



CHAPTER 4

Using the Startup Wizard

The ASDM Startup Wizard guides you through the initial configuration of the adaptive security appliance, and helps you define the following settings for the adaptive security appliance:

- The hostname
- The domain name
- A password to restrict administrative access through ASDM or the CLI
- The IP address information of the outside interface
- Other interfaces, such as the inside or DMZ interfaces
- NAT or PAT rules
- DHCP settings for the inside interface, for use with a DHCP server

To access this feature from the main ASDM application window, choose one of the following:

- **Wizards > Startup Wizard.**
- **Configuration > Device Setup > Startup Wizard**, and then click **Launch Startup Wizard**.

For More Information

- See [Starting ASDM from a Web Browser, page 3-8](#).
- See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

This section includes the following topics:

- [Startup Wizard Screens for ASA 5500 Series and PIX 500 Series Security Appliances, page 4-2](#)
- [Startup Wizard Screens for the ASA 5505 Adaptive Security Appliance, page 4-2](#)

Modes

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

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

Startup Wizard Screens for ASA 5500 Series and PIX 500 Series Security Appliances

Table 4-1 lists all of the required Startup Wizard screens for configuring the ASA 5500 series adaptive security appliances and PIX 500 series security appliances only. The actual sequence of screens is determined by your specified configuration selections. The sequence shown applies only to the ASA 5505 adaptive security appliance. The Availability columns lists the mode or modes in which each screen appears and provides additional configuration information. Click the name to view information for the selected screen.

Table 4-1 Startup Wizard Screens for ASA 5500 Series and PIX 500 Series Security Appliances

Screen Name	Availability
Step 1 - Starting Point or Welcome, page 4-3	All modes. The factory default option in Step 1 is not available on the PIX security appliance.
Step 2 - Basic Configuration, page 4-4	
Step 3 - Auto Update Server, page 4-5	Single, routed and transparent modes. If enabled in single transparent mode, the Interface Configuration and Step 13 - DHCP Server screens are not available.
Step 4 - Management IP Address Configuration, page 4-6	Single, transparent mode only.
Outside Interface Configuration, page 4-22	Single, routed mode only.
Outside Interface Configuration - PPPoE, page 4-21	
Interface Configuration, page 4-21	Single, transparent mode only.
Other Interfaces Configuration, page 4-19	All modes.
Step 12 - Static Routes, page 4-13	
Step 13 - DHCP Server, page 4-13	
Step 14 - Address Translation (NAT/PAT), page 4-14	Single, routed mode only.
Step 15 - Administrative Access, page 4-15	All modes.
Step 17 - Startup Wizard Summary, page 4-19	

Startup Wizard Screens for the ASA 5505 Adaptive Security Appliance

Table 4-2 lists all of the required Startup Wizard screens for configuring the ASA 5505 adaptive security appliance only. The sequence of screens listed represents configuration for the single, routed mode. The Availability columns lists the mode or modes in which each screen appears and provides additional configuration information. Click the name to view information for the selected screen.

Table 4-2 Startup Wizard Screens for the ASA 5505 Adaptive Security Appliance

Screen Name and Sequence	Availability
Step 1 - Starting Point or Welcome, page 4-3	All modes. The Teleworker option in Step 2 is available only on the ASA-5505.
Step 2 - Basic Configuration, page 4-4	
Step 3 - Auto Update Server, page 4-5	Single, routed and transparent modes. Enabled only if configured for teleworker usage.
Step 4 - Management IP Address Configuration, page 4-6	Single, transparent mode only.
Step 5 - Interface Selection, page 4-6	Single, routed mode only.
Step 6 - Switch Port Allocation, page 4-7	
Step 7 - Interface IP Address Configuration, page 4-8	
Step 8 - Internet Interface Configuration - PPOE, page 4-9	
Step 9 - Business Interface Configuration - PPOE, page 4-10	
Step 10 - Home Interface Configuration - PPOE, page 4-11	
Step 11 - General Interface Configuration, page 4-12	
Step 12 - Static Routes, page 4-13	All modes. Enabled only if configured for teleworker usage.
Step 13 - DHCP Server, page 4-13	All modes.
Step 14 - Address Translation (NAT/PAT), page 4-14	Single, routed mode only.
Step 15 - Administrative Access, page 4-15	All modes.
Step 16 - Easy VPN Remote Configuration, page 4-17	Single, routed mode, only when enabled for teleworker usage.
Step 17 - Startup Wizard Summary, page 4-19	All modes.

