



CHAPTER 1

Introduction

The CiscoWorks Auto Update Server (AUS) 3.2 is a web-based interface for upgrading device configuration files and software images on PIX security appliances and Adaptive Security Appliances (ASA) that use the auto update feature.

Security appliances with dynamic IP addresses that use the auto update feature connect to AUS periodically to upgrade device configuration files and to pass device and status information.



Note

PIX security appliances and ASA are collectively referred to as security appliances throughout this guide.

Cisco IOS routers that have dynamic IP addresses communicate with AUS that is running the Cisco Networking Services (CNS) Gateway Protocol to provide their IP addresses.

Cisco Security Manager (Security Manager) can interoperate with AUS. You can choose whether to install AUS when you install Security Manager. To manage the devices in Security Manager, you must provide the device identity and the AUS information when you add a device. Security Manager uses the device identity information to retrieve the device IP address from an AUS that can be reached.



Note

To install AUS, you must use the **Cisco_Security_Manager_3.2.exe** installation application available on the Security Manager DVD. For more information on how to install AUS and other related server applications, see the *Installation Guide for Cisco Security Manager 3.2*.

These topics will help you understand AUS:

- [AUS Product Overview, page 1-2](#)
- [AUS 3.2 Product Features, page 1-3](#)
- [Understanding User Roles and Permissions, page 1-6](#)

AUS Product Overview

The Auto Update Server (AUS) is a tool for upgrading PIX security appliance software images, ASA software images, PIX Device Manager (PDM) images, Adaptive Security Device Manager (ASDM) images, and PIX security appliance and ASA configuration files.

A network management server cannot directly initiate communication to devices that acquire their interface addresses using DHCP because their IP addresses are not known ahead of time. Furthermore, these devices might not be running, or they might be behind firewalls and NAT boundaries when the management system needs to make changes.

These devices use the auto update feature to connect to AUS at periodic intervals. The device gives AUS its current state and device information. AUS responds to the device by providing a list of versions for the software images and configuration files that the device should be running. The device compares the file versions with the versions it is running. If the versions are different, the device downloads the new versions from the URLs provided by AUS. After the device is up-to-date with the new file versions, it sends AUS its state and device information again.

AUS 3.2 includes a CNS Event Gateway feature that operates in conjunction with Security Manager. The CNS Event Gateway feature enables Security Manager to manage local or remote IOS devices with dynamically assigned addresses. After you bootstrap these devices (see [Appendix D, “Bootstrapping Devices to Operate with AUS”](#)), IOS devices contact AUS and provide their IP addresses and interface names. Then, Security Manager communicates with the AUS to retrieve the IP address of an IOS device, which it uses to contact the IOS devices and update IOS configurations. You can also configure additional CNS Event Gateways to communicate with a large number of Cisco IOS routers managed by Security Manager. For more information, see [Support for Additional IOS Devices to be Managed by the CNS Event Gateway, page D-10](#).

**Note**

For a complete list of devices and OS versions supported by AUS, please see *Supported Devices and Software Versions for Auto Update Server 3.2* on Cisco.com.

AUS 3.2 Product Features

Auto Update Server 3.2 has the following features:

- **Auto Update Feature**—Facilitates automatic and on-request updating of PIX security appliance software images, ASA software images, PDM images, ASDM images, and security appliance configuration files.
- **Number of Security Appliances Supported**—Facilitates the managing of up to 1000 security appliances. Security appliances operating in auto-update mode periodically contact AUS to upgrade software images, configurations, and versions of PDM or ASDM and to pass device information and status to AUS.
- **DHCP**—Facilitates the management of devices that obtain their addresses through Dynamic Host Configuration Protocol (DHCP).
- **Network Address Translation (NAT)**—Facilitates the management of devices that sit behind NAT boundaries.
- **Devices**—Lists all managed devices and their status, such as whether devices have contacted AUS yet and whether image files are up-to-date.
- **Images**—Enables you to manage PIX security appliance software images, ASA software images, ASDM files, and PDM files and to view information about configuration files. In AUS 1.1 and later releases, this feature (tab) is called Files.
- **Assignments**—Enables you to assign devices to images and to assign an image to devices. AUS 1.1 added the capability to assign and unassign PIX security appliance configuration files. In AUS 3.0 and later, you can assign and unassign ASDM images and ASA configuration files.
- **CNS Event Gateway**—Enables you to manage IOS devices with dynamic IP addresses.
- **Adding Devices**—Enables you to add devices directly, instead of adding devices through Security Manager.

- **Deleting Devices**—Enables you to delete devices so that you can maintain consistency between the Security Manager and AUS databases.
- **Launching Device Manager**—Starts a browser to access PDM or ASDM on a selected device.
- **Viewing Configuration Files**—Enables you to display a selected configuration file to help you verify settings and troubleshoot problems.
- **Assigning and Unassigning Configuration Files**—Enables you to assign devices to and unassign devices from configuration files. The configuration files remain in AUS and can be reassigned at any time.
- **Deleting Configuration Files**—Enables you to remove configuration files from AUS. Deleting configuration files automatically unassigns them as well.
- **Generating reports**—Contains reports to help you troubleshoot and monitor AUS operations:
 - **System Info Report**—Provides general information about AUS and shows server activity for the last 24 hours. For more information, see [Viewing the System Info Report, page 6-1](#).
 - **Event Report**—Lists the devices that contacted or tried to contact AUS on a specified date. For more information, see [Viewing the Event Report, page 6-3](#).
 - **Event Failure Summary Report**—Lists the devices that had failure events on a specified date. For more information, see [Viewing the Event Failure Summary Report, page 6-8](#).
 - **Event Success Summary Report**—Lists the devices that had success events on a specified date. For more information, see [Viewing the Event Success Summary Report, page 6-10](#).
 - **No Contact Since Report**—Lists the devices that have not contacted AUS since the date specified. For more information, see [Viewing the No Contact Since Report, page 6-11](#).
 - **CNS Device Summary Report**—Lists the CNS devices and provides contact information with AUS. For more information, see [Viewing the CNS Devices Report, page 6-14](#).
- **Cisco ACS roles for AUS**—Provides AUS roles that are more consistent with the CiscoWorks format.

- Integration of AUS with Cisco Security Manager—Enables you to cross-launch AUS from the Security Manager application. Security Manager provides an integrated interface for the provisioning of VPN and security appliance services across many different device types, including IOS routers, security appliances (PIX and ASA), Catalyst 6000 devices, and Catalyst security service modules (such as VPN Acceleration Services Module [VPNSM] and Firewall Services Module [FWSM]). Security Manager enables the management of hundreds and even thousands of devices simultaneously, instead of your having to configure each device individually. For more information, see [Appendix A, “Interoperation of AUS and Cisco Security Manager.”](#)
- Support for Cisco PIX Security Appliance Software Version 7.x and 8.0—Supports Cisco PIX Software Version 7.x and 8.0 for PIX security appliances. PIX software version 7.x and 8.0 introduce significant enhancements to all major functional areas, including: firewalling and inspection services, VPN services, network integration, high availability services, and management/monitoring.
- Support for ASA Devices—Allows ASA devices to be managed for secure remote networks. The Cisco ASA 5500 Series Adaptive Security Appliance delivers unprecedented levels of defense against threats to the network with deeper web inspection and flow-specific analysis, improved secure connectivity by way of end-point security posture validation, and voice- and video-over-VPN support.
- Blocking Updates—Disables the auto update feature for selected devices.
- Scheduling Updates—Provides you with different methods for scheduling configuration updates to help you maintain your configuration files and keep your devices current.
- Canceling Updates—Enables you to change the auto update schedule you already configured on a device to recognize the polling time set on the device.
- Auto Update Immediate feature—Enables you to configure a device to contact AUS for updates immediately, instead of waiting for the device to contact AUS at the specified interval.

- Backup and Restore of AUS Databases—Provides a single backup and restore facility to back up and restore all applications installed on a CiscoWorks server. You cannot back up or restore individual AUS databases as you could do in earlier releases. Use the Common Services Backup dialog box to schedule system backups at regular intervals. See CiscoWorks Common Services online help for more information.

You can install AUS on another server and export the existing database to the new server. You can transfer the database only to a server of the same platform type. For example, if AUS is installed on a Windows platform, you can export the database only to another Windows platform.

Deploying AUS Behind a NAT Boundary

If you want to deploy AUS behind a NAT boundary in either the Enterprise network or in the Enterprise DMZ, then the PIX security appliance and ASA devices being managed by AUS must all be on the same side of the NAT boundary. For example, you can deploy AUS in the DMZ behind a NAT boundary and manage devices that were deployed only on the Internet; however, you cannot deploy AUS in the DMZ behind a NAT boundary with some devices using private addresses on the inside of the boundary and some outside on the Internet.

Understanding User Roles and Permissions

AUS supports two methods for authentication: CiscoWorks Server or Cisco Secure Access Control Server (ACS). When you install CiscoWorks Common Services, the CiscoWorks Server is chosen to provide authentication services by default. You can change this to ACS before or after installing AUS. See the *User Guide for CiscoWorks Common Services 3.1* for details. For more information, see [Appendix C, “User Roles and Permissions.”](#)