



Worldwide Sales Enablement

Global Online Lab Delivery
Hosting global hands on field training anytime, anywhere

ISE Posture Services Lab Guide

Developers and Lab Proctors

This lab was created by: Craig Hyps

Lab Overview

This lab is designed to help attendees understand how to deploy Identity Services Engine (ISE) Posture Services. ISE Posture Services provide assessment and policy enforcement for endpoints including optional remediation and traffic control for Windows and MacOS clients. This lab covers the configuration of Posture Services including Client Provisioning, Posture Policy creation, and configuration of access policies based on endpoint assessment results. Attendees will use a Windows client to validate assessment, remediation, and access policies. Lab participants should be able to complete the lab within the allotted lab time of 3 hours.

Lab Exercises

This lab guide includes the following exercises:

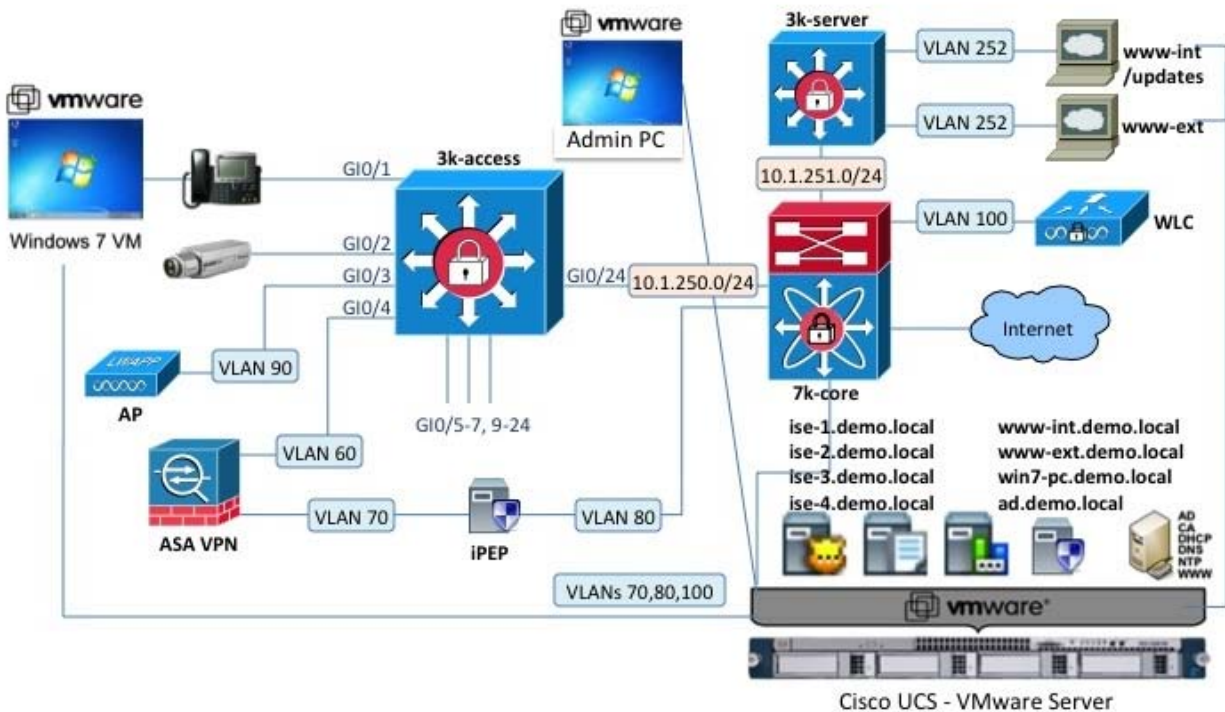
- Lab Exercise 1: Introduction to ISE Posture Services and Configuration Workflow
- Lab Exercise 2: Configure and Deploy Client Provisioning Services
- Lab Exercise 3: Define Authorization Policy for Client Provisioning and Posture Compliance
- Lab Exercise 4: Test and Monitor Client Provisioning Services for Web Agent
- Lab Exercise 5: Test and Monitor Client Provisioning Services for NAC Agent
- Lab Exercise 6: Configure an AV Posture Policy

- Lab Exercise 7: OPTIONAL: Configure a Secure Screen Saver Posture Policy
- Lab Exercise 8: Test Posture Assessment and Posture Policies using NAC Agent
- Lab Exercise 9: Test Posture Assessment and Posture Policies using Web Agent
- Lab Exercise 10: Monitor and Report on Posture Services

Product Overview: ISE

The Cisco Identity Services Engine (ISE) is an identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security and streamline their service operations. Its unique architecture allows enterprises to gather real time contextual information from network, users, and devices to make proactive governance decisions by tying identity back into various network elements including access switches, wireless controllers, VPN gateways, and datacenter switches. Cisco Identity Services Engine is a key component of the Cisco TrustSec™ Solution.

TrustSec Lab Topology



Internal IP addresses

The table that follows lists the internal IP addresses used by the devices in this setup.

| Device | Name/Hostname | IP Address |
|--|------------------------------------|--------------------------|
| Core Switch (Nexus 7k) | 7k-core.demo.local | 10.1.100.1 10.1.250.1 |
| Access Switch (3560X) | 3k-access.demo.local | 10.1.250.2 |
| Data Center Switch (3560X) | 3k-server.demo.local | 10.1.251.2 |
| ISE Appliance | ise-1.demo.local | 10.1.100.21 |
| ISE Appliance | ise-2.demo.local | 10.1.100.22 |
| ISE Appliance | ise-3.demo.local | 10.1.100.23 |
| ISE Appliance | ise-4.demo.local | 10.1.100.24 |
| AD Server (CA/DNS/DHCP) | ad.demo.local | 10.1.100.10 |
| NTP Server | ntp.demo.local | 128.107.220.1 |
| Public Web Server | www-ext.demo.local | 10.1.252.10 |
| Internal Web Server | www-int.demo.local | 10.1.252.20 |
| Admin (Management) Client (also FTP Server) | admin.demo.local ftp.demo.local | 10.1.100.6 |
| Windows 7 Client PC | w in7-pc.demo.local | DHCP (10.1.10.x/24) |

Internal VLANs and IP Subnets

The table that follows lists the internal VLANs and corresponding IP subnets used by the devices in this setup.

| VLAN Number | VLAN Name | IP Subnet | Description |
|-------------|---------------|--------------|--|
| 10 | ACCESS | 10.1.10.0/24 | Network for authenticated users or access network using ACLs |
| 20 | MACHINE | 10.1.20.0/24 | Microsoft machine-authenticated devices (L2 segmentation) |
| 30 | QUARANTINE | 10.1.30.0/24 | Unauthenticated or non-compliant devices (L2 segmentation) |
| 40 | VOICE | 10.1.40.0/24 | Dedicated Voice VLAN |
| 50 | GUEST | 10.1.50.0/24 | Network for authenticated and compliant guest users |
| 60 | VPN | 10.1.60.0/24 | VPN Client VLAN to ASA outside interface |
| 70 | ASA (trusted) | 10.1.70.0/24 | ASA inside network to IPEP untrusted interface |

| | | | |
|-------|----------------|---------------|--|
| 80 | IPEP (trusted) | 10.1.80.0/24 | Dedicated IPEP VLAN for trusted interface |
| 90 | AP | 10.1.90.0/24 | Wireless AP connection for LWAPP tunnel |
| 100 | DATA CENTER | 10.1.100.0/24 | Network services (AAA, AD, DNS, DHCP, NTP, etc.) |
| (250) | | 10.1.250.0/24 | Dedicated interconnect subnet between Core and Access switch. |
| (251) | | 10.1.251.0/24 | Dedicated interconnect subnet between Core and Data Center switch. |
| 252 | WEBSVR | 10.1.252.0/24 | Web Server network |

Note: Dedicated VLANs have been preconfigured for optional access policy assignments based on user identity, profiling, or compliance status. These VLANs include MACHINE, QUARANTINE, and GUEST. This lab will focus on the use of downloadable ACLs (dACLs) rather than VLAN assignment for policy enforcement. By default, all client PC access will remain in the ACCESS VLAN 10 and IP phones will be placed in VOICE VLAN 40.

Accounts and Passwords

The table that follows lists the accounts and passwords used in this lab.

| Access To | Account (username/password) |
|--|--|
| Core Switch (Nexus 7k) | admin / Cisco123 |
| Access Switch (3560X) | admin / cisco123 |
| Data Center Switch (3560X) | admin / cisco123 |
| ASA (VPN gateway) | admin / cisco123 |
| ISE Appliances | admin / default1A |
| AD Server (DNS/DHCP/DHCP) | administrator / cisco123 |
| Web Servers | administrator / cisco123 |
| Admin (Management) Client | admin / cisco123 |
| Windows 7 Client (Local = WIN7-PC) (Domain = DEMO) | WIN7-PC\administrator / cisco123 WIN7-PC\admin / cisco123 DEMO\admin / cisco123 DEMO\employee1 / cisco123 |

Connecting to Lab Devices

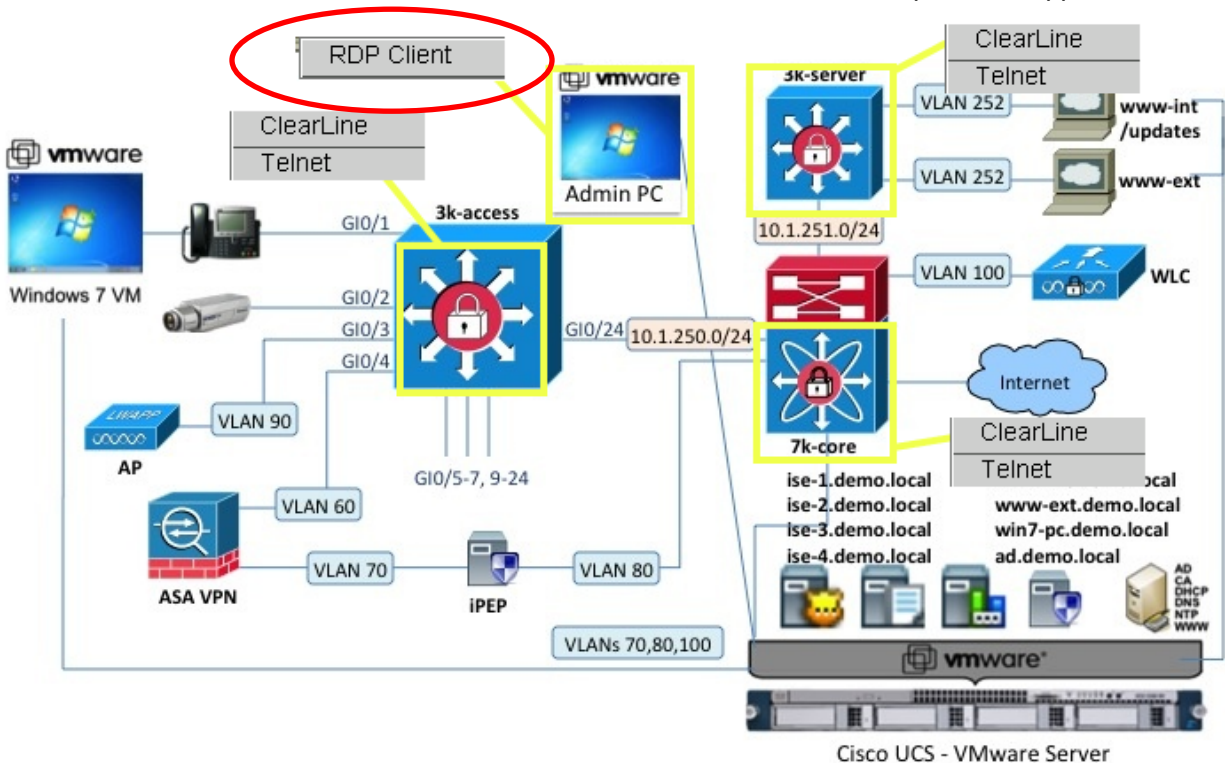
Note: To access the lab, you must first connect to the Admin PC. The Admin PC provides a launching point for access to all the other lab components

Note: Admin PC access is through RDP, therefore you must have an RDP client installed on your computer

Connect to a POD

Step 1 Launch the Remote Desktop application on your system.

- a. In the LabOps student portal, click on the Topology tab
- b. Click on the Admin PC, then click on the RDP Client option that appears:



- c. Clicking on this option should launch your RDP client and connect you to the Admin PC. Log in as **DEMOadmin / cisco123** (Domain = DEMO)
- d. All lab configurations can be performed from the Admin client PC.

Connect to ESX Server Virtual Machines

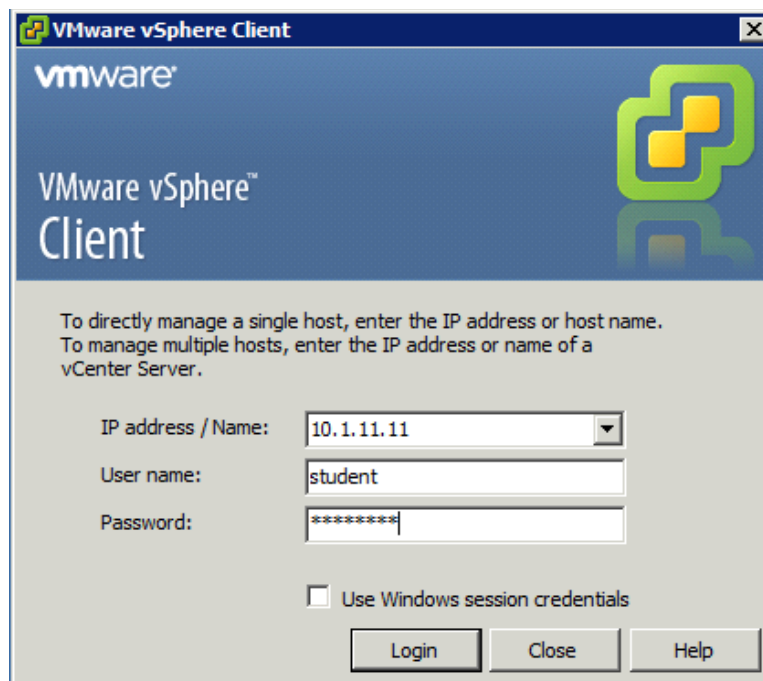
During the lab exercises, you may need to access and manage the computers running as virtual machines.

Step 1 From the Admin client PC, click the **VMware vSphere Client** icon on the desktop 

Step 2 The IP address of your pod's ESX server is 10.1.11.X where X = 10+(your pod number)
e.g. pod 1 = 10.1.11.11, pod 9 = 10.1.11.19, pod 15 = 10.1.11.25, pod 24 = 10.1.11.34

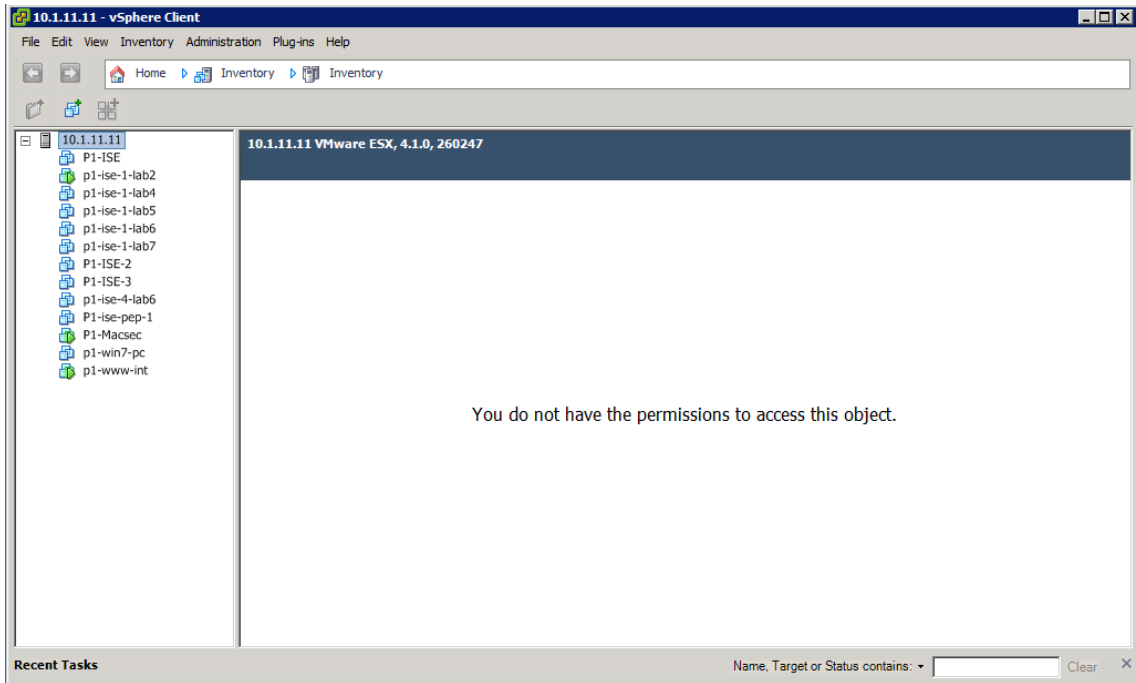
Note: Be careful to only connect to your pod's ESX server. If unsure, contact your class proctor.

Step 3 Enter **student / cisco123** for the username and password:

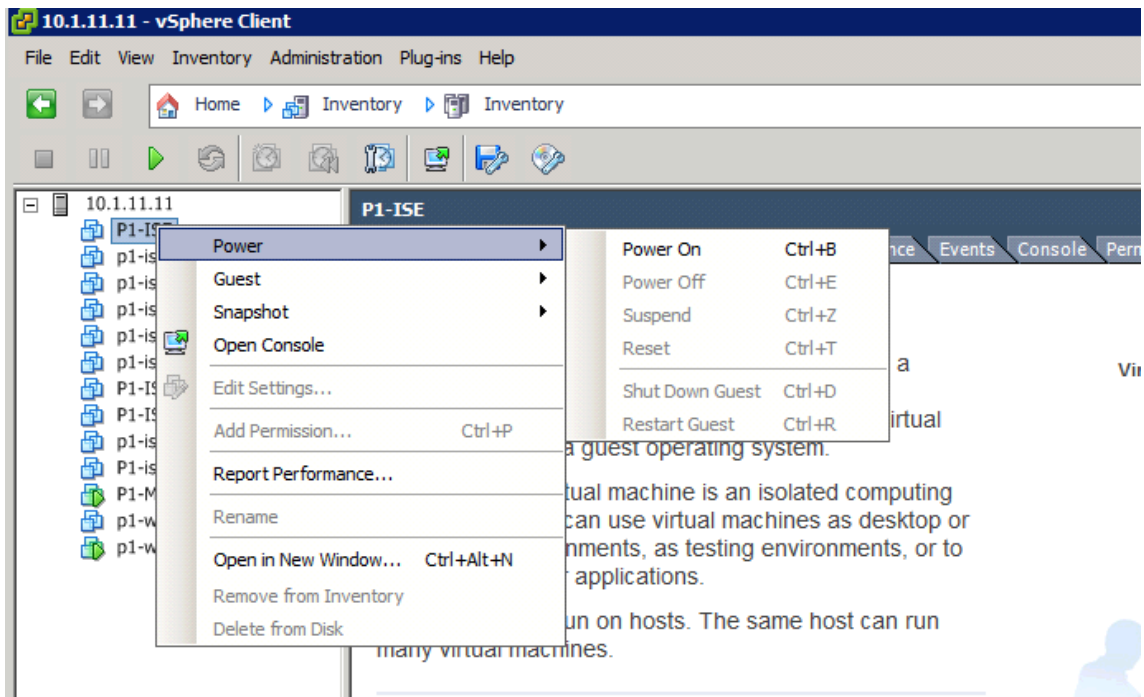


Step 4 Click **Login**.

Step 2 Once logged in, you will see a list of VMs that are available on your ESX server:

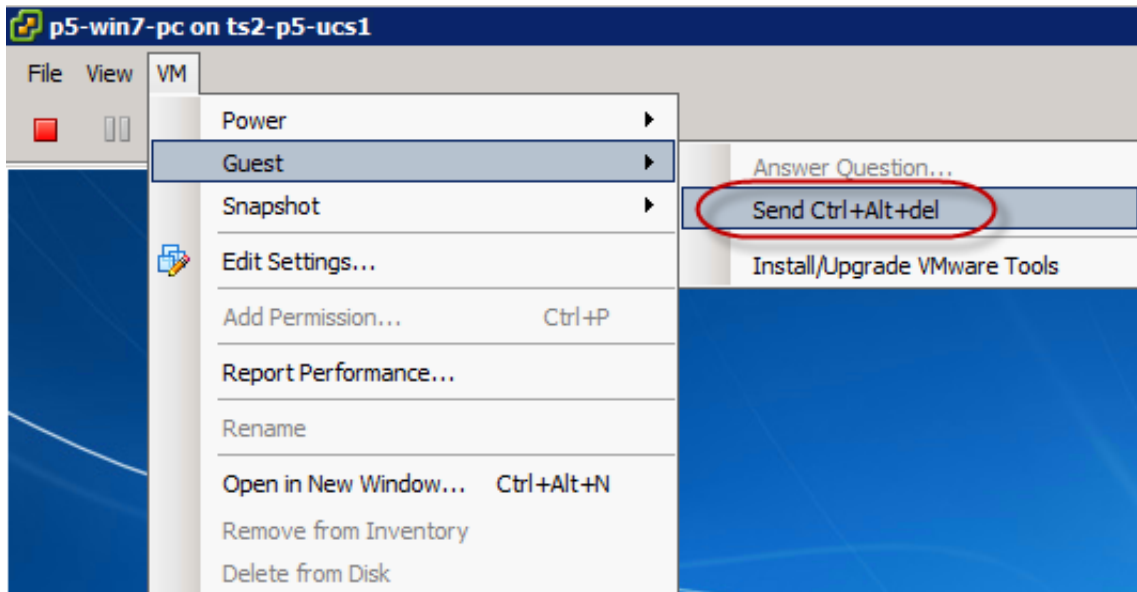


Step 5 You have the ability to power on, power off, or open the console (view) these VMs. To do so, place the mouse cursor over VM name in the left-hand pane and right-click to select one of these options:



Step 6 To access the VM console, select **Open Console** from the drop-down.

