



CHAPTER 4

Configuring Interfaces

This chapter describes how to configure each interface and subinterface for a name, security level, and IP address. In multiple context mode, you can configure hardware properties and create subinterfaces in the system execution space, while you configure the IP address, name, and security level in each context.



Note

To configure interfaces for the ASA 5505 adaptive security appliance, see [Chapter 5, “Configuring Switch Ports and VLAN Interfaces for the Cisco ASA 5505 Adaptive Security Appliance.”](#)

This chapter includes the following sections:

- [Security Level Overview, page 4-1](#)
- [Configuring the Interfaces, page 4-2](#)

Security Level Overview

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

For some security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some application inspection engines are dependent on the security level. For some security interfaces, inspection engines apply to traffic in either direction.
 - NetBIOS inspection engine—Applied only for outbound connections.
 - SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.
- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

For some security interfaces, you can filter traffic in either direction.

- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for some security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

For some security interfaces, you can configure **established** commands for both directions.

Configuring the Interfaces

By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through an enabled subinterface. For multiple context mode, if you allocate a physical interface or subinterface to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.



Note

If you are using failover, do not use this procedure to name interfaces that you are reserving for failover and Stateful Failover communications. See [Chapter 12, “Failover.”](#) to configure the failover and state links.

For multiple context mode, follow these guidelines:

- Configure the context interfaces from within each context.
- You can only configure context interfaces that you already assigned to the context in the system configuration.
- The system configuration only lets you configure Ethernet settings and VLANs. The exception is for failover interfaces; do not configure failover interfaces with this procedure. See the Failover chapter for more information.

This section includes the following topics:

- [Interfaces \(System\), page 4-2](#)
- [Interfaces \(Single Mode and Context\), page 4-5](#)

Interfaces (System)

The Interfaces pane displays configured interfaces and subinterfaces. Before you can assign an interface to a security context (see the [“Configuring Security Contexts”](#) section on page 7-16), define the interface in this pane. Although the system configuration does not include any networking parameters for these interfaces, the system controls the allocation of interfaces to security contexts.

Fields

- Interface—Displays the interface ID. All physical interfaces are listed automatically. Subinterfaces are indicated by the interface ID followed by *.n*, where *n* is the subinterface number.

If you use failover, you need to assign a dedicated physical interface as the failover link and an optional interface for Stateful Failover on the [Failover: Setup](#) tab. (You can use the same interface for failover and state traffic, but we recommend separate interfaces). To ensure that you can use an interface for failover, do not configure an interface name in the Interfaces pane. Other settings, including the IP address, are ignored; you set all relevant parameters in the [Failover: Setup](#) tab. You can use a subinterface for failover as long as you do not set a name for the physical interface or the subinterface. After you assign an interface as the failover link or state link, you cannot edit or delete the interface in this pane. The only exception is if you set a physical interface to be the state link, then you can configure the speed and duplex.

- **Enabled**—Indicates if the interface is enabled, Yes or No.

By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through an enabled subinterface. For multiple context mode, if you allocate a physical interface or subinterface to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

- **VLAN**—Shows the VLAN assigned to a subinterface. Physical interfaces show “native,” meaning that the physical interface is untagged.
- **Description**—Displays a description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description.
- **Add**—Adds a subinterface.
- **Edit**—Edits the selected interface. If you assign an interface as the failover link or state link (see the [Failover: Setup](#) tab), you cannot edit the interface in this pane. The only exception is if you set a physical interface to be the state link, then you can configure the speed and duplex.
- **Delete**—Deletes the selected subinterface. You cannot delete physical interfaces or allocated interfaces in a context. If you assign an interface as the failover link or state link (see the [Failover: Setup](#) tab), you cannot delete the interface in this pane.

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 Interface

The Add Interface dialog box lets you add a subinterface. The Edit Interface dialog box lets you edit an interface or subinterface.

