



Logical Devices

- [About Logical Devices, on page 1](#)
- [Requirements and Prerequisites for Logical Devices, on page 1](#)
- [Guidelines and Limitations for Logical Devices, on page 3](#)
- [Add a Standalone Logical Device, on page 4](#)
- [Add a High Availability Pair, on page 9](#)
- [Add a Cluster, on page 9](#)
- [Manage Logical Devices, on page 17](#)
- [Monitoring Logical Devices, on page 24](#)
- [History for Logical Devices, on page 25](#)

About Logical Devices

A logical device lets you run one application instance .

When you add a logical device, you also define the application instance type and version, assign interfaces, and configure bootstrap settings that are pushed to the application configuration.

Standalone and Clustered Logical Devices

You can add the following logical device types:

- **Standalone**—A standalone logical device operates as a standalone unit or as a unit in a High Availability pair.
- **Cluster**—A clustered logical device lets you group multiple units together, providing all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. Multiple module devices, like the Firepower 9300, support intra-chassis clustering. For the Firepower 9300, all three modules must participate in the cluster.

Requirements and Prerequisites for Logical Devices

See the following sections for requirements and prerequisites.

Requirements and Prerequisites for Hardware and Software Combinations

The Firepower 9300 supports multiple models, security modules, application types, and high availability and scalability features. See the following requirements for allowed combinations.

Firepower 9300 Requirements

The Firepower 9300 includes 3 security module slots and multiple types of security modules. See the following requirements:

- Security Module Types—All modules in the Firepower 9300 must be the same type.
- Clustering—All security modules in the cluster, whether it is intra-chassis or inter-chassis, must be the same type. You can have different quantities of installed security modules in each chassis, although all modules present in the chassis must belong to the cluster including any empty slots. For example, you can install 2 SM-36s in chassis 1, and 3 SM-36s in chassis 2.
- High Availability—High Availability is only supported between same-type modules on the Firepower 9300.
- ASA and FTD application types—You can only install one application type on the chassis, ASA or FTD.
- ASA or FTD versions—You can run different versions of an application instance type on separate modules. For example, you can install FTD 6.3 on module 1, FTD 6.4 on module 2, and FTD 6.5 on module 3.

Requirements and Prerequisites for Clustering

Switch Requirements for Inter-Chassis Clustering

- Be sure to complete the switch configuration and successfully connect all the EtherChannels from the chassis to the switch(es) before you configure clustering on the Firepower 9300 chassis.
- For supported switch characteristics, see [Cisco FXOS Compatibility](#).

Requirements and Prerequisites for High Availability

- The two units in a High Availability Failover configuration must:
 - Be on a separate chassis; intra-chassis High Availability for the Firepower 9300 is not supported.
 - Be the same model.
 - Have the same interfaces assigned to the High Availability logical devices.
 - Have the same number and types of interfaces. All interfaces must be preconfigured in FXOS identically before you enable High Availability.
- For High Availability system requirements, see the application configuration guide chapter for High Availability.

Guidelines and Limitations for Logical Devices

See the following sections for guidelines and limitations.

General Guidelines and Limitations

Firewall Mode

You can set the firewall mode to routed or transparent in the bootstrap configuration for the FTD. For the ASA, you can change the firewall mode to transparent after you deploy. See [Change the ASA to Transparent Firewall Mode, on page 21](#).

High Availability

- Configure high availability within the application configuration.
- You can use any data interfaces as the failover and state links.

Context Mode

- Multiple context mode is only supported on the ASA.
- Enable multiple context mode in the ASA after you deploy.

Clustering Guidelines and Limitations

- When adding a unit to an existing cluster, or when reloading a unit, there will be a temporary, limited packet/connection drop; this is expected behavior. In some cases, the dropped packets can hang connections; for example, dropping a FIN/ACK packet for an FTP connection will make the FTP client hang. In this case, you need to reestablish the FTP connection.
- If you use a Windows 2003 server connected to a Spanned EtherChannel interface, when the syslog server port is down, and the server does not throttle ICMP error messages, then large numbers of ICMP messages are sent back to the cluster. These messages can result in some units of the cluster experiencing high CPU, which can affect performance. We recommend that you throttle ICMP error messages.
- We recommend connecting EtherChannels to a VSS or vPC for redundancy.
- Within a chassis, you cannot cluster some security modules and run other security modules in standalone mode; you must include all security modules in the cluster.

