



## CHAPTER 3

# Using the Startup Wizard

---

## Startup Wizard

The ASDM Startup Wizard walks you through, step by step, the initial configuration of your security appliance. As you click through the configuration screens, you will be prompted to enter information about your security appliance. The Startup Wizard will apply these settings, so you should be able to start using your security appliance right away.

The Startup Wizard defines the following in your configuration:

- A hostname for your security appliance.
- A domain name for your security appliance.
- An enable password that is used to restrict administrative access to the security appliance through ASDM or the command-line interface.
- The IP address information of the outside interface on the security appliance.
- The other interfaces of your security appliance, such as the inside or DMZ interfaces, can be configured from the Startup Wizard.
- NAT or PAT rules for your security appliance.
- DHCP settings for the inside interface, such as for use with a DHCP server.

More information about each setting is available by clicking the Help button on the corresponding configuration screen.

Before you begin using the Startup Wizard, make sure you have the following information available:

- A unique hostname to identify the security appliance on your network.
- The IP addresses of your outside, inside, and other interfaces.
- The IP addresses to use for NAT or PAT configuration.
- The IP address range for the DHCP server.

Remember:

- You can access the Startup Wizard from the Cisco ASDM 5.2 Start page by selecting the 'Run Startup Wizard as a Java Applet' button.
- You can access the Startup Wizard at any time using the Wizards menu in ASDM.
- The Help button is an icon with a question mark.
- On subsequent Startup Wizard pages, you can click **Finish** to complete the wizard at any time. This sends changes made in the Startup Wizard to the security appliance.

**Important Notes**

- The security appliance can run in two modes:
  - Routed—In routed mode, the security appliance acts as a router between connected networks. Each interface requires an IP address on a different subnet. The security appliance performs NAT between connected networks. In single context mode, the routed firewall supports OSPF and RIP (in passive mode). Multiple context mode supports static routes only. Routed mode supports up to 256 interfaces per context or in single mode, with a maximum of 1000 interfaces divided between all contexts. Each interface is on a different subnet. You can share interfaces between contexts.

In routed mode, some types of traffic cannot pass through the security appliance even if you allow it in an ACL. The transparent firewall, however, can allow any traffic through using either an extended ACL (for IP traffic) or an EtherType ACL.




---

**Note** We recommend using the advanced routing capabilities of the upstream and downstream routers, such as the MSFC, instead of relying on the security appliance for extensive routing needs.

---

- Transparent—In transparent mode, the security appliance is not seen as a router hop to connected devices, but acts like a “bump in the wire,” or a “stealth firewall.” The security appliance connects the same network on its inside and outside ports, but uses different VLANs on the inside and outside. No dynamic routing protocols or NAT are required. Transparent mode only supports two interfaces, an inside interface and an outside interface. Transparent mode helps simplify the configuration and reduces its visibility to attackers. You can also use a transparent firewall for traffic that would otherwise be blocked in routed mode. For example, a transparent firewall can allow multicast streams.

Even though transparent mode acts as a bridge, Layer 3 traffic, such as IP traffic, cannot pass through the security appliance unless you explicitly permit it with an extended ACL. The only traffic allowed through the transparent firewall without an ACL is ARP traffic. ARP traffic can be controlled by ARP inspection.




---

**Note** The transparent mode security appliance does not pass CDP packets.

---

- The context mode (single or multiple) is not stored in the configuration file, even though it does endure reboots. If you need to copy your configuration to another device, set the mode on the new device to match using the mode command.

When you convert from single mode to multiple mode, the security appliance converts the running configuration into two files: a new startup configuration that comprises the system configuration, and admin.cfg that comprises the admin context (in the root directory of the internal Flash memory).

- With a full license, the security appliance supports up to five interfaces with a maximum of three interfaces named ‘interface.’ In restricted mode, the security appliance supports up to three interfaces, and in transparent mode, the security appliance supports up to two interfaces.

Once the maximum number of interfaces has been created, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and may have to select from an existing VLAN.

- You should use a port in Slot 0 for the inside interface and a port in Slot 1 for the outside interface. Using two different slots puts traffic on two different internal buses, which could improve performance.

- The security appliance can be used as an Easy VPN remote device. However, if the security appliance is configured to function as an Easy VPN remote device, it cannot establish other types of tunnels. For example, the security appliance cannot function simultaneously as both an Easy VPN remote device and as one end of a standard peer-to-peer VPN deployment.

There are two modes of operation when using the security appliance as an Easy VPN remote device:

- Client Mode
- Network Extension Mode

When configured in Easy VPN Client Mode, the security appliance does not expose the IP addresses of clients on its inside network. Instead, it uses NAT (Network Address Translation) to translate the IP addresses on the private network to a single, assigned IP address. When the security appliance is configured in Client Mode, you cannot ping or access any device from outside the private network.

When configured in Easy VPN Network Extension Mode, the security appliance does not protect the IP addresses of local hosts by substituting a assigned IP address. Therefore, hosts on the other side of the VPN connection can communicate directly with hosts on the local network.

### Fields

Launch Startup Wizard—Launches the Startup Wizard.



#### Note

The Launch Startup Wizard button does not appear if you click Wizards >Startup Wizard on the toolbar.

With the exception of this screen, all screens in the Startup Wizard display the following buttons:

- Back—Returns you to the previous screen (the button is dim in this screen).
- Next—Advances you to the next screen.
- Finish—Submits your configuration to the security appliance based upon choices made in this screen (the button is dim in this screen).
- Cancel—Discards any changes without applying them. The Wizard prompts you with the Exit Wizard dialog box when Cancel is clicked. Clicking Exit closes the Wizard, and clicking Cancel again returns you to the Wizard screen. Remember at any time in the Wizard you can click Back to return to the previous screen.

### Modes

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

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

## Starting Point

### Benefits

The Starting Point screen lets you continue with your existing configuration or reset the configuration to the factory default values. If you check the box 'Reset configuration to existing defaults,' you revert back to the IP address and subnet mask of the default inside interface. If you continue with your existing configuration, you automatically retain your IP address and subnet mask.

