ClearPass NAC and Posture Assessment for Campus Networks

Configuring ClearPass OnGuard, Switching, and Wireless (v1.0)

Dell Network Solutions Engineering
September 2015

A Dell EMC Deployment and Configuration Guide

Revisions

Date	Version	Description	Authors
September 2015	1.0	Initial release	Dell_Networking_Solutions@Dell.com

Table of contents

1 Introduction

Dell Networking provides customers with the most efficient use of modern networking equipment at the lowest cost for Data Center, Campus and Remote networks. Dell Servers, Storage and Networking products with Dell Solutions and Services enable organizations achieve unique business goals, improve competitiveness and better serve their customers.

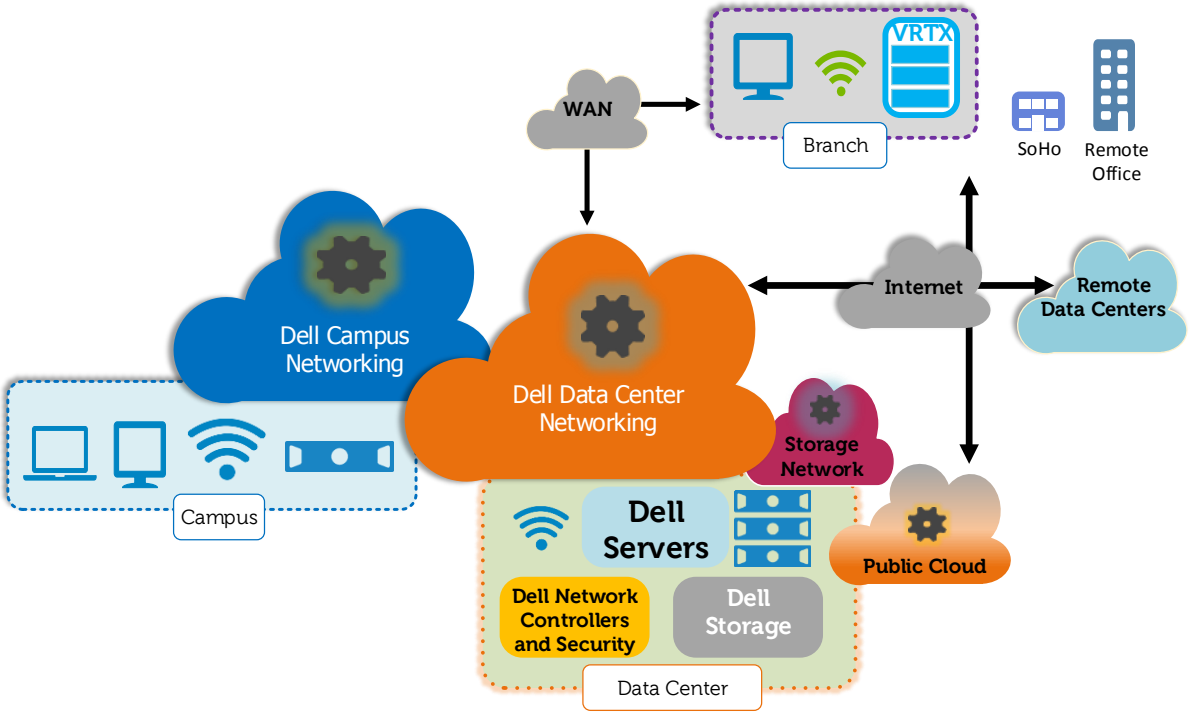

Figure 1 Comprehensive Modern Network

Dell Campus Networking solutions provide fast, efficient and secure wired and wireless access to help you meet new application and service delivery requirements.

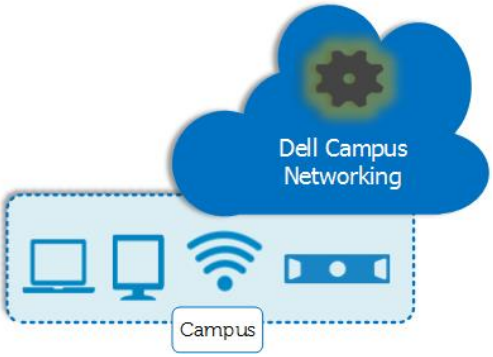

Figure 2 Campus Network

Dell Networking N-Series switches and W-Series wireless networking and access management products provide solutions for Network Access Control (NAC) with posture assessment. While typically categorized as Campus Networking, these features can also extend into the Remote and Branch Office.

The Dell Networking W-Series ClearPass Access Management System is a comprehensive solution for policy management, Bring Your Own Device (BYOD) and guest access. The W-ClearPass OnGuard module can provide advanced endpoint posture assessments and health checks to help ensure security compliance and network protection. Dell Networking provides exceptional feature integration with N-Series switches and W-Series wireless products. This document highlights the key features necessary to deliver a Network Access Control (NAC) solution for customers deploying health and posture compliance.

This deployment guide is designed to lead a network administrator through the design and configuration of network access services and features for several Dell Networking products. Specifically, this guide is focused on the integration of the W-ClearPass Access Management product with the Dell Networking N-Series switches and W-Series WLAN products.

The examples in the following sections are designed to demonstrate the basic configuration necessary to enable OnGuard. An administrator should use these configuration steps as a base, adding the specific security and policy requirements that are required by their organization. While the example networks are simplified, these solutions can scale to any size network.

2 Campus Network Solution

2.1 Campus Networking Topology

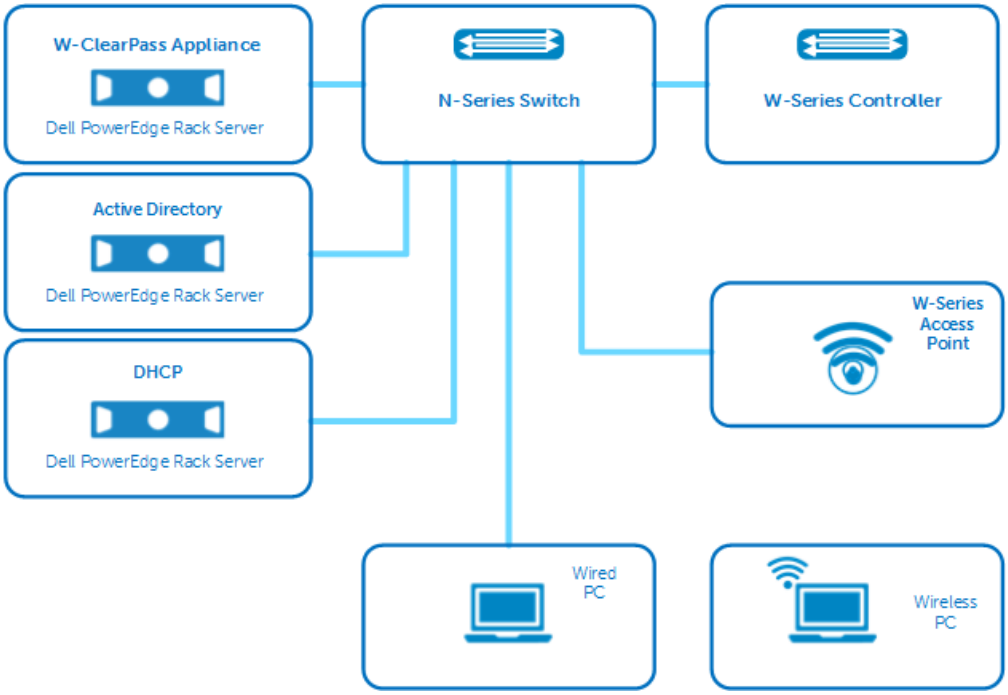

Figure 3 Campus Network, Wired and Wireless

The topology above (Figure 3) shows a complete wired plus wireless solution. The NAC and posture examples in sections 3, 4 and 5 can be used independently or they can work in unison for a complete solution.

2.2 W-ClearPass Access Management System

At the center of the access management system is the W-ClearPass Policy Manager. The ClearPass Policy Manager is a comprehensive policy management solution that can secure next-generation mobility services, enhance network access security and compliance and streamline network operations for wired, wireless and virtual private network (VPN) environments. Specific network access privileges can be based on user role, device type, health of endpoint, time-of-day and more.

The W-ClearPass OnGuard application is used with the Policy Manager to enable advanced posture assessments and health checks of devices that are on the network or requesting access to the network. OnGuard can be used as a persistent client application or a dissolvable client (i.e. a client that does not require permanent installation) that is used at the time of network access.

2.3 Networking Equipment and Features Utilized

2.3.1 N-Series Switches

The N-Series is a family of energy-efficient and cost-effective 1GbE and 10GbE switches designed for modernizing and scaling network infrastructure. The variety of models and options, including PoE+, makes these switches an optimal choice for access switches in any campus environment.

RADIUS Change of Authorization (RADIUS CoA)

Radius CoA enables W-ClearPass OnGuard to detect changes in posture and automatically enforce policies without the need to force a disconnect. This allows the user to maintain connectivity while issues with their device are assessed. Dell Networking N-Series Firmware Version v6.2, introduced this key feature to enable a better NAC and posture assessment with W-ClearPass OnGuard. This document contains examples validated using firmware version 6.2.6.6.

N-Series switches capable of running the v6.2.6.6 firmware include:

- N1500 Series
- N2000 Series
- N3000 Series
- N4000 Series

For further information on the N-Series line of switching products, see www.dell.com/networking.

2.3.2 W-Series Controllers, Access Points, and Instant Access Points

W-Series wireless networking products include a wide variety of solutions to enable wireless networking access. Controller based products offer high performance, fully featured solutions to satisfy any size business. Controller-less W-Instant Access Point (W-IAP) products offer many of the same features in a simple to use and affordable solution. Both controller-based and W-IAP solutions offer integration with W-ClearPass for unmatched access and policy control of wireless devices.

For further information on the W-Series line of wireless networking products, see www.dell.com/wireless

3 Wired Access with Dell N-Series

3.1 Topology

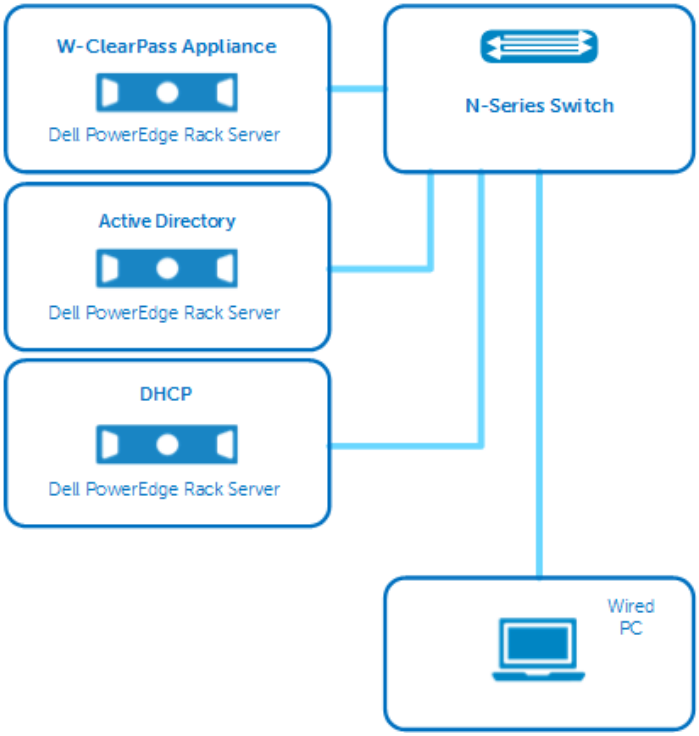

Figure 4 Wired Topology

3.2 Example Scenario - Wired

The following example details a typical scenario involving a user requiring wired access to a corporate or guest network. Posture compliance with OnGuard is the key feature demonstrated.

In this scenario, a user requires network access with a device not supplied by a corporate IT department and is connecting to network via a wired Ethernet connection.

1. The user connects to the network via a wired Ethernet connection.
2. The user is prompted for credentials to access the network.
3. W-ClearPass authenticates the user's credentials.
4. W-ClearPass detects if OnGuard has been installed and if the device is healthy.
   a. If OnGuard is installed and the device is healthy, W-ClearPass places the user in the appropriate vlan.
   b. If OnGuard is installed and the device is not healthy, W-ClearPass places the user in a quarantine vlan.
   Users are automatically re-authenticated and placed into the appropriate vlan, once the issue is resolved. In some cases, auto-remediation can perform changes without user action.

c. If OnGuard has not been installed, the user is manually directed to a webpage to run a one-time scan, or to install the OnGuard persistent client.
   OnGuard scans the device and determines if the client is compliant with the health policy.
   i. If healthy, W-ClearPass places the user in the appropriate vlan.
   ii. If not healthy, W-ClearPass places the user in a quarantine vlan
   Users are automatically re-authenticated once the issue is resolved and placed into the appropriate vlan. In some cases, auto-remediation can perform changes without user action.

The above scenario can be used for any type of guest or employee network. The example in this paper uses a single employee vlan and a quarantine vlan. Administrators can setup W-ClearPass to assign users to different vlans to support guest networks, contractor networks, or multiple employee group vlans.

This example uses username/password credentials that are stored in a Windows Server Active Directory. Any type of authentication, including certificates, can be used with OnGuard posture policies. This guide does not go into detail on configuring authentication types. For further information on BYOD topics through Onboard and Guest access, please see the W-ClearPass User Guide or other available deployment guides at www.dell.com/support.

The configuration examples in sections 3.3 and 3.4 detail a basic solution utilizing W-ClearPass OnGuard and an N-Series switch. All the scenarios presented contain a policy decision and enforcement based on posture information from OnGuard.

The configuration for the N-Series switch remains the same regardless of the type of OnGuard client or OS used. The configuration for W-ClearPass differentiates between the following combinations of OnGuard client types and PC OS:

- OnGuard Persistent application
- OnGuard Dissolvable application
- Windows 7/8
- Mac OSX
- Linux Ubuntu

The solution utilizes a webpage hosted by W-ClearPass for access to both OnGuard application types for employees and guests scenarios. In scenario step 4c, the user is given the URL to this webpage manually. See the Creating an OnGuard Landing Webpage section for details.

3.3 Dell N-Series Configuration - Wired

Note: The following configuration commands are not intended to comprise the full configuration needed for a fully functional access switch. The commands below contain the key configurations needed to enable the features described in this document. See the attached configuration file (N-Series Configuration example.txt) for the running-config.

N3048P configuration commands	Description of commands
configure vlan 6,8 exit ip routing	← Create 2 VLANs, one for employee (vlan 6) and another for quarantine (vlan 8).
interface vlan 1 ip address 172.25.172.47 255.255.0.0 exit	← Configure IP address. Vlan 1 is used for corporate resource traffic.
interface vlan 6 ip address 10.1.6.2 255.255.255.0 ip dhcp relay information option-insert exit	← Configure IP address. Vlan 6 is used for employee traffic. ← Configure dhcp relay to enable circuit ID option (option 82).
interface vlan 8 ip address 10.1.8.2 255.255.255.0 ip dhcp relay information option-insert exit	← Configure IP address. Vlan 8 is used for quarantined employee traffic. ← Configure dhcp relay to enable circuit ID option (option 82)
ip dhcp relay information option	← Configure global dhcp relay to enable circuit ID option (option 82).
ip helper-address 172.25.172.189 dhcp	← Configure global relay of DHCP UDP packets to corporate DHCP server address.
dot1x system-auth-control aaa authentication dot1x default radius aaa authorization network default radius	← Configure to enable dot1x authentication. ← Specifies authentication method. ← Specifies authorization method.
aaa server radius dynamic-author client 172.25.172.188 server-key "radius_key" auth-type any exit	← Configure system to begin listening for RADIUS CoA requests. ← Configure shared secret key used for RADIUS CoA requests. ← Configure accepted authorization types.
radius-server host auth 172.25.172.188 name "Default-RADIUS-Server" source-ip 172.25.172.47 usage 802.1x key "radius_key" exit	← Configure to specify a RADIUS server. ← Descriptive name (default). ← Specify a source ip address used with the RADIUS server. ← Specify usage type. ← Configure shared secret used for the RADIUS server.

Note: This example uses a single switch for Layer2 and Layer3 traffic. Some of the commands shown above, particularly for the DHCP relay feature, may not be required on the access switch being used. Commands unique to the interface ports are not shown. For more detail, see the attached configuration file.

3.4 Dell W-ClearPass Configuration - Wired

W-ClearPass is configured using the ClearPass GUI through a standard browser. This guide presents the key steps necessary to configure the example scenario. To improve readability, the included screenshots do not

show the entire browser. In most cases, the navigation window on the left hand side of the screen is not shown. To ensure readers understand the configuration location currently shown, the navigation path is provided in the configuration steps. In the screenshots, the current tab is highlighted with a dark blue color.

W-ClearPass allows administrators to configure policies and profiles directly from the main service configuration screen. When using this method of configuration, the necessary windows are opened automatically, which can streamline the amount of time it takes an experienced user to configure a fully functional service. In this guide, each profile and policy will be built prior to the creation of the service to aid in the description of navigating the configuration provided in this document.

Note: This guide does not detail the initial setup of the W-ClearPass server. For more information on VM installation, initial server configuration and licensing, refer to the W-ClearPass User Guides at www.dell.com/support.

Figure 5 W-ClearPass Welcome Screen

The W-ClearPass welcome screen (Figure 5) is the main screen used to navigate to each W-ClearPass application. W-ClearPass Policy Manager is at the core of the solution and is the focus of most of this document. For more information on each of the W-ClearPass applications, see the W-ClearPass User Guide at http://www.dell.com/support.

3.4.1 Add the N-Series Switch as a Network Device

Before W-ClearPass will recognize authentication requests, the switch originating the request must be added to the list of network devices in W-ClearPass. The IP Address and RADIUS shared secret (step 4) must match the configuration used on the switch.

1. From the **W-ClearPass Welcome** screen (Figure 5), click the **ClearPass Policy Manager** module. The **ClearPass Policy Manager** opens.
2. Navigate to the Network Devices page by selecting, Configuration > Network > Devices.
3. Click **+Add**.
   The **Add Device** window opens.
4. Enter the Name of the switch, IP Address, Description and RADIUS Shared Secret (Figure 6).
5. Select **IETF** from the **Vendor Name:** dropdown box.
6. Click **Add**.

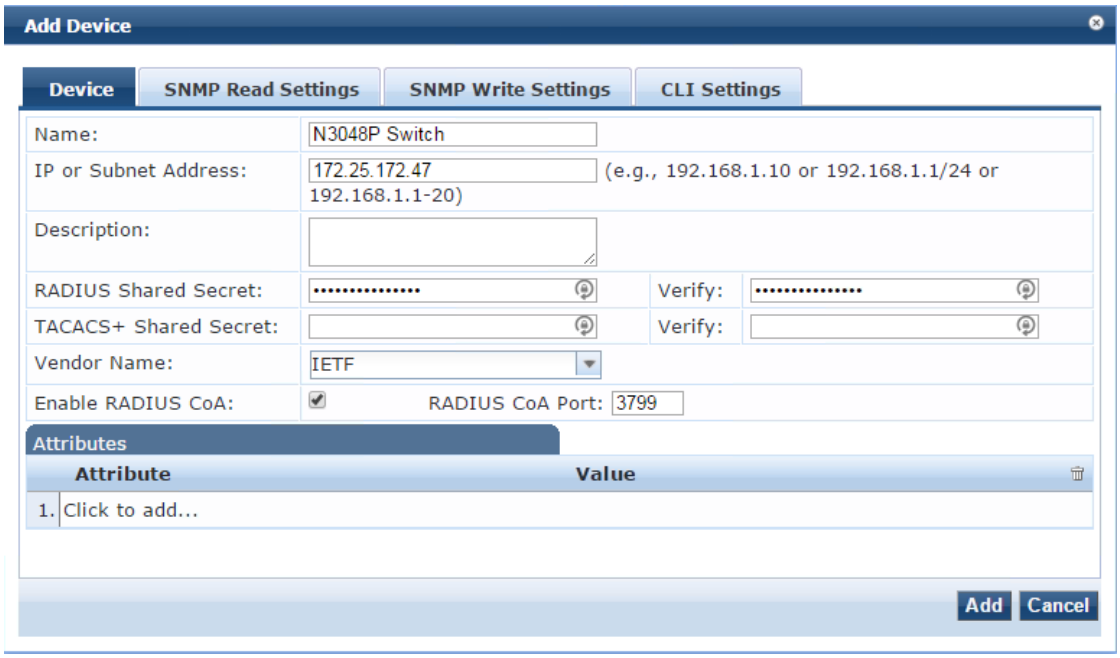

Figure 6 N-Series device settings

3.4.2 Add Active Directory as an Authentication Source

1. To add Active Directory as an authentication source, open the **Authentication Sources** page by selecting **Configuration > Authentication > Sources**.
2. Click **+Add**.
3. Enter details for the authentication source as shown in Figure 7.

Figure 7 shows a partial configuration of the Active Directory Authentication Source. This example uses a Windows Server with Active Directory installed as the source for username/password credential store. W-ClearPass supports many different authentication sources. For additional details on configuring Active Directory and other authentication source types, see the W-ClearPass User Guide at www.dell.com/support.

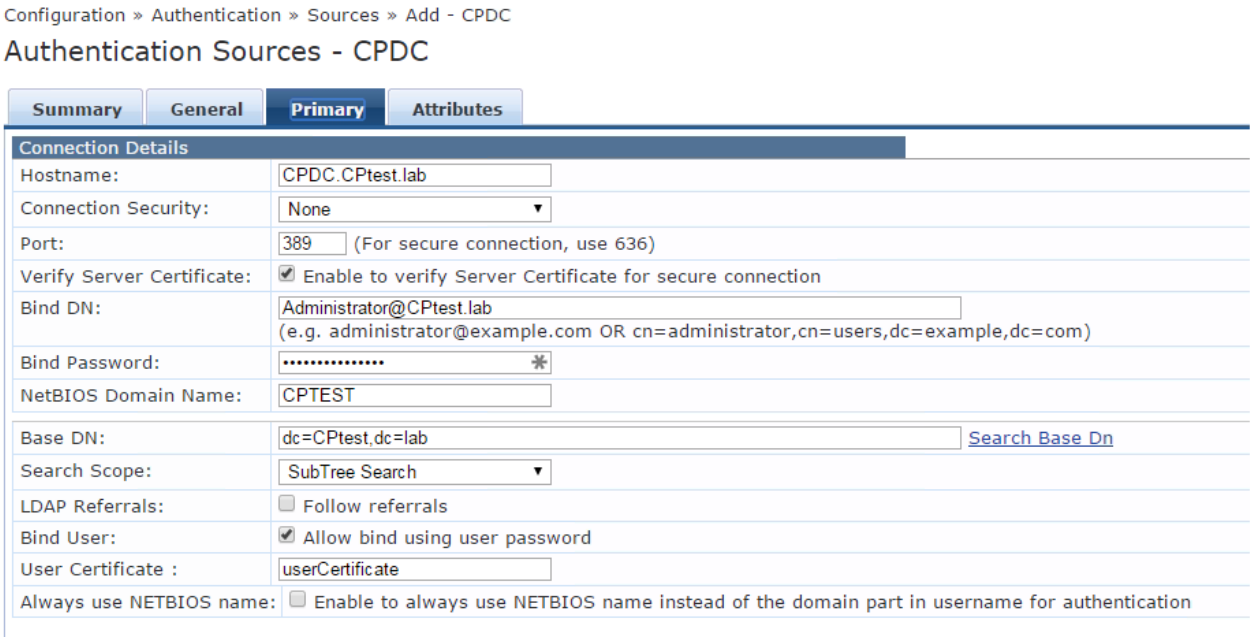

Figure 7 Active Directory Authentication Source

3.4.3 Create the 802.1x Wired Service with Posture Checks

W-ClearPass includes templates for many common services. These templates allow administrators to easily build the services and their associated policies. This section details the use of the 802.1X Wired template located in the **Start Here** (Figure 8) section within the **Configuration** section.

1. To create an 802.1x Wired Service with Posture Checks, navigate to **Configuration > Start Here**. The template list is displayed.
2. Click the **802.1X Wired** template (Figure 8).
   The **General** tab of the **802.1X Wired Service Template** (Figure 9) opens.

Figure 8 802.1X Wired Template

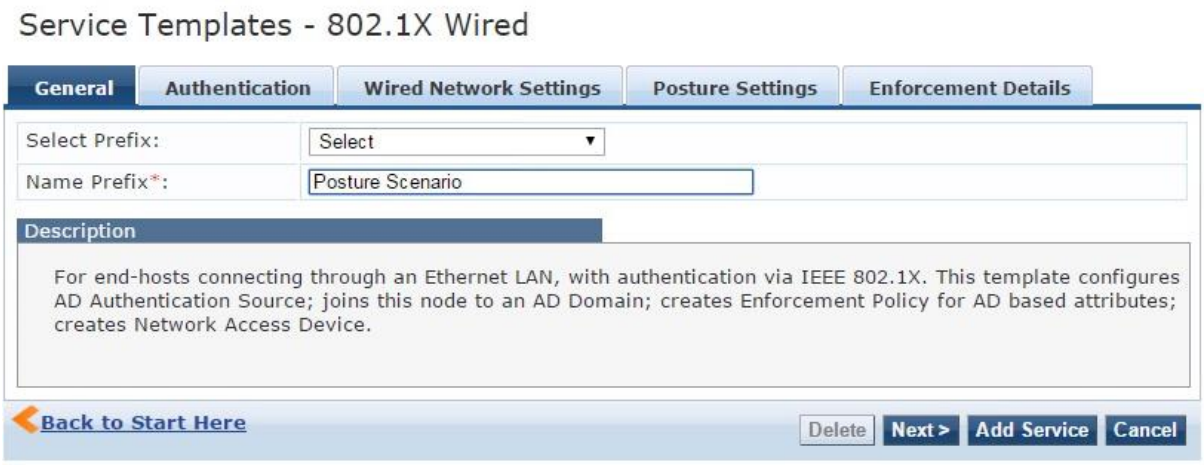

Figure 9 802.1X Wired – General Tab

3. Type in the Name Prefix to identify the service name and policy names generated by the template. ***802.1X Wired*** will be appended to the Name Prefix.
4. Click **Next >**.
   The **Authentication** tab (Figure 10) opens.

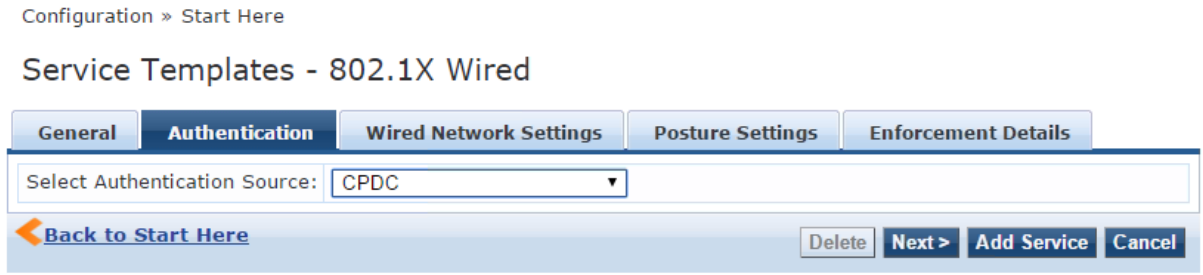

Figure 10 802.1X Wired – Authentication Tab

5. From the dropdown menu, select the Authentication Source that was configured in the previous steps. Additional authentication sources can be added later.
6. Click **Next >**.
   The **Wired Network Settings** tab (Figure 11) opens.

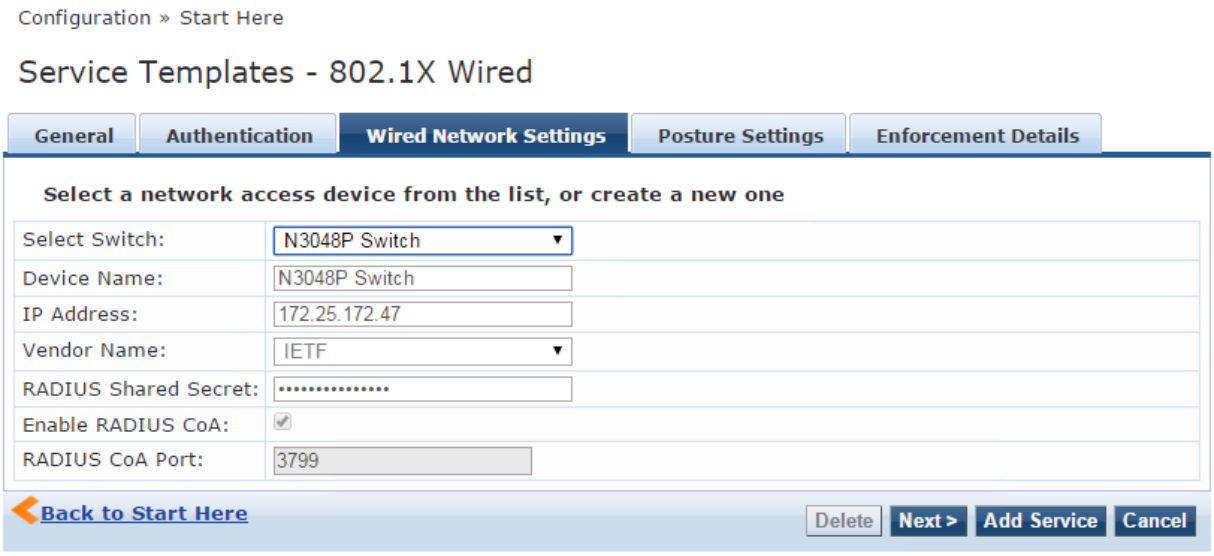

Figure 11 802.1X Wired – Wired Network Settings Tab

7. From the dropdown menu, select the network device (N-Series switch) that was configured in the previous steps.
8. Click **Next >**.
   The **Posture Settings** tab (Figure 12) opens.

