Logical Devices on the Firepower 4100/9300

The Firepower 4100/9300 is a flexible security platform on which you can install one or more *logical devices*.

You must configure chassis interfaces, add a logical device, and assign interfaces to the device on the Firepower 4100/9300 chassis using the Firepower Chassis Manager or the FXOS CLI. You cannot perform these tasks in the FDM.

This chapter describes basic interface configuration and how to add a standalone or High Availability logical device using the Firepower Chassis Manager. To use the FXOS CLI, see the FXOS CLI configuration guide. For more advanced FXOS procedures and troubleshooting, see the FXOS configuration guide.

About Interfaces

The Firepower 4100/9300 シャーシ supports physical interfaces and EtherChannel (port-channel) interfaces. EtherChannel interfaces can include up to 16 member interfaces of the same type.

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firepower Chassis Manager によって、FXOS シャーシの管理に使用されます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLI から設定にする必要があります。このインターフェイスについての情報を FXOS CLI で表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER **connect local-mgmt**

firepower(local-mgmt) # **show mgmt-port**

物理ケーブルまたは SFP モジュールが取り外されている場合や **mgmt-port shut** コマンドが実行されている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

（注） シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

インターフェイス タイプ

物理インターフェイスおよび EtherChannel（ポートチャネル）インターフェイスは、次のいずれかのタイプになります。

- Data：通常のデータに使用します。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。

- Data-sharing：通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは 1 つまたは複数の論理デバイス/コンテナインスタンス（FTDFMC 専用）で共有できます。

- Mgmt：アプリケーション インスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために 1 つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを 1 つだけ割り当てることができます。アプリケーションと管理によっては、後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。

（注） 管理インターフェイスを変更すると、論理デバイスが再起動します。たとえば、e1/1 から e1/2 に1回変更すると、論理デバイスが再起動して新しい管理が適用されます。

- Eventing： FMC デバイスを使用した FTD のセカンダリ管理インターフェイスとして使用します。

（注） 各アプリケーション インスタンスのインストール時に、仮想イーサネット インターフェイスが割り当てられます。アプリケーションがイベントインターフェイスを使用しない場合、仮想インターフェイスは管理上ダウンの状態になります。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster：クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。クラスタタイプは、EtherChannel インターフェイスのみでサポートされます。FDM および CDO はクラスタリングをサポートしていません。

FXOS インターフェイスとアプリケーション インターフェイス

Firepower 4100/9300 は、物理インターフェイスおよび EtherChannel（ポートチャネル）インターフェイスの基本的なイーサネット設定を管理します。アプリケーション内で、より高いレベルの設定を行います。たとえば、FXOS では Etherchannel のみを作成できます。ただし、アプリケーション内の EtherChannel に IP アドレスを割り当てることができます。

続くセクションでは、インターフェイスの FXOS とアプリケーション間の連携について説明します。

VLAN サブインターフェイス

すべての論理デバイスで、アプリケーション内に VLAN サブインターフェイスを作成できます。

シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるため、シャーシとアプリケーションの間で不一致が発生することがあります。

Requirements and Prerequisites for Firepower 9300 Hardware and Software Combinations

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

- Security Module Types—You can install modules of different types in the Firepower 9300. For example, you can install the SM-48 as module 1, SM-40 as module 2, and SM-56 as module 3.
- Native and Container instances—When you install a container instance on a security module, that module can only support other container instances. A native instance uses all of the resources for a module, so you can only install a single native instance on a module. You can use native instances on some modules, and container instances on the other module. For example, you can install a native instance on module 1 and module 2, but container instances on module 3.
- High Availability—High Availability is only supported between same-type modules on the Firepower 9300. However, the two chassis can include mixed modules. For example, each chassis has an SM-40, SM-48, and SM-56. You can create High Availability pairs between the SM-40 modules, between the SM-48 modules, and between the SM-56 modules.
- ASA and FTD application types—You can install different application types on separate modules in the chassis. For example, you can install ASA on module 1 and module 2, and FTD on module 3.
- ASA or FTD versions—You can run different versions of an application instance type on separate modules, or as separate container instances on the same module. For example, you can install the FTD 6.3 on module 1, FTD 6.4 on module 2, and FTD 6.5 on module 3.

Guidelines and Limitations for Logical Devices

See the following sections for guidelines and limitations.

Guidelines and Limitations for Interfaces

Default MAC Addresses

Default MAC address assignments depend on the type of interface.

- Physical interfaces—The physical interface uses the burned-in MAC address.
- EtherChannels—For an EtherChannel, all interfaces that are part of the channel group share the same MAC address. This feature makes the EtherChannel transparent to network applications and users, because they only see the one logical connection; they have no knowledge of the individual links. The port-channel interface uses a unique MAC address from a pool; interface membership does not affect the MAC address.

