



# CHAPTER 2

## Before You Start

---

This section contains the following topics:

- [Factory Default Configurations](#)
- [Configuring the Security Appliance for ASDM Access](#)
- [Setting Transparent or Routed Firewall Mode at the CLI](#)
- [Downloading the ASDM Launcher](#)
- [Starting ASDM](#)
- [History Metrics](#)
- [Configuration Overview](#)

## Factory Default Configurations

The factory default configuration is the configuration applied by Cisco to new security appliances. The factory default configuration is supported on all models except for the PIX 525 and PIX 535 security appliances.

For the PIX 515/515E and the ASA 5510 and higher security appliances, the factory default configuration configures an interface for management so you can connect to it using ASDM, with which you can then complete your configuration.

For the ASA 5505 adaptive security appliance, the factory default configuration configures interfaces and NAT so that the security appliance is ready to use in your network immediately.

The factory default configuration is available only for 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 2-2](#)
- [ASA 5505 Default Configuration, page 2-2](#)
- [ASA 5510 and Higher Default Configuration, page 2-3](#)
- [PIX 515/515E Default Configuration, page 2-4](#)

## 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 to an IP address of your choosing, check **Use this address** for the <default interface> which will be named as <name> check box.
  - Step 3** Enter the new IP address in the Management IP Address field.
  - Step 4** Enter the new subnet mask in the Management Mask field.
  - Step 5** Click **OK**.
- 

If you specify the *ip\_address*, then you set the inside or management interface IP address, depending on your model, instead of using the default IP address of 198.168.1.1. The **http** command uses the subnet you specify. Similarly, the **dhcpd address** command range consists of addresses within the subnet that you specify.

After you restore the factory default configuration, save it to internal Flash memory using the **write memory** command. The **write memory** command saves the running configuration to the default location for the startup configuration, even if you previously configured the **boot config** command to set a different location; when the configuration was cleared, this path was also cleared. See the

**Note**

---

This command also clears the **boot system** command, if present, along with the rest of the configuration. The **boot system** command lets you boot from a specific image, including an image on the external Flash memory card. The next time you reload the security appliance after restoring the factory configuration, it boots from the first image in internal Flash memory; if you do not have an image in internal Flash memory, the security appliance does not boot.

---

To configure additional settings that are useful for a full configuration, see the **setup** command.

## ASA 5505 Default Configuration

The default factory configuration for the ASA 5505 adaptive security appliance configures 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 using interface 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 security appliance, so a PC connecting to the VLAN 1 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 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 Default Configuration

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

- The management 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 security appliance, so a PC 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 configures 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 mask are 192.168.1.1 and 255.255.255.0.
- The DHCP server is enabled on the security appliance, so a PC 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 to configure the security appliance instead of the command-line interface, you can connect to the default management address of 192.168.1.1 (if your security appliance includes a factory default configuration. See the [“Factory Default Configurations” section on page 2-1](#)). On the ASA 5510 and higher adaptive security appliances, the interface to which you connect with ASDM is Management 0/0. For the ASA 5505 adaptive security appliance, the switch port to which you connect with ASDM is any port, except for Ethernet 0/0. For the PIX 515/515E security appliance, the interface to which you connect with ASDM is Ethernet 1.

If you do not have a factory default configuration, see the *Cisco ASA 5500 Series Configuration Guide using the CLI* to access the command-line interface. You can then configure the minimum parameters to access ASDM by entering the **setup** command.

# Setting Transparent or Routed Firewall Mode at the CLI

You can set the security appliance to run in routed firewall mode (the default) or transparent firewall mode. For more information about the firewall mode, see [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 security appliance clears the configuration because many commands are not supported for both modes. If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration. For multiple context mode, the system configuration is erased. This action removes any contexts from running. If you then re-add a context that has an existing configuration that was created for the wrong mode, the context configuration will not work correctly. Be sure to recreate your context configurations for the correct mode before you re-add them, or add new contexts with new paths for the 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 security appliance changes the mode as soon as it reads the command and then continues reading the configuration you downloaded. If the command is later in the configuration, the security appliance clears all the preceding lines in the configuration.

To set the firewall mode, perform the following steps. In multiple context mode, perform these steps in the system execution space.

