



## Using Map View

---

The following topics describe how to use the Map view:

- [Understanding Maps and Map View, page 35-1](#)
- [Working With Maps, page 35-8](#)
- [Displaying Your Network on the Map, page 35-14](#)
- [Managing VPNs in Map View, page 35-20](#)
- [Managing Device Policies in Map View, page 35-22](#)

## Understanding Maps and Map View

The Security Manager Map view provides a graphical view of your VPN and Layer 3 network topology.

Using the map view, you can investigate details of your VPN configuration graphically. Topological display of tunnels enables you to easily derive the relationship among multiple VPN configurations (for example, a hierarchical VPN). You can group devices to achieve a more complete picture of your VPN configuration. This is useful in situations where a hub failover pair is a peer with hundreds of spokes.

You can represent your Layer 3 network topology graphically, populating it with managed devices (called device nodes). You can make the picture of the topology more complete by adding unmanaged objects (called map objects) such as devices, clouds, and networks. For large networks, you can choose to simplify the topology graph by incorporating only a portion of the overall topology. You can save the topology maps for future use.

You can save multiple topology maps to reflect your network's geographical or functional organization. You can link a saved map to a node on a parent map, so that from the parent map you can drill down to the linked map with more detailed information (for more information, see [Using Linked Maps, page 35-13](#)). Saved maps are shared among all users who have the necessary access privileges.

You can launch other Security Manager features from the map view. In some cases, you can simplify the use of features by selecting nodes from the map before you start another feature. For example, you can select multiple nodes, then create a VPN that includes those nodes as members.



**Tip**

---

The network data that is displayed on maps is typically updated as this data changes. However, to be certain that a map displays current network data, you can refresh it manually by selecting **Map > Refresh Map**.

---

This section contains the following topics:

- [Understanding the Map View Main Page, page 35-2](#)
- [Map Toolbar, page 35-4](#)
- [Using the Navigation Window, page 35-4](#)
- [Maps Context Menus, page 35-5](#)
- [Access Permissions for Maps, page 35-8](#)

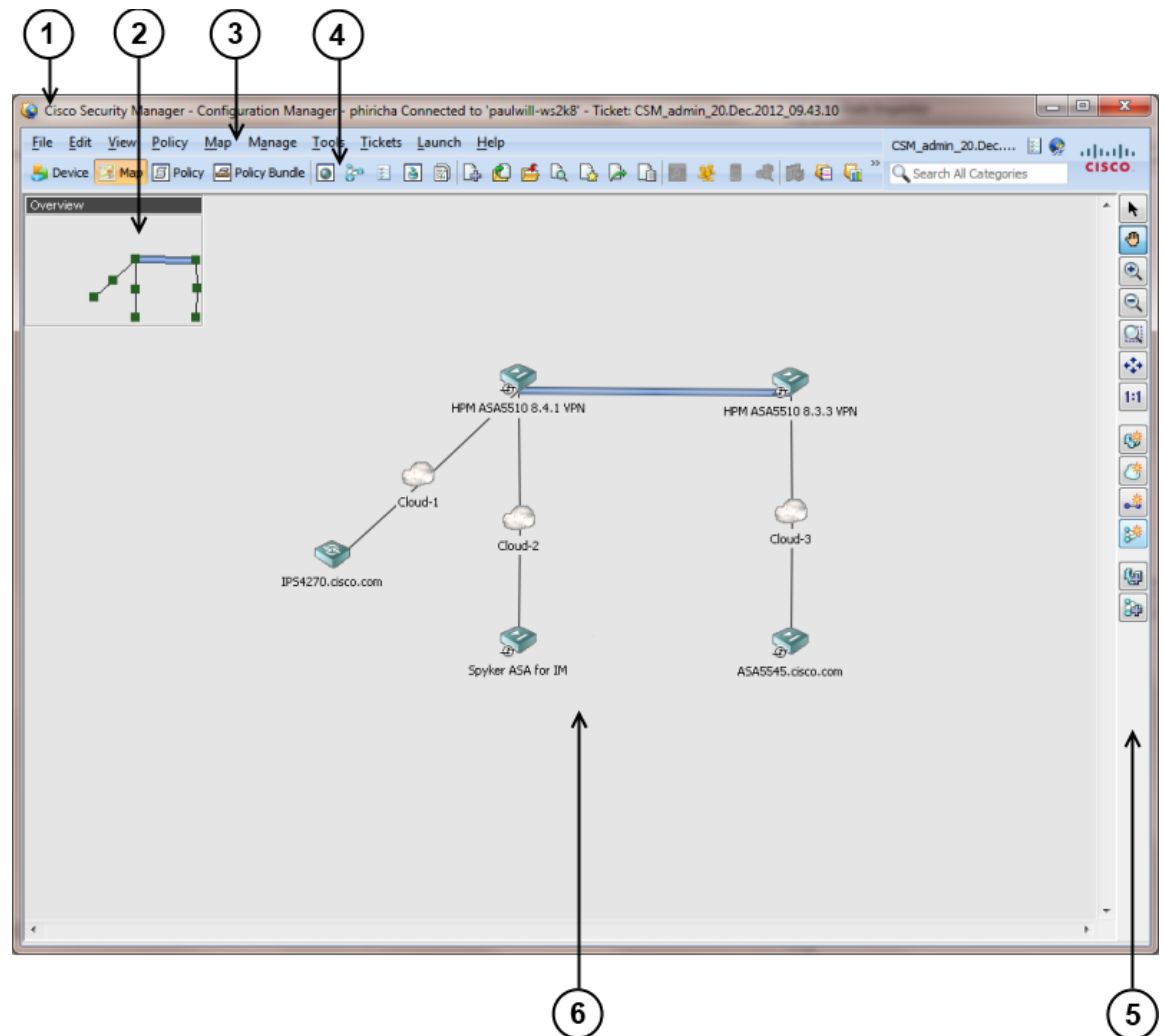
## Understanding the Map View Main Page

Map view enables you to create customized, visual topology maps of your network, within which you can view connections between your devices and easily configure VPNs and access control settings. The following figure identifies the functional areas of the Map view.