Step 7 To login to a Windows VM, select **Guest > Send Ctrl+Alt+del** from the VM Console menu:



Connect to Lab Device Consoles:

Step 1 To access the consoles of the lab switches and ISE servers using SSH:


- a. From the Admin client PC, double-click the desired PuTTY shortcut on the Windows desktop. Example:



You can also use the shortcuts in the Windows Quick Launch toolbar.

- b. If prompted, click **Yes** to cache the server host key and to continue login.
- c. Login using the credentials listed in the Accounts and Passwords table.

Step 2 To access the console for other devices using SSH:

- a. From the Admin client PC, go to **Start** and select  from the Windows Start Menu to open a terminal session using PuTTY.
- b. Refer to the Internal IP Addresses table, and then enter the hostname or IP address of the desired device in the *Host Name (or IP address)*.
- c. Click **Open**.
- d. If prompted, click **Yes** to cache the server host key and to continue login.
- e. Login using the credentials listed in the Accounts and Passwords table

Pre-Lab Setup Instructions

Basic Connectivity Test

To perform a basic connectivity test for the primary lab devices, run the pingtest.bat script from the Windows desktop of the Admin client PC:



Verify that ping succeeds for all devices tested by script.

Note: The ping test may fail for VMs that have not yet completed the boot process.

Rejoin ISE to AD Domain

Step 1 As part of a previous lab, the ISE appliance was joined to the Windows AD domain *demo.local*. To prevent issues after lab pod initialization, the ISE appliance was deliberately removed from the domain using the Leave function. To complete this lab, it will be necessary to rejoin the ISE appliance to the AD domain. Access the ISE admin interface to rejoin the Windows AD domain.

- a. Go to the Admin client PC and launch the Mozilla Firefox web browser. Enter the following URL in the address field:

<https://ise-1.demo.local>

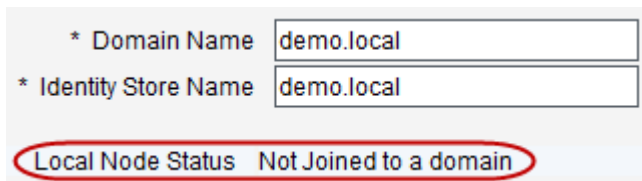
- b. Login with username **admin** and password **default1A**

(Accept/Confirm any browser certificate warnings if present)

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

Step 2 Go to **Administration > Identity Management > External Identity Stores** and select **Active Directory** from the left-hand pane.

Step 3 Verify the Connection Status as *Not Joined to a domain*:



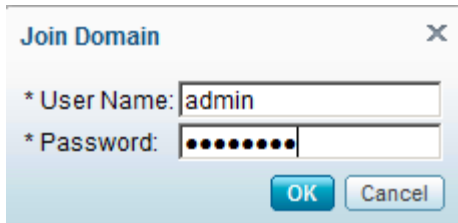
| | |
|-----------------------|------------------------|
| * Domain Name | demo.local |
| * Identity Store Name | demo.local |
| Local Node Status | Not Joined to a domain |

Step 4 Click **Join** at the bottom of the configuration page:

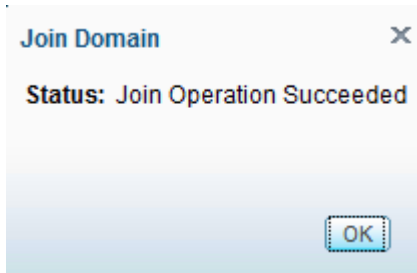


Save Configuration Join Delete Configuration

Step 5 Enter the credentials **admin / cisco123** when prompted to allow the AD operation, and then click **OK**.



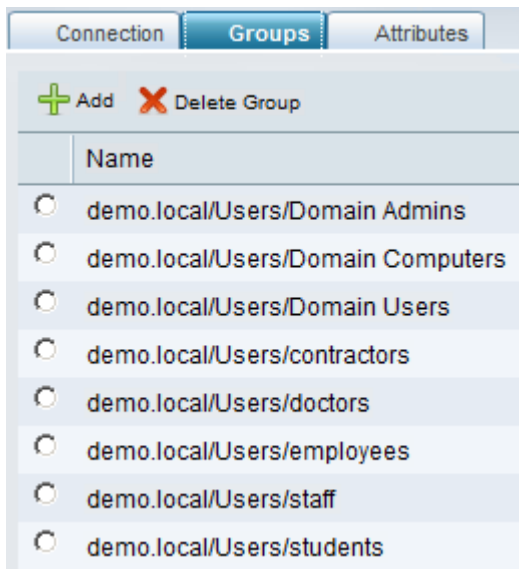
Step 6 After a few moments, a message should appear to indicate that the node has successfully left the domain. Click **OK**.



Step 7 Click **Save Configuration** at the bottom of the page.

Step 8 Select the **Groups** tab at the top of the AD Server configuration page.

Step 9 Since AD groups were retrieved during a join in a previous lab, the original saved configuration should still be present. Verify the following groups are displayed. If not, re-add them and re-save the configuration:



Lab Exercise 1: Introduction to ISE Posture Services and Configuration Workflow

Exercise Description

This exercise reviews the overall workflow for configuring ISE Posture Services including Client Provisioning, Posture Policy, and Authorization Policy for posture compliant access.

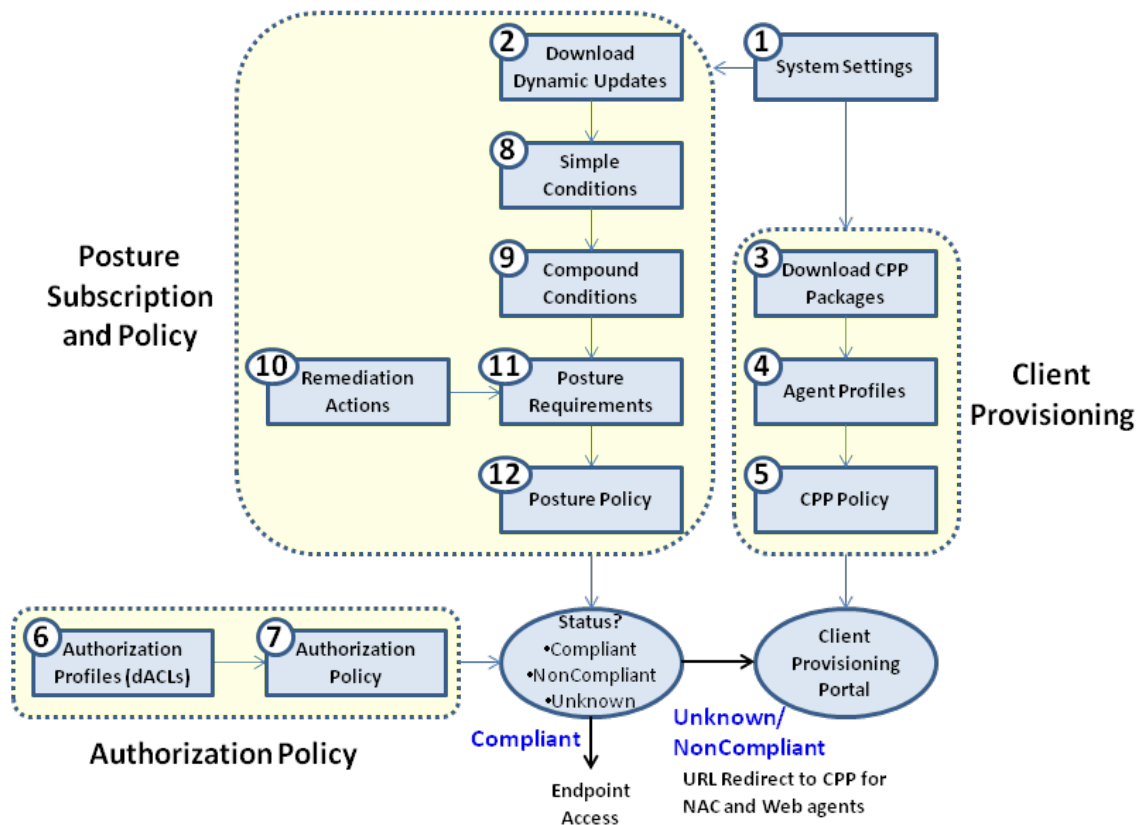
Exercise Objective

In this exercise, your goal is to:

- Understand basic ISE Posture Services and configuration workflow

Lab Exercise Steps

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:

- Client Provisioning
- Posture Subscription and Policy
- 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. NAC Agents are also responsible for facilitating remediation and providing an optional Acceptable Use Policy (AUP) to the end user. Therefore, one of the first steps in the workflow is to retrieve the agent files from the Cisco website and to create policies that determine agent and configuration files downloaded to endpoints based on their attributes, for example, user identity and client OS type.

Posture Policy: 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:

- Unknown (no data collected to determine posture state)
- NonCompliant (posture assessment performed and one or more requirements failed)
- Compliant (compliant with all mandatory requirements)

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

Authorization Policy: 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 4 Understanding Lab Configuration Workflow:

In this lab, you will download both persistent (NAC Agent) and temporal (Web Agent) agent files to ISE and define client provisioning policies that require Employees to download the NAC 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).

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.

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.

Testing will be conducted using both NAC Agents for Employees and Web Agents for Guest Users.

| |
|---|
| <input checked="" type="checkbox"/> End of Exercise: You have successfully completed this exercise. Proceed to next section. |
|---|

Lab Exercise 2: Configure and Deploy Client Provisioning Services

Exercise Description

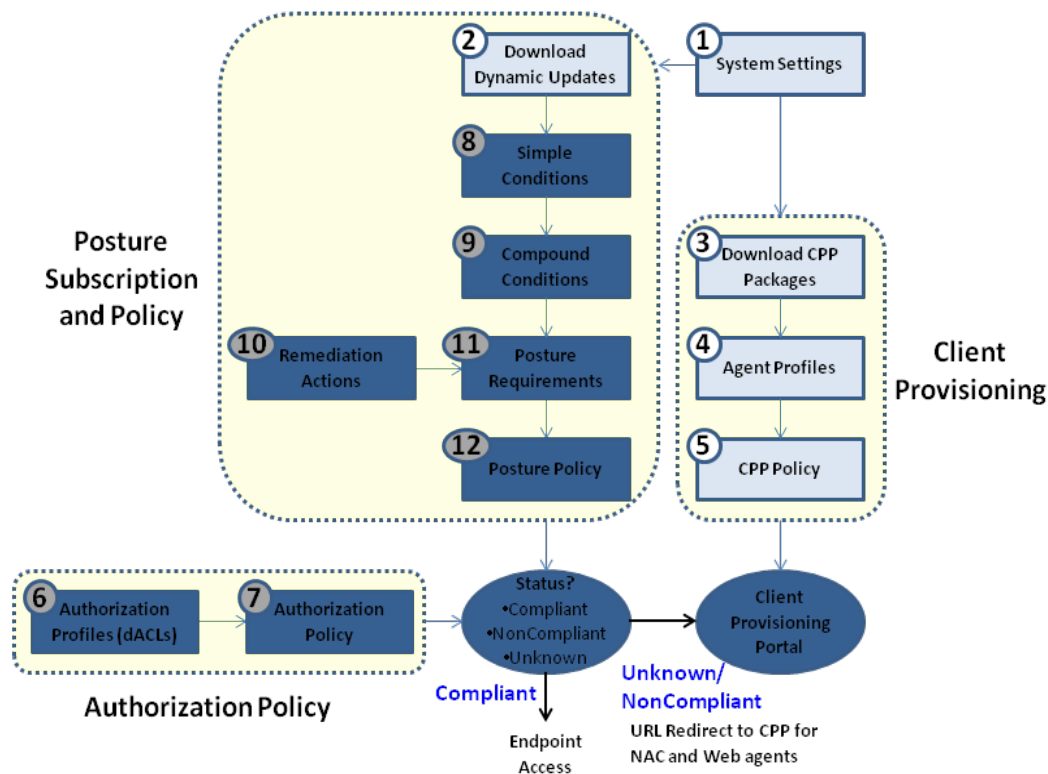
Client Provisioning allows ISE administrators to centrally configure and deploy client software to network users such as posture agents and configuration files. This lab exercise covers how to download client software from Cisco to the ISE appliance and how to configure policies to automatically deploy the NAC Agent and Web Agent. Creation and deployment of a NAC Agent 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 a NAC Agent 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 1 Access the admin interface of the ISE Administrative node.

Go to the Admin client PC and launch the Mozilla Firefox web browser. Enter the following URL in the address field:

<https://ise-1.demo.local>

Step 2 Login with username **admin** and password **default1A**

(Accept/Confirm any browser certificate warnings if present)

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


Step 3 Verify the ISE proxy configuration for software downloads.

Navigate to **Administration > System > Settings** and select **Proxy** from the left-hand pane.

For Reference Only: This page defines the web proxy configuration if required for the ISE Administrative node to download software from the Internet (Cisco).

This lab does not require a proxy for ISE updates. Leave the proxy settings blank.

Step 4 Download pre-built posture checks for AV/AS and Microsoft Windows.

- a. 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 should be empty since no updates have been downloaded yet.
- b. Configure the following values:

| Attribute | Value |
|---|---|
| Web | (o) |
| Update Feed URL: | http://www.perfigo.com/ise/posture-update.xml |
| Proxy Address: | - |
| Proxy Port: | - |
| Automatically check for updates starting from initial delay | [<input checked="" type="checkbox"/>] every 2 hours |

- c. Click the **Save** button.
- d. Click **Update Now** and acknowledge the warning that the updates may take some time to complete. If updates fail, verify the update URL value and that www.perfigo.com resolves to IP Address 10.1.252.21 from the ISE CLI by sending a ping to this domain name.

Note: You may continue with the lab exercise at this time. Please return to this page in approximately fifteen minutes to verify that the Update Information has been populated with date/time of Last Update and version info for Cisco conditions and AV/AS support.

Step 5 Configure general settings for agent behavior:

- a. 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.

- b. **Check** (enable) the checkbox to “Automatically Close Login Success Screen After” and set time to **2** seconds per the following:

| Attribute | Value |
|--|---|
| Remediation Timer | 4 (Minutes) |
| Network Transition Delay | 3 (Seconds) |
| Default Posture Status | Compliant |
| Automatically Close Login Success Screen After | [<input checked="" type="checkbox"/>] |
| | 2 (Seconds) |

- c. Click **Save**.

Note: Values assigned through the agent profile will override these global settings.

Step 6 Configure an Acceptable Use Policy for NAC Agent users.

- Select **Acceptable Use Policy** from the left-hand pane under the **Posture** settings.
- Click **Add** from the right-hand pane.
- Enter the following values for the new AUP policy:

| Attribute | Value |
|---|---|
| Configuration Name | AUP_Any_User |
| Configuration Description | Simple Acceptable Use Policy |
| Show AUP to Agent Users | [<input checked="" type="checkbox"/>] |
| Use URL for AUP message Use file for AUP message | (<input type="radio"/>) (<input type="radio"/>) |
| AUP URL / AUP File | http://updates.demo.local/AUP.html |
| Select Roles | Any |

- d. Click **Submit** when finished.

Note: The AUP for web-authenticated users is set under **Administration > Guest Management > Settings > Guest > Multi-Portal Configurations > (Portal Name)**.

Step 7 Set the location and policy for downloading Client Provisioning updates.

Click **Client Provisioning** from the left-hand pane and verify the following default values are set:

| Attribute | Value |
|---------------------------|---|
| Enable Provisioning | Enable |
| Enable Automatic Download | Disable |
| Update Feed URL | http://www.perfigo.com/ise/provisioning-update.xml |

Step 8 Download Agent files.

- Go to **Policy > Policy Elements > Results** and click the ► icon to left of **Client Provisioning** to expand its contents.
- Select **Resources** in the left-hand pane.

- c. From the right-hand pane, click **Add** then click **Agent Resources from Cisco site** from the drop-down list.
- d. A popup window similar to the following should display.

| <input type="checkbox"/> | Name | Type | Version | Description |
|-------------------------------------|---------------------------|------------------|-----------|---------------------------------------|
| <input checked="" type="checkbox"/> | ComplianceModule 3.4.13.1 | ComplianceModule | 3.4.13.1 | Compliance Module |
| <input checked="" type="checkbox"/> | ComplianceModule 3.4.20.1 | ComplianceModule | 3.4.20.1 | Compliance Module |
| <input type="checkbox"/> | MacOsXAgent 4.9.0.614 | MacOsXAgent | 4.9.0.614 | This is the Mac OS X Agent v4.9.0.614 |
| <input type="checkbox"/> | MacOsXAgent 4.9.0.633 | MacOsXAgent | 4.9.0.633 | This is the Mac OS X Agent v4.9.0.633 |
| <input checked="" type="checkbox"/> | NACAgent 4.9.0.15 | NACAgent | 4.9.0.15 | This is the NAC Agent 4.9.0.15 |
| <input checked="" type="checkbox"/> | NACAgent 4.9.0.27 | NACAgent | 4.9.0.27 | This is the NAC Agent 4.9.0.27 |
| <input checked="" type="checkbox"/> | WebAgent 4.9.0.14 | WebAgent | 4.9.0.14 | This is the Web Agent |
| <input checked="" type="checkbox"/> | WebAgent 4.9.0.6 | WebAgent | 4.9.0.6 | This is the Web Agent |

- e. At a minimum, select the current NAC Agent, Web Agent and Compliance Module (AV/AS support module) from the list and click **Save**.
- f. Wait until the files are downloaded to the ISE appliance.

CLIENT PROVISIONING FILE REFERENCE:

- **NAC Agent:** Persistent posture agent for Windows client PCs
- **Mac OS X Agent:** Persistent posture agent for Mac OS X client PCs
- **Web Agent:** Temporal posture agent for Windows only PCs.
- **Compliance Module:** OPSWAT module that provides updates to current AV/AS vendor support for both the NAC Agent and Mac OS X Agent. Not applicable to Web Agent.
- **Profiles:** Agent configuration files for NAC Agent and Mac OS X Agent. Updates locally installed XML files on client PCs. Not applicable to Web Agent.

Step 9 Create a NAC Agent configuration profile for Windows clients.

From the right-hand pane, click **Add** then select **ISE Posture Agent Profile** from the drop-down list. Enter the following values for the new Agent profile. When finished, click **Submit**


| Attribute | Value | Mode |
|--|------------------|-----------|
| Profile Name | ProfileWindows | |
| VLAN detect interval in secs (VlanDetectInterval): (0-900) | 5 | overwrite |
| Enable VLAN detect without UI? (EnableVlanDetectWithoutUI) | Yes | overwrite |
| Disable Agent exit? (DisableExit) | No | merge |
| Allow CRL checks? (AllowCRLChecks) | Yes | overwrite |
| Accessibility mode? (AccessibilityMode) | No | merge |
| Check signature? (SignatureCheck) | No | overwrite |
| Bypass summary screen? (BypassSummaryScreen) | Yes | merge |
| MAC exception list (ExceptionMACList) | | merge |
| Discovery host (DiscoveryHost) | ise-1.demo.local | overwrite |
| Discovery host editable? (DiscoveryHostEditable) | Yes | overwrite |

| Attribute | Value | Mode |
|---|---------------|-----------|
| Server name rules (ServerNameRules) | | overwrite |
| Generated MA C (GeneratedMA C) | | merge |
| Language info (Locale) | Default | merge |
| Posture report filter (PostureReportFilter) | displayFailed | merge |
| Log file size in MB (LogFileSize) | 5 | merge |
| Detect retries (RetryDetection): Min=0 | 3 | merge |
| Ping ARP (PingArp): (0-2) | 2 | merge |
| Max timeout for ping - in secs (PingMaxTimeout): (1-10) | 1 | merge |
| Sw iss timeout - in secs (Sw issTimeout): Min=1 | 1 | merge |
| Disable L3 Sw iss delay? (DisableL3Sw issDelay) | No | merge |
| Http discovery timeout - in secs (HttpDiscoveryTimeout): Min=0 | 30 | merge |
| Http timeout - in secs (HttpTimeout): Min=0 | 120 | merge |
| Remediation timer - in mins (RemediationTimer): Min=1 | 4 | overwrite |
| Netw ork Transition Delay - in secs (Netw orkTransitionDelay): (2-30) | 3 | overwrite |
| Enable auto close login screen? (EnableAutoClose) | Yes | overwrite |
| Auto close login screen after - in secs (AutoCloseTimer): Min=0 | 2 | overwrite |
| Enable MA C agent iprefresh after vlan change? (EnableAgentIpRefresh) | No | overwrite |
| Dhcp Renew Delay (DhcpRenew Delay): (0-60) | 12 | overwrite |
| Dhcp Release Delay (DhcpReleaseDelay): (0-60) | 1 | overwrite |

Note: The “merge” option updates the current agent profile parameter only if value not already defined; this option will not update parameters with an existing value. The “overwrite” option will update a parameter whether explicitly defined or not.

Step 10 Define Client Provisioning Policy for AD Employees and Guest users.

