# Getting Started with SecureView ACL

The SecureView ACL application enables you to create ACL policies that specify Access Control List provided for network traffic. Policy Rules are stored on an LDAP (Lightweight Directory Access Protocol) repository that is automatically installed with the SecureView ACL application and resides on the same device as the OmniVista server. Devices in the network are notified when new or modified Policy Rules are available on the LDAP repository via an SNMP interface. Software resident in the switch is responsible for retrieving the Policy Rules from the LDAP repository, interpreting the Policy Rules, and enforcing them on the switch.

When you first open the ACL application, the **One Touch** and **Expert** tabs are displayed. Any existing devices that are configured for the **One Touch** mode are displayed.

SecureView ACL provides easy, simplified "One Touch" modes that enable you to create ACL policies with minimal effort and maximum simplicity. If you use the **One Touch** mode to create ACL policies for your network, there is no need to understand the underlying ACL definitions and constructs. The **One Touch** mode enable you to create ACL policies without bothering with the normal complexity associated with ACL.

The SecureView ACL application also provides an "Expert" mode that enables you to create more complex ACL policies using standard ACL constructs. ACL policies created in the **Expert** mode can be applied to all the devices in the list of All Discovered Devices or to selected devices.

## One Touch Mode Overview

The **One Touch** tab enables you to easily create ACL policies for all traffic originating from, and/or flowing to, specific Network Groups. This tab displays the existing One Touch ACL policies. It also enables you to create, edit, and delete ACL policies using pre-defined conditions and actions.

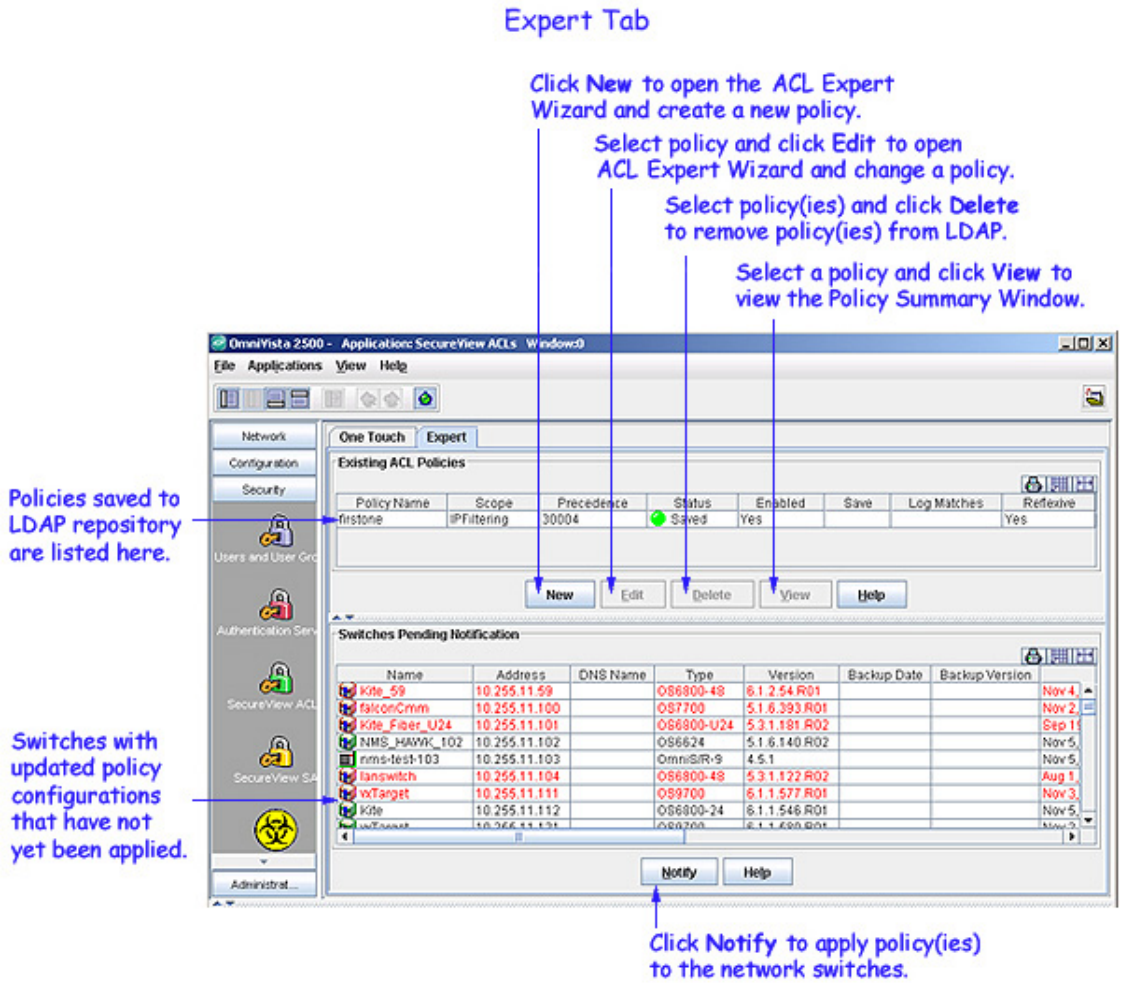
One Touch Tab

To learn more about the **One Touch** tab, See “One Touch Tab” on page 2.

## Expert Mode Overview

In the **Expert** tab, conditions and actions are not created automatically. The **Expert** tab enables you to create conditions and actions manually, by specifying each individual parameter. In this mode, you can create conditions that specify L1 Interfaces, L2 MACs, L2 VLANs, L3 IPs, L4 Services, and Validity Period values. See “Creating a Policy Condition” on page 9for more information on creating conditions in the **Expert** tab.

The **Expert** tab also enables you to define action parameters that specify the treatment traffic will receive as it flows. This includes the accessibility the traffic will have, the minimum and maximum output rates, and the values to which specified bits in the frame headers will be set upon egress from the switch. See “Creating a Policy Action” on page 10 for more information on creating actions in the **Expert** tab.




## One Touch Tab

The **One Touch** tab, shown below, enables you to configure ACL policies easily. This tab displays the policy status, assigned ACL IP network group, and the accessibility details of existing One Touch ACL policies. Using the One Touch tab, you can do the following:

- Create One Touch Policies
- Edit One Touch Policies
- Delete One Touch Policies

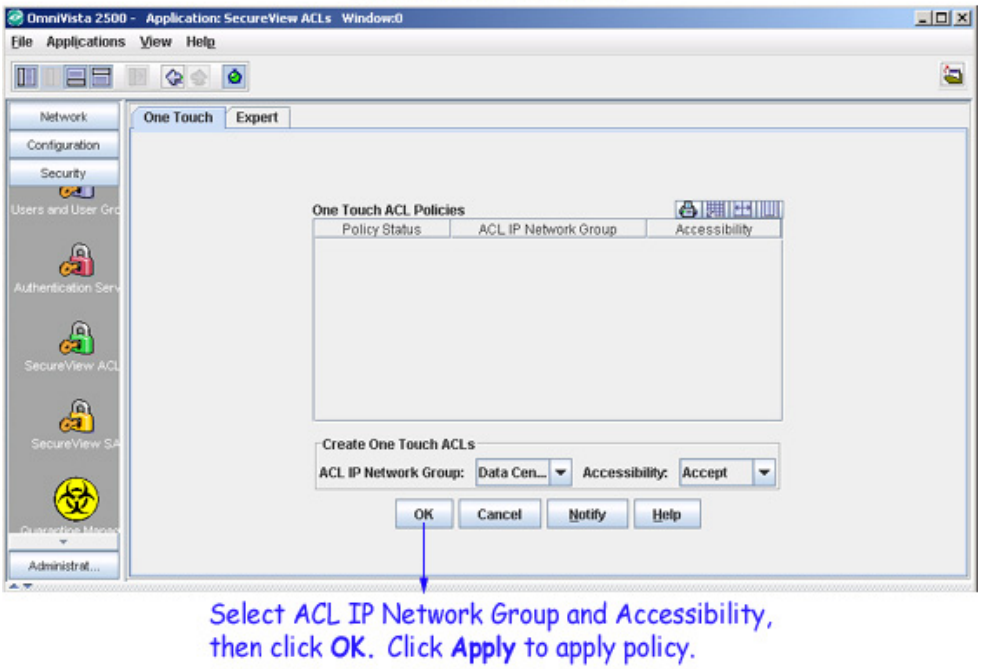
One Touch Tab


## Creating One Touch Policies

Follow the steps below to create One Touch policies.

**1.** Click the **New** button. The **Create One Touch ACLs** panel appears (shown below).

One Touch ACL Policies




Select ACL IP Network Group and Accessibility, then click **OK**. Click **Apply** to apply policy.

**2.** Select the group from the **ACL IP Network Group** drop-down list.

**3.** Select the accessibility from the **Accessibility** drop-down list (Accept or Drop).

**4.** Click the **OK** button. The created policy appears in the One Touch ACL Policies table as "Unsaved".

**5.** Click the **Save** button to apply the policy to the LDAP repository. Repeat the same steps to create additional policies.

**6.** Click the **Notify** button to notify the network switch(es) assigned to the created One Touch ACL policy to re-cache their policy information.

Clicking the **Notify** button causes the selected switches in the list to flush their policy tables and reload policies from the LDAP repository, which is very expensive in terms of switch resources and time. If any ACL Expert mode policy has already been defined, the switch(es) to which the policy was assigned will also re-cache its policy tables. It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime.

**Note**: If you click the **Notify** button without selecting any policy in the list, all policy information will be re-cached.

## Editing One Touch Policies

Follow the steps below to edit One Touch policies.

**1.** Select the desired policy from the **One Touch ACL Policies** table.

**2.** Click the **Edit** button. The **Edit One Touch ACLs** panel appears.

**3.** Make the necessary change in the **Accessibility** drop-down list.

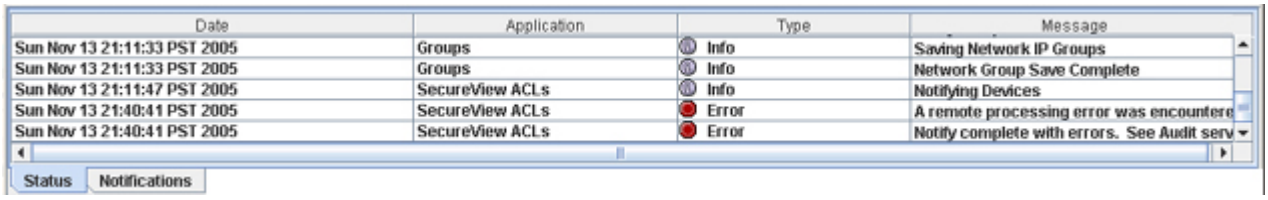
**Note**: An ACL IP network group name cannot be changed. If you want to change the group name, you have to delete and recreate the group.

**4.** After making the changes, click the **OK** button. The edited policy appears in the **One Touch ACL Policies** table as "Unsaved".

**5.** Click the **Save** button to apply the policy to the LDAP repository. Repeat the same steps to create additional policies.

## Verifying the Notify Operation

When the information entered in the One Touch tab is successfully applied to the LDAP repository, a "One Touch ACL Policies Save Complete" message is displayed. The success or failure of the LDAP "Save" operation is reported in the Status panel, as shown below.



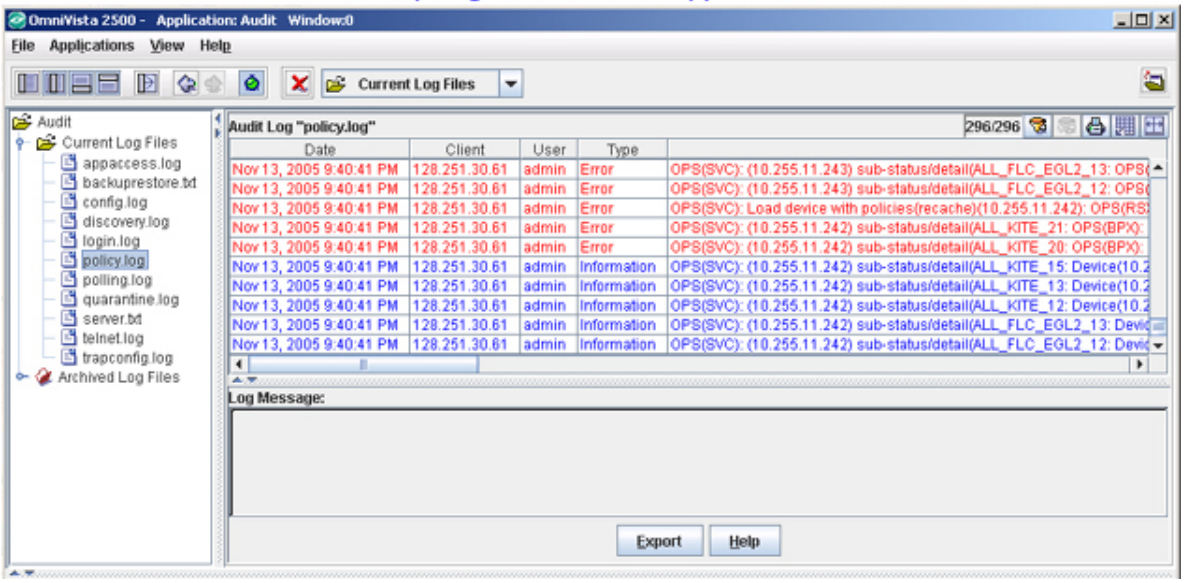

When the **Notify** button is clicked, an SNMP message is sent to selected switch(es) in the list, informing them that the information in the LDAP repository has changed and commanding them

to update their cached policies with the current information from the LDAP repository. The success or failure of the "Notify" operation is reported in the Status panel.

