



コマンドライン リファレンス

このリファレンスでは、FirePOWER アプライアンス、仮想デバイス、および ASA FirePOWER デバイスの ASA FirePOWER モジュールのコマンドラインインターフェイス (CLI) について説明します。CLI を使用して、FireSIGHT システムを表示、設定、およびトラブルシューティングすることができます。



(注)

コマンドライン インターフェイスは、防御センター、シリーズ 2 アプライアンス、Blue Coat X-Series 向け Cisco NGIPS、および ASA FirePOWER デバイスの ASA モジュールではサポートされていません。

CLI モードには `show` や `configure` など多数あり、これらのモードにはモード名で始まる一連のコマンドが含まれています。モードを開始して、そのモードで有効なコマンドを入力することも、任意のモードからフル コマンドを入力することもできます。たとえば、`Analyst1` というユーザ アカウントの情報を表示するには、CLI プロンプトで次のように入力します。

```
show user Analyst1
```

すでに `show` モードを開始している場合は、CLI プロンプトで次のように入力します。

```
user Analyst1
```

各モードで、ユーザが使用できるコマンドは、ユーザの CLI アクセスによって異なります。ユーザ アカウントを作成する場合は、手動で次のいずれかの CLI アクセス レベルに割り当てることができます。

- 基本
ユーザは読み取り専用のアクセス権を持ち、システムのパフォーマンスに影響を与えるコマンドを実行することはできません。
- 設定 (Configuration)
ユーザは、読み取り/書き込みアクセス権があり、システムのパフォーマンスに影響を与えるコマンドを実行することができます。
- なし
ユーザはシェルにログインできません。

シリーズ 3 デバイスでは、Web インターフェイスの [ユーザ管理 (User Management)] ページでコマンドラインの権限を割り当てることができます。詳細については、[ユーザの管理 \(61-1 ページ\)](#) を参照してください。仮想デバイスと ASA FirePOWER デバイスでは、CLI 自身を通じてコマンドラインの権限を割り当てます。



(注)

シリーズ 3 デバイスをリブートし、できるだけ早く CLI にログインしても、Web インターフェイスが使用できるようになるまで、実行するすべてのコマンドは監査ログに記録されません。

CLI コマンドでは大文字と小文字が区別されません。ただし、ユーザ名や検索フィルタなど、テキストが CLI フレームワークの一部ではないパラメータでは区別されることに注意してください。コマンドラインへのログインの詳細については、[アプライアンスへのログイン\(2-1 ページ\)](#)を参照してください。

以降の項で、CLI コマンドについて説明します。

- [基本的な CLI コマンド\(D-2 ページ\)](#)
- [Show コマンド\(D-5 ページ\)](#)
- [コンフィギュレーション コマンド\(D-31 ページ\)](#)
- [system コマンド\(D-47 ページ\)](#)

基本的な CLI コマンド

基本的な CLI コマンドを使用して、CLI とやりとりすることができます。これらのコマンドはデバイスの処理に影響しません。基本的なコマンドは、すべての CLI ユーザが使用できます。

以降の項で、基本のコマンドについて説明します。

- [configure password\(D-2 ページ\)](#)
- [end\(D-3 ページ\)](#)
- [exit\(D-3 ページ\)](#)
- [help\(D-3 ページ\)](#)
- [history\(D-4 ページ\)](#)
- [logout\(D-4 ページ\)](#)
- [?\(疑問符\)\(D-4 ページ\)](#)
- [??\(二重の疑問符\)\(D-5 ページ\)](#)

configure password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLI は現在の(古い)パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

アクセス(Access)

基本

構文

```
configure password
```

例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

end

ユーザをデフォルトのモードに戻します(ユーザを任意の下位レベルの CLI コンテキストから最大デフォルト モードまで移動します)。

アクセス (Access)

基本

構文

```
end
```

例

```
configure network ipv4> end  
>
```

exit

CLI コンテキストを、次に高い CLI コンテキスト レベルへ移動します。デフォルト モードからこのコマンドを発行すると、ユーザは現行の CLI セッションからログアウトします。これは、CLI コマンドの `logout` を発行するのと同じです。

アクセス (Access)

基本

構文

```
exit
```

例

```
configure network ipv4> exit  
configure network>
```

help

CLI 構文の概要を表示します。

アクセス (Access)

基本

構文

```
help
```

例

```
> help
```

history

現行のセッションのコマンドラインの履歴を表示します。

アクセス (Access)

基本

構文

```
history limit
```

ここで *limit* は履歴リストのサイズを設定します。サイズを無制限に設定するには、0 を入力します。

例

```
history 25
```

logout

現行の CLI コンソールセッションから現行のユーザをログアウトします。

アクセス (Access)

基本

構文

```
logout
```

例

```
> logout
```

? (疑問符)

CLI コマンドおよびパラメータの状況依存ヘルプを表示します。次のように、疑問符(?) のコマンドを使用します。

- 現在の CLI コンテキスト内で使用できるコマンドのヘルプを表示するには、コマンドプロンプトで疑問符(?) を入力します。
- 特定文字セットから始まる使用可能なコマンドのリストを表示するには、疑問符(?) に続けて短縮されたコマンドを入力します。
- コマンドの正式な引数のヘルプを表示するには、コマンドプロンプトの引数の代わりに疑問符(?) を入力します。

疑問符(?) は、コンソールにエコーバックされないことに注意してください。

アクセス (Access)

基本

構文

```
?
abbreviated_command ?
command [arguments] ?
```

例

```
> ?
```

?? (二重の疑問符)

CLI コマンドおよびパラメータの詳細な状況依存ヘルプを表示します。

アクセス (Access)