To open the Map view main page, click the **Map View** button in the toolbar.

You can undock the map window, which enables you to use other product features while keeping the map open. To undock the map, select **Map > Undock Map View**. To dock the map window, select **Map > Dock Map View**.

Figure 35-1 Map View Main Page



1	Title bar	2	Navigation window (see <a href="#">Using the Navigation Window, page 35-4</a> )
3	Menu bar (see <a href="#">Map Menu (Configuration Manager), page 1-33</a> )	4	Toolbar (see <a href="#">Toolbar Reference (Configuration Manager), page 1-39</a> )
5	Map toolbar (see <a href="#">Map Toolbar, page 35-4</a> )	6	Map (see <a href="#">Understanding Map Elements, page 35-14</a> )














### Related Topics

- [Understanding Maps and Map View, page 35-1](#)
- [Working With Maps, page 35-8](#)
- [Displaying Your Network on the Map, page 35-14](#)
- [Managing VPNs in Map View, page 35-20](#)
- [Managing Device Policies in Map View, page 35-22](#)

## Map Toolbar

The following table describes the buttons on the map toolbar.

**Table 35-1** Map Toolbar

Toolbar Button	Description
	Selects objects on the map. Click the button, then click items on the map.
	Pans the map. Click the button, click and hold on the map, then drag the cursor.
	Zooms in on the map.
	Zooms out from the map.
	Zooms the map to fill a rectangle that you draw.
	Zooms the map to include the entire map.
	Zooms the map to actual size.
	Creates a new Security Manager-managed node. After you create the new device in the inventory, it is added to the active map as a device node.
	Adds a new map object to the map.
	Adds a new link to the map.
	Creates a new VPN connection between nodes on the map.
	Select devices to show on the map as device nodes.
	Select VPNs to show on the map.

## Using the Navigation Window

The navigation window displays a smaller version of the entire active map. The shaded rectangle defines the area of the map that is currently displayed.

Use the navigation window to select the portion of the map to view and to change the map zoom level.

- To toggle the display of the navigation window, select **Map > Show/Hide Navigation Window**.
- To pan the navigation control to select which portion of the map to display, click within the shaded rectangle and drag it to a new location.
- To change the zoom level, click one of the resizing handles in the corners of the shaded rectangle, then drag it to increase or decrease the area of the map to display. The map zooms to display the area covered by the map indicator.

The title bar in the navigation window displays the name of the map. If the map has unsaved changes, an asterisk (\*) appears next to the map name.

For information on other ways to pan and zoom maps, see [Panning, Centering, and Zooming Maps](#), page 35-11.

## Maps Context Menus

The following topics describe the menus that contain maps commands. To open the context menus, right-click map elements.

- [Managed Device Node Context Menu](#), page 35-5
- [Multiple Selected Nodes Context Menu](#), page 35-6
- [VPN Connection Context Menu](#), page 35-6
- [Layer 3 Link Context Menu](#), page 35-7
- [Map Object Context Menu](#), page 35-7
- [Map Background Context Menu](#), page 35-7

## Managed Device Node Context Menu

The Managed Device Node context menu opens when you right-click a map node that represents a managed device. The commands that you see depend on the type of device you select. The following table lists all commands that you might see.

**Table 35-2** *Managed Device Node Context Menu*

Menu Command	Description
Edit Firewall Policies	Edits firewall policies on the device. Select a firewall policy type from the submenu to edit it.
Edit Firewall Settings	Edits firewall settings on the device. Select a setting from the submenu to edit it.
Edit VPN Peers	Edits peers in VPNs in which the device participates.
Edit VPN Policies	Edits VPN policies on the device.
Device Properties	Displays device properties.
Clone Device	Creates a copy of the device. See <a href="#">Cloning a Device</a> , page 3-57.
Copy Policies Between Devices	Copies policies between the device and other devices. See <a href="#">Copying Policies Between Devices</a> , page 5-33.
Share Device Policies	Shares device local policies.
Catalyst Summary Info	Allows you to view high-level system information, including any service modules, ports, and VLANs that Security Manager has discovered. See <a href="#">Viewing Catalyst Summary Information</a> , page 68-2.
Show in Device View	Opens the Device View for the selected device.
Device Manager	Launches the Device Manager. See <a href="#">Starting Device Managers</a> , page 72-14.

**Table 35-2** *Managed Device Node Context Menu (continued)*

Menu Command	Description
Inventory Status	Displays the Inventory Status window for the device. See <a href="#">Inventory Status Window</a> , page 72-13.
Show VPN Peers	Shows peers in VPNs in which the device participates.
Preview Configuration	Previews the device configuration with all committed changes included.
Show Containment	Shows the security contexts and service modules in devices that have them.
Node Properties	Displays node properties.
Set Linked Map	Creates a link from this node to another map.
Open Linked Map	Opens the map that is linked to the node.
Discover Policies on Device	Discovers policies on the device.
Move To Center	Pans the map to display the node in the center.
Delete Device	Deletes the device from the device inventory.
Remove from Map	Removes the node from the map.

## Multiple Selected Nodes Context Menu

The Multiple Selected Device Node context menu opens when you select more than one map node, then right-click on a selected node.

If all of the selected nodes are not VPN-capable, the commands to configure VPNs do not appear.

**Table 35-3** *Multiple Selected Nodes Context Menu*

Menu Command	Description
Create Point to Point VPN	Creates a point to point VPN between two selected devices. All selected nodes must be managed and VPN-capable.
Create Hub and Spoke VPN	Creates a hub and spoke VPN that includes the selected nodes. The node that you right-click becomes the VPN hub. All selected nodes must be managed and VPN-capable.
Create Meshed VPN	Creates a full mesh VPN that includes the selected nodes. All selected nodes must be managed and VPN-capable.
Remove Selected Nodes	Removes all selected device nodes. Appears only if you right-click on a selected device node.
Delete Map Objects	Deletes all selected map objects. Appears only if you right-click on a selected map object.

