No Failed Authentication Seen in ISE Live Logs
Verify
Troubleshoot

Introduction

This document describes posture services, client provisioning, posture policy creation, and access policy configuration for the Cisco Identity Services Engine (ISE). Endpoint assessment results for both wired clients (connected to Cisco switches) and wireless clients (connected to Cisco wireless controllers) are discussed.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Identity Services Engine (ISE)
- Cisco IOS® software switch configuration
- Cisco Wireless LAN Controller (WLC) configuration

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE Version 1.1.3
- Cisco Catalyst 3560 Series Switch Version 15.0(2) SE2
- Cisco 2504 Series WLC Version 7.4.100.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

ISE Posture Services

The posture services workflow is comprised of three main configuration sections:

- Client provisioning
- Posture policy
- Authorization policy

Client Provisioning

In order to perform posture assessment and determine the compliance state of an endpoint, it is necessary to provision the endpoint with an agent. The Network Admission Control (NAC) Agent can be persistent, whereby the agent is installed and is automatically loaded each time a user logs
in. Alternatively, the NAC Agent can be temporal, whereby a web-based agent is dynamically downloaded to the endpoint for each new session and then removed after the posture assessment process. NAC Agents also facilitate remediation and provide 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 which agent and configuration files are downloaded to endpoints, based upon attributes such as user identity and client OS type.

**Posture Policy**

The posture policy defines the set of requirements for an endpoint to be deemed compliant based upon file presence, registry key, process, application, Windows, and anti-virus (AV)/anti-spyware (AS) checks and rules. Posture policy is applied to endpoints based upon a defined set of conditions such as user identity and client OS type. The compliance (posture) status of an endpoint can be:

- **Unknown**: No data was collected in order to determine posture state.
- **Noncompliant**: A posture assessment was performed, and one or more requirements failed.
- **Compliant**: The endpoint is 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 are a logical group of one or more simple conditions. Each requirement is associated with a remediation action that helps endpoints satisfy the requirement, such as AV signature update.

**Authorization Policy**

The 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; for example, 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 with downloadable access control lists (dACLs) or dynamic VLAN assignment. In this configuration example, dACLs are used for endpoint access enforcement.

**Posture Example Workflow**

In this configuration example, both persistent (NAC Agent) and temporal (Web Agent) agent files are downloaded to ISE, and client provisioning policies are defined that require domain users to download the NAC Agent and guest users to download the Web Agent.

Before posture assessment policies and requirements are configured, the authorization policy is updated to apply authorization profiles to domain users and guests that are flagged as noncompliant. The new authorization profile defined in this configuration limits access to posture and remediation resources. Employees and guest users flagged as compliant are allowed regular network access. Once client provisioning services have been verified, posture requirements are configured in order to check for anti-virus installation, virus definition updates, and Windows critical updates.
**Note:** Verify all items on these endpoint and ISE checklists before you attempt to configure posture.

### Endpoint Checklist

1. ISE Fully Qualified Domain Name (FQDN) must be resolvable by the endpoint device.
2. Verify that the endpoint browser is configured as shown here:

   **Firefox or Chrome:** Java plugin must be enabled on the browsers. **Internet Explorer:** ActiveX must be enabled in the browser settings. **Internet Explorer 10:** Importing Self-Signed Certificate: If you are using a self-signed certificate for ISE, run Internet Explorer 10 in Administrator mode in order to install these certificates. **Compatibility Mode:** Compatibility mode must be changed on Internet Explorer 10 settings in order to allow NAC Agent download. In order to change this setting, right-click the blue bar at the top of the Internet Explorer 10 screen, and choose Command bar. Navigate to Tools > Compatability View settings, and add the ISE IP or FQDN to the site list. **Enabling ActiveX Control:** Cisco ISE installs the Cisco NAC Agent and Web Agent with the ActiveX control. In Internet Explorer 10, the option to prompt for ActiveX controls is disabled by default. Take these steps in order to enable this option: Navigate to Tools > Internet Options. Navigate to the Security tab, and click Internet and Custom Level. In the ActiveX Controls and Plugins section, enable Automatic Prompting for ActiveX controls.
3. If a firewall exists locally on the client or along the network path to the ISE, you must open these ports for ISE NAC communication:
   
   UDP/TCP 8905: Used for posture communication between NAC Agent and ISE (Swiss port). UDP/TCP 8909: Used for client provisioning. TCP 8443: Used for guest and posture discovery. **Note:** ISE no longer uses legacy port TCP 8906.
4. If the client has a proxy server configured, modify the proxy settings in order to exclude the IP address of the ISE. Failure to do so breaks the communications required for Central Web Authentication (CWA) and client provisioning.