Defaults

- The cluster health check feature is enabled by default with the holdtime of 3 seconds. Interface health monitoring is enabled on all interfaces by default.

Add a Standalone Logical Device

Standalone logical devices can be used alone or as high availability units. For more information about high availability usage, see [Add a High Availability Pair, on page 9](#).

Add a Standalone ASA

Standalone logical devices work either alone or in a High Availability pair. On the Firepower 9300 with multiple security modules, you can deploy either a cluster or standalone devices. The cluster must use all modules, so you cannot mix and match a 2-module cluster plus a single standalone device, for example.

You can deploy a routed firewall mode ASA from the Firepower 9300 chassis. To change the ASA to transparent firewall mode, complete this procedure, and then see [Change the ASA to Transparent Firewall Mode, on page 21](#).

For multiple context mode, you must first deploy the logical device, and then enable multiple context mode in the ASA application.

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then download that image to the Firepower 9300 chassis.
- Configure a management interface to use with the logical device. The management interface is required. Note that this management interface is not the same as the chassis management port that is used only for chassis management (in FXOS, you might see it displayed as MGMT, management0, or other similar names).
- Gather the following information:
 - Interface IDs for this device
 - Management interface IP address and network mask
 - Gateway IP address

Procedure

Step 1 Enter security services mode.

scope ssa

Example:

```
Firepower# scope ssa
Firepower /ssa #
```

Step 2 Set the application instance image version.

a) View available images. Note the Version number that you want to use.

show app

Example:

```

Firepower /ssa # show app
  Name          Version      Author      Supported Deploy Types CSP Type      Is Default
  App
  -----
  asa           9.9.1       cisco       Native
  asa           9.10.1      cisco       Native
  ftd           6.2.3       cisco       Native
  Application No
  Application Yes
  Application Yes

```

- b) Set the scope to the security module/engine slot.

scope slot *slot_id*

The *slot_id* is 1, 2, or 3 for the Firepower 9300.

Example:

```

Firepower /ssa # scope slot 1
Firepower /ssa/slot #

```

- c) Create the application instance.

enter app-instance *asa*

Example:

```

Firepower /ssa/slot # enter app-instance asa
Firepower /ssa/slot/app-instance* #

```

- d) Set the ASA image version.

set startup-version *version*

Example:

```

Firepower /ssa/slot/app-instance* # set startup-version 9.10.1

```

- e) Exit to slot mode.

exit

Example:

```

Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #

```

- f) Exit to ssa mode.

exit

Example:

```

Firepower /ssa/slot* # exit
Firepower /ssa* #

```

Example:

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

Step 3 Create the logical device.

enter logical-device *device_name* **asa** *slot_id* **standalone**

Example:

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

Step 4 Assign the management and data interfaces to the logical device. Repeat for each interface.

create external-port-link *name* *interface_id* **asa**

set description *description*

exit

- *name*—The name is used by the Firepower 9300 chassis supervisor; it is not the interface name used in the ASA configuration.
- *description*—Use quotes (") around phrases with spaces.

The management interface is not the same as the chassis management port. You will later enable and configure the data interfaces on the ASA, including setting the IP addresses.

Example:

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

Step 5 Configure the management bootstrap information.

a) Create the bootstrap object.

create mgmt-bootstrap **asa**

Example:

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- b) Specify the admin password.

```
create bootstrap-key-secret PASSWORD
```

```
set value
```

```
Enter a value: password
```

```
Confirm the value: password
```

```
exit
```

Example:

The pre-configured ASA admin user is useful for password recovery; if you have FXOS access, you can reset the admin user password if you forget it.

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- c) Configure the IPv4 management interface settings.

```
create ipv4 slot_id default
```

```
set ip ip_address mask network_mask
```

```
set gateway gateway_address
```

```
exit
```

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

- d) Configure the IPv6 management interface settings.

```
create ipv6 slot_id default
```

```
set ip ip_address prefix-length prefix
```

```
set gateway gateway_address
```

```
exit
```

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) Exit the management bootstrap mode.

exit

Example:

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

Step 6 Save the configuration.

commit-buffer

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the status of the deployment using the **show app-instance** command. The application instance is running and ready to use when the **Admin State is Enabled** and the **Oper State is Online**.

Example:

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Deploy Type	Profile Name	Cluster	State	Cluster Role		
asa	asal	2	Disabled	Not Installed		9.12.1
	Native		Not Applicable	None		
ftd	ftdl	1	Enabled	Online	6.4.0.49	6.4.0.49
	Container	Default-Small	Not Applicable	None		

Step 7 See the ASA configuration guide to start configuring your security policy.

Example

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
```



```
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

Add a High Availability Pair

ASA High Availability (also known as failover) is configured within the application, not in FXOS. However, to prepare your chassis for high availability, see the following steps.

Before you begin

See [Requirements and Prerequisites for High Availability, on page 2](#).

Procedure

Step 1 Allocate the same interfaces to each logical device.

Step 2 Allocate 1 or 2 data interfaces for the failover and state link(s).

These interfaces exchange high availability traffic between the 2 chassis. We recommend that you use a 10 GB data interface for a combined failover and state link. If you have available interfaces, you can use separate failover and state links; the state link requires the most bandwidth. You cannot use the management-type interface for the failover or state link. We recommend that you use a switch between the chassis, with no other device on the same network segment as the failover interfaces.

Step 3 Enable High Availability on the logical devices.

Step 4 If you need to make interface changes after you enable High Availability, perform the changes on the standby unit first, and then perform the changes on the active unit.

Note For the ASA, if you remove an interface in FXOS (for example, if you remove a network module, remove an EtherChannel, or reassign an interface to an EtherChannel), then the ASA configuration retains the original commands so that you can make any necessary adjustments; removing an interface from the configuration can have wide effects. You can manually remove the old interface configuration in the ASA OS.

Add a Cluster

Clustering lets you group multiple devices together as a single logical device. A cluster provides all the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices. The Firepower 9300, which includes multiple modules, supports intra-chassis clustering where you group all modules within a single chassis into a cluster.



Note The Firepower 9300 does not support a cluster across multiple chassis (inter-chassis); only intra-chassis clustering is supported.

About Clustering on the Firepower 9300 Chassis

The cluster consists of multiple devices acting as a single logical unit. When you deploy a cluster on the Firepower 9300 chassis, it does the following:

- Creates a *cluster-control link* (by default, port-channel 48) for unit-to-unit communication.
For intra-chassis clustering, this link utilizes the Firepower 9300 backplane for cluster communications.
- Creates the cluster bootstrap configuration within the application.

When you deploy the cluster, the chassis supervisor pushes a minimal bootstrap configuration to each unit that includes the cluster name, cluster control link interface, and other cluster settings. Some parts of the bootstrap configuration may be user-configurable within the application if you want to customize your clustering environment.

- Assigns data interfaces to the cluster as *Spanned* interfaces.

For intra-chassis clustering, spanned interfaces are not limited to EtherChannels. The Firepower 9300 supervisor uses EtherChannel technology internally to load-balance traffic to multiple modules on a shared interface, so any data interface type works for Spanned mode.



Note Individual interfaces are not supported, with the exception of a management interface.

- Assigns a management interface to all units in the cluster.

The following sections provide more detail about clustering concepts and implementation.

Primary and Secondary Unit Roles

One member of the cluster is the primary unit. The primary unit is determined automatically. All other members are secondary units.

You must perform all configuration on the primary unit only; the configuration is then replicated to the secondary units.

Cluster Control Link

The cluster control link is automatically created using the Port-channel 48 interface.

For intra-chassis clustering, this interface has no member interfaces. This Cluster type EtherChannel utilizes the Firepower 9300 backplane for cluster communications for intra-chassis clustering.

Cluster control link traffic includes both control and data traffic.

Management Interface

You must assign a Management type interface to the cluster. This interface is a special *individual* interface as opposed to a Spanned interface. The management interface lets you connect directly to each unit.

