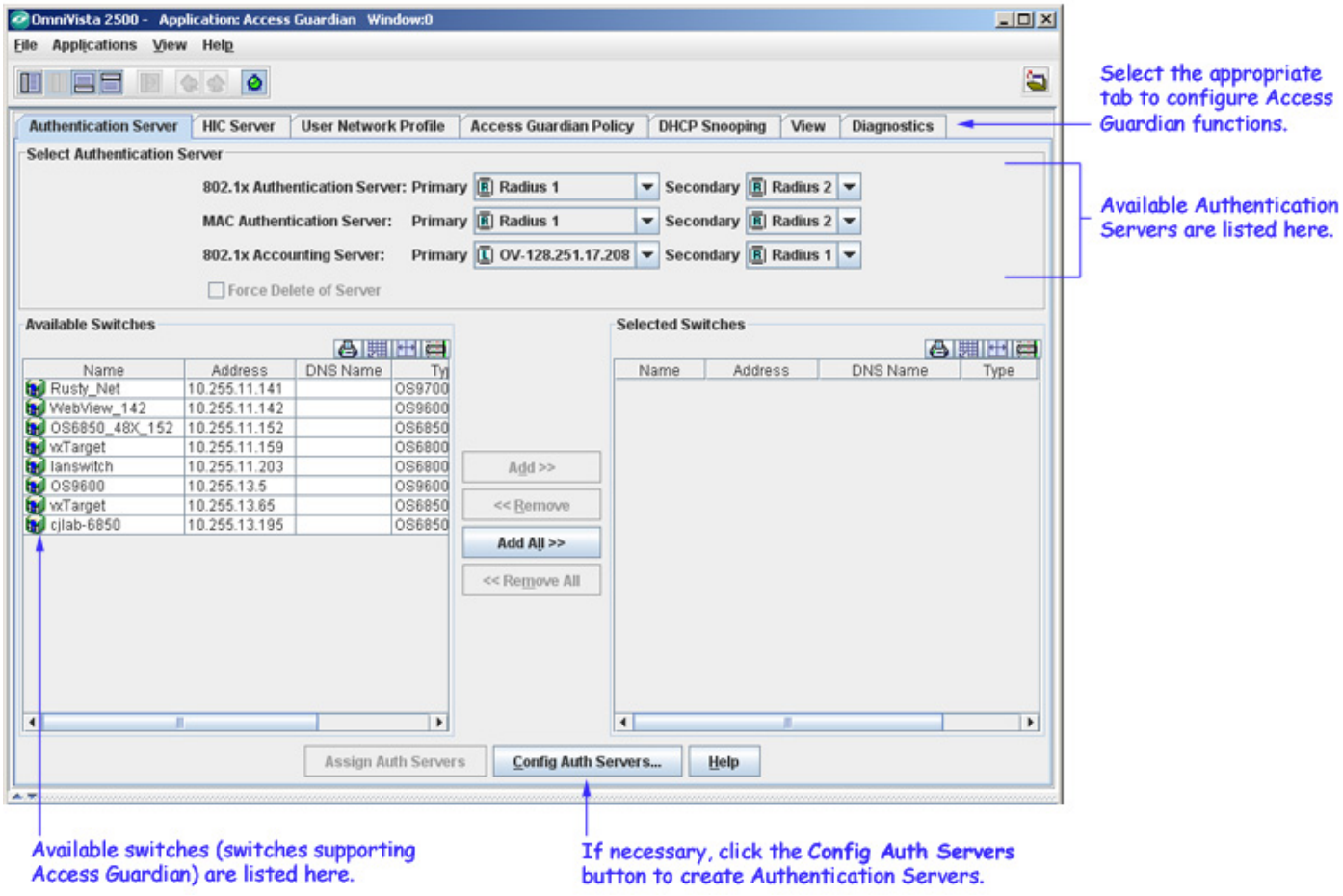
Getting Started with Access Guardian

The Access Guardian application in OmniVista includes a collection of Alcatel-Lucent security functions that work together to provide a dynamic, proactive network security solution. Access Guardian policies enable you to apply 802.1x functionality across a set of ports on one or more switches in a single operation. Moreover, this functionality is supported for both 802.1x clients (Supplicants) and non-802.1x clients (Non-Supplicants) through configurable 802.1x device classification policies to handle access to 802.1x ports.

In addition to device authentication and classification, you can also create User Network Profiles (UNP) to configure network access controls for one or more user devices; and use the Host Integrity Check (HIC) feature, to verify compliance of an end user device when it connects to the switch. These functions, as well as additional diagnostic tools can be configured by clicking on the applicable tab within the Access Guardian application.

> **Note:** The Access Guardian application is only supported on 6400, 6850, 6855, and 9000 Series devices using AOS 6.1.3 or later; and is only available on 802.1x-enabled ports. The User Network Profile (UNP) and Host Integrity Check (HIC) features within Access Guardian are only supported on 6400, 6850, and 6855 devices. A user must have Network Administrator privileges to access the application.

The Access Guardian Application



Access Guardian Tabs

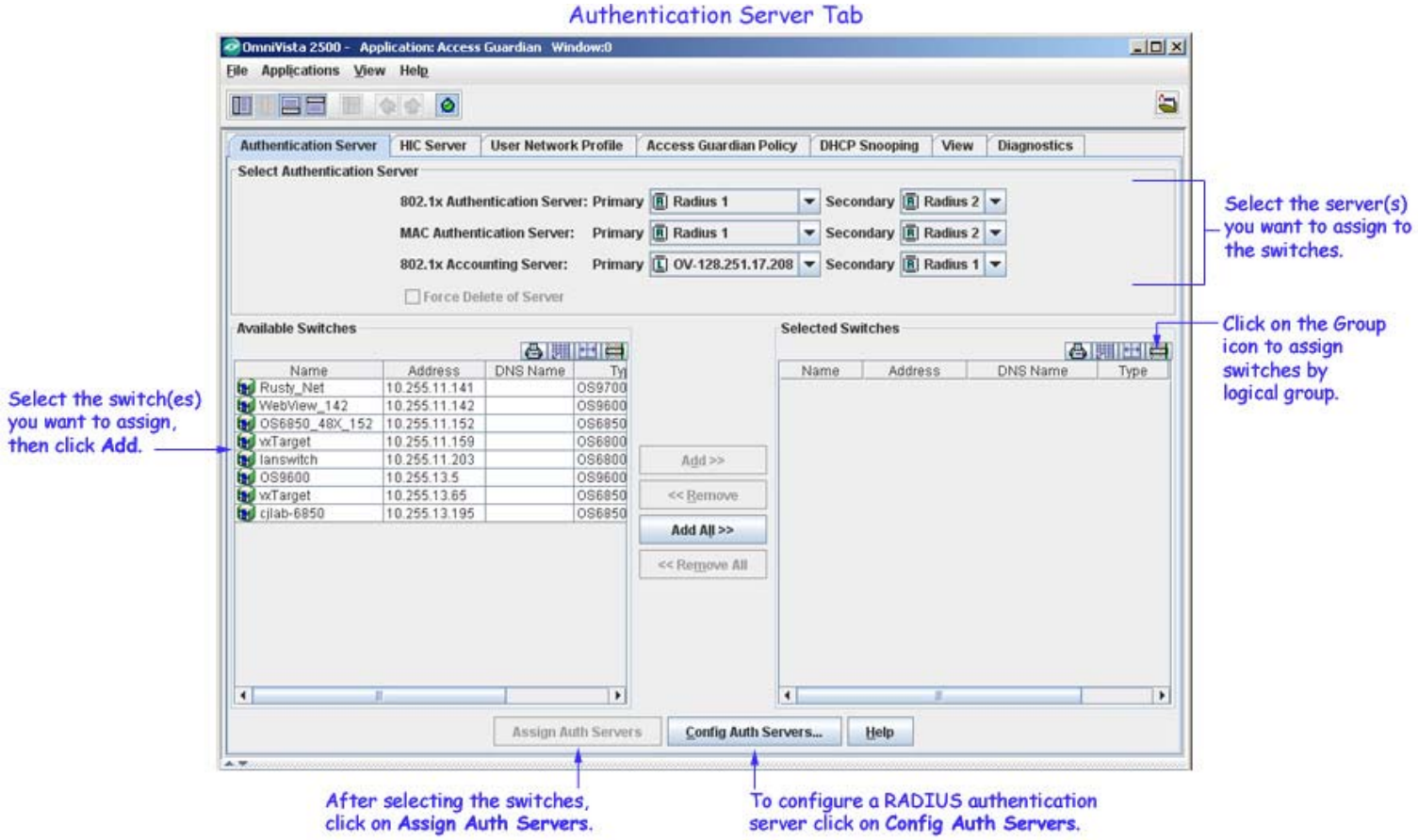
Access Guardian configuration, as well as additional diagnostic tools, are accessed by clicking on the applicable tab:

- **Authentication Server** - is used to assign Authentication Servers to a set of switches. These RADIUS servers are used to authenticate and provide network access based on user-configured Access Guardian policies. Note that before Access Guardian can be used, you must assign at least one RADIUS Server to a switch and assign that server to either 802.1x Authentication or MAC Authentication (usually both).
- **HIC Server** - is a web-based solution for device integrity verification. This solution consists of the InfoExpress CyberGatekeeper server, a permanent or web-based downloadable agent to verify host compliance, and User Network Profiles (UNP). Host Integrity Check (HIC) is triggered when a UNP is applied to a device and HIC is enabled for the UNP.
- **User Network Profile** - is used to configure a user profile(s). Users are assigned to a profile based on IP or MAC address. The profile determines the user's VLAN assignment, whether or not a Host Integrity Check (HIC) is required, and if any QoS access control list (ACL) policies are applied to the device.
- **Access Guardian Policy** - is used to configure device classification policies. A policy can specify the use of one or more types of authentication methods (802.1X, MAC-based, or Web-based Captive Portal) for the same port. For each type of authentication, the policy also specifies the classification method (RADIUS, Group Mobility, Default VLAN, User Network Profile, or block device access).
- **DHCP Snooping** - is used to configure DHCP Snooping, and monitor DHCP Snooping violations for ports on selected devices. DHCP Snooping improves network security by filtering DHCP messages received from devices outside the network and building and maintaining a binding table (database) to track access information for such devices.
- **View** - is used to view specific policies assigned to switch ports. The tab displays Access Guardian Policies, Supplicant/Non-Supplicant information, and the 802.1x Authentication Servers, the MAC Authentication Servers and the 802.1x Accounting Servers that have been assigned to the selected switch.
- **Diagnostics** - is used to diagnose end user problems by locating the user's end station and displaying any Access Guardian Policies for the End Station.

Authentication Server Tab

The **Authentication Server** Tab is used to assign Authentication Servers to a set of switches. You can assign the Authentication Server(s) to specific switches listed in the "Available Switches" Area or to a group of switches from a Logical Subnet. Only those switches that support Access Guardian are displayed in the "Available Switches" Area.

> **Note:** Before Access Guardian can be used, the Network administrator must assign at least one RADIUS Server to a switch and must assign that server to either 802.1x Authentication and/or MAC authentication. If necessary, click on the **Config Auth Servers** button to bring up the **Authentication Servers** application and create the server(s)



Assigning Authentication Servers

Supplicant policies use 802.1x Authentication via a remote RADIUS server and provide alternative methods for classifying Supplicants if the authentication process either fails or does not return a VLAN ID. Non-Supplicant policies use MAC authentication via a remote RADIUS server or can bypass authentication and only allow strict assignment to specific VLANs. MAC Authentication verifies the source MAC address of a non-supplicant device via a remote RADIUS server. Similar to 802.1x Authentication, the switch sends RADIUS frames to the server with the source MAC address embedded in the username and password attributes.

Assigning Authentication Servers to Specific Switches

Follow the steps below to assign Authentication Servers to specific switches.

1. Select the applicable **Primary** and **Secondary** Authentication Servers from one or more of the drop-down lists at the top of the page. You cannot select the same server for both Primary and Secondary. If you select "None" for the Primary, the only choice for Secondary is “None”.

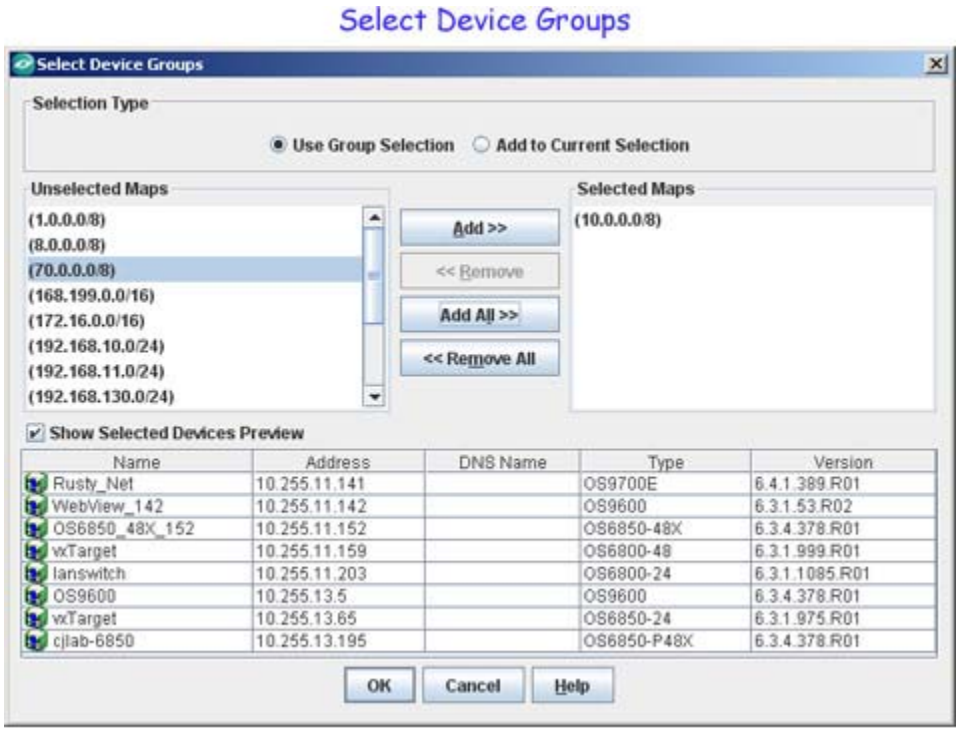
2. In the "Available Switches" Area, select the switch(es) that you want to assign to the Authentication Server(s) selected in Step 1, and click on one of the **Add/Remove** buttons to move them to the "Selected Switches" Area.

3. Click on the **Assign Auth Servers** button.

Assigning Authentication Servers to Logical Groups

1. Select the applicable **Primary** and **Secondary** Authentication Servers from one or more of the drop-down lists at the top of the page. You cannot select the same server for both Primary and Secondary. If you select "None" for the Primary, the only choice for Secondary is “None”.

2. Click on the **Group** icon in the "Selected Switches" Area. The **Select Device Groups** screen will appear.



3. Select the group(s) that you want to assign to the Authentication Server(s) selected in Step 1, and click on one of the **Add/Remove** buttons to move them to the "Selected Switches" Area. The switches contained in the selected group are displayed at the bottom of the screen if the **Show Selected Devices in Preview** checkbox is selected.

> **Note:** If you select the **Use Group Selection** radio button, only the switches contained in the selected group will be configured. If you select the **Add to the Current Selection** radio button, the switches contained in the selected group(s) will be added to any switches you selected individually, if applicable.

4. Click the **OK** button. The **Select Device Groups Screen** will close.

5. Click on the **Assign Auth Servers** button.

Deleting Authentication Servers

Generally, you should not remove an Authentication Server for a switch that has Access Guardian policies assigned to 1 or more ports. If you attempt to set either the primary 802.1x or MAC Authentication Server to "None" (effectively removing the authentication server), the operation will fail if there is at least one Access Guardian policy assigned to the switch. If you select the **Force Delete of Server** checkbox, you will be able to remove the Authentication Server. The check box is enabled if one of the primary authentication servers is set to "None".

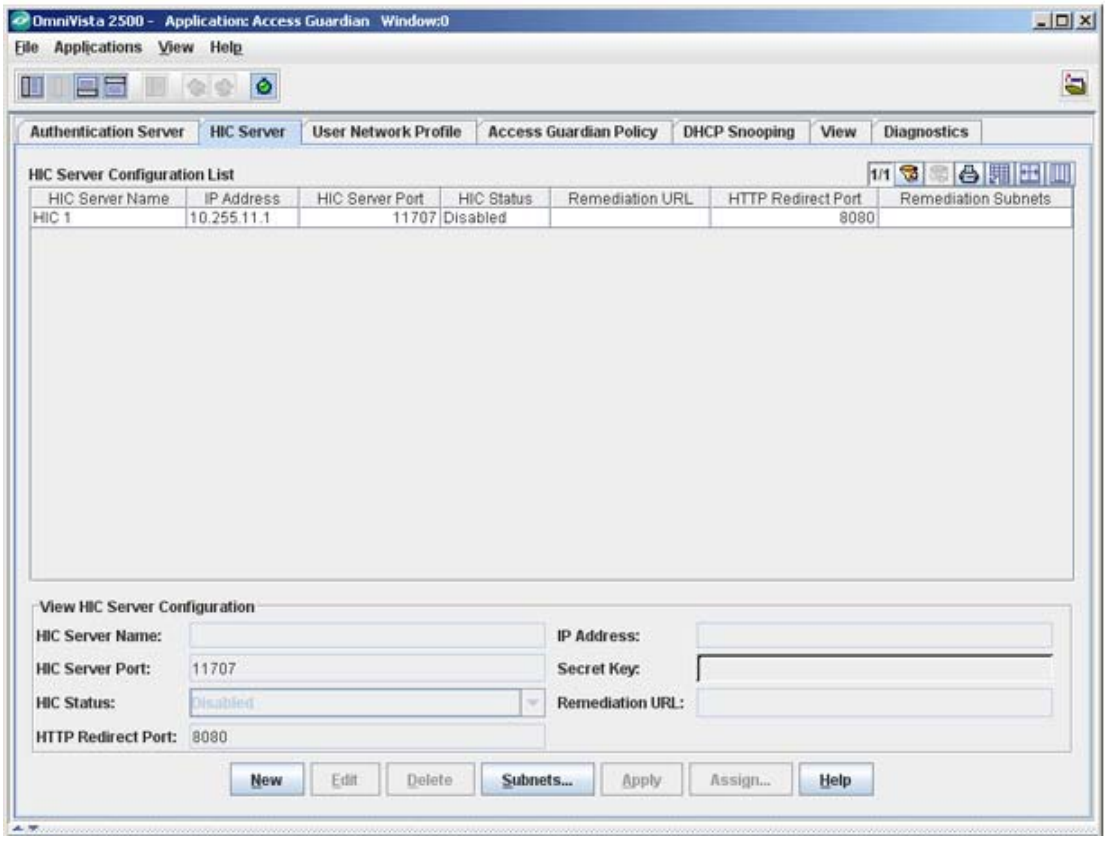
HIC Server Tab

The **HIC Server** Tab is used to configure a Host Integrity Check (HIC) server for the switch. HIC is a mechanism for verifying the compliance of an end user device when it connects to the switch. Configurable HIC policies are used to specify, evaluate, and enforce network access requirements for the host. (For example, is the host running a required version of a specific operating system or anti-virus software up to date.) The Access Guardian implementation of HIC is an integrated solution consisting of AOS switch-based functionality, the InfoExpress compliance agent for the host device (desktop or Web-based), and interaction with the InfoExpress CyberGatekeeper Server (the HIC Server) and its Policy Manager application.

HIC is enabled/disabled on a User Network Profile (UNP). The Access Guardian HIC process is triggered when a device initially connects to an 802.1X port and a device classification policy for that port applies a HIC-enabled UNP to the device. The host device is then granted limited access to the network; only DHCP, DNS, ARP, and any IP traffic between the host and any HIC-related servers is allowed. During this time, the host invokes the HIC compliance agent to complete the verification process. If the HIC server determines the host is compliant, the host is then granted the appropriate access to the network. If the HIC server determines the host is not compliant, the host's network access remains restricted to the HIC-related servers and any other remediation servers that can provide the host with the necessary updates to achieve compliance.

> **Note:** HIC is disabled by default. The HIC feature is not available unless the feature is enabled for the switch. This is true even if HIC servers are configured for the switch or the HIC attribute is enabled for a profile.

HIC Server Tab

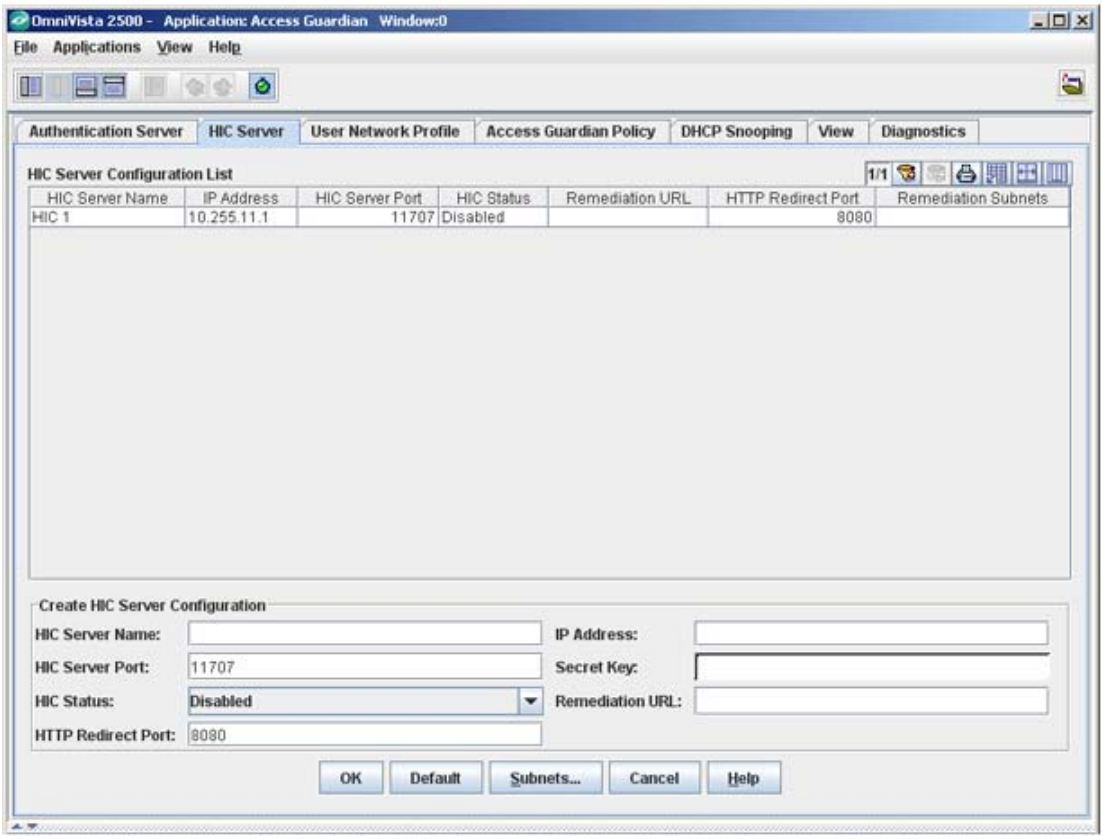


Creating a HIC Server

After setting up the InfoExpress CyberGatekeeper Server, follow the steps below to identify the server to the OmniVista Access Guardian application. Access Guardian can then interact to interact with the InfoExpress application on the server to verify the compliance of an end user device when it connects to the switch. Follow the steps below to configure a new HIC Server.

> **Note:** This section describes how to configure the AOS switch-based functionality to allow OmniVista to interact with the InfoExpress CyberGatekeeper Server. See the InfoExpress user documentation for more information regarding the configuration of compliance agents and the CyberGatekeeper server.

Creating a HIC Server



1. Click the **New** button to bring up the "Create HIC Server Configuration" pane.

2. Complete the fields as described below.

- **HIC Server Name -** Enter a name for the HIC Server (e.g., HIC 1).
- **IP Address** - Enter the IP Address of the InfoExpress CyberGatekeeper Server.
- **HIC Server Port** - Enter the UDP port number to be used for HIC requests.
- **Secret Key** - Enter a shared secret required to access the HIC Server.
- **HIC Status** - Enable HIC by selecting **Enabled** from the drop-down menu. By default, the HIC feature is disabled for the switch. This means that all HIC functionality is disabled. For example, if the HIC attribute of a UNP is enabled, the HIC process is not invoked when the profile is applied if the HIC feature is not enabled for the switch.
- **Remediation URL**. - Enter the URL of the Remediation Server. A host can use the InfoExpress desktop compliance agent or a Web-based agent. If the desktop agent is not installed on the host, the switch redirects the host to a Web agent download server.
- **HTTP Redirect Port** - Enter the proxy port number for the Remediation Server (Default = 8080).