### Fields

The Starting Point screen displays the Next, Cancel, and Help buttons, in addition to the following:

- Modify existing configuration—Click to start the wizard with the existing configuration.
- Reset configuration to factory defaults—Click to start the wizard at the factory default values for the inside interface.
  - Configure the IP address of the management interface—Check this box to configure the IP address and subnet mask of the management interface.

IP Address—Lets you enter the IP address of the management interface to configure.

Subnet Mask—Lets you enter the subnet mask of the management interface to configure.



**Note** If you reset the configuration to the factory defaults, you cannot undo the change by cancelling the wizard.



**Note** The Back and Finish buttons are disabled on this screen.

### Modes

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

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

### For More Information

This feature is available in the main ASDM application screen:

File > Reset Device to the Factory Default Configuration

## Basic Configuration

### Benefits

The Basic Configuration screen lets you configure the hostname of your security appliance and the enable password, as well as a domain name for the security appliance.

The domain name should be less than 64 characters (maximum 63 characters) alphanumeric and mixed case.

The enable password is used to administer ASDM or to administer the security appliance from the Command Line Interface. The password is case-sensitive and can be up to 16 alphanumeric characters. If you want to change the current password, check **Change privileged mode (enabled) password**, enter the old password, then enter the new password, and confirm the new password in the fields provided.

**Note**

If you leave the password field blank, a Password Confirmation screen displays and notifies you that this is a high security risk.

**Fields**

The Basic Configuration screen displays the Back, Next, Finish, Cancel, and Help buttons, in addition to the following:

- **Host Name**—Lets you enter a hostname for the security appliance. The hostname can be up to 63 alphanumeric characters and mixed case. Note: This field will list either ASA or PIX before Host Name, depending on the platform you are using.
- **Domain Name**—Specifies the IPsec domain name of the security appliance. This can be used later for certificates. There is a 64-character limit on the domain name (maximum 63 characters), and it must be alphanumeric with no special characters or spaces.
- **Privileged Mode (Enable) Password area**—Lets you restrict administrative access to the security appliance through ASDM or the Command Line Interface.
  - **Change privileged mode (enable) Password**—Check this box to change the current privileged mode (enable) password.
  - **Old Password**—Lets you enter the old enable password, if one exists.
  - **New Password**—Lets you enter the new enable password. The password is case-sensitive and can be up to 16 alphanumeric characters.
  - **Confirm New Password**—Lets you reenter the new enable password.

**Modes**

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

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

**For More Information**

This feature is available in the main ASDM application screen:

Configuration > Properties > Device Administration > Device

Configuration > Properties > Device Administration > Password

## Outside Interface Configuration

### Benefits

The Outside Interface Configuration screen lets you configure your outside interface by specifying an IP address, or obtaining one from a PPPoE or a DHCP server.

### Fields

The Outside Interface Configuration screen displays the Back, Next, Finish, Cancel, and Help buttons, in addition to the following:

- **Interface Properties area**
  - Interface—Lets you add a new interface, or select an interface from the drop-down list.
  - Interface Name—Lets you add a name to a new interface, or displays the name associated with an existing interface.
  - Enable interface—Check this box to activate the interface in privileged mode.
  - Security Level—Displays the security level range for the interface from 0 to 100, with 100 assigned to the inside interface and 0 assigned to the outside interface. Perimeter interfaces can use any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default.

- **IP Address area**

- **Use PPPoE—Click to obtain an IP address from a PPP over Ethernet (PPPoE) server for the interface.**

The default authentication method for PPPoE is Password Authentication Protocol (PAP). You have the option of configuring Challenge Handshake Authentication Protocol (CHAP) or Microsoft CHAP (MSCHAP) manually.

- **Use DHCP—Click to obtain an IP address from a Dynamic Host Configuration Protocol server so that IP addresses can be reused when hosts no longer need them.**




---

**Note** DHCP clients initially have no configured IP address, and must send a broadcast request to obtain an IP address from a DHCP server.

---

Obtain default route using DHCP—Check this box to obtain an IP address for the default gateway using DHCP.




---

**Note** DHCP is used by workstations (hosts) to get initial configuration information, such as an IP address, subnet mask, and default gateway upon bootup.

---

- **Use the following IP address—Click to manually specify an IP address for the interface:**
  - IP Address**—Lets you enter an IP address for an outside interface.
  - Subnet Mask**—Lets you enter a subnet mask for an outside interface, or alternatively, choose a selection from the drop-down list.

### Modes

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

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

**For More Information**

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## Internet (Outside) VLAN Configuration

**Benefits**

The Internet (Outside) VLAN Configuration screen lets you configure your Internet interface by specifying an IP address, or obtaining one from a PPPoE or a DHCP server.

**Important Notes**

With a full license, the security appliance supports up to five interfaces with a maximum of three interfaces named ‘interface.’ In restricted mode, the security appliance supports up to three interfaces, and in transparent mode, the security appliance supports up to two interfaces.

Once the maximum number of interfaces has been created, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and may have to select from an existing VLAN.

**Fields**

The Internet (Outside) VLAN Configuration screen displays the Back, Next, Finish, Cancel, and Help buttons, in addition to the following:

- **Select Internet Interface area**
  - Choose an interface—Click to choose an interface to configure, then select an interface from the drop-down list.
  - Create new VLAN interface—Click to create a new VLAN interface, then enter the new VLAN number.
 

If the maximum number of interfaces has already been created, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and may have to select from an existing VLAN. See the [Important Notes](#) section for additional information.
- Enable interface—Check this box to activate the interface in privileged mode.
- **Interface Name**—Lets you specify a name for the interface.
- **Security Level**—Lets you enter a security level range for the interface from 0 to 100, with 100 assigned to the inside interface and 0 assigned to the outside interface. Perimeter interfaces can use any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default.
- **IP Address area**
  - Use PPPoE—Click to obtain a dynamic IP address from a PPPoE server for an Internet interface.

- **Use DHCP**—Click to obtain an IP address for the Internet interface from a DHCP server.



**Note** DHCP clients initially have no configured IP address, and must send a broadcast request to obtain an IP address from a DHCP server.