In addition to the Status panel, the success or failure of the policy re-cache operation for each switch is reported in the policy.log file with an indication of any error that may have occurred (shown below). Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Be sure to check the policy.log file for the re-cache status of the "Notify" operation.

Note that any errors that occur will also be reported in the file server.txt, which can be viewed from the Audit application.

Policy Log in the Audit Application




## Example of a One Touch ACL Policy Creation

Let's say we have selected **Data centre switches** as the network group and **Accept** as the accessibility option in the **Create One Touch ACLs** panel.

When saved, the following policies are created and written to the LDAP repository:

**OneTouchAR$SData Center Switches**
Condition specifies traffic originating from source IP Network group 'Data centre switches'
Action specifies accept as the disposition for this traffic

**OneTouchAR$DData Center Switches**
Condition specifies traffic transmitted to destination IP Network group 'Data centre switches'
Action specifies accept as the disposition for this traffic

Please note that the names beginning with "OneTouchAR" are the names used for the One Touch ACL policies in the LDAP repository. Within the SecureView ACL application, all One Touch ACL policies are referred to by the generic composite name OneTouchAR, no matter how many individual One Touch ACL policies have been written to the LDAP repository. One Touch ACL rules that have been created automatically by SecureView can be viewed in the Expert mode tab.

## Deleting One Touch Policies

Follow the steps below to delete One Touch Policies.

**1.** Select the desired policy from the **One Touch ACL Policies** table, and then click the **Delete** button. The policy status changes to "Unsaved Delete".

**2.** Click the **Save** button to apply the changes to the LDAP respostory.

When you click the **Save** button:

- All One Touch ACL policies for the ACL IP network groups you selected are removed from the LDAP repository.
- All One Touch ACL policies for the ACL IP network groups you selected are removed from switch attributes in the LDAP "role" objects.
- The network groups are removed from the **One Touch ACL Policies** table.
- A confirmation message is displayed when the LDAP repository has been successfully updated. The success of the LDAP "Save" operation is also reported in the policy.log file.

**3.** Repeat the same steps to delete additional policies.

## Icons in the One Touch ACL Policies Table

Network group icons in the **One Touch ACL Policies** table are color coded. The Policy Status column displays Yellow, Green, or Red LEDs depending on the status.

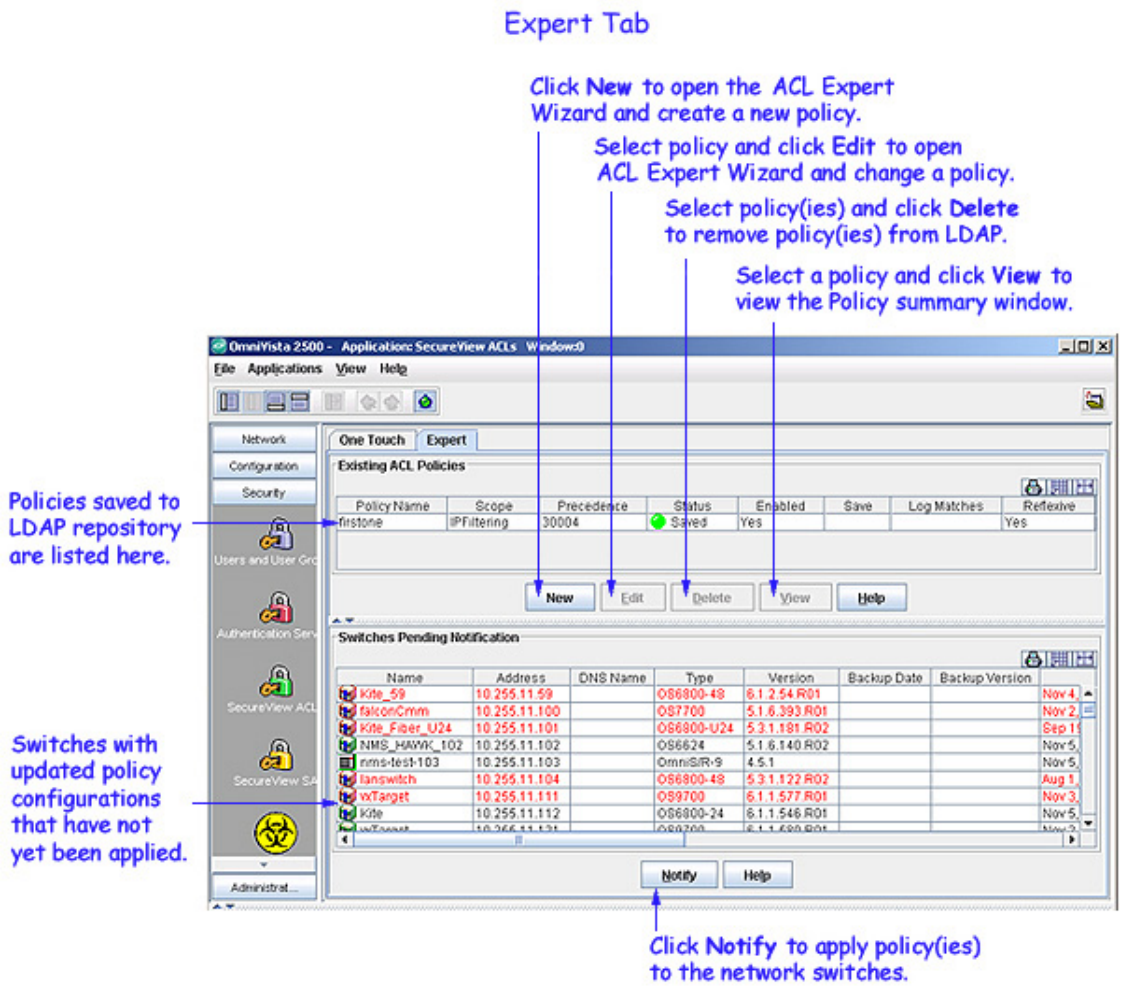
- A Yellow LED indicates that the policy is in a "pending" state and the changes have not been propagated to the LDAP repository.
- A Green LED indicates that the policy has been successfully written to the LDAP repository.
- A Red LED indicates that an error condition has made it impossible to write the One Touch ACL policy to the LDAP repository.

# Expert Tab

The **Expert** tab (shown below) is used to create, edit, delete, and view custom ACL policies. It also displays a list of switches that need to be notified to re-cache their policy configurations from the LDAP repository.

All current ACL polices are listed in the **Existing ACL Policies** table. To edit, delete, or view a policy, select the policy from the **Existing ACL Policies** table, and then click the corresponding button at the bottom of the Existing ACL Policies panel. To create a custom policy, click the **New** button to open the SecureView ACL Expert Wizard window. All switches pending notification are displayed in the **Switches Pending Notification** table.

> **Note**: One Touch policies cannot be modified or deleted in the Expert mode. To modify or delete One Touch policies, use the One Touch Tab.




## Editing a Custom ACL Policy

Follow the steps below to edit a custom ACL policy.

**1.** Select the desired custom ACL policy from the **Existing ACL Policies** table, and then click the **Edit** button. The **SecureView ACL Expert Wizard** window appears.

**2.** You can make the necessary changes in this wizard.

**Note**: A policy name cannot be changed. If you want to change the policy name, you have to delete and recreate the policy.

**3.** After making the necessary changes, click the **Finish** button. A dialog box displaying a confirmation message appears.

**4.** Click the **OK** button in the confirmation message dialog box to save the changes to the server.

## Deleting a Custom ACL Policy

Follow the steps below to delete a custom ACL policy.

**1.** Select the desired custom ACL policy from the **Existing ACL Policies** table, and then click the **Delete** button. A dialog box displaying a warning message is displayed.

**2.** Click the **Yes** button in the warning message dialog box to delete the policy. A dialog box displaying a confirmation message appears.

**3.** Click the **OK** button in the confirmation message dialog box to apply the changes to the server.

### Viewing a Custom ACL Policy

**1.** Select a desired policy from the **Existing ACL Policies** table, and then click the **View** button. The **Policy** window is displayed.

**2.** View the policy rules, policy conditions, policy actions, policy validity periods, and the switches assigned to that policy.

### Notifying Operation

The **Switches Pending Notification** table contains a list of switches whose assigned policies and/or LDAP role configurations has changed as a result of a policy configuration, but has not been notified to re-cache. Click the **Notify** button to notify these devices to re-cache their configurations..

> **Note**: The switch notification operation is expensive in terms of switch resources and will not take place until invoked by the user.

## Creating Policies in the Expert Mode

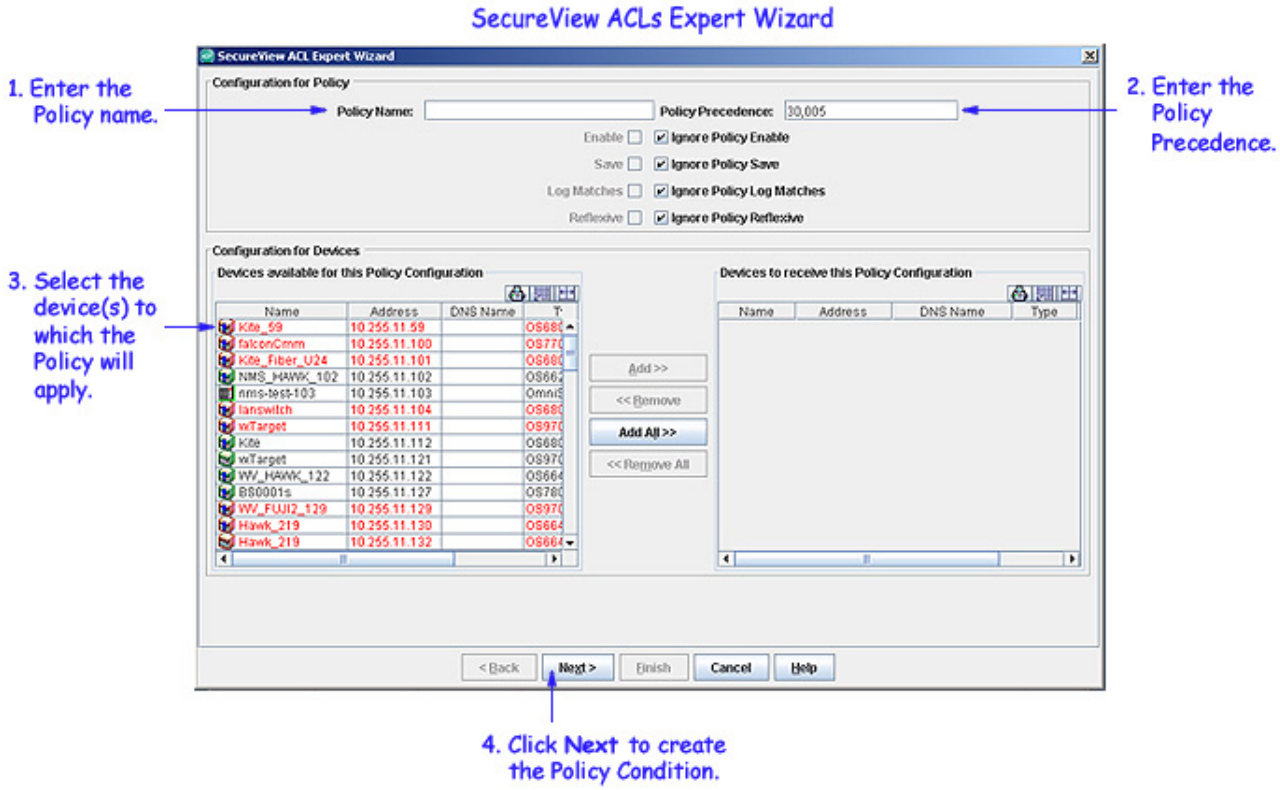
The **SecureView ACL Expert Wizard** window is used to create a new policy. Creating a new policy consists of the following basic steps:

- Creating a Policy
  - Enter a name for the policy.
  - Set the policy precedence value.
  - Specify the devices to which the policy will apply.
- Creating a Policy Condition that specifies the conditions that must be true before traffic will be allowed to flow.
- Creating a Policy Action that specifies parameters for the traffic that will flow.
- Applying a Policy to the network.

  **Note**:You cannot create, delete, or edit a One Touch policy in the Expert mode. You must use the One Touch Tab to create, edit, or delete a One Touch policy.

### Creating a Policy

To start creating a custom ACL policy, go to the **Expert** tab and click the **New** button. The **SecureView ACL Expert Wizard** window appears. In this screen you can enter the name of the policy, set the policy precedence, and specify the devices to which the policy will apply.




Follow the steps below to create a new policy.