Go to **Policy > Client Provisioning**. Add two new Client Provisioning rules per the following table values, and then click **Save**:

Note: Click  to the right of any rule entry to insert or duplicate entries.

Note: If multiple versions of same file type (NAC Agent/Web Agent/Compliance module) were downloaded to the Client Provisioning repository, select the most current version available.

| Rule Name | Identity Groups | Operating Systems | Conditions | Results | Is Upgrade Mandatory? |
|-------------------|-----------------|-------------------|---|--|-----------------------|
| Employee_Window s | Any | Window s All | demo.local:ExternalGroups EQUALS demo.local/Users/employees | NA CAgent 4.9.x.x + ProfileWindow s + Compliance 3.4.x.x | [✓] |
| Guest_Window s | Guest | Window s All | - | WebAgent 4.9.x.x | [✓] |

Step 11 Configure web authentication portal to download posture agent per Client Provisioning Policy.

- Navigate to **Administration > Guest Management > Settings** and click the ► icon to left of **Guest** (or double-click **Guest**) to expand its contents.
- Select **Multi-Portal Configurations** from the left-hand pane and then select **DefaultGuestPortal**.

- c. Under the General tab, enable the option to allow guest users to download agents.

| Attribute | Value |
|--|-------|
| Guest users should download the posture client | [✓] |

- d. Optionally set the Acceptable Use Policy for guest users as shown below:

| Attribute | Value |
|--|--|
| Guest users should agree to an acceptable use policy | <input type="checkbox"/> Not Used <input checked="" type="radio"/> First Login and when AUP is changed <input type="checkbox"/> EveryLogin |

- e. Click **Save** when finished.

End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 3: Define Authorization Policy for Client Provisioning and Posture Compliance

Exercise Description

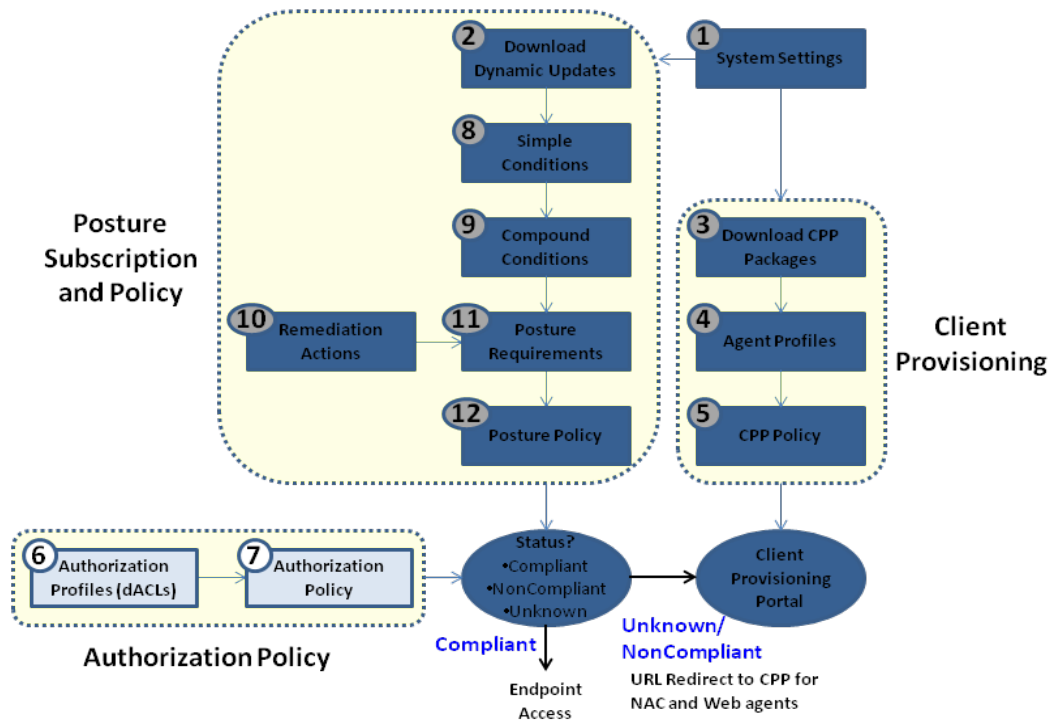
The Authorization Policy sets the types of access and services to be granted to endpoints based on their attributes such as identity, access method, and compliance with posture policies. This exercise includes modifications to an existing Authorization Policy to ensure that endpoints that are not posture 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 1 Access the admin interface of the ISE Administrative node.

- a. Go to the Admin client PC and launch the Mozilla Firefox web browser. Enter the following URL in the address field:

<https://ise-1.demo.local>

- b. Login with username **admin** and password **default1A**
(Accept/Confirm any browser certificate warnings if present)

The ISE Home Dashboard page should display. Navigate the interface using the multi-level menu.

Step 2 Define a dACL that restricts network access for endpoints that are not posture compliant.

- d. Go to **Policy > Policy Elements > Results** and click ► icon to left of **Authorization** (or double-click **Authorization**) to expand its contents.
 - a. Select **Downloadable ACLs** from the left-hand pane.
 - b. Click **Add** from the right-hand pane under DACL Management and enter the following values for the new dACL:

| Attribute | Value |
|--------------|--|
| 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 any eq domain permit icmp any any permit tcp any host 10.1.100.21 eq 8443 |

| Attribute | Value |
|-----------|---|
| | permit tcp any any eq 80 permit tcp any any eq 443 permit tcp any host 10.1.100.21 eq 8905 permit udp any host 10.1.100.21 eq 8905 permit udp any host 10.1.100.21 eq 8906 permit tcp any host 10.1.252.21 eq 80 |

Note: There is currently NO ACL syntax checking for DACL contents so it is imperative that entries be carefully reviewed for errors prior to submitting.


The following describes the purpose of individual ACL entries:

| Downloadable ACL Entry | 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 any eq 80 | Allow http for redirection to Policy Service node |
| permit tcp any any eq 443 | Allow https for redirection to 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 udp any host 10.1.100.21 eq 8906 | Allow Agent discovery and keep-alives |
| permit tcp any host 10.1.252.21 eq 80 | Explicit allow to remediation server |

c. Click **Submit** when completed.

Note: The final access list entry in the POSTURE_REMEDIATION dACL is technically not required since http is already permitted for any destination in a previous entry. Its inclusion here is simply to emphasize the need to make sure that access is allowed to remediation servers. It also highlights the need to include an entry in the URL Redirect ACL to explicitly deny redirection of traffic destined to remediation servers.

Step 3 Define a new URL Redirect ACL on the access switch.

- From the Admin client PC, use the desktop shortcut for the PuTTY SSH client  to launch a terminal session to the **3k-access** switch (10.1.250.2) using the credentials **admin / cisco123** (enabled password **cisco123**).
- Enter configuration mode and add the following IP access list named **ACL-POSTURE-REDIRECT** if not already present:

```

3k-access# conf t
3k-access(config)# ip access-list extended ACL-POSTURE-REDIRECT
3k-access(config-ext-nacl)# deny udp any any eq domain
3k-access(config-ext-nacl)# deny udp any host 10.1.100.21 eq 8905
3k-access(config-ext-nacl)# deny tcp any host 10.1.100.21 eq 8906
3k-access(config-ext-nacl)# deny tcp any host 10.1.100.21 eq 8443
3k-access(config-ext-nacl)# deny tcp any host 10.1.100.21 eq 8905
3k-access(config-ext-nacl)# deny tcp any host 10.1.252.21 eq www
3k-access(config-ext-nacl)# permit ip any any
3k-access(config-ext-nacl)# end
3k-access# wr mem

```

This ACL will be called by the Authorization Profile and work in conjunction with the accompanying dACL applied to the switchport interface.

In the example URL Redirect ACL above, the entries marked “deny” will not redirect the specified packets. These entries include traffic that is specifically destined to the ISE Policy Service node for redirection to Central Web Auth and Client Provisioning services, NAC Agent discovery, and posture assessment. This also includes traffic destined to remediation servers.

- c. Enter the following command at the access switch exec shell prompt to verify the contents of the new ACL:

```
3k-access# show ip access-lists
```

Step 4 Define a new Authorization Profile for 802.1X-authenticated/NAC Agent users named **Posture_Remediation** that leverages both the new dACL for port access control and the URL Redirect ACL for traffic redirection.

- a. Return to the ISE admin interface from the Admin client PC.
- b. Click **Authorization Profiles** from the left-hand pane under **Policy > Policy Elements > Results > Authorization**.
- c. Click **Add** from the right-hand pane and enter the values for the Authorization Profile as shown below.

| Attribute | Value |
|-------------------|--|
| Name | Posture_Remediation |
| Description | Permit access to posture and remediation services; redirect traffic to client provisioning and posture services. |
| Access Type | ACCESS_ACCEPT |
| DA CL Name | [<input checked="" type="checkbox"/>] POSTURE_REMEDIATION |
| Posture Discovery | [<input checked="" type="checkbox"/>] ACL-POSTURE-REDIRECT |

- d. The resultant Attribute Details should appear at the bottom of the page as the following:

```
Access Type = ACCESS_ACCEPT
DA CL = POSTURE_REMEDIATION
cisco:cisco-av-pair=url-redirect-acl=ACL-POSTURE-REDIRECT
cisco:cisco-av-pair=url-redirect =https://ip:8443/guestportal/gatew ay?sessionId=SessionIdValue@action=cpp
```

- e. Click **Submit** to apply your changes.

Step 5 Define a new Authorization Profile for web-Authenticated/Web Agent users named **CWA_Posture_Remediation** that leverages both the new dACL for port access control and the URL Redirect ACL for traffic redirection.

- a. Click **Authorization Profiles** from the left-hand pane under **Policy > Policy Elements > Results > Authorization**.
- b. Click **Add** from the right-hand pane and enter the values for the Authorization Profile as shown below.

| Attribute | Value |
|-------------|---|
| Name | CWA_Posture_Remediation |
| Description | Permit access to posture and remediation services; redirect traffic to central web auth services. |
| Access Type | ACCESS_ACCEPT |

| Attribute | Value |
|--------------------------------|----------------------------|
| DA CL Name | [✓] POSTURE_REMEDIATION |
| Centralized Web Authentication | [✓] ACL-POSTURE-REDIRECT |

c. The resultant Attribute Details should appear at the bottom of the page as the following:

```
Access Type = ACCESS_ACCEPT
DA CL = POSTURE_REMEDIATION
cisco:cisco-av-pair=url-redirect-acl=ACL-POSTURE-REDIRECT
cisco:cisco-av-pair=url-redirect =https://ip:8443/guestportal/gate way?sessionId=SessionIdValue@action=cw a
```

d. Click **Submit** to apply your changes.

Note: The difference between the two profiles is the URL Redirect cisco-av-pair attribute. Users that need to be authenticated using CWA will be initially redirected to the guest portal for web authentication (cwa) and then automatically redirected to the Client Provisioning Portal (cpp) as needed. Users authenticated through 802.1X will be redirected directly to the Client Provisioning Portal.

Step 6 Update the Authorization Policy to support posture compliance.

a. Go to **Policy > Authorization**.

Update the existing Authorization Policy with the following values as highlighted using the



selector at the end of a rule entry to insert or duplicate rules:

| Status | Rule Name | Identity Groups | Other Conditions | Permissions |
|-------------------------------------|--------------------------|-----------------|---|-------------------------|
| <input checked="" type="checkbox"/> | Profiled Cisco IP Phones | Cisco-IP-Phone | - | Cisco_IP_Phones |
| <input checked="" type="checkbox"/> | Domain_Computer | Any | demo.local:ExternalGroups EQUALS demo.local/Users/Domain Computers | AD_Login |
| <input checked="" type="checkbox"/> | Employee | Any | demo.local:ExternalGroups EQUALS demo.local/Users/employees AND Session:PostureStatus EQUALS Compliant | Employee |
| <input checked="" type="checkbox"/> | Employee_PreCompliant | Any | demo.local:ExternalGroups EQUALS demo.local/Users/employees AND Session:PostureStatus NOT EQUALS Compliant | Posture_Remediation |
| <input checked="" type="checkbox"/> | Contractor | Contractor | Session:PostureStatus EQUALS Compliant | Guest |
| <input checked="" type="checkbox"/> | Guest | Guest | Session:PostureStatus EQUALS Compliant | Guest |
| <input checked="" type="checkbox"/> | Default | Any | - | CWA_Posture_Remediation |

b. Click **Save** to apply your changes.

End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 4: Test and Monitor Client Provisioning Services for 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 1 Log into the Windows 7 PC client as **DEMO\employee1 / cisco123**, where *DEMO* is the Windows domain name.

Step 2 Establish a terminal session with the access switch (10.1.250.2) and simulate a new network connection from the Win7 Client PC connected behind a Cisco IP phone on port GigabitEthernet0/1.

- a. From the Admin client PC, use the desktop shortcut for the PuTTY SSH client  to launch a terminal session to the **3k-access** switch (10.1.250.2) using the credentials **admin / cisco123**. If not already in privileged mode, enter enable mode using password **cisco123**.
- b. 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.

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

```
3k-access> en
Password: cisco123
3k-access# conf t
Enter configuration commands, one per line. End with CNTL/Z.
3k-access(config)# int gi0/1
3k-access(config-if)# shut
```

```
3k-access(config-if)# no shut
3k-access(config-if)# end
3k-access#
```

- d. 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 3 After issuing the 'no shut' command, use the following exec command to view the current authorization status of interface GigabitEthernet 0/1:

```
3k-access# show authentication sessions interface gi0/1
```

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 gi0/1
```

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

```
3k-access(config-if)# do sh auth sess int gi0/1
  Interface: GigabitEthernet0/1
    MAC Address: 0050.56b4.0169
    IP Address: 10.1.10.101
    User-Name: 00-50-56-b4-01-69
    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-POSTURE_REMEDIATION-4d816c3a
  URL Redirect ACL: ACL-POSTURE-REDIRECT
  URL Redirect: https://ise-1.demo.local:8443/guestportal/gateway?
                sessionId=0A01640100000090728C037&action=cwa
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A01640100000090728C037
  Acct Session ID: 0x0000000B
    Handle: 0xBA000009

Runnable methods list:
  Method  State
  mab     Authc Success
  dot1x   Not run
```

Note: For this exercise, disregard the authorization status info for the IP phone on VLAN 40 and IP address 10.1.40.x (Domain = VOICE).

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 = **ACL-POSTURE-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.

Step 4 Display the current dACL applied to the interface using the command **show ip access-lists interface GigabitEthernet 0/1**. The output should appear similar to the following:

```
3k-access(config-if)# do sh ip access int gi0/1
  permit udp host 10.1.10.101 any eq domain
  permit icmp host 10.1.10.101 any
  permit tcp host 10.1.10.101 host 10.1.100.21 eq 8443
  permit tcp host 10.1.10.101 any eq www
  permit tcp host 10.1.10.101 any eq 443
  permit tcp host 10.1.10.101 host 10.1.100.21 eq 8905
  permit udp host 10.1.10.101 host 10.1.100.21 eq 8905
  permit udp host 10.1.10.101 host 10.1.100.21 eq 8906
  permit tcp host 10.1.10.101 host 10.1.252.21 eq www
  permit ip host 10.1.40.100 any
3k-access(config-if)#
```

The following provides descriptions for the individual dACL entries applied to the interface (Host 10.1.40.x is the Cisco IP phone and this entry does not apply to the Win7 client with an address in the 10.1.10.0/24 subnet in VLAN 10):

| Downloadable ACL Entry | Description |
|--|---|
| permit udp host 10.1.10.101 any eq domain | Allow DNS resolution |
| permit icmp host 10.1.10.101 any | Allow ICMP for initial policy testing |
| permit tcp host 10.1.10.101 host 10.1.100.21 eq 8443 | Allow access to CWA/ CPP portals |
| permit tcp host 10.1.10.101 any eq www | Allow any http for redirection to CWA/ CPP |
| permit tcp host 10.1.10.101 any eq 443 | Allow any https for redirection to CWA/ CPP |
| permit tcp host 10.1.10.101 host 10.1.100.21 eq 8905 | Allow agent discovery |
| permit udp host 10.1.10.101 host 10.1.100.21 eq 8905 | Allow agent discovery |
| permit udp host 10.1.10.101 host 10.1.100.21 eq 8906 | Allow agent discovery |
| permit tcp host 10.1.10.101 host 10.10.100.11 eq www | Allow access to remediation server |
| permit ip host 10.1.40.100 any | dACL from separate IP Phone authorization |

Step 5 Return to the Win7 PC client and login as a guest user.

- From the Win7 client, launch a web browser. The page should be redirected to the URL specified in the URL Redirect output and display the ISE web authentication portal.
- Click the **Self Service** button from the login portal and enter the following values into the form, and then click **Submit**:

| Attribute | Value |
|-----------------|------------------------------|
| First Name | Guest |
| Last Name | User |
| Email Address | guestuser@company.com |
| Phone Number | (optional) |
| Company | Company ABC |
| Optional Data 1 | Web Agent test |
| Optional Data 2 | (enter optional comments) |
| Timezone | UTC |

- c. 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.

- d. The web authentication login page again displays. Enter your new Username/Password credentials and click the **Log In** button.
- e. If an AUP was enabled for web authentication, **check the box** to *Accept terms and conditions* and then click **Accept**.
- f. The Agent download page should appear. Click the button **Click to install agent**.
- g. The ISE certificate is self-signed and has not been installed on the client PC. 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.
- h. 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:



- i. Click **Continue**. A successful login notice will appear. Since we have previously enabled the global setting to “Automatically close login success screen after” with a value of 2 seconds, the window should automatically close.
- j. The original browser window should display a message at the bottom of page “Cisco Agent finished checking your system.”

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.

- k. When finished, close the web browser session.

Step 6 Verify the session status on the switchport for Guest authorization.

- a. Return to the terminal session on the access switch.
- b. Repeat the **show authentication sessions** and the **show ip access-lists** output for interface GigabitEthernet0/1. The output should appear similar to that shown below:

```

3k-access(config-if)# do sh auth sess int gi0/1
    Interface: GigabitEthernet0/1
    MAC Address: 0050.56b4.0169
    IP Address: 10.1.10.101
    User-Name: guser601
    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-INTERNET_ONLY-4d4337d4
    Session timeout: 2460s (server), Remaining: 1547s
    Timeout action: Terminate
    Idle timeout: N/A
    Common Session ID: 0A016401000000090728C037
    Acct Session ID: 0x0000000B
    Handle: 0xBA000009