If you intend to use a physical interface for failover, do not configure the interface in this dialog box; instead, use the [Failover: Setup](#) tab. In particular, do not set the interface name, as this parameter disqualifies the interface from being used as the failover link; other parameters are ignored.

After you assign the interface as the failover link or state link, you cannot edit or delete the interface from the Interfaces pane. The only exception is if you set a physical interface to be the state link, then you can configure the speed and duplex.

Fields

- **Hardware Port**—When you add a subinterface, you can choose any enabled physical interface to which you want to add a subinterface. If you do not see an interface ID, be sure that the interface is enabled.
- **Configure Hardware Properties**—For a physical interface, opens the [Hardware Properties](#) dialog box so you can set the speed and duplex.
- **Enable Interface**—Enables this interface to pass traffic.

By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through an enabled subinterface. For multiple context mode, if you allocate a physical interface or subinterface to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

- **VLAN ID**—For a subinterface, sets the VLAN ID, between 1 and 4095. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. For multiple context mode, you can only set the VLAN in the system configuration.
- **Sub-interface ID**—Sets the subinterface ID as an integer between 1 and 4294967293. The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it.
- **Description**—Sets an optional description up to 240 characters on a single line, without carriage returns. The system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.

Modes

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

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

Hardware Properties

The Hardware Properties dialog box lets you set the speed and duplex of physical interfaces.

Fields

- **Hardware Port**—*Display only*. Displays the interface ID.
- **Media Type**—Sets the media type to RJ45 or SFP. The default is RJ45.
- **Duplex**—Lists the duplex options for the interface, including Full, Half, or Auto, depending on the interface type.

- **Speed**—Lists the speed options for the interface. The speeds available depend on the interface type. For SFP interfaces, which are always 1000 Mbps, and you can set the speed to Negotiate or Nonegotiate. Negotiate (the default) enables link negotiation, which exchanges flow-control parameters and remote fault information. Nonegotiate does not negotiate link parameters. For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

Modes

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

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

Interfaces (Single Mode and Context)

The Interfaces pane displays configured interfaces and subinterfaces. You can add or delete subinterfaces (single mode only), and also enable communication between interfaces on the same security level or enable traffic to enter and exit the same interface.

Transparent firewall mode allows only two interfaces to pass through traffic; however, if your platform includes a dedicated management interface, Management 0/0, you can use it (either the physical interface or a subinterface) as a third interface for management traffic.

Benefits

This pane lets you enable communication between interfaces on the same security level.

By default, interfaces on the same security level cannot communicate with each other. Allowing communication between same security interfaces provides the following benefits:

- You can configure more than 101 communicating interfaces.
 - If you use different levels for each interface and do not assign any interfaces to the same security level, you can configure only one interface per level (0 to 100).
- You want traffic to flow freely between all same security interfaces without access lists.

Fields

- **Interface**—Displays the interface ID. All physical interfaces are listed automatically. Subinterfaces are indicated by the interface ID followed by .*n*, where *n* is the subinterface number.

If you use failover, you need to assign a dedicated physical interface as the failover link and an optional interface for Stateful Failover on the [Failover: Setup](#) tab. (You can use the same interface for failover and state traffic, but we recommend separate interfaces). To ensure that you can use an interface for failover, do not configure an interface name in the Interfaces pane. Other settings, including the IP address, are ignored; you set all relevant parameters in the [Failover: Setup](#) tab. You can use a subinterface for failover as long as you do not set a name for the physical interface or the

subinterface. After you assign an interface as the failover link or state link, you cannot edit or delete the interface in this pane. The only exception is if you set a physical interface to be the state link, then you can configure the speed and duplex.

For multiple context mode, the physical interfaces are listed only in the system configuration. When you allocate interfaces to a context, each allocated interface is listed automatically in the context.