Step 1 - Starting Point or Welcome

To access this feature from the main ASDM application window (except in multiple mode), choose **File > Reset Device to the Factory Default Configuration**.

Fields

- Modify existing configuration—Choose this option to change the existing configuration.
- Reset configuration to factory defaults—Choose this option to set the configuration at the factory default values for the inside interface.
- Configure the IP address of the management interface—Check this check box to configure the IP address and subnet mask of the management interface.
- IP Address—Specifies the IP address of the management interface.
- Subnet Mask—Choose the subnet mask of the management interface from the drop-down list.

**Note**

If you reset the configuration to factory defaults, you cannot undo these changes by clicking **Cancel** or by closing this screen.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 2 - Basic Configuration

To access this feature from the main ASDM application window, choose one of the following:

- **Configuration > Properties > Device Administration > Device**
- **Configuration > Properties > Device Administration > Password**

Fields

- Configure the device for Teleworker usage—Check this check box to specify a group of configuration settings for a remote worker. For more information, see [Step 16 - Easy VPN Remote Configuration, page 4-17](#).
- Host Name—Specifies a hostname for the adaptive security appliance. The hostname can be up to 63 alphanumeric characters in mixed case. Either “ASA” or “PIX” appears as the device type, according to the security appliance you are using.
- Domain Name—Specifies the IPSec domain name of the adaptive security appliance, which can be used for certificates. The domain name can be a maximum of 63 alphanumeric characters, with no special characters or spaces.
- Privileged Mode (Enable) Password section—Allows you to restrict administrative access to the adaptive security appliance through ASDM or the CLI.

**Note**

If you leave the password field blank, a Password Confirmation dialog box appears to notify you that to do so is a high security risk.

- Change privileged mode (enable) password—Check this check box to change the current privileged mode (enable) password.
- Old Password—Specifies the old enable password, if one exists.
- New Password—Specifies the new enable password. The password is case-sensitive and can be up to 32 alphanumeric characters.
- Confirm New Password—Lets you reenter the new enable password.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 3 - Auto Update Server

This screen allows you to manage the adaptive security appliance remotely from an Auto Update server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

Fields

- **Enable Auto Update**—Check this check box to enable communication between the security appliance and an Auto Update server.
- **Server URL**—From the drop-down list, choose either HTTPS or HTTP to define the beginning of the URL for the Auto Update server.
- **Verify Server SSL certificate**—Check this check box to confirm that an SSL certificate is enabled on the Auto Update server.
- **Username**—Specifies the username to log in to the Auto Update server.
- **Password**—Specifies the password to log in to the Auto Update server.
- **Confirm Password**—Reenter the password to confirm it.
- **Device ID Type**—Click the drop-down list to choose the type of ID to uniquely identify the adaptive security appliance. Choose **User-defined name** to enable the Device ID field, where you specify a unique ID.
- **Device ID**—Specifies a unique string to use as the adaptive security appliance ID.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 4 - Management IP Address Configuration

This screen lets you configure the management IP address of the host for this context. To access this feature from the main ASDM application window, choose **Configuration > Properties > Management IP**.

Fields

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

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 5 - Interface Selection

This screen allows you to group the eight, Fast Ethernet switch ports on the ASA 5505 into three VLANs. These VLANs function as separate, Layer 3 networks. You can then choose or create the VLANs that define your network—one for each interface: outside (Internet), inside (Business), or DMZ (Home). A DMZ is a separate network located in the neutral zone between a private (inside) network and a public (outside) network.

Fields

Outside VLAN or Internet VLAN section

- Choose a VLAN—Choose a predefined outside VLAN by number from the drop-down list.
- Create a VLAN—Check this check box to create a new outside VLAN.
- Enable VLAN—Check this check box to enable the outside VLAN.

Inside VLAN or Business VLAN section

- Choose a VLAN—Choose a predefined inside VLAN by number from the drop-down list.
- Create a VLAN—Check this check box to create a new inside VLAN.
- Enable VLAN—Check this check box to enable the inside VLAN.

DMZ VLAN or Home VLAN (Optional) section

- Choose a VLAN—Choose a predefined VLAN by number from the drop-down list.
- Create a VLAN—Check this check box to create a new VLAN.

- Do not configure—Check this check box to disable configuration of this VLAN.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 6 - Switch Port Allocation

This screen lets you allocate switch ports to outside (Internet), inside (Business), or DMZ (Home) interfaces. The DMZ interface is not available in transparent mode. You must add the ports to the associated VLANs. By default, all switch ports begin with VLAN1. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

Fields

Switch Ports for Outside VLAN (*vlanid*) or Switch Ports for Internet VLAN (*vlanid*) section

- 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.