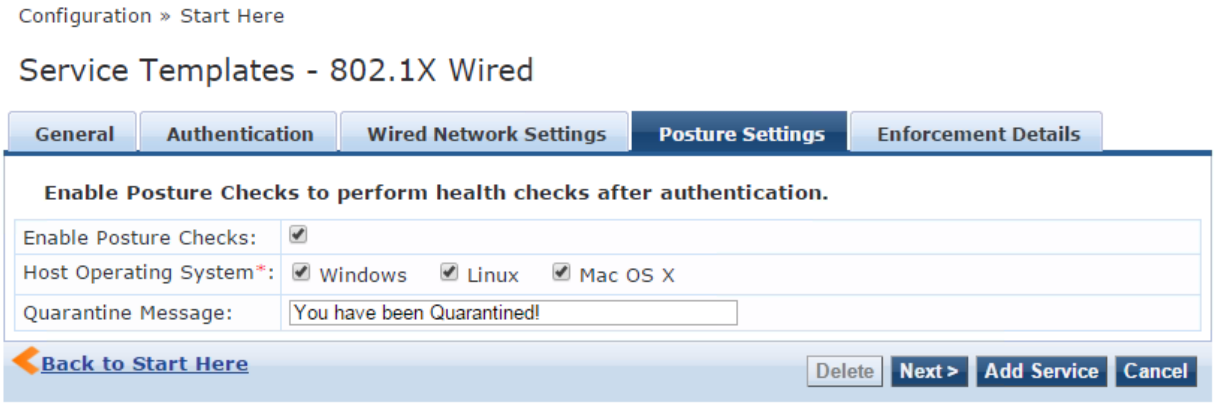

Figure 12 802.1X Wired – Posture Settings Tab

9. Select the operating systems OnGuard needs to support.
10. Enter a quarantine message in the **Quarantine Message:** field.
    This message is displayed anytime OnGuard detects a posture compliance issue.
11. Click **Next >**.
    The **Enforcement Details** tab (Figure 13) opens.

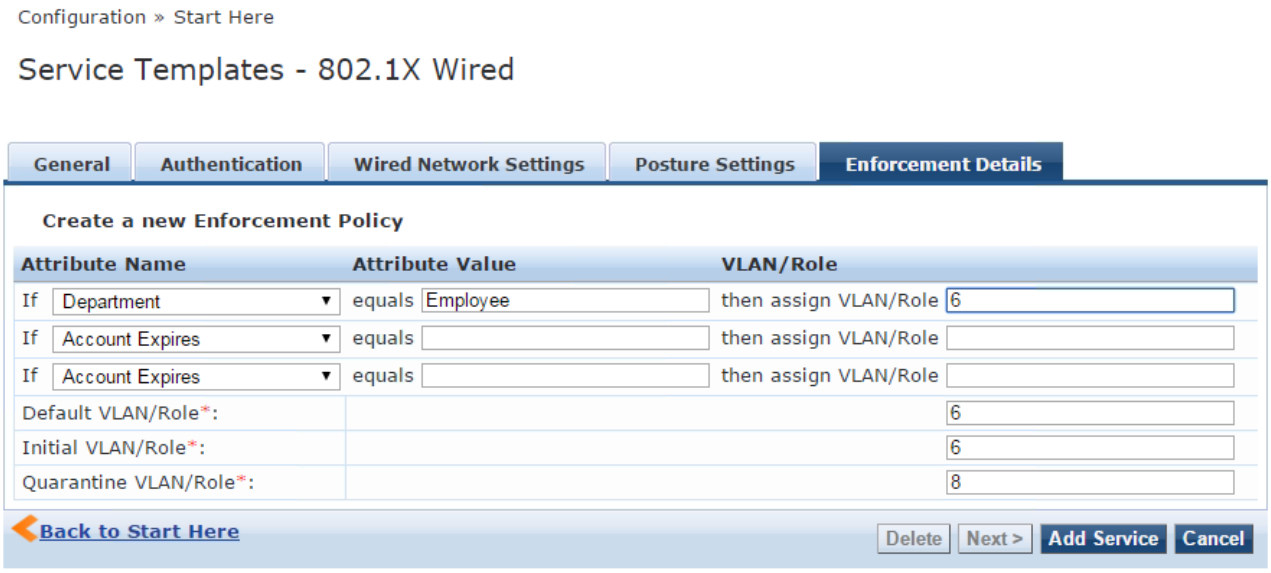

Figure 13 802.1X Wired – Enforcement Details Tab

12. Enter the VLAN information for your network. At least one rule and the three VLAN/Role fields at the bottom of the list are required. These settings can be changed and added to later.
13. Click **Add Service**.
    Two Services are now added to the list of Services (Figure 14). Numbering may vary between deployments.

The services can be viewed by selecting **Configuration > Services**. The two services shown in Figure 14 will be modified after the Posture, Role Mapping and Enforcement Policies are configured.

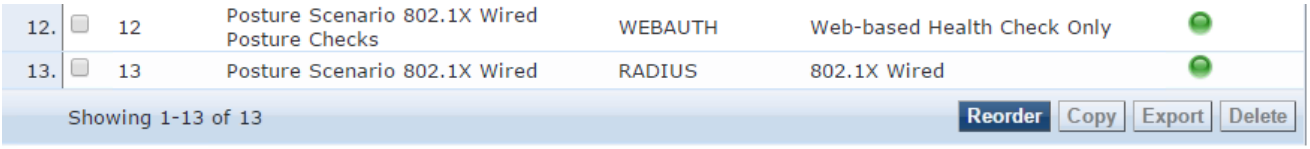

Figure 14 Services added from the 802.1X Wired Service Template Wizard

3.4.4 Define Posture Policies

The 802.1x Wired template creates three posture policies (Figure 15) with the prefix name used in the template. To view the posture policies, navigate to **Configuration > Posture > Posture Policies**.

Figure 15 Posture Policy List

Edit the Posture Policy for Windows, Mac OS X and Linux

Figure 16 shows the default policy that was created by the Service Template. For the purposes of this example, the only posture check will be to enable checks for a firewall.

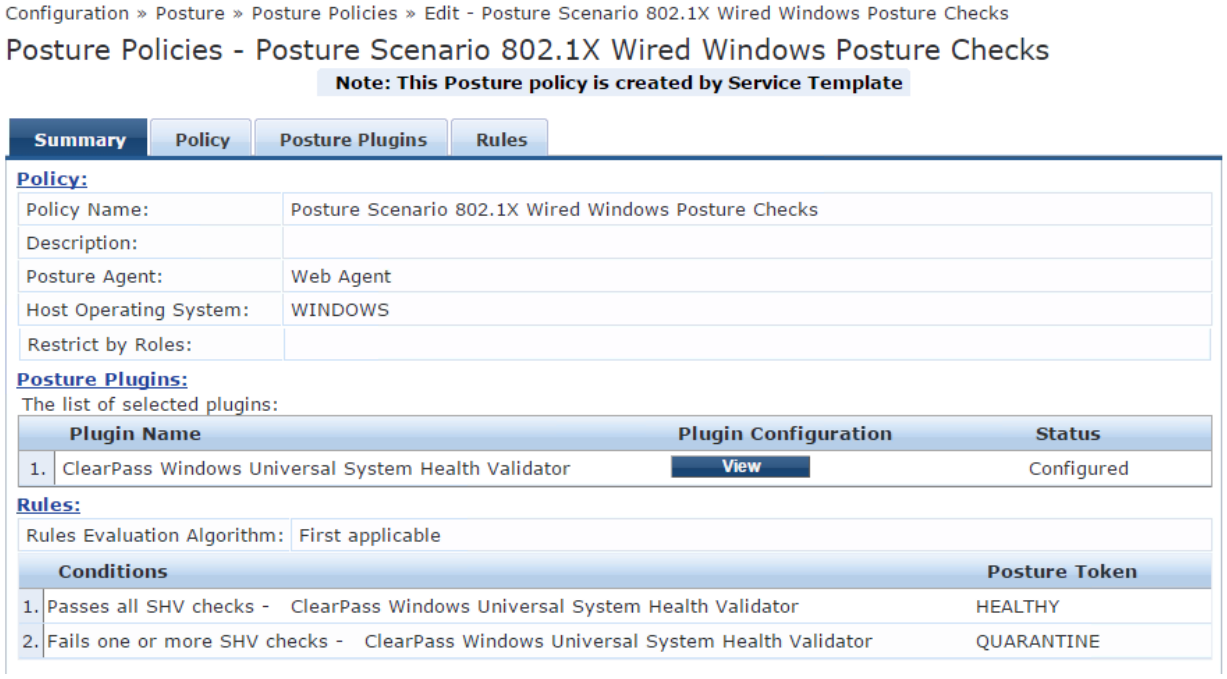

Figure 16 Windows Posture Policy - Summary Tab

1. To edit the Windows posture policy, navigate to **Configuration > Posture > Posture Policies** and select the Windows Posture Policy (**Posture Scenario 802.1X** in this example).
2. Keep all the default settings on the **Policy** tab, as shown in Figure 17.

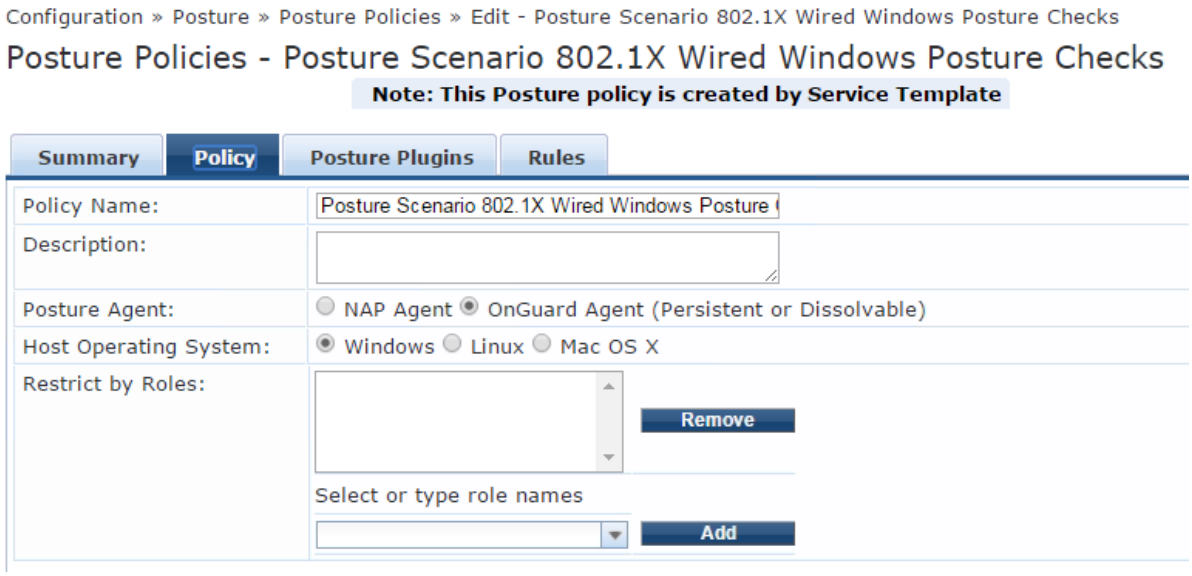

Figure 17 Windows Posture Policy – Policy Tab

3. To configure each individual posture check, select the **Posture Plugins** tab and click the **Configure** button (Figure 18) next to the **ClearPass Windows Universal System Health Validator** (a.k.a. OnGuard).
   The **ClearPass Windows Universal System Health Validator** window (Figure 19) will open. This window allows customization of each posture category for each type of Windows OS. In this example, only checks for firewall applications on Windows 7 OS will be enabled.

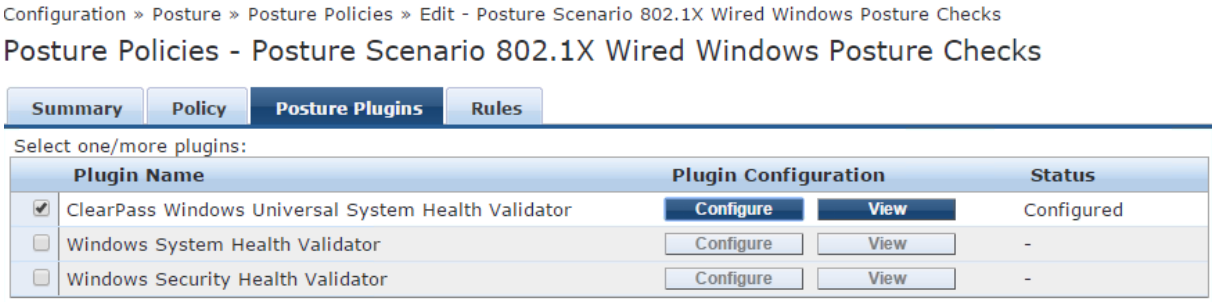

Figure 18 Windows Posture Policy – Posture Plugins Tab

4. In the left pane, navigate to **Windows 7 > Firewall** (Figure 19).
5. Keep all default settings as shown in Figure 19.
   These options will check Windows 7 devices for any active firewalls. If there is not an active (on) firewall application, then OnGuard will report the device as unhealthy.
6. At this time, other health check options can be enabled or disabled depending on the organization's security policies.

Note: The AntiVirus check is also enabled by default. If you do not want OnGuard to quarantine your test device due to the absence of an antivirus client, disable it at this time by unchecking the appropriate box.

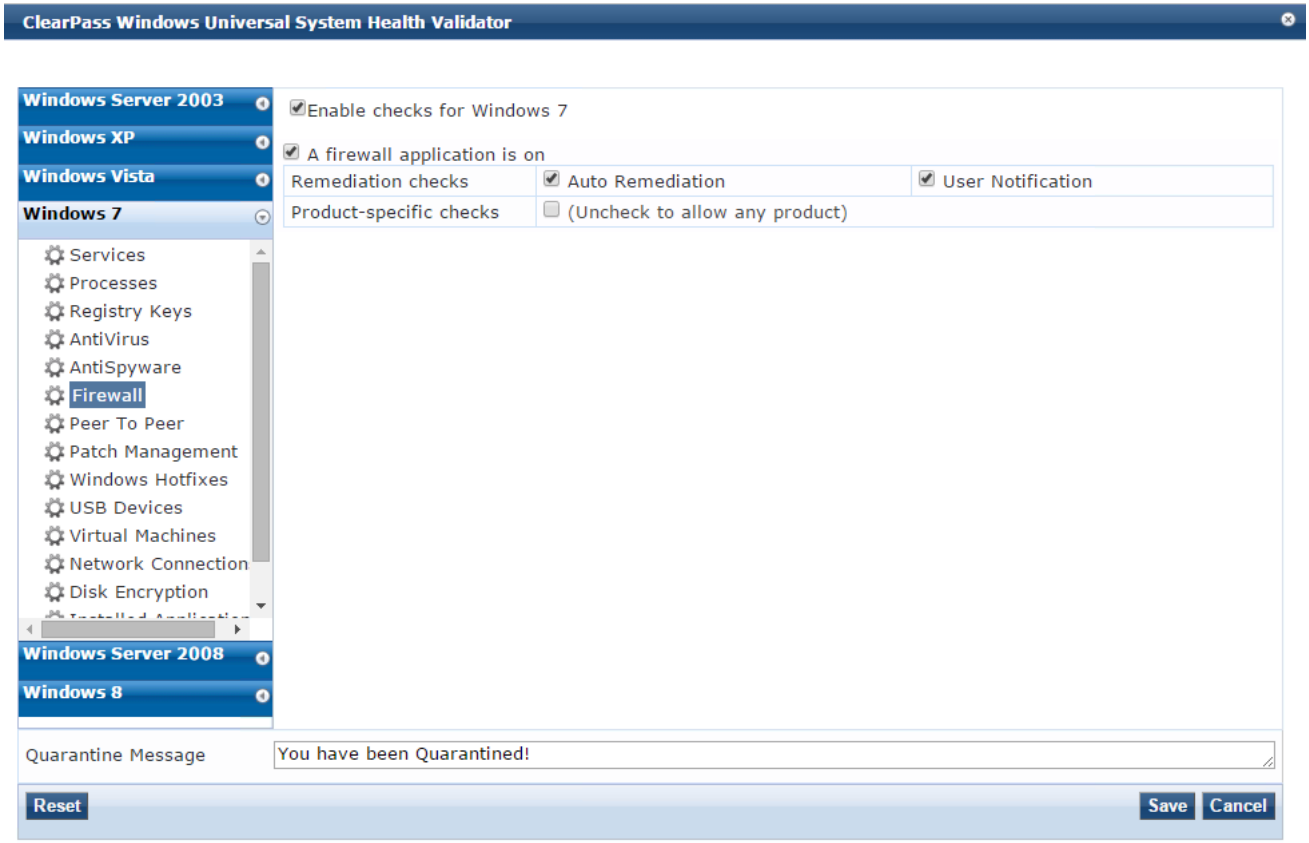

Figure 19 Windows Posture Policy – Validator settings

7. Click **Save** and move to the **Rules** tab.
   The **Rules** tab (Figure 20) allows the administrator to define the conditions that determine the type of posture token assigned, based on the outcome of the health scan. In this example, the default settings are used. Any single failure of the health scan will produce a Quarantine token. This token will be used later to determine enforcement policies during authentication or a re-authentication forced by OnGuard.

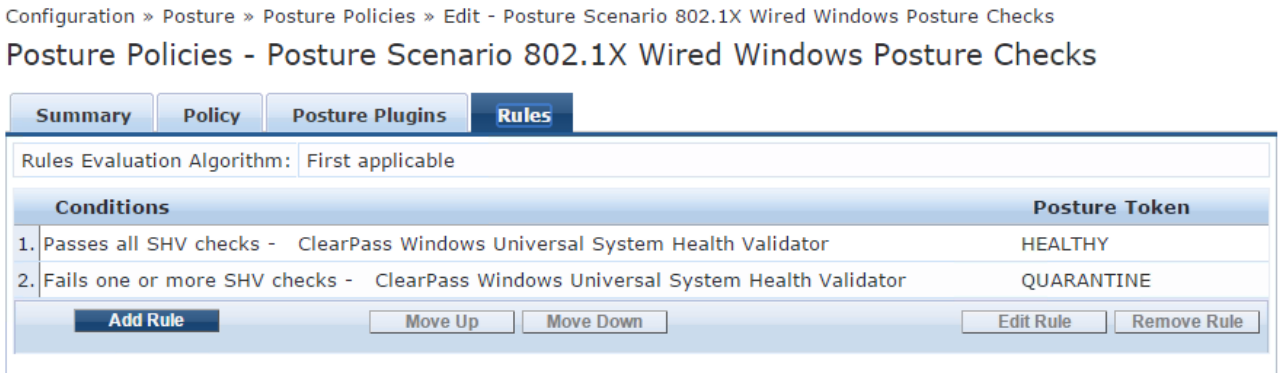

Figure 20 Windows Posture Policy – Rules Tab

8. Repeat the posture policy configurations for Mac OS X and Linux Posture Policies. These policies are located in the same Posture Polices area as the Windows example above (i.e. **Configuration > Posture > Posture Policies**).

3.4.5 Define Roles and Role Mappings

Role mappings are used to apply conditions to each user to classify them into roles. The roles are then used to identify users and can be used to enforce policies within the service. There are numerous conditions and rules that can be used to form a Role Mapping. For more information on roles and Role Mapping, refer to the W-ClearPass Policy Manger User Guide at www.dell.com/support.

For the purpose of this guide, this example will use default roles built into the W-ClearPass Policy Manager. The two roles used are **[Employee]** and **[Guest]**. Default configurations in W-ClearPass are identified by the brackets surrounding the name.

3.4.5.1 Create a new Role Mapping

1. Navigate to Configuration > Identity > Role Mappings.
2. Click the **+ Add** link in the upper right hand corner.
3. Name the policy. For this example, the name ***N-Series Wired Role Mapping*** is used. In the **Default Role** drop down, choose **[Guest]**.
4. Click **Next >**.
5. On the **Mapping Rules** tab, click **Add Rule**.
   The **Rules Editor** opens (Figure 21), enter the following:
   - Type: **Authorization: *CPDC*** (Name of the Active Directory used in this example.)
   - Name: **Department**
   - Operator: **CONTAINS**
   - Value: **Employee** (Value used in the department field of the Active Directory user account.)
6. Use the **[Employee]** role for the Role Name.

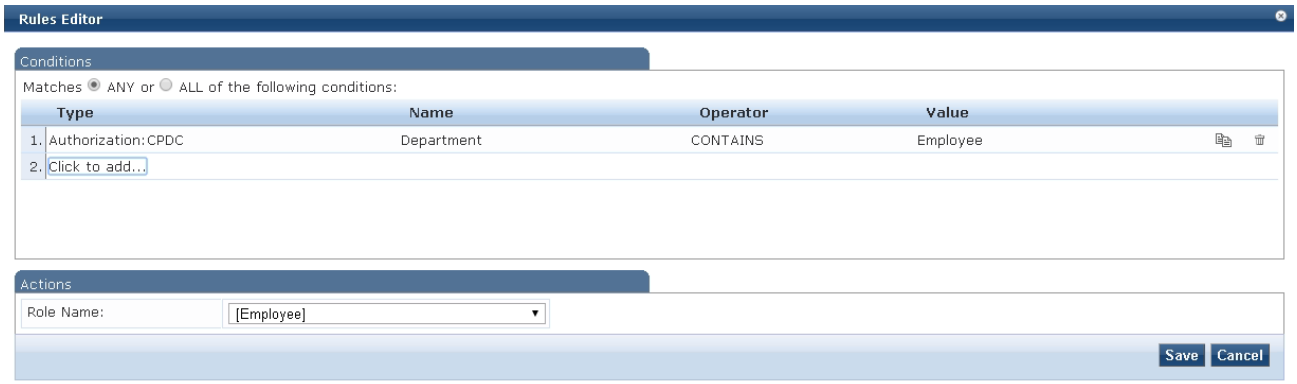

Figure 21 Role Mapping – Mapping Rule

Administrators can build sophisticated condition lists and any number of rules to be as specific as needed to identify multiple user types. This simplistic example will result in any user with the "Employee" department name in Active Directory being assigned the **[Employee]** role. Any user that does not have the Active Directory department field populated with "Employee" will be assigned the default **[Guest]** role.

7. Click **Save**.
8. Click **Next >** to move to the **Summary** tab.
9. Verify the information is correct, then click **Save**.
   The new Role Mapping will appear in the **Role Mapping** list.

The Role Mapping that was just created will be used in the 802.1X RADIUS Service. No Role Mapping will be used for the Health Check Service. A more detailed explanation of the two services is discussed later in this section.

3.4.6 Define Enforcement Profiles and Policies

Enforcement Policies are a group of rules with conditions that direct enforcement actions that ultimately are sent to the Network Access Device, which in this example is the N-Series switch. Enforcement profiles are a collection of attributes that define those enforcement actions.

The 802.1x Wired template with posture checks produced two services, the Health Check Service and the Radius Service. Both of these services need Enforcement Policies, and their associated Enforcement Profiles. The Health Check Service will produce a posture token (by executing an action), while the Radius Service will use that token (within its conditions) to determine a VLAN assignment action.

Enforcement Profiles are used within the Enforcement Policies, so the profiles are configured first.

3.4.6.1 Health Check Enforcement Profiles and Policies

Terminate Session Profile for the Health Check Service

The Health Check Service requires a profile to terminate the session so that the RADIUS 802.1X authentication Service can use the posture token in a new authentication routine. The terminate session profile will utilize the Change of Authorization feature to force a re-authentication.

1. Navigate to the list of Enforcement Profiles by selecting, **Configuration > Enforcement > Profiles**.
2. Click the **+ Add** link in the upper right hand corner.
3. From the Template dropdown menu, choose RADIUS Change of Authorization (CoA).
4. Name the policy.
   This example uses **Dell Terminate Session** as the profile name.
5. Leave all the other settings as default, and click **Next >** to move to the **Attributes** tab.
6. On the dropdown menu for Select RADIUS CoA Template, choose IETF-Terminate-Session-IETF.
7. Click **Next >** and review the **Summary** tab (Figure 22).
8. Click **Save.**

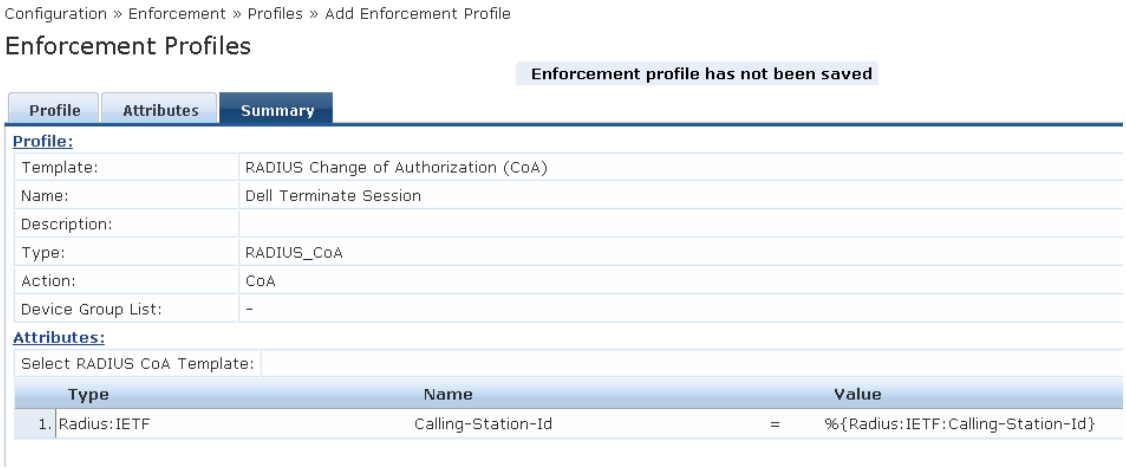

Figure 22 Enforcement Profile – RADIUS_CoA

Enforcement Policy for the Health Check Service

The following details an example of configuring the Enforcement Policy for the Health Check Service. The pre-populated policy from the template is sufficient for this example and most of the default settings are kept.

1. Navigate to the list of Enforcement Policies by selecting, Configuration > Enforcement > Policies.
2. Click the pre-populated policy name for the Health Check Service.
   In this example, the name is ***Posture Scenario 802.1X Wired OnGuard Agent Enforcement Policy***, and its type is ***WEBAUTH***. The template automatically generates this policy based on the prefix name.
3. Click the **Enforcement** tab.
4. Under the Default Profile, choose the [RADIUS_CoA] Dell Terminate Session configured previously.
5. Navigate to the **Rules** tab.
6. Highlight the first rule by clicking it, then click **Edit Rule** to open the rule.
   For the example in this guide, the pre-populated conditions work well. No changes are made to the default conditions.
7. Within the list of **Profile Names** (Figure 23), select the [**RADIUS_CoA] [Aruba Terminate Session]** and click **Remove**. Use the dropdown menu to select **[RADIUS_CoA] Dell Terminate Session**.

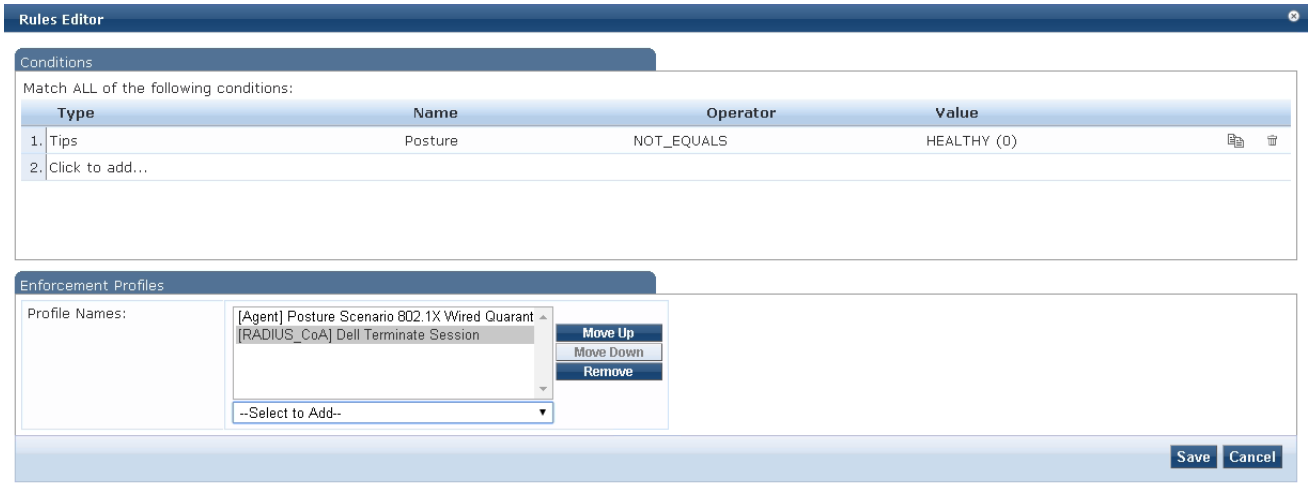

Figure 23 Enforcement Rule #1 – Enforcement Policy for OnGuard Service

The first part of the rule states that any posture token values not equal to HEALTHY(0) will trigger this rule to be enforced. The Enforcement Profiles under the condition are the actions that will be applied if the conditions in this rule are met. The first profile in the list is named **[Agent] Posture Scenario 802.1X Wired Quarantined Agent Enforcement**. This profile simply displays a quarantine message to the client. This profile can be seen in the list of Enforcement Profiles at **Configuration > Enforcement > Profiles**. The profile was created from the Service template during the Service creation earlier. The settings for this profile are kept as default and are not shown in this guide.

