

# 管理からデータインターフェイスへのFTDでのマネージャアクセスの設定

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

### [設定](#)

#### [インターフェイスの移行を進める](#)

#### [プラットフォーム設定でのSSHの有効化](#)

### [確認](#)

#### [FMCのグラフィカルユーザインターフェイス\(GUI\)からの確認](#)

#### [FTDコマンドラインインターフェイス\(CLI\)からの確認](#)

### [トラブルシューティング](#)

#### [管理接続ステータス](#)

##### [正常動作シナリオ](#)

##### [動作しないシナリオ](#)

#### [ネットワーク情報の検証](#)

#### [マネージャの状態の検証](#)

#### [ネットワーク接続の検証](#)

##### [Management Centerへのping](#)

##### [インターフェイスのステータス、統計情報、パケットカウントの確認](#)

##### [FMCに到達するためのFTD上のルートの検証](#)

##### [Sftunnelと接続の統計情報の確認](#)

### [関連情報](#)

---

## はじめに

このドキュメントでは、Firepower Threat Defense(FTD)上のManager Access(MA)を管理インターフェイスからデータインターフェイスに変更するプロセスについて説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Firepower Threat Defense(Ftd)
- Firepower Management Center

## 使用するコンポーネント

- Firepower Management Center(FMC)仮想7.4.1
- Firepower Threat Defense(FTD)仮想7.2.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

各デバイスには、FMCと通信するための単一の専用管理インターフェイスが含まれています。必要に応じて、専用管理インターフェイスの代わりにデータインターフェイスを使用するようにデバイスを設定できます。データインターフェイスのFMCアクセスは、Firepower Threat Defenseを外部インターフェイスからリモートで管理する場合や、個別の管理ネットワークがない場合に便利です。この変更は、FMCによって管理されるFTDのFirepower Management Center(FMC)で実行する必要があります。

データインターフェイスからのFMCアクセスには、いくつかの制限があります。

- 1つの物理データインターフェイスでのみマネージャアクセスを有効にできます。サブインターフェイスまたはEtherChannelは使用できません。
- ルーテッドファイアウォールモードのみ（ルーテッドインターフェイスを使用）
- PPPoEはサポートされていません。ISPがPPPoEを必要とする場合は、Firepower Threat Defense(FTD)とWANモデムの間にはPPPoEをサポートするルータを配置する必要があります。
- 個別の管理インターフェイスとイベント専用インターフェイスは使用できません。

## 設定

### インターフェイスの移行を進める

---

注：変更を行う前に、FTDとFMCの両方の最新のバックアップを用意することを強く推奨します。

---

1. Devices > Device Managementページに移動し、変更するデバイスのEditをクリックします

○

[Collapse All](#) [Download Device List Report](#)

<input type="checkbox"/>	Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack	Group	
<input type="checkbox"/>	▼ FMT Test (1)								
<input type="checkbox"/>	● FTD-Test Short 3 192.168.1.8 - Routed	FTDv for VMware	7.2.5	N/A	Essentials	Base-ACP	↺		Edit → ↗

2. Device > Managementセクションに移動し、Manager Access Interfaceのリンクをクリックします。

Management <span style="float: right;">✎ 🔵</span>	
Remote Host Address:	192.168.1.8
Secondary Address:	
Status:	✔
Manager Access Interface:	 Management Interface

Manager Access Interfaceフィールドに既存の管理インターフェイスが表示されます。リンクをクリックして、新しいインターフェイスタイプを選択します。これは、「Manage device by」ドロップダウンリストの「Data Interface」オプションで、「Save」をクリックします。

### Manager Access Interface ?

i This is an advanced setting and need to be configured only if needed.  
See the [online help](#) for detailed steps.

Manage device by

Management Interface ▼

Management Interface

Data Interface

Close Save

3. 次に、データインターフェイスで管理アクセスをイネーブルにするに進み、Devices > Device Management > Interfaces > Edit Physical Interface > Manager Accessの順に移動します。

## Edit Physical Interface



General

IPv4

IPv6

Path Monitoring

Hardware Configuration

Manager Access

Advanced

Enable management access

Available Networks



Search

10.201.204.129

192.168.1.0\_24

any-ipv4

any-ipv6

CSM

Data\_Store

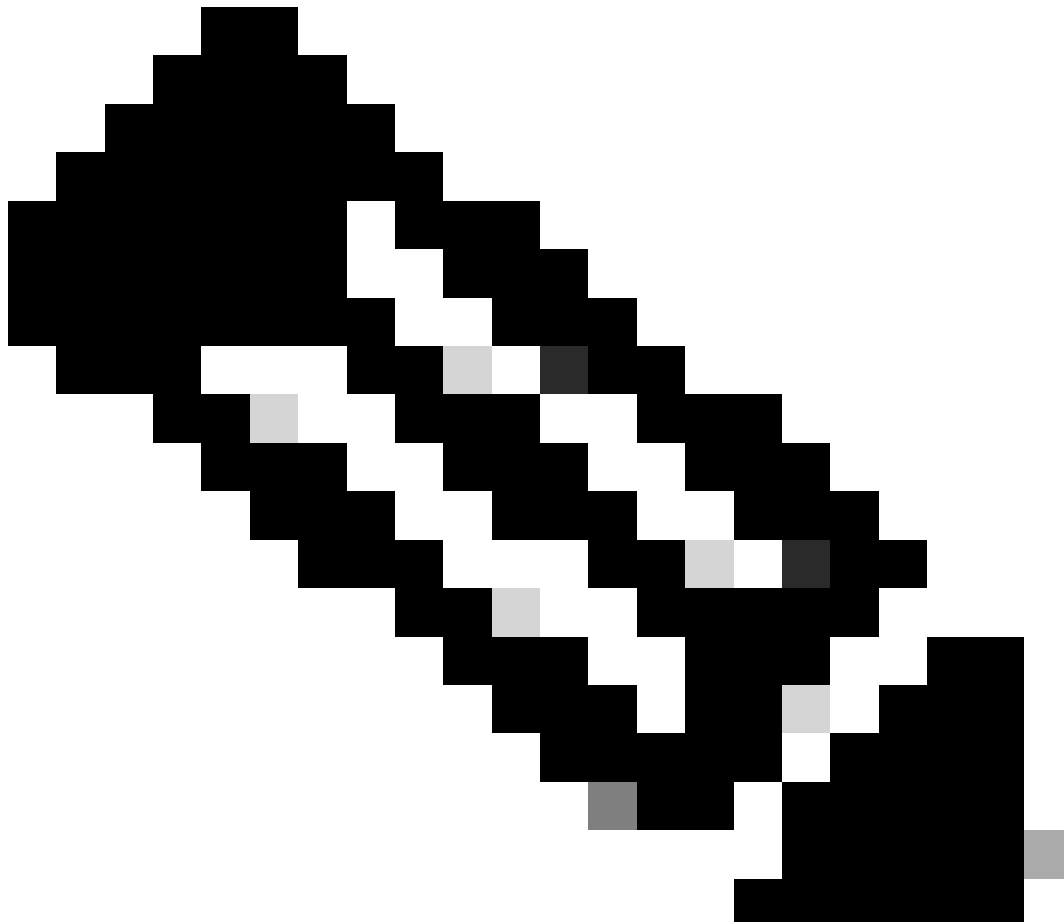
Add

Allowed Management Networks

any

Cancel

OK



---

注: ( オプション ) 冗長性のためにセカンダリインターフェイスを使用する場合は、冗長性のために使用するインターフェイスで管理アクセスを有効にします。

( オプション ) インターフェイスにDHCPを使用する場合は、Devices > Device Management > DHCP > DDNSダイアログでWebタイプのDDNS方式を有効にします。

( オプション ) プラットフォーム設定ポリシーでDNSを設定し、デバイス>プラットフォーム設定> DNSでこのデバイスに適用します。

---

4. 脅威対策がデータインターフェイスを介してManagement Centerにルーティングできることを確認し、必要に応じてDevices > Device Management > Routing > Static Routeでスタティックルートを追加します。

1. 追加するスタティックルートのタイプに応じて、IPv4またはIPv6をクリックします。
2. このスタティックルートを適用するインターフェイスを選択します。
3. Available Networkリストで、宛先ネットワークを選択します。
4. GatewayまたはIPv6 Gatewayフィールドで、このルートのネクストホップであるゲートウェイルータを入力または選択します。

( オプション ) ルートのアベイラビリティをモニタするには、モニタリングポリシーを定義するサービスレベル契約(SLA)モニタオブジェクトの名前をルートトラッキングフィールドで入力または選択します。

## Add Static Route Configuration



Type:  IPv4  IPv6

Interface\*



(Interface starting with this icon  signifies it is available for route leak)

Available Network  +

Add

Selected Network



10.201.204.129  
192.168.1.0\_24  
any-ipv4  
CSM  
Data\_Store  
FDM

Gateway\*

+



Metric:

(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

+

Cancel

OK

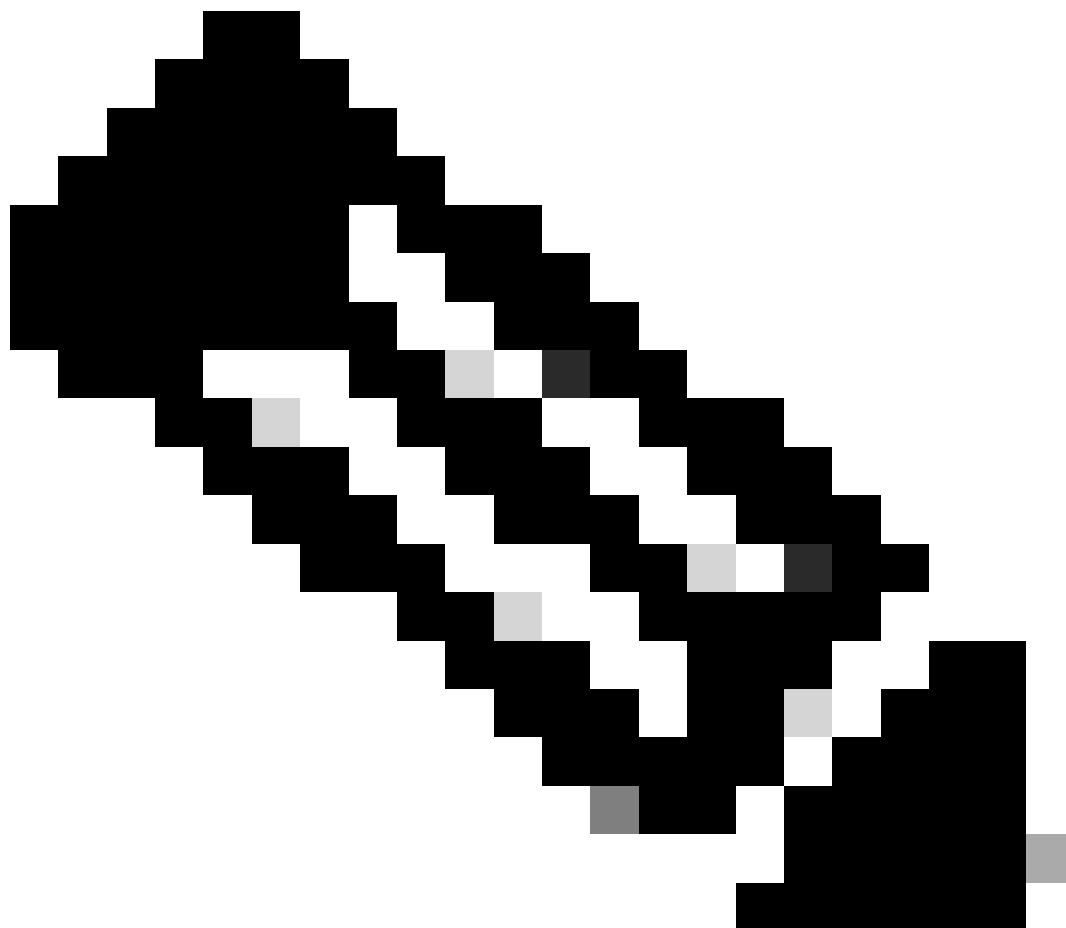
5. 設定変更を導入します。現在の管理インターフェイスに設定の変更が適用されています。

6. FTD CLIで、静的IPアドレスを使用するように管理インターフェイスを設定し、データインターフェイスになるようにゲートウェイを設定します。

- `configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces`

```
>
>
> configure network ipv4 manual IP_ADDRESS192.168.1.8 NETMASK255.255.255.0 GATEWAYdata-interfaces
Setting IPv4 network configuration...
Interface eth0 speed is set to '10000baseT/Full'
Network settings changed.
```



---



注：管理インターフェイスを使用する予定はありませんが、固定IPアドレスを設定する必要があります。たとえば、ゲートウェイをdata-interfacesに設定できるようにするプライベートアドレスです。この管理は、tap\_nlpインターフェイスを使用してデータインターフェイスに管理トラフィックを転送するために使用されます。



、脅威対策のリモートホストアドレスIPアドレス ( オプション ) セカンダリアドレス ( オプション ) セカンダリアドレスを更新し、接続を有効にします。

Management	
Remote Host Address:	192.168.1.8
Secondary Address:	
Status:	
Manager Access Interface:	 <a href="#">Data Interface</a>
Manager Access Details:	<a href="#">Configuration</a>

#### プラットフォーム設定でのSSHの有効化

Platform Settingsポリシーでデータインターフェイス用にSSHを有効にし、Devices > Platform Settings > SSH Accessの順に選択してこのデバイスに適用します。Addをクリックします。

- SSH接続の作成を許可しているホストまたはネットワーク。
- SSH接続を許可するインターフェイスを含むゾーンを追加します。ゾーンに含まれないインターフェイスの場合は、Selected Zones/Interfacesリストのフィールドにインターフェイス名を入力して、Addをクリックします。
- [OK] をクリックします。 変更の展開

# Add Secure Shell Configuration



IP Address\* +



Available Zones/Interfaces C

- DMZ
- Inside
- outside

Add



Selected Zones/Interfaces

Add

Cancel

OK



注：データインターフェイスではSSHはデフォルトで有効になっていません。そのため、SSHを使用して脅威に対する防御を管理する場合は、明示的に許可する必要があります。

---

## 確認

データインターフェイスで管理接続が確立されていることを確認します。



FMCのグラフィカルユーザインターフェイス(GUI)からの確認

Management Centerで、Devices > **Device Management** > Device > **Management** > **Manager Access - Configuration Details** > **Connection Status**ページの管理接続ステータスを確認します。

## Management

Remote Host Address: 192.168.1.30

Secondary Address:

Status: **Connected**  

Manager Access Interface: [Data Interface](#)

Manager Access Details: [Configuration](#)

FTDコマンドラインインターフェイス(CLI)からの確認

threat defense CLIで**thesftunnel-status-brief**コマンドを入力し、管理接続のステータスを表示します。

```
>
> sftunnel-status-brief
PEER:192.168.1.2
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'
Registration: Completed.
IPv4 Connection to peer '192.168.1.2' Start Time: Tue Jul 16 22:23:54 2024 UTC
Heartbeat Send Time: Tue Jul 16 22:39:52 2024 UTC
Heartbeat Received Time: Tue Jul 16 22:39:52 2024 UTC
Last disconnect time : Tue Jul 16 22:17:42 2024 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

ステータスには、データインターフェイスの接続が成功したことが示され、内部のtap\_nlpインターフェイスが示されます。

トラブルシューティング

Management Centerで、Devices > **Device Management** > Device > **Management** > **Manager Access - Configuration Details** > **Connection Status**ページの管理接続ステータスを確認します。

threat defense CLIで**thesftunnel-status-brief**コマンドを入力し、管理接続のステータスを表示します。また、**ftunnel-status**を使用して詳細な情報を表示することもできます。

管理接続ステータス

正常動作シナリオ

```
> sftunnel-status-brief
```

```
PEER:192.168.1.2
```

```
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '192.168.1.2' via '192.168.1.8'  
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '192.168.1.2' via '169.254.1.2'  
Registration: Completed.  
IPv4 Connection to peer '192.168.1.2' Start Time: Wed Jul 17 06:21:15 2024 UTC  
Heartbeat Send Time: Wed Jul 17 17:15:20 2024 UTC  
Heartbeat Received Time: Wed Jul 17 17:16:55 2024 UTC  
Last disconnect time : Wed Jul 17 06:21:12 2024 UTC  
Last disconnect reason : Process shutdown due to stop request from PM
```

## 動作しないシナリオ

```
> sftunnel-status-brief
```

```
PEER:192.168.1.2
```

```
Registration: Completed.  
Connection to peer '192.168.1.2' Attempted at Wed Jul 17 17:20:26 2024 UTC  
Last disconnect time : Wed Jul 17 17:20:26 2024 UTC  
Last disconnect reason : Both control and event channel connections with peer went down
```

## ネットワーク情報の検証

脅威に対する防御のCLIで、管理およびマネージャのアクセスデータインターフェイスのネットワーク設定を表示します。

```
> show network
```

```
> show network
===== [ System Information ] =====
Hostname                : ftdcdo.breakstuff.com
Domains                 : breakstuff.com
DNS Servers             : 192.168.1.103
DNS from router        : enabled
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

===== [ eth0 ] =====
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 00:0C:29:54:D4:47
----- [ IPv4 ] -----
Configuration           : Manual
Address                 : 192.168.1.8
Netmask                 : 255.255.255.0
Gateway                 : 192.168.1.1
----- [ IPv6 ] -----
Configuration           : Disabled

===== [ Proxy Information ] =====
State                   : Disabled
Authentication          : Disabled

===== [ System Information - Data Interfaces ] =====
DNS Servers             :
Interfaces              : GigabitEthernet0/0

===== [ GigabitEthernet0/0 ] =====
State                   : Enabled
Link                    : Up
Name                    : Outside
MTU                     : 1500
MAC Address             : 00:0C:29:54:D4:5B
```

---

注：このコマンドでは、管理接続の現在のステータスは表示されません。

---

## ネットワーク接続の検証

### Management Centerへのping

脅威に対する防御のCLIで、データインターフェイスから管理センターに対してpingを実行するコマンドを使用します。

> **fmc\_ip**にpingします。

```
> ping 192.168.1.2
Please use 'CTRL+C' to cancel/abort...
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

脅威に対する防御のCLIで、管理インターフェイスから管理センターにpingするコマンドを使用します。管理インターフェイスは、バックプレーンを介してデータインターフェイスにルーティングします。

> pingシステム**fmc\_ip**

```
> ping system 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.340 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.291 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=0.333 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=0.282 ms
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 132ms
rtt min/avg/max/mdev = 0.282/0.311/0.340/0.030 ms
```

インターフェイスのステータス、統計情報、パケットカウントの確認

threat defenseCLIでは、内部バックプレーンインターフェイスであるnlp\_int\_tapに関する次の情報を参照してください。

> **show interface detail**

```
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
(Full-duplex), (1000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0000.0100.0001, MTU 1500
IP address 169.254.1.1, subnet mask 255.255.255.248
311553 packets input, 41414494 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops
232599 packets output, 165049822 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
input queue (blocks free curr/low): hardware (0/0)
output queue (blocks free curr/low): hardware (0/0)
Traffic Statistics for "nlp_int_tap":
  311553 packets input, 37052752 bytes
  232599 packets output, 161793436 bytes
  167463 packets dropped
  1 minute input rate 0 pkts/sec, 3 bytes/sec
  1 minute output rate 0 pkts/sec, 0 bytes/sec
  1 minute drop rate, 0 pkts/sec
  5 minute input rate 0 pkts/sec, 3 bytes/sec
  5 minute output rate 0 pkts/sec, 0 bytes/sec
  5 minute drop rate, 0 pkts/sec
Control Point Interface States:
  Interface number is 14
  Interface config status is active
  Interface state is active
```

FMCに到達するためのFTD上のルートの検証

threat defenseCLIで、デフォルトルート(S\*)が追加されていること、および管理インターフェイス(nlp\_int\_tap)に対する内部NATルールが存在することを確認します。

> show route



```
> show route
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP  
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area  
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2  
E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN  
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2  
ia - IS-IS inter area, * - candidate default, U - per-user static route  
o - ODR, P - periodic downloaded static route, + - replicated route  
SI - Static InterVRF, BI - BGP InterVRF
```

```
Gateway of last resort is not set
```

```
C      192.168.1.0 255.255.255.0 is directly connected, Outside  
L      192.168.1.30 255.255.255.255 is directly connected, Outside
```

```
> show nat
```

```
> show nat  
Manual NAT Policies Implicit (Section 0)  
1 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel_0.0.0.0_intf3 interface destination static 0_0.0.0.0_5 0_0.0.0.0_5 service tcp 8305 8305  
   translate_hits = 5, untranslate_hits = 6  
2 (nlp_int_tap) to (Outside) source static nlp_server__sftunnel::_intf3 interface ipv6 destination static 0::_6 0::_6 service tcp 8305 8305  
   translate_hits = 0, untranslate_hits = 0  
3 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_intf3 interface  
   translate_hits = 10, untranslate_hits = 0  
4 (nlp_int_tap) to (Outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6  
   translate_hits = 0, untranslate_hits = 0
```

Sftunnelと接続の統計情報の確認

```
> show running-config sftunnelの順に選択します。
```

```
> show running-config sftunnel  
sftunnel interface Outside  
sftunnel port 8305
```



警告：マネージャアクセスの変更中は、FTD上のマネージャを削除したり、FTDをFMCから登録解除したり強制的に削除したりしないでください。

---

#### 関連情報

- [プラットフォーム上でのDNSの設定](#)
- [FMCを介したFTD \(HTTPSおよびSSH\) への管理アクセスの設定](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。