### ISE Checklist

- Navigate to Administration > External Identity Sources > Active Directory, and verify that ISE is joined to the Active Directory (AD) domain.
- Click the Groups tab, and verify that the Domain Users group is added to AD configuration.
- Navigate to Administration > Network Resources > Network Devices, and verify that the switch and WLC are defined as Network Access Devices (NAD).
- Under Policy > Authentication, ensure the dot1x and MAC Authentication Bypass (MAB) rules are configured as described here:

  Dot1x authentications for wired and wireless clients are sent to AD Identity Store.
MAB authentications for wired and wireless devices are sent to internal endpoints; be sure to check the option **If user not found CONTINUE**.

### Configure ISE

**ISE Configuration Overview**

This example ISE configuration is comprised of these steps:

1. Configure and deploy client provisioning services.
2. Configure authorization policies.
3. Configure posture policies.

#### Configure and Deploy Client Provisioning Services

1. Verify the ISE proxy configuration.

   Navigate to **Administration > System > Settings > Proxy**. If a proxy is required for Internet access, complete the server and port details.

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

   Navigate to **Administration > System > Settings > Posture > Updates**. The Update Information in the bottom right-hand pane should be empty since no updates have been downloaded yet. Configure these values:

   Click **Update Now**, and acknowledge the warning that the updates may take some time to complete.
Note: If ISE does not have Internet access, offline posture updates are available for
download on Cisco.com.
3. (Optional) Configure general settings for agent behavior.

Select Administration > System > Settings > Posture > General Settings, and review the
default values for the Remediation Timer, Network Transition Delay, and Default Posture
Status. Set the Remediation Timer to 8 minutes. Check (enable) the Automatically Close
Login Success Screen After checkbox, and set time to 5 seconds as shown here:

Click Save.
Note: Values assigned through the agent profile override these global settings. Default
posture status defines the status for clients that do not have a NAC Agent installed. If client
provisioning is not being used, this value can be set to noncompliant.
4. Set the location and policy to download client provisioning updates.

Click Administration > System > Settings > Client Provisioning from the left-hand pane,
and verify that these default values are set:

5. Download the agent files.

Navigate to Policy > Policy Elements > Results, expand the Client Provisioning folder,
and select Resources. From the right-hand pane, click Add > Agent Resources from Cisco
site from the drop-down list. A pop-up window displays the remote resources:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ComplianceModule 3.5.598U.2</td>
<td>ComplianceModule</td>
<td>3.5.598U.2</td>
<td>ComplianceModule v.3.5.598U.2</td>
</tr>
<tr>
<td>MacOSXAgent 4.9.0.654</td>
<td>MacOSXAgent</td>
<td>4.9.0.654</td>
<td>Posture Agent for Mac OSX ISE ...</td>
</tr>
<tr>
<td>MacOSXAgent 4.9.0.655</td>
<td>MacOSXAgent</td>
<td>4.9.0.655</td>
<td>Posture Agent for Mac OSX ISE ...</td>
</tr>
<tr>
<td>MacOSXAgent 4.9.0.659</td>
<td>MacOSXAgent</td>
<td>4.9.0.659</td>
<td>Posture Agent for Mac OS X v.4.3 ...</td>
</tr>
<tr>
<td>MacOSXGPWizard 1.0.0.11</td>
<td>MacOSXGPWizard</td>
<td>1.0.0.11</td>
<td>Supplicant Provisioning Wizard f...</td>
</tr>
<tr>
<td>MacOSXGPWizard 1.0.0.18</td>
<td>MacOSXGPWizard</td>
<td>1.0.0.18</td>
<td>Supplicant Provisioning Wizard f...</td>
</tr>
<tr>
<td>NACAgent 4.9.0.37</td>
<td>NACAgent</td>
<td>4.9.0.37</td>
<td>Windows Agent (ISE 1.0MR only)</td>
</tr>
<tr>
<td>NACAgent 4.9.0.42</td>
<td>NACAgent</td>
<td>4.9.0.42</td>
<td>Windows Agent (ISE 1.1.1 or later)</td>
</tr>
<tr>
<td>NACAgent 4.9.0.47</td>
<td>NACAgent</td>
<td>4.9.0.47</td>
<td>Windows Agent with Win 8 OS ...</td>
</tr>
<tr>
<td>NACAgent 4.9.0.51</td>
<td>NACAgent</td>
<td>4.9.0.51</td>
<td>Windows Agent (ISE 1.1.3 Release)</td>
</tr>
<tr>
<td>WebAgent 4.9.0.20</td>
<td>WebAgent</td>
<td>4.9.0.20</td>
<td>Web Agent (ISE 1.0MR only)</td>
</tr>
<tr>
<td>WebAgent 4.9.0.24</td>
<td>WebAgent</td>
<td>4.9.0.24</td>
<td>Web Agent (ISE 1.1.1 or later)</td>
</tr>
<tr>
<td>WebAgent 4.9.0.27</td>
<td>WebAgent</td>
<td>4.9.0.27</td>
<td>Web Agent with Win 8 OS support ...</td>
</tr>
<tr>
<td>WebAgent 4.9.0.28</td>
<td>WebAgent</td>
<td>4.9.0.28</td>
<td>Web Agent (ISE 1.1.3 release)</td>
</tr>
<tr>
<td>WinISPWizard 1.0.0.22</td>
<td>WinISPWizard</td>
<td>1.0.0.22</td>
<td>Supplicant Provisioning Wizard f...</td>
</tr>
</tbody>
</table>

At a minimum, select the current NAC Agent, Web Agent, and Compliance Module (AV/AS
support module) from the list, and click Save. The client provisioning file types are:
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. Wait until the files are downloaded to the ISE appliance.

6. (Optional) Create a NAC Agent configuration profile for your clients.

From the right-hand pane, click Add, then select ISE Posture Agent Profile from the drop-down list. Modify the profile in order to satisfy the deployment requirements.

The merge option updates the current agent profile parameter only if no other value is defined. The overwrite option updates the parameter value whether explicitly defined or not. For a complete list of configurable NAC Agent parameters, refer to the Cisco Identity Services Engine User Guide, Release 1.1.x.

7. Define the client provisioning policy for domain users and guest users.

Navigate to Policy > Client Provisioning. Add two new client provisioning rules as outlined in this table. Click the ACTIONS button to the right of any rule entry in order to insert or duplicate rules.

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 when you configure the rule. Click Save when finished.

8. Configure the web authentication portal in order to download the posture agent as defined by the client provisioning policy.

Navigate to Administration > Web Portal Management > Settings, expand the Guest folder, select Multi-Portal Configurations, and select DefaultGuestPortal. Under the Operation tab, enable the option in order to allow guest users to download agents and to self register.

Define a Self Registration Guest Role and Self Registration Time Profile as shown here. Guest self service is an optional configuration that lets users create accounts without sponsor intervention. This example enables self service in order to simplify the guest registration process.

(Optional) Set the AUP for guest users as shown here:

Click Save when finished.
Configure Authorization Policy for Client Provisioning and Posture

The authorization policy sets the types of access and services to be granted to endpoints based upon their attributes such as identity, access method, and compliance with posture policies. The authorization policies in this example ensure that endpoints that are not posture compliant are quarantined; that is, the endpoints are granted limited access sufficient to provision agent software and to remediate failed requirements. Only posture compliant endpoints are granted privileged network access.

1. (Optional). Define a dACL that restricts network access for endpoints that are not posture compliant.

Navigate to Policy > Policy Elements > Results, expand the Authorization folder, and select Downloadable ACLs. Click Add from the right-hand pane under DACL Management, and enter these values for the new dACL.

This is a sample posture dACL. Review dACL entries for accuracy, because ISE 1.1.x does not currently support ACL syntax validation.

Click Submit when completed.

