



A-C コマンド

- [acknowledge fault](#) (3 ページ)
- [acknowledge server](#) (4 ページ)
- [acknowledge slot](#) (5 ページ)
- [activate firmware](#) (6 ページ)
- [backup sel](#) (7 ページ)
- [cancel](#) (8 ページ)
- [clear lock-status](#) (9 ページ)
- [clear message](#) (10 ページ)
- [clear password-history](#) (12 ページ)
- [clear sel](#) (13 ページ)
- [commit-buffer](#) (14 ページ)
- [connect adapter](#) (15 ページ)
- [connect asa](#) (17 ページ)
- [connect cimc](#) (19 ページ)
- [connect ftd](#) (21 ページ)
- [connect fxos](#) (23 ページ)
- [connect local-mgmt](#) (25 ページ)
- [connect module](#) (27 ページ)
- [connect vdp](#) (29 ページ)
- [create app-instance](#) (31 ページ)
- [create bootstrap-key FIREWALL_MODE](#) (32 ページ)
- [create bootstrap-key MANAGEMENT_TYPE](#) (33 ページ)
- [create bootstrap-key PERMIT_EXPERT_MODE](#) (34 ページ)
- [create bootstrap-key-secret PASSWORD](#) (35 ページ)
- [create bootstrap-key-secret REGISTRATION_KEY](#) (36 ページ)
- [create bootstrap-key DNS_SERVERS](#) (37 ページ)
- [create bootstrap-key FIREPOWER_MANAGER_IP](#) (38 ページ)
- [create bootstrap-key SEARCH_DOMAINS](#) (39 ページ)
- [create breakout](#) (40 ページ)

- [create certreq \(42 ページ\)](#)
- [create class \(44 ページ\)](#)
- [create connection \(47 ページ\)](#)
- [create destination \(49 ページ\)](#)
- [create dns \(51 ページ\)](#)
- [create hw-crypto \(52 ページ\)](#)
- [create ip-block \(53 ページ\)](#)
- [create ipv6-block \(55 ページ\)](#)
- [create keyring \(57 ページ\)](#)
- [create local-user \(58 ページ\)](#)
- [create member-port \(60 ページ\)](#)
- [create ntp-server \(62 ページ\)](#)
- [create policy \(callhome\) \(63 ページ\)](#)
- [create policy \(flow control\) \(66 ページ\)](#)
- [create port-channel \(68 ページ\)](#)
- [create pre-login-banner \(70 ページ\)](#)
- [create profile \(72 ページ\)](#)
- [create property \(74 ページ\)](#)
- [create resource-profile \(76 ページ\)](#)
- [create server \(scope ldap\) \(78 ページ\)](#)
- [create snmp-trap \(80 ページ\)](#)
- [create snmp-user \(82 ページ\)](#)
- [create ssh-server \(84 ページ\)](#)
- [create stats-threshold-policy \(86 ページ\)](#)
- [create subinterface \(88 ページ\)](#)
- [create threshold-value \(91 ページ\)](#)
- [create trustpoint \(93 ページ\)](#)
- [cycle \(95 ページ\)](#)

acknowledge fault

システム障害を確認するには、**acknowledge fault** コマンドを使用します。

acknowledge fault *id*

構文の説明	fault <i>id</i>	障害の ID 番号。指定できる有効範囲は 0 ~ 18446744073709551615 です。
-------	------------------------	---

コマンドモード	マルチ モード
---------	---------

コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン **acknowledge fault** コマンドを使用して障害の有無を確認します。

例

次の例は、障害に対して確認応答を行う方法を示しています。

```
firepower # acknowledge fault 11347599
firepower* # commit-buffer
firepower #
```

関連コマンド	コマンド	説明
	acknowledge server	デバイスでサーバに対して確認応答を行います。
	acknowledge slot	デバイス内のスロットの有無を確認します。
	show fault	障害ポリシー情報を表示します。

acknowledge server

サーバに対して確認応答を行うには、**acknowledge server** コマンドを使用します。

acknowledge server {id|chassis/blade_id}

構文の説明

server
{id|chassis/blade_id}

サーバ ID 番号を使用して確認応答を行うサーバを識別するには、*id* と入力します。

シャーシおよびブレード ID 番号を使用して確認応答を行うサーバを識別するには、n/n 形式で *chassis/blade_id* と入力します。

(注) シャーシ ID 番号は常に **1** です。

コマンドモード

EXEC
scope chassis/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

acknowledge server コマンドを使用して、ネットワーク内のデバイスの有無を確認します。たとえば、最近作動させたサーバに対して確認応答を行い、そのサーバが存在することを確認できます。

シャーシモードで確認応答を行うサーバを識別するのに使用できる変数は *id* のみです。

例

次の例は、シャーシモードでモジュール 2 のサーバに対して確認応答を行う方法を示しています。

```
firepower# scope chassis 1
firepower /chassis # acknowledge server 2
firepower /chassis* # commit-buffer
firepower /chassis #
```

関連コマンド

コマンド	説明
acknowledge fault	システム障害を確認します。
acknowledge slot	最近作動させたスロットの有無を確認します。
show server	show server コマンドはサーバに関連するさまざまな設定情報を表示します。

acknowledge slot

スロットに対して確認応答を行うには、**acknowledge slot** コマンドを使用します。

acknowledge slot {*id*|*chassis/blade_id*}

構文の説明

EXEC モードでシャーシおよびブレード ID 番号を使用して確認応答を行うスロットを識別するには、n/n 形式で *chassis/blade_id* と入力します。

(注) シャーシ ID 番号は常に **1** です。

コマンドモード

EXEC
scope chassis/
scope fabric-interconnect/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

acknowledge slot コマンドを使用して、最近作動させたスロットの有無を確認します。

シャーシモードで確認応答を行うスロットを識別するのに使用できる変数は *id* のみです。

EXEC モードで、確認応答を行うスロットを識別するのに使用できるのは、シャーシおよびブレード ID 番号 (*chassis/blade_id*) のみです。

例

次の例は、シャーシモードでスロットに対して確認応答を行う方法を示しています。

```
firepower# scope chassis 1
firepower /chassis # acknowledge slot 2
firepower /chassis* # commit-buffer
firepower /chassis #
```

関連コマンド

コマンド	説明
acknowledge fault	システム障害を確認します。
acknowledge server	ネットワーク内のサーバの有無を確認します。

activate firmware

ファームウェア パッケージをアクティブにするには、**activate firmware** コマンドを使用します。

activate firmware *version*

構文の説明	<i>version</i>	バージョン番号を使用して、アクティブにするファームウェアパッケージを指定します。
-------	----------------	--

コマンドモード	scope system/
---------	---------------

コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン アクティベーションプロセスの一部として、すべての CLI セッションが終了します。

例

次の例では、ファームウェア パッケージをアクティブにする方法を示します。

```
firepower# scope system
firepower /system # activate firmware 2.4(1.52)
As part of activation, all cli sessions will be terminated.
Continue with activation? (yes/no)
```

関連コマンド	コマンド	説明
	show firmware	システムファームウェアのバージョンとステータス情報を表示します。
	show server firmware	サーバファームウェアのバージョンとステータス情報を表示します。

backup sel

システムイベントログ (SEL) をバックアップするには、**backup sel** コマンドを使用します。

backup sel {*id*|*chassis/blade_id*}

構文の説明	<i>id</i>	サーバID。9300 デバイスでは、最大3台のサーバを設定できます。
	<i>chassis/blade_id</i>	x/y 形式のアプライアンスのシャーシ番号とブレード番号。 (注) シャーシ ID 番号は常に 1 です。

コマンドモード 任意のコマンドモード

コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン このコマンドを使用して、サーバのシステム イベント ログ (SEL) をバックアップします。特定のサーバのコマンドモード (/chassis/server) では、オプションを指定せずにこのコマンドを実行できます。

例

次の例は、シャーシ 1 のサーバ 2 の SEL をバックアップする方法を示しています。

```
firepower# backup sel 1/2
firepower* # commit-buffer
firepower#
```

関連コマンド	コマンド	説明
	clear sel	サーバのシステム イベント ログ (SEL) をクリアします。

cancel

予約要求をキャンセルするには、**cancel** コマンドを使用します。

cancel

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

scope license/scope reservation/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

認証コードがすでに生成されている場合は、そのコードをインストールする必要があります。

例

次の例では、予約要求をキャンセルする方法を示します。

```
firepower# scope license
firepower /license # scope reservation
firepower /license/reservation # cancel
Warning : If you have already generated the authorization code from CSSM, please abort
the cancellation by issuing discard-buffer and then install the authorization code.
firepower /license/reservation* #
```

関連コマンド

コマンド	説明
enable reservation	パーマネント ライセンスの予約をイネーブルにします。
show license	現在のライセンス情報を表示します。

clear lock-status

ユーザのロックアウトステータスをクリアするには、ローカルユーザモードで **clear lock-status** コマンドを使用します。

clear lock-status

構文の説明	このコマンドには引数またはキーワードはありません。	
コマンドモード	ローカルユーザ (/security/local-user)	
コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。
使用上のガイドライン	ユーザ（管理者ユーザを含む）が指定されたログイン試行最高回数を超えると、ユーザはシステムからロックアウトされるため、ユーザのロックアウトステータスをクリアしない限り、ログインが許可されるまで、指定された時間待機する必要があります。	

例

次の例では、ローカルユーザモードを開始し、ロックアウトされたユーザがログインできるまでに経過する時間を指定する方法を示します。

```
FP9300-A # scope security
FP9300-A # scope local-user test_user1
FP9300-A /security/local-user # clear lock-status
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

関連コマンド	コマンド	説明
	set max-login-attempts	ユーザがシステムからロックアウトされるまで、ログイン試行を失敗できる回数を指定します。
	set user-account-unlock-time	ログイン試行の最高回数に達した後、ユーザがシステムからロックアウトされる時間を指定します。

clear message

現在のログイン前バナーテキストをクリアするには、**clear message** コマンドを使用します。ログイン前バナー オブジェクト自体は削除されません。

clear message

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドモード

scope security/scope banner/scope pre-login-banner/

コマンド履歴

リリース

変更内容

1.1(1)

コマンドが追加されました。

使用上のガイドライン

このコマンドを入力すると、ログイン前バナーテキストがクリアされます。ログイン前バナーオブジェクト自体は削除されません。

例

次の例では、現在のログイン前バナーを表示する方法、そのバナーをクリアする方法、および変更を適用して確定する例を示します。

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # scope pre-login-banner
firepower /security/banner/pre-login-banner # show

Pre login banner:
  Message
  -----
  Firepower-9300-2
  Western Data Center

firepower /security/banner/pre-login-banner # clear message
firepower /security/banner/pre-login-banner* # commit
firepower /security/banner/pre-login-banner # show

Pre login banner:
  Message
  -----

firepower /security/banner/pre-login-banner #
```

関連コマンド

コマンド	説明
create pre-login-banner	ログイン画面の前に表示されるバナーを作成します。初期のバナーオブジェクトは空です。

コマンド	説明
set message	ログイン前バナーとして表示されるテキストの行を追加または置き換えます。

clear password-history

ローカルユーザのパスワード履歴をクリアするには、**clear password-history** コマンドを使用します。

clear password-history

構文の説明	このコマンドには引数またはキーワードはありません。	
コマンドモード	ローカルユーザ (/security/local-user) モード	
コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。
使用上のガイドライン	このコマンドを使用するには、admin または AAA 権限を持つユーザである必要があります。	

例

次の例では、ローカルユーザモードを開始し、ユーザのパスワード履歴をクリアする方法を示します。

```
FP9300-A # scope security
FP9300-A /security # scope local-user test_user
FP9300-A /security/local-user # clear password history
FP9300-A /security/local-user* # commit-buffer
FP9300-A /security/local-user #
```

コマンド	説明
create local-user	新規のローカルユーザアカウントを作成します。
set password	ユーザアカウントのパスワードを指定します。

clear sel

サーバのシステム イベント ログ (SEL) をクリアするには、**clear sel** コマンドを使用します。

clear sel {*id* | *chassis_id/blade_id*}

構文の説明	<i>id</i>	(オプション) サーバ ID。9300 デバイスには最大 3 台のサーバがあります。
	<i>chassis_id/blade_id</i>	(オプション) n/n 形式のシャーシ番号およびブレード番号。 (注) シャーシ ID 番号は常に 1 です。

コマンドモード 任意のコマンドモード

コマンド履歴	リリース	変更内容
	1.4(1)	コマンドが追加されました。

使用上のガイドライン このコマンドを使用して、サーバのシステム イベント ログ (SEL) をクリアします。
特定のサーバ (/chassis/server) のコマンドモードでは、サーバを指定せずにこのコマンドを実行できます。

例

次の例では、組織モードでシャーシ 1 にあるサーバ 1 のシステム イベント ログをクリアする方法を示します。

```
FP9300-A # scope org Test
FP9300-A /org # clear sel 1/1
FP9300-A /org* # commit-buffer
FP9300-A /org #
```

関連コマンド	コマンド	説明
		backup sel

commit-buffer

設定変更を保存または確認するには、**commit-buffer** コマンドを使用します。

commit-buffer [**verify-only**]

構文の説明	verify-only (オプション) パッファ コンテンツのみを確認/検証します。コンテンツはコミットされていません。
コマンドモード	任意のコマンドモード
コマンド履歴	リリース 変更内容 1.1(1) コマンドが追加されました。
使用上のガイドライン	このコマンドを使用して、保留中のすべての設定変更を実行または確認します。設定変更の保留中は、コマンドプロンプトの前にアスタリスク (*) が表示されます。 commit-buffer コマンドが入力されると、保留中のコマンドがコミットされ、アスタリスクがなくなります。

例

次の例は、設定変更の保存方法を示しています。

```
FP9300-A# create org 3
FP9300-A /org* # commit-buffer
FP9300-A /org #
```