Obtain default route using DHCP—Check this box to obtain an IP address for the default gateway using DHCP.



**Note** DHCP is used by workstations (hosts) to get initial configuration information, such as an IP address, subnet mask, and default gateway upon bootup.

- **Use the following IP address**—Click to specify an IP address for an Internet interface rather than obtaining one from a PPPoE server or DHCP server:

**IP Address**—Lets you enter an IP address for an Internet interface.

**Subnet Mask**—Lets you enter a subnet mask for an Internet interface, or alternatively, choose a selection from the drop-down list.

**Modes**

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

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

**For More Information**

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## Outside Interface Configuration - PPPoE

**Benefits**

The Outside Interface Configuration - PPPoE screen lets you configure your interface by obtaining an IP address from a PPPoE server. The ASA device is the PPPoE on the specified interface.

Before any network layer protocols can be routed, a connection must be opened and negotiated, in this case, using PPPoE authentication.

**Fields**

The Outside Interface Configuration - PPPoE screen displays the Back, Next, Finish, Cancel, and Help buttons, in addition to the following:

- **Group Name**—Lets you specify the name of the interfaces.



**Note** You must specify a group name in order to proceed.

- **User Authentication area**

- PPPoE Username—Lets you specify the PPPoE username for authentication purposes.
- PPPoE Password—Lets you specify the PPPoE password for authentication purposes.
- Confirm PPPoE Password—Lets you confirm the PPPoE password.

- **Authentication Method area**

The default authentication method for PPPoE is Password Authentication Protocol (PAP). You have the option of configuring Challenge Handshake Authentication Protocol (CHAP) or Microsoft CHAP (MSCHAP) manually.

- PAP—Check this to select the Password Authentication Protocol as the authentication method. PAP is the simplest authentication protocol. The username and password are sent unencrypted using this method.
- CHAP—Check this to select the Challenge Handshake Authentication Protocol method.  
CHAP does not prevent unauthorized access; it merely identifies the remote end. Then, the access server determines whether the user is allowed access.
- MSCHAP—Check this to select the Microsoft Challenge Handshake Authentication Protocol authentication for PPP connections between a computer using a Microsoft Screens operating system and an access server.

- **IP Address area**

- **Obtain IP Address using PPPoE—Click to obtain an IP address using a PPPoE server.**

The default authentication method for PPPoE is Password Authentication Protocol (PAP). You have the option of configuring Challenge Handshake Authentication Protocol (CHAP) or Microsoft CHAP (MSCHAP) manually.

- **Specify an IP address—Click to specify an IP address for an interface rather than obtaining one from a PPPoE server:**

**IP Address**—Lets you enter an IP address for an interface.

**Subnet Mask**—Lets you enter a subnet mask for an interface, or alternatively, choose a selection from the drop-down list.

- **Obtain default route using PPPoE—Click to obtain the default route between the PPPoE server and the PPPoE client.**

### Modes

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

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

### For More Information

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## Internet (Outside) VLAN Configuration - PPPoE

### Benefits

The Internet (Outside) VLAN Configuration - PPPoE screen lets you configure your interface by obtaining an IP address from a PPPoE server. The ASA device is the PPPoE on the specified interface.

Before any network layer protocols can be routed, a connection must be opened and negotiated, in this case, using PPPoE authentication.

### Fields

The Internet (Outside) VLAN Configuration - PPPoE screen displays the Back, Next, Finish, Cancel, and Help buttons, in addition to the following:

- **Group Name**—Lets you specify the name of the interfaces.



---

**Note** You must specify a group name in order to proceed.

---

- **User Authentication area**

- PPPoE Username—Lets you specify the PPPoE username for authentication purposes.
- PPPoE Password—Lets you specify the PPPoE password for authentication purposes.
- Confirm PPPoE Password—Lets you confirm the PPPoE password.

- **Authentication Method area**

The default authentication method for PPPoE is Password Authentication Protocol (PAP). You have the option of configuring Challenge Handshake Authentication Protocol (CHAP) or Microsoft CHAP (MSCHAP) manually.

- PAP—Check this to select the Password Authentication Protocol as the authentication method. PAP is the simplest authentication protocol. The username and password are sent unencrypted using this method.
- CHAP—Check this to select the Challenge Handshake Authentication Protocol method. CHAP does not prevent unauthorized access; it merely identifies the remote end. Then, the access server determines whether the user is allowed access.
- MSCHAP—Check this to select the Microsoft Challenge Handshake Authentication Protocol authentication for PPP connections between a computer using a Microsoft screens operating system and an access server.

- **IP Address area**

- **Obtain IP Address using PPPoE**—Click to obtain an IP address using a PPPoE server.

The default authentication method for PPPoE is Password Authentication Protocol (PAP). You have the option of configuring Challenge Handshake Authentication Protocol (CHAP) or Microsoft CHAP (MSCHAP) manually.

- **Specify an IP address**—Click to specify an IP address for an interface rather than obtaining one from a PPPoE server:

**IP Address**—Lets you enter an IP address for an interface.

**Subnet Mask**—Lets you enter a subnet mask for an interface, or alternatively, choose a selection from the drop-down list.

- Obtain default route using PPPoE—Click to obtain the default route between the PPPoE server and the PPPoE client.

### Modes

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

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

### For More Information

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## Inside Interface Configuration

### Benefits

The Inside Interface Configuration screen lets you configure an inside interface by specifying an IP address, or obtaining one from a PPPoE or a DHCP server.



#### Note

If VLAN is configured, the screen displays a message that in order to make additional changes, you should go to Configuration > Interfaces.

### Important Notes

With a full license, the security appliance supports up to five interfaces with a maximum of three interfaces named ‘interface.’ In restricted mode, the security appliance supports up to three interfaces, and in transparent mode, the security appliance supports up to two interfaces.

Once the maximum number of interfaces has been created, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and may have to select from an existing VLAN.

