



APPENDIX **Q**

Tools User Interface Reference

These topics describe the pages that are accessed from the Tools menu:

- [Device Properties Page](#), page C-53
- [Policy Object Manager User Interface Reference](#), page F-1
- [Site-to-Site VPN Manager Window](#), page G-2
- [Deployment User Interface Reference](#), page O-1
- [Activity Manager Window](#), page E-1
- [Policy Discovery Status Page](#), page Q-2
- [Inventory Status Window](#), page Q-6
- [Catalyst Summary Information Window](#), page Q-8
- [Device Managers](#), page 21-2
- [IPS Event Viewer](#), page 21-31
- [Apply IPS Update](#), page Q-18
- [Preview Config Dialog Box](#), page O-8
- [Audit Report Page](#), page Q-8
- [Configuration Archive Window](#), page Q-12
- [Backup and Restore](#), page 20-25
- [Administrative Settings User Interface Reference](#), page A-1

Policy Discovery Status Page

Use the Policy Discovery Status page to view the status of policy discovery and device import.

Navigation Path

Select **Tools > Policy Discovery Status**.

Related Topics

- [Understanding Show Containment, page 20-5](#)
- [Viewing Policy Discovery Status Information, page 20-4](#)

Field Reference

Table Q-1 *Policy Discovery Status Page*

Element	Description
Tasks	Provides information and status of the overall discovery or device import task.
Name	The unique task name that you entered in the Discovery Task Name field in the Discover Policies on Device page.
Type	One of the following: <ul style="list-style-type: none"> • Discovery—Initiated from the Discover Policies on Device page. • Device Import—Initiated after you add a new device into Security Manager, then select the Policies and Inventory option.
Start Time	The time the task started.
End Time	The time the task stopped.

Table Q-1 Policy Discovery Status Page

Element	Description
Status	The overall status of the task. One of the following: <ul style="list-style-type: none"> Completed successfully—Discovery or device import task succeeded. Completed with errors—Discovery and device import were partially successful. This could occur if all policies were not discovered or if device import succeeded, but no policies were discovered. Look at the Messages text box for details. Completed with warnings—Discovery and device import were successful but a minor problem occurred. Look at the Messages text box for details. Failed—No policies were discovered or device import failed because of errors or because you stopped discovery.
Refresh button	Refreshes the task list if the tasks are running in the background or new tasks were created.
Delete button	Deletes the selected task from the database.
Discovery Details or Import Details —Depending on the type of task, discovery or device import, this pane is called either Discovery Details or Import Details.	
For a description of the fields in Discovery Details, see Discovery Details Pane, page Q-4 .	
For a description of the fields in Import Details, see Import Details Pane, page Q-5 .	
Messages	Displays messages about the selected device.
Severity	Information about the severity of the problem. An icon for one of the following is displayed: <ul style="list-style-type: none"> Error—A problem was detected. Warning—A minor problem occurred during discovery. Information—Informational message about the selected device.
Description	Details about each message. When you click a message row, detailed information about that message appears in the Description text box.
Action	The steps you can take to resolve the problem.
Close button	Closes the page.
Help button	Opens help for this page.

Discovery Details Pane

If the task type you selected in the Policy Discovery Status page is Discovery, the Discovery Details pane is displayed.

Navigation Path

Select **Tools > Policy Discovery Status**.

Related Topics

- [Policy Discovery Status Page, page Q-2](#)

Field Reference

Table Q-2 *Discovery Details*

Element	Description
Device	The name of each device that was involved in the policy discovery for a selected task.
Severity	An icon for one of the following is displayed: <ul style="list-style-type: none"> • Error—Discovery failed. • Information—Discovery completed successfully.
State	The status of the policy discovery for each device that was involved in the policy discovery for a selected task. Displays one of the following: <ul style="list-style-type: none"> • Discovery Completed—Discovery succeeded and the discovered policies are added to the Security Manager database. • Discovery Failed—No polices were discovered because errors occurred.
Discovered from	One of the following: <ul style="list-style-type: none"> • Live Device—Security Manager contacted the device to obtain configuration and policy information. • File—Security Manager obtained the configuration and policy information from a configuration file.