関連コマンド	コマンド	説明
	discard-buffer	すべてのコミットされていないコンフィギュレーションの変更を廃棄します。
	show configuration pending	保留中のすべての設定変更を表示します。

connect adapter

アダプタ コマンド シェルに接続するには、**connect** コマンドを使用します。

connect adapter { *chassis/server/id* | *rack_server/id* }

構文の説明	<i>chassis/server/id</i>	シャーシ、サーバ (モジュール) 、およびアダプタ ID (n/n/n 形式で入力) を指定します。Firepower 9300 では、モジュール番号は 1、2、または 3 を指定できます。Firepower 4100 では、1 です。 (注) シャーシ ID 番号は常に 1 です。
	<i>rack_server/id</i>	ラック番号とモジュール ID (n/n 形式で入力) を指定します。
コマンドモード	任意のコマンドモード	
コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン **help** を使用して、利用可能なメザニオンアダプタ コマンドをリストします。**help** コマンドを使用して、利用可能なコマンドの情報を表示します。

追加情報については、[connect adapter : コマンドリスト](#)を参照してください。



(注) アダプタ コマンド シェルに接続すると、コマンドラインプロンプトはデフォルト コマンドから変更されます。adapter n/n/n というアプライアンスに割り当てた名前に変更されます。この場合、n/n/n は、接続用に入力したアダプタのシャーシ/サーバ/ID の組み合わせです。

アダプタ モードを終了するには、**exit** と入力します。

例

次の例では、アダプタ コマンド シェルに接続し、利用可能なコマンドを表示する方法を示します。

```
firepower# connect adapter 1/1/1
adapter 1/1/1 # help
Available commands:
  connect      - Connect to remote debug shell
  exit         - Exit from subshell
  help         - List available commands
  history      - Show command history
  show-fwlist  - Show firmware versions on the adapter
  show-identity - Show adapter identity
```

```
show-phyinfo      - Show adapter phy info
show-systemstatus - Show adapter status
adapter 1/1/1 # exit
firepower#
```

関連コマンド

コマンド	説明
exit	前の CLI モードに戻ります。

connect asa

ASA CLI に接続するには、**connect asa** コマンドを使用します。

connect asa [*name*]

構文の説明	<i>name</i>	(オプション) ASA アプリケーション インスタンス名を指定します。これは論理デバイス名と同じです。
コマンド モード	connect module/	
コマンド履歴	リリース	変更内容
	2.4(1)	<i>name</i> 引数が追加されました。
	1.1(4)	コマンドが追加されました。

使用上のガイドライン CLI から利用可能なコマンドについては、ASA のマニュアルを参照してください。

ASA コンソールを終了するには、**Ctrl-a, d** と入力します

FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

~ と入力し、Telnet アプリケーションを終了するには **quit** と入力します。

例 :

```
asa> Ctrl-a, d
Firepower-module1> ~
telnet> quit
firepower#
```

Telnet セッションを終了します。

Ctrl-], . と入力

例 :

```
asa> Ctrl-a, d
Firepower-module1> Ctrl-], .
firepower#
```

例

次の例では、モジュール 1 の ASA CLI に接続する方法を示します。

```
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> connect asa  
asa>
```

関連コマンド

コマンド	説明
connect ftd	Threat Defense CLI に接続します。
connect module	モジュール CLI に接続します。
connect vdp	vDP CLI に接続します。

connect cimc

Cisco Integrated Management Controller (CIMC) コマンドシェルに接続するには、**connect cimc** コマンドと入力します。

connect cimc { *chassis_id/blade_id* | *rack_id* }

構文の説明

chassis_id/blade_id シャーシおよびモジュール番号を指定します (n/n 形式で入力)。
(注) シャーシ ID 番号は常に **1** です。

rack-id ラック番号を指定します。

コマンドモード

任意のコマンドモード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

help を使用して、利用可能な CIMC ファームウェア デバッグ ユーティリティ コマンドをリストします。**help** コマンドを入力して、利用可能なコマンドの情報を表示します。



(注) CIMC コマンドシェルに接続すると、コマンドラインプロンプトがデフォルトプロンプトから変更されます。[*xxx*] というアプライアンスに割り当てた名前です。この場合、*xxx* は入力した最後のコマンドです。次の例を参照してください。

ユーティリティを終了するには、**exit** と入力します。

Cisco TAC から指示がない限り、このユーティリティは使用しないでください。追加情報については、[connect cimc : コマンドリスト](#)を参照してください。

例

次の例では、CIMC モードに接続し、利用可能なコマンドをリストする方法を示します。

```
firepower# connect cimc 1/1
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '^]'.

CIMC Debug Firmware Utility Shell [ support ]
[ help ]# help

Debug Firmware Utility
```

Command List

```

alarms
cores
dimmb1
exit
i2cstats
images
mctools
memory
messages
mrcout
network
obfl
post
power
programmables
sensors
sel
fru
tasks
top
update
users
version
cert
sldp
help
help [COMMAND]

```

Notes:

```

"enter Key" will execute last command
"COMMAND ?" will execute help for that command

```

```

[ help ]# exit
Connection closed by foreign host.
firepower#

```

関連コマンド

コマンド	説明
exit	前の CLI モードに戻ります。

connect ftd

Threat Defense CLI に接続するには、**connect ftd** コマンドを使用します。

connect ftd *name*

構文の説明	<i>name</i>	Threat Defense アプリケーション インスタンス名を指定します。これは論理デバイス名と同じです。アプリケーションタイプに複数のアプリケーションインスタンスがある場合、インスタンス名を指定する必要があります。インスタンス名を表示するには、名前を付けずにコマンドを入力します。
コマンドモード	connect module/	
コマンド履歴	リリース	変更内容
	2.4(1)	<i>name</i> 引数が追加されました。エスケープ文字が exit から Ctrl-a, d に変更されました。
	1.1(4)	コマンドが追加されました。

使用上のガイドライン CLI から利用可能なコマンドについては、Threat Defense のマニュアルを参照してください。

Threat Defense コンソールを終了するには、**exit** と入力します。2.4(1) より前のバージョンの場合は、**Ctrl-a, d** と入力します

FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

~ と入力し、Telnet アプリケーションを終了するには **quit** と入力します。

例：

```
> exit
Firepower-module1> ~
telnet> quit
firepower#
```

Telnet セッションを終了します。

Ctrl-], . と入力

例：

```
> exit
Firepower-module1> Ctrl-], .
firepower#
```

例

次の例では、モジュール 1 の Threat Defense CLI に接続する方法を示します。

```
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> connect ftd
>
```

関連コマンド

コマンド	説明
connect asa	ASA CLI に接続します。
connect module	モジュール CLI に接続します。
connect vdp	vDP CLI に接続します。

connect fxos

FXOS コマンド シェルに接続するには、**connect fxos** コマンドを使用します。

connect fxos [a]

構文の説明	a	(オプション) ファブリック a に接続します。 (注) ファブリック ID は常に a です。ファブリック ID を省略すると、ファブリック A に接続されます。
コマンドモード	任意のコマンドモード	
コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。
使用上のガイドライン	? と入力して、利用可能な FXOS シェル コマンドをリストします。 <i>command ?</i> と入力して、個別のコマンドの情報を表示します。	



- (注) FXOS コマンドシェルに接続すると、コマンドラインプロンプトがデフォルトプロンプトから変更されます。(fxos) が付加されたデフォルトプロンプトというアプライアンスに割り当てられた名前です。次の例を参照してください。

FXOS シェルを終了するには、**exit** と入力します。

例

次の例では、FXOS コマンドシェルに接続し、利用可能なコマンドを表示する方法を示します。

```
firepower# connect fxos
firepower(fxos)# ?
clear          Reset functions
cli            CLI commands
debug         Debugging functions
debug-filter   Enable filtering for debugging functions
ethanalyzer    Configure cisco packet analyzer
no            Negate a command or set its defaults
ntp           NTP configuration
show          Show running system information
system        System management commands
terminal      Set terminal line parameters
test          Test command
undebug       Disable Debugging functions (See also debug)
end           Go to exec mode
exit          Exit from command interpreter
```

```
pop          Pop mode from stack or restore from name
push        Push current mode to stack or save it under name
where       Shows the cli context you are in
```

```
firepower (fxos)# exit
firepower#
```

関連コマンド

コマンド	説明
connect local-mgmt	特定のアダプタに接続している間に、リモート デバッグ シェルに接続します。
exit	前の CLI モードに戻ります。

connect local-mgmt

ローカル管理コマンドシェルに接続するには、**connect local-mgmt** コマンドを使用します。

connect local-mgmt [a]

構文の説明

a (オプション) ファブリック **a** に接続します。

(注) ファブリック ID は常に **a** です。ファブリック ID を省略すると、ファブリック **A** に接続されます。

コマンドモード

任意のコマンドモード

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

?を入力して、利用可能なローカル管理シェルコマンドをリストします。 *command ?* を入力して、個別のコマンドの情報を表示します。

追加情報については、[connect local-mgmt : コマンドリスト](#) を参照してください。



(注) ローカル管理コマンドシェルに接続すると、コマンドラインプロンプトがデフォルトプロンプトから変更されます。(local-mgmt)が付加されたデフォルトプロンプトというアプライアンスに割り当てられた名前です。次の例を参照してください。

ローカル管理モードを終了するには、**exit** と入力します。

例

次の例では、ローカル管理コマンドシェルに接続し、利用可能なコマンドを表示する方法を示します。

```
firepower# connect local-mgmt
firepower(local-mgmt)# ?
  cd          Change current directory
  clear      Clear managed objects
  cluster    Cluster mode
  connect    Connect to Another CLI
  copy      Copy a file
  cp        Copy a file
  delete    Delete managed objects
  dir       Show content of dir
  enable    Enable
  end       Go to exec mode
  erase     Erase
  erase-log-config Erase the mgmt logging config file
```

```

exit          Exit from command interpreter
fips          FIPS compliance
ls            Show content of dir
mgmt-port    Management Port
mkdir         Create a directory
move         Move a file
mv           Move a file
ping         Test network reachability
ping6        Test IPv6 network reachability
pwd          Print current directory
reboot       Reboots Fabric Interconnect
restore-check Check if in restore mode
rm           Remove a file
rmdir        Remove a directory
run-script   Run a script
show         Show system information
shutdown     Shutdown
ssh          SSH to another system
tail-mgmt-log tail mgmt log file
telnet       Telnet to another system
terminal     Terminal
top          Go to the top mode
traceroute   Traceroute to destination
traceroute6  Traceroute to IPv6 destination
verify       Verify Application Image

```

```

firepower(local-mgmt)# exit
firepower#

```

関連コマンド

コマンド	説明
connect fxos	FXOS コマンド シェルに接続します。
exit	前の CLI モードに戻ります。

connect module

モジュール コマンド シェルに接続するには、**connect module** コマンドを使用します。

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

構文の説明	console	シリアル コンソールに接続します。 コンソール接続の利点は永続的であることです。
	<i>module_id</i>	9300 デバイスの場合、モジュール番号は 1、2、または 3 に指定できます。4100 デバイスは 1 です。
	telnet	Telnet 接続を使用して接続します。Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

コマンドモード 任意のコマンドモード

コマンド履歴	リリース	変更内容
	2.4(1)	Telnet サポートが追加されました。
	1.1(1)	コマンドが追加されました。

使用上のガイドライン モジュール CLI から、**connect application** コマンドを使用してアプリケーション CLI に接続できます。

help と入力して、利用可能なモジュールシェルコマンドをリストします。**help command** を使用して、個別のコマンドの情報を表示します。また、**help** の代わりに **?** を使用すると、ヘルプ情報を表示することもできます。



- (注) モジュール コマンド シェルに接続すると、コマンドラインプロンプトがデフォルトプロンプトから変更されます。Firepower-modulen というアプライアンスに割り当てた名前です。この場合、n は接続先のモジュール番号です。次の例を参照してください。

追加情報については、[connect module : コマンドリスト](#)を参照してください。

例

次の例では、モジュール 1 コンソールに接続し、利用可能なコマンドを表示する方法を示します。

```
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>?
  secure-login    => Enable blade secure login
  show            => Display system information. Enter show ? for options
  config         => Configure the system. Enter config ? for options
  terminalLength  => Terminal settings. Enter terminal ? for options
  ping           => Ping a host to check reachability
  nslookup       => Look up an IP address or host name with the DNS servers
  traceroute     => Trace the route to a remote host
  connect        => Connect to specific csp console (asa, etc)
  support        => System file operations
  help           => Get help on command syntax

Firepower-module1> ~
telnet> close
Connection closed.
firepower#

```

次の例では、Telnet を使用してモジュール 1 に接続し、利用可能なコマンドを表示する方法を示します。

```

firepower# connect module 1 telnet
Type exit or Ctrl-] followed by . to quit.
Firepower-module1>?
  secure-login    => Enable blade secure login
  show            => Display system information. Enter show ? for options
  config         => Configure the system. Enter config ? for options
  terminalLength  => Terminal settings. Enter terminal ? for options
  ping           => Ping a host to check reachability
  nslookup       => Look up an IP address or host name with the DNS servers
  traceroute     => Trace the route to a remote host
  connect        => Connect to specific csp console (asa, etc)
  support        => System file operations
  exit           => Exit the session
  help           => Get help on command syntax
Firepower-module1> <Ctrl-], .>
firepower#

```

関連コマンド

コマンド	説明
connect asa	ASA CLI に接続します。
connect ftd	Threat Defense CLI に接続します。
connect vdp	vDP CLI に接続します。

connect vdp

Radware DefensePro (vDP) CLI に接続するには、**connect vdp** コマンドを使用します。

connect vdp [*name*]

構文の説明	<i>name</i>	(オプション) vDP アプリケーション インスタンス名を指定します。これはメイン アプリケーションの論理デバイス名/アプリケーション インスタンス名と同じです。
コマンドモード	connect module/	
コマンド履歴	リリース	変更内容
	2.4(1)	<i>name</i> 引数が追加されました。
	1.1(4)	コマンドが追加されました。

