Note: Copy-and-paste the DACL content from http://tools.demo.local/cp/DACL_GUEST_INTERNET.txt

* Name	INTERNET_ONLY
Description	Internet Access
* DACL Content	permit udp any any eq domain permit icmp any any permit tcp any host 10.1.100.21 eq 8443 deny ip any 10.1.0.0 0.0.255.255 permit ip any any

Step 120

Step 121 Review URL Redirect ACL on the access switch.

Step 122 From the Admin client PC, use the desktop shortcut for the PuTTY to launch a terminal session to the **3k-access** switch using the credentials **admin / ISEisC00L**.

Step 123 Enter the following command at the access switch exec shell prompt to verify the contents of the ACL:

```
3k-access# show ip access-lists ISE-URL-REDIRECT
 Extended IP access list ISE-URL-REDIRECT
     5 deny tcp any host 10.1.129.8 eq www
     10 permit tcp any any eq www
```

Step 124

Step 125 Authorization Profiles will reference this ACL and work in conjunction with the accompanying dACL applied to the switchport interface.

Step 126 In the example URL Redirect ACL above, the entry marked “deny” will not redirect the specified packets. This is for traffic specifically destined to the remediation server.

Step 127

Step 128 Define a new Authorization Profile **Posture Remediation** that leverages both the new dACL for port access control and the URL Redirect ACL for traffic redirection.

Step 129 Return to the ISE admin interface from the Admin client PC.

Step 130 Click Authorization Profiles from the left-hand pane under Policy > Policy Elements > Results > Authorization.

Step 131 Click **Add** from the right-hand pane and enter the values for the Authorization Profile as shown below.

Name	Posture Remediation
Description	Permit access to posture and remediation services; redirect traffic to client provisioning and posture services.
Access Type	ACCESS_ACCEPT
☑ DACL Name	POSTURE_REMEDIATION
☑ Web Redirection (CWA, MDM, NSP, CPP)	Client Provisioning (Posture) ACL: ISE-URL-REDIRECT Value: Client Provisioning Portal (default) [ ] Static IP/Host name

Step 132 The resultant Attribute Details should appear at the bottom of the page as the following:

```
Access Type = ACCESS_ACCEPT
DACL = POSTURE_REMEDIATION
cisco:cisco-av-pair=url-redirect-acl=ISE-URL-REDIRECT
cisco:cisco-av-pair=url-redirect =https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=…&action=cpp
```

Step 133 Scroll to bottom of page and click **Submit** to apply your changes.

Step 134

Step 135 Define a new Authorization Profile **CWA Posture Remediation** that leverages both the new dACL for port access control and the URL Redirect ACL for traffic redirection.

Step 136 From the left-hand pane under Policy → Policy Elements → Results → Authorization.

Step 137 Click **Add** from the right-hand pane and enter the values for the Authorization Profile as shown below.

Name	CWA Posture Remediation
Description	Permit access to posture and remediation services; redirect traffic to central web auth services.
Access Type	ACCESS_ACCEPT
☑ DACL Name	POSTURE_REMEDIATION
☑ Web Redirection (CWA, MDM, NSP, CPP)	Centralized Web Auth ACL: ISE-URL-REDIRECT Value: Self-Registered Guest Portal (default) [ ] Display Certificates Renewal Message [ ] Static IP/Host name

Step 138 The resultant Attribute Details should appear at the bottom of the page as the following:

```
Access Type = ACCESS_ACCEPT
DACL = POSTURE_REMEDIATION
cisco:cisco-av-pair=url-redirect-acl=ISE-URL-REDIRECT
cisco:cisco-av-pair=url-redirect =https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=…&action=cwa
```

Step 139 Scroll to bottom of page and click **Submit** to apply your changes.

Step 140

Step 141 Define a new Authorization Profile for Compliant Employees named **Employee** that allows complete access.

Step 142 From the left-hand pane under Policy → Policy Elements → Results → Authorization → Authorization Profiles.

Step 143 Click **Add** from the right-hand pane and enter the values for the Authorization Profile as shown below.

Name	**Employee**
Description	Full Access
Access Type	ACCESS_ACCEPT
☑ DACL Name	PERMIT_ALL_TRAFFIC

Step 144 The resultant Attribute Details should appear at the bottom of the page as the following:

```
Access Type = ACCESS_ACCEPT

            DACL =  PERMIT_ALL_TRAFFIC
```

Step 145 Scroll to the bottom and click **Submit** to apply your changes.

Step 146

Step 147 Define a new Authorization Profile for AD Login

Step 148 Click Authorization Profiles from the left-hand pane under Policy → Policy Elements → Results → Authorization.

Step 149 Click **Add** from the right-hand pane and enter the values for the Authorization Profile as shown below.

Name	**AD Login**
Description	Allow machine to login to AD through dot1.x
Access Type	ACCESS_ACCEPT
☑ DACL Name	AD_LOGIN_ACCESS

Step 150 The resultant Attribute Details should appear at the bottom of the page as the following:

```
Access Type = ACCESS_ACCEPT

            DACL =   AD_LOGIN_ACCESS
```

Step 151 Scroll to the bottom and click **Submit** to apply your changes.

Step 152 Define a new Authorization Profile for Guest access which would be used for Guest as well as contractor access

Step 153 Click Authorization Profiles from the left-hand pane under Policy → Policy Elements → Results → Authorization.

Step 154 Click **Add** from the right-hand pane and enter the values for the Authorization Profile as shown below.

Name	**Guest**
Description	Allow access to Guest and Contractors
Access Type	ACCESS_ACCEPT

☑ DACL Name	INTERNET_ONLY

Step 155 The resultant Attribute Details should appear at the bottom of the page as the following:

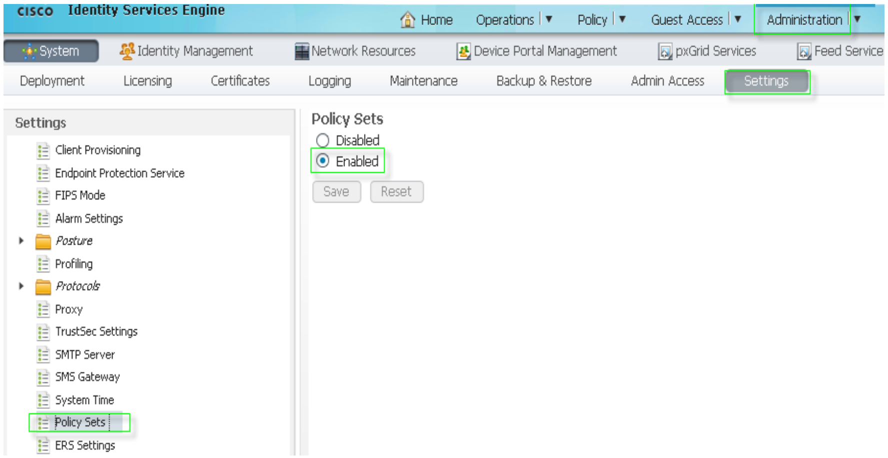
```
Access Type = ACCESS_ACCEPT
DACL =   INTERNET_ONLY
```

Step 156 Scroll to the bottom and click **Submit** to apply your changes.

Step 157

Step 158 Enable Policy Sets

Administration → Settings → Policy Sets and select 'Enabled'



Policy Sets
○ Disabled
● Enabled

Step 159 Policy set wiredMAB

Step 160 Navigate to Policy → Policy Sets

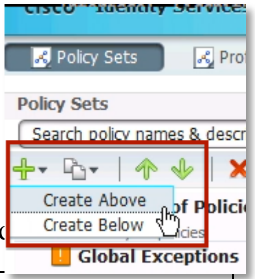
Step 161 Select **Default** policy set in the left-hand pane

Step 162 Click on ✚ → **Create Above**

Step 163

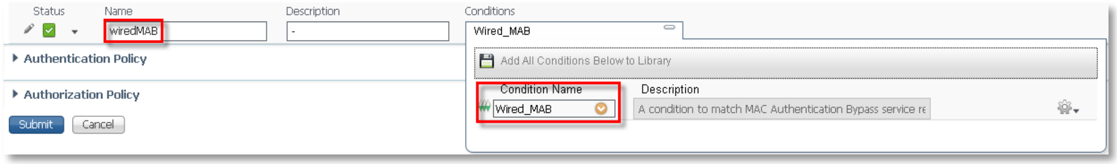
Step 164

Step 165 Click **Edit** on the far right to edit the Policy Name and



Name	**wiredMAB**
Description	-
Select Condition(s)	[Select Existing Condition from Library] → Compound Condition → Wired_MAB

Step 166



Name: wiredMAB
Description: -
Conditions: Wired_MAB
Condition Name: Wired_MAB
Description: A condition to match MAC Authentication Bypass service re

Step 167 Click **Done**

Step 168

Step 169 Policy set wiredMAB Authentication Policy

Step 170 Expand the Authentication Policy

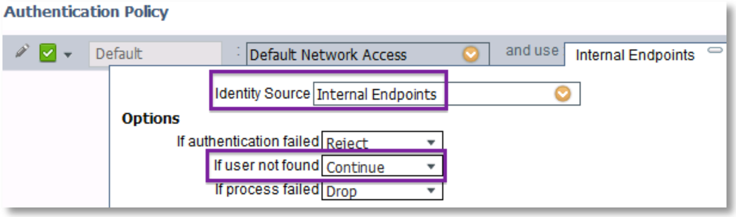
Step 171 Click **Edit** for the **Default Rule**

Step 172 Select Identity Source → Internal Endpoints

Step 173 Select Continue for *If user not found*

Step 174 Click Done

Step 175



Authentication Policy

Default : Default Network Access and use Internal Endpoints

Options

Identity Source Internal Endpoints

If authentication failed Reject

If user not found Continue

If process failed Drop

S	Rule Name	Identity Groups	Other Conditions	Permissions
✓	Guest Internet Access	Any	NetworkAccess:UseCase EQUALS Guest Flow	Guest
✓	Default	(no matches)		CWA Posture Remediation

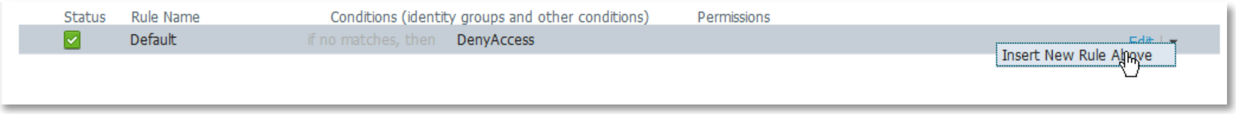
Step 176 Policy set wiredMAB Authorization Policy

Step 177

Step 178 Collapse Authentication Policy and expand Authorization Policy

Step 179 Insert **Guest Internet Acces** authorization rule

Step 180 Click the down arrow to the right of Edit of Default Rule and [**insert a new rule above**]



Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Default	if no matches, then	DenyAccess

Step 181

Step 182 Enter Rule Name as **Guest**

i. Click the ✚ next to Condition(s)

ii. Choose **Condition → Create New Condition (Advance Option)**

iii. Select Attribute **NetworkAccess → UseCase EQUALS Guest Flow**

iv. Click on **gear** icon and select [Add attribute/Value] from the drop-down menu.

v. Select Attribute **Session → PostureStatus EQUALS Compliant**

vi. Click ✚ under Permissions **→ Select a profile → Standard → Guest**

Step 183 Click Done

Step 184 Update **Default** rule

Step 185 Click Edit for the **Default Rule**

Step 186 Click ✚ next to DenyAccess **→ Select a profile**

Step 187 → Standard → CWA Posture Remediation

Step 188 Click Done

Step 189 Click **Submit** to save policy set **wiredMAB**

Step 190 Policy set wiredDOT1X

Step 191 Navigate to Policy → Policy Sets

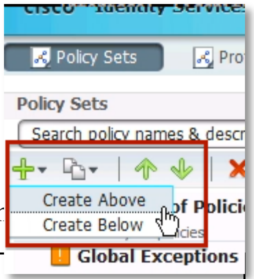
Step 192 Select **Default** policy set in the left-hand pane

Step 193 Click on ✚ → **Create Above**

Step 194

Step 195

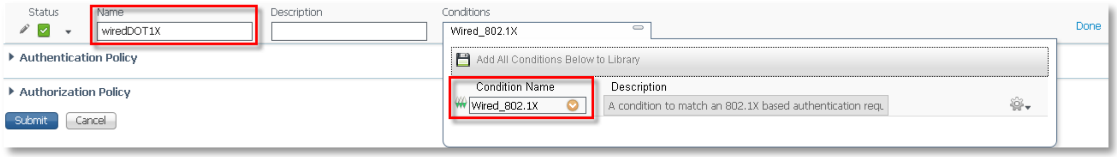
Step 196 Click Edit on the far right to edit the Policy Name ar



Name	**wiredDOT1X**
Description	-
Select Attribute	[Select Existing Condition from Library] → Compound Condition

	→ Wired_802.1X

Step 197



Status ☑ | Name: wiredDOT1X | Description: | Conditions: Wired_802.1X | Done

▸ Authentication Policy

▸ Authorization Policy

Submit | Cancel

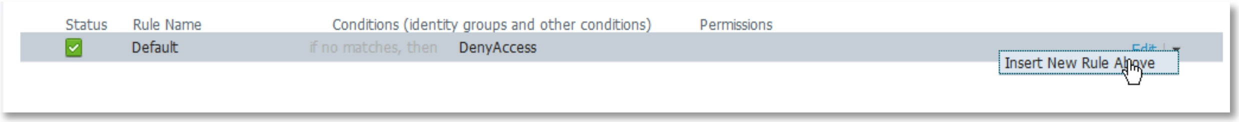
Add All Conditions Below to Library

Condition Name	Description
Wired_802.1X	A condition to match an 802.1X based authentication requ

Step 198 Click **Done**
Step 199 Policy set wiredDOT1X Authentication Policy
Step 200 Expand the Authentication Policy
Step 201 Click **Edit** for the **Default Rule**
Step 202 Select Identity Source → demoAD
Step 203 Click **Done**
Step 204 Policy set wiredDOT1X Authorization Policy

S	Rule Name	Identity Groups	Other Conditions	Permissions
✓	Domain Computer	Any	demoAD:ExternalGroups EQUALS demo.local/Users/Domain Computers	AD Login
✓	Employee	Any	demoAD:ExternalGroups EQUALS demo.local/HCC/Groups/Employees AND Session:PostureStatus EQUALS Compliant	Employee
✓	Employee Posture Assessment	Any	demoAD:ExternalGroups EQUALS demo.local/HCC/Groups/Employees AND Session:PostureStatus NOT_EQUALS Compliant	Posture Remediation
✓	Default	(no matches)		DenyAccess

Step 205
Step 206 Collapse Authentication Policy and expand Authorization Policy
Step 207 Insert **Domain Computer** authorization rule
Step 208 Click the down arrow to the right of **Edit** of Default Rule and [**insert a new rule above**]



Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
☑	Default	if no matches, then	DenyAccess

Step 209 Enter Rule Name as **Domain Computer**

vii. Click the ✚ next to Condition(s)

viii. Choose **Condition → Create New Condition (Advance Option)**

ix. Select Attribute **demoAD → ExternalGroups EQUALS demo.local/Users/Domain Computers**

x. Click ✚ under Permissions → **Select a profile**
→ Standard → AD Login

xi. Click **Done**

b. Add **Employee** authorization rule

Step 210 Click the down arrow to the right of **Edit** of Domain Computer rule and [**Duplicate Below**]
Step 211 Change Rule Name to **Employee**

i. Click the ✚ under Conditions

Step 212 Update Attribute demoAD → ExternalGroups EQUALS demo.local/HCC/Groups/Employees

ii. Click on **gear** icon and select [Add attribute/Value] from the drop-down menu.

iii. Select Attribute **Session → PostureStatus EQUALS Compliant**

iv. Click ✚ next to AD Login → **Select a profile**
→ **Standard** → **Employee**

v. Click **Done**

c. Add **Employee Posture Assessment** authorization rule

Step 213 Click the down arrow to the right of **Edit** of Employee rule and then [**Duplicate Below**]

Step 214 Update Rule Name as Employee Posture Assessment

i. Click the ✚ under Conditions

Step 215 Update the second condition Session:PostureStatus ... and change its operator from **EQUALS** to **NOT_EQUALS**

ii. Click ✚ next to Employee → **Select a profile**
→ **Standard** → **Posture Remediation**

iii. Click **Done**

Step 216 Click [**Submit**] to save policy set **wiredDOT1X**.

Step 217

Test and Monitor Client Provisioning Services for NAC Web Agent

Exercise Description

This exercise validates the Client Provisioning and Authorization Policy configuration completed in the previous lab exercises. Since no Posture Policy has been configured, all users should be posture compliant. The Web Agent will be tested and monitored in detail in this exercise. In addition to Web Agent provisioning, this exercise will also validate agent policies such as AUP and auto-closure of login success screens.

Exercise Objective

In this exercise, your goal is to complete the following tasks:

- Login to the secured lab network from a Windows 7 PC client as a Guest user via Central Web-based Authentication (CWA) and verify Web Agent provisioning.
- Review ISE and switch logs to validate proper operation and application of the Authorization Policy.

Lab Exercise Steps

Step 218 Power **OFF** VM p##**_w7pc-corp** if ON

Step 219 Power **ON** VM p##**_w7pc-guest** if OFF

Step 220 Console and log into VM **w7pc-guest** as **admin** / **ISEisC00L**.

Step 221 Establish a terminal session with the 3k-access switch and simulate a new network connection from w7pc-guest connected on port GigabitEthernet1/0/1.

Note: **Note:** You may need to enable the NIC on the w7pc-guest. Click the **w7pc-guest Network Connections** short cut and double-click on ***w7pc-guest-wired*** to enable it.

From the Admin client PC, use the desktop shortcut for the PuTTY SSH client to launch a terminal session to the **3k-access** switch from the PuTTY list and login using the credentials **admin / ISEisC00L**. If not already in privileged mode, enter enable mode using password **ISEisC00L**.

To view log messages from the terminal session, enter the **terminal monitor** command at the switch exec prompt:

```
3k-access# terminal monitor
```

Note: Use the command **terminal no monitor** if need to disable the monitoring of terminal logging without exiting the session.

Enter configuration mode for interface GigabitEthernet 1/0/1and enter **shut** followed shortly by a **no shut** command:

```
3k-access# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
3k-access(config)# int gi 1/0/1
3k-access(config-if)# shut
3k-access(config-if)# no shut
```

```
3k-access(config-if)# end
3k-access#
```

Step 222 If logging to terminal is enabled, a series of log messages should appear on the screen during port shutdown and re-activation. Enter **CTRL+Z** or **end** to exit configuration mode.

Step 223 After issuing the 'no shut' command, use the following exec command to view the current authorization status of interface GigabitEthernet 1/0/1:

```
3k-access# show authentication sessions interface gi 1/0/1 detail
```

Note: You can also issue exec-level commands from within configuration mode using the **do** command. Example:

```
3k-access(config-if)# do sh auth sess int gi 1/0/1 detail
```

After approximately 10-15 seconds, the output should appear similar to the following:

```
3k-access#sh auth sess int g1/0/1 de
             Interface:  GigabitEthernet1/0/1
                IIF-ID:  0x1059000000000A3
           MAC Address:  0050.5687.ea65
          IPv6 Address:  Unknown
          IPv4 Address:  10.1.50.201
             User-Name:  00-50-56-87-EA-65
                Status:  Authorized
                Domain:  DATA
        Oper host mode:  multi-auth
      Oper control dir:  both
       Session timeout:  N/A
     Common Session ID:  0A01640100000FF8513EF2B4
       Acct Session ID:  0x00000FE5
                Handle:  0xB200003D
        Current Policy:  POLICY_Gi1/0/1

 Local Policies:
         Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

 Server Policies:
          URL Redirect:  https://ise-
1.demo.local:8443/portal/gateway?sessionId=0A01640100000FF8513EF2B4&portal=19b72310-5e4e-11e4-
b905-005056bf2f0a&action=cwa&token=a99a35f1ec4c4975f891a43cc2d17804

      URL Redirect ACL:  ISE-URL-REDIRECT
               ACS ACL:  xACSACLx-IP-POSTURE_REMEDIATION-54bf6344

 Method status list:
        Method                   State
        dot1x                    Stopped
        mab                      Authc Success
```

In the above output, note that the dACL (ACS ACL) = **POSTURE-REMEDIATION** has been pushed to the interface along with a named URL Redirect ACL = **ISE-URL-REDIRECT** that defines the traffic to be redirect to the link specified by URL Redirect. The redirect URL must include the domain name of the ISE Policy Service node, reference to port 8443, the current session ID, and reference action to **cwa** (CWA portal). If any of these items are missing, then web authentication will fail.