Switch Ports for Inside VLAN (*vlanid*) or Switch Ports for Business VLAN (*vlanid*) section

- 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.

Switch Ports for DMZ VLAN (*vlanid*) or Switch Ports for Home VLAN (*vlanid*) section

- 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.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 7 - Interface IP Address Configuration

This screen allows you to configure the interface by obtaining an IP address from a PPPoE server or a DHCP server, or by specifying an IP address and subnet mask.

Fields

Outside IP Address or Internet IP Address section

- Use the following IP address—Choose this option to specify an outside IP address.
- IP Address/ Mask—Enter the specific IP address and choose the subnet mask from the drop-down list.
- Use DHCP—Choose this option to obtain an outside IP address from a DHCP server.
- Obtain default route using DHCP—Check this check box to obtain the default route for an outside IP address from a DHCP server.
- Use PPoE—Choose this option to obtain an outside IP address from a PPoE server.

Inside IP Address or Business IP Address section

- Use the following IP address—Choose this option to specify an inside IP address.
- IP Address/ Mask—Enter the specific inside IP address and choose the subnet mask from the drop-down list.
- Use DHCP—Choose this option to obtain an inside IP address from a DHCP server.
- Use PPoE—Choose this option to obtain an inside IP address from a PPoE server.

DMZ IP Address or Home IP Address section

- Use the following IP address—Choose this option to specify a DMZ IP address.
- IP Address/ Mask—Enter the specific DMZ IP address and choose the subnet mask from the drop-down list.
- Use DHCP—Choose this option to obtain a DMZ IP address from a DHCP server.
- Use PPoE—Choose this option to obtain a DMZ IP address from a PPoE server.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 8 - Internet Interface Configuration - PPOE

This screen lets you configure the specified outside interface by obtaining an IP address from a PPOE server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.



Note

For all ASA 5500 series models except ASA 5505, with a full license, the adaptive security appliance supports up to five interfaces, with a maximum of three outside interfaces. In restricted mode, the adaptive security appliance supports up to three interfaces, and in transparent mode, the adaptive security appliance supports up to two interfaces. After you have created the maximum number of interfaces, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and must select an existing one.

Fields

- Group Name—Specifies the name of your group on the PPOE server. You must specify a group name to proceed.

User Authentication section

- PPOE Username—Specifies your username on the PPOE server.
- PPOE Password—Specifies your password on the PPOE server.
- Confirm PPOE Password—Specifies the PPOE password you originally entered.

Authentication Method section

- PAP—Click to use PAP authentication.
- CHAP—Click to use CHAP authentication.
- MSCHAP—Click to use MSCHAP authentication.

IP Address section

- Obtain an IP address using PPOE—Choose this option to obtain an IP address for the interface from the PPOE server. This field is not visible in transparent mode.
- Specify an IP Address—Specifies an IP address for the Internet interface. This field is not visible in transparent mode.
 - IP Address—Specifies the IP address that you want to use for the Internet interface.
 - Subnet Mask—Choose a subnet mask for the Internet interface from the drop-down list.
- Obtain default route using PPOE—Check this check box to set the default routing using the PPOE server.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 9 - Business Interface Configuration - PPOE

This screen lets you configure the inside interface by obtaining an IP address from a PPPoE server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.



Note

For all ASA 5500 series models except ASA 5505, with a full license, the adaptive security appliance supports up to five interfaces, with a maximum of three outside interfaces. In restricted mode, the adaptive security appliance supports up to three interfaces, and in transparent mode, the adaptive security appliance supports up to two interfaces. After you have created the maximum number of interfaces, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and must select an existing one.

Fields

- **Group Name**—Specifies the name of your group on the PPOE server. You must specify a group name to proceed.

User Authentication section

- **PPoE Username**—Specifies your username on the PPOE server.
- **PPoE Password**—Specifies your password on the PPOE server.
- **Confirm PPOE Password**—Specifies the PPOE password you originally entered.

Authentication Method section

- **PAP**—Click to use PAP authentication.
- **CHAP**—Click to use CHAP authentication.
- **MSCHAP**—Click to use MSCHAP authentication.