3. Click on the **Subnets...** button to add any exception servers needed for initial HIC processing. When the HIC process is initiated for a host device, the host has limited access to the network for communicating with the HIC server and any servers included in the exception list. There are specific servers that a host device may need access to during the HIC process. For example, if

the host is going to use the Web-based compliance agent, access to the Web agent download server is required.

4. Click the **New** button and enter the **Name**, **IP Address** and **Subnet Mask** of the exception server. Click **OK**, then click **Apply**. Repeat the process for any additional exception servers. When you are done adding servers, click the **OK** button to close the window and return to the HIC Server window.

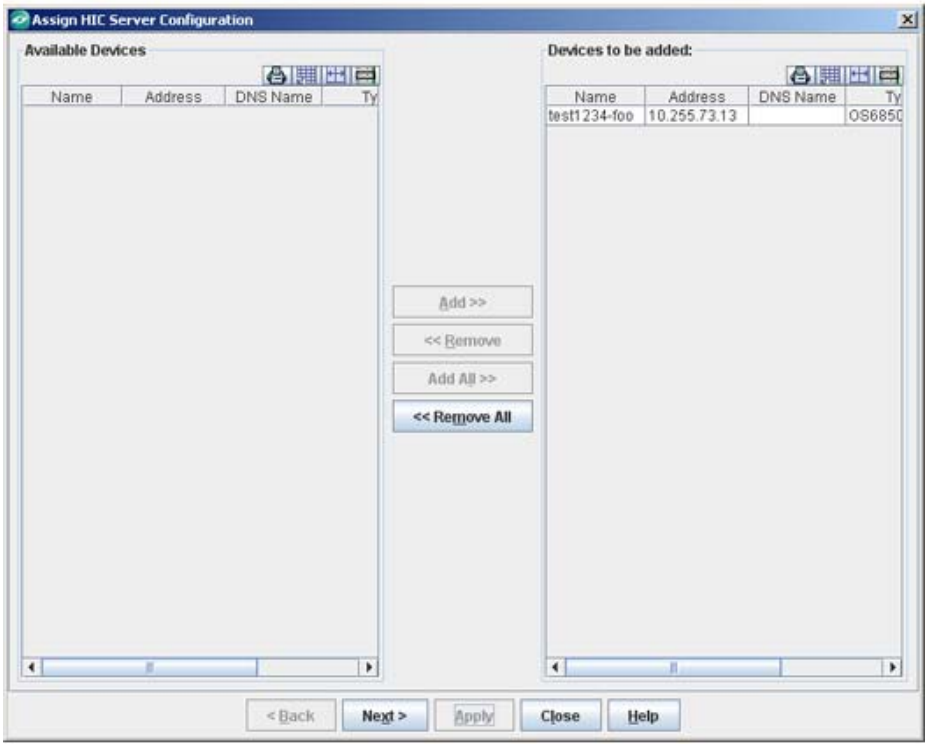
5. Select a HIC server from the "HIC Server Configuration List, and click the **Assign** button to assign the HIC Server to a switch or switches on the network.

Assigning HIC Servers to Switches

Once you have configured a HIC Server, you must assign the server to a switch or switches on the network. If a HIC-enabled UNP is triggered on these switches, Access Guardian will redirect traffic to the HIC Server for compliance before allowing the user access to the network. After clicking the **Assign** button, as described above, the "Assign HIC Server Configuration" Wizard appears. The switches supporting HIC appear in the "Available Device" area.

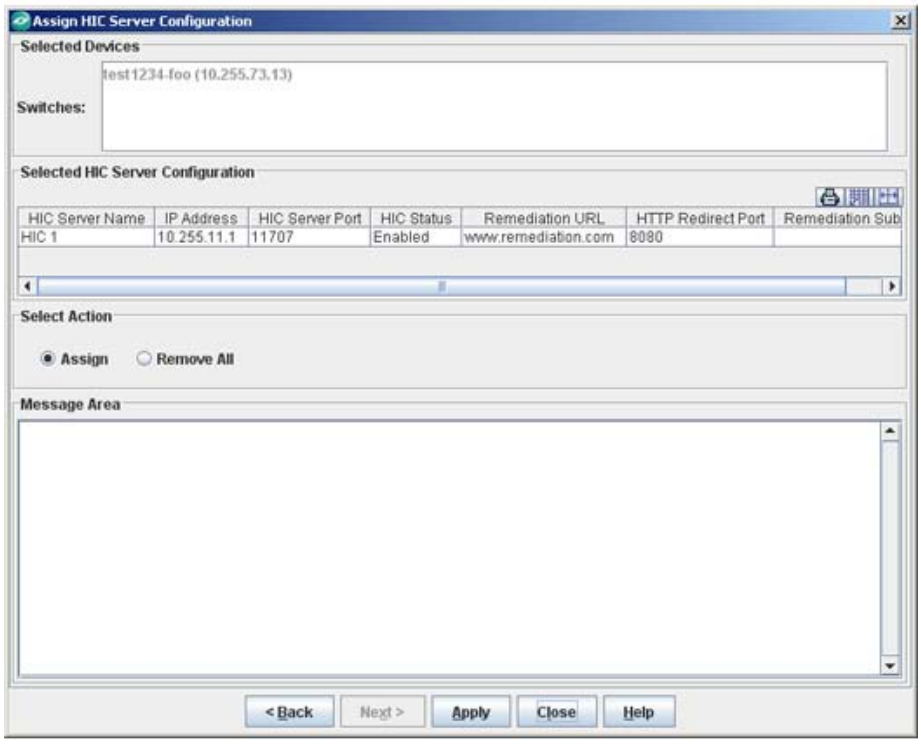
1. Select the switch(es) that you want to assign to the server and use the **Add** button to move the devices to the "Devices to be added" area. (Use the **Add** or **Remove** buttons to add or delete switches.) When you are done selecting devices, click the **Next** button.

Assign HIC Server Wizard - Page 1



After selecting the switches that you want to assign to the server, you must apply the server to those switches. As shown below, the switches to that you are assigning to the HIC Server appear in the "Selected Switches" area.

Assign HIC Server Wizard - Page 2



2. Click the **Apply** button to apply the profile(s). The Message Area shows the progress of the operation.

Editing a HIC Server

Follow the steps below to edit an existing HIC Server.

1. Select the Server in the HIC Server Configuration List and click the **Edit** button. The "Edit HIC Server Configuration" pane appears.

2. Complete the fields as described below:

- I**P Address** - Enter the IP Address of the InfoExpress CyberGatekeeper Server.
- **HIC Server Port** - Enter the UDP port number to be used for HIC requests.
- **Secret Key** - Enter a shared secret required to access the HIC Server.
- **HIC Status** - Enable HIC by selecting **Enabled** from the drop-down menu. By default, the HIC feature is disabled for the switch. This means that all HIC functionality is disabled. For example, if the HIC attribute of a UNP is enabled, the HIC process is not invoked when the profile is applied if the HIC feature is not enabled for the switch.
- **Remediation URL**. - Enter the URL of the Remediation Server. A host can use the InfoExpress desktop compliance agent or a Web-based agent. If the desktop agent is not installed on the host, the switch redirects the host to a Web agent download server.
- **HTTP Redirect Port** - Enter the proxy port number for the Remediation Server (Default = 8080).

3. When you have completed all of the fields, as described above, click the **OK** button. The edited profile will appear in the HIC Server Configuration List.

4. Click the **Apply** button to write the changes to the server.

5. Click the **Assign** button to bring up the "Assign HIC Server" Wizard and assign the server to specific switches.

Deleting a HIC Server

Follow the steps below to delete an existing HIC Server.

1. Select the server in the HIC Server Configuration List and click the **Delete** button. The profile will be highlighted in the List.

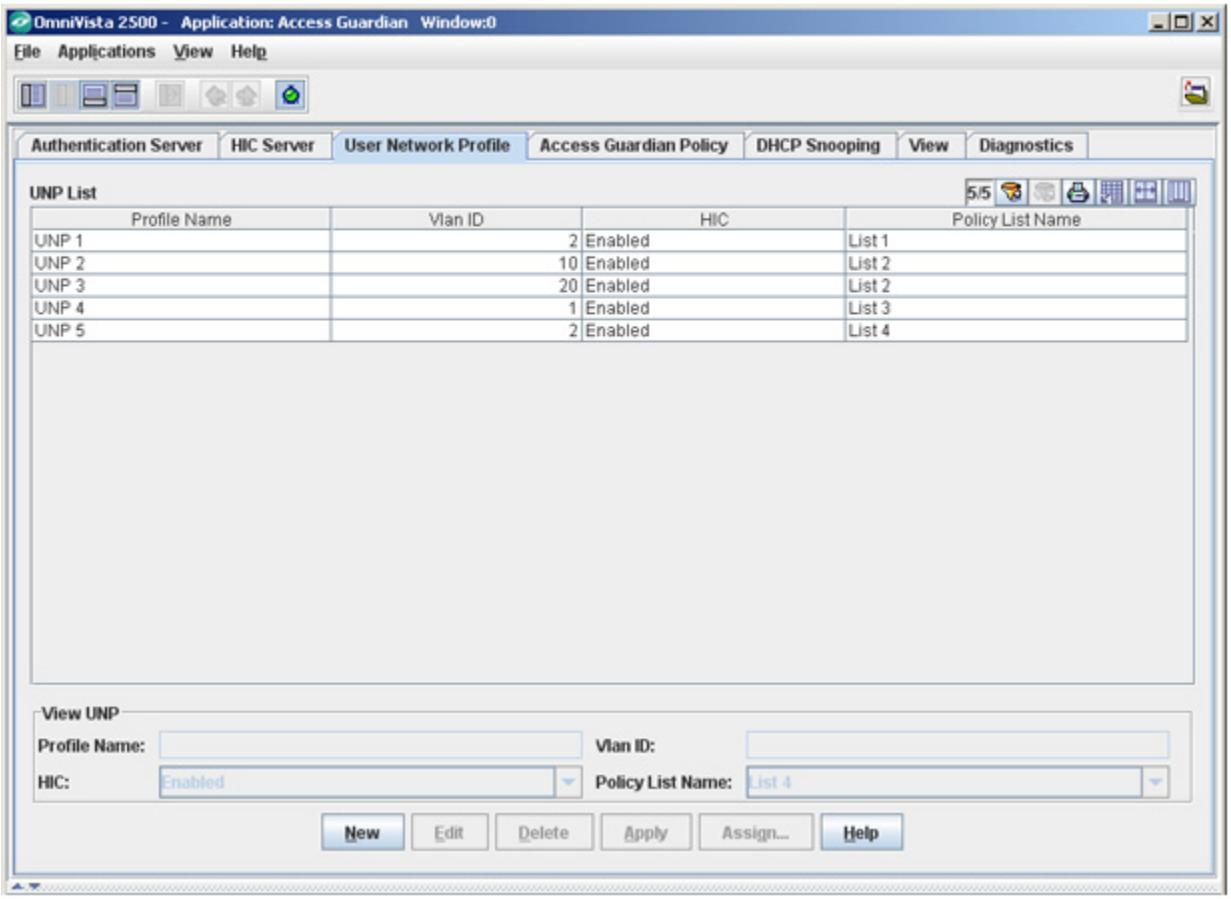
2. Click the **Apply** button to delete the server.

User Network Profile Tab

The **User Network Profile** Tab is used to create/edit/delete User Network Profiles (UNP). A User Network Profile (UNP) defines network access controls for one or more user devices. Each device that is assigned to a specific profile is granted network access based on the profile criteria, instead of on an individual MAC address, IP address, or port.

Assigning users to a profile provides greater flexibility and scalability across the network. Administrators can use profiles to group users according to function. All users assigned to the same UNP become members of that profile group. The UNP then determines what network access resources are available to a group of users, regardless of source subnet, VLAN or other characteristics.

User Network Profile Tab



A UNP consists of the following attributes:

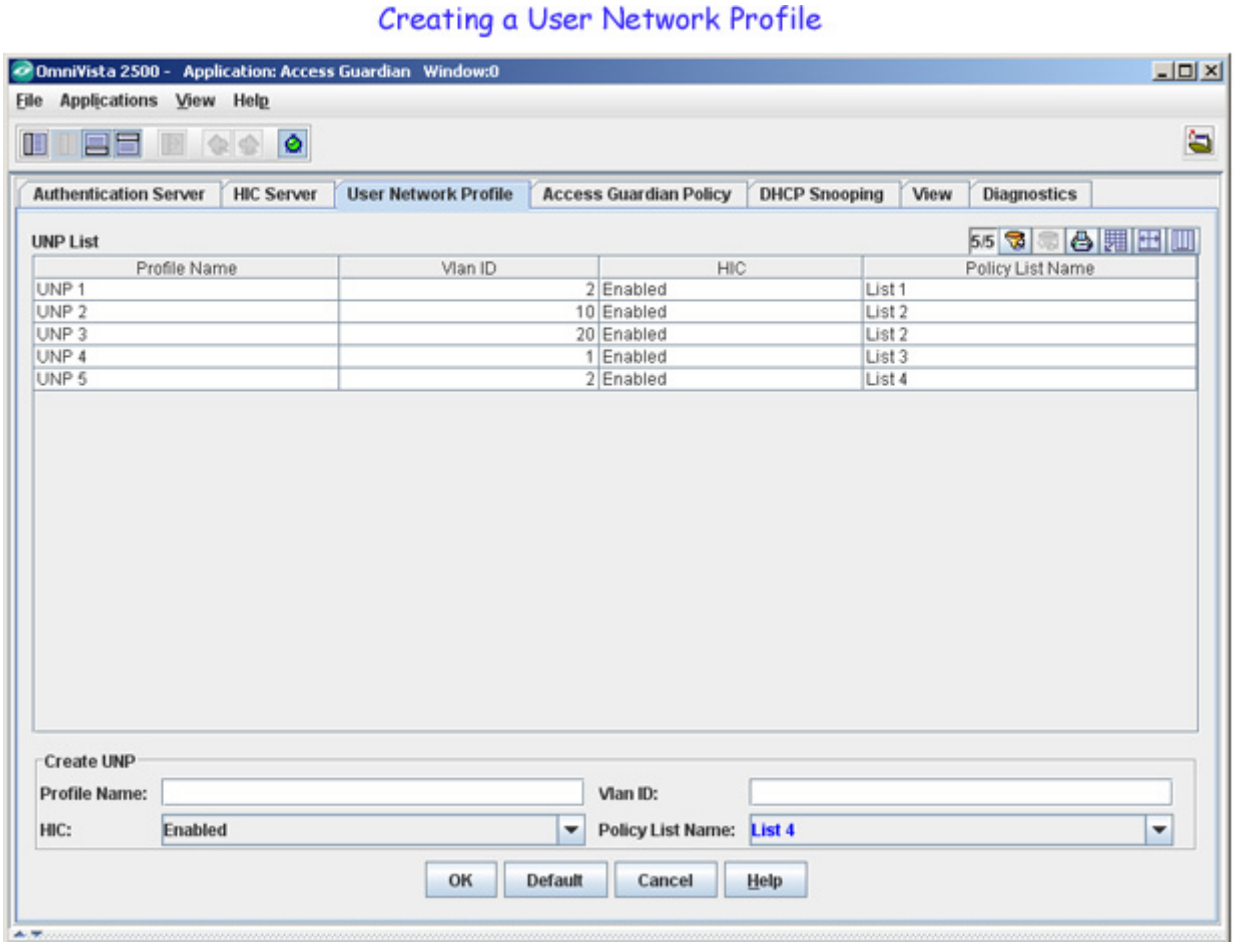
- **Profile Name** - The UNP Profile Name is obtained from the RADIUS server and mapped to the same profile name configured on the switch. The switch profile then identifies three attribute values: VLAN ID, Host Integrity Check (HIC) status, and a QoS Policy List name.
- **VLAN ID** - All members of the profile group are assigned to the VLAN ID specified by the profile.

- **HIC** - Host Integrity Check (HIC) enables or disables device integrity verification for all members of the profile group.
- **Policy List Name** - The Policy List Name is the name of an existing list of QoS policy rules. The rules within the list are applied to all members of the profile to enforce access to network resources.

Creating a User Network Profile

Follow the steps below to create a UNP.

1. Click on the **New** button to bring up the "Create UNP" pane as shown below.



2. Complete the fields as described below:

- **Profile Name** - Enter a name for the UNP.
- **VLAN ID** - Enter the VLAN to which all members of the UNP will be assigned.
- **HIC** - Use the drop-down menu to Enable or Disable HIC.
- **Policy List Name** - Select an existing QoS Policy List from the drop-down menu. The QoS Policy Rules within the list will be applied to all members of the profile to enforce access to network resources. To create a new Policy List, select **New** from the drop-down menu. The **PolicyView/QoS** application will open to the Policy List Tab.

3. When you have completed all of the fields, as described above, click the **OK** button. The new profile will appear in the UNP List.

4. Click the **Apply** button to write the new profile to the server.

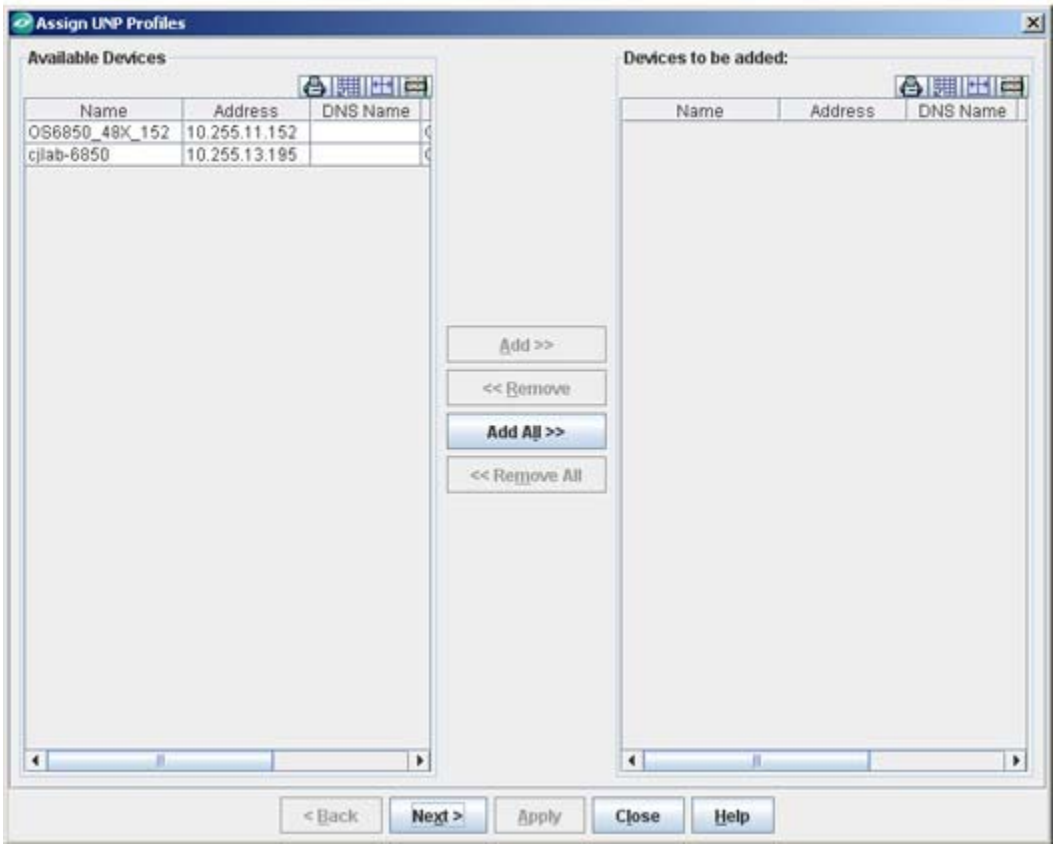
5. Click the **Assign** button to bring up the "Assign UNP" Wizard and assign the profile(s) to specific switches.

Assigning a User Network Profile

Once a UNP has been created, you must assign the profile(s) to specific switches on the network. After clicking the Assign button, as described above, the "Assign UNP" Wizard appears. The switches supporting Access Guardian appear in the "Available Device" area.

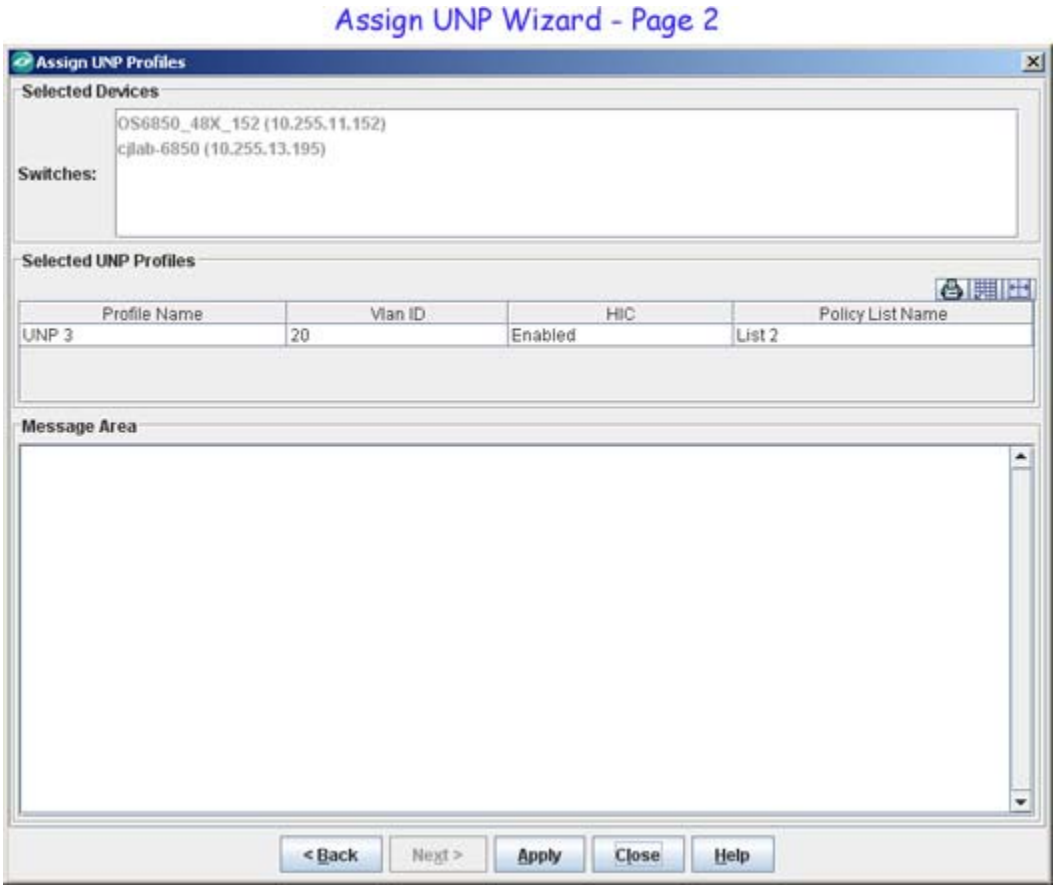
1. Select the switch(es) to which you want to assign the profile(s) and use the **Add** button to move the devices to the "Devices to be added" area. (Use the **Add** or **Remove** buttons to add or delete switches.) When you are done selecting devices, click the **Next** button.

Assign UNP Wizard - Page 1



After selecting the switches to which you want to apply the profile, you must apply the profiles to those switches. As shown below, the User Network Profile(s) you are applying appear in the "Selected UNP" area.

2. Click the **Apply** button to apply the profile(s). The Message Area shows the progress of the operation.



Editing a User Network Profile

Follow the steps below to edit an existing profile.

1. Select the profile in the UNP List and click the **Edit** button. The "Edit UNP" pane appears.

2. Complete the fields as described below:

- **Profile Name** - Enter a name for the UNP.
- **VLAN ID** - Enter the VLAN to which all members of the UNP will be assigned.
- **HIC** - Use the drop-down menu to **Enable** or **Disable** HIC.
- **Policy List Name** - Select a an existing QoS Policy List from the drop-down menu. The QoS Policy Rules within the list will be applied to all members of the profile to enforce access to network
- . To create a new Policy List, select **New** from the drop-down menu.