2. Define a new authorization profile for 802.1X-authenticated/NAC Agent users named Posture_Remediation. The profile leverages both the new dACL for port access control and the URL redirect ACL for traffic redirection.

Navigate to Policy > Policy Elements > Results > Authorization, and select Authorization Profiles. Click Add from the right-hand pane, and enter these values for the authorization profile:

These resultant attribute details should appear at the bottom of the page:

Access Type = ACCESS_ACCEPT
DACL = POSTURE_REMEDIATION
cisco:cisco-av-pair=url-redirect-acl=ACL-POSTURE-REDIRECT
cisco:cisco-av-pair=url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionIdValue@action=cpp
Click Submit in order to apply your changes.

Note: The ACL-POSTURE-REDIRECT ACL must be configured locally on the switch or WLC. The ACL is referenced by name in the ISE authorization policy. For the switch redirect ACL, the permit entries determine what traffic should be redirected to ISE whereas, on a WLC, the permit entries define what traffic should not be redirected.

3. Define a new authorization profile for web-authenticated/Web Agent users named CWA_Posture_Remediation. The profile leverages both the new dACL for port access control and the URL redirect ACL for traffic redirection.

Navigate to Policy > Policy Elements > Results > Authorization, and select
Authorization Profiles. Click Add from the right-hand pane, and enter these values for the authorization profile:

These resultant attribute details should appear at the bottom of the page:

Access Type = ACCESS_ACCEPT
DACL = POSTURE_REMEDIATION
cisco:cisco-av-pair=url-redirect-acl=ACL-POSTURE-REDIRECT
cisco:cisco-av-pair=url-redirect=https://ip:8443/guestportal/gateway?sessionId=SessionIdValue@action=cwa

Click Submit in order 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 are redirected to the guest portal for CWA. Once authenticated, users are automatically redirected to the CPP as needed. Users authenticated through 802.1X are redirected directly to the CPP.

4. Update the authorization policy in order to support posture compliance.

Navigate to Policy > Authorization. Update the existing Authorization Policy with these values. Use the selector at the end of a rule entry in order to insert or duplicate rules:

Click Save in order to apply your changes.

Note: This authorization profile is applied to both wired and wireless user access. The WLC does not take into consideration the dACL. The dACL feature is supported only on switches. For wireless, the redirect ACL is enough to deny all traffic except for remediation server and ISE posture.

Configure AV Posture Policy

This example shows how to define an AV policy with these posture conditions:

- Posture policy for domain users to have ClamWin AV installed and current.
- Posture policy for guest users to install ClamWin AV if no anti-virus is installed.

1. 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.

Navigate to Policy > Policy Elements > Conditions, expand the Posture folder, and select AV Compound Condition. Click Add from the right-hand pane menu. If no AV products appear under Vendor field, posture updates have not yet been downloaded or the download has not yet completed. Enter these values:

Click Submit at the bottom of the page.

2. 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 click Add from the right-hand pane menu. Enter these values:

Click Submit at the bottom of the page.

3. 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 click Add from the right-hand pane menu. Enter these values:

Click Submit at the bottom of the page.

4. Define a posture remediation action that installs ClamWin AV on an endpoint.

Navigate to Policy > Policy Elements > Results, and expand the Posture folder. Expand the contents of Remediation Actions. Select Link Remediation, and click Add from the right-hand pane menu. Enter these values:

Click Submit.

Note: REM SERVER IP represents the IP address of your remediation server where the installation of ClamWin exists. The executable file in this example was pre-positioned on the remediation server. For remediation to work, ensure that the ClamWin update server IP is included in the previously configured dACL and redirect ACL.

5. Define a posture remediation action that updates ClamWin AV on an endpoint.

Select AV/AS Remediation from the left-hand pane, and click Add from the right-hand pane menu. Enter these values:

Click Submit.

6. Define posture requirements that will be applied to employees and guest users.

Select Requirements from Policy > Policy Elements > Results > Posture. Enter these entries into the table. Use the selector at the end of a rule entry in order to insert or duplicate rules:

Click Save when finished.

Note: If a preconfigured condition does not display under the list of conditions, verify that the appropriate OS has been selected for both the condition as well as the requirement rule. Only conditions that are the same or are a subset of the OS selected for the rule display in the conditions selection list.