使用上のガイドライン CLI から利用可能なコマンドについては、vDP のマニュアルを参照してください。

vDP コンソールを終了するには、**Ctrl-],.** と入力します。

FXOS CLI のスーパーバイザ レベルに戻ります。

コンソールを終了します。

~ と入力し、Telnet アプリケーションを終了するには **quit** と入力します。

例：

```
> Ctrl-], .
Firepower-module1> ~
telnet> quit
firepower#
```

Telnet セッションを終了します。

Ctrl-],. と入力

例：

```
> Ctrl-], .
Firepower-module1> Ctrl-], .
firepower#
```

例

次の例では、モジュール 1 の vDP CLI に接続する方法を示します。

```
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> connect vdp
```

関連コマンド

コマンド	説明
connect asa	ASA CLI に接続します。
connect ftd	Threat Defense CLI に接続します。
connect module	モジュール CLI に接続します。

create app-instance

アプリケーションインスタンスを定義するには、**create app-instance** コマンドを使用します。

create app-instance *app_type* *app_name*

構文の説明	<i>app_name</i>	アプリケーションインスタンスの名前は 1 ～ 64 文字です。このインスタンスの論理デバイスを作成するときに、このデバイス名を使用します。
	<i>app_type</i>	アプリケーションタイプは、 asa 、 ftd 、または vdp のいずれかです。
コマンドモード	scope ssa/scope slot/	
コマンド履歴	リリース	変更内容
	2.4(1)	<i>app_name</i> 引数が必須になりました。
	1.1(1)	コマンドが追加されました。
使用上のガイドライン	イメージバージョン、展開タイプ、リソースプロファイル、モードなど、このアプリケーションインスタンスには多くのパラメータを設定できます。また、アプリケーションの有効化、無効化、および再起動も可能です。	
	<p>例</p> <p>次の例では、Threat Defense アプリケーションインスタンスのイメージバージョンを設定する方法を示します。</p> <pre>firepower# scope ssa firepower /ssa # scope slot 1 firepower /ssa/slot # create app-instance ftd MyDevice1 firepower /ssa/slot/app-instance* # set deploy-type container firepower /ssa/slot/app-instance* # set resource-profile-name silver 1 firepower /ssa/slot/app-instance* # set startup-version 6.3.0 firepower /ssa/slot/app-instance* #</pre>	
関連コマンド	コマンド	説明
	show app-attri	現在のアプリケーション属性を表示します。

create bootstrap-key FIREWALL_MODE

Threat Defense と ASA のブートストラップ コンフィギュレーションでファイアウォール モードをルーテッドまたはトランスペアレントに指定するには、**create bootstrap-key FIREWALL_MODE** コマンドを指定します。

create bootstrap-key FIREWALL_MODE

コマンド モード	scope ssa/create logical-device/create mgmt-bootstrap/	
コマンド デフォルト	デフォルト モードはルーテッドです。	
コマンド履歴	リリース	変更内容
	2.4(1)	ASA のサポートが追加されました。
	1.1(4)	FTD に対してコマンドが追加されました。

使用上のガイドライン ブートストラップの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、アプリケーション CLI の設定でほとんどの値を変更できます。

例

次に、モードをルーテッドに設定する例を示します。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド	コマンド	説明
	create logical-device	論理デバイスを作成します。
	create mgmt-bootstrap	アプリケーションのブートストラップコンフィギュレーションを作成します。
	set value	このコマンドの値を設定します。

create bootstrap-key MANAGEMENT_TYPE

Threat Defense のブートストラップ設定でマネージャ（FMC または FDM）を指定するには、**create bootstrap-key MANAGEMENT_TYPE** コマンドを使用します。

create bootstrap-key MANAGEMENT_TYPE

コマンドモード scope ssa/create logical-device/create mgmt-bootstrap/

コマンドデフォルト デフォルトのマネージャは FMC です。

コマンド履歴	リリース	変更内容
	2.7(1)	FTD に対してコマンドが追加されました。

使用上のガイドライン ブートストラップの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、アプリケーション CLI の設定でほとんどの値を変更できます。

例

次の例は、マネージャを FDM に設定する方法を示しています。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key MANAGEMENT_TYPE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value LOCALLY_MANAGED
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド	コマンド	説明
	create logical-device	論理デバイスを作成します。
	create mgmt-bootstrap	アプリケーションのブートストラップコンフィギュレーションを作成します。
	set value	このコマンドの値を設定します。

create bootstrap-key PERMIT_EXPERT_MODE

Threat Defense の FTD SSH セッションでエキスパート モードを許可するには、**create bootstrap-key PERMIT_EXPERT_MODE** コマンドを使用します。

create bootstrap-key PERMIT_EXPERT_MODE

コマンド モード scope ssa/create logical-device/create mgmt-bootstrap/

コマンド デフォルト デフォルトは no です。

コマンド履歴	リリース	変更内容
	2.4(1)	コマンドが追加されました。

使用上のガイドライン エキスパート モードでは、高度なトラブルシューティングに FTD シェルからアクセスできません。デフォルトでは、コンテナ インスタンスの場合、エキスパート モードを使用できるのは FXOS CLI から FTD CLI にアクセスするユーザだけです。この制限は、インスタンス間の分離を増やす場合、コンテナ インスタンスのみに適用されます。マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパート モードを使用します。このモードを開始するには、FTD CLI で **expert** コマンドを使用します。

例

次に、SSH でエキスパート モードを有効にする例を示します。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key PERMIT_EXPERT_MODE
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value yes
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド	コマンド	説明
	create logical-device	論理デバイスを作成します。
	create mgmt-bootstrap	アプリケーションのブートストラップコンフィギュレーションを作成します。
	set value	このコマンドの値を設定します。

create bootstrap-key-secret PASSWORD

Threat Defense のブートストラップ設定で管理者パスワードを指定するには、**create bootstrap-key-secret PASSWORD** コマンドを使用します。

create bootstrap-key-secret PASSWORD

コマンド モード scope ssa/create logical-device/create mgmt-bootstrap/

コマンド デフォルト 管理者パスワードが設定されていない場合。

コマンド履歴	リリース	変更内容
	1.1(4)	FTD に対してコマンドが追加されました。
	2.4(1)	ASA のサポートが追加されました。

使用上のガイドライン 事前設定されている ASA 管理者ユーザおよびイネーブル パスワードはパスワードの回復時に役立ちます。FXOS アクセスができる場合、管理者ユーザパスワードを忘れたときにリセットできます。

例

次に、モードをルーテッドに設定する例を示します。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # create bootstrap-key-secret
PASSWORD
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド	コマンド	説明
	create logical-device	論理デバイスを作成します。
	create mgmt-bootstrap	アプリケーションのブートストラップコンフィギュレーションを作成します。
	set value	このコマンドの値を設定します。

create bootstrap-key-secret REGISTRATION_KEY

ブートストラップ設定において、Threat Defense デバイスと Management Center 間で共有される登録キーを指定するには、**create bootstrap-key-secret REGISTRATION_KEY** コマンドを使用します。

create bootstrap-key-secret REGISTRATION_KEY

コマンド モード scope ssa/create logical-device/create mgmt-bootstrap/

コマンド デフォルト 登録済みのキーは生成されません。

コマンド履歴	リリース	変更内容
	1.1(4)	FTD に対してコマンドが追加されました。

使用上のガイドライン この登録キーのパスフレーズは、1～37文字の範囲で選択できます。FTDを追加するときに、FMCに同じキーを入力します。ブートストラップの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、アプリケーション CLI の設定でほとんどの値を変更できます。

例

次の例は、登録キーの値を設定する方法を示しています。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # create bootstrap-key-secret
REGISTRATION_KEY
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: gratuitousapples
Confirm the value: gratuitousapples
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド	コマンド	説明
	create logical-device	論理デバイスを作成します。
	create mgmt-bootstrap	アプリケーションのブートストラップコンフィギュレーションを作成します。
	set value	このコマンドの値を設定します。

create bootstrap-key DNS_SERVERS

Threat Defense の DNS サーバーのカンマ区切りリストを指定するには、**create bootstrap-key DNS_SERVERS** コマンドを使用します。

create bootstrap-key DNS_SERVERS

コマンド モード scope ssa/create logical-device/create mgmt-bootstrap/

コマンド デフォルト デフォルトは no です。

コマンド履歴	リリース	変更内容
	2.4(1)	コマンドが追加されました。

使用上のガイドライン FMC は、FMC のホスト名を指定すると、DNS を使用します。

例

次の例は、ホスト名を指定する方法を示しています。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key DNS_SERVERS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.9.8.7,10.9.6.5
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド	コマンド	説明
	create logical-device	論理デバイスを作成します。
	create mgmt-bootstrap	アプリケーションのブートストラップコンフィギュレーションを作成します。
	set value	このコマンドの値を設定します。

create bootstrap-key FIREPOWER_MANAGER_IP

管理側の Firepower Management Center の IP アドレスまたはホスト名もしくは NAT ID を指定するには、**create bootstrap-key FIREPOWER_MANAGER_IP** コマンドを使用します。

create bootstrap-key FIREPOWER_MANAGER_IP

コマンドモード scope ssa/create logical-device/create mgmt-bootstrap/

コマンドデフォルト デフォルトは no です。

コマンド履歴	リリース	変更内容
	2.4(1)	コマンドが追加されました。

使用上のガイドライン 通常は、ルーティングと認証の両方の目的で両方の IP アドレス（登録キー付き）が必要です。FMC がデバイスの IP アドレスを指定し、デバイスが FMC の IP アドレスを指定します。ただし、IP アドレスの1つのみがわかっている場合（ルーティング目的の最小要件）は、最初の通信用に信頼を確立して正しい登録キーを検索するために、接続の両側に一意の NAT ID を指定する必要もあります。NAT ID として、1~37 文字の任意のテキスト文字列を指定できます。FMC およびデバイスでは、初期登録の認証と承認を行うために、登録キーおよび NAT ID（IP アドレスではなく）を使用します。

例

次に、SSH でエキスパートモードを有効にする例を示します。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREPOWER_MANAGER_IP
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value 10.10.10.7
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド	コマンド	説明
	create logical-device	論理デバイスを作成します。
	create mgmt-bootstrap	アプリケーションのブートストラップコンフィギュレーションを作成します。
	set value	このコマンドの値を設定します。

create bootstrap-key SEARCH_DOMAINS

検索ドメインのカンマ区切りリストを指定するには、**create bootstrap-key SEARCH_DOMAINS** コマンドを使用します。

create bootstrap-key SEARCH_DOMAINS

コマンド モード scope ssa/create logical-device/create mgmt-bootstrap/

コマンド デフォルト デフォルトは no です。

コマンド履歴	リリース	変更内容
	2.4(1)	コマンドが追加されました。

例

次に、SSH でエキスパート モードを有効にする例を示します。

```
firepower# scope ssa
firepower /ssa # create logical-device FTD1 ftd 1 standalone
Firepower /ssa/logical-device* # create mgmt-bootstrap ftd
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key SEARCH_DOMAINS
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value
cisco.com,example.com
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

関連コマンド	コマンド	説明
	create logical-device	論理デバイスを作成します。
	create mgmt-bootstrap	アプリケーションのブートストラップコンフィギュレーションを作成します。
	set value	このコマンドの値を設定します。

create breakout

ブレイクアウトポートを作成するには、**create breakout** コマンドを使用します。指定されたスロットとポートIDを持つブレイクアウトがすでに存在している場合、コマンドは失敗します。

ブレイクアウトポートを追加または開始するには、**enter breakout** コマンドを使用します。指定されたブレイクアウトが存在しない場合は、作成されて開始されます。ブレイクアウトポートが存在する場合は、そのポートが開始されます。

また、このコマンドの **scope** を使用して、既存のブレイクアウトポートを開始し、プロパティを表示することもできます。

既存のブレイクアウトポートを削除するには、このコマンドの **delete** を使用します。

create breakout *slot_ID* *port_ID*

構文の説明	<i>slot_ID</i>	このスロット番号を使用して、ブレイクアウトするポートモジュールを特定します。
	<i>port_ID</i>	このブレイクアウトポートに ID 番号を割り当てます。
コマンドモード	scope cabling/scope fabric a/	
コマンド履歴	リリース	変更内容
	1.1.1	コマンドが追加されました。

使用上のガイドライン ブレイクアウトケーブルと組み合わせ、このコマンドを使用すると、40ギガビットイーサネットポートを「ブレイクアウト」し、最大4個の未設定の10ギガビットポートを作成できます。

ハードウェアバイパス対応のインターフェイスをブレイクアウトポートとして設定することはできません。



(注) ポートでブレイクアウトを設定するとシステムが再起動するため、変更をコミットする前に、必要なすべてのポートをブレイクアウトすることをお勧めします。

例

次に、スロット2に4つのブレイクアウトポートを作成する例を示します。

```
firepower# scope cabling
firepower /cabling/fabric/ # scope fabric
firepower /cabling/fabric/ # create breakout 2 1
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # up
```