For the ASA, the Main cluster IP address is a fixed address for the cluster that always belongs to the current primary unit. You must configure a range of addresses so that each unit, including the current primary unit, can use a Local address from the range. The Main cluster IP address provides consistent management access to an address; when a primary unit changes, the Main cluster IP address moves to the new primary unit, so management of the cluster continues seamlessly. The Local IP address is used for routing, and is also useful for troubleshooting. For example, you can manage the cluster by connecting to the Main cluster IP address, which is always attached to the current primary unit. To manage an individual member, you can connect to the Local IP address. For outbound management traffic such as TFTP or syslog, each unit, including the primary unit, uses the Local IP address to connect to the server.

Add an ASA Cluster

You can add a single Firepower 9300 chassis as an intra-chassis cluster.

Create an ASA Cluster

Set the scope to the image version.

You can easily deploy the cluster from the Firepower 9300 chassis supervisor. All initial configuration is automatically generated for each unit.

In a Firepower 9300 chassis, you must enable clustering for all 3 module slots, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

For multiple context mode, you must first deploy the logical device, and then enable multiple context mode in the ASA application.

To change the ASA to transparent firewall mode, complete the initial deployment, and then change the firewall mode within the ASA CLI.

Before you begin

- Download the application image you want to use for the logical device from Cisco.com, and then upload that image to the Firepower 9300 chassis.
- Gather the following information:
 - Management interface ID, IP address, and network mask
 - Gateway IP address

Procedure

- Step 1** Configure interfaces.
- Step 2** Enter security services mode.
- ```
scope ssa
```

**Example:**

```
Firepower# scope ssa
Firepower /ssa #
```

**Step 3** Set the application instance image version.

- a) View available images. Note the Version number that you want to use.

**show app****Example:**

```
Firepower /ssa # show app
Name Version Author Supported Deploy Types CSP Type Is Default
App

asa 9.9.1 cisco Native Application No
asa 9.10.1 cisco Native Application Yes
ftd 6.2.3 cisco Native Application Yes
```

- b) Set the scope to the image version.

**scope app asa *application\_version*****Example:**

```
Firepower /ssa # scope app asa 9.10.1
Firepower /ssa/app #
```

- c) Set this version as the default.

**set-default****Example:**

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

- d) Exit to ssa mode.

**exit****Example:**

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

**Example:**

```
Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

**Step 4** Create the cluster.

**enter logical-device** *device\_name* **asa slots clustered**

- *device\_name*—Used by the Firepower 9300 chassis supervisor to configure clustering settings and assign interfaces; it is not the cluster name used in the security module configuration. You must specify all three security modules, even if you have not yet installed the hardware.
- *slots*—Assigns the chassis modules to the cluster. For the Firepower 4100, specify **1**. For the Firepower 9300, specify **1,2,3**. You must enable clustering for all 3 module slots in a Firepower 9300 chassis, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.

**Example:**

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

**Step 5** Configure the cluster bootstrap parameters.

These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

a) Create the cluster bootstrap object.

**enter cluster-bootstrap**

**Example:**

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) Configure an authentication key for control traffic on the cluster control link.

**set key**

**Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: diamonddogs
```

You are prompted to enter the shared secret.

The shared secret is an ASCII string from 1 to 63 characters. The shared secret is used to generate the key. This option does not affect datapath traffic, including connection state update and forwarded packets, which are always sent in the clear.

c) Set the cluster interface mode.

**set mode spanned-etherchannel**

Spanned EtherChannel mode is the only supported mode.

**Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- d) Set the cluster group name in the security module configuration.

```
set service-type cluster_name
```

The name must be an ASCII string from 1 to 38 characters.

**Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

- e) Configure the management IP address information.

This information is used to configure a management interface in the security module configuration.

1. Configure a pool of Local IP addresses, one of which will be assigned to each cluster unit for the interface.

```
set ipv4 pool start_ip end_ip
```

```
set ipv6 pool start_ip end_ip
```

Include at least as many addresses as there are units in the cluster. Note that for the Firepower 9300, you must include 3 addresses per chassis, even if you do not have all module slots filled. If you plan to expand the cluster, include additional addresses. The Virtual IP address (known as the Main cluster IP address) that belongs to the current control unit is *not* a part of this pool; be sure to reserve an IP address on the same network for the Main cluster IP address. You can use IPv4 and/or IPv6 addresses.

2. Configure the Main cluster IP address for the management interface.

```
set virtual ipv4 ip_address mask mask
```

```
set virtual ipv6 ip_address prefix-length prefix
```

This IP address must be on the same network as the cluster pool addresses, but not be part of the pool.

3. Enter the network gateway address.

```
set ipv4 gateway ip_address
```

```
set ipv6 gateway ip_address
```

**Example:**

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11 2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

- f) Exit the cluster bootstrap mode.

```
exit
```

**Example:**

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
```

```

Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #

```

### Step 6 Configure the management bootstrap parameters.

These settings are meant for initial deployment only, or for disaster recovery. For normal operation, you can later change most values in the application CLI configuration.

- a) Create the management bootstrap object.

**enter mgmt-bootstrap asa**

**Example:**

```

Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #

```

- b) Specify the admin password.

**create bootstrap-key-secret PASSWORD**

**set value**

Enter a value: *password*

Confirm the value: *password*

**exit**

**Example:**

The pre-configured ASA admin user is useful for password recovery; if you have FXOS access, you can reset the admin user password if you forget it.

**Example:**

```

Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #

```

- c) Exit the management bootstrap mode.

**exit**

**Example:**

```

Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #

```

### Step 7 Save the configuration.

**commit-buffer**

The chassis deploys the logical device by downloading the specified software version and pushing the bootstrap configuration and management interface settings to the application instance. Check the status of the deployment using the **show app-instance** command. The application instance is running and ready to use when the **Admin State** is **Enabled** and the **Oper State** is **Online**.

#### Example:

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
```

| App Name    | Identifier   | Slot ID | Admin State    | Oper State    | Running Version | Startup Version |
|-------------|--------------|---------|----------------|---------------|-----------------|-----------------|
| Deploy Type | Profile Name | Cluster | State          | Cluster Role  |                 |                 |
| ftd         | cluster1     | 1       | Enabled        | Online        | 6.4.0.49        | 6.4.0.49        |
| Native      |              |         | In Cluster     | Slave         |                 |                 |
| ftd         | cluster1     | 2       | Enabled        | Online        | 6.4.0.49        | 6.4.0.49        |
| Native      |              |         | In Cluster     | Master        |                 |                 |
| ftd         | cluster1     | 3       | Disabled       | Not Available |                 | 6.4.0.49        |
| Native      |              |         | Not Applicable | None          |                 |                 |

### Step 8

Connect to the control unit ASA to customize your clustering configuration.

#### Example

For chassis 1:

```
scope eth-uplink
 scope fabric a
 enter port-channel 1
 set port-type data
 enable
 enter member-port Ethernet1/1
 exit
 enter member-port Ethernet1/2
 exit
 exit
 enter port-channel 2
 set port-type data
 enable
 enter member-port Ethernet1/3
 exit
 enter member-port Ethernet1/4
 exit
 exit
 enter port-channel 3
 set port-type data
 enable
 enter member-port Ethernet1/5
 exit
 enter member-port Ethernet1/6
 exit
 exit
 enter port-channel 4
 set port-type mgmt
 enable
 enter member-port Ethernet2/1
 exit
```



```
 enter member-port Ethernet2/2
 exit
 exit

 exit
 exit
commit-buffer

scope ssa
 enter logical-device ASA1 asa "1,2,3" clustered
 enter cluster-bootstrap
 set chassis-id 1
 set ipv4 gateway 10.1.1.254
 set ipv4 pool 10.1.1.11 10.1.1.27
 set ipv6 gateway 2001:DB8::AA
 set ipv6 pool 2001:DB8::11 2001:DB8::27
 set key
 Key: f@arscape
 set mode spanned-etherchannel
 set service-type cluster1
 set virtual ipv4 10.1.1.1 mask 255.255.255.0
 set virtual ipv6 2001:DB8::1 prefix-length 64
 exit
 exit
scope app asa 9.5.2.1
 set-default
 exit
commit-buffer
```

## Manage Logical Devices

You can delete a logical device, convert an ASA to transparent mode, change the interface configuration, and perform other tasks on existing logical devices.

## Connect to the Console of the Application

Use the following procedure to connect to the console of the application.

### Procedure

---

**Step 1** Connect to the module CLI.

**connect module *slot\_number* console**

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot\_number*.

#### Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

**Step 2** Connect to the application console.

**connect asa**

**Example:**

```
Firepower-module1> connect asa
Connecting to asa(asa1) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

**Example:**

```
Firepower-module1> connect ftd
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

**Step 3** Exit the application console to the FXOS module CLI.

- ASA—Enter **Ctrl-a, d**

**Step 4** Return to the supervisor level of the FXOS CLI.

a) Enter ~

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

## Delete a Logical Device

### Procedure

**Step 1** Enter security services mode:

```
Firepower# scope ssa
```

**Step 2** View details for the logical devices on the chassis:

```
Firepower /ssa # show logical-device
```

**Step 3** For each logical device that you want to delete, enter the following command:

```
Firepower /ssa # delete logical-device device_name
```

**Step 4** View details for the applications installed on the logical devices:

```
Firepower /ssa # show app-instance
```

**Step 5** For each application that you want to delete, enter the following commands:

- a) Firepower /ssa # **scope slot** *slot\_number*
- b) Firepower /ssa/slot # **delete app-instance** *application\_name*
- c) Firepower /ssa/slot # **exit**

**Step 6** Commit the configuration:

```
commit-buffer
```

Commits the transaction to the system configuration.

### Example

```
Firepower# scope ssa
Firepower /ssa # show logical-device
```

Logical Device:

| Name | Description | Slot ID | Mode      | Operational State | Template Name |
|------|-------------|---------|-----------|-------------------|---------------|
| FTD  |             | 1,2,3   | Clustered | Ok                | ftd           |

```
Firepower /ssa # delete logical-device FTD
```

```
Firepower /ssa* # show app-instance
```

| Application Name | Slot ID | Admin State | Operational State | Running Version | Startup Version |
|------------------|---------|-------------|-------------------|-----------------|-----------------|
| ftd              | 1       | Disabled    | Stopping          | 6.0.0.837       |                 |
| ftd              | 2       | Disabled    | Offline           | 6.0.0.837       |                 |
| ftd              | 3       | Disabled    | Not Available     |                 |                 |

```

```

```
ftd 1 Disabled Stopping 6.0.0.837
```

```
6.0.0.837 Not Applicable
```

```
ftd 2 Disabled Offline 6.0.0.837
```

```
6.0.0.837 Not Applicable
```

```
ftd 3 Disabled Not Available
```

```
6.0.0.837 Not Applicable
```

```
Firepower /ssa* # scope slot 1
```

```
Firepower /ssa/slot # delete app-instance ftd
```

```
Firepower /ssa/slot* # exit
```

```
Firepower /ssa* # scope slot 2
```

```
Firepower /ssa/slot # delete app-instance ftd
```

```
Firepower /ssa/slot* # exit
```

```
Firepower /ssa* # scope slot 3
```

```
Firepower /ssa/slot # delete app-instance ftd
```

```
Firepower /ssa/slot* # exit
```

```
Firepower /ssa* # commit-buffer
```

## Remove a Cluster Unit

The following sections describe how to remove units temporarily or permanently from the cluster.

### Temporary Removal

A cluster unit will be automatically removed from the cluster due to a hardware or network failure, for example. This removal is temporary until the conditions are rectified, and it can rejoin the cluster. You can also manually disable clustering.

To check whether a device is currently in the cluster, check the cluster status within the application using the **show cluster info** command:

```
ciscoasa# show cluster info
Clustering is not enabled
```

- **Disable clustering in the application**—You can disable clustering using the application CLI. Enter the **cluster remove unit name** command to remove any unit other than the one you are logged into. The bootstrap configuration remains intact, as well as the last configuration synced from the control unit, so you can later re-add the unit without losing your configuration. If you enter this command on a data unit to remove the control unit, a new control unit is elected.

When a device becomes inactive, all data interfaces are shut down; only the Management interface can send and receive traffic. To resume traffic flow, re-enable clustering. The Management interface remains up using the IP address the unit received from the bootstrap configuration. However if you reload, and the unit is still inactive in the cluster, the Management interface is disabled.

To reenable clustering, on the ASA enter **cluster group name** and then **enable**.

- **Disable the application instance**—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa asa1
Firepower-chassis /ssa/slot/app-instance # disable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

To reenable:

```
Firepower-chassis /ssa/slot/app-instance # enable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

- **Shut down the security module/engine**—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope service-profile server 1/1
Firepower-chassis /org/service-profile # power down soft-shut-down
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

To power up:

```
Firepower-chassis /org/service-profile # power up
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

- **Shut down the chassis**—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

### Permanent Removal

You can permanently remove a cluster member using the following methods.

- Delete the logical device—At the FXOS CLI, see the following example:

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- Remove the chassis or security module from service—If you remove a device from service, you can add replacement hardware as a new member of the cluster.

## Change the ASA to Transparent Firewall Mode

You can only deploy a routed firewall mode ASA from the Firepower 9300 chassis. To change the ASA to transparent firewall mode, complete the initial deployment, and then change the firewall mode within the ASA CLI. For standalone ASAs, because changing the firewall mode erases the configuration, you must then redeploy the configuration from the Firepower 9300 chassis to regain the bootstrap configuration. The ASA then remains in transparent mode with a working bootstrap configuration. For clustered ASAs, the configuration is not erased, so you do not need to redeploy the bootstrap configuration from FXOS.

### Procedure

**Step 1** Connect to the ASA console according to [Connect to the Console of the Application, on page 17](#). For a cluster, connect to the primary unit. For a failover pair, connect to the active unit.

**Step 2** Enter configuration mode:

**enable**

**configure terminal**

By default, the enable password is blank.

**Step 3** Set the firewall mode to transparent:

**firewall transparent**

**Step 4** Save the configuration:

**write memory**

For a cluster or failover pair, this configuration is replicated to secondary units:

```
asa(config)# firewall transparent
asa(config)# write memory
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
Beginning configuration replication to unit-1-2
End Configuration Replication to data unit.
```

```
asa(config)#
```

- Step 5** On the Firepower Chassis Manager **Logical Devices** page, click the **Edit** icon to edit the ASA. The **Provisioning** page appears.
- Step 6** Click the device icon to edit the bootstrap configuration. Change any value in your configuration, and click **OK**.  
You must change the value of at least one field, for example, the **Password** field.  
You see a warning about changing the bootstrap configuration; click **Yes**.
- Step 7** Click **Save** to redeploy the configuration to the ASA.  
Wait several minutes for the chassis/security modules to reload, and for the ASA to become operational again. The ASA now has an operational bootstrap configuration, but remains in transparent mode.
- 

## Change an Interface on a Firepower Threat Defense Logical Device

You can allocate or unallocate an interface on the FTD logical device. You can then sync the interface configuration in .

Adding a new interface, or deleting an unused interface has minimal impact on the FTD configuration. However, deleting an interface that is used in your security policy will impact the configuration. Interfaces can be referenced directly in many places in the FTD configuration, including access rules, NAT, SSL, identity rules, VPN, DHCP server, and so on. Policies that refer to security zones are not affected. You can also edit the membership of an allocated EtherChannel without affecting the logical device or requiring a sync on the .

### Before you begin

- Configure your interfaces, and add any EtherChannels according to [Configure a Physical Interface](#) and [Add an EtherChannel \(Port Channel\)](#).
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the interface from the logical device first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the device.
- If you want to replace the management or firepower eventing interface, you must use the Firepower Chassis Manager; the CLI does not support this change.
- For clustering or High Availability, make sure you add or remove the interface on all units before you sync the configuration in the . We recommend that you make the interface changes on the data/standby unit(s) first, and then on the control/active unit. Note that new interfaces are added in an administratively down state, so they do not affect interface monitoring.

## Procedure

---

- Step 1** Enter security services mode:  
Firepower# **scope ssa**
- Step 2** Edit the logical device:  
Firepower /ssa # **scope logical-device** *device\_name*
- Step 3** Allocate a new interface to the logical device:  
Firepower /ssa/logical-device\* # **create external-port-link** *name interface\_id ftd*  
Do not delete any interfaces yet.
- Step 4** Commit the configuration:  
**commit-buffer**  
Commits the transaction to the system configuration.
- Step 5** In FXOS, unallocate an interface from the logical device:  
Firepower /ssa/logical-device # **delete external-port-link** *name*  
Enter the **show external-port-link** command to view interface names.
- Step 6** Commit the configuration:  
**commit-buffer**  
Commits the transaction to the system configuration.
- Step 7** Sync the interfaces again in .
- 

## Change an Interface on an ASA Logical Device

You can allocate, unallocate, or replace a management interface on an ASA logical device. ASDM discovers the new interfaces automatically.

Adding a new interface, or deleting an unused interface has minimal impact on the ASA configuration. However, if you remove an allocated interface in FXOS (for example, if you remove a network module, remove an EtherChannel, or reassign an allocated interface to an EtherChannel), and the interface is used in your security policy, removal will impact the ASA configuration. In this case, the ASA configuration retains the original commands so that you can make any necessary adjustments. You can manually remove the old interface configuration in the ASA OS.



---

**Note** You can edit the membership of an allocated EtherChannel without impacting the logical device.

---

**Before you begin**

- Configure your interfaces and add any EtherChannels according to [Configure a Physical Interface](#) and [Add an EtherChannel \(Port Channel\)](#).
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the interface from the logical device first, then add the interface to the EtherChannel. For a new EtherChannel, you can then allocate the EtherChannel to the device.
- For clustering or failover, make sure you add or remove the interface on all units. We recommend that you make the interface changes on the data/standby unit(s) first, and then on the control/active unit. New interfaces are added in an administratively down state, so they do not affect interface monitoring.

**Procedure**


---

**Step 1** Enter security services mode:

```
Firepower# scope ssa
```

**Step 2** Edit the logical device:

```
Firepower /ssa # scope logical-device device_name
```

**Step 3** Unallocate an interface from the logical device:

```
Firepower /ssa/logical-device # delete external-port-link name
```

Enter the **show external-port-link** command to view interface names.

For a management interface, delete the current interface then commit your change using the **commit-buffer** command before you add the new management interface.

**Step 4** Allocate a new interface to the logical device:

```
Firepower /ssa/logical-device* # create external-port-link name interface_id asa
```

**Step 5** Commit the configuration:

```
commit-buffer
```

Commits the transaction to the system configuration.

---

## Monitoring Logical Devices

- **show app**

View available images.

```
Firepower# scope ssa
Firepower /ssa # show app
 Name Version Author Supported Deploy Types CSP Type Is Default
App
```



```

asa 9.10.1 cisco Native Application Yes
ftd 6.2.3 cisco Native Application Yes

```

• **show app-instance**

View the application instance status and information.

```

Firepower# scope ssa
Firepower /ssa # show app-instance
App Name Slot ID Admin State Oper State Running Version Startup Version
Cluster State Cluster Role

ftd 1 Enabled Online 6.2.1.62 6.2.1.62 Not
Applicable None

```

• **show logical-device**

View details for logical devices.

```

Firepower# scope ssa
Firepower /ssa # show logical-device

Logical Device:
 Name Description Slot ID Mode Oper State Template Name

 asal 1 Standalone Ok

```

## History for Logical Devices

| Feature Name                                               | Platform Releases | Feature Information                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------------------------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Intra-chassis Clustering for the ASA on the Firepower 9300 | 1.1.1             | You can cluster all ASA security modules within the Firepower 9300 chassis.<br>We introduced the following commands: <b>enter cluster-bootstrap</b> , <b>enter logical-device clustered</b> , <b>set chassis-id</b> , <b>set ipv4 gateway</b> , <b>set ipv4 pool</b> , <b>set ipv6 gateway</b> , <b>set ipv6 pool</b> , <b>set key</b> , <b>set mode spanned-etherchannel</b> , <b>set port-type cluster</b> , <b>set service-type</b> , <b>set virtual ipv4</b> , <b>set virtual ipv6</b> |