Display the current dACL applied to the interface using the command **show ip access-lists <ACS-ACL-name>**, where ACS-ACL-name is taken from the output from the previous step.

```
3k-access#show ip access-lists xACSACLx-IP-POSTURE_REMEDIATION-54bf6344
```

```
Extended IP access list xACSACLx-IP-POSTURE_REMEDIATION-54bf6344 (per-user)
    1 permit udp any any eq domain
    2 permit icmp any any
    3 permit tcp any host 10.1.100.21 eq 8443
    4 permit tcp any host 10.1.100.21 eq 8905
    5 permit udp any host 10.1.100.21 eq 8905
    7 permit tcp any host 10.1.100.222 eq www
    9 permit tcp any host 10.1.129.8 eq www
```

Return to the **w7pc-guest** PC client and login as a guest user.

From the **w7pc-guest** PC client, launch the Firefox web browser and enter in cisco.com. The page should be redirected to the URL specified in the URL Redirect output and display the ISE web authentication portal.

Click the **Don't have an account?** hyperlink from the login portal and enter the following values into the form, and then click **Submit**:

User Name	**jdoe**
First Name	**John**
Last Name	**Doe**
Email Address	**guest@demo.local**
Phone Number	(optional)
Company	**GOLD**
Person Being Visited	(optional)
Reason for Visit	**Web Agent test**

Step 224 Write down the assigned username and password credentials:

Username: ______________________________

Password: ______________________________

To facilitate login, select and copy the password entry, making sure not to include any extra characters. Click the **OK** button.

The web authentication login page again displays. Enter your new Username/Password credentials and click the **Sign On** button.

If an AUP was enabled for web authentication, **check the box** to *Accept terms and conditions* and then click **Accept**. And then click **Continue**

The Agent download page should appear. Click [Allow...] when asked 'Allow ise-1.demo.local to run "Java Platform SE 7"?'. Click the **Continue** button to **install Web agent**. If asked to **update Java**, please click later.

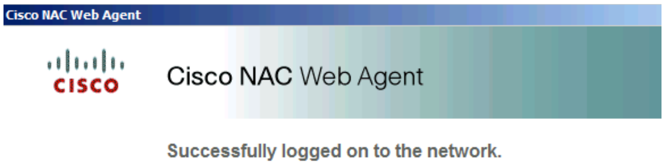
Note: Be cautious of bug **CSCuh75971**- Issue running applet in Windows or Macintosh OS with latest java 7 update 25. **CSCum76079** Client JAR manifest missing Permissions attribute & blocked by Java 7u51.

The ISE server certificate is signed by Active Directory Certificate Services but the root CA certificate has not been installed on the client PC w7pc-guest. Click **Yes** if prompted with any browser certificate warnings. Also, applets may be required to facilitate download of the Web Agent. Click **Yes** (or **Install**) if prompted to install applets as part of Web Agent download and install process.

Notice the yellow bar at the top of the page asking you to allow the install

You may be required to enter in your admin credentials of the machine **admin / ISEisC00L.** If a security warning appears please select continue. If this times out just refresh the page.

Step 225 The Cisco NAC Web Agent window should appear and indicate that posture assessment is being performed. Since no posture policy has been configured yet, the client will pass assessment and the agent will indicate "Host is compliant with network security policy" as shown below:



Successfully logged on to the network.

Reattempt access to the browser's home page via the home icon, or else manually enter the address of www.cisco.com in the address field. Access to the external website should now display.

Step 226 When finished, close the web browser session.

Step 227 Verify the session status on the switchport for Guest authorization.

Step 228 Return to the terminal session on the access switch.

Repeat the **show authentication sessions** output for interface GigabitEthernet 1/0/1. The output should appear similar to that shown below:

```
3k-access#sh auth sessions interface gigabitEthernet 1/0/1 detail
             Interface:  GigabitEthernet1/0/1
                IIF-ID:  0x1059000000000A3
           MAC Address:  0050.5687.ea65
          IPv6 Address:  Unknown
          IPv4 Address:  10.1.50.201
             User-Name:  jdoe
                Status:  Authorized
                Domain:  DATA
        Oper host mode:  multi-auth
      Oper control dir:  both
       Session timeout:  N/A
     Common Session ID:  0A01640100000FF8513EF2B4
       Acct Session ID:  0x00000FE5
                Handle:  0xB200003D
        Current Policy:  POLICY_Gi1/0/1

 Local Policies:
         Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

 Server Policies:
               ACS ACL:  xACSACLx-IP-INTERNET_ONLY-54bf6773

 Method status list:

        Method           State
        dot1x            Stopped
        mab              Authc Success

3k-access#show ip access-lists xACSACLx-IP-INTERNET_ONLY-54bf6773
 Extended IP access list xACSACLx-IP-INTERNET_ONLY-54bf6773 (per-user)
     1 permit udp any any eq domain
     2 permit icmp any any
     3 permit tcp any host 10.1.100.21 eq 8443
```

```
    4 deny ip any 10.1.0.0 0.0.255.255
    5 permit ip any any
```

Note: Note that URL redirection is no longer applied and that the dACL (ACS ACL) named **INTERNET_ONLY** is applied to the interface.

Step 229 Verify the authentication/authorization phases of the Central Web Auth and Client Provisioning session from the ISE admin interface.

From the Admin client PC, access the admin interface of the ISE Administrative node (**admin** / **ISEisC00L**).

Go to **Operations → Authentications**. View the recent entries associated with the web authentication session by MAC Address, IP address, interface, or Session ID. It may be help to filter the log entries by entering a couple bytes of the Session ID or MAC address (Calling Station ID) into the appropriate column header and hitting Enter. Click the circled x in the field to clear the filter.

Step 230 Referring to the example authentication log below (split across two screens), you should see entries similar to the following that match the output received from the switch:

Step 231 Successful MAB authentication of the MAC Address (username 00:50:56:B4:01:69 in example) and Authorization Profile named CWA_Posture_Remediation applied

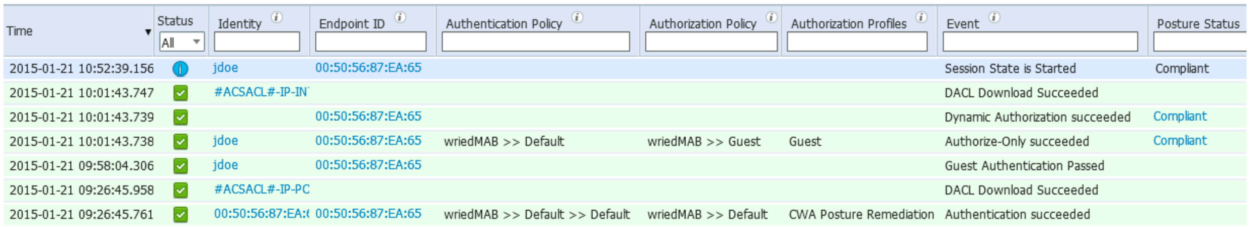
Step 232 dACL named POSTURE_REMEDIATION has been successfully downloaded.

Step 233 Guest login.

Step 234 Dynamic Authorization (CoA) succeeded for session.

Successful CWA authentication for Guest User (username *guser001* in example) and Authorization Profile named Guest applied.

Step 235 dACL named INTERNET_ONLY has been successfully downloaded.



Time	Status All	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Event	Posture Status
2015-01-21 10:52:39.156	i	jdoe	00:50:56:87:EA:65				Session State is Started	Compliant
2015-01-21 10:01:43.747	✓	#ACSACL#-IP-IN					DACL Download Succeeded	
2015-01-21 10:01:43.739	✓		00:50:56:87:EA:65				Dynamic Authorization succeeded	Compliant
2015-01-21 10:01:43.738	✓	jdoe	00:50:56:87:EA:65	wriedMAB >> Default	wriedMAB >> Guest	Guest	Authorize-Only succeeded	Compliant
2015-01-21 09:58:04.306	✓	jdoe	00:50:56:87:EA:65				Guest Authentication Passed	
2015-01-21 09:26:45.958	✓	#ACSACL#-IP-PC					DACL Download Succeeded	
2015-01-21 09:26:45.761	✓	00:50:56:87:EA:(	00:50:56:87:EA:65	wriedMAB >> Default >> Default	wriedMAB >> Default	CWA Posture Remediation	Authentication succeeded	

Note: **Note:** Session ID can be found by clicking on the details on a specific transaction. You also have the option to Show Live Sessions.

Test and Monitor Client Provisioning Services for AnyConnect Unified Agent

Exercise Description

This exercise validates the Client Provisioning and Authorization Policy configuration completed in the previous lab exercises. Since no Posture Policy has been configured, all users should be posture compliant. The AnyConnect Unified Agent will be tested and monitored in detail in this exercise. In addition to Agent provisioning, this exercise will also validate agent policies such as AUP, auto-closure of login success screens, and agent profile configuration.

Exercise Objective

In this exercise, your goal is to complete the following tasks:

- Login to the secured lab network from a Windows 7 PC client as an Employee via 802.1X machine authentication and user authentication and verify AnyConnect provisioning.
- Review ISE and switch logs to validate proper operation and application of the Authorization Policy.

Lab Exercise Steps

Power ON VM guest p##**_w7pc-corp**.

Step 236 Establish a terminal session with the 3k-access switch (10.1.100.1).

Validate the session status of the switchport authorization after Windows login (802.1X User authentication):

At the w7pc-corp VM console, send Ctrl+Alt+del and login to Windows domain as user **DEMO\employee1 / ISEisC00L**. Issue **show authentication sessions** for interface GigabitEthernet1/0/1. After successful 802.1X user authentication, the Authorization Policy should match the [Employee Posture Assessment] rule (Authorization Profile = Posture_Remedation). The output should appear similar to that shown below:

```
3k-access# sh auth sess int g1/0/1 details
            Interface:  GigabitEthernet1/0/1
          MAC Address:  0050.5693.6399
         IPv6 Address:  Unknown
          IPv4 Address:  10.1.50.202
             User-Name:  DEMO\employee1
           Device-type:  Microsoft-Workstation
                Status:  Authorized
                Domain:  DATA
        Oper host mode:  multi-auth
      Oper control dir:  both
       Session timeout:  N/A
     Common Session ID:  0A01640100000FFB52933346
       Acct Session ID:  0x00000FE8
                Handle:  0x2100003F
        Current Policy:  POLICY_Gi1/0/1

 Local Policies:
         Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

 Server Policies:
               ACS ACL:  xACSACLx-IP-POSTURE_REMEDIATION-54bf6344
          URL Redirect:  https://ise-
1.demo.local:8443/portal/gateway?sessionId=0A01640100000FFB52933346&portal=19f9d160-5e4e-11e4-
b905-005056bf2f0a&action=cpp&token=ed5181d4510d712bd6f49f1ccf03c0be
      URL Redirect ACL:  ISE-URL-REDIRECT
```

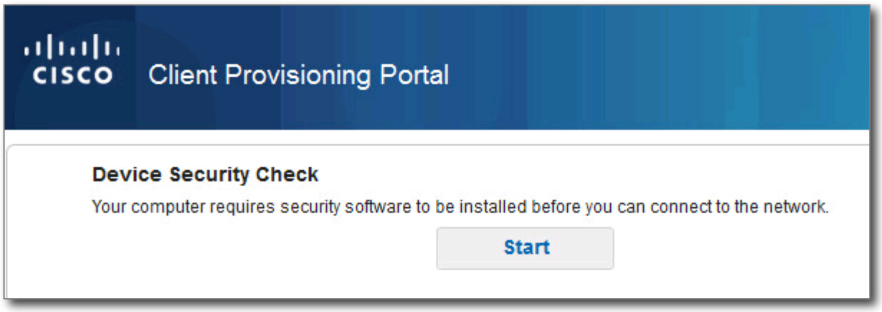
```
Method status list:
       Method           State
       dot1x            Authc Success
```

Verify that 802.1X user authentication (User-Name = **DEMO\employee1**) completed successfully and that the dACL (ACS ACL) named **POSTURE-REMEDIATION** pushed to the interface.

A named URL Redirect ACL = **ISE-URL-REDIRECT** has also been applied that defines the traffic to be redirected to the link specified by URL Redirect. The redirect URL must include the domain name of the ISE Policy Service node, reference to port 8443, the current session ID, and reference action to **cpp** (Client Provisioning Portal). If any of these items are missing, then web authentication will fail.

Step 237 Validate Client Provisioning (aka Web-Deploy) for the AnyConnect.

From w7pc-corp Windows session, launch Firefox web browser and go to www.cisco.com. It will immediately redirect to ISE client provisioning portal (CPP). (Accept/Confirm any browser certificate warnings if present)



Client Provisioning Portal

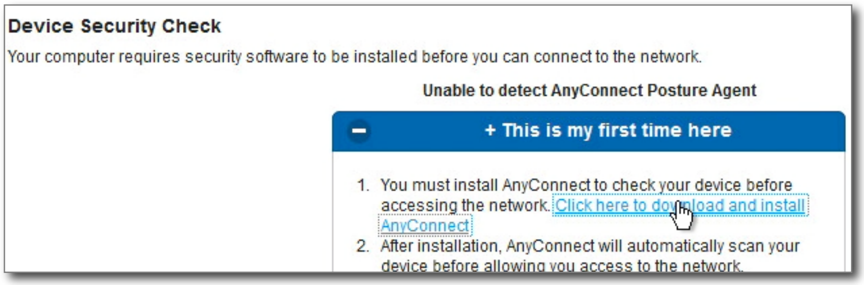
Device Security Check

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

Click the **Start** button.

Step 238 After CPP takes ~ 10 seconds to detect any existing AnyConnect installation, it shows an info page for the location to download and install AnyConnect.

Expand **+ This is my first time here** and click the hyperlink to download and install AnyConnect.



Device Security Check

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

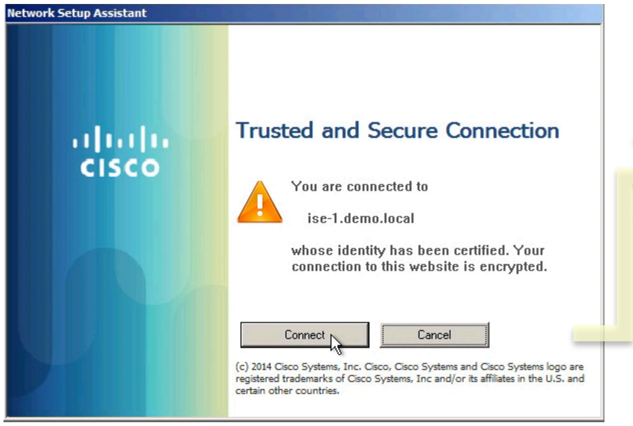
Unable to detect AnyConnect Posture Agent

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

Double click to run the downloaded program. If prompted by Windows UAC, enter credentials **admin / ISEisC00L**.

Note: Admin privileges are required to install AnyConnect for the first time. Once installed, upgrades can occur without escalated privileges. AnyConnect can also be distributed using an MSI installer package.

AnyConnect ISE Network Setup Assistant window appears. Click **Connect** to start running AnyConnect Downloader… Click **Yes** to restart your computer now when prompted.



Network Setup Assistant

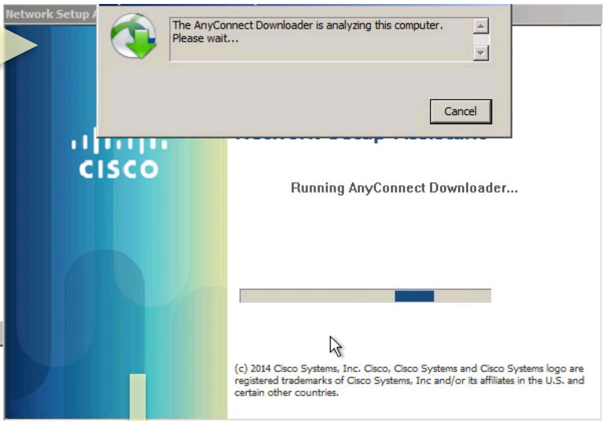
Trusted and Secure Connection

You are connected to

ise-1.demo.local

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

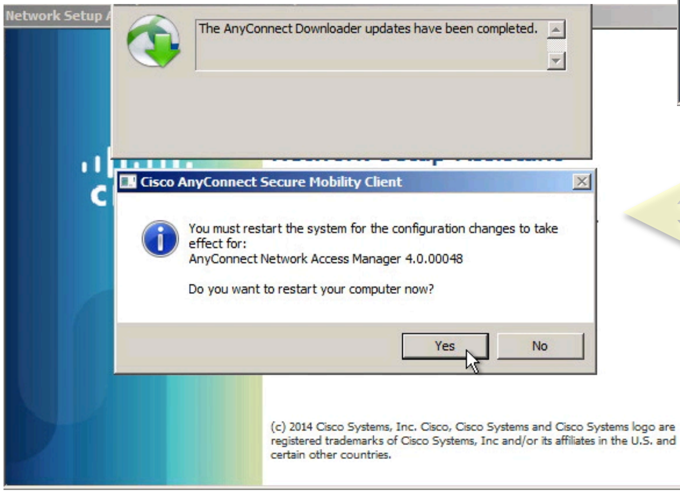
(c) 2014 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.



The AnyConnect Downloader is analyzing this computer. Please wait...

Running AnyConnect Downloader...

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



The AnyConnect Downloader updates have been completed.

Cisco AnyConnect Secure Mobility Client

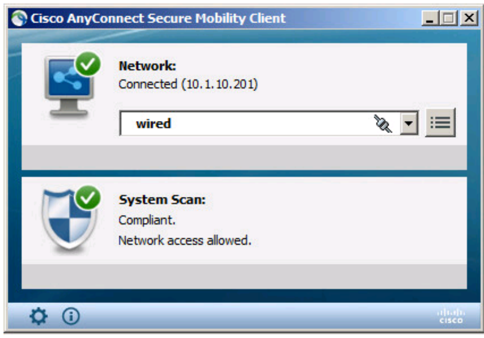
You must restart the system for the configuration changes to take effect for:
AnyConnect Network Access Manager 4.0.00048

Do you want to restart your computer now?

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

Step 239 After reboot and re-login, AnyConnect shows an AUP.

Click **Accept** to agree to the AUP. The System Scan tile should display indicating *Compliant. Network access allowed.*



Cisco AnyConnect Secure Mobility Client

Network:
Connected (10.1.10.201)
wired

System Scan:
Compliant.
Network access allowed.

The client should now have full network access. To validate, open a web browser and verify that access to www.cisco.com is allowed.

Note: Note: If the Client fails to obtain an IP address, shut/no shut interface gig 1/0/1 on the 3k-access switch.

Step 240 Verify the session status of the switchport authorization for a compliant Employee.