Import Details Pane

If the task type you selected in the Policy Discovery Status page is Device Import, the Import Details pane is displayed.

Navigation Path

Select **Tools > Policy Discovery Status**.

Related Topics

- [Policy Discovery Status Page, page Q-2](#)

Field Reference

Table Q-3 *Import Details*

Element	Description
Device	The name of each device that was involved in device import and policy discovery for a selected task.
Config File	The location of the configuration file. This field is displayed only if you are importing from a configuration file.
Task Type	One of the following: <ul style="list-style-type: none"> • Import only—Adding devices to Security Manager. • Import and Discover—Adding devices and discovering policies and inventory, or adding devices and discovering policies.
Severity	An icon for one of the following is displayed: <ul style="list-style-type: none"> • Error—Device add failed. • Information—Device was added successfully.
State	The status of the device addition: Device Added or Device Add Failed.

Inventory Status Window

The Inventory Status window displays a summary of device properties for all devices that you are authorized to manage. This summary includes device contact information and all device configurations, indicating which settings are local, which are using a shared policy, and whether any policy-object overrides in effect.

For more information and a procedure on how to filter and export data, see [Understanding Inventory Status, page 20-6](#).

Navigation Path

Select **Tools > Inventory Status**.

Related Topics

- [Credentials Page, page C-57](#)
- [Device Groups Page, page C-59](#)
- [General Page, page C-54](#)
- [Working with Status Providers, page 2-94](#)
- [Understanding Inventory Status, page 20-6](#)
- [Understanding Device Credentials, page 5-43](#)
- [Understanding Device Properties, page 5-51](#)

Field Reference

The Inventory Status window contains two panes. Use the upper pane to view a complete listing of all devices, or to sort the devices by attribute, or to filter out certain ones. Use the lower pane to view the device property details of the selected device in the upper pane.

Table Q-4 *Inventory Status Window*

Element	Description
Device Summary Information for All Devices (Upper Pane)	
Export button	Opens the Export Inventory Status window allowing you to select a directory in the Security Manager server file system in which to store a CSV (comma separated values) file for reference or further study.

Table Q-4 *Inventory Status Window*

Element	Description
Filter	When expanded, displays the filter bar, which enables you to filter the information based on conditions you set. Tables can be filtered according to a particular value in a column (all firewall devices, for example), making it easier for you to reduce the number of visible rows and maintain objects in the tables. For more information, see Filtering Tables , page 3-24.
[Column Headings]	You can click on the column headings in the upper pane to sort the list.
Display Name	Name assigned to the device when it was added to Security Manager.
Status Provider Column(s)	If enabled, up to two status provider columns will appear: Deployment, and Monitoring Center for Performance, displaying status messages according to the interval established in Administrative Settings > Status page. For more information, see Working with Status Providers , page 2-94.
OS Type	The family of the operating system running on the device, for example, IOS, IPS, ASA, FWSM, or PIX.
Running OS Version	The version of the operating system running on the device. “Unknown” indicates OS version not available.
Target OS Version	The target OS version for which you want to apply the configuration.
HostName.Domain Name	The DNS host and domain names for the device.
IP Address	The management IP address of the device.
Device Type	The type of device. For example, if the device is a firewall device, the type of firewall, such as PIX or ASA is displayed.
Device Properties by Device (Lower Pane)	
Inventory	Lists summary information for selected device from upper pane. This list includes parent and device grouping information if applicable.
Policy	Lists the policy types assigned to the device selected in the upper pane.
Policy Object Overrides	Lists policy object overrides by object type for the device selected in the upper pane. For more information on policy object overrides, see Policy Object Override Pages , page C-60.

Table Q-4 *Inventory Status Window*

Element	Description
Status	Lists status providers with any status messages for device selected in the pane. For more information on status providers, see Working with Status Providers, page 2-94 .
Navigation buttons	From left to right, buttons mean jump to first, previous, number in list, next, and last device in the upper pane list. The center button indicates which number device is highlighted (for example 5/10 means the fifth of 10 devices in list).

