



CHAPTER 4

Before You Start

This section describes the tasks you must perform before you use ASDM, and includes the following topics:

- [Factory Default Configurations, page 4-1](#)
- [Configuring the Security Appliance for ASDM Access, page 4-4](#)
- [Setting Transparent or Routed Firewall Mode at the CLI, page 4-4](#)
- [Starting ASDM, page 4-6](#)
- [Configuration Overview, page 4-9](#)

Factory Default Configurations

The factory default configuration is supported on all security appliances, except for the PIX 525 and PIX 535 models.

For the ASA 5505 model, the factory default configuration includes predefined interfaces and NAT, so that the adaptive security appliance is ready to use in your network as delivered.

For the PIX 515, PIX515E, ASA 5510, and higher version models, the factory default configuration provides a management interface to allow you to connect to the security appliance using ASDM, from which you can then complete your configuration.

The factory default configuration is available only in routed firewall mode and single context mode. See [Configuring Security Contexts](#) for more information about multiple context mode. See the [Firewall Mode Overview](#) for more information about routed and transparent firewall mode.

This section includes the following topics:

- [Restoring the Factory Default Configuration, page 4-1](#)
- [ASA 5505 Default Configuration, page 4-2](#)
- [ASA 5510 and Higher Version Default Configuration, page 4-3](#)
- [PIX 515/515E Default Configuration, page 4-4](#)

Restoring the Factory Default Configuration

To restore the factory default configuration, perform the following steps:

Step 1 Choose **File > Reset Device to the Factory Default Configuration**.

Step 2 To change the default IP address, do one of the following:

- For the ASA 5500 series, check the **Use this address for the Management 0/0 interface that will be named as “management”** check box, enter the new IP address in the Management IP Address field, and then choose the new subnet mask in the Management Subnet Mask drop-down list.
- For the PIX series, check the **Use this address for the Ethernet 1 interface, which will be named “inside”** check box, enter the new inside IP address in the Inside IP Address field, and then choose the new inside subnet mask in the Inside Subnet Mask drop-down list.

Step 3 Click **OK**.



Note

After restoring the factory default configuration, the next time you reload the adaptive security appliance, it boots from the first image in internal Flash memory. If an image does not exist in internal Flash memory, the adaptive security appliance does not boot.

ASA 5505 Default Configuration

The default factory configuration for the ASA 5505 adaptive security appliance provides the following:

- An inside VLAN 1 interface that includes the Ethernet 0/1 through 0/7 switch ports. If you did not set the IP address in the **configure factory-default** command, then the VLAN 1 IP address and mask are 192.168.1.1 and 255.255.255.0.
- An outside VLAN 2 interface that includes the Ethernet 0/0 switch port. VLAN 2 derives its IP address using DHCP.
- The default route is also derived from DHCP.
- All inside IP addresses are translated when accessing the outside interface using PAT.
- By default, inside users can access the outside with an access list, and outside users are prevented from accessing the inside.
- The DHCP server is enabled on the adaptive security appliance, so that a computer connecting to the VLAN 1 interface receives an IP address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface Ethernet 0/0
  switchport access vlan 2
  no shutdown
interface Ethernet 0/1
  switchport access vlan 1
  no shutdown
interface Ethernet 0/2
  switchport access vlan 1
  no shutdown
interface Ethernet 0/3
  switchport access vlan 1
  no shutdown
interface Ethernet 0/4
  switchport access vlan 1
  no shutdown
```

```
interface Ethernet 0/5
  switchport access vlan 1
  no shutdown
interface Ethernet 0/6
  switchport access vlan 1
  no shutdown
interface Ethernet 0/7
  switchport access vlan 1
  no shutdown
interface vlan2
  nameif outside
  no shutdown
  ip address dhcp setroute
interface vlan1
  nameif inside
  ip address 192.168.1.1 255.255.255.0
  security-level 100
  no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 and Higher Version Default Configuration

The default factory configuration for the ASA 5510 and higher version adaptive security appliance provides the following:

- The Management 0/0 interface. If you did not set the IP address in the **configure factory-default** command, then the IP address and mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the adaptive security appliance, so a computer connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E Default Configuration

The default factory configuration for the PIX 515/515E security appliance provides the following:

- The inside Ethernet1 interface. If you did not set the IP address in the **configure factory-default** command, then the IP address and subnet mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the security appliance, so a computer connecting to the interface receives an address between 192.168.1.2 and 192.168.1.254.
- The HTTP server is enabled for ASDM and is accessible to users on the 192.168.1.0 network.

The configuration consists of the following commands:

```
interface ethernet 1
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

Configuring the Security Appliance for ASDM Access

If you want to use ASDM instead of the CLI to configure the security appliance and you have a factory default configuration, you can connect to the default management address by pointing your browser to <https://192.168.1.1>. Alternatively, you can use the Cisco ASDM Launcher (if it is already installed) to connect to ASDM. For more information, see [Factory Default Configurations, page 4-1](#).

For the ASA 5505 adaptive security appliance, the switch port to which you connect to ASDM can be any port, except for Ethernet 0/0. On the ASA 5510 and higher version adaptive security appliances, the interface to which you connect to ASDM is Management 0/0. For the PIX 515/515E security appliance, the interface to which you connect to ASDM is Ethernet 1.

If you do not have a factory default configuration, see the *Cisco Security Appliance Command Line Configuration Guide* for instructions to access the CLI.

Setting Transparent or Routed Firewall Mode at the CLI

You can set the adaptive security appliance to run in the default routed firewall mode or transparent firewall mode. For more information about the firewall mode, see the [Firewall Mode Overview](#). For multiple context mode, you can use only one firewall mode for all contexts. You must set the mode in the system execution space.

When you change modes, the adaptive security appliance clears the configuration, because many commands are not supported in both modes. If you already have a populated configuration, be sure to back up this configuration before changing the mode; you can use this backup configuration for reference when you create a new configuration.

For multiple context mode, the system configuration is erased, which removes any contexts. If you again add a context that has an existing configuration that was created for the wrong mode, the context configuration will not work correctly.

**Note**

Be sure to create your context configurations for the correct mode before you add them again, or add new contexts with new paths for new configurations.

If you download a text configuration to the security appliance that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the adaptive security appliance changes the mode as soon as the command is executed, and then continues reading the configuration that you downloaded. If the command occurs later in the configuration, the adaptive security appliance clears all preceding lines in the configuration.

To set the firewall mode, perform the following steps.

**Note**

In multiple context mode, you must perform these steps in the system execution space.

Step 1

Make sure you back up the startup or running configuration file to use for reference before creating the new configuration. In single context mode or from the system configuration in multiple mode, you can copy the startup configuration file or running configuration file to an external server or to local Flash memory, using one of the following commands.

- To copy to a TFTP server, enter the following command:

```
hostname# copy {startup-config | running-config} tftp://server[/path]/filename
```

Where *server* is the name of the TFTP server, *path* is the directory path to the configuration file, and *filename* is the name of the configuration file.

- To copy to an FTP server, enter the following command:

```
hostname# copy {startup-config | running-config}
ftp://[user[:password]@]server[/path]/filename
```

Where *user* is your username, *password* is the password to the FTP server, *server* is the name of the FTP server, *path* is the directory path to the configuration file, and *filename* is the name of the configuration file.

- To copy to local Flash memory, enter the following command:

```
hostname# copy {startup-config | running-config} {flash:/ | disk0:/ |
disk1:/}[/path]/filename
```

Where *path* is the directory path to the configuration file, and *filename* is the name of the configuration file.

**Note**

Be sure the destination directory exists. If it does not exist, use the **mkdir** command to create the destination directory.

Step 2

To change the mode, enter one of the following commands:

- To set the mode to transparent, enter the following command:

```
hostname(config)# firewall transparent
```

This command also appears in each context configuration for information only; you cannot enter this command in a context.

- To set the mode to routed, enter the following command:

```
hostname(config)# no firewall transparent
```

Starting ASDM

This section describes how to start ASDM according to one of the following methods:

- [Downloading the ASDM Launcher, page 4-6](#)
- [Starting ASDM from the ASDM Launcher, page 4-6](#)
- [Using ASDM in Demo Mode, page 4-7](#)
- [Starting ASDM from a Web Browser, page 4-8](#)

Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. The ASDM Launcher avoids double authentication and certificate dialog boxes, launches more quickly, and caches previously entered IP addresses and usernames.

To download the ASDM launcher, perform the following steps:

Step 1 On the ASDM Welcome screen, click the applicable button to download the ASDM Launcher installation file.

Step 2 Double-click the **asdm-launcher.exe** file.



Note In transparent firewall mode, enter the management IP address. Be sure to enter **https**, not **http**.

Step 3 Click **OK** or **Yes** to all prompts, including the name and password prompt. Leave the name and password blank.

The installer downloads to your computer.

Step 4 Run the installer to install the ASDM Launcher.

Starting ASDM from the ASDM Launcher

To start ASDM from the ASDM Launcher, perform the following steps:

Step 1 Double-click the Cisco ASDM Launcher shortcut on your desktop, or open it from the **Start** menu. Alternatively, from the ASDM Welcome screen, you can click **Run Startup Wizard** to configure ASDM.

- Step 2** Enter or choose the adaptive security appliance IP address or hostname to which you want to connect. To clear the list of IP addresses, click the trash can icon next to the Device/IP Address/Name field.
- Step 3** Enter your username and your password, and then click **OK**.
- If there is a new version of ASDM on the adaptive security appliance, the ASDM Launcher automatically downloads the new version and requests that you update the current version before starting ASDM.
-

Using ASDM in Demo Mode

The ASDM Demo Mode, a separately installed application, lets you run ASDM without having a live device available. In this mode, you can do the following:

- Perform configuration and selected monitoring tasks via ASDM as though you were interacting with a real device.
- Demonstrate ASDM or security appliance features using the ASDM interface.
- Perform configuration and monitoring tasks with the CSC SSM.
- Obtain simulated monitoring and logging data, including real-time system log messages. The data shown is randomly generated; however, the experience is identical to what you would see when you are connected to a real device.

This mode does not support the following:

- Saving changes made to the configuration that appear in the GUI.
- File or disk operations.
- Historical monitoring data.
- Non-administrative users.
- These features:
 - File menu:
 - Save Running Configuration to Flash
 - Save Running Configuration to TFTP Server
 - Save Running Configuration to Standby Unit
 - Save Internal Log Buffer to Flash
 - Clear Internal Log Buffer
 - Tools menu:
 - Command Line Interface
 - Ping
 - File Management
 - Update Software
 - File Transfer
 - Upload image from Local PC
 - System Reload
 - Toolbar/Status bar > Save


- Configuration > Interface > Edit Interface > Renew DHCP Lease
- Configuring a standby device after failover
- Operations that cause a rereading of the configuration, in which the GUI reverts to the original configuration:
 - Switching contexts
 - Making changes in the Interface pane
 - NAT pane changes
 - Clock pane changes

To run ASDM in Demo Mode, perform the following steps:

-
- Step 1** Download the ASDM Demo Mode installer, `asdm-demo-version.msi`, from one of the following locations:
- <http://www.cisco.com/cgi-bin/tablebuild.pl/asa>
 - <http://www.cisco.com/cgi-bin/tablebuild.pl/pix>
- Step 2** Double-click the installer to install the software.
- Step 3** Double-click the Cisco ASDM Launcher shortcut on your desktop, or open it from the **Start** menu.
- Step 4** Check the **Run in Demo Mode** check box.
- The Demo Mode window appears.
-

Starting ASDM from a Web Browser

To start ASDM from a web browser, perform the following steps:

-
- Step 1** From a supported web browser on the security appliance network, enter the following URL:
- ```
https://interface_ip_address
```
- Where *interface\_ip\_address* is the IP address of ASDM on the adaptive security appliance network.
-  **Note** In transparent firewall mode, enter the management IP address. Be sure to enter **https**, not **http**.
- 
- Step 2** Click **OK** or **Yes** to all browser prompts, including the username and password, which you should leave blank.
- The Cisco ASDM 6.0(3) Welcome page displays with the following buttons:
- **Install ASDM Launcher and Run ASDM**
  - **Run ASDM**
  - **Run Startup Wizard**
- Step 3** Click **Run ASDM**.
- Step 4** Click **OK** or **Yes** to all the browser prompts.
-

# Configuration Overview

To configure and monitor the adaptive security appliance, perform the following steps:

- 
- Step 1** For initial configuration [Using the Startup Wizard](#), choose **Wizards > Startup Wizard**.
  - Step 2** To use the IPsec [VPN Wizard](#) to configure IPsec VPN connections, choose **Wizards > IPsec VPN Wizard** and complete each screen that appears.
  - Step 3** To use the SSL [VPN Wizard](#) to configure SSL VPN connections, choose **Wizards > SSL VPN Wizard** and complete each screen that appears.
  - Step 4** To configure high availability and scalability settings, choose **Wizards > High Availability and Scalability Wizard**. See [Configuring Failover with the High Availability and Scalability Wizard](#) for more information.
  - Step 5** To use the [Packet Capture Wizard](#) to configure packet capture, choose **Wizards > Packet Capture Wizard**.
  - Step 6** To display different colors and styles available in the ASDM GUI, choose **View > Office Look and Feel**.
  - Step 7** To configure features, click the **Configuration** button on the toolbar and then click one of the following feature buttons to display the associated configuration pane: **Device Setup**, **Device Management**, **Firewall**, **Remote Access VPN**, **Site-to-Site VPN**, **IPS**, and **Trend Micro Content Security**.

**Note**

If the Configuration screen is blank, click **Refresh** on the toolbar to display the screen content.

---

- The Device Setup pane lets you do the following:
  - Launch the Startup Wizard to create security policy.
  - Configure basic interface parameters, including the IP address, name, security level, and the bridge group for transparent mode. For more information, see [Configuring Interfaces in Single Mode](#).
  - Configure OSPF, RIP, static, and asymmetric routing (single mode only). For more information, see [Configuring Dynamic And Static Routing](#).
  - Configure AAA services.
  - Configure digital certificates.
  - Configure the device name and device password.
  - Configure DHCP services.
  - Configure DNS services.
- The Firewall pane lets you configure security policy, including access rules, AAA rules, filter rules, service policy rules, as well as NAT rules, URL filtering servers, global objects, and perform advanced configuration for the following:
  - [Configuring Access Rules](#) determine the access of IP traffic through the security appliance. For transparent firewall mode, you can also apply an EtherType access list to allow non-IP traffic.
  - [Ethertype Rules \(Transparent Mode Only\)](#) determine the access of non-IP traffic through the security appliance.
  - [Configuring Access Rules](#) determine authentication and/or authorization for certain types of traffic, for example, HTTP. The security appliance also sends accounting information to a RADIUS or TACACS+ server.

- [Filter Rules](#) prevent outbound access to specific websites or FTP servers. The security appliance works with a separate server running either Websense Enterprise or Sentian by N2H2. Choose **Configuration > Properties > URL Filtering** to configure the URL filtering server, which you must do before adding a rule.
- [Configuring Service Policy Rules](#) apply application inspection, connection limits, and TCP normalization. Inspection engines are required for services that embed IP addressing information in the user data packet or that open secondary channels on dynamically assigned ports. These protocols require the adaptive security appliance to do a deep packet inspection. You can also limit TCP and UDP connections, and embryonic connections. Limiting the number of connections and embryonic connections protects you from a DoS attack. An embryonic connection is a connection request that has not finished the necessary handshake between a source and destination. TCP normalization drops packets that do not appear normal.
- [NAT](#) translates addresses used on a protected network to addresses used on the public Internet. This setting lets you use private addresses, which are not routable on the Internet, on your inside networks.
- [Adding Global Objects](#) provides a single location where you can configure, view, and modify the reusable components that you need to implement your policy on the adaptive security appliance. These reusable components, or objects, include the following:
  - Network Objects/Groups
  - Service Groups
  - Class Maps
  - Inspect Maps
  - Regular Expressions
  - TCP Maps
  - Global Pools
  - Time Ranges
- The Remote Access VPN pane lets you configure network client access, clientless SSL VPN browser access and advanced web-related settings, AAA setup, certificate management, load balancing, and perform additional advanced configuration, including the following:
  - Configure IPsec connections for VPN tunnels.
  - Configure clientless SSL VPN connections. [Clientless SSL VPN](#) lets users establish a secure, remote-access VPN tunnel to the adaptive security appliance using a web browser.
  - [IKE](#) sets the IP addresses of clients after they connect through the VPN tunnel.
  - [Load Balancing](#) configures load balancing for VPN connections.
  - [E-Mail Proxy](#) configures e-mail proxies. E-mail proxies extend remote e-mail capability to clientless SSL VPN users.
- The Site-to-Site VPN pane lets you configure site-to-site VPN connections, group policies, certificate management, and perform advanced configuration, including the following:
  - [IKE Policies](#) and [IKE Parameters](#) (also called ISAKMP), which provide the negotiation protocol that lets two hosts agree on how to build an IPsec security association.
- The Device Management pane lets you configure settings to access and manage the following:
  - ASDM and HTTP over SSL management sessions.
  - FTP and TFTP clients.

- The CLI.
- SNMP and ICMP.
- Logging, including e-mail, event lists, filters, rate limit, syslog servers, and SMTP. For more information, see [Configuring Logging](#).
- User and AAA authentication.
- High availability, the Scalability Wizard, and failover.
- Advanced configuration.

**Note**

If you have a CSC SSM card or IPS software installed, either the **Trend Micro Content Security** or **IPS** feature button also appears.

- The IPS pane lets you configure the IPS sensor. For more information, see [Configuring IPS](#).
- The Trend Micro Content Security pane lets you configure the CSC SSM (available for the ASA 5500 series adaptive security appliance). For more information, see [Configuring Trend Micro Content Security](#).

**Step 8**

To monitor the adaptive security appliance, click the **Monitoring** button on the toolbar and then click one of the following feature buttons to display the associated monitoring pane: **Interfaces**, **VPN**, **Trend Micro Content Security**, **Routing**, **Properties**, and **Logging**.

- The Interfaces pane lets you monitor the ARP table, DHCP services, dynamic access lists, the PPOE client, connection status, and interface statistics. For more information, see [Monitoring Interfaces](#).
- The VPN pane lets you monitor VPN connections. For more information, see [Monitoring VPN](#).
- The Routing pane lets you Monitors routes, OSPF LSAs, and OSPF neighbors. For more information, see [Monitoring Routing](#).
- The Properties pane lets you monitor management sessions, AAA servers, failover, CRLs, the DNS cache, and system statistics. For more information, see [Monitoring Properties](#).
- The Logging pane lets you monitor system log messages, the Real-Time Log Viewer, and the log buffer. For more information, see [Monitoring Logging](#).
- The Trend Micro Content Security pane lets you monitor CSC SSM connections. For more information, see [Monitoring Trend Micro Content Security](#).