3. When you have completed all of the fields, as described above, click the **OK** button. The edited profile will appear in the UNP List.

4. Click the **Apply** button to write the profile to the server.

5. Click the **Assign** button to bring up the "Assign UNP" Wizard and assign the profile(s) to specific switches.

Deleting a User Network Profile

Follow the steps below to delete an existing UNP.

1. Select the profile in the UNP List and click the **Delete** button. The profile will be highlighted in the UNP List.

3. Click the **OK** button. The profile will be removed from the UNP List.

4. Click the **Apply** button to delete the profile from the server.

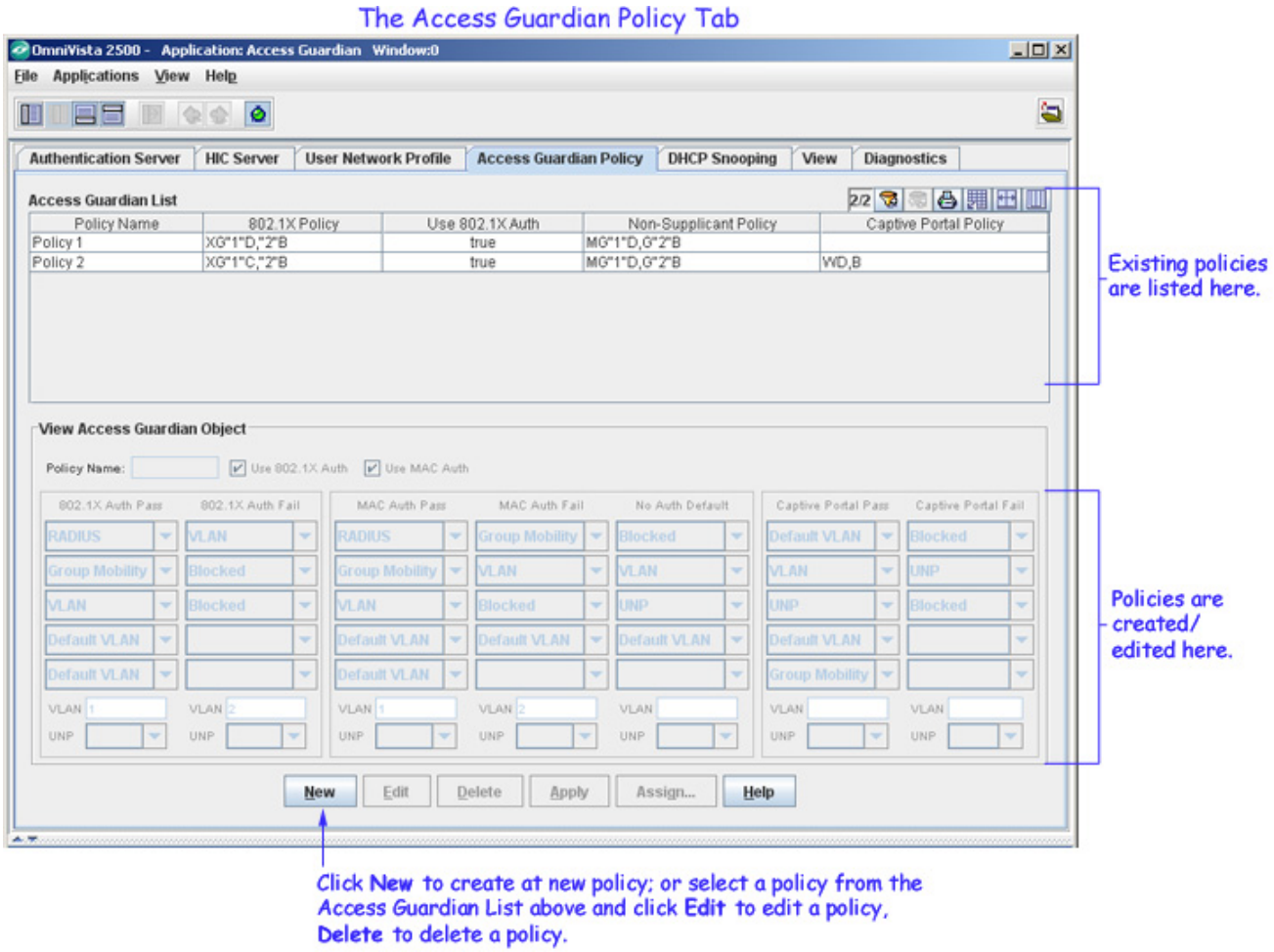
Access Guardian Policy Tab

The **Access Guardian Policy** tab is used to create Access Guardian policies and assign those policies to switches in the network. Access Guardian enables you to apply 802.1x functionality across a set of ports on one or more switches in a single operation. Moreover, this functionality is supported for both 802.1x clients (Supplicants) and non-802.1x clients (Non-Supplicants) through configurable 802.1x device classification policies to handle access to 802.1x ports.

Access Guardian uses 802.1x or MAC Authentication via a remote RADIUS Server to create policies to determine the action to take when a device passes or fails Access Guardian authentication. Based on these policies, a device can be assigned to a specified VLAN (or blocked) depending on whether the device passes or fails authentication.

You can also configure Captive Portal policies for web-based authentication and device classification via a remote RADIUS Server. Web-based authentication is particularly useful for providing guest access to the network. The Captive Portal feature can be used to set up temporary accounts for guests and visitors. Such accounts are accessed through a web-based login screen and require the user to enter valid credentials to access the network.

> **Note:** The Access Guardian application is only available on 6800, 6850, and 9000 Series devices using AOS 6.1.3 or later; and is only accessible to a user with Network Administrator privileges. Before using Access Guardian, several prerequisites must be met.



Access Guardian Prerequisites

Before Access Guardian can be used, the Network Administrator must assign at least one RADIUS Server to a switch and assign that server to either 802.1x Authentication or MAC Authentication (usually both). If necessary, click on the **Config Auth Servers** button on the **Assign Authentication Server** Tab to bring up the **Authentication Servers** application and create the server(s).

Note: Access Guardian is only available on 802.1x-enabled ports.

Access Guardian Policy Defaults

When 802.1x is enabled for a switch port, default Access Guardian device classification policies are applied to all devices connected to the port. As a result, it is only necessary to configure such policies if the default policy is not sufficient for network access control.

Default Supplicant Policies

Pass - Apply Group Mobility Rules. If no rules are configured, assign the user to the Default VLAN.
Fail - Block the user from accessing the port.

Default Non-Supplicant Policies

By default, non-supplicant devices are blocked from accessing the port.

Default Captive Portal Policies
Pass - Assign the user to the Default VLAN
Fail - Block the user from accessing the port.

Access Guardian Policy Types

There are three type of Access Guardian policies: Supplicant Policies (802.1x clients), Non-Supplicant Policies (non-802.1x clients), which use MAC authentication, and Captive Portal Policies, which provide web-based authentication. One Supplicant, one Non-Supplicant, and one Captive Portal policy is allowed for each 802.1x port. Configuring a new policy overwrites any policies that may already exist for the port. Also note that if a non-supplicant policy is not configured for an 802.1x port, non-supplicants are automatically blocked from accessing the port. All policy types use a remote RADIUS server for authentication as described below.

- **Supplicant Policies -** Use 802.1x authentication via a remote RADIUS server to classify 802.1x devices connected to 802.1x-enabled ports when 802.1x authentication does not return a VLAN ID or authentication fails.
- **Non-Supplicant Policies -** Use MAC authentication via a remote RADIUS server for non-802.1x-enabled ports. MAC authentication verifies the source MAC address of a Non-Supplicant device via the remote RADIUS server. Similar to 802.1x authentication, the switch sends RADIUS frames to the server with the source MAC address embedded in the username and password attributes.
    - **Non-Supplicant Non-Authentication Policies -** Are policies for non-supplicant devices that do not perform any authentication and limit the device assignment to non-authenticated VLANs.
- **Captive Portal Policies -** Are a configurable option for both supplicant and non-supplicant policies. Captive Portal allows web-based clients to authenticate through switch using 802.1x or MAC authentication via a RADIUS Server. When the Captive Portal option is invoked, a Login Web Page is presented to the user device. If authentication returns a VLAN ID, the device is assigned to that VLAN. If a VLAN ID is not returned or authentication fails, a separate Captive Portal policy then determines the network access control for the supplicant or non-supplicant. Captive Portal Web Pages are configured/customized using the Resource Manager application.

    Note: The following browsers support the Captive Portal feature: Internet Explorer 6 and 7 (Java 1.6, updates 5 through 12), Firefox 2 and 3 (Java 1.6, updates 5 through 12). Also, **avoid using the 10.123.0.0/16 subnet** within the network This subnet is used exclusively by the Captive Portal feature to redirect DNS requests to the Captive Portal login screen (Captive Portal IP 10.123.0.1) and to assign a temporary IP address for a client device that is attempting web-based authentication.

Configuring Access Guardian Policies

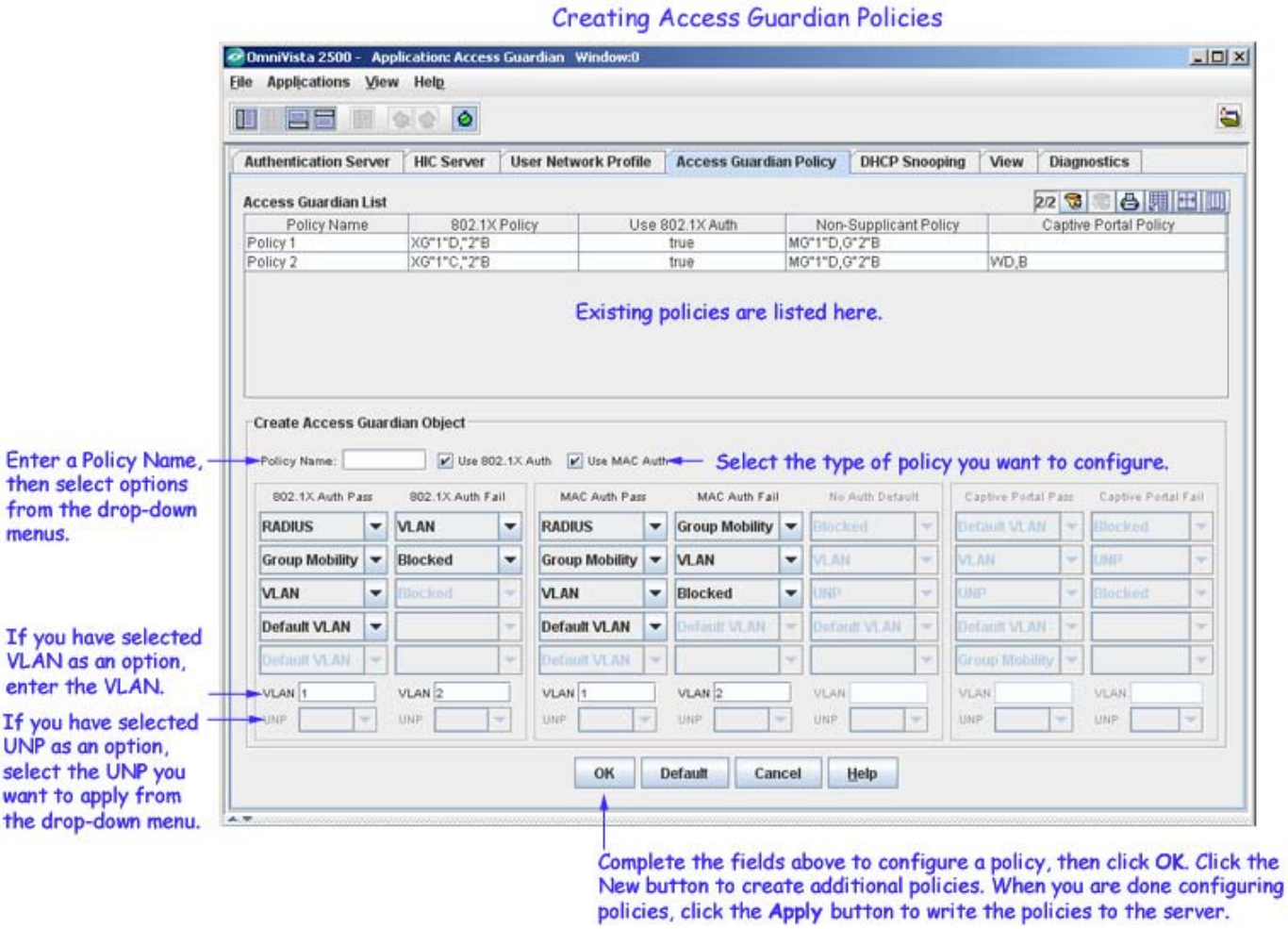
There are two (2) steps involved in configuring Access Guardian Policies a the network:

- Creating an Access Guardian Policy - You must first create the policy(ies) that you want to employ.
- Applying an Access Guardian Policy - After the policy(ies) are created, you must apply the policy(ies) to specific switches and ports.

Creating Access Guardian Policies

You must first create Access Guardian policies, then assign the policies to specific switches/ports on the network. Follow the steps below to create Access Guardian policies.

1. Click the **New** button. The policy configuration fields will be activated as shown below.



2. Enter a name for the policy in the **Policy Name** field. You **must** enter a name for the policy.

3. Select the type of policy(ies) you want to configure by selecting the checkbox next to the policy(ies):

- **Use 802.1x Authentication** (Supplicant Policy) - Supplicant policies are used to classify 802.1x devices connected to 802.1x-enabled switch ports when 802.1x authentication does not return a VLAN ID or authentication fails.
- **Use MAC Authentication** (Non-Supplicant Policy) - Non-Supplicant policies are used to classify non-802.1x devices connected to 802.1x-enabled switch ports. There are two types of non-supplicant policies. One type uses MAC authentication to verify the non-802.1x device. The second type does not perform any authentication and limits device assignment to VLANs that are not authenticated VLANs.

Note: By default, both 802.1x and MAC Authentication are selected. However, you can create only Supplicant or Non-Supplicant policies. You can also create Non-Supplicant policies for Supplicant devices, by selecting only the "Use MAC Authentication" checkbox. The Captive Portal fields are activated when you select **Captive Portal** from a drop-down menu when configuring a Supplicant or Non-Supplicant policy.

4. Select options from the drop-down menus to configure the policy(ies) to apply when the client passes authentication (first column in each policy type) or fails authentication (second column in each policy type). If the device passes authentication it is assigned to the VLAN specified in the RADIUS Server, which is shown in the first field. The remaining fields are used, in order, to assign the device to a VLAN.

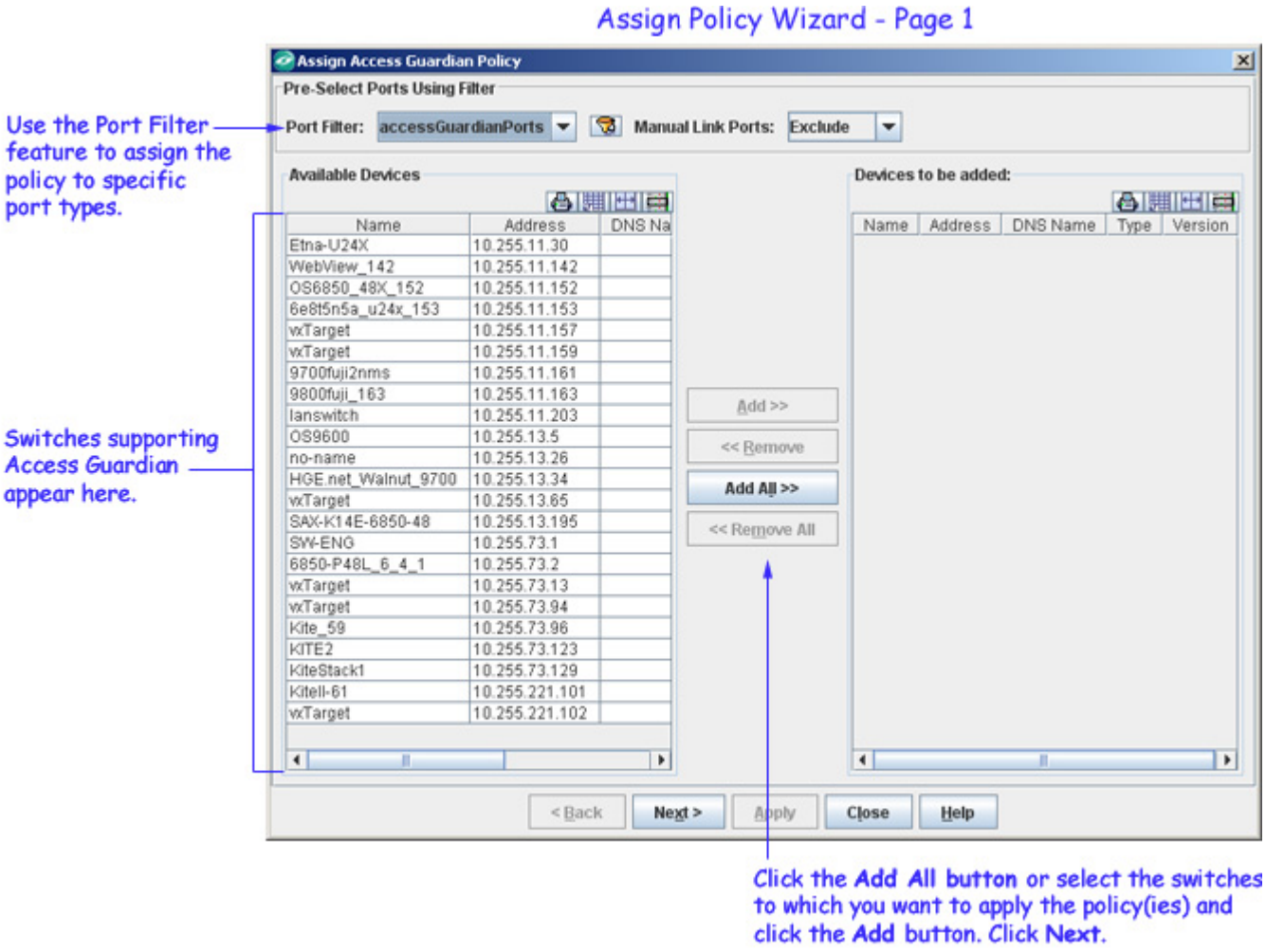
- **Group Mobility -** Use Group Mobility rules to determine the VLAN assignment for a device.
- **VLAN -** Assign the device to the VLAN specified in the **VLAN** field. (If you select this option, you must enter a VLAN in the VLAN field at the bottom of the table.)
- **UNP** - Apply the User Network Profile configured for the device. (If you select this option, you must select a UNP from the drop-down menu in the UNP field at the bottom of the table.)
- **Default VLAN -** Assign the Device to the default VLAN for the 802.1x port.
- **Blocked -** Block the device from accessing the 802.1x port.
- **Captive Portal** - Use Captive Portal policy authentication. When the Captive Portal option is selected when configuring a Supplicant or Non-Supplicant Policy, the Captive Portal drop-down menus are activated, enabling the user to configure Captive Portal Policies.

Note: Policies are enforced in the order in which they are configured. For example, if you create a Supplicant policy with the following "Pass" criteria: Group Mobility, VLAN, Default VLAN, Access Guardian will first use Group Mobility Rules for VLAN assignment. If no Group Mobility Rules apply to the device, VLAN Rules will be used. If no VLAN rules apply, the user will assigned to the Default VLAN.

5. Click **OK**, then click **Apply** to write the policy(ies) to the OmniVista Server. Follow the steps above to configure additional policies. When you are finished configuring policies, click **Assign** to assign the policy(ies) to specific switches/ports on the network, as described below.

Assigning Access Guardian Policies

After creating Access Guardian policies, you must assign the policies to specific switches/ports on the network. When you click **Apply** after creating the policy(ies) (Step 4 above), the following window appears and the Assign Access Guardian Policies wizard guides you through the steps to apply the policy(ies) to specific switches/ports. Follow the steps below to assign the Access Guardian policies you created above.

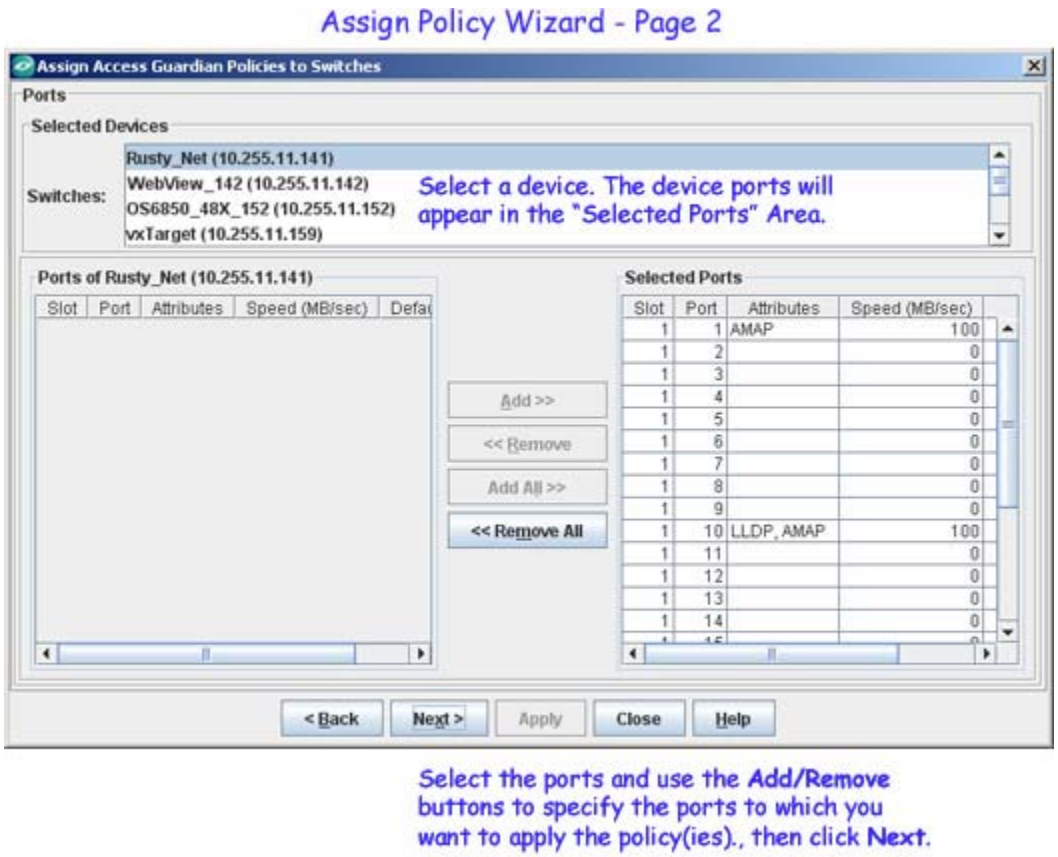


1. As shown above, the switches supporting Access Guardian appear in the "Available Device" area. Select the switch(es) to which you want to assign the policies and use the **Add** button to move the devices to the "Devices to be added" area. (Use the **Add** or **Remove** buttons to add or delete switches.) When you are done selecting devices, click the **Next** button. The following screen appears. Each selected switch appears in the "Selected Devices". The active ports for the highlighted switch appear in the "Selected Ports" area.