## VPN Connection Context Menu

The VPN Connection context menu opens when you right-click on a VPN connection on the map. For more information, see [Editing VPN Policies or Peers From the Map](#), page 35-22.

**Table 35-4 VPN Connection Context Menu**

Menu Command	Description
Edit VPN Peers	Edits the peers in the VPN.
Edit VPN Policies	Edits the VPN policies.

## Layer 3 Link Context Menu

The Layer 3 Link context menu opens when you right-click on a layer 3 link on the map.

**Table 35-5 Layer 3 Link Context Menu**

Menu Command	Description
Link Properties	Displays the link properties.
Delete Link	Deletes the link from the map.

## Map Object Context Menu

The Map Object context menu opens when you right-click a map object that does not represent a managed device.

**Table 35-6 Map Object Context Menu**

Menu Command	Description
Node Properties	Displays the node properties.
Move To Center	Pans the map to display the node in the center.
Set Linked Map	Links the node to a map.
Open Linked Map	Opens the map to which the node is linked.
Delete Map Object	Deletes the map object.

## Map Background Context Menu

The Map Background context menu opens when you right-click in the background area of a map, that is, not on any object or link.

**Table 35-7 Map Background Context Menu**

Menu Command	Description
Show Devices on Map	Selects the managed devices to show on the map.
Show VPNs on Map	Selects the VPNs to display on the map.
Add Map Object	Adds a map object to the map.
Add Link	Adds a Layer 3 link to the map.
New Device	Creates a new managed device and adds it to the map as a device node.
New VPN	Creates a new VPN and adds it to the map.
Find Map Node	Finds nodes on the map.

**Table 35-7** *Map Background Context Menu (continued)*

Menu Command	Description
Open Map	Opens a saved map.
Save Map	Saves the open map.
Show/Hide Navigation Window	Toggles the display of the navigation window on the map.
Map Properties	Displays the properties of the map.
Hierarchical layout	Arranges the network nodes in a hierarchical layout.
Radial layout	Arranges the network nodes in a radial layout.
Circular layout	Arranges the network nodes in a circular layout.
Dock/Undock Map	Undocks the Map view.

## Access Permissions for Maps

Access to maps is controlled based on two systems of user privileges:

- Device privileges—You must have at least read privileges to all the devices in a map to open the map.
- Map privileges—Access to maps is based on your Security Manager user role. There are two levels of map access:
  - Read-only—You can open maps, but you cannot modify them. If you have this map privilege level, the features for modifying maps are not available.
  - Read-write—You can modify maps. All map modification features are available.

## Working With Maps

A map is a representation of a portion of your network. You can create and save multiple maps to address your network management needs. To work with any map, you must be in Map view (select **View > Map View**).

After you create and save a map, the map is available to all users on the system that have at least read privileges to all the devices on the map. Users that do not have read privileges to a device on a map do not see the map in the list of existing maps when they try to open a map. For more information, see [Access Permissions for Maps, page 35-8](#).

You can only have one map open at a time. If a map is open and you create a new map or open an existing map, you are prompted to save or discard any unsaved changes that you made to the current map.

Multiple users can open and modify a map at the same time. When a user saves changes to a map, any other users who are using the map are notified and have the option to do one of the following:

- Update their map to the version saved by the other user, losing any changes they have made.
- Save their version of the map as a new map, preserving any changes they made.

This section contains the following topics:

- [Creating New or Default Maps, page 35-9](#)
- [Opening Maps, page 35-10](#)



- [Saving Maps](#), page 35-10
- [Deleting Maps](#), page 35-10
- [Exporting Maps](#), page 35-11
- [Arranging Map Elements](#), page 35-11
- [Panning, Centering, and Zooming Maps](#), page 35-11
- [Selecting Map Elements](#), page 35-12
- [Searching for Map Nodes](#), page 35-12
- [Using Linked Maps](#), page 35-13
- [Setting the Map Background Properties](#), page 35-13

## Creating New or Default Maps

You have two options for creating a new map:

- Create an empty map—To create a new empty map, select **Map > New Map**. You must already be in Map view (select **View > Map View**). If you currently have a map open with unsaved changes, you are asked if you want to save it. For information about adding elements to a map, see [Displaying Your Network on the Map](#), page 35-14.
- Create a new map containing all managed devices and VPNs in the inventory—This is called the default map. Generating the default map is a good way to create a map. After generating the map, save it with a unique name to make it a standard map and modify it as desired.

You can generate the default map whenever you want to, and it contains the inventory as it exists at the time you generate it. You cannot specifically save the default map *as* the default map; it is regenerated every time you select it.

The following procedure explains how to create a new map using the default map.

### Tips

- If you refresh the map (select **Map > Refresh Map**), items that you added to the inventory after generating the default map are not added to the map. You must reopen the default map to see new devices.

---

**Step 1** In Map view, select **Map > Open Map**.

**Step 2** Select **Default Map** from the Available Maps list, then click **OK**.



**Note** If you do not have sufficient access rights to all devices in the inventory, the default map that opens shows only the subset of devices for which you do have access rights. For more information, see [Access Permissions for Maps](#), page 35-8.

---

**Step 3** To save the default map as a standard map, select **Map > Save Map** or **Map > Save Map As**, enter a name for the map and click **OK**.

---

## Opening Maps

To open an existing map, select **Map > Open Map**, select the desired map from the list of available maps, and click **OK**. You must already be in Map view (select **View > Map View**). If you currently have a map open with unsaved changes, you are asked if you want to save it.

The list of available maps includes a special map called the **Default Map**. This map contains all of the managed devices and VPNs in the inventory. You are essentially creating a new map each time you open it. For more information about the default map, see [Creating New or Default Maps, page 35-9](#).