Repeat the **show authentication sessions** output for interface GigabitEthernet1/0/1. The Authorization Policy should match the Employee rule (Authorization Profile = Employee) and output should appear similar to that shown below:

```
3k-access#sh auth sess int g1/0/1 details
            Interface:  GigabitEthernet1/0/1
          MAC Address:  0050.5693.6399
           IP Address:  10.1.10.202
            User-Name:  employee1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
           Vlan Group:  N/A
              ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-4d269051
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A01FA02000000711F4E7514
```

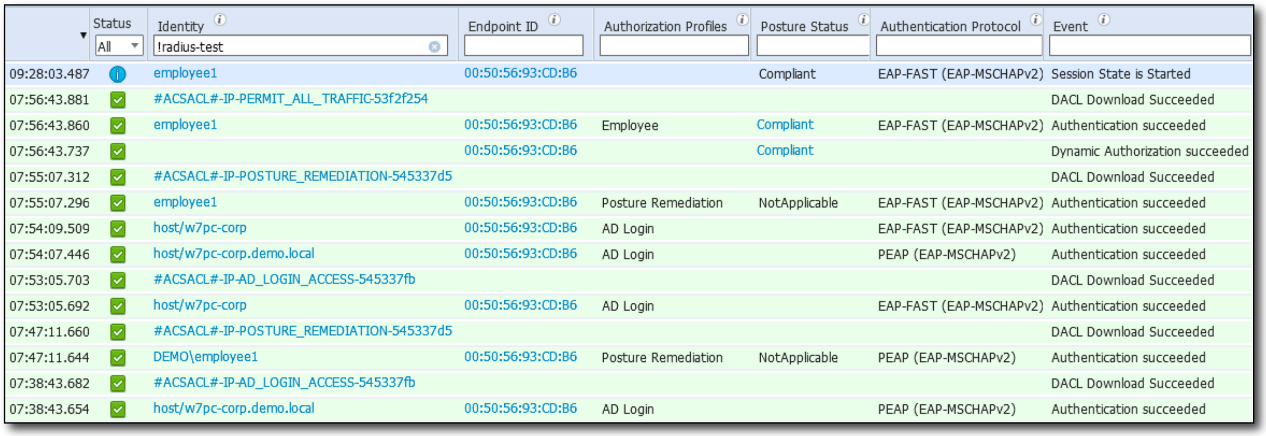
```
      Acct Session ID:  0x0000009C
               Handle:  0x0C000071

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

In the above output, note that the dACL (ACS ACL) = **PERMIT_ALL_TRAFFIC** has been successfully downloaded to the interface to grant the compliant Employee full network access.

Step 241 Verify the authentication/authorization phases of the 802.1X Auth and Client Provisioning from the ISE admin interface.

Go to **Operations > Authentications**. View the recent entries associated with the Employee session by MAC Address, IP address, Interface, or Session ID. It may be help to filter the log entries by entering a couple bytes of the Session ID or MAC address (Calling Station ID) into the appropriate column header and hitting Enter. Click the circled x in the field to clear the filter.

Referring to the sample log below, you should see entries similar to the following that match the output received from the switch, where 1 is the lowest or first entry:



▾	Status All	Identity !radius-test	Endpoint ID	Authorization Profiles	Posture Status	Authentication Protocol	Event
09:28:03.487	ⓘ	employee1	00:50:56:93:CD:B6		Compliant	EAP-FAST (EAP-MSCHAPv2)	Session State is Started
07:56:43.881	✓	#ACSACL#-IP-PERMIT_ALL_TRAFFIC-53f2f254					DACL Download Succeeded
07:56:43.860	✓	employee1	00:50:56:93:CD:B6	Employee	Compliant	EAP-FAST (EAP-MSCHAPv2)	Authentication succeeded
07:56:43.737	✓		00:50:56:93:CD:B6		Compliant		Dynamic Authorization succeeded
07:55:07.312	✓	#ACSACL#-IP-POSTURE_REMEDIATION-545337d5					DACL Download Succeeded
07:55:07.296	✓	employee1	00:50:56:93:CD:B6	Posture Remediation	NotApplicable	EAP-FAST (EAP-MSCHAPv2)	Authentication succeeded
07:54:09.509	✓	host/w7pc-corp	00:50:56:93:CD:B6	AD Login		EAP-FAST (EAP-MSCHAPv2)	Authentication succeeded
07:54:07.446	✓	host/w7pc-corp.demo.local	00:50:56:93:CD:B6	AD Login		PEAP (EAP-MSCHAPv2)	Authentication succeeded
07:53:05.703	✓	#ACSACL#-IP-AD_LOGIN_ACCESS-545337fb					DACL Download Succeeded
07:53:05.692	✓	host/w7pc-corp	00:50:56:93:CD:B6	AD Login		EAP-FAST (EAP-MSCHAPv2)	Authentication succeeded
07:47:11.660	✓	#ACSACL#-IP-POSTURE_REMEDIATION-545337d5					DACL Download Succeeded
07:47:11.644	✓	DEMO\employee1	00:50:56:93:CD:B6	Posture Remediation	NotApplicable	PEAP (EAP-MSCHAPv2)	Authentication succeeded
07:38:43.682	✓	#ACSACL#-IP-AD_LOGIN_ACCESS-545337fb					DACL Download Succeeded
07:38:43.654	✓	host/w7pc-corp.demo.local	00:50:56:93:CD:B6	AD Login		PEAP (EAP-MSCHAPv2)	Authentication succeeded

Successful 802.1X *machine* authentication of the Domain Computer host/w7pc-corp.demo.local using PEAP(EAP-MSCHAPv2); Authorization Profile named AD_Login applied.

dACL AD_LOGIN_ACCESS has been successfully downloaded.

Successful 802.1X *user* authentication of the Domain User DEMO\employee1; Authorization Profile named Posture_Remediation applied.

dACL POSTURE_REMEDIATION has been successfully downloaded.

Successful authentication of host/w7pc-corp using EAP-FAST(EAP-MSCHAPv2) due to NAM installation.

dACL AD_LOGIN_ACCESS has been successfully downloaded.

Successful machine authentication of host/w7pc-corp.demo.local using PEAP(EAP-MSCHAPv2) due to reboot.

Successful machine authentication of host/w7pc-corp using EAP-FAST(EAP-MSCHAPv2) due to reboot.

Successful 802.1X *user* authentication of the Domain User employee1; Authorization Profile named Posture_Remediation applied.

dACL POSTURE_REMEDIATION has been successfully downloaded.

Posture reported compliant and dynamic authorization (CoA) succeeded for session based on posture status change.

Authorization Profile named Employee applied; dACL PERMIT_ALL_TRAFFIC applied.

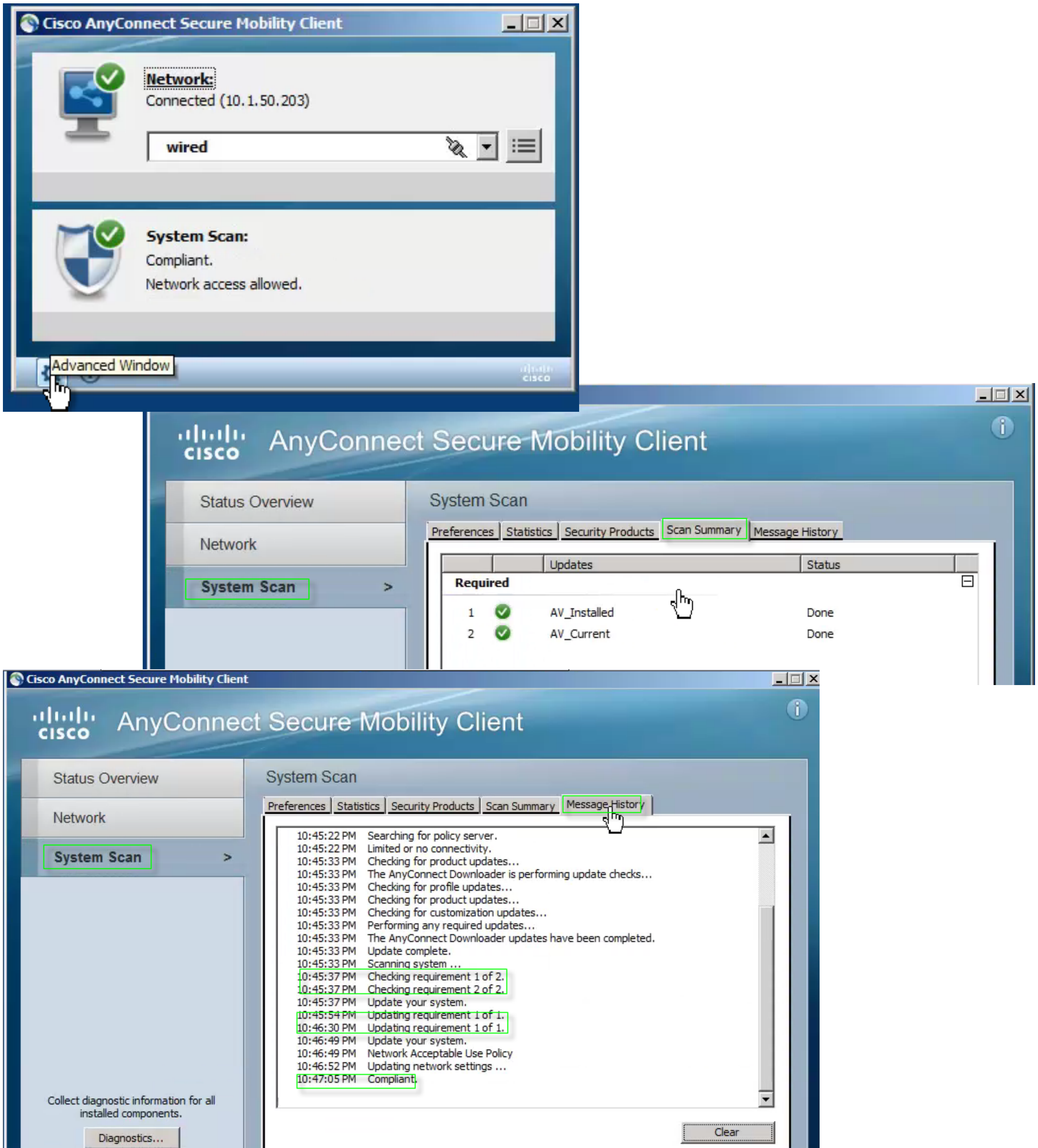
dACL PERMIT_ALL_TRAFFIC has been successfully downloaded.

Session State is Started.

Step 242 Review the AnyConnect installation.

Step 243 Click on the Advanced Window (gear symbol) to view more information about the current session.

Note: At this time, we will not see the requirements in Scan Summary or Message History as in the sample screen shots below, because of no posture policy yet.



Cisco AnyConnect Secure Mobility Client
Advanced Window
AnyConnect Secure Mobility Client
Status Overview
Network
System Scan
Preferences
Statistics
Security Products
Scan Summary
Message History
Collect diagnostic information for all installed components.
Diagnostics...
Clear

Network:
Connected (10.1.50.203)
wired

System Scan:
Compliant.
Network access allowed.

System Scan

	Updates	Status
Required		
1 ✓	AV_Installed	Done
2 ✓	AV_Current	Done