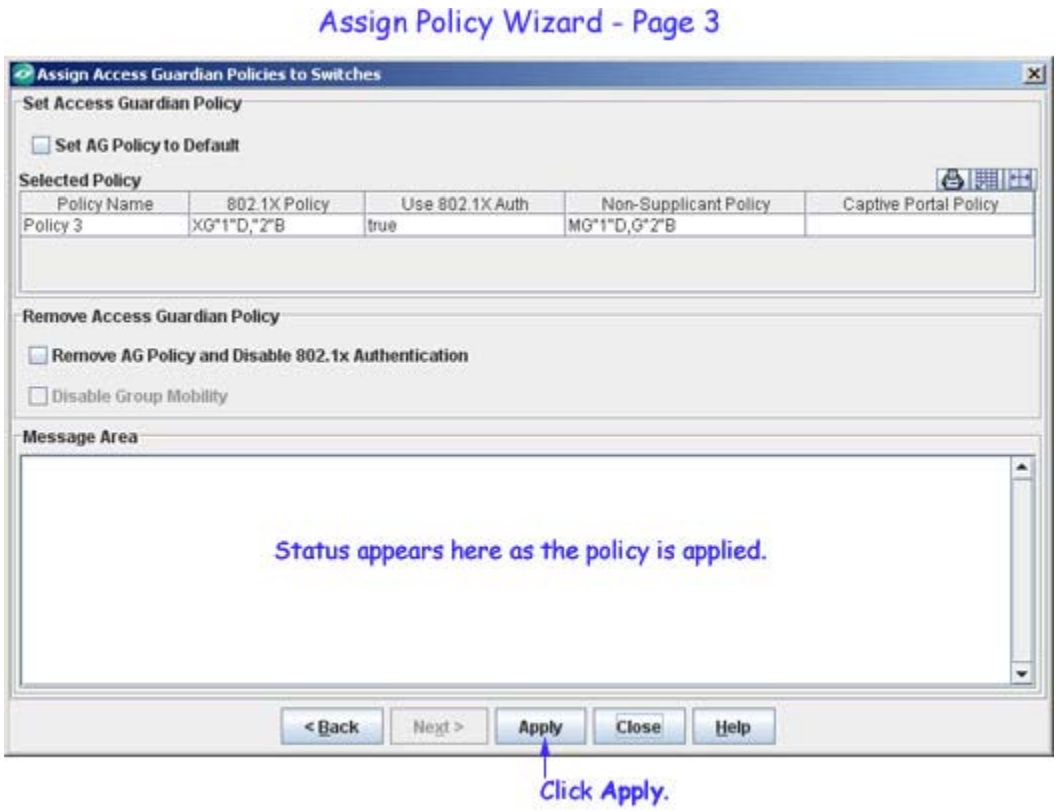
> **Note:** Before clicking the **Next** button, you can use the optional Port Filter and Manual Link Ports features to filter the types of ports to which you want to assign the policy. If you filter for a type of port, those port types will automatically appear on the "Selected Ports) area on page 2 of the Assign Policy Wizard.

The following pre-configured filters are available in the drop-down menu: **accessGuardianPorts** (Access Guardian ports in each device will be selected, **allPorts** (all ports in each device will be selected), **edgePorts** (only mobile or authenticated ports will be selected), **networkPorts** (only the ports that are AMAP, LLDP, LAG or 802.1ab, or ports with a speed >= 2.4Gb/sec will be selected). The user can also edit these filters or configure custom port filters by clicking on the Filter icon to the right of the Port Filter drop-down menu.

The Manual Links Ports feature is used to Include, Exclude, or Pre-Select manual links. By default, "Exclude" is selected for all cases where the user filters for Edge or Non-Network ports. If the user selects Network Ports (DHCP Snooping Trust Mode) "Pre-Select" is selected.



2. Select a switch in the "Selected Devices" area. By default, all active ports on the switch will appear in the Ports" area on the left. If you have used the Port Filter feature, ports that match your selected type will appear in the "Selected Ports" area. Use the **Add**/**Remove** buttons to select the ports to which you want to apply the policy(ies). Repeat this step for each switch in the "Selected Devices" area. When you have selected the ports for each switch, click **Next**. The following screen appears.



3. Click **Apply** to apply the policy. The Message Area shows the progress of the operation.

> **Note:** You can also remove an Access Guardia Policy from selected switches/ports, by editing the policy, selecting the switches/ports and selecting the "Remove AG Policy and Disable 802.1x Authentication" checkbox on page 3 of the "Assign Policy" Wizard.

Editing a Policy

To edit an existing policy, select the policy in the Access Guardian List at the top of the page and click on the **Edit** button. Edit the fields in the Edit Access Guardian Policy Area and click the **Apply** button. Assign the edited policy to specific switches/ports as detailed in "Assigning Access Guardian Policies", above.

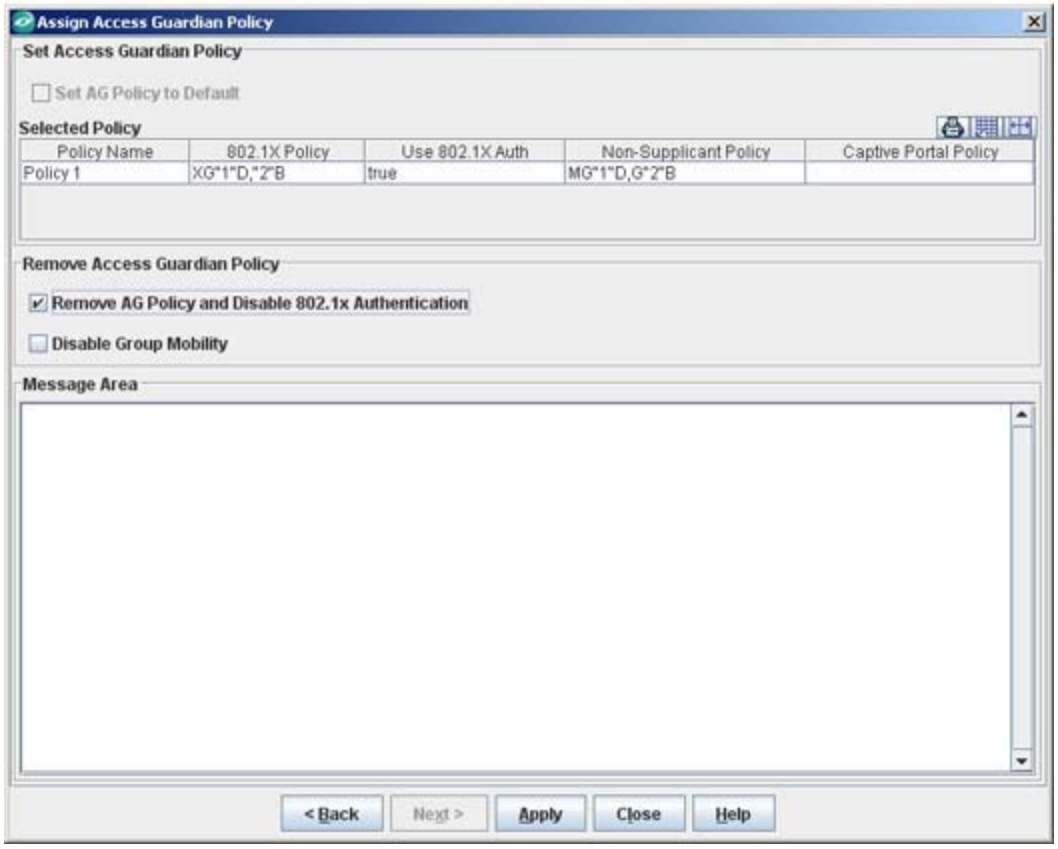
Deleting a Policy

To delete an existing policy from the server, select the policy in the Access Guardian List at the top of the page, click on the **Delete** button, then click on the **Apply** button to delete the policy. This will remove the policy from the server. However, this will not remove a policy(ies) from a switch(es) to which it has already been assigned.

Removing a Policy from a Switch

As noted above, deleting a policy from the Access Guardian List does not remove the policy from any switch(es) to which it has been assigned. To remove a policy from a switch, select the policy in the Access Guardian List, then click the **Assign** button. Use the "Assign Policy" Wizard to select the switches/ports that you want to configure. On the final page of the wizard, select the "Remove AG Policy and Disable 802.1x Authentication" checkbox. then click the **Apply** button, as shown below.

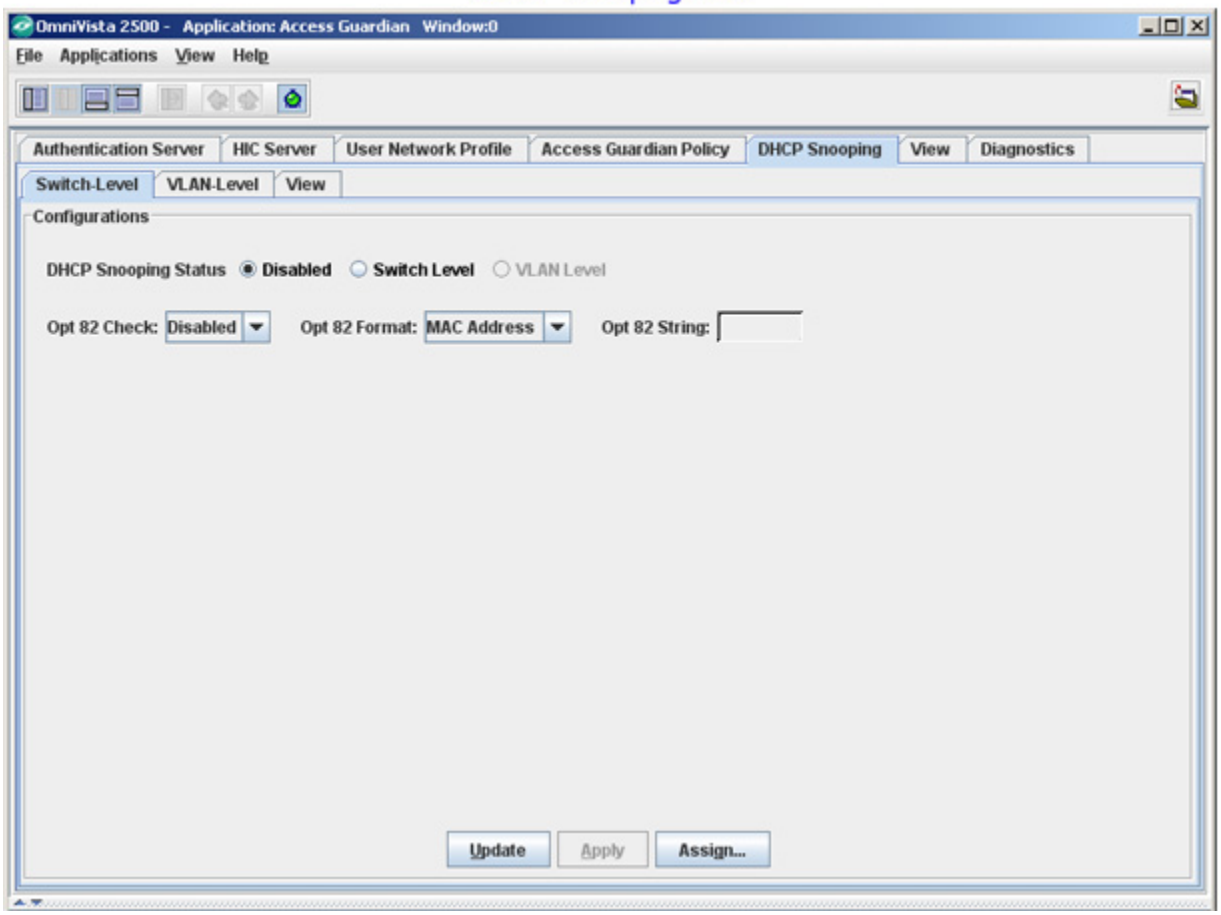
Removing a Policy from a Switch



DHCP Snooping Tab

The **DHCP Snooping** Tab is used to configure DHCP Snooping, and monitor DHCP Snooping violations for ports on selected device. This feature is supported in Release 6.1.3.R01 and later for 6250, 6400, 6800, 6850, 6855, 9000, and 9000E Series Switches. DHCP Snooping improves network security by filtering DHCP messages received from devices outside the network and building and maintaining a binding table (database) to track access information for such devices.

DHCP Snooping Tab



The following tabs within the DHCP Tab allow the user to configure and view DHCP Snooping parameters:

Switch Level Tab - Is used to configure global DHCP Snooping parameters on specific switches/ports on the network.

VLAN-Level Tab - Is used to configure global DHCP Snooping parameters on specific VLANs and their associated ports in the network.

View - Is used to view and configure DHCP Snooping at the Switch Level, VLAN Level, and Port Level, as well as view and configure entries in the DHCP Snooping MAC Address Binding Table.

DHCP Snooping Overview

The User Datagram Protocol (UDP) is a connectionless transport protocol that runs on top of IP networks. DHCP Relay allows you to use non-routable protocols (such as UDP) in a routing environment and forward these packets across VLANs that have IP routing enabled. UDP is used for applications that do not require the establishment of a session and end-to-end error checking, such as E-mail and file transfer.

DHCP Snooping improves network security by filtering DHCP messages received from devices outside the network and building and maintaining a binding table (database) to track access information for such devices. In order to identify DHCP traffic that originates from outside the

network, DHCP Snooping categorizes ports as either trusted or untrusted. A port is trusted if it is connected to a device inside the network, such as a DHCP server. A port is untrusted if it is connected to a device outside the network, such as a customer switch or workstation.

There are two DHCP security features available: DHCP relay agent information option (Option 82) and DHCP Snooping. The Option 82 feature enables the relay agent to insert identifying information into client-originated DHCP packets before the packets are forwarded to the DHCP server. The DHCP Snooping feature filters DHCP packets between untrusted sources and a trusted DHCP server and builds a binding database to log DHCP client information. Although Option 82 is a subcomponent of DHCP Snooping, these two features are mutually exclusive. If the Option 82 feature is enabled for the switch, DHCP Snooping is not available. The reverse is also true; if DHCP Snooping is enabled, Option-82 is not available. In addition, the following differences exist between these two features:

- DHCP Snooping does require and use the Option-82 data insertion capability, but does not implement any other behaviors defined in RFC 3046.
- DHCP Snooping is configurable at the switch level and on a per-VLAN basis, but Option-82 is only configurable at the switch level.

Note: The Option 82 feature is enabled/disabled using the **ip helper dhcp-snooping option-82 data-insertion {enable | disable}** command in the CLI.

Using DHCP Snooping

DHCP Snooping improves network security by filtering DHCP messages received from devices outside the network and building and maintaining a binding table (database) to track access information for such devices. In order to identify DHCP traffic that originates from outside the network, DHCP Snooping categorizes ports as either trusted or untrusted. A port is trusted if it is connected to a device inside the network, such as a DHCP server. A port is untrusted if it is connected to a device outside the network, such as a customer switch or workstation.

When DHCP Snooping is first enabled, all ports are considered untrusted. It is important to then configure ports connected to a DHCP server inside the network as trusted ports. If a DHCP packet is received on an untrusted port, it is considered an untrusted packet. If a DHCP packet is received on a trusted port, it is considered a trusted packet. DHCP Snooping only filters untrusted packets and will drop such packets if one or more of the following conditions are true:

- The packet received is a DHCP server packet, such as a DHCPOFFER, DHCPACK, or DHCPNAK packet. When a server packet is received on an untrusted port, DHCP Snooping knows that it is not from a trusted server and discards the packet.
- The source MAC address of the packet and the DHCP client hardware address contained in the packet are not the same address.
- The packet is a DHCPRELEASE or DHCPDECLINE broadcast message that contains a source MAC address found in the DHCP Snooping binding table, but the interface information in the binding table does not match the interface on which the message was received.
- The packet includes a relay agent IP address that is a non-zero value.

- The packet already contains Option 82 data in the options field and the Option 82 check function is enabled.

If none of the above are true, DHCP Snooping accepts and forwards the packet. When a DHCP packet is received from a server, the following information is extracted from the packet to create an entry in the DHCP Snooping binding table:

- MAC address of the DHCP client.
- IP address for the client that was assigned by the DHCP server.
- The port from where the DHCP packet originated.
- The VLAN associated with the port from where the DHCP packet originated.
- The lease time for the assigned IP address.
- The binding entry type; dynamic or static (user-configured).

After extracting the above information and populating the binding table, the packet is then forwarded to the port from where the packet originated. Basically, the DHCP Snooping features prevent the normal flooding of DHCP traffic. Instead, packets are delivered only to the appropriate client and server ports.

DHCP Snooping Configuration Guidelines

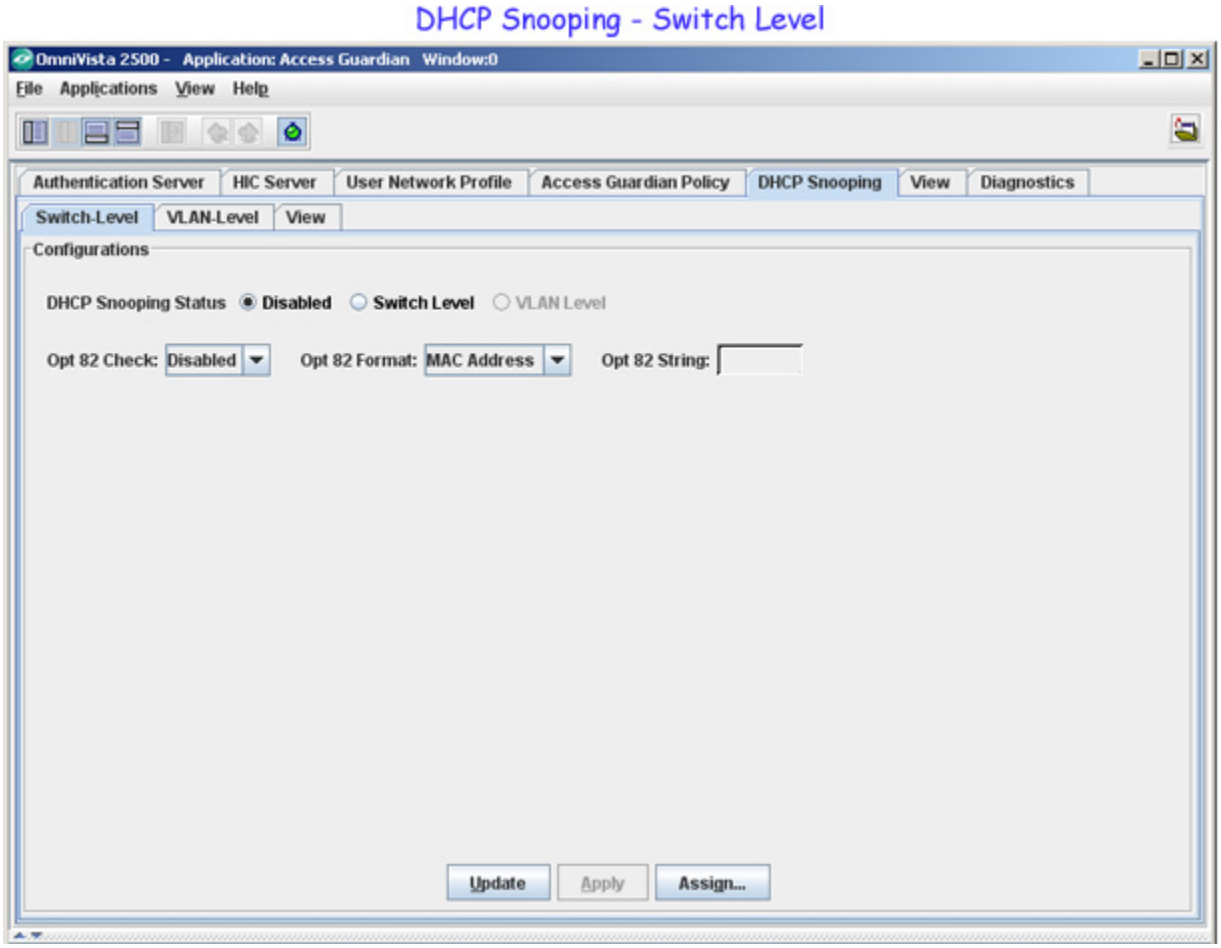
Keep the following guidelines in mind when configuring DHCP Snooping:

- Layer 3 DHCP Snooping requires the use of the relay agent to process DHCP packets. As a result, DHCP clients and servers must reside in different VLANs so that the relay agent is engaged to forward packets between the VLAN domains.
- Layer 2 DHCP Snooping does not require the use of the relay agent to process DHCP packets. As a result, an IP interface is not needed for the client/server VLAN. By default, DHCP broadcasts are flooded on the default VLAN of the client/server port. If the DHCP client and server are both members of the same VLAN domain, the broadcast packets from these sources are bridged as Layer 2 traffic and not processed by the relay agent.
- Both Layer 2 and Layer 3 DHCP Snooping are active when DHCP Snooping is globally enabled for the switch or enabled on one or more VLANs.
- Configure ports connected to DHCP servers within the network as trusted ports.
- Make sure that Option-82 data insertion is always enabled at the switch or VLAN level.
- DHCP packets received on untrusted ports that already contain the Option-82 data field are discarded by default. To accept such packets, configure DHCP Snooping to bypass the Option-82 check.
- By default, rate limiting of DHCP traffic is done at a rate of 512 DHCP messages per second per switching ASIC. Each switching ASIC controls 12 ports (e.g., ports 1–12, 13–24, etc.) on an OS6800 and 24 ports (e.g. ports 1–24, 25–48, etc.) on an OS6850 unit or OS9000 module.

For more information on DHCP Snooping, see the *OmniSwitch AOS Release 6 Network Configuration Guide*.

DHCP Snooping Tab - Switch Level

The **DHCP Snooping - Switch Level** Tab is used to configure DHCP Snooping on a per-switch/port basis. There are two DHCP security features available: DHCP Snooping and the Relay Agent Information option (Option 82) . The DHCP Snooping feature filters DHCP packets between untrusted sources and a trusted DHCP server and builds a binding database to log DHCP client information. The Option 82 feature enables the relay agent to insert identifying information into client-originated DHCP packets before the packets are forwarded to the DHCP server.



Configuring Switch-Level DHCP Snooping

DHCP Snooping and Option 82 are mutually exclusive. If the Option 82 feature is enabled for a switch, DHCP Snooping is not available. The reverse is also true; if DHCP Snooping is enabled, Option 82 is not available.

> **Note:** The Option 82 feature is enabled/disabled using the **ip helper dhcp-snooping option-82 data-insertion {enable | disable}** command in the CLI.

DHCP Snooping

To enable **DHCP Snooping**, select the **Switch Level** radio button. Click the **Apply** button, then click the **Assign** button to bring up the Assign DHCP Snooping Switch-Level Configuration" Wizard to enable DHCP Snooping on specific switches.

Option 82 Check

The Option 82 field in a packet contains identifying information that is inserted into client-originated DHCP packets before the packets are forwarded to the DHCP server. The Option 82 Check fields in OmniVista allow you to configure the Option 82 checking on a switch. If the Option 82 Check Field is **enabled**, the switch checks the incoming packets for the Option 82 field.

Opt 82 Check

- **Enable -** Switch checks for Option 82 field. If the packet contains the Option 82 field and is received on an untrusted port, the packet is dropped

- **Disable -** Switch does not check for the Option 82 field. The packet is processed normally, whether or not an Option 82 Field is present.

Option 82 Format

These fields are used to specify the type of data that is inserted into the Option 82 field before a packet is forwarded.

- **MAC Address -** The MAC address of the router interface from which the DHCP packet originated.
- **System Name** - The System Name
- **User Defined** - A user-defined text string up to 64 characters. Enter the text string in the **Opt 82 String Field**.