```

firepower /cabling/fabric/ # create breakout 2 2
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # up
firepower /cabling/fabric/ # create breakout 2 3
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # up
firepower /cabling/fabric/ # create breakout 2 4
Warning: This action will reboot the system and any existing configurations on 40G port
will be erased.!
firepower /cabling/fabric/breakout* # commit-buffer
firepower /cabling/fabric/breakout #

```

関連コマンド

コマンド	説明
delete breakout	既存のブレイクアウト ポートを削除します。
enter aggr-interface	パラメータを設定できる集約インターフェイスを開始します。

create certreq

キーリング認証要求を追加するには、**create certreq** コマンドを使用します。キーリングの要求が現在すでに存在する場合、コマンドは失敗します。

既存の認証要求を編集するには、**enter certreq** コマンドを使用します。

また、このコマンドの **scope** を使用して、既存の認証要求を入力し、プロパティを割り当てまたは変更することもできます。

既存の認証要求を削除するには、**delete** コマンドを使用します。

create certreq [**ip** | **subject-name**]

delete certreq

enter certreq
scope certreq

構文の説明

ip *ip_address* (オプション) このデバイスが配置されているドメインの **ip** キーワードと IPv4 アドレスを入力します。要求のパスワードの入力と確定が求められます。このパラメータは、コマンドの **create certreq** 形式にのみ適用されます。

subject-name *name* (オプション) この要求の **subject-name** キーワードと識別子を入力します。たとえば、アプライアンスのホスト名を入力します。要求のパスワードの入力と確定が求められます。このパラメータは、コマンドの **create certreq** 形式にのみ適用されます。

コマンドモード

scope security/scope keyring/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

新しいキーリング認証要求を作成すると、新しい認証要求が定義およびコミットされていないことを示すアスタリスクが付いた認証要求モード (**security/keyring/certreq**) が自動的に開始されます。また、既存のキーリングの認証要求モードを調査することもできます。

認証要求パラメータを指定するには、認証要求モードで **set** コマンドを使用します。



(注) 新しい認証要求を作成またはコミットする前に、**set modulus** を使用して RSA キー係数 (SSL キーの長さ) を設定する必要があります。

例

次の例は、新しいキーリングとその認証要求の作成方法を示しています。

```
firepower # scope security
firepower /security # create keyring test-ring2
firepower /security/keyring* # create certreq ip 209.165.201.20
Certificate request password:
Confirm certificate request password:
firepower /security/keyring* # scope certreq
firepower /security/keyring/certreq* #
firepower /security/keyring/certreq* # set ?
country          Country name (2 letter code)
dns              DNS name (subject alternative name)
e-mail          E-mail name
fi-a-ip         Certificate request FI A ip address
fi-a-ipv6       Certificate request FI A ipv6 address
fi-b-ip         Certificate request FI B ip address
fi-b-ipv6       Certificate request FI B ipv6 address
ip              Certificate request ip address
ipv6            Certificate request ipv6 address
locality        Locality name (eg, city)
org-name        Organisation name (eg, company)
org-unit-name   Organisational Unit Name (eg, section)
password        Certificate request password
state           State, province or county (full name)
subject-name    Certificate request subject name

firepower /security/keyring/certreq* # set
```

関連コマンド

コマンド	説明
delete certreq	既存のキーリング認証要求を削除します。
set (certreq)	キーリング認証要求関連の情報を設定します。

create class

統計情報のしきい値ポリシーに新しいクラスの統計情報を追加するには、**create class** コマンドを使用します。名前が指定されたクラスがすでに存在する場合、コマンドは失敗します。

統計情報クラスを追加または編集するには、**enter class** コマンドを使用します。指定されたクラスが存在しない場合は、作成されて入力されます。クラスが存在する場合は、そのクラスが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のクラスを入力し、プロパティを割り当てまたは変更することもできます。通常、オブジェクトの「調査」は入力するよりも簡単です。これは、オブジェクトの名前がすべて必要になるため、このコマンドの **enter** 形式では、すべての定義パラメータを入力する必要があります。

既存のクラスの統計情報を削除するには、このコマンドの **delete** 形式を使用します。

```
create class type
delete class type
enter class type
scope class type
```

構文の説明

type

任意の統計情報クラスを指定します。

利用可能なクラスは、現在のモードの統計情報のしきい値ポリシーによって異なります。たとえば、eth-server/ モードの場合、利用可能なクラスは chassis-stats および ether-error-stats があります。eth-uplink/ モードの場合、利用可能なクラスは ether-rx-stats および ether-rx-stats があります。org/ モードの場合、利用可能なクラスは cpu-env-stats および ethernet-port-err-stats です。

現在の統計情報のしきい値ポリシーで利用可能なクラスのリストを表示するには、**create class ?** コマンドを使用します。

コマンドモード

```
scope eth-server/scope stats-threshold-policy/
scope eth-uplink/scope stats-threshold-policy/
scope org/scope stats-threshold-policy/
```

コマンド履歴

リリース

変更内容

1.1(1)

コマンドが追加されました。

使用上のガイドライン

特定の統計情報セットに対してしきい値を設定するには、クラスを使用します。たとえば、ドロップされたパケットの平均数が特定の量を超えた場合に障害を出すしきい値をポートで定義できます。このクラスでは、イーサネット エラー統計情報のしきい値プロパティを作成します。

統計情報しきい値ポリシーには複数のクラスを設定できます。

set collection-interval コマンドを使用して、統計情報を収集する頻度を定義し、**set reporting-interval** コマンドを使用して、統計情報を報告する頻度を定義します。これらの間隔で統計情報収集ポリシーが定義されます。



- (注) イーサネット サーバポートまたはイーサネット アップリンク ポートごとにデフォルトの統計情報しきい値ポリシーが1つあります。追加の統計情報収集ポリシーは作成できません。また、このコンポーネントの既存のデフォルト ポリシーを削除できません。デフォルト ポリシーを変更するだけです。ただし、組織モード (scope org/) では統計情報のしきい値ポリシーを作成および削除できます。

例

次の例では、イーサネットサーバの統計情報しきい値ポリシークラスを調査し、シャーシ統計情報クラスを作成し、入力電力 (W) プロパティを作成し、通常電力を 8kW に指定し、通常超えの警告しきい値 11 kW を作成し、クラスをコミットする方法を示します。

```
firepower # scope eth-server
firepower /eth-server # scope stats-threshold-policy default
firepower /eth-server/stats-threshold-policy # create class chassis-stats
firepower /eth-server/stats-threshold-policy/class* # create property input-power
firepower /eth-server/stats-threshold-policy/class/property* # set normal-value 8000.0
firepower /eth-server/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* # set
escalating 11000.0
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* #
commit-buffer
firepower /eth-server/stats-threshold-policy/class/property/threshold-value #
```

次の例では、組織モードを調査し、サーバとサーバコンポーネント統計情報に新しい統計情報しきい値ポリシーを作成し、CPU 環境統計情報のしきい値ポリシークラスを作成し、CPU 温度プロパティを作成し、通常の CPU 温度を摂氏 48.5 度に指定し、通常超えの警告しきい値を摂氏 50 度に作成し、トランザクション全体をコミットする方法を示します。

```
firepower # scope org
firepower /org # create stats-threshold-policy ServStatsPolicy
firepower /org/stats-threshold-policy* # create class cpu-env-stat
firepower /org/stats-threshold-policy/class* # create property temperature
firepower /org/stats-threshold-policy/class/property* # set normal-value 48.5
firepower /org/stats-threshold-policy/class/property* # create threshold-value above-normal
warning
firepower /org/stats-threshold-policy/class/property/threshold-value* # set escalating
50.0
firepower /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /org/stats-threshold-policy/class/property/threshold-value #
```

関連コマンド

コマンド	説明
------	----

コマンド	説明
delete class	統計情報の既存のクラスを削除します。
enter class	統計情報クラスを入力します。クラスが存在しない場合は、クラスが作成されます。
enter property	統計情報のクラスにプロパティを入力または作成します。
scope stats-threshold-policy	stats-threshold-policy ポリシー モードを開始します。このモードでは、特定の統計情報クラスを管理します。

create connection

新しい IPSec 接続を追加するには、**create connection** コマンドを使用します。名前が指定された接続がすでに存在する場合、コマンドは失敗します。

IPSec 接続を追加または編集するには、**enter connection** コマンドを使用します。指定された接続が存在しない場合は、作成されて入力されます。接続が存在する場合は、その接続が入力されます。

また、このコマンドの **scope** 形式を使用して、既存の接続を入力し、プロパティを割り当てまたは変更することもできます。通常、オブジェクトの「調査」は入力するよりも簡単です。これは、オブジェクトの名前がすべて必要になるため、このコマンドの **enter** 形式では、すべての定義パラメータを入力する必要があります。

既存の接続を削除するには、このコマンドの **delete** 形式を使用します。

create connection *name*

enter connection *name*

delete connection *name*

scope connection *name*

構文の説明	<i>name</i>	接続名には 16 文字以内の英数字を使用できます。
コマンドモード	scope security/scope ipsec/	
コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン 新しい IPSec 接続を作成すると、新しい接続はまだコミットされていないことを示すアスタリスクが付いた security/ipsec/connection モードが自動的に開始されます。接続はコミットする前に設定できます。

接続を作成すると、名前を変更することはできません。接続を削除し、新しい接続を作成する必要があります。

例

次の例では、新しい IPSec 接続を作成して入力する方法を示します。

```
firepower # scope security
firepower /security # scope ipsec
firepower /security/ipsec # enter connection ipsec_conn2
firepower /security/ipsec/connection* #
```

関連コマンド	コマンド	説明
	set adminstate	IPSec 接続の管理状態を有効または無効に設定します。
	show connection	現在の IPSec 接続情報を表示します。

create destination

新しい Smart Call Home の宛先を追加するには、**create destination** コマンドを使用します。名前が指定された宛先がすでに存在する場合、コマンドは失敗します。

Smart Call Home の宛先を追加または編集するには、**enter destination** コマンドを使用します。指定された宛先が存在しない場合は、作成されて入力されます。宛先が存在する場合は、その宛先が入力されます。

また、このコマンドの **scope** 形式を使用して、既存の宛先を入力し、プロパティを割り当てまたは変更することもできます。通常、オブジェクトの「調査」は入力するよりも簡単です。これは、オブジェクトの名前がすべて必要になるため、このコマンドの **enter** 形式では、すべての定義パラメータを入力する必要があります。

既存の宛先を削除するには、このコマンドの **delete** 形式を使用します。

create destination *name*

delete destination *name*

enter destination *name*

scope destination *name*

構文の説明	<i>name</i>	Smart Call Home 宛先を識別する名前。
コマンドモード	scope monitoring/scope callhome/scope profile/	
コマンド履歴	リリース	変更内容
	1.4(1)	コマンドが追加されました。

使用上のガイドライン 新しい Smart Call Home 宛先を作成すると、新しい宛先がまだコミットされていないことを示すアスタリスクが付いた **callhome/profile** モード (**monitoring/callhome/profile**) が自動的に開始されます。宛先パラメータ (トランスポート プロトコルと電子メールアドレス) を設定してから、新しい宛先情報をコミットできます。



(注) **callhome** プロファイルで許可されている唯一の宛先アドレスは電子メールアドレスです。

Smart Call Home 宛先を作成すると、宛先名を変更することはできません。宛先を削除し、新しい宛先を作成する必要があります。

例

次の例では、Smart Call Home 宛先を作成、入力、および設定する方法を示します。

```
firepower # scope monitoring
firepower /monitoring # scope callhome
```

create destination

```

firepower /monitoring/callhome # scope profile SLProfile
firepower /monitoring/callhome/profile # enter destination TestDest
firepower /monitoring/callhome/profile/destination* # set address user1@test.com
firepower /monitoring/callhome/profile/destination* # set protocol email
firepower /monitoring/callhome/profile/destination* # commit-buffer
firepower /monitoring/callhome/profile/destination #

```

関連コマンド

コマンド	説明
delete destination	既存の Smart Call Home 宛先を削除します。
enter destination	Smart Call Home 宛先を入力します。
set address	Smart Call Home 宛先の電子メール アドレスを設定します。
set protocol	Smart Call Home 宛先のトランスポート プロトコルを設定します。

create dns

FXOS で DNS ネームサーバーを作成するには、**create dns** コマンドを使用します。

create dns

構文の説明	create dns	このコマンドは、FXOS で DNS ネームサーバーを作成するために使用されます。
コマンドモード	scope system/scope services	
コマンド履歴	リリース 変更内容 1.1(1) コマンドが追加されました。	
使用上のガイドライン	デフォルトでは、このコマンドは FXOS に DNS ネームサーバーを作成します。	

例

次の例は、DNS ネームサーバーを作成する方法を示しています。

```
firepower# scope system; scope services  
firepower /system /services # create dns 192.0.2.1  
firepower /system /services* # commit
```

create hw-crypto

コンテナインスタンスの TLS 暗号化アクセラレーション 設定を作成するには、**create hw-crypto** コマンドを使用します。TLS 暗号化アクセラレーションに関する詳細については、*Management Center* コンフィギュレーション ガイドを参照してください。

create hw-crypto

コマンドモード

connect module

コマンド履歴

リリース	変更内容
2.7.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、コンテナインスタンスの TLS 暗号化アクセラレーション 設定を削除できます。コンテナインスタンスで TLS 暗号化アクセラレーション が有効になっている場合、このコマンドを使用すると、設定は、削除される前に無効になります。

例

次に、TLS 暗号化アクセラレーション 設定を作成する例を示します。

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

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
Version	Deploy Type	Turbo Mode	Profile Name	Cluster State	Cluster	Role
ftd	FTD-FDM	1	Enabled	Online	6.5.0.1159	6.5.0.1159
	Native	No		Not Applicable	None	
ftd	ftd2	2	Enabled	Online	6.5.0.1159	6.5.0.1159
	Container	No	Default-Small	Not Applicable	None	

```
/ssa # sc slot 2
/ssa/slot # scope app-instance ftd ftd2
/ssa/slot/app-instance # create hw-crypto
/ssa/slot/app-instance* # commit-buffer
```

関連コマンド

コマンド	説明
delete hw-crypto	コンテナインスタンスの TLS 暗号化アクセラレーション 設定を削除します。
scope hw-crypto	コンテナインスタンスの TLS 暗号化アクセラレーション 設定を有効または無効にします。
show hw-crypto	コンテナインスタンスの TLS 暗号化アクセラレーション 設定のステータスを表示します。

create ip-block

サービスアクセスにIPv4アドレスの新しいブロックを追加するには、**create ip-block** コマンドを使用します。プロパティが指定されたアドレスブロックがすでに存在する場合、コマンドは失敗します。

IPv4 アドレスのブロックを追加または編集するには、**enter ip-block** コマンドを使用します。指定されたアドレスブロックが存在しない場合は、作成されて入力されます。アドレスブロックが存在する場合は、そのブロックが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のアドレスブロックを入力し、プロパティを割り当てまたは変更することもできます。

既存のアドレス ブロックを削除するには、このコマンドの **delete** 形式を使用します。