**1.** Click the **New** button in the Expert tab. The **SecureView ACL Expert Wizard** window appears.

**2.** Enter a policy name in the **Policy Name** field.

**3.** Enter the policy precedence (range = 30001 - 500000) in the **Policy Precedence** field.

**4.** Select the device(s) to which you want to apply the policy, and then click the **Add** button.

**5**. Click the **Next** button to create the policy condition.

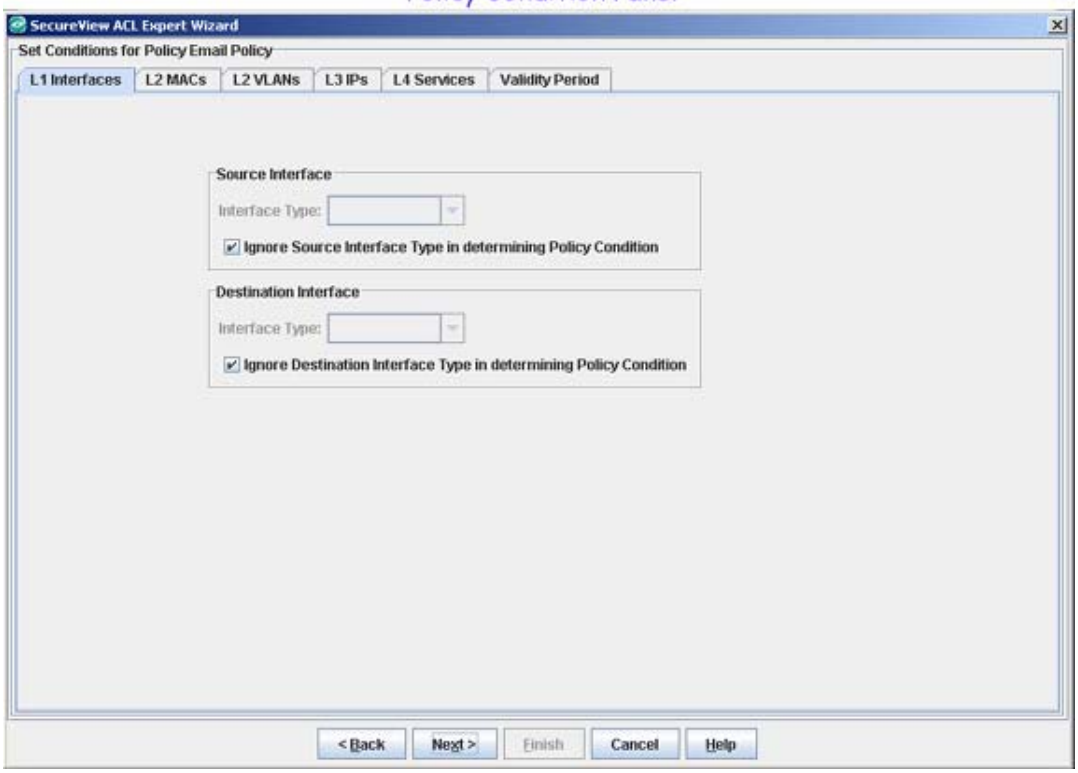
> **Note**: In the Expert mode, the **Policy Precedence** field is pre-filled with the lowest unused precedence value.

### Creating a Policy Condition

The Policy Condition panel contains tabs and parameters that enable you to create a policy condition. A policy condition enables you to specify one or more conditions that must be true before traffic is allowed to flow. Each tab in the Policy Condition panel enables you to specify a different type of condition for the traffic flow. Policy conditions for ACLs is limited to interface type, MAC ranges and MAC groups, VLANS, IP subnets and network groups, IP protocols,and Services and Service Groups. A brief description of each tab is provided below. Click the hyperlink for each condition for detailed configuration steps.

> **Note**: When creating conditions, do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

Policy Condition Panel




- **L1 Interfaces -** Create a condition that applies the policy to traffic originating from a specific source interface type or to traffic flowing to a specific destination interface type.
- **L2 MACs -** Create a condition that applies the policy to traffic originating from a MAC address/group or to traffic flowing to a MAC address/group. (Note that any MAC address may contain wildcard characters.)
- **L2 VLANs -** Create a condition that applies the policy to traffic flowing from one source VLAN to one destination VLAN, or to traffic flowing from one source VLAN to any destination VLAN, or to traffic flowing from any source VLAN to one destination VLAN.
- **L3 IPs -** Create a condition that applies the policy to traffic originating from an IP address/network group or to traffic flowing to an IP address/network group. (Note that any IP address can be masked.)
- **L4 Services -** Create a condition that applies the policy to traffic flowing between two TCP or UDP ports, or to all traffic originating from a TCP or UDP port, or to all traffic flowing to a TCP or UDP port, or from an existing service/service group, or to an existing service/service group.
- **Validity Period -** Specify the dates and times when you wish the policy to be valid (that is, when you wish the policy to be enforced.)

### Creating a Policy Action

A policy action enables you to specify the treatment traffic will receive when it flows. The treatment is based on the disposition (**Accept**/**Drop**) that the traffic will have. If the disposition chosen is **Accept**, then its minimum and maximum output rates, and the values to which specified bits in the frame headers will be set upon egress from the switch may be specified. If

the disposition chosen is **Drop**, then such specifications are not available. When the conditions specified in the Policy Condition panel are true, traffic will flow as specified by the policy action. See “Creating an Action” on page 25 for more information on configuring a policy action.

## Applying a Policy

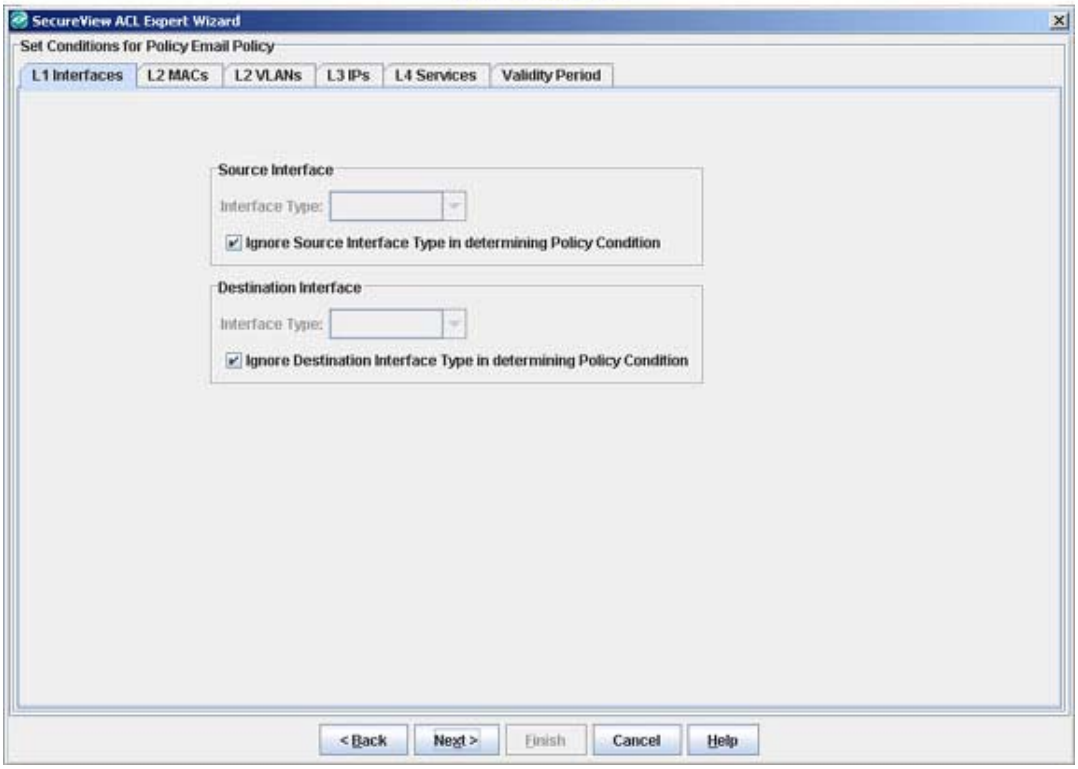
After reviewing the policy, you save the policy to the LDAP repository. When the policy information is saved to LDAP, the **Switches Pending Notification** table is updated. Make sure that the switches assigned to that policy are marked as "Unsaved" in the **Changes** column before clicking the **Notify** button.

When you click the **Notify** button, the switches listed in the **Switches Pending Notification** table are notified to re-cache their policies from the LDAP repository. See “Applying Policies to the Network” on page 29 for more information on applying a policy to the network.

## The Interfaces Tab

The Interfaces tab, shown below, enables you to create a condition that restricts the policy to traffic flowing from a source interface to a destination interface, or to traffic flowing from a source interface to any destination interface, or to traffic flowing from any source interface to a destination interface. Follow the steps below to create an interface condition.

Interfaces Tab



### Creating an Interface Condition

Create a source and/or destination interface type condition as described below. Do not click the **Next** button until you have completed all the desired tabs in the Policy Condition panel.

#### Source

**1.** Uncheck the **Ignore Source Interface Type in determining Policy Condition** checkbox. The source **Interface Type** drop-down list is activated.

**2.** Select the interface type from the source **Interface Type** drop-down list.

Selecting a source interface type, restricts the policy to traffic that flow from that interface only. If you leave the field blank or check the **Ignore Source Interface Type in determining Policy Condition** checkbox, you are effectively stating that the source interface type of traffic is not a criterion for the policy.

#### Destination

**1.** Uncheck the **Ignore Destination Interface Type in determining Policy Condition** checkbox. The destination **Interface Type** drop-down list is activated.

**2.** Select the interface type from the destination **Interface Type** in the drop-down list.

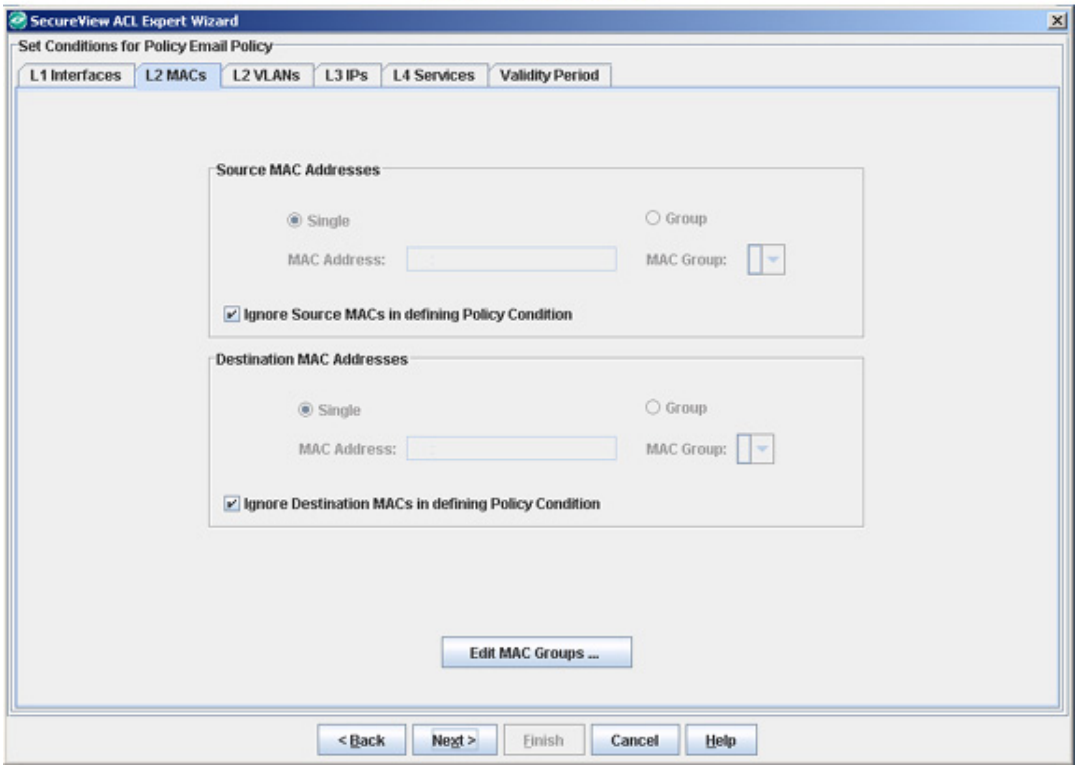
Selecting a destination interface type, restricts the policy to traffic that flows to this interface type only. If you leave the field blank or check the **Ignore Destination Interface Type in determining Policy Condition** checkbox, you are effectively stating that the destination interface type of traffic is not a criterion for the policy.

## The MACs Tab

The MACs tab, shown below, enables you to create a condition that applies the policy to traffic originating from, or flowing to, a MAC address/group. Note that Layer 2 conditions (conditions that specify MAC addresses) are "lost" when traffic passes through a router. For this reason, it may be advisable to specify other types of conditions (such as a Layer 3 condition, which specifies IP addresses) when traffic is expected to travel through more than one router hop. Using the MACs tab, you can create the following MAC conditions:

- Source MAC address
- Source MAC group
- Destination MAC address
- Destination MAC group

MAC Address Tab




Conditions that specify both a source and a destination MAC address may be rejected by some switch platforms as invalid. However, if you wish to create policies for both source and destination traffic, you can create one policy for the source traffic and a second policy for the destination traffic.

MAC addresses may contain the wildcard character *. However, one * character must be entered for each individual hex digit in the MAC address: for example, **00435C:******, not **00435C:***.

The following MAC address ranges are assigned to Alcatel voice devices and Alcatel IP phones. You can create conditions specifying these address ranges using the MAC Address tab.