8. Click **Save** to commit changes to the rule.
9. Click the second rule to highlight it, then click **Edit Rule** to open the rule.
   For the example in this guide, the pre-populated conditions work well. No changes need to be made to the default conditions.
10. Within the list of **Profile Names** (Figure 24), select the **[RADIUS_CoA] [Aruba Terminate Session]** and click **Remove**. Use the dropdown menu to select **[RADIUS_CoA] Dell Terminate Session**.

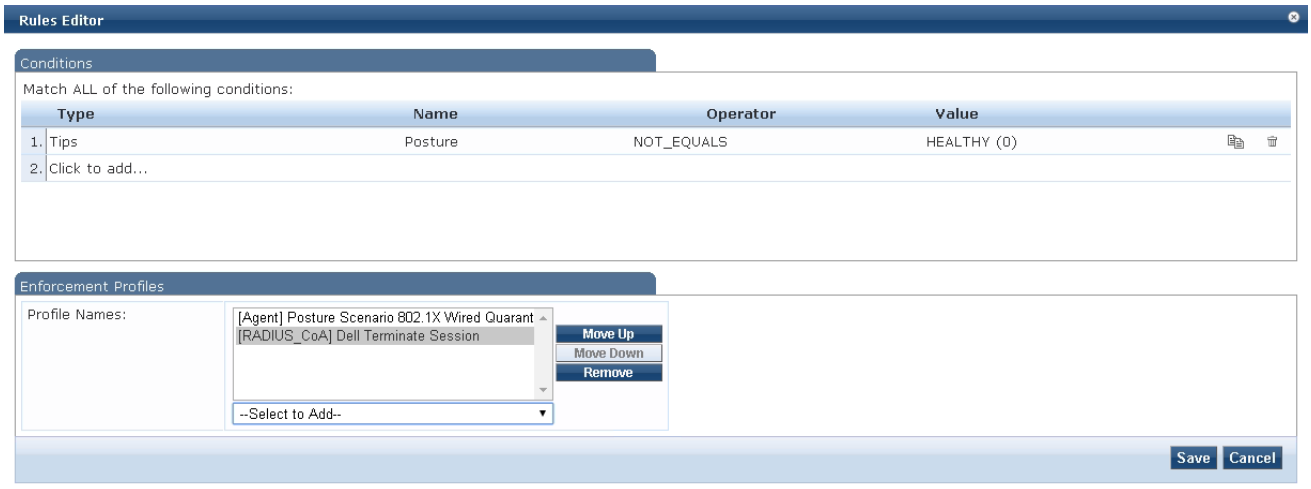

Figure 24 Enforcement Rule #2 – Enforcement Policy for OnGuard Service

The first part of the rule states that any posture token values equal to HEALTHY(0) will trigger this rule to be enforced. The Enforcement Profiles underneath the condition are the actions that will be applied if the conditions in this rule are met. The first profile in the list is named **[Agent] Posture Scenario 802.1X Wired Healthy Agent Enforcement**. This profile simply displays a healthy message to the client. This profile can be seen in the list of Enforcement Profiles at **Configuration > Enforcement > Profiles**. The profile was also created from the Service template during the Service creation earlier. The settings for this profile are being kept as default and are not shown in this guide.

11. Click **Save** to commit changes to the rule.
12. Click **Save** again to commit changes to the Enforcement Policy.
    This concludes the Enforcement Policy and profiles for the Health Check Service.

The next steps detail the configuration for the policy and profiles used in the RADIUS 802.1X Service.

3.4.6.2 RADIUS 802.1X Enforcement Profiles and Policies

Enforcement Profile for the RADIUS 8021.X Service

The RADIUS 8021.X Service requires an Enforcement profile to enable the assignment of VLANs. In this example, a client device that fails a health check will be assigned to a Quarantine VLAN. A client device that passes a health check will be assigned an Employee VLAN.

The following steps create a profile to enforce an Employee VLAN assignment.

1. Navigate to the list of Enforcement Profiles by selecting, Configuration > Enforcement > Profiles.
2. Click the **+ Add** link in the upper right hand corner.
3. From the **Template** dropdown menu, choose **VLAN Enforcement**.
4. Name the policy.
   This example uses *N-Series VLAN Employee* as the profile name.
5. Leave all other settings as default, and click **Next >** to move to the **Attributes** tab.
6. On the fifth attribute, **Tunnel-Private-Group-Id**, click **Enter VLAN**. Manually enter the number of the VLAN used for Employees.
   In this example, Employees are assigned to VLAN 6.
7. Save the attribute line by clicking the disk icon to the right.
8. Click **Next >** and review the **Summary** tab.
9. Click **Save**.
10. Review the **Summary** tab.
    The Summary tab should look similar to Figure 25.

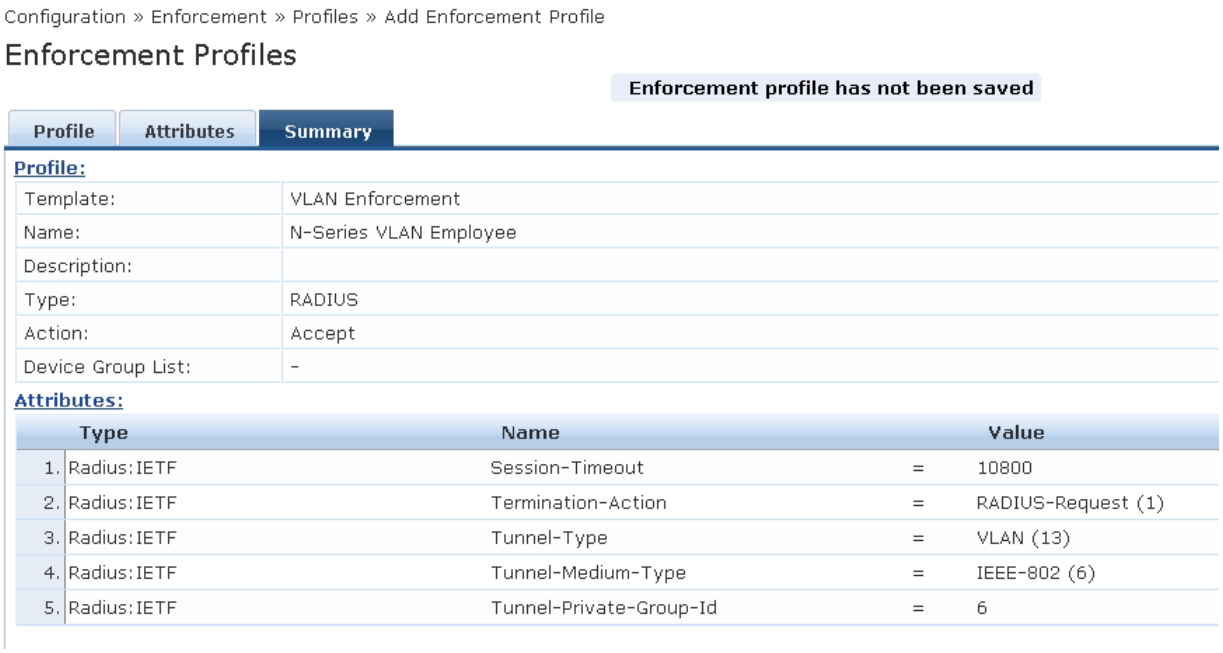

Figure 25 Enforcement Profile – VLAN Employee

The following steps create a profile to enforce a Quarantine VLAN assignment.

1. Navigate to the list of Enforcement Profiles by selecting, Configuration > Enforcement > Profiles.
2. Click the **+ Add** link in the upper right hand corner.
3. From the **Template** dropdown menu, choose **VLAN Enforcement**.
4. Name the policy. This example uses *N-Series VLAN Quarantine* as the profile name.
5. Leave all other settings as default, and click **Next >** to move to the **Attributes** tab.
6. On the fifth attribute, click **Enter VLAN**. Manually enter the number of the VLAN used for Quarantined users.
   In this example, Quarantined users are assigned to VLAN 8.
7. Save the attribute line by clicking the disk icon to the right.
8. Click **Next >** and review the **Summary** tab.
9. Click **Save**.
10. Review the **Summary** tab.

Enforcement Policy for the RADIUS 8021.X Service

The following steps configure the Enforcement Policy for the RADIUS 802.1X Service. The pre-populated policy from the template is sufficient for this example and many settings will be kept as default. The next steps will describe the contents of the Enforcement Policy.

1. Navigate to the list of Enforcement Policies by selecting, **Configuration > Enforcement > Policies**.
2. Click the pre-populated policy name for the Health Check Service.
   In this example, the name is ***Posture Scenario 802.1X Wired Enforcement Policy***, and its type is ***RADIUS***. The template has automatically generated this policy based on the prefix name.
3. Click the **Enforcement** tab.

4. Under the Default Profile, choose **[N-Series VLAN Quarantine]**.
   This example uses the quarantine profile to place users that fail authentication checks into quarantine. If the administrator chooses, a profile to deny access or place users into a different vlan is possible here.
5. Navigate to the **Rules** tab.
6. Remove all the default rules by selecting each rule and clicking **Remove Rule**.
   In this example, this authentication policy has only two outcomes given the correct credentials.

The user is authenticated, is identified as an Employee, and has a Healthy token.
The user is authenticated, and does not have a Healthy token.

The first outcome will place the user in the Employee Vlan (6). The second outcome will place the user into a Quarantine Vlan (8).

If the administrator has other user classifications and conditions, they can be added now. Additional profiles or user roles may be required.

7. To configure rules per the example above, click **Add Rule**.
8. Create two conditions.
   Note: The first condition must be saved before the second condition can be created.
   Condition 1

   - Type: **Tips**
   - Name: **Role**
   - Operator: **MATCHES_ANY** (could also use **EQUALS**)
   - Value: **[Employee]** (add other roles to the list here if applicable)

   Condition 2

   - Type: **Tips**
   - Name: **Posture**
   - Operator: **EQUALS**
   - Value: **HEALTHY (0)**

9. Under the Enforcement Profiles section, choose [RADIUS] N-Series VLAN Employee.
10. The **Rules Editor** window should look like Figure 26 below.

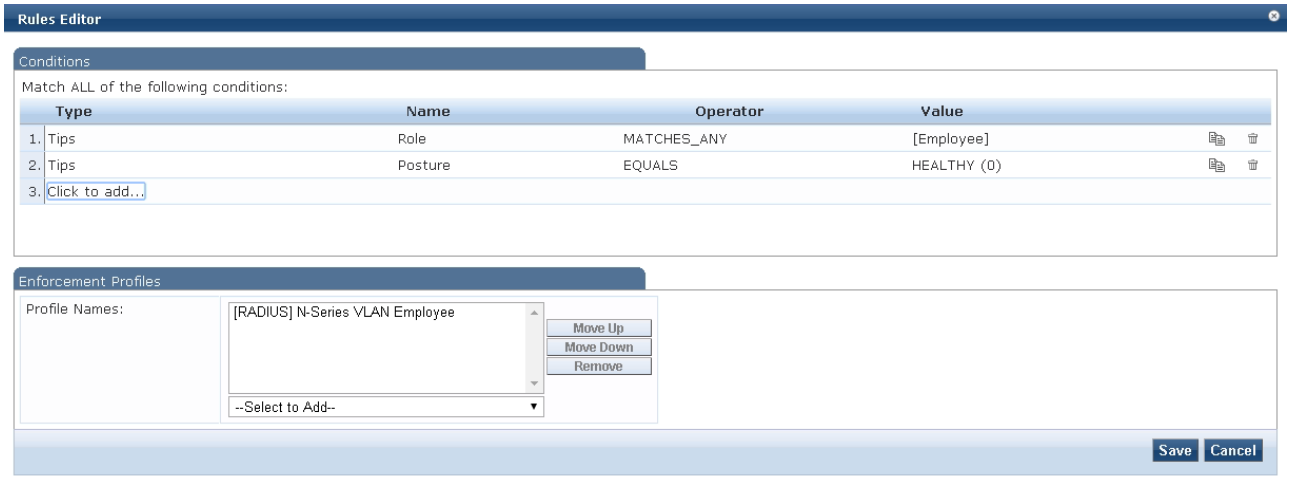

Figure 26 Enforcement Policy – Healthy Employee Rule

11. Click **Save**.
12. To create a second rule, click **Add Rule**.
13. Create two conditions.
    Note: The first condition must be saved before the second condition can be created.
    Condition 1

    - Type: **Tips**
    - Name: **Role**
    - Operator: **EQUALS**
    - Value: **[User Authenticated]**

    Condition 2

    - Type: **Tips**
    - Name: **Posture**
    - Operator: **NOT_EQUALS**
    - Value: **HEALTHY (0)**

14. Under the Enforcement Profiles section, choose [RADIUS] N-Series VLAN Quarantine.
15. The **Rules Editor** window should look like Figure 27 below.

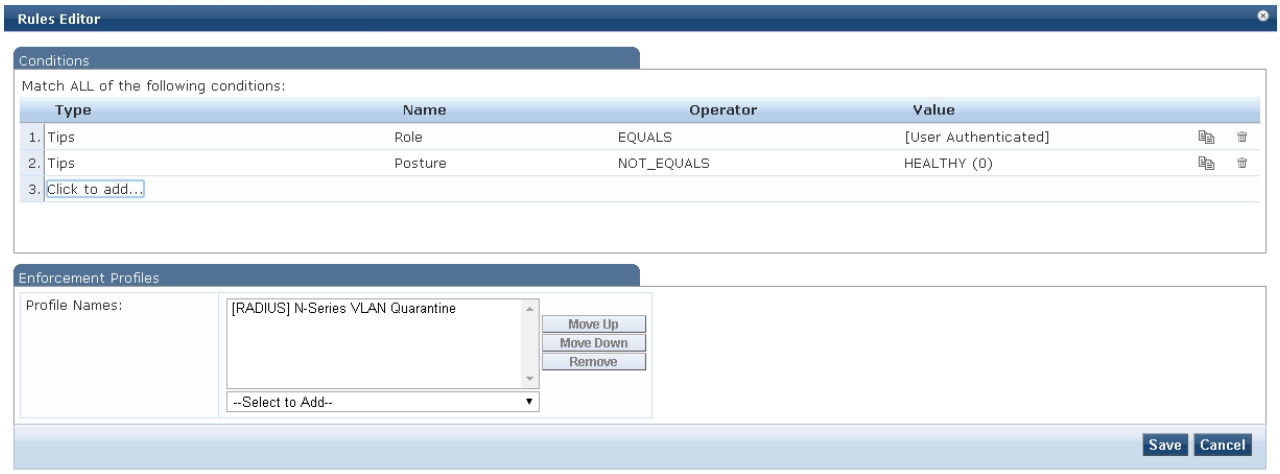

Figure 27 Enforcement Policy – Not Healthy Rule

16. Click **Save** to save the rule.
17. Click **Save** again to save the Enforcement Policy.

3.4.7 Configure the Services

Now that all the components of the Services are defined and configured, the Services themselves need to be configured.

1. Navigate to Configuration > Services.
1. Select the Service: Posture Scenario 802.1X Wired.
2. Select the **Service** tab.
   The template populates the Service Rules with two rules that require all rules to match. In this example, a simpler configuration is used. Only the first condition is used. All devices connecting via Ethernet are classified by this Service. Administrators can add other rules to narrow the devices that this Service will be applied to at any time.
3. Click the second rule, named **Service-Type**, and delete it by clicking the delete icon (trashcan). The **Service** tab should look like Figure 28. Deleting this is optional, and can be added back in for an actual deployed service.

Note: Configuring the Service Rules are key to properly map the authentication request to the proper service. In a complex deployment, administrators can have multiple Services with similar functions that have different actions depending on the method of network access. This allows for a posture check Service for both wired and wireless access to enable different enforcement actions. For more information on Service Rules, see the Dell Networking W-Series ClearPass Policy Manager User Guide at http://www.dell.com/support/.

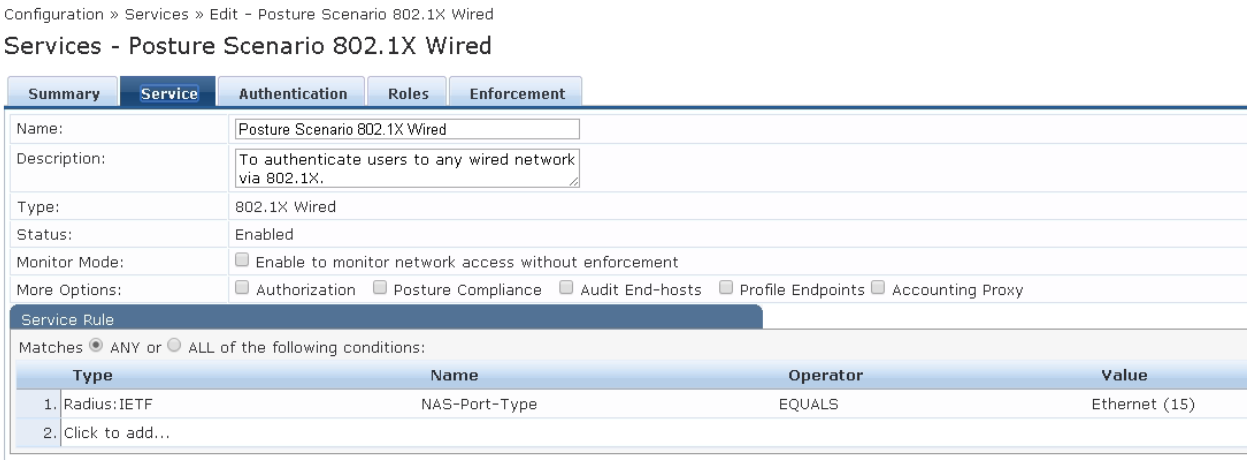

Figure 28 802.1X Wired Service - Service tab

4. Move to the **Authentication** tab (Figure 29).
   This example uses Microsoft Active Directory with username/password for the credentials. Authentication methods for this example are satisfied by using MSCHAPv2 and PEAP. Administrators can use any type of authentication method required by their network security policy.

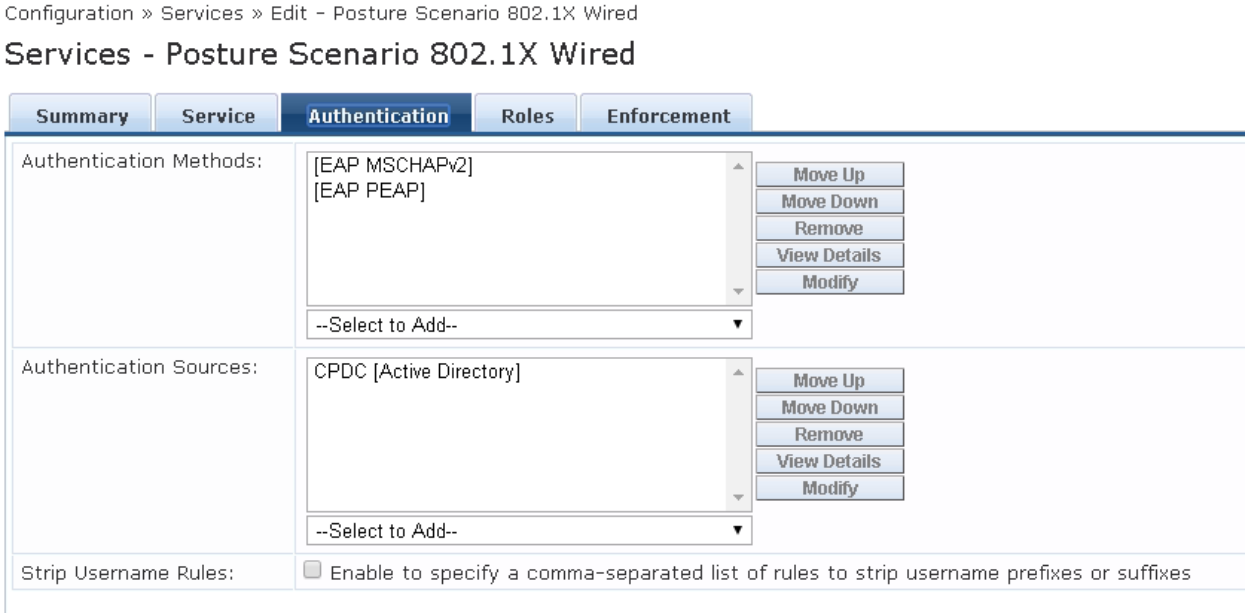

Figure 29 802.1X Wired Service – Authentication tab

5. Remove or add authentication methods as needed.
6. Remove or add authentication sources as needed.
7. Move to the **Roles** tab (Figure 30).
8. For the Role Mapping Policy, select N-Series Wired Role Mapping from the dropdown menu.

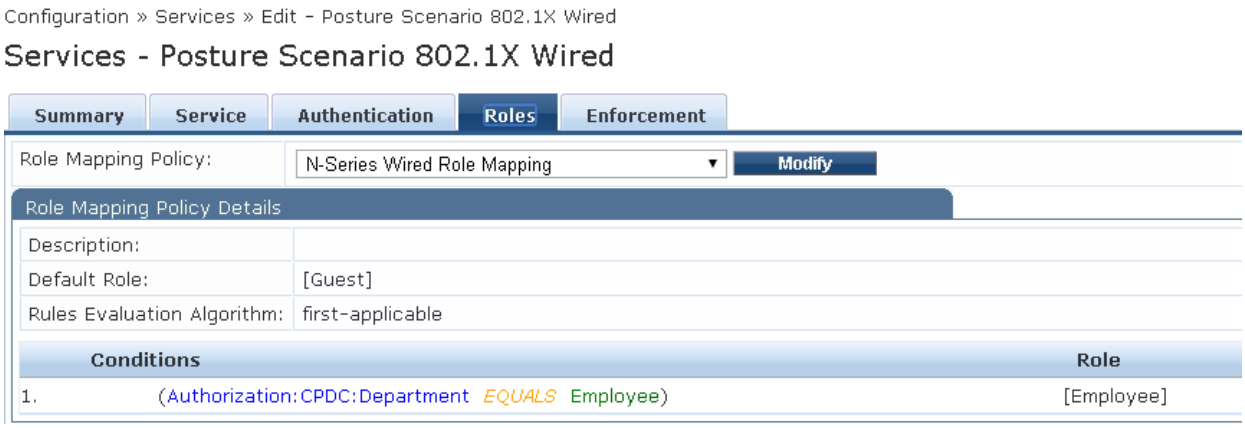

Figure 30 802.1X Wired Service- Roles tab

9. Move to the **Enforcement** tab.
   The template populates the appropriate Enforcement Policy in the dropdown menu.
10. Verify that the correct policy details are shown (Figure 31).

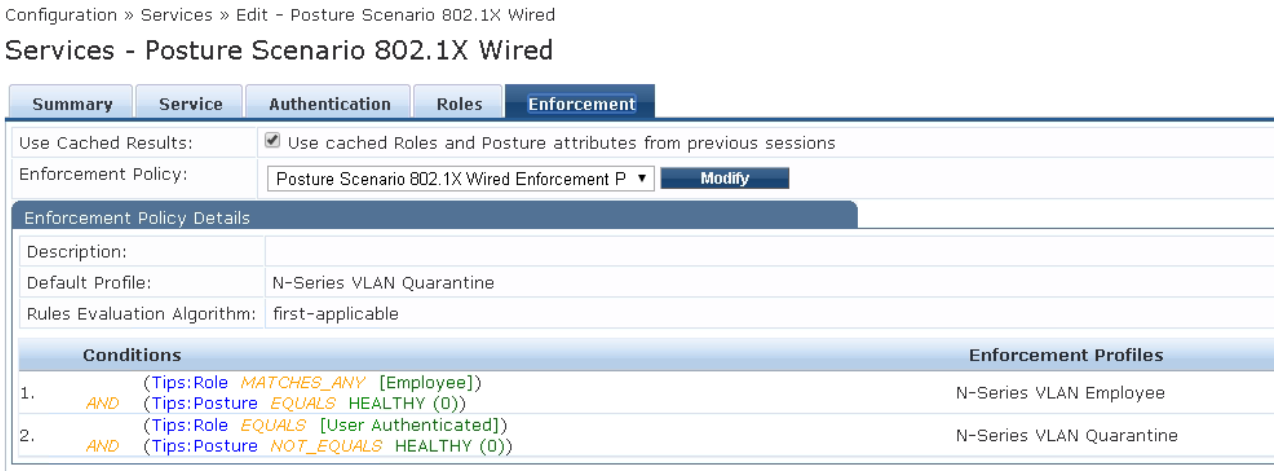

Figure 31 802.1X Wired Service – Enforcement tab

11. Click **Save** to save the Service.
12. Select the Service: Posture Scenario 802.1X Wired Posture Checks.
13. Select the **Service** tab.
    For this example, keep all the default settings.
14. Select the **Roles** tab.
    In this example, no Roles are needed for this Health Check Service.
15. Select the **Posture** tab (Figure 32).
    During testing, Posture Policies can be kept as default, but it is recommended to modify each OS specific policy to reflect the heath posture being tested. Click the desired policy agent type and click **Modify** to open the policy window. Select the **Posture Plugins** tab, and click the **Configure** button under Plugin Configuration. Default settings enable **AntiVirus** and **Firewall** checks for each OS version. For initial testing, it is recommended that functionality be validated with a single OS and health check setting (e.g. Windows 7 and Firewall). Click **Save** to save the Plugin Configuration, and **Save** again to save the Posture Policy.

It is also useful to have control over the health status of the client. Auto-remediation can automatically fix many health issues on the device. If administrators want to verify assigned vlans and other enforcement actions, it is recommended that they uncheck the **Remediate End-Hosts** checkbox. This box can be checked at any time after verifying the policy actions are behaving as expected.

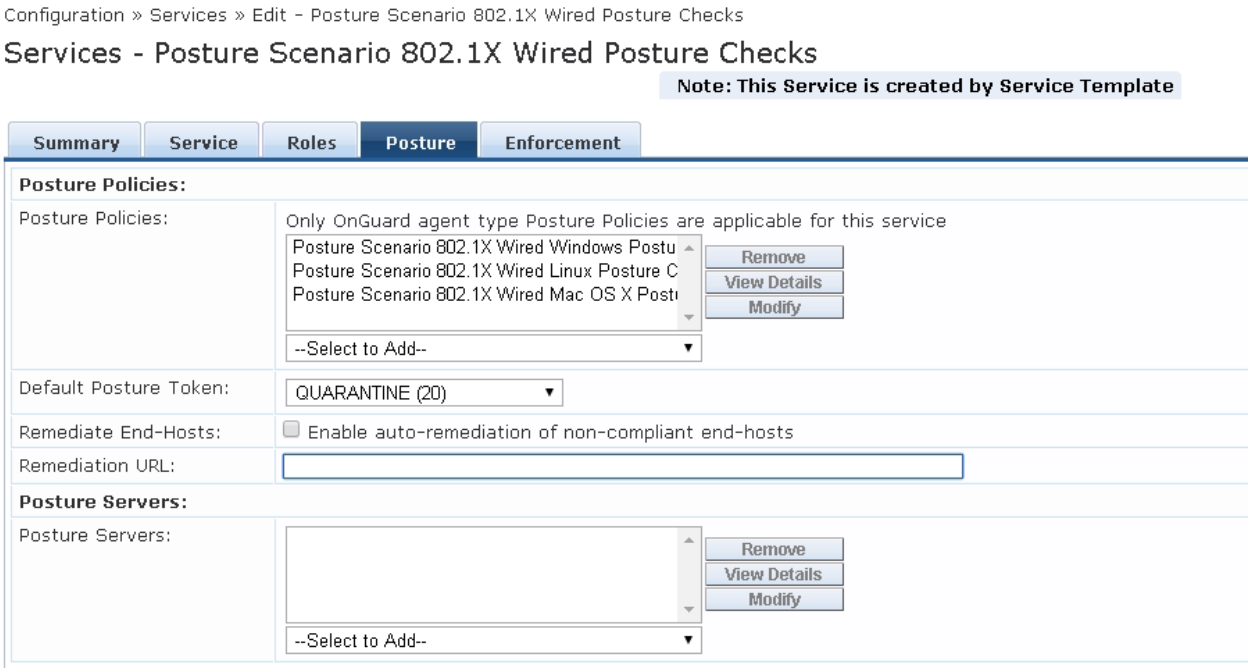

Figure 32 802.1X Wired Posture Service – Posture tab

16. Move to the **Enforcement** tab (Figure 33).
    The template populates the appropriate Enforcement Policy in the dropdown menu.
17. Verify that the correct policy details are shown.

