Using the High Availability and Scalability Wizard

The High Availability and Scalability Wizard guides you through configuring failover with high availability and configuring VPN cluster load balancing. This chapter includes the following sections:

- Information About the High Availability and Scalability Wizard, page 7-1
- Licensing Requirements for the High Availability and Scalability Wizard, page 7-2
- Prerequisites for the High Availability and Scalability Wizard, page 7-3
- Configuring Failover with the High Availability and Scalability Wizard, page 7-3
- Configuring VPN Cluster Load Balancing with the High Availability and Scalability Wizard, page 7-9
- Feature History for the High Availability and Scalability Wizard, page 7-12

Information About the High Availability and Scalability Wizard

For more information about failover, see Introduction to Failover and High Availability, page 65-1.
Licensing Requirements for the High Availability and Scalability Wizard

**Active/Standby Failover**

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5505</td>
<td>Security Plus License. (Stateful failover is not supported).</td>
</tr>
<tr>
<td>ASA 5510, ASA 5512-X</td>
<td>Security Plus License.</td>
</tr>
<tr>
<td>All other models</td>
<td>Base License.</td>
</tr>
</tbody>
</table>

**Active/Active Failover**

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5505</td>
<td>No support.</td>
</tr>
<tr>
<td>ASA 5510, ASA 5512-X</td>
<td>Security Plus License.</td>
</tr>
<tr>
<td>All other models</td>
<td>Base License.</td>
</tr>
</tbody>
</table>

**VPN Load Balancing**

This feature is not available on No Payload Encryption models.

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5505 and 5512-X</td>
<td>No support.</td>
</tr>
<tr>
<td>ASA 5510</td>
<td>You need the following licenses:</td>
</tr>
<tr>
<td></td>
<td>• Security Plus License.</td>
</tr>
<tr>
<td></td>
<td>• Strong Encryption (3DES/AES) License.</td>
</tr>
<tr>
<td>All other models</td>
<td>You need the following licenses:</td>
</tr>
<tr>
<td></td>
<td>• Base License.</td>
</tr>
<tr>
<td></td>
<td>• Strong Encryption (3DES/AES) License.</td>
</tr>
</tbody>
</table>
Prerequisites for the High Availability and Scalability Wizard

To complete the High Availability and Scalability Wizard, make sure that you have the following information available:

- LAN failover settings and stateful failover settings, including the following:
  - Interface name
  - Active IP address of the primary unit and secondary unit
  - Subnet mask of the primary unit and secondary unit
  - Logical name
  - Role (either primary or secondary)
- A 32-character shared key in hexadecimal format (optional) for encrypted communication on the failover link

Configuring Failover with the High Availability and Scalability Wizard

You can configure either Active/Active or Active/Standby failover with the High Availability and Scalability Wizard. This section explains how to use the wizard and contains the following topics:

- Accessing the High Availability and Scalability Wizard, page 7-3
- Configuring Active/Active Failover with the High Availability and Scalability Wizard, page 7-4
- Configuring Active/Standby Failover with the High Availability and Scalability Wizard, page 7-5
- High Availability and Scalability Wizard Screens, page 7-5

Accessing the High Availability and Scalability Wizard

From the ASDM main application window, access the High Availability and Scalability Wizard by choosing one of the following:

- Wizards > High Availability and Scalability Wizard
- Configuration > Device Management > High Availability > HA/Scalability Wizard, and then click Launch High Availability and Scalability Wizard.

To move to the next screen of the wizard, click Next. You must complete the required fields of each screen before you may proceed to the next one.

To return to a previous screen of the wizard, click Back. If settings added in later screens of the wizard are not affected by the changes that you made to an earlier screen, that information remains on the screen as you proceed through the wizard again. You do not need to reenter it.

To leave the wizard at any time without saving any changes, click Cancel.

To send configuration settings to the ASA in the Summary screen of the wizard, click Finish.

To obtain additional online information, click Help.
Configuring Active/Active Failover with the High Availability and Scalability Wizard

The following procedure provides a high-level overview for configuring Active/Active failover using the High Availability and Scalability Wizard. Each step in the procedure corresponds to a wizard screen. Click Next after completing each step, except for the last one, before proceeding to the next step. Each step also includes a reference to additional information that you may need to complete the step.