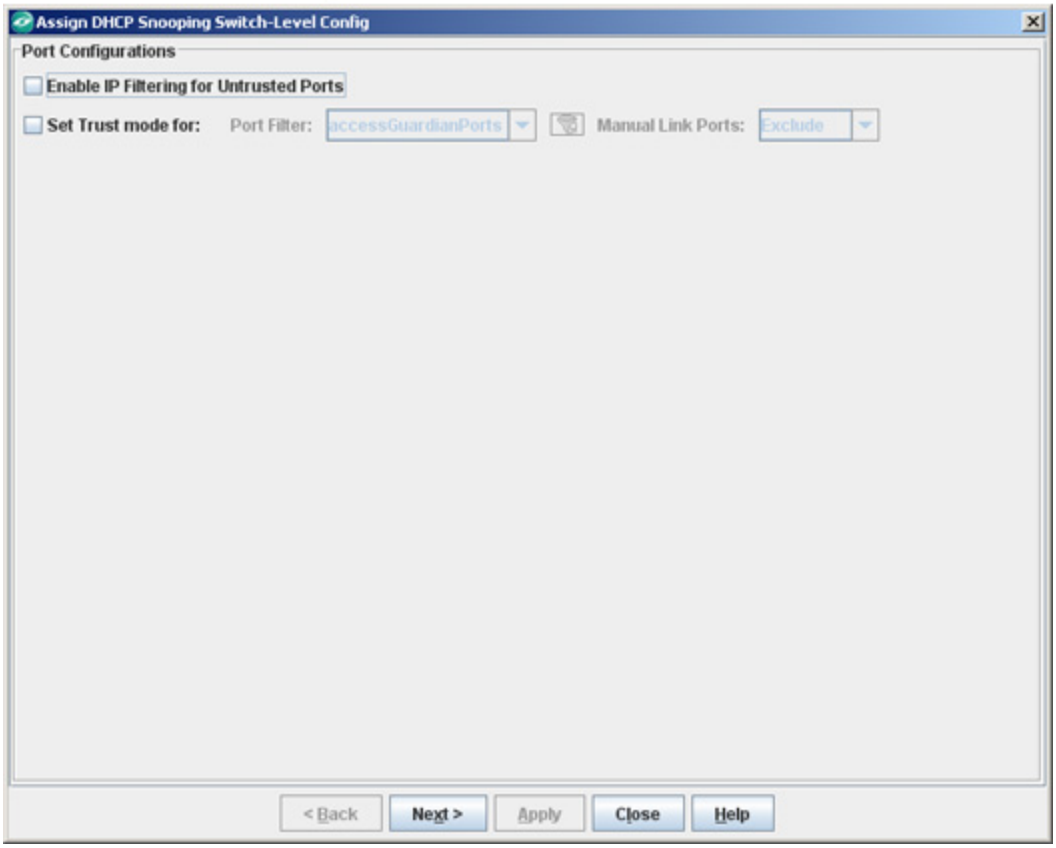
When you have completed the DHCP Snooping and Option 82 Fields, click the **Apply** button, the click the **Assign...** button to bring up the Assign DHCP Snooping Switch-Level Configuration" Wizard.

Assigning the DCHP Configuration

After configuring DHCP Snooping as described above, you must assign the configuration to specific switches/ports. Follow the steps below to assign the DHCP Snooping Configuration.

1. Click the **Assign...** button. The "Assign DHCP Snooping Switch-Level Configuration" Wizard appears.

Assign DHCP Snooping Switch-Level Configuration Wizard (Page 1)



2. Configure the Port Configuration

- **Enable IP Filtering for Untrusted Ports -** When this function is enabled, traffic on the port is restricted to packets received on the port that contain the client MAC address and IP address that have been learned. All other packets are dropped. IP source filtering applies only to ports that are associated with a VLAN that has DHCP Snooping enabled or to all ports when DHCP Snooping is globally enabled for the switch.

  Note: Trust mode assigned by OmniVista and the default mode of Client-Only assigned by the switch to ports are mutually exclusive and Trust mode from OmniVista will overwrite the default mode. Trusted ports will allow both DHCP server and DHCP client messages to pass through, while Client-Only mode allows for only DHCP client messages.

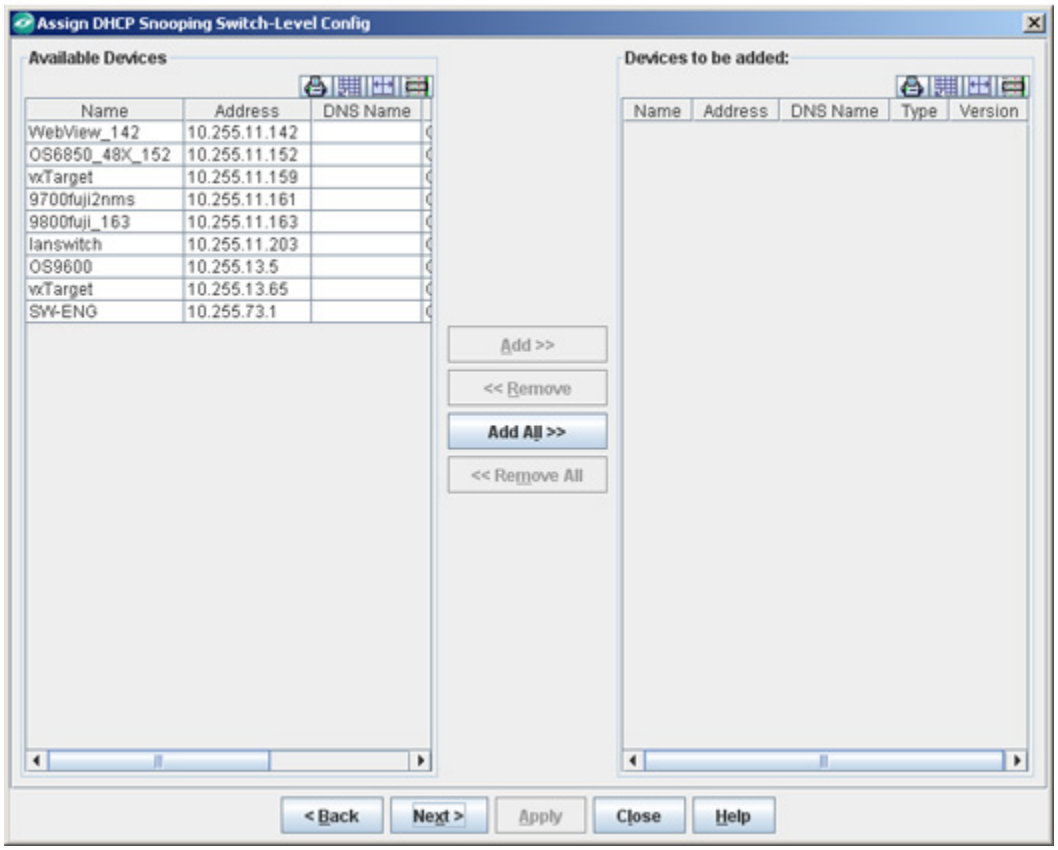
- **Set Trust Mode -** Enable this function to set a port type to "Trusted" mode.
  - **Port Filter -** Select one of the pre-configured port types (e.g., networkPorts) from the drop-down menu to set those port types to "Trusted" mode. The following pre-configured filters are available in the drop-down menu: **accessGuardianPorts** (Access Guardian ports in each device will be selected, **allPorts** (all ports in each device will be selected), **edgePorts** (only mobile or authenticated ports will be selected), **networkPorts** (only the ports that are AMAP, LLDP, LAG or 802.1ab, or ports with a speed >= 2.4Gb/sec will be

selected). You can also edit these filters or configure custom port filters by clicking on the Filter icon to the right of the Port Filter drop-down menu.

- **Manual Link Ports -** Select a filtering option from the drop-down menu to Ignore, Exclude, or Pre-Select manually configured ports. By default, "Exclude" is selected for all cases where the user filters for Edge or Non-Network ports. If the user selects Network Ports (DHCP Snooping Trust Mode) "Pre-Select" is selected.

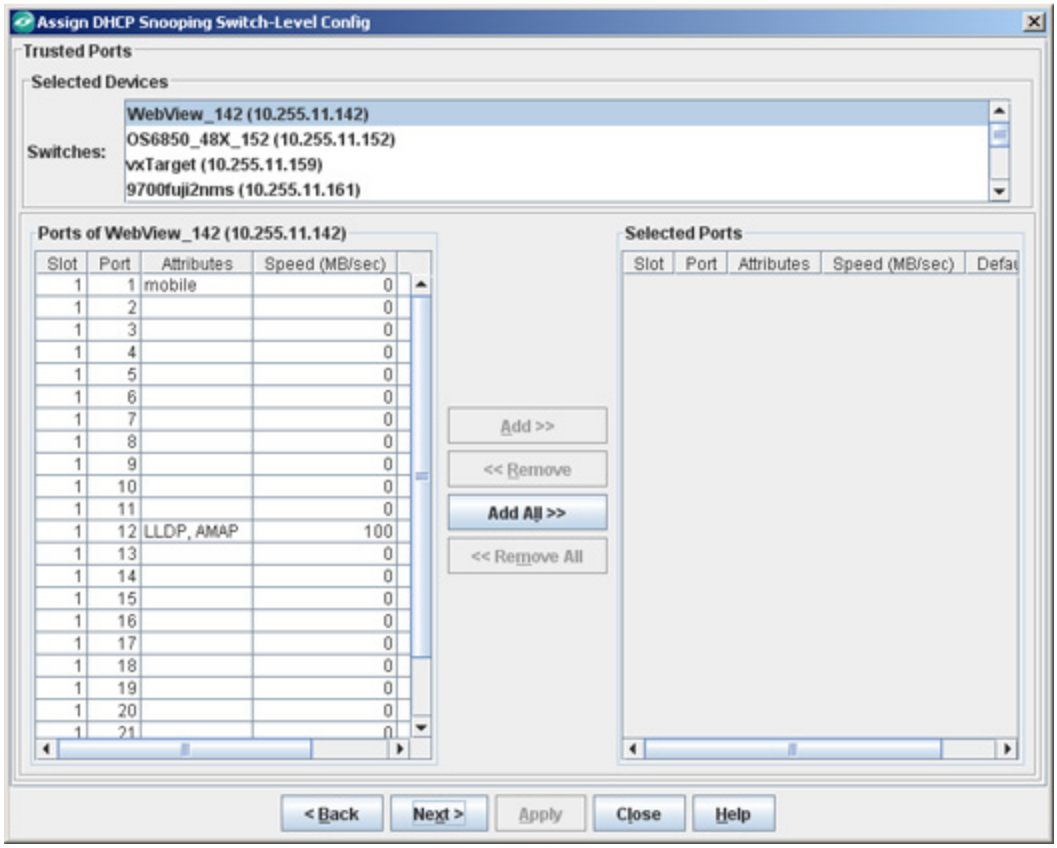
3. Click the **Next** button. Page 2 of the wizard appears.

Assign DHCP Snooping Switch-Level Configuration Wizard (Page 2)



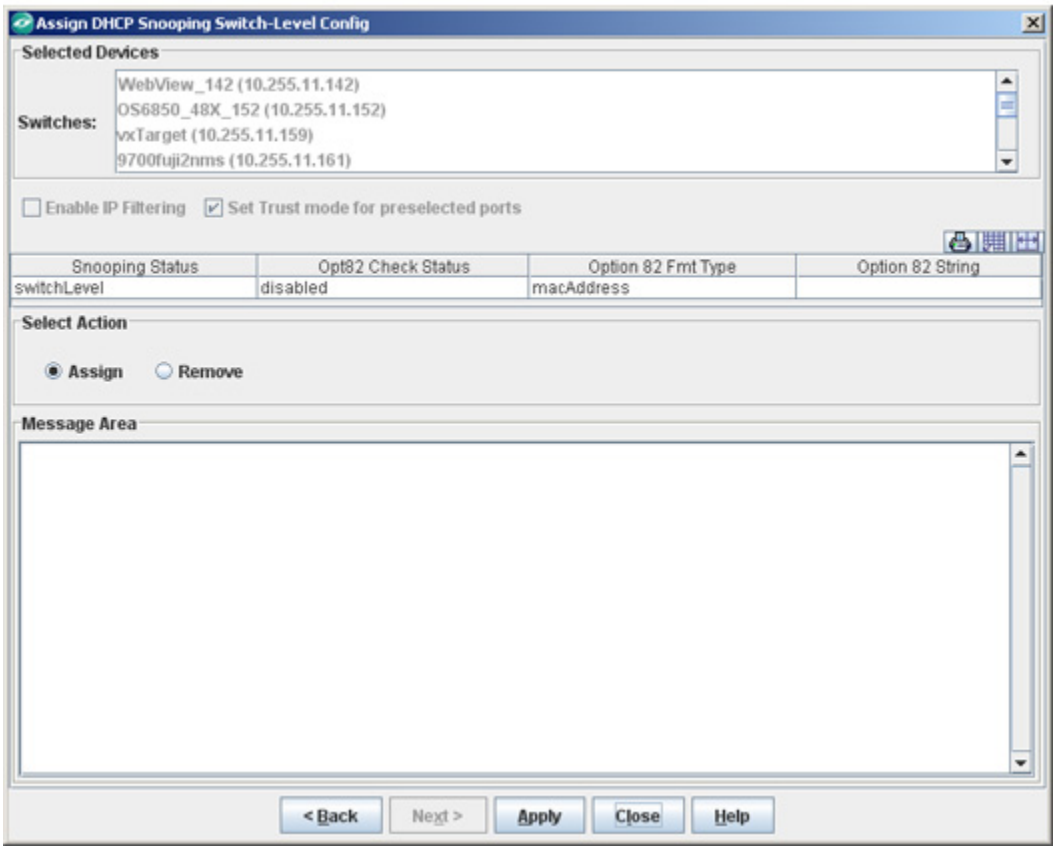
4. Select the switch(es) to which you want to assign DHCP Snooping/Option 82 configuration and use the **Add** button to move the devices to the "Devices to be added" area. (Use the **Add** or **Remove** buttons to add or delete switches.) When you are done selecting devices, click the **Next** button. Page 3 of the Wizard appears.

Assign DHCP Snooping Switch-Level Configuration Wizard (Page 3)



5. Select a switch in the "Selected Devices" area. By default, all active ports on the switch will appear in the Ports" area on the left. If you have used the Port Filter feature, ports that match your selected type will appear in the "Selected Ports" area. Use the **Add**/**Remove** buttons to select the ports to which you want to apply the policy(ies). Repeat this step for each switch in the "Selected Devices" area. When you have selected the ports for each switch, click **Next**. Page 4 of the Wizard appears.

Assign DHCP Snooping Switch-Level Configuration Wizard (Page 4)

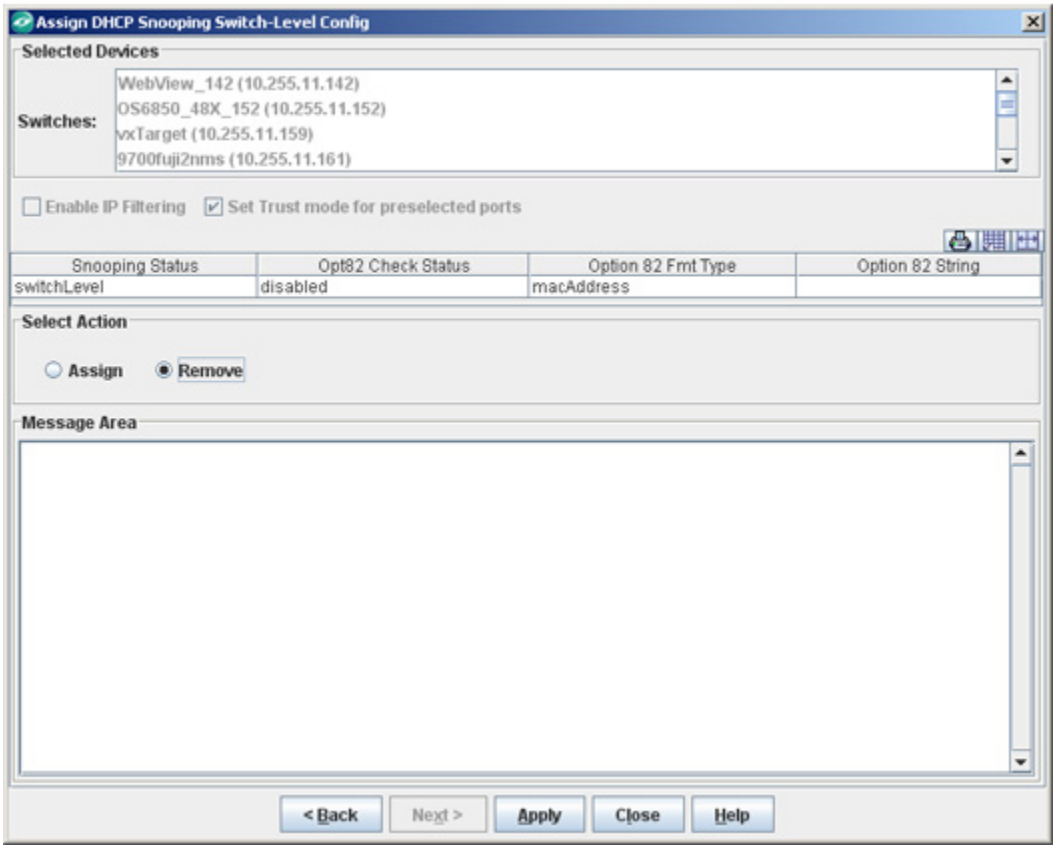


6. Click the **Apply** button to apply the configuration to the selected switches/ports. The Message Area shows the progress of the operation.

Removing a DHCP Snooping Switch-Level Configuration

Use the "Assign DHCP Snooping Switch-Level Configuration" wizard to remove a policy from a switch(es). Click the **Assign** button at the bottom of the Switch Level Tab, then click the **Next** button at the bottom of the first page and select the switches/ports from which you want to remove the configuration. On the final page of the wizard, select the **Remove** radio button in the "Select Action" area, then click the **Apply** button.

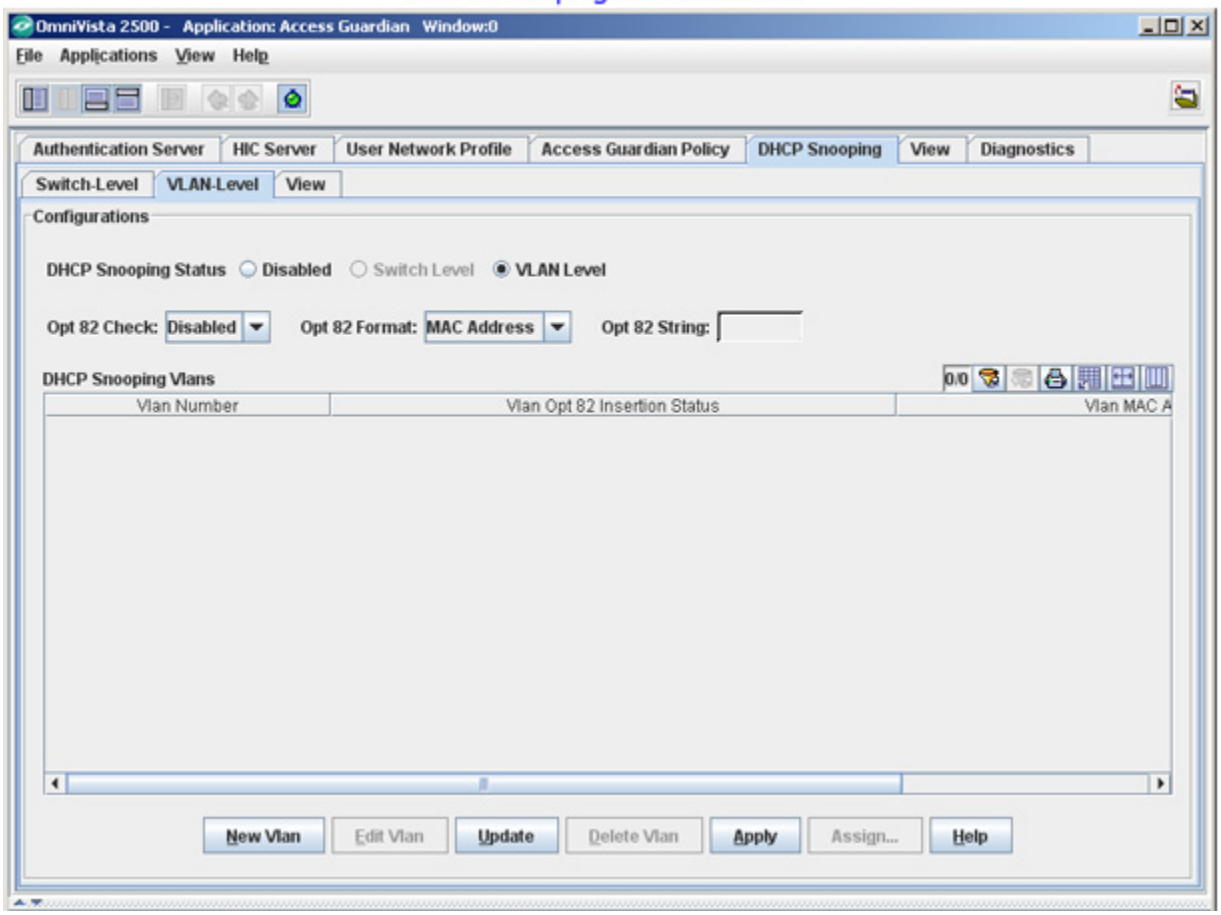
Removing DHCP Snooping Switch-Level Configuration



DHCP Snooping Tab - VLAN Level

The **DHCP Snooping - VLAN Level** Tab is used to configure DHCP Snooping on a per-VLAN/port basis. There are two DHCP security features available: DHCP Snooping and the Relay Agent Information option (Option 82). The DHCP Snooping feature filters DHCP packets between untrusted sources and a trusted DHCP server and builds a binding database to log DHCP client information. The Option 82 feature enables the relay agent to insert identifying information into client-originated DHCP packets before the packets are forwarded to the DHCP server.

DHCP Snooping - VLAN Level



Configuring VLAN-Level DHCP Snooping

DHCP Snooping and Option 82 are mutually exclusive. If the Option 82 feature is enabled for a switch, DHCP Snooping is not available. The reverse is also true; if DHCP Snooping is enabled, Option 82 is not available.

> **Note:** The Option 82 feature is enabled/disabled using the **ip helper dhcp-snooping option-82 data-insertion {enable | disable}** command in the CLI..

Configuring DHCP Snooping at the VLAN level consists of the following steps:

- Configuring DCHP Snooping Options
- Adding the DCHP Snooping Configuration to the VLAN(s)
- Assigning the DHCP Snooping Configuration to the VLAN(s).

Configuring DCHP Snooping Options

DHCP Snooping

To enable **DHCP Snooping**, select the **VLAN Level** radio button. Click the **Apply** button, then click the **Assign** button to bring up the Assign DHCP Snooping VLAN-Level Configuration" Wizard.

Option 82 Check

The Option 82 field in a packet contains identifying information that is inserted into client-originated DHCP packets before the packets are forwarded to the DHCP server. The Option 82 Check fields in OmniVista allow you to configure the Option 82 checking on a switch. If the Option 82 Check Field is **enabled**, the switch checks the incoming packets for the Option 82 field.

Opt 82 Check

- **Enable -** Switch checks for Option 82 field. If the packet contains the Option 82 field and is received on an untrusted port, the packet is dropped.

- **Disable -** Switch does not check for the Option 82 field. The packet is processed normally, whether or not an Option 82 Field is present.

Option 82 Format

These fields are used to specify the type of data that is inserted into the Option 82 field before a packet is forwarded.

- **MAC Address -** The MAC address of the router interface from which the DHCP packet originated.
- **System Name -** The System Name
- **User Defined -** A user-defined text string up to 64 characters. Enter the text string in the **Opt 82 String Field**.

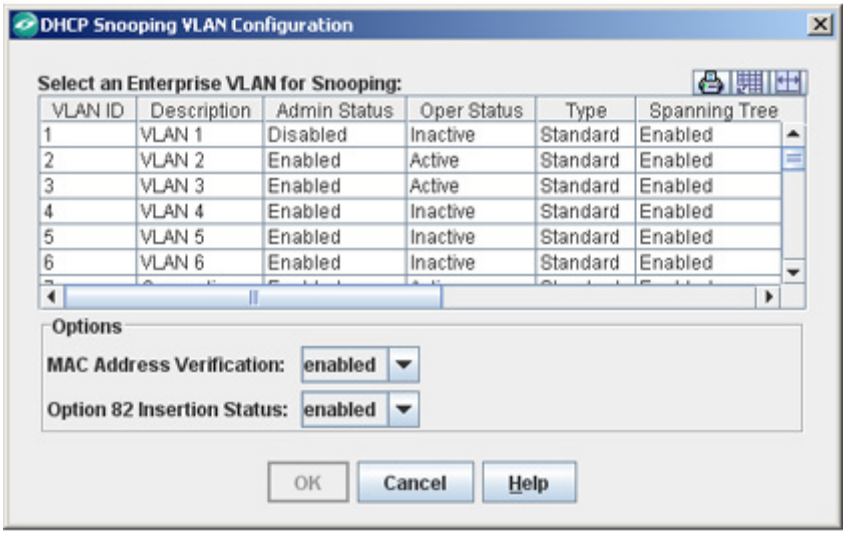
When you have completed the DHCP Snooping and Option 82 Fields, click the **Apply** button, the click the **Assign...** button to bring up the Assign DHCP Snooping VLAN-Level Configuration" Wizard.

Adding the DCHP Snooping Configuration to the VLAN(s)

After configuring DHCP Snooping options as described above, you must add this configuration to the VLAN(s).

