Deploy a Cluster for Firepower Threat Defense for Scalability and High Availability

Deploying a Cluster for Firepower Threat Defense for Scalability and High Availability

Clustering lets you group multiple FTD units together as a single logical device. Clustering is only supported for the FTD device on the Firepower 9300 and the Firepower 4100 series. 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.

Note
Some features are not supported when using clustering. See Unsupported Features with Clustering, on page 7.

Note
This document covers the latest Firepower Threat Defense version features; see History for Clustering, on page 37 for details about feature changes. If you are on an old version of software, refer to the procedures in the FXOS configuration guide and Firepower Management Center configuration guide for your version.

Benefit of this Integration

The FXOS platform lets you run multiple logical devices, including the FTD. Deploying standalone and clustered logical devices is easy for both intra-chassis clusters (for the Firepower 9300) and inter-chassis clusters. When you deploy a cluster from FXOS, you pre-configure the FTD bootstrap configuration so very little customization is required within the FTD application. You can also add additional cluster members by exporting the cluster configuration in FXOS.

Integrated Products

This table lists the products required for this integration.
Table 1: Integrated Products for Clustering

<table>
<thead>
<tr>
<th>Products</th>
<th>Function</th>
<th>Minimum Version</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower 4100 or 9300</td>
<td>Hardware platform to run the FTD</td>
<td>FXOS 1.1(4)</td>
<td>Required</td>
</tr>
<tr>
<td>Firepower Chassis Manager</td>
<td>FXOS GUI device manager</td>
<td>Firepower Chassis Manager 1.1(4)</td>
<td>Optional; you can alternatively use the CLI</td>
</tr>
<tr>
<td>FTD</td>
<td>Next-generation Firewall application</td>
<td>Firepower 6.0.1</td>
<td>Required</td>
</tr>
<tr>
<td>FMC</td>
<td>GUI multidevice manager</td>
<td>Firepower 6.0.1</td>
<td>Required</td>
</tr>
</tbody>
</table>

**Workflow**

This workflow uses Firepower Chassis Manager on FXOS and FMC for the FTD to complete your clustering deployment.

**Procedure**

**Step 1**
FXOS prerequisites:

- Configure one management and all data interfaces that you intend to assign to the FTD. The cluster interface is defined by default as Port-Channel 48.

**Step 2**
FXOS tasks:

a) Create a Firepower Threat Defense Cluster, on page 14.

b) Add More Cluster Members, on page 21

**Step 3**
FMC tasks:

a) FMC: Add a Cluster, on page 23.

b) FMC: Configure Data and Diagnostic Interfaces, on page 24. The management interface was pre-configured when you deployed the cluster.

**Step 4**
FXOS and/or FMC tasks:

a) FMC: Manage Cluster Members, on page 27.

**About Clustering on the Firepower 4100/9300 Chassis**

The cluster consists of multiple devices acting as a single logical unit. When you deploy a cluster on the Firepower 4100/9300 chassis, it does the following:

- Creates a *cluster-control link* (by default, port-channel 48) for unit-to-unit communication. For intra-chassis clustering (Firepower 9300 only), this link utilizes the Firepower 9300 backplane for cluster
communications. For inter-chassis clustering, you need to manually assign physical interface(s) to this EtherChannel for communications between chassis.

• Creates the cluster bootstrap configuration within the application.

When you deploy the cluster, the Firepower 4100/9300 chassis supervisor pushes a minimal bootstrap configuration to each unit that includes the cluster name, cluster control link interface, and other cluster settings.

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

For intra-chassis clustering, spanned interfaces are not limited to EtherChannels, like it is for inter-chassis clustering. 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. For inter-chassis clustering, you must use Spanned EtherChannels for all data interfaces.

---

**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. See also Reference for Clustering, on page 32.

### Bootstrap Configuration

When you deploy the cluster, the Firepower 4100/9300 chassis supervisor pushes a minimal bootstrap configuration to each unit that includes the cluster name, cluster control link interface, and other cluster settings.

### Cluster Members

Cluster members work together to accomplish the sharing of the security policy and traffic flows.

One member of the cluster is the **master** unit. The master unit is determined automatically. All other members are **slave** units.

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

Some features do not scale in a cluster, and the master unit handles all traffic for those features. See Centralized Features for Clustering, on page 7.

### 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.
Size the Cluster Control Link for Inter-Chassis Clustering

If possible, you should size the cluster control link to match the expected throughput of each chassis so the cluster-control link can handle the worst-case scenarios.

Cluster control link traffic is comprised mainly of state update and forwarded packets. The amount of traffic at any given time on the cluster control link varies. The amount of forwarded traffic depends on the load-balancing efficacy or whether there is a lot of traffic for centralized features. For example:

- NAT results in poor load balancing of connections, and the need to rebalance all returning traffic to the correct units.
- When membership changes, the cluster needs to rebalance a large number of connections, thus temporarily using a large amount of cluster control link bandwidth.

A higher-bandwidth cluster control link helps the cluster to converge faster when there are membership changes and prevents throughput bottlenecks.

---

**Note**

If your cluster has large amounts of asymmetric (rebalanced) traffic, then you should increase the cluster control link size.

Cluster Control Link Redundancy for Inter-Chassis Clustering

The following diagram shows how to use an EtherChannel as a cluster control link in a Virtual Switching System (VSS) or Virtual Port Channel (vPC) environment. All links in the EtherChannel are active. When the switch is part of a VSS or vPC, then you can connect Firepower 9300 chassis interfaces within the same EtherChannel to separate switches in the VSS or vPC. The switch interfaces are members of the same EtherChannel port-channel interface, because the separate switches act like a single switch. Note that this EtherChannel is device-local, not a Spanned EtherChannel.
Cluster Control Link Reliability for Inter-Chassis Clustering

To ensure cluster control link functionality, be sure the round-trip time (RTT) between units is less than 20 ms. This maximum latency enhances compatibility with cluster members installed at different geographical sites. To check your latency, perform a ping on the cluster control link between units.

The cluster control link must be reliable, with no out-of-order or dropped packets; for example, for inter-site deployment, you should use a dedicated link.

Cluster Control Link Network

The Firepower 4100/9300 chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.chassis_id.slot_id. You can customize this IP address when you deploy the cluster. The cluster control link network cannot include any routers between units; only Layer 2 switching is allowed.

Management Network

We recommend connecting all units to a single management network. This network is separate from the cluster control link.

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. This Management logical interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firepower Management Center. It uses its own local authentication, IP address, and static routing. Each cluster member uses a separate IP address on the management network that you set as part of the bootstrap configuration.

The management interface is shared between the Management logical interface and the Diagnostic logical interface. The Diagnostic logical interface is optional and is not configured as part of the bootstrap configuration. The Diagnostic interface can be configured along with the rest of the data interfaces. If you choose to configure the Diagnostic interface, configure a Main cluster IP address as a fixed address for the cluster that always belongs to the current master unit. You also configure a range of addresses so that each unit, including the current master, can use a Local address from the range. The Main cluster IP address provides consistent diagnostic access to an address; when a master unit changes, the Main cluster IP address moves to the new master unit, so access to the cluster continues seamlessly. For outbound management traffic such as TFTP or syslog, each unit, including the master unit, uses the Local IP address to connect to the server.