- Voice Devices
  - 00809F3A0000 - 00809F3AFFFF
  - 00809F3B0000 - 00809F3BFFFF
  - 00809F3C0000 - 00809F3CFFFF
- IP phones
  - 00809F3D0000 - 00809F3DFFFF
- Multimedia Devices
  - 00809F3E0000 - 00809F3EFFFF
  - 00809F3F0000 - 00809F3FFFFF

### Creating a MAC Address Condition

Create a source and/or destination MAC address/group condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

### Source MAC Address

**1.** Uncheck the **Ignore Source MACs in defining Policy Condition** checkbox.

**2.** The **Single** radio button is selected and the source **MAC Address** field is activated.

**3.** Enter the source MAC address in the **MAC Address** field.

Entering a source MAC address, restricts the policy to traffic that originates from this address only. If you check the **Ignore Source MACs in defining Policy Condition** checkbox, you are effectively stating that the source MAC address/group of traffic is not a criterion for the policy.

### Source MAC Group

**1.** Uncheck the **Ignore Source MACs in defining Policy Condition** checkbox.

**2**. Click the **Group** radio button. The destination **MAC Group** drop-down list is activated.

**3.** Select the group from the **MAC Group** drop-down list. If you want to create, edit, or delete a MAC group click the **Edit MAC Groups...** button.

Selecting a source MAC group, restricts the policy to traffic that originates from this MAC group only. If you check the **Ignore Source MACs in defining Policy Condition** checkbox, you are effectively stating that the source MAC address/group of traffic is not a criterion for the policy.

### Destination MAC Address

**1.** Uncheck the **Ignore Destination MACs in defining Policy Condition** checkbox.

**2.** Click the **Single** radio button. The destination **MAC Address** field is activated. By default, the **Single** radio button is selected.

**3.** Enter the destination MAC address in the **MAC Address** field.

Entering a destination MAC address, restricts the policy to traffic that flows to this address only. If you check the **Ignore Destination MACs in defining Policy Condition** checkbox, you are effectively stating that the destination MAC address/group of traffic is not a criterion for the policy.

### Destination MAC Group

**1.** Uncheck the **Ignore Destination MACs in defining Policy Condition** checkbox.

**2.** Click the **Group** radio button. The destination **MAC Group** drop-down list is activated.

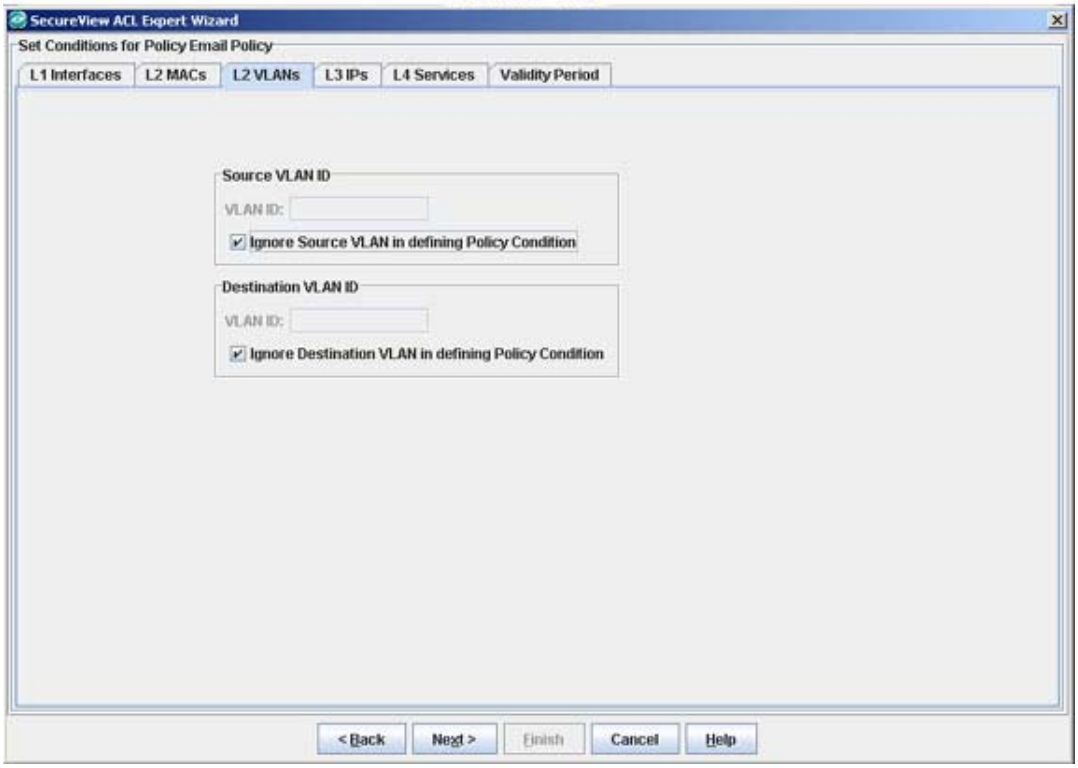
**3.** Select the group from the **MAC Group** drop-down list. If you want to create, edit, or delete a MAC group click the **Edit MAC Groups...** button.

Selecting a destination MAC group, restricts the policy to traffic that flows to this address only. If you check the **Ignore Destination MACs in defining Policy Condition** checkbox, you are effectively stating that the destination MAC address/group of traffic is not a criterion for the policy.

## The VLANs Tab

The VLANs tab, shown below, enables you to create a condition that restricts the new policy to traffic flowing from a source VLAN to a destination VLAN, or to traffic flowing from a source VLAN to any destination VLAN, or to traffic flowing from any source VLAN to a destination VLAN. Follow the steps below to create a VLAN condition.

VLANs Tab




### Creating a VLAN Condition

Create a VLAN condition as described below. Do not click the **Next** button until you have completed all the desired tabs in the Policy Condition panel.

### Source

**1.** Uncheck the **Ignore Source VLAN in defining Policy Condition** checkbox. The source **VLAN ID** field is enabled.

**2.** Enter the desired VLAN ID.

Entering a VLAN ID restricts the policy rule to traffic originating from that VLAN only. If you leave the field blank or check the **Ignore Source VLAN in defining Policy Condition** checkbox, you are effectively stating that the source VLAN ID of traffic is not a criterion for the policy.

### Destination

**1.** Uncheck the **Ignore Destination VLAN in defining Policy Condition** checkbox. The destination **VLAN ID** field is enabled.

**2.** Enter the desired VLAN ID.

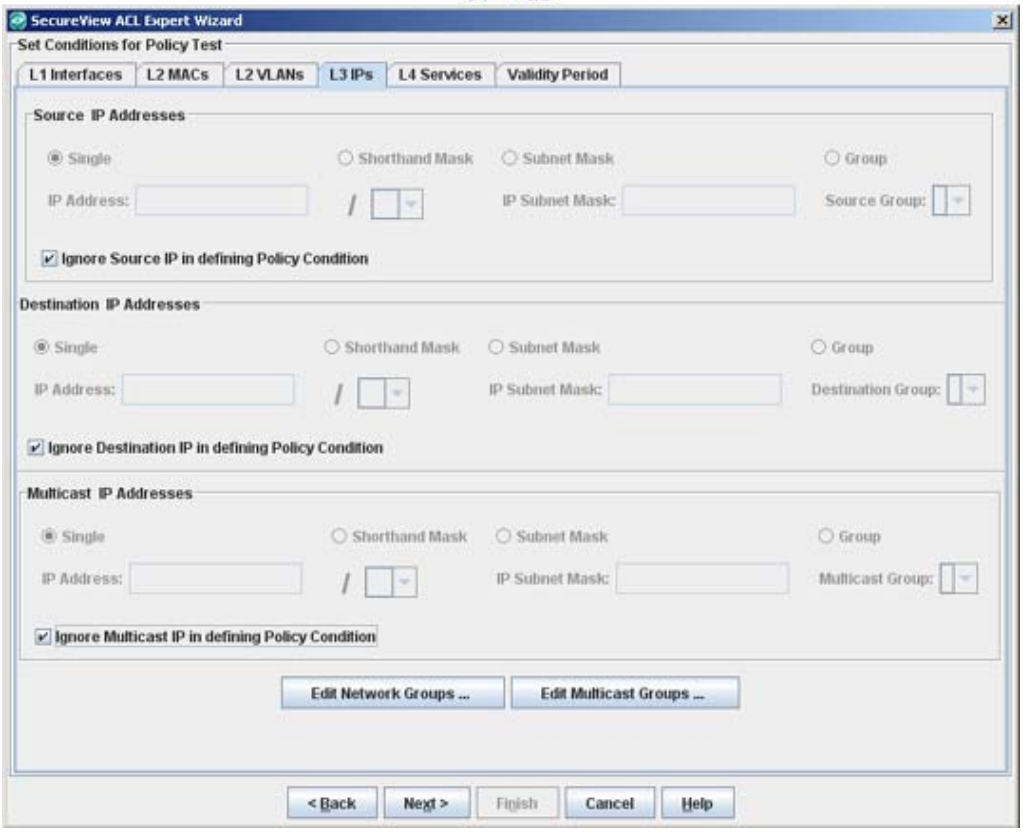
Entering a VLAN ID restricts the policy rule to traffic flowing to that VLAN only. If you leave the field blank or check the **Ignore Destination VLAN in defining Policy Condition** checkbox, you are effectively stating that the destination VLAN ID of traffic is not a criterion for the policy.

## The IPs Tab

The IPs tab, shown below, enables you to create a condition that applies the policy to all traffic originating from, or flowing to, an IP address/network group or Multicast IP address. Note that conditions that specify both a source and a destination address/group will be rejected by the switch as invalid. However, if you wish to create policies for both source and destination traffic, you can create one policy for the source traffic and the second policy for the destination traffic. Using the IP tab, you can create the following IP conditions:

- Source IP Address
- Source Network Group
- Destination IP Address
- Destination Network Group
- Multicast IP Address
- Multicast IP Group

IP Tab



### Creating an IP Address Condition

Create a source and/or destination IP address/network group condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

### Source IP Address

**1.** Uncheck the **Ignore Source IPs in defining Policy Condition** checkbox.

**2**. Click the **Single** radio button and enter a source **IP Address**

**3**. Click either the **Shorthand Mask** or **Subnet Mask** radio button. If you are using a shorthand mask, set the shorthand mask drop-down list to the desired value. If you are using a full subnet mask, enter the mask in the **IP Subnet Mask** field.

**Note**: The * wildcard character is not allowed in IP addresses.

Entering an IP address restricts the policy rule to traffic originating from that IP address (or masked IP address). If you leave the field blank or check the **Ignore Source IPs in defining Policy Condition** checkbox, you are effectively stating that the source IP address/network group of traffic is not a criterion for the policy.

### Source Network Group

**1.** Uncheck the **Ignore Source IPs in defining Policy Condition** checkbox.

**2.** Click the **Group** radio button, and then select the group from the **Network Group** drop-down list. If you want to create, edit, or delete a group, click the **Edit Network Groups...** button.

Selecting a network group restricts the policy rule to traffic originating from that network group. If you leave the field blank or check the **Ignore Source IPs in defining Policy Condition** checkbox, you are effectively stating that the source IP address/network group of traffic is not a criterion for the policy.

### Destination IP Address

**1.** Uncheck the **Ignore Destination IPs in defining Policy Condition** checkbox.

**2**. Click the **Single** radio button is and enter an destination **IP Address**.

**3.** Click either the **Shorthand Mask** or **Subnet Mask** radio button. If you are using a shorthand mask, set the shorthand mask drop-down field to the desired value. If you are using a full subnet mask, enter the mask in the IP Subnet Mask field.

**Note**: The * wildcard character is not allowed in IP addresses.

Entering an IP address restricts the policy rule to traffic flowing to that IP address (or masked IP address). If you leave the field blank or check the **Ignore Destination IPs in defining Policy Condition** checkbox, you are effectively stating that the destination IP address/network group of traffic is not a criterion for the policy.

### Destination Network Group

**1.** Uncheck the **Ignore Destination IPs in defining Policy Condition** checkbox.

**2.** Click the **Group** radio button, and then select the group from the **Network Group** drop-down list. If you want to create, edit, or delete a group, click the **Edit Network Groups...** button.

Selecting a network group restricts the policy rule to traffic that flows to this network group. If you leave the field blank or check the **Ignore Destination IPs in defining Policy Condition** checkbox, you are effectively stating that the destination IP address/network group of traffic is not a criterion for the policy.

### Multicast IP Address

**1.** Uncheck the **Ignore Multicast IP in defining Policy Condition** checkbox.

**2.** Click the **Single ratio** button, and enter an **IP Address**.

**3**. Click either the **Shorthand Mask** or **Subnet Mask** radio button. If you are using a shorthand mask, set the shorthand mask drop-down list to the desired value. If you are using a full subnet mask, enter the mask in the **IP Subnet Mask** field.

**Note**: The * wildcard character is not allowed in IP addresses.

Entering an IP address restricts the policy rule to traffic originating from that address (or masked IP address). If you leave the field blank or check the **Ignore Source IPs in defining Policy Condition** checkbox, you are effectively stating that the Multicast IP address of traffic is not a criterion for the policy.

### Multicast Group

**1.** Uncheck the **Ignore Destination IPs in defining Policy Condition** checkbox.

**2.** Click the **Group** ratio button, and then select the group from the **Multicast Group** drop-down list. If you want to create, edit, or delete a group, click the **Edit Multicast Groups...** button.

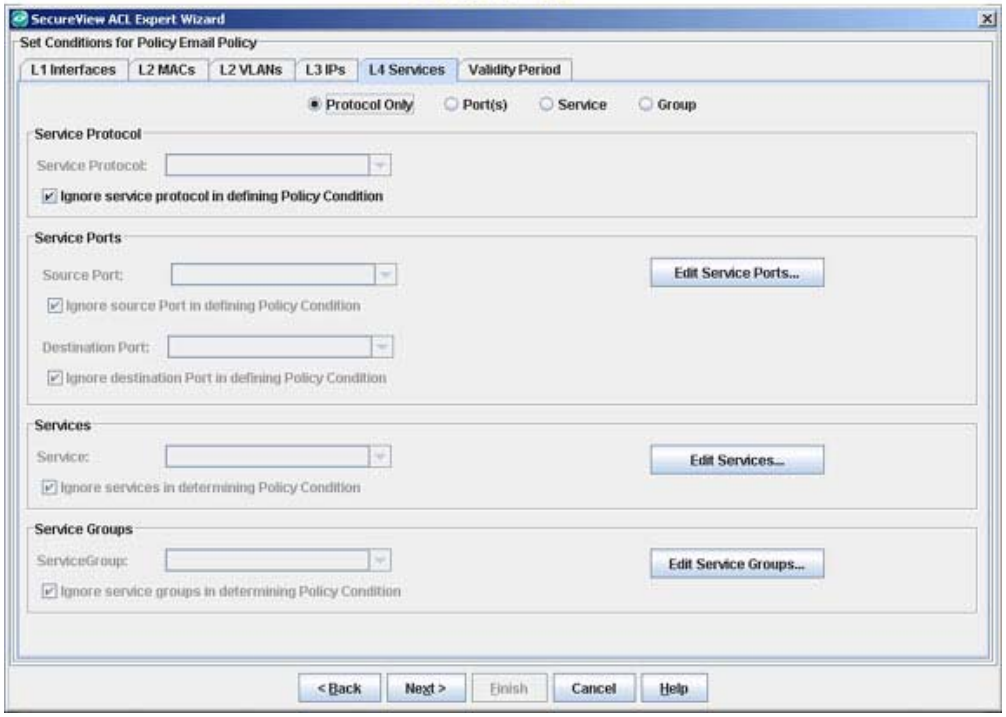
Selecting a multicast group restricts the policy rule to traffic that flows to this network group. If you leave the field blank or check the **Ignore Multicat IP in defining Policy Condition** checkbox, you are effectively stating that the Multicast group of traffic is not a criterion for the policy.

## The Services Tab

The Services tab, shown below enables you to create a condition that applies the policy to traffic flowing between two TCP or UDP ports, or to all traffic originating from a TCP or UDP port, or to all traffic flowing to a TCP or UDP port. The Services tab also enables you to create a condition using a service or a service group. Using the Services tab, you can create the following conditions:

- Service Protocol condition
- Service condition
- Service Group condition

Services Tab




### Creating a Service Protocol Condition

Create a Service Protocol condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

**1.** Select the **Protocol Only** radio button. The **Service Protocol** drop-down list is enabled.

**2.** Select a protocol from the **Service Protocol** drop-down list (TCP or UDP) to define the type of ports you will specify.

**3.** Select the **Port(s)** radio button to specify the source or destination ports.

- If you want to specify a source port, uncheck the **Ignore source Port in defining Policy Condition** checkbox. The **Source Port** drop-down list is enabled. Select a source port from the **Source Port** drop-down list.
- If you want to specify a destination port, uncheck the **Ignore destination Port in defining Policy Condition** checkbox. The **Destination Port** drop-down list is enabled. Select a destination port from the **Destination Port** drop-down list.

**Note**: You can also create a service protocol condition without specifying the source and destination ports.

If you want to create, edit, or delete a service port, click the **Edit Services Ports...** button.

### Creating a Service Condition

Create a Service condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

**1.** Select the **Service** radio button.

**2.** Uncheck the **Ignore services in determining Policy Condition** checkbox. The **Service** drop-down list is enabled.

**3**. Select a service from the **Service** drop-down list.

If you want to create, edit, or delete a service, click the **Edit Services...** button.

### Creating a Service Group Condition

Create a Service Group condition as described below. Do not click the **Next** button until you have completed all desired tabs in the Policy Condition panel.

**1.** Select the **Group** radio button.

**2.** Uncheck the **Ignore service groups in determining Policy Condition** checkbox.

**3.** Select a service from the **ServiceGroup** drop-down list.

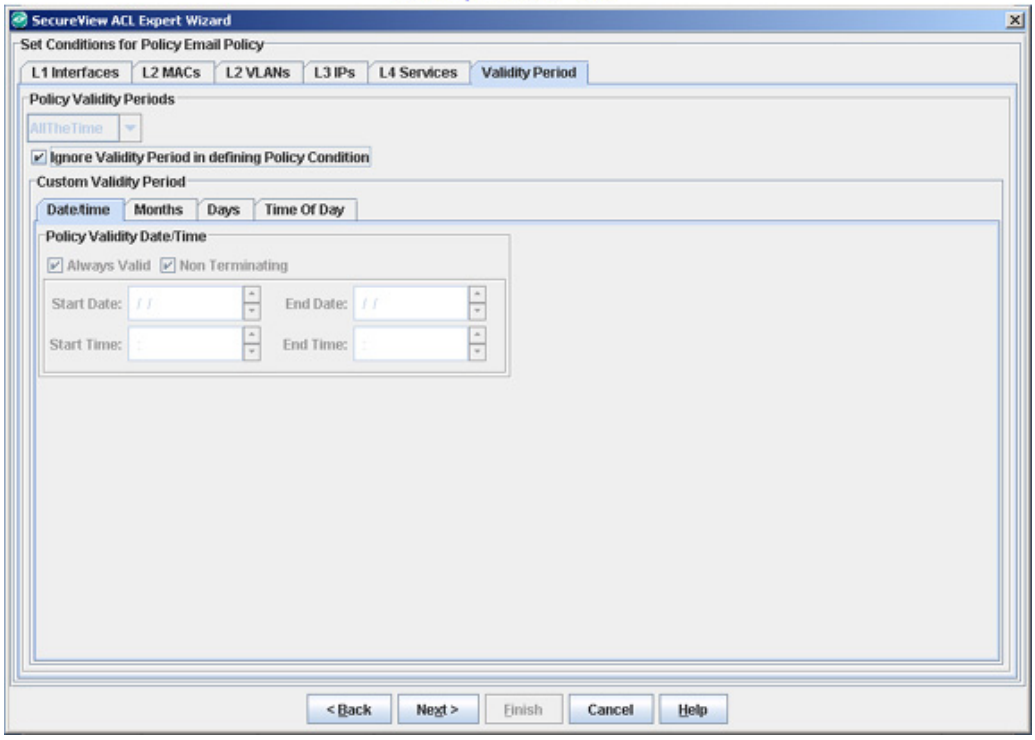
If you want to create, edit, or delete a group, click the **Edit Service Groups...** button.

## The Validity Period Tab

The Validity Period tab (shown below) enables you to add a validity period to a condition by specifying the time periods when the policy is active and enforced. Four pre-configured policy validity periods are provided in the drop-down list in the **Policy Validity Periods** pane. They are **AllTheTime**, **Weekdays**, **Weekends**, and **WorkingDay**. You can also create custom validity periods.

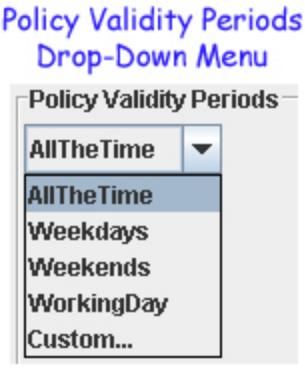
> **Note**: The pre-configured validity period **AllTheTime** is the default and is automatically assigned to the condition when the **Ignore Validity Period in defining Policy Condition** checkbox is unchecked.

Validity Period Tab



### Pre-Configured Validity Periods

To use one of the pre-configured policy validation periods, uncheck the **Ignore Validity Period in defining Policy Condition** checkbox and select the desired validity period from the **Policy Validity Periods** drop-down list (shown and described below).




- **AlltheTime** - Specifies all months of the year, all days of the week, and all hours of the day.
- **Weekdays** - Specifies weekdays (Monday - Friday), all months of the year. Each weekday is 24 hours (midnight to midnight).
- **Weekends** - Specifies Saturday and Sunday, all months of the year. Each Saturday and Sunday is 24 hours (midnight to midnight).
- **WorkingDay** - Specifies weekdays (Monday - Friday), from 9:00 a.m. to 5:00 p.m. all months of the year.
- **Custom** - Select to create a custom validity period.

**Note**: If you do not want a validity period to be part of the policy, make sure that the **Ignore Validity Period in defining Policy Condition** checkbox is checked.

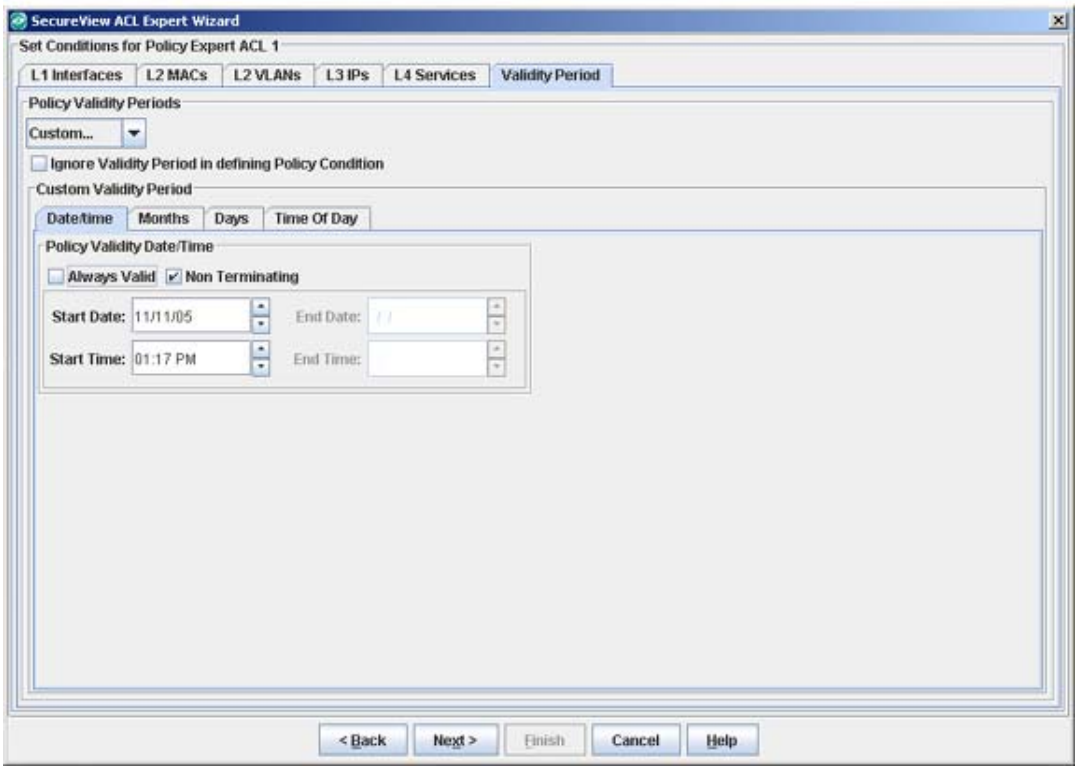
### Creating a Custom Validity Period

To create a custom validity period, uncheck the **Ignore Validity Period in defining Policy Condition** checkbox and select **Custom** from the **Policy Validity Periods** drop-down list. A custom validity period can specify any desired month, and/or day of the week, and/or time of day. The four subtabs in the Custom Validity Period pane - **Date/time**, **Months**, **Days**, and **Time Of Day** - enable you to create custom validity periods.

### Date/time Subtab

The **Date/time** subtab enables you to specify a starting date/time and an ending date/time for a custom validity period.

Date/Time Subtab




Uncheck the **Always Valid** checkbox to specify that the policy validity period will have a start date and a start time, but no end date and end time. Uncheck the **Non Terminating** checkbox to specify that the policy validity period will have a start date and time (you enter in the **Start Date** and **Start Time** fields), and also an end date and time (you enter in the **End Date** and **End Time** fields). Enter a value in the desired fields, or use the up and down arrows.

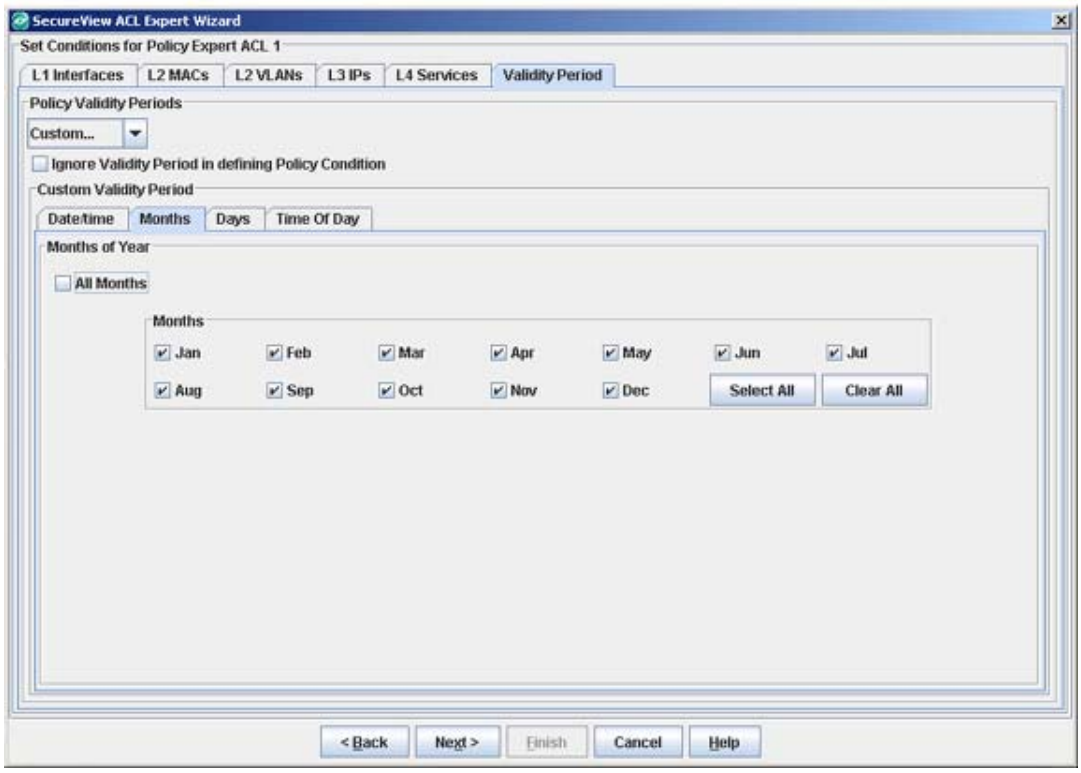
If you check both the **Always Valid** and the **Non Terminating** checkboxes, you cannot enter any desired dates and times in the **Start Date**, **Start Time**, **End Date**, and **End Time** fields.

> **Note**: The **Date/time** subtab enables you to define overall starting and ending dates/times for the entire validity period. However, the validity period can include specified months, days, or times of day when it is not active. These inactive periods can be defined using the Months subtab, the Days subtab, and the Time Of Day subtab.

### Months Subtab

The **Months** subtab enables you to specify the months of the year that the validity period will be active. A check by a month means the policy will be active and enforced during that month. Check the **All Months** checkbox to automatically check all the months of the year, or uncheck the **All Months** checkbox and select specific months. Click the **Clear All** button to uncheck all the months of the year. You can then check individual months as desired.

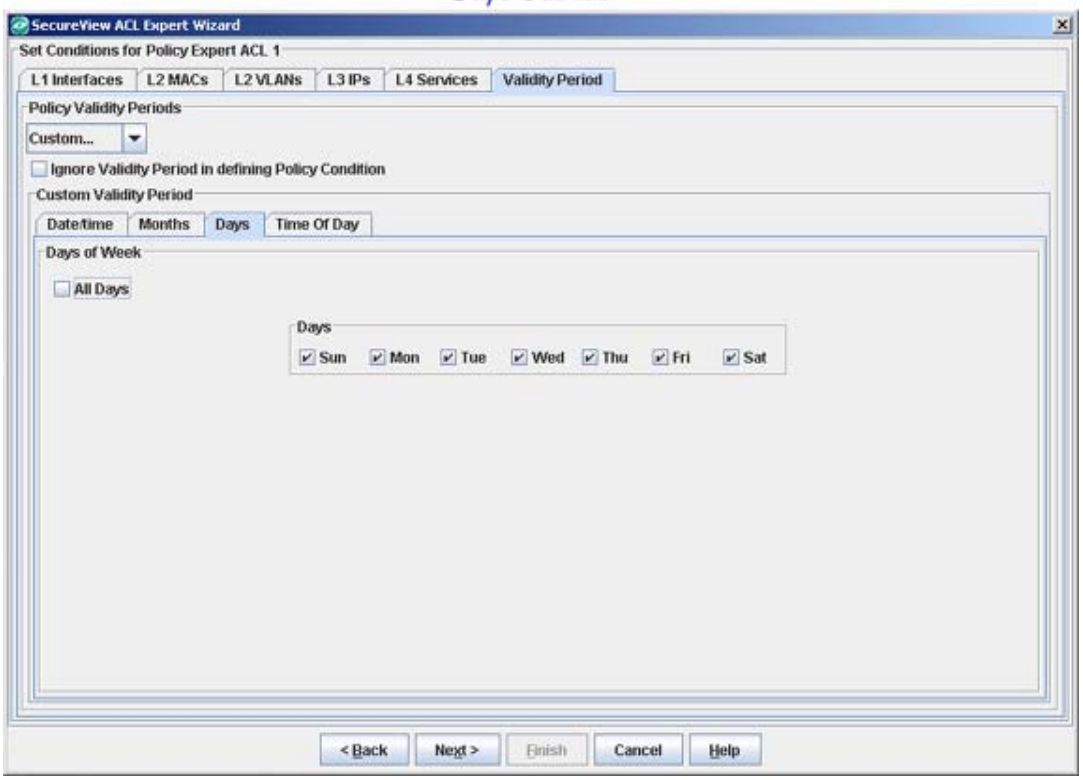
Months Subtab




## Days Subtab

The **Days** subtab enables you to individually specify the days of the week that the validity period will be active. Check the **All Days** checkbox to automatically check all the days of the week, or uncheck the **All Days** checkbox and select specific days. A check against a specific day implies that the policy will be active and enforced during that day.

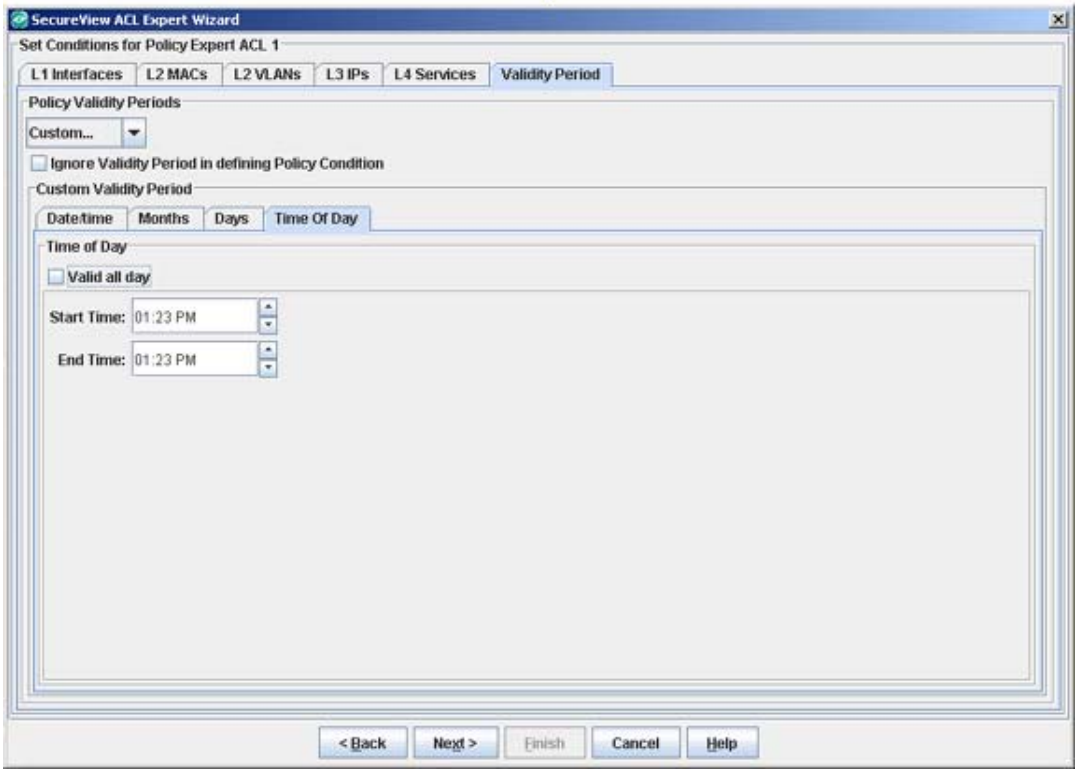
Days Subtab




## Time Of Day Subtab

The **Time Of Day** subtab enables you to specify a daily starting time and ending time that will apply to each day that the validity period is active. Check the **Valid all day** checkbox to make the validity period active 24 hours a day during the days that it is active. To specify specific starting and ending times, uncheck the **Valid all day** checkbox and enter the desired times in the **Start Time** and **End Time** fields. Enter a value in the desired fields, or use the up and down arrows.

Time of Day Subtab



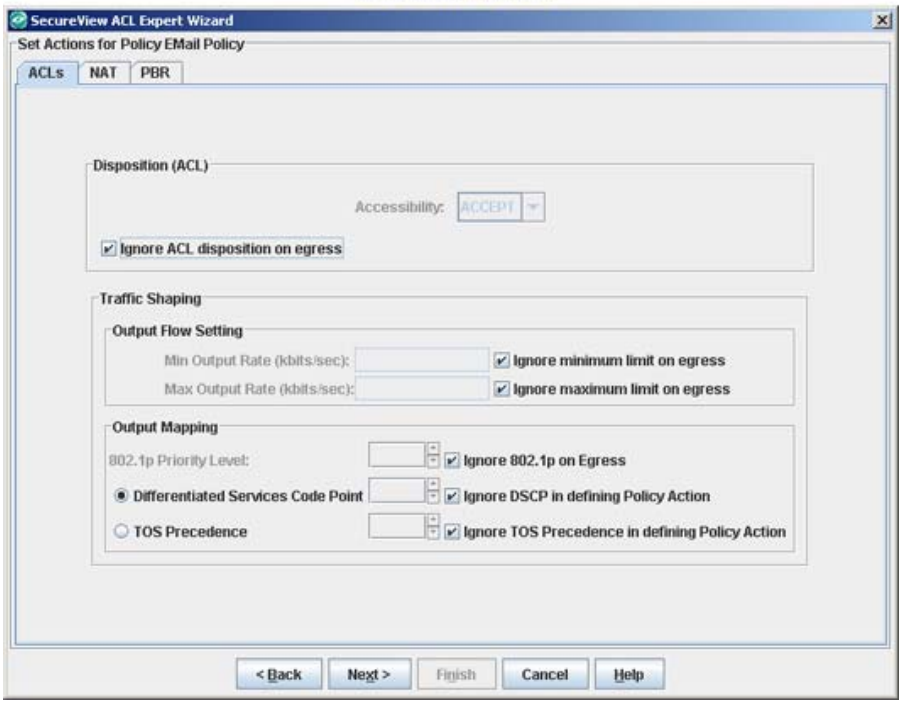

**Note**: Click the **Next** button when you have completed all the desired tabs in the Policy Conditions panel.

## Creating an Action

### ACL Policy Action

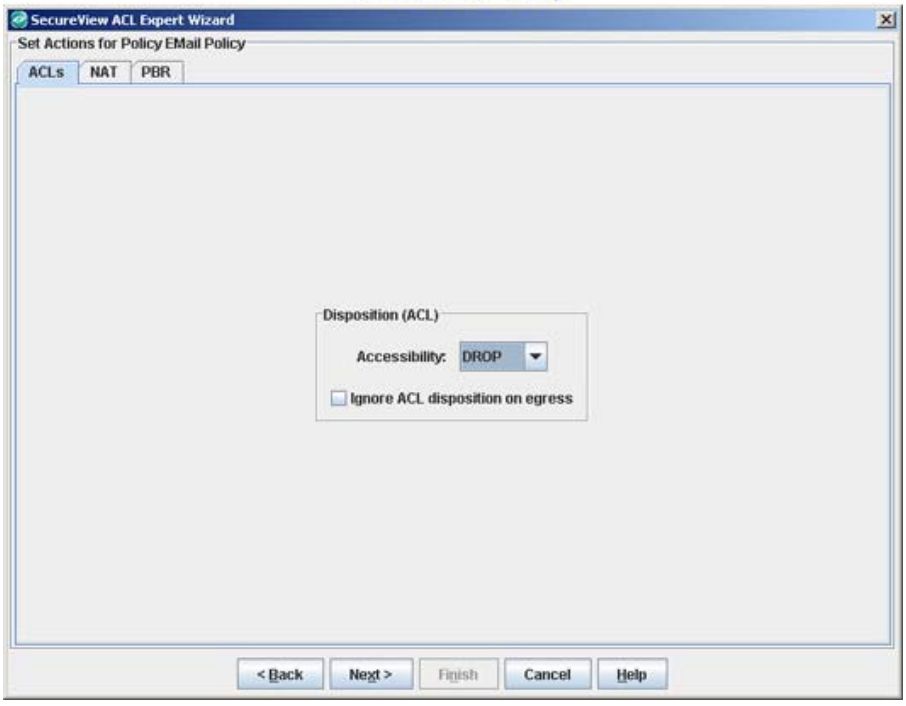
The ACL Policy Action tab enables you to specify actions to impose on traffic that meets the configured condition(s). When the specified conditions are true, traffic will flow as specified by the action. The access controls defined for SecureView ACL policies are **Accept** and **Drop**. When the accessibility is set to **Accept**, you can set the minimum and maximum output rates and the values to which specified bits in the frame headers will be set upon egress from the switch.

ACL Action Panel




However, if the accessibility is set to **Drop**, the additional parameters are removed from the screen, as shown below, until the "Accept" option is selected again. You can return to the "Accept" option from this window by clicking in the **Ignore ACL disposition on egress** checkbox.

ACL Action - Drop



### Disposition (ACL) Parameters

When the accessibility is set to **Accept**, you can set the minimum and maximum output rates and the values to which specified bits in the frame headers will be set upon egress from the switch. If you set the accessibility value to **Drop**, traffic meeting the criteria specified is dropped. To set the accessibility value, uncheck the **Ignore QoS priority on egress** checkbox, and select the priority from the drop-down menu. Leave the box checked if you don't want to apply any ACL actions to traffic.

### Traffic Shaping Parameters

The **Traffic Shaping** fields are used to specify the egress traffic flow rates and packet tagging characteristics for traffic matching the policy condition(s).

### Output Flow Settings

**Min Output Rate (kbits/sec) -** If you want to specify a minimum output rate, uncheck the **Ignore minimum limit on egress** checkbox, and specify the minimum amount of traffic, in kilobits-per-second, which is guaranteed to be transmitted from the port.

**Max Output Rate (kbits/sec) -** If you want to specify a maximum output rate, uncheck the **Ignore maximum limit on egress** checkbox, and specify the maximum amount of traffic, in kilobits-per-second, which is guaranteed to be transmitted from the port. Even if no other traffic exists, the output will be limited to the rate specified here.

### Output Mapping

The following parameters enable you to specify how packets that match the policy conditon(s) will be tagged upon egress from the switch.

**802.1p Priority Level -** If you want outgoing packets tagged with an 802.1p priority level, uncheck the **Ignore 802.1p on Egress** checkbox. Set the **802.1p Priority Level** field to any value between 0 to 7 to specify the desired outgoing 802.1p priority for the traffic. A value of **7** indicates the highest priority and a value of 0 indicates the lowest priority.

For ports that are configured for 802.1q, this value is used in the 802.1q header and indicates the outgoing priority of the frame. When a frame is de-queued for transmission, it is assigned the priority of the queue and mapped to the outgoing 802.1p priority. This priority is combined with the VLAN group ID to create the 802.1p/q header for transmission. Note that if traffic matches the criteria specified by the policy condition, but the outgoing port does not support 802.1p tagging, the policy action will fail.

**Differentiated Services Code Point (DSCP) -** DSCP is defined in RFC 2474. Differentiated Services defines the QoS treatment a frame is to receive from each network device. This is referred to as per-hop behavior. If you enable the **Differentiated Services Code Point** radio button, you can set the associated field to any value from **0-63** to specify the Differentiated Services byte value with which to tag frames upon egress from the switch.

**TOS Precedence -** The TOS byte is defined in RFC 791. This byte contains two fields. The precedence field is the three high-order bits (0-2) and is used to indicate the priority for the frame. The type of service field (bits 3-6) defines the throughput, delay, reliability, or cost for the frame; however, in practice these bits are not used. If you enable the **TOS Precedence** radio button, set the associated field to any value from 0-7 to specify the value that will be inserted

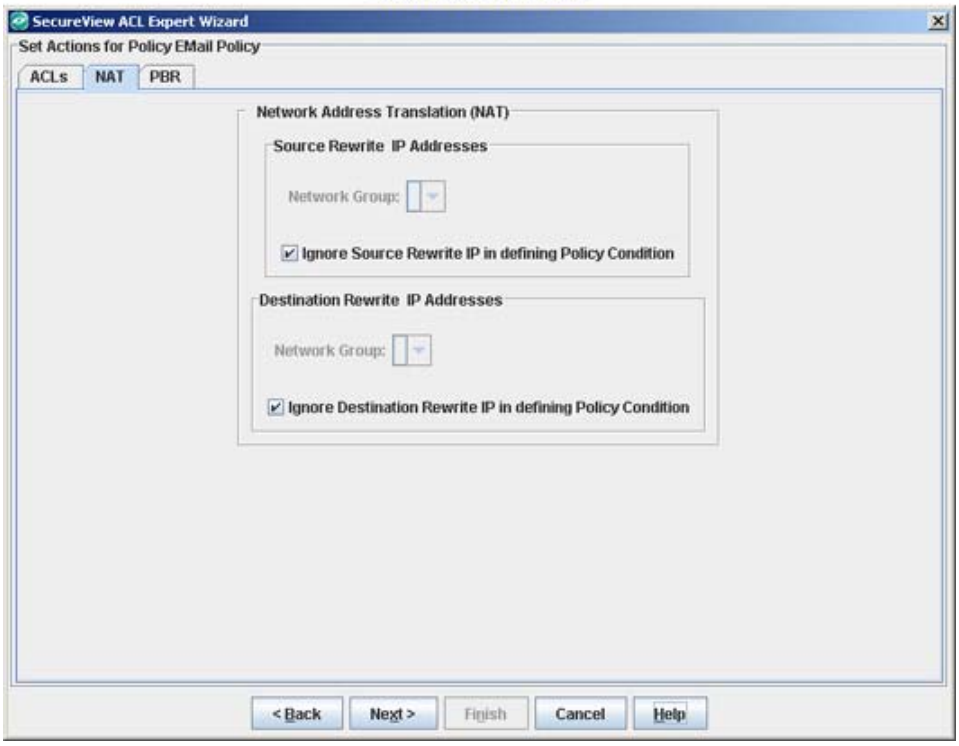
into the precedence field of the TOS byte upon egress from the switch. A value of 7 has the highest precedence and a value of 0 has the lowest precedence.

> **Note:** You can enable **either** the DSCP or the TOS Precedence radio button to specify the mechanism you want to use (if any) to convey QoS information in the IP header of frames. DSCP and TOS are mutually exclusive. You can use either DSCP or TOS, but not both

### NAT Policy Action

The NAT Policy Action tab enables you to specify Network Address Translation actions to impose on traffic that meets the configured condition(s). When the conditions specified are true, traffic will flow as specified by the policy action.

NAT Action Panel




### Source Rewrite IP Address

To include Source Rewrite IP in the NAT Policy condition, uncheck the **Ignore Source Rewrite IPs in defining Policy Condition** option and select Network Group to be used for policy condition from the **Network Group** drop-down menu.

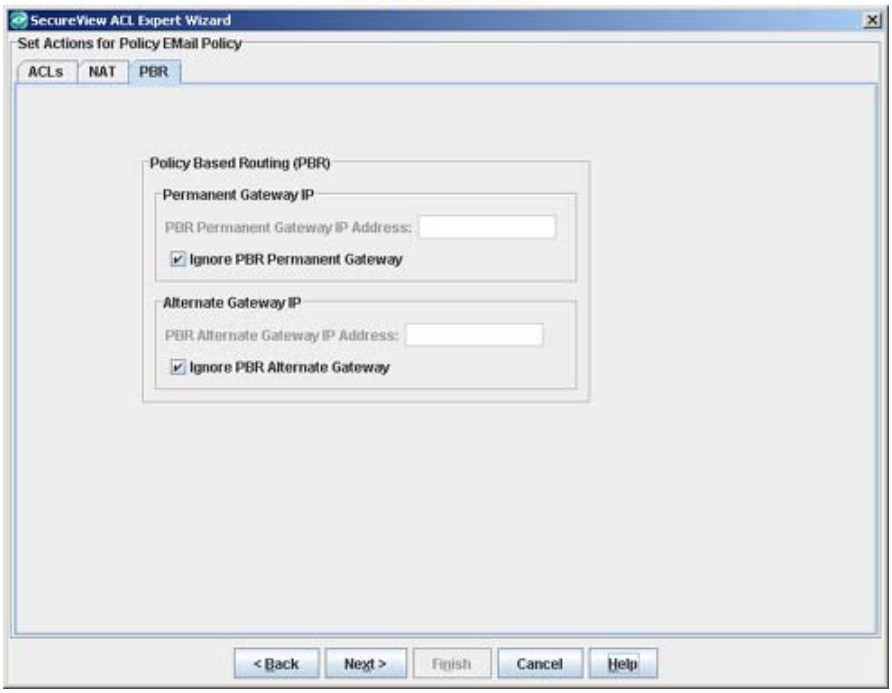
### Destination Rewrite IP Address

To include Destination IP in the Policy Conditions, uncheck the **Ignore Destination Rewrite IPs in defining Policy Condition** option and select Network Group to be used for policy condition from the **Network Group** drop-down menu.

### PBR Policy Action

The PBR Policy Action tab enables you to specify to specify the default IP address to be used for Policy Based Routing on traffic that meets the configured condition(s). When the conditions specified are true, traffic will flow as specified by the action.

PBR Action Panel




### Permanent Gateway IP

To set a Permanent Gateway IP address for traffic that meets the condition(s), uncheck the **Ignore PBR Permanent Gateway** checkbox and enter the default IP address in the **PBR Permanent Gateway IP Address** field.

### Alternate Gateway IP

To specify an alternate IP address for traffic that meets the policy condition(s), uncheck the **Ignore PBR Alternate Gateway** checkbox and enter the alternate IP address in the **PBR Alternate Gateway IP Address** field.

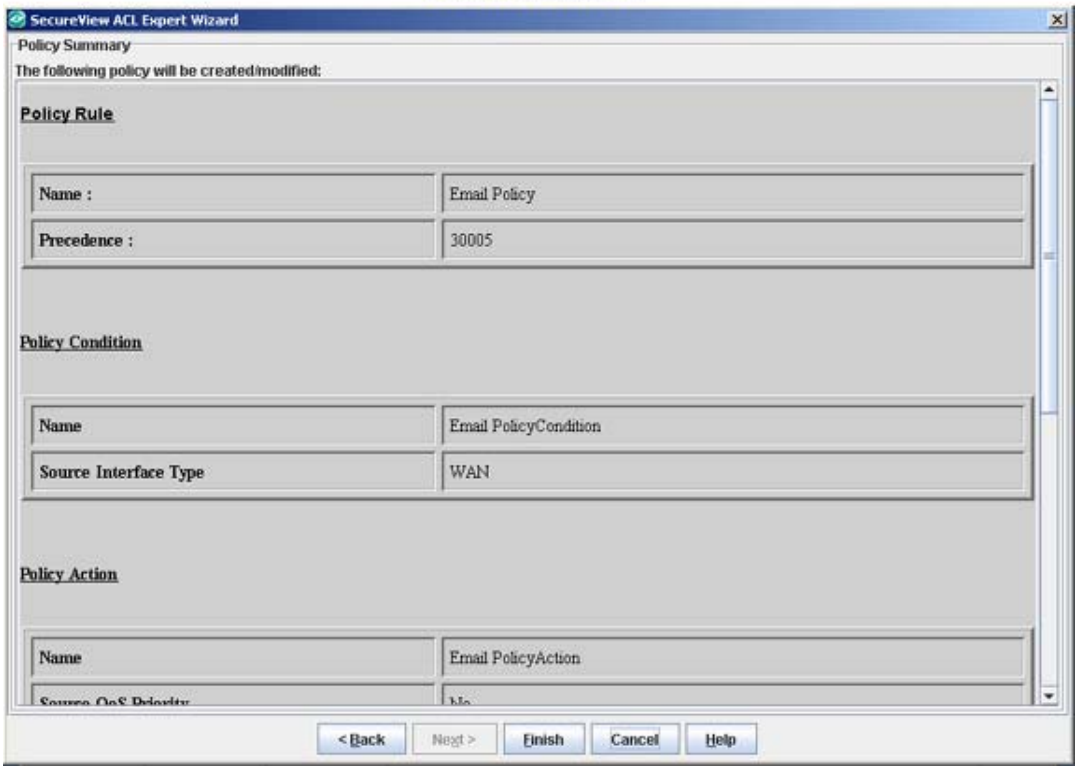
> **Note**: The OmniSwitch 68006850//7000/8000/9000 series switches support the 802.1 priority, DSCP, and TOS. However, 6600 series switches and some current XOS hardware and firmware releases do not. Please refer to the switch Release Notes for information on the specific QoS functions available on various current platforms and combinations of hardware/firmware.

## Applying Policies to the Network

The final screen of **SecureView ACL Expert Wizard** is the Policy Summary panel. This panel provides a summary of all of the policy parameters (conditions, actions etc.) for you to review. Applying a policy to the network consists of the following steps:

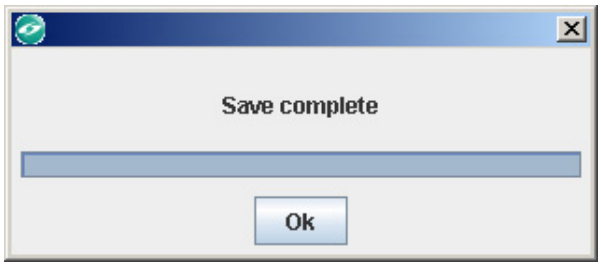
- Saving the policy to the LDAP repository
- Notifying the switches

Summary Window




### Saving the Policy to the LDAP Repository

After reviewing the policy, click the **Finish** button to save the policy to the LDAP repository. When the policy is saved, the following confirmation window will appear. Click the **OK** button to return to the **Expert** tab.