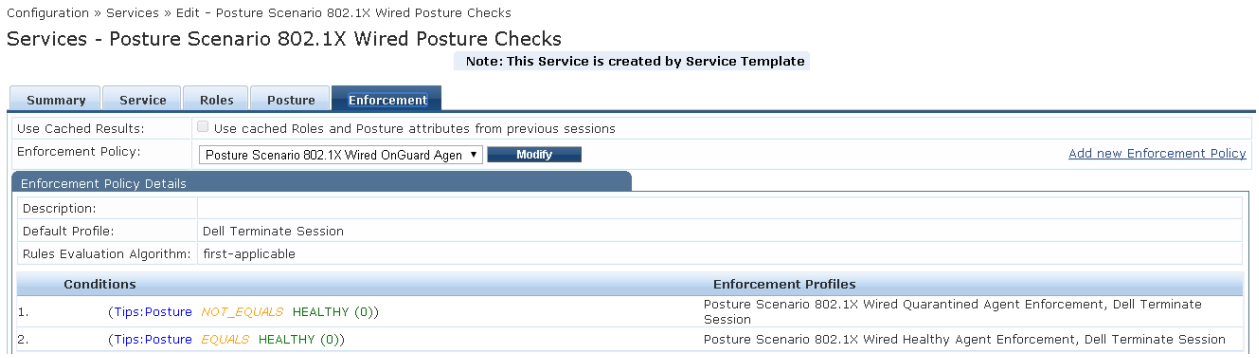

Figure 33 802.1X Wired Posture – Enforcement tab

18. Click **Save** to save the Service.
    Configuration of the W-ClearPass Services to include all supporting policies and roles is now complete.

3.4.8 Testing the Configuration

The W-ClearPass and N-Series configuration in this guide can be tested with any client. The following details the use of a Windows 7 laptop.

1. Ensure the Windows 7 client WiredAutoConfig is started and 802.1x Authentication is properly configured on the Local Area Connection.
2. Ensure the user is defined and entered into the Active Directory with a Department of “Employee”.
3. Ensure the laptop is part of the domain.
4. Connect the laptop to an access port on the switch.
5. Ensure firewall is enabled.
6. Enter credentials when prompted on the laptop.
   User is authenticated, placed into quarantine due to absence of a health token.
7. Install OnGuard through browsing to download URL.
8. Wait for OnGuard to scan health once installed.
   OnGuard initiates a re-authentication. User is placed into the employee vlan.
9. Turn off firewall.
10. Wait for OnGuard to rescan health after detecting a change to the firewall.
    OnGuard initiates a re-authentication. User is placed into the quarantine vlan.
11. Turn firewall on.
12. Wait for OnGuard to rescan health after detecting a change to the firewall.
    OnGuard initiates a re-authentication. User is placed into the employee vlan.

3.4.9 Miscellaneous Items for Wired Posture Checks

There are several issues that need to be solved to enable health checks on any unmanaged device through BYOD. This section discusses some common issues and how they may be addressed, but does not cover all the potential issues and solutions.

Access to OnGuard clients

In this example, a user without OnGuard is placed into a quarantine vlan. This vlan can be setup to allow access to the W-ClearPass sever, where the user can download either the persistent client or use the dissolvable application. The method that is used to inform the user of, or redirect the user to the W-ClearPass URL is left to the administrator. There are several options available:

Manually communicate the direct agent URL listed on W-ClearPass at **Administration > Agents and Software Updates > OnGuard Settings**.
Create a landing page with W-ClearPass Guest to simplify the URL and provide links for all OS and agent types. This landing page is detailed in the wireless example in the Creating an OnGuard Landing Webpage section.
Use third party software or a dedicated DNS server to enable redirection to the URL noted in one of the previous two options.

Once the user has access to OnGuard and performs a health check, the user can be allowed onto the network for full access.

Client behavior with DHCP

When utilizing the example of placing users into a different vlan for quarantine, the device must obtain another IP address through DHCP for the new vlan. Client behavior relating to the release and renewal of IP addresses can depend on the OS, network card and network driver. Some clients may not release their IP address, even after the port on the switch transitions to a new vlan. In these cases, the client must be forced to renew their DHCP lease.

Some solutions that force a DHCP renewal are:

- Short lease times
- Manual disconnect from OS
- Manual disconnect through reseating cable
- Bounce the switch port
- Reboot or restart the device

In many of the above cases, the user will need to be notified that they may need to perform an action. Providing directions, through instructions either on a landing page or through client messages from the W-ClearPass OnGuard agent, is always a good practice.

4 Wireless Access with Dell W-Series Controllers

4.1 Topology

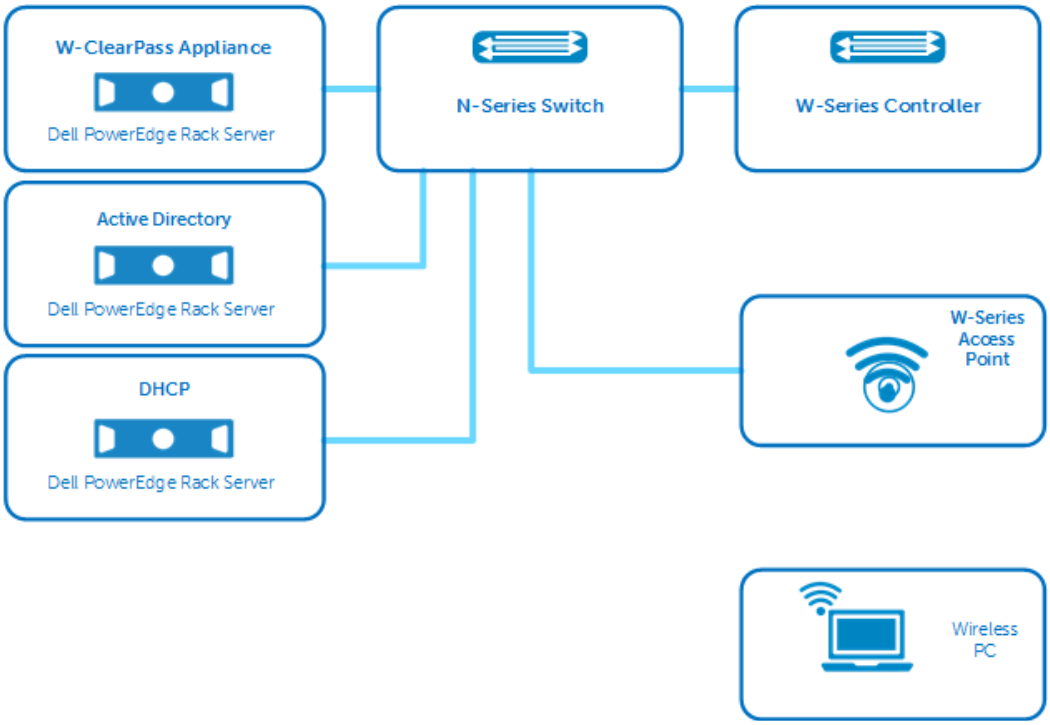

Figure 34 Wireless Topology

4.2 Example Scenario - Wireless

The following example details a typical scenario involving a user requiring access to a corporate or guest network. Posture compliance with OnGuard is the key feature demonstrated.

In this scenario, a user requires network access with a device not supplied by a corporate IT department and is connecting to network via a wireless connection.

1. The user connects to the network via a wireless SSID.
2. The user is prompted for credentials to access the network.
3. W-ClearPass authenticates the user's credentials.
4. W-ClearPass detects if OnGuard has been installed and if the device is healthy.
   d. If OnGuard is installed and the device is healthy, W-ClearPass places the user in the appropriate User Role.
   e. If OnGuard is installed and the device is not healthy, W-ClearPass places the user in a quarantine User Role.
   Users are automatically re-authenticated once the issue is resolved and placed into the appropriate User Role. In some cases, auto-remediation can perform changes without user action.

f. If OnGuard has not been installed, the user is automatically redirected to a webpage to run a one-time scan, or to install the OnGuard persistent client.
   OnGuard scans the device and determines if the client is compliant with the health policy.
   i. If healthy, W-ClearPass places the user in the appropriate vlan.
   ii. If not healthy, W-ClearPass places the user in a quarantine vlan
   Users are automatically re-authenticated once the issue is resolved and placed into the appropriate User Role. In some cases, auto-remediation can perform changes without user action.

The scenario detailed above can be used for any type of guest or employee network. The example in this paper uses a single employee vlan. The user is assigned a full access Employee Role or a restricted Quarantine Role. Administrators can setup W-ClearPass to assign users to different Roles to support guests, contractors or employees.

The credentials used in this example are username/password, and are stored in a Windows Server Active Directory. Any authentication type, including certificates, can be used with OnGuard posture policies. This guide does not go into detail on configuring all authentication types. For further information on BYOD topics through Onboard and Guest access, please see the W-ClearPass User Guide or other available deployment guides at www.dell.com/support/.

The configuration examples in sections 4.3 and 4.4 detail a basic solution utilizing W-ClearPass OnGuard and an N-Series switch. All scenarios contain a policy decision and enforcement based on posture information from OnGuard.

The configuration for the W-Series controller remains the same regardless of the type of OnGuard client or OS used. The configuration for W-ClearPass will differentiate between the following combinations of OnGuard client types and PC OS:

OnGuard Persistent application
OnGuard Dissolvable application
Windows 7/8
Mac OSX
Linux Ubuntu

The solution will enable a webpage hosted by W-ClearPass for access to both OnGuard application types for employees and guests scenarios. See the Creating an OnGuard Landing Webpage section for details.

4.3 Dell W-Series Controllers Configuration – Wireless

The full configuration necessary to enable wireless access has many components and options. This example assumes the administrator has a fully functioning basic WLAN configuration. The administrator should configure the following prior to implementing this example.

Controller Network settings – VLANs, Ports, IP
AP configuration – AP Group, Virtual AP, SSID
AP Installation – APs provisioned to an AP Group

For more information on basic configuration, see the Dell Networking W-Series ArubaOS User Guide.

The configuration settings in this section are crucial to enable the authentication and access per the OnGuard example scenario.

Note: Most configuration changes require the administrator to commit the change by pressing the **Apply** button. This saves the change to the running config. Clicking on another area of the GUI before committing the changes will cause the changes not to be saved. Clicking **Save Configuration** saves the running config to the start-up config. The instructions below do not detail when to save the configuration.

4.3.1 Define 802.11 Security

1. Navigate to Wireless > AP Configuration, on the Configuration tab click the "*AP Group Name*".
   Note: AP group names, SSIDs, and other descriptive settings are unique to this example. Screenshots will show the names as used in the test setup.
2. Expand **Wireless LAN** + **Virtual AP** + **SSID** (Figure 35).
   Figure 35 shows authentication and encryption settings of the Virtual AP within the *"AP Group"*. Administrators may keep their current security settings. W-ClearPass will support all types and sources used by the W-Series controller.
3. Select **WPA2** and **AES** using the radio buttons in the **802.11 Security** section.

Figure 35 SSID Profile – 802.11 Security

4. Click **Apply** to commit the changes.

4.3.2 Set W-ClearPass as the RADIUS Server

1. Navigate to **Security > Authentication,** on the **Servers** tab, select **RADIUS Server** (Figure 36).
2. Add **W-ClearPass**, specify the Host, Key and NAS IP.

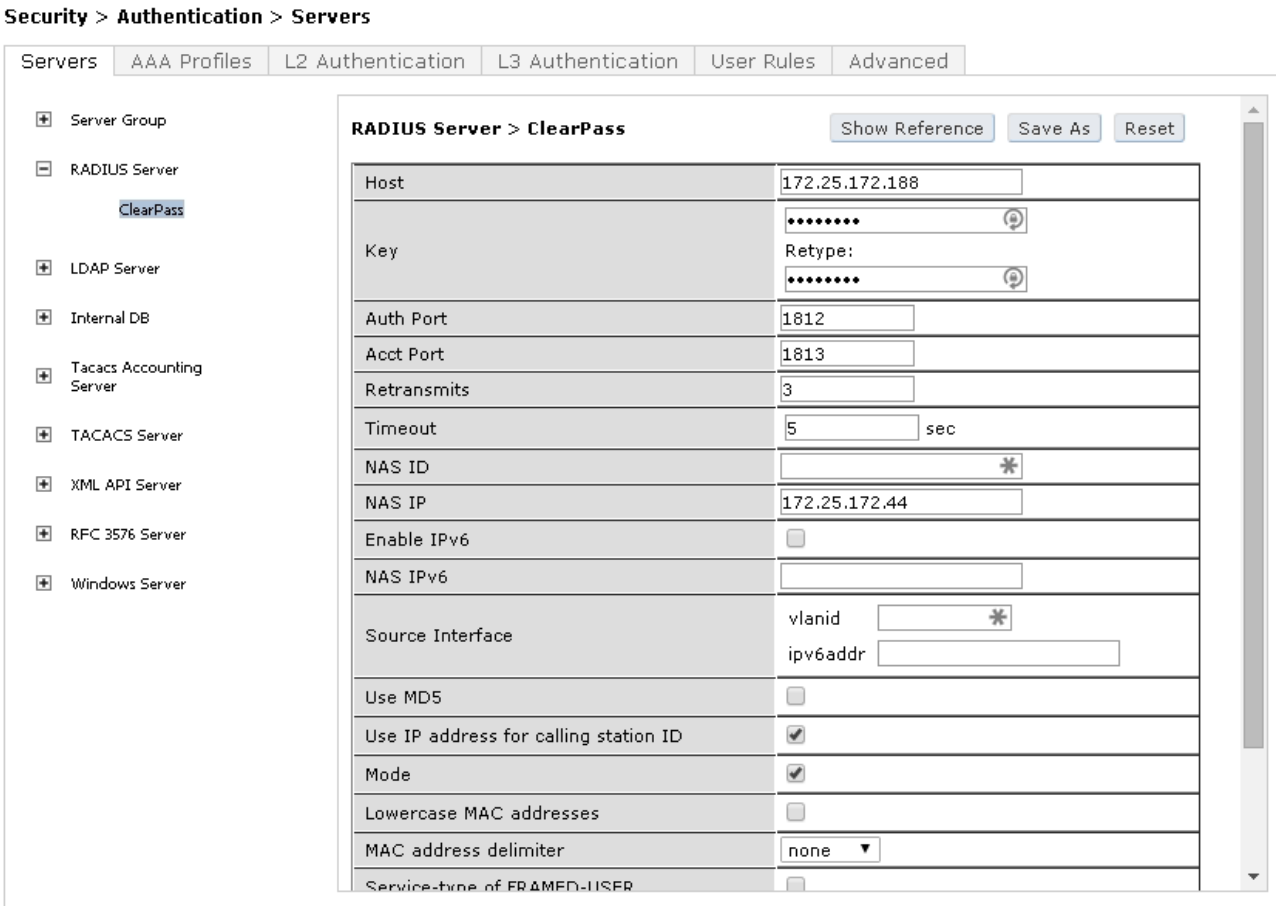

Figure 36 RADIUS Server settings

3. Click **Apply** to commit the changes.

4.3.3 Set W-ClearPass as the RFC 3576 Server

1. Navigate to **Security > Authentication,** on the **Servers** tab, select **RFC 3576 Server** (Figure 37).
2. Add the server using the IP address of W-ClearPass.
3. Specify the Key.
4. Click **Apply** to commit the changes.

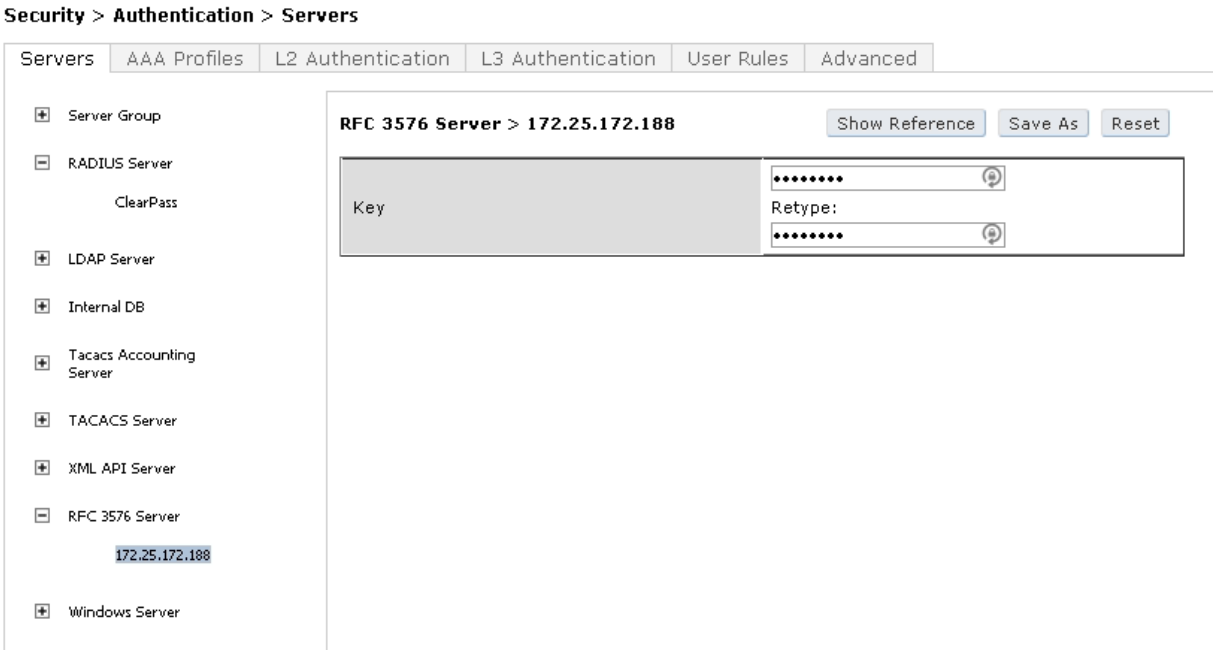

Figure 37 RFC 3576 Server

4.3.4 Create a Server Group

1. Navigate to **Security > Authentication,** on the **Servers** tab, select **Server Group** (Figure 38).
2. Add a server group using a descriptive name (example: **Employee_CPDG_svrgrp-vgs43**).
3. Under **Servers**, click the **New** button.
4. Under **Server Name**, use the dropdown menu and choose the **W-ClearPass Radius sever** previously configured.
5. Click Add Server.
6. Click **Apply** to commit the changes.

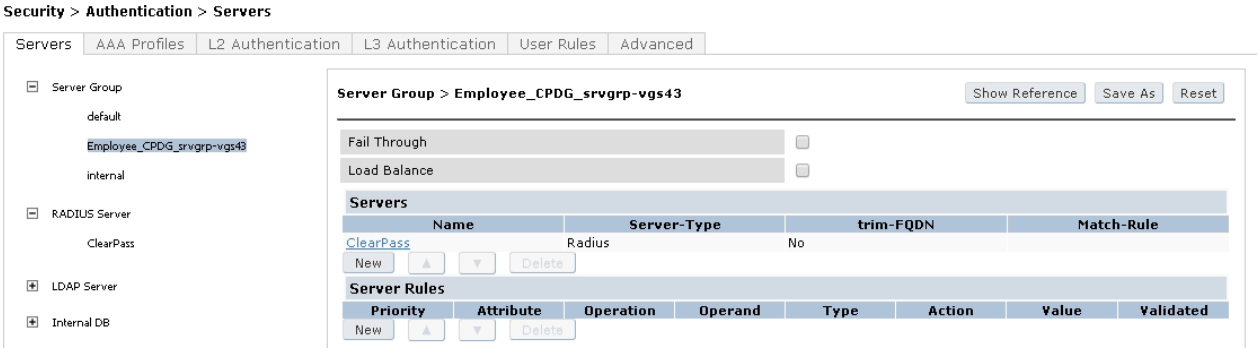

Figure 38 Server Group

4.3.5 Define User Roles

This example contains two roles. If the device is healthy, the user is assigned an “Employee” role. To keep it simple, this example uses an “Employee” role with just an “allow-all” policy. If the device is not healthy, the user is assigned a quarantine role to allow only a set of restricted protocols and destinations. In this example, the user will only be allowed to access the W-ClearPass server OnGuard landing webpage. The details of this landing page are shown in the Creating an OnGuard Landing Webpage section.

4.3.5.1 Creating an Employee User Role

1. Navigate to **Security > Access Control,** select the **User Roles** tab. (Figure 39).
2. Click **Add**.
3. Enter a Role Name under Misc. Configuration (example: Employee).
4. Select the appropriate **Role VLAN ID**.
5. Click **Add** under the **Firewall Policies** tab.
6. Select Choose From Configured Polices, choose allowall (session) from the dropdown menu.
7. Click the **Done** button.
8. Click **Apply** to commit the changes.

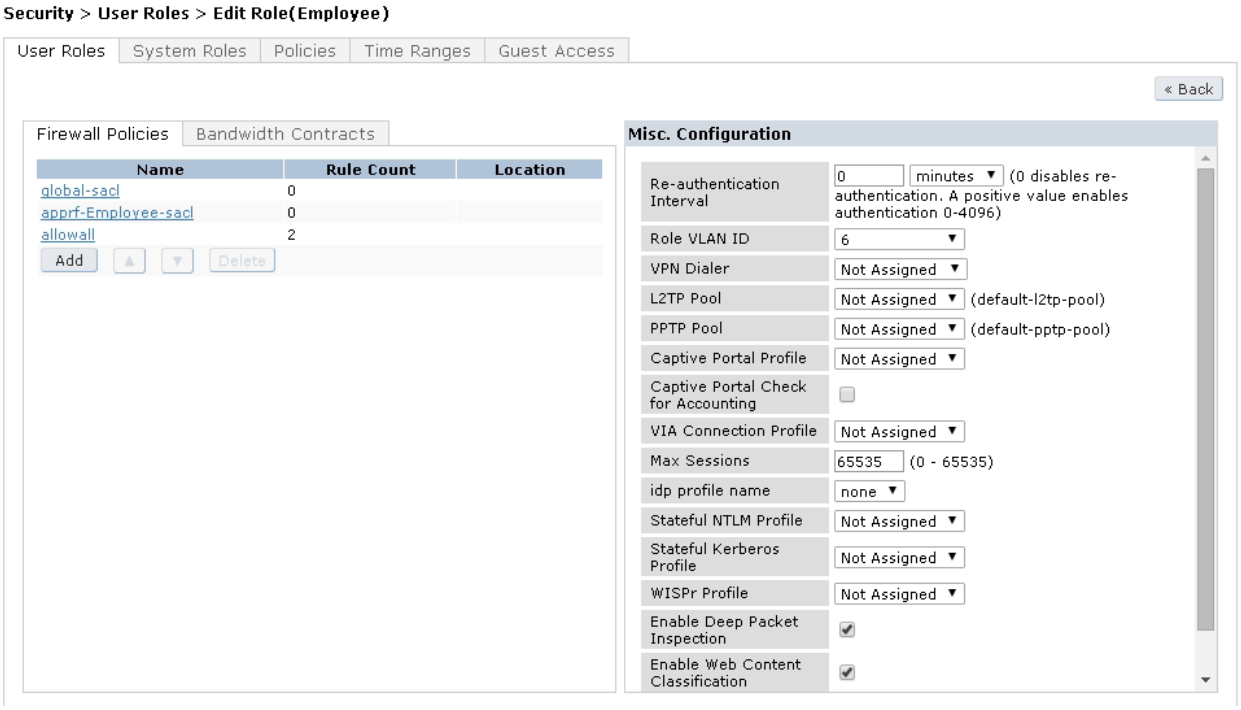

Figure 39 Employee Role

4.3.5.2 Creating a Quarantine User Role

Create a Destination Alias

The first step is to create a destination alias, which will be used in the firewall rules.

1. Navigate to **Advanced Services** > **Stateful Firewall,** select the **Destinations** tab (Figure 40).
2. Click **Add**.
3. Enter a descriptive Destination Name (example: **OnGuard-page**).

4. Click **Add** under **Type**.
5. Select **host** from **Rule Type** dropdown menu.
6. Enter the IP Address of W-ClearPass server.
7. Click **Add**.
8. **Apply** configuration.

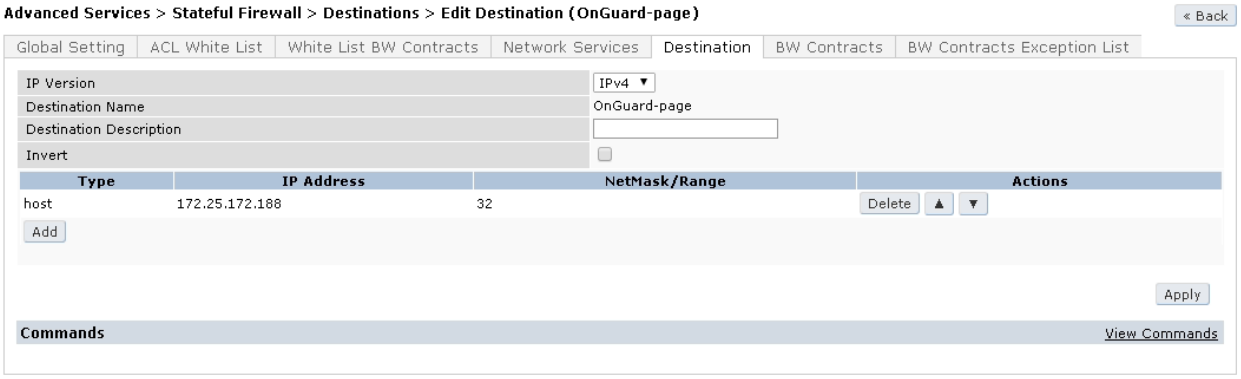

Figure 40 Destination configuration

Create a Quarantine User Role

1. Navigate to Security > Access Control, select the User Roles tab.
2. Click **Add**.
3. Enter a Role Name under **Misc. Configuration** (example: **OnGuard-redirect**).
4. Select the appropriate **Role VLAN ID** (example uses the same vlan as employee vlan).
5. Click **Add** under the **Firewall Policies** tab.
6. Select Create New Policy, click Create.
7. Enter a descriptive Policy Name (example: **Allow_Access_OnGuard_Weblogin_page**).
8. Select **Session** as the Policy Type.
9. Click **Add**.
   Select the following (leave others as default):

Source – **user**.
Destination – **alias** – select **OnGuard-page** (destination from previous steps).
Service/Application – **service** – select **svc-http (tcp 80)**.
Action – **permit**.

10. Click **Add**.
11. Click **Add**.
    Select the following (leave others as default):

Source – **user**.
Destination – **alias** – select **OnGuard-page** (destination from previous step).
Service/Application – **service** – select **svc-https (tcp 443)**.
Action – **permit**.

12. Click **Add**.
13. Click **Done**.

Note: Administrators will need to add rules to this firewall policy to enable access to services and hosts that are key to joining and authenticating to the network. One example of a service needed to communicate while in this quarantine role is DHCP. In Figure 41, only the http(s) rules with the destination alias are shown.

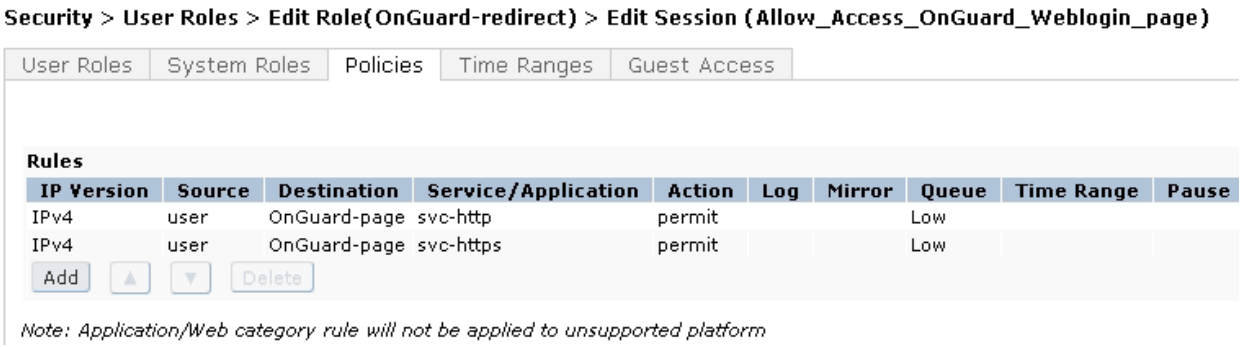

Figure 41 Firewall Rule for user role

14. Click **Add** under the **Firewall Policies** tab (Figure 42).
15. Select Choose From Configured Polices, choose captiveportal (session) from the dropdown menu.
16. Click Done.
17. Click **Apply** to commit the changes.