Runnable methods list:
    Method State
    mab Authc Success
    dot1x Not run

3k-access(config-if)# do sh ip access-list int gi0/1
    permit udp host 10.1.10.101 any eq domain
    permit icmp host 10.1.10.101 any
    permit tcp host 10.1.10.101 host 10.1.100.21 eq 8443
    deny ip host 10.1.10.101 10.1.0.0 0.0.255.255
    permit ip host 10.1.10.101 any
    permit ip host 10.1.40.100 any

```

- c. Note that URL redirection is no longer applied and that the dACL (ACS ACL) named **INTERNET_ONLY** is applied to the interface.
- d. For reference, the following table provides descriptions for the dACL entries:

| Downloadable ACL Entry | Description |
|--|--|
| permit udp host 10.1.10.101 any eq domain | Allow DNS resolution |
| permit icmp host 10.1.10.101 any | Allow ICMP for initial policy testing |
| permit tcp host 10.1.10.101 host 10.1.100.21 eq 8443 | Allow access to CWA/ CPP portals |
| deny ip host 10.1.10.101 10.1.0.0 0.0.255.255 | Deny access to all other internal lab networks |
| permit ip host 10.1.10.101 any | Permit access to all other external networks |
| permit ip host 10.1.40.100 any | dACL from separate IP Phone authorization |

Step 7 Verify the authentication/authorization phases of the Central Web Auth and Client Provisioning session from the ISE admin interface.

- a. From the Admin client PC, access the admin interface of the ISE Administrative node (**admin / default1A**).
- b. Go to **Monitor > 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.
- c. 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:
 1. Successful MAB authentication of the MAC Address (username 00:50:56:B4:01:69 in example) and Authorization Profile named CWA_Posture_Remediation applied
 2. dACL named POSTURE_REMEDIATION has been successfully downloaded.
 3. Dynamic Authorization (CoA) succeeded for session.
 4. Successful CWA authentication for Guest User (username *guser601* in example) and Authorization Profile named Guest applied.
 5. dACL named INTERNET_ONLY has been successfully downloaded.

| Time | Status | Details | Username | Calling Station ID | IP Address |
|------|------------------------|---------|--|--------------------|-------------|
| 5 | 02, 11 09:21:59.546 AM | ✓ | #ACSACL#-IP-INTERNET_ONLY-4d4337d4 | | |
| 4 | 02, 11 09:21:59.508 AM | ✓ | guser601 | 00:50:56:B4:01:69 | 10.1.10.101 |
| 3 | 02, 11 09:21:57.115 AM | ✓ | | | |
| 2 | 02, 11 09:20:22.884 AM | ✓ | #ACSACL#-IP-POSTURE_REMEDIATION-4d45ac82 | | |
| 1 | 02, 11 09:20:22.874 AM | ✓ | 00:50:56:B4:01:69 | 00:50:56:B4:01:69 | 10.1.10.101 |

| Session ID | Server | NAS Port ID | Event | Failure Reason | Authorization Profiles |
|------------|---------------------|-------------|-------------------------|-------------------------------|-------------------------|
| | ise-pap-1 | | DACL Download Succeeded | | |
| 5 | ise-pap-1 | | DACL Download Succeeded | | |
| 4 | 640100000090728C037 | ise-pap-1 | FastEthernet0/1 | Authentication succeeded | Guest |
| 3 | 640100000090728C037 | ise-pap-1 | | Dynamic Authorization success | |
| 2 | ise-pap-1 | | DACL Download Succeeded | | |
| 1 | 640100000090728C037 | ise-pap-1 | FastEthernet0/1 | Authentication succeeded | CWA_Posture_Remediation |

End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 5: Test and Monitor Client Provisioning Services for NAC 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 NAC Agent will be tested and monitored in detail in this exercise. In addition to NAC 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 NAC Agent provisioning.
- Review ISE and switch logs to validate proper operation and application of the Authorization Policy.

Lab Exercise Steps

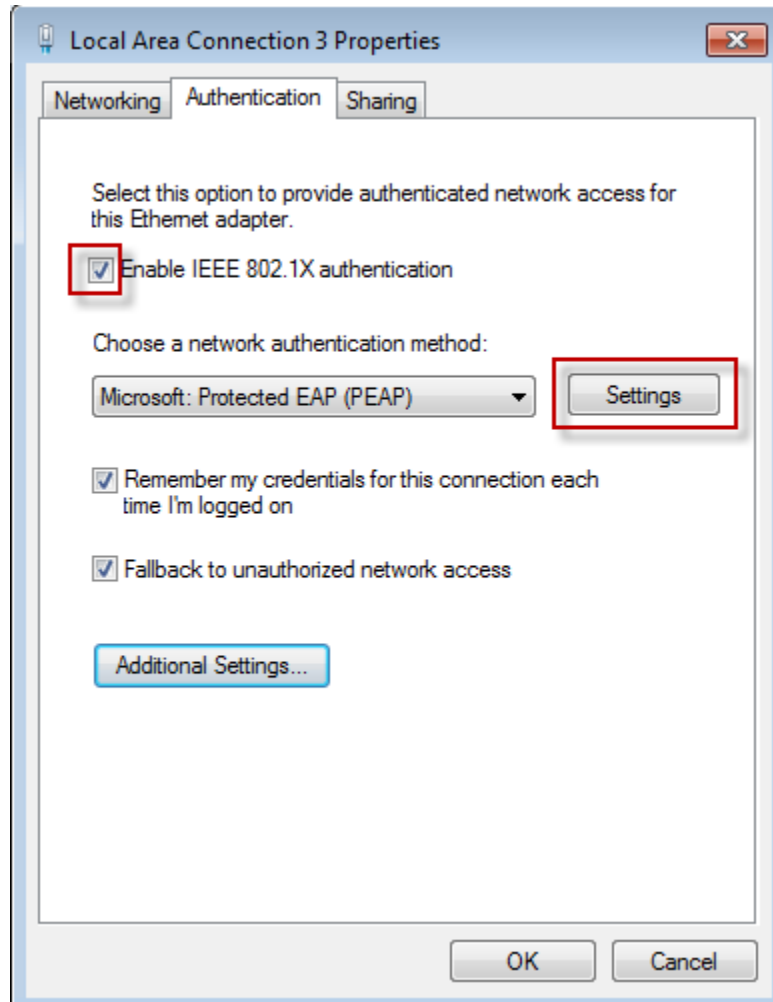
Step 1 Establish a terminal session with the access switch (10.1.250.2).

Step 2 Log into the Windows 7 PC client as **DEMO\employee1 / cisco123**, where *DEMO* is the Windows domain name.

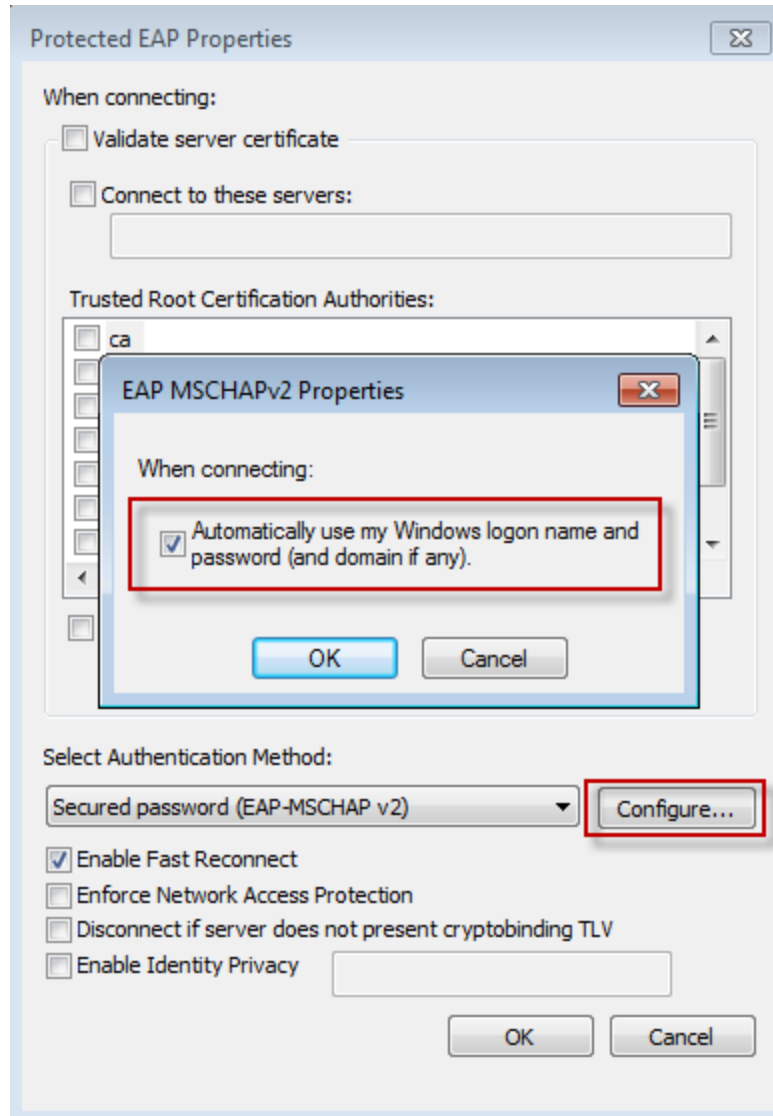
Step 3 Configure the Win7-PC client for 802.1X authentication to simulate an Employee:

- a. Enable 802.1X wired services on the Win7-PC client:
 - i. Launch the **Services** shortcut from the Windows 7 desktop.
 - ii. Open the **Wired AutoConfig** service from the list:
 - iii. Change Startup type: to **Automatic** and click **Apply**.
 - iv. Click **Start** and ensure that Service status = *Started*.
 - v. Click **OK** and close the Services window.
- b. Enable 802.1X authentication on the Win7-PC client:
 - i. Open the **Lab Tools** shortcut from the Windows desktop.
 - ii. Open the **Network Connections** shortcut from the Lab Tools window.
 - iii. 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 / cisco123**.
 - iv. Select the **Authentication** tab at the top of the Properties window.

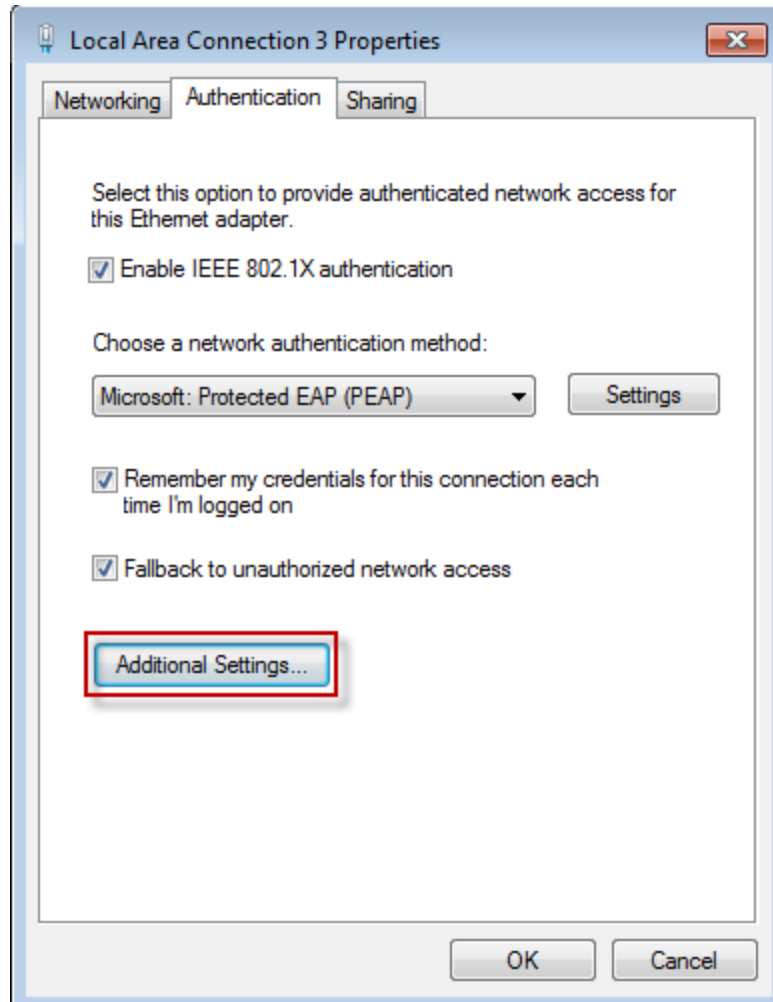
- v. Verify that 802.1X authentication is **enabled** (checked) for *Enable IEEE802.1X authentication* as shown below:



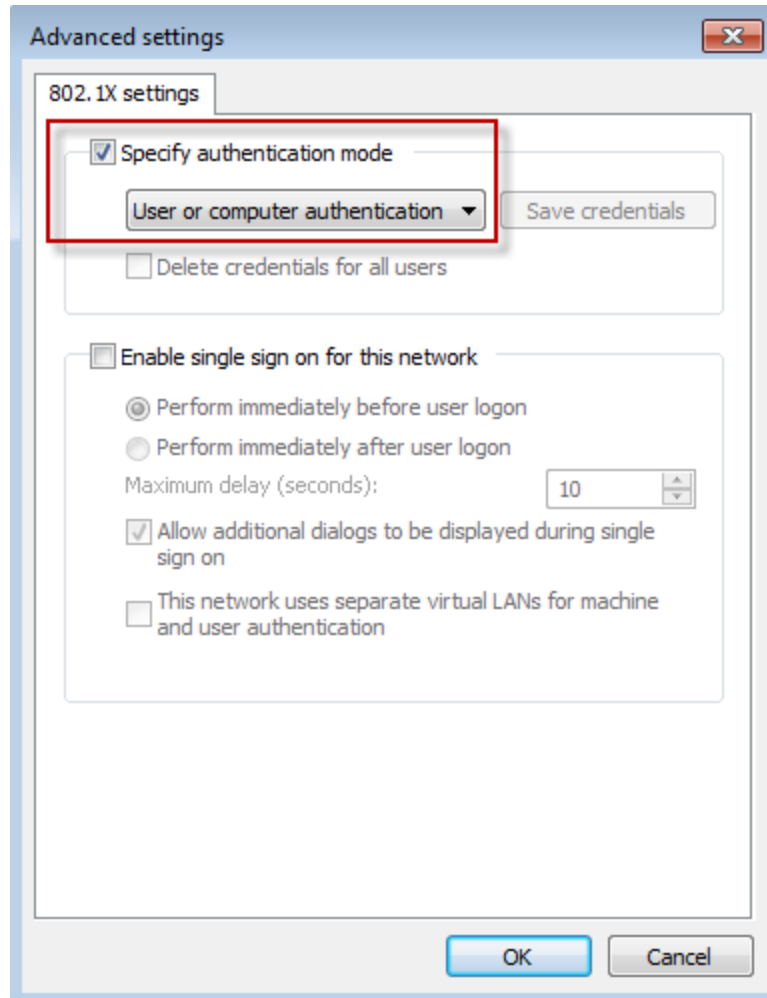
- vi. Verify that authentication method is set to **Microsoft: Protected EAP (PEAP)** and then click **Settings** to open the PEAP Properties page.
- vii. Under *Select Authentication Method.*; click **Configure** and verify that the EAP MSCHAPv2 Properties are set to **enable** *Automatically use my Windows login name and password (and domain if any)* as shown:



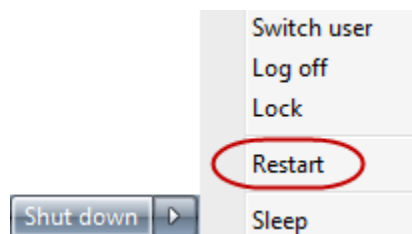
- viii. Click **OK** twice to close the PEAP Properties page and then click **Additional Settings**:



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



- x. Click **OK** twice to save changes and exit the LANProperties page.
- xi. Exit any open windows and restart the PC by going to **Start** (Start menu) and selecting **Restart**



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.

Step 4 Verify the authorization status on the switchport before Windows login (802.1X Machine authentication):

Wait until the Win7-PC client has restarted and returned to the CTRL+ALT+DEL screen, then return to the terminal session of the access switch. Run the **show authentication sessions** and the **show ip access-lists** commands for interface GigabitEthernet0/1.

Upon detection of the PC connection, the switchport will first attempt MAB authentication due to the switchport configuration (authentication order mab dot1x). MAB authentication may even complete with the default Authorization Policy rule (Authorization Profile = CWA_Posture_Remediation) being applied to the interface as shown in the example below:

```
3k-access(config-if)# do sh auth sess int gi0/1
Interface: GigabitEthernet0/1
MAC Address: 0010.1888.2224
IP Address: 10.1.10.101
User-Name: 00-10-18-88-22-24
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-POSTURE_REMEDIATION-4d816c3a
URL Redirect ACL: ACL-POSTURE-REDIRECT
URL Redirect: https://ise-1.demo.local:8443/guestportal/gateway?
              sessionId=0A01FA02000000711F4E7514&action=cwa
Session timeout: N/A
Idle timeout: N/A
Common Session ID: 0A01FA02000000711F4E7514
Acct Session ID: 0x0000009B
Handle: 0x0C000071

Runnable methods list:

Method State
mab Not run
dot1x Authc Success

3k-access(config-if)# do sh ip access-list int gi0/1
permit ip host 10.1.40.100 any
permit udp host 10.1.10.101 any eq domain
permit icmp host 10.1.10.101 any
permit tcp host 10.1.10.101 host 10.1.100.21 eq 8443
permit tcp host 10.1.10.101 any eq www
permit tcp host 10.1.10.101 any eq 443
permit tcp host 10.1.10.101 host 10.1.100.21 eq 8905
permit udp host 10.1.10.101 host 10.1.100.21 eq 8905
permit udp host 10.1.10.101 host 10.1.100.21 eq 8906
permit tcp host 10.1.10.101 host 10.1.252.21 eq www
```

Note: Due to actual timing, it is possible that 802.1X authentication may initiate prior to the completion of MAB processing. Therefore, the above output may not be seen.

Since 802.1X authentication has been given higher priority as per the switchport configuration (authentication priority dot1x mab), a new authentication will be triggered on the port once the Win7 supplicant initiates an EAPOL-Start message for 802.1X machine authentication. After successful 802.1X machine authentication, the Authorization Policy should match the

Domain_Computer rule (Authorization Profile = AD_Login). The output should appear similar to that shown below:

```

3k-access(config-if)# do sh auth sess int gi0/1
    Interface: GigabitEthernet0/1
    MAC Address: 0010.1888.2224
    IP Address: 10.1.10.101
    User-Name: host/win7-pc.demo.local
    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-AD_LOGIN_ACCESS-4d78ffbf
    Session timeout: N/A
    Idle timeout: N/A
    Common Session ID: 0A01FA02000000711F4E7514
    Acct Session ID: 0x0000009B
    Handle: 0x0C000071

Runnable methods list:
    Method   State
    mab      Not run
    dot1x    Authc Success

3k-access(config-if)# do sh ip access-list int gi0/1
    permit ip host 10.1.40.100 any
    permit udp host 10.1.10.101 eq bootpc any eq bootps
    permit udp host 10.1.10.101 any eq domain
    permit icmp host 10.1.10.101 any
    permit tcp host 10.1.10.101 host 10.1.100.10 eq 88
    permit udp host 10.1.10.101 host 10.1.100.10 eq 88
    permit udp host 10.1.10.101 host 10.1.100.10 eq ntp
    permit tcp host 10.1.10.101 host 10.1.100.10 eq 135
    permit udp host 10.1.10.101 host 10.1.100.10 eq netbios-ns
    permit tcp host 10.1.10.101 host 10.1.100.10 eq 139
    permit tcp host 10.1.10.101 host 10.1.100.10 eq 389
    permit udp host 10.1.10.101 host 10.1.100.10 eq 389
    permit tcp host 10.1.10.101 host 10.1.100.10 eq 445
    permit tcp host 10.1.10.101 host 10.1.100.10 eq 636
    permit udp host 10.1.10.101 host 10.1.100.10 eq 636
    permit tcp host 10.1.10.101 host 10.1.100.10 eq 1025
    permit tcp host 10.1.10.101 host 10.1.100.10 eq 1026
  
```

Verify that 802.1X machine authentication (User-Name = **host/Win7-PC.demo.local**) has completed successfully and that the dACL (ACS ACL) named **AD_LOGIN_ACCESS** is applied to the interface. The dACL includes entries to support AD login for the Windows domain user. For reference, the following table provides descriptions for the dACL entries:

| Downloadable ACL Entry | Description |
|---|-------------------------------|
| permit ip host 10.1.40.100 any | IP Phone dACL entry |
| permit udp host 10.1.10.101 eq bootpc any eq bootps | Allow DHCP |
| permit udp host 10.1.10.101 any eq domain | Allow DNS resolution |
| permit icmp host 10.1.10.101 any | Allow ICMP for policy testing |

| | |
|--|-------------|
| permit tcp host 10.1.10.101 host 10.1.100.10 eq 88 | Kerberos |
| permit udp host 10.1.10.101 host 10.1.100.10 eq 88 | Kerberos |
| permit udp host 10.1.10.101 host 10.1.100.10 eq 123 | NTP |
| permit tcp host 10.1.10.101 host 10.1.100.10 eq 135 | EpMap |
| permit udp host 10.1.10.101 host 10.1.100.10 eq 137 | Netbios-ns |
| permit tcp host 10.1.10.101 host 10.1.100.10 eq 139 | Netbios-ssn |
| permit tcp host 10.1.10.101 host 10.1.100.10 eq 389 | LDAP |
| permit udp host 10.1.10.101 host 10.1.100.10 eq 389 | LDAP |
| permit tcp host 10.1.10.101 host 10.1.100.10 eq 445 | MS-DC/SMB |
| permit tcp host 10.1.10.101 host 10.1.100.10 eq 636 | LDAP w/SSL |
| permit udp host 10.1.10.101 host 10.1.100.10 eq 636 | LDAP w/SSL |
| permit tcp host 10.1.10.101 host 10.1.100.10 eq 1025 | MS-AD |
| permit tcp host 10.1.10.101 host 10.1.100.10 eq 1026 | MS-AD |

Step 5 Verify the session status of the switchport authorization after Windows login (802.1X User authentication):

From the Win7-PC client, login to Windows domain as user **DEMO\employee1 / cisco123**. Repeat the **show authentication sessions** and the **show ip access-lists** output for interface GigabitEthernet0/1. After successful 802.1X user authentication, the Authorization Policy should match the Employee_NonCompliant rule (Authorization Profile = Posture_Remediation). The output should appear similar to that shown below:

```

3k-access(config-if)# do sh auth sess int gi0/1
    Interface: GigabitEthernet0/1
    MAC Address: 0010.1888.2224
    IP Address: 10.1.10.101
    User-Name: DEMO\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-POSTURE_REMEDIATION-4d816c3a
    URL Redirect ACL: ACL-POSTURE-REDIRECT
    URL Redirect: https://ise-1.demo.local:8443/guestportal/gateway?
    sessionId=0A01FA02000000711F4E7514&action=cpp
    Session timeout: N/A
    Idle timeout: N/A
    Common Session ID: 0A01FA02000000711F4E7514
    Acct Session ID: 0x0000009C
    Handle: 0x0C000071

Runnable methods list:

    Method    State
    mab       Not run
    dot1x     Authc Success

3k-access(config-if)# do sh ip access-list int gi0/1
    permit ip host 10.1.40.100 any
    permit udp host 10.1.10.101 any eq domain
    permit icmp host 10.1.10.101 any
    permit tcp host 10.1.10.101 host 10.1.100.21 eq 8443
    permit tcp host 10.1.10.101 any eq www

```