**Step 1**  
In the Configuration Type screen, click **Configure Active/Active failover**.  
See Configuration Type, page 7-6 for more information about this screen.

**Step 2**  
Enter the IP address of the failover peer in the Failover Peer Connectivity and Compatibility Check screen. Click **Test Compatibility**. You cannot move to the next screen until all compatibility tests have been passed.  
See Failover Peer Connectivity and Compatibility Check, page 7-6 for more information about this screen.

**Step 3**  
If the ASA or the failover peer are in single context mode, change them to multiple context mode in the Change Device to Multiple Mode screen. When you change the ASA to multiple context mode, it reboots. ASDM automatically reestablishes communication with the ASA when it has finished rebooting.  
See Change a Device to Multiple Mode, page 7-7 for more information about this screen.

**Step 4**  
Assign security contexts to failover groups in the Context Configuration screen. You can add and delete contexts in this screen.  
See Security Context Configuration, page 7-7 for more information about this screen.

**Step 5**  
Define the Failover Link in the Failover Link Configuration screen.  
See Failover Link Configuration, page 7-7 for more information about this screen.

**Step 6**  
(Not available on the ASA 5505 ASA) Define the Stateful Failover link in the State Link Configuration screen.  
See State Link Configuration, page 7-8 for more information about this screen.

**Step 7**  
Add standby addresses to the ASA interfaces in the Standby Address Configuration screen.  
See Standby Address Configuration, page 7-8 for more information about this screen.

**Step 8**  
Review your configuration in the Summary screen. If necessary, click Back to return to a previous screen and make changes.  
See Summary, page 7-9 for more information about this screen.

**Step 9**  
Click Finish.  
The failover configuration is sent to the ASA and to the failover peer.
Chapter 7      Using the High Availability and Scalability Wizard

Configuring Active/Standby Failover with the High Availability and Scalability Wizard

The following procedure provides a high-level overview for configuring Active/Standby failover using the High Availability and Scalability Wizard. Each step in the procedure corresponds to a wizard screen. Click Next after completing each step, except for the last one, before proceeding to the next step. Each step also includes a reference to additional information that you may need to complete the step.

Step 1 In the Configuration Type screen, click Configure Active/Standby failover.
See Configuration Type, page 7-6 for more information about this screen.

Step 2 Enter the IP address of the failover peer on the Failover Peer Connectivity and Compatibility Check screen. Click Test Compatibility. You cannot move to the next screen until all compatibility tests have been passed.
See Failover Peer Connectivity and Compatibility Check, page 7-6 for more information about this screen.

Step 3 Define the Failover Link in the Failover Link Configuration screen.
See Failover Link Configuration, page 7-7 for more information about this screen.

Step 4 (Not available on the ASA 5505 ASA) Define the Stateful Failover link in the State Link Configuration screen.
See State Link Configuration, page 7-8 for more information about this screen.

Step 5 Add standby addresses to the ASA interfaces in the Standby Address Configuration screen.
See Standby Address Configuration, page 7-8 for more information about this screen.

Step 6 Review your configuration in the Summary screen. If necessary, click Back to go to a previous screen and make changes.
See Summary, page 7-9 for more information about this screen.

Step 7 Click Finish.
The failover configuration is sent to the ASA and to the failover peer.

High Availability and Scalability Wizard Screens

The High Availability and Scalability Wizard guides you through a step-by-step process of creating either an Active/Active failover configuration, an Active/Standby failover configuration, or a VPN Cluster Load Balancing configuration.

As you go through the wizard, screens appear according to the type of failover that you are configuring and the hardware platform that you are using.

This section includes the following topics:

- Configuration Type, page 7-6
- Failover Peer Connectivity and Compatibility Check, page 7-6
- Change a Device to Multiple Mode, page 7-7
- Security Context Configuration, page 7-7
Configuration Type

The Configuration Type screen lets you select the type of failover or VPN cluster load balancing to configure. The Firewall Hardware/Software Profile area shows the following display-only information:

- Hardware model number of the ASA.
- Number of interfaces available on the ASA.
- Number of modules installed on the ASA.
- Version of the platform software on the ASA.
- Type of failover license installed on the device. You may need to purchase an upgraded license to configure failover.
- Firewall mode (routed or transparent) and the context mode (single or multiple).