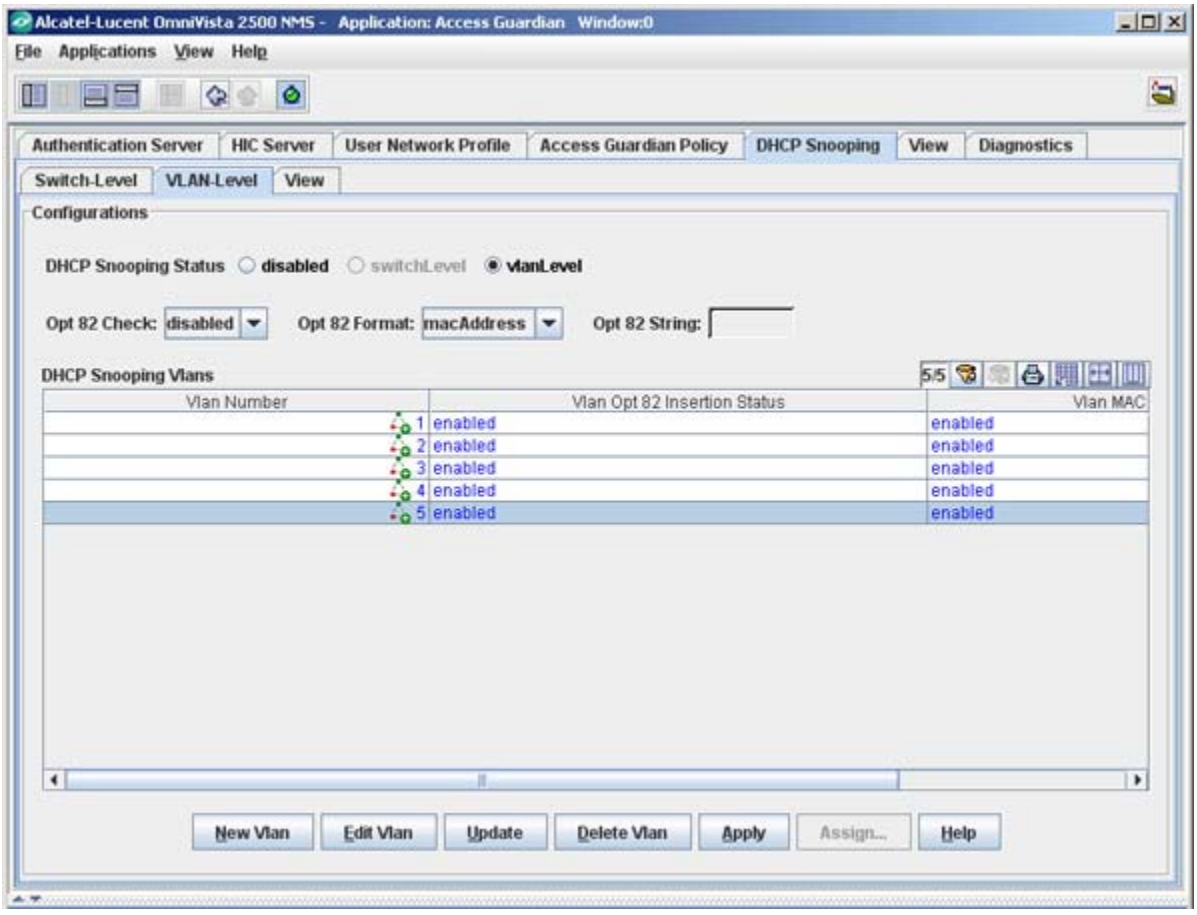
1. Click the **New VLAN** button. The following screen appears listing all VLANs configured on the switch.

Creating a DHCP Snooping VLAN



2. Select the VLAN(s) you want to configure, then Enable/Disable the Option 82 feature for the VLAN(s).

3. Click **OK**. The DHCP Snooping VLAN(s) appear in the table as shown below.



4. Click the **Apply** button to write the configuration to the server.

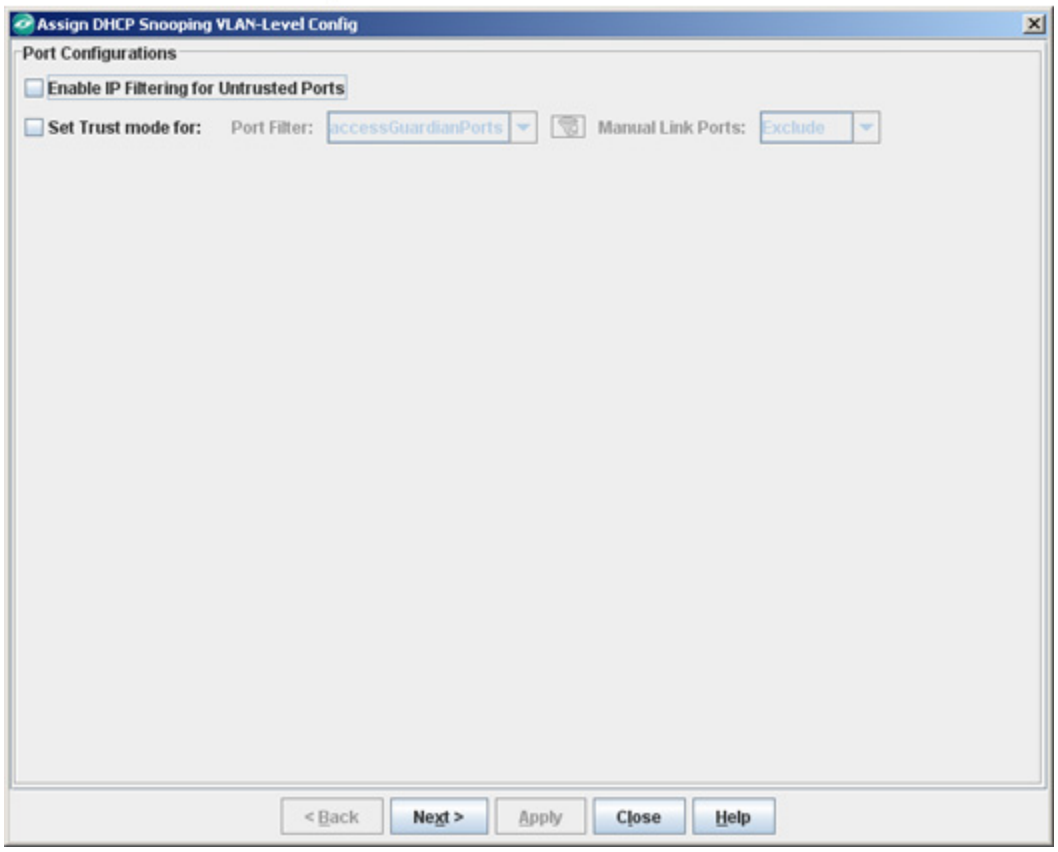
5. Click the **Assign...**button to assign the configuration to the VLAN(s).

Assigning the DCHP Snooping Configuration to the VLAN(s)

After adding DHCP Snooping configuration options to the VLAN(s) as described above, you must assign the configuration to the VLAN. Follow the steps below to assign the DHCP Snooping Configuration.

1. Click the **Assign...** button. The "Assign DHCP Snooping VLAN-Level Configuration" wizard appears.

Assign DHCP Snooping VLAN-Level Configuration Wizard (Page 1)



2. Configure the Port Configuration

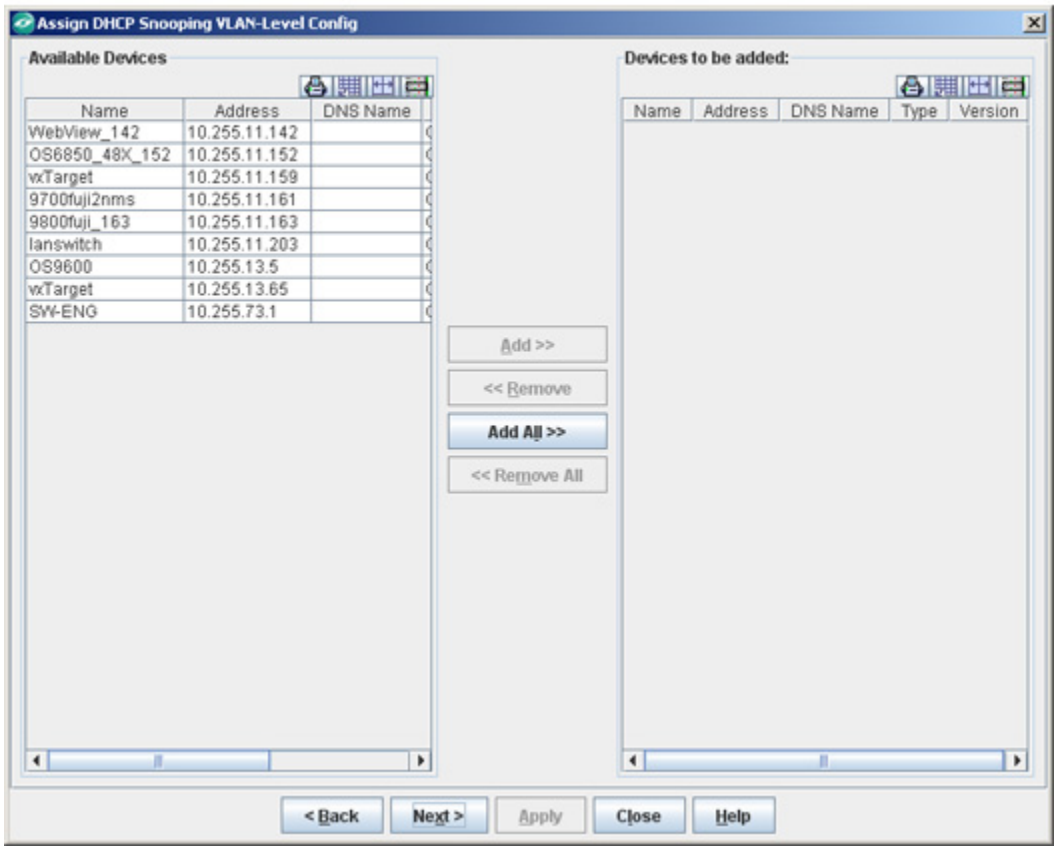
- **Enable IP Filtering for Untrusted Ports -** When this function is enabled, traffic on the port is restricted to packets received on the port that contain the client MAC address and IP address that have been learned. All other packets are dropped. IP source filtering applies only to ports that are associated with a VLAN that has DHCP Snooping enabled or to all ports when DHCP Snooping is globally enabled for the switch.

  Note: Trust mode assigned by OmniVista and the default mode of Client-Only assigned by the switch to ports are mutually exclusive and Trust mode from OmniVista will overwrite the default mode. Trusted ports will allow both DHCP server and DHCP client messages to pass through, while Client-Only mode allows for only DHCP client messages.

- **Set Trust Mode -** Enable this function to set a port type to "Trusted" mode.
  - **Port Filter -** Select one of the pre-configured port types (e.g., networkPorts) from the drop-down menu to set those port types to "Trusted" mode. The following pre-configured filters are available in the drop-down menu: **accessGuardianPorts** (Access Guardian ports in each device will be selected, **allPorts** (all ports in each device will be selected), **edgePorts** (only mobile or authenticated ports will be selected), **networkPorts** (only the ports that are AMAP, LLDP, LAG or 802.1ab, or ports with a speed >= 2.4Gb/sec will be selected). You can also edit these filters or configure custom port filters by clicking on the Filter icon to the right of the Port Filter drop-down menu.
  - **Manual Link Ports -** Select a filtering option from the drop-down menu to Ignore, Exclude, or Pre-Select manually configured ports. By default, "Exclude" is selected for all cases where the user filters for Edge or Non-Network ports. If the user selects Network Ports (DHCP Snooping Trust Mode) "Pre-Select" is selected.

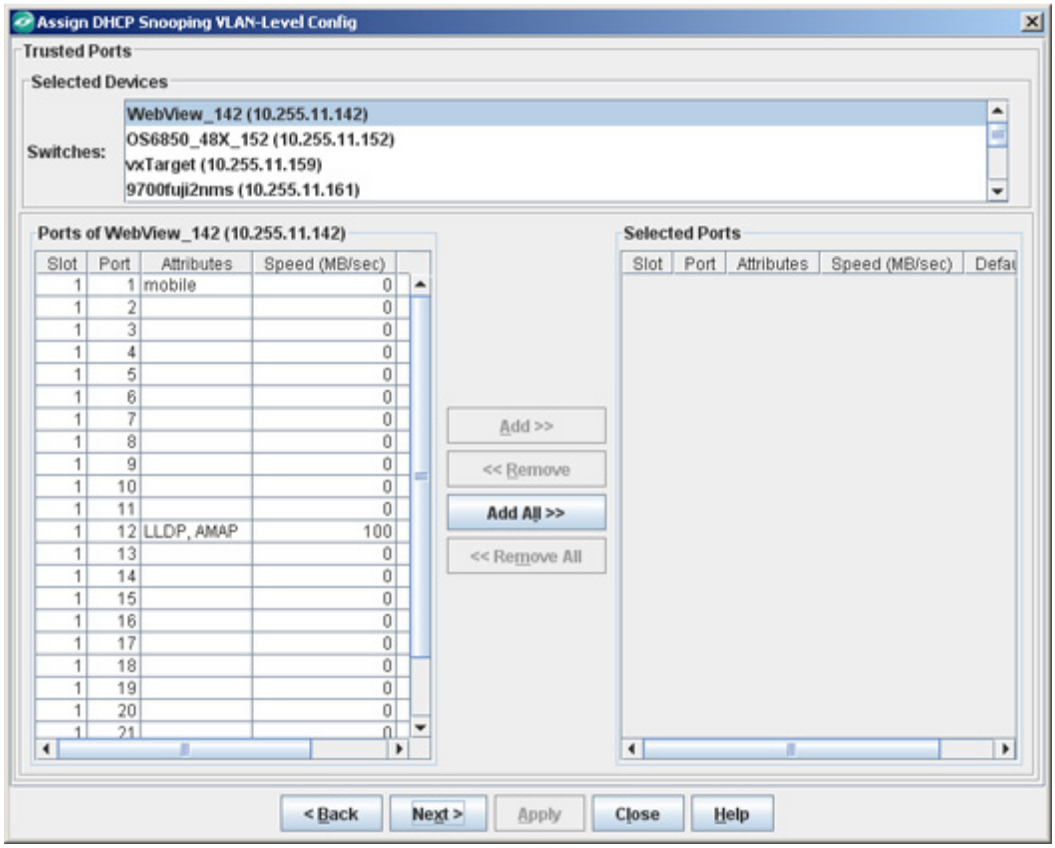
3. Click the **Next** button. Page 2 of the wizard appears.

Assign DHCP Snooping VLAN-Level Configuration Wizard (Page 2)



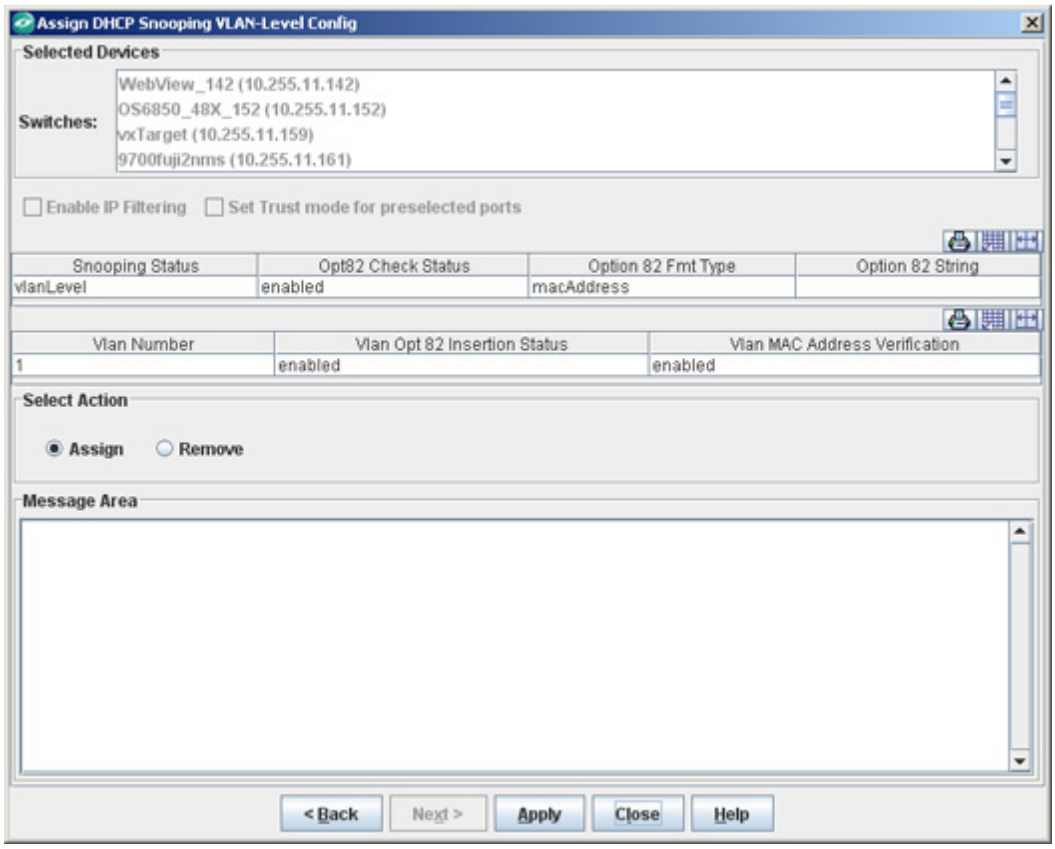
4. Select the switch(es) to which you want to add DHCP the VLAN-Level Snooping/Option 82 configuration and use the **Add** button to move the devices to the "Devices to be added" area. (Use the **Add** or **Remove** buttons to add or delete switches.) When you are done selecting devices, click the **Next** button. Page 3 of the Wizard appears.

Assign DHCP Snooping VLAN-Level Configuration Wizard (Page 3)



5. Select a switch in the "Selected Devices" area. By default, all active ports on the switch will appear in the Ports" area on the left. If you have used the Port Filter feature, ports that match your selected type will appear in the "Selected Ports" area. Use the **Add**/**Remove** buttons to select the ports to which you want to apply the policy(ies). Repeat this step for each switch in the "Selected Devices" area. When you have selected the ports for each switch, click **Next**. Page 4 of the Wizard appears.

Assign DHCP Snooping VLAN-Level Configuration Wizard (Page 4)



6. Click the **Apply** button to apply the configuration to the selected switches/ports. The Message Area shows the progress of the operation.

Editing VLAN-Level DHCP Snooping

To edit a DHCP Snooping VLAN, select the VLAN in the "DHCP Snooping VLANs" table, then click the **Edit VLAN** button. The "Edit DHCP Snooping VLANs" widow appears.

Editing a DHCP Snooping VLAN

Edit the VLAN, then click **OK**. Click the **Apply** button to write the edit the server, then click the **Assign** button to assign the edit to the VLAN(s).

Deleting VLAN-Level DHCP Snooping

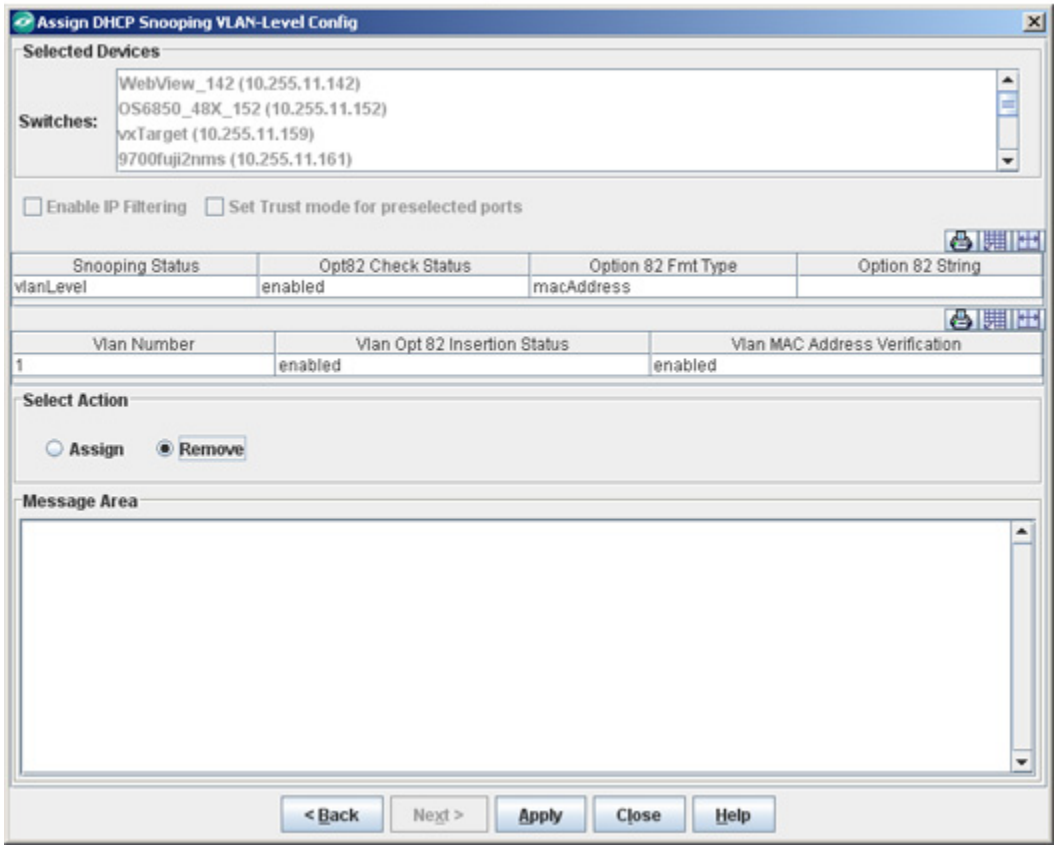
To delete a DHCP VLAN profile from the server, select the VLAN in the "DHCP Snooping VLANs" table, click the **Delete VLAN** button then click the **Apply** button. The DHCP profile will be removed from the server.

> **Note:** Removing a DHCP-Snooping VLAN on this screen only removes it from the profile to be sent to the switch(es). This screen is used to enable/disable VLAN-Level DHCP Snooping and to create/delete DHCP Snooping VLANs from a profile to be assigned. Use the View Tab to delete a DHCP Snooping VLAN from a switch or the Assign DHCP Snooping VLAN-Level Configuration" Wizard to delete a DHCP Snooping VLAN from multiple switches.

Removing a VLAN-Level DHCP Snooping Configuration

As noted above, deleting a DHCP Snooping VLAN from the "DHCP Snooping VLANs" Table does not remove the configuration from any switch(es) to which it has been assigned. To remove VLAN-Level DHCP Snooping configuration from a switch, select the DHCP Snooping VLAN in the "DHCP Snooping VLANs" Table, then click the **Assign** button. Use the "Assign DHCP Snooping VLAN-Level Configuration" Wizard to select the switches/ports that you want to configure. On the final page of the wizard, select the **Remove** radio button in the "Select Action" area then click the **Apply** button.