Cluster Interfaces

For intra-chassis clustering, you can assign both physical interfaces or EtherChannels (also known as port channels) to the cluster. Interfaces assigned to the cluster are Spanned interfaces that load-balance traffic across all members of the cluster.

For inter-chassis clustering, you can only assign data EtherChannels to the cluster. These Spanned EtherChannels include the same member interfaces on each chassis; on the upstream switch, all of these interfaces are included in a single EtherChannel, so the switch does not know that it is connected to multiple devices.

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

You can group one or more interfaces per chassis into an EtherChannel that spans all chassis in the cluster. The EtherChannel aggregates the traffic across all the available active interfaces in the channel. A Spanned EtherChannel can be configured in both routed and transparent firewall modes. In routed mode, the EtherChannel is configured as a routed interface with a single IP address. In transparent mode, the IP address is assigned to the BVI, not to the bridge group member interface. The EtherChannel inherently provides load balancing as part of basic operation.

Connecting to a VSS or vPC

We recommend connecting EtherChannels to a VSS or vPC to provide redundancy for your interfaces.

Configuration Replication

All units in the cluster share a single configuration. You can only make configuration changes on the master unit, and changes are automatically synced to all other units in the cluster.

Firepower Threat Defense Features and Clustering

Some FTD features are not supported with clustering, and some are only supported on the master unit. Other features might have caveats for proper usage.
Unsupported Features with Clustering

These features cannot be configured with clustering enabled, and the commands will be rejected.

- Remote access VPN (SSL VPN and IPsec VPN)
- DHCP client, server, and proxy. DHCP relay is supported.
- High Availability
- Integrated Routing and Bridging
- Dead Connection Detection (DCD)

Centralized Features for Clustering

The following features are only supported on the master unit, and are not scaled for the cluster.

Note
Traffic for centralized features is forwarded from member units to the master unit over the cluster control link.

If you use the rebalancing feature, traffic for centralized features may be rebalanced to non-master units before the traffic is classified as a centralized feature; if this occurs, the traffic is then sent back to the master unit.

For centralized features, if the master unit fails, all connections are dropped, and you have to re-establish the connections on the new master unit.

- The following application inspections:
  - DCERPC
  - NetBIOS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- Dynamic routing
- Static route monitoring

Dynamic Routing and Clustering

The routing process only runs on the master unit, and routes are learned through the master unit and replicated to secondaries. If a routing packet arrives at a slave, it is redirected to the master unit.
After the slave members learn the routes from the master unit, each unit makes forwarding decisions independently.

The OSPF LSA database is not synchronized from the master unit to slave units. If there is a master unit switchover, the neighboring router will detect a restart; the switchover is not transparent. The OSPF process picks an IP address as its router ID. Although not required, you can assign a static router ID to ensure a consistent router ID is used across the cluster. See the OSPF Non-Stop Forwarding feature to address the interruption.

NAT and Clustering

NAT can affect the overall throughput of the cluster. Inbound and outbound NAT packets can be sent to different Firepower Threat Defense devices in the cluster, because the load balancing algorithm relies on IP addresses and ports, and NAT causes inbound and outbound packets to have different IP addresses and/or ports. When a packet arrives at the Firepower Threat Defense device that is not the NAT owner, it is forwarded over the cluster control link to the owner, causing large amounts of traffic on the cluster control link. Note that the receiving unit does not create a forwarding flow to the owner, because the NAT owner may not end up creating a connection for the packet depending on the results of security and policy checks.

If you still want to use NAT in clustering, then consider the following guidelines:

- NAT pool address distribution for dynamic PAT—The master unit evenly pre-distributes addresses across the cluster. If a member receives a connection and they have no addresses left, then the connection is dropped even if other members still have addresses available. Make sure to include at least as many NAT addresses as there are units in the cluster to ensure that each unit receives an address.

- No round-robin—Round-robin for a PAT pool is not supported with clustering.

- Dynamic NAT xlates managed by the master unit—The master unit maintains and replicates the xlate table to slave units. When a slave unit receives a connection that requires dynamic NAT, and the xlate is not in the table, it requests the xlate from the master unit. The slave unit owns the connection.

- No static PAT for the following inspections—
  - FTP
  - RSH
  - SQLNET
• TFTP
• XDMCP
• SIP

SIP Inspection and Clustering

A control flow can be created on any unit (due to load balancing); its child data flows must reside on the same unit.

Syslog and Clustering

• Each unit in the cluster generates its own syslog messages. You can configure logging so that each unit uses either the same or a different device ID in the syslog message header field. For example, the hostname configuration is replicated and shared by all units in the cluster. If you configure logging to use the hostname as the device ID, syslog messages generated by all units look as if they come from a single unit. If you configure logging to use the local-unit name that is assigned in the cluster bootstrap configuration as the device ID, syslog messages look as if they come from different units.

SNMP and Clustering

An SNMP agent polls each individual Firepower Threat Defense device by its Diagnostic interface Local IP address. You cannot poll consolidated data for the cluster.

You should always use the Local address, and not the Main cluster IP address for SNMP polling. If the SNMP agent polls the Main cluster IP address, if a new master is elected, the poll to the new master unit will fail.

FTP and Clustering

• If FTP data channel and control channel flows are owned by different cluster members, then the data channel owner will periodically send idle timeout updates to the control channel owner and update the idle timeout value. However, if the control flow owner is reloaded, and the control flow is re-hosted, the parent/child flow relationship will not longer be maintained; the control flow idle timeout will not be updated.

Cisco TrustSec and Clustering

Only the master unit learns security group tag (SGT) information. The master unit then populates the SGT to slaves, and slaves can make a match decision for SGT based on the security policy.

VPN and Clustering

Site-to-site VPN is a centralized feature; only the master unit supports VPN connections.

Note

Remote access VPN is not supported with clustering.
VPN functionality is limited to the master unit and does not take advantage of the cluster high availability capabilities. If the master unit fails, all existing VPN connections are lost, and VPN users will see a disruption in service. When a new master is elected, you must reestablish the VPN connections.

When you connect a VPN tunnel to a Spanned interface address, connections are automatically forwarded to the master unit.

VPN-related keys and certificates are replicated to all units.

**Licenses for Clustering**

The FTD uses Smart Licensing. You assign licenses to the cluster as a whole, not to individual units. However, each unit of the cluster consumes a separate license for each feature.

When you add a cluster member to the FMC, you can specify the feature licenses you want to use for the cluster. You can modify licenses for the cluster in the Devices > Device Management > Cluster > License area.

---

**Note**

If you add the cluster before the FMC is licensed (and running in Evaluation mode), then when you license the FMC, you can experience traffic disruption when you deploy policy changes to the cluster. Changing to licensed mode causes all slave units to leave the cluster and then rejoin.

---

**Requirements and Prerequisites for Clustering**

**Cluster Model Support**

- Firepower 9300—You can include up to 6 units in the cluster in up to 6 chassis. Supports intra-chassis and inter-chassis clustering.
- Firepower 4100 series—Supported for up to 6 units using inter-chassis clustering.

**Inter-Chassis Clustering Hardware and Software Requirements**

All chassis in a cluster:

- For the Firepower 4100 series: All chassis must be the same model. For the Firepower 9300: All security modules 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.