To choose the type of failover configuration that you want, click one of the following options:

- **Configure Active/Active Failover** for Active/Active failover.
- **Configure Active/Standby Failover** for Active/Standby failover.
- **Configure VPN Cluster Load Balancing** to participate in VPN load balancing as part of a cluster.

Failover Peer Connectivity and Compatibility Check

The Failover Peer Connectivity and Compatibility Check screen lets you verify that the selected failover peer is reachable and compatible with the current unit. If any of the connectivity and compatibility tests fail, you must correct the problem before you can proceed with the wizard.

To check failover peer connectivity and compatibility, perform the following steps:

**Step 1**
Enter the IP address of the peer unit. This address does not have to be the failover link address, but it must be an interface that has ASDM access enabled on it. The field accepts both IPv4 and IPv6 addresses.

**Step 2**
Click **Next** to perform the following connectivity and compatibility tests:

- Connectivity test from this ASDM to the peer unit
- Connectivity test from this firewall device to the peer firewall device
- Hardware compatibility test for the platform
- Software version compatibility
- Failover license compatibility
- Firewall mode compatibility (routed or transparent)
- Context mode compatibility (single or multiple)
### Change a Device to Multiple Mode

The Change Device to Multiple Mode dialog box appears *only* for an Active/Active failover configuration. Active/Active failover requires that the ASA be in multiple context mode. This dialog box lets you convert a ASA in single context mode to multiple context mode.

When you convert from single context mode to multiple context mode, the ASA creates the system configuration and the admin context from the current running configuration. The admin context configuration is stored in the admin.cfg file. The conversion process does not save the previous startup configuration, so if the startup configuration differed from the running configuration, those differences are lost.

Converting the ASA from single context mode to multiple context mode causes the ASA and its peer to reboot. However, the High Availability and Scalability Wizard restores connectivity with the newly created admin context and reports the status in the Devices Status field in this dialog box.

**Note**

You must convert both the current ASA and its peer to multiple context mode before you can proceed.

To change the current ASA to multiple context mode, perform the following steps:

**Step 1** Click *Change device To Multiple Context*, where *device* is the hostname of the ASA.

**Step 2** Repeat this step for the peer ASA.

The status of the ASA appears during conversion to multiple context mode.

### Security Context Configuration

The Security Context Configuration screen appears *only* for an Active/Active configuration, and lets you assign security contexts to failover groups. It displays the name of currently configured security contexts, lets you add new ones, and change or remove existing ones as needed. In addition, it displays the failover group number to which the context is assigned and lets you change the failover group as needed. Although you can create security contexts in this screen, you cannot assign interfaces to those contexts or configure other properties for them. To configure context properties and assign interfaces to a context, choose *System > Security Contexts*.

### Failover Link Configuration

The Failover Link Configuration screen appears *only* if you are configuring LAN-based failover.

To configure LAN-based failover, perform the following steps:

**Step 1** Choose the LAN interface to use for failover communication from the drop-down list.

**Step 2** Enter a name for the interface.

**Step 3** Enter the IP address used for the failover link on the unit that has failover group 1 in the active state. This field accepts an IPv4 or IPv6 address.

**Step 4** Enter the IP address used for the failover link on the unit that has failover group 1 in the standby state. This field accepts an IPv4 or IPv6 address.
Step 5 Enter or choose a subnet mask (IPv4 addresses or a prefix (IPv6 Addresses) for the Active IP and Standby IP addresses.

Step 6 (For ASA 5505 only) Choose the switch port from the drop-down list, which includes the current VLAN assigned to each switch port and any name associated with the VLAN. Because a default VLAN exists for every switch port, do not choose VLAN 1 for the inside port, because one less inside port will be available for another use.

*Note* To provide sufficient bandwidth for failover, do not use trunks or PoE for failover.

Step 7 (Optional) Enter the secret key used to encrypt failover communication. If you leave this field blank, failover communication, including any passwords or keys in the configuration that are sent during command replication, will be in clear text.