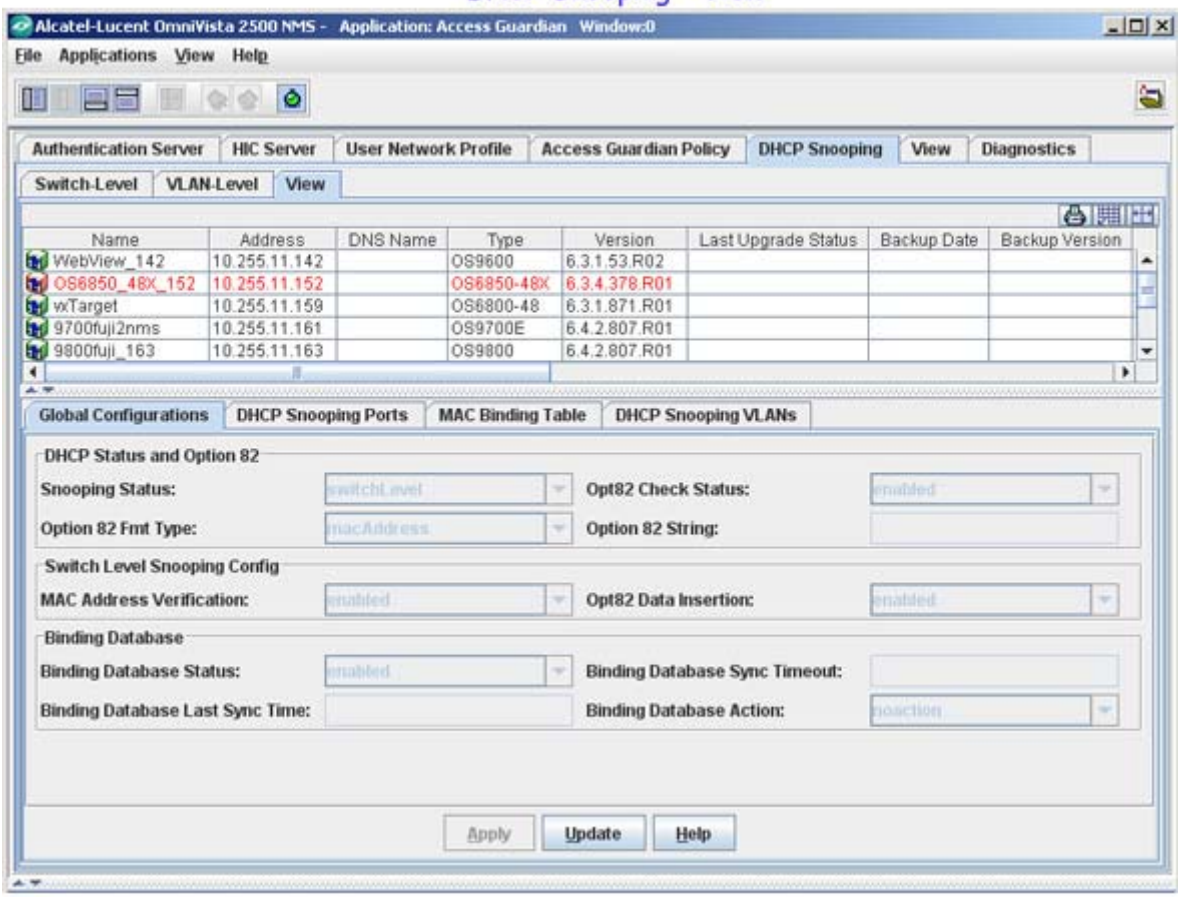
Removing DHCP Snooping VLAN-Level Configuration



DHCP Snooping Tab - View

The **DHCP Snooping - View** Tab is used to view/update DHCP Global Configuration parameters and view DHCP Snooping Port trust configurations and statistics, MAC Binding, and DHCP Snooping VLAN level configurations for switches on the network. All of the switches for which DHCP has been enabled are displayed in the top pane. To view/configure a specific switch, select the switch in the table. The DHCP configuration information for that switch will be displayed under each of the tabs in the bottom pane.

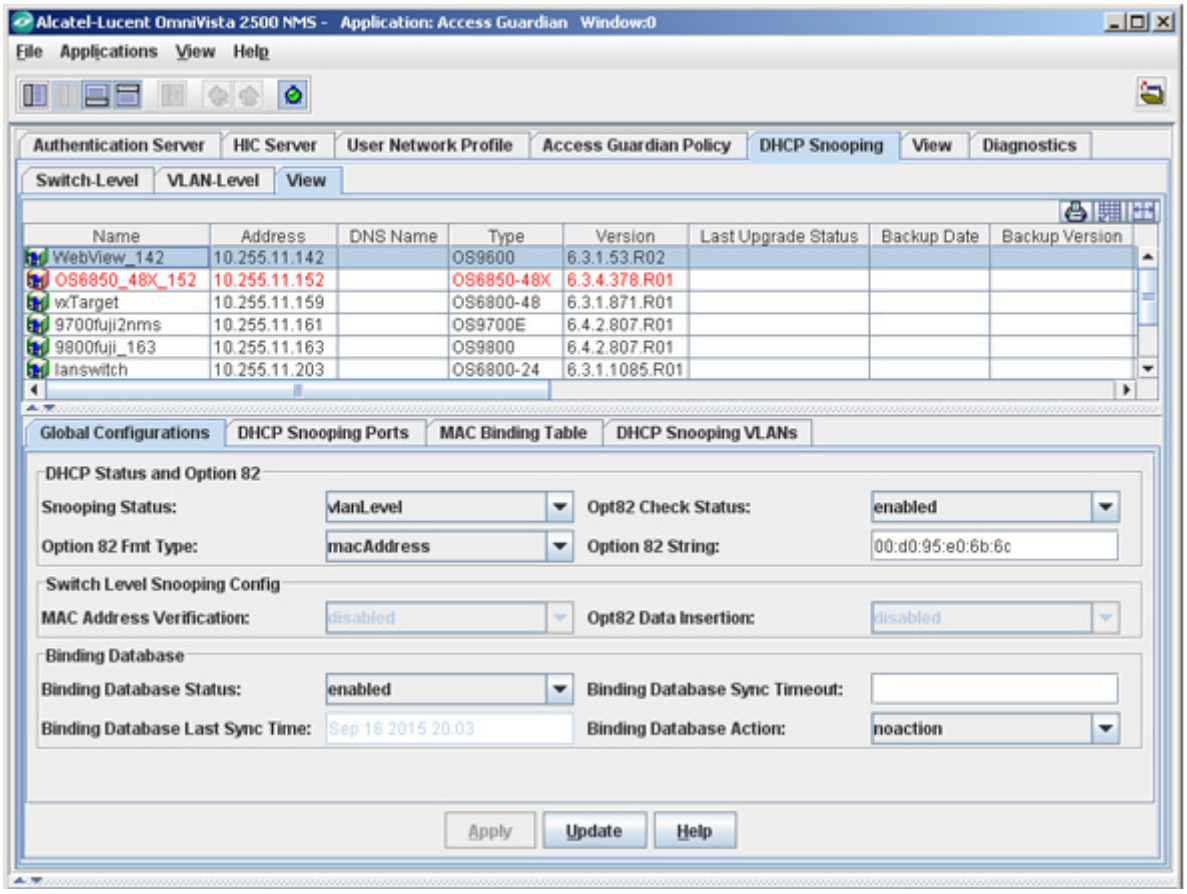
DHCP Snooping - View



Global Configurations

The Global Configuration tab is used to view and change DHCP Snooping parameters on a single switch. To check/update parameters, select the switch in the switch table, select the configuration(s) from the drop-down menus then click the **Apply** button. To update DHCP configurations for more than one switch, click on the Switch Level tab or the VLAN Level tab.

DHCP Snooping - Global Configurations



DHCP Snooping Global Configuration

The information in the DHCP Global Configuration tab is defined below.

DHCP Status and Option 82

Snooping Status

Is used to enable/disable DHCP Snooping.

- **switchLevel -** Enables Switch Level DHCP Snooping for the selected device
- **vlanLevel -** Enables VLAN Level DHCP Snooping for the selected device.
- **disabled -** Disables DHCP Snooping for the selected device.

Opt 82 Check Status

Enables/Disables the Option 82 check. "Enabled" means that switch will check for the Option 82 date field in incoming packets. If the packet contains the Option 82 field and is received on an untrusted port, the packet is dropped "Disabled" means the switch will not check for Option 82 field. The packets will be processed whether or not the Option 82 data field is present.

Option 82 Fmt Type

The Option 82 Format used. The Opt 82 Format is the type of data that is inserted into client-originated DHCP packets before the packets are forwarded to the DHCP server.

- **MAC Address -** The MAC address of the router interface from which the DHCP packet originated.
- **System Name -** The System Name
- **User Defined -** A user-defined text string up to 64 characters.

Option 82 String
If the Option 82 format Type is "User Defined", the text string appears here.

Switch Level Snooping Config
MAC Address Verification
Enables/Disables the MAC address option for Option 82 processing.

Option 82 Data Insertion
Enables/Disabled Option 82 date insertion..

Binding Database
Binding Database Status
Enables or disables the DHCP Snooping binding table functionality. By default, the binding table functionality is enabled when the DHCP Snooping feature is enabled for a switch or for a VLAN.

Binding Database Sync Timeout
The amount of time, in seconds, between each automatic save of the DHCP Snooping binding table contents maintained in memory to a file on the switch. This functionality preserves binding table contents across switch reboots. (Range = 180 to 600, Default = 300)

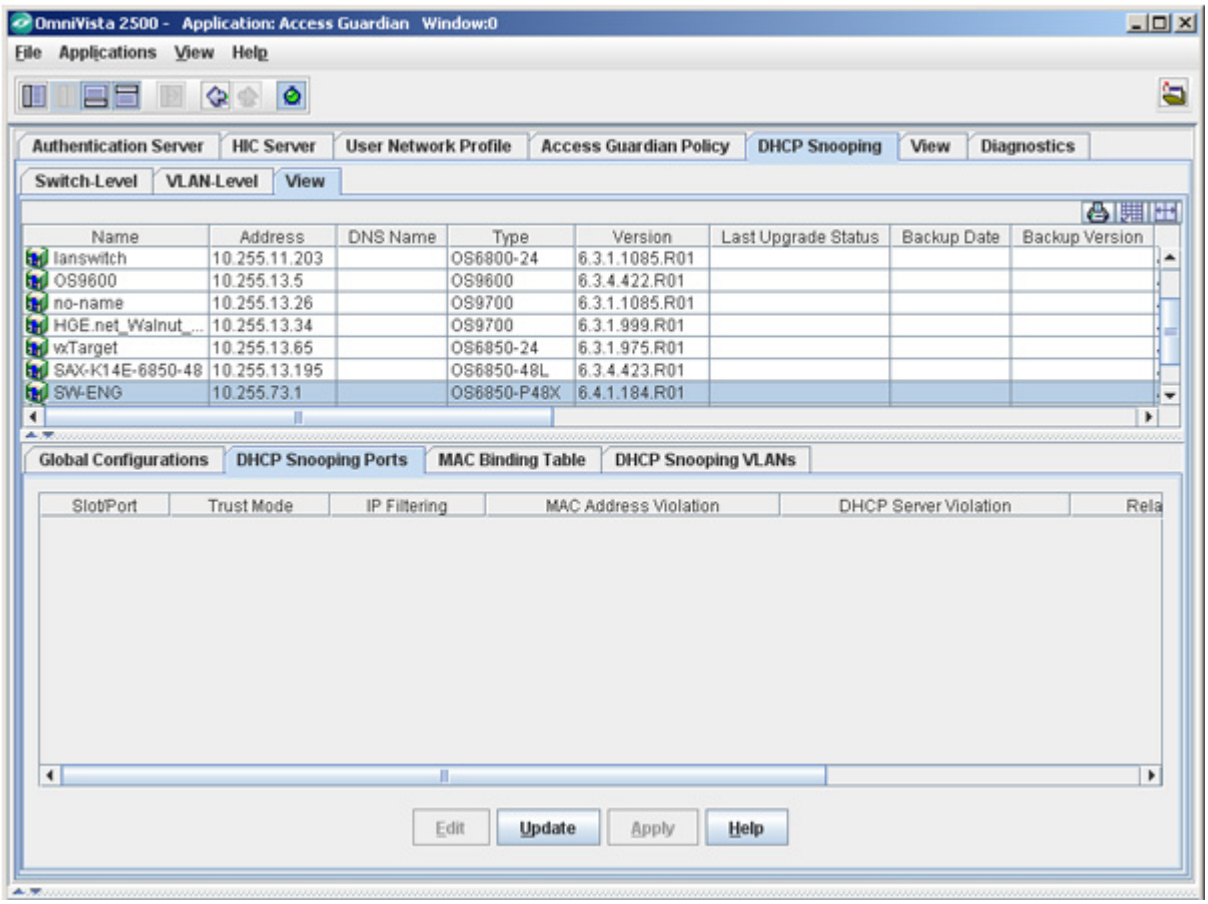
Binding Database Last Sync Time
The last time and day the DHCP snooping binding table was synchronized with the dhcpBinding.db file

Binding Database Action
Triggers a purge or renew action against the DHCP Snooping binding table. A purge action clears the contents of the table. A renew action populates the table with entries saved in the dhcpBinding.db file.

DHCP Snooping Ports

The DHCP Snooping Ports tab displays DHCP Snooping Ports configuration information for all ports on the selected switch. You can also edit a port's Trust Mode and IP Filtering configuration.

DHCP Snooping - View DHCP Snooping Ports



DHCP Snooping Port Configuration

The information in the DHCP Snooping Ports tab is defined below.

Slot/Port

The slot/port designation for the switch port.

Trust Mode

he DHCP Snooping trust mode for the port (Blocked, Client-Only, or Trusted)

IP Filtering

Indicates whether or not IP source filtering is enabled for the port (Enabled or Disabled).

MAC Address Violation

The number of DHCP packets dropped due to a mismatch between the packet source MAC address and the client hardware address contained within the packet.

DHCP Server Violation

The number of DHCP server packets dropped because they originated from outside the network or firewall.

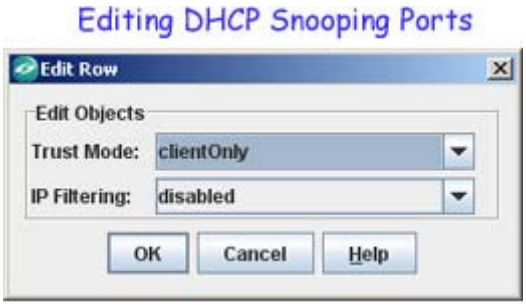
Relay Agent Violation

The number of DHCP packets dropped because the packet included a relay agent IP address that was not 0.0.0.0.

Port Binding Violation
The number of DHCP packets dropped due to a mismatch between the packets received and the MAC Binding Table information.

Editing DCHP Snooping Ports

To edit DHCP Snooping Ports, complete the fields as described below, click **OK**, then click on the **Apply** button.



Field Definitions

Trust Mode
Configures the DHCP Snooping trust mode for the port. The trust mode determines if the port will accept all DHCP traffic, block all DHCP traffic, or accept only client DHCP traffic.

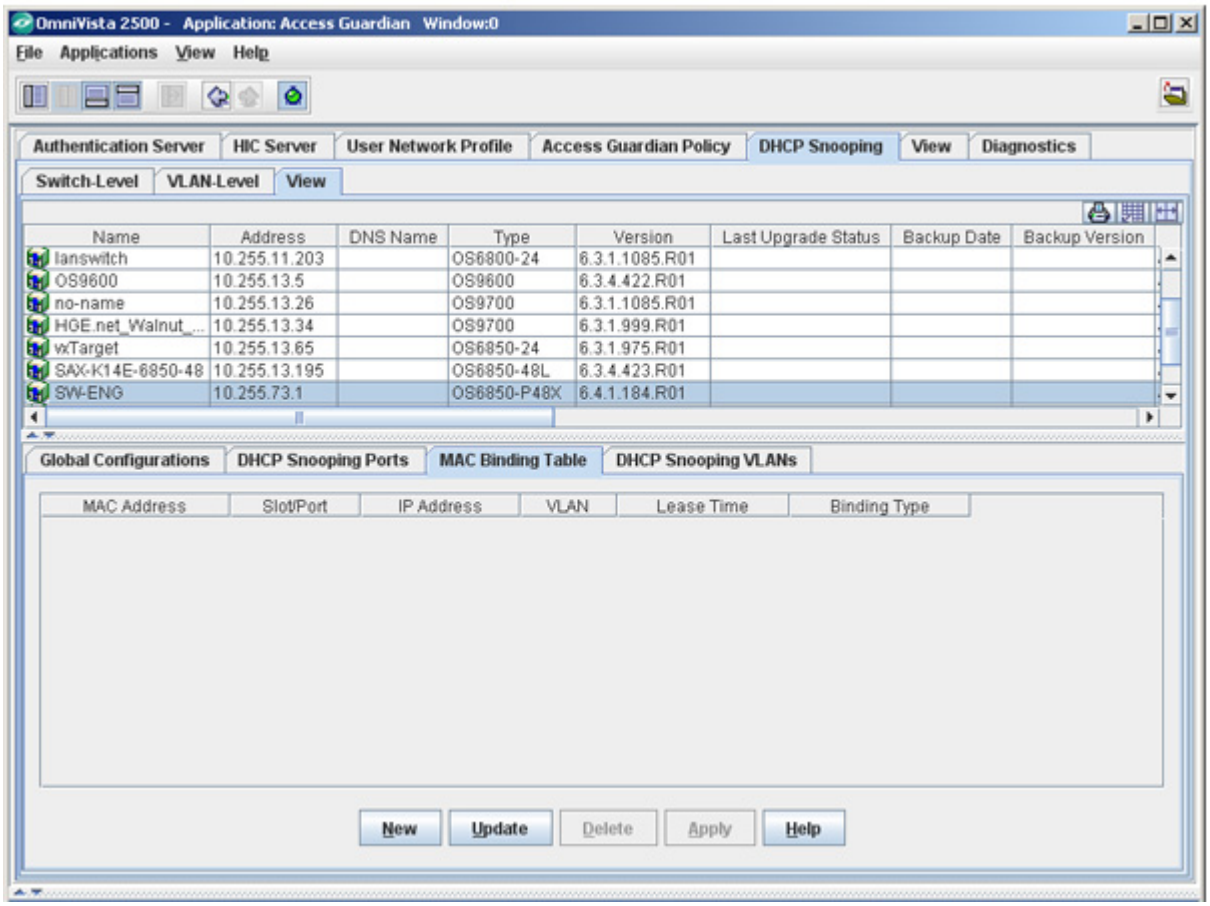
- **Blocked -** Blocks all DHCP traffic on the port.
- **Client Only -** Allows only DHCP client traffic on the port.
- **Trusted -** Allows all DHCP traffic on the port. The port behaves as if DHCP Snooping was not enabled.

IP Filtering
Configures the IP source filtering status for the port. When this function is enabled, traffic on the port is restricted to packets received on the port that contain the client MAC address and IP address. All other packets are dropped.

MAC Binding Table

The MAC Binding Table tab displays DHCP Snooping MAC Binding Table information for the selected switch. Normally, MAC bindings are learned through DHCP messages; but you can also add a static entry to the table by clicking on the **New** button, or delete and entry by selecting the entry and clicking on the **Delete** button, then clicking on the **Apply** button. Note that MAC Binding Table shows entries only if Binding Database Status is enabled.

DHCP Snooping - View MAC Binding Table



MAC Binding Table Configuration

The information in the MAC Binding Table tab is defined below.

MAC Address

The MAC address of the client.

Slot/Port

The slot/port designation for the switch port that received the DHCP request

IP Address

The IP address offered by the DHCP server.

VLAN

The VLAN to which the client belongs.

Lease Time

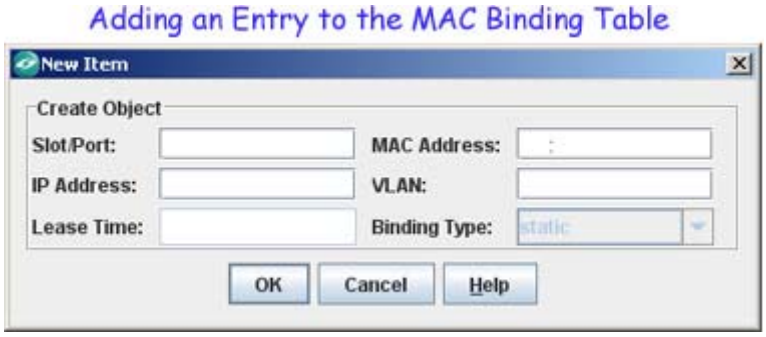
The IP address lease time assigned by the DHCP server. A value of 0 indicates a static entry.

Binding Type

Indicates whether the binding table entry is dynamic or static.

Adding an Entry to the MAC Binding Table

To add an entry to the MAC Binding Table, complete the fields as described below, click **OK**, then click on the **Apply** button.



Field Definitions

Slot/Port
The slot/port designation for the switch port that receives the DHCP request.

MAC Address
The MAC address of the client.

IP Address
The IP address offered by the DHCP server.

VLAN
The VLAN to which the client belongs.

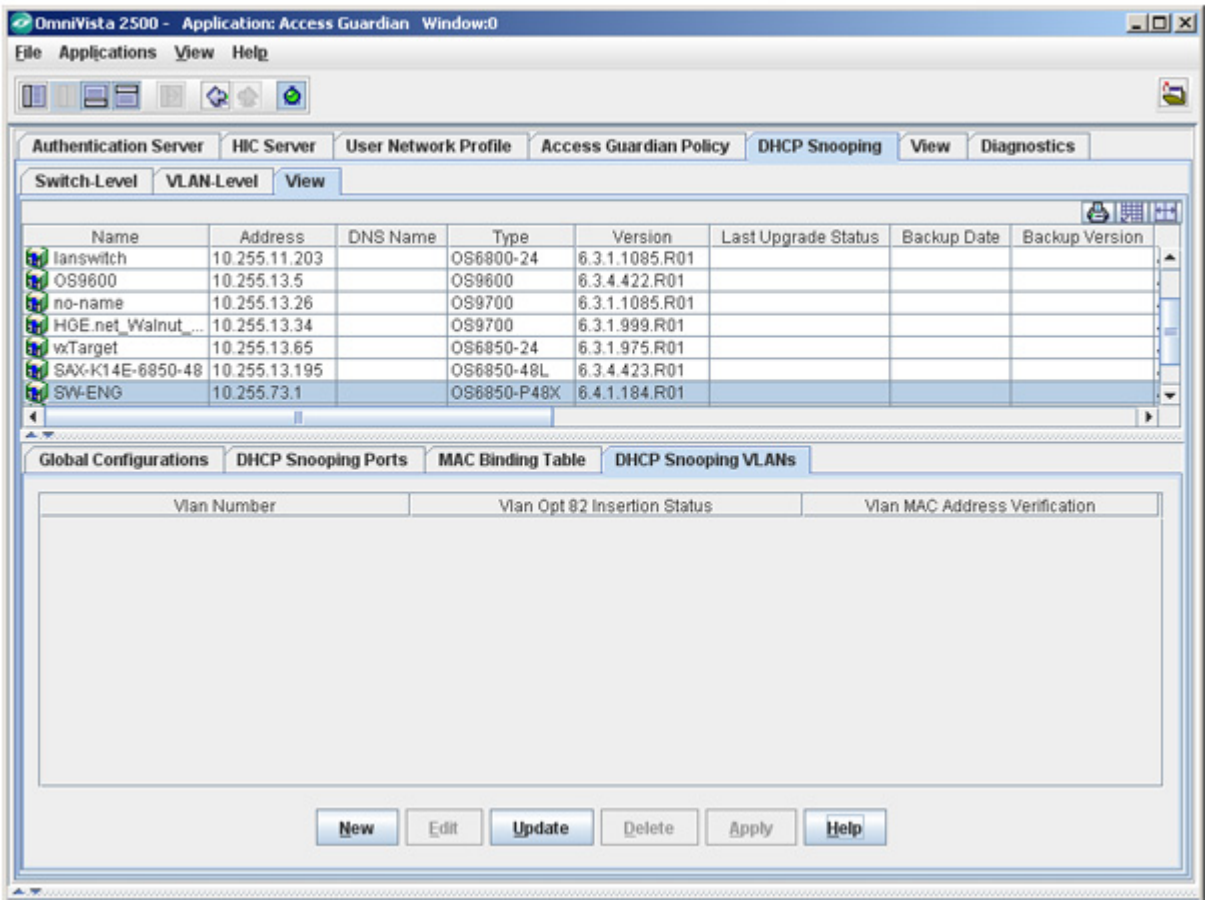
Lease Time
The IP address lease time assigned by the DHCP server. A value of 0 indicates a static entry.

Binding Type
Indicates whether the binding table entry is dynamic or static.

DHCP Snooping VLANs

The DHCP Snooping VLANs tab displays DHCP Snooping VLAN information for all VLANs on the selected switch. You can also create a DHCP Snooping VLAN by clicking on the **New** button, edit a DHCP Snooping VLAN by selecting a VLAN in the table and clicking on the **Edit** button then clicking on the **Apply** button, or delete a VLAN by selecting a VLAN in the table, clicking on the **Delete** button then clicking on the **Apply** button.

DHCP Snooping - View DHCP Snooping VLANs



DHCP Snooping VLANs Configuration

The information in the DHCP Snooping VLANs tab is defined below.

VLAN Number

The DHCP Snooping VLAN.

VLAN MAC Address Verification

Indicates whether or not MAC address verification is enabled for the VLAN (Enabled/Disabled).