General Guidelines and Limitations

High Availability

- Configure high availability within the application configuration.
- You can use any data interfaces as the failover and state links.
- The two units in a High Availability Failover configuration must:
  - 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 more information, see System Requirements for High Availability.

Configure Interfaces

By default, physical interfaces are disabled. You can enable interfaces, add EtherChannels, and edit interface properties.

Enable or Disable an Interface

You can change the **Admin State** of each interface to be enabled or disabled. By default, physical interfaces are disabled.

手順

ステップ **1** Choose **Interfaces** to open the Interfaces page.

The Interfaces page shows a visual representation of the currently installed interfaces at the top of the page and provides a listing of the installed interfaces in the table below.

ステップ **2** To enable the interface, click the disabled **無効なスライダ**（✕） so that it changes to the enabled **有効なスライダ**（✓）．

Click **Yes** to confirm the change. The corresponding interface in the visual representation changes from gray to green.

ステップ **3** To disable the interface, click the enabled **有効なスライダ**（✓） so that it changes to the disabled **無効なスライダ**（✕）．

Click **Yes** to confirm the change. The corresponding interface in the visual representation changes from green to gray.

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスをFXOSで物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

Add an EtherChannel (Port Channel)

An EtherChannel (also known as a port channel) can include up to 16 member interfaces of the same media type and capacity, and must be set to the same speed and duplex. The media type can be either RJ-45 or SFP; SFPs of different types (copper and fiber) can be mixed. You cannot mix interface capacities (for example 1GB and 10GB interfaces) by setting the speed to be lower on the larger-capacity interface. The Link Aggregation Control Protocol (LACP) aggregates interfaces by exchanging the Link Aggregation Control Protocol Data Units (LACPDUs) between two network devices.

You can configure each physical Data interface in an EtherChannel to be:

- Active—Sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.
- On—The EtherChannel is always on, and LACP is not used. An “on” EtherChannel can only establish a connection with another “on” EtherChannel.

（注） It may take up to three minutes for an EtherChannel to come up to an operational state if you change its mode from On to Active or from Active to On.

The Firepower 4100/9300 シャーシ only supports EtherChannels in Active LACP mode so that each member interface sends and receives LACP updates. An active EtherChannel can establish connectivity with either an active or a passive EtherChannel. You should use the active mode unless you need to minimize the amount of LACP traffic.

LACP coordinates the automatic addition and deletion of links to the EtherChannel without user intervention. It also handles misconfigurations and checks that both ends of member interfaces are connected to the correct channel group. “On” mode cannot use standby interfaces in the channel group when an interface goes down, and the connectivity and configurations are not checked.

When the Firepower 4100/9300 シャーシ creates an EtherChannel, the EtherChannel stays in a **Suspended** state for Active LACP mode or a **Down** state for On LACP mode until you assign it to a logical device, even if the physical link is up. The EtherChannel will be brought out of this **Suspended** state in the following situations:

- The EtherChannel is added as a data or management interface for a standalone logical device
- The EtherChannel is added as a management interface or cluster control link for a logical device that is part of a cluster
- The EtherChannel is added as a data interface for a logical device that is part of a cluster and at least one unit has joined the cluster

Note that the EtherChannel does not come up until you assign it to a logical device. If the EtherChannel is removed from the logical device or the logical device is deleted, the EtherChannel will revert to a **Suspended** or **Down** state.

Configure a Logical Device

Add a standalone logical device or a High Availability pair on the Firepower 4100/9300 シャーシ.

Add a Standalone FTD for the FDM

You can use the FDM with a native instance. Container instances are not supported. Standalone logical devices work either alone or in a High Availability pair.

始める前に

- Download the application image you want to use for the logical device from Cisco.com, and then that image to the Firepower 4100/9300 シャーシ.
- 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.
- You must also configure at least one Data type interface.
- Gather the following information:
  - Interface IDs for this device
  - Management interface IP address and network mask
  - Gateway IP address
  - DNS server IP address
  - FTD hostname and domain name

手順

See the FDM configuration guide to start configuring your security policy.

Add a High Availability Pair

FTD 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.

始める前に

See System Requirements for High Availability.

手順

ステップ 1 Allocate the same interfaces to each logical device.

ステップ 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.

ステップ 3 Enable High Availability on the logical devices. See High Availability (Failover).

ステップ 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.

Change an Interface on a FTD Logical Device

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

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 the FDM.

You can migrate the configuration from one interface to another interface before you delete the old interface.