- Must run the identical FXOS software except at the time of an image upgrade.

- Must include the same interface configuration for interfaces you assign to the cluster, such as the same Management interface, EtherChannels, active interfaces, speed and duplex, and so on. You can use different network module types on the chassis as long as the capacity matches for the same interface IDs and interfaces can successfully bundle in the same spanned EtherChannel. Note that all data interfaces must be EtherChannels in inter-chassis clustering. If you change the interfaces in FXOS after you enable clustering (by adding or removing interface modules, or configuring EtherChannels, for example), then perform the same changes on each chassis, starting with the slave units, and ending with the master.
• Must use the same NTP server. For Firepower Threat Defense, the Firepower Management Center must also use the same NTP server. Do not set the time manually.

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 4100/9300 chassis.

• For a list of supported switches, see Cisco FXOS Compatibility.

Clustering Guidelines and Limitations

Switches for Inter-Chassis Clustering

• For the ASR 9006, if you want to set a non-default MTU, set the ASR interface MTU to be 14 bytes higher than the cluster device MTU. Otherwise, OSPF adjacency peering attempts may fail unless the "mtu-ignore" option is used. Note that the cluster device MTU should match the ASR IPv4 MTU.

• On the switch(es) for the cluster control link interfaces, you can optionally enable Spanning Tree PortFast on the switch ports connected to the cluster unit to speed up the join process for new units.

• When you see slow bundling of a Spanned EtherChannel on the switch, you can enable LACP rate fast for an individual interface on the switch. Note that some switches, such as the Nexus series, do not support LACP rate fast when performing in-service software upgrades (ISSUs), so we do not recommend using ISSUs with clustering.

• On the switch, we recommend that you use one of the following EtherChannel load-balancing algorithms: "source-dest-ip" or "source-dest-ip-port" (see the Cisco Nexus OS and Cisco IOS "port-channel load-balance" command). Do not use a "vlan" keyword in the load-balance algorithm because it can cause unevenly distributed traffic to the devices in a cluster.

• If you change the load-balancing algorithm of the EtherChannel on the switch, the EtherChannel interface on the switch temporarily stops forwarding traffic, and the Spanning Tree Protocol restarts. There will be a delay before traffic starts flowing again.

• Some switches do not support dynamic port priority with LACP (active and standby links). You can disable dynamic port priority to provide better compatibility with Spanned EtherChannels.

• Switches on the cluster control link path should not verify the L4 checksum. Redirected traffic over the cluster control link does not have a correct L4 checksum. Switches that verify the L4 checksum could cause traffic to be dropped.

• Port-channel bundling downtime should not exceed the configured keepalive interval.

• On Supervisor 2T EtherChannels, the default hash distribution algorithm is adaptive. To avoid asymmetric traffic in a VSS design, change the hash algorithm on the port-channel connected to the cluster device to fixed:

  router(config)# port-channel id hash-distribution fixed

  Do not change the algorithm globally; you may want to take advantage of the adaptive algorithm for the VSS peer link.
EtherChannels for Inter-Chassis Clustering

- For connecting switches, set the EtherChannel mode to Active; On mode is not supported on the Firepower 4100/9300 chassis, even for the cluster control link.

- FXOS EtherChannels have the LACP rate set to fast by default. Some switches, such as the Nexus series, do not support LACP rate fast when performing in-service software upgrades (ISSUs), so we do not recommend using ISSUs with clustering.

- In Catalyst 3750-X Cisco IOS software versions earlier than 15.1(1)S2, the cluster unit did not support connecting an EtherChannel to a switch stack. With default switch settings, if the cluster unit EtherChannel is connected cross stack, and if the master switch is powered down, then the EtherChannel connected to the remaining switch will not come up. To improve compatibility, set the stack-mac persistent timer command to a large enough value to account for reload time; for example, 8 minutes or 0 for indefinite. Or, you can upgrade to more a more stable switch software version, such as 15.1(1)S2.

- Spanned vs. Device-Local EtherChannel Configuration—Be sure to configure the switch appropriately for Spanned EtherChannels vs. Device-local EtherChannels.
  
  - Spanned EtherChannels—For cluster unit Spanned EtherChannels, which span across all members of the cluster, the interfaces are combined into a single EtherChannel on the switch. Make sure each interface is in the same channel group on the switch.
Device-local EtherChannels—For cluster unit Device-local EtherChannels including any EtherChannels configured for the cluster control link, be sure to configure discrete EtherChannels on the switch; do not combine multiple cluster unit EtherChannels into one EtherChannel on the switch.

Additional Guidelines

- 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.
- The cluster auto-rejoin feature for a failed cluster control link is set to unlimited attempts every 5 minutes.
- The cluster auto-rejoin feature for a failed data interface is set to 3 attempts every 5 minutes, with the increasing interval set to 2.
- Connection replication delay of 5 seconds is enabled by default for HTTP traffic.

**Configure Clustering**

You can easily deploy the cluster from the Firepower 4100/9300 chassis supervisor. All initial configuration is automatically generated for each unit. You can then add the units to the FMC and group them into a cluster.

**FXOS: Add a Firepower Threat Defense Cluster**

You can add a single Firepower 9300 chassis as an intra-chassis cluster, or add multiple chassis for inter-chassis clustering. For inter-chassis clustering, you must configure each chassis separately. Add the cluster on one chassis; you can then copy the bootstrap configuration from the first chassis to the next chassis for ease of deployment.

**Create a Firepower Threat Defense Cluster**

You can easily deploy the cluster from the Firepower 4100/9300 chassis supervisor. All initial configuration is automatically generated for each unit.

For inter-chassis clustering, you must configure each chassis separately. Deploy the cluster on one chassis; you can then copy the bootstrap configuration from the first chassis to the next chassis for ease of deployment.

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.

**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 4100/9300 chassis.
- Gather the following information:
  - Management interface ID, IP addresses, and network mask
  - Gateway IP address
  - FMC IP address and/or NAT ID of your choosing
  - DNS server IP address
  - FTD hostname and domain name
**Procedure**

**Step 1** Configure interfaces.

a) Add at least one Data type interface or EtherChannel (also known as a port-channel) before you deploy the cluster.

   For inter-chassis clustering, all data interfaces must be Spanned EtherChannels with at least one member interface. Add the same EtherChannels on each chassis. Combine the member interfaces from all cluster units into a single EtherChannel on the switch. See Clustering Guidelines and Limitations, on page 11 for more information about EtherChannels for inter-chassis clustering.

   All interfaces are assigned to the cluster by default. For inter-chassis clustering, only EtherChannels are assigned; you cannot assign other interface types. You can also add data interfaces to the cluster after you deploy it.

b) Add a Management type interface or EtherChannel.

   The management interface is required. Note that this management interface is not the same as the chassis management interface that is used only for chassis management (in FXOS, you might see the chassis management interface displayed as MGMT, management0, or other similar names).

   For inter-chassis clustering, add the same Management interface on each chassis.

c) For inter-chassis clustering, add a member interface to port-channel 48, which is used as the cluster control link.

   Do not add a member interface for intra-chassis clustering. If you add a member, the chassis assumes this cluster will be inter-chassis, and will only allow you to use Spanned EtherChannels, for example.

   On the Interfaces tab, the port-channel 48 cluster type interface shows the **Operation State** as **failed** if it does not include any member interfaces. For intra-chassis clustering, this EtherChannel does not require any member interfaces, and you can ignore this Operational State.

   Add the same member interfaces on each chassis. The cluster control link is a device-local EtherChannel on each chassis. Use separate EtherChannels on the switch per device. See Clustering Guidelines and Limitations, on page 11 for more information about EtherChannels for inter-chassis clustering.

d) (Optional) Add a Firepower-eventing interface.

   This interface is a secondary management interface for FTD devices. To use this interface, you must configure its IP address and other parameters at the FTD CLI. For example, you can separate management traffic from events (such as web events). See the **configure network** commands in the Firepower Threat Defense command reference.

   For inter-chassis clustering, add the same eventing interface on each chassis.

**Step 2** Choose **Logical Devices**.

**Step 3** Click **Add Device**, and set the following parameters:
a) **Provide a Device Name.**

   This name is used by the chassis supervisor to configure management settings and to assign interfaces; it
   is not the device name used in the application configuration.

b) For the **Template**, choose **Cisco Firepower Threat Defense**.

c) **Choose the Image Version**.

d) For the **Instance Type**, only the **Native** type is supported.

e) For the **Usage**, click the **Cluster** radio button.

f) Click the **Create New Cluster** radio button.

g) Click **OK**.

   You see the Provisioning - *device name* window. All interfaces are assigned to the cluster by default.

**Step 4**

Click the device icon in the center of the screen.

A dialog box appears where you can configure initial bootstrap settings. 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.

**Step 5**

On the **Cluster Information** page, complete the following.
a) For inter-chassis clustering, in the **Chassis ID** field, enter a chassis ID. Each chassis in the cluster must use a unique ID.

   This field only appears if you added a member interface to cluster control link Port-Channel 48.

b) For inter-site clustering, in the **Site ID** field, enter the site ID for this chassis between 1 and 8. This feature is only configurable using the Firepower Management Center FlexConfig feature.

c) In the **Cluster Key** field, configure an authentication key for control traffic on the cluster control link.

   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.

d) Set the **Cluster Group Name**, which is the cluster group name in the logical device configuration.

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

e) Choose the **Management Interface**.

   This interface is used to manage the logical device. This interface is separate from the chassis management port.

   If you assign a Hardware Bypass-capable interface as the Management interface, you see a warning message to make sure your assignment is intentional.
f) Set the **CCL Subnet IP** as `a.b.0.0`.

By default, the cluster control link uses the 127.2.0.0/16 network. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. In this case, specify any /16 network address on a unique network for the cluster, except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses. If you set the value to 0.0.0.0, then the default network is used.

The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: `a.b.chassis_id.slot_id`.

**Step 6** On the **Settings** page, complete the following.

![Cisco Firepower Threat Defense - Bootstrap Configuration](bootstrapconfiguration.png)

a) In the **Registration Key** field, enter the key to be shared between the Firepower Management Center and the cluster members during registration.

You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the FMC when you add the FTD.

b) Enter a **Password** for the FTD admin user for CLI access.

c) In the **Firepower Management Center IP** field, enter the IP address of the managing Firepower Management Center. If you do not know the FMC IP address, leave this field blank and enter a passphrase in the **Firepower Management Center NAT ID** field.

d) In the **Search Domains** field, enter a comma-separated list of search domains for the management network.
e) From the **Firewall Mode** drop-down list, choose **Transparent** or **Routed**.

In routed mode, the FTD is considered to be a router hop in the network. Each interface that you want to route between is on a different subnet. A transparent firewall, on the other hand, is a Layer 2 firewall that acts like a “bump in the wire,” or a “stealth firewall,” and is not seen as a router hop to connected devices.

The firewall mode is only set at initial deployment. If you re-apply the bootstrap settings, this setting is not used.

f) In the **DNS Servers** field, enter a comma-separated list of DNS servers.

The FTD uses DNS if you specify a hostname for the FMC, for example.

g) (Optional) In the **Firepower Management Center NAT ID** field, enter a passphrase that you will also enter on the FMC when you add the cluster as a new device.

Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the FMC specifies the device IP address, and the device specifies the FMC IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. You can specify any text string as the NAT ID, from 1 to 37 characters. The FMC and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

h) In the **Fully Qualified Hostname** field, enter a fully qualified name for the FTD device.

i) From the **Eventing Interface** drop-down list, choose the interface on which Firepower events should be sent. If not specified, the management interface will be used.

To specify a separate interface to use for Firepower events, you must configure an interface as a **firepower-eventing** interface. If you assign a Hardware Bypass-capable interface as the Eventing interface, you see a warning message to make sure your assignment is intentional.

**Step 7**

On the **Interface Information** page, configure a management IP address for each security module in the cluster. Select the type of address from the **Address Type** drop-down list and then complete the following for each security module.

**Note** You must set the IP address for all 3 module slots in a chassis, even if you do not have a module installed. If you do not configure all 3 modules, the cluster will not come up.
a) In the **Management IP** field, configure an IP address. Specify a unique IP address on the same network for each module.

b) Enter a **Network Mask** or **Prefix Length**.

c) Enter a **Network Gateway** address.

**Step 8**

On the **Agreement** tab, read and accept the end user license agreement (EULA).

**Step 9**

Click **OK** to close the configuration dialog box.

**Step 10**

Click **Save**.

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 **Logical Devices** page for the status of the new logical device. When the logical device shows its **Status** as **online**, you can start configuring the security policy in the application.
Step 11  
For inter-chassis clustering, add the next chassis to the cluster:

a) On the first chassis Firepower Chassis Manager, click the Show Configuration icon ( ) at the top right; copy the displayed cluster configuration.
b) Connect to the Firepower Chassis Manager on the next chassis, and add a logical device according to this procedure.
c) Choose Join an Existing Cluster.
d) Click the Copy config check box, and click OK. If you uncheck this check box, you must manually enter the settings to match the first chassis configuration.
e) In the Copy Cluster Details box, paste in the cluster configuration from the first chassis, and click OK.
f) Click the device icon in the center of the screen. The cluster information is mostly pre-filled, but you must change the following settings:
   • **Chassis ID**—Enter a unique chassis ID.
   • **Site ID**—For inter-site clustering, enter the site ID for this chassis between 1 and 8. This feature is only configurable using the Firepower Management Center FlexConfig feature.
   • **Cluster Key**—(Not prefilled) Enter the same cluster key.
   • **Management IP**—Change the management address for each module to be a unique IP address on the same network as the other cluster members.

   Click OK.

   g) Click Save.

Step 12  
Add the master unit to the Firepower Management Center using the management IP address.
All cluster units must be in a successfully-formed cluster on FXOS prior to adding them to Firepower Management Center.
The Firepower Management Center then automatically detects the slave units.

Add More Cluster Members  
Add or replace a FTD cluster member in an existing cluster.
The FXOS steps in this procedure only apply to adding a new chassis; if you are adding a new module to a Firepower 9300 where clustering is already enabled, the module will be added automatically. However, you must still add the new module to the Firepower Management Center; skip to the Firepower Management Center steps.

**Note**

Before you begin

- In the case of a replacement, you must delete the old cluster member from the Firepower Management Center. When you replace it with a new unit, it is considered to be a new device on the Firepower Management Center.
- The interface configuration must be the same on the new chassis. You can export and import FXOS chassis configuration to make this process easier.

**Procedure**

**Step 1** On an existing cluster chassis Firepower Chassis Manager, choose Logical Devices to open the Logical Devices page.

**Step 2** Click the Show Configuration icon ( ) at the top right; copy the displayed cluster configuration.

**Step 3** Connect to the Firepower Chassis Manager on the new chassis, and click Add Device.

**Step 4** For the Device Name, provide a name for the logical device.

**Step 5** For the Template, choose Cisco Firepower Threat Defense.

**Step 6** For the Image Version, choose the FTD software version.

**Step 7** For the Device Mode, click the Cluster radio button.

**Step 8** Choose Join an Existing Cluster.

**Step 9** Click the Copy config check box, and click OK. If you uncheck this check box, you must manually enter the settings to match the first chassis configuration.

**Step 10** In the Copy Cluster Details box, paste in the cluster configuration from the first chassis, and click OK.

**Step 11** Click the device icon in the center of the screen. The cluster information is mostly pre-filled, but you must change the following settings:

- **Chassis ID**—Enter a unique chassis ID.
- **Site ID**—For inter-site clustering, enter the site ID for this chassis between 1 and 8. This feature is only configurable using the Firepower Management Center FlexConfig feature.
- **Cluster Key**—(Not prefilled) Enter the same cluster key.
- **Management IP**—Change the management address for each module to be a unique IP address on the same network as the other cluster members.

Click OK.

**Step 12** Click Save.

**Step 13** In the Firepower Management Center, choose Devices > Device Management, and select the Add > Add Device to add the new logical device.
Step 14  Choose Add > Add Cluster.
Step 15  Choose the current Master device from the drop-down list.

When you choose a master device that is already in a cluster, then the existing cluster name is auto-filled, and all eligible slave devices are added to the Slave Devices box, including the new unit you just added to the FMC.

Step 16  Click Add, and then Deploy.
The cluster is updated to include the new member(s).

FMC: Add a Cluster

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>FTD on the F 4100 and 9300</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>

Add one of the cluster units as a new device to the Firepower Management Center; the FMC auto-detects all other cluster members.

Before you begin

- This method for adding a cluster requires Firepower Threat Defense Version 6.2 or later. If you need to manage an earlier version device, then refer to the Firepower Management Center configuration guide for that version.

- All cluster units must be in a successfully formed cluster on FXOS prior to adding the cluster to the Management Center. You should also check which unit is the master unit. Refer to the Firepower Chassis Manager Logical Devices screen or use the Firepower Threat Defense show cluster info command.

Procedure

Step 1  In the FMC, choose Devices > Device Management, and then choose Add > Add Device to add one of the cluster units using the management IP address you assigned when you deployed the cluster.

We recommend adding the master unit for the best performance, but you can add any unit.

The FMC identifies and registers the master unit, and then registers all slave units. If the master unit does not successfully register, then the cluster is not added. A registration failure can occur if the cluster was not up on the chassis, or because of other connectivity issues. In this case, we recommend that you try re-adding the cluster unit.

The cluster name shows on the Devices > Device Management page; expand the cluster to see the cluster units. A unit that is currently registering shows the loading icon. You can monitor cluster unit registration by clicking the system status icon and choosing the Tasks tab. The FMC updates the Cluster Registration task as each unit registers. If any units fail to register, see Reconcile Cluster Members, on page 29.
Step 2 Configure device-specific settings by clicking the edit icon (✎) for the cluster; you can only configure the cluster as a whole, and not member units in the cluster.

Step 3 On the Devices > Device Management > Cluster tab, you see General, License, System, and Health settings.

- In the General area, view cluster status by clicking the Current Cluster Summary link to open the Cluster Status dialog box. The Cluster Status dialog box also lets you retry slave registration by clicking Reconcile.

- In the License area, click the edit icon (✎) to set license entitlements.

Step 4 On the Devices > Device Management > Devices tab, you can choose each member in the cluster from the top right drop-down menu.

If you change the management IP address in the device configuration, you must match the new address in the FMC so that it can reach the device on the network; edit the Host address in the Management area.

---

**FMC: Configure Data and Diagnostic Interfaces**

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat Defense on the Firepower 4100 and 9300</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>

This procedure configures basic parameters for each data interface that you assigned to the cluster when you deployed it in FXOS. For inter-chassis clustering, data interfaces are always Spanned EtherChannel interfaces. You can also configure the Diagnostic interface, which is the only interface that can run as an individual interface.

**Note** When using Spanned EtherChannels for inter-chassis clustering, the port-channel interface will not come up until clustering is fully enabled. This requirement prevents traffic from being forwarded to a unit that is not an active unit in the cluster.

---

**Procedure**

Step 1 Choose Devices > Device Management, and click the edit icon (✎) next to the cluster.

Step 2 Click the Interfaces tab.

Step 3 (Optional) Configure VLAN subinterfaces on the interface. The rest of this procedure applies to the subinterfaces.

Step 4 Click the edit icon (✎) for the data interface.

Step 5 For inter-chassis clusters, set a manual global MAC address for the EtherChannel.

You must configure a MAC address for a Spanned EtherChannel to avoid potential network connectivity problems. With a manually-configured MAC address, the MAC address stays with the current master unit. If
you do not configure a MAC address, then if the master unit changes, the new master unit uses a new MAC address for the interface, which can cause a temporary network outage.

a) Click the Advanced tab. The Information tab is selected.

b) In the Active MAC Address field, enter a MAC address 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. The MAC address must not have the multicast bit set, that is, the second hexadecimal digit from the left cannot be an odd number.

Do not set the Standby MAC Address; it is ignored.

Step 6 Configure the name, IP address, and other parameters.

Step 7 Click OK. Repeat the above steps for other data interfaces.

Step 8 (Optional) Configure the Diagnostic interface.

The Diagnostic interface is the only interface that can run in Individual interface mode. You can use this interface for syslog messages or SNMP, for example.

a) Choose Objects > Object Management > Address Pools to add an IPv4 and/or IPv6 address pool.

Include at least as many addresses as there are units in the cluster. The Virtual IP address is not a part of this pool, but needs to be on the same network. You cannot determine the exact Local address assigned to each unit in advance.

b) On Devices > Device Management > Interfaces, click the edit icon (EDIT) for the Diagnostic interface.

c) On the IPv4 tab, enter the Virtual IP Address and mask. This IP address is a fixed address for the cluster, and always belongs to the current master unit.

d) From the IPv4 Address Pool drop-down list, choose the address pool you created.

e) On the IPv6 > Basic tab, from the IPv6 Address Pool drop-down list, choose the address pool you created.

f) Configure other interface settings as normal.

Step 9 Click Save.

You can now click Deploy and deploy the policy to assigned devices. The changes are not active until you deploy them.

---

**FXOS: Remove a Cluster Member**

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

**Temporary Removal**

A cluster member 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 on the Firepower Chassis Manager Logical Devices page:
For FTD using FMC, you should leave the device in the FMC device list so that it can resume full functionality after you reenable clustering.

- 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 master unit, so you can later re-add the unit without losing your configuration. If you enter this command on a slave unit to remove the master unit, a new master 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 FTD enter `cluster enable`.

- Disable the application instance—In Firepower Chassis Manager on the Logical Devices page, click the Disable slider (). You can later reenable it using the Enable slider ()

- Shut down the security module/engine—In Firepower Chassis Manager on the Security Module/Engine page, click the Power off icon ().

- Shut down the chassis—In Firepower Chassis Manager on the Overview page, click the Shut down icon ().

### Permanent Removal

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

For FTD using FMC, be sure to remove the unit from the FMC device list after you disable clustering on the chassis.

- Delete the logical device—In Firepower Chassis Manager on the Logical Devices page, click the delete icon (). You can then deploy a standalone logical device, a new cluster, or even add a new logical device to the same cluster.

- 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.
FMC: Manage Cluster Members

After you deploy the cluster, you can change the configuration and manage cluster members.

Add a New Cluster Member

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat Defense on the Firepower 4100 and 9300</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>

When you add a new cluster member in FXOS, the Firepower Management Center adds the member automatically.

Before you begin

- Make sure the interface configuration is the same on the replacement unit as for the other chassis.

Procedure

Step 1

Add the new unit to the cluster in FXOS. See the FXOS configuration guide.
Wait for the new unit to be added to the cluster. Refer to the Firepower Chassis Manager Logical Devices screen or use the Firepower Threat Defense show cluster info command to view cluster status.

Step 2

The new cluster member is added automatically. To monitor the registration of the replacement unit, view the following:

- Cluster Status dialog box (Devices > Device Management > Cluster tab > General area > Current Cluster Summary link)—A unit that is joining the cluster on the chassis shows "Joining cluster..." After it joins the cluster, the FMC attempts to register it, and the status changes to "Available for Registration". After it completes registration, the status changes to "In Sync." If the registration fails, the unit will stay at "Available for Registration". In this case, force a re-registration by clicking Reconcile.

- System status icon > Tasks tab—The FMC shows all registration events and failures.

- Devices > Device Management—When you expand the cluster on the devices listing page, you can see when a unit is registering when it has the loading icon to the left.

Replace a Cluster Member

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>FTD on the Firepower 4100 and 9300</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>
You can replace a cluster member in an existing cluster. The Firepower Management Center auto-detects the replacement unit. However, you must manually delete the old cluster member in the Firepower Management Center. This procedure also applies to a unit that was reinitialized; in this case, although the hardware remains the same, it appears to be a new member.

**Before you begin**
- Make sure the interface configuration is the same on the replacement unit as for other chassis.

**Procedure**

**Step 1**
For a new chassis, if possible, backup and restore the configuration from the old chassis in FXOS.

If you are replacing a module in a Firepower 9300, you do not need to perform these steps.

If you do not have a backup FXOS configuration from the old chassis, first perform the steps in Add a New Cluster Member, on page 27.

For information about all of the below steps, see the FXOS configuration guide.

a) Use the configuration export feature to export an XML file containing logical device and platform configuration settings for your Firepower 4100/9300 chassis.
b) Import the configuration file to the replacement chassis.
c) Accept the license agreement.
d) If necessary, upgrade the logical device application instance version to match the rest of the cluster.

**Step 2**
In the Firepower Management Center, choose **Devices > Device Management**, and click the delete icon ( unlink ) next to the old unit.

**Step 3**
Confirm that you want to delete the unit.
The unit is removed from the cluster and from the FMC devices list.

**Step 4**
The new or reinitialized cluster member is added automatically. To monitor the registration of the replacement unit, view the following:

- **Cluster Status** dialog box ( Devices > Device Management > Cluster tab > General area > Current Cluster Summary link )—A unit that is joining the cluster on the chassis shows "Joining cluster..." After it joins the cluster, the FMC attempts to register it, and the status changes to "Available for Registration". After it completes registration, the status changes to "In Sync." If the registration fails, the unit will stay at "Available for Registration". In this case, force a re-registration by clicking **Reconcile**.

- System status icon > **Tasks** tab—The FMC shows all registration events and failures.

- **Devices > Device Management**—When you expand the cluster on the devices listing page, you can see when a unit is registering when it has the loading icon to the left.
Delete a Slave Member

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>FTD on the</td>
<td>Any</td>
<td>Access Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firepower 4100</td>
<td></td>
<td>Administrator Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and 9300</td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

If you need to permanently remove a cluster member (for example, if you remove a module on the Firepower 9300, or remove a chassis), then you should delete it from the FMC.

Before you begin

Do not delete the member if it is still a healthy part of the cluster, or if you only want to disable the member temporarily. To delete it permanently from the cluster in FXOS, see FXOS: Remove a Cluster Member, on page 25. If you remove it from the FMC, and it is still part of the cluster, it will continue to pass traffic, and could even become the master unit—a master unit that the FMC can no longer manage.

Procedure

Step 1

Make sure the unit is ready to be deleted from the FMC.

a) Choose Devices > Device Management, and click the edit icon (📝) for the cluster.
b) On the Devices > Device Management > Cluster tab > General area, click the Current Cluster Summary link to open the Cluster Status dialog box.
c) Ensure that the devices you want to delete are in the "Available for Deletion" state.

If the status is stale, click Reconcile to force an update.

Step 2

In the FMC, choose Devices > Device Management, and click the delete icon (ลบ) next to the slave unit.

Step 3

Confirm that you want to delete the unit.

The unit is removed from the cluster and from the FMC devices list.

Reconcile Cluster Members

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat</td>
<td>Any</td>
<td>Access Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defense on the</td>
<td></td>
<td>Administrator Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firepower 4100</td>
<td></td>
<td>Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and 9300</td>
<td></td>
<td>Admin</td>
</tr>
</tbody>
</table>

If a cluster member fails to register, you can reconcile the cluster membership from the chassis to the Firepower Management Center. For example, a slave unit might fail to register if the FMC is occupied with certain processes, or if there is a network issue.
Procedure

Step 1  Choose Devices > Device Management, and click the edit icon (edit) for the cluster.

Step 2  On the Cluster tab > General area, click the Current Cluster Summary link to open the Cluster Status dialog box.

Step 3  Click Reconcile.

For more information about the cluster status, see FMC: Monitoring the Cluster, on page 31.

Deactivate a Member

To deactivate a member other than the unit you are logged into, perform the following steps at the FTD CLI. This procedure is meant to temporarily deactivate a member, and you should keep the unit in the FMC device list.

When a unit becomes inactive, all data interfaces are shut down; only the Management interface can send and receive traffic. To resume traffic flow, reenable 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. You must use the console for any further configuration.

Procedure

Step 1  Access the FTD CLI.

Step 2  Remove the unit from the cluster:

```
cluster remove unit unit_name
```

The bootstrap configuration remains intact, as well as the last configuration synched from the master unit, so that you can later re-add the unit without losing your configuration. If you enter this command on a slave unit to remove the master unit, a new master unit is elected.

To view member names, enter `cluster remove unit ?`, or enter the `show cluster info` command.