VLAN Opt 82 Insertion Status

Indicates whether or not Option-82 data insertion is enabled for the VLAN (Enabled/Disabled).

Creating a DHCP Snooping VLAN

To create a DHCP Snooping VLAN, complete the fields as described below, click **OK**, then click on the **Apply** button.

Add DHCP Snooping VLAN

Field Definitions

VLAN Number
The DHCP Snooping VLAN.

VLAN MAC Address Verification
Indicates whether or not MAC address verification is enabled for the VLAN (Enabled/Disabled).

VLAN Opt 82 Insertion Status
Indicates whether or not Option-82 data insertion is enabled for the VLAN (Enabled/Disabled).

Editing a DHCP Snooping VLAN

To edit a DHCP Snooping VLAN, complete the fields as described below, click **OK**, then click on the **Apply** button.

Edit DHCP Snooping VLAN

Field Definitions

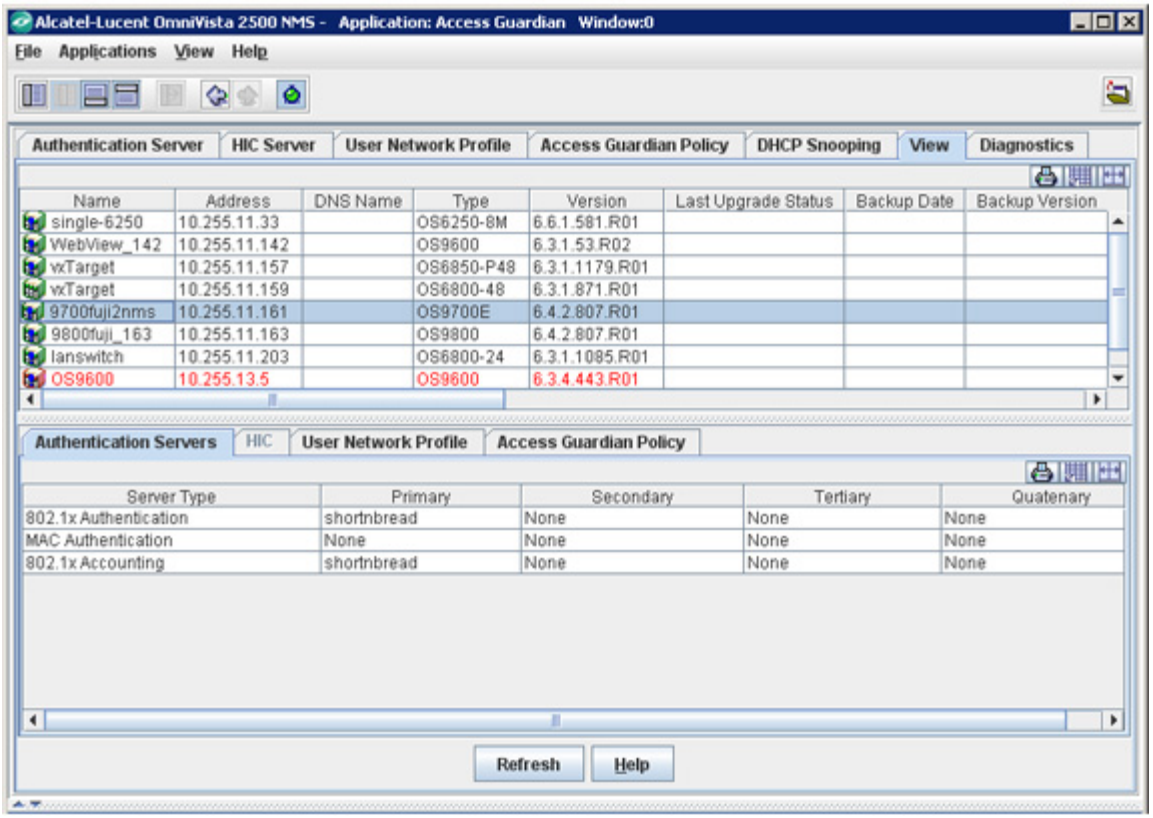
VLAN Opt 82 Insertion Status
Indicates whether or not Option-82 data insertion is enabled for the VLAN (Enabled/Disabled).

VLAN MAC Address Verification
Indicates whether or not MAC address verification is enabled for the VLAN (Enabled/Disabled).

View Tab

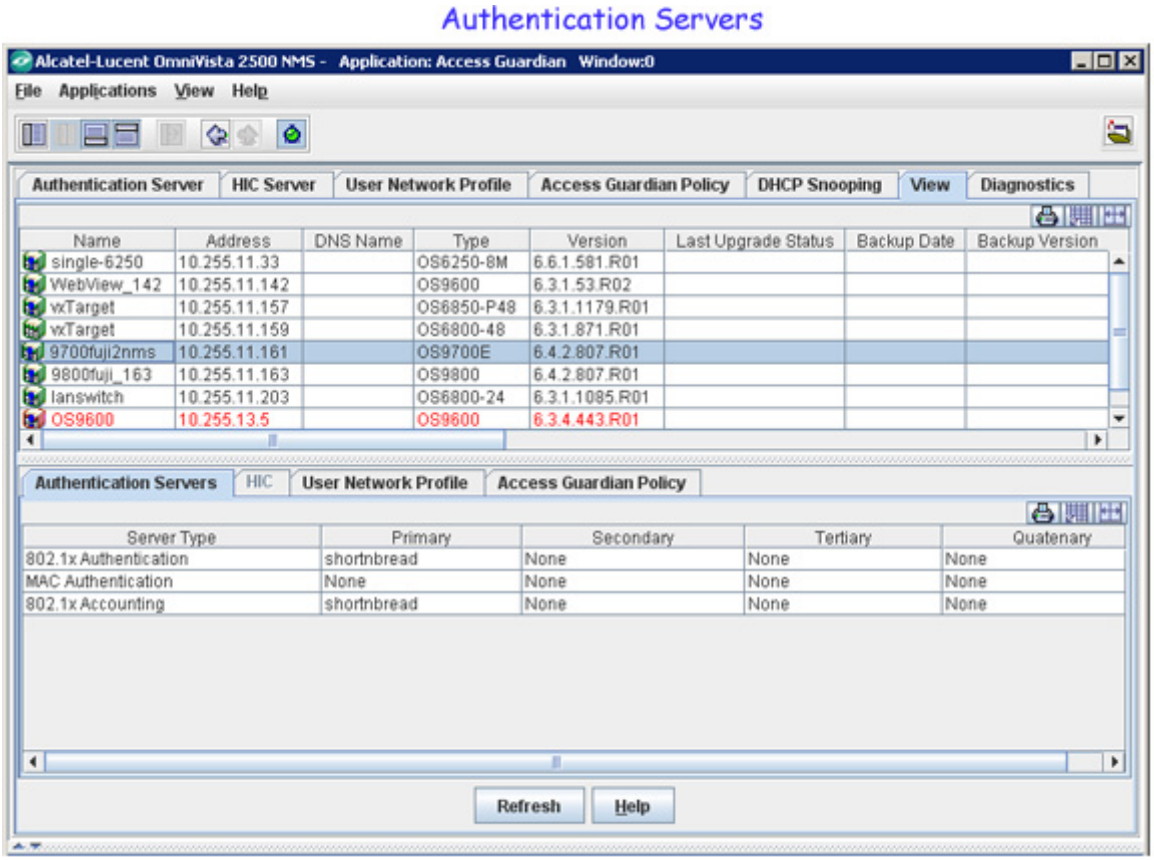
The **View** Tab is used to view specific policies assigned to switch ports. The tab displays information for all discovered devices that support Access Guardian, including: Authentication Servers, HIC Servers, User Network Profile, and Access Guardian Policy used for Access Guardian. To view information for a specific switch, select the switch in the table in the top pane. Click on the tabs in the bottom pane for specific information.

View Tab



Authentication Servers

The Authentication Servers tab displays information for Authentication Servers assigned to the selected switch.



Authentication Servers Information

Server Type
The type of Authentication Server (e.g., 802.1X Authentication, MAC Authentication).

Primary
The name or IP address of the Primary Authentication Server.

Secondary
The name or IP address of the Secondary Authentication Server.

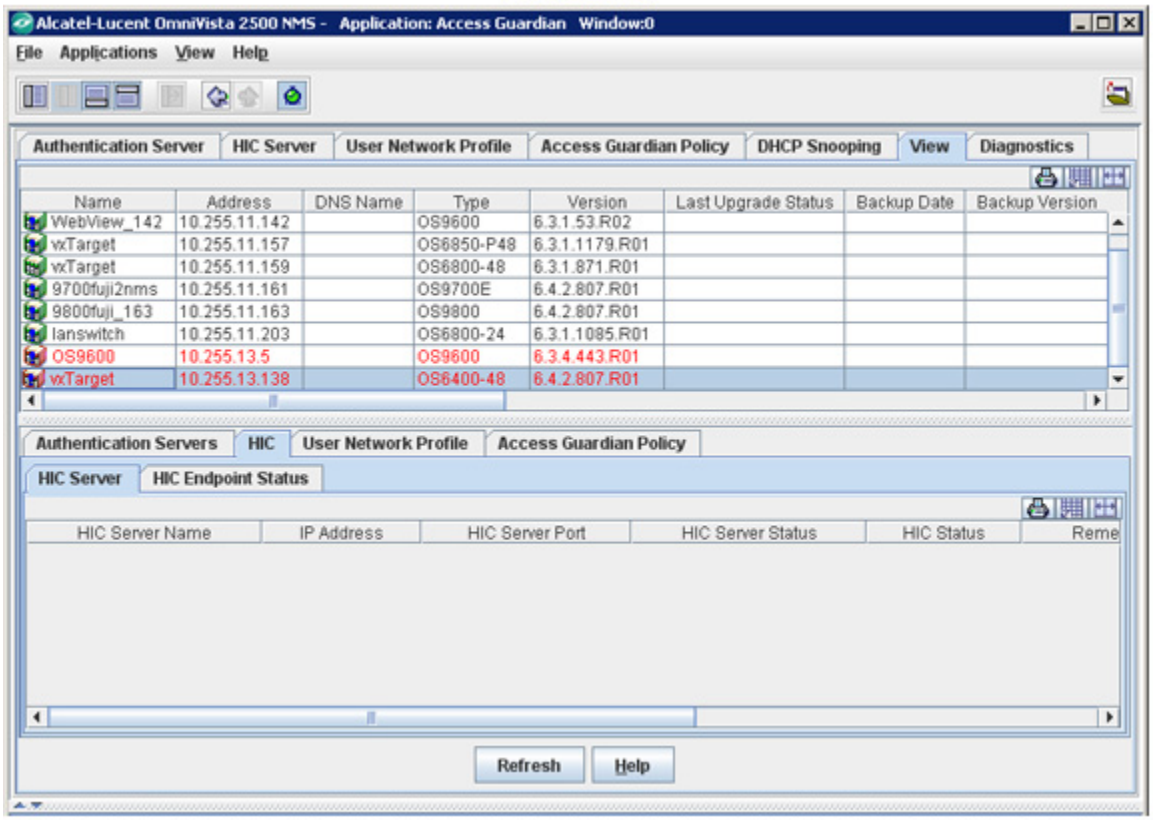
Tertiary
The name or IP address of the third Authentication Serve, if configured.

Quatenary
The name or IP address of the fourth Authentication Server, if configured.

HIC

The HIC tab displays Host Integrity Check (HIC) Server and HIC Endpoint Status information for the selected switch, if configured.

HIC Server



HIC Server Information

HIC Server

HIC Server Name
The user-configured name for the HIC Server.

IP Address
The HIC Server IP address.

HIC Server Port
The HIC Server Port.

HIC Server Status
The operational status of the HIC Server (Up/Down).

HIC Status
The administrative state of HIC on the switch (Enabled/Disabled).

Remediation URL
The URL of the Remediation Server.

HTTP Redirect Port
The proxy port number used when the web-based host is redirected to the HIC server.

Remediation Subnets
Subnets allowed access to the switch and host device as part of the HIC process.

HIC Endpoint Status

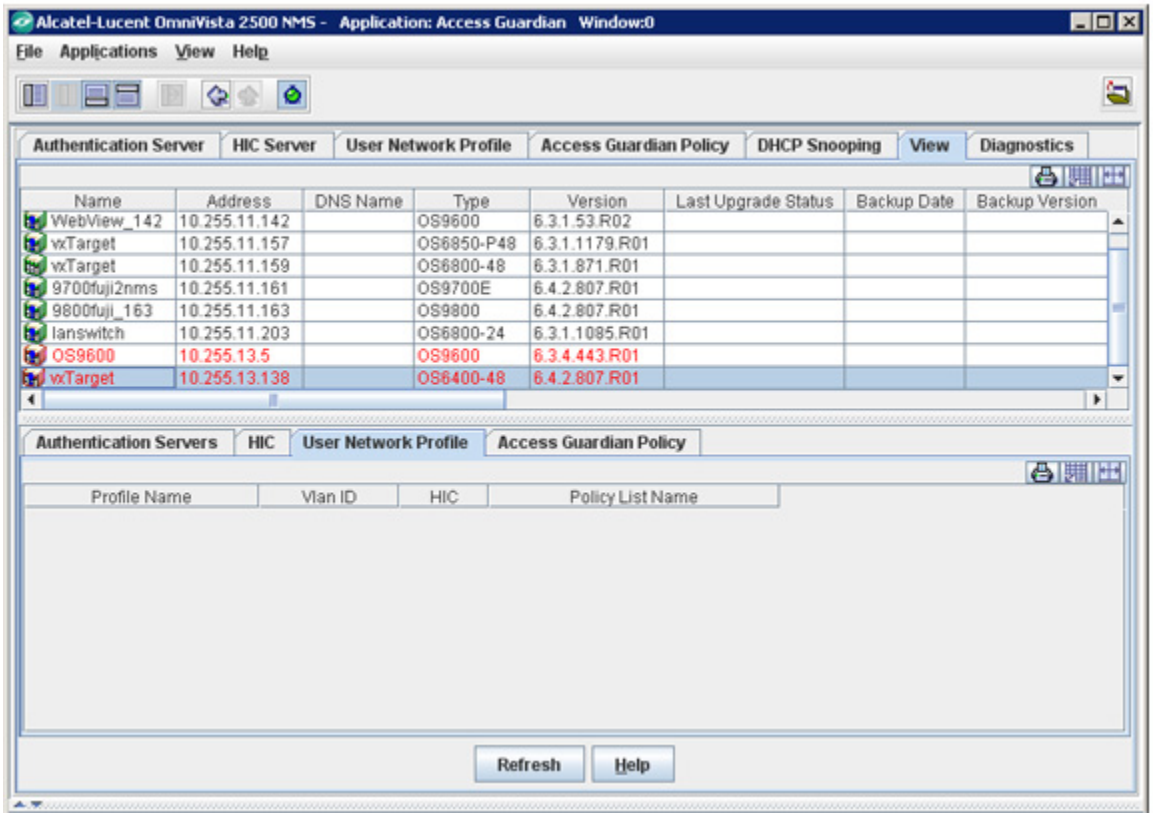
MAC Address
The HIC Endpoint device MAC address.

Status
The HIC Endpoint device status.

User Network Profile

The User Network Profile tab displays information for User Network Profiles configured for the switch.

User Network Profile



User Network Profile Information

Profile Name
Profile name for the UNP.

VLAN ID
VLAN to which all members of the UNP are assigned.

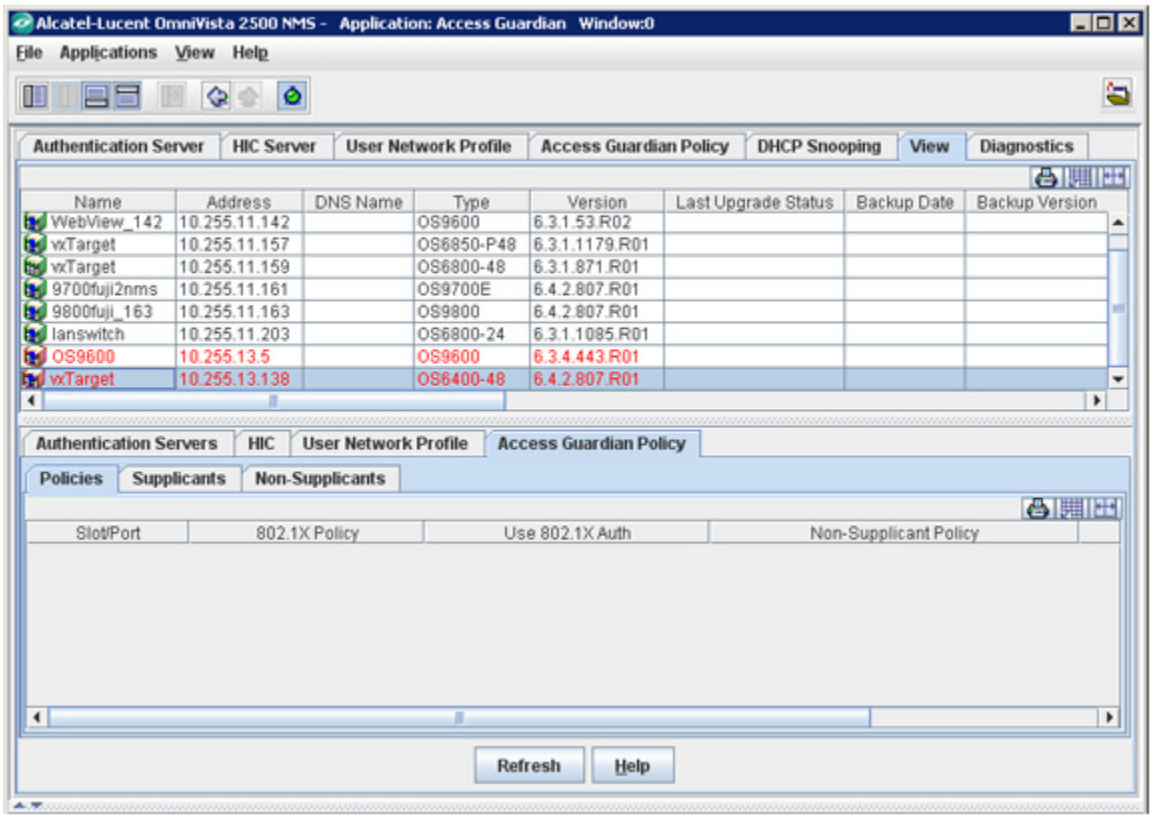
HIC
HIC Server assigned to the UNP

Policy List Name
Policy List associated with the UNP.

Access Guardian Policy

The Access Guardian Policy tab displays Access Guardian Policy information for the selected switch. The sub-tabs provide information on all Policies, Supplicant Policies, and Non-Supplicant Policies.

Access Guardian Policies



Access Guardian Policy Information

Policies

Slot/Port
The 802.1X slot/port that provides access to the device.

802.1x Policy
The 801.1x policy configured for the slot/port.

User 802.1X Auth
Indicates whether or not MAC Authentication is included in the policy.

Non-Supplicant Policy
The 801.1x non-supplicant policy configured for the slot/port.

Captive Portal Policy
The Captive Portal policy configured for the slot/port, if applicable.

Supplicants

Slot/Port
The 802.1X slot/port that provides access to the device.

MAC Address
The source MAC address of the device connected to the slot/port.

Port State
The administrative status of the 802.1X port.

Policy
The 802.1x device classification policy applied to the device.

User Name
The user name that is used for authentication.

VLAN Learned
The VLAN in which the source MAC address of the non-802.1x device was learned.

Non-Supplicants

Slot/Port
The 802.1X slot/port that provides access to the device.

MAC Address
The source MAC address of the device connected to the slot/port.

Authentication State
The administrative status of the 802.1X port.

Classification Policy
The 802.1x device classification policy applied to the device.

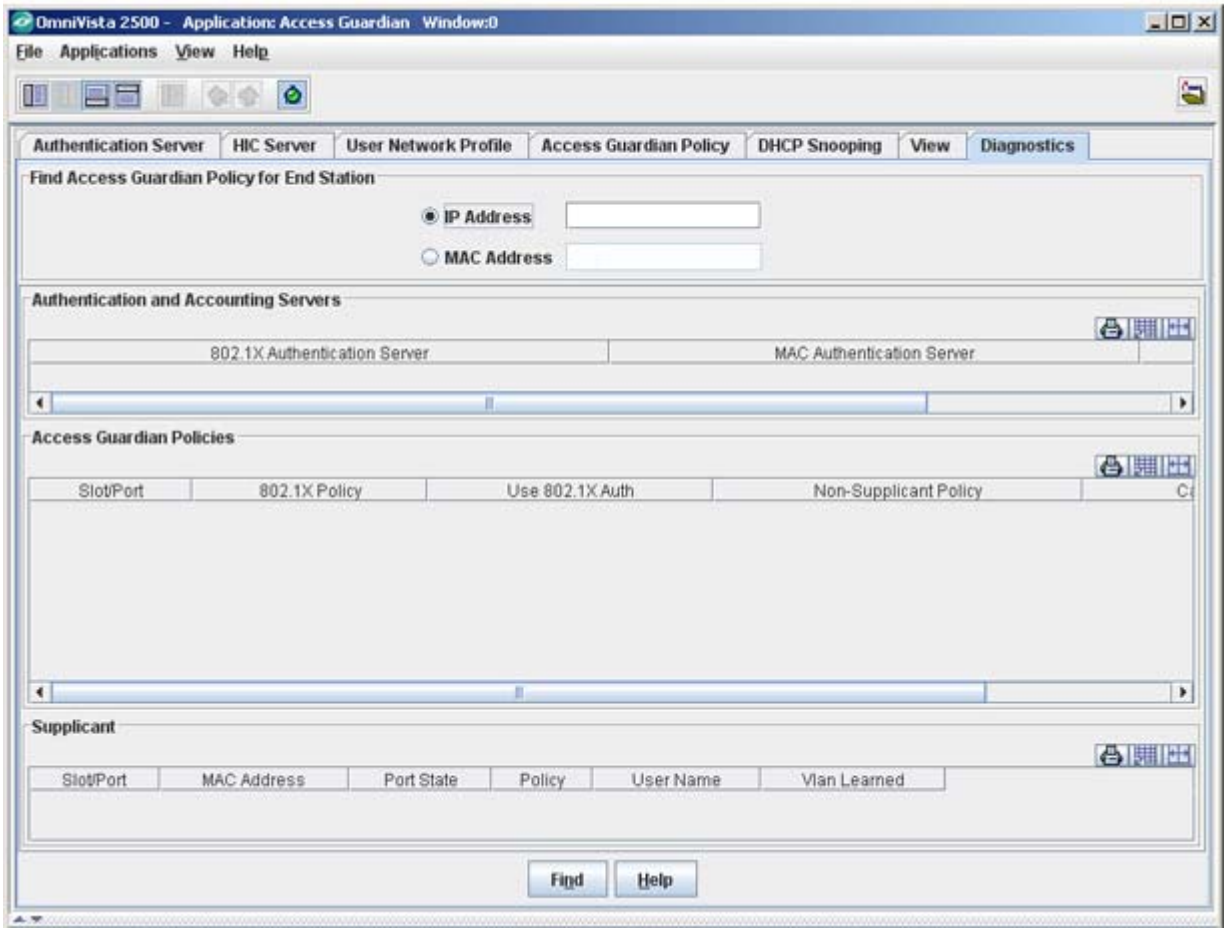
VLAN Learned
The VLAN in which the source MAC address of the non-802.1x device was learned.

Diagnostics Tab

The **Diagnostics** Tab can be used by a Network Administrator to diagnose end user problems by locating the user's end station and displaying any Access Guardian Policies for the End Station. If, for example, a user cannot access certain resources, the Network Administrator can enter the user's IP or MAC address to determine the switch and port of the End Station to which the user is attached. The Diagnostic Tab also displays the 802.1x Authentication server, MAC Authentication Server and 802.1x Accounting Server for the switch.

As shown below, once the user's station is located, the Authentication Servers as well as any Supplicant and Non-Supplicant Policies for the user's end station port are displayed.

Diagnostics Tab



You can mouse over a policy in the Access Guardian Policies table for specific policy information. In addition, the following Supplicant and Non-Supplicant information is displayed

Non-Supplicant Policy:

- Authentication State
- Classification
- VLAN learned

Supplicant Policy:

- Port State
- Policy
- User's Name
- VLAN learned.