



APPENDIX **A**

Interoperation of AUS and Cisco Security Manager

The following topics describe how Security Manager interoperates with AUS:

- [Security Manager Overview, page A-1](#)
- [Configuring Security Manager to Use AUS, page A-2](#)
- [Adding Devices of Auto Update Type to the Security Manager Inventory, page A-4](#)
- [Configuring AUS Settings on Security Appliances After Adding the Devices to Security Manager, page A-7](#)
- [Discovery Mechanisms for Devices that Communicate with AUS, page A-8](#)
- [Deployment Mechanisms for Devices Managed by AUS, page A-9](#)
- [Interoperability with Common Services, page A-11](#)

Security Manager Overview

Security Manager enables you to manage security policies on Cisco security devices. Security Manager supports integrated provisioning of VPN and firewall services across IOS routers, PIX and ASA security appliances, and Catalyst 6500/7600 services modules (FWSM and VPNSM). Security Manager also supports provisioning of many platform-specific settings, for example, interfaces, routing, identity, QoS, logging, and so on.

Security Manager efficiently manages a wide range of networks, from small networks consisting of a few devices through to large networks with thousands of devices. Scalability is achieved through a rich feature set of shareable objects and policies and device grouping capabilities.

Configuring Security Manager to Use AUS

To prepare a PIX security appliance and ASA device to obtain configuration files from the AUS and to enable Security Manager to publish configuration files to AUS, you must do the following:

1. Configure the PIX security appliance and ASA devices to use AUS.

You can specify that you want your PIX security appliance and ASA devices to poll AUS and retrieve any configuration changes. However, before you can use Security Manager to publish configurations to AUS, you must ensure that the devices you are administering are configured to pull their configurations from AUS. You must prepare *each* PIX security appliance and ASA device to use AUS.

You can specify this option before or after you add the PIX security appliance and ASA devices.

- To configure this option before adding a PIX security appliance or ASA device, see [Appendix D, “Bootstrapping Devices to Operate with AUS.”](#)
 - To configure this option after adding the PIX security appliance and ASA devices, you can use the Security Manager GUI to configure the information required to contact AUS. For more information, see [Configuring AUS Settings on Security Appliances After Adding the Devices to Security Manager, page A-7.](#)
2. Configure Security Manager and AUS to communicate with the PIX security appliance and ASA devices.

Although the PIX security appliance and ASA devices are configured to obtain information from the AUS, you must specify the contact information that AUS requires to authenticate with the PIX security appliance and ASA devices. This contact information enables AUS to perform an immediate auto update, if so configured. When you add an AUS-managed device using Security Manager, you must enter the enable password in the Primary

Credentials section of the Device Credentials wizard page. For more information on how to enter device credentials information when adding a device, see the the *User Guide for Cisco Security Manager 3.1*.

3. Deploy the settings defined in Security Manager to AUS.

After you prepare the devices to be managed by AUS, you can deploy the configurations to them. You must deploy the settings and policies you define in Security Manager to AUS, where it is stored to be later imported to your devices, so that you can implement them in your network. When you add a device to be managed by AUS using the Security Manager GUI, the device is added to the AUS GUI only after deployment is successful. The steps you take to deploy configurations to a transport server such as AUS for later retrieval by devices depend on whether you are using Workflow mode or non-Workflow mode. A deployment job defines how configuration changes are sent to devices or to the transport mechanism specified for the device such as AUS. In a deployment job, you can define several parameters, such as the devices or VPNs to which you want to deploy configurations and the method used to deploy configurations to devices. In Workflow mode, you can also specify the dates and times for future deployments.

Workflow mode is an advanced mode of operation that imposes a formal change-tracking and management system. Workflow mode is suitable for organizations in which responsibility is divided among security and network operators for defining VPN or firewall policies and deploying these policies to devices. Some organizations do not divide responsibility and can work in non-Workflow mode, which is the default. When using non-Workflow mode, you do not need to create activities and jobs. When you log in, Security Manager automatically creates an activity for you. This activity is transparent to you and does not need to be managed in any way.

If Workflow mode is enabled, you can select whether to deploy to AUS as part of the job deployment and you can configure the default deployment to use AUS. In Workflow mode, if you want to change Security Manager to deploy configurations to AUS instead of directly sending configurations to devices, or to another location, such as Configuration Engine or Token Management Server (TMS), make sure that you modify the transport protocol as AUS, select an AUS from the Server list, and specify the enable password in the Device Properties page for the devices that you want to be managed by AUS. After you make these changes, the device communicates with AUS and downloads the configuration files. If Workflow mode is not enabled, deployment is more automated than workflow mode, but you can still configure the default deployment to use AUS.