7. Configure the posture policy in order to ensure that ClamWin AV is installed and current on employee computers with Windows 7 and that any supported AV is installed and current on guest user computers.

Navigate to Policy > Posture, and create new policy rules with the values provided in this table. In order to specify a posture requirement as Mandatory, Optional, or Audit, click the
icon to the right of the requirement name, and choose an option from the drop-down list.

Click **Save** in order to apply your changes.

**Configure WSUS Remediation**

This example shows how to ensure that all employee computers with Windows 7 have the latest critical patches installed. Windows Server Update Services (WSUS) are internally managed.

1. Define a posture remediation action that checks for and installs the latest Windows 7 patches.

Navigate to **Policy > Policy Elements > Results**, and expand the **Posture** folder. Expand the contents of **Remediation Actions**. Select **Windows Server Update Remediation**, and click **Add** from the right-hand pane menu. Enter these values, and click **Submit**:

   **Note:** If you want to use Cisco rules in order to validate Windows update, create your posture conditions, and define your conditions in Step 2.

2. Define posture requirements that will be applied to employees.

Navigate to **Policy > Policy Elements > Results > Posture**, and select **Requirements**. Enter these entries into the table. Use the selector at the end of a rule entry in order to insert or duplicate rules:

   **Note:** You can find condition **pr_WSUSRule** under **Cisco Defined Condition > Regular Compound Condition**. (This is a dummy rule chosen because Step1 set the Windows updates to be validated by Severity Level.)

3. Configure the posture policy in order to ensure that employee computers with Windows 7 have the latest critical Windows 7 patches.

Navigate to **Policy > Posture**, and create new policy rules with the values in this table:

   Click **Save** in order to apply your changes.

**Sample Switch Configuration**

This section provides an excerpt of the switch configuration. It is intended for reference only and should not be copied or pasted into a production switch.