IP Address section

- **Obtain an IP address using PPOE**—Choose this option to obtain an IP address for the interface from the PPOE server. This field is not visible in transparent mode.
- **Specify an IP Address**—Specifies an IP address for the inside interface. This field is not visible in transparent mode.
 - **IP Address**—Specifies the IP address that you want to use for the inside interface.
 - **Subnet Mask**—Choose a subnet mask for the Internet interface from the drop-down list.
- **Obtain default route using PPOE**—Check this check box to set the default routing using the PPOE server.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 10 - Home Interface Configuration - PPOE

This screen lets you configure the DMZ interface by obtaining an IP address from a PPOE server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

**Note**

For all ASA 5500 series models except ASA 5505, with a full license, the adaptive security appliance supports up to five interfaces, with a maximum of three outside interfaces. In restricted mode, the adaptive security appliance supports up to three interfaces, and in transparent mode, the adaptive security appliance supports up to two interfaces. After you have created the maximum number of interfaces, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and must select an existing one.

Fields

- **Group Name**—Specifies the name of your group on the PPOE server. You must specify a group name to proceed.

User Authentication section

- **PPoE Username**—Specifies your username on the PPOE server.
- **PPoE Password**—Specifies your password on the PPOE server.
- **Confirm PPOE Password**—Specifies the PPOE password you originally entered.

Authentication Method section

- **PAP**—Click to use PAP authentication.
- **CHAP**—Click to use CHAP authentication.
- **MSCHAP**—Click to use MSCHAP authentication.

IP Address section

- **Obtain an IP address using PPOE**—Choose this option to obtain an IP address for the interface from the PPOE server. This field is not visible in transparent mode.
- **Specify an IP Address**—Specifies an IP address for the DMZ interface. This field is not visible in transparent mode.
 - **IP Address**—Specifies the IP address that you want to use for the DMZ interface.
 - **Subnet Mask**—Choose a subnet mask for the Internet interface from the drop-down list.

- Obtain default route using PPOE—Check this check box to set the default routing using the PPOE server.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 11 - General Interface Configuration

This screen lets you enable and restrict traffic between interfaces and between hosts connected to the same interface.

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

Fields

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

Restrict traffic area

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

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 12 - Static Routes

This screen lets you create, edit, and remove static routes that will access networks connected to a router on any interface.

For More Information

- [Static Routes, page 16-40](#)
- [Add/Edit Static Routes, page 4-13](#)
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*

Modes

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

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

Add/Edit Static Routes

This dialog box lets you add or edit a static route. See [Add/Edit Static Route, page 16-43](#) for more information.

Step 13 - DHCP Server

This screen lets you configure the adaptive security appliance as a DHCP server to hosts on the inside interface. To configure the DHCP server for other interfaces from the main ASDM application window, choose **Configuration > Properties > DHCP Services > DHCP Server**. For more information, see [DHCP Server, page 11-4](#).

Fields

- Enable DHCP server on the inside interface—Check this check box to allow connection to the DHCP server from the inside interface.

DHCP Address Pool section

- Starting IP Address—Specifies the starting range of the DHCP server pool in a block of IP addresses from the lowest to highest.



Note

The adaptive security appliance supports up to 256 IP addresses.

- Ending IP Address—Specifies the ending range of the DHCP server pool in a block of IP addresses from the lowest to highest.

DHCP Parameters section

- Enable auto-configuration—Check this check box to allow automatic configuration of the DNS server, WINS server, lease length, and ping timeout settings.
- DNS Server 1—Specifies the IP address of the DNS server.
- WINS Server 1—Specifies the IP address of the WINS server.
- DNS Server 2—Specifies the IP address of the alternate DNS server.
- WINS Server 2—Specifies the IP address of the alternate WINS server.
- Lease Length (secs)—Specifies the amount of time (in seconds) that the client can use its allocated IP address before the lease expires. The default value is 3600 seconds (1 hour).
- Ping Timeout—Specifies the parameters for the ping timeout value in milliseconds.
- Domain Name—Specifies the domain name of the DNS server to use DNS.
- Enable auto-configuration from interface—Check this check box to enable DHCP auto-configuration and select the interface from the menu. The values you specify in the previous sections of the screen take precedence over the auto-configured values.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 14 - Address Translation (NAT/PAT)

This screen lets you configure NAT and PAT on your security appliance. To access this feature from the main ASDM application window, choose **Configuration > NAT**.

PAT lets you set up a single IP address for use as the global address. In addition, you can set multiple outbound sessions to appear as if they originate from a single IP address. 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 all 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.

When you use PAT, be aware of the following:

- PAT 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.
- PAT does not work with the **established** command.

- With passive FTP, use the **inspect protocol ftp strict** command with the **access-list** command to allow outbound FTP traffic.
- A DNS server on a higher level security interface cannot use PAT.

Fields

- Use Network Address Translation (NAT)—Choose to enable NAT and a range of IP addresses to be used for translation.
- Starting Global IP Address—Specifies the first IP address in a range of IP addresses to be used for translation.
- Ending Global IP Address—Specifies 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)—Choose to enable PAT. Choose one of the following if you select this option:



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

- Use the IP address on the outside interface—Choose to use the IP address of the outside interface for PAT.
- Specify an IP address—Enter an IP address to be used for PAT.
 - IP Address—Specifies an IP address for the outside interface for PAT.
 - Subnet Mask (optional)—Choose a subnet mask from the drop-down list.
- Enable traffic through the firewall without translation—Choose to allow traffic through the firewall without translation.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 15 - Administrative Access

This screen lets you configure management access on the security appliance.

Fields

- **Type**—Specifies whether the host or network is accessing the security appliance through HTTP over SSL in 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.
- **Enable HTTP server for HTTPS/ASDM access**—Check this check box to enable a secure connection to an HTTP server to access ASDM.
- **Add**—Click to add the access type, an interface, and then specifies the IP address and netmask of the host network that may connect to that interface for management purposes only. See [Add/Edit Administrative Access Entry](#) for more information.
- **Edit**—Changes an interface. See [Add/Edit Administrative Access Entry](#) for more information.
- **Delete**—Removes an interface.
- **Enable ASDM history metrics**—Check this check box to allow ASDM to collect and display statistics.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Add/Edit Administrative Access Entry

This dialog box let you configure the hosts. To access this feature from the main ASDM application window, choose one of the following:

- **Configuration > Properties > Device Access > HTTPS/ASDM.**
- **Configuration > Properties > Device Access > Telnet.**
- **Configuration > Properties > Device Access > SSH.**
- **Configuration > Properties > History Metrics.**

Fields

- **Access Type**—Choose one of the following types of preconfigured connections for the CLI console sessions from the drop-down list:
 - ASDM/HTTPS
 - SSH
 - Telnet

**Note**

ASDM uses HTTP over SSL for all communication with the security appliance.

- Interface Name—Choose from a list of predetermined interfaces.
- IP Address—Specifies an IP address for the interface.
- Subnet Mask—Specifies 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
•	•	•	•	—

Step 16 - Easy VPN Remote Configuration

This screen lets you form a secure VPN tunnel between the adaptive security appliance and a remote Cisco VPN 3000 concentrator, Cisco router, or adaptive security appliance that is acting as an Easy VPN server. The adaptive security appliance acts as an Easy VPN remote device to enable deployment of VPNs to remote locations.

**Note**

To access this screen, you must check the **Configure the device for Teleworker usage** check box in [Step 2 - Basic Configuration](#) and uncheck the **Enable Auto Update** check box in the [Interface Configuration](#).

Two modes of operation are available:

- Client mode
- Network extension mode

In client mode, the adaptive security appliance does not expose the IP addresses of clients on the inside network. Instead, the adaptive security appliance uses NAT to translate the IP addresses on the private network to a single, assigned IP address. In this mode, you cannot ping or access any device from outside the private network.

In extension mode, the adaptive security appliance does not protect the IP addresses of local hosts by substituting an assigned IP address. Therefore, hosts on the other side of the VPN connection can communicate directly with hosts on the local network.

To configure the adaptive security appliance in one of these two modes, use the following guidelines:

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.

Fields

- Enable Easy VPN remote—Check this check box to enable the adaptive security appliance to act as an Easy VPN remote device. If you do not enable this feature, any host that has access to the adaptive security appliance outside interface through a VPN tunnel can manage it remotely.

Mode section

- Client Mode—Click if you are using a DHCP server to generate dynamic IP addresses for hosts on your inside network.
- Network extension—Click if hosts on your inside network have static IP addresses.

Group Settings section

- Use X.509 Certificate—Click to use X.509 certificates to enable the IPsec main mode. Choose or enter the trustpoint from the drop-down list.
- 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 section

- 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 section

- 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

The adaptive security appliance supports a maximum of 11 Easy VPN servers: one primary and up to ten secondary. 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 ISP. After you have connected the ASA 5500 series adaptive security appliance to the DSL or cable modem, follow the instructions provided by your ISP to complete the network connection. You can obtain an IP address through a PPPoE server, a DHCP server, or a static configuration.

For More Information

See the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Step 17 - Startup Wizard Summary

This screen summarizes all of the settings you have made for the security appliance.

- To change any of the settings in previous screens, click **Back**.
- If you started the Startup Wizard directly from a browser, when you click **Finish**, the configuration that you created through the wizard is sent to the adaptive security appliance and saved in Flash memory automatically.
- If you ran the Startup Wizard from within ASDM, you must explicitly save the configuration in Flash memory.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide* and the *Cisco ASA 5505 Getting Started Guide*.

Modes

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

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

Other Interfaces Configuration

This screen lets you configure the remaining interfaces.

Fields

- Interface—Displays the network interface on which the original host or network resides.
- Name—Displays the name of the interface being configured.
- 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 check box to assign the same security level to two or more interfaces, and enable traffic between them.
- Enable traffic between two or more hosts connected to the same interface—Check this check box if you have an interface between two or more hosts and want to enable traffic between them.

- Edit—Click to change the configuration of the interface in the [Edit Interface](#) dialog box.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Modes

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

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

Edit Interface

To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

Fields

- 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. If you change the security level of the interface to a lower level, a warning message appears.
- Use PPPoE—Check this check box to use PPPoE to provide an authenticated method of assigning an IP address to an outside interface.



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 check box to use the adaptive security appliance as a DHCP server.
- Uses the following IP address—Check this check box to enter a specific IP address for an interface.
- IP Address—Edits the IP address of the interface.
- Subnet Mask—Choose an existing subnet mask 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
•	•	•	•	—

Interface Configuration

This screen lets you configure the remaining interfaces and enable traffic between two or more interfaces.

Fields

- Edit—Click to change the configuration of the interface in the [Edit Interface](#) dialog box.
- Enable traffic between two or more interfaces with the same security level—Check this check box to enable traffic between two or more interfaces with the same security level.



Note

IP address-related fields are not available in transparent mode.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Modes

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

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

Outside Interface Configuration - PPPoE

This screen lets you configure the outside interface by obtaining an IP address from a PPPoE server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

Fields

- Group Name—Lets you specify the name of the interface. You must specify a group name 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 PAP. You have the option of configuring CHAP or MS-CHAP manually.

- PAP—Check this check box to select PAP as the authentication method. The username and password are sent unencrypted using this method.
- CHAP—Check this check box to select CHAP authentication. CHAP does not prevent unauthorized access; it identifies the remote end. The access server then determines whether the user is allowed access.

- MSCHAP—Check this check box to select MS-CHAP authentication for PPP connections between a computer using a Windows operating system and an access server.
- IP Address area

The default authentication method for PPPoE is PAP. You have the option of configuring CHAP or MS-CHAP manually.

 - Obtain IP Address using PPPoE—Click to obtain an IP address using a PPPoE server.
 - Specify an IP address—Click to specify an IP address for an interface:
 - IP Address—Lets you enter an IP address for an interface.
 - Subnet Mask—Lets you enter or choose a subnet mask for an interface from the drop-down list.
 - Obtain default route using PPPoE—Click to obtain the default route between the PPPoE server and the PPPoE client.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Modes

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

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

Outside Interface Configuration

This screen lets you configure your outside interface by specifying an IP address, or obtaining one from a PPPoE or a DHCP server. To access this feature from the main ASDM application window, choose **Configuration > Interfaces**.

**Note**

For all ASA 5500 series models except ASA 5505, with a full license, the adaptive security appliance supports up to five interfaces, with a maximum of three outside interfaces. In restricted mode, the adaptive security appliance supports up to three interfaces, and in transparent mode, the adaptive security appliance supports up to two interfaces. After you have created the maximum number of interfaces, or the maximum number of interfaces has already been named, you may not be able to create a new VLAN, and must select an existing one.

Fields

- Interface—Choose an interface from the drop-down list.
- Interface Name—Adds a name to a new interface, or displays the name associated with an existing interface.
- Enable interface—Check this check 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.
- **Use PPPoE**—Click to obtain an IP address from a PPPoE server.
- **Use DHCP**—Click to obtain an IP address from a DHCP server.
- **Obtain default route using DHCP**—Check this check box to obtain an IP address for the default gateway using DHCP.
- **Use the following IP address**—Choose this option to specify an IP address manually for the interface. This field is not visible in transparent mode.
- **IP Address**—Specifies an IP address for an outside interface. This field is not visible in transparent mode.
- **Subnet Mask**—Choose a subnet mask for an outside interface from the drop-down list.

For More Information

See the *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*.

Modes

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

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