```
create ip-block ip_address prefix_length {https|snmp|ssh}
delete ip-block ip_address prefix_length {https|snmp|ssh}
enter ip-block ip_address prefix_length {https|snmp|ssh}
scope ip-block ip_address prefix_length {https|snmp|ssh}
```

構文の説明

<i>ip_address</i>	IPv4 アドレス ブロックの開始アドレス。
<i>prefix_length</i>	プレフィックス長。ブロック内のアドレスの数を決定します。値は 0 ~ 32 です。
https snmp ssh	アドレスブロックが割り当てられるサービス (HTTPS、SNMP、または SSH)。

コマンドモード

scope system/scope services/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、IPv4アドレスのブロックを割り当て、指定されたサービス (HTTPS、SNMP、または SSH) にアクセスできます。

新しい IP ブロックを作成すると、新しいブロック割り当てがまだコミットされていないことを示すアスタリスクが付いた **ip-block** モード (system/services/ip-block) が自動的に入力されません。

FXOS バージョン 2.3.1 以前では、サービスごとに最大 25 個の異なるブロックを設定できます。FXOS バージョン 2.4.1 以降では、サービスごとに最大 100 個の異なるブロックを設定できます。アドレスを 0.0.0.0、プレフィックスを 0 と指定すると、サービスに無制限にアクセスできるようになります。アドレスの各ブロックは、自身の開始 IPv4 アドレスによって識別されます。

例

次の例では、IPv4アドレスブロックを作成、入力、および確認し、SSHにアクセスする方法を示します。

```
firepower # scope system
firepower /system # scope services
firepower /system/services # enter ip-block 192.168.200.101 32 ssh
firepower /system/services/ip-block* # commit-buffer
firepower /system/services/ip-block # up
firepower /system/services # show ip-block
```

```
Permitted IP Block:
  IP Address      Prefix Length Protocol
  -----
  0.0.0.0         0 https
  0.0.0.0         0 snmp
  0.0.0.0         0 ssh
  192.168.200.101 32 ssh
firepower /system/services #
```

関連コマンド

コマンド	説明
create ipv6-block	IPv6 アドレス ブロックを作成します。
delete ip-block	既存の IPv4 ブロックを削除します。

create ipv6-block

サービスアクセスにIPv6アドレスの新しいブロックを追加するには、**create ipv6-block** コマンドを使用します。プロパティが指定されたアドレスブロックがすでに存在する場合、コマンドは失敗します。

IPv6アドレスのブロックを追加または編集するには、**enter ipv6-block** コマンドを使用します。指定されたアドレスブロックが存在しない場合は、作成されて入力されます。アドレスブロックが存在する場合は、そのブロックが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のアドレスブロックを入力し、プロパティを割り当てまたは変更することもできます。

既存のアドレスブロックを削除するには、このコマンドの **delete** 形式を使用します。

```
create ipv6-block ipv6_address prefix_length {https|snmp|ssh}
delete ipv6-block ipv6_address prefix_length {https|snmp|ssh}
enter ipv6-block ipv6_address prefix_length {https|snmp|ssh}
scope ipv6-block ipv6_address prefix_length {https|snmp|ssh}
```

構文の説明

<i>ipv6_address</i>	IPv6 アドレス ブロックの開始アドレス。
<i>prefix_length</i>	プレフィックス長。ブロック内のアドレスの数を決定します。値は 0 ~ 128 です。
https snmp ssh	アドレスブロックが割り当てられるサービス (HTTPS、SNMP、または SSH)。

コマンドモード

scope system/scope services/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、IPv6アドレスのブロックを割り当て、指定されたサービス (HTTPS、SNMP、または SSH) にアクセスできます。

新しい IPv6 ブロックを作成すると、新しいブロック割り当てがまだコミットされていないことを示すアスタリスクが付いた **ipv6-block** モード (`system/services/ipv6-block`) が自動的に入力されます。

FXOS バージョン 2.3.1 以前では、サービスごとに最大 25 個の異なるブロックを設定できます。FXOS バージョン 2.4.1 以降では、サービスごとに最大 100 個の異なるブロックを設定できます。アドレスを `0:0:0:0:0:0:0`、プレフィックスを `0` と指定すると、サービスに無制限にアクセスできるようになります。アドレスの各ブロックは、自身の開始 IPv6 アドレスによって識別されます。

例

次の例では、IPv6アドレスブロックを作成、入力、および確認し、SSHにアクセスする方法を示します。

```
firepower # scope system
firepower /system # scope services
firepower /system/services # create ipv6-block 2001:DB8:1::1 64 ssh
firepower /system/services/ipv6-block* # commit-buffer
firepower /system/services/ipv6-block # up
firepower /system/services # show ipv6-block
```

```
Permitted IPv6 Block:
  IPv6 Address Prefix Length Protocol
  -----
  ::                      0 https
  ::                      0 snmp
  ::                      0 ssh
  2001:DB8:1::1
                          64 ssh
firepower /system/services #
```

関連コマンド

コマンド	説明
create ip-block	IPv4 ブロックを作成します。
delete ipv6-block	既存の IPv6 ブロックを削除します。

create keyring

新しい RSA キーリングを追加するには、**create keyring** コマンドを使用します。名前が指定されたキーリングがすでに存在する場合、コマンドは失敗します。

既存のキーリングを編集するには、**enter keyring** コマンドを使用します。

また、このコマンドの **scope** 形式を使用して、既存のキーリングを入力し、プロパティを割り当てまたは変更することもできます。

既存のキーリングを削除するには、このコマンドの **delete** 形式を使用します。

create keyring *name*

delete keyring *name*

enter keyring *name*

scope keyring *name*

構文の説明	<i>name</i>	キーリングを識別する名前には、1～16文字を使用できます。
コマンドモード	scope security/	
コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン 新しいキーリングを作成すると、新しいキーリングがまだコミットされていないことを示すアラートが付いた **keyring** モード (**security/keyring**) が自動的に開始されます。キーリング認証要求を作成し、RSA キー係数や認証局トラストポイントなどのキーリングパラメータを設定して、新しいキーリング情報をコミットすることができます。

例

次の例では、新しい RSA キーリングを作成して入力する方法を示します。

```
firepower # scope security
firepower /security # enter keyring test_keyring
firepower /security/keyring* # set ?
    cert          Keyring certificate
    modulus       RSA key modulus
    regenerate    Regenerate keyring
    trustpoint    Trustpoint CA

firepower /security/keyring* # set
```

関連コマンド	コマンド	説明
	delete keyring	既存の RSA キーリングを削除します。

create local-user

新しいローカルユーザアカウントを追加するには、**create local-user** コマンドを使用します。名前が指定されたローカルユーザアカウントがすでに存在する場合、コマンドは失敗します。

ローカルユーザアカウントを追加または編集するには、**enter local-user** コマンドを使用します。指定されたアカウントが存在しない場合は、作成されて入力されます。アカウントが存在する場合は、そのクラスが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のローカルユーザアカウントを入力し、プロパティを割り当てまたは変更することもできます。

既存のローカルユーザアカウントを削除するには、このコマンドの **delete** 形式を使用します。

create local-user *user_name*

delete local-user *user_name*

enter local-user *user_name*

scope local-user *user_name*

構文の説明

user_name

このローカルユーザアカウントにログインする場合に使用される ID。ユーザ名を入力する場合は、次のガイドラインおよび制限事項に留意してください。

- 名前には、次を含む 1 ~ 32 文字を使用できます。
 - 任意の英字
 - 任意の数字
 - _ (アンダースコア)
 - - (ダッシュ)
 - . (ドット)
- 名前は一意である必要があります。
- 名前の先頭を英字にする必要があります。アンダースコアなどの特殊文字や数字から始めることはできません。
- 名前では、大文字と小文字が区別されます。
- すべて数字の名前を作成することはできません。

ユーザアカウントの作成後は、その名前を変更できません。ユーザアカウントを削除し、新しいユーザアカウントを作成する必要があります。

コマンドモード

scope security/

コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン 最大48のローカルユーザアカウントを設定できます。各アカウントには、一意のユーザ名とパスワードが必要です。

新しいユーザアカウントを作成すると、新しいアカウントがまだコミットされていないことを示すアスタリスクが付いた **local user** モード (`/security/local-user`) が自動的に開始されます。パスワードや姓名など、追加のユーザアカウント情報を指定してから、新しいアカウント情報をコミットすることができます。

ユーザアカウントの作成後は、アカウント名を変更できません。ユーザアカウントを削除し、新しいユーザアカウントを作成する必要があります。

例

次の例では、セキュリティモードを開始し、ローカルユーザアカウントを入力し（存在しないために新しいアカウントを同時に作成）、アカウントに姓と名を割り当てる方法を示します。

```
firepower # scope security
firepower /security # enter local-user test_user
firepower /security/local-user* # set firstname test
firepower /security/local-user* # set lastname user
firepower /security/local-user* # commit-buffer
firepower /security/local-user #
```

関連コマンド	コマンド	説明
	delete local-user	既存のローカルユーザアカウントを削除します。
	set expiration	ユーザアカウントが期限切れになる日付を指定します。
	set password	ユーザアカウントのパスワードを設定します。

create member-port

ポートチャネルメンバーポートを作成するには、**create member-port** コマンドを使用します。指定された ID を持つメンバーポートがすでに存在している場合、コマンドは失敗します。

メンバーポートを追加または開始するには、**enter member-port** コマンドを使用します。指定されたメンバーポートが存在しない場合は、作成されて開始されます。メンバーポートが存在する場合は、そのポートが開始されます。

また、このコマンドの **scope** 形式を使用して、既存のメンバーポートを入力し、プロパティを割り当てまたは変更することもできます。

既存のメンバーポートを削除するには、このコマンドの **delete** 形式を使用します。

create member-port *interface_id*

構文の説明	<i>interface_id</i>	次のいずれかの形式を使用して、このポートチャネルに追加するインターフェイスを特定します。 <ul style="list-style-type: none"> • <i>slot_id port_id</i> : スロット番号とポート番号で表されるシャーシ内のポートの場所。 • Ethernetslot_idport_id : イーサネットポートラベル。
コマンドモード	scope eth-uplink/scope fabric a/port-channel	
コマンド履歴	リリース	変更内容
	1.1.1	コマンドが追加されました。

使用上のガイドライン このコマンドを使用する前に、ポートチャネルを作成または入力する必要があります。

新しいメンバーポートを作成すると、新しいメンバーポートがまだコミットされていないことを示すアスタリスクが付いたメンバーポートモード (**eth-uplink/fabric/port-channel/member-port**) が自動的に開始されます。

例

次の例は、新しいポートチャネルを作成し、それを有効にしてメンバーポートを追加する方法を示しています。

```
firepower # scope eth-uplink
firepower /eth-uplink/fabric # scope fabric a
firepower /eth-uplink/fabric # create port-channel 4
firepower /eth-uplink/fabric/port-channel* # enable
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
```

```
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

関連コマンド

コマンド	説明
create port-channel	新しい EtherChannel (ポートチャネル) を作成します。

create ntp-server

FXOS で NTP サーバーを作成するには、**create ntp-server** コマンドを使用します。

create ntp-server

構文の説明	create ntp-server	このコマンドは、FXOS で NTP サーバーを作成するために使用されます。
コマンドモード	scope system/scope services/	
コマンド履歴	リリー	変更内容
	1.1(1)	コマンドが追加されました。
使用上のガイドライン	デフォルトでは、このコマンドは FXOS に NTP サーバーを作成します。	

例

次の例は、NTP サーバーを作成する方法を示しています。

```
firepower# scope system;scope services

firepower /system/services # create ntp-server 192.0.2.1
firepower /system/services # commit

firepower /system/services/ntp-server # set
ntp-sha1-key-id      NTP SHA-1 key id      <===== [Optional] Configure NTP
authentication key ID
ntp-sha1-key-string NTP SHA-1 key string  <===== [Optional] Configure NTP
authentication key string

firepower /system/services/ntp-server # commit
```

関連コマンド	コマンド	説明
	show ntp-server	このコマンドは、NTP サーバーを表示します。

create policy (callhome)

新しい Smart Call Home およびスマート ライセンス ポリシーを追加するには、**create policy** コマンドを使用します。名前が指定されたポリシーがすでに存在する場合、コマンドは失敗します。

IPSec 接続を追加または編集するには、**enter policy** コマンドを使用します。指定されたポリシーが存在しない場合は、作成されて入力されます。ポリシーが存在する場合は、そのポリシーが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のポリシーを入力し、プロパティを割り当てまたは変更することもできます。

既存のポリシーを削除するには、このコマンドの **delete** 形式を使用します。

create policy *event*

delete policy *event*

enter policy *event*

scope policy *event*

構文の説明	<i>event</i>	障害またはシステムイベントのタイプ。イベントのオプションについては、次の使用ガイドラインを参照してください。
コマンドモード	scope monitoring/scope callhome/	
コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン 新しい Smart Call Home ポリシーを作成すると、新しいポリシーがまだコミットされていないことを示すアスタリスクが付いた **callhome/policy** モード (**monitoring/callhome/policy**) が自動的に開始されます。プロパティ値を設定し、サービスを有効/無効にしてから、新しいポリシーをコミットすることができます。

Smart Call Home ポリシーを作成した後は、ポリシー名を変更することはできません。ポリシーを削除し、新しいポリシーを作成する必要があります。

このコマンドを使用して、既存の障害またはシステムイベントの種類に対するポリシーのインスタンスを作成します。Call Home ポリシーのイベントタイプに使用できるキーワードは次のとおりです。

- adaptor-mismatch
- arp-targets-config-error
- association-failed
- configuration-failure
- connectivity-problem