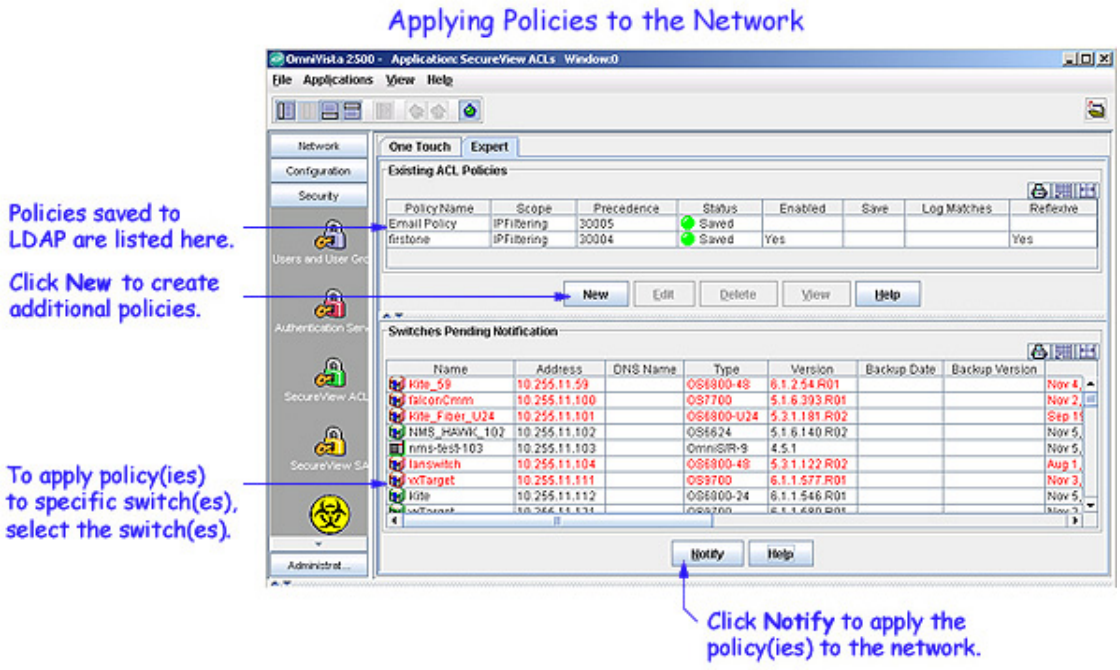



You can create additional policies or apply any policies you have created to the network.

> **Note:** Network segmentation, which can be performed using Quarantine Manager, does not work if the SecureView ACL application is used to create the ACLs for Quarantine Manager. SecureView ACL overrides the Quarantine Manager network segmentation setup.

### Notifying the Switches

After saving a policy to the LDAP repository, you will be returned to the **Expert** tab. This tab lists all the policies that have been created and saved to the LDAP repository. You can apply a policy to all the switches configured for the policy, or you can apply the policy to individual switches within that group.




When you click the **Notify** button, all the policies listed in the **Existing ACL Policies** table are applied to all the switches configured for each policy. To apply the policy(ies) only to certain switches within the configured group of switches, select those switches from the **Switches Pending Notification** table.

> **Note:** Press **Ctrl** or **Shift** while clicking the mouse to select multiple switches.
>
> **Note:** Re-caching policies from the LDAP repository is very expensive in terms of switch resources and time. It is recommended that you verify all policies that you have created and notify the switches at the same time to minimize switch downtime.

### Error and Status Reporting

Messages in the policy.log file report the success or failure of the re-cache operation on an individual switch.

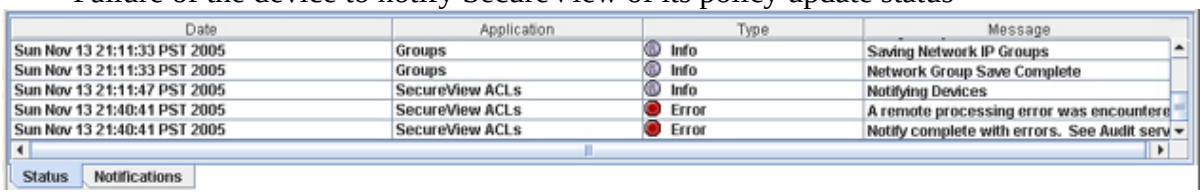
### The Status Panel

When you save policies to the LDAP repository and apply policies to the network, any error that may occur is reported in the Status panel (shown below).

Possible errors include:

- Failure to update the LDAP repository
- Failure to notify selected devices that they must re-cache their policies from the LDAP repository (which will occur if there is an SNMP timeout for any reason)

- Failure of the device to notify SecureView of its policy update status



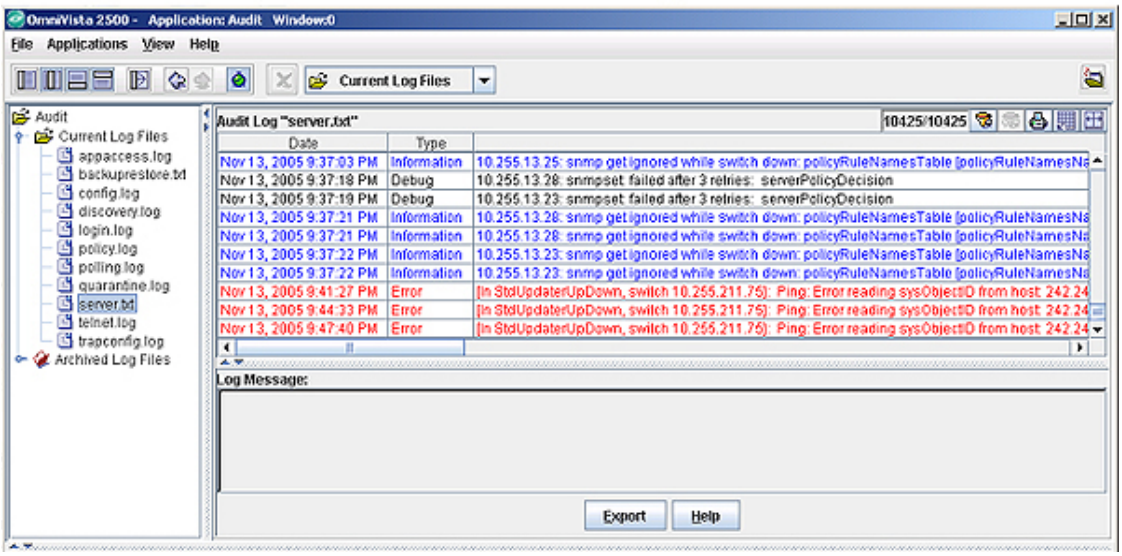

## Traps

When QoS-enabled Alcatel devices are notified that the LDAP repository has been changed, they re-cache their policies from LDAP, and then generate a trap notification to OmniVista informing that they have read the LDAP changes and have updated their internal policy information. Traps can be viewed in the Notifications application.

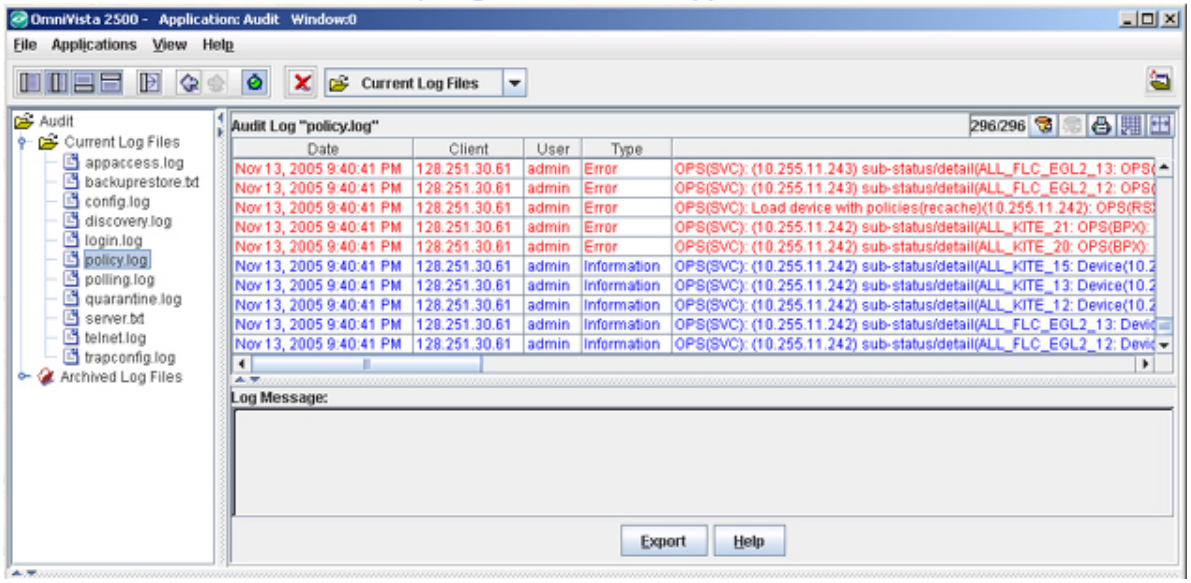
## The policy.log File and the server.txt File in the Audit Application

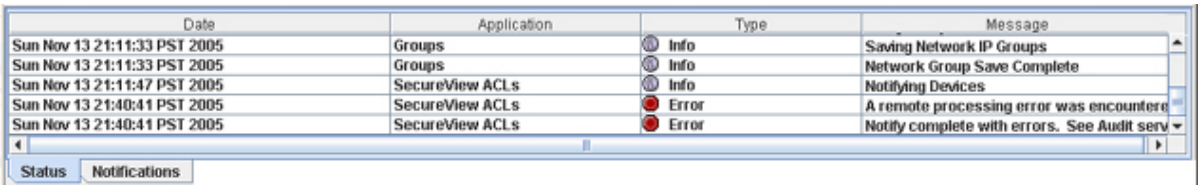
When the SecureView ACL application detects that a re-cache of policy information has failed on any device, the application writes a report to the OmniVista server.txt file and the policy.log file, which can be viewed from the Audit application.

The server.txt File in the Audit Application



Policy Log in the Audit Application

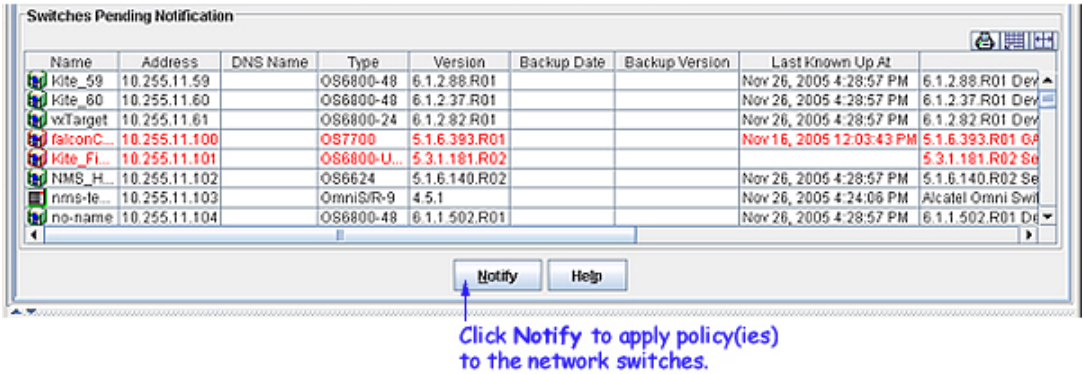



## Notifying Policies in Expert Tab

The **Switches Pending Notification** table in the **Expert** tab, shown below, contains a list of switches whose assigned policies and/or LDAP role configurations have changed as a result of a policy configuration, but have not been notified to re-cache.

Switches Pending Notification Table



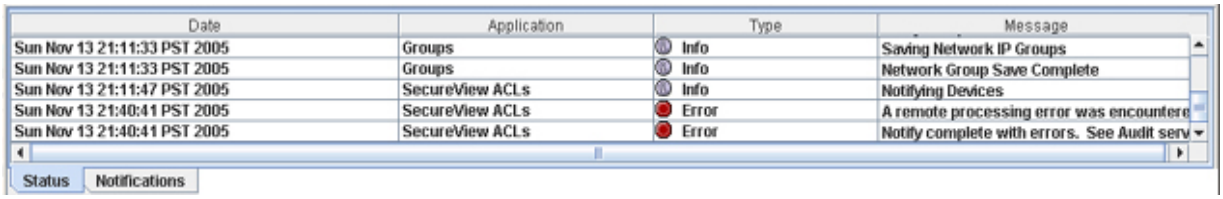

To notify a switch in the **Switches Pending Notification** table, select the desired switch, and then click the **Notify** button to re-cache its policy configurations.

If you click the **Notify** button without selecting any switch in the **Switches Pending Notification** table, it will enable all the switches in the list to flush their policy tables and reload policies from the LDAP repository. This is very expensive in terms of switch resources and time. If any One

Touch mode policy has been defined, the switches to which that policy was assigned will re-cache their policy tables also. It is recommended that you verify all policies that you have created and apply them at the same time to minimize switch downtime.

When the **Notify** button is clicked, an SNMP message is sent to the selected switch(es) in the list, informing the switch that the information in the LDAP repository has changed and commanding it to update its cached policies with current information from the LDAP repository.

The success or failure of the policy re-cache operation is reported in the **Status** panel, including an indication of any error that might have occurred, as shown below.




In addition to the **Status** panel, the success or failure of the policy re-cache operation for each switch is reported in the policy.log file, including an indication of any error that might have occurred as shown below. Note that the re-cache operation for each switch occurs in a separate thread and may take some time. Be sure to check the policy.log file for the re-cache status of the "Notify" operation.

Policy Log in the Audit Application