**Tip**

You can open any map that you have created or the default map. You can also open any map that another user has created provided you have the requisite permission settings with regard to the devices shown on that map (see [Access Permissions for Maps, page 35-8](#)).

**Related Topics**

- [Working With Maps, page 35-8](#)
- [Understanding Map Elements, page 35-14](#)

## Saving Maps

To save the active map, select **Map > Save Map**. Any changes that you made since you last saved it are saved. If you did not save the map previously, the Save Map As dialog box opens, enabling you to assign a name to the map and save it.

To save a map under a new name, select **Map > Save Map As**. The map name can be as long as 256 characters, but cannot be the reserved names “Default Map” or “New Map.”

If you close a map that contains unsaved changes, you are prompted to save the changes.

If your Security Manager session closes automatically because of inactivity when a map is open with unsaved changes, the current version of the map is saved if it has a name. If you have not yet saved the map, the map is discarded. For example, if you generate the default map, or create a new map, and do not save it before your session times out, you cannot retrieve that map.

## Deleting Maps

If you no longer need a map, you can delete it (presuming that you have edit permission). Deleting a map does not delete any devices or VPNs shown on the map, nor does it delete or modify their configurations; only the map is deleted.

When you delete a map, it is permanently deleted from the server. Other users cannot use the deleted map.

To delete a map, select **Map > Delete Map**, select the map you want to delete from the available maps list and click **OK**. You are asked to confirm the deletion.

You must already be in Map view (select **View > Map View**) to delete a map.

## Exporting Maps

When viewing a map, you can export the map to a scalable vector graphics (SVG) image file for use outside of Security Manager.

### Related Topics

- [Working With Maps, page 35-8](#)
- [Understanding Map Elements, page 35-14](#)

- 
- Step 1** Select **Map > Export Map**. The Export Topology Map to SVG dialog box opens.
- Step 2** Browse to the location in which to save the file.
- Step 3** Enter a filename in the File name field. The correct file extension will be added for you.
- Step 4** Click **Save**.
- 

## Arranging Map Elements

To move a map element, click and hold, then drag it to the desired position. Attached links move automatically, but the other end of the link remains where it is.

You can also automatically arrange the network nodes on the map in several predefined layouts. Only nodes that are already displayed on the map are arranged. Any nodes that you later add do not follow the layout.

To select a map layout, right-click the map background, then select one of the following layouts from the map context menu:

- Hierarchical Layout—Arranges the nodes in a hierarchical layout.
- Radial Layout—Arranges the nodes in a radial layout.
- Circular Layout—Arranges the nodes in a circular layout.

## Panning, Centering, and Zooming Maps

There are many options for navigating maps. You can pan the map (move around in the map without changing the zoom level), pan a map so that a particular map element is centered in your view, or zoom in or out to see a different map extent.

### To pan a map without changing the zoom level:

- Click the Pan Map toolbar button, then click and hold anywhere on the map and drag the cursor.
- Use the vertical and horizontal scroll bars that are available if the entire map does not fit in the visible page.
- Click and drag the shaded rectangle in the navigation window.
- To center the display of the map on a particular map element, right-click the element, then select **Move to Center**.

**To zoom in or out of a map:**

- To change the zoom level of the map in predefined increments:
  - To zoom in on the map, select **Map > Zoom In**, or click the **Zoom In** toolbar button.
  - To zoom out from the map, select **Map > Zoom Out**, or click the **Zoom Out** toolbar button.
- To zoom into a specific area of the map, click **Zoom Rectangle** in the map toolbar, then click the map and drag a rectangle around the area. When you release the mouse button, the map zooms to display the area defined by the rectangle.
- Alternatively, to zoom in to or out of a specific area of the map, click and drag the corner of the shaded rectangle in the navigation window.
- To display the entire map, select **Map > Fit to Window**.
- To display the map at actual size, select **Map > Display Actual Size**.

**Related Topics**

- [Using the Navigation Window, page 35-4](#)

## Selecting Map Elements

The following table describes how to select map elements. If the selected element contains other elements (for example, a Catalyst switch that contains an FWSM), the containment relationship is shown. For more information, see [Showing Containment of Catalyst Switches, Firewalls, and Adaptive Security Appliances, page 35-16](#).

**Table 35-8**      *Selecting Network Elements*

To select...	Do the following
A single map element	Click the element.
Multiple noncontiguous map elements	Ctrl+click each element.
Multiple contiguous map elements	Click the map and drag a rectangle that includes the elements.

## Searching for Map Nodes

To search for a map node to help you find it in the active map, select **Map > Find Map Node**. This command opens the Find Node dialog box.

The Find Node dialog box initially lists all objects on the map. Use the fields above the list to filter it (the list shows only objects that satisfy all filter criteria). When you find the desired node, select it in the list and click **OK** to have the node centered and selected in the map.

To filter the list, you can:

- Select a node type from the **Type** list to show only objects of that type.
- Enter the name, or at least the initial characters of the name, in the **Name** field. The list is filtered as you type. Your search term must be from the start of the object name. You cannot use wildcard characters.
- Enter all or part of the IP address or subnet mask. The list is filtered as you enter information.

## Using Linked Maps

A linked map is a map that you associate with a map element on another map. Because it is not practical to include all the nodes on a large network in a single map, you can use linked maps to create a hierarchical topology of your network.

You cannot link a node to the another node in the same map.

### Before You Begin

You must create the map to link to before you can link to it.

- 
- Step 1** Right-click the map element to which to link a map, then select **Set Linked Map**. The Set Linked Map dialog box opens.
- Step 2** Select a map to associate with the selected map element, then click **OK**.
- Step 3** To open the linked map, right-click the linked node, then select **Open Linked Map**. The current map closes and the linked map opens.
- 

## Setting the Map Background Properties

You can change the background of a map by changing the color or by configuring an image. A suggested use for a background image is to use an image that represents a geographic area. Then you can position map elements according to their geographic locations.