**Global Radius and Dot1x Configuration**

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
dot1x system-auth-control
```
ip radius source-interface Vlan (x)
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server host <ISE IP> key <pre shared key>
radius-server vsa send accounting
radius-server vsa send authentication

Default ACL to be Applied on the Port

ip access-list extended permitany
permit ip any any

Enable Radius Change of Authorization

aaa server radius dynamic-author
client <ISE IP> server-key <pre shared key>

Enable URL Redirection and Logging

Ip device tracking
Epim logging
Ip http server
Ip http secure server

Redirection ACL

ip access-list extended ACL-POSTURE-REDIRECT
deny udp any eq bootpc any eq bootps
deny udp any any eq domain
deny udp any any host <ISE IP> eq 8905
deny tcp any any host <ISE IP> eq 8905
deny tcp any any host <ISE IP> eq 8909
deny udp any any host <ISE IP> eq 8909
deny tcp any any host <ISE IP> eq 8443
deny tcp any any host <REM SERVER IP>
deny ip any any host 192.230.240.8 (one of the ip of CLAMwin database virus Definitions)
permit ip any any

Note: The IP address of the endpoint device must be reachable from the switch virtual interface (SVI) in order for redirection to work.

SwitchPort Configuration

switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
Sample WLC Configuration

Global Configuration

1. Ensure that the RADIUS server has RFC3576 (CoA) enabled; it is not enabled by default.

2. Navigate to Security > Access Control Lists, create an ACL on the WLC and call it 'ACL-POSTURE-REDIRECT.'

15 and 16 are used in this example for ClamWin AV update where 192.230.240.8 contains the database definition file.

For FlexConnect with Local Switching, you must create a FlexConnect ACL, and apply it to the WebPolicy ACL. The ACL has the same name as the ACL on the WLC and has the same attributes.

1. Click FlexConnect ACLs.
2. Click **External WebAuthentication ACLs**.

3. Add the WebPolicy ACL.

4. Click **Apply**.
Employee SSID Configuration

Create a new employee Service Set Identifier (SSID) or modify the current one.

1. In the WLAN tab, click Create New or click an existing WLAN.

2. Click the Security tab, click the Layer 2 tab, then set the appropriate security. Here is a configuration of WPA with dot1x.

3. Click the AAA Servers tab, and check (enable) the ISE as the Radius Server for both Authentication and Accounting.

4. Click the Advanced tab, check (enable) the Allow AAA Override and the DHCP Addr. Assignment checkboxes, and set the NAC State to Radius NAC.
Guest SSID Configuration

Create a new WLAN with guest SSID or modify a current one.

1. In the WLAN tab, click Create New or click an existing WLAN.

2. Click the Security tab, click the Layer 2 tab, then check (enable) the MAC Filtering checkbox.

3. Click the Layer 3 tab, and ensure all options are disabled.
4. Click the **AAA Servers** tab, and check (enable) the ISE as both an Authentication Server and an Accounting Server.

5. Click the **Advanced** tab, check (enable) the **Allow AAA Override** and the **DHCP Addr. Assignment** checkboxes, and set the **NAC State** to Radius NAC.

**Employee Dot1x Posture (NAC Agent)**
This is the procedure of the posture itself from a client perspective, once the client connects to the WLANs previously configured.

1. Configure your wireless SSID (employee) or wired network for PEAP MSCHAP V2, and connect with an AD user in the domain user group.
2. Open a browser, and try to navigate to a site. A redirect prompt is displayed.
3. Click **Click to Install Agent**.

4. Click **Next**.

5. Click **I accept the terms of the license agreement**, and click **Next**.
6. Click **Complete**, and click **Next**.

7. Click **Install**.
8. Select **Finish**.

9. Once installation is complete, the NAC Agent pops up. Click **Show Details**.
The output shows that ClamWin is not installed and is not updated. Some Windows critical updates are not installed.

10. Click **Go To Link** in order to install the anti-virus from the remediation server.
11. Click **Run**, and proceed with ClamWin AV installation.

12. After the anti-virus is installed, the NAC Agent prompts for updates. Click **Update** in order to get the latest virus definition file. When the same screen is presented a second time, click **Update** again in order to install the Windows updates.
The NAC Agent contacts your WSUS in order to check for and install the latest critical updates.

13. Click **Restart Now** in order to complete the update.
14. After the restart, the system is compliant.
Guest CWA Posture (NAC Web Agent)

This is the procedure that users perform, once they connect to the guest SSID with posture enabled.

1. Connect to your Guest SSID, or do not configure dot1x on your wired network.
2. Open a browser, and try to navigate to a site.
3. The browser is redirected to the guest portal.
4. Click **Self registration**, and proceed with authentication.
5. Click **Accept** in order to accept the AUP.
6. Select **Click to install agent**.
7. Click **Click here to remediate**.

8. Click **Run**, and proceed with anti-virus installation.
The PC is now found to be compliant.

9. Check the ISE authentication logs in order to verify that dynamic authorization succeeded and that you are matching the authorization profile related to the compliant status.
Frequently Asked Questions

Deployment Options Other than Client Provisioning

Refer to Cisco Identity Services Engine User Guide, Release 1.1x: Provisioning Client Machines with the Cisco NAC Agent MSI Installer.

Discovery Host for the NAC Agent

The NAC Agent reaches the right ISE Policy Decision Point (PDP) in different ways, depending upon whether the discovery host is defined:

1. If no discovery host is defined: The NAC Agent sends HTTP request on port 80 to the gateway; this traffic must be redirected to the posture discovery link (CPP) in order for discovery to work properly.