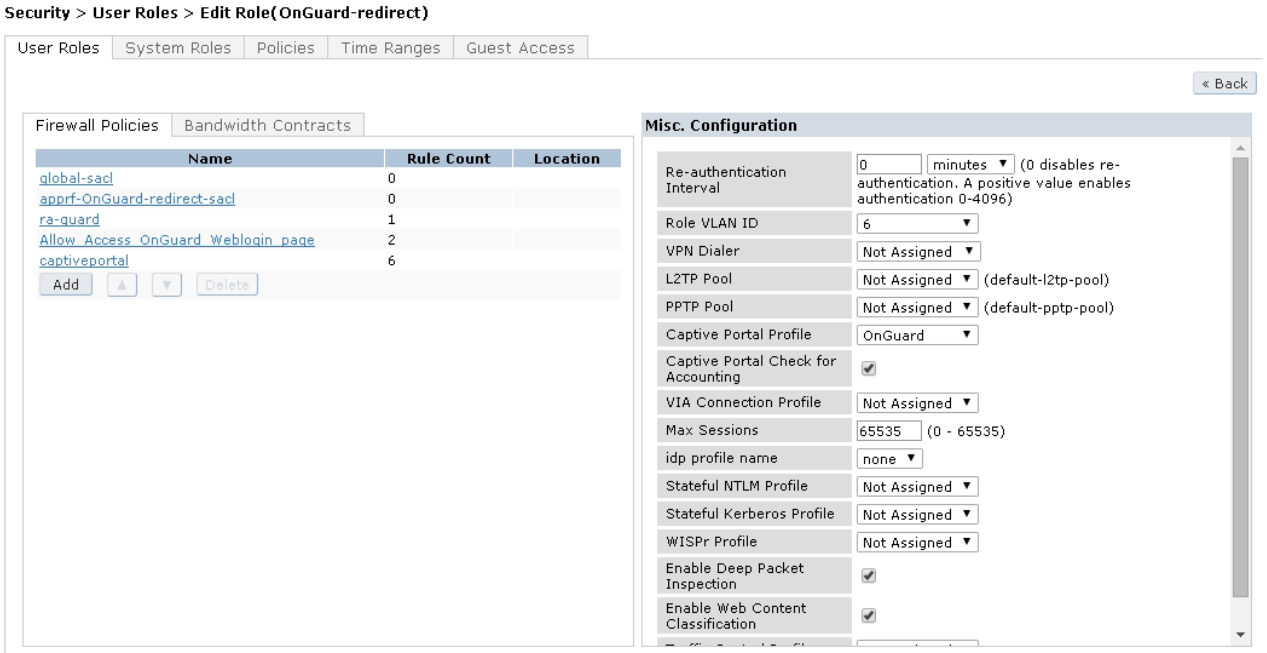

Figure 42 Quarantine user role

Note: The **Captive Portal Profile** setting under **Misc. Configuration** shows an **OnGuard** profile in the figure above. This profile will be created in the next steps. This role must be revisited to set this profile after creating it.

4.3.6 Create Captive Portal Authentication Profile

This example utilizes a captive portal for users to access the OnGuard installation files. Users that do not have OnGuard installed can open a browser and be redirected to a webpage instructing the user to run a health scan. This is an easy, no-touch method to provide access to installation links. Details on building the webpage are shown in the Creating an OnGuard Landing Webpage section.

1. Navigate to Security > Authentication, select the L3 Authentication tab > Captive Portal Authentication.
2. Enter a descriptive name, click **Add** (example: **OnGuard**).
3. Click the name that was added under **Captive Portal Authentication** in the left-hand column.
4. Under **Default Role** select the quarantine role previously created (example: **OnGuard-redirect**).
5. Under **Default Guest Role** select the quarantine role previously created (example: **OnGuard-redirect**).
6. Under **Login** page, the URL for the landing page described above should be entered. For this example, the configured webpage is hosted on W-ClearPass. The URL in this example is **http://172.25.172.188/guest/OnGuard.php**. This page name will be used in the Creating an OnGuard Landing Webpage section.
7. Click **Apply** to commit the changes.
8. Click the **Server Group** setting located under the profile created above.
9. Under the **Server Group** dropdown menu, choose the server group created previously (example: **Employee_CPDG_svrgrp-vgs43**).
10. Click **Apply** to commit the changes.

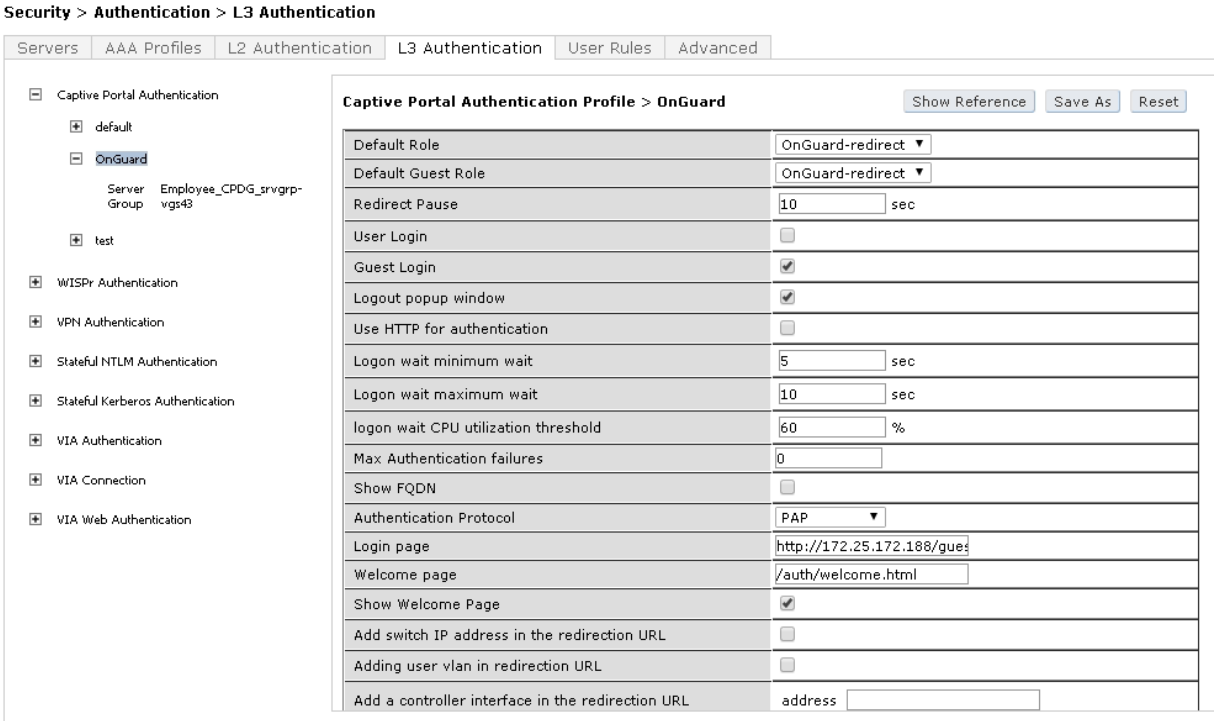

Figure 43 Captive Portal Profile

4.3.7 Update the Quarantine User Role

Now that the captive portal profile has been created, the quarantine user role is updated.

1. Navigate to Security > Access Control, select the User Roles tab.
2. Click **Edit** corresponding to the quarantine user role (example: **OnGuard-redirect**).
3. On the right-hand side, under **Captive Portal Profile**, select the profile created in the last step (example: **OnGuard**).
4. Under **Captive Portal Check for Accounting**, ensure the checkbox is selected.
5. Click **Apply** to commit the changes.

4.3.8 Add AAA Profile

Note: Administrators may already have a functional AAA profile. Modifying the existing profile is also an option.

1. Navigate to Security > Authentication, select the AAA Profiles tab.
2. Click **Add**.
3. Enter a descriptive name (example: **Employee_CPDG-aaa_prof**) and click **Add**.
4. Click the name to edit the profile.
5. Under **Initial role**, select the quarantine role created previously (example: **OnGuard-redirect**). This setting ensures the initial role given to any user is the role designated for devices with unknown health status. The other settings can remain default for this example. It is always a good practice to specify all default role settings per your network security policies.
6. Click **Apply**.
7. Click the **802.1x Authentication Server Group** setting located under the profile created above.
8. From the dropdown menu, choose the server group created previously (example: **Employee_CPDG_svrgrp-vgs43**).
9. Click **Apply** to commit the changes.
10. Click the **RADIUS Accounting Server Group** setting located under the profile created above.
11. From the dropdown menu, choose the server group created previously (example: **Employee_CPDG_svrgrp-vgs43**).
12. Click **Apply** to commit the changes.
13. Click RFC 3576 server.
14. Enter the IP address of the ClearPass server in the box, click **Add**.
15. Click **Apply** to commit the changes.
16. Click the IP address, and enter the same key used for the RADIUS Server settings.
17. Click **Apply** to commit the changes.

All other settings can remain default.

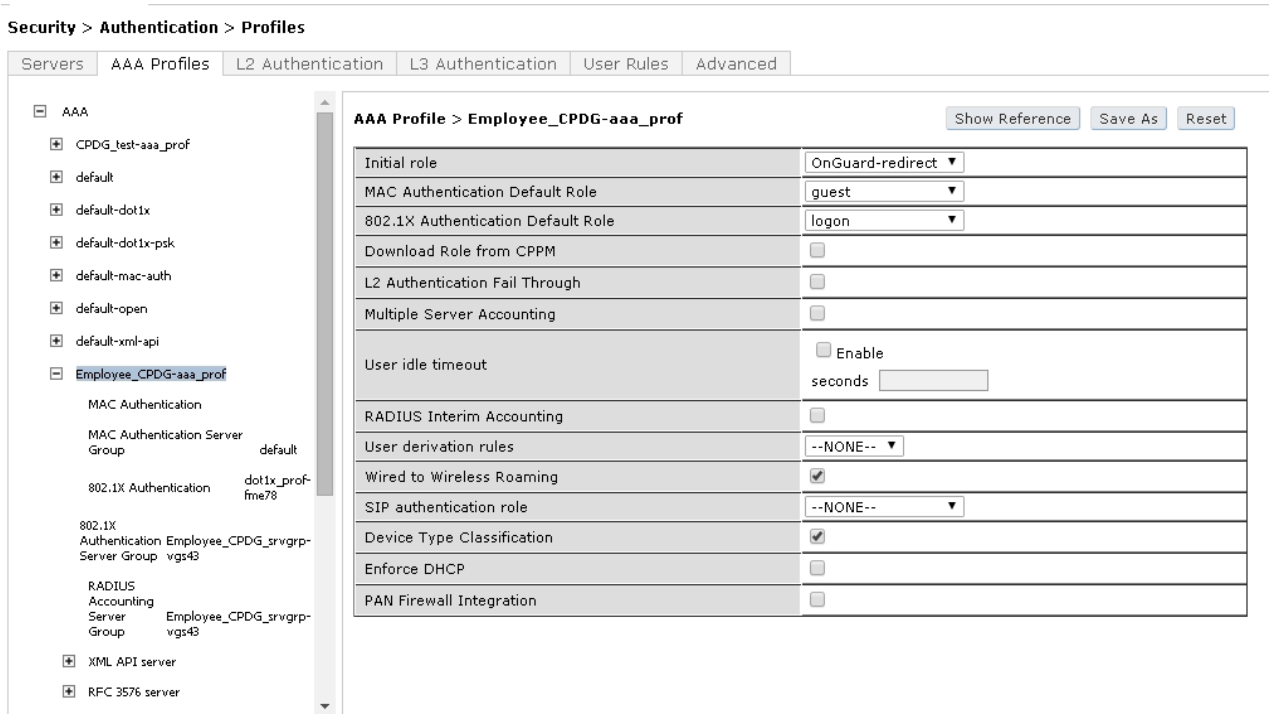

Figure 44 AAA profile

4.3.9 Add the AAA Profile to the Virtual AP Profile

The AAA profile needs to be used within the Virtual AP profile used for wireless user access.

1. Navigate to Wireless > AP Configuration, on the Configuration tab click the "*AP Group Name*".
2. Expand Wireless LAN + Virtual AP.
3. Click the Virtual AP profile in use (example: **Employeee_CPDG-vap_prof**).
4. Click the **AAA** setting.
5. Under the **AAA Profile** drop down menu, select the profile created in the previous step (example: **Employee_CPDG-aaa_prof**).
6. Click **Apply** to commit the changes.

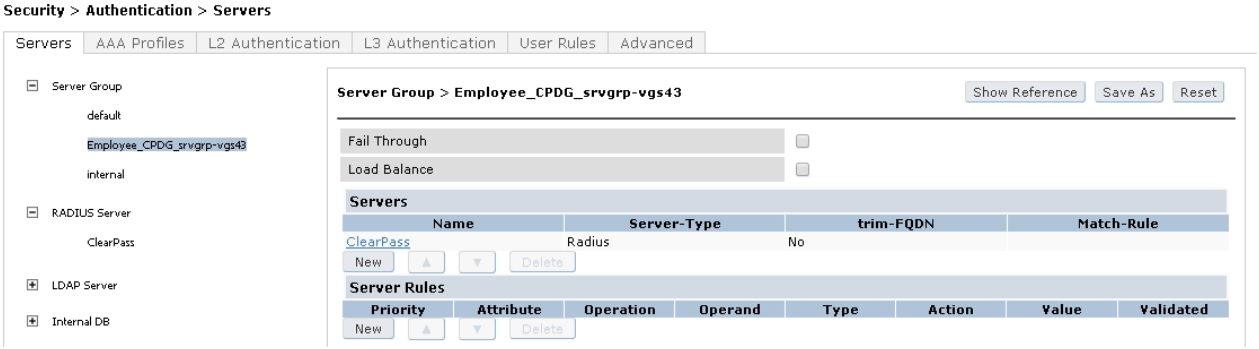

Figure 45 Server Group

4.4 Dell W-ClearPass Configuration - Wireless

W-ClearPass is configured via a GUI on standard browsers. This guide will show the key steps and screenshots for configuring the example scenario. The entire browser window is not shown in each screenshot to improve readability. In most cases, the navigation window on the left hand side of the screen is not shown. To ensure readers understand the configuration location currently shown, the navigation path is given before each screenshot. Within each major section, the current tab is highlighted with a dark blue color.

W-ClearPass allows administrators to configure policies and profiles directly from the main service configuration screen. When using this method of configuration, the necessary windows are opened automatically, which can streamline the amount of time it takes an experienced user to configure a fully functional service. In this guide, each profile and policy will be built prior to the creation of the service to aid in the description of navigating this configuration in this document.

Note: This guide does not detail the initial setup of the W-ClearPass server. For more information on VM install, initial server configuration and licensing; refer to the W-ClearPass User Guides at www.dell.com/support

4.4.1 Add W-Series as a Network Device

Before W-ClearPass will recognize authentication requests, the controller originating the request must be added to the list of network devices in W-ClearPass. The IP Address and RADIUS shared secret must match the configuration used on the controller (Figure 46).

1. From the W-ClearPass Welcome screen, click the ClearPass Policy Manager module.
   The ClearPass Policy Manager opens.
2. Navigate to the Network Devices page by selecting, Configuration > Network > Devices.
3. Click **+Add**.
   The **Add Device** window opens.
4. Enter the Name of the switch, IP Address, Description and RADIUS Shared Secret (Figure 46).
5. Select **Aruba** from the **Vendor Name:** dropdown box.
6. Click **Add**.

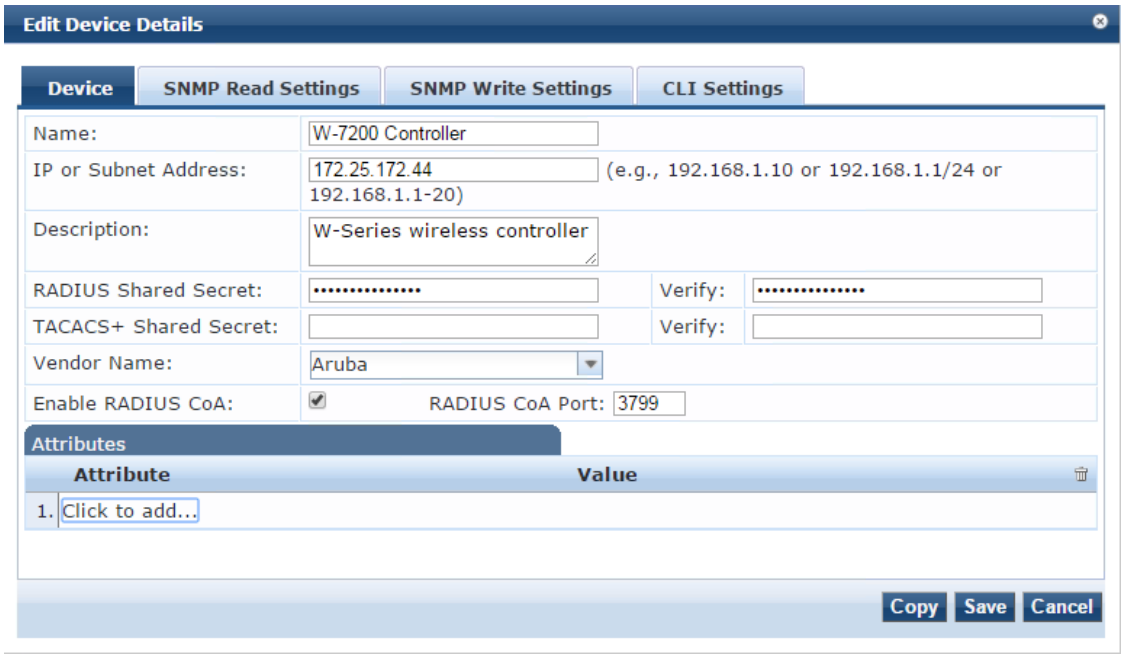

Figure 46 W-Series device settings

4.4.2 Add Active Directory as an Authentication Source

Note: This is the same step documented previously in the wired example.

1. To Add Active Directory as an authentication source, open the **Authentication Sources** page by selecting **Configuration > Authentication > Sources**.
2. Click **+Add**.
3. Enter details for the authentication source as shown in Figure 47.

Figure 47 shows a partial configuration of the Active Directory Authentication Source. This example uses a Windows Server with Active Directory installed as the source for username/password credential store. W-ClearPass supports many different authentication sources. For more details on Active Directory configuration and other source types, see the W-ClearPass User Guide at www.dell.com/support.

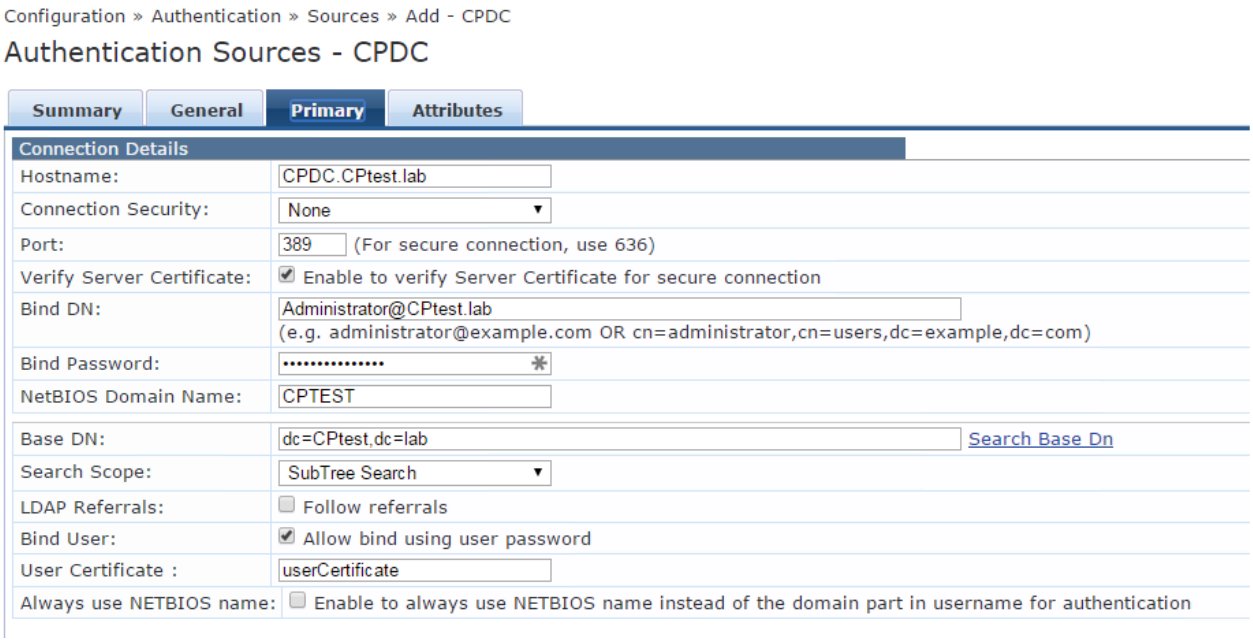

Figure 47 Active Directory Authentication Source

4.4.3 Create 802.1x Wireless Service with Posture Checks

W-ClearPass includes templates for many common services. These templates allow administrators to easily build the services and their associated policies. This section details the use of the *Aruba 802.1X Wireless* template located in the **Start Here** section within **Configuration**.

Figure 48 Aruba 802.1X Wireless Template

1. To create an 802.1x Wireless Service with Posture checks, navigate to **Configuration > Start Here**.
2. Select **802.1x Wireless** (Figure 48).
   The **General** tab (Figure 49) opens.

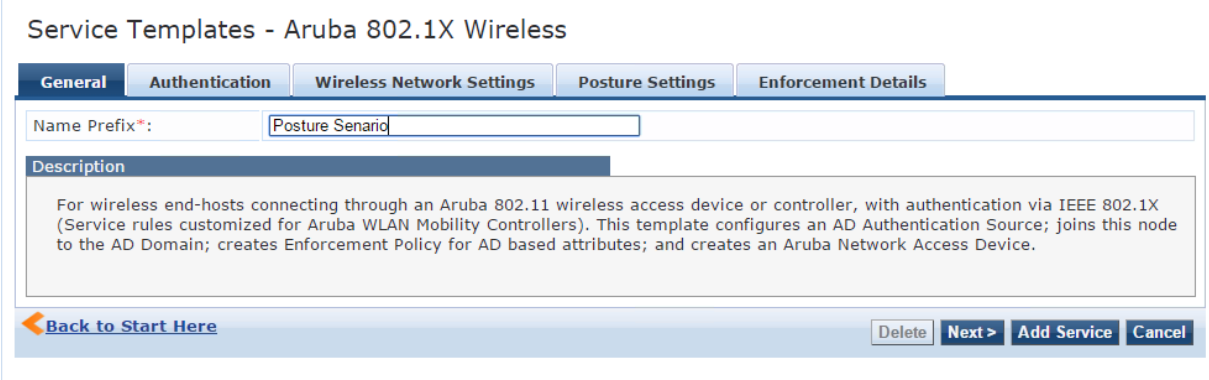

Figure 49 Aruba 802.1X wireless – General Tab

3. Type in the name prefix to identify the service name and policy names generated by the template. The name ***802.1X Wireless*** will be appended to the name prefix.
4. Click **Next >**.
   The **Authentication** tab (Figure 50) opens.

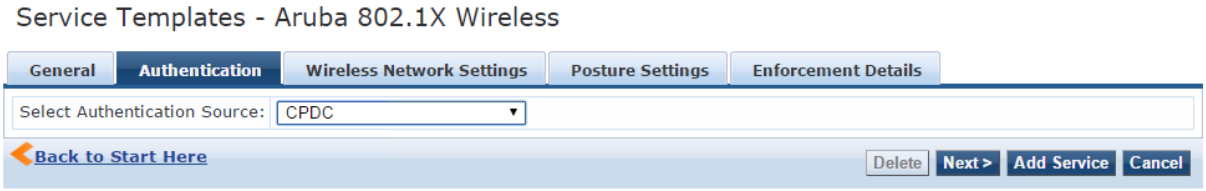

Figure 50 Aruba 802.1X wireless – Authentication Tab

5. From the dropdown menu, select the Authentication Source that was configured in the previous steps. Additional authentication sources can be added later.
6. Click **Next >**.
   The **Wired Network Settings** tab (Figure 51) opens.

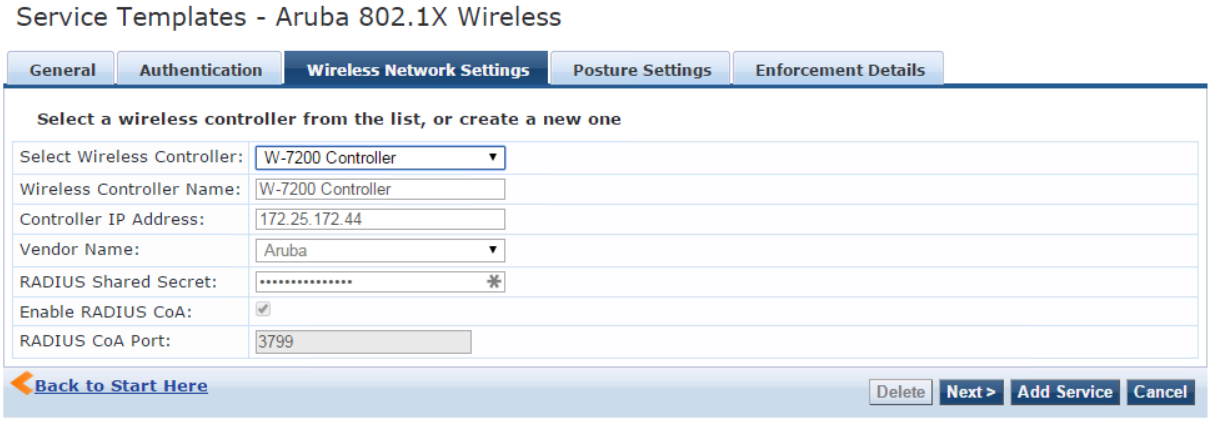

Figure 51 Aruba 802.1X wireless – Wireless Network Settings Tab

7. From the dropdown menu, select the network device (W-Series controller) that was configured in the previous steps.

8. Click **Next >**
   The **Posture Settings** tab (Figure 52) opens.

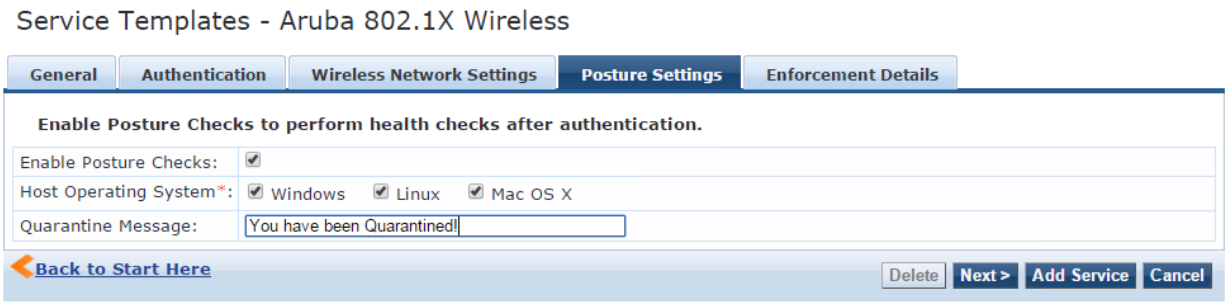

Figure 52 Aruba 802.1X wireless – Posture Settings Tab

9. Select the operating systems OnGuard needs to support.
10. Enter a Quarantine Message in the **Quarantine Message:** field.
    This message is displayed anytime OnGuard detects a posture compliance issue.
11. Click **Next >**
    The **Enforcement Details** tab (Figure 53) opens.

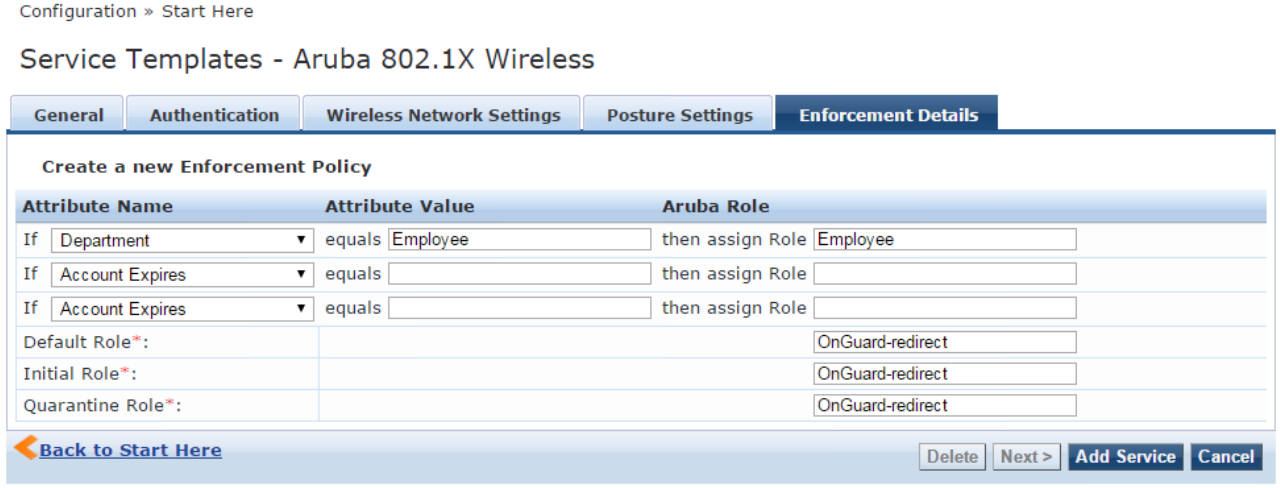

Figure 53 Aruba 802.1X wireless – Enforcement Details Tab

12. Enter in the user role information configured on the wireless controller. User Role names must match exactly. These settings can be changed and added to later.
13. Click **Add Service**.
    Two Services are now added to the list of **Services** (Figure 54). (Numbering may vary between deployments).

The services can be viewed by navigating to **Configuration > Services**. The two Services shown in Figure 54 will be modified after the Posture, Role Mapping and Enforcement Policies are configured.