Some background images are included with Security Manager. You can also transfer images to the server to use as background images. You can use background images of the following file formats: JPEG, GIF, PNG, IVL, and SVG. If you want to use a new image, copy the image file to the Security Manager server file system by connecting directly to the server. For security reasons, Security Manager does not provide a method of transferring files to the server.

To configure the map background, in Map view, select **Map > Map Properties** to open the Map Settings dialog box.

- To configure a background image, select it in the file list. (Select **none** to remove the map's background image.)

If the image is not listed, click **Add** and browse to the file you placed on the server using the Import Background Image dialog box. Click **OK** to have Security Manager add it to the list of available background images.

If you no longer need a listed image, select it and click **Delete**.



### Tip

---

You can control the position and scale of the image using the X and Y coordinates and scale settings. The X,Y source point is the upper left corner of the image. You can use positive or negative numbers. You must experiment to get the results you desire. The scale setting is in percentage.

---

- To change the background color, click **Select** next to the background color field and choose the desired color.

# Displaying Your Network on the Map

You use the map view to represent your network topology by creating maps. A map is a visual representation of your network, or a portion of it if it is too large to fit on a single map. Maps consist of map elements that represent devices, links, and other objects in your network. For more information about map, see [Working With Maps, page 35-8](#).

The following topics describe how to create maps:

- [Understanding Map Elements, page 35-14](#)
- [Displaying Managed Devices on the Map, page 35-16](#)
- [Showing Containment of Catalyst Switches, Firewalls, and Adaptive Security Appliances, page 35-16](#)
- [Using Map Objects To Represent Network Topology, page 35-17](#)
- [Creating and Managing Layer 3 Links on the Map, page 35-19](#)






## Understanding Map Elements

All objects that can appear on a map are map elements. You display map elements on a map to create a representation of a portion of your network. For more information about maps, see [Working With Maps, page 35-8](#). To open a map, see [Opening Maps, page 35-10](#).






The following tables describe the elements that can appear on a map:

- [Table 35-9 on page 35-14](#) describes the device nodes that can appear on a map. These elements are managed by Security Manager.
- [Table 35-10 on page 35-15](#) describes the map objects that can appear on a map. These elements are not managed by Security Manager.
- [Table 35-11 on page 35-15](#) describes the map element indicators that can appear with a device node.






**Table 35-9**     *Device Node Types*

Node Type	Icon	Description
Firewall		When you select a device, its security contexts are highlighted.
Firewall security context		When you select a security context, the parent device is highlighted. The dotted outline distinguishes the icon as a security context.
Adaptive Security Appliance		When you select a device, its security contexts are highlighted.
Adaptive Security Appliance security context		When you select a security context, the parent device is highlighted. The dotted outline distinguishes the icon as a security context.
Router		Router or VPN concentrator.


**Table 35-9** Device Node Types (continued)

Node Type	Icon	Description
Catalyst 6500/7600 or Catalyst switch		When you select a Catalyst device node, any Firewall Service Modules contained in it are highlighted.
Firewall Services Module (FWSM)		When you select a Firewall Services Module, the security contexts it contains are highlighted on the map.
FWSM security context		When you select a security context, the parent device is highlighted. The dotted outline distinguishes the icon as a security context.
IPS Sensor or Security Service Module		An IPS sensor.
VPN connection		Any type of VPN connection. For GET VPNs, a dashed line indicates the connection between group members and key servers.

**Table 35-10** Map Object Types

Node Type	Icon	Description
Unmanaged firewall		Unmanaged firewall device.
Unmanaged router		Unmanaged router.
Network		Network with a specified address space.
Host		Network host. Examples: CSA, Syslog Server, CA Server, AAA Host
Cloud		An unspecified group of map objects that provides connectivity between specified nodes.
Layer 3 link	—	Layer 3 network connection

**Table 35-11** Map Element Indicators

Indicator	Icon	Description
Linked map		Node is linked to another map.

**Related Topics**

- [Using Map Objects To Represent Network Topology, page 35-17](#)

- [Creating and Managing Layer 3 Links on the Map, page 35-19](#)

## Displaying Managed Devices on the Map

A device node represents a device that is managed by Security Manager. You add a device node to a map by selecting the device from the Security Manager inventory.

When you add a device node to a map, its layer 3 connectivity to other nodes on the map is created automatically. For more information, see [Creating and Managing Layer 3 Links on the Map, page 35-19](#).

You can add, remove, or show managed nodes by the following means:

- **To add devices that are already in the Security Manager inventory**—Select **Map > Show Devices on Map** to open a device selector. Select the desired devices from the list of available devices and click **>>** to move them to the selected devices list. You can select device groups to move all devices in the group. Click **OK** when the list of selected devices has the desired nodes. Only those devices in the selected list are shown on the map.

You can remove devices by selecting them in the selected list and clicking **<<**.

- **To add a new device to the map and the device inventory**—Click the **New Device** button in the map toolbar or right-click the map background and select **New Device**. The New Device dialog box opens. Follow the procedures for adding new devices described in [Adding Devices to the Device Inventory, page 3-6](#).
- **To remove a managed node**—Right-click the node and select **Remove from Map**.
- **To locate a device on the open map when in Device view**—Right-click the device in the device selector and select **Show in Map view**. If the device is shown on the active map, it is shown centered and highlighted on the undocked map. You are told that the device cannot be found if the device is not shown on the active map.
- **To locate a device in Device view from the map**—Right-click the device and select **Show in Device View**. Device view is opened with the device selected so that you can edit its policies.

### Related Topics

- [Understanding Map Elements, page 35-14](#)
- [Showing Containment of Catalyst Switches, Firewalls, and Adaptive Security Appliances, page 35-16](#)

## Showing Containment of Catalyst Switches, Firewalls, and Adaptive Security Appliances



### Note

---

From version 4.17, though Cisco Security Manager continues to support Cisco Catalyst switches features/functionality, it does not support any enhancements.