Example:

```
> cluster remove unit ?
Current active units in the cluster:
ftd1
ftd2
ftd3

> cluster remove unit ftd2
WARNING: Clustering will be disabled on unit ftd2. To bring it back to the cluster please logon to that unit and re-enable clustering
```
Step 3  To reenable clustering, see Rejoin the Cluster, on page 31.

Rejoin the Cluster

<table>
<thead>
<tr>
<th>Smart License</th>
<th>Classic License</th>
<th>Supported Devices</th>
<th>Supported Domains</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>N/A</td>
<td>Firepower Threat Defense on the Firepower 4100 and 9300</td>
<td>Any</td>
<td>Access Admin Administrator Network Admin</td>
</tr>
</tbody>
</table>

If a unit was removed from the cluster, for example for a failed interface, you must manually rejoin the cluster by accessing the unit CLI. Make sure the failure is resolved before you try to rejoin the cluster. See Rejoining the Cluster, on page 34 for more information about why a unit can be removed from a cluster.

Procedure

Step 1  Access the CLI of the unit that needs to rejoin the cluster, either from the console port or using SSH to the Management interface. Log in with the username admin and the password you set during initial setup.

Step 2  Enable clustering:

    cluster enable

FMC: Monitoring the Cluster

You can monitor the cluster in Firepower Management Center and at the FTD CLI.

- Devices > Device Management > Cluster tab > General area > Current Cluster Summary link > Cluster Status dialog box.

Cluster member states include:

- In Sync.—The unit is registered with the FMC.
- Available for Registration—The unit is part of the cluster, but has not yet registered with the FMC. If a unit fails to register, you can retry registration by clicking Reconcile.
- Available for Deletion—The unit is registered with the FMC, but is no longer part of the cluster and should be deleted.
- Joining cluster...—The unit is joining the cluster on the chassis, but has not completed joining. After it joins, it will register with the FMC.

To refresh this dialog box, close and reopen it.

- System status icon > Tasks tab.

The Tasks tab shows updates of the Cluster Registration task as each unit registers.
• **Devices > Device Management** > _cluster_name_.

When you expand the cluster on the devices listing page, you can see all member units, including the master unit shown with "(master)" next to the IP address. For units that are still registering, you can see the loading icon.

**show cluster** {access-list [acl_name] | conn [count] | cpu [usage] | history | interface-mode | memory | resource usage | service-policy | traffic | xlate count}

To view aggregated data for the entire cluster or other information, use the `show cluster` command.

**show cluster info** [auto-join | clients | conn-distribution | flow-mobility counters | goid [options] | health | incompatible-config | loadbalance | old-members | packet-distribution | trace [options] | transport { asp | cp}]

To view cluster information, use the `show cluster info` command.

---

**Reference for Clustering**

This section includes more information about how clustering operates.

**Performance Scaling Factor**

When you combine multiple units into a cluster, you can expect the total cluster performance to be approximately:

- 80% of the combined TCP or CPS throughput
- 90% of the combined UDP throughput
- 60% of the combined Ethernet MIX (EMIX) throughput, depending on the traffic mix.

For example, for TCP throughput, the Firepower 9300 with 3 modules can handle approximately 135 Gbps of real world firewall traffic when running alone. For 2 chassis, the maximum combined throughput will be approximately 80% of 270 Gbps (2 chassis x 135 Gbps): 216 Gbps.

**Master Unit Election**

Members of the cluster communicate over the cluster control link to elect a master unit as follows:

1. When you deploy the cluster, each unit broadcasts an election request every 3 seconds.
2. Any other units with a higher priority respond to the election request; the priority is set when you deploy the cluster and is not configurable.
3. If after 45 seconds, a unit does not receive a response from another unit with a higher priority, then it becomes master.
4. If a unit later joins the cluster with a higher priority, it does not automatically become the master unit; the existing master unit always remains as the master unless it stops responding, at which point a new master unit is elected.
You can manually force a unit to become the master. For centralized features, if you force a master unit change, then all connections are dropped, and you have to re-establish the connections on the new master unit.

**High Availability Within the Cluster**

Clustering provides high availability by monitoring chassis, unit, and interface health and by replicating connection states between units.

**Chassis-Application Monitoring**

Chassis-application health monitoring is always enabled. The Firepower 4100/9300 chassis supervisor checks the Firepower Threat Defense application periodically (every second). If the Firepower Threat Defense device is up and cannot communicate with the Firepower 4100/9300 chassis supervisor for 3 seconds, the Firepower Threat Defense device generates a syslog message and leaves the cluster.

If the Firepower 4100/9300 chassis supervisor cannot communicate with the application after 45 seconds, it reloads the Firepower Threat Defense device. If the Firepower Threat Defense device cannot communicate with the supervisor, it removes itself from the cluster.

**Unit Health Monitoring**

The master unit monitors every slave unit by sending keepalive messages over the cluster control link periodically. Each slave unit monitors the master unit using the same mechanism. If the unit health check fails, the unit is removed from the cluster.

**Interface Monitoring**

Each unit monitors the link status of all hardware interfaces in use, and reports status changes to the master unit. For inter-chassis clustering, Spanned EtherChannels use the cluster Link Aggregation Control Protocol (cLACP). Each chassis monitors the link status and the cLACP protocol messages to determine if the port is still active in the EtherChannel, and informs the Firepower Threat Defense application if the interface is down. When you enable health monitoring, all physical interfaces are monitored by default (including the main EtherChannel for EtherChannel interfaces). Only named interfaces that are in an Up state can be monitored. For example, all member ports of an EtherChannel must fail before a named EtherChannel is removed from the cluster.

If a monitored interface fails on a particular unit, but it is active on other units, then the unit is removed from the cluster. The amount of time before the Firepower Threat Defense device removes a member from the cluster depends on whether the unit is an established member or is joining the cluster. The Firepower Threat Defense device does not monitor interfaces for the first 90 seconds that a unit joins the cluster. Interface status changes during this time will not cause the Firepower Threat Defense device to be removed from the cluster. For an established member, the unit is removed after 500 ms.

For inter-chassis clustering, if you add or delete an EtherChannel from the cluster, interface health-monitoring is suspended for 95 seconds to ensure that you have time to make the changes on each chassis.

**Status After Failure**

When a unit in the cluster fails, the connections hosted by that unit are seamlessly transferred to other units; state information for traffic flows is shared over the control cluster link.
If the master unit fails, then another member of the cluster with the highest priority (lowest number) becomes the master unit.

The Firepower Threat Defense device automatically tries to rejoin the cluster, depending on the failure event.

---

**Note**

When the Firepower Threat Defense device becomes inactive and fails to automatically rejoin the cluster, all data interfaces are shut down; only the Management/Diagnostic interface can send and receive traffic.

---

### Rejoining the Cluster

After a cluster member is removed from the cluster, how it can rejoin the cluster depends on why it was removed:

- **Failed cluster control link**—After you resolve the problem with the cluster control link, you must manually rejoin the cluster by re-enabling clustering.

- **Failed data interface**—The FTD application automatically tries to rejoin at 5 minutes, then at 10 minutes, and finally at 20 minutes. If the join is not successful after 20 minutes, then the FTD application disables clustering. After you resolve the problem with the data interface, you have to manually enable clustering.

- **Failed unit**—If the unit was removed from the cluster because of a unit health check failure, then rejoining the cluster depends on the source of the failure. For example, a temporary power failure means the unit will rejoin the cluster when it starts up again as long as the cluster control link is up. The FTD application attempts to rejoin the cluster every 5 seconds.

- **Failed Chassis-Application Communication**—When the FTD application detects that the chassis-application health has recovered, it tries to rejoin the cluster automatically.

- **Internal error**—Internal failures include: application sync timeout; inconsistent application statuses; and so on.

### Data Path Connection State Replication

Every connection has one owner and at least one backup owner in the cluster. The backup owner does not take over the connection in the event of a failure; instead, it stores TCP/UDP state information, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner is usually also the director.

Some traffic requires state information above the TCP or UDP layer. See the following table for clustering support or lack of support for this kind of traffic.

<table>
<thead>
<tr>
<th>Traffic</th>
<th>State Support</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up time</td>
<td>Yes</td>
<td>Keeps track of the system up time.</td>
</tr>
<tr>
<td>ARP Table</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>MAC address table</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>User Identity</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>IPv6 Neighbor database</td>
<td>Yes</td>
<td>—</td>
</tr>
</tbody>
</table>
How the Cluster Manages Connections

Connections can be load-balanced to multiple members of the cluster. Connection roles determine how connections are handled in both normal operation and in a high availability situation.

Connection Roles

See the following roles defined for each connection:

- **Owner**—Usually, the unit that initially receives the connection. The owner maintains the TCP state and processes packets. A connection has only one owner. If the original owner fails, then when new units receive packets from the connection, the director chooses a new owner from those units.

- **Backup owner**—The unit that stores TCP/UDP state information received from the owner, so that the connection can be seamlessly transferred to a new owner in case of a failure. The backup owner does not take over the connection in the event of a failure. If the owner becomes unavailable, then the first unit to receive packets from the connection (based on load balancing) contacts the backup owner for the relevant state information so it can become the new owner.

    As long as the director (see below) is not the same unit as the owner, then the director is also the backup owner. If the owner chooses itself as the director, then a separate backup owner is chosen.

- **Director**—The unit that handles owner lookup requests from forwarders. When the owner receives a new connection, it chooses a director based on a hash of the source/destination IP address and ports, and sends a message to the director to register the new connection. If packets arrive at any unit other than the owner, the unit queries the director about which unit is the owner so it can forward the packets. A connection has only one director. If a director fails, the owner chooses a new director.

    As long as the director is not the same unit as the owner, then the director is also the backup owner (see above). If the owner chooses itself as the director, then a separate backup owner is chosen.

- **Forwarder**—A unit that forwards packets to the owner. If a forwarder receives a packet for a connection it does not own, it queries the director for the owner, and then establishes a flow to the owner for any other packets it receives for this connection. The director can also be a forwarder. Note that if a forwarder receives the SYN-ACK packet, it can derive the owner directly from a SYN cookie in the packet, so it does not need to query the director. (If you disable TCP sequence randomization, the SYN cookie is not used; a query to the director is required.) For short-lived flows such as DNS and ICMP, instead of querying, the forwarder immediately sends the packet to the director, which then sends them to the owner. A connection can have multiple forwarders; the most efficient throughput is achieved by a good load-balancing method where there are no forwarders and all packets of a connection are received by the owner.
New Connection Ownership

When a new connection is directed to a member of the cluster via load balancing, that unit owns both directions of the connection. If any connection packets arrive at a different unit, they are forwarded to the owner unit over the cluster control link. If a reverse flow arrives at a different unit, it is redirected back to the original unit.

Sample Data Flow

The following example shows the establishment of a new connection.

1. The SYN packet originates from the client and is delivered to one Firepower Threat Defense device (based on the load balancing method), which becomes the owner. The owner creates a flow, encodes owner information into a SYN cookie, and forwards the packet to the server.

2. The SYN-ACK packet originates from the server and is delivered to a different Firepower Threat Defense device (based on the load balancing method). This Firepower Threat Defense device is the forwarder.

3. Because the forwarder does not own the connection, it decodes owner information from the SYN cookie, creates a forwarding flow to the owner, and forwards the SYN-ACK to the owner.

4. The owner sends a state update to the director, and forwards the SYN-ACK to the client.

5. The director receives the state update from the owner, creates a flow to the owner, and records the TCP state information as well as the owner. The director acts as the backup owner for the connection.

6. Any subsequent packets delivered to the forwarder will be forwarded to the owner.

7. If packets are delivered to any additional units, it will query the director for the owner and establish a flow.

8. Any state change for the flow results in a state update from the owner to the director.
## History for Clustering

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
</table>
| Improved Firepower Threat Defense cluster addition to the Firepower Management Center | 6.3.0   | You can now add any unit of a cluster to the Firepower Management Center, and the other cluster units are detected automatically. Formerly, you had to add each cluster unit as a separate device, and then group them into a cluster in the Management Center. Adding a cluster unit is also now automatic. Note that you must delete a unit manually. New/Modified screens:  
Devices > Device Management > Add drop-down menu > Device > Add Device dialog box  
Devices > Device Management > Cluster tab > General area > Cluster Registration Status > Current Cluster Summary link > Cluster Status dialog box  
Supported platforms: Firepower 4100/9300                                                                                          |
| Support for Site-to-Site VPN with clustering as a centralized feature    | 6.2.3.3 | You can now configure site-to-site VPN with clustering. Site-to-site VPN is a centralized feature; only the master unit supports VPN connections.  
Supported platforms: Firepower 4100/9300                                                                                          |
| Automatically rejoin the cluster after an internal failure               | 6.2.3   | Formerly, many internal error conditions caused a cluster unit to be removed from the cluster, and you were required to manually rejoin the cluster after resolving the issue. Now, a unit will attempt to rejoin the cluster automatically at the following intervals: 5 minutes, 10 minutes, and then 20 minutes. Internal failures include: application sync timeout; inconsistent application statuses; and so on.  
New/Modified command: `show cluster info auto-join`  
No modified screens.  
Supported platforms: Firepower Threat Defense on the Firepower 4100/9300                                                                 |
With FXOS 2.1.1, you can now enable inter-chassis clustering on the Firepower 9300 and 4100. You can include up to 6 units in up to 6 chassis.

**Note**  Inter-site clustering is now supported using FlexConfig only.

No modified screens.

Supported platforms: Firepower Threat Defense on the Firepower 4100/9300

### Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inter-chassis clustering for 6 modules; Firepower 4100 support</td>
<td>6.2.0</td>
<td>With FXOS 2.1.1, you can now enable inter-chassis clustering on the Firepower 9300 and 4100. You can include up to 6 units in up to 6 chassis. <strong>Note</strong> Inter-site clustering is now supported using FlexConfig only. No modified screens. Supported platforms: Firepower Threat Defense on the Firepower 4100/9300</td>
</tr>
<tr>
<td>Intra-chassis Clustering for the Firepower 9300</td>
<td>6.0.1</td>
<td>You can cluster up to 3 security modules within the Firepower 9300 chassis. All modules in the chassis must belong to the cluster. New/Modified screens: Devices &gt; Device Management &gt; Add &gt; Add Cluster Devices &gt; Device Management &gt; Cluster Supported platforms: Firepower Threat Defense on the Firepower 9300</td>
</tr>
</tbody>
</table>