---

**State Link Configuration**

*Note* The State Link Configuration screen does not appear on the ASA 5505.

The State Link Configuration screen lets you enable and disable Stateful Failover, and configure Stateful Failover link properties.

To enable Stateful Failover, perform the following steps:

Step 1 To pass state information across the LAN-based failover link, click *Use the LAN link as the State Link*.

Step 2 To disable Stateful Failover, click *Disable Stateful Failover*.

Step 3 To configure an unused interface as the Stateful Failover interface, click *Configure another interface for Stateful failover*.

Step 4 Choose the interface to use for Stateful Failover communication from the drop-down list.

Step 5 Enter the name for the Stateful Failover interface.

Step 6 Enter the IP address for the Stateful Failover link on the unit that has failover group 1 in the active state. This field accepts an IPv4 or IPv6 address.

Step 7 Enter the IP address for the Stateful Failover link on the unit that has failover group 1 in the standby state. This field accepts an IPv4 or IPv6 address.

Step 8 Enter or choose a subnet mask (IPv4 addresses or a prefix (IPv6 Addresses) for the Active IP and Standby IP addresses.

---

**Standby Address Configuration**

Use the Standby Address Configuration screen to assign standby IP addresses to the interface on the ASA. The interfaces currently configured on the failover devices appear. The interfaces are grouped by context, and the contexts are grouped by failover group.

To assign standby IP addresses to the interface on the ASA, perform the following steps:
Step 1  (For Active/Standby failover) Click the plus sign (+) by a device name to display the interfaces on that device. Click the minus sign (-) by a device name to hide the interfaces on that device.

Step 2  (For Active/Active failover) Click the plus sign (+) by a device, failover group, or context name to expand the list. Click the minus sign (-) by a device, failover group, or context name to collapse the list.

Step 3  Double-click the Active IP field to edit or add an active IP address. Changes to this field also appear in the Standby IP field for the corresponding interface on the failover peer unit. This field accepts IPv4 or IPv6 addresses.

Step 4  Double-click the Standby IP field to edit or add a standby IP address. Changes to this field also appear in the Active IP field for the corresponding interface on the failover peer unit. This field accepts IPv4 or IPv6 addresses.

Step 5  Check the Is Monitored check box to enable health monitoring for that interface. Uncheck the check box to disable health monitoring. By default, health monitoring of physical interfaces is enabled, and health monitoring of virtual interfaces is disabled.

Step 6  Choose the asynchronous group ID from the drop-down list. This setting is only available for physical interface. For virtual interfaces, this field displays “None.”

Summary

The Summary screen displays the results of the configuration steps that you performed in the previous wizard screens.

Verify your settings and click Finish to send your configuration to the device. If you are configuring failover, the configuration is also sent to the failover peer. If you need to change a setting, click Back to return to the screen that you want to change. Make the change, and click Next until you return to the Summary screen.

Configuring VPN Cluster Load Balancing with the High Availability and Scalability Wizard

The following procedure provides a high-level overview for configuring VPN cluster load balancing using the High Availability and Scalability Wizard. See Accessing the High Availability and Scalability Wizard, page 7-3, for information about accessing the wizard.

Each step in the procedure corresponds to a wizard screen. Click Next after completing each step, except for the last one, before proceeding to the next step. Each step also includes a reference to additional information that you may need to complete the step.

Step 1  In the Configuration Type screen, click Configure VPN Cluster Load Balancing.

See Configuration Type, page 7-6 for more information about this screen.

Step 2  Configure the VPN load balancing settings in the VPN Cluster Load Balancing Configuration screen.

See VPN Cluster Load Balancing Configuration, page 7-10 for more information about this screen.

Step 3  Review your configuration in the Summary screen. If necessary, click Back to return to a previous screen and make changes.

See Summary, page 7-9 for more information about this screen.
Step 4  Click **Finish**.

The VPN cluster load balancing configuration is sent to the ASA.

---

### VPN Cluster Load Balancing Configuration

If you have a remote-client configuration in which you are using two or more ASAs connected to the same network to handle remote sessions, you can configure these devices to share their session load. This feature is called load balancing, which directs session traffic to the least loaded device, thereby distributing the load among all devices. Load balancing makes efficient use of system resources and provides increased performance and system availability.