```
10:45:22 PM   Searching for policy server.
10:45:22 PM   Limited or no connectivity.
10:45:33 PM   Checking for product updates...
10:45:33 PM   The AnyConnect Downloader is performing update checks...
10:45:33 PM   Checking for profile updates...
10:45:33 PM   Checking for product updates...
10:45:33 PM   Checking for customization updates...
10:45:33 PM   Performing any required updates...
10:45:33 PM   The AnyConnect Downloader updates have been completed.
10:45:33 PM   Update complete.
10:45:33 PM   Scanning system ...
10:45:37 PM   Checking requirement 1 of 2.
10:45:37 PM   Checking requirement 2 of 2.
10:45:37 PM   Update your system.
10:45:54 PM   Updating requirement 1 of 1.
10:46:30 PM   Updating requirement 1 of 1.
10:46:49 PM   Update your system.
10:46:49 PM   Network Acceptable Use Policy
10:46:52 PM   Updating network settings ...
10:47:05 PM   Compliant.
```

Step 244 Close out all windows

Configure an Anti-Virus Posture Policy

Exercise Description

Posture assessment allows administrators to validate the applications and configurations on user endpoints through the use of posture agents such as the AC ISE Posture Module or NAC Web Agent. Posture assessment can utilize file, registry, application process, service, Windows and AV/AS checks to accomplish the task of determining endpoint compliance with Posture Policy. The Posture Policy defines the set of conditions that must be satisfied for an endpoint to be considered compliant, and if not, the methods to be used for remediation.

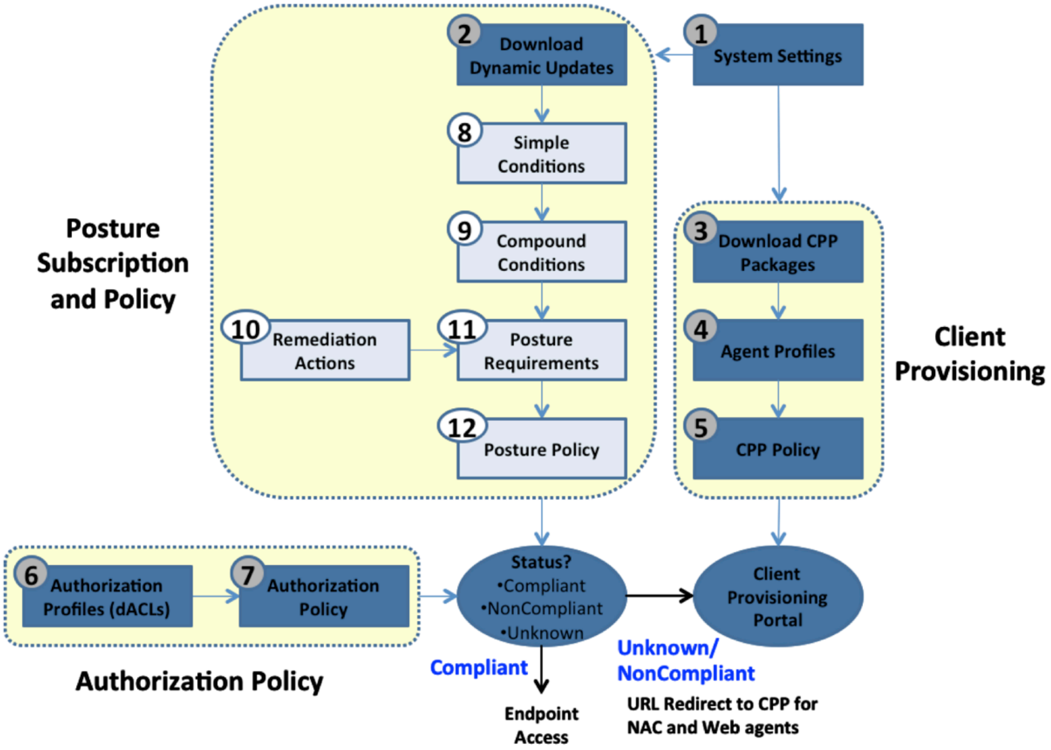
This exercise covers the configuration of a Posture Policy based on Antivirus (AV) conditions.

Exercise Objective

In this exercise, your goal is to complete the following tasks:

- Define AV posture conditions that validate the installation and signature version of ClamWin AV on an endpoint.
- Define AV posture conditions that validate the installation and signature version of *any* approved AV on an endpoint.
- Define remediation actions for installing and updating AV software.
- Configure requirements for AV to be installed and signatures current on an endpoint.
- Configure a Posture Policy for Employees to have ClamWin AV installed and current
- Configure a Posture Policy for Guest users to have *any* AV installed and current

The diagram highlights the key tasks covered in this exercise including Simple and Compound Conditions, Remediation Actions, Posture Requirements, and Posture Policy:



Lab Exercise Steps

Step 245 If not already completed from earlier lab step, make sure AV/AS and Cisco checks have been downloaded to the ISE appliance.

Step 246 Navigate to **Administration > System > Settings** and click the ▸ icon to the left of **Posture** in the left-hand pane to expand the contents of the Posture settings, and then click **Updates**. The Update Information section in the bottom right-hand pane should show information regarding update time and versions as shown in sample below. If values are empty, repeat lab steps to download updates.

Step 247

Step 248

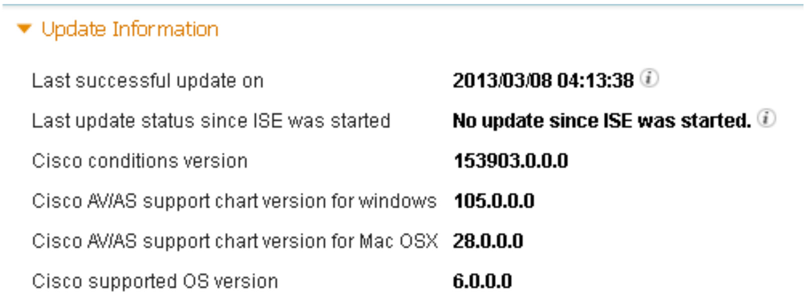
Step 249

Step 250

Step 251

Step 252

Step 253



▾ Update Information

Last successful update on	2013/03/08 04:13:38 ⓘ
Last update status since ISE was started	No update since ISE was started. ⓘ
Cisco conditions version	153903.0.0.0
Cisco AV/AS support chart version for windows	105.0.0.0
Cisco AV/AS support chart version for Mac OSX	28.0.0.0
Cisco supported OS version	6.0.0.0

Step 254 Define an AV posture condition that validates the *installation* of ClamWin AV on an endpoint. This check will be used in posture requirements applied to Employees.

Step 255 Go to **Policy → Policy Elements → Conditions** and click the ▸ icon to right of **Posture**. Select **AV Compound Condition** from the left-hand pane and then click **+ Add** from the right-hand pane menu. Enter the following values and then click **Submit** at the bottom of the page:

Name	ClamWin_AVinstalled
Description	Check ClamWin AV is installed
* Operating System	Windows 7 (All)
Vendor	ClamWin *** Note: There is also an entry for ClamAV ***
Check Type	⦿ Installation ○ Definition

Products for Selected Vendor
☑ ClamWin FREE Antivirus

Note: If no AV products appear under *Vendor* field, then posture updates have not yet been downloaded or download has not yet completed.

Step 256 Define an AV posture condition that validates the *signature version* of ClamWin AV on an endpoint. This check will be used in posture requirements applied to Employees.

Step 257 Click **Add** from the right-hand pane menu.

Step 258 Enter the following values and then click **Submit** at the bottom of the page:

Name	ClamWin_AVcurrent
Description	Check ClamWin AV is current
* Operating System	Windows 7 (All)
Vendor	ClamWin *** Note: There is also an entry for ClamAV ***
Check Type	○ Installation ⦿ Definition

○ Check against latest AV definition file version if available. Otherwise check against latest definition file date.

⦿ Allow virus definition files to be	7	days older than
	○ latest file date	⦿ current system date

Products for Selected Vendor
☑ ClamWin FREE Antivirus

Step 259

Step 260 Define a Posture Remediation Action that *installs* ClamWin AV on an endpoint.

Step 261 Go to **Policy > Policy Elements > Results** and click the ▸ icon to left of **Posture** (or double-click **Posture**) in the left-hand pane to expand its contents. Next, expand the contents of **Remediation Actions**.

Step 262 Select **Link Remediation** and then click **Add** from the right-hand pane menu. Enter the following values and then click **Submit**:

* Name	Install_ClamWin_AV
Description	Link distribution to ClamWin AV install package
Remediation Type	Manual
Interval	0
Retry Count	0
* URL	http://updates.demo.local/clamwin-0.97.6-setup.exe

Step 263

Step 264 Define a Posture Remediation Action that *updates* ClamWin AV on an endpoint.

Step 265 Select **AV Remediation** from the left-hand pane and then click **Add** from the right-hand pane menu. Enter the following values and then click **Submit**:

* Name	Update_ClamWin_AV_Definitions
Description	Link distribution to ClamWin AV install package
Remediation Type	Manual
* Interval	0
* Retry Count	0
Operation System	⦿ Windows ○ Mac
* AV Vendor Name	ClamWin *** Note: There is also an entry for ClamAV ***

Step 266

Step 267 Update a pre-built Posture Remediation Action that updates *any* supported AV on an endpoint.

Step 268 Select **AV Remediation** from the left-hand pane, select **AnyAVDefRemediationWin** from the list, and then click **Edit** from the right-hand pane menu. Change the remediation type from Automatic to Manual, and then click **Save**:

* Name	AnyAVDefRemediationWin
Description	Remediation for any AV
Remediation Type	Manual
* Interval	0
* Retry Count	0
Operation System	⦿ Windows ○ Mac
* AV Vendor Name	ANY

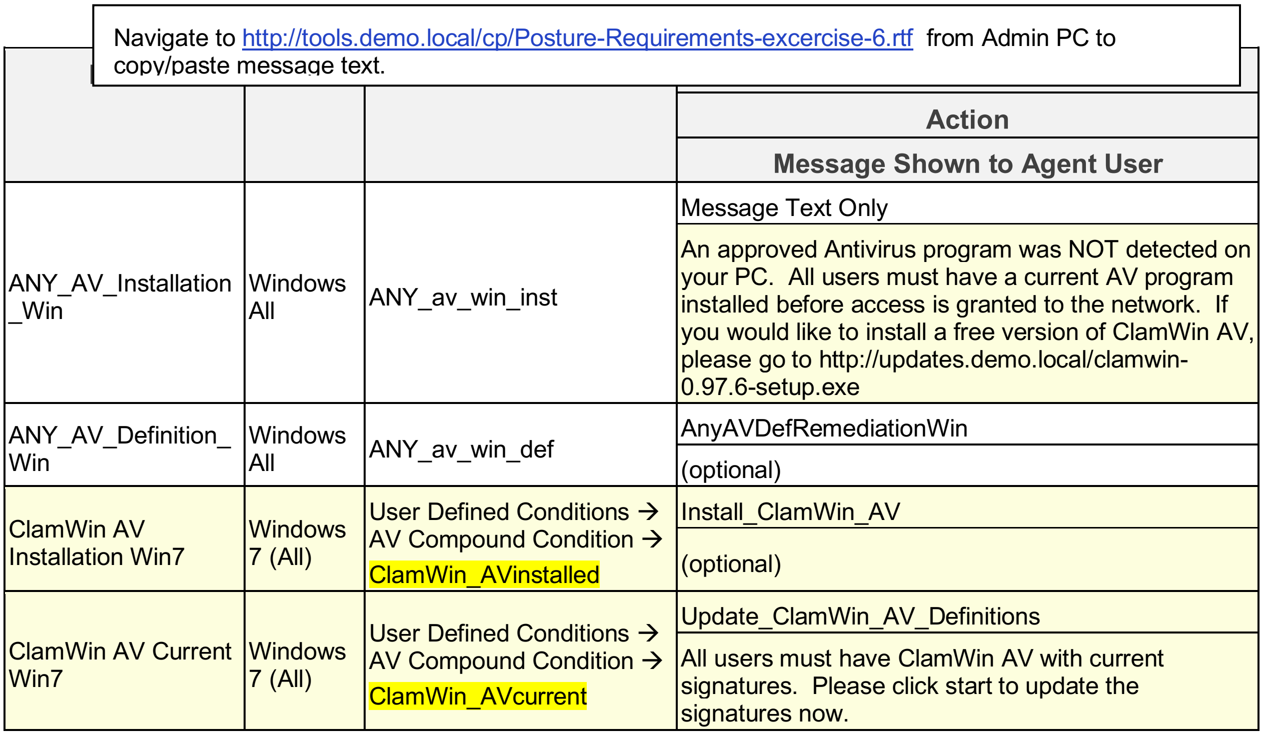
Step 269

Step 270

Step 271 Define Posture Requirements that will be applied to Employees and Guest users.

Step 272 Select Requirements from the left-hand pane (under Policy → Policy Elements → Results → Posture).

Enter the following entries into the table using the Edit ▾ selector at the end of a rule entry to insert or duplicate or update rules. Note that ordering does not matter. Click **Save** when finished.



Navigate to http://tools.demo.local/cp/Posture-Requirements-excercise-6.rtf from Admin PC to copy/paste message text.

			Action
			Message Shown to Agent User
ANY_AV_Installation_Win	Windows All	ANY_av_win_inst	Message Text Only
			An approved Antivirus program was NOT detected on your PC. All users must have a current AV program installed before access is granted to the network. If you would like to install a free version of ClamWin AV, please go to http://updates.demo.local/clamwin-0.97.6-setup.exe
ANY_AV_Definition_Win	Windows All	ANY_av_win_def	AnyAVDefRemediationWin
			(optional)
ClamWin AV Installation Win7	Windows 7 (All)	User Defined Conditions → AV Compound Condition → ClamWin_AVinstalled	Install_ClamWin_AV
			(optional)
ClamWin AV Current Win7	Windows 7 (All)	User Defined Conditions → AV Compound Condition → ClamWin_AVcurrent	Update_ClamWin_AV_Definitions
			All users must have ClamWin AV with current signatures. Please click start to update the signatures now.

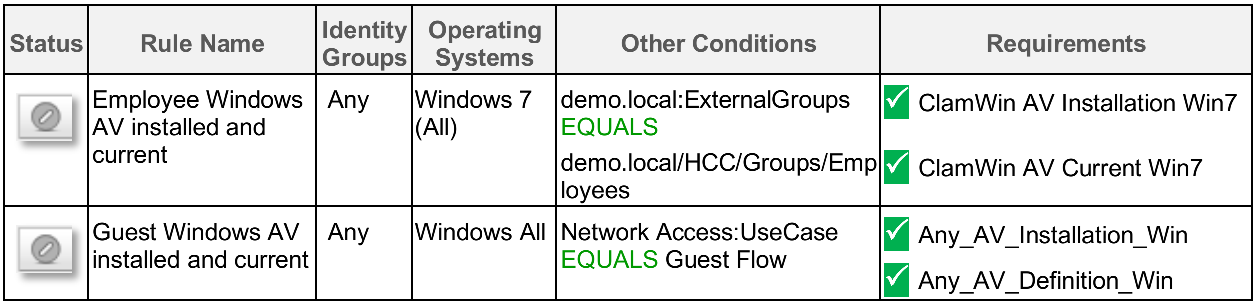
Note: If a preconfigured condition does not display under the list of Conditions, be sure you have selected the appropriate Operating System setting for both the condition as well as requirement rule. Only conditions that are the same or subset of the OS selected for the rule will display in the Conditions selection list.

Note: A remediation action of Message Text Only provides the message content in the Description field to the user if requirement fails. This can be used to provide instructions to end user such Help Desk contact numbers, URL links, or other text to assist in the remediation process. Also note that basic html can be entered into this field.

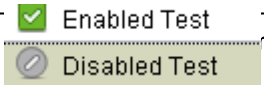
Note: Save your configuration

Step 273 Configure the Posture Policy to ensure ClamWin AV is installed and current on Employee computers running Windows 7 and that Any supported AV is installed and current on Guest user computers.

Step 274 Go to **Policy → Posture** and create new policy rules using the values provided in the table, and then click **Save** to apply your changes:

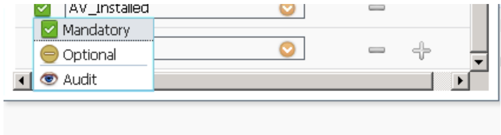


Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
⊘	Employee Windows AV installed and current	Any	Windows 7 (All)	demo.local:ExternalGroups EQUALS demo.local/HCC/Groups/Employees	✓ ClamWin AV Installation Win7 ✓ ClamWin AV Current Win7
⊘	Guest Windows AV installed and current	Any	Windows All	Network Access:UseCase EQUALS Guest Flow	✓ Any_AV_Installation_Win ✓ Any_AV_Definition_Win



Note: re policy rules to DISABLED using the selector on the left hand side of the rule:

Note: You will enable the posture rules individually during testing.



Note: ry, Optional, or Audit, click the ✓ icon to the right of the e drop-down menu:

OPTIONAL: Configure a Secure Screen Saver Posture Policy

Exercise Description

Posture assessment allows administrators to validate the applications and configurations on user endpoints through the use of posture agents such as the AC ISE Posture Module or NAC Web Agent. Posture assessment can utilize file, registry, application process, service, Windows and AV/AS checks to accomplish the task of determining endpoint compliance with Posture Policy. The Posture Policy defines the set of conditions that must be satisfied for an endpoint to be considered compliant, and if not, the methods to be used for remediation.

This exercise covers the configuration of a Posture Policy based on registry conditions to validate a Windows client PC has a secure screen saver configured.

Exercise Objective

In this exercise, your goal is to complete the following tasks:

- Define Registry posture conditions that validate the Windows desktop screen saver settings to be enabled and secure (require password to unlock computer) with a short timeout and screen saver selected (not set to *None*).
- Define a Remediation Action to update the registry configuration that controls the screen saver to policy compliant values.
- Configure a Posture Requirement for the screen saver to be enabled and secure.
- Configure a Posture Policy to apply the screen saver policy to any Windows user

Lab Exercise Steps

Step 275 Define Registry Conditions that validate the compliance of Windows screen saver settings with our lab policy.

Step 276 Go to **Policy → Policy Elements → Conditions** and click the › icon to right of **Posture**. Select **Registry Condition** from the left-hand pane.

Step 277 Create a Registry Condition that checks that the current user's screen saver is enabled.

Step 278 Click **Add** from the right-hand pane menu. Enter the following values and then click **Submit**.

* Name	ScreenSaver_On		
Description	(optional)		
Registry Type	RegistryValue		
Registry Root Key	HKCU	* Sub Key \	Control Panel\Desktop
* Value Name	ScreenSaveActive		
Value Data Type	Number		
Value Operator	equals		
Value Data	1		
* Operating System	Windows All		

Step 279 Create a Registry Condition that checks that the current user's screen saver is set to a value other than *(None)*.

Step 280 Click **Add** from the right-hand pane menu. Enter the following values and then click **Submit**.

* Name	ScreenSaver_SCR
Description	(optional)

Registry Type	RegistryValue		
Registry Root Key	HKCU	* Sub Key \	Control Panel\Desktop
* Value Name	SCRNSAVE.EXE		
Value Data Type	String		
Value Operator	ends with		
Value Data	scr		
* Operating System	Windows All		

Step 281 Create a Registry Condition that checks that the current user's screen saver is secure (password set).

Step 282 Click **Add** from the right-hand pane menu. Enter the following values and then click **Submit**.

* Name	ScreenSaver_Secure		
Description	(optional)		
Registry Type	RegistryValue		
Registry Root Key	HKCU	* Sub Key \	Control Panel\Desktop
* Value Name	ScreenSaverIsSecure		
Value Data Type	Number		
Value Operator	equals		
Value Data	1		
* Operating System	Windows All		

Step 283 Create a Registry Condition that checks that the current user's screen saver timeout is less than or equal to 300 seconds (5 minutes).

Step 284 Click **Add** from the right-hand pane menu. Enter the following values and then click **Submit**.

* Name	ScreenSaver_Timeout		
Description	(optional)		
Registry Type	RegistryValue		
Registry Root Key	HKCU	* Sub Key \	Control Panel\Desktop
* Value Name	ScreenSaveTimeOut		
Value Data Type	Number		
Value Operator	less than or equal to		
Value Data	300		
* Operating System	Windows All		

Step 285 Create a Compound Condition that includes each of the specific Screen Saver registry checks as a single condition.

Step 286 Select **Compound Condition** from the left-hand pane, and then click **Add** from the right-hand pane menu. Enter the following values from the table:

<table>
<tr><td>* Name</td><td>ScreenSaver</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Description</td><td>(optional)</td><td></td><td></td><td></td><td></td></tr>
<tr><td>* Operating System</td><td>Windows All</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Expression</td><td>Select a condition to insert below</td><td>( )</td><td>!</td><td>&</td><td>|</td></tr>
</table>

ScreenSaver_On & ScreenSaver_Secure & ScreenSaver_SCR & ScreenSaver_Timeout

Note: Although the Expression content in a Compound Condition can be manually entered, it is recommend that the Condition List be used to navigate and select the desired checks. This helps to ensure values are entered correctly. Use the operand buttons [**( ) & ! |**] to select the correct logical separators.

Step 287 Click the › icon to right of **Registry Condition** in the Condition List section.
Step 288 Select **ScreenSaver_On** from the list. Item should appear in open text field.
Step 289 Click the **&** symbol button under the open text field. The symbol should be appended to the content in the open text field.
Step 290 Complete the condition expression using the following selections:
Step 291 ScreenSaver_Secure
Step 292 &
Step 293 ScreenSaver_SCR
Step 294 &
Step 295 ScreenSaver_Timeout
Step 296 Click ⓘ icon to the right of the expression window to see basic syntax help for creating a compound condition based on individual checks (simple conditions).
Step 297 Click **Validate Expression** to have the system verify the basic expression logic and that expression is composed of valid checks.
Step 298 Click **Submit** when finished.
Step 299 Define a Posture Remediation Action that updates the screen saver registry keys on a Windows PC to compliant values.
Step 300 Navigate to **Policy → Policy Elements → Results** and expand the contents under **Posture**, and then expand **Remediation Actions**.
Step 301 Select **Link Remediation** from the left-hand pane and then click **Add** from the right-hand pane menu. Enter the following values and then click **Submit**:

* Name	Enable_Secure_Screen_Saver
Description	Download compliant screen saver registry values
Remediation Type	Manual
Interval	0
Retry Count	0
* URL	http://updates.demo.local/ScreenSaver.reg

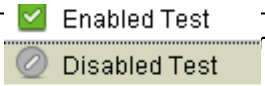
Step 302 Define Posture Requirements that will be applied to Employees and Guest users.
Step 303 Select Requirements from the left-hand pane (under Policy → Policy Elements → Results → Posture).
Step 304 Add a Screen Saver requirement into the table using the following values and then click **Save**:

Name	Operating System	Conditions	Remediation Actions
			Action
			Message Shown to Agent User
Screen Saver On and Secure	Windows All	User Defined Conditions → Regular Compound Condition → ScreenSaver	Enable_Secure_Screen_Saver
			PCs must have a screen saver enabled and password protected. You may manually make changes to these settings or else click the link to download and run a file that contains secure screen saver settings

Step 305
Step 306 Configure the Posture Policy to ensure a Secure Screen Saver is present on Employee and Guest user computers running Windows.
Step 307 Go to **Policy → Posture** and create new policy rules using the values highlighted in the table, and then click **Save** to apply your changes:

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
⊘	Employee ScreenSaver	Any	Windows All	demo.local:ExternalGroups EQUALS demo.local/HCC/Groups/Employees	✓ Screen Saver On and Secure
⊘	Employee Windows AV installed and current	Any	Windows 7 (All)	demo.local:ExternalGroups EQUALS demo.local/HCC/Groups/Employees	✓ ClamWin AV Installation Win7 ✓ ClamWin AV Current Win7
⊘	Guest ScreenSaver	Any	Windows All	Network Access:UseCase EQUALS Guest Flow	✓ Screen Saver On and Secure
⊘	Guest Windows AV installed and current	Any	Windows All	Network Access:UseCase EQUALS Guest Flow	✓ Any_AV_Installation_Win ✓ Any_AV_Definition_Win

Step 308



Note: re policy rules to DISABLED using the selector on the left hand side of the rule:

Note: You will enable the posture rules individually during testing

Test Posture Assessment and Posture Policies using AnyConnect Unified Agent

Exercise Description

- In the previous lab exercises you have configured and tested Client Provisioning services to validate policy-based distribution of the AnyConnect Agent to Employees. Posture Policies have also been configured. This exercise will test the Posture Requirements and Policies for Employees running the AnyConnect Agent.

Exercise Objective

- In this exercise, your goal is to complete the following tasks:
- Login as an Employee via 802.1X authentication and verify proper execution of AC ISE Posture Module discovery, posture, and remediation process.
- Test AV Posture Policy using AnyConnect Agent.
- OPTIONAL: Test Screen Saver Posture Policy using AnyConnect Agent.
- Review switch commands to validate correct application of policies.
- Review ISE authentication log monitoring tools to validate correct application of policies.
- OPTIONAL: Configure and test Passive Re-Assessment (PRA).

Lab Exercise Steps

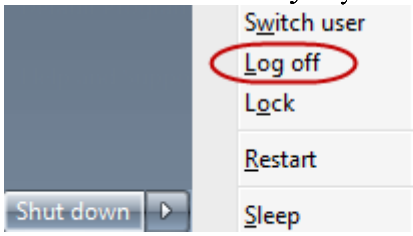
AV POSTURE TESTING

Step 309 Delete ClamWin AV signatures on the w7pc-corp to ensure that the client AV software is out of compliance with AV signature updates.

Step 310 Log into the w7pc-corp client as **DEMO\employee1** / **ISEisC00L**, where *DEMO* is the Windows domain name.

Step 311 From the w7pc-corp client, open the **Lab Tools** shortcut from the Windows desktop and run (double-click) the **Delete_ClamWin_AV_Updates** script.

Step 312 A command window should open to execute processing of the script and indicate “Process Complete!” when finished. Press ***any*** key to continue.



Step 313 Close the **Lab Tools** window.

Step 314 **Logoff** Windows using the Start menu:

Step 315 Enable the AV Posture Policy for Employees.

From the Admin client PC, access the ISE admin interface and go to **Policy > Posture**.

Enable the **Employee Windows AV Installed and Current** rule by setting its status as follows:

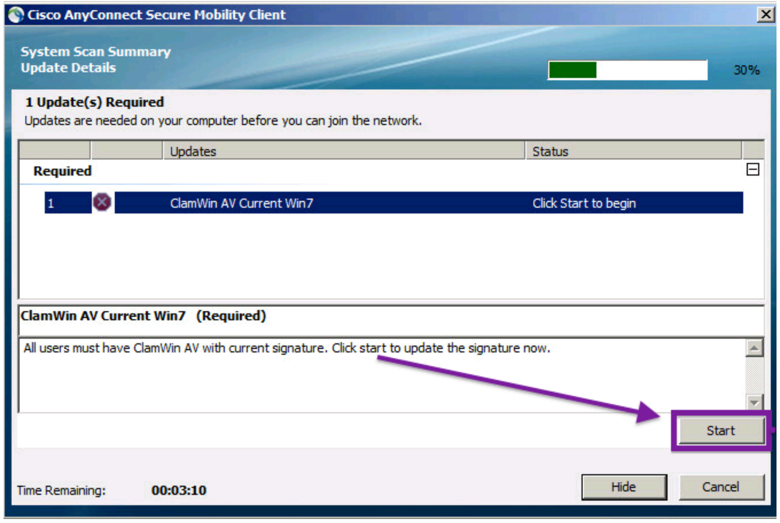
✓ ▾

Click **Save** to apply changes.

Step 316 Test AV Posture Policy for Employees.

Log back in to w7pc-corp as **DEMO\employee1 / ISEisC00L**, where *DEMO* is the Windows domain name.

The previously installed AnyConnect should automatically launch after Windows login and begin the posture assessment process. Due to an out-of-compliance condition for the AV policy and the remediation action was set to *manual*, click **Start** to initiate it.



Cisco AnyConnect Secure Mobility Client

System Scan Summary
Update Details

30%

1 Update(s) Required
Updates are needed on your computer before you can join the network.

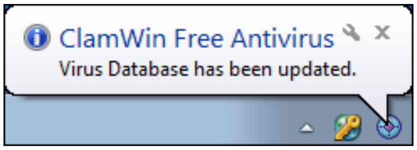
	Updates	Status
Required		
1	ClamWin AV Current Win7	Click Start to begin

ClamWin AV Current Win7 (Required)

All users must have ClamWin AV with current signature. Click start to update the signature now.

Time Remaining: 00:03:10

Step 317 This manual remediation will trigger the ClamAV client to update its signature definitions. It may take ~ 2 minutes because downloading full ~ 100-Mbyte definition files. A notification should be viewable from the Windows task tray upon successful update.



ClamWin Free Antivirus
Virus Database has been updated.

Note: If the ClamWin update process fails…

Note: The remediation server (updates.demo.local) is configured to download current AV signature files upon start of the p##_**lob-web** VM. If this process fails to complete, then the ClamAV client may fail to download the AV signature files from the remediation server as shown above. If the above process fails, then go to **Policy → Posture** from the ISE admin interface, and change the requirements for the posture rule named *Employee Windows AV Installed and Current* policy from Mandatory to Optional.

Note: To specify posture requirements as Optional, navigate to the Requirements column of the posture policy rule and expand the contents of the requirement. Click the ✓ icon to the right of the requirement name and select **Optional** from the drop-down menu. Repeat for each requirement in the rule.

The AUP page should display following successful remediation. Click **Accept** to accept the Network Usage Policy Terms and Conditions.

Step 318 Validate the authorization status of the w7pc-corp client on the access switch.

Step 319 Return to the access switch terminal session.

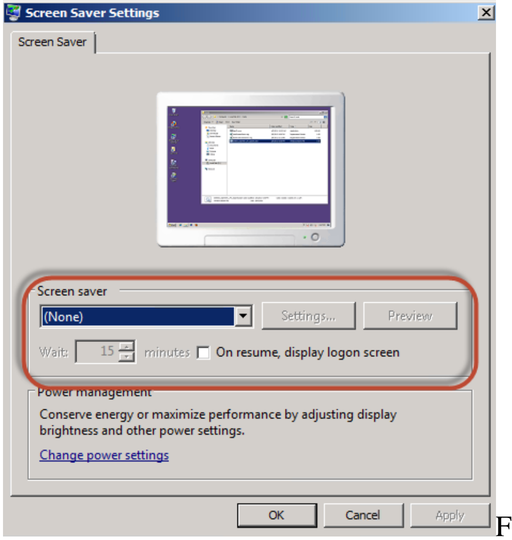
Verify the authorization status of the PC switchport using the command **show authentication sessions interface GigabitEthernet 1/0/1**.

Step 320 The DATA domain should show successful 802.1X authentication from user auth (User-Name = DEMO\employee1) and the current dACL (ACS ACL) should be PERMIT_ALL_TRAFFIC.

SCREEN SAVER POSTURE TESTING

Step 321 Prepare the PC client w7pc-corp for testing the full Posture Policy for Employees.

Step 322 Run the **Delete_ClamWin_AV_Updates** script from the Lab Tools shortcut on the Windows desktop. This will remove the AV client's current signature definitions.



Screen Saver Settings

Screen Saver

Screen saver: (None)

Wait: 15 minutes □ On resume, display logon screen

Power management

Conserve energy or maximize performance by adjusting display brightness and other power settings.

Change power settings

Step 323 From the Windows desktop, double-click the **Screen Saver** shortcut to open the Control Panel's Personalization settings.

Step 324 Verify that the Windows screen saver settings are disabled:

Step 325 Screen saver = **(None)**

Step 326 On resume, display logon screen = **<Not checked>**

Step 327

Step 328 Click **OK** to close the Screen Saver Settings and close the Control Panel window.

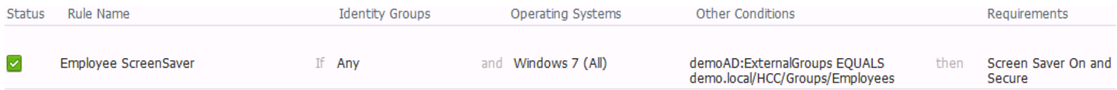
Step 329

Step 330 Log off from w7pc-corp.

Step 331 Enable the Screen Saver Posture Policy for Employees.

From the Admin client PC, access the ISE admin interface and go to **Policy > Posture**.

Enable the **Employee ScreenSaver** rule by setting its status as ✓ follows:



Status	Rule Name		Identity Groups		Operating Systems	Other Conditions		Requirements
☑	Employee ScreenSaver	If	Any	and	Windows 7 (All)	demoAD:ExternalGroups EQUALS demo.local/HCC/Groups/Employees	then	Screen Saver On and Secure

Click **Save** to apply changes.

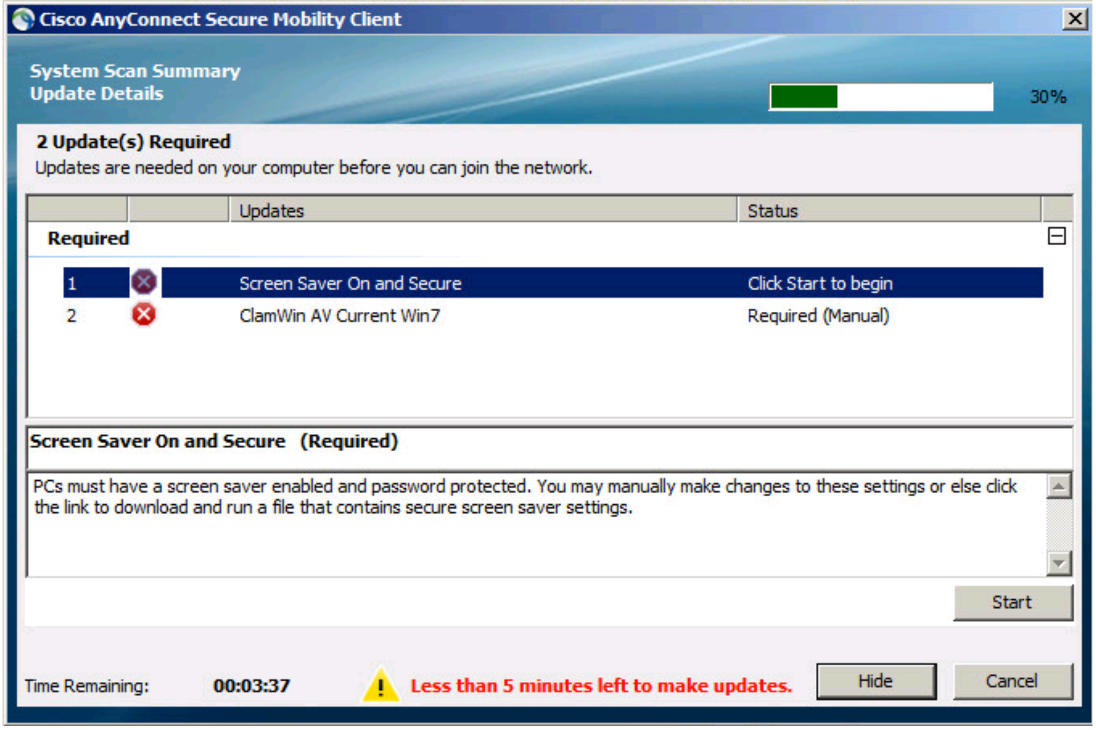
Step 332 Test Screen Saver Posture Policy for Employees.

Log back in to the Windows 7 PC client as **DEMO\employee1 / ISEisC00L**, where *DEMO* is the Windows domain name.

Step 333 The AnyConnect Agent should automatically launch after Windows login and begin the posture assessment process. Since we reverted the AV signatures to a non-compliant state, automatic AV signature remediation will again need to be performed.

The Remediation Action for the Screen Saver Posture Requirement was set to *Manual* so deliberate user input is required to trigger remediation.

Read the instructions (this information was entered into the requirement description during creation of the Posture Requirement) and click **Go To Link**:



2 Update(s) Required

Updates are needed on your computer before you can join the network.

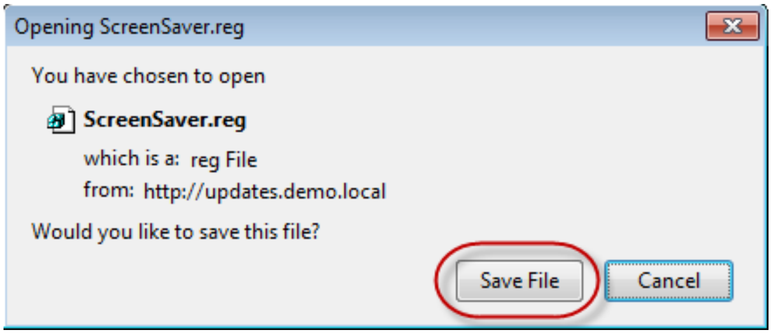
		Updates	Status
Required			
1	☒	Screen Saver On and Secure	Click Start to begin
2	☒	ClamWin AV Current Win7	Required (Manual)

Screen Saver On and Secure (Required)

PCs must have a screen saver enabled and password protected. You may manually make changes to these settings or else click the link to download and run a file that contains secure screen saver settings.

Time Remaining: 00:03:37 Less than 5 minutes left to make updates.

Click on 'Start and a window will appear to download the registry fixes from the lab update server. Click **Save File**:



You have chosen to open

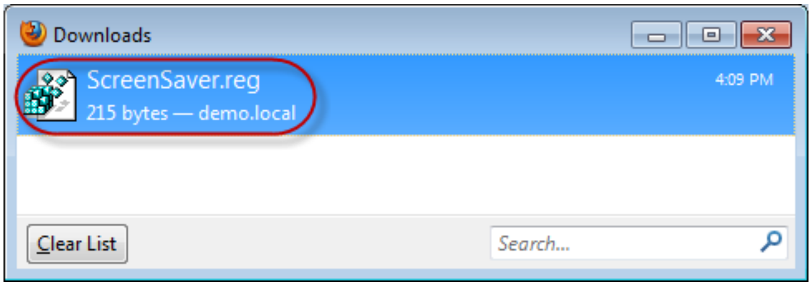
ScreenSaver.reg

which is a: reg File

from: http://updates.demo.local

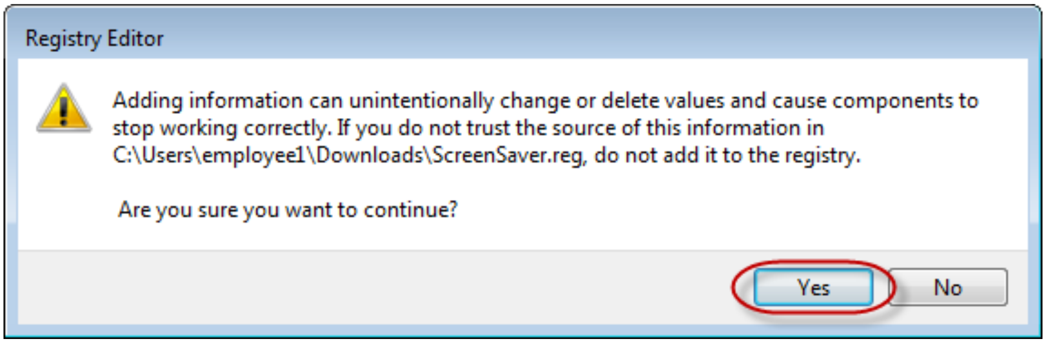
Would you like to save this file?

Step 334 The file ScreenSaver.reg is downloaded to w7pc-corp. Double-click the filename to install the new registry settings:



Note: If the link only provides text and no download, then open Lab Tool folder short cut and double click the **AddScreenSaver.reg**

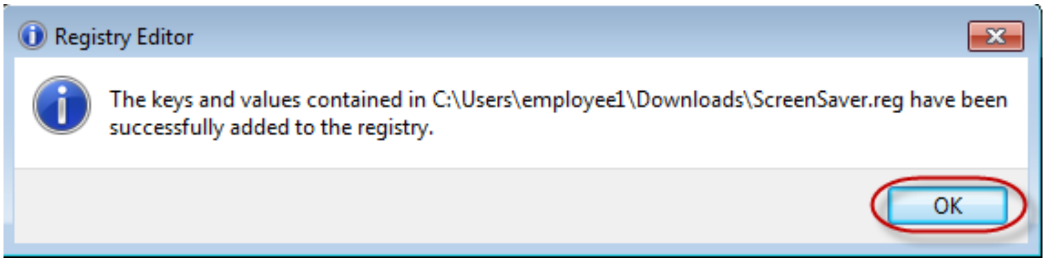
A Windows warning message appears to inform you that the registry will be modified. Click **Yes** to apply the changes:


Registry Editor

Adding information can unintentionally change or delete values and cause components to stop working correctly. If you do not trust the source of this information in C:\Users\employee1\Downloads\ScreenSaver.reg, do not add it to the registry.

Are you sure you want to continue?

Click **OK** to acknowledge the successful registry update:


Registry Editor

The keys and values contained in C:\Users\employee1\Downloads\ScreenSaver.reg have been successfully added to the registry.

Step 335 Close any remaining browser windows opened as part of the remediation process.

The AUP page should display following successful remediation. Click **Accept** to accept the Network Usage Policy Terms and Conditions.

A message will appear stating *Network access allowed*.

Step 336 Test the Employee login experience when fully compliant with Posture Policy.

Step 337 Logoff from w7pc-corp and then log back in as user DEMO\employee1.

Step 338 Upon Windows login, the AnyConnect ISE Posture Module (System Scan) should open and detect that the client PC is fully compliant with Posture Policy. Only the AUP should require user input. Click **Accept** to accept the AUP. The AC ISE Posture Module should show Network access allowed.

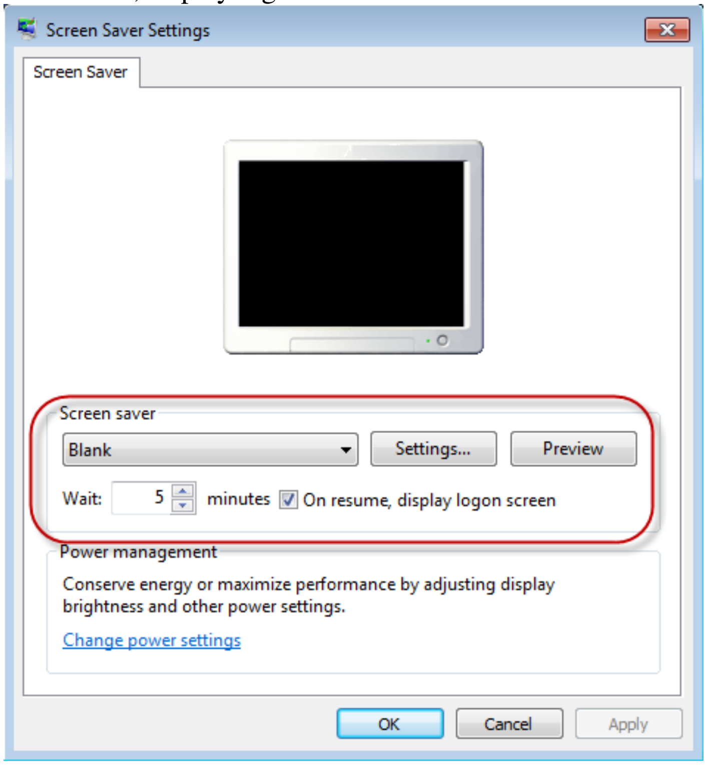
Step 339 Verify the Screen Saver policy settings:

Step 340 From the Lab Tools shortcut on the Windows desktop, double-click the **Personalization** shortcut to open the Control Panel's Personalization settings.

Step 341 Select **Screen Saver** from the Control Panel windows (bottom right corner).

Step 342 Verify that the Windows screen saver settings are disabled:

Step 343 Screen saver = **Blank**
Step 344 Wait = 5 minutes
Step 345 On resume, display logon screen = **<Checked>**



Screen saver

Blank

Wait: 5 minutes ☑ On resume, display logon screen

Power management

Conserve energy or maximize performance by adjusting display brightness and other power settings.

Change power settings

Step 346 Click **OK** to close the Screen Saver Settings and close the Control Panel window.

Step 347 Review the ISE Authentication logs for proper authentication, authorization, and policy assignment.
Step 348 Access the ISE admin interface from the Admin client PC.
Step 349 Go Operations → Authentications.
Step 350 Review the entries associated with w7pc-corp based on IP address. Note the following progression of entries that indicate proper application of the Authorization Policy based on authentication and posture compliance state:
Step 351 Username=host/w7pc-corp.demo.local, Authorization Profile=AD Login
Step 352 Username=DEMO\employee1, Authorization Profile=Posture Remediation
Step 353 Username=DEMO\employee1, Authorization Profile=Employee
Step 354
Step 355 OPTIONAL: Passive Re-Assessment (PRA) TESTING
Step 356 Configure the PRA policy from the system posture settings:

Go to **Administration → System → Settings** and click the ▸ icon to the left of **Posture** in the left-hand pane to expand the contents of the Posture settings

Click **Reassessments** in the left-hand pane, and then click **Add** from the menu in the right-hand pane.

Step 357 Enter the following values for the new PRA policy and click **Submit** when finished:

* Configuration Name	**PRA_Any_User**
Configuration Description	(optional)
Use Reassessment Enforcement?	☑
Enforcement Type	**remediate**
Interval	**2**

Grace Time	**1**
Select Roles	**Any**

Step 358

Note: The standard minimum settings for PRA Interval and Grace Time are 240 and 5 minutes, respectively. The settings used in this lab are for training purposes only. Specific code changes were necessary for the ISE appliance in this lab to allow these lower values to be configured.

Step 359

Step 360 Configure the Posture Policy for PRA.

Step 361 By default, all matching posture requirements are validated upon initial posture assessment and then periodically according to the PRA policy. The Session attribute **Agent-Request-Type** can be defined in the Posture Policy to selectively apply posture requirements to either the initial assessment only or to periodic reassessment only:

Step 362 To apply a matching posture requirement to the initial assessment only, set the Session:Agent-Request-Type attribute EQUAL to **Initial**.

Step 363 To apply a matching posture requirement to periodic reassessments only, set the Session:Agent-Request-Type attribute EQUAL to **Periodic Reassessment**.

Step 364 To apply a matching posture requirement to *both* the initial assessment *and* periodic reassessments, then simply leave the attribute undefined for the policy rule, i.e. do not set Session:Agent-Request-Type.

Step 365

Step 366 Access the ISE admin interface from the Admin client PC.

Step 367 Go to **Policy → Posture** and update the Posture Policy conditions for Employees with the values shown below:

Status	Rule Name	Identity Groups	Operating Systems	Other Conditions	Requirements
✓	Employee ScreenSaver	Any	Windows All	demo.local:ExternalGroups EQUALS demo.local/HCC/Groups/Employees **AND** Session:Agent-Request-Type EQUALS Periodic Reassessment	✓ Screen Saver On and Secure
✓	Employee Windows AV installed and current	Any	Windows 7 (All)	demo.local:ExternalGroups EQUALS demo.local/HCC/Groups/Employees **AND** Session:Agent-Request-Type EQUALS Initial	✓ ClamWin AV Installation Win7 ✓ ClamWin AV Current Win7
⊘	Guest ScreenSaver	Any	Windows All	Network Access:UseCase EQUALS Guest Flow	✓ Screen Saver On and Secure
⊘	Guest Windows AV installed and current	Any	Windows All	Network Access:UseCase EQUALS Guest Flow	✓ Any_AV_Installation_Win ✓ Any_AV_Definition_Win

Step 368 Click **Save** to apply change

Note: If you have not completed the OPTIONAL Screen Saver posture policy configuration, you can alternatively test PRA for the AV policy by setting the **Session:Agent-Request-Type EQUALS Periodic Reassessment** for the **Employee Windows AV Installed and Current** policy.

Step 369 Test PRA from the Windows 7 client PC:

Step 370 Logoff from the w7pc-corp and then log back in as user DEMO\employee1.

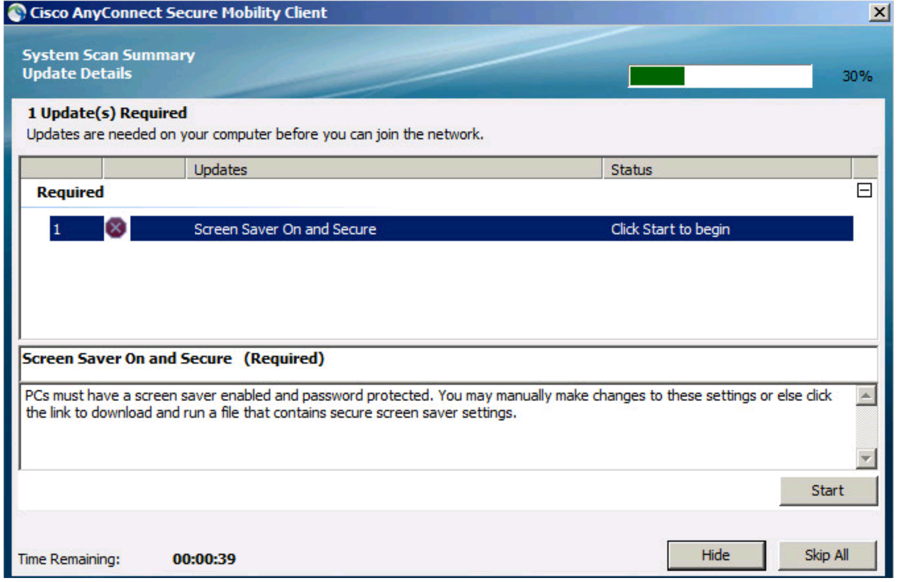
Note: If login is required to unlock screen, be sure to login first to active login session to unlock desktop, and then logoff Windows.

Step 371 Upon Windows login, the AnyConnect Agent should open and detect that the client PC is fully compliant with Posture Policy. Only the AUP should require user input. Click **Accept** to accept the AUP. The AnyConnect Agent should show network access allowed.

Step 372 From the Lab Tools shortcut on the Windows desktop, run the **Delete_ClamWin_AV_Updates** script from the Windows desktop to remove the AV client's signature definitions.

Step 373 Run the **Remove Screensaver** script from the Windows desktop to revert the screen saver settings to non-compliant values. Click **Run**, then **Yes** and then **OK** to accept and acknowledge the registry changes.

Step 374 Wait up to two minutes for the posture reassessment Interval to trigger. The AnyConnect Agent should open to alert the failure of the Screen Saver and AV policy.


Cisco AnyConnect Secure Mobility Client

System Scan Summary
Update Details

30%

1 Update(s) Required
Updates are needed on your computer before you can join the network.

		Updates	Status
Required			
1	☒	Screen Saver On and Secure	Click Start to begin

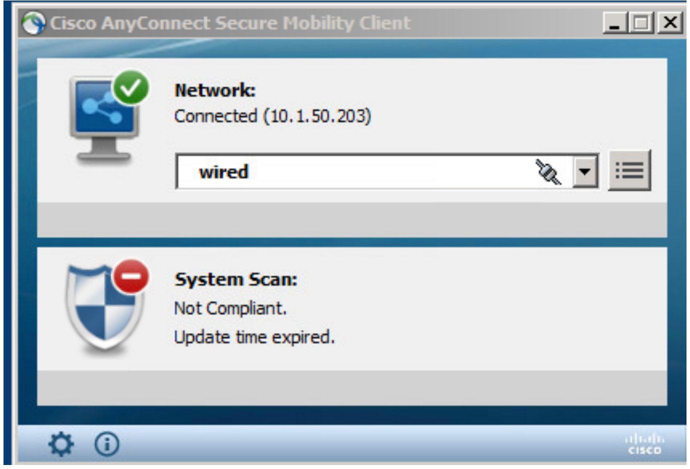
Screen Saver On and Secure (Required)

PCs must have a screen saver enabled and password protected. You may manually make changes to these settings or else click the link to download and run a file that contains secure screen saver settings.

Time Remaining: 00:00:39

Step 375

Step 376 Allow the 1 minute Grace Time to expire. The following message will display:


Cisco AnyConnect Secure Mobility Client

Network:
Connected (10.1.50.203)

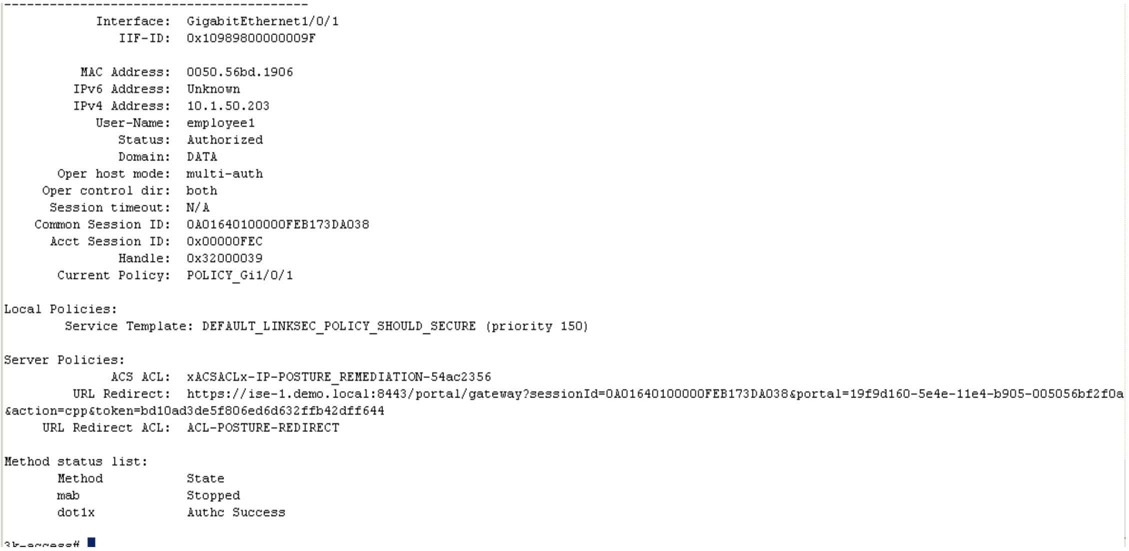
wired

System Scan:
Not Compliant.
Update time expired.

Step 377

Step 378 Review the switchport authorization status on the access switch.

Return to the access switch terminal session and verify the authorization status of the PC switchport using the command **show authentication sessions interface GigabitEthernet 1/0/1**. The current dACL (ACS ACL) should now be POSTURE-REMEDIATION (changed from PERMIT_ALL_TRAFFIC).