Catalyst Summary Information Window

The Catalyst 6500/7600 Device Manager (DM-6500/7600) component is embedded in Security Manager. For information, please see [Managing Catalyst Devices, page 16-1](#).

Navigation Path

Highlight a Catalyst 6500/7600 device and select **Tools > Catalyst 6500/7600 Device Manager**.

Audit Report Page

When state changes occur in Security Manager, an audit entry is created. You can display the aggregated results of the audit entries by defining the parameters in the Audit Report page. See [Understanding Audit Reports, page 20-7](#).

Navigation Path

Select **Tools > Audit Report**.

Related Topics

- [Understanding Audit Reports, page 20-7](#)
- [Audit Message Details Dialog Box, page Q-11](#)

Field Reference

The Audit Report page contains two panes. Use the left pane to define the parameters for generating the audit report.

Table Q-5 **Audit Report Page Left Pane**

Element	Description
Search by action (source)	Specify the source or sources of the actions that generate the audit report. Selections include Objects, License, Admin, Firewall, Policy Manager, Devices, Topology, VPN, Config Archive, Deployment, System, and Activity. You can select All to include all action sources.
Search by date	<p>From—The date to begin the audit report search. Click the calendar icon to open a calendar, then select the start date.</p> <p>To—The date to finish the audit report search. Click the calendar icon to open a calendar, then select the end date.</p> <p>This filter's default (reset position) is from the day before.</p>
Search for activity by state	<p>Filters actions by their activity workflow state. If the action has an associated activity, such as, Approved, Created, Discarded, Submitted, Edited and so on, click the arrow in the filter field, then select the activity from the list.</p> <p>Note This field applies only if you are in workflow-enable mode. Only policies and objects can have activities associated to them.</p> <p>Associated activities are a set of actions that you perform on a particular activity. For example, when you assign policies to a device, you create an activity. Later, to make policy changes, you open that activity in the edit state, make the policy changes, then submit it for approval. The approver, before approving or rejecting the activity, might choose to review the proposed policy changes and all the actions (associated activities) performed on that policy, such as, created and edited in this example.</p>
Search by message warning level	The message warning level: Information, Warning, Success, Failure and Internal System Error.
Search by user name	<p>The username of the person who performed the action.</p> <p>For example, if you select Activity in the Actions field, and you know the username of the person who created that activity, enter that name in the username field.</p>

Table Q-5 **Audit Report Page Left Pane**

Element	Description
Search by phrase in the message body	A search string. You can enter a maximum of 1025 characters.
Search by all or part of the object name	A search string. You can enter a maximum of 1025 characters.
Search button	Starts generating the report.
Reset button	Resets or deletes the values in each field.

The right pane displays the audit report with each row being another audit entry or message. The content of the audit report depends on the parameters you defined in the left pane. Therefore, all columns listed in the table might not be displayed in the generated audit report.

Table Q-6 **Audit Report Page Right Pane**

Element	Description
Message Level	Message warning level. These include: Information, Warning, Success, Failure and Internal System Error.
Date	The date and time the action occurred.
Source	The origin of the audit entry: Objects, License, Admin, Firewall, Policy Manager, Devices, Topology, VPN, Config Archive, Deployment, System, and Activity.
Action	The action performed on the category: Add, Assign, Create, Delete, Open, Purge, Unassign, and Update.
Object	The identifier of the action. For example, if the category is device, then the object identifier could be device name or IP address. If the category is deployment, then the object identifier could be job name, job id, and so on.
User Name	The username of the person performing the action.
Activity	The name of the activity.
# of rows per page	The number of rows to display on each page.
< arrow	Returns to the previous page of the audit report.
> arrow	Advances to the next page of the audit report.

Audit Message Details Dialog Box

Use the Audit Message Details dialog box to see details about an audit message. Double-click a message row in the audit report page to display details about that message.