- election-failure
- equipment-degraded
- equipment-disabled
- equipment-inaccessible
- equipment-inoperable
- equipment-offline
- equipment-problem
- equipment-removed
- fru-problem
- health-led-amber
- health-led-amber-blinking
- identity-unestablishable
- inventory-failed
- license-graceperiod-expired
- limit-reached
- link-down
- management-services-failure
- management-services-unresponsive
- memory-error
- mgmtif-down
- ndisc-targets-config-error
- near-max-limit
- port-failed
- power-problem
- psu-insufficient
- psu-mixed-mode
- thermal-problem
- version-incompatible
- vif-ids-mismatch
- voltage-problem

例

次の例では、link-down イベントの Call Home ポリシー インスタンスを作成、入力、および有効にする方法を示します。

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # enter policy link-down
firepower /monitoring/callhome/policy* # set admin-state enabled
firepower /monitoring/callhome/policy* # commit-buffer
firepower /monitoring/callhome/policy #
```

関連コマンド

コマンド	説明
delete policy	既存の Smart Call Home ポリシーを削除します。
set admin-state	Smart Call Home ポリシー用のポリシーの管理状態を有効または無効にします。

create policy (flow control)

新しい名前付きフロー制御ポリシーを追加するには、**create policy** コマンドを使用します。名前が指定されたポリシーがすでに存在する場合、コマンドは失敗します。

名前付きフロー制御ポリシーを追加または編集するには、**enter policy** コマンドを使用します。指定されたポリシーが存在しない場合は、作成されて入力されます。ポリシーが存在する場合は、そのポリシーが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のポリシーを入力し、プロパティを割り当てまたは変更することもできます。

既存のポリシーを削除するには、このコマンドの **delete** 形式を使用します。

create policy *name*

delete policy *name*

enter policy *name*

scope policy *name*

構文の説明	<i>name</i>	フロー制御ポリシーを識別するための名前。名前には 1 ~ 16 文字を使用できます。
コマンドモード	scope eth-uplink/scope flow-control/	
コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン

フロー制御ポリシーは、ポートの受信バッファがいっぱいになったときに、アプライアンスドメインのアップリンクイーサネットポートが IEEE 802.3x ポーズフレームを送信および受信するかどうかを決定します。これらのポーズフレームは、バッファがクリアされるまでの数ミリ秒間、送信側ポートからのデータの送信を停止するように要求します。デバイス間でフロー制御が行われるようにするには、両方のデバイスで、対応する送信および受信フロー制御パラメータを有効にする必要があります。

デフォルトのフロー制御ポリシーは、送受信の制御を無効にし、自動ネゴシエーションに優先順位を設定します。

新しいフロー制御ポリシーを作成すると、新しいポリシーがまだコミットされていないことを示すアスタリスクが付いたフロー制御/ポリシーモード (**eth-uplink/flow-control/policy**) が自動的に開始されます。ポリシープロパティ値を設定し、新しいポリシーをコミットすることができます。

フロー制御ポリシーを作成した後にポリシー名を変更することはできません。ポリシーを削除し、新しいポリシーを作成する必要があります。

例

次の例は、フロー制御の名前付きポリシーを作成する方法を示しています。

```
firepower # scope eth-uplink
firepower /eth-uplink # scope flow-control
firepower /eth-uplink/flow-control # enter policy FCpolicy1
firepower /eth-uplink/flow-control/policy* # commit-buffer
firepower /eth-uplink/flow-control/policy #
```

関連コマンド

コマンド	説明
delete policy	既存のフロー制御ポリシーを削除します。
set	フロー制御/ポリシーモードで、フロー制御ポリシーのプロパティを設定します。
show policy	フロー制御ポリシーのプロパティ値を表示します。

create port-channel

EtherChannel（ポートチャネルとも呼ばれる）を作成するには、**create port-channel** コマンドを使用します。指定された ID を持つポートチャネルがすでに存在している場合、コマンドは失敗します。

ポートチャネルを追加または開始するには、**enter port-channel** コマンドを使用します。指定されたポートチャネルが存在しない場合は、作成されて入力されます。ポートチャネルが存在する場合は、そのポートチャネルが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のポートチャネルを入力し、プロパティを割り当てまたは変更することもできます。

既存のポートチャネルを削除するには、このコマンドの **delete** 形式を使用します。

create port-channelid

構文の説明	<i>id</i>	このポートチャネルに ID 番号を割り当てます。
コマンドモード	scope eth-uplink/scope fabric a/	
コマンド履歴	リリース	変更内容
	1.1.1	コマンドが追加されました。

使用上のガイドライン 新しいポートチャネルを作成すると、新しいポートチャネルがまだコミットされていないことを示すアスタリスクが付いたポートチャネルモード（eth-uplink/fabric/port-channel）が自動的に開始されます。ポートチャネルパラメータを設定してから、新しいポートチャネルをコミットできます。

新しいポートチャネルを作成したら、それを有効にして、メンバーポートを追加します。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止 (Suspended)] 状態になり、物理リンクがアップしても論理デバイスに割り当てられるまでそのままになります。EtherChannel は次のような状況でこの [一時停止 (Suspended)] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理ポートとして追加された。
- EtherChannel がクラスタの一部である論理デバイスの管理または CCL ポートとして追加された。
- EtherChannel がデータがクラスタの一部である論理デバイスのデータポートとして追加され、また少なくとも 1 つのセキュリティモジュールがクラスタに参加している。

EtherChannel は論理デバイスに割り当てられるまで動作しないことに注意してください。EtherChannel が論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止 (Suspended)] 状態に戻ります。



- (注) Firepower 4100/9300 シャーシは、アクティブ Link Aggregation Control Protocol (LACP) モードでのみ EtherChannel をサポートします。最適な互換性を得るために、接続スイッチポートをアクティブモードに設定することを推奨します。

例

次の例は、新しいポートチャネルを作成し、それを有効にしてメンバーポートを追加する方法を示しています。

```
firepower # scope eth-uplink
firepower /eth-uplink/fabric # scope fabric a
firepower /eth-uplink/fabric # create port-channel 4
firepower /eth-uplink/fabric/port-channel* # enable
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
firepower /eth-uplink/fabric/port-channel/member-port* # exit
firepower /eth-uplink/fabric/port-channel* # commit-buffer
firepower /eth-uplink/fabric/port-channel #
```

関連コマンド

コマンド	説明
create member-port	ポートチャネルにメンバーポートを追加します。
set (port-channel)	既存のポートチャネルのパラメータを設定または変更します。

create pre-login-banner

ログイン画面の前に表示されるバナーを作成するには、**create pre-login-banner** コマンドを使用します。ログイン前バナーがすでに存在する場合、コマンドは失敗します。

ログイン前バナーを追加または編集するには、**enter pre-login-banner** コマンドを使用します。バナーが存在しない場合は、作成されて入力されます。バナーが存在する場合は、そのバナーが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のバナーを入力し、メッセージを設定またはクリアすることもできます。

既存のバナーを削除するには、このコマンドの **delete** 形式を使用します。

create pre-login-banner

構文の説明	このコマンドには引数またはキーワードはありません。				
コマンドモード	scope security/scope banner/				
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>1.1(1)</td> <td>コマンドが追加されました。</td> </tr> </tbody> </table>	リリース	変更内容	1.1(1)	コマンドが追加されました。
リリース	変更内容				
1.1(1)	コマンドが追加されました。				

使用上のガイドライン 新しいログイン前バナーを作成すると、最初は空白になり、バナーがまだ指定およびコミットされていないことを示すアスタリスクが付いた **pre-login-banner** モード (**security/banner/pre-login-banner**) が自動的に開始されます。

ログイン前バナー テキストを入力するには、**set message** コマンドを使用します。バナーメッセージを終了するには、ENDOFBUF (すべて大文字) と入力する必要があります。

このコマンドを入力したときにログイン前バナーがすでに存在する場合、コマンドは失敗し、「Error: Managed object already exists」というメッセージが表示されます。

例

次の例は、ログイン前バナーを作成および指定し、コミットおよび表示する方法を示します。

```
firepower # scope security
firepower /security # scope banner
firepower /security/banner # create pre-login-banner
firepower /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Firepower-9300-2
>Western Data Center
>ENDOFBUF
firepower /security/banner/pre-login-banner* # commit
firepower /security/banner/pre-login-banner # show
```

```
Pre login banner:
  Message
  -----
  Firepower-9300-2
  Western Data Center

firepower /security/banner/pre-login-banner #
```

関連コマンド

コマンド	説明
clear message	既存のログイン前バナーからテキストを削除します。実際のバナーオブジェクト自体は削除されません。
set message	ログイン前バナーとして表示されるテキスト行を指定します。

create profile

新しい Smart Call Home およびスマートライセンスの宛先プロファイルを追加するには、**create profile** コマンドを使用します。名前が指定されたプロファイルがすでに存在する場合、コマンドは失敗します。

宛先プロファイルを追加または編集するには、**enter profile** コマンドを使用します。指定されたプロファイルが存在しない場合は、作成されて入力されます。プロファイルが存在する場合は、そのプロファイルが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のプロファイルを入力し、プロパティを割り当てまたは変更することもできます。プロファイルが存在しない場合、コマンドは失敗します。

既存のプロファイルを削除するには、このコマンドの **delete** 形式を使用します。

```
create profile name
delete profile name
enter profile name
scope profile name
```

構文の説明	<i>name</i>	宛先プロファイルを識別する名前。
コマンドモード	scope monitoring/scope callhome/	
コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン 新しい Smart Call Home プロファイルを作成すると、新しいプロファイルがまだコミットされていないことを示すアスタリスクが付いた `callhome/profile` モード (`monitoring/callhome/profile`) が自動的に開始されます。プロファイルを定義して、新しいプロファイル情報をコミットすることができます。

Smart Call Home の宛先プロファイルを作成すると、プロファイル名を変更することはできません。プロファイルを削除し、新しいプロファイルを作成する必要があります。

例

次の例は、Smart Call Home の宛先プロファイルを作成および入力する方法を示しています。

```
firepower # scope monitoring
firepower /monitoring # scope callhome
firepower /monitoring/callhome # enter profile TestProfile
firepower /monitoring/callhome/profile* # commit-buffer
firepower /monitoring/callhome/profile #
```


関連コマンド	コマンド	説明
	delete profile	既存の Smart Call Home の宛先プロファイルを削除します。
	set	monitoring/callhome モードで、プロファイルプロパティを設定します。
	show profile	現在定義されている Smart Call Home とスマート ライセンシングのプロファイルをリストします。monitoring/callhome モードで使用できます。

create property

ネットワーク統計情報のしきい値ポリシークラスに新しいプロパティを追加するには、**create property** コマンドを使用します。名前が指定されたプロパティがすでに存在する場合、コマンドは失敗します。

統計情報のしきい値プロパティを追加または編集するには、**enter property** コマンドを使用します。指定されたプロパティが存在しない場合は、作成されて入力されます。プロパティが存在する場合は、そのプロパティが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のプロパティを入力し、パラメータを割り当てまたは変更することもできます。通常、オブジェクトの「調査」は入力するよりも簡単です。これは、オブジェクトの名前がすべて必要になるため、このコマンドの **enter** 形式では、すべての定義パラメータを入力する必要があります。

既存のプロパティを削除するには、このコマンドの **delete** 形式を使用します。

create property *property-name*

delete property *property-name*

enter property *property-name*

scope property *property-name*

構文の説明

property-name

任意の統計情報プロパティを指定します。

利用可能なプロパティは、現在のモードと定義された統計情報のクラスによって異なります。たとえば、eth-server モードの chassis-stats クラスの場合、input-power および output-power オプションが使用できます。eth-uplink モードの ether-rx-stats クラスの場合、broadcast-packets-delta や total-bytes-delta などのプロパティが使用できます。

現在の統計情報のクラスで利用可能なプロパティのリストを表示するには、**create property ?** コマンドを使用します。

コマンドモード

scope eth-server/scope stats-threshold-policy/scope class/

scope eth-uplink/scope stats-threshold-policy/scope class/

scope org/scope stats-threshold-policy/scope class/

コマンド履歴

リリース

変更内容

1.1(1)

コマンドが追加されました。

使用上のガイドライン

特定の統計情報セットに対してしきい値を設定するには、クラスを使用します。プロパティを使用して、ポリシークラスの特定の値と統計情報のしきい値を定義します。たとえば、ドロップされたパケットの平均数が特定の量を超えた場合に障害を出すしきい値をポートで定義でき

ます。このクラスでは、イーサネットエラー統計情報クラスのしきい値プロパティを作成します。

ポリシー クラスには複数のプロパティを設定できます。



- (注) イーサネット サーバ ポートまたはイーサネット アップリンク ポートごとにデフォルトの統計情報しきい値ポリシーが1つあります。追加の統計情報収集ポリシーは作成できません。また、このコンポーネントの既存のデフォルト ポリシーを削除できません。デフォルト ポリシーを変更するだけです。ただし、組織モード (scope org/) では統計情報のしきい値ポリシーを作成および削除できます。

例

次の例は、デフォルトのイーサネットアップリンク統計情報のしきい値ポリシーを調査し、エラー統計情報クラスを作成し、巡回冗長検査 (CRC) エラーカウントプロパティを作成し、各ポーリング間隔の通常のCRCエラーカウントを1000に指定し、通常超えの警告しきい値1250を作成し、クラスをコミットする方法を示しています。

```
firepower # scope eth-uplink
firepower /eth-uplink # scope stats-threshold-policy default
firepower /eth-uplink/stats-threshold-policy # create class ether-error-stats
firepower /eth-uplink/stats-threshold-policy/class* # create property crc-delta
firepower /eth-uplink/stats-threshold-policy/class/property* # set normal-value 1000
firepower /eth-uplink/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value* # set
escalating 1250
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value* #
commit-buffer
firepower /eth-uplink/stats-threshold-policy/class/property/threshold-value #
```

関連コマンド

コマンド	説明
delete property	既存のプロパティを削除します。
enter property	クラスプロパティを入力します。プロパティが存在しない場合は、プロパティが作成されます。
enter property	統計情報のクラスにプロパティを入力または作成します。
scope property	プロパティモードを開始します。このモードでは、統計情報のクラスのプロパティを管理します。

create resource-profile

コンテナインスタンスで使用するリソースプロファイルを追加するには、**create resource-profile** コマンドを使用します。

create resource-profile *name*

構文の説明	<i>name</i>	プロファイルの名前を 1 ~ 64 文字で設定します。追加後にこのプロファイルの名前を変更することはできません。
コマンドモード	scope ssa/	
コマンド履歴	リリース	変更内容
	2.4(1)	コマンドが追加されました。

使用上のガイドライン コンテナインスタンスごとにリソース使用率を指定するには、1つまたは複数のリソースプロファイルを作成します。論理デバイス/アプリケーションインスタンスを展開するときに、使用するリソースプロファイルを指定します。リソースプロファイルはCPU コアの数を設定します。RAM はコアの数に従って動的に割り当てられ、ディスク容量はインスタンスごとに 40 GB に設定されます。

- コアの最小数は 6 です。
- 内部アーキテクチャにより 8 コアを指定することはできません。
- コアを偶数 (6、10、12、14 など) で最大値まで割り当てることができます。
- 利用可能な最大コア数は、セキュリティ モジュール/シャーシ モデルによって異なります。

シャーシには、「Default-Small」と呼ばれるデフォルトリソースプロファイルが含まれています。このコア数は最小です。このプロファイルの定義を変更したり、使用されていない場合には削除することもできます。シャーシをリロードし、システムに他のプロファイルが存在しない場合は、このプロファイルが作成されます。

使用中のリソースプロファイルの設定を変更することはできません。そのリソースプロファイルを使用しているすべてのインスタンスを無効にしてから、リソースプロファイルを変更し、最後にインスタンスを再度有効にする必要があります。確立されたハイ アベイラビリティ ペア内のインスタンスのサイズを変更する場合、できるだけ早くすべてのメンバを同じサイズにする必要があります。

Threat Defense インスタンスを Management Center に追加した後にリソース プロファイル設定を変更する場合は、**[Devices] > [Device Management] > [Device] > [System] > [Inventory]** ダイアログボックスで各ユニットのインベントリを更新します。

例

次の例では、3つのリソース プロファイルを追加します。

```
firepower# scope ssa
firepower /ssa # enter resource-profile basic
firepower /ssa/resource-profile* # set description "lowest level"
firepower /ssa/resource-profile* # set cpu-core-count 6
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile standard
firepower /ssa/resource-profile* # set description "middle level"
firepower /ssa/resource-profile* # set cpu-core-count 10
firepower /ssa/resource-profile* # exit
firepower /ssa # enter resource-profile advanced
firepower /ssa/resource-profile* # set description "highest level"
firepower /ssa/resource-profile* # set cpu-core-count 12
firepower /ssa/resource-profile* # commit-buffer
firepower /ssa/resource-profile #
```

関連コマンド

コマンド	説明
set cpu-count	リソース プロファイルの CPU の数を設定します。
set resource-profile-name	リソース プロファイルがアプリケーション インスタンスに割り当てられました。
show monitor detail	セキュリティ モジュール/エンジン スロットのリソース使用率を表示します。
show resource detail	アプリケーションインスタンスのリソース割り当てを表示します。
show resource-profile user-defined	リソース プロファイルの割り当てを表示します。

create server (scope ldap)

Lightweight Directory Access Protocol (LDAP) サーバーオブジェクトを作成するには、セキュリティ/LDAP モードで **create server** コマンドを使用します。名前が指定されたサーバーがすでに存在する場合、コマンドは失敗します。

LDAP サーバーを追加または編集するには、セキュリティ/LDAP モードで **enter server** コマンドを使用します。指定されたサーバーが存在しない場合は、作成されて入力されます。サーバーが存在する場合は、そのサーバーが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のサーバーを入力し、プロパティを割り当てまたは変更することもできます。

既存のサーバーを削除するには、このコマンドの **delete** 形式を使用します。

create server *id*

構文の説明	<i>id</i>	ホスト名、完全修飾ドメイン名 (FQDN)、または IP アドレス (IPv4 アドレスまたは IPv6 アドレスを使用可能) を使用して、サーバー ID を指定します。
コマンドモード	scope security/scope ldap/	
コマンド履歴	リリース	変更内容
	1.1.1	コマンドが追加されました。

使用上のガイドライン ホスト名または FQDN を使用してサーバー *ID* を指定する場合は、DNS サーバーも設定する必要があります。

SSL が有効の場合、サーバー *ID* は、LDAP サーバーのセキュリティ証明書内の Common Name (CN) と正確に一致している必要があります。

新しい LDAP サーバーを作成すると、新しいサーバーがまだコミットされていないことを示すアスタリスクが付いたセキュリティ/LDAP/サーバーモードが自動的に開始されます。サーバーはコミットする前に設定できます。



(注) FXOS では、最大 16 の LDAP プロバイダーをサポートします。

例

次に、新しい LDAP サーバーを作成し、トランザクションをコミットする例を示します。

```
firepower # scope security
firepower # scope ldap
```

```
firepower /security/ldap # create server 192.168.100.112  
Warning: LDAP server name has to be DNS name in Secure LDAP connection. It has to match  
the LDAP server certificate SAN field.  
firepower /security/ldap/server* # commit-buffer  
firepower /security/ldap/server #
```

関連コマンド

コマンド	説明
create ldap-group-rule	LDAP プロバイダー グループ ルール パラメータを作成します。
set	セキュリティ/LDAP/サーバーモードで、SSL の有効化/無効化などのさまざまな LDAP サーバー関連パラメータを設定します。

create snmp-trap

Simple Network Management Protocol (SNMP) のトラップ宛先を削除するには、**create snmp-trap** コマンドを使用します。名前が指定されたトラップがすでに存在する場合、コマンドは失敗します。

SNMP トラップを追加または編集するには、**enter snmp-trap** コマンドを使用します。指定されたトラップが存在しない場合は、作成されて入力されます。トラップが存在する場合は、そのトラップが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のトラップを入力し、プロパティを割り当てまたは変更することもできます。通常、オブジェクトの「調査」は入力するよりも簡単です。これは、オブジェクトの名前がすべて必要になるため、このコマンドの **enter** 形式では、すべての定義パラメータを入力する必要があります。

既存のトラップを削除するには、このコマンドの **delete** 形式を使用します。

create snmp-trap destination

構文の説明	<i>destination</i>	ホスト名または IP アドレス (IPv4 または IPv6 アドレスを指定可能) を使用して、トラップ宛先サーバを指定します。
コマンドモード	scope monitoring/	
コマンド履歴	リリース	変更内容
	1.1.1	コマンドが追加されました。

使用上のガイドライン SNMP (**enable snmp**) を有効にするには、事前に SNMP コミュニティ (**set snmp community**) を作成する必要があります。

新しい SNMP トラップを作成すると、新しいトラップがまだコミットされていないことを示すアスタリスクが付いた `monitoring/snmp-trap` モードが自動的に開始されます。



(注) 最大 8 つの SNMP トラップを作成できます。

例

次の例は、SNMP トラップを作成し、トランザクションをコミットする方法を示しています。

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-trap 192.168.100.112
firepower /monitoring/snmp-trap* # commit-buffer
```



```
firepower /monitoring/snmp-trap #
```

関連コマンド

コマンド	説明
enable snmp	SNMP を有効にします。
set snmp	SNMP 設定パラメータを設定します。これは、コミュニティ、SNMP を担当するシステム担当者、およびホストの場所です。

create snmp-user

新しい SNMPv3 ユーザを作成するには、**create snmp-user** コマンドを使用します。名前が指定されたユーザがすでに存在する場合、コマンドは失敗します。

SNMP ユーザを追加または編集するには、**enter snmp-user** コマンドを使用します。指定されたユーザが存在しない場合は、作成されて入力されます。ユーザが存在する場合は、そのユーザが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のユーザを入力し、プロパティを割り当てまたは変更することもできます。通常、オブジェクトの「調査」は入力するよりも簡単です。これは、オブジェクトの名前がすべて必要になるため、このコマンドの **enter** 形式では、すべての定義パラメータを入力する必要があります。

既存のユーザを削除するには、このコマンドの **delete** 形式を使用します。

create snmp-user *user_name*

構文の説明

<i>user_name</i>	SNMPv3 ユーザー名を指定します。最大 32 文字の英数字、アンダースコア (_)、ドット (.)、アットマーク (@)、およびダッシュ (-) を使用できます。
------------------	---

コマンドモード

scope monitoring/

コマンド履歴

リリース	変更内容
1.1.1	コマンドが追加されました。

使用上のガイドライン

SNMP (**enable snmp**) を有効にするには、SNMP ユーザを作成する前に SNMP コミュニティ (**set snmp community**) を作成する必要があります。

新しい SNMP ユーザを作成すると、そのユーザのパスワードを作成するように求められます。このパスワードの長さは 8 文字以上にする必要があります。パスワードは入力しても表示されません。

新しい SNMP ユーザを作成すると、新しいユーザがまだコミットされていないことを示すアスタリスクが付いた **monitoring/snmp-user** モードが自動的に開始されます。

例

次の例は、SNMPv3 ユーザを作成する方法を示しています。

```
firepower # scope monitoring
firepower /monitoring/ # enable snmp
firepower /monitoring/ # create snmp-user test1
Password:
firepower /monitoring/snmp-user* # commit-buffer
firepower /monitoring/snmp-user #
```

関連コマンド	コマンド	説明
	enable snmp	SNMP を有効にします。
	set snmp	SNMP 設定パラメータを設定します。これは、コミュニティ、SNMP を担当するシステム担当者、およびホストの場所です。

create ssh-server

新しい SSH ホスト キーを作成するには、**host-key** キーワードが指定された **create ssh-server** コマンドを使用します。

既存の SSH ホスト キーを作成するには、**host-key** キーワードが指定された **delete ssh-server** コマンドを使用します。

```
create ssh-server host-key
create ssh-server host-key
```

構文の説明

このコマンドには、追加の引数はありません。

コマンドモード

scope system/scope services/

コマンド履歴

リリース	変更内容
1.1(1)	コマンドが追加されました。

使用上のガイドライン

このコマンドの **create** 形式を使用して、新しい SSH ホスト キーを生成します。

このコマンドの **delete** 形式を使用して、新しい SSH ホスト キーを作成する前に既存のキーを破棄します。

例

次の例は、新しい SSH サーバ ホスト キーを生成する方法を示しています。

```
firepower # scope system
firepower /system # scope services
firepower /system/services # create ssh-server host-key
firepower /system/services* # commit-buffer
firepower /system/services #
```

次の例は、既存の SSH ホスト キーを削除して、自身の宛先を確認する方法を示しています。

```
firepower # scope system
firepower /system # scope services
firepower /system/services # delete ssh-server host-key
firepower /system/services* # commit-buffer
firepower /system/services # show ssh-server host-key
Host Key Size: 2048
Deleted: Yes
firepower /system/services #
```

関連コマンド	コマンド	説明
	set ssh-server	SSH サーバのホスト キーのサイズを設定します。
	show ssh-server	SSH サーバのプロパティを表示します。

create stats-threshold-policy

新しい統計情報しきい値ポリシーを作成するには、**create stats-threshold-policy** コマンドを使用します。名前が指定されたポリシーがすでに存在する場合、コマンドは失敗します。

organization モードでしきい値ポリシーを追加または編集するには、**enter stats-threshold-policy** コマンドを使用します。指定されたポリシーが存在しない場合は、作成されて入力されます。ポリシーが存在する場合は、そのポリシーが入力されます。

また、このコマンドの **scope** 形式を使用して、**organization** モードで既存の統計情報しきい値ポリシーを入力し、プロパティを割り当てまたは変更することもできます。通常、オブジェクトの「調査」は入力するよりも簡単です。これは、オブジェクトの名前がすべて必要になるため、このコマンドの **enter** 形式では、すべての定義パラメータを入力する必要があります。

既存のポリシーを削除するには、このコマンドの **delete** 形式を使用します。

create stats-threshold-policy *policy-name*

構文の説明

policy-name

新しい統計情報しきい値ポリシーの名前。

(注) イーサネットサーバポート (`scope eth-server/`) またはイーサネットアップリンクポート (`scope eth-uplink/`) のデフォルトの統計情報しきい値ポリシーを作成または削除することはできません。

コマンドモード

scope org/

コマンド履歴

リリース

変更内容

1.1(1)

コマンドが追加されました。

使用上のガイドライン

統計情報しきい値ポリシーは、システムの特定の側面についての統計情報をモニタし、指定されたしきい値を超えた場合にはイベントを生成します。最小値と最大値の両方のしきい値を設定できます。たとえば、CPUの温度が特定の値を超えた場合や、サーバを過度に使用していたり、サーバの使用に余裕がある場合には、アラームを発生するようにポリシーを設定できます。

組織モードで追加の統計情報のしきい値ポリシーを作成、入力、および削除できます。イーサネットサーバポートまたはイーサネットアップリンクポートでは、追加の統計情報のしきい値ポリシーを作成できません。また、このコンポーネントの既存のデフォルトポリシーを削除することもできません。デフォルトポリシーを変更できるだけです。



- (注) **set collection-interval** コマンドを使用して、統計情報を収集する頻度を定義し、**set reporting-interval** コマンドを使用して、統計情報を報告する頻度を定義します。これらの間隔で統計情報収集ポリシーが定義されます。

例

次の例では、組織モードを調査し、サーバとサーバコンポーネント統計情報に新しい統計情報しきい値ポリシーを作成し、CPU 環境統計情報のしきい値ポリシークラスを作成し、CPU 温度プロパティを作成し、通常の CPU 温度を摂氏 48.5 度に指定し、通常超えの警告しきい値を摂氏 50 度に作成し、トランザクション全体をコミットする方法を示します。

```
firepower # scope org
firepower /org # create stats-threshold-policy ServStatsPolicy
firepower /org/stats-threshold-policy* # create class cpu-env-stat
firepower /org/stats-threshold-policy/class* # create property temperature
firepower /org/stats-threshold-policy/class/property* # set normal-value 48.5
firepower /org/stats-threshold-policy/class/property* # create threshold-value above-normal
warning
firepower /org/stats-threshold-policy/class/property/threshold-value* # set escalating
50.0
firepower /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
firepower /org/stats-threshold-policy/class/property/threshold-value #
```

関連コマンド

コマンド	説明
create class	統計情報の新しいクラスを作成します。
create property	統計情報のクラスの新しいプロパティを作成します。
create threshold-value	クラスプロパティにしきい値 (above-normal または below-normal) を指定します。
scope org	組織モードを開始します。

create subinterface

コンテナ インスタンスで使用する物理または EtherChannel インターフェイスにサブインターフェイスを追加するには、**create subinterface** コマンドを使用します。

create subinterface *id*

構文の説明	<i>id</i>	ID を 1 ~ 4294967295 で設定します。この ID は、 <i>interface_id.subinterface_id</i> のように親インターフェイスの ID に追加されます。たとえば、サブインターフェイスを ID 100 でイーサネット 1/1 に追加する場合、そのサブインターフェイス ID はイーサネット 1/1.100 になります。利便性を考慮して一致するように設定することができますが、この ID は VLAN ID と同じではありません。
コマンド モード	scope eth-uplink/scope fabric a/scope interface/ scope eth-uplink/scope fabric a/create port-channel/	
コマンド履歴	リリース	変更内容
	2.4(1)	コマンドが追加されました。

使用上のガイドライン シャーシには最大 500 個のサブインターフェイスを追加できます。

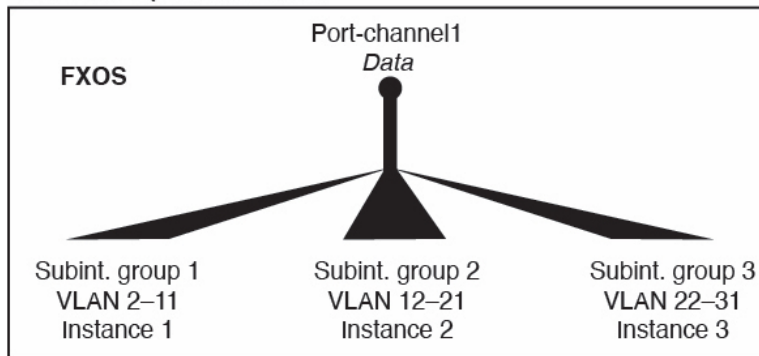
スタンドアロンインターフェイスの場合、サブインターフェイスは、データまたはデータ共有タイプのインターフェイスでのみサポートされます。マルチインスタンス クラスターリングの場合、クラスタタイプのインターフェイスにサブインターフェイスを追加するだけです。データインターフェイス上のサブインターフェイスはサポートされません。

インターフェイスごとの VLAN ID は一意である必要があります。コンテナ インスタンス内では、VLAN ID は割り当てられたすべてのインターフェイス全体で一意である必要があります。異なるコンテナ インターフェイスに割り当てられている限り、VLAN ID を別のインターフェイス上で再利用できます。ただし、同じ ID を使用していても、各サブインターフェイスが制限のカウント対象になります。

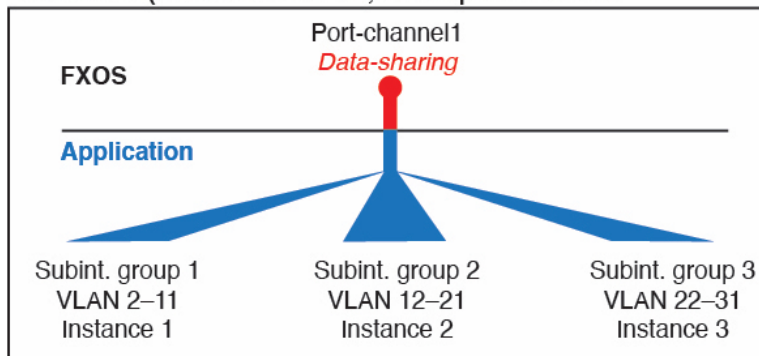
ネイティブ インスタンスの場合、アプリケーション内にものみ VLAN サブインターフェイスを作成できます。コンテナ インスタンスの場合、FXOS VLAN サブインターフェイスが定義されていないインターフェイスのアプリケーション内でも VLAN サブインターフェイスを作成できます。これらのサブインターフェイスには FXOS 制限が適用されません。サブインターフェイスを作成するオペレーティングシステムの選択は、ネットワーク導入および個人設定によって異なります。たとえば、サブインターフェイスを共有するには、FXOS でサブインターフェイスを作成する必要があります。FXOS サブインターフェイスを優先するもう 1 つのシナリオでは、1 つのインターフェイス上の別のサブインターフェイスグループを複数のインスタンスに割り当てます。たとえば、インスタンス A で VLAN 2-11 を、インスタンス B で VLAN 12-21 を、インスタンス C で VLAN 22-31 を使用して Port-Channel1 を使うとします。アプリケーション内でこれらのサブインターフェイスを作成する場合、FXOS 内で親インターフェイスを共有

しますが、これはお勧めしません。このシナリオを実現する3つの方法については、次の図を参照してください。

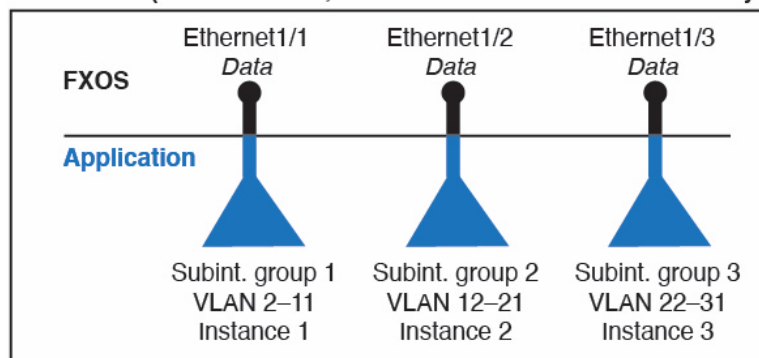
Scenario 1 (recommended)



Scenario 2 (not recommended, worse performance)



Scenario 3 (recommended, but lacks EtherChannel redundancy)



現在論理デバイスに割り当てられている物理インターフェイスにサブインターフェイスを追加することはできません。親の他のサブインターフェイスが割り当てられている場合、その親インターフェイス自体が割り当てられていない限り、新しいサブインターフェイスを追加できません。

例

次に、イーサネット 1/1 上の3つのサブインターフェイスを作成し、データ共有インターフェイスに設定する例を示します。

create subinterface

```

firepower# scope eth-uplink
firepower /eth-uplink # scope fabric a
firepower /eth-uplink/fabric # scope interface Ethernet1/1
firepower /eth-uplink/fabric/interface # create subinterface 10
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 10
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 11
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 11
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # exit
firepower /eth-uplink/fabric/interface # create subinterface 12
firepower /eth-uplink/fabric/interface/subinterface* # set vlan 12
firepower /eth-uplink/fabric/interface/subinterface* # set port-type data-sharing
firepower /eth-uplink/fabric/interface/subinterface* # commit-buffer
firepower /eth-uplink/fabric/interface/subinterface #

```

関連コマンド

コマンド	説明
create port-channel	EtherChannel (ポート チャンネル) を作成します。
scope interface	物理インターフェイス オブジェクトを入力します。
set port-type	インターフェイス タイプを設定します。
set vlan	サブインターフェイスの VLAN ID を設定します。

create threshold-value

クラス プロパティにしきい値 (above-normal または below-normal) を追加するには、**create threshold-value** コマンドを使用します。名前が指定されたしきい値がすでに存在する場合、コマンドは失敗します。

しきい値を追加または編集するには、**enter threshold-value** コマンドを使用します。指定されたしきい値が存在しない場合は、作成されて入力されます。しきい値が存在する場合は、そのしきい値が入力されます。

また、このコマンドの **scope** 形式を使用して、既存のしきい値を入力し、パラメータを割り当てまたは変更することもできます。通常、オブジェクトの「調査」は入力するよりも簡単です。これは、オブジェクトの名前がすべて必要になるため、このコマンドの **enter** 形式では、すべての定義パラメータを入力する必要があります。

既存のしきい値を削除するには、このコマンドの **delete** 形式を使用します。

create threshold-value { **above-normal** | **below-normal** *event_type* }

構文の説明

above-normal | **below-normal** しきい値のタイプ (above-normal または below-normal) を指定します。これは、モニタ対象の値 (個別に設定) が関連する通常値 (個別に設定) に対して増減した場合に、指定された *event_type* が記録されるかどうかを決定します。

event_type ログに記録されるイベントのタイプを指定します。

- cleared
- condition
- critical
- info
- major
- minor
- warning

コマンドモード

scope eth-server/scope stats-threshold-policy/scope class/scope property/
 scope eth-uplink/scope stats-threshold-policy/scope class/scope property/
 scope org/scope stats-threshold-policy/scope class/scope property/

コマンド履歴

リリース 変更内容

1.1(1) コマンドが追加されました。

使用上のガイドライン

特定の統計情報セットに対してしきい値を設定するには、クラスを使用します。プロパティを使用して、ポリシークラスの通常値やしきい値などの特定の値を定義します。たとえば、ドロップされたパケットの平均数が特定の量を超えた場合に障害を出すしきい値をポートで定義できます。このクラスでは、イーサネットエラー統計情報クラスのしきい値プロパティを作成します。

1つのポリシークラスに複数のプロパティを設定できます。また、1つのプロパティに対して複数のしきい値を作成することもできます。



- (注) イーサネットサーバポートまたはイーサネットアップリンクポートごとにデフォルトの統計情報しきい値ポリシーが1つあります。追加の統計情報収集ポリシーは作成できません。また、このコンポーネントの既存のデフォルトポリシーを削除できません。デフォルトポリシーを変更するだけです。ただし、組織モード (scope org/) では統計情報のしきい値ポリシーを作成および削除できます。

例

次の例では、デフォルトのイーサネットサーバの統計情報しきい値ポリシークラスを調査し、シャーシ統計情報クラスを作成し、入力電力 (W) プロパティを作成し、通常電力レベルを 8 kW に指定し、通常超えの警告しきい値 11 kW を作成し、クラスをコミットする方法を示します。

```
firepower # scope eth-server
firepower /eth-server # scope stats-threshold-policy default
firepower /eth-server/stats-threshold-policy # create class chassis-stats
firepower /eth-server/stats-threshold-policy/class* # create property input-power
firepower /eth-server/stats-threshold-policy/class/property* # set normal-value 8000.0
firepower /eth-server/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* # set
escalating 11000.0
firepower /eth-server/stats-threshold-policy/class/property/threshold-value* #
commit-buffer
firepower /eth-server/stats-threshold-policy/class/property/threshold-value #
```

関連コマンド

コマンド	説明
enter class	統計情報のクラスを入力または作成します。
enter property	統計情報のクラスにプロパティを入力または作成します。
scope stats-threshold-policy	stats-threshold-policy ポリシー モードを開始します。このモードでは、統計情報クラスを管理します。
set normal-value	クラス プロパティに通常値を指定します。

create trustpoint

インターネットキーエクスチェンジ (IKE) 認証時に証明書検証用の新しいトラストポイントを追加するには、**create trustpoint** コマンドを使用します。名前が指定された接続がすでに存在する場合、コマンドは失敗します。

トラストポイントを追加または編集するには、**enter trustpoint** コマンドを使用します。指定されたトラストポイントが存在しない場合は、作成されて入力されます。トラストポイントが存在する場合は、そのトラストポイントが入力されます。

また、このコマンドの **scope** 形式を使用して、既存のトラストポイントを入力し、プロパティを割り当てまたは変更することもできます。

既存のトラストポイントを削除するには、このコマンドの **delete** 形式を使用します。

create trustpoint *name*

delete trustpoint *name*

enter trustpoint *name*

scope trustpoint *name*

構文の説明	<i>name</i>	トラストポイント名には 32 文字以内の英数字を使用できます。
コマンドモード	scope security/	
コマンド履歴	リリース	変更内容
	1.1(1)	コマンドが追加されました。

使用上のガイドライン このコマンドを使用して、インターネットキーエクスチェンジ (IKE) 認証時の証明書検証に使用するトラストポイントを識別します。

新しいトラストポイントを作成すると、新しいトラストポイントがまだコミットされていないことを示すアスタリスクが付いた **security/trustpoint** モードが自動的に開始されます。トラストポイントを作成した後は、名前を変更することはできません。トラストポイントを削除し、新しいトラストポイントを作成する必要があります。

例

次の例は、トラストポイントの作成方法と入力方法を示しています。

```
firepower # scope security
firepower /security # enter trustpoint tPoint4
firepower /security/trustpoint* #
```

関連コマンド	コマンド	説明
	set certchain	トラストポイントの証明書情報を設定します。
	show trustpoint	現在のトラストポイント情報を表示します。

cycle

セキュリティ モジュール/サーバの電源を再投入するには、いずれかの **cycle** コマンドを使用します。

cycle { **cycle-immediate** | **cycle-wait** }

構文の説明	cycle-immediate	すぐにモジュールの電源の再投入を行います。
	cycle-wait	システムはモジュールで実行中のアプリケーションがシャットダウンするまで最大5分待ってから、モジュールの電源の再投入を行います。
コマンドモード	scope service-profile/	
コマンド履歴	リリース	変更内容
	1.1(1)	このコマンドが導入されました。

例

次の例は、実行中のアプリケーションがシャットダウンされた後にモジュールの電源を再投入する方法を示しています。

```
firepower # scope service-profile server 1/1
firepower /org/service-profile # cycle cycle-wait
firepower /org/service-profile* # commit-buffer
firepower /org/service-profile #
```

関連コマンド	コマンド	説明
	set adminstate	ネットワーク モジュールのオフラインまたはオンラインを切り替えます。

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。