---

The containment relationship between Catalyst and Adaptive Security Appliance (ASA) devices and their service modules and security contexts, between PIX 7.x+ devices and FWSM and their security contexts, or between IPS devices and their virtual sensors, is displayed in maps as follows:

- When you select a Catalyst device, nodes that represent its Firewall Services Modules (FWSM) are highlighted.



- When you select an ASA, nodes that represent its Security Service Modules are highlighted.
- When you select a service module, the device that contains it is highlighted.
- When you select an IPS device, the nodes that represent virtual sensors defined on the device are highlighted.
- You can view a list of the security contexts contained in an ASA, firewall, or FWSM device, or the virtual sensors contained in an IPS device, by right-clicking the node and selecting **Show Containment**. This command also shows the service modules in a device that has them.
- When you select a security context node, all its ancestor device nodes are highlighted.
- When you select a virtual sensor, the device on which it is defined is highlighted.

## Using Map Objects To Represent Network Topology

You can add map elements to a map that represent objects (such as devices and links) that Security Manager does not manage. These nodes are called map objects. You can use map objects to create a more useful representation of your network topology. (If you want to add a managed device, see [Displaying Managed Devices on the Map, page 35-16](#).)

You can add layer 3 links between any map elements, whether they are device nodes, map nodes, or a combination of both types.

**Tip**

---

To delete a map object, right-click the object and select **Delete Map Object**.

---

- Step 1** Select **Map > Add Map Object**. The Add Map Object dialog box appears (see [Add Map Object and Node Properties Dialog Boxes, page 35-18](#)).
- Step 2** Do one of the following:
- If you are adding a map object based on the definition of an Security Manager policy object, click **Copy Policy Object** to open the [Select Policy Object Dialog Box, page 35-18](#). Then, select the type of object (AAA server, network/host, PKI enrollment), click **Select** to choose the object, then click **OK** in the Select Policy Object dialog box. Information from the policy object is entered in the Add Map Object dialog box.  
The name of the object is used as the map object name, but you can edit this if desired.
  - If you are adding a map object that is not based on a policy object, enter a name for the map object in the **Name** field.
- Step 3** Select the type of object that the node represents from the **Type** list. If you selected a policy object, the type is pre-selected, but you can change the selection.
- Step 4** (Optional) Add interfaces to the node by doing the following for each interface:
- a. Click **Add** to open the [Interface Properties Dialog Box, page 35-19](#). If items already appear in the list, you can select them and click **Edit** to change them.
  - b. Enter an interface name, IP address, and network mask, then click **OK**.
- Step 5** Click **OK**. The map object is added to the center of the map. Move it to the desired location.
-

## Add Map Object and Node Properties Dialog Boxes

For unmanaged map objects, the Add Map Object and Node Properties dialog boxes are the same. Use the Add Map Object dialog box to add an object to the map. Use the Node Properties dialog box to view or edit map object properties. For more information, see [Using Map Objects To Represent Network Topology, page 35-17](#).

For managed map objects (such as a managed device), the Node Properties dialog box is read-only. It displays the object name, type, and list of interface names and IP addresses (if any are defined in Security Manager for the device). The reference information below does not apply to this version of the Node Properties dialog box.

### Navigation Path

- To open the Add Map Object dialog box, select **Map > Add Map Object**.
- To open the Node Properties dialog box, right-click a map object or managed device and select **Node Properties**.

### Field Reference

**Table 35-12 Add Map Object and Node Properties Dialog Boxes for Unmanaged Nodes**

Element	Description
Name	The name of the map object. If you select a policy object, the name of the object is automatically used, but you can change it.
Copy Policy Object button	Click to browse for a policy object to use as the basis for the map object using the <a href="#">Select Policy Object Dialog Box, page 35-18</a> .
Type list	The type of object you are creating. If you select a policy object, a type is selected for you, but you can change it if necessary.
Interfaces table	The interfaces on the node. If you select a policy object, information might have been added to this table. <ul style="list-style-type: none"> <li>• To add an interface, click the <b>Add (+)</b> button and fill in the <a href="#">Interface Properties Dialog Box, page 35-19</a>.</li> <li>• To edit an interface, select it and click the <b>Edit (pencil)</b> button.</li> <li>• To delete an interface, select it and click the <b>Delete (trash can)</b> button.</li> </ul>

## Select Policy Object Dialog Box

Use the Select Policy Object dialog box to add an object to the map that is defined in a policy object.

Select the type of object that defines the node you want to add to the map from the **Select a Policy Object** list, then click **Select** to select the specific policy object. If you know the object’s name, you can type it into the text box instead of clicking Select.

For more information, see [Using Map Objects To Represent Network Topology, page 35-17](#).

### Navigation Path

To open this dialog box, click **Copy Policy Object** in the Add Map Object dialog box (see [Add Map Object and Node Properties Dialog Boxes, page 35-18](#)).

## Interface Properties Dialog Box

Use the Interface Properties dialog box to add and edit interfaces on map objects. For more information, see [Using Map Objects To Represent Network Topology, page 35-17](#).

### Navigation Path

To open this dialog box, click the **Add** or **Edit** button in the [Add Map Object and Node Properties Dialog Boxes, page 35-18](#).

### Field Reference

**Table 35-13** *Interface Properties Dialog Box*

Element	Description
Interface Name	The interface name.
Interface IP Addr/Mask	The interface IP address and network mask, for example, 10.100.10.0/24 or 10.100.10.0/255.255.255.0.

## Creating and Managing Layer 3 Links on the Map

A layer 3 link is a line on the map that represents a network connection between two device interfaces.

Layer 3 connectivity information is automatically added to the map when you add map elements that have interface information. When you add a map element that has interface information, one of the following happens:

- If the interface is on a network that is not represented on the map as a network map object, a network map object is added to the map with a layer 3 link to the new map element.
- If the interface is on a network that is represented on the map as a network map object, a layer 3 link is added between the new map element and the network map object.

When you remove a node interface that is a layer 3 link endpoint, the link is also removed.

You can add additional layer 3 links between device nodes and map objects to illustrate your network's connectivity. Adding Layer 3 links to a map does not configure any network devices. Layer 3 links are just visual elements on the map.

You create layer 3 links to connect any two interfaces on a map. Depending on the interfaces that you choose, the layer 3 link might include intermediary networks or network clouds. In some cases, you have the option to select which intermediary networks and networks clouds are inserted between the connected interfaces.

The following procedure explains how to manually create a new layer 3 link.

### Tips

- The automatic addition of network objects and links is called Autolink. You can configure Autolink to not automatically add private or certain reserved network addresses. To configure these settings, select **Tools > Security Manager Administration**, then click **Autolink**.
- To view the properties of a link, right-click the layer 3 link and select **Link Properties**.
- To delete a layer 3 link, right-click the layer 3 link to be removed and select **Delete Link**. Deleting a layer 3 link does not delete any intermediary network or network clouds between map elements.

- 
- Step 1** In Map view, click **Map > Add Link** or the Add Link button in the toolbar.
- Step 2** Click one of the map elements to connect, then click the other map element to connect.
- Step 3** If the map elements contain interfaces, select the source and destination interfaces for the link in the [Select Interfaces and Link Properties Dialog Boxes](#), then click **OK**.  
The Add Link dialog box might open, depending on which interfaces you select.
- Step 4** If the [Add Link Dialog Box](#) opens, select which intermediary objects and network clouds to insert, then click **OK**.
- 

## Select Interfaces and Link Properties Dialog Boxes

The Select Interfaces and Link Properties dialog boxes are used with layer 3 links on maps. These dialog boxes show information about the source and destination devices for the link (the source being the first device you clicked when making the link).

If you are creating a link, the Select Interfaces dialog box is used. If there are interfaces defined for the device in Security Manager, select the desired source and destination interfaces for the link you are creating from the **Source/Destination Interface** list.

**Tip**

When creating a link, if there are no interfaces defined for either device, the Interface lists are greyed out. If one device has interfaces defined, both fields are active, but empty for the device that does not have interfaces defined for it. You cannot change the interface when viewing link properties.

---

### Navigation Path

For information on how to create layer 3 links or view their properties, see [Creating and Managing Layer 3 Links on the Map, page 35-19](#).

## Add Link Dialog Box

Use the Add Link dialog box to select how to represent the layer 3 link that you are adding to the map.

The contents of the Add Link dialog box vary according to which nodes and interfaces you are connecting. Select the check boxes for each intermediary map object (network or cloud) that you want to insert between the connected nodes. If desired, you can change the names of the map objects.

### Navigation Path

This dialog box might open when you add a link between nodes, depending on which interfaces you select to connect. For the procedure, see [Creating and Managing Layer 3 Links on the Map, page 35-19](#).

# Managing VPNs in Map View

The following topics describe how to manage VPNs in the Map view:

- [Displaying Existing VPNs on the Map, page 35-21](#)
- [Creating VPN Topologies in Map View, page 35-21](#)
- [Editing VPN Policies or Peers From the Map, page 35-22](#)

## Displaying Existing VPNs on the Map

To display an existing VPN on the map, select **Map > Show VPNs on Map**. You are prompted with a list of existing VPNs. Select the ones you want from the available VPNs list and click >> to move them to the selected list.



You can also remove a VPN using this command. Select the VPNs you want to remove from the selected VPNs list and click <<. When you remove a VPN, only the VPN tunnels are removed. The device nodes remain on the map.

When you display a VPN, all of its member devices are added to the map as device nodes, and all of its tunnels are highlighted. However, devices that you removed from the map previously are not added, even if they are members of a VPN that you display. You can add such devices to the map manually, and their VPN connectivity is displayed.

A VPN tunnel is a line on the map that represents a VPN connection between two devices. VPN tunnels are not added to the map automatically when you add a device node that is a member of a VPN. However, if the VPN was already selected to be shown on the map, adding a device in the VPN to the map will also display the tunnel.

For an explanation of the icons used in the map, see [Understanding Map Elements, page 35-14](#).

## Creating VPN Topologies in Map View

You can create VPN connections between VPN-capable managed device nodes that are displayed on the map. You cannot create Extranet VPNs, however.

To create a VPN, do one of the following:

- Click the **New VPN** button in the toolbar and select the type of VPN you want to configure: point-to-point, hub and spoke, or full mesh.
- Select the devices that you want to participate in the VPN (use Ctrl+click to select multiple devices), and either right click and select the command for the desired type of VPN, or click the **New VPN** button and select the VPN type.

Consider the following tips:

- Select only 2 devices to create a point-to-point VPN.
- If you create a hub-and-spoke VPN, the device you right-click is initially defined as the hub, but you can change that in the wizard.
- While in the wizard, you can add or remove devices. You are not restricted to the devices you selected on the map.

Using either technique, the Create VPN wizard opens, where you can create the VPN. For more information, see [Creating or Editing VPN Topologies, page 25-28](#) or click the Help button in the wizard.

The VPN is displayed on the map when you are finished with the wizard.

### Related Topics

- [Selecting Map Elements, page 35-12](#)

## Editing VPN Policies or Peers From the Map

You can edit VPN policies, or the peers that participate in a VPN, from map view. To edit policies or peers, right-click a VPN tunnel or device node and select one of these commands:

- **Edit VPN Policies**—To open the Site-to-Site VPN Manager, where you can edit the policies that define the VPN. For more information, see [Site-to-Site VPN Manager Window, page 25-18](#).
- **Edit VPN Peers**—To open a dialog box that allows you to configure the peers that participate in the VPN. Click the **Help** button in the dialog box for more information.
- **Show VPN Peers**—To see which devices participate in a VPN without editing the list (VPN Peers dialog box).

If the device participates in more than one VPN, you are first prompted to select the desired VPN (with the Select VPN to Configure dialog box) before the appropriate dialog box is opened.

## Managing Device Policies in Map View

You can perform only basic policy management and configure firewall services policies in Map view. You cannot configure other types of policies. The following topics describe how to manage policies from the Map view:

- [Performing Basic Policy Management in Map View, page 35-22](#)
- [Managing Firewall Policies in Map View, page 35-23](#)
- [Managing Firewall Settings in Map View, page 35-23](#)

## Performing Basic Policy Management in Map View

You can perform some basic policy management tasks in Map view. Right click the device and select one of the following commands:

- **Copy Policies Between Devices**—To copy local device policies from one device to another. For more information on copying policies, see [Copying Policies Between Devices, page 5-33](#).
- **Share Device Policies**—To create shared policies from local device policies. For more information on sharing policies, see [Sharing Multiple Policies of a Selected Device, page 5-42](#).
- **Clone Device**—To create a copy of a device, including its policies. For more information on cloning devices, see [Cloning a Device, page 3-57](#).
- **Preview Configuration**—To view the configuration file that will be generated for the device, including the changes from the previous deployment. For more information on previewing configurations, see [Previewing Configurations, page 8-44](#).
- **Discover Policies on Device**—To discover the policies defined on the device and configure them in Security Manager, wiping out whatever policies are defined in Security Manager for the device. For more information device discovery, see [Discovering Policies on Devices Already in Security Manager, page 5-15](#).

### Related Topics

- [Chapter 8, “Managing Deployment”](#)
- [Chapter 3, “Managing the Device Inventory”](#)

- [Chapter 5, “Managing Policies”](#)

## Managing Firewall Policies in Map View

You can configure firewall policies on a device in Map view. These policies are local to the device rather than being shared policies (you must use Policy view to configure shared policies).



Tip

---

If you want to assign a shared policy to a device, see [Performing Basic Policy Management in Map View, page 35-22](#).

---

To configure local firewall policies on a device in Map view, right click the device and select one of the following commands:

- **Edit Firewall Policies > AAA Rules**—To configure AAA policies, which control who is allowed access to the device and what services they are allowed to use once they have access. For more information on configuring AAA rules, see [AAA Rules Page, page 15-10](#).
- **Edit Firewall Policies > Access Rules**—To configure Access Rules policies, which control the traffic that flows through a device. For more information on configuring access rules, see [Access Rules Page, page 16-10](#).
- **Edit Firewall Policies > Inspection Rules**—To configure Inspection Rules policies, which analyze traffic at the application layer and track TCP and UDP sessions to perform refined access control. For more information on configuring inspection rules, see [Inspection Rules Page, page 17-8](#).
- **Edit Firewall Policies > Botnet Traffic Filter Rules**—(ASA 8.2 and later only) To configure Botnet Traffic Filter Rules policies, which monitor web traffic. For more information on configuring botnet traffic filter rules, see [Botnet Traffic Filter Rules Page, page 19-9](#).
- **Edit Firewall Policies > Transparent Rules**—To configure Transparent Rules policies, which define EtherType rules for transparent firewalls. For more information on configuring inspection rules, see [Transparent Rules Page, page 23-3](#).
- **Edit Firewall Policies > Web Filter Rules**—To configure Web Filter Rules policies, which define rules for web access. For more information on configuring web filter rules, see [Web Filter Rules Page \(ASA/PIX/FWSM\), page 18-3](#) or [Web Filter Rules Page \(IOS\), page 18-12](#).
- **Edit Firewall Policies > Zone Based Firewall Rules**—(IOS 12.4(6)T and later only) To configure Zone Based Firewall Rules policies, which configure inspection and web filtering using security zones. For more information on configuring zone based firewall rules, see [Zone-based Firewall Rules Page, page 21-58](#).

### Related Topics

- [Chapter 12, “Introduction to Firewall Services”](#)
- [Chapter 5, “Managing Policies”](#)

## Managing Firewall Settings in Map View

You can configure firewall settings policies on a device in Map view. These policies are local to the device rather than being shared policies (you must use Policy view to configure shared policies).

**Tip**

If you want to assign a shared policy to a device, see [Performing Basic Policy Management in Map View, page 35-22](#).

To configure local firewall settings policies on a device in Map view, right click the device and select one of the following commands:

- **Edit Firewall Settings > AAA Firewall**—(ASA/PIX/FWSM only) To configure AAA Firewall settings policies, which configures proxy, authentication challenge, MAC exempt lists, and other general AAA settings. For more information on configuring AAA firewall settings, see [AAA Firewall Settings Page, Advanced Setting Tab, page 15-20](#) and [AAA Firewall Page, MAC-Exempt List Tab, page 15-26](#).
- **Edit Firewall Settings > Access Control**—To configure Access Control settings policies, which configures optimization and other general access control settings. For more information on configuring access control settings, see [Access Control Settings Page, page 16-24](#).
- **Edit Firewall Settings > AuthProxy**—(IOS devices only) To configure AuthProxy settings policies, which configure general settings for authorization proxies. For more information on configuring authorization proxies, see [AAA Page, page 15-28](#).
- **Edit Firewall Settings > Inspection**—(IOS devices only) To configure Inspection settings policies, which configure timeout and session settings for inspection rules. For more information on configuring inspection settings, see [Configuring Settings for Inspection Rules for IOS Devices, page 17-112](#).
- **Edit Firewall Settings > Web Filter**—To configure Web Filter settings policies, which configure the server used for web filtering. For more information on configuring web filter settings, see [Web Filter Settings Page, page 18-16](#).
- **Edit Firewall Settings > Zone Based Firewall**—(IOS 12.4(6)T and later devices) To configure Zone Based Firewall settings policies, which configure zones and Trend web filter server settings.