Navigation Path

You can access the Audit Report Details dialog box from the Audit Reports page. To access the Audit Report page, select **Tools > Audit Report**.

Related Topics

- [Audit Report Page, page Q-8](#)
- [Generating the Audit Report, page 20-9](#)

Field Reference

Table Q-7 ***Audit Message Details***

Element	Description
Date	The date and time the action occurred.
User	The username of the person performing the action.
Source	The origin of the audit entry: Objects, License, Admin, PolicyManager, Devices, Cofig Archive, Deployment, System, and Activity.
Action	The action performed on the category: Create, Assign, Purge, and Delete.
Message Level	Message levels: Information, Warning, Success, Failure, and Internal System Error.

Table Q-7 **Audit Message Details**

Element	Description
Associated Activity	<p>The action associated with the activity.</p> <p>Note This field applies only if you are in workflow-enable mode. Only policies and objects can have activities associated to them.</p> <p>Associated activities are a set of actions that you perform on a particular activity. For example, when you assign policies to a device you create an activity. Later, to make policy changes, you open that activity in the edit state, make the policy changes, then submit it for approval. The approver, before approving or rejecting the activity, might choose to review the proposed policy changes and all the actions (associated activities) performed on that policy such as created and edited in this example.</p>
Object Id	The identifier of the category. For example, if the category is device, the object identifier could be device name or IP address. If the category is deployment, the object identifier could be job name, job id, and so on.
Description	Describes the operation.
Top and bottom arrows	<p>Moves to the previous or next audit message:</p> <ul style="list-style-type: none"> • The top arrow advances you to the previous audit message (up). • The bottom arrow advances you to the next audit message (down).
OK button	Closes the dialog box.

Configuration Archive Window

Configuration Archive stores configuration versions for each device managed by Security Manager.



Note Security Manager does not support the archiving of VLAN configurations.

You can use Configuration Archive to:

- View the transcript of a configuration deployment for a selected device.
- View and compare configuration versions.
- View CLI differences between deployed configuration versions.
- Rollback to an earlier configuration version, provided that the configuration originated from the device. For more information see [Using Rollback to Deploy Archived Configurations](#), page 20-15.
- Retrieve a current running device configuration.

The Configuration Archive window lists device configuration versions that have been added to the archive. You can view and sort the configuration file versions by certain criteria as shown in [Table Q-8 on page Q-14](#). You can view and compare configuration versions for a specific device. You can also view deployment transcripts and delta configurations. For detailed procedures, see [Using the Configuration Archive Tool](#), page 20-11.

Navigation Path


Select **Tools > Configuration Archive**.

Related Topics

- [Configuration Version Viewer](#), page Q-15
- [Transcript Viewer Window](#), page Q-17
- [Defining Configuration Archive Settings](#), page 2-62
- [Using the Configuration Archive Tool](#), page 20-11
- [Customizing the Configuration Archive Toolbar](#), page 20-12
- [Viewing Transcripts](#), page 20-13
- [Viewing and Comparing Configurations](#), page 20-14
- [Using Rollback to Deploy Archived Configurations](#), page 20-15
- [Understanding Rollback for Devices in Multiple Context Mode](#), page 20-18
- [Understanding Rollback for Failover Devices](#), page 20-18
- [Understanding Rollback for Catalyst 6500/7600](#), page 20-19
- [Understanding Rollback for IPS and IOS IPS](#), page 20-19
- [Adding Configuration Versions from a Device to the Archive](#), page 20-23