```
permit tcp host 10.1.10.101 any eq 443
permit tcp host 10.1.10.101 host 10.1.100.21 eq 8905
permit udp host 10.1.10.101 host 10.1.100.21 eq 8905
permit udp host 10.1.10.101 host 10.1.100.21 eq 8906
permit tcp host 10.1.10.101 host 10.1.252.21 eq www
```

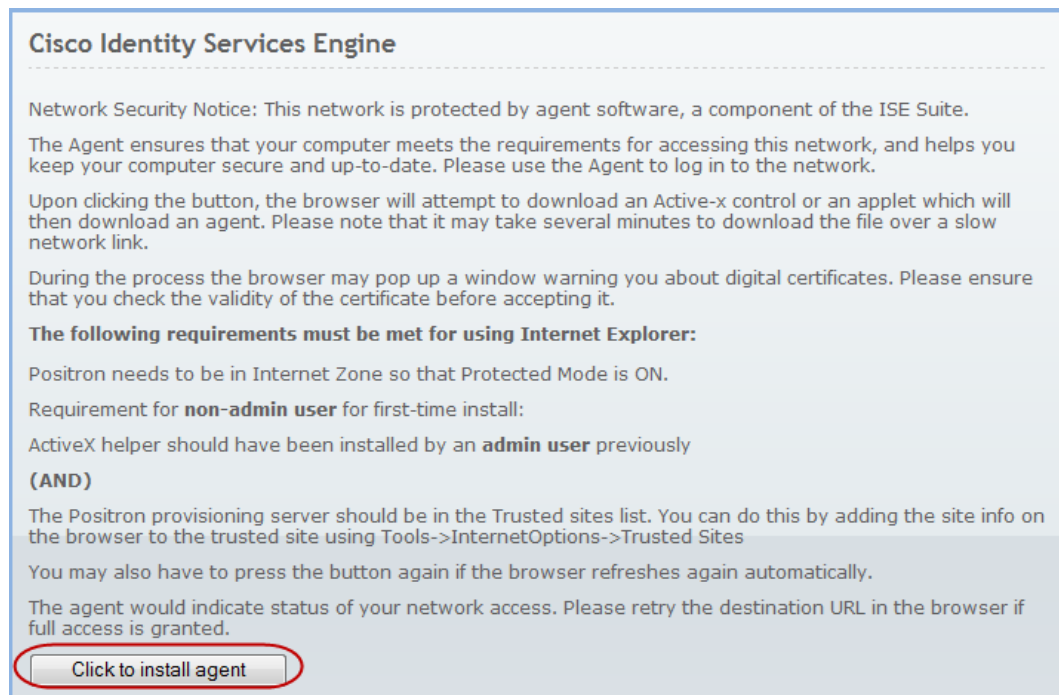
Verify that 802.1X user authentication (User-Name = **DEMO\employee1**) has completed successfully and that the dACL (ACS ACL) named **POSTURE-REMEDIA TION** has been pushed to the interface.

A named URL Redirect ACL = **ACL-POSTURE-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.

Note: The authorization dACL named POSTURE_REMEDIA TION is the same one applied during the Web Agent lab exercise for users in a non-compliant posture state. Please refer to the previous lab exercise for reference on individual dACL entries.

Step 6 Validate Client Provisioning for the NAC Agent.

- a. Launch a web browser. Immediate redirection to the agent provisioning page (CPP) should occur as shown:



Cisco Identity Services Engine

Network Security Notice: This network is protected by agent software, a component of the ISE Suite.

The Agent ensures that your computer meets the requirements for accessing this network, and helps you keep your computer secure and up-to-date. Please use the Agent to log in to the network.

Upon clicking the button, the browser will attempt to download an Active-x control or an applet which will then download an agent. Please note that it may take several minutes to download the file over a slow network link.

During the process the browser may pop up a window warning you about digital certificates. Please ensure that you check the validity of the certificate before accepting it.

The following requirements must be met for using Internet Explorer:

Positron needs to be in Internet Zone so that Protected Mode is ON.

Requirement for **non-admin user** for first-time install:

ActiveX helper should have been installed by an **admin user** previously

(AND)

The Positron provisioning server should be in the Trusted sites list. You can do this by adding the site info on the browser to the trusted site using Tools->InternetOptions->Trusted Sites

You may also have to press the button again if the browser refreshes again automatically.

The agent would indicate status of your network access. Please retry the destination URL in the browser if full access is granted.

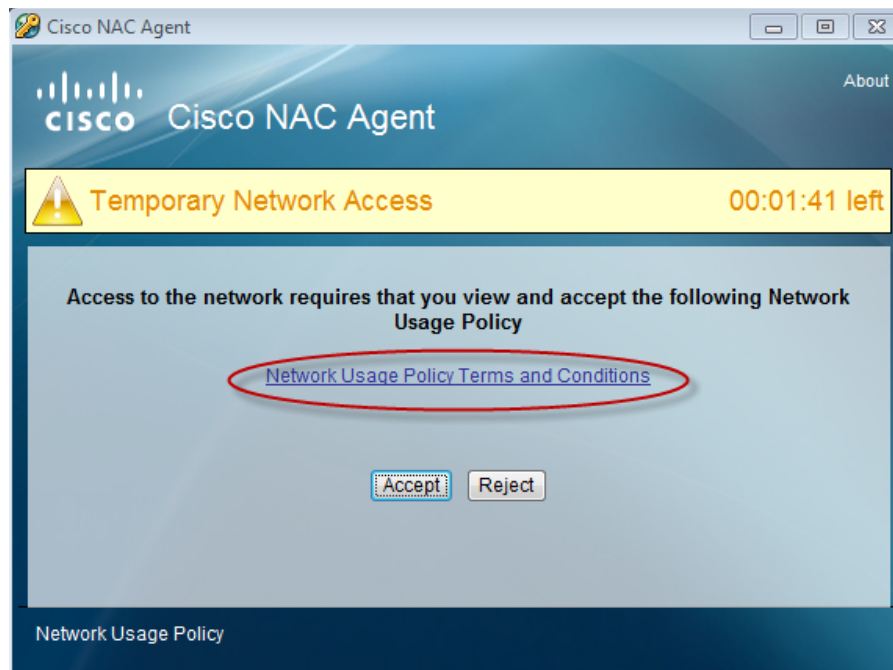
[Click to install agent](#)

- b. Click the **Click to install agent** button to begin NAC Agent installation.
- c. Accept any prompts regarding permissions to install software.

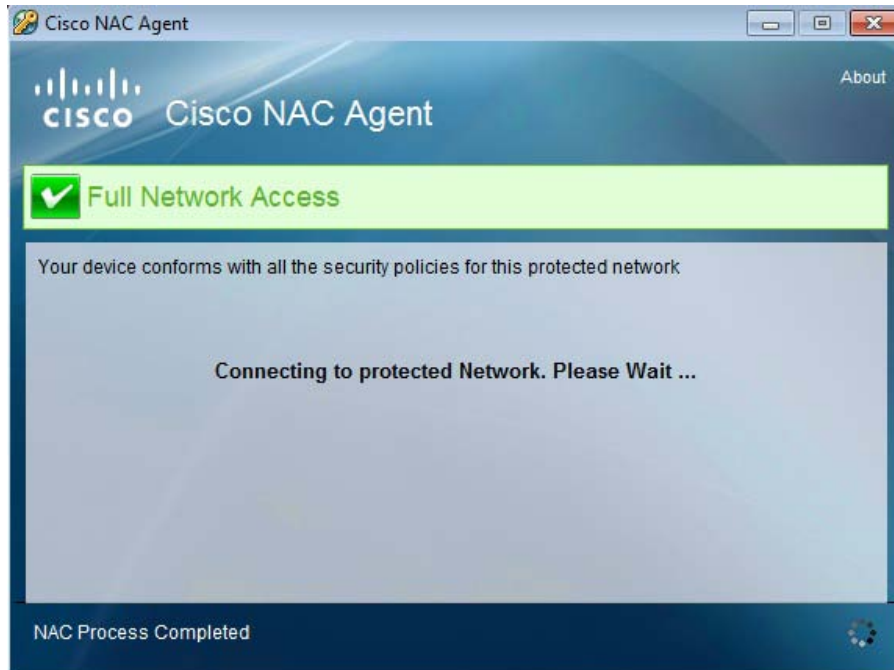
- d. Follow the NAC Agent installation prompts and accept the license agreement and default values to complete the provisioning process. If prompted by Windows UAC, enter credentials **admin / cisco123**.

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

- e. A message should appear in original window indicating “Cisco Agent was successfully installed!” Close this window.
- f. The Acceptable Use Policy page should display indicating *Temporary Network Access*. The AUP was configured in a previous lab step to display for any NAC Agent user and to point to a URL on an internal web server. Click the link **Network Usage Policy Terms and Conditions** to see the hosted AUP:



- g. A new web page will open to display the AUP. Close this window when ready to proceed.
- h. Click **Accept** to agree to the AUP. The login success screen should display indicating *Full Network Access* and automatically close after 2 seconds per the NAC Agent profile configuration named ProfileWindows.



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

Step 7 Verify the session status of the switchport authorization for a compliant Employee.

- a. Repeat the **show authentication sessions** and the **show ip access-lists** output for interface GigabitEthernet0/1. The Authorization Policy should match the Employee rule (Authorization Profile = Employee) and output should appear similar to that shown below.

```

3k-access(config-if)#do sh auth sess int gi0/1
  Interface: GigabitEthernet0/1
  MAC Address: 0010.1888.2224
  IP Address: 10.1.10.101
  User-Name: DEMO\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
  mab     Not run
  dot1x   Authc Success

3k-access(config-if)#do show ip access int gi0/1
  permit ip host 10.1.40.100 any

```