始める前に

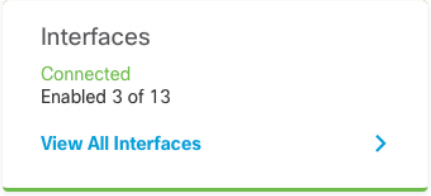
- Configure your interfaces, and add any EtherChannels according to 物理インターフェイスの設定（5 ページ） and Add an EtherChannel (Port Channel) （6 ページ）.
- If you want to add an already-allocated interface to an EtherChannel (for example, all interfaces are allocated by default to a cluster), you need to unallocate the 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 High Availability, make sure you add or remove the interface on all units before you sync the configuration in the the FDM. We recommend that you make the interface changes on the standby unit first, and then on the active unit. Note that new interfaces are added in an administratively down state, so they do not affect interface monitoring.

手順

ステップ 1 Sync and migrate the interfaces in the FDM.

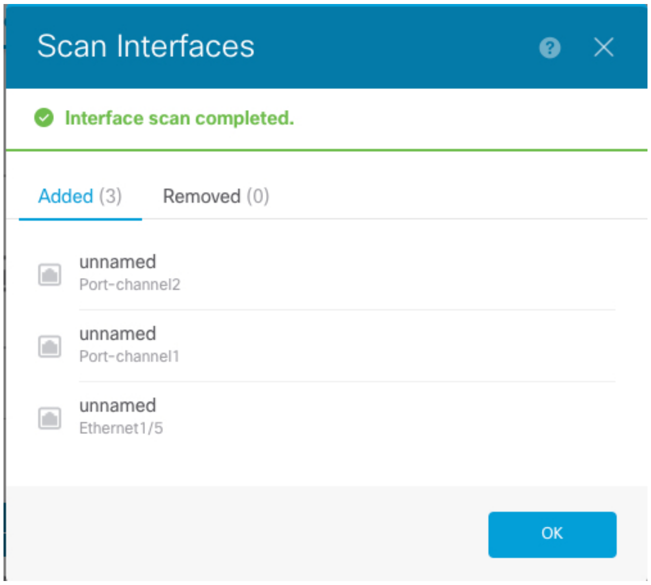
a) Log into the FDM.

b) Click **Device**, then click the **View All Interfaces** link in the **Interfaces** summary.



c) Click the **Scan Interfaces icon**.

d) Wait for the interfaces to scan, and then click **OK**.


Interface scan completed.

e) Configure the new interfaces with names, IP addresses, and so on.

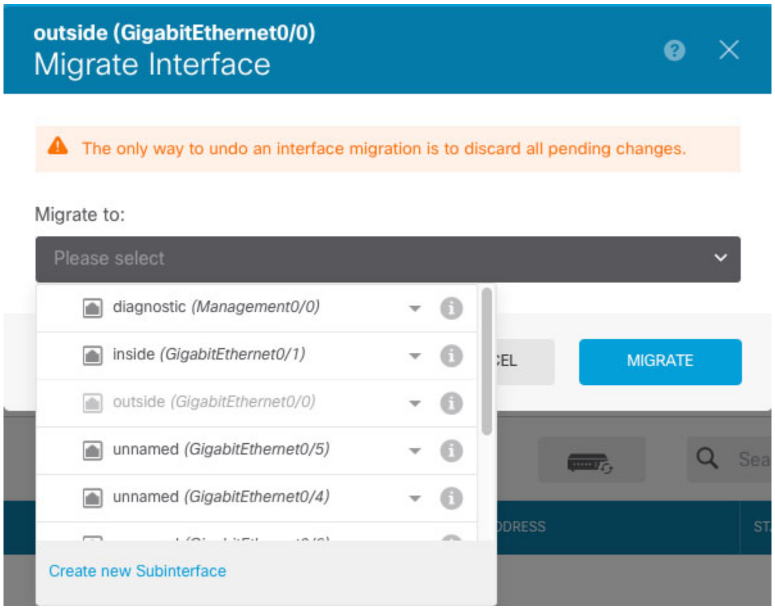
If you want to use the existing IP address and name of an interface that you want to delete, then you need to reconfigure the old interface with a dummy name and IP address so that you can use those settings on the new interface.

f) To replace an old interface with a new interface, click the Replace icon for the old interface.

Replace icon

This process replaces the old interface with the new interface in all configuration settings that refer to the interface.

g) Choose the new interface from the **Replacement Interface** drop-down list.



outside (GigabitEthernet0/0)

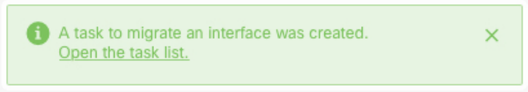
Migrate Interface

The only way to undo an interface migration is to discard all pending changes.