Field Reference

Table Q-8 Configuration Archive Window

Element	Description
Version ID	The version number of the configuration version.
Created On	The date and time that the configuration version was archived.
Created By	The user ID or system ID associated with adding the configuration version to Configuration Archive.
Archival Source	The origin of the archiving event (for example, User Request, Job Name).
Creation Comment	Information about the configuration version created.
Transcript Icon	When double-clicked, displays a transcript of a configuration version that deployed to a device. A transcript is the log file of Security Manager server and device transactions captured during a deployment or rollback operation. It includes commands sent and received between server and device from the time of deployment or rollback request.
View button	<p>Opens the configuration version viewer in which you can view or compare selected configuration versions for a device.</p>  <p>Note Configuration files deployed to Catalyst 6000/7600 series devices will appear as two entries in Configuration Archive due to deployment constraints of those device types. These are duplicates of the same version, <i>not</i> separate configuration versions.</p>
Rollback button	Rolls back to the selected configuration version, provided that the configuration originated from the device. For more information see Using Rollback to Deploy Archived Configurations, page 20-15 .
Add from Device button	<p>Enables you to retrieve a current configuration from a device and add it to the archive for that device. This is useful for any device whose configuration might have been changed directly in its CLI.</p> <p>For more information on adding configuration versions, see Adding Configuration Versions from a Device to the Archive, page 20-23.</p>

Transcript Viewer

Table Q-8 **Configuration Archive Window (continued)**

Element	Description
Viewing Area	Opens when the Transcript icon is double-clicked. The viewing area contains text of a transcript file created during the roll back of a configuration or a message stating that no transcript is available. If a configuration was added to the archive from a file, no transcript is available.

Configuration Version Viewer

From the Configuration version viewer you can view full and delta configuration versions line by line for a selected device. You can compare any version to any other version in the archive for a selected device. The selected version appears in the left pane, and you can select another version for comparison from the list on the upper right of this window. For information on viewing full and delta configuration versions, see [Viewing and Comparing Configurations, page 20-14](#).

Navigation Path

Select **Tools > Configuration Archive** select a configuration and click **View**.

Related Topics

- [Configuration Archive Window, page Q-12](#)
- [Transcript Viewer Window, page Q-17](#)
- [Viewing and Comparing Configurations, page 20-14](#)
- [Adding Configuration Versions from a Device to the Archive, page 20-23](#)

Field Reference

Table Q-9 Configuration Version Viewer Window

Element	Description
Version ID	<p>Lists the configuration versions that are available for the selected device. You can select a version for viewing in the left pane.</p> <ul style="list-style-type: none"> • Previous—Displays the version in the sequence before the one showing. • Next—Displays the version in the sequence after the one showing. • Last—Displays the last version in the list. • Version <i>n</i>—Displays the version in the sequence by ID.
Compare with version	<p>Lists the configuration versions that are available for the selected device. You can select a version for viewing in the right pane.</p> <ul style="list-style-type: none"> • Previous—Displays the version in the sequence before the one showing in the left pane. • Next—Displays the version in the sequence after the one showing in the left pane. • Last—Displays the last version in the sequence. • Version X—Displays the version by ID.
Config Type	<p>Types of configurations that are available for viewing:</p> <ul style="list-style-type: none"> • Full Configuration—The full configuration for the selected device as saved in the Configuration Archive. You can compare full configurations for a device. • Delta Configuration—The file that is generated by Security Manager during deployment and that represents policy changes between the configuration selected in the Version ID field and the most recently deployed version. <p>Note Configuration versions resulting from out-of-band changes (for example, in the CLI) can be added to Configuration Archive using Add from Device, but no delta configuration file is generated.</p>
Left pane	Displays the configuration version that you selected in the Configuration Archive window or from the Version ID list.
Right pane	Displays the configuration version that you selected in the Configuration Archive window or from the Compare with version list.

Table Q-9 Configuration Version Viewer Window (continued)

Element	Description
Line Numbers	Configuration text line numbers.
First Difference button	Moves the view of the config forward or backward to the next difference. Note Text is color-coded to show the type and number of changes according to legend to the right of change indicator buttons.
Previous Difference button	Moves the cursor to the previous difference noted between the configuration versions.
Current Difference button	Using the cursor, focuses on the currently selected difference in the window.
Next Difference button	Moves the cursor to the next difference noted between the configuration versions.
Last Difference button	Moves the cursor to the last difference noted between the configuration versions.
Transcript View button	Opens the transcript viewer window.
Print button	Prints the configuration.