- Name—Displays the interface name.
- Enabled—Indicates if the interface is enabled, Yes or No. By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through an enabled subinterface. For multiple context mode, if you allocate a physical interface or subinterface to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.
- Security Level—Displays the interface security level between 0 and 100. By default, the security level is 0.
- IP Address—Displays the IP address, or in transparent mode, the word “native.” Transparent mode interfaces do not use IP addresses. To set the IP address for the context or the security appliance, see the [Management IP](#) pane.
- Subnet Mask—For routed mode only. Displays the subnet mask.
- Management Only—Indicates if the interface allows traffic to the security appliance or for management purposes only.
- MTU—Displays the MTU. By default, the MTU is 1500.
- Active MAC Address—Shows the active MAC address, if you assigned one manually on the [Add/Edit Interface > Advanced](#) tab.
- Standby MAC Address—Shows the standby MAC address (for failover), if you assigned one manually.
- Description—Displays a description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description.
- Add—Adds a subinterface.
- Edit—Edits the selected interface. If you assign an interface as the failover link or state link (see the [Failover: Setup](#) tab), you cannot edit the interface in this pane. The only exception is if you set a physical interface to be the state link, then you can configure the speed and duplex.
- Delete—Deletes the selected subinterface. You cannot delete physical interfaces or allocated interfaces in a context. If you assign an interface as the failover link or state link (see the [Failover: Setup](#) tab), you cannot delete the interface in this pane.
- Enable traffic between two or more interfaces which are configured with same security levels—Enables communication between interfaces on the same security level. If you enable same security interface communication, you can still configure interfaces at different security levels as usual.
- Enable traffic between two or more hosts connected to the same interface—Enables traffic to enter and exit the same interface.

Modes

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

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System ¹
•	•	•	•	—

1. For the system Interfaces pane, see the system [Interfaces \(System\)](#) pane.

Add/Edit Interface > General


The Add Interface > General tab lets you add a subinterface. The Edit Interface > General tab lets you edit an interface or subinterface. In multiple context mode, you can only add interfaces in the system configuration. See the “[Configuring Security Contexts](#)” section on page 7-16 to assign interfaces to contexts.

If you intend to use a physical interface for failover, do not configure the interface in this dialog box; instead, use the [Failover: Setup](#) tab. In particular, do not set the interface name, as this parameter disqualifies the interface from being used as the failover link; other parameters are ignored.

After you assign the interface as the failover link or state link, you cannot edit or delete the interface from the Interfaces pane. The only exception is if you set a physical interface to be the state link, then you can configure the speed and duplex.

Fields

- **Hardware Port**—When you add a subinterface, you can choose any enabled physical interface to which you want to add a subinterface. If you do not see an interface ID, be sure that the interface is enabled.
- **Configure Hardware Properties**—For a physical interface, opens the [Hardware Properties](#) dialog box so that you can set the speed and duplex, and for some interfaces, the media type. For multiple context mode, you can only set physical properties in the system configuration.
- **Enable Interface**—Enables this interface to pass traffic. In addition to this setting, you need to set an IP address (for routed mode) and a name before traffic can pass according to your security policy. By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through an enabled subinterface. For multiple context mode, if you allocate a physical interface or subinterface to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.
- **Dedicate this interface to management only**—Sets the interface to accept traffic to the security appliance only, and not through traffic.
- **VLAN ID**—For a subinterface, sets the VLAN ID, between 1 and 4095. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. For multiple context mode, you can only set the VLAN in the system configuration.
- **Sub-interface ID**—Sets the subinterface ID as an integer between 1 and 4294967293. The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it.
- **Interface Name**—Sets an interface name up to 48 characters in length.
- **Security Level**—Sets the security level between 0 (lowest) and 100 (highest). The security appliance lets traffic flow freely from an inside network to an outside network (lower security level). Many other security features are affected by the relative security level of two interfaces.