基本

構文

```
??  
abbreviated_command end??  
command [arguments] ??
```

例

```
> configure manager add ??
```

Show コマンド

Show コマンドは、デバイスの状態に関する情報を提供します。これらのコマンドはデバイスの動作モードを変更しません。また、これらのコマンドを実行しても、システムの動作に対する影響は最小限になります。ほとんどの show コマンドはすべての CLI ユーザが利用できますが、show user コマンドを発行できるのは、configuration CLI アクセス権限を持つユーザのみです。

以降の項では、show コマンドについて説明します。

- [access-control-config \(D-7 ページ\)](#)
- [alarms \(D-7 ページ\)](#)
- [arp-tables \(D-7 ページ\)](#)
- [audit-log \(D-8 ページ\)](#)
- [bypass \(D-8 ページ\)](#)
- [clustering \(D-8 ページ\)](#)
- [cpu \(D-9 ページ\)](#)
- [database \(D-10 ページ\)](#)
- [device-settings \(D-11 ページ\)](#)
- [disk \(D-11 ページ\)](#)
- [disk-manager \(D-12 ページ\)](#)
- [dns \(D-12 ページ\)](#)
- [expert \(D-12 ページ\)](#)
- [fan-status \(D-12 ページ\)](#)
- [fastpath-rules \(D-13 ページ\)](#)
- [gui \(D-13 ページ\)](#)
- [hostname \(D-13 ページ\)](#)
- [hosts \(D-14 ページ\)](#)
- [hyperthreading \(D-14 ページ\)](#)
- [iab \(D-14 ページ\)](#)

- [ifconfig \(D-15 ページ\)](#)
- [inline-sets \(D-15 ページ\)](#)
- [interfaces \(D-15 ページ\)](#)
- [lcd \(D-16 ページ\)](#)
- [link-state \(D-17 ページ\)](#)
- [log-ips-connection \(D-17 ページ\)](#)
- [managers \(D-17 ページ\)](#)
- [memory \(D-18 ページ\)](#)
- [model \(D-18 ページ\)](#)
- [mpls-depth \(D-18 ページ\)](#)
- [NAT \(D-18 ページ\)](#)
- [netstat \(D-20 ページ\)](#)
- [network \(D-21 ページ\)](#)
- [network-modules \(D-21 ページ\)](#)
- [network-static-routes \(D-21 ページ\)](#)
- [ntp \(D-22 ページ\)](#)
- [perfstats \(D-22 ページ\)](#)
- [portstats \(D-22 ページ\)](#)
- [power-supply-status \(D-23 ページ\)](#)
- [process-tree \(D-23 ページ\)](#)
- [processes \(D-23 ページ\)](#)
- [route \(D-24 ページ\)](#)
- [routing-table \(D-24 ページ\)](#)
- [serial-number \(D-24 ページ\)](#)
- [ssl-policy-config \(D-25 ページ\)](#)
- [stacking \(D-25 ページ\)](#)
- [summary \(D-25 ページ\)](#)
- [time \(D-26 ページ\)](#)
- [traffic-statistics \(D-26 ページ\)](#)
- [user \(D-26 ページ\)](#)
- [users \(D-27 ページ\)](#)
- [version \(D-28 ページ\)](#)
- [virtual-routers \(D-28 ページ\)](#)
- [virtual-switches \(D-28 ページ\)](#)
- [vmware-tools \(D-29 ページ\)](#)

access-control-config

次のように現在適用されているアクセス コントロールの設定を表示します:セキュリティ インテリジェンス設定、参照された SSL ポリシー、ネットワーク分析ポリシー、侵入ポリシー、およびファイル ポリシーの名前、侵入変数セットのデータ、ロギング設定、およびポリシー レベルのパフォーマンス、前処理、一般設定などのその他の詳細設定。

また、送信元と宛先のポート データ (ICMP エントリのタイプとコードを含む) および各アクセス コントロール ルールに一致した接続数 (ヒット数) などの、ポリシーに関連する接続情報も表示します。

アクセス (Access)

基本

構文

```
show access-control-config
```

例

```
> show access-control-config
```

alarms

デバイス上で、現行のアクティブな (失敗した/停止している) ハードウェアのアラームを表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show alarms
```

例

```
> show alarms
```

arp-tables

ネットワークに適用できる該当するアドレス解決プロトコル テーブルを表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show arp-tables
```

例

```
> show arp-tables
```

audit-log

監査ログが時系列の逆順に表示され、最も新しい監査ログ イベントが最初に示されます。

アクセス (Access)

基本

構文

```
show audit-log
```

例

```
> show audit-log
```

bypass

シリーズ 3 デバイスでは、使用中のインラインセットが一覧表示され、それらのセットのバイパス モード ステータスが次のいずれかとして表示されます。

- **armed**: インターフェイス ペアは、障害が発生した場合にハードウェア バイパスに移行するように設定されているか、`configure bypass close` コマンドでフェールクローズへの移行が強制されています。
- **engaged**: インターフェイス ペアが、オープンに失敗したか、または、`configure bypass open` コマンドを使用して強制的にハードウェア バイパスになりました。
- **off**: インターフェイス ペアは、フェールクローズに設定されています (**Bypass Mode: Non-Bypass**)。インターフェイス ペアで障害が発生した場合は、パケットがブロックされます。

アクセス (Access)

基本

構文

```
show bypass
```

例

```
> show bypass
s1p1 <-> s1p2: status 'armed'
s1p1 <-> s1p2: status 'engaged'
```

clustering

デバイスのクラスタリング設定、ステータス、およびメンバー スタックの情報を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

config

デバイスにおけるクラスタリング設定を表示します。

構文

```
show clustering config
```

例

```
> show clustering config
```

clustering ha-statistics

クラスタ内のデバイスについて、状態共有統計情報を表示します。

構文

```
show clustering ha-statistics
```

例

```
> show clustering ha-statistics
```

cpu

デバイス上のすべての CPU のプラットフォームに適合する現行の CPU の使用率の統計情報を表示します。管理対象デバイスでは、次の値が表示されます。

- CPU

プロセッサの数。

- ロード

0~100 の数値で表される CPU の使用率。0 はロードされていない状態で、100 は完全にロードされたことを表します。

仮想デバイスおよび ASA FirePOWER デバイスについては、次の値が表示されます。

- CPU

プロセッサの数。

- %user

ユーザ レベル(アプリケーション)で実行中に生じた CPU 使用率のパーセンテージ。

- %nice

高い優先度で実行中に生じた CPU 使用率のパーセンテージ。

- %sys

システム レベル(カーネル)で実行中に生じた CPU 使用率のパーセンテージ。これには、サービスの割り込みや softirqs で経過する時間は含まれません。softirq(ソフトウェアの割り込み)は、複数の CPU で同時に実行できる最大 32 個の列挙されたソフトウェア割り込みの 1 つです。