For more information on selecting a workflow mode and managing deployment, see the *User Guide for Cisco Security Manager 3.1*.

Adding Devices of Auto Update Type to the Security Manager Inventory

If you are using AUS in conjunction with Security Manager and want PIX security appliance and ASA devices to be managed by AUS, you add them to Security Manager. When you add an AUS-managed device to Security Manager, you bring in a range of identifying information for the device, such as its device identity, DNS name, its IP address, AUS details, and the Cisco IOS release. After you add the device to be managed by AUS, it appears in the Security Manager device inventory. You can manage a device in Security Manager only after you add it to the inventory. After the device is added to Security Manager, you must select the device in a deployment job to deploy the configuration to AUS. The device appears in the Device Summary page in the AUS GUI only after the deployment is successful.

When you add devices that have dynamic IP addresses using the Add Device from DCR or Add New Device wizards, select the dynamic IP type, then select an AUS that is managing the device from the list of available servers displayed. If the server does not appear in the list, you can add a new AUS and enter the server properties. For information on how to add or edit AUS information when adding a device to Security Manager, see the *User Guide for Cisco Security Manager 3.1*.

To add PIX security appliance and ASA devices to be managed by AUS to the Security Manager inventory, you use the Add new device or Add device from DCR option. This option enables you to add one device at a time. You can create the device in the system, assign policies to the device, and generate configuration files before receiving the device hardware.

When you add the device, you can specify if the device has a static IP address or a dynamic IP address. For Cisco IOS devices, the IP address for the device with a dynamic IP address is retrieved from AUS. For more information on how to add PIX security appliance and ASA devices using the Add New Device or Add Device from DCR option, see the *User Guide for Cisco Security Manager 3.1*.

**Note**

You must use only the Add New Device or the Add Device from DCR option. You cannot use the Add Device from Network or Add Device from Config File options. To change the mode of staged delivery of configurations to use AUS as the transport protocol for a device that has been imported to the Security Manager inventory, see [Changing the Transport Protocol to AUS After Discovering a Device](#), page A-5.

You can add only devices that are running in the network from DCR into Security Manager to be managed by AUS.

Cisco IOS routers with dynamic IP addresses connect to the Auto Update Server (AUS) that is running the CNS Gateway protocol to retrieve the IP address of the device. You can add these devices, which have dynamic IP addresses obtained from a Dynamic Host Configuration Protocol (DHCP) server, to the Security Manager inventory from the Add Device from Network page or the Add New Device page. When you add a device, select AUS to specify that a device has a dynamic IP address. Security Manager then uses the device identity information to retrieve the device IP address from an AUS manager that can be reached. For more information on how to add Cisco IOS routers that have dynamic IP addresses to connect to the AUS, see the *User Guide for Cisco Security Manager 3.1*.

Changing the Transport Protocol to AUS After Discovering a Device

Security Manager uses SSL as the default transport protocol for PIX security appliances and ASA devices. In addition, Security Manager supports staged delivery of configurations using AUS, CNS, and TMS transport protocols. If you bring in the identifying information of a device to Security Manager by discovering the device policies and want to deploy the configuration files to AUS instead of to the device directly or to a transport server, such as Configuration Engine or TMS, make sure you perform the following tasks from the Security Manager GUI to enable the device to be managed by AUS.

- Double-click the device in the Device selector, then click **General** from the Device Properties page. Select the transport protocol as **AUS** from the Transport Protocol list in the DCS Settings element. Security Manager deploys the configuration to the device according to the transport mechanism or protocols you set on the device.
- On the General page, select an AUS to manage the device from the Server drop-down list in the Auto Update element. If you selected a server, that server name is displayed in the field. If you want to select another server but it does not appear in the list, you can add it. To do so, select **+ Add Server...** to display the Server Properties dialog box.
- Click **Credentials** on the Device Properties page. Enter the enable password for the device under the Primary Credentials section.
- Navigate to the AUS page under the Device Administration element in one of the following ways:
 - (Device view) Select **Platform > Device Admin > Server Access > AUS** from the Device Policy selector.
 - (Policy view) Select **PIX/ASA/FWSM Platform > Device Admin > Server Access > AUS** from the Policy Types selector. Right-click AUS and select New AUS Policy to create a policy, or select an existing policy from the Policies selector.