- IP Address—For routed mode only. For multiple context mode, set the IP address in the context configuration.
 - Use Static IP—Manually sets the IP address.
 - IP address—Sets the IP address.
 - Subnet Mask—Sets the subnet mask.
 - Obtain Address via DHCP—Dynamically sets the IP address using DHCP.
 - For the client identifier in DHCP option 61—To force a MAC address to be stored inside a DHCP request packet for option 61 instead of the default internally-generated string, click **Use MAC address**. Some ISPs expect option 61 to be the interface MAC address. If the MAC address is not included in the DHCP request packet, then an IP address will not be assigned. To use the default string, click **Use “Cisco-<MAC>-<interface_name>-<host>”**.
 - Obtain Default Route Using DHCP—Obtains a default route from the DHCP server so that you do not need to configure a default static route.
 - Renew DHCP Lease—Renews the DHCP lease.
 - Retry Count—Sets the number of times between 4 and 16 that the security appliance resends a DHCP request if it does not receive a reply after the first attempt. The total number of attempts is the retry count plus the first attempt. For example, if you set the retry count to 4, the security appliance sends up to 5 DHCP requests.
 - DHCP Learned Route Metric—Assigns an administrative distance to the learned route. Valid values are from 1 to 255. If this field is left blank, the administrative distance for the learned routes is 1.
 - Enable tracking—Check this checkbox to enable route tracking for DHCP-learned routes.
-
- 

Note Route tracking is only available in single, routed mode.
-
- Track ID—A unique identifier for the route tracking process. Valid values are from 1 to 500.
 - Track IP Address—Enter the IP address of the target being tracked. Typically, this would be the IP address of the next hop gateway for the route, but it could be any network object available off of that interface.
 - SLA ID—A unique identifier for the SLA monitoring process. Valid values are from 1 to 2147483647.
 - Monitoring Options—Click this button to open the [Route Monitoring Options](#) dialog box. In the [Route Monitoring Options](#) dialog box you can configure the parameters of the tracked object monitoring process.
 - Enable DHCP Broadcast flag for DHCP request and discover messages—Allows the security appliance to set the broadcast flag in the DHCP client packet. This option sets the broadcast flag to 1 in the DHCP packet header when the DHCP client sends a discover requesting an IP address. The DHCP server listens to this broadcast flag and broadcasts the reply packet if the flag is set to 1. Without this option, the broadcast flag is set to 0, and the DHCP server unicasts the reply packets to the client with the offered IP address. The DHCP client can receive both broadcast and unicast offers from the DHCP server.
 - Use PPPoE—Dynamically sets the IP address using PPPoE.



Note PPPoE is not supported with failover, or in Multiple context mode and Transparent mode. PPPoE is only supported in Single-Routed mode without failover.

Group Name—Specify a group name.

PPPoE Username—Specify the username provided by your ISP.

PPPoE Password—Specify the password provided by your ISP.

Confirm Password—Specify the password provided by your ISP.

PPP Authentication—Select either PAP, CHAP, or MSCHAP. PAP passes cleartext username and password during authentication and is not secure. With CHAP, the client returns the encrypted [challenge plus password], with a cleartext username in response to the server challenge. CHAP is more secure than PAP, but it does not encrypt data. MSCHAP is similar to CHAP but is more secure because the server stores and compares only encrypted passwords rather than cleartext passwords as in CHAP. MSCHAP also generates a key for data encryption by MPPE.

Store Username and Password in Local Flash—Stores the username and password in a special location of NVRAM on the security appliance. If an Auto Update Server sends a clear config command to the security appliance and the connection is then interrupted, the security appliance can read the username and password from NVRAM and re-authenticate to the Access Concentrator.

IP Address and Route Settings—displays the PPPoE IP Address and Route Settings dialog where you can choose addressing and tracking options.

- Description—Sets an optional description up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.

Modes

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

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System ¹
•	•	•	•	—

1. For the system Add/Edit Interfaces dialog box, see the system [Add/Edit Interface](#) dialog box.

Add/Edit Interface > Advanced

The Add/Edit Interface > Advanced tab lets you set the MTU and MAC address of the interface.