2. If a discovery host is defined: The NAC Agent sends HTTP request on port 80 to the host; this traffic must be redirected to the posture discovery link (CPP) in order for discovery to work properly. If there is a problem with redirection, the NAC Agent tries to directly contact the discovery host defined on port 8905; posture validation is not guaranteed, because the session information may not be available on that PDP unless node groups are defined, and the PDP is within the same group.
3. If the discovery host cannot be reached at all, NAC Agent falls back to the method 1, so tries to contact with the default gateway.

Choosing the Discovery Host, one should take into the consideration, that the initial traffic from the NAC Agent towards the Discovery Host should be visible to the PDP. So, good choices could be: PDP address itself, non-existent host in the same subnet as PDP nodes.

Employee Browsers are Configured with Proxy

1. If you are not using client provisioning and the employee PCs are configured with proxy, there is no need for changes since the posture discovery packets are sent on port 80 and bypass the proxy settings.
2. If you are using the client provisioning service, make these changes to the switch configuration and to the WLC in order to intercept HTTP traffic on the defined port of the proxy (here 8080 in this example) if the proxy is not on port 80.

   • Proxy Configuration on port 8080 on the switch:

     ```
     switchport access Vlan xx
     switchport voice Vlan yy
     switchport mode access
     dot1x pae authenticator
     authentication port-control auto
     ```
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab

switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab

- Proxy Configuration WLC. By default, the WLC intercepts HTTP requests with destination TCP port 80 only. This command must be configured through the command-line interface (CLI) if you want to intercept other HTTP traffic on port 8080:

switchport access Vlan xx
switchport voice Vlan yy
switchport mode access
dot1x pae authenticator
authentication port-control auto
authentication host-mode multi-domain
authentication violation restrict
ip access-group permitany in (Note: This is mandatory for dACL for versions of Cisco IOS earlier than Release 12.2(55)SE.)
dot1x timeout tx-period 7
authentication order dot1x mab
authentication priority dot1x mab
mab

Note: Switches allow redirection on one port. Therefore, if you specify another port for switch redirection, posture discovery fails, and posture traffic is sent to the discovery host defined in the NACAgentCFG.xml (the NAC Agent profile).

**dACL and Redirection ACL**

Redirection ACL is mandatory for client provisioning, Central Web Authentication, and Posture Discovery. However, dACL is used in order to limit network access and is applied only to non-redirected traffic.

In order to resolve this situation, you can:

1. Define only a redirection ACL, and redirect all the traffic that you want to be dropped (as done in the example).
2. Define a redirection ACL that is less restrictive, and apply a dACL that filters the traffic that is not redirected.
3. Define a redirection ACL, and apply a VLAN that restricts network access. This is the best approach because VLAN traffic can be filtered by an application-aware firewall.

**NAC Agent Does Not Pop Up**

1. Check ISE live authentication, and verify that authentication matches your posture authorization profile.
2. From the client PC, open cmd. Type `nslookup`, and verify you can resolve ISE PDP hostname.

If all of these steps are successful and if your switch or WLC configuration complies with this document, your next steps should be:

- Use Wireshark in order to start a capture on the PC.
- Restart NAC Agent service.
- Collect Cisco Log Packager.
- Locate NACAgentCFG.xml in the NAC Agent directory.
- Contact Cisco TAC once you have gathered the packet capture, NAC Agent logs, NACAgentCFG configuration file, and Windows Event Viewer logs.

**Unable to Access WSUS for Remediation**

If you are using WSUS 3.0 SP2 and the NAC Agent is unable to access WSUS Windows updates, verify that you have the latest patch of WSUS installed. This patch is mandatory for Windows clients in order to browse updates from WSUS.

Verify that you are able to access this file: `http://ip wsus/selfupdate/iuident.cab`.

Refer to the [Windows Server Update Services 3.0 SP2 Step By Step Guide](#) for additional information.

**Do Not Have an Internal Managed WSUS**

You can still use Windows Update Servers while you configure your posture remediation rule.

Client must be allowed to access these sites, so these URLs must not be redirected:

- `http://windowsupdate.microsoft.com`
- `http://*.windowsupdate.microsoft.com`
- `https://*.windowsupdate.microsoft.com`
- `http://*.update.microsoft.com`
- `https://*.update.microsoft.com`
- `http://*.windowsupdate.com`
- `http://download.windowsupdate.com`
- `http://*.download.windowsupdate.com`
- `http://wustat.windows.com`
- `http://ntservicepack.microsoft.com`
- `http://stats.microsoft.com`
No Failed Authentication Seen in ISE Live Logs

You might be tempted to create an authorization policy rule that triggers on the condition of a noncompliant client in order to restrict access. However, you will not see that the authentication attempt fails until the remediation timer expires, especially when you are using the Web Agent. In fact, the agent notices the noncompliance and starts the remediation timer.

The ISE is notified that the posture was a failure only when the remediation timer expires or the user clicks Cancel. Therefore, it is a good practice to give a default access to all clients that allows for remediation but blocks any other form of access.

Verify

Some verification procedures are included in the preceding sections.

Troubleshoot

Some troubleshooting procedures are included in the preceding sections.