### Fields

The Inside Interface Configuration screen displays the Back, Next, Finish, Cancel, and Help buttons, in addition to the following:

- **Select Inside Interface area**
  - Choose an interface—Choose an interface to configure from the drop-down list.
  - Create new VLAN interface—Click to create a new inside interface
  - Enable interface—Check this box to activate the interface in privileged mode.
- **Interface Name**—Lets you specify a name for the interface.

- **Security Level**—Lets you enter a security level range for the interface from 0 to 100, with 100 assigned to the inside interface and 0 assigned to the outside interface. Perimeter interfaces can use any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default.
- **IP Address area**
  - **Use PPPoE**—Click to obtain an IP address from a PPPoE server for an inside interface.
  - **Use DHCP**—Click to obtain an IP address for the inside interface from a DHCP server.



**Note** DHCP clients initially have no configured IP address, and must send a broadcast request to obtain an IP address from a DHCP server.

Obtain default route using DHCP—Check this box to obtain an IP address for the default gateway using DHCP.



**Note** DHCP is used by workstations (hosts) to get initial configuration information, such as an IP address, subnet mask, and default gateway upon bootup.

- **Use the following IP address**—Lets you specify an IP address for an inside interface rather than obtaining one from a PPPoE server or DHCP server:

**IP Address**—Lets you specify an IP address for an inside interface.

**Subnet Mask**—Lets you specify a subnet mask for an inside interface; the list displays a selection of subnet mask IP addresses.

**Modes**

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

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

**For More Information**

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## Business (Inside) VLAN Configuration

**Benefits**

The Business (Inside) VLAN Configuration screen lets you configure an inside interface by specifying an IP address, or obtaining one from a PPPoE or a DHCP server.

**Note**

If VLAN is configured, the screen displays a message that in order to make additional changes, you should go to Configuration > Interfaces.

**Important Notes**

With a full license, the security appliance supports up to five interfaces with a maximum of three interfaces named 'interface.' In restricted mode, the security appliance supports up to three interfaces, and in transparent mode, the security appliance supports up to two interfaces.

Once the maximum number of interfaces has been created, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and may have to select from an existing VLAN.

**Fields**

The Business (Inside) VLAN Configuration screen displays the Back, Next, Finish, Cancel, and Help buttons, in addition to the following:

- **Select Inside Interface area**
  - Choose an interface—Choose an interface to configure from the drop-down list.
  - Create new VLAN interface—Click to create a new inside interface
  - Enable interface—Check this box to activate the interface in privileged mode.
- **Interface Name**—Lets you specify a name for the interface.
- **Security Level**—Lets you enter a security level range for the interface from 0 to 100, with 100 assigned to the inside interface and 0 assigned to the outside interface. Perimeter interfaces can use any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default.
- **IP Address area**
  - **Use PPPoE**—Click to obtain an IP address from a PPPoE server for an inside interface.
  - **Use DHCP**—Click to obtain an IP address for the inside interface from a DHCP server.

**Note**

DCHP clients initially have no configured IP address, and must send a broadcast request to obtain an IP address from a DHCP server.

Obtain default route using DHCP—Check this box to obtain an IP address for the default gateway using DHCP.

**Note**

DHCP is used by workstations (hosts) to get initial configuration information, such as an IP address, subnet mask, and default gateway upon bootup.

- **Use the following IP address**—Lets you specify an IP address for an inside interface rather than obtaining one from a PPPoE server or DHCP server:

**IP Address**—Lets you specify an IP address for an inside interface.

**Subnet Mask**—Lets you specify a subnet mask for an inside interface; the list includes a selection of subnet mask IP addresses.

### Modes

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

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

### For More Information

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## DMZ Interface Configuration

### Benefits

The DMZ Interface Configuration screen lets you configure a work interface.

The security appliance supports up to three fully functional named interfaces; in transparent mode, the security appliance supports up to two interfaces. Typically one interface connects to the outside Internet (known as an Internet zone), another connects to a home network (known as a home zone), and the third interface (known as a work interface), operates similarly to a demilitarized zone (DMZ). A DMZ is a separate network located in the neutral zone between a private (inside) network and a public (outside) network.

### Important Notes

With a full license, the security appliance supports up to five interfaces with a maximum of three interfaces named 'interface.' In restricted mode, the security appliance supports up to three interfaces, and in transparent mode, the security appliance supports up to two interfaces.

Once the maximum number of interfaces has been created, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and may have to select from an existing VLAN.

### Fields

The DMZ Interface Configuration screen displays the Back, Next, Finish, Cancel, and Help buttons, in addition to the following:

- **Select Work Interface area**
  - Choose an interface—Choose an interface to configure from the drop-down list.
  - Create new VLAN interface—Check this box to create a new work interface.
  - Enable interface—Check this box to activate the interface in privileged mode.
- **Interface Name**—Lets you specify a name for the interface.
- **Security Level**—Lets you enter a security level range for the interface from 0 to 100, with 100 assigned to the inside interface and 0 assigned to the outside interface. Perimeter interfaces can use any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default.
- **IP Address area**

- **Use PPPoE**—Check this box to obtain an IP address from a PPPoE server for a work interface.
- **Use DHCP**—Check this box to obtain an IP address for a work interface from a DHCP server.



**Note** DHCP clients initially have no configured IP address, and must send a broadcast request to obtain an IP address from a DHCP server.

Obtain default route using DHCP—Check this box to obtain an IP address for the default gateway using DHCP.



**Note** DHCP is used by workstations (hosts) to get initial configuration information, such as an IP address, subnet mask, and default gateway upon bootup.

- **Use the following IP address**—Lets you specify an IP address for a work interface rather than obtaining one from a PPPoE server or DHCP server:

**IP Address**—Lets you specify an IP address for a work interface.

**Subnet Mask**—Lets you specify a subnet mask for a work interface; use the drop-down list to select a subnet mask IP address.

### Modes

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

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

### For More Information

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## Home (DMZ) VLAN Configuration

### Benefits

The Home (DMZ) VLAN Configuration screen lets you configure a work interface.