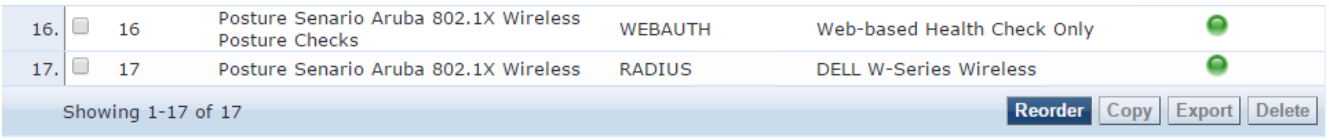

Figure 54 Services added from template wizard

4.4.4 Define Posture Policies

The Aruba 802.1x Wireless template creates three posture policies (Figure 55) with the prefix name used in the template. These policies are identical to the policies generated during the wired example.

Administrators can use the same policies for both wired and wireless to simplify the configuration. In this example, using the previous policies will easily work.

Figure 55 Posture Policy List

If the wired example has not been completed in your network, go to the Wired Define Posture Policies section and configure the posture policy. Return to this section after completing the posture profile configurations.

4.4.5 Define Roles and Role Mappings

Role Mappings are used to apply conditions to each user to classify them into Roles. The Roles are then used to identify users and can be used to enforce policies within the Service. There are numerous conditions and rules that can be used to form a Role Mapping. For more information on Roles and Role Mapping, refer to the W-ClearPass Policy Manger User Guide at www.dell.com/support.

For the purpose of this guide, this example will use default Roles built into the W-ClearPass Policy Manger. The two Roles being used are **[Employee]** and **[Guest]**. Default configurations in W-ClearPass are identified by the brackets surrounding the name.

4.4.5.1 Create a new Role Mapping

1. Navigate to **Configuration > Identity > Role Mappings** (Figure 56).
2. Click the **+ Add** link in the upper right hand corner.
3. Name the policy. For this example, the name ***W-Series Wireless Role Mapping*** is used. In the **Default Role** drop down, choose **[Guest]**.
4. Click **Next >**.
5. On the **Mapping Rules** tab, click **Add Rule**.
   The **Rules Editor** opens (Figure 56), enter the following.
   - Type: **Authorization: CPDC** (name of the Active Directory used in this example)
   - Name: **Department**
   - Operator: **CONTAINS**
   - Value: **Employee** (value used in the department field of an Active Directory user account)

6. Use the **[Employee]** Role for the Role Name.

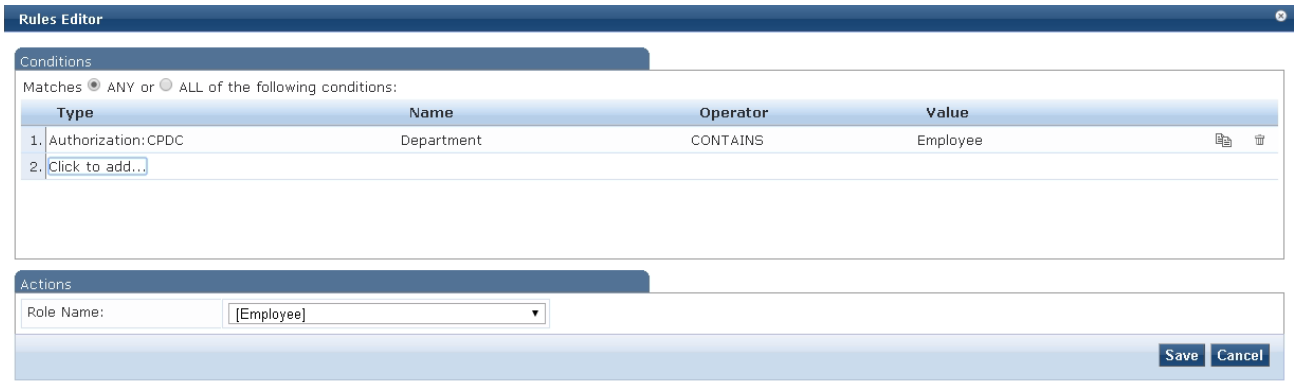

Figure 56 Role Mapping – Mapping Rule

Administrators can build sophisticated condition lists and any number of Rules to be as specific as needed to identify many types of users. This simplistic example will result in any user with the *Employee* department name in Active Directory being assigned the **[Employee]** Role. Any user that does not have this Active Directory department field populated with *Employee* will be assigned the default **[Guest]** Role.

7. **Save** the Rule.
8. **Next >** to move to the **Summary** tab.
9. Verify the information is correct, then click **Save**.
   The new role mapping will appear in the **Role Mapping** list.

The Role Mapping that was just created will be used in the 802.1x RADIUS Service. No Role Mapping will be used for the Health Check Service. A more detailed explanation of the two services is discussed later in this section.

4.4.6 Define Enforcement Policies and Profiles

Enforcement Policies are a group of rules with conditions that direct enforcement actions that ultimately are sent to the Network Access Device, which in this example is the W-Series controller. Enforcement profiles are a collection of attributes that define those enforcement actions.

The Aruba 802.1x Wireless template with posture checks produced two Services the Health Check Service and the Radius Service. Both of these services need Enforcement Policies, and their associated Enforcement Profiles. The Health Check Service will produce a posture token (by executing an action), while the Radius Service will use that token (within its conditions) to determine a User Role assignment action.

Enforcement Profiles are used within the Enforcement Policies, so the profiles are configured first.

4.4.6.1 Health Check Enforcement Profiles and Policies

Terminate Session Profile for the Health Check Service

The Health Check Service requires a profile to terminate the session so that the RADIUS 802.1X

authentication Service can use the posture token in a new authentication routine. The terminate session profile will utilize the Change of Authorization feature to force a re-authentication.

W-ClearPass has a default terminate session profile that can be used with the W-Series controller. The name of the profile is **[Aruba Terminate Session]**. This example uses the default profile.

Enforcement Policy for the Health Check Service

The following will detail an example of configuring the Enforcement Policy for the Health Check Service. The pre-populated policy from the template is sufficient for this example and most of the default settings are kept.

1. Navigate to the list of Enforcement Policies by selecting **Configuration > Enforcement > Policies**.
2. Click the pre-populated policy name for the Health Check Service.
   In this example, the name is ***Posture Scenario Aruba 802.1X Wireless OnGuard Agent Enforcement Policy***, and its type is ***WEBAUTH***. The template automatically generates this policy based on the prefix name.
3. Click the **Enforcement** tab.
4. Under the Default Profile, ensure the [RADIUS_CoA] Aruba Terminate Session is selected.
5. Navigate to the **Rules** tab (Figure 57).
   For the example in this guide, the pre-populated conditions and actions work well. No changes are made to the default conditions.

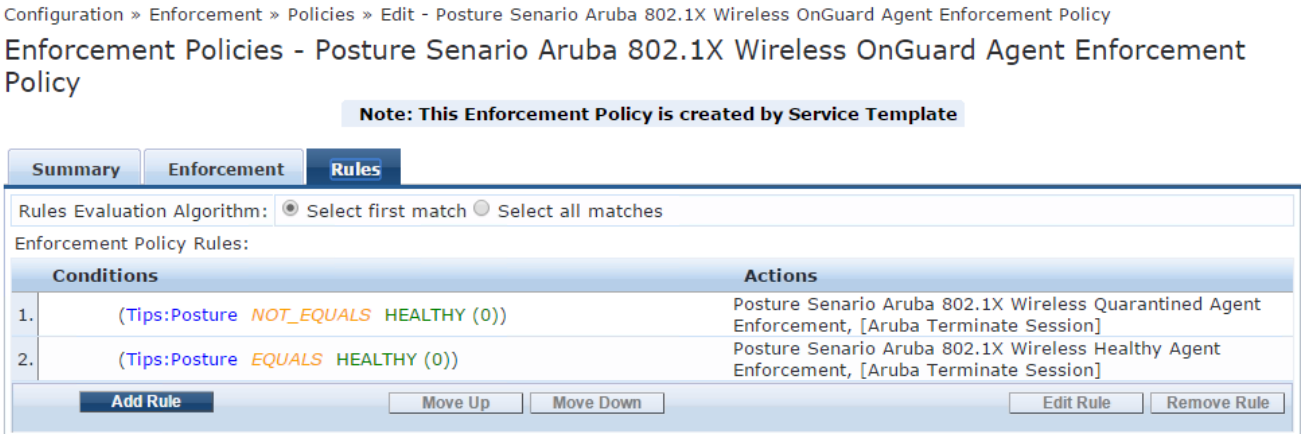

Figure 57 Enforcement Policy for OnGuard Service

The first condition states that any posture token values not equal to HEALTHY (0) will trigger this rule to be enforced. The Enforcement Profiles underneath the condition are the actions that will be applied if the conditions in this rule are met. The first profile in the list is named **[Agent] Posture Scenario Aruba 802.1X Wireless Quarantined Agent Enforcement**. This profile simply displays a quarantine message to the client. This profile can be seen in the list of Enforcement Profiles at **Configuration > Enforcement > Profiles**. The profile was also created from the Service template during the Service creation earlier. The settings for this profile are being kept as default and are not shown in this guide.

The second condition states that any posture token values equal to HEALTHY(0) will trigger this rule to be enforced. The Enforcement Profiles underneath the condition are the actions that will be applied if the conditions in this rule are met. The first profile in the list is named **[Agent] Posture Scenario Aruba 802.1X Wireless Healthy Agent Enforcement**. This profile simply displays a healthy message to the client. This

profile can be seen in the list of Enforcement Profiles at **Configuration > Enforcement > Profiles**. The profile was also created from the Service template during the Service creation earlier. The settings for this profile are being kept as default and are not shown in this guide.

This concludes the Enforcement Policy and profiles for the Health Check Service. The next steps detail the configuration for the policy and profiles used in the RADIUS 802.1X Service.

4.4.6.2 RADIUS 802.1X Enforcement Profiles and Policies

Enforcement Profile for RADIUS 802.1X Service

The RADIUS 8021.X Service requires an Enforcement profile to enable the assignment of a user role. In this example, a client device that fails a health check will be assigned to a quarantine user role named **OnGuard-redirect**. A client device that passes a health check will be assigned an employee user role named **Employee**. These user roles were previously configured in the W-Series controller.

The following steps create a profile to enforce a user role assignment.

1. Navigate to the list of Enforcement Profiles by selecting **Configuration > Enforcement > Profiles**.
2. Click the **+ Add** link in the upper right hand corner.
3. From the **Template** dropdown menu, choose **Aruba RADIUS Enforcement**
4. Name the policy.
   This example uses *W-Series Employee Role* as the profile name.
5. Leave all other settings as default, and click **Next >** to move to the **Attributes** tab.
6. On the attribute value, click the value **Enter role here**. Manually enter the name of the user roles configured on the W-Series controller for employees.
   In this example, **Employee** was the user role. Ensure the user role name exactly matches the user role name on the controller.
7. Save the attribute line by clicking the disk icon to the right.
8. Click **Next >** and review the **Summary** tab.
9. Click **Save**.
   The summary tab should look similar to the picture below (Figure 58).

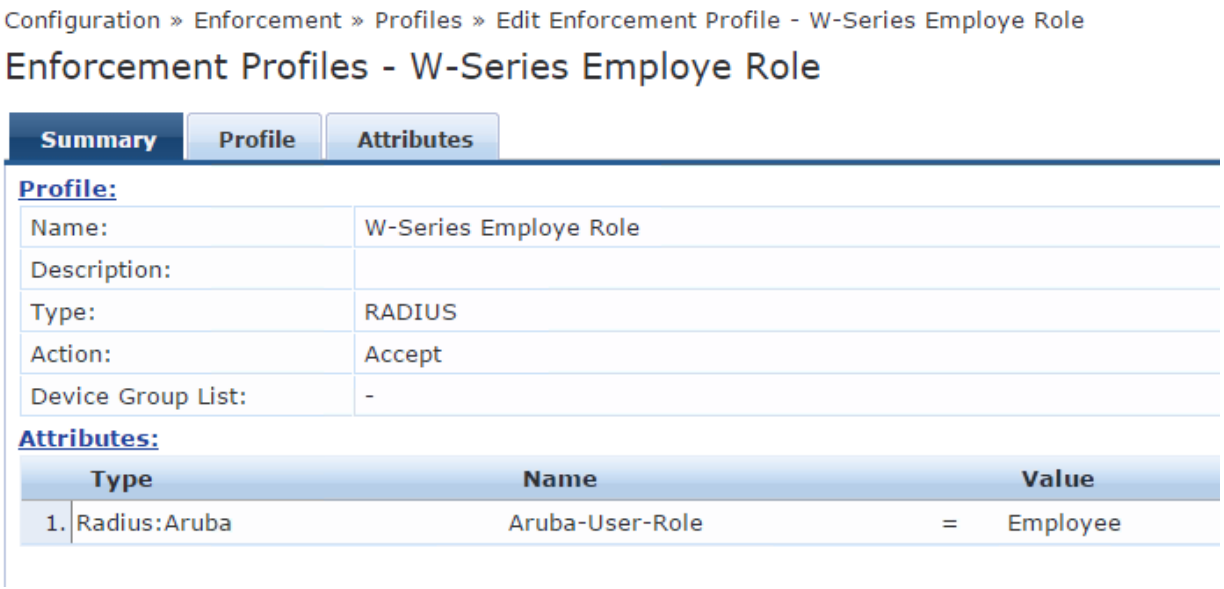

Figure 58 Enforcement Profile – Employee Role

The following steps create a profile to enforce a quarantine user role assignment.

1. Navigate to the list of Enforcement Profiles by selecting **Configuration > Enforcement > Profiles**.
2. Click the **+ Add** link in the upper right hand corner.
3. From the **Template** dropdown menu, choose **Aruba RADIUS Enforcement**.
4. Name the policy.
   This example uses *W-Series Redirect to OnGuard* as the profile name.
5. Leave all other settings as default, and click **Next >** to move to the **Attributes** tab.
6. On the attribute value, click the value **Enter role here**. Manually enter the name of the user roles configured on the W-Series controller for employees.
   In this example, **OnGuard-redirect** was the user role. Ensure the user role name exactly matches the user role name on the controller.
7. Save the attribute line by clicking the disk icon to the right.
8. Click **Next >** and review the **Summary** tab.
9. Click **Save**.

Enforcement Policy for the RADIUS 802.1X Service

The following steps configure the Enforcement Policy for the RADIUS 802.1X Service. The pre-populated policy from the template is sufficient for this example and many settings will be kept as default. The next steps will describe the contents of the Enforcement Policy.

1. Navigate to Configuration > Enforcement > Policies.
2. Click the pre-populated policy name for the Health Check Service.
   In this example, the name is ***Posture Scenario Aruba 802.1X Wireless Enforcement Policy***, and its type is ***RADIUS***. The template has automatically generated this policy based on the prefix name.
3. Click the **Enforcement** tab.
4. Under the Default Profile, choose **[W-Series Redirect to OnGuard]**.
   This example uses the quarantine profile to place users that fail authentication checks into the

quarantine user role. If the administrator chooses, a profile to deny access or place users into a different user role is possible here.

5. Navigate to the **Rules** tab. Remove all the default rules by selecting each rule and clicking **Remove Rule**.
   In this example, this authentication policy has only two outcomes given the correct credentials.
   - The user is authenticated, is identified as an Employee, and has a Healthy token
   - The user is authenticated, and does not have a Healthy token

   The first outcome will place the user in the employee user role **Employee**. The second outcome will place the user into a quarantine user role **OnGuard-redirect**.

   If the administrator has other user classifications and conditions, they can add them here at this time. Additional profiles or user roles may be required.

6. To configure rules per the example above, click **Add Rule**.
7. Create two conditions
   Note: The first condition must be saved before the second condition can be created.
   Condition 1

   - Type: **Tips**
   - Name: **Role**
   - Operator: **EQUALS**
   - Value: **[Employee]** (add other roles to the list here if applicable)

   Condition 2

   - Type: **Tips**
   - Name: **Posture**
   - Operator: **EQUALS**
   - Value: **HEALTHY (0)**

8. Under the Enforcement Profiles section, choose [RADIUS] W-Series Employee Role.
9. The **Rules Editor** windows should look like Figure 59 below.

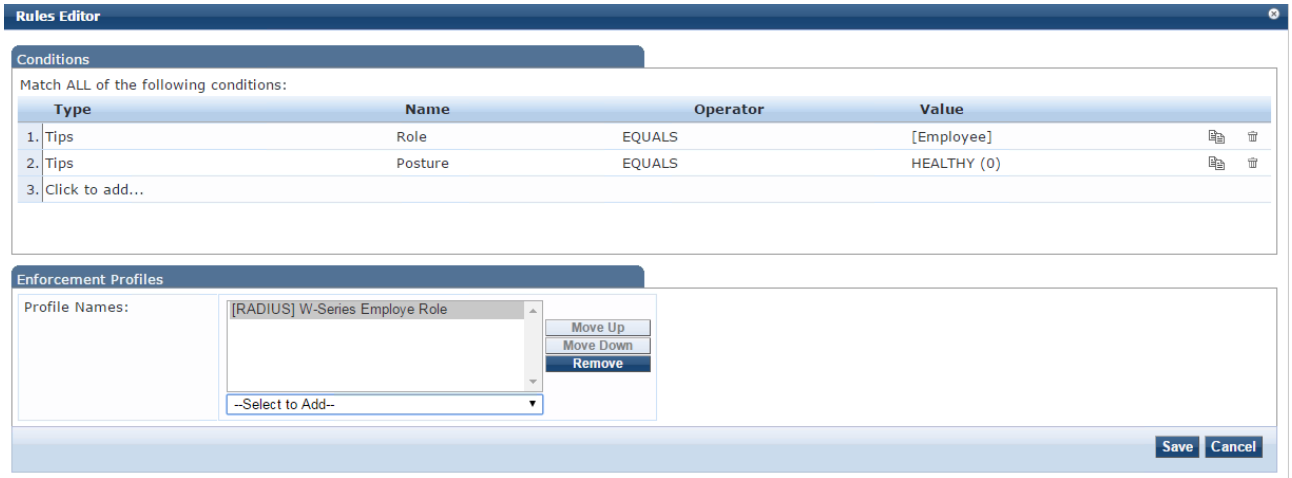

Figure 59 Enforcement Policy – Healthy Employee Rule

10. Click **Save**.
11. Create a second rule, click **Add Rule.**
12. Create two conditions.
    Note: The first condition must be saved before the second condition can be created.
    Condition 1
    - Type: **Tips**
    - Name: **Role**
    - Operator: **EQUALS**
    - Value: **[User Authenticated]**

    Condition 2
    - Type: **Tips**
    - Name: **Posture**
    - Operator: **NOT_EQUALS**
    - Value: **HEALTHY (0)**
13. Under the Enforcement Profiles section, choose [RADIUS] W-Series Redirect to OnGuard.
14. The **Rules Editor** windows should look like Figure 60 below.

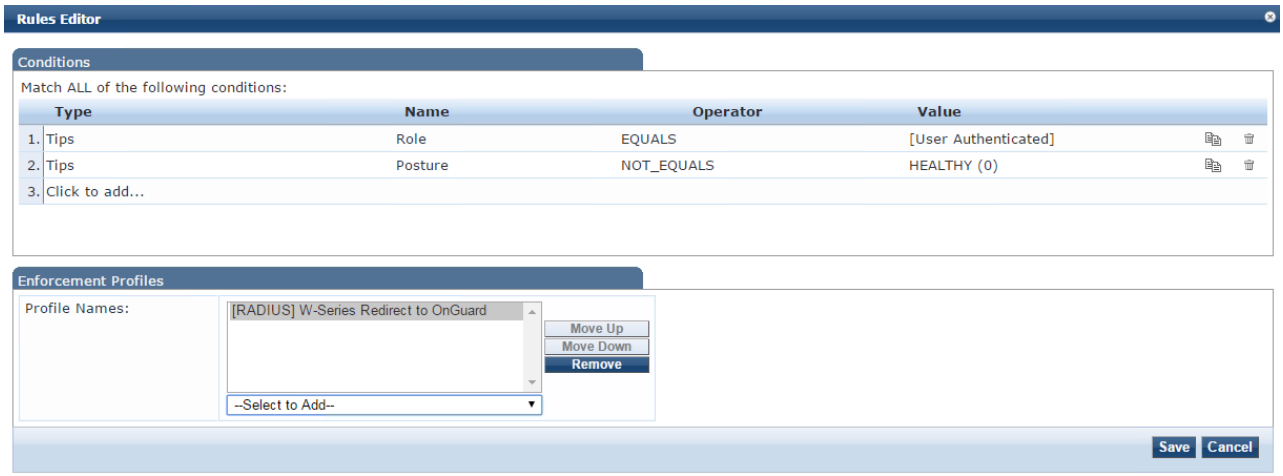

Figure 60 Enforcement Policy – Not Healthy Rule

15. Click **Save** to save the rule.
16. Click **Save** again to save the Enforcement Policy.

4.4.7 Configure the Services

Now that all the components of the Service are defined and configured, the Services themselves need to be configured.

1. Navigate to Configuration > Services.
2. Select Service: Posture Scenario Aruba 802.1X Wireless.
3. Select the **Service** tab.
   The template populates the Service Rules with two rules and requires all rules match. For this example, the only change will be to define the SSID name. Administrators can add other rules to narrow the devices that this Service will be applied to at any time.
4. Click the third rule and change **Operator** to **CONTAINS** and the **Value** to the name of the SSID of your network. In this example, the SSID name is **Employee_CPDG**. The Service tab should look like Figure 61.

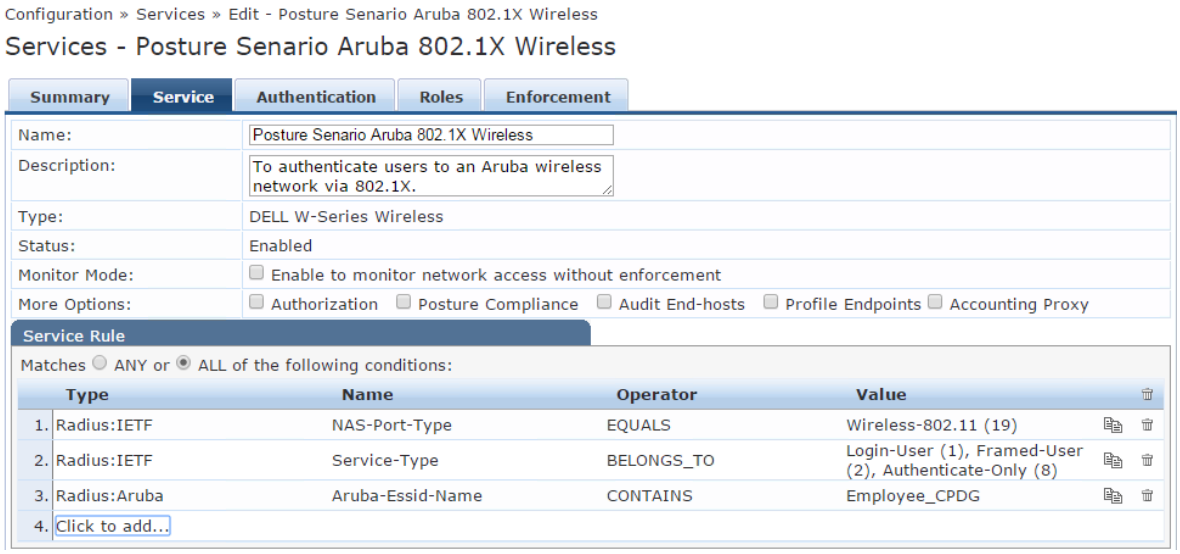

Figure 61 802.1X Wireless Service - Service tab

5. Move to the **Authentication** tab (Figure 62).
   This example uses Microsoft Active Directory with username/password for the credentials. Authentication methods for this example can be kept as default. Administrators can use any type of authentication method required by their network security policy.
6. Remove or add authentication methods.
7. Remove or add authentication sources as needed.

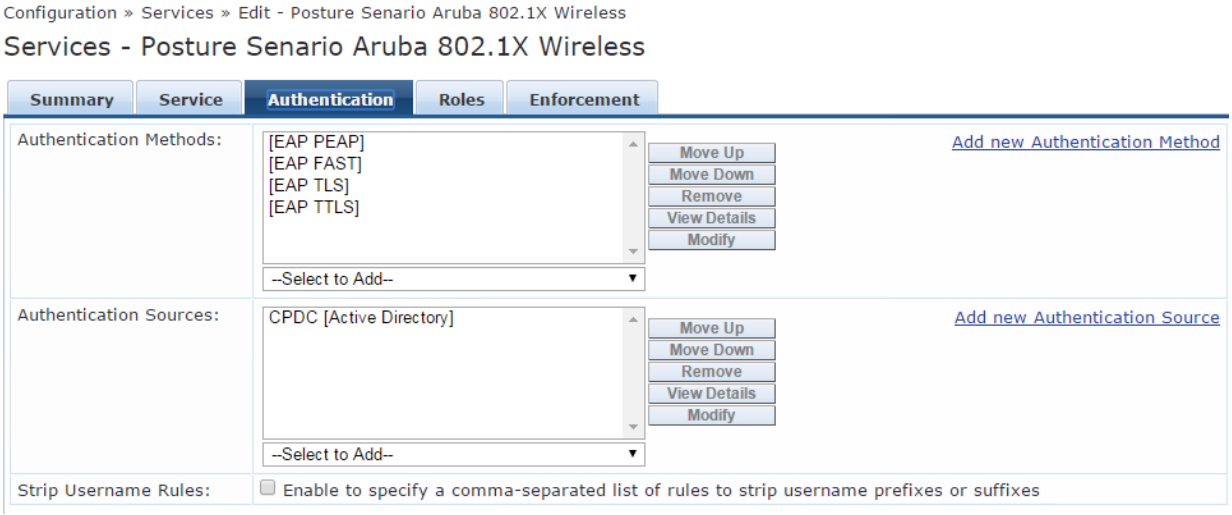

Figure 62 802.1X Wireless Service – Authentication tab

8. Move to the **Roles** tab (Figure 63).
9. For the Role Mapping Policy, select **W-Series Wireless Role Mapping** from the dropdown menu.

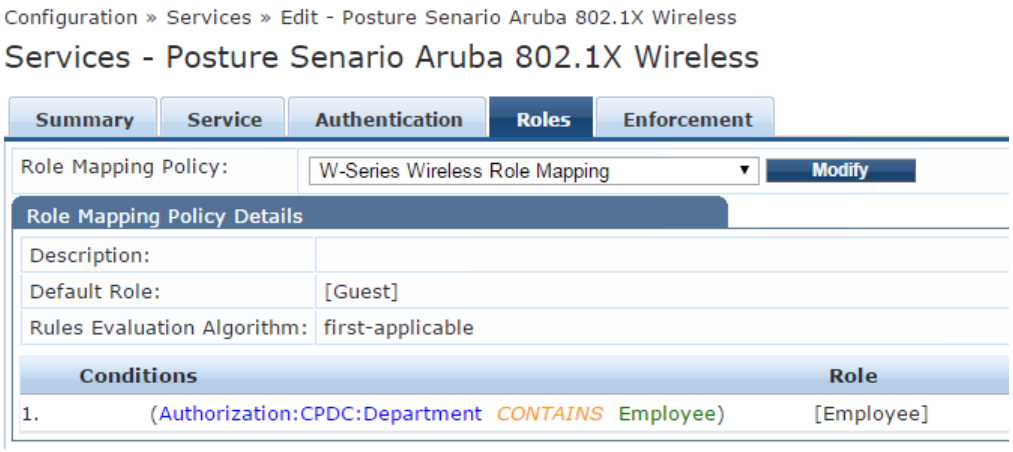

Figure 63 802.1X Wireless Service- Roles tab

10. Move to the **Enforcement** tab.
    The template has populated the appropriate Enforcement Policy in the dropdown menu.
11. Verify that the correct policy details are shown (Figure 64).