```
----------------------------------------
            Interface:  GigabitEthernet1/0/1
               IIF-ID:  0x10989800000009F

          MAC Address:  0050.56bd.1906
         IPv6 Address:  Unknown
         IPv4 Address:  10.1.50.203
            User-Name:  employee1
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0A01640100000FEB173DA038
      Acct Session ID:  0x00000FEC
               Handle:  0x32000039
       Current Policy:  POLICY_Gi1/0/1

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
              ACS ACL:  xACSACLx-IP-POSTURE_REMEDIATION-54ac2356
         URL Redirect:  https://ise-1.demo.local:8443/portal/gateway?sessionId=0A01640100000FEB173DA038&portal=19f9d160-5e4e-11e4-b905-005056bf2f0a
&action=cpp&token=bd10ad3de5f806ed6d632ffb42dff644
     URL Redirect ACL:  ACL-POSTURE-REDIRECT

Method status list:
       Method           State
       mab              Stopped
       dot1x            Authc Success

3k-access#
```

Step 379 Modify the PRA policy for audit only mode.

From the ISE admin interface, go to **Administration → System → Settings** and click the ▸ icon to the left of **Posture** in the left-hand pane to expand the contents of the Posture settings

Click **Reassessments** in the left-hand pane, select **PRA_Any_User** and then click **Edit** from the menu in the right-hand pane.

Change the PRA policy per the following table and then click **Save** to apply changes:

* Configuration Name	**PRA_Any_User**
Configuration Description	(optional)
Use Reassessment Enforcement?	[☑]
Enforcement Type	**continue**
Interval	**60**
Grace Time	**5**
Select Roles	**Any**

Test Posture Assessment and Posture Policies using NAC Web Agent

Exercise Description

- In the previous lab exercises you have configured and tested Client Provisioning services to validate policy-based distribution of the Web Agent to Guest users. Posture Policies have also been configured. This exercise will test the Posture Requirements and Policies for Guest users running the Web Agent.

Exercise Objective

- In this exercise, your goal is to complete the following tasks:
- Login as a Guest user via Central Web Authentication and verify proper execution of the Web Agent posture and remediation process.
- Test AV Posture Policy using Web Agent.
- OPTIONAL: Test Screen Saver Posture Policy using Web Agent.
- Review switch commands to validate correct application of policies.
- Review ISE authentication log monitoring tools to validate correct application of policies.

Lab Exercise Steps

AV POSTURE TESTING

Step 380 Prepare w7pc-corp for Web Agent posture assessment and policy testing as a Guest user.

Step 381 Login as DEMO\employee1

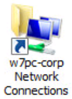
Step 382 From the Lab Tools shortcut on the Windows desktop, run the **Delete_ClamWin_AV_Updates** script to remove the AV client's signature definitions.

Step 383 Run the **RemoveScreenSaver** script under Lab Tools to revert the screen saver settings to non-compliant values. Click **Yes** and then **OK** to accept and acknowledge the registry changes, and then close the Lab Tools window.

Step 384 Disable AnyConnect NAM and Windows native 802.1X on w7pc-corp's wired interface:

Step 385 Double-click on short-cut w7pc-corp Network Connections on the desktop.

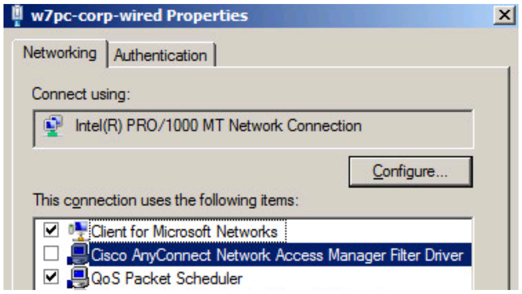
Step 386 Right-click on the connection w7pc-corp-wired and select **properties** from the drop-down menu. When UAC prompted, enter admin / ISEisC00L to continue.



Step 387 In tab **<u>Networking</u>**, un-check Cisco AnyConnect Network Access Manager Filter Driver to disable NAM on this interface.

Step 388 In tab **<u>Authentication</u>**, un-check □ Enable IEEE 802.1X authentication

Step 389 Click **OK** when done.



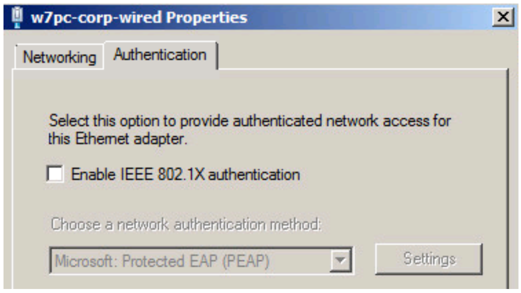
w7pc-corp-wired Properties

Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- □ Cisco AnyConnect Network Access Manager Filter Driver
- ☑ QoS Packet Scheduler



w7pc-corp-wired Properties

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

□ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

Step 390

Step 391 Re-establish new authorization sessions on the switchport

Step 392 Go to the Putty session for the 3k-access

Step 393 Issue the following from the IOS exec mode:

```
clear auth sessions interface g1/0/1
```

Step 394 After ~ 30 seconds, we should see DOT1X and EPM events in the 3k-access terminal session.

Step 395 To verify the switch authorization status at any point during the Guest login and Web Agent posture process, use the following switch commands:

```
show authentication sessions interface GigabitEthernet 1/0/1
```

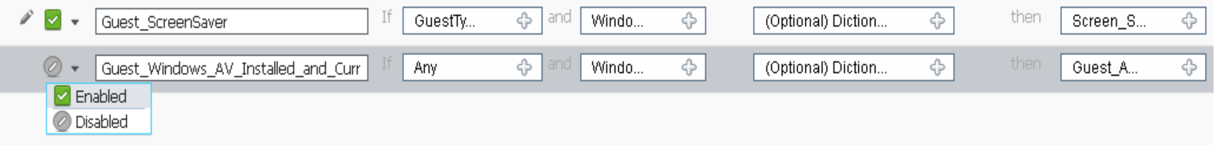
Step 396 Enable the AV and Screen Saver Posture Policies for Guest users.

From the Admin client PC, access the ISE admin interface and go to **Policy > Posture**.

Enable the Guest Windows AV Installed and Current rule.

Enable the Guest Screen Saver rule.

Click **Save** to apply changes.



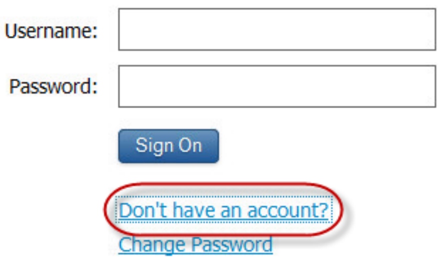
Status	Rule Name		Identity Groups		Operating Systems	Other Conditions		Requirements
☑	Guest_ScreenSaver	If	GuestTy...	and	Windo...	(Optional) Diction...	then	Screen_S...
⊘	Guest_Windows_AV_Installed_and_Curr	If	Any	and	Windo...	(Optional) Diction...	then	Guest_A...

Step 397 Create a new self-service Guest user account.

Step 398 From w7pc-corp, login as user **DEMO\employee1 / ISEisC00L**

Step 399 Launch the Mozilla Firefox Web browser. Type in cisco.com and the page should be redirected to the ISE Web authentication portal.

Step 400 Click the **Don't have an account?** hyperlink from the login portal…



Username:

Password:

…and enter the following values into the form, and then click **Submit**:

Username	**bsmith**
First Name	**Bob**
Last Name	**Smith**
Email Address	(optional)
Phone Number	(optional)
Company	**GOLD**
Person being visited(email)	(optional)
Reason for visit	(optional)

Step 401 Write down the assigned username and password credentials:

Username: ___________________________

Password: ____________________________

To facilitate login, select and copy the password entry, making sure not to include any extra characters.

Click the **OK** button to display the Web authentication login page again.

Step 402 Login as a Guest user and run the Web Agent.

Enter your new Username/Password credentials and click the **Log In** button.

If an AUP was enabled for Web authentication, check the box to *Accept terms and Conditions* and then click **Accept**.

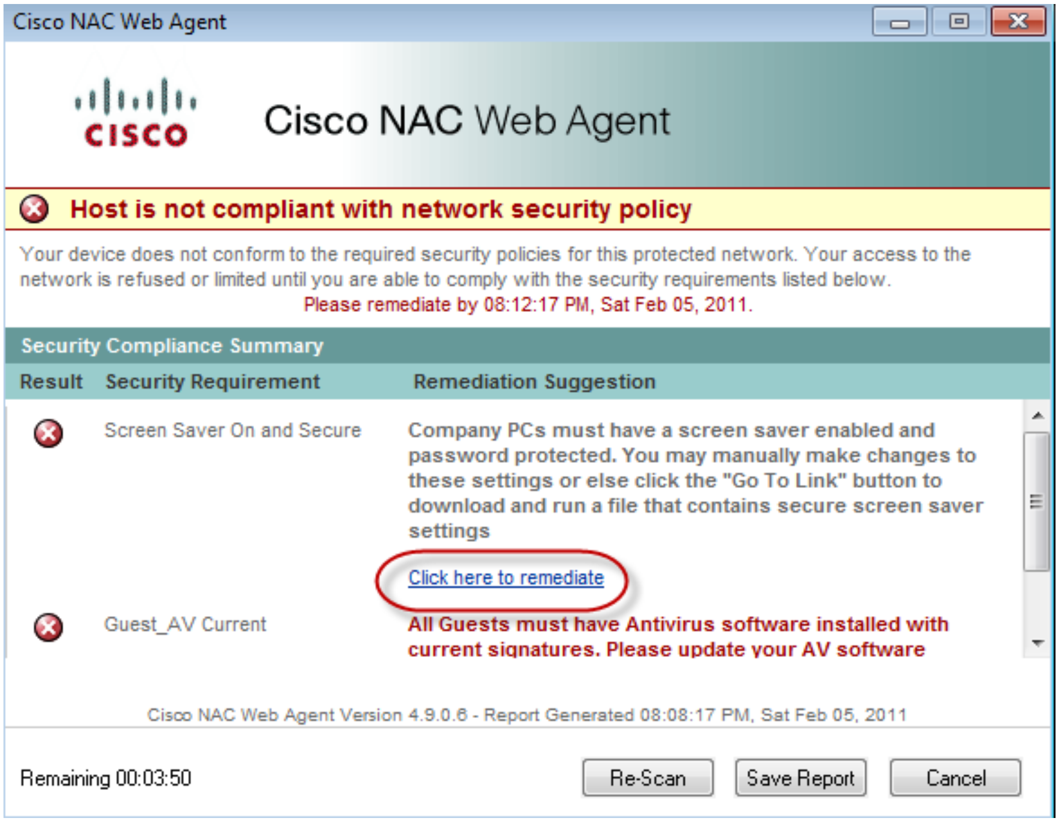
The ISE Agent Downloader page should appear. Click the button **Click to install agent** at the bottom of the page.

Step 403 Accept any certificate warnings if prompted.

Step 404 The Cisco NAC Web Agent window should appear and indicate that posture assessment is being performed.

Step 405 Remediate the non-compliant screen saver policy using the Web Agent.

Step 406 Both Guest user Posture Policies for AV and Screen Saver should fail as shown below:



Host is not compliant with network security policy

Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 08:12:17 PM, Sat Feb 05, 2011.

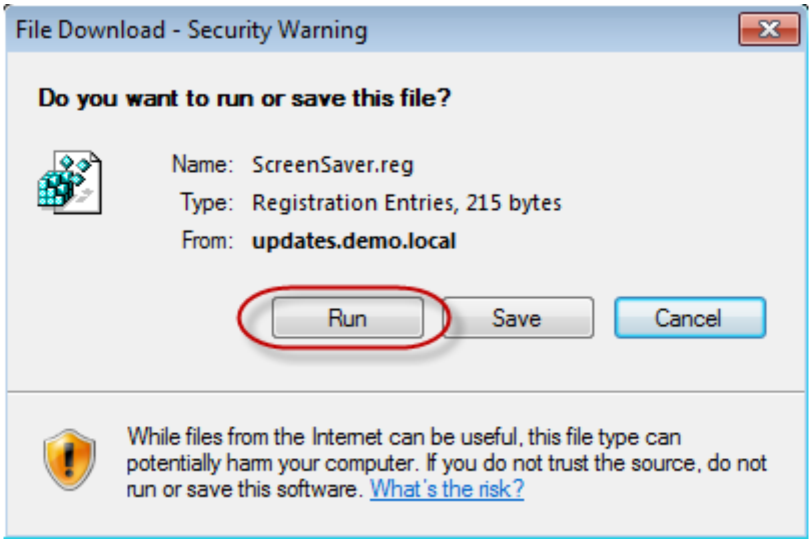
Result	Security Requirement	Remediation Suggestion
☒	Screen Saver On and Secure	Company PCs must have a screen saver enabled and password protected. You may manually make changes to these settings or else click the "Go To Link" button to download and run a file that contains secure screen saver settings Click here to remediate
☒	Guest_AV Current	All Guests must have Antivirus software installed with current signatures. Please update your AV software

Cisco NAC Web Agent Version 4.9.0.6 - Report Generated 08:08:17 PM, Sat Feb 05, 2011

Remaining 00:03:50

Click the link **Click here to remediate** under the failed Screen Saver Requirement suggestions.

A File Download warning will appear. Click **Run**:



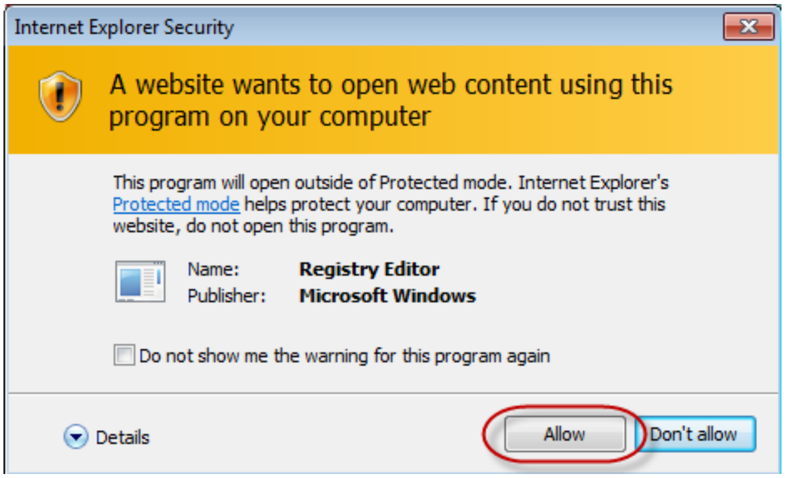
Do you want to run or save this file?

Name: ScreenSaver.reg
Type: Registration Entries, 215 bytes
From: **updates.demo.local**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

Click **Allow** if presented with a browser security warning:

Note: If you see text when selecting remediate, copy the text to notepad and save the file as .reg



Internet Explorer Security

A website wants to open web content using this program on your computer

This program will open outside of Protected mode. Internet Explorer's Protected mode helps protect your computer. If you do not trust this website, do not open this program.

Name: **Registry Editor**
Publisher: **Microsoft Windows**

□ Do not show me the warning for this program again

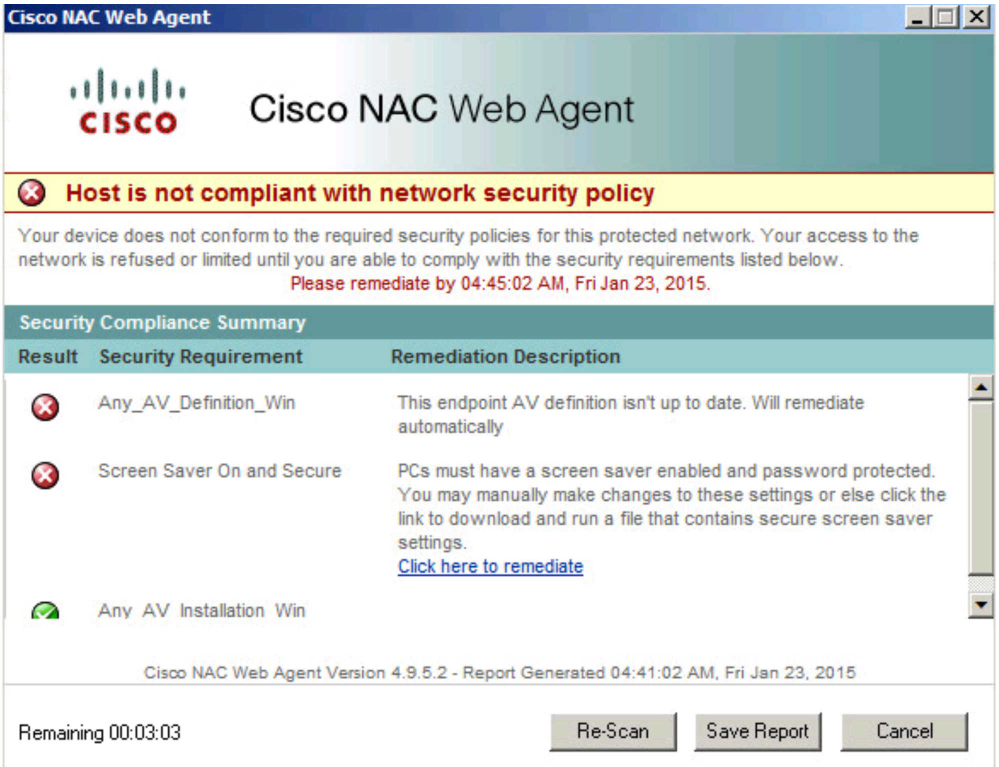
A Registry Editor window will appear asking if you wish to continue with the registry modifications. Click **Yes** to allow the registry to be modified.

Click **OK** to acknowledge the successful registry update.

Note: If excessive time has passed and the Remediation Timer has expired, you can repeat the Web Agent posture assessment process by returning to the ISE Agent Downloader page and re-clicking the button **Click to install agent** at the bottom of the page.

Step 407 Remediate the non-compliant AV policy.

Click the **Re-Scan** button in the Web Agent window to have posture re-assessed based on the recent remediation. The Web Agent should be updated as per the following:



Cisco NAC Web Agent

Cisco NAC Web Agent

Host is not compliant with network security policy

Your device does not conform to the required security policies for this protected network. Your access to the network is refused or limited until you are able to comply with the security requirements listed below.
Please remediate by 04:45:02 AM, Fri Jan 23, 2015.

Security Compliance Summary

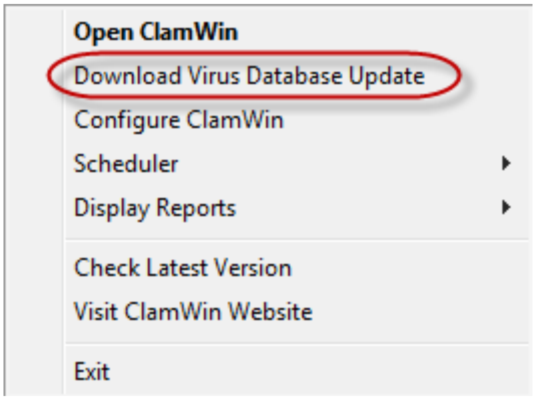
Result	Security Requirement	Remediation Description
☒	Any_AV_Definition_Win	This endpoint AV definition isn't up to date. Will remediate automatically
☒	Screen Saver On and Secure	PCs must have a screen saver enabled and password protected. You may manually make changes to these settings or else click the link to download and run a file that contains secure screen saver settings. Click here to remediate
✓	Any_AV_Installation_Win	

Cisco NAC Web Agent Version 4.9.5.2 - Report Generated 04:41:02 AM, Fri Jan 23, 2015

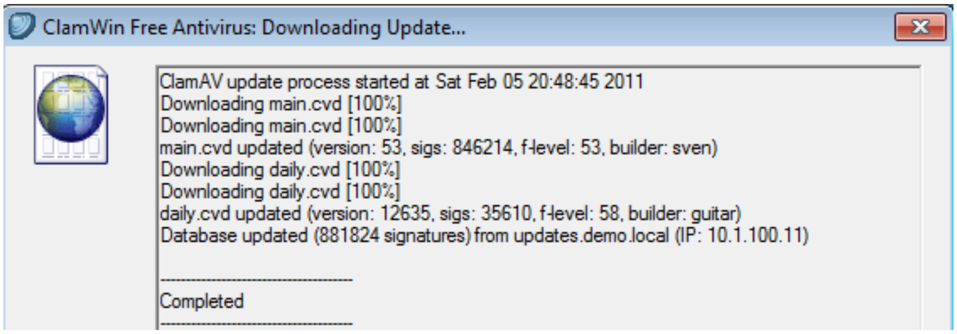
Remaining 00:03:03

Step 408 As a temporal client for use by any Windows PC including non-admin users, the Web Agent does not allow for triggered code execution. Therefore, the Guest user must initiate the remediation.

Right-click on the ClamWin icon in the Windows task tray and click **Download Virus Database Update**:



The ClamWin AV window will open and show the progress of the signature updates. Click **Close** when AV update is complete:



```
ClamAV update process started at Sat Feb 05 20:48:45 2011
Downloading main.cvd [100%]
Downloading main.cvd [100%]
main.cvd updated (version: 53, sigs: 846214, f-level: 53, builder: sven)
Downloading daily.cvd [100%]
Downloading daily.cvd [100%]
daily.cvd updated (version: 12635, sigs: 35610, f-level: 58, builder: guitar)
Database updated (881824 signatures) from updates.demo.local (IP: 10.1.100.11)

--------------------------------
Completed
--------------------------------
```

Note: If the ClamWin update process fails…

Note: The remediation server (updates.demo.local) is configured to download current AV signature files upon start of the p##_**lob-web** VM. If this process fails to complete, then the ClamAV client may fail to download the AV signature files from the remediation server as shown above. If the above process fails, then go to **Policy > Posture** from the ISE admin interface, and change the requirements for the posture rule named *Contractor_Windows_AV_Installed_and_Current* policy from Mandatory to Optional.

Note: To specify posture requirements as Optional, navigate to the Requirements column of the posture policy rule and expand the contents of the requirement. Click the ✓ icon to the right of the requirement name and select **Optional** from the drop-down menu. Repeat for each requirement in the rule.

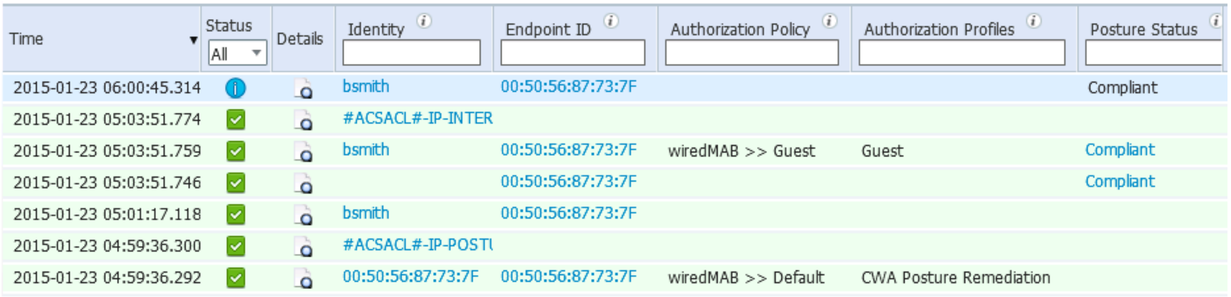
Step 409 Complete the Web Agent posture process.

Click the **Re-Scan** button in the Web Agent window to have posture re-assessed based on the recent remediation. The Web Agent should be updated.

Step 410 The login success screen should auto-close after five seconds per the configured policy.

From the original agent install window, click the browser Home icon, or re-enter www.cisco.com into the URL address field to verify the Guest user now has Internet access.

Step 411 Review the ISE Authentication logs for proper authentication, authorization, and policy assignment.
Step 412 Access the ISE admin interface from the Admin client PC.
Step 413 Go Operations > Authentications.
Step 414 Review the entries associated with w7pc-corp based on IP address. Note the following progression of entries that indicate proper application of the Authorization Policy based on authentication and posture compliance state:
Step 415 Username=<MAC_Address>, Authorization Profile=CWA_Posture_Remdiation
Step 416 Username=<Guest_Username>, Authorization Profile=Guest



Time ▾	Status All ▾	Details	Identity ⓘ	Endpoint ID ⓘ	Authorization Policy ⓘ	Authorization Profiles ⓘ	Posture Status ⓘ
2015-01-23 06:00:45.314	ⓘ	🔍	bsmith	00:50:56:87:73:7F			Compliant
2015-01-23 05:03:51.774	✓	🔍	#ACSACL#-IP-INTER				
2015-01-23 05:03:51.759	✓	🔍	bsmith	00:50:56:87:73:7F	wiredMAB >> Guest	Guest	Compliant
2015-01-23 05:03:51.746	✓	🔍		00:50:56:87:73:7F			Compliant
2015-01-23 05:01:17.118	✓	🔍	bsmith	00:50:56:87:73:7F			
2015-01-23 04:59:36.300	✓	🔍	#ACSACL#-IP-POSTU				
2015-01-23 04:59:36.292	✓	🔍	00:50:56:87:73:7F	00:50:56:87:73:7F	wiredMAB >> Default	CWA Posture Remediation	

Monitor and Report on Posture Services

Exercise Description

ISE includes both monitoring and reporting utilities to validate and troubleshoot Posture Services. This exercise reviews some of these tools.

Exercise Objective

In this exercise, your goal is to complete the following tasks:

- Review ISE Authentications log and verify session details related to Posture Services.
- Review the ISE Dashboard for high-level posture status and statistics.
- Troubleshoot posture events using ISE Diagnostic Tools.
- Run ISE reports for Posture Services.

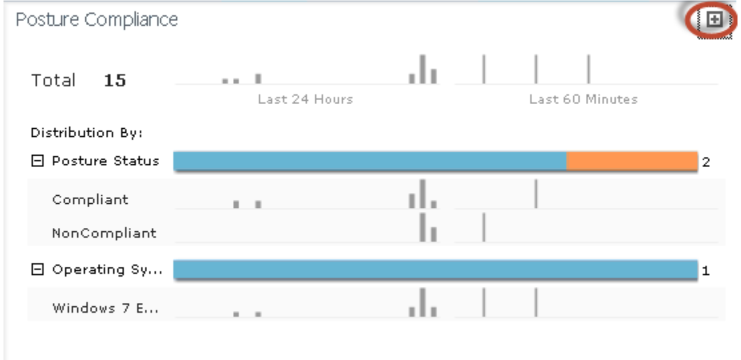
Lab Exercise Steps

Step 417 Review the ISE Authentication logs for proper authentication, authorization, and policy assignment.

From the ISE admin interface, go to **Operations → Authentications**.

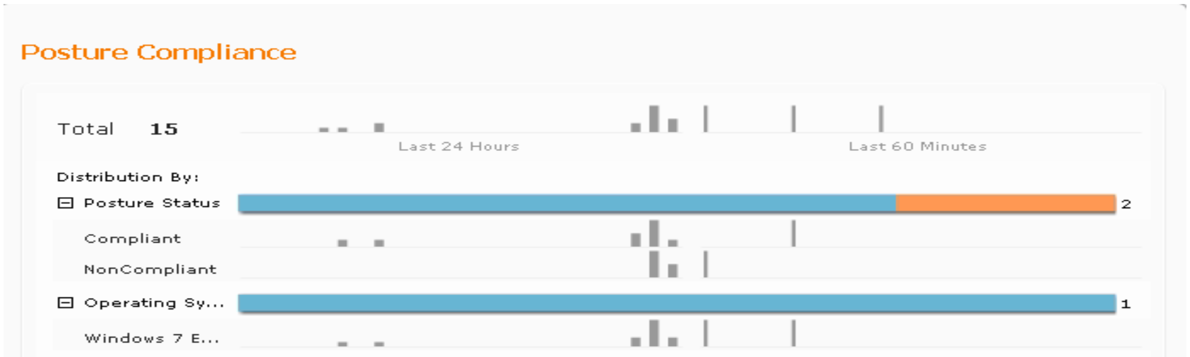
Review the log entries associated with w7pc-corp sessions. Click the **Details** link to see information regarding how the endpoint was authenticated, identity store used, Authorization Profile applied including dACLs and other RADIUS attributes assigned.

From the ISE admin interface, go to **Home** (Dashboard). Review the Posture Compliance dashlet including Compliance pass percentage by hovering over the Posture Status.



Step 418 Click the upper right corner of the dashlet to expand in a new window and hover over the bar to see percentage compliant:

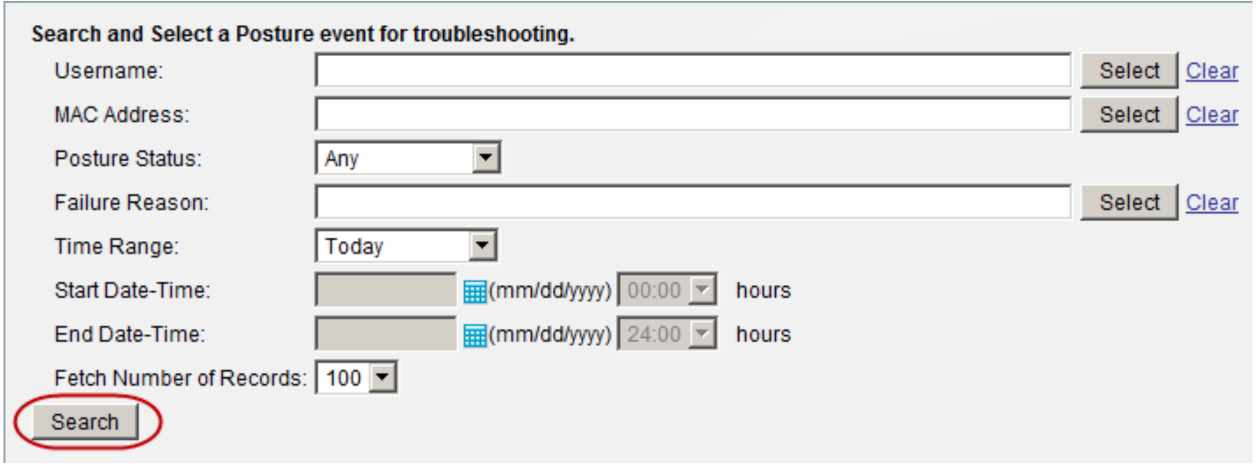
Step 419



Step 420 Click the **OS** and **Posture Status** entries to display additional details.

Step 421 Go to **Operations > Diagnostic Tools**. Click the ▸ icon to the left of **General Tools** in the left-hand pane to expand its contents, and then click **Posture Troubleshooting**. The Search page displays.

Step 422 Click **Search**: (you may have to adjust Time Range)



Search and Select a Posture event for troubleshooting.

Username: Select Clear

MAC Address: Select Clear

Posture Status: Any

Failure Reason: Select Clear

Time Range: Today

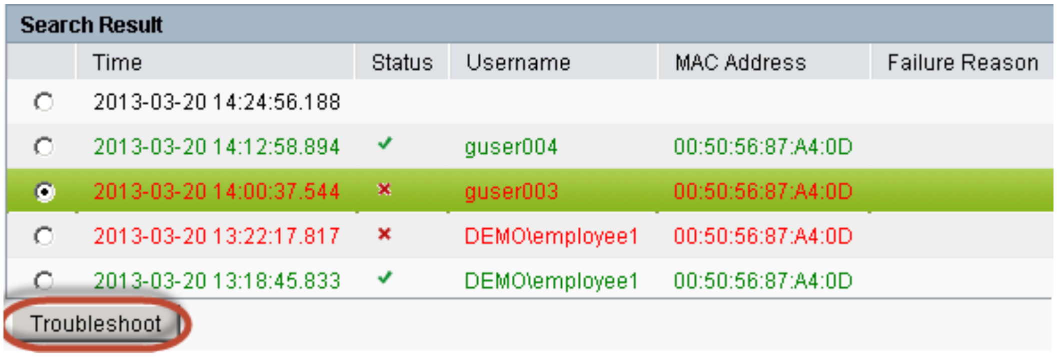
Start Date-Time: (mm/dd/yyyy) 00:00 hours

End Date-Time: (mm/dd/yyyy) 24:00 hours

Fetch Number of Records: 100

Search

Step 423 Select one of the pass/fail (green/red) entries and then click **Troubleshoot** at the bottom of the page:



Search Result

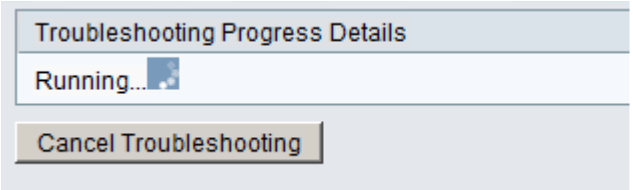
	Time	Status	Username	MAC Address	Failure Reason
○	2013-03-20 14:24:56.188				
○	2013-03-20 14:12:58.894	✓	guser004	00:50:56:87:A4:0D	
●	2013-03-20 14:00:37.544	✗	guser003	00:50:56:87:A4:0D	
○	2013-03-20 13:22:17.817	✗	DEMO\employee1	00:50:56:87:A4:0D	
○	2013-03-20 13:18:45.833	✓	DEMO\employee1	00:50:56:87:A4:0D	

Troubleshoot

Step 424

Step 425

Step 426 A message displays to indicate the status of the request:

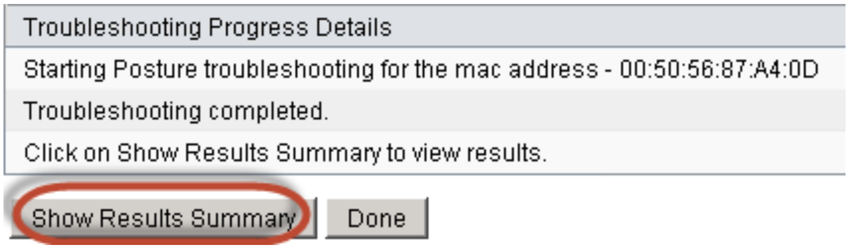


Troubleshooting Progress Details

Running...

Cancel Troubleshooting

Step 427 When processing is complete, a window similar to the following will display:



Troubleshooting Progress Details

Starting Posture troubleshooting for the mac address - 00:50:56:87:A4:0D

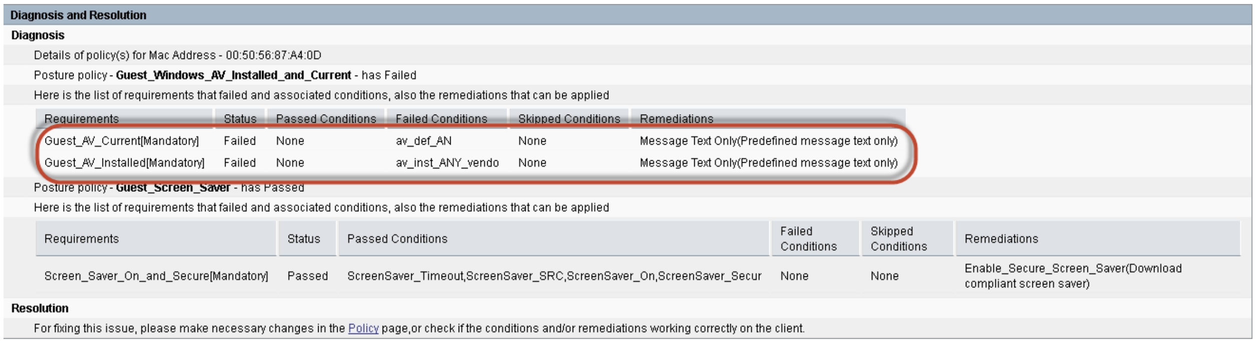
Troubleshooting completed.

Click on Show Results Summary to view results.

Show Results Summary   Done

Step 428 Click **Show Results Summary**. The output displays a summary of all the passed and failed requirements for the posture event along with the condition names and associated remediation actions:

Step 429



Diagnosis and Resolution

Diagnosis

Details of policy(s) for Mac Address - 00:50:56:87:A4:0D

Posture policy - **Guest_Windows_AV_Installed_and_Current** - has Failed

Here is the list of requirements that failed and associated conditions, also the remediations that can be applied

Requirements	Status	Passed Conditions	Failed Conditions	Skipped Conditions	Remediations
Guest_AV_Current[Mandatory]	Failed	None	av_def_AN	None	Message Text Only(Predefined message text only)
Guest_AV_Installed[Mandatory]	Failed	None	av_inst_ANY_vendo	None	Message Text Only(Predefined message text only)

Posture policy - **Guest_Screen_Saver** - has Passed

Here is the list of requirements that failed and associated conditions, also the remediations that can be applied

Requirements	Status	Passed Conditions	Failed Conditions	Skipped Conditions	Remediations
Screen_Saver_On_and_Secure[Mandatory]	Passed	ScreenSaver_Timeout,ScreenSaver_SRC,ScreenSaver_On,ScreenSaver_Secur	None	None	Enable_Secure_Screen_Saver(Download compliant screen saver)

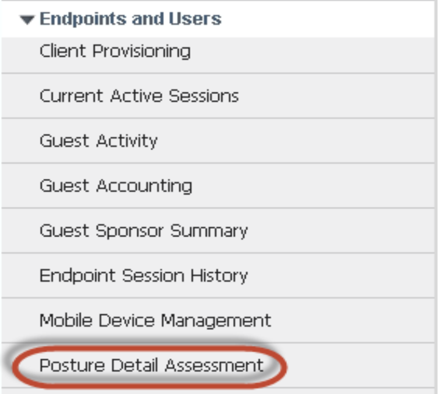
Resolution

For fixing this issue, please make necessary changes in the Policy page,or check if the conditions and/or remediations working correctly on the client.

Step 430

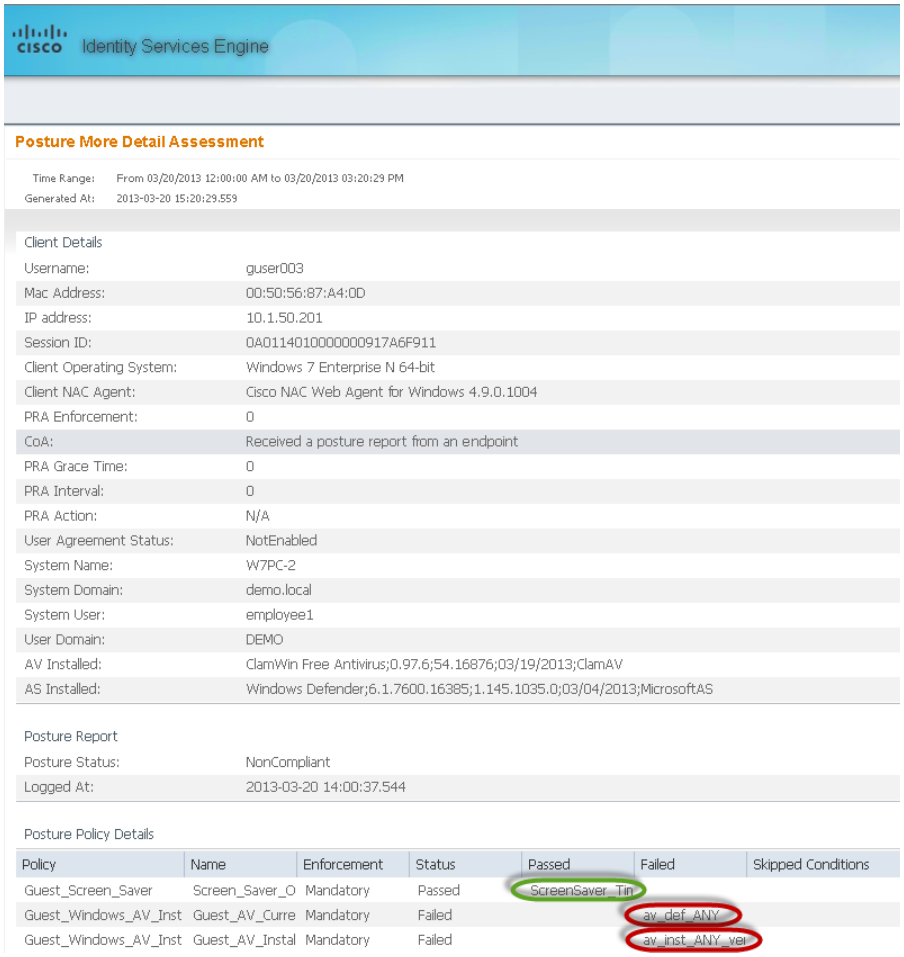
Step 431 Click **Done** to return to the Search page. Optionally enter new search criteria and repeat the steps to troubleshoot passed/failed posture events.

Step 432 Go to Operations → Reports → ISE Reports → Endpoints and Users. Select Posture Detail Assessment from the left-hand pane:



Step 433 Run the **Posture Detail Assessment** report for today and review the contents.

Step 434 Click the Details icon for any Failed (Red) posture entry. Review the overall details for the posture session.



Posture More Detail Assessment

Time Range: From 03/20/2013 12:00:00 AM to 03/20/2013 03:20:29 PM
Generated At: 2013-03-20 15:20:29.559

Client Details

Username:	guser003
Mac Address:	00:50:56:87:A4:0D
IP address:	10.1.50.201
Session ID:	0A0114010000000917A6F911
Client Operating System:	Windows 7 Enterprise N 64-bit
Client NAC Agent:	Cisco NAC Web Agent for Windows 4.9.0.1004
PRA Enforcement:	0
CoA:	Received a posture report from an endpoint