Fields

- MTU—Sets the MTU from 300 to 65,535 bytes. The default is 1500 bytes. For multiple context mode, set the MTU in the context configuration.

- **Mac Address Cloning**—Manually assigns MAC addresses.

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address.

In multiple context mode, if you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the security appliance easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See the “[How the Security Appliance Classifies Packets](#)” section on page 7-2 for more information. You can assign each MAC address manually, or you can automatically generate MAC addresses for shared interfaces in contexts. See the “[Security Contexts](#)” section on page 7-16 to automatically generate MAC addresses. If you automatically generate MAC addresses, you can use this option to override the generated address.

For single context mode, or for interfaces that are not shared in multiple context mode, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

- **Active Mac Address**—Assigns a MAC address to the interface in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.
- **Standby Mac Address**—For use with failover, set the Standby Mac Address. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

Modes

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

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System ¹
•	•	•	•	—

1. For the system Add/Edit Interfaces dialog box, see the system [Add/Edit Interface](#) dialog box.

PPPoE IP Address and Route Settings

The PPPoE IP Address and Route Settings dialog lets you choose addressing and tracking options for PPPoE connections.

Fields

- **IP Address area**—Lets you choose between Obtaining an IP address using PPP or specifying an IP address, and contains the following fields:
 - **Obtain IP Address using PPP**—Select to enable the security appliance to use PPP to get an IP address.
 - **Specify an IP Address**—Specify an IP address and mask for the security appliance to use instead of negotiating with the PPPoE server to assign an address dynamically.
- **Route Settings Area**—Lets you configure route and tracking settings and contains the following fields:

- Obtain default route using PPPoE—Sets the default routes when the PPPoE client has not yet established a connection. When using this option, you cannot have a statically defined route in the configuration.

PPPoE learned route metric—Assigns an administrative distance to the learned route. Valid values are from 1 to 255. If this field is left blank, the administrative distance for the learned routes is 1.

- Enable tracking—Check this checkbox to enable route tracking for PPPoE-learned routes.



Note Route tracking is only available in single, routed mode.

- Primary Track—Select this option to configure the primary PPPoE route tracking.
- Track ID—A unique identifier for the route tracking process. Valid values are from 1 to 500.
- Track IP Address—Enter the IP address of the target being tracked. Typically, this would be the IP address of the next hop gateway for the route, but it could be any network object available off of that interface.
- SLA ID—A unique identifier for the SLA monitoring process. Valid values are from 1 to 2147483647.
- Monitor Options—Click this button to open the [Route Monitoring Options](#) dialog box. In the [Route Monitoring Options](#) dialog box you can configure the parameters of the tracked object monitoring process.
- Secondary Track—Select this option to configure the secondary PPPoE route tracking.
- Secondary Track ID—A unique identifier for the route tracking process. Valid values are from 1 to 500.

Hardware Properties

The Hardware Properties dialog box lets you set the speed and duplex of physical interfaces, and for an interface SSM, the media type. In multiple context mode, configure these settings in the system configuration.

Fields

- Hardware Port—*Display only*. Displays the interface ID.
- MAC Address—*Display only*. Displays the Interface MAC address.
- Media Type—Sets the media type to RJ45 or SFP. SFP is only available for SSM interfaces on the ASA 5500 series adaptive security appliance. The default is RJ45.
- Duplex—Lists the duplex options for the interface, including Full, Half, or Auto, depending on the interface type.
- Speed—Lists the speed options for the interface. The speeds available depend on the interface type. For SFP interfaces, which are always 1000 Mbps, and you can set the speed to Negotiate or Nonnegotiate. Negotiate (the default) enables link negotiation, which exchanges flow-control parameters and remote fault information. Nonnegotiate does not negotiate link parameters. For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the

auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

Modes

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

Firewall Mode		Security Context		
Routed	Transparent	Single	Multiple	
			Context	System ¹
•	•	•	•	—

1. For the system Hardware Properties dialog box, see the system [Hardware Properties](#) dialog box.