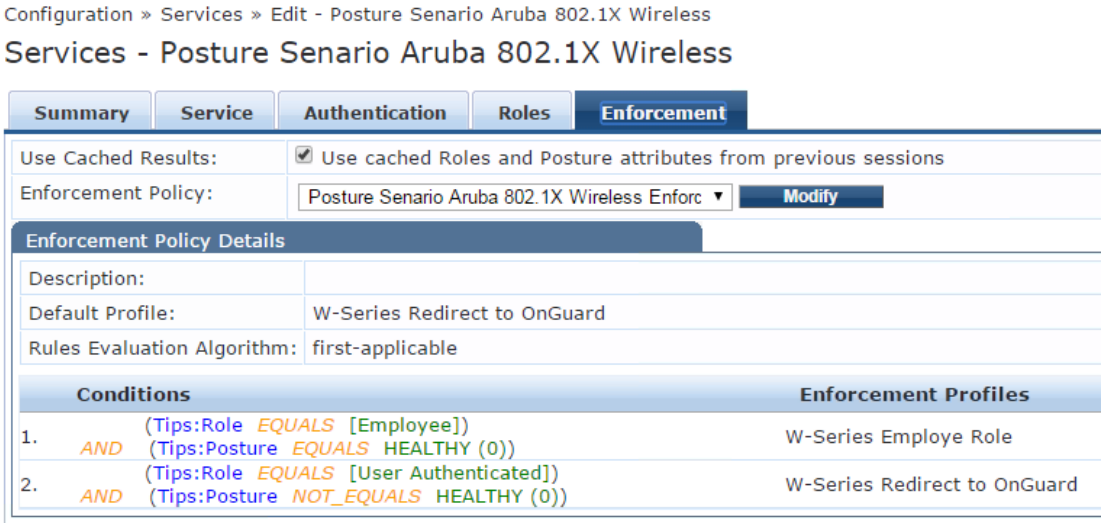

Figure 64 802.1X Wireless Service – Enforcement tab

12. Click **Save** to save the Service.
13. Select the Service: Posture Scenario Aruba 802.1X Wireless Posture Checks.
14. Select the **Service** tab.
    For this example, keep all the default settings.
15. Select the **Roles** tab.
    For this example, no Roles are needed for this Health Check Service.
16. Select the **Posture** tab (Figure 65).
    During testing, Posture Policies can be kept as default, but it is recommended to modify each OS specific policy to reflect the heath posture being tested. Click the desired policy agent type and click **Modify** to open the policy window. Select the **Posture Plugins** tab, and click the **Configure** button under Plugin Configuration. Default settings enable **AntiVirus** and **Firewall** checks for each OS

version. For initial testing, it is recommend that functionality be validated with a single OS and health check setting (e.g. Windows 7 and Firewall). Click **Save** to save the Plugin Configuration, and **Save** again to save the Posture Policy.
It is also useful to have control over the health status of the client. Auto-remediation can fix many health issues automatically on the device. If administrators want to verify assigned vlans and other enforcement actions, it is recommended that they uncheck the **Remediate End-Hosts** checkbox. This box can be checked at any time after verifying the policy actions are behaving as expected.

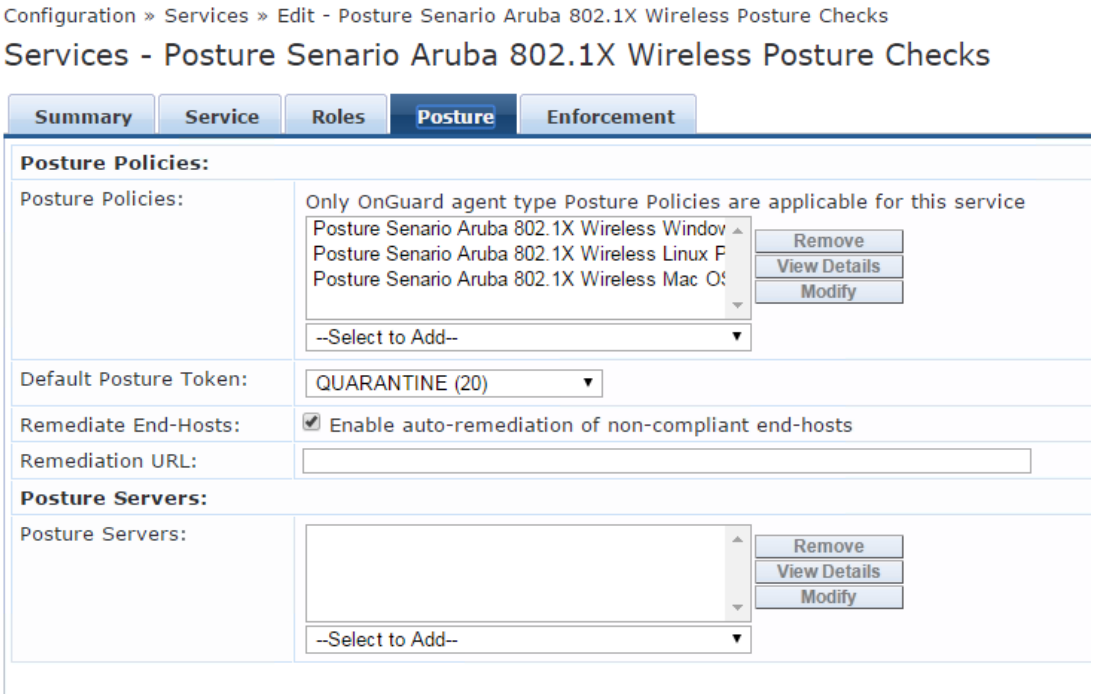

Figure 65 802.1X Wireless Posture Service – Posture tab

17. Move to the **Enforcement** tab (Figure 66).
    The template has populated the appropriate Enforcement Policy in the dropdown menu.
18. Verify that the correct policy details are shown.

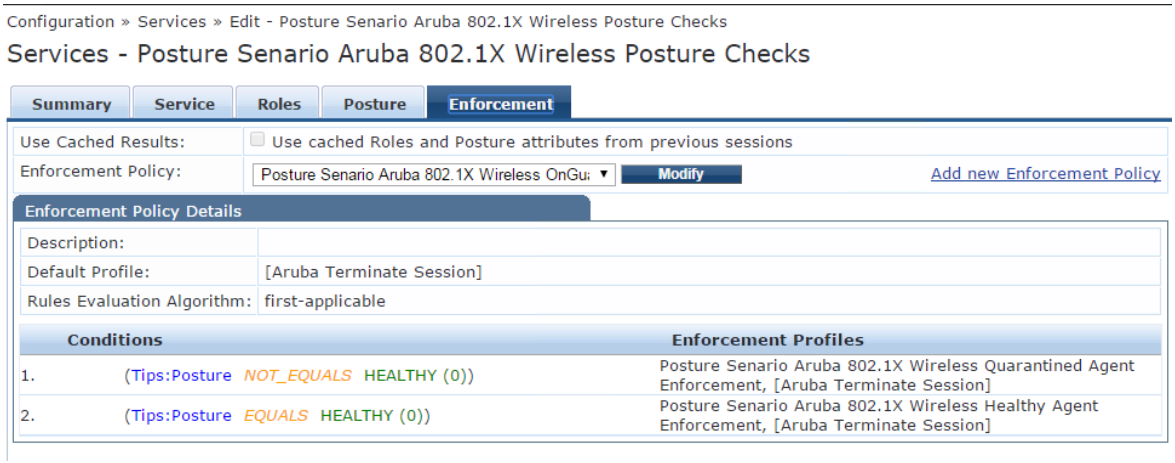

Figure 66 802.1X Wireless Posture – Enforcement tab

19. Click **Save** to save the Service.
    Configuration of the W-ClearPass Services to include all supporting policies and roles is now complete.

4.4.8 Creating an OnGuard Landing Webpage

The W-Series controller has a very useful captive portal function that can be used on both guest and employee networks. In this example, an employee network is enabled with a captive portal to allow easy access to the OnGuard download URL. It also provides access to the OnGuard dissolvable client URL.

W-ClearPass Guest provides a web-hosting feature. Using this feature allows for a single solution that does not require a separate webpage. Administrators also have the option of using their own web hosting solution if desired.

1. From the W-ClearPass Welcome screen (Figure 67), select the **ClearPass Guest** module.
   W-ClearPass Guest will open in a new browser tab.

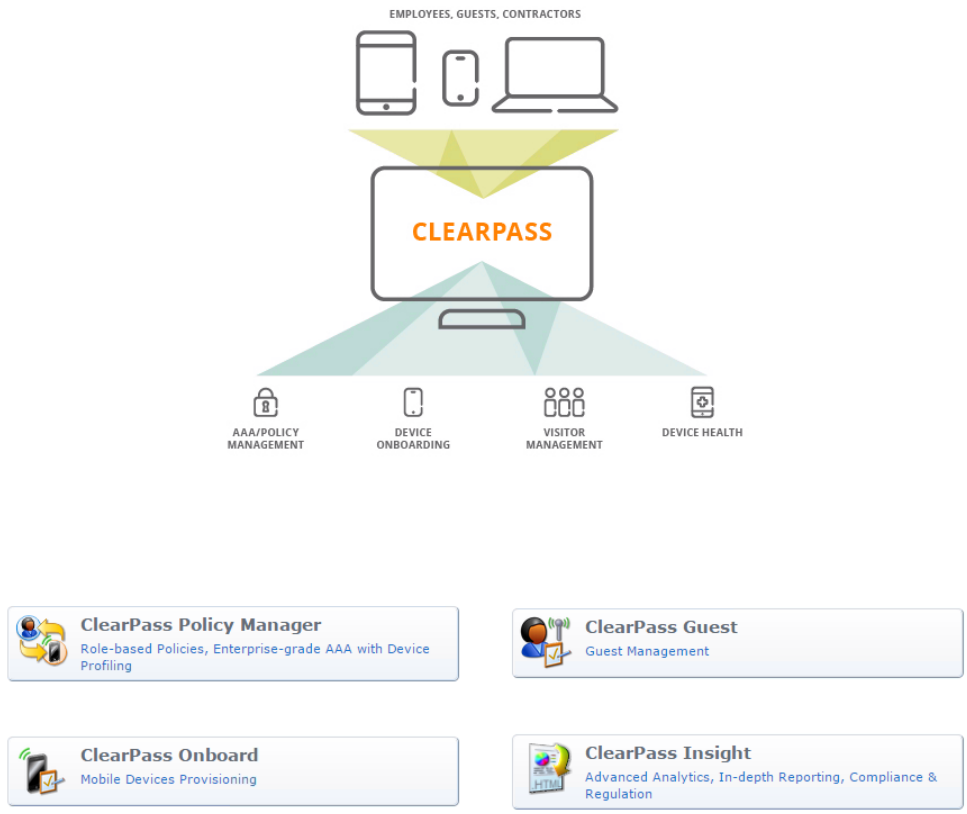

Figure 67 W-ClearPass Welcome page

2. Navigate to Home > Configuration > Pages > Web Logins.
3. Click Create a new web login page on the upper right.
4. Enter a descriptive name in the **Name** field (example: **OnGuard Portal**).
5. Enter a name used in the URL for the **Page Name** field (example: **OnGuard**).
   The Page Name should match name used in the URL in the Create Captive Portal Authentication Profile section (http://ClearPass.IP.address/guest/*page_name*.php where *page_name* is the name entered in this step).
6. Under **Login Method**, choose **Policy –initiated** – An enforcement policy will control a change of authorization.
7. Under **Login Form - Authentication**, choose **Anonymous** – Do not require a username or password.
8. Check **Auto-Generate the anonymous account** (leave the **Anonymous User** field blank, it will be auto-populated).
9. Check Enable bypassing the Apple Captive Network Assistant if desired.
10. Under Login Form – Custom Labels check Override the default labels and error messages.
11. Under Login Form - Pre-Auth Check, select Local- match a local account.
12. Under **Login Form** – **Log In Label**, enter a descriptive label (example: **Press to Run Health Check**).
13. Under **Login Page – Header HTML,** enter any instructions or webpage html customization for the header. In this example, the following html was used:

```
{nwa_text id=7980}<p>
<br>
   To determine if your client meets the minimum security requirements:
<br>
<br>
Press the button below to run the dissolvable agent
<br>
<br>

</p>{/nwa_text}
```

14. Under **Login Page – Footer HTML,** enter addition instructions and the URL for each OnGuard download link. The URL can be determined by accessing the W-ClearPass Policy Manager GUI, and navigating to **Administration > Agents and Software Updates > OnGuard Settings.**
In this example, the following html was used:

```
{nwa_text id=7979}<p>
<br>
<p>OR</p>

<br>
<br>
<p>Click the link to download the persistent client.
<br>
<br>
</p>
<a href="http://172.25.172.188/agent/installer/windows/ClearPassOnGuardInstall.exe">Windows
OnGuard Persistent Agent
</a>
<br>
<br>
<a href="http://172.25.172.188/agent/installer/mac/ClearPassOnGuardInstall.dmg">Mac OSX
OnGuard Persistent Agent
</a>
<br>
<br>
<a
href="http://172.25.172.188/agent/installer/ubuntu/ClearPassOnGuardInstall.tar.gz">Ubuntu
OnGuard Persistent Agent
</a>
</p>{/nwa_text}
```

15. Under Post-Authentication - Health Check, check the checkbox for Require a successful OnGuard health check.
16. Under Post-Authentication - Health Check, select Native agents only.
17. Click Save Changes.

The following figures (Figure 68 - Figure 72) detail the steps above.

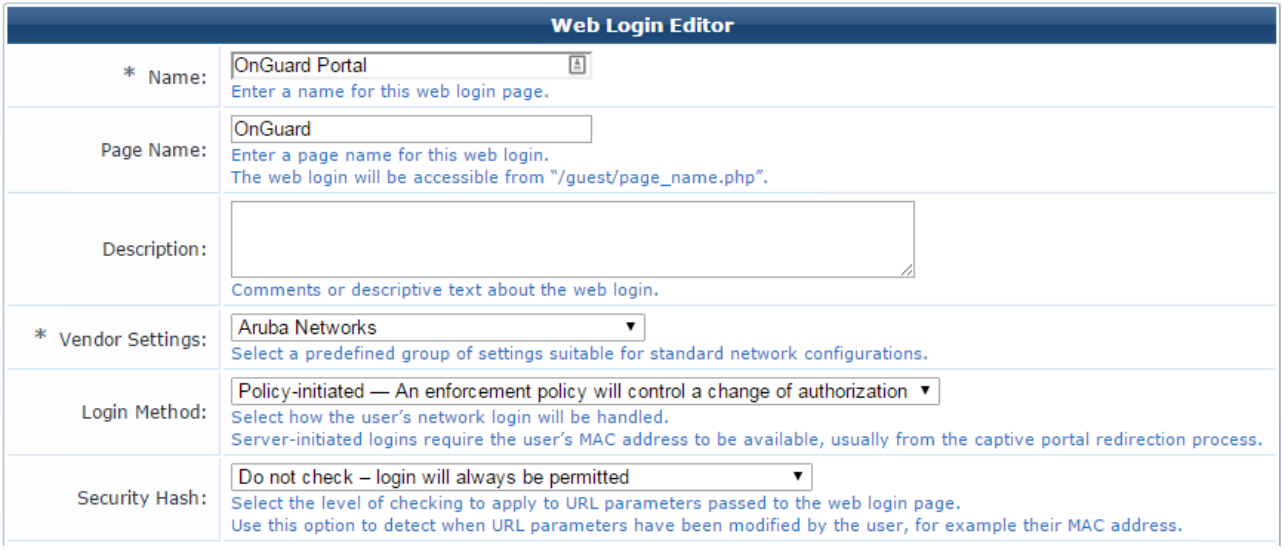

Figure 68 Web Login Page

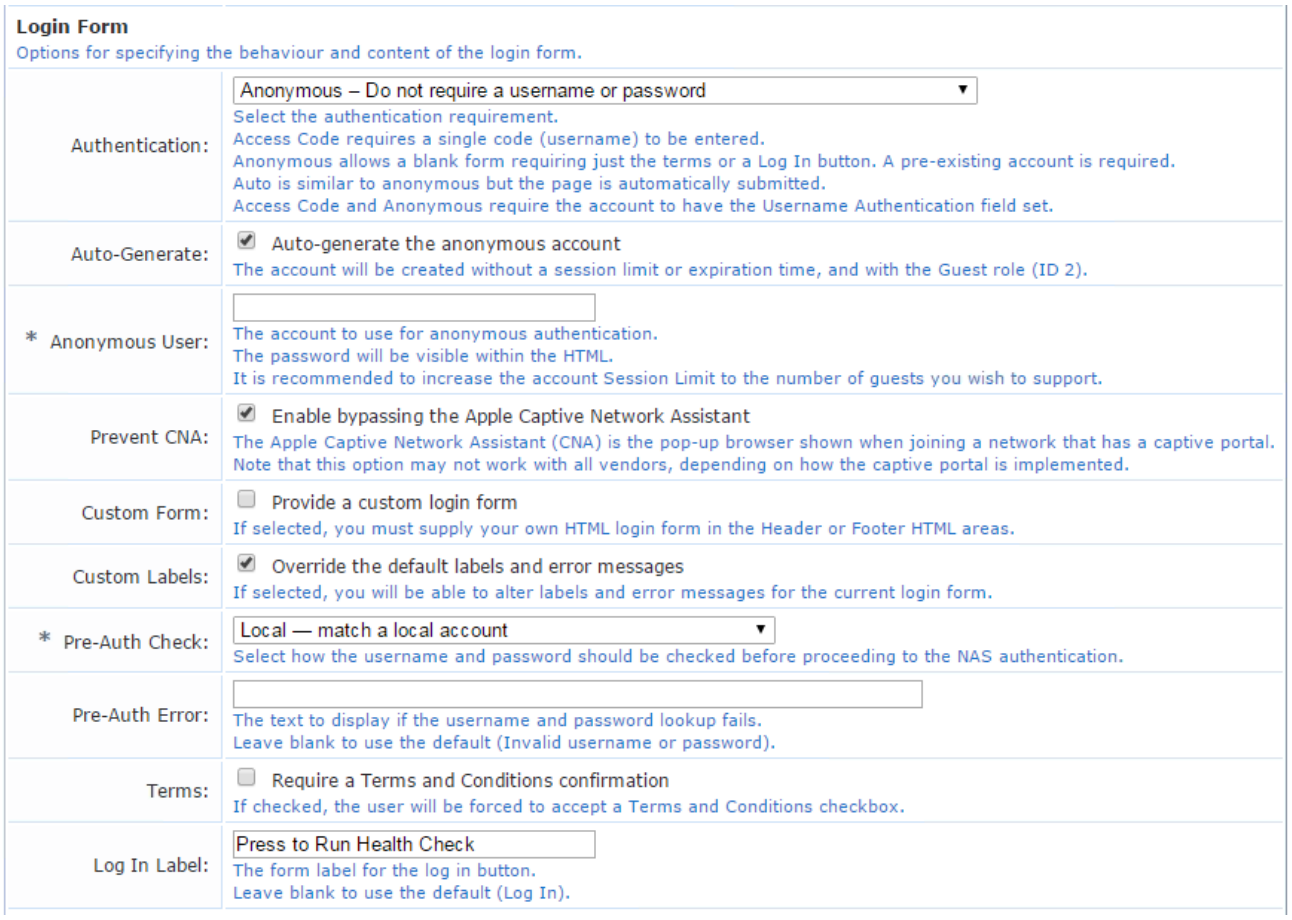

Figure 69 Web Login Page Continued

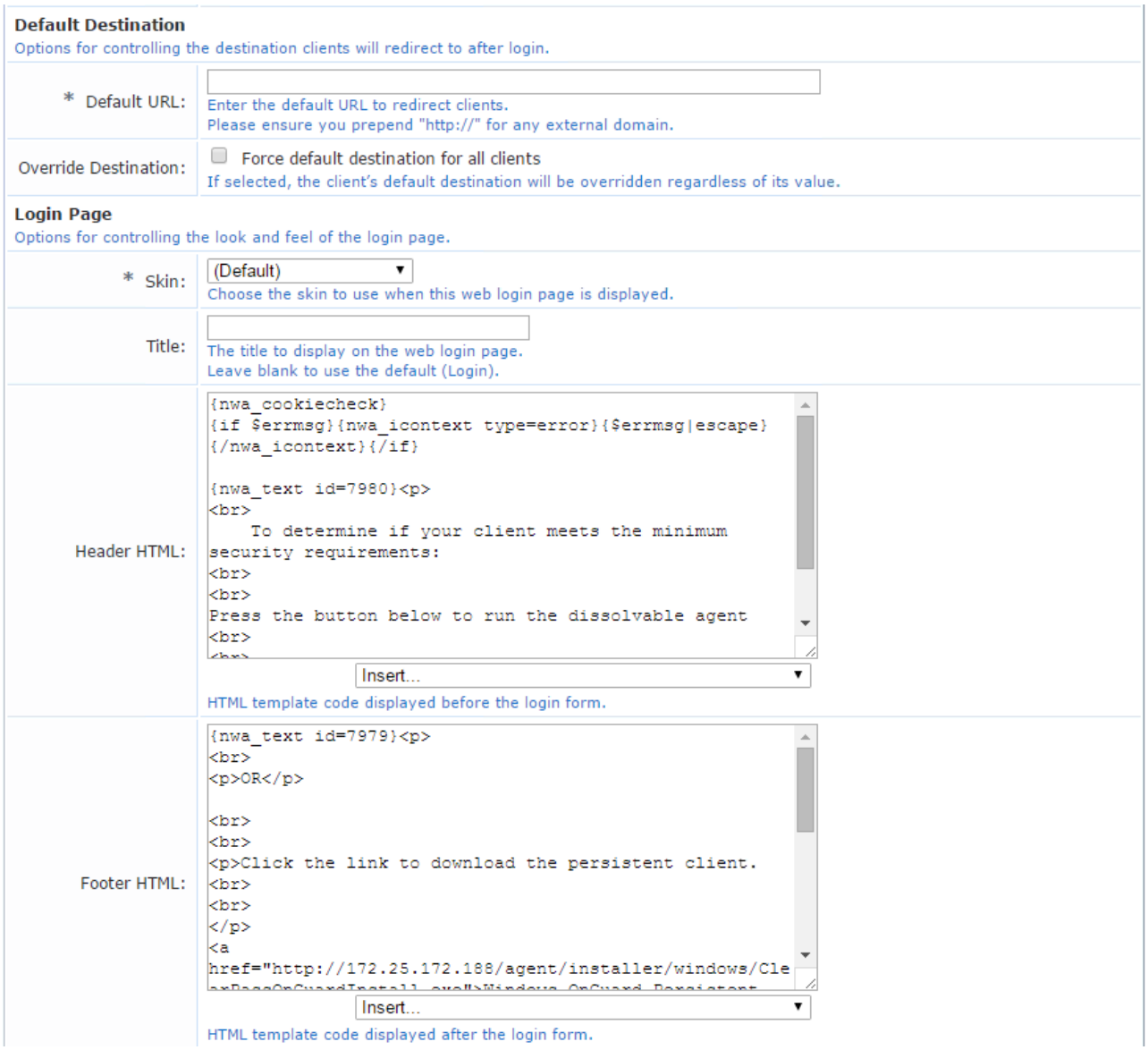

Figure 70 Web Login Page Continued

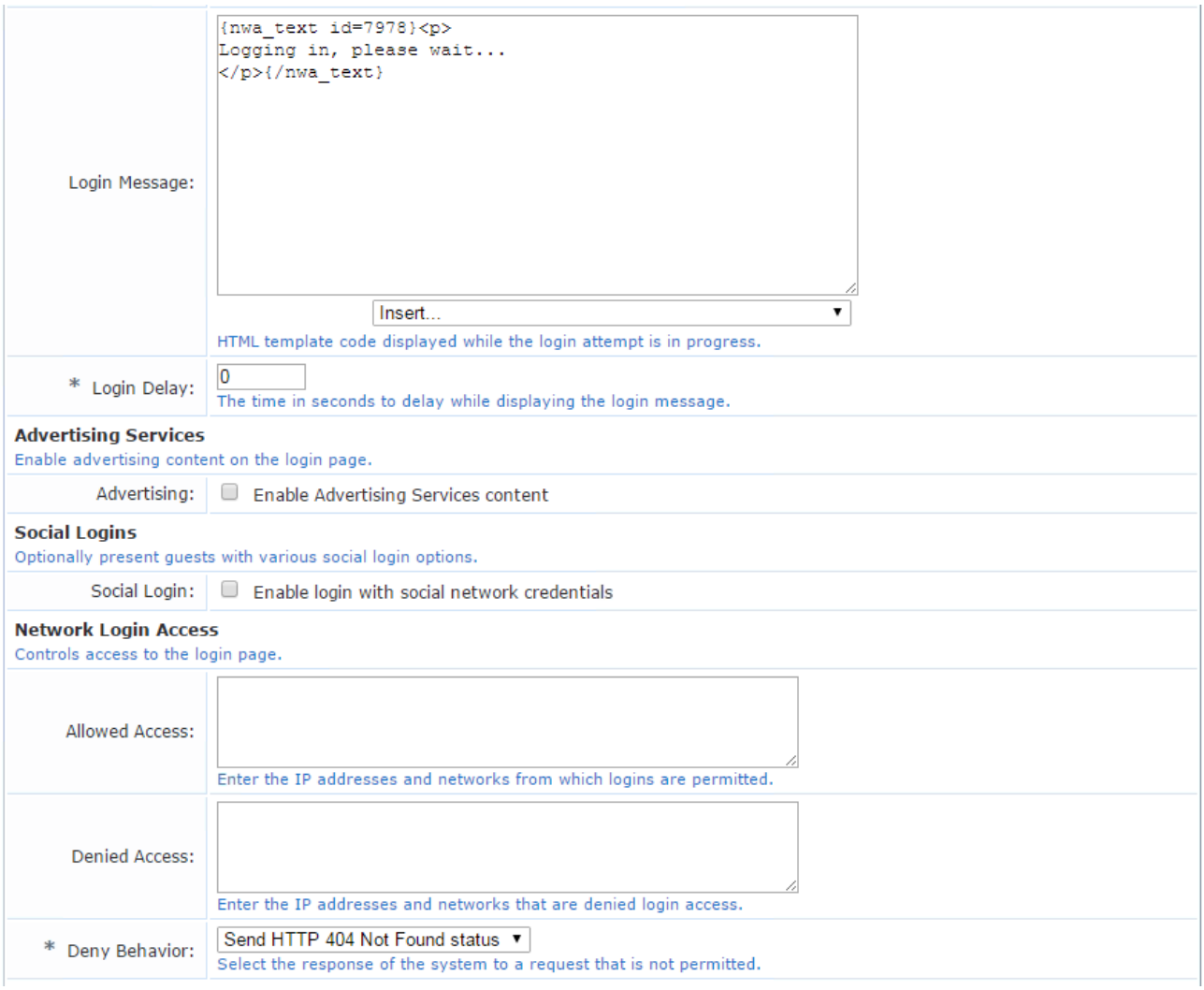

Figure 71 Web Login Page Continued

Figure 72 Web Login Page Continued

The web login page can be viewed directly from the configuration page by selecting the name of the web login and clicking **Test** underneath the name (Figure 73).

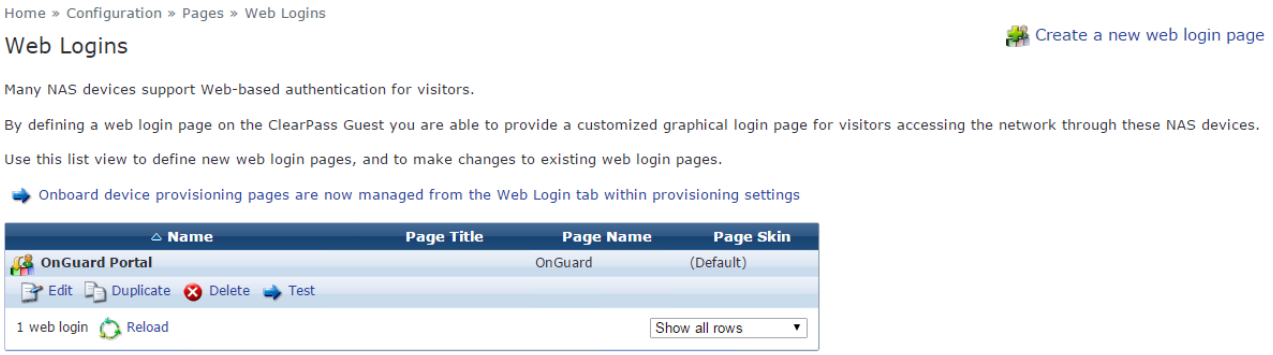

Figure 73 Displaying the web login page

The page will be displayed in a new browser tab. It should look like the Figure 74 if all the example settings and html are used.

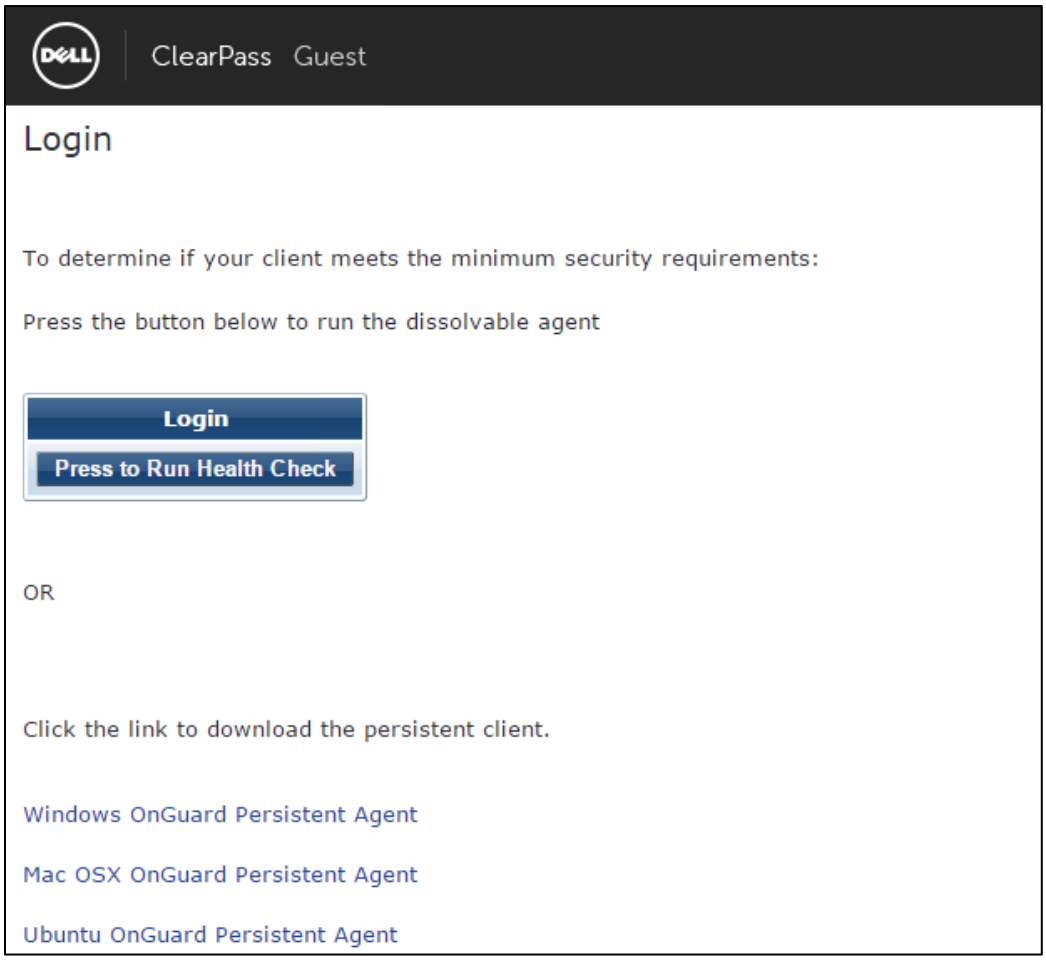

Figure 74 Example Web Login Page

4.4.9 Testing the Configuration

The W-ClearPass and N-Series configuration in this guide can be tested with any client. The following details the use of a Windows 7 laptop.