PRA Grace Time:	0
PRA Interval:	0
PRA Action:	N/A
User Agreement Status:	NotEnabled
System Name:	W7PC-2
System Domain:	demo.local
System User:	employee1
User Domain:	DEMO
AV Installed:	ClamWin Free Antivirus;0.97.6;54.16876;03/19/2013;ClamAV
AS Installed:	Windows Defender;6.1.7600.16385;1.145.1035.0;03/04/2013;MicrosoftAS

Posture Report

Posture Status:	NonCompliant
Logged At:	2013-03-20 14:00:37.544

Posture Policy Details

Policy	Name	Enforcement	Status	Passed	Failed	Skipped Conditions
Guest_Screen_Saver	Screen_Saver_O	Mandatory	Passed	ScreenSaver_Tin		
Guest_Windows_AV_Inst	Guest_AV_Curre	Mandatory	Failed		av_def_ANY	
Guest_Windows_AV_Inst	Guest_AV_Instal	Mandatory	Failed		av_inst_ANY_ver	

Review the requirements which passed and those that failed.

APPENDIX A : Configure Windows Wired 802.1X Native Supplicant Manually

The client PC w7pc-corp is pre-configured with wired 802.1X in the lab pods. For references, below are the steps to configure the client PC for 802.1X authentication to simulate an Employee:

Step 435 Enable 802.1X wired services on the client PC:

Click Start and type **Services** Services Right click the Services ICON and **Run as administrator**. Log in as **Admin/ISEisC00L**

Open the **Wired AutoConfig** service from the list:

Change Startup type: to **Automatic** and click **Apply**.

Click **Start** and ensure that Service status = *Started*.

Click **OK** and close the Services window.

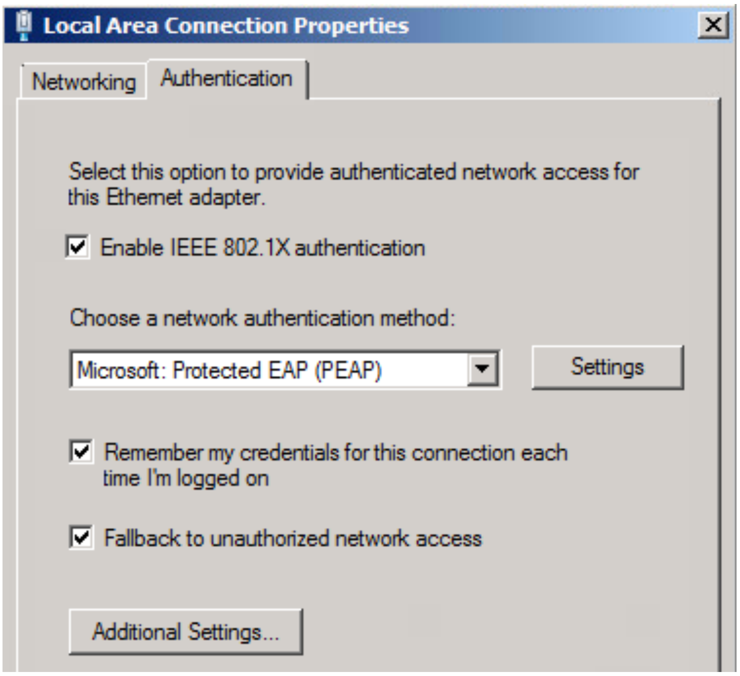
Step 436 Enable 802.1X authentication on the w7pc-corp-wired:

Open the **Network Connections** shortcut from desktop

Right-click on the entry for the **Local Area Connection** and select **Properties**. If prompted by Windows 7 User Account Control (UAC), enter the Domain Administrator credentials **admin / ISEisC00L**.

Select the **Authentication** tab at the top of the Properties window.

Verify that 802.1X authentication is **enabled** (checked) for *Enable IEEE802.1X authentication* as shown below:



Local Area Connection Properties

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

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

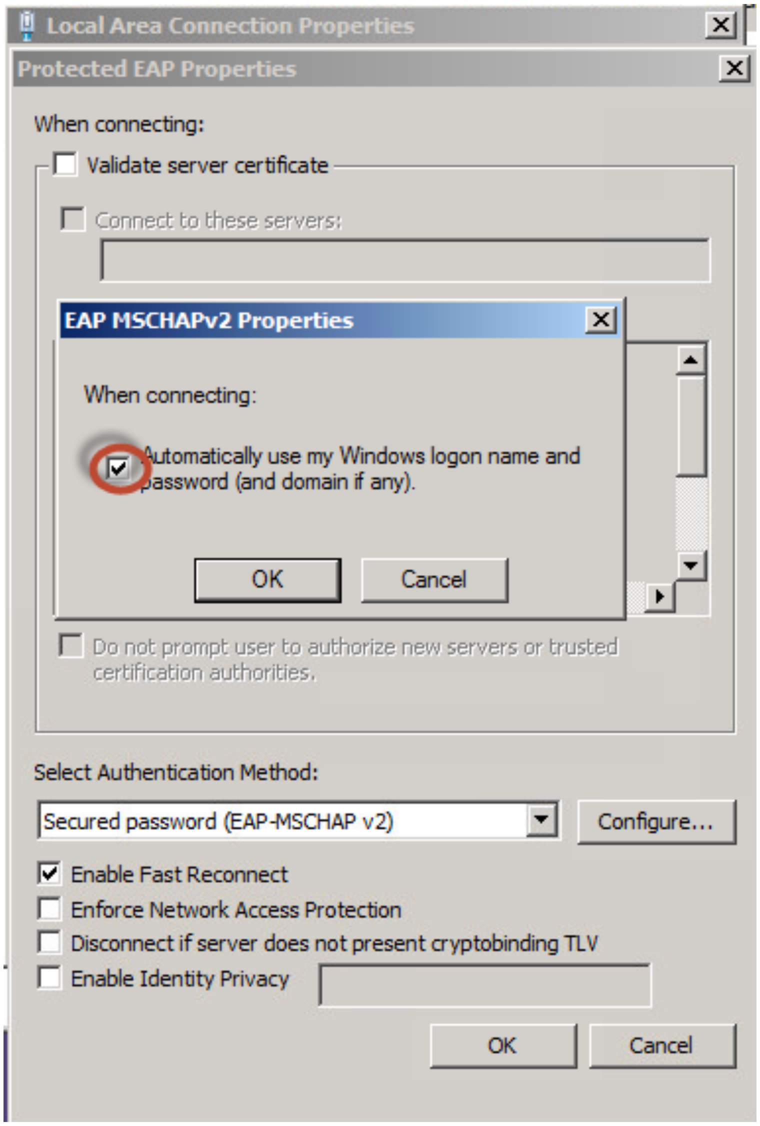
☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

Verify that "Choose a network authentication method" is set to **Microsoft: Protected EAP (PEAP)**.

Check Remember my credentials for this connection each time I'm logged in"

Click **Settings** and under Select Authentication Method: verify that the EAP MSCHAPv2 Click **Configure** and **enable** *Automatically use my Windows login name and password (and domain if any)* as shown:



Local Area Connection Properties

Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

EAP MSCHAPv2 Properties

When connecting:

☑ Automatically use my Windows logon name and password (and domain if any).

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

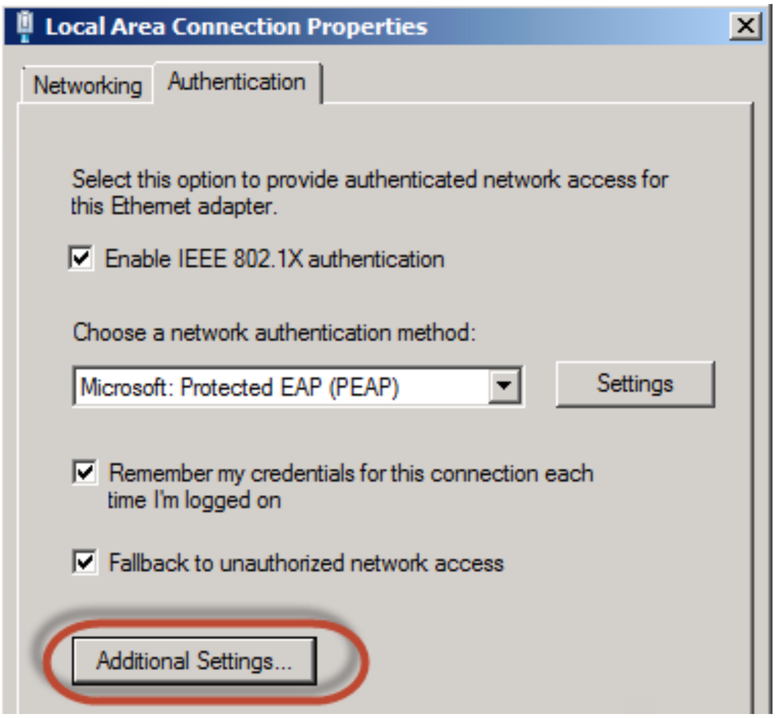
☑ Enable Fast Reconnect

□ Enforce Network Access Protection

□ Disconnect if server does not present cryptobinding TLV

□ Enable Identity Privacy

Click **OK** twice to close the PEAP Properties page and then click **Additional Settings**:



Local Area Connection Properties

Networking | Authentication

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

☑ Enable IEEE 802.1X authentication

Choose a network authentication method:

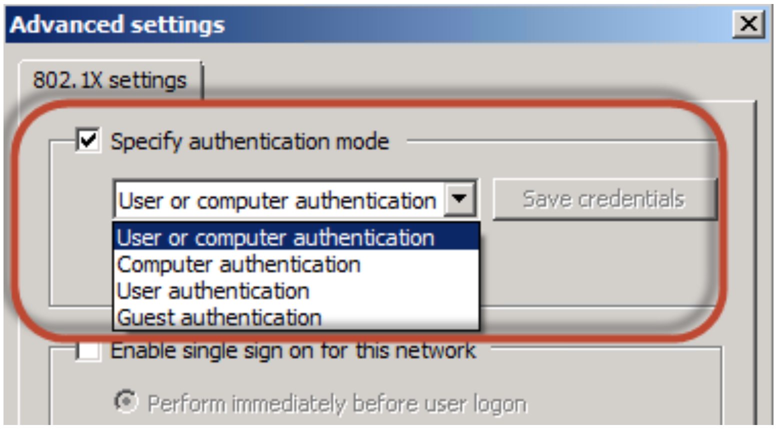
Microsoft: Protected EAP (PEAP) ▾ | Settings

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

☑ Fallback to unauthorized network access

Additional Settings...

Verify that the *Specify authentication mode* setting is **enabled** (checked) and set to **User or computer authentication** as shown:



Advanced settings

802.1X settings

☑ Specify authentication mode

User or computer authentication ▾ | Save credentials

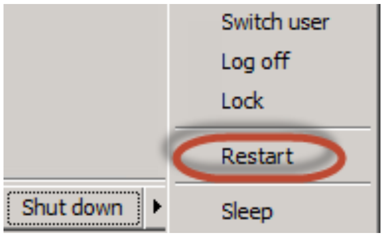
- User or computer authentication
- Computer authentication
- User authentication
- Guest authentication

□ Enable single sign on for this network

○ Perform immediately before user logon

Click **OK** twice to save changes and exit the LAN Properties page.

Exit any open windows and restart the PC by going to **Start** (Start menu) and selecting **Restart**:



Note: **Warning:** **Do NOT select Shutdown or Sleep.** If PC is shut or powered down, then any changes made to client will be lost upon restart and you will need to redo changes made from the start of this lab exercise.

Heading 2

Body text style Body text.

Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style

Heading 2

Body text style Body text.

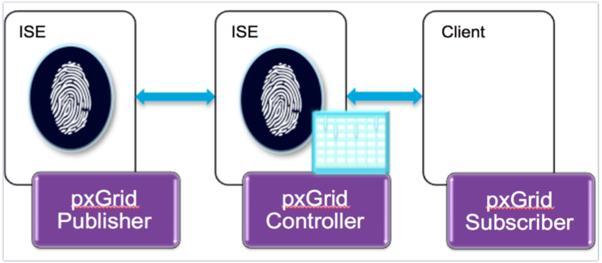
Body text style:

- Bullet_Level 1
- Bullet_Level 1
- Bullet_Level 1
- Bullet_Level 1

  Bullet_Level_1 Text Bullet_Level_1 Text Bullet_Level_1 Text Bullet_Level_1 Text Bullet_Level_1 Text Bullet_Level_1 Text Bullet_Level_1 Text Bullet_Level_1 Text Bullet_Level_1 Text Bullet_Level_1 Text Bullet_Level_1 Text Bullet_Level_1 Text

Heading 3

Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style



(Figure style)

Figure 2. Figure Caption (Note: Numbers update automatically)

Figures should be sized with the following dimensions:

- **Width** - 5.00”
- **Height** - 2.00”

Heading 1

Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style.

Note_Level_1: Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1 Note_Level_1

Sub-heading

- Bullet_Level 1
- Bullet_Level 1
- Bullet_Level 1

Note_Level_1_text: Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text.

Heading 2

Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style

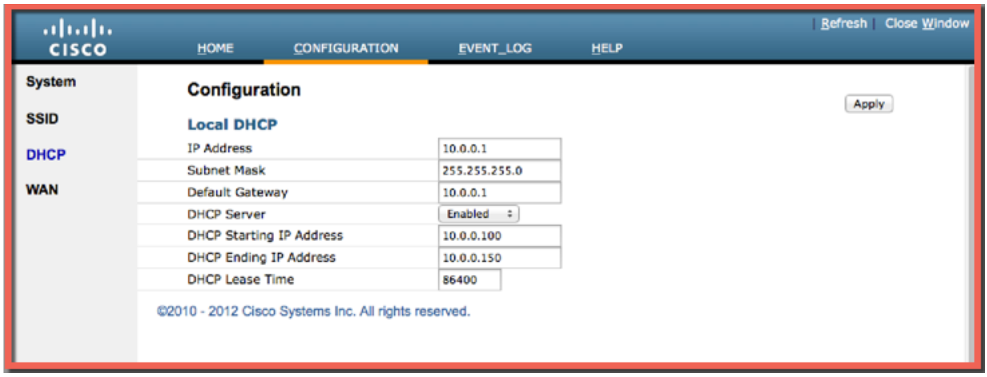
To <task>, complete the following steps (Step_Level 1):

Step 437 Body text style with numbering applied. Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style.

Step 438 Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style.

Step_Level_1_Text style Step_Level_1_Text style Step_Level_1_Text style Step_Level_1_Text style Step_Level_1_Text style Step_Level_1_Text style Step_Level_1_Text style Step_Level_1_Text style Step_Level_1_Text style.

Note_Level_1_text: Steps will increment automatically.



Configuration

Local DHCP

IP Address 10.0.0.1
Subnet Mask 255.255.255.0
Default Gateway 10.0.0.1
DHCP Server Enabled
DHCP Starting IP Address 10.0.0.100
DHCP Ending IP Address 10.0.0.150
DHCP Lease Time 86400

©2010 - 2012 Cisco Systems Inc. All rights reserved.

(Figure)

Figure 3. Figure Caption (Note: Numbers update automatically)

Note_Level_1_text: Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text

Heading 2

Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style Body text style

Note_Level_1: Note_Level 1 Body Text Note_Level 1 Body Text Note_Level 1 Body Text.

Step 1 Step_Level 1 text Step_Level 1 text Step_Level 1 text Step_Level 1 text Step_Level 1 text Step_Level 1 text Step_Level 1 text Step_Level 1 text

```
Cisco-CLI style Cisco-CLI style Cisco-CLI style Cisco-CLI style Cisco-CLI style Cisco-CLI style
Cisco-CLI style Cisco-CLI style Cisco-CLI style Cisco-CLI style Cisco-CLI style Cisco-CLI style

Cisco-CLI style Cisco-CLI style Cisco-CLI style Cisco-CLI style
```

Step 2 Step_Level 1 text Step_Level 1 text Step_Level 1 text Step_Level 1 text Step_Level 1 text Step_Level 1 text Step_Level 1 text Step_Level 1 text

```
Cisco-CLI style
Cisco-CLI style
Cisco-CLI style
Cisco-CLI style
Cisco-CLI style Cisco-CLI style
```

Note_Level_1_text: Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text Note_Level_Text To test the pxGrid client connection, ping the IP address of the Cisco DMZ gateway:

```
Cisco-CLI style
```

Step 3 Step_Level 1 text Step_Level 1 text

```
Cisco-CLI style
```

Step_Level 1_Text Step_Level 1_Text Step_Level 1_Text Step_Level 1_Text Step_Level 1_Text Step_Level 1_Text Step_Level 1_Text Step_Level 1_Text

Step 4 Step_Level 1 text >Step_Level 1 text > Step_Level 1 text Step_Level 1 text > Step_Level 1 text.

Step 5 Step_Level 1 text >Step_Level 1 text > Step_Level 1 text Step_Level 1 text > Step_Level 1 text.

Step 6 Step_Level 1 text >Step_Level 1 text > Step_Level 1 text Step_Level 1 text > Step_Level 1 text.

Heading 3

Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text Body text.

Table 1. Table_Caption (Copy this table structure and insert/delete rows or columns for your need)

Table_Heading	Table_Heading
Table_Text	Table_Text
Table_Text	Table_Text
Table_Text	Table_Text
Table_Text	Table_Text
Table_Text	Table_Text
Table_Text	Table_Text
Table_Text	Table_Text
Table_Text	Table_Text
Table_Text	Table_Text
Table_Text	Table_Text
Table_Text	Table_Text

Note_Level 1: Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1 Note_Level 1

APPENDIX A Title