**Step 1** In single context mode or from the system configuration in multiple mode, you can copy the startup configuration or running configuration to an external server or to the local Flash memory using one of the following commands. You can use this backup configuration for reference when creating your new configuration.

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

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

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

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

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

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

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

**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 informational purposes only; you cannot enter this command in a context.

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

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

---

## Downloading the ASDM Launcher

The ASDM Launcher is for Windows only. The ASDM Launcher is an improvement over running ASDM as a Java Applet. The ASDM Launcher avoids double authentication and certificate dialog boxes, launches faster, and caches previously-entered IP addresses and usernames.

To download the ASDM launcher, perform the following steps:

---

**Step 1** From a supported web browser on the security appliance network, enter the following URL:

`https://interface_ip_address`

In transparent firewall mode, enter the management IP address.



---

**Note** Be sure to enter `https`, not `http`.

---

**Step 2** Click **OK** or **Yes** to all prompts, including the name and password prompt. By default, leave the name and password blank.

A page displays with the following buttons:

- **Download ASDM Launcher and Start ASDM**
- **Run ASDM as a Java Applet**

**Step 3** Click **Download ASDM Launcher and Start ASDM**.

The installer downloads to your PC.

**Step 4** Run the installer to install the ASDM Launcher.

---

## Starting ASDM

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

- [Starting ASDM from the ASDM Launcher, page 2-6](#)
- [Using ASDM in Demo Mode, page 2-7](#)
- [Starting ASDM from a Web Browser, page 2-8](#)

## Starting ASDM from the ASDM Launcher

The ASDM Launcher is for Windows only.

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

---

**Step 1** Double-click the Cisco ASDM Launcher shortcut on your desktop, or start it from the **Start** menu.

- Step 2** Enter the security appliance IP address or hostname, your username, and your password, and then click **OK**.

If there is a new version of ASDM on the security appliance, the ASDM Launcher automatically downloads it before starting ASDM.

---

## Using ASDM in Demo Mode

ASDM Demo Mode is available as a separately installed application running under Windows. It makes use of the ASDM Launcher and pre-packaged configuration files to let you run ASDM without having a live device available. ASDM Demo Mode lets you:

- Perform configuration and select 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 Content Security and Control SSM (CSC SSM).

ASDM Demo Mode provides simulated monitoring data, including real-time system log messages. The data shown is randomly generated, but the experience is identical to what you would see when connecting to a real device.

ASDM Demo Mode has the following limitations:

- Changes made to the configuration will appear in the GUI but are not applied to the configuration file. That is, when you click the Refresh button, it will revert back to the original configuration. The changes are never saved to the configuration file.
- File/Disk operations are not supported.
- Monitoring and logging data are simulated. Historical monitoring data is not available.
- You can only log in as an admin user; you cannot login as a monitor-only or read-only user.
- Demo Mode does not support the following 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 Image
    - File Transfer
    - Upload image from Local PC
    - System Reload

- Toolbar/Status bar > Save
- Configuration > Interface > Edit Interface > Renew DHCP Lease
- Failover—Configuring a standby device
- These operations cause a reread of the configuration and therefore will revert it back to the original configuration.
  - Switching contexts
  - Making changes in the Interface panel
  - NAT panel changes
  - Clock panel changes

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

- 
- Step 1** If you have not yet installed the Demo Mode application, perform the following steps:
- a. Download the ASDM Demo Mode installer from <http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm>.  
The filename is `asdm-version-demo.msi`.
  - b. Double-click the installer to install the software.
- Step 2** Double-click the Cisco ASDM Launcher shortcut on your desktop, or start it from the **Start** menu.
- Step 3** Click the **Run in Demo Mode** check box.
- Step 4** To set the platform, context and firewall modes, and ASDM Version, click the **Demo** button and make your selections from the Demo Mode area.
- Step 5** If you want to use new ASDM images as they come out, you can either download the latest installer, or you can download the normal ASDM images and install them for Demo Mode:
- a. Download the image from <http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm>.  
The filename is `asdm-version.bin`.
  - b. In the Demo Mode area, click **Install ASDM Image**.  
A file browser appears. Find the ASDM image file in the browser.
- Step 6** Click **OK** to launch ASDM Demo Mode.  
You see a Demo Mode label in the title bar of the window.
- 

## 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`

In transparent firewall mode, enter the management IP address.