The security appliance supports up to three fully functional named interfaces; in transparent mode, the security appliance supports up to two interfaces. Typically one interface connects to the outside Internet (known as an Internet zone), another connects to a home network (known as a home zone), and the third interface (known as a work interface), operates similarly to a demilitarized zone (DMZ). A DMZ is a separate network located in the neutral zone between a private (inside) network and a public (outside) network.

### Important Notes

With a full license, the security appliance supports up to five interfaces with a maximum of three interfaces named 'interface.' In restricted mode, the security appliance supports up to three interfaces, and in transparent mode, the security appliance supports up to two interfaces.

Once the maximum number of interfaces has been created, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and may have to select from an existing VLAN.

### Fields

The Home (DMZ) VLAN Configuration screen displays the Back, Next, Finish, Cancel, and Help buttons, in addition to the following:

- **Select Work Interface area**
  - Choose an interface—Choose an interface to configure from the drop-down list.
  - Create new VLAN interface—Check this box to create a new work interface.
  - Enable interface—Check this box to activate the interface in privileged mode.
- **Interface Name**—Lets you specify a name for the interface.
- **Security Level**—Lets you enter a security level range for the interface from 0 to 100, with 100 assigned to the inside interface and 0 assigned to the outside interface. Perimeter interfaces can use any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default.
- **IP Address area**
  - **Use PPPoE**—Check this box to obtain an IP address from a PPPoE server for a work interface.
  - **Use DHCP**—Check this box to obtain an IP address for a work interface from a DHCP server.




---

**Note** DHCP clients initially have no configured IP address, and must send a broadcast request to obtain an IP address from a DHCP server.

---

Obtain default route using DHCP—Check this box to obtain an IP address for the default gateway using DHCP.




---

**Note** DHCP is used by workstations (hosts) to get initial configuration information, such as an IP address, subnet mask, and default gateway upon bootup.

---

- **Use the following IP address**—Lets you specify an IP address for a work interface rather than obtaining one from a PPPoE server or DHCP server:

**IP Address**—Lets you specify an IP address for a work interface.

**Subnet Mask**—Lets you specify a subnet mask for a work interface; use the drop-down list to display a selection of subnet mask IP addresses.

### Modes

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

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

**For More Information**

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## Switch Port Allocation

**Benefits**

The Switch Port Allocation screen lets you allocate switch ports to your outside, inside, and work interface. As VLANs are port-based, you must add the ports to their respective VLANs. By default, all switch ports begin in VLAN1.

**Fields**

The Switch Port Allocation screen displays the Back, Next, Finish, Cancel, and Help buttons, in addition to the following:

Allocate Switch Ports to your Outside Interface (*vlanid*) area

- Available Ports—Lets you select a port to add or remove from the available list of ports.
- Allocated Ports—Lets you select a port to add or remove from the allocated list of ports.
- Add—Lets you add a port to the available or allocated list of ports.
- Remove—Lets you remove a port from the available or allocated list of ports.

Allocate Switch Ports to your Inside Interface (*vlanid*) area

- Available Ports—Lets you select a port to add or remove from the available list of ports.
- Allocated Ports—Lets you select a port to add or remove from the allocated list of ports.
- Add—Lets you add a port to the available or allocated list of ports.
- Remove—Lets you remove a port from the available or allocated list of ports.

Allocate Switch Ports to your Work Interface (*vlanid*) area

- Available Ports—Lets you select a port to add or remove from the available list of ports.
- Allocated Ports—Lets you select a port to add or remove from the allocated list of ports.
- Add—Lets you add a port to the available or allocated list of ports.
- Remove—Lets you remove a port from the available or allocated list of ports.

**Modes**

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

Firewall Mode		Security Context		
Routed	Transparent <sup>1</sup>	Single	Multiple	
			Context	System
•	•	•	•	—

1. Work interface is hidden in transparent mode.

#### For More Information

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## General Interface Configuration

### Benefits

The General Interface Configuration screen lets you enable and restrict traffic between interfaces and between hosts connected to the same interface.

### Important Notes

Restricted traffic is not an optional configuration. If you only have a restricted license, you must restrict from one interface to any of the other interfaces. Typically, this is the traffic from the work interface to the inside interface, but any pair can be chosen. The Restrict Traffic area fields are hidden if you have a full license or if the device is in transparent mode.

### Fields

The General Interface **Configuration** screen displays the **Back**, **Next**, **Finish**, **Cancel**, and **Help** buttons, in addition to the following:

- Enable traffic between two or more interfaces with the same security level—Check this box to enable traffic between two or more interfaces with the same security level.
- Enable traffic between two or more hosts connected to the same interface—Check this box to enable traffic between two or more hosts connected to the same interface.

Restrict traffic area



#### Note

Restricted traffic is not an optional configuration. If you only have a restricted license, you must restrict from one interface to any of the other interfaces. These fields are hidden if you have a full license or if the device is in transparent mode.

- From interface—Lets you restrict traffic from an interface by selecting an interface from the drop-down menu.
- To interface—Lets you restrict traffic to an interface by selecting an interface from the drop-down menu.

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

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

**For More Information**

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## Static Routes

**Benefits**

The [Static Routes](#) screen lets you create static routes that will access networks connected to a router on any interface. To enter a default route, set the IP address and mask to 0.0.0.0, or the shortened form of 0.

If an IP address from one security appliance interface is used as the gateway IP address, the security appliance will ARP the designated IP address in the packet instead of ARPing the gateway IP address.

Leave the Metric at the default of 1 unless you are sure of the number of hops to the gateway router.

## Add/Edit Static Routes

**Benefits**

The [Add/Edit Static Route](#) dialog box lets you add or edit a static route.

## Route Monitoring Options

**Benefits**

The [Route Monitoring Options](#) dialog box lets you set the parameters for monitoring the static route.

## Auto Update Server

**Benefits**

The Auto Update Server screen allows you to remotely manage the ASA device. This includes automatically updating the ASA configuration, ASA image, and the ASDM image.

**Fields**

The Auto Update Server screen displays the **Back**, **Next**, **Finish**, **Cancel**, and **Help** buttons, in addition to the following:

- **Enable Auto Update**—Check this box to enable communication between the security appliance and an Auto Update Server.

- Server area
  - Server URL—Click the drop-down list to select either the secure http (https) or http to designate the beginning of the URL for the Auto Update server. In the next box, enter the remainder of the IP address for the Auto Update server.
  - Verify server SSL certificate—Check this box to confirm that a SSL certificate is enabled on the Auto Update Server.
- User area
  - Username—Enter the username to log in to the Auto Update server.
  - Password—Enter the password to log in to the Auto Update server.
  - Confirm Password—Enter the password again to confirm it.
- Device Identify area
  - Device ID Type—Click the drop-down list to select the type of ID to uniquely identify the security appliance. Selecting User-defined name enables the Device ID field, where you can specify a unique ID.
  - Device ID—Enter a unique string to use as security appliance ID.

### Modes

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

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

### For More Information

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## DHCP Server

### Benefits

The DHCP Server screen lets you configure the security appliance as a Dynamic Host Control Protocol (DHCP) server to hosts on the inside interface. You can configure a range of IP addresses in an address pool, then when a host on the inside interface makes a request for an IP address using DHCP, the security appliance assigns it an address from this pool.

### Important Notes

- DNS, WINS and other information for interfaces with the lowest security level (inside interfaces) can be set in this screen. To configure the DHCP server for other interfaces, go to the Configuration > Properties > DHCP Services > DHCP Server in the main ASDM screen.
- The number of addresses allowed in the DHCP pool is 256.

- If you configure ASDM to use the DHCP server option, the security appliance uses the inside IP address, adds one address, and configures the address pool based on the number of addresses available according to your feature license and platform. The pool size varies, and might be configured for fewer IP addresses than you are licensed to use to simplify the configuration.

### Fields

The **DHCP Server** screen displays the **Back**, **Next**, **Finish**, **Cancel**, and **Help** buttons, in addition to the following:

- **Enable DHCP server on the inside interface**—Check this box to turn on DHCP for the security appliance.
  - **DHCP Address Pool area**
    - Starting IP Address**—Enter the starting range of the DHCP server pool in a block of IP addresses from the lowest to highest. The security appliance supports 256 IP addresses.
    - Ending IP Address**—Enter the ending range of the DHCP server pool in a block of IP addresses from the lowest to highest. The security appliance supports 256 IP addresses.
  - **DHCP Parameters area**
    - Enable auto-configuration—Check this box to allow the wizard to configure the DNS server, WINS server, lease length, and ping timeout.
    - DNS Server 1**—Enter the IP address of the DNS server to use DNS.
    - WINS Server 1**—Enter the IP address of the WINS (screens Internet Naming Service) server to use DNS.
    - DNS Server 2**—Enter the IP address of the alternate DNS server to use DNS.
    - WINS Server 2**—Enter the IP address of the alternate WINS server to use DNS.
    - Lease Length (secs)**—Enter the amount of time (in seconds) the client can use its allocated IP address before the lease expires. The default value is 3600 seconds (1 hour).
    - Ping Timeout**—Enter the parameters for the ping timeout value in milliseconds.
    - Domain Name**—Enter the domain name of the DNS server to use DNS.

### Modes

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

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

### For More Information

This feature is available in the main ASDM application screen:

Configuration > Properties > DHCP Services > DHCP Server

## Address Translation (NAT/PAT)

**Note**

This feature is not available in transparent mode.

**Benefits**

The **Address Translation (NAT/PAT)** screen lets you configure NAT and PAT on your security appliance.

PAT lets you set up a single IP address for use as the global address. With PAT, you can set multiple outbound sessions to appear as if they originate from a single IP address. When enabled, the security appliance chooses a unique port number from the PAT IP address for each outbound translation slot. This feature is useful in smaller installations where there are not enough unique IP addresses for all outbound connections. An IP address that you specify for a port address cannot be used in another global address pool. PAT lets up to 65,535 hosts start connections through a single outside IP address.

If you decide to use NAT, enter an address range to use for translating addresses on the inside interface to addresses on the outside interface. The global addresses in the pool provide an IP address for each outbound connection, and for those inbound connections resulting from outbound connections.

**Important Notes**

If you use NAT, the range of IP addresses required on this screen creates a pool of addresses that is used outbound on the security appliance. If you have been assigned a range of Internet-registered, global IP addresses by your ISP, enter them here.

The following are limitations when using the PAT address configuration:

- Does not work with caching name servers.
- You may need to enable the corresponding inspection engine to pass multimedia application protocols through the security appliance.
- Does not work with the established command.
- When in use with a passive FTP, use the **Inspect protocol ftp strict** command statement with an **access-list** command statement to permit outbound FTP traffic.
- A DNS server on a higher level security interface, needing to get updates from a root name server on the outside interface, cannot use PAT.

**Fields**

The **Address Translation (NAT/PAT)** screen displays the **Back**, **Next**, **Finish**, **Cancel**, and **Help** buttons, in addition to the following:

- Enable traffic through the firewall without translation—Click to allow traffic through the firewall without translation.  
NAT is a one-to-one address translation; PAT is a many (inside the firewall)-to-one translation.
- **Use Network Address Translation (NAT)**—Select to enable NAT and a range of IP addresses to be used for translation.
  - **Starting Global IP Address**—Enter the first IP address in a range of IP addresses to be used for translation.
  - **Ending Global IP Address**—Enter the last IP address in a range of IP addresses to be used for translation.

- **Subnet Mask (optional)**—Specify the subnet mask for the range of IP addresses to be used for translation.
- **Use Port Address Translation (PAT)**—Select to enable PAT. You must choose one of the following if you select this option.



**Note** IPsec with PAT may not work properly because the outside tunnel endpoint device cannot handle multiple tunnels from one IP address.

- **Use the IP address on the outside interface**—The security appliance uses the IP address of the outside interface for PAT.
- **Specify an IP address**—Specify an IP address to be used for PAT.  
IP Address—Lets you enter an IP address for the outside interface for PAT.  
Subnet Mask (optional)—Lets you enter a subnet mask for the outside interface for PAT, or click the down arrow to select a subnet mask.

### Modes

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

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

### For More Information

This feature is available in the main ASDM application screen:

Configuration > NAT

## Administrative Access

### Benefits

The **Administrative Access** screen lets you configure management access on the security appliance. ASDM automatically lists the interfaces available for configuration, and in this screen you can set the IP address, interface name, and security level to make each interface unique.



### Note

This screen allows configuration of management access to interfaces already configured in other places. User cannot change such things as the IP address and the name of the interface in this screen.

### Fields

The **Administrative Access** screen displays the **Back**, **Next**, **Finish**, **Cancel**, and **Help** buttons, in addition to the following:

- **Type**—Specifies whether the host or network is accessing security appliance via HTTPS/ASDM, SSH, or Telnet.
- **Interface**—Displays the host or network name.

- **IP Address**—Displays the IP address of the host or network.
- **Mask**—Displays the subnet mask of the host or network.
- **Add**—Lets you choose access type, an interface, then specify the IP address and netmask of the host/network that will be allowed to connect to that interface for management purposes only.
- **Edit**—Lets you edit an interface.
- **Delete**—Lets you delete an interface.

## Add/Edit Administrative Access Entry

### Benefits

The **Add/Edit Administrative Access Entry** dialog box let you configure the hosts.

You must use one the following types of preconfigured connections for the Command Line Interface console sessions:

- **Telnet protocol**—A network connection using the Telnet protocol.
- **ASDM/HTTPS protocol**—A network connection using the HTTPS (HTTP over SSL) protocol for **Tools > Command Line Interface**.



---

**Note** ASDM uses HTTPS for all communication with the security appliance.

---

- **Secure Shell (SSH) protocol**—A network connection using the Secure Shell (SSH) protocol.

Before configuring your security appliance from the ASDM Command Line Interface tool, we recommend that you review the security appliance Technical Documentation. See also Password, Authentication.

For more information about the Command Line Interface commands used by each ASDM screen, see **Command Line Interface Commands Used by ASDM screens Help > About the security appliance** that will display, among other useful things, which user last changed the configuration.

### Fields

The **Add/Edit Administrative Access Entry** screen displays the **OK**, **Cancel**, and **Help** buttons, in addition to the following:

- **Access Type**—Select one of the following types of preconfigured connections for the Command Line Interface console sessions from the drop-down menu: ASDM/HTTP, SSH, or Telnet.
- **Interface Name**—Lets you select from a list of predetermined interfaces.
- **IP Address**—Lets you specify an IP address for the interface.
- **Subnet Mask**—Lets you specify a subnet mask for the interface from a selection of subnet mask IP addresses.

### Modes

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

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

#### For More Information

This feature is available in the main ASDM application screen:

Configuration > Properties > Device Access > HTTPS/ASDM

Configuration > Properties > Device Access > Telnet

Configuration > Properties > Device Access > SSH

Configuration > Properties > History Metrics

## Easy VPN Remote Configuration

### Benefits

Companies with multiple sites can establish secure communications and resource sharing among them by deploying a Cisco Easy VPN solution that consists of an Easy VPN Server at its main site and Easy VPN remote devices at remote offices. Using an Easy VPN solution simplifies the deployment and management of a Virtual Private Network in the following ways:

- Hosts at remote sites no longer have to run VPN client software.
- Security policies reside on a central server and are pushed to the remote devices when a VPN connection is established.
- Few configuration parameters need to be set locally.

When used as an Easy VPN remote device, the security appliance can also be configured to perform basic firewall services, such as protecting a web server on a DMZ from unauthorized access. However, if the security appliance is configured to function as an Easy VPN remote device, it cannot establish other types of tunnels. For example, the security appliance cannot function simultaneously as both an Easy VPN remote device and as one end of a standard peer-to-peer VPN deployment.

The Easy VPN Remote Configuration screen lets you form a secure VPN tunnel between the security appliance and a remotely located Cisco VPN 3000 Concentrator, Cisco IOS-based router, or security appliance that is acting as an Easy VPN server. The security appliance itself acts as an Easy VPN remote device to enable deployment of VPNs to remote locations via the devices listed above.

There are two modes of operation when using the security appliance as an Easy VPN remote device:

- Client Mode
- Network Extension Mode

When configured in Easy VPN Client Mode, the security appliance does not expose the IP addresses of clients on its inside network. Instead, it uses NAT (Network Address Translation) to translate the IP addresses on the private network to a single, assigned IP address. When the security appliance is configured in Client Mode, you cannot ping or access any device from outside the private network.

When configured in Easy VPN Network Extension Mode, the security appliance does not protect the IP addresses of local hosts by substituting a assigned IP address. Therefore, hosts on the other side of the VPN connection can communicate directly with hosts on the local network.

Use the following guidelines when deciding whether to configure the security appliance in Easy VPN Client or Network Extension Mode:

Use Client Mode if:

- You want VPN connections to be initiated by client traffic
- You want the IP addresses of local hosts to be hidden from remote networks
- You are using DHCP on the ASA 5505 to provide IP addresses to local hosts.

Use Network Extension Mode if:

- You want VPN connections to remain open even when not required for transmitting traffic.
- You want remote hosts to be able to communicate directly with hosts on the local network.
- Hosts on the local network have static IP addresses.

### Important Notes

- ASA supports a maximum of 11 Easy VPN Servers: one primary and up to 10 secondary.
- In Easy VPN Client Mode, you use a DHCP server to generate dynamic IP addresses for hosts on the inside network.

To use Easy VPN Client Mode, you must enable the DHCP server on the inside interface.

- Before you can connect the ASA Easy VPN remote device to the Easy VPN Server, you must establish network connectivity between both devices through your Internet service provider (ISP).

After connecting your ASA to the DSL or cable modem, you should follow the instructions provided by your ISP to complete the network connection. Basically, there are three methods of obtaining an IP address when establishing connectivity to your ISP:

- PPPoE client
- DHCP client
- Static IP address configuration

The Easy VPN Server controls the policy enforced on the ASA Easy VPN remote device. However, to establish the initial connection to the Easy VPN Server, you must complete some configuration locally.

You can perform this configuration by following the steps in this Wizard or by using the command-line interface.

### Fields

The **Easy VPN Remote Configuration** screen displays the **Back**, **Next**, **Finish**, **Cancel**, and **Help** buttons, in addition to the following:

- Enable Easy VPN remote—Check this box to enable the ASA to act as an Easy VPN remote device. Enabling the ASA to act as an Easy VPN Remote allows you to choose the networks from which your ASA can be remotely managed. If you do not enable this feature, any host that has access to the ASA outside interface through a VPN tunnel can manage it remotely.
- Mode area
  - Client Mode—Click if you are using a DHCP server to generate dynamic IP addresses for hosts on your inside network.

Client Mode enables VPN connections by traffic, allowing resources to be only used on demand. The ASA applies Network Address Translation (NAT) to all IP addresses of clients connected to the inside (higher security) interface of the ASA.



**Note** To use Client Mode, you must enable the DHCP server on the inside interface.

- Network extension—Click if hosts on your inside network have static IP addresses.

In Network Extension Mode, IP addresses of clients on the inside interface are received without change at the Easy VPN Server, and VPN connections are kept open even when not required for transmitting traffic. This option does not apply NAT to any IP addresses of clients on the inside (higher security) interface of the ASA.

- Group Settings area
  - Use X.509 Certificate—Click to use X.509 certificates to allow IPSec Main Mode. Use the drop-down list to select a trustpoint or to enter a trustpoint.
  - Use group password—Lets you enter a password for a group of users.
    - Group Name—Lets you enter a name for the user group.
    - Password—Lets you enter a password for the user group.
    - Confirm password—Requires that you confirm the password.
- User Settings area
  - Username—Lets you enter a username for your settings.
  - Password—Lets you enter a password for your settings.
  - Confirm Password—Requires that you confirm the password for your settings.
- Easy VPN Server area—Using the ASA as an Easy VPN Server lets you configure your VPN policy in a single location on the ASA, and then push this configuration to multiple Easy VPN remote devices.
  - Primary server—Lets you enter the IP address of the primary Easy VPN Server.
  - Secondary server—Lets you enter the IP address of a secondary Easy VPN Server.



**Note** ASA supports a maximum of 11 Easy VPN Servers (one primary and up to 10 secondary).

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

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

#### For More Information

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## Management IP Address Configuration



### Note

This feature is available only in transparent mode.

### Benefits

The **Management IP Address Configuration** screen lets you configure the management IP address of the host for this context.

### Fields

The **Management IP Address Configuration** screen displays the **Back**, **Next**, **Finish**, **Cancel**, and **Help** buttons, in addition to the following:

- **Management IP Address**—The IP address of the host that can access this context for management purposes using ASDM or a session protocol.
- **Subnet Mask**—Subnet mask for the Management IP address.

### Modes

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

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

### For More Information

This feature is available in the main ASDM application screen:

Configuration > Properties > Management IP

## Other Interfaces Configuration

### Benefits

The Other Interfaces Configuration screen lets you configure the remaining interfaces. You highlight a listed interface, select the Edit button, and configure it from the Edit screen.

### Fields

The Other **Interfaces Configuration** screen displays the **Back**, **Next**, **Finish**, **Cancel**, and **Help** buttons, in addition to the following:

- **Interface**—Displays the network interface on which the original host or network resides.
- **Name**—Displays the name of the interface being edited.
- **Security Level**—Displays the security level range for the interface from 0 to 100, with 100 assigned to the inside interface and 0 assigned to the outside interface. Perimeter interfaces can use any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default.

- Enable traffic between two or more interfaces with same security levels—Check this box if you assign the same security level to two or more interfaces, and want to enable traffic between the interfaces.
- Enable traffic between two or more hosts connected to the same interface—Check this box if you have an interface between two or more hosts and want to enable traffic between them.
- **Edit**—Click **Edit** to configure the interface in the [Edit Interface](#) dialog box.

## Edit Interface

### Benefits

Use the Edit Interfaces to edit existing interfaces.

### Fields

The **Edit Interface** dialog box displays the **OK**, **Cancel**, and **Help** buttons, in addition to the following:

- **Interface**—Displays the name of the selected interface to edit.
- **Interface Name**—Displays the name of the selected interface, and lets you change the name of the interface.
- **Security Level**—Displays the security level of the selected interface, or lets you select a security level for the interface. Either 0 for the outside network or 100 for the inside network. Perimeter interfaces can use any number between 1 and 99. Security levels between 0 and 100 for perimeter interfaces are not set by default. If you change the security level of the interface to a lower level, a caution warning appears.
- **IP Address area**
  - Use PPPoE—Check this box to use PPPoE to provide an authenticated method of assigning an IP address to an outside interface. PPPoE provides a standard method of employing the authentication methods of the Point-to-Point Protocol (PPP) over an Ethernet network.



---

**Note** Because PPPoE is permitted on multiple interfaces, each instance of the PPPoE client may require different authentication levels with different usernames and passwords.

---

- Use DHCP—Check this box to use ASA as a DHCP server to provide network configuration parameters, including dynamically assigned IP addresses, to DHCP clients.
- Uses the following IP address—Check this box to input a specific IP address for an interface.
  - IP Address—Lets you edit the IP address of the interface.
  - Subnet Mask—Lets you edit the subnet mask by entering a new address or selecting an existing IP address from the drop-down list.

### Modes

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

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

**For More Information**

This feature is available in the main ASDM application screen:

Configuration > Interfaces

## Startup Wizard Summary

**Benefits**

The Startup Wizard Summary screen lets you submit all of the settings you made to the security appliance.

- If you would like to change any of the settings you made, click **Back**.
- If you started the Startup Wizard directly from a browser, when you click **Finish**, the configuration created by the wizard is sent to the security appliance and saved to Flash memory.
- If you ran the Startup Wizard from within ASDM, you must explicitly save the configuration to Flash memory just like any other configuration changes.

**Fields**

The **Startup Wizard Summary** screen displays the **Back**, **Finish**, **Cancel** and **Help** buttons.

**Modes**

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

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