1. Ensure user is defined and entered into the Active Directory with a Department of *Employee*. Ensure the laptop is part of the domain.
2. Connect laptop to the appropriate SSID. Ensure the laptop firewall is enabled.
3. Enter credentials when prompted on the laptop.
4. User is authenticated, placed into the quarantine user role due to absence of a health token.
5. Open a browser to be redirected to the landing page. Install OnGuard by clicking the appropriate download link (persistent or dissolvable).
6. Wait for OnGuard to scan health once installed. OnGuard initiates a re-authentication. User is placed into the employee user role.
7. Turn off the laptop firewall.
8. Wait for OnGuard to rescan health after detecting a change to the firewall. OnGuard initiates a re-authentication. User is placed into the quarantine user role.
9. Turn firewall on.
10. Wait for OnGuard to rescan health after detecting a change to the firewall. OnGuard initiates a re-authentication. User is placed into the employee user role.

5 Wireless Access with Dell W-Series Instant Access Points

5.1 Topology

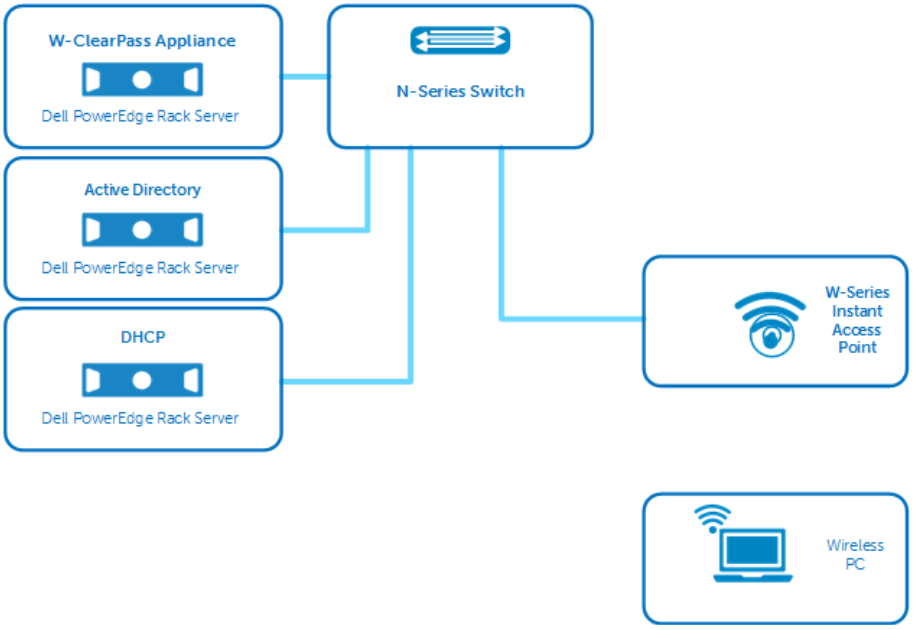

Figure 75 Wireless topology with W-Series Instant Access Points

5.2 Example Scenario – W-Series Instant

The following example details a typical scenario involving a user requiring access to a corporate or guest network. Posture compliance with OnGuard is the key feature demonstrated.

Example of Wireless Network Access BYOD with Posture Checks

In this scenario, a user requires network access with a device not supplied by a corporate IT department and is connecting to network via a wireless connection.

1. The user connects to the network via a wireless SSID.
2. The user is prompted for credentials to access the network.
3. W-ClearPass authenticates the user's credentials.
4. W-ClearPass detects if OnGuard has been installed and if the device is healthy.
   g. If OnGuard is installed and the device is healthy, W-ClearPass places the user in the appropriate User Role.
   h. If OnGuard is installed and the device is not healthy, W-ClearPass places the user in a quarantine User Role.
   Users are automatically re-authenticated once the issue is resolved and placed into the

appropriate User Role. In some cases, auto-remediation can perform changes without user action.

i. If OnGuard has not been installed, the user is automatically redirected to a webpage to run a one-time scan, or to install the OnGuard persistent client.
   OnGuard scans the device and determines if the client is compliant with the health policy.
   i. If healthy, W-ClearPass places the user in the appropriate vlan.
   ii. If not healthy, W-ClearPass places the user in a quarantine vlan
   Users are automatically re-authenticated once the issue is resolved and placed into the appropriate User Role. In some cases, auto-remediation can perform changes without user action.

The scenario detailed above can be used for any type of guest or employee network. The example in this paper uses a single employee vlan. The user is assigned a full access Employee Role or a restricted Quarantine Role. Administrators can setup W-ClearPass to assign users to different Roles to support guests, contractors or employees.

The credentials used in this example are username/password and are stored in a Windows Server Active Directory. Any authentication type, including certificates, can be used with OnGuard posture policies. This guide does not go into detail on configuring all authentication types. For further information on BYOD topics through Onboard and Guest access, please see the W-ClearPass User Guide or other available deployment guides at www.dell.com/support/.

The configuration examples in sections 4.3 and 4.4 detail a basic solution utilizing W-ClearPass OnGuard and an N-Series switch. All scenarios contain a policy decision and enforcement based on posture information from OnGuard.

The configuration for the W-Series IAP remains the same regardless of the type of OnGuard client or OS used. The configuration for W-ClearPass will differentiate between the following combinations of OnGuard client types and PC OS:

OnGuard Persistent application
OnGuard Dissolvable application
Windows 7/8
Mac OSX
Linux Ubuntu

The solution will enable a webpage hosted by W-ClearPass for access to both OnGuard application types for employees and guests scenarios. See the Creating an OnGuard Landing Webpage section for details.

5.3 Dell W-Series Instant AP Configuration – Wireless

The full configuration to enable wireless access has many components and options. This example assumes the administrator has a fully functioning basic WLAN configuration. The administrator should have the following configurations prior to implementing this example:

- Virtual Controller Network settings – VLANs, Ports, IP
- AP configuration – Networks

For more information on basic configuration, see the Dell Networking W-Series Instant User Guide at http://www.dell.com/support/.

The configuration settings in this section are the crucial settings to enable the authentication and access per the OnGuard example scenario.

5.4 Configure Authentication Server

1. Click **Security** in the upper right-hand corner of the Instant GUI.
2. On the Authentication Servers tab, click New.
3. Enter the Name, IP address and Shared key for the W-ClearPass server (Figure 76).
4. Enable **RFC 3576** by selecting **Enabled** from the drop down list.
5. Click **OK**.

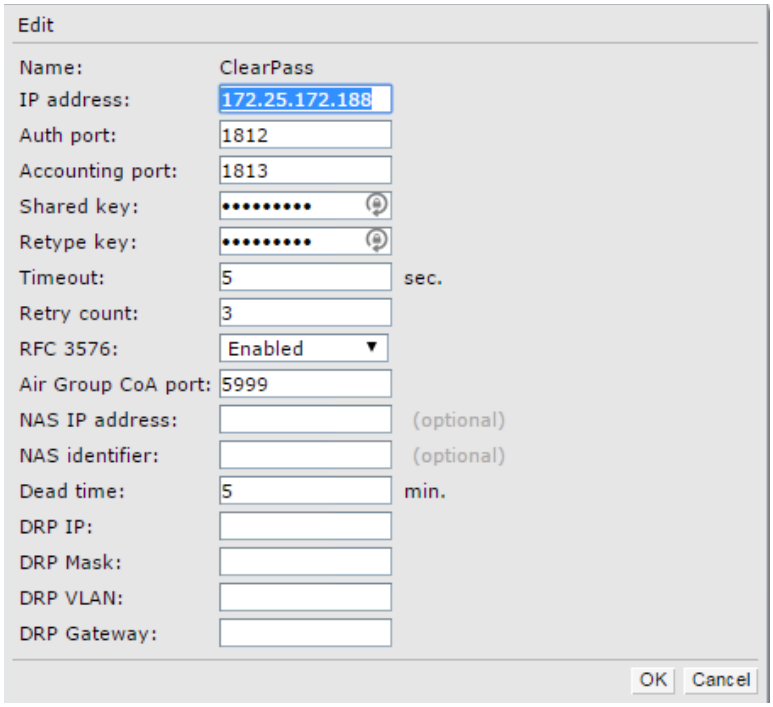

Figure 76 Authentication Server settings

5.4.1 Configure External Captive Portal

1. Continuing within the Security settings, click the **External Captive Portal** tab.
2. Click **New** to add a new captive portal.
3. Enter the information corresponding to the web login page created in the W-ClearPass Guest configurations in the previous section. The final configuration should look like Figure 77.
4. Click **OK**.

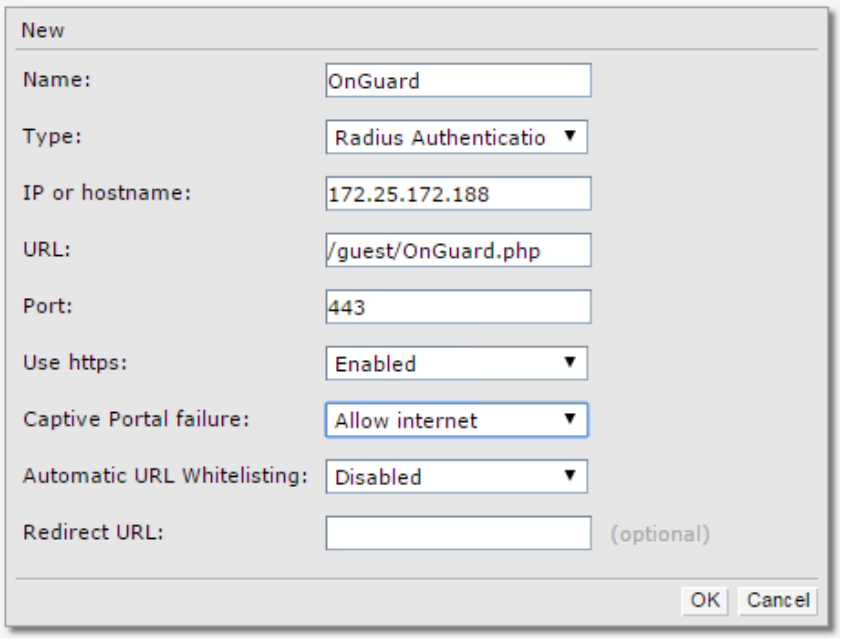

Figure 77 Instant captive portal settings

Note: The URL is case sensitive. Ensure the page name from the web login configuration is the same as the URL entered in the captive portal.

5.4.2 Configure User Roles

1. Click the **Roles** tab.
2. Click **New** to add a new role.
3. Enter the name **Employee**, and click **OK**.
   The default access rules are “allow all” to all destinations. Similar to the controller-based example, this example will use the default “allow all” rules. Administrators will need to add access rules for their employee roles to comply with their specific security policy.
4. Click **New** under the **Roles** window to add a new role. This role will be the quarantine role designed to direct users to the captive portal to access OnGuard information and links.
5. Enter the name **OnGuard-redirect,** and click **OK**.
6. Click **New** under **Access Rules** window.
7. Under Rule type, select Captive portal.
8. Under Splash page type, select External.
9. Under **Captive portal profile** (Figure 78), select the profile created in the previous step.

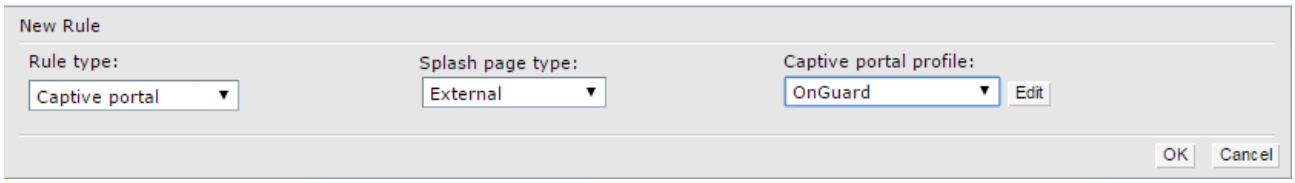

Figure 78 Instant Role settings – captive portal rule

10. Click **New** under **Access Rules** window.
11. Under **Rule type**, select **Access control** (Figure 79).
12. Under **Service**, select **Network**, choose **http** from the drop down list.
13. Under **Action**, keep **Allow**.
14. Under **Destination**, select to a particular server.
15. Enter the IP address to the W-ClearPass server.

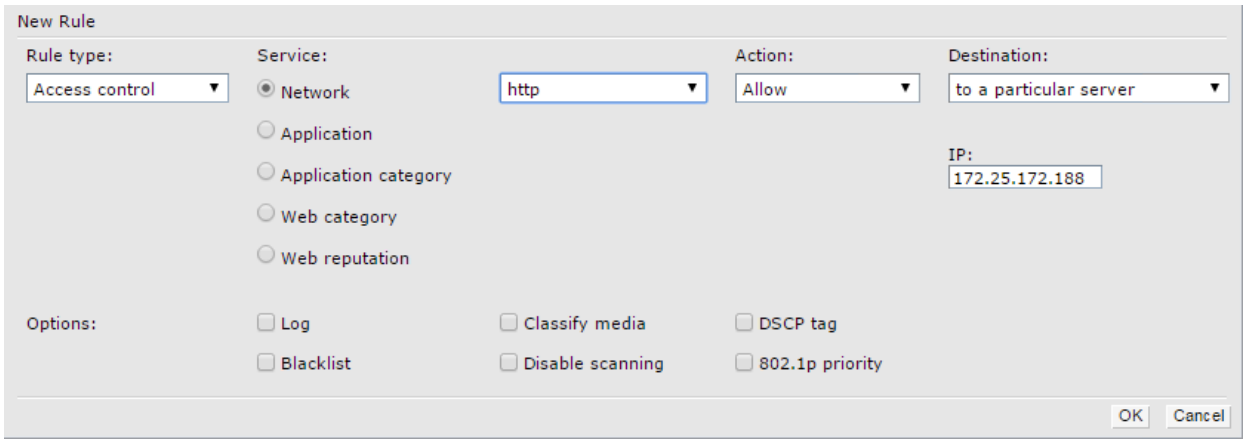

Figure 79 Instant Role settings – http rule

16. Repeat the above rule for **https**.
17. Click **OK**.

Note: Administrators will need to add rules to this firewall policy to enable access to services and hosts that are key to joining and authenticating to the network. One example of a service needed to communicate while in this quarantine role is DHCP and RADIUS. In Figure 80, only the http(s) rules with examples for dhcp and dns are shown.

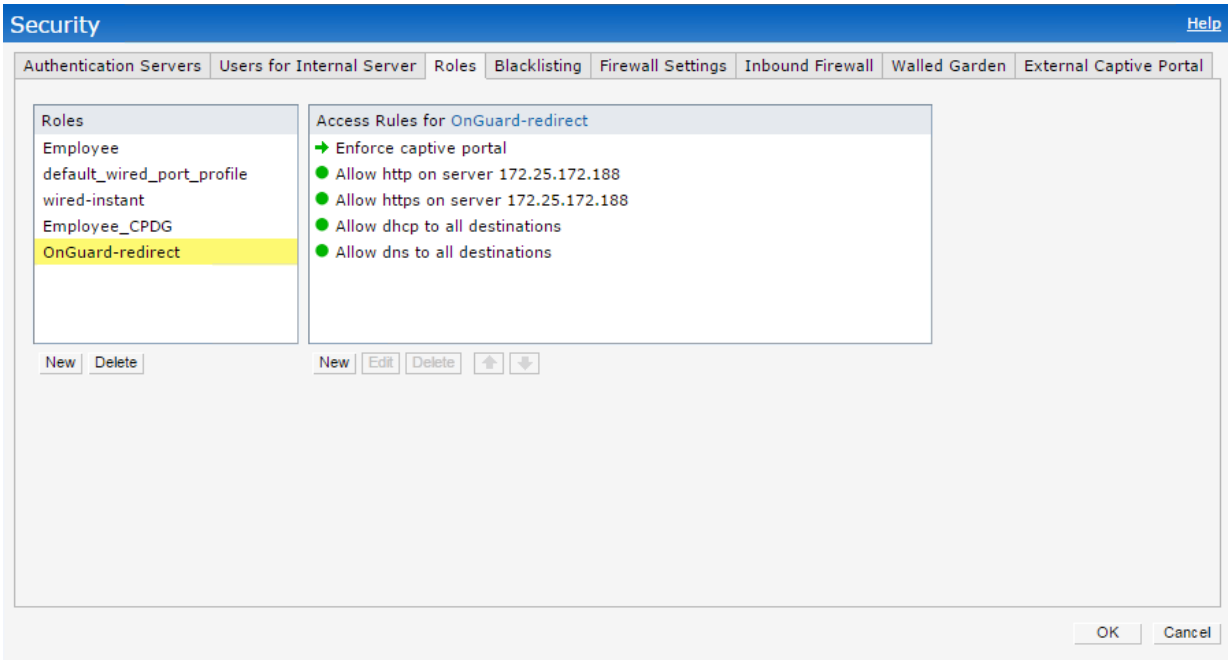

Figure 80 Instant Role Settings – Quarantine Role

5.4.3 Configure the Employee Network

If there is not a WLAN network configured, you can create a new one at this time. If you are editing an existing network, click the network name and then click **edit**

1. Navigate to WLAN Settings tab – Employee.
2. Click **Next**.
3. VLAN tab – Virtual controller managed, and Default.
4. Click Next.
5. Security tab.
6. Choose **Enterprise** on the sliding bar to the left.
7. Select WPA-2 Enterprise.
8. Under **Authentication server 1**, choose the authentication server configured at the beginning of this section (example: **ClearPass**).

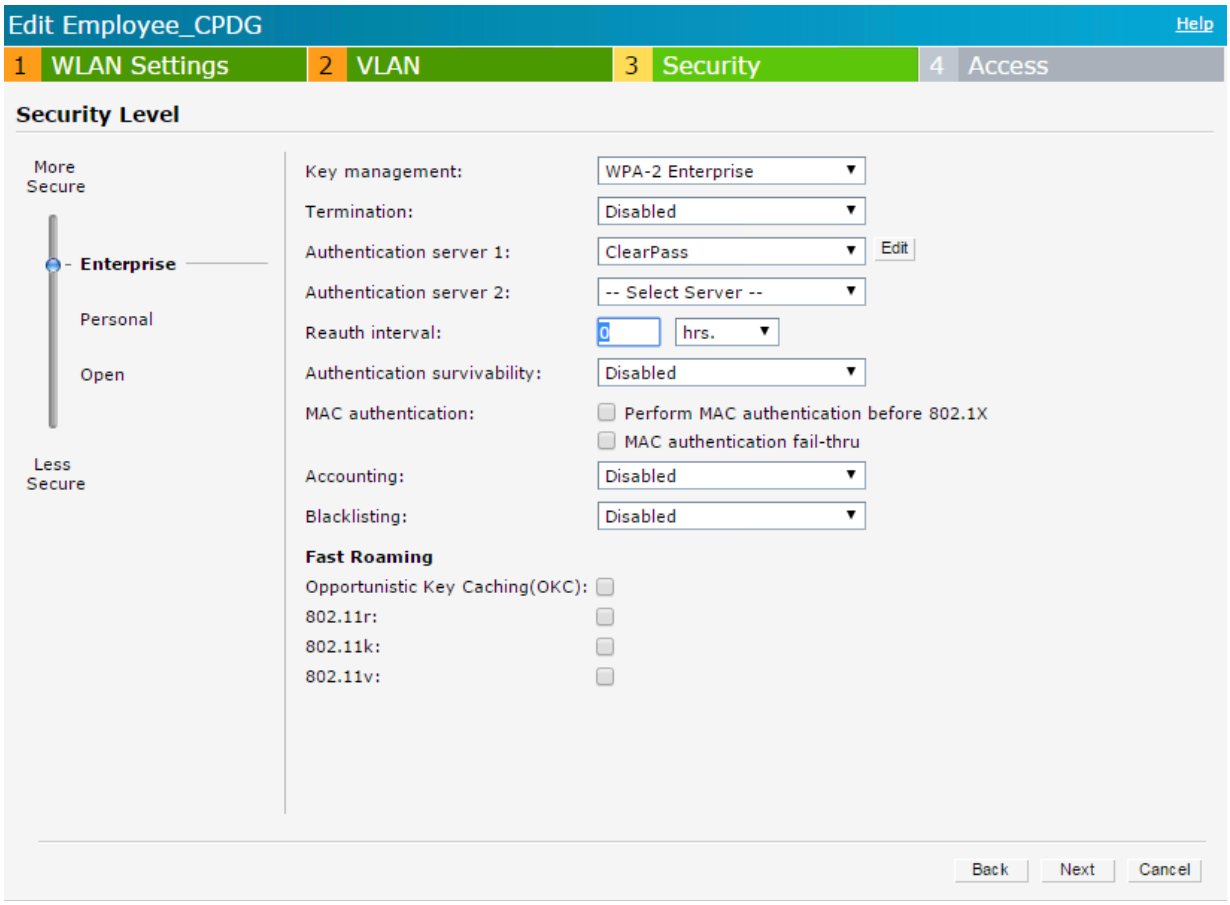

Figure 81 Instant WLAN Network Settings – Security tab

9. Click **Next**.
10. For the **Access Rules**, leave it as **Unrestricted**. During the 802.1x authentication, W-ClearPass will assign either the **Employee** role, or the **OnGuard-redirect** quarantine role.
11. Click **Finish**.

Note: In this example, the **Employee_CPDG** SSID was configured to be the same as the SSID in the controller-based example. Using the same SSID in two independent systems within range of each other is not recommended. This document assumes only one system is running at a time.

This concludes the Instant access point configuration.

5.5 Dell W-ClearPass Configuration – Instant

The W-Instant example heavily leverages the controller-based configuration for the W-ClearPass portion.

All Services, Roles, Role Mappings, Posture Policies, Enforcement Polices and Enforcement Profiles can be used exactly as they are configured in Section 4.4. The web login page used for the captive portal can also be used again.

Note: If the example from Section 4.4 was completed, the services can be kept active and used with the Instant example from Section 5. If the reader has not competed those steps, go back to Section 4.4 once the network device setting has been done below. Ensure all named settings from both examples correlate with any uniquely named settings used during your configuration.

5.5.1 Add the N-Series Switch as a Network Device

The only additional configuration needed is to add the W-Instant APs as Network Devices. This will allow each W-IAP to be identified as a trusted network access device.

The W-IAPs are added in **Configuration > Network > Devices**.

1. From the W-ClearPass Welcome screen, click the ClearPass Policy Manager module.
   The ClearPass Policy Manager opens.
2. Navigate to the **Network Devices** page by selecting, **Configuration > Network > Devices**.
3. Click **+Add**.
   The **Add Device** window opens.
4. Enter the Name of the W-IAP, IP Address, Description and RADIUS Shared Secret.
5. Select **Aruba** from the **Vendor Name:** dropdown box.
6. Click **Add**.

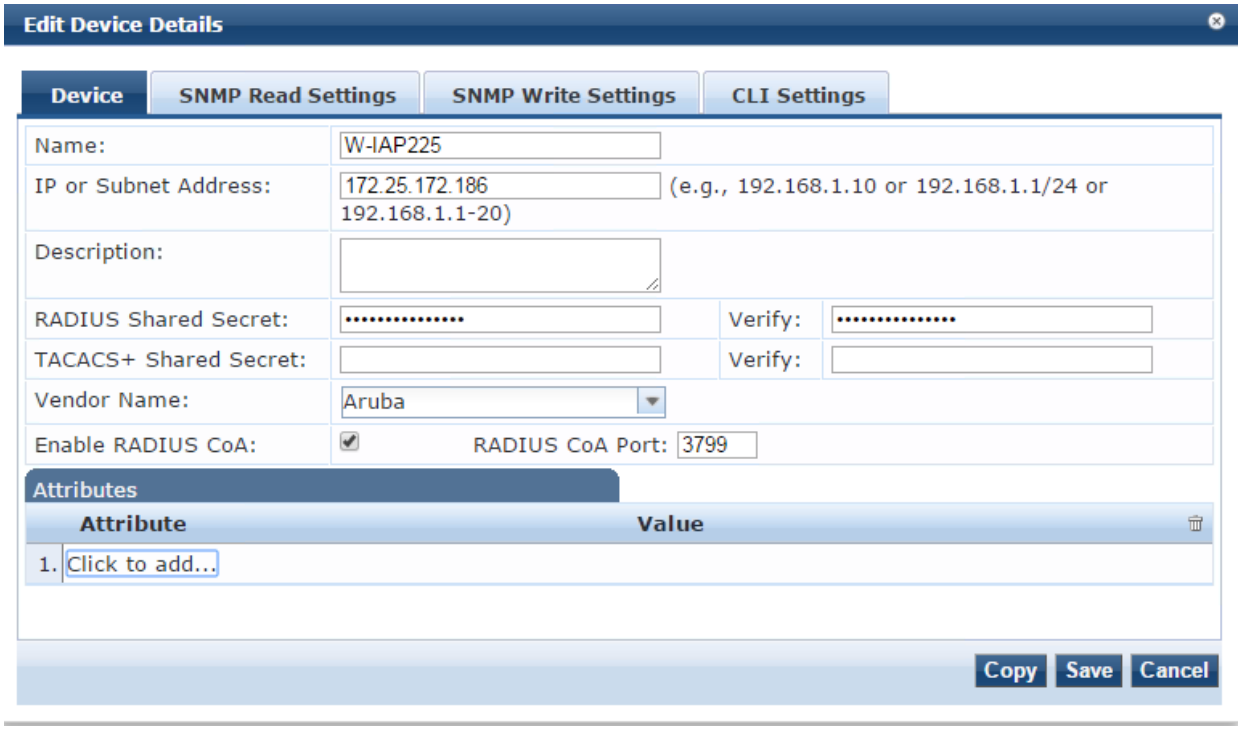

Figure 82 Network Device settings

Note: Each access point will need to be added to the list. The request originates from the access point IP address, not the common virtual controller IP address.

5.5.2 Testing the Configuration

The W-ClearPass and W-Series configuration in this guide can be tested with any client. The following details the use of a Windows 7 laptop.

1. Ensure the user is defined and entered into the Active Directory with a Department of *Employee*. Ensure the laptop is part of the domain.
2. Connect laptop to the appropriate SSID. Ensure the laptop firewall is enabled.
3. Enter credentials when prompted on the laptop.
4. User is authenticated, placed into the quarantine user role due to absence of a health token.
5. Open a browser to be redirected to the landing page. Install OnGuard by clicking the appropriate download link (persistent or dissolvable).
6. Wait for OnGuard to scan health once installed. OnGuard initiates a re-authentication. User is placed into the employee user role.
7. Turn off the laptop firewall.
8. Wait for OnGuard to rescan health after detecting a change to the firewall. OnGuard initiates a re-authentication. User is placed into the quarantine user role.
9. Turn firewall on.
10. Wait for OnGuard to rescan health after detecting a change to the firewall. OnGuard initiates a re-authentication. User is placed into the employee user role.

A Configuration details

Table 1 presents the versions of the hardware and software components used to configure and validate the examples presented in this guide.

Table 1 Component table example

Component	Description
N-Series firmware	6.2.6.6
W-Series Controller firmware	6.4.2.3
W-Instant firmware	6.4.2.3-4.1.1.4
W-ClearPass version	6.5.0.71095

B Additional resources

Support.dell.com is focused on meeting your needs with proven services and support.

DellTechCenter.com is an IT Community where you can connect with Dell EMC Customers and Dell EMC employees to share knowledge, best practices and information about Dell EMC products and installations.

Referenced or recommended Dell EMC publications:

- Manuals and documentation for W-ClearPass Virtual Appliances

C Attachments

This document includes the following attachments.

N-Series Configuration example.txt
W-Series Controller Configuration example.txt

D Support and Feedback

Contacting Technical Support

Support Contact Information

Web: http://Support.Dell.com/
Telephone: USA: 1-800-945-3355

Feedback for this document

We encourage readers of this publication to provide feedback on the quality and usefulness of this deployment guide by sending an email to Dell_Networking_Solutions@Dell.com