---

**Note** Be sure to enter `https`, not `http`.

---

- Step 2** Click **OK** or **Yes** to all browser prompts, including the name and password prompt. By default, leave the name and password blank.
- A page displays with the following buttons:
- **Download ASDM Launcher and Start ASDM**
  - **Run ASDM as a Java Applet**
- Step 3** Click **Run ASDM as a Java Applet**.
- Step 4** Click **OK** or **Yes** to all Java prompts, including the name and password prompt. By default, leave the name and password blank.
- 

## History Metrics

The History Metrics pane lets you configure the security appliance to keep a history of various statistics, which can be displayed by ASDM on any [Graph/Table](#). If you do not enable history metrics, you can only monitor statistics in real time. Enabling history metrics lets you view statistics graphs from the last 10 minutes, 60 minutes, 12 hours, and 5 days.

### Fields

- **ASDM History Metrics**—Enables history metrics. Unchecking this check box clears and disables the history metrics.

### Modes

The following table shows the modes in which this feature is available:

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System
•	•	•	•	—

## Configuration Overview

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

- Step 1** Use the [Startup Wizard](#) for initial configuration by clicking **Wizards > Startup Wizard**.
- Step 2** To configure VPN connections, use the [VPN Wizard](#) by clicking **Wizards > VPN Wizard** and completing each screen that appears.
- Step 3** Configure advanced features by clicking the **Configuration** button on the toolbar and then clicking a feature button. Features include:
- **Configuring Interfaces**—Configures basic interface parameters including the IP address, name, security level, and for transparent mode, the bridge group.
  - **Security Policy**—Includes access rules, AAA rules, filter rules, and service policy rules.

- **Access Rules**—Permits or denies 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)**—Permits or denies non-IP traffic through the security appliance.
- **AAA Rules**—Requires authentication and/or authorization for certain types of traffic, for example, for HTTP. The security appliance also sends accounting information to a RADIUS or TACACS+ server.
- **Filter Rules**—Prevents outbound access to specific websites or FTP servers. The security appliance works with a separate server running either Websense Enterprise or Sentian by N2H2. See Configuration > Properties > URL Filtering to configure the URL filtering server, which must be configured before you add a rule.
- **Service Policy Rules**—Applies 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 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 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 lets you use private addresses, which are not routable on the Internet, on your inside networks.
- **VPN**—Configures VPN connections.
  - **VPN Wizard**—Runs the VPN wizard.
  - **E-Mail Proxy**—Configures e-mail proxies. E-mail proxies extend remote e-mail capability to WebVPN users.
  - **General**—Sets general VPN configuration parameters.
  - **IKE**—IKE, also called ISAKMP, is the negotiation protocol that lets two hosts agree on how to build an IPsec security association.
  - **IP Address Management**—Sets the IP addresses of clients after they connect through the VPN tunnel.
  - **IPsec**—Configures the IPsec protocol for VPN tunnels.
  - **Load Balancing**—Configures load balancing for VPN connections.
  - **WebVPN**—Configures WebVPN. WebVPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser.
- **CSD Manager**—Configures the CSC SSM (available for the ASA 5500 series adaptive security appliance).
- **Configuring IPS**—Configures the AIP SSM (available for the ASA 5500 series adaptive security appliance).
- **Configuring Dynamic And Static Routing**—(Single mode only) Configures OSPF, RIP, static, and asymmetric routing.
- **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 security appliance. These reusable components, or global objects, include the following:
  - Hosts/Networks
  - Inspect Maps

- TCP Maps
- Time Ranges

- Step 4** Monitor the security appliance by clicking the **Monitoring** button on the toolbar and then clicking the feature button. Features include:
- [Monitoring Interfaces](#)—Monitors the ARP table, DHCP, dynamic access list, and interface statistics.
  - [Monitoring Routing](#)—Monitors routes, OSPF LSAs, and OSPF neighbors.
  - [Monitoring Properties](#)—Monitors management sessions, AAA servers, failover, CRLs, the DNS cache, and system statistics.
  - [Monitoring System Log Messages](#)—Monitors system log messages.
  - [Monitoring Failover](#)—(For the system in multiple mode) Monitors failover in the system.