Migrate to:

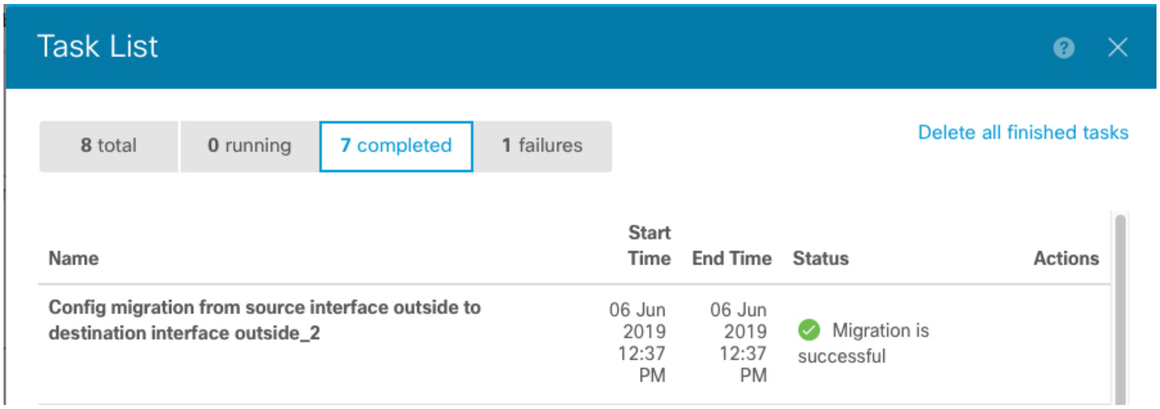
Please select
diagnostic (Management0/0)
inside (GigabitEthernet0/1)
outside (GigabitEthernet0/0)
unnamed (GigabitEthernet0/5)
unnamed (GigabitEthernet0/4)
Create new Subinterface
CEL
MIGRATE
Sea
DDRESS
ST

h) A message appears on the **Interfaces** page. Click the link in the message.



A task to migrate an interface was created.
Open the task list.

i) Check the **Task List** to ensure that the migration was successful.

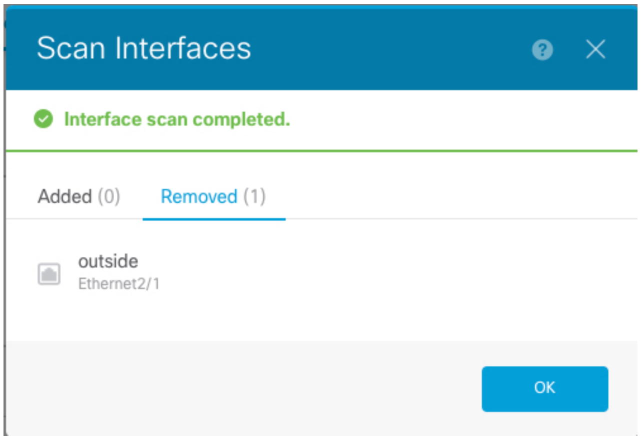


Task List

Name	Start Time	End Time	Status	Actions
Config migration from source interface outside to destination interface outside_2	06 Jun 2019 12:37 PM	06 Jun 2019 12:37 PM	✓ Migration is successful	

ステップ **2** Sync the interfaces again in the the FDM.

図 1 : FDM Scan Interfaces



Interface scan completed.

outside
Ethernet2/1

Connect to the Console of the Application

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

手順

ステップ **1** Connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* {**console** | **telnet**}

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

The benefits of using a Telnet connection is that you can have multiple sessions to the module at the same time, and the connection speed is faster.

例 :

```
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>
```

ステップ **2** Connect to the application console.

connect ftd *name*

To view the instance names, enter the command without a name.

例：

```
Firepower-module1> connect ftd ftd1
Connecting to ftd(ftd-native) console... enter exit to return to bootCLI
[...]
>
```

ステップ 3 Exit the application console to the FXOS module CLI.

- FTD—Enter **exit**

ステップ 4 Return to the supervisor level of the FXOS CLI.

Exit the console:

a) Enter ~

You exit to the Telnet application.

b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

a) Enter **Ctrl-], .**

History for Firepower 4100/9300 Logical Devices

Feature	Version	Details
Support for the FDM on the Firepower 4100/9300	6.5.0	You can now use the FDM with FTD logical devices on the Firepower 4100/9300. The FDM does not support Multi-Instance capability; only native instances are supported. （注） Requires FXOS 2.7.1.

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。