On the AUS page, configure the AUS server access settings to enable AUS to manage the device.

After you configure these settings, you can use Security Manager to deploy configuration files to AUS, after which the device downloads the configuration from AUS.

Adding Devices to Security Manager that Already Exist in DCR

If you are in the Add New Device page and you enter a device display name that already exists in DCR (but not in Security Manager), a Duplicate Device Notification popup window displays the following message:

A device with the same display name exists in DCR. Duplicate display names are not allowed in DCR. To change the display name, click No. To import the existing device from DCR into SM, click Yes.

If you click No, the Add New Device page appears. You can enter another display name and continue adding the device. If you click Yes, the Add Device from DCR page appears, with the device name selected in the DCR List of Devices pane. Click >>. The selected device moves to the Selected Devices pane.

When you are in the Add New Device page and you enter a hostname and domain name combination for a device that already exists in DCR (but not in Security Manager), a Duplicate Device Notification popup window displays the following message:

```
A device with the same hostname and domain name combination exists in DCR. Duplicate hostname and domain name combinations are not allowed in DCR. To change the hostname and domain name combination, click No. To import the existing device from DCR into SM, click Yes.
```

If you click No, the Add New Device page appears. You can enter another hostname and domain name combination and continue adding the device. If you click Yes, the Add Device from DCR page appears, with the device name selected in the DCR List of Devices pane. Click >>. The selected device moves to the Selected Devices pane.

Configuring AUS Settings on Security Appliances After Adding the Devices to Security Manager

After you import the PIX security appliance and ASA devices into the Security Manager inventory (see [Discovery Mechanisms for Devices that Communicate with AUS, page A-8](#)), you can choose the Device Administration policy to configure server access settings, such as AUS settings, on these devices. Then, after you change the AUS settings, you can deploy the new configuration to the devices. Security Manager deploys the configuration file to AUS, where it is stored for later retrieval from the device. Devices, such as PIX security appliances, that use a DHCP server contact AUS for configuration (and image) updates. For information on configuring AUS settings and bootstrapping the PIX security appliance and ASA devices after adding the devices to Security Manager, see the *User Guide for Cisco Security Manager 3.1*.



Note

PIX security appliance and ASA devices come from the factory with certain settings already configured. We highly recommend that after you add a firewall device to Security Manager manually, you discover (import) the factory-default

policies for that device. Bringing these policies, such as the settings configured from the firewall command line interface, into Security Manager prevents you from unintentionally removing them the first time you deploy to that device. For more information about importing policies, see the *User Guide for Cisco Security Manager 3.1*.

Discovery Mechanisms for Devices that Communicate with AUS

When you add a device to Security Manager to be managed by AUS, you can discover its interfaces and certain policies that were already configured on it. Make sure that you configure the transport settings on the devices to enable communication between AUS and devices before you discover policies and settings. To discover the configuration on the device, you must be able to access the device directly on the network and the device credentials must be available. Discovery brings information into the Security Manager database that can later be deployed to AUS for continued management with AUS.

When you initiate policy discovery for a new device, Security Manager analyzes the configuration, then imports the configured service and platform policies into Security Manager. Warnings are displayed if the imported configuration completes only a partial policy definition. If additional settings are required, you must go to the relevant page in Security Manager to finish defining the policy. After policy discovery is complete, you can deploy the configuration to AUS to be imported to the device later, during auto update polling interval.

If you performed policy discovery on a device, ensure that you configure the policies and settings for that device from the Security Manager GUI. Otherwise, when you deploy the configuration file to AUS, the factory-default values will be deployed. Also, if policies exist on the device before you perform discovery, the previously configured settings will be overwritten by the deployed policies.

Deployment Mechanisms for Devices Managed by AUS

After you discover the configuration from the device, you can modify the policies and settings from the Security Manager GUI. Policy definition is done within your private view. Your definitions are not committed to the database and cannot be seen by other Security Manager users until you submit them. When you submit your policy definitions, Security Manager validates their integrity. Errors or warnings inform you of any problems that need to be addressed before the policies can be deployed to the devices. Before you deploy configurations to AUS-managed devices, you can preview them. You can also compare that configuration to one that was last imported from the device or is running on the device. After a successful deployment to the device, you can view a transcript of the configuration commands given to the device and the device's responses.

If you deploy configurations to devices, and then determine that something is wrong, you can revert to and deploy the previous configurations for those devices. You can schedule deployment jobs to occur at future times. For more information on discovery and deployment mechanisms, see the *User Guide for Cisco Security Manager 3.1*.

When you deploy configurations to AUS-managed devices that were added from Security Manager, the Status column in the Deployment Manager window displays the status of the deployment job as Deployed, regardless of whether the configuration changes were downloaded. If an error occurs when the device downloads the configuration from AUS, the running configuration on the device is reverts to the device startup configuration. To learn whether configuration files were downloaded to one or more devices in the job successfully, view the AUS reports. You can use these AUS reports to troubleshoot and monitor any errors. For more information on AUS reports, see [Chapter 6, “Viewing Reports.”](#)

Depending on how you are adding devices to be managed by AUS to Security Manager, the transport protocols used for discovery and deployment differ. See the following sections for details:

- [Transport Protocols—Adding a New Device, page A-10](#)
- [Transport Protocols—Adding Device from Network, page A-10](#)

Transport Protocols—Adding a New Device

Table A-1 The lists the device types, the IP types they support (static or dynamic), and discovery and deployment methods. It shows how what you select in the IP type field, static or dynamic, affects the discovery and deployment methods.

Table A-1 *Discovery/Deployment Methods and Transport Protocols - Add New Device*

Device Type	Static or Dynamic IP Address	Discovery Method	Deployment Method
PIX and ASA	Auto Update (for static IP addresses) Depending on the server managing the device, select an AUS from the Server Properties dialog box.	Discovers from one of the following: <ul style="list-style-type: none"> File Device using the default transport protocol you selected, SSL or SSH. 	Deploys to one of the following: <ul style="list-style-type: none"> File Device using the AUS transport protocol.
	Auto Update (for dynamic IP addresses) Depending on the server managing the device, select an AUS from the Server Properties dialog box.	Discovers from file only.	Deploys to one of the following: <ul style="list-style-type: none"> File Device using the AUS transport protocol.

Transport Protocols—Adding Device from Network

Table A-2 lists the device types, the IP types they support (static or dynamic), and discovery and deployment methods used for Cisco IOS routers. It shows how what you select in the IP type field, static or dynamic, affects the discovery and deployment methods.

Table A-2 *Discovery/Deployment Methods and Transport Protocols - Add Device From Network*

Device Type	Static or Dynamic IP Address	Discovery Method	Deployment Method
Cisco IOS routers	Dynamic IP address is supported. From the CNS Gateway field, click the arrow to display a list of available AUS, then select the AUS that is running the CNS Gateway protocol.	Discovers from file and device using the SSL or SSH as the transport protocol. Security Manager communicates with the AUS that is running the CNS Gateway protocol to determine the IP address of the device, then performs discovery directly from the device.	Deploys to one of the following: <ul style="list-style-type: none"> • File. • Device using the SSL or SSH transport protocol—Communicates with the AUS that is running the CNS Gateway protocol to determine the IP address of the device, then deploys directly to the device.

Interoperability with Common Services

CiscoWorks Common Services 3.0.5 is required for AUS to work. It is installed automatically when you install Security Manager. Common Services provides a model for data storage, login, user role definitions, access privileges, security protocols, and navigation. It also provides a common framework for installation, data management, event and message handling, and job and process management. Common Services supplies essential server-side components to AUS that include the following:

- SSL libraries.
- An embedded SQL database.
- The Apache webserver.
- The Tomcat servlet engine.
- The CiscoWorks home page.

For more information, see the Common Services online help.

You can use the Common Services GUI to add, edit, and delete servers used for auto updates and add, edit, and delete devices managed by AUS, as described in the following sections:

- [Adding Devices of Auto Update Type, page A-12](#)
- [Managing Auto Update Servers, page A-14](#)

Adding Devices of Auto Update Type

The Device and Credential Repository (DCR) helps applications share device lists and credentials using a client-server mechanism, with secured storage and communications. The applications can read or retrieve the information. The applications can also update the information in DCR so that the updated information could be shared with other applications. The Device Management option in the DCR Administration helps you manage the list of devices and their credentials. Apart from having its own attributes and credentials as do DCR devices in DCR, each AUS-managed device has the following additional attributes:

- Device Identity is the string value that uniquely identifies this device in the parent AUS.
- The DCR device ID is a string that uniquely identifies the parent AUS.



Note

If you add devices of Auto Update type to DCR using the following procedure, you can add them from DCR to Security Manager with the Add Device from DCR option. For more information, see [Adding Devices to Security Manager that Already Exist in DCR, page A-6](#). However, if you added a device to DCR, you cannot add the device with same properties, such as display name, hostname, and domain name, directly to AUS. You must delete such devices from DCR and then try to add them from AUS directly.

This procedure describes how to add devices and credentials using Auto Update type to the device list.

- Step 1** On the CiscoWorks home page, select **Common Services > Device and Credentials > Device Management**. The Device Management page appears.

The Device Management page helps you perform operations on standard devices, cluster managed devices and auto update devices. Operations on AUS can be performed only on the Auto Update Server Management page.

The Device Summary section in the Device Management page displays the devices and groups in DCR Administration.

Step 2 Click **Add**. The Device Properties page appears.

Step 3 Select **Auto Update** from the Select a Management Type list.

Enter the device type, display name, auto update device ID, hostname, domain name, and IP address in the corresponding fields.

To select the server for auto updates, domain name, and the device type, click **Select** and select from the resulting popup windows. For AUS-managed devices, display name and device identity are enough.

DCR uses a device record to represent an AUS. You can add an AUS on the Auto Update Server Management page. You can select this AUS to be the field AUS.

Step 4 Click **Add to List**.

The device is added to the Added Device List.

To remove the device from the Device List, select the device, then click **Remove from List**.

Step 5 Click **Next**. The Standard Credentials page appears.

Step 6 Enter the credentials in the Standard Credentials page.

You can add the following credentials:

- primary credentials (username, password, enable password)
- (Optional) SNMPv2c/SNMPv1 credentials (read-only community string, read-write community string)
- (Optional) SNMPv3 credentials (username, password, authentication algorithm, engine ID)
- (Optional) Rx boot mode credentials (username, password)

Step 7 Click **Next**. The HTTP Settings page appears.

Step 8 (Optional) Enter the following credentials in the HTTP Settings page.

- HTTP username
- HTTP password. Reenter the HTTP password in the Verify field.

- HTTP port
- HTTPS port
- Certificate common name

Specify the current connection mode (HTTP or HTTPS) by selecting the appropriate radio button.

Step 9 Click **Next**. The Auto Update Server Credentials page appears.

Step 10 Enter the username and password. Reenter the password in the Verify field.



Note These are the credentials for logging in to the AUS, not for accessing the managed device. These credentials are used by Security Manager to contact AUS.

Step 11 Click **Next**. The User Defined Fields page appears.

Step 12 Enter your attributes, then click **Finish**.

You can define four attribute (user-defined) fields for a device. These fields are used to store additional user-defined data for a device.

If you want to change these attribute fields, you can select **Device and Credentials > Admin > User Defined Fields**.

Managing Auto Update Servers

Auto Update Servers (AUS) have the following credentials in DCR:

- AUS URL
- Username
- Password

The AUS management feature helps you in:

- [Adding an AUS](#)
- [Editing an AUS](#)
- [Deleting an AUS](#)

Adding an AUS

This procedure describes how to add a server for auto updates.

-
- Step 1** On the CiscoWorks home page, select **Common Services > Device and Credentials > Auto Update Server Management**.

The Auto Update Server Management page appears.

- Step 2** Click **Add**. The Auto Update Server dialog box appears.

- Step 3** Enter the display name, IP address, hostname, port number, URN, username, and password in the corresponding fields. Reenter the password in the Verify field.

DCR uses a device record to represent an AUS.

You can select an AUS that you added in the Auto Update Server Management page in the Auto Update Server field when you add devices using the Auto Update management type.

- Step 4** Click **OK**.
-

Editing an AUS

This procedure describes how to edit the properties of an AUS.

-
- Step 1** On the CiscoWorks home page, select **Common Services > Device and Credentials > Auto Update Server Management**.

The Auto Update Server Management page appears.

- Step 2** Select the device you want to edit from the list, then click **Edit**.

The Auto Update Server dialog box appears.

- Step 3** Edit Display Name, Domain Name, IP address, Port, URN, User name, and Password fields.

- Step 4** Click **OK**.
-

Deleting an AUS

This procedure describes how to delete an AUS.

-
- Step 1** On the CiscoWorks home page, select **Common Services > Device and Credentials > Auto Update Server Management**.
The Auto Update Server Management page appears.
- Step 2** Select the device you want to delete from the list.
- Step 3** Click **Delete**.
-