```

permit ip host 10.1.10.101 any
3k-access(config-if)#

```

- b. 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 8 Verify the authentication/authorization phases of the 802.1X Auth and Client Provisioning session from the ISE admin interface.

- a. Go to **Monitor > 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.
- b. 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, where 1 is the lowest, or first, entry:

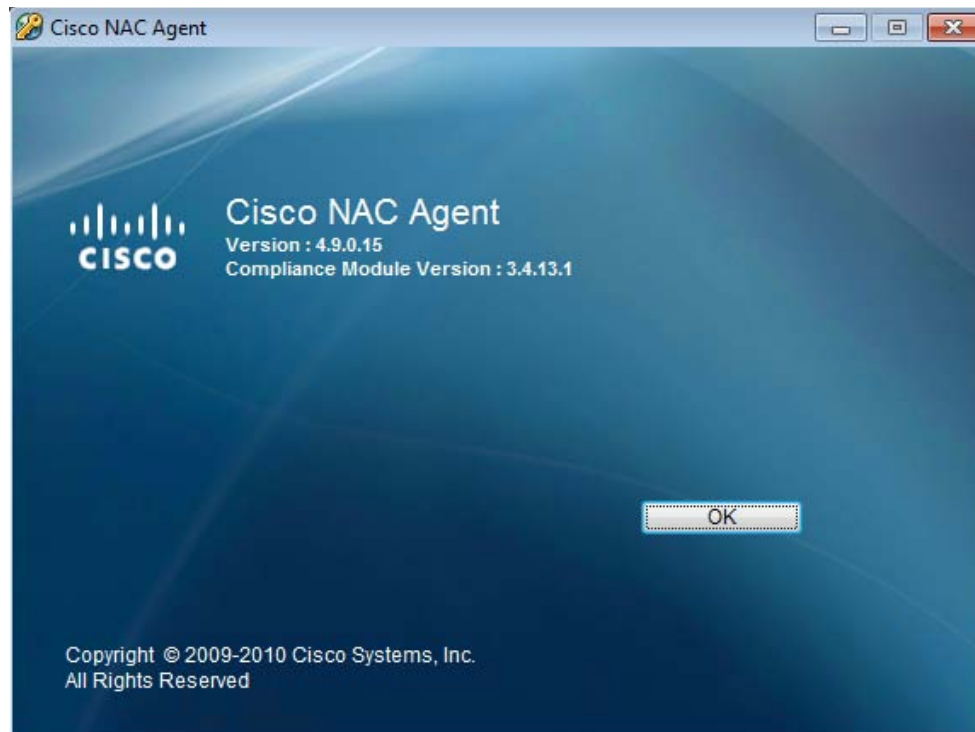
1. Successful MAB authentication for the endpoint (User-Name: 00-10-18-88-22-24); Authorization Profile CWA_Posture_Remediation applied.
2. dACL named POSTURE_REMEDIATION has been successfully downloaded.
3. Successful 802.1X *machine* authentication of the Domain Computer host/win7-pc.demo.local using PEAP(EAP-MSCHAPv2); Authorization Profile named AD_Login applied.
4. dACL named AD_LOGIN_ACCESS has been successfully downloaded.
5. Successful 802.1X *user* authentication of the Domain User DEMO\employee1; Authorization Profile named Posture_Remediation applied.
6. dACL named POSTURE_REMEDIATION has been successfully downloaded.
7. Posture reported compliant and dynamic authorization (CoA) succeeded for session based on posture status change.
8. Authorization Profile named Employee applied; dACL PERMIT_ALL_TRAFFIC applied.

| Time | Status | Details | Username | Calling Station ID | IP Address | NAD |
|------|--------|---------|------------------------------------|--------------------|-------------|-----------|
| 8 | ✓ | | DEMO\employee1 | 00:10:18:88:22:24 | 10.1.10.101 | 3k-access |
| 7 | ✓ | | | | | 3k-access |
| 6 | ✓ | | #ACSACL#IP-POSTURE_REMEDIATION-4d | | | 3k-access |
| 5 | ✓ | | DEMO\employee1 | 00:10:18:88:22:24 | 10.1.10.101 | 3k-access |
| 4 | ✓ | | #ACSACL#IP-AD_LOGIN_ACCESS-4d78ffb | | | 3k-access |
| 3 | ✓ | | host\win7-pc.demo.local | 00:10:18:88:22:24 | 10.1.10.101 | 3k-access |
| 2 | ✓ | | #ACSACL#IP-POSTURE_REMEDIATION-4d | | | 3k-access |
| 1 | ✓ | | 00:10:18:88:22:24 | 00:10:18:88:22:24 | 10.1.10.101 | 3k-access |

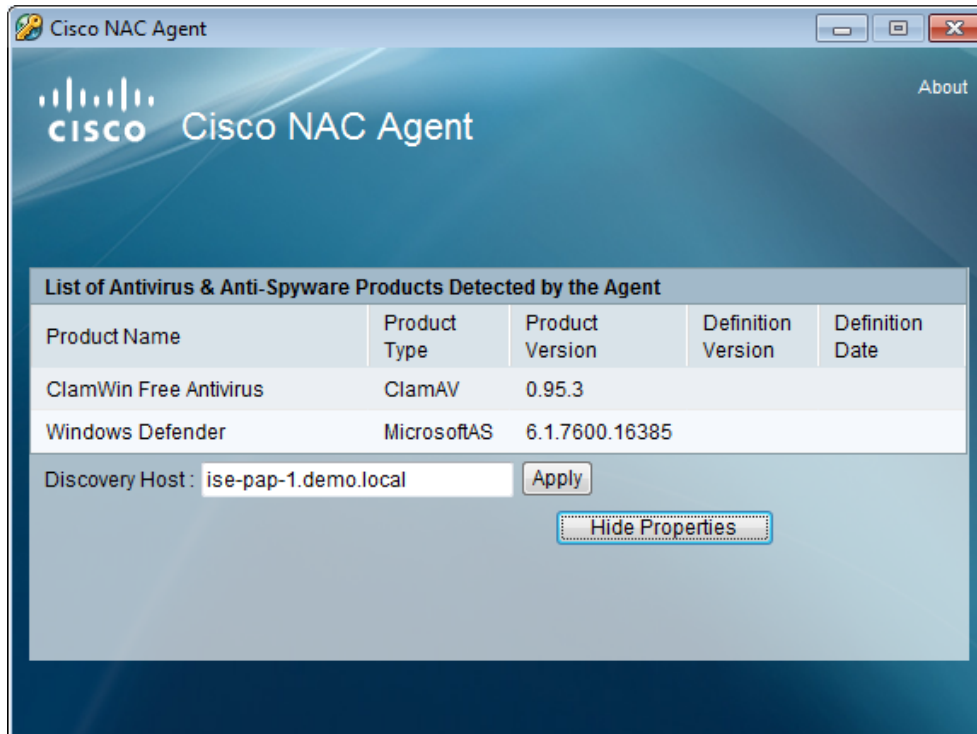
| Session ID | Server | NAS Port ID | Event | Failure Reason | Authorization Profiles | Auth Method |
|------------|-----------------------|-------------|--------------------|-------------------|-------------------------|-------------|
| 8 | 11FA0200000711F4E7514 | ise-1 | GigabitEthernet0/1 | Authentication su | Employee | dot1x |
| 7 | 11FA0200000711F4E7514 | ise-1 | | Dynamic Authoriz | | |
| 6 | | ise-1 | | DAACL Download | | |
| 5 | 11FA0200000711F4E7514 | ise-1 | GigabitEthernet0/1 | Authentication su | Posture_Remediation | dot1x |
| 4 | | ise-1 | | DAACL Download | | |
| 3 | 11FA0200000711F4E7514 | ise-1 | GigabitEthernet0/1 | Authentication su | AD_Login | dot1x |
| 2 | | ise-1 | | DAACL Download | | |
| 1 | 11FA0200000711F4E7514 | ise-1 | GigabitEthernet0/1 | Authentication su | CWA_Posture_Remediation | mab |

Step 9 Review the NAC Agent installation.

- a. From the Win7-PC client, the NAC Agent tray icon should now be present in the Windows task tray. Right-click the icon and select **About** to view NAC Agent and Compliance Module software versions:



- b. Click **OK** to close the window.
- c. Right-click the task tray icon again and select **Properties** to view current Discovery Host setting and detected AV/AS software as per the following:



d. Click **OK** to close the window.

Note: By default, the NAC Agent program files are installed under <Root_Drive>\Program Files\Cisco\Cisco NAC Agent. The agent XML-based profiles and configuration files are also located in this directory. By default, the log and report files are stored under <Root_Drive>\ProgramData\Cisco\Cisco NAC Agent.

End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 6: Configure an AV 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 NAC Agent or 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.

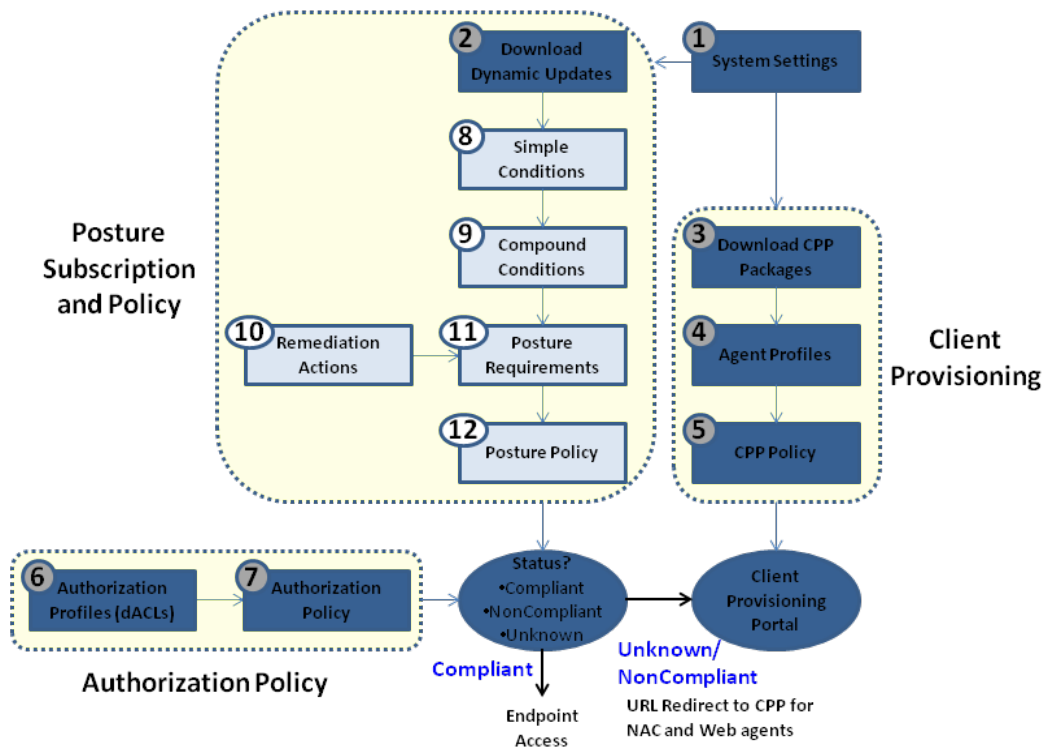
This exercise covers the configuration of a Posture Policy based on Antivirus (AV) conditions.

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

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.

| ▼ Update Information | |
|---|---------------------|
| Last update on | 2011/03/14 13:38:56 |
| Cisco conditions version | 102163.0.0.0 |
| Cisco AV/AS support chart version for windows | 85.0.0.0 |
| Cisco AV/AS support chart version for Mac OSX | 8.0.0.0 |
| Cisco supported OS version | 1 |

Step 2 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.

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:

| Attribute | Value |
|------------------------------|---|
| Name | ClamWin_AV_Installed |
| Description | Check ClamWin AV is installed |
| Operating System | Windows 7 (All) |
| Vendor | ClamWin *** Note: There is also an entry for ClamAV *** |
| Check Type | <input type="radio"/> Installation <input type="radio"/> Definition |
| | <input type="checkbox"/> Allow virus definition files to be |
| days older than | 0 days older than |
| | <input type="radio"/> latest file date <input type="radio"/> current system date |
| Products for Selected Vendor | <input checked="" type="checkbox"/> ClamWin Antivirus <input checked="" type="checkbox"/> 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 3 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.

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:

| Attribute | Value |
|------------------------------|---|
| Name | ClamWin_AV_Current |
| Description | Check ClamWin AV is current |
| Operating System | Windows 7 (All) |
| Vendor | ClamWin *** Note: There is also an entry for ClamAV *** |
| Check Type | <input type="radio"/> Installation <input checked="" type="radio"/> Definition |
| | <input checked="" type="checkbox"/> Allow virus definition files to be |
| days older than | 0 days older than |
| | <input type="radio"/> latest file date <input type="radio"/> current system date |
| Products for Selected Vendor | <input checked="" type="checkbox"/> ClamWin Antivirus <input checked="" type="checkbox"/> ClamWin FREE Antivirus |

Step 4 Define an AV posture condition that validates the installation of *any* supported AV on an endpoint. This check will be used for posture requirements applied to Guest users.

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**

| Attribute | Value |
|------------------|--|
| Name | Any_AV_Installed |
| Description | Check Any AV is installed |
| Operating System | Windows All |
| Vendor | ANY |
| Check Type | <input type="radio"/> Installation <input type="radio"/> Definition |

| Attribute | Value |
|------------------------------|---|
| | <input type="checkbox"/> Allow virus definition files to be |
| days older than | 0 days older than |
| | <input type="checkbox"/> latest file date <input type="checkbox"/> current system date |
| Products for Selected Vendor | <input checked="" type="checkbox"/> ANY |

Step 5 Define an AV posture condition that validates the signature version of *any* supported AV on an endpoint. This check will be used for posture requirements applied to Guest users.

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**

| Attribute | Value |
|------------------------------|--|
| Name | Any_AV_Current |
| Description | Check Any AV is current |
| Operating System | Windows All |
| Vendor | ANY |
| Check Type | <input type="checkbox"/> Installation <input type="radio"/> Definition |
| | <input checked="" type="checkbox"/> Allow virus definition files to be |
| days older than | 0 days older than |
| | <input type="radio"/> latest file date <input type="checkbox"/> current system date |
| Products for Selected Vendor | <input checked="" type="checkbox"/> ANY |

Step 6 Define a Posture Remediation Action that *installs* ClamWin AV on an endpoint.

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**.

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

| Attribute | Value |
|------------------|--|
| Name | Install_ClamWin_AV |
| Description | Link distribution to ClamWin AV install package |
| Remediation Type | Manual |
| Retry Count | 0 |
| Interval | 0 |
| URL | http://updates.demo.local/clamwin-0.05.3-setup.exe |

Step 7 Define a Posture Remediation Action that *updates* ClamWin AV on an endpoint.

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

| Attribute | Value |
|------------------------|--|
| Name | Update_ClamWin_AV_Definitions |
| Description | Trigger signature updates for ClamWin AV |
| AV/AS Remediation Type | AV Definition Update |
| Remediation Type | Automatic |
| Interval | 2 |
| Retry Count | 2 |
| Operating System | <input type="radio"/> Windows <input type="radio"/> Mac |
| AV Vendor Name | ClamWin *** Note: There is also an entry for ClamAV *** |


Step 8 Define a Posture Remediation Action that updates *any* supported AV on an endpoint.

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

| Attribute | Value |
|------------------------|--|
| Name | Update_Any_AV_Definitions |
| Description | Trigger signature updates for Any AV vendor |
| AV/AS Remediation Type | AV Definition Update |
| Remediation Type | Automatic |
| Interval | 2 |
| Retry Count | 2 |
| Operating System | <input type="radio"/> Windows <input type="radio"/> Mac |
| AV Vendor Name | ANY |

Step 9 Define Posture Requirements that will be applied to Employees and Guest users.

Select **Requirements** from the left-hand pane (under **Policy > Policy Elements > Results > Posture**).

Enter the following entries into the table using the  **Actions** selector at the end of a rule entry to insert or duplicate rules. Click **Save** when finished:

| Name | Operating System | Conditions | Remediation Actions | |
|--------------|------------------|----------------------|-------------------------------|-----------------------------|
| | | | Action | Message Shown to Agent User |
| AV_Installed | Windows 7 (All) | ClamWin_AV_Installed | Install_ClamWin_AV | (optional) |
| AV_Current | Windows 7 (All) | ClamWin_AV_Current | Update_ClamWin_AV_Definitions | (optional) |



| | | | | |
|--------------------|----------------|------------------|----------------------|---|
| Guest_AV_Installed | Windows All | Any_AV_Installed | Message Text Only | <H3>An approved Antivirus program was NOT detected on your PC. All guest 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 ClamAV, please click <a href "here" http://updates.demo.local/clamwin-0.95.3-setup.exe</H3> |
| Guest_AV_Current | Windows All | Any_AV_Current | Message Text Only | <H2> All Guests must have Antivirus software installed with current signatures. Please update your AV software signatures now.</H2> |

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.

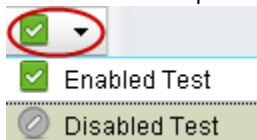
Note: A remediation action of Message Text Only provides the message content in the Description field to the user if requirement fails. This can be used to provide instructions to end user such as Help Desk contact numbers, URL links, or other text to assist in the remediation process. Also note that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

Step 10 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.


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

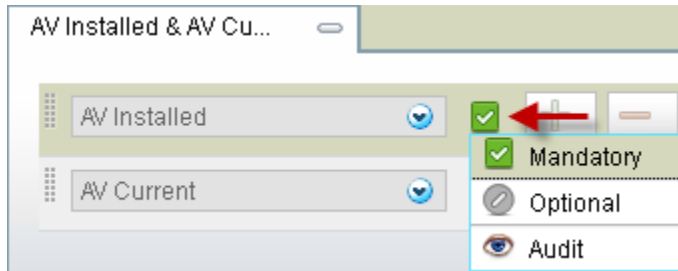
| Status | Rule Name | Identity Groups | Operating Systems | Other Conditions | Requirements |
|---|---|-----------------|-------------------|---|--|
|  | Employee_Windows_AV_Installed_and_Current | Any | Windows 7 (All) | demo.local: External Groups EQUALS demo.local/Users/employees | AV_Installed (Mandatory) AV_Current (Mandatory) |
|  | Guest_Windows_AV_Installed_and_Current | Guest | Windows All | - | Guest_AV_Installed (Mandatory) Guest_AV_Current (Mandatory) |

Note: Be sure to set the posture policy rules to DISABLED using the selector on the left hand side of the rule:



You will enable the posture rules individually during testing.

Note: To specify a Posture Requirement as Mandatory, Optional, or Audit, click the  icon to the right of the requirement name and select an option from the drop-down menu:



End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 7: 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 NAC Agent or 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 1 Define Registry Conditions that validate the compliance of Windows screen saver settings with our lab policy.

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

Step 2 Create a Registry Condition that checks that the current user's screen saver is enabled.

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

| Attribute | Value |
|-------------------|-----------------------|
| 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 3 Create a Registry Condition that checks that the current user's screen saver is set to a value other than *(None)*.

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

| Attribute | Value |
|-------------------|-----------------------|
| 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 4 Create a Registry Condition that checks that the current user's screen saver is secure (password set).

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

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

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


| Attribute | Value |
|-------------------|-----------------------|
| 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 6 Create a Compound Condition that includes each of the specific Screen Saver registry checks as a single condition.

- a. 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:

| Attribute | Value |
|------------------|---|
| Name | ScreenSaver |
| Description | (optional) |
| Operating System | Windows All |
| Expression | ((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.

- i. Click the  icon to right of **Registry Condition** in the Condition List section.