Transcript Viewer Window

A transcript is the log file of Security Manager server and device transactions captured during a deployment or rollback operation. It includes commands sent and received between server and device from the time of deployment or rollback request. For more information, see [Viewing Transcripts, page 20-13](#).

Navigation Path

Select **Tools > Configuration Archive** then in the Device selector, click the device for which you want to view a transcript and double-click the **Transcript** icon.

Related Topics

- [Configuration Archive Window, page Q-12](#)
- [Configuration Version Viewer, page Q-15](#)

- [Viewing Transcripts, page 20-13](#)

Field Reference

Table Q-10 **Transcript Viewer Window**

Element	Description
Version Id	Lists the configuration versions that are available for the selected device. You can select a version for viewing in the left pane. <ul style="list-style-type: none"> • Previous—Displays the version in the sequence before the one showing. • Next—Displays the version in the sequence after the one showing. • Last—Displays the last version in the list. • Version <i>n</i>—Displays the version in the sequence by ID.
Transcript Type	Identifies the type of transcript viewed.
Transcript Window	Displays the selected transcript details.
View button	Displays the transcript data.
Print button	Prints the transcript data.

Apply IPS Update

The Apply IPS Updates wizard allows you to *manually* apply image and signature updates to compatible IPS devices. Step-by-step details on the Apply IPS Updates wizard are contained in this topic.



Note

Automatic updates can be configured via **Tools > Security Manager Administration > IPS Updates**. For details on automatic updates, refer to [IPS Updates Page, page A-19](#).

When applying signature updates, the wizard displays those signatures in the update that are not configured on the target IPS devices. In this view, you can configure the new signatures before they are applied.

When applying image and signature updates, only those devices to which the updates can be applied are available for selection. Inapplicable devices are grayed out.

**Caution**

If you did not set Category CLI commands on your IOS IPS device to select a subset of IPS signatures that the device will attempt to compile, Security Manager will push CLI commands to enable the IOS IPS Basic category to prevent the device resources from being overloaded. These CLI commands are not managed by Security Manager after they are deployed. You can change these manually on the device to select another set of signatures to compile.

Navigation Path

Select **Tools > Apply IPS Updates**.

Related Topics

- [Administering IPS Update Settings, page 2-77](#)
- [IPS Updates Page, page A-19](#)

Field Reference

The Apply IPS Updates Wizard has three steps:

- [Apply IPS Updates Wizard: Step 1: Select Update to Apply Page](#)
- [Apply IPS Updates Wizard: Step 2: Select Policies Update will be Applied To Page](#)
- [Apply IPS Updates Wizard: Step 3: Edit Signatures Page](#)

**Tip**

The **Type** field in Step 2 of the Apply IPS Updates Wizard identifies which policies (devices) the selected update should be applied to: local signature policies or shared signature policies. These are explained in [Apply IPS Updates Wizard: Step 2: Select Policies Update will be Applied To Page](#).

Table Q-11 **Apply IPS Updates Wizard: Step 1: Select Update to Apply Page**

Element	Description
Updates Downloaded	<p>Displays the name of either the signature update or sensor update package.</p> <ul style="list-style-type: none"> • Sensor Updates. Displays the filename, the major, minor, and service pack, and patch versions, as well as the supported engine release. You must apply all major sensor updates, however, minor updates are cumulative. • Signature Updates. Displays the filename, the signature number, and the supported engine release. Signature updates are cumulative; however, applying them as separate packages allows you to separate your work into more manageable units if you intend to tune the updates to match the specific needs of your network. <p>The update packages appearing in this list are either:</p> <ul style="list-style-type: none"> • auto downloaded from the update server, as configured under the Update Server on the Tools > Security Manager Administration > IPS Update page • manually downloaded and placed in the <code>CSCOpX\MDC\ips\updates</code> folder of the Security Manager server.
Type	Select between Sensor Update and Signature Update. Selection determines which updates appear in the Updates Downloaded list.
Update Details	Lists the filename, description, release number, release date, file size, and required engine level for the package selected in the Updates Downloaded list.
Update Status	<p>Lists the following:</p> <ul style="list-style-type: none"> • name of most current update returned by Check for Updates • name of most current update downloaded to the Security Manager server • name of most recent update applied to device configuration in Security Manager • name of most recent update deployed to real device • last time the list of available updates was requested in month day, year hour:minute:second format. • last time a new update was downloaded in month day, year hour:minute:second format. • last time an update was deployed

Table Q-11 **Apply IPS Updates Wizard: Step 1: Select Update to Apply Page**

Element	Description
Check For Updates button	Manually retrieves the list of updates from either Cisco.com or a local HTTP server, as configured under the Update Server on the Tools > Security Manager Administration > IPS Updates page. The type of updates that are checked for depends on the option selected under Type. This list is a read-only version of the updates available for download. To download the updates, you must click Download Latest Updates.
Download Latest Updates button	Retrieves the update packages from either Cisco.com or a local HTTP server, as configured under the Update Server on the Tools > Security Manager Administration > IPS Updates page. This list includes all updates available since the last time updates were downloaded, whether that download was manually initiated or occurred as part of an automatic download.
Next button	Advances to the Select Policies Update will be Applied To page in the wizard.
Cancel button	Closes the wizard and discards your changes.

Table Q-12 **Apply IPS Updates Wizard: Step 2: Select Policies Update will be Applied To Page**


Element	Description
Apply Updates to	Select the local signature policies (representing devices not assigned to any shared signature policy) and/or shared signature policies that the selected update from Step 1 should be applied to. Inapplicable devices are grayed out.
Type	<p>Identifies which policies (devices) the selected update should be applied to.</p> <ul style="list-style-type: none"> Local Signature Policies: They represent devices not assigned to any shared signature policy. Inapplicable devices are grayed out and not selectable. Shared Signature Policies: If a shared signature policy is selected, all devices assigned to the shared signature policies are selected and will be shown on the right hand side panel. Inapplicable devices from the shared signature policy are grayed out. <p> Tip After you make this selection, the signature summary table appears. You can pre-tune the signatures in this table by right-clicking on a particular row (a particular signature).</p>
Select All button	Selects all options in the Apply Updates to list.
Deselect All button	Clears any selections in the Apply Updates to list.
Devices Assigned to Selected Policies	Displays a read-only list of the devices assigned to the selected local or shared signature policies.
Back button	Returns to Select Update to Apply page.
Next button	Advances to the Edit Signatures page in the wizard. It can only be used when the selected update is a signature update package. If you do not plan to edit/tune any signature before update, then you can click on Finish without clicking this button.
Finish button	Apply the selected update to the selected device(s). If the selected update is a signature update package and you want to edit/tune signature(s), click on the Next button instead of this button.
Cancel button	Closes the wizard and discards your changes.

Table Q-13 **Apply IPS Updates Wizard: Step 3: Edit Signatures Page**

Element	Description
Filter	Allows you to restrict the set of signature displayed in the list base on values contained in one of the signature fields, such as ID, name, risk rating, or engine.
Apply button	Applies the selected filter criteria to the list of signatures displayed in the Signature List.
Clear button	Removes the filter from the list of signatures displayed in the Signature list.
Signature List	<p>Display the new and modified signatures between the signature level of the selected update and the lowest signature level among the selected devices.</p> <p>This list displays the following information about each signature:</p> <ul style="list-style-type: none"> • ID • Sub • Name • Actions • Severity • Fidelity • Source • Enabled • Risk Rating • Retired • Obsolete • Engine • Status: a delta indicates it is a modified signature; a star indicates it is a new signature. <p>For details on available signature information, see Signature Summary Table, page N-2. In the Signature Summary Table, you can also add custom signatures and delete signatures, but you cannot do that on this page (Edit Signatures) of the Apply IPS Updates Wizard.</p>
Back button	Returns to Select Policies page.

Table Q-13 ***Apply IPS Updates Wizard: Step 3: Edit Signatures Page***

Element	Description
Cancel button	Closes the wizard and discards your changes.
Finish button	Applies the selected update to the selected device(s), and saves the edited/tuned signature, if any.