Use the VPN Cluster Load Balancing Configuration screen to set required parameters for a device to participate in a load balancing cluster.

Enabling load balancing involves the following:

- Configuring the load-balancing cluster by establishing a common virtual cluster IP address, UDP port (if necessary), and IPsec shared secret for the cluster. These values are identical for each device in the cluster.
- Configuring the participating device by enabling load balancing on the device and defining device-specific properties. These values vary from device to device.

---

**Note**  
Load balancing is effective only on remote sessions initiated with the Cisco VPN client (Version 3.0 and later), the Cisco VPN 3002 hardware client (Version 3.5 and later), or the ASA 5505 configured as an Easy VPN client. All other clients, including LAN-to-LAN connections, can connect to a ASA on which load balancing is enabled, but these clients cannot participate in load balancing.

To implement load balancing, you logically group together two or more devices on the same private LAN-to-LAN network into a virtual cluster by performing the following steps:

---

**Step 1**  
Choose the single IP address that represents the entire virtual cluster. Specify an IP address that is within the public subnet address range shared by all the ASAs in the virtual cluster.

**Step 2**  
Specify the UDP port for the virtual cluster in which this device is participating. The default value is 9023. If another application is using this port, enter the UDP destination port number that you want to use for load balancing.

**Step 3**  
To enable IPsec encryption and ensure that all load-balancing information communicated between the devices is encrypted, check the **Enable IPsec Encryption** check box. You must also specify and verify a shared secret. The ASAs in the virtual cluster communicate via LAN-to-LAN tunnels using IPsec. To disable IPsec encryption, uncheck the **Enable IPsec Encryption** check box.
Chapter 7  Using the High Availability and Scalability Wizard

Configuring VPN Cluster Load Balancing with the High Availability and Scalability Wizard

Note
When using encryption, you must have previously configured the load balancing inside interface. If that interface is not enabled on the load balancing inside interface, an error message appears when you try to configure cluster encryption.

If the load balancing inside interface is enabled when you configured cluster encryption, but is disabled before you configure the participation of the device in the virtual cluster, an error message appears when you check the Participate in Load Balancing Cluster check box, and encryption is not enabled for the cluster.

Step 4  Specify the shared secret to between IPsec peers when you enable IPsec encryption. The value that you enter appears as consecutive asterisk characters.

Step 5  Specify the priority assigned to this device within the cluster. The range is from 1 to 10. The priority indicates the likelihood of this device becoming the virtual cluster master, either at startup or when an existing master fails. The higher the priority set (for example, 10), the more likely that this device will become the virtual cluster master.

Note
If the devices in the virtual cluster are powered up at different times, the first device to be powered up assumes the role of virtual cluster master. Because every virtual cluster requires a master, each device in the virtual cluster checks when it is powered up to ensure that the cluster has a virtual master. If none exists, that device assumes the role. Devices powered up and added to the cluster later become secondary devices. If all the devices in the virtual cluster are powered up simultaneously, the device with the highest priority setting becomes the virtual cluster master. If two or more devices in the virtual cluster are powered up simultaneously, and both have the highest priority setting, the one with the lowest IP address becomes the virtual cluster master.

Step 6  Specify the name or IP address of the public interface for this device.

Step 7  Specify the name or IP address of the private interface for this device.

Step 8  Check the Send FQDN to client instead of an IP address when redirecting check box to have the VPN cluster master send a fully qualified domain name using the host and domain name of the cluster device instead of the outside IP address when redirecting VPN client connections to that cluster device.
Feature History for the High Availability and Scalability Wizard

Table 7-1 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 7-1 Feature History for the High Availability and Scalability Wizard

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Availability and Scalability Wizard</td>
<td>7.2(1)</td>
<td>This feature was introduced.</td>
</tr>
<tr>
<td>IPv6 Address Support in Failover Configurations</td>
<td>8.2(5)</td>
<td>This feature was introduced. The following screens of the High Availability and Scalability Wizard were modified to allow the use of IPv6 Addresses:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failover Peer Connectivity and Compatibility Check</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failover Link Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• State Link Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standby Address Configuration</td>
</tr>
</tbody>
</table>