- ii. Select **ScreenSaver_On** from the list. Item should appear in open text field.
- iii. Click the **&** symbol button under the open text field. The symbol should be appended to the content in the open text field.
- iv. Complete the condition expression using the following selections:


ScreenSaver_Secure

&

ScreenSaver_SCR

&

ScreenSaver_Timeout

- b. 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).
- c. Click **Validate Expression** to have the system verify the basic expression logic and that expression is composed of valid checks.
- d. Click **Submit** when finished.

Step 7 Define a Posture Remediation Action that updates the screen saver registry keys on a Windows PC to compliant values.

Navigate to **Policy > Policy Elements > Results** and expand the contents under **Posture**, and then expand **Remediation Actions**.

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**:

| Attribute | Value |
|------------------|---|
| Name | Enable_Secure_Screen_Saver |
| Description | Download compliant screen saver registry values |
| Remediation Type | Manual |

| Attribute | Value |
|-------------|---|
| Retry Count | 0 |
| Interval | 0 |
| URL | http://updates.demo.local/ScreenSaver.reg |

Step 8 Define Posture Requirements that will be applied to Employees and Guest users.

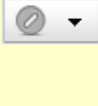


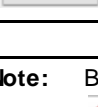
Select **Requirements** from the left-hand pane (under **Policy > Policy Elements > Results > Posture**).

Add a Screen Saver requirement into the table using the following values and then click **Save**:

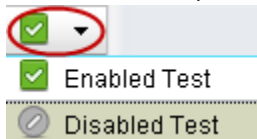
| Name | Operating System | Conditions | Remediation Actions | |
|----------------------------|------------------|-------------|----------------------------|--|
| | | | Action | Message Shown to Agent User |
| Screen_Saver_On_and_Secure | Windows All | ScreenSaver | Enable_Secure_Screen_Saver | <H3>Company 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</H3> |

Step 9 Configure the Posture Policy to ensure a Secure Screen Saver is present on Employee and Guest user computers running Windows.

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:External Groups EQUALS demo.local/Users/employees | Screen_Saver_On_and_Secure (Mandatory) |
|  | Employee_Windows_AV_Installed_and_Current | Any | Windows 7 (All) | demo.local:External Groups EQUALS demo.local/Users/employees | AV_Installed (Mandatory) AV_Current (Mandatory) |
|  | Guest_ScreenSaver | Guest | Windows All | - | Screen_Saver_On_and_Secure (Mandatory) |
|  | Guest_Windows_AV_Installed_and_Current | Guest | Windows All | - | Guest_AV_Installed (Mandatory) Guest_AV_Current (Mandatory) |

Note: Be sure to set the posture policy rules to DISABLED using the selector on the left hand side of the rule:



You will enable the posture rules individually during testing

☑ End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 8: Test Posture Assessment and Posture Policies using NAC Agent

Exercise Description

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

Exercise Objective

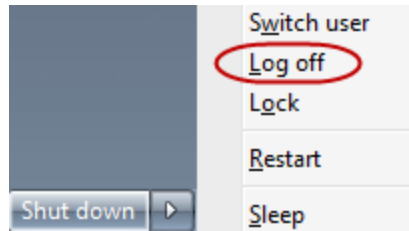
In this exercise, your goal is to complete the following tasks:

- Login as an Employee via 802.1X authentication and verify proper execution of NAC Agent discovery, posture, and remediation process.
- Test AV Posture Policy using NAC Agent.
- OPTIONAL: Test Screen Saver Posture Policy using NAC 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 1** Delete ClamWin AV signatures on the Win7 PC to ensure that the client AV software is out of compliance with AV signature updates.
- a. Log into the Windows 7 PC client as **DEMO\employee1 / cisco123**, where *DEMO* is the Windows domain name.
 - b. From the Win7-PC client, open the **Lab Tools** shortcut from the Windows desktop and run (double-click) the **Delete_ClamWin_AV_Updates** script.
 - c. A command window should open to execute processing of the script and indicate "Process Complete!" when finished. Press **any** key to continue.
 - d. Close the **Lab Tools** window.
 - e. **Logoff** Windows using the Start menu:



Step 2 Validate the authorization status of the Win7-PC client on the access switch.

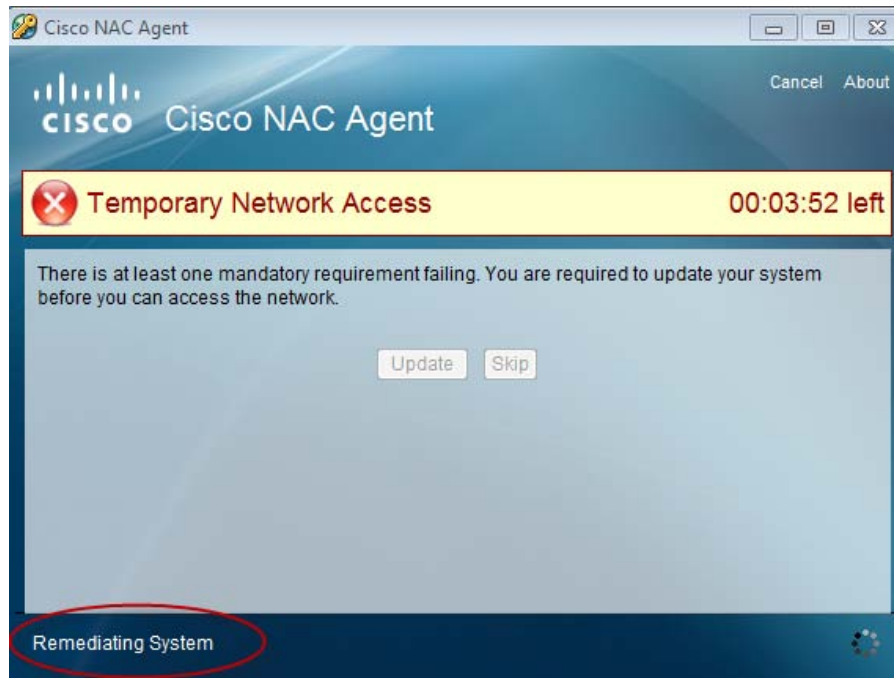
- a. Establish a terminal session with the access switch (10.1.250.2)
- b. Verify the authorization status of the PC switchport using the command **show authentication sessions interface GigabitEthernet 0/1**.
- c. The DATA domain should show successful 802.1X authentication from machine auth (User-Name: host/Win7-PC.demo.local) and the current dACL (ACS ACL) should be AD_LOGIN_ACCESS.
 - If so, then continue to the next step.
 - If the current status is not as described above, then perform a **shut / no shut** on interface gi0/1. This will clear out any previous session that may have been established. After about 30 seconds, the port status should indicate that 802.1X machine authentication has completed successfully and AD login privileges have been granted.

Step 3 Enable the AV Posture Policy for Employees.

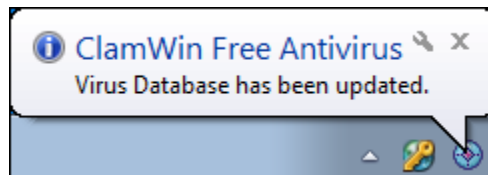
- a. From the Admin client PC, access the ISE admin interface and go to **Policy > Posture**.
- b. Enable the **Employee_Windows_AV_Installed_and_Current** rule by setting its status as follows:  as follows:
 - c. Click **Save** to apply changes.

Step 4 Test AV Posture Policy for Employees.

- a. Log back in to the Windows 7 PC client as **DEMO\employee1 / cisco123**, where *DEMO* is the Windows domain name.
- b. The previously installed NAC Agent should automatically launch after Windows login and begin the posture assessment process. Due to an out-of-compliance condition for the AV policy, remediation should be initiated. The Remediation Action was set to *Automatic* so the message "Remediating System" should appear at the bottom of the agent window as shown:



- c. Auto-remediation will trigger the ClamAV client to update its signature definitions and a notification should be viewable from the Windows task tray upon successful update:

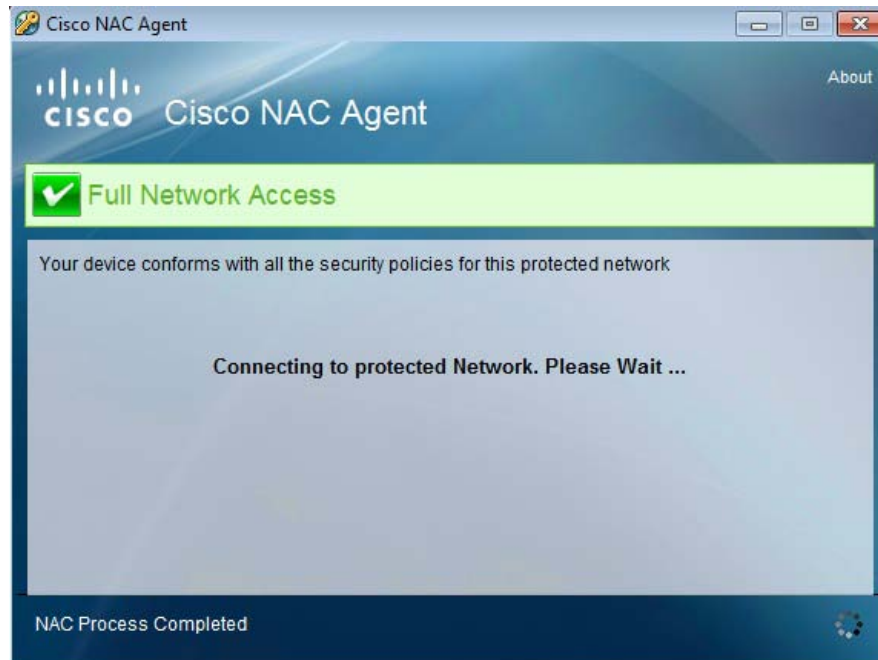


Note: If the ClamWin update process fails...

The remediation server (updates.demo.local) is configured to download current AV signature files upon start of the pX-www-int 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.

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.

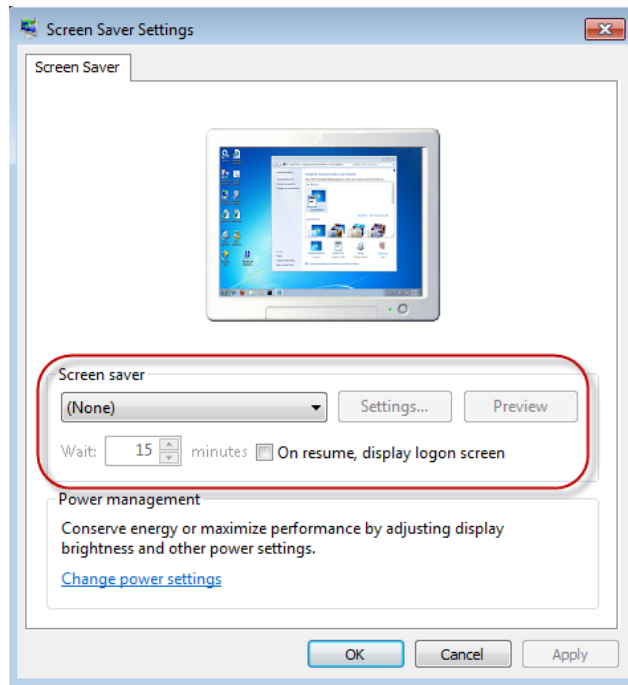
- d. The AUP page should display following successful remediation. Click **Accept** to accept the Network Usage Policy Terms and Conditions.
- e. A message will appear stating *Full Network Access* and will auto-close per our NAC Agent profile settings.



- Step 5** Validate the authorization status of the Win7-PC client on the access switch.
- Return to the access switch terminal session.
 - Verify the authorization status of the PC switchport using the command **show authentication sessions interface GigabitEthernet 0/1**.
 - 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 6** Prepare the Win7-PC client for testing the full Posture Policy for Employees.
- 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.
 - From the Lab Tools shortcut on the Windows desktop, double-click the **Personalization** shortcut to open the Control Panel's Personalization settings.
 - Select **Screen Saver** from the Control Panel windows (bottom right corner).
 - Verify that the Windows screen saver settings are disabled:
 - Screen saver = **(None)**
 - Wait = **Value > 5 minutes**
 - On resume, display logon screen = **<Not checked>**



- e. Click **OK** to close the Screen Saver Settings and close the Control Panel window.
- f. Log off from the Windows 7 PC client.

Step 7 Enable the Screen Saver Posture Policy for Employees.

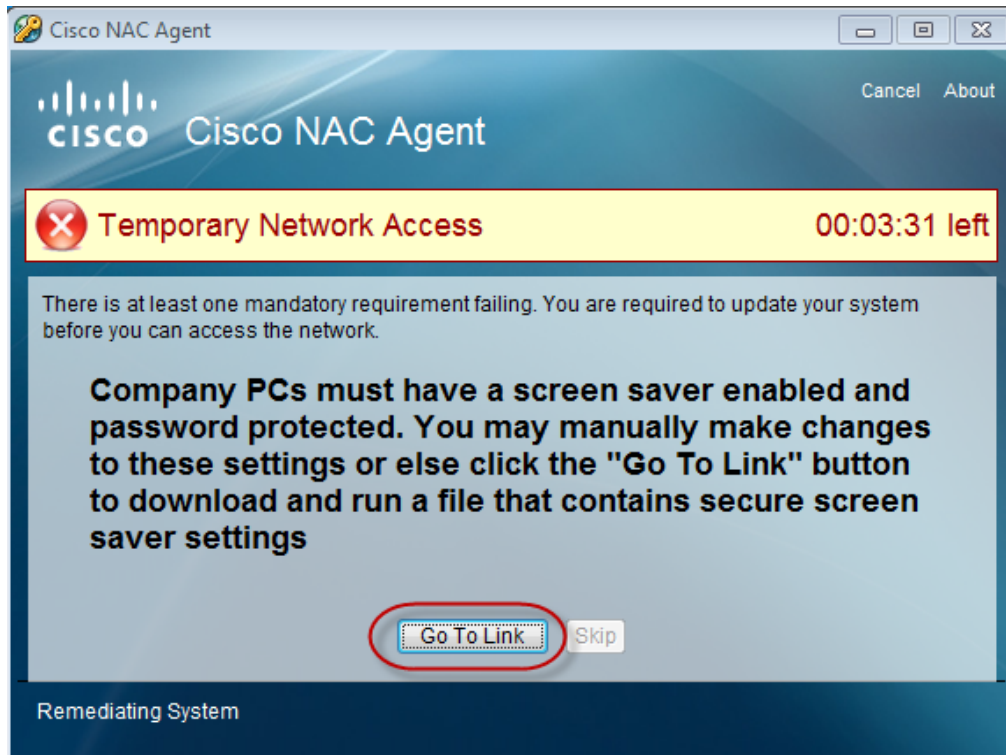
- a. From the Admin client PC, access the ISE admin interface and go to **Policy > Posture**.
- b. Enable the **Employee_ScreenSaver** rule by setting its status as follows: 
- c. Click **Save** to apply changes.

Step 8 Test Screen Saver Posture Policy for Employees.

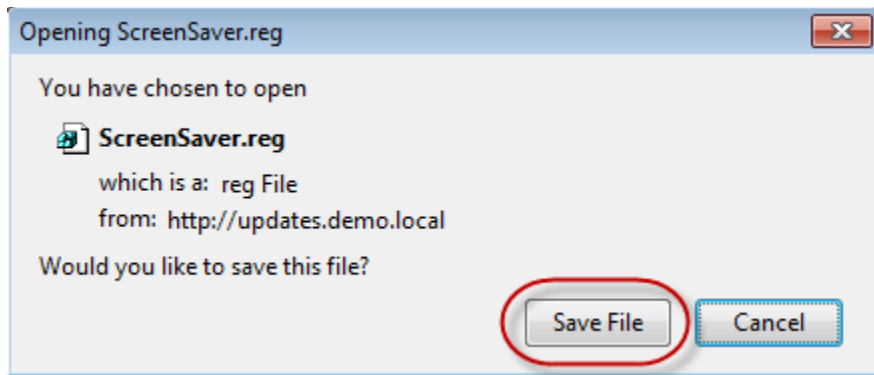
- a. Log back in to the Windows 7 PC client as **DEMO\employee1 / cisco123**, where *DEMO* is the Windows domain name.
- b. The NAC Agent should automatically launch after Windows login and begin the posture assessment process. Since we reverted the AV signatures to a non-compliant state, automatic AV 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.

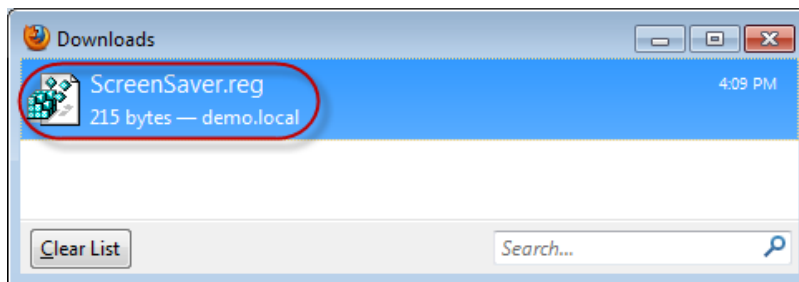
Read the instructions (this information was entered into the requirement description during creation of the Posture Requirement) and click **Go To Link**:



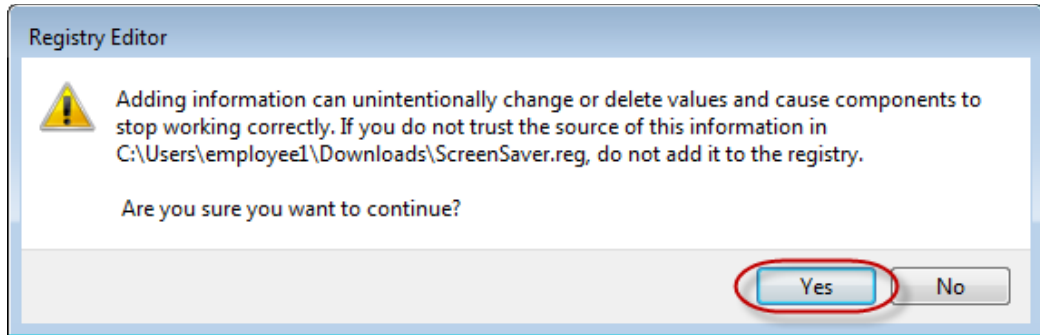
- c. A window will appear to download the registry fixes from the lab update server. Click **Save File**:



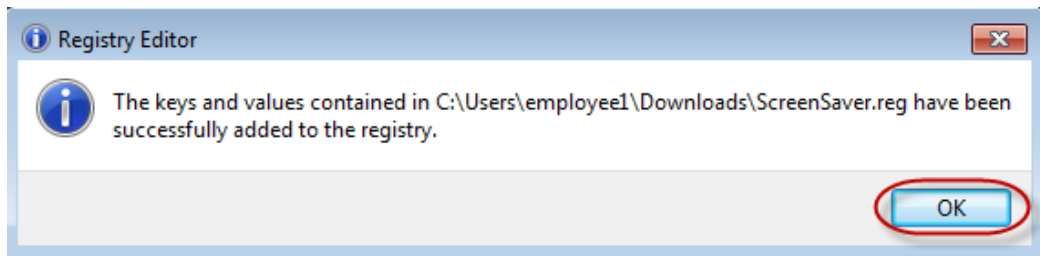
- d. The file ScreenSaver.reg is downloaded to the Win7-PC client. Double-click the filename to install the new registry settings:



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



- f. Click **OK** to acknowledge the successful registry update:



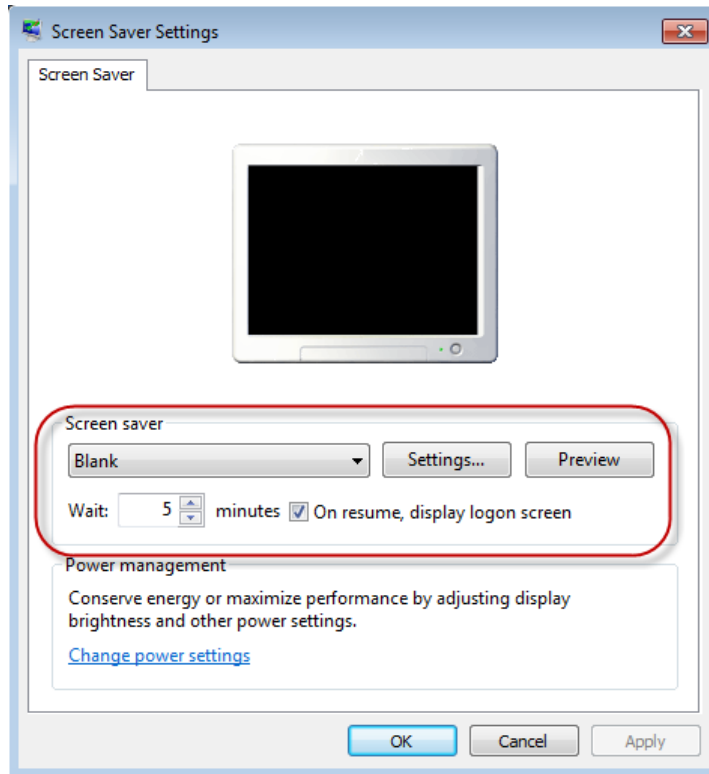
- g. Close any remaining browser windows opened as part of the remediation process.
- h. The AUP page should display following successful remediation. Click **Accept** to accept the Network Usage Policy Terms and Conditions.
- i. A message will appear stating *Full Network Access* and will auto-close per our NAC Agent profile settings.

Step 9 Test the Employee login experience when fully compliant with Posture Policy.

- a. Logoff from the Win7-PC and then log back in as user DEMO\employee1.
- b. Upon Windows login, the NAC 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 NAC Agent should close and full network access be granted.

Step 10 Verify the Screen Saver policy settings:

- a. From the Lab Tools shortcut on the Windows desktop, double-click the **Personalization** shortcut to open the Control Panel's Personalization settings.
- b. Select **Screen Saver** from the Control Panel windows (bottom right corner).
- c. Verify that the Windows screen saver settings are disabled:
- Screen saver = **Blank**
 - Wait = **5 minutes**
 - On resume, display logon screen = **<Checked>**



- d. Click **OK** to close the Screen Saver Settings and close the Control Panel window.

- Step 11** Review the ISE Authentication logs for proper authentication, authorization, and policy assignment.
- Access the ISE admin interface from the Admin client PC.
 - Go **Monitor > Authentications**.
 - Review the entries associated with the Win7-PC client 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:
 - Username=host\Win7-PC.demo.local, Authorization Profile=AD_Login
 - Username=DEMO\employee1, Authorization Profile=Posture_Remediation
 - Username=Demo\employee1, Authorization Profile=Employee

OPTIONAL: Passive Re-Assessment (PRA) TESTING

Step 12 Configure the PRA policy from the system posture settings:

- a. 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
- b. Click **Reassessments** in the left-hand pane, and then click **Add** from the menu in the right-hand pane.
- c. Enter the following values for the new PRA policy and click **Submit** when finished:





| Attribute | Value |
|-------------------------------|---------------------|
| Configuration Name | PRA_Any_User |
| Configuration Description | (optional) |
| Use Reassessment Enforcement? | [✓] |
| Enforcement Type | remediate |
| Interval | 2 |
| Grace Time | 1 |
| Select Roles | Any |

Note: The standard minimum settings for PRA Interval and Grace Time are 60 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 13 Configure the Posture Policy for PRA.

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:

- To apply a matching posture requirement to the initial assessment only, set the Session:Agent-Request-Type attribute EQUAL to **Initial**.
 - To apply a matching posture requirement to periodic reassessments only, set the Session:Agent-Request-Type attribute EQUAL to **Periodic Reassessment**.
 - 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.
- a. Access the ISE admin interface from the Admin client PC.
 - b. 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/Users/employees AND Session: Agent-Request-Type EQUALS Periodic Reassessment | Screen_Saver_On_and_Secure (Mandatory) |
|  | Employee_Windows_AV_Installed_and_Current | Any | Windows (All) | demo.local:ExternalGroups EQUALS demo.local/Users/employees AND Session: Agent-Request-Type EQUALS Initial | AV_Installed (Mandatory) AV_Current (Mandatory) |
|  | Guest_ScreenSaver | Guest | Windows All | - | Screen_Saver_On_and_Secure (Mandatory) |
|  | Guest_Windows_AV_Installed_and_Current | Guest | Windows All | - | Guest_AV_Installed (Mandatory) Guest_AV_Current (Mandatory) |

c. Click **Save** to apply changes.

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 14 Test PRA from the Windows 7 client PC:

a. Logoff from the Win7-PC and then log back in as user DEMO\employee1.

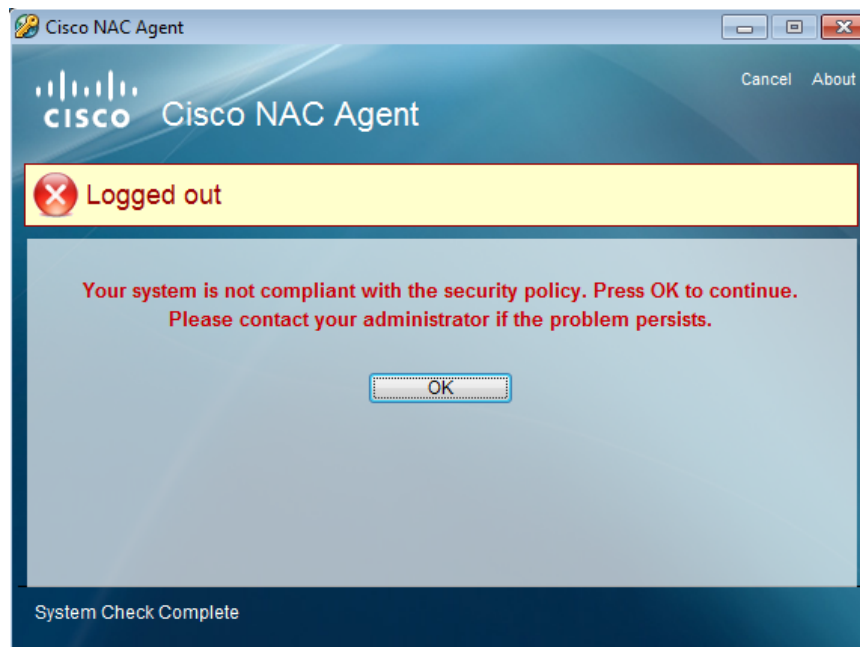
Note: If login is required to unlock screen, be sure to login first to active login session to unlock desktop, and then logoff Windows.

- b. Upon Windows login, the NAC 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 NAC Agent should close with full network access granted.
- c. 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.
- d. Run the **RemoveScreenSaver** script from the Windows desktop to revert the screen saver settings to non-compliant values. Click **Yes** and then **OK** to accept and acknowledge the registry changes.

- e. Wait up to two minutes for posture reassessment Interval to trigger. The NAC Agent should open to alert the failure of the Screen Saver policy.



- f. Allow the 1 minute Grace Time to expire. The following message will display:



- g. Click **OK** to close the NAC Agent window.
- h. Place your mouse cursor over the Cisco NAC Agent icon in the Windows task tray. The status should now display "Quarantined" (changed from "Logged-In").

Step 15 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 FastEthernet 0/1**. The current dACL (ACS ACL) should now be POSTURE-REMEDIATION (changed from PERMIT_ALL_TRAFFIC).

Step 16 Modify the PRA policy for audit only mode.

- a. 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
- b. Click **Reassessments** in the left-hand pane, select **PRA_Any_User** and then click **Edit** from the menu in the right-hand pane.
- c. Change the PRA policy per the following table and then click **Save** to apply changes:

| Attribute | Value |
|-------------------------------|---------------------|
| Configuration Name | PRA_Any_User |
| Configuration Description | (optional) |
| Use Reassessment Enforcement? | [✓] |
| Enforcement Type | continue |
| Interval | 60 |
| Grace Time | 5 |
| Select Roles | Any |

End of Exercise: You have successfully completed this exercise. Proceed to next section.

Lab Exercise 9: Test Posture Assessment and Posture Policies using 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.

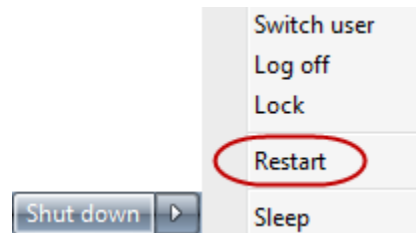
Lab Exercise Steps

AV POSTURE TESTING

- Step 1** Prepare the Win7-PC client for Web Agent posture assessment and policy testing as a Guest user.
- a. Login as **DEMO\employee1**
 - b. From the Lab Tools shortcut on the Windows desktop, run the **Delete_ClamWin_AV_Updates** script to remove the AV client's signature definitions.
 - c. 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.
 - d. Uninstall the NAC Agent:
 - i. Go to **Start (Start Menu) > Control Panel > Programs and Features**. Select **Cisco NAC Agent** from the list and click **Uninstall** from the menu options.
 - ii. Click **Yes** if prompted to confirm the uninstall process.
 - iii. If prompted, enter the Domain Admin credentials **admin / cisco123** to permit the process as a non-admin user.
 - iv. When the uninstall process is complete, the program listing for **Cisco NAC Agent** will be removed. Exit the Control Panel window.

- e. Disable 802.1X wired services on the Windows 7 client:
 - i. Launch the **Services** shortcut from the Windows 7 desktop.
 - ii. Open the **Wired AutoConfig** service from the list:
 - iii. Change Startup type: to **Disabled** and click **Apply**.
 - iv. Click **Stop** and ensure that Service status = *Stopped*.
 - v. Click **OK** and close the Services window.

Step 2 Exit any open windows and restart the PC by going to **Start** (Start menu) and selecting **Restart**:



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.

Step 3 Verify the authorization status on the switchport:

Wait until the Win7-PC client has restarted and returned to the CTRL+ALT+DEL screen, then return to the terminal session of the access switch.

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

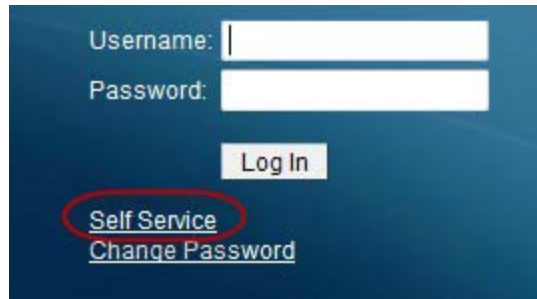
```
show authentication sessions interface GigabitEthernet 0/1  
show ip access-lists interface GigabitEthernet 0/1
```

Step 4 Enable the AV and Screen Saver Posture Policies for Guest users.

- a. From the Admin client PC, access the ISE admin interface and go to **Policy > Posture**.
- b. Enable the **Guest_Windows_AV_Installed_and_Current** rule.
- c. Enable the **Guest_Screen_Saver** rule.
- d. Click **Save** to apply changes.

Step 5 Create a new self-service Guest user account.

- a. From the Win7-PC client, login as user **DEMOemployee1 / cisco123**
- b. Launch the Mozilla Firefox Web browser. The page should be redirected to the ISE Web authentication portal.
- c. Click the **Self Service** button from the login portal...



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

| Attribute | Value |
|-----------------|--|
| First Name | Guest |
| Last Name | User |
| Email Address | guestuser@company.com |
| Phone Number | (optional) |
| Company | Company ABC |
| Optional Data 1 | (enter reason for access) |
| Optional Data 2 | (enter optional comments) |
| Timezone | UTC |

- d. 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.

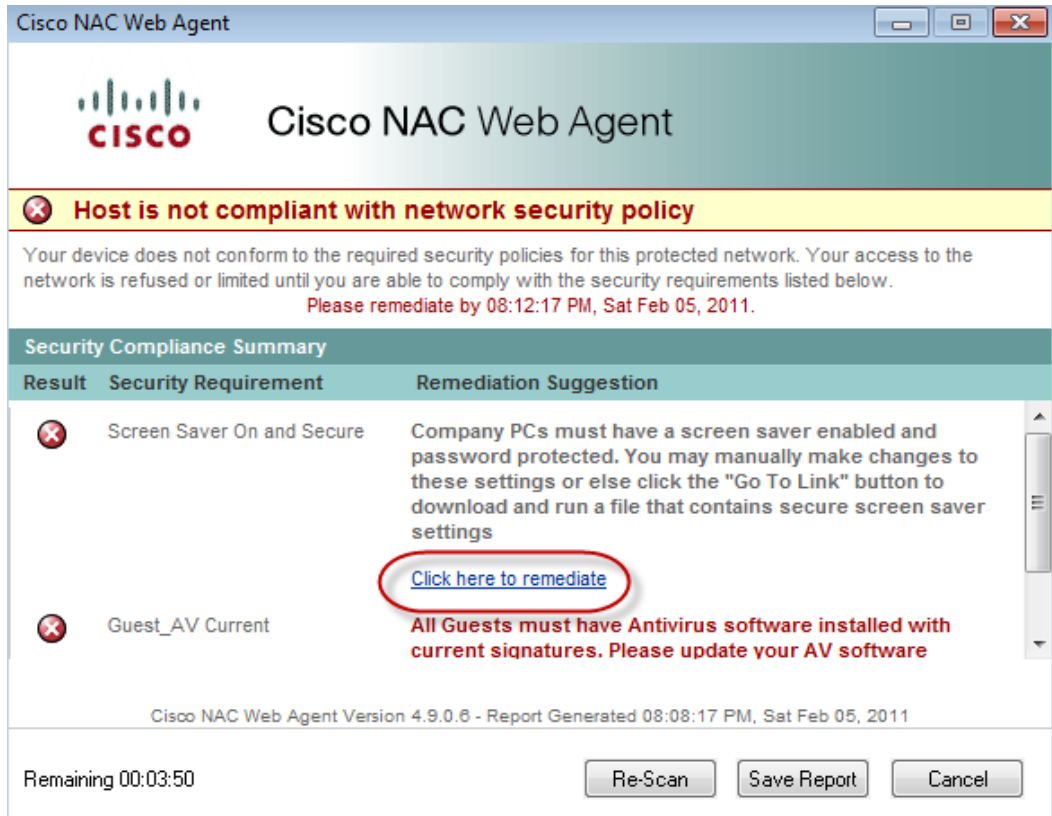
- e. Click the **OK** button to display the Web authentication login page again.

Step 4 Login as a Guest user and run the Web Agent.

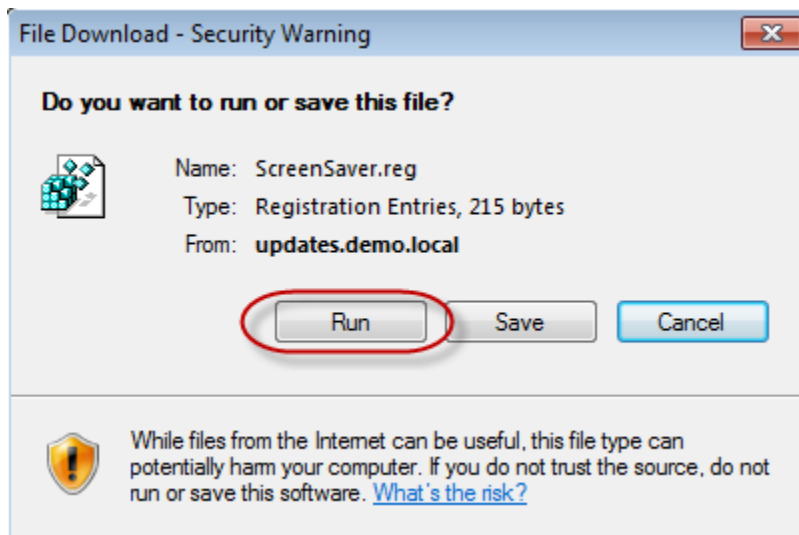
- Enter your new Username/Password credentials and click the **Log In** button.
- If an AUP was enabled for Web authentication, check the box to *Accept terms and Conditions* and then click **Accept**.
- The ISE Agent Downloader page should appear. Click the button **Click to install agent** at the bottom of the page.
- Accept any certificate warnings if prompted.
- The Cisco NAC Web Agent window should appear and indicate that posture assessment is being performed.

Step 5 Remediate the non-compliant screen saver policy using the Web Agent.

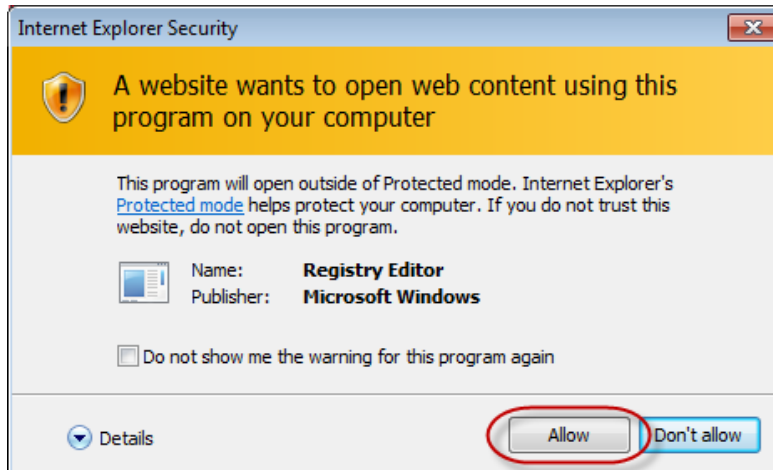
- Both Guest user Posture Policies for AV and Screen Saver should fail as shown below:



- b. Click the link **Click here to remediate** under the failed Screen Saver Requirement suggestions.
- c. A File Download warning will appear. Click **Run**:



- d. Click **Allow** if presented with a browser security warning:

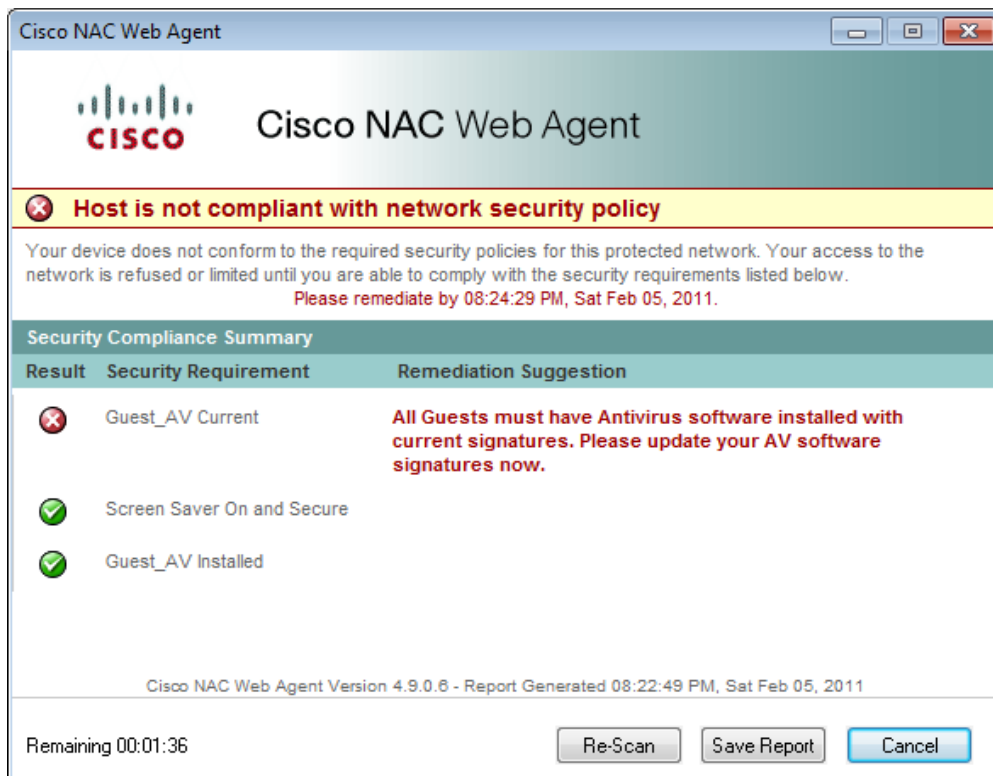


- e. A Registry Editor window will appear asking if you wish to continue with the registry modifications. Click **Yes** to allow the registry to be modified.
- f. Click **OK** to acknowledge the successful registry update.

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 Down loader page and re-clicking the button **Click to install agent** at the bottom of the page.

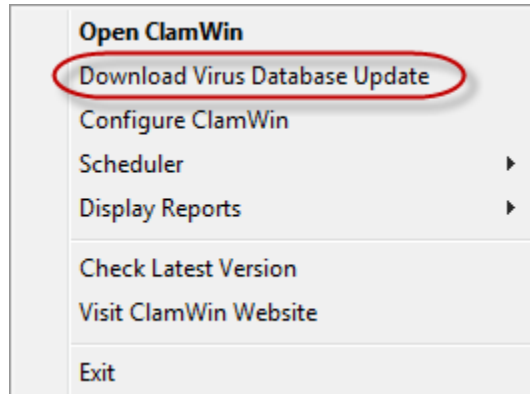
Step 6 Remediate the non-compliant AV policy.

- a. 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:

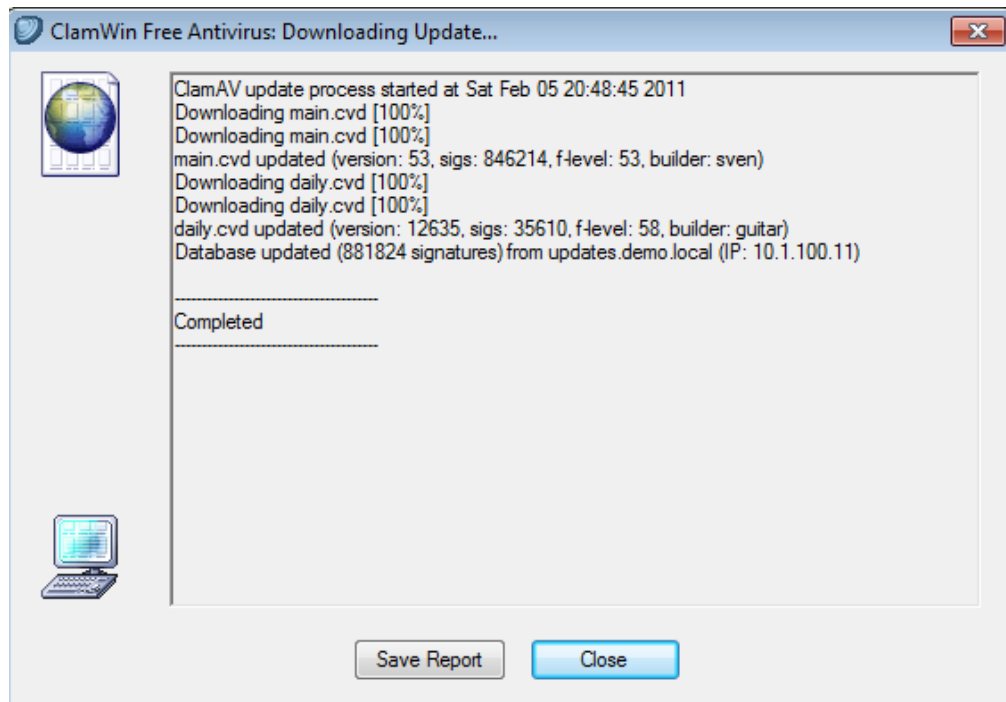


- b. As a temporal client for use by any Windows PC including non-admin users, the Web Agent does not allow for triggered code execution. Therefore, the Guest user must initiate the remediation.

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




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



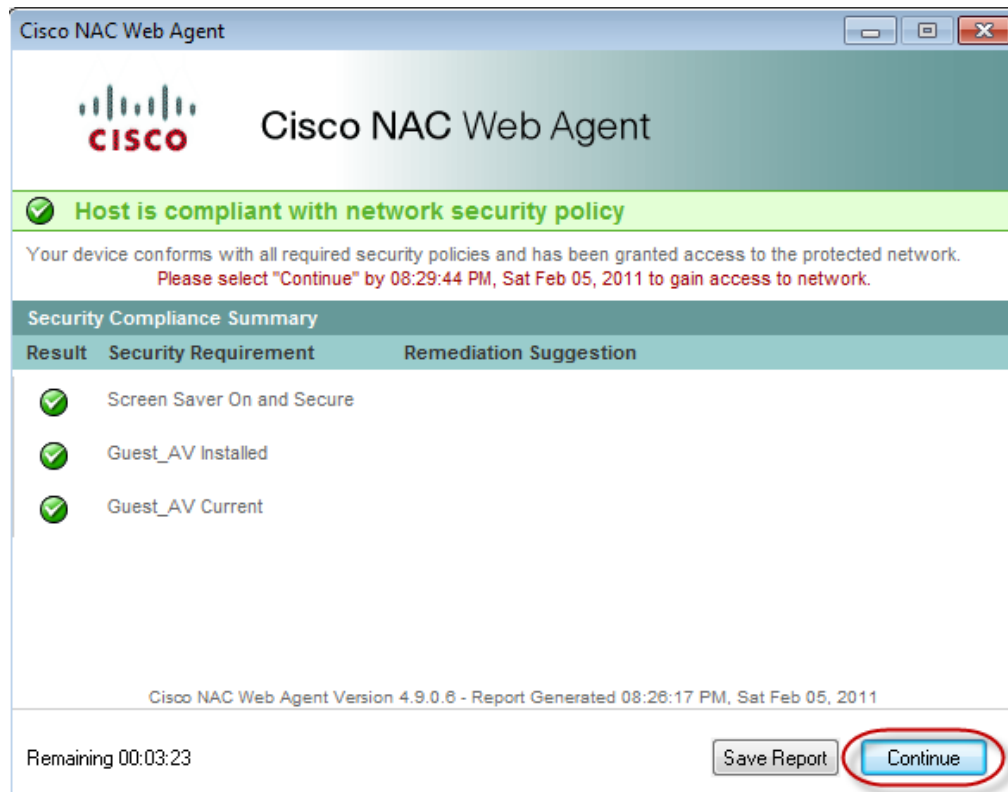
Note: If the ClamWin update process fails...

The remediation server (updates.demo.local) is configured to download current AV signature files upon start of the pX-www-int 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.

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 7 Complete the Web Agent posture process.

- a. 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:



- b. Click **Continue** to complete the Web Agent session. The login success screen should auto-close after two seconds per the configured policy.
- c. 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 8 Review the ISE Authentication logs for proper authentication, authorization, and policy assignment.

- a. Access the ISE admin interface from the Admin client PC.
- b. Go **Monitor > Authentications**.
- c. Review the entries associated with the Win7-PC client 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:

- i. Username=<MAC_Address>, Authorization Profile=CWA_Posture_Reemdiation
- ii. Username=<Guest_Username>, Authorization Profile=Guest

**End of Exercise: You have successfully completed this exercise.
Proceed to next section.**

Lab Exercise 10: 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:

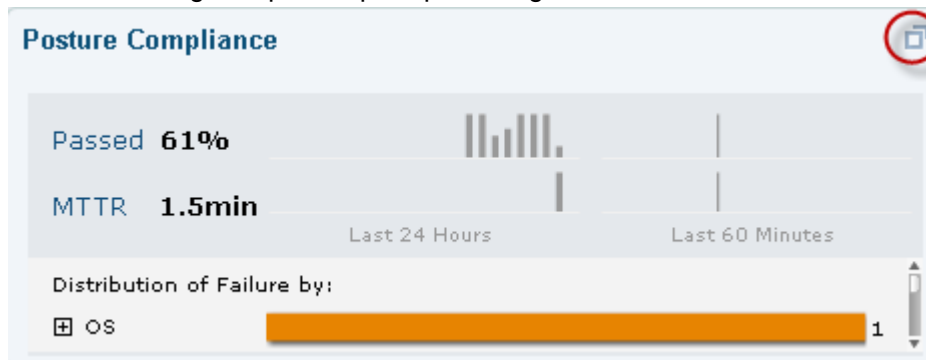
- Review ISE Authentications log and verify session details related to Posture Services.
- Review the ISE Dashboard for high-level posture status and statistics.
- Troubleshoot posture events using ISE Diagnostic Tools.
- Run ISE reports for Posture Services.

Lab Exercise Steps

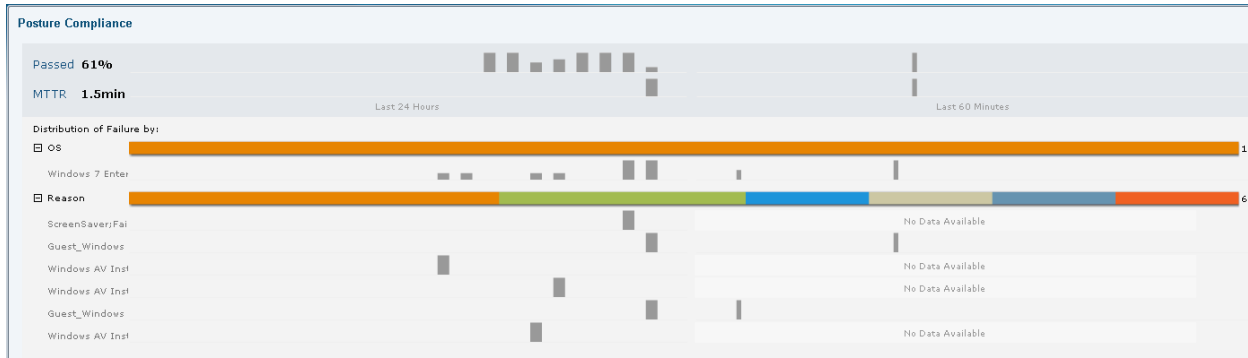
Step 1 Review the ISE Authentication logs for proper authentication, authorization, and policy assignment.

- a. From the ISE admin interface, go to **Monitor > Authentications**.
- b. Review the log entries associated with the Win7-PC client 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.


Step 2 From the ISE admin interface, go to **Home** (Dashboard). Review the Posture Compliance dashlet including Compliance pass percentage and Mean-Time-To-Remediate values.



Step 3 Click the upper right corner of the dashlet to expand in a new window:



Step 4 Click the **OS** and **Reason** entries to display additional details.

Step 5 Go to **Monitor > 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 6 Click **Search**:

Search and Select a Posture event for troubleshooting.

Username: [Select](#) [Clear](#)

MAC Address: [Select](#) [Clear](#)

Posture Status: [Select](#) [Clear](#)

Failure Reason: [Select](#) [Clear](#)

Time Range:

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

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

Fetch Number of Records:

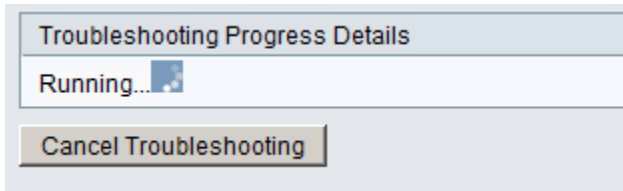
Search

Step 7 Select one of the pass/fail (green/red) entries and then click **Troubleshoot** at the bottom of the page:

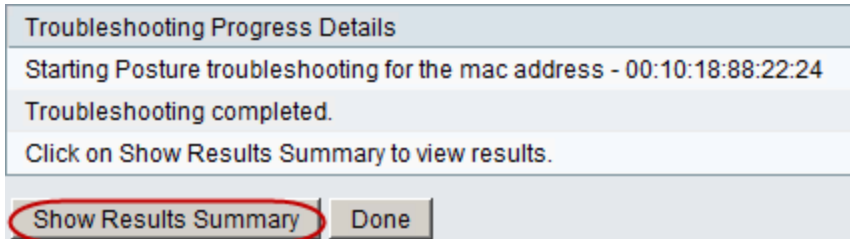
| Search Result | | | | | |
|----------------------------------|-------------------------|--------|-------------|-------------------|----------------|
| | Time | Status | Username | MAC Address | Failure Reason |
| <input type="radio"/> | 2011-03-30 05:52:36.804 | ✓ | contractor1 | 00:10:18:88:22:24 | |
| <input type="radio"/> | 2011-03-30 05:52:36.804 | ∅ | contractor1 | | |
| <input checked="" type="radio"/> | 2011-03-30 05:52:03.305 | ✗ | contractor1 | 00:10:18:88:22:24 | |
| <input type="radio"/> | 2011-03-30 05:52:03.305 | ∅ | contractor1 | | |

Troubleshoot

A message displays to indicate the status of the request:



Step 8 When processing is complete, a window similar to the following will display:



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:

Diagnosis and Resolution

Diagnosis

Details of policy(s) for Mac Address - 00:10:18:88:22:24

Posture policy - **Contractor_Windows AV Installed and Curren** - 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 Installed[Mandatory] | Passed | av_inst_ANY_vendo | None | None | LocalCheck(Predefined local check) |
| Guest_AV Current[Mandatory] | Failed | None | av_def_AN | None | LocalCheck(Predefined local check) |

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.

Troubleshooting Summary

✓ Investigated posture record with following details:

Show Progress Details Done

Step 9 Click **Done** to return to the Search page. Optionally enter new search criteria and repeat the steps to troubleshoot passed/failed posture events.

Step 10 Go to **Monitor > Reports > Catalog**. Select **Posture** from the left-hand pane:

Reports

Filter: Go Clear Filter

| Report Name | Type | Modified At |
|---------------------------|---------------|------------------------------|
| Posture Detail Assessment | System Report | Fri Jan 07 04:11:28 UTC 2011 |
| Posture Trend | System Report | Fri Jan 07 04:11:28 UTC 2011 |

Run Add To Favorite Delete

Step 11 Run the **Posture Detail Assessment** report and review the contents.

Step 12 Click the **Details** icon for any Failed (Red) posture entry. Review the overall details for the posture session. Review the requirements which passed and those that failed:

Posture > Posture Detail Assessment

Generated on February 6, 2011 5:11:50 AM UTC

✔=Compliant ✖=NonCompliant ⌚=Pending

| Client Details | |
|---------------------------|-----------------------------------|
| Username : | guse002 |
| Mac Address : | 00:50:56:B4:01:69 |
| Session ID : | 0A0164010000001A1058C122 |
| Client Operating System : | Windows 7 Enterprise 32-bit Intel |
| Client NAC Agent : | Cisco NAC Web Agent 4.9.0.6 |
| PRA Enforcement : | No |
| PRA Grace Time : | |
| PRA Interval : | |
| PRA Action : | |
| User Agreement Status : | Enabled |
| System Name : | WIN7-PC |
| System Domain : | demo.local |
| System User : | employee1 |
| User Domain : | DEMO |

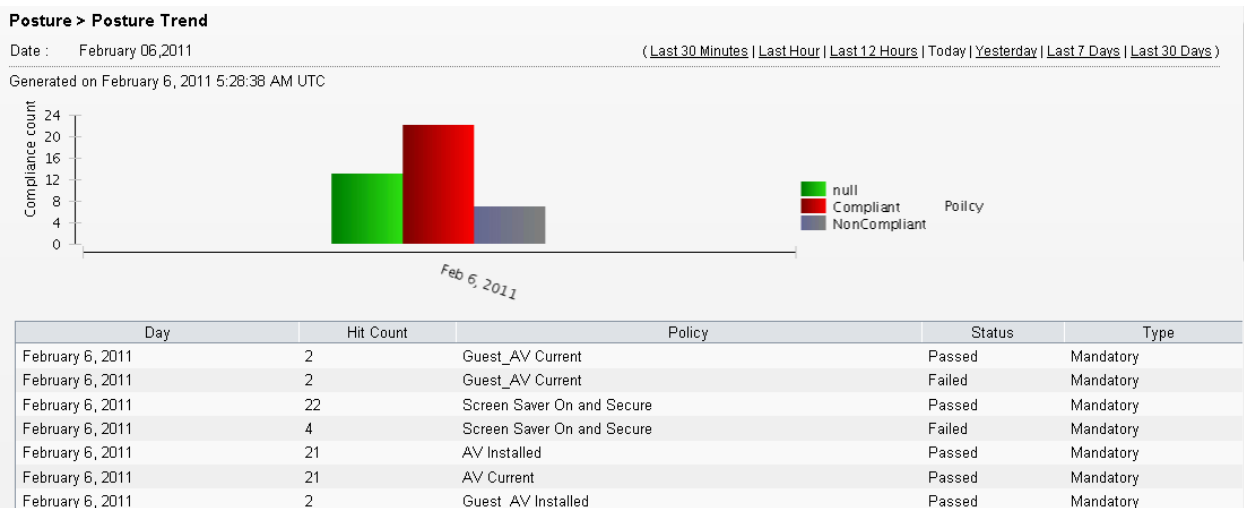
| AntiVirus Details | | | | |
|-------------------|------------------------|-----------------|--------------------|-----------------|
| Product Id | Product Name | Product Version | Definition Version | Definition Date |
| ClamAV | ClamWin Free Antivirus | 0.95.3 | | |

| AntiSpyware Details | | | | |
|---------------------|------------------|-----------------|--------------------|-----------------|
| Product Id | Product Name | Product Version | Definition Version | Definition Date |
| MicrosoftAS | Windows Defender | 6.1.7600.16385 | | |

| Posture Report | |
|-----------------|----------------------------|
| Posture Status: | NonCompliant |
| Logged At: | Feb 6, 2011 4:24:56.076 AM |

| Posture Policy Details | | | | | | |
|--|----------------------------|------------------|--------|---|-------------------|--------------------|
| Policy | Requirement | | | Passed Conditions | Failed Conditions | Skipped Conditions |
| | Name | Enforcement Type | Status | | | |
| Guest_Windows AV Installed and Current | Guest_AV Installed | Mandatory | Passed | av_inst_ANY_vendor | | |
| Guest_Windows AV Installed and Current | Guest_AV Current | Mandatory | Failed | | av_def_ANY | |
| Guest_ScreenSaver | Screen Saver On and Secure | Mandatory | Passed | ScreenSaver_Secure:ScreenSaver_On:ScreenSaver_Timeout:ScreenSaver_SCR | | |

Step 13 Select **Posture** again from the left-hand pane and run the **Posture Trend** report as shown:



This report provides an overall picture of posture compliance and non-compliance as well as the number of passes/failures by posture requirement.

End of Lab: Congratulations! You have successfully completed the lab. Please let your proctor know you finished and provide any feedback to help improve the lab experience.