- %iowait

システムに未処理のディスク I/O 要求があったときに、CPU がアイドル状態だった時間の割合(パーセンテージ)。

- %irq
割り込みを行うために CPU が費やした時間の割合(パーセンテージ)。
- %soft
softirqs を行うために CPU が費やした時間の割合(パーセンテージ)。
- %steal
ハイパーバイザが別の仮想プロセッサを実行しているときに、仮想 CPU が強制的な待機で費やした時間の割合(パーセンテージ)
- %guest
仮想プロセッサを実行するために CPU が費やした時間の割合(パーセンテージ)。
- %idle
CPU がアイドル状態で、システムに未処理のディスク I/O 要求がなかった時間の割合(パーセンテージ)。

アクセス (Access)

基本

構文

```
show cpu [procnum]
```

ここで *procnum* は、使用率の情報を表示するプロセッサの数を表します。有効な値は、0 からシステム上のプロセッサ数よりも少ない数です。*procnum* が管理対象デバイスで使用されている場合は無視されます。このプラットフォームについては、使用率の情報はすべてのプロセッサについてのみ表示されるためです。

例

```
> show cpu
```

database

`show database` コマンドは、デバイスの管理インターフェイスを設定します。

アクセス (Access)

基本

processes

実行中のデータベース クエリを表示します。

アクセス (Access)

基本

構文

```
show database processes
```

例

```
> show database processes
```

slow-query-log

データベースのスロー クエリを表示します。

アクセス (Access)

基本

構文

```
show database slow-query-log
```

例

```
> show database slow-query-log
```

device-settings

現行のデバイスに特有のアプリケーションのバイパス設定に関する情報を表示します。

アクセス (Access)

基本

構文

```
show device-settings
```

例

```
> show device-settings
```

disk

現行のディスクの使用率を表示します。

アクセス (Access)

基本

構文

```
show disk
```

例

```
> show disk
```

disk-manager

システムの各部分のディスク使用率の詳細情報を表示します(サイロ、低水位、高水位など)。

アクセス (Access)

基本

構文

```
show disk-manager
```

例

```
> show disk-manager
```

dns

現行の DNS サーバのアドレスと検索ドメインを表示します。

アクセス (Access)

基本

構文

```
show dns
```

例

```
> show dns
```

expert

シェルを起動します。

アクセス (Access)

基本

構文

```
expert
```

例

```
> expert
```

fan-status

ハードウェア ファンの現在のステータスを表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show fan-status
```

例

```
> show fan-status
```

fastpath-rules

現在設定されている **fastpath** ルールを表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show fastpath-rules
```

例

```
> show fastpath-rules
```

gui

Web インターフェイスの現在の状態を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show gui
```

例

```
> show gui
```

hostname

デバイスのホスト名およびアプライアンス **UUID** を表示します。**CLI** を使用してデバイスのホスト名を編集する場合は、管理する 防御センター に変更が反映されることを確認します。場合によっては、デバイス管理設定を手動で編集する必要があります。詳細については、[デバイス管理設定の編集 \(4-58 ページ\)](#) を参照してください。

アクセス (Access)

基本

構文

```
show hostname
```

例

```
> show hostname
```

hosts

ASA FirePOWER モジュールの /etc/hosts ファイルの内容を表示します。

アクセス (Access)

基本

構文

```
show hosts
```

例

```
> show hosts
```

hyperthreading

ハイパースレッディングが有効か無効かを表示します。このコマンドは ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show hyperthreading
```

例

```
> show hyperthreading
```

iab

現在のインテリジェント アプリケーション バイパス (IAB) 設定を表示します。このコマンドには、管理対象デバイスでバージョン 5.4.0.10 以降が必要です。Defense Center では、IAB 機能を実装するにはバージョン 5.4.1.9 以降が必要で、IAB イベントを提供するにはバージョン 5.4.1.10 以降が必要です。

アクセス (Access)

基本

構文

```
show iab
```

例

```
> show iab
IAB configuration:
Performance Sample Interval      5 seconds
Bytes per Flow                   500000 kbytes
Flow Velocity                    25000 kbytes/second
Drop Percentage                  1%
Processor Utilization Percentage 95%
Packet Latency                   250 microseconds
```

inline-sets

すべてのインラインセキュリティゾーンと関連するインターフェイスの設定データを表示します。このコマンドは ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show inline-sets
```

例

```
> show inline-sets
```

interfaces

パラメータが指定されていない場合は、設定されているすべてのインターフェイスのリストが表示されます。パラメータが指定されている場合は、指定されたインターフェイスの詳細情報が表示されます。

アクセス (Access)

基本

構文

```
show interfaces [interface]
```

ここで *interface* は詳細情報を表示する特定のインターフェイスです。

例

```
> show interfaces
```

ifconfig

ASA FirePOWER モジュールに対するインターフェイスの設定を表示します。

アクセス (Access)

基本

構文

```
show ifconfig
```

例

```
> show ifconfig
```

lcd

LCD のハードウェア ディスプレイが有効か無効かを表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show lcd
```

例

```
> show lcd
```

link-aggregation

show link-aggregation コマンドは、リンク集約グループ (LAG) の設定および統計情報を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

設定:

LAG ID、インターフェイスの数、コンフィギュレーションモード、ロードバランシングモード、LACP 情報、および物理インターフェイスのタイプなど、設定された各 LAG の設定の詳細を表示します。

アクセス (Access)

基本

構文

```
show link-aggregation configuration
```

例

```
> show link-aggregation configuration
```

統計情報

ステータス、リンク ステートと速度、コンフィギュレーションモード、送受信されたパケットのカウンタ、および送受信されたバイトのカウンタなど、設定された各 LAG の統計情報をインターフェイスごとに表示します。

アクセス (Access)

基本

構文

```
show link-aggregation statistics
```

例

```
> show link-aggregation statistics
```


link-state

デバイスのポートのタイプ、リンク、スピード、速度、デュプレックスの状態およびバイパス モードを表示します。このコマンドは ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show link-state
```

例

```
> show link-state
```

log-ips-connection

記録された侵入イベントに関連付けられている接続イベントのログギングが有効か無効かを表示します。

アクセス (Access)

基本

構文

```
show log-ips-connection
```

例

```
> show log-ips-connection
```

managers

防御センターの設定および通信のステータスを表示します。登録キーおよび NAT ID は、登録が保留中の場合のみ表示されます。デバイスが高可用性ペアに登録されている場合、管理している両方の 防御センター の情報が表示されます。デバイスが、スタック設定のセカンダリ デバイスとして設定されている場合、管理している両方の 防御センター、およびプライマリ デバイスに関する情報が表示されます。

アクセス (Access)

基本

構文

```
show managers
```

例

```
> show managers
```

memory

デバイスの合計メモリ、使用中のメモリ、使用可能なメモリを表示します。

アクセス (Access)

基本

構文

```
show memory
```

例

```
> show memory
```

model

デバイスのモデル情報を表示します。

アクセス (Access)

基本

構文

```
show model
```

例

```
> show model
```

mpls-depth

管理インターフェイスに設定されている MPLS レイヤ数を 0~6 で表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show mpls-depth
```

例

```
> show mpls-depth
```

NAT

show nat コマンドは、管理インターフェイスの NAT データと設定情報を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

active-dynamic

ダイナミック ルールに従って変換されている NAT フローを表示します。これらのエントリは、フローがルールに一致している場合に、ルールがタイムアウトになるまで表示されます。したがって、リストは正確ではないことがあります。タイムアウトはプロトコルに依存します。ICMP は 5 秒、UDP は 120 秒、TCP は 3600 秒、他のすべてのプロトコルは 60 秒です。

構文

```
show nat active-dynamic
```

例

```
> show nat active-dynamic
```

active-static

スタティック ルールに従って変換されている NAT フローを表示します。これらのエントリは、デバイスにルールが適用されるとすぐに表示されます。リストは、スタティックな NAT ルールに一致しているアクティブな フローを示しているわけではありません。

構文

```
show nat active-static
```

例

```
> show nat active-static
```

allocators

すべての NAT アロケータの情報、ダイナミック ルールで使用されている変換済みアドレスのプールを表示します。

構文

```
show nat allocators
```

例

```
> show nat allocators
```

config

管理インターフェイスの現行の NAT ポリシーの設定を表示します。

構文

```
show nat config
```

例

```
> show nat config
```

dynamic-rules

指定されたアロケータ ID を使用しているダイナミックな NAT ルールを表示します。

構文

```
show nat dynamic-rules allocator_id
```

例

```
> show nat dynamic-rules 9
```

ここで `allocator_id` は有効なアロケータ ID 番号です。

flows

指定されたアロケータ ID を使用しているルールについてフローの数を表示します。

構文

```
show nat flows allocator-id
```

例

```
> show nat flows 81
```

ここで `allocator_id` は有効なアロケータ ID 番号です。

static-rules

すべてのスタティック NAT ルールを表示します。

構文

```
show nat static-rules
```

例

```
> show nat static-rules
```

netstat

ASA FirePOWER モジュールのアクティブなネットワーク接続を表示します。

アクセス (Access)

基本

構文

```
show netstat
```

例

```
> show netstat
```

network

管理インターフェイスの IPv4 および IPv6 の設定、MAC アドレス、HTTP プロキシアドレス、ポート、ユーザ名(設定されている場合)を表示します。

アクセス (Access)

基本

構文

```
show network
```

例

```
> show network
```

network-modules

インストールされているすべてのモジュール、およびモジュールの情報(シリアル番号など)を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show network-modules
```

例

```
> show network-modules
```

network-static-routes

インターフェイス、宛先アドレス、ネットワーク マスク、およびゲートウェイ アドレスなど、設定済みのすべてのネットワーク スタティック ルートとその情報が表示されます。

アクセス (Access)

基本

構文

```
show network-static-routes
```

例

```
> show network-static-routes
```

ntp

NTP コンフィギュレーションを表示します。

アクセス (Access)

基本

構文

```
show ntp
```

例

```
> show ntp
```

perfstats

デバイスのパフォーマンスの統計情報を表示します。

アクセス (Access)

基本

構文

```
show perfstats
```

例

```
> show perfstats
```

portstats

デバイスにインストールされているすべてのポートのポート統計情報を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show portstats [copper | fiber | internal | external | all]
```

ここで **copper** はすべての銅線ポートを表し、**fiber** はすべてのファイバポート、**internal** はすべての内部ポート、**external** はすべての外部 (銅線およびファイバ) ポート、**all** はすべてのポート (外部および内部) を表します。

例

```
> show portstats fiber
```

power-supply-status

ハードウェアの電源の現在の状態を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show power-supply-status
```

例

```
> show power-supply-status
```

process-tree

デバイスで実行中のプロセスについて、タイプごとにツリー形式でソートして表示します。

アクセス (Access)

基本

構文

```
show process-tree
```

例

```
> show process-tree
```

processes

デバイス上で実行中のプロセスについて、CPU 使用率の降順で表示します。

アクセス (Access)

基本

構文

```
show processes [sort-flag] [filter]
```

ここで、メモリ (の降順) でソートする場合は、`sort-flag` に `-m` を指定し、プロセス名ではなくユーザ名でソートする場合は `-u` を指定します。また、コマンドのフルネームおよびパスを表示する場合は `verbose` を指定します。`filter` パラメータは、コマンドの検索語または結果をフィルタするために使用するユーザ名を指定します。見出し行は表示されたままです。

例

```
> show processes -u user1
```

route

ASA FirePOWER モジュールのルーティング情報を表示します。

アクセス (Access)

基本

構文

```
show route
```

例

```
> show route
```

routing-table

パラメータが指定されていない場合は、すべての仮想ルータのルーティング情報を表示します。パラメータが指定されている場合は、指定されたルータのルーティング情報、および該当する場合は、指定されたルーティングのプロトコルタイプを表示します。パラメータはすべてオプションです。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show routing-table [name] [ ospf | rip | static ]
```

name は、情報を必要とする特定のルータ名です。*ospf*、*rip*、*static* は、ルーティング プロトコルタイプを指定します。

例

```
> show routing-table Vrouter1 static
```

serial-number

シャーシのシリアル番号を表示します。このコマンドは仮想デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show serial-number
```

例

```
> show serial-number
```


ssl-policy-config

現在適用されている SSL ポリシーの設定(ポリシーの説明、デフォルトのロギング設定、有効なすべての SSL ルールとルールの設定など)、信頼できる CA 証明書、および復号化不可能なトラフィックのアクションを表示します。

アクセス (Access)

基本

構文

```
show ssl-policy-config
```

例

```
> show ssl-policy-config
```

stacking

管理対象デバイスのスタッキングの設定とポジションを表示します。プライマリとして設定されているデバイスでは、すべてのセカンダリ デバイスのデータも示されます。クラスタ化されたスタックでは、このコマンドにより、スタックがクラスタのメンバーであることも示します。スタッキングを有効または無効にする(大半の場合は無効にする)には、ユーザは Web インターフェイスを使用する必要があります。スタッキングが有効になっていない場合、コマンドは Stacking not currently configured というメッセージを返します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show stacking
```

例

```
> show stacking
```

summary

デバイスに関して最もよく使用される情報(バージョン、タイプ、UUID など)のサマリーを表示します。詳細については、show コマンド: [version \(D-28 ページ\)](#)、[interfaces \(D-15 ページ\)](#)、[device-settings \(D-11 ページ\)](#)、および [access-control-config \(D-7 ページ\)](#) を参照してください。

アクセス (Access)

基本

構文

```
show summary
```

例

```
> show summary
```

time

現在の日付と時刻を、UTC および現行のユーザに設定されているローカル タイム ゾーンで表示します。

アクセス (Access)

基本

構文

```
show time
```

例

```
> show time
```

traffic-statistics

パラメータが指定されていない場合は、すべてのポートから送信された、および受信したバイトの詳細情報を表示します。ポートが指定されている場合は、指定されたポートの情報のみを表示します。ASA FirePOWER デバイスに対してポートを指定することはできません。システムはデータのプレーン インターフェイスのみを表示します。

アクセス (Access)

基本

構文

```
show traffic-statistics [port]
```

ここで port は、情報を表示させたい特定のポートです。

例

```
> show traffic-statistics s1p1
```

user

仮想デバイスに対してのみ適用されます。指定されたユーザに関する設定の詳細情報を表示します。次の値が表示されます。

- Login: ログイン名
- UID: ユーザ ID (数値)
- Auth (Local または Remote): ユーザがどのように認証されているか
- Access (Basic または Config): ユーザの権限レベル
- Enabled (Enabled または Disabled): ユーザがアクティブかどうか
- Reset (Yes または No): 次のログイン時にユーザがパスワードを変更する必要があるかどうか
- Exp (Never または数値): ユーザのパスワード変更が必要になるまでの日数
- Warn (N/A または数値): パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数

- **Str**(Yes または No) : ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- **Lock**(Yes または No) : ログインの失敗が多すぎたためユーザのアカウントがロックされているかどうか
- **Max**(N/A または 数値) : ユーザのアカウントがロックされる前に失敗するログインの最大回数

アクセス (Access)

設定 (Configuration)

構文

```
show user username username username ...
```

ここで `username` はユーザの名前を表します。複数の `username` はスペースで区切って指定します。

例

```
> show user jdoe
```

users

仮想デバイスに対してのみ適用されます。すべてのローカル ユーザの設定の詳細情報を表示します。次の値が表示されます。

- **Login**: ログイン名
- **UID**: ユーザ ID (数値)
- **Auth**(Local または Remote) : ユーザがどのように認証されているか
- **Access**(Basic または Config) : ユーザの権限レベル
- **Enabled**(Enabled または Disabled) : ユーザがアクティブかどうか
- **Reset**(Yes または No) : 次のログイン時にユーザがパスワードを変更する必要があるかどうか
- **Exp**(Never または 数値) : ユーザのパスワード変更が必要になるまでの日数
- **Warn**(N/A または 数値) : パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- **Str**(Yes または No) : ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- **Lock**(Yes または No) : ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- **Max**(N/A または 数値) : ユーザのアカウントがロックされる前に失敗するログインの最大回数

アクセス (Access)

設定 (Configuration)

構文

```
show users
```

例

```
> show users
```

version

製品のバージョンとビルドを表示します。`detail` パラメータが指定されている場合は、追加のコンポーネントのバージョンが表示されます。

アクセス (Access)

基本

構文

```
show version [detail]
```

例

```
> show version
```

virtual-routers

パラメータが指定されていない場合は、現在設定されているすべての仮想ルータのリスト、および DHCP リレー、OSPF、および RIP の情報が表示されます。パラメータが指定されている場合は、指定されたルータに関する情報が、指定されたルート タイプによって制限されて表示されます。パラメータはすべてオプションです。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show virtual-routers [ dhcprelay | ospf | rip ] [name]
```

ここで `dhcprelay`、`ospf`、および `rip` はルート タイプを表します。`name` は、情報を表示する特定のルータの名前を表します。`ospf` を指定した場合は、ルート タイプ、および(存在する場合は)ルート名に対して `neighbors`、`topology`、または `lsadb` を指定することができます。

例

```
> show virtual-routers ospf VRouter2
```

virtual-switches

パラメータが指定されていない場合は、設定されているすべての仮想スイッチのリストが表示されます。パラメータが指定されている場合は、指定されたスイッチに関する情報が表示されます。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

構文

```
show virtual-switches [name]
```

例

```
> show virtual-switches Vswitch1
```

vmware-tools

VMware Tools が、仮想デバイス上で現在有効になっているかどうかを示します。このコマンドは、仮想デバイスでのみ使用できます。

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティスイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- スナップショット
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト (<http://www.vmware.com>) を参照してください。

アクセス (Access)

基本

構文

```
show vmware-tools
```

例

```
> show vmware-tools
```

VPN

show VPN コマンドは、VPN ステータス、および VPN 接続の設定情報を表示します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

基本

config

すべての VPN 接続の設定を表示します。

構文

```
show vpn config
```

例

```
> show vpn config
```

config by virtual router

仮想ルータについて、すべての VPN 接続の設定を表示します。

構文

```
show vpn config [virtual router]
```

例

```
> show vpn config VRouter1
```

status

VPN 接続すべてのステータスを表示します。

構文

```
show vpn status
```

例

```
> show vpn status
```

status by virtual router

仮想ルータについて、すべての VPN 接続のステータスを表示します。

構文

```
show vpn status [virtual router]
```

例

```
> show vpn status VRouter1
```

counters

すべての VPN 接続のカウンタを表示します。

構文

```
show vpn counters
```

例

```
> show vpn counters
```

counters by virtual router

仮想ルータについて、すべての VPN 接続のカウンタを表示します。

構文

```
show vpn counters [virtual router]
```

例

```
> show vpn counters VRouter1
```

コンフィギュレーション コマンド

コンフィギュレーション コマンドを使用して、システムを設定および管理することができます。これらのコマンドはシステムの動作に影響を与えます。そのため、Basic レベルの `configure password` を除いては、Configuration CLI アクセス権限を持つユーザのみがこれらのコマンドを発行できます。

以降の項で、コンフィギュレーション コマンドについて説明します。

- [clustering \(D-31 ページ\)](#)
- [bypass \(D-31 ページ\)](#)
- [gui \(D-32 ページ\)](#)
- [iab \(D-32 ページ\)](#)
- [lcd \(D-34 ページ\)](#)
- [log-ips-connections \(D-35 ページ\)](#)
- [manager \(D-35 ページ\)](#)
- [mpls-depth \(D-36 ページ\)](#)
- [network \(D-36 ページ\)](#)
- [password \(D-43 ページ\)](#)
- [stacking disable \(D-43 ページ\)](#)
- [user \(D-43 ページ\)](#)
- [vmware-tools \(D-46 ページ\)](#)

clustering

デバイス上のクラスタリングに対してバイパスを無効にするか、または設定します。このコマンドは仮想デバイス、ASA FirePOWER デバイス、およびセカンダリ スタック メンバーとして設定されているデバイスでは使用できません。

アクセス (Access)

設定 (Configuration)

構文

```
configure clustering {disable | bypass}
```

例

```
> configure clustering disable
```

bypass

シリーズ 3 デバイスでは、インライン ペアがフェールオープン(ハードウェア バイパス)またはフェールクローズ モードに移行されます。このコマンドは、**Bypass Mode** インライン設定オプションが **Bypass** に設定されている場合にのみ使用できます。

**注意**

このコマンドでインライン セットがフェールオープン モードに移行された管理対象デバイスにアクセス コントロール ポリシーを適用したり、侵入ポリシーを再適用したりすることはできません。

デバイスをリブートすると、インターフェイス ペアがフェールオープン モードから抜けることに注意してください。

アクセス (Access)**設定 (Configuration)****構文**

```
configure bypass {open | close} {interface}
```

ここで、*interface* はインライン ペアのいずれかのハードウェア ポートの名前です。

例

```
> configure bypass open s1p1
```

gui

デバイスの Web インターフェイス (システムのメジャーな更新時に表示される、簡潔なアップグレード Web インターフェイスなど) を有効または無効にします。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)**設定 (Configuration)****構文**

```
configure gui {enable | disable}
```

例

```
> configure gui disable
```

iab

インテリジェント アプリケーション バイパス (IAB) を設定します。このコマンドには、管理対象デバイスでバージョン 5.4.0.10 以降が必要です。Defense Center では、IAB 機能を実装するにはバージョン 5.4.1.9 以降が必要で、IAB イベントを提供するにはバージョン 5.4.1.10 以降が必要です。

IAB は、パフォーマンスとフローのしきい値を超過した場合に追加のインスペクションなしでネットワークを通過するトラフィックを信頼します。システムはトラフィックがディープインスペクションの対象となる前に、アクセス コントロール ルールまたはアクセス コントロール ポリシーのデフォルトのアクションで許可されたトラフィック上で IAB を実行します。テストモードでは、実際に IAB を実行していた場合にしきい値を超えるかどうかの判断と、超えた場合にどのフローが信頼されていたかの特定を行うことができます。IAB を設定した後で、管理対象デバイスにアクセス コントロール ポリシーを展開する必要があります。

表 D-1 基本的な IAB パラメータ

パラメータ	説明
on	アクティブ モードで IAB を設定します。
test	テスト モードで IAB を設定します。
disable	IAB を無効にします。

パフォーマンスおよびフローのしきい値

パフォーマンス スキャン間隔を設定し、4 つのインスペクション パフォーマンスしきい値のうち少なくとも 1 つと、4 つのフロー バイパスしきい値のうち 1 つを設定する必要があります。パフォーマンスしきい値を超えると、フローしきい値が調べられ、さらにフローしきい値を超えた場合にはトラフィックが信頼されます。いずれかの種類のしきい値を複数設定した場合は、それぞれの 1 つのみを超過する必要があります。いずれのしきい値も、デフォルトでは無効になっています (0 に設定されています)。

インスペクション パフォーマンスしきい値: 侵入インスペクションのパフォーマンスの限界を定めるもので、この限界を超えると、フローしきい値のインスペクションがトリガーされます。IAB では、0 に設定された インスペクション パフォーマンスしきい値は使用しません。

表 D-2 インスペクションパフォーマンスしきい値パラメータ

パラメータ	説明的名前	説明	範囲
間隔	パフォーマンス サンプル インターバル (Performance Sample Interval)	システムが IAB パフォーマンスしきい値との比較のためにシステム パフォーマンス メトリックを収集する IAB パフォーマンス サンプリング スキャンの間隔。	1 ~ 1000 秒
drops	ドロップ率 (Drop Percentage)	消費が激しい侵入ルール、ファイル ポリシー、圧縮解除などによってパフォーマンス過負荷となったためにパケットがドロップされた場合にドロップされたパケットが、パケット全体に占める割合の平均。侵入ルールのような通常の設定によってドロップされるパケットは含まれません。1 より大きい整数を指定すると、指定されたパーセンテージのパケットがドロップされたときに IAB がアクティブ化することに注意が必要です。1 を指定すると、0 ~ 1 までのパーセンテージによって IAB がアクティブ化します。これにより、少ないパケット数で IAB がアクティブ化します。	0 ~ 100 %
cpu	プロセッサ使用率 (Processor Utilization Percentage)	プロセッサ リソースの平均使用率。	0 ~ 100 %
遅延	パケット遅延	平均パケット遅延。	0 ~ 1000000 マイクロ秒
レート	フロー レート (Flow Rate)	1 秒あたりのフロー数で測定される、システムによるフロー処理率。このオプションでは、IAB は、フローを件数ではなく レートで測定するように設定されることに注意が必要です。	0 ~ 1000000 フロー/秒

フロー バイパスしきい値: フローの限界を定めるもので、この限界を超えると、IAB は、アクティブ モードではトラフィックを信頼し、テスト モードではトラフィックを許可してさらなるインスペクションの対象にします。IAB では、0 に設定された フロー バイパスしきい値は使用しません。

表 D-3 フローバイパスしきい値パラメータ

パラメータ	説明的名前	説明	範囲
kbytes	フローあたりのバイト数 (Bytes per Flow)	フローに含めることができる最大サイズ (KB)。	0 ~ 2147483647 キロバイト
packets: パケット数	フローあたりのパケット数 (Packets per Flow)	フローに含めることができるパケットの最大個数。	0 ~ 2147483647 パケット
duration	フロー継続時間 (Flow Duration)	フローをオープンのままにできる最長時間 (秒)。	0 ~ 2147483647 秒
velocity	フロー速度 (Flow Velocity)	最大転送速度 (KB/秒)。	0 ~ 2147483647 キロバイト/秒

すべてのパラメータを同時に正しい順序で設定します。入力したパラメータの数がパラメータの最大数よりも少ない場合は、次のパラメータを入力するように求められます。

アクセス (Access)

設定 (Configuration)

構文

```
configure iab {on | test} interval drops cpu latency rate kbytes packets duration
velocity
```

例

```
configure iab on 5 1 95 250 0 500000 0 0 25000
```

関連コマンド

```
show iab
```

lcd

デバイスの正面の LCD ディスプレイを有効または無効にします。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

設定 (Configuration)

構文

```
configure lcd {enable | disable}
```

例

```
> configure lcd disable
```

log-ips-connections

記録された侵入イベントに関連付けられている接続イベントのロギングを有効または無効にします。

アクセス (Access)

設定 (Configuration)

構文

```
configure log-ips-connections {enable | disable}
```

例

```
> configure log-ips-connections disable
```

manager

`configure manager` コマンドは、管理元の 防御センター へのデバイスの接続を設定します。

アクセス (Access)

設定 (Configuration)

追加

管理元の 防御センター からの接続を承認するようデバイスを設定します。このコマンドは、デバイスがアクティブに管理されていない場合にのみ機能します。

デバイスを 防御センター に登録するには、一意の英数字登録キーが必須です。ほとんどの場合は、登録キーと一緒にホスト名または IP アドレスを指定する必要があります。ただし、デバイスと 防御センター が NAT デバイスによって分けられている場合は、登録キーと一緒に一意の NAT ID を入力し、ホスト名の代わりに DONTRESOLVE を指定します。

構文

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey [nat_id]
```

ここで {hostname | IPv4_address | IPv6_address | DONTRESOLVE} は、このデバイスを管理する 防御センター の DNS ホスト名、または IP アドレス (IPv4 または IPv6) を表します。防御センター が直接アドレス指定できない場合は、DONTRESOLVE を使用します。DONTRESOLVE を使用する場合は、nat_id が必要です。Regkey はデバイスを 防御センター へ登録するのに必要な、英数字の一意の登録キーです。nat_id は、防御センター とデバイス間の登録プロセス中に使用されるオプションの英数字文字列です。ホスト名が DONTRESOLVE に設定されている場合に必須です。

例

```
> configure manager add DONTRESOLVE abc123 efg456
```

削除

防御センターの接続情報をデバイスから削除します。このコマンドは、デバイスがアクティブに管理されていない場合のみ機能します。

構文

```
configure manager delete
```

例

```
> configure manager delete
```

mpls-depth

管理インターフェイスで MPLS レイヤの数を設定します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス (Access)

設定 (Configuration)

構文

```
configure mpls-depth {depth}
```

ここで *depth* は 0~6 の数値です。

例

```
> configure mpls-depth 3
```

network

`configure network` コマンドは、デバイスの管理インターフェイスを設定します。

アクセス (Access)

設定 (Configuration)

dns searchdomains

DNS 検索ドメインの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure network dns searchdomains {searchlist}
```

searchlist はカンマで区切られたドメインのリストです。

例

```
> configure network dns searchdomains foo.bar.com,bar.com
```

dns servers

DNS サーバの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure network dns servers {dnslist}  
dnslist は、カンマで区切られた DNS サーバのリストです。
```

例

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

hostname

デバイスのホスト名を設定します。

構文

```
configure network hostname {name}  
name は新しいホスト名です。
```

例

```
> configure network hostname sfrocks
```

http-proxy

シリーズ 3 および仮想デバイスで、HTTP プロキシを設定します。コマンドを発行した後で、CLI はユーザに対して HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかを尋ねます。認証が必要な場合はプロキシのユーザ名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

仮想デバイス上でこのコマンドを使用して、HTTP プロキシサーバを設定し、仮想デバイスが動的解析のためにファイルを Collective Security Intelligence クラウドへ送信できるようにします。

構文

```
configure network http-proxy
```

例

```
> configure network http-proxy  
Manual proxy configuration  
Enter HTTP Proxy address:  
Enter HTTP Proxy Port:  
Use Proxy Authentication? (y/n) [n]:  
Enter Proxy Username:  
Enter Proxy Password:  
Confirm Proxy Password:
```

http-proxy-disable

シリーズ 3 および仮想デバイスで、すべての HTTP プロキシの設定を削除します。

構文

```
configure network http-proxy-disable
```

例

```
> configure network http-proxy-disable
Are you sure that you wish to delete the current http-proxy configuration? (y/n):
```

ipv4 delete

デバイスの管理インターフェイスの IPv4 設定を無効にします。

構文

```
configure network ipv4 delete
```

例

```
> configure network ipv4 delete
```

ipv4 dhcp

デバイスの管理インターフェイスの IPv4 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

構文

```
configure network ipv4 dhcp
```

例

```
> configure network ipv4 dhcp
```

ipv4 manual

デバイスの管理インターフェイスの IPv4 設定を手動で設定します。

構文

```
configure network ipv4 manual ipaddr netmask gw
```

ここで *ipaddr* は IP アドレスで、*netmask* はサブネットマスク、*gw* はデフォルト ゲートウェイの IPv4 アドレスです。

例

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

ipv6 delete

デバイスの管理インターフェイスの IPv6 設定を無効にします。

構文

```
configure network ipv6 delete
```

例

```
> configure network ipv6 delete
```

ipv6 dhcp

デバイスの管理インターフェイスの IPv6 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

構文

```
configure network ipv6 dhcp
```

例

```
> configure network ipv6 dhcp
```

ipv6 router

デバイスの管理インターフェイスの IPv6 設定をルータに設定します。管理インターフェイスは IPv6 ルータと通信して、設定情報を取得します。

構文

```
configure network ipv6 router
```

例

```
> configure network ipv6 router
```

ipv6 manual

デバイスの管理インターフェイスの IPv6 設定を手動で設定します。

構文

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw]
```

ここで *ip6addr/ip6prefix* は IP アドレスと接頭辞の長さで、*ip6gw* はデフォルト ゲートウェイの IPv6 アドレスを表します。

例

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

management-interface disable

指定した管理インターフェイスを無効にします。

構文

```
configure network management-interface disable ethn  
n は、無効にする管理インターフェイスの数です。
```

例

```
> configure network management-interface disable eth1
```

management-interface disable-event-channel

指定した管理インターフェイスを介したイベント伝送を無効にします。

構文

```
configure network management-interface disable-event-channel ethn  
n は、無効にする管理インターフェイスの数です。
```

例

```
> configure network management-interface disable-event-channel eth1
```

management-interface disable-management-channel

指定した管理インターフェイスを介した管理伝送を無効にします。

構文

```
configure network management-interface disable-management-channel ethn  
n は、無効にする管理インターフェイスの数です。
```

例

```
> configure network management-interface disable-management-channel eth1
```

management-interface enable

指定した管理インターフェイスを有効にします。

構文

```
configure network management-interface enable ethn  
n は、有効にする管理インターフェイスの数です。
```

例

```
> configure network management-interface enable eth1
```


management-interface enable-event-channel

指定した管理インターフェイスを介したイベント伝送を有効にします。

構文

```
configure network management-interface enable-event-channel ethn  
n
```

n は、有効にする管理インターフェイスの数です。

例

```
> configure network management-interface enable-event-channel eth1
```

management-interface enable-management-channel

指定した管理インターフェイスを介した管理伝送を有効にします。

構文

```
configure network management-interface enable-management-channel ethn  
n
```

n は、有効にする管理インターフェイスの数です。

例

```
> configure network management-interface enable-management-channel eth1
```

management-interface tcpport

管理用の TCP ポートの値を変更します。

構文

```
configure network management-interface tcpport port  
port
```

port は設定する管理ポートの値です。

例

```
> configure network management-interface tcpport 8500
```

management-port

デバイスの TCP 管理ポートの値を設定します。

構文

```
configure network management-port number  
number
```

number は設定する管理ポートの値を表します。

例

```
> configure network management-port 8500
```

static-routes ipv4 add

指定した管理インターフェイスの IPv4 スタティック ルートを追加します。

構文

```
configure network static-routes ipv4 add interface destination netmask gateway
```

interface は管理インターフェイス、*destination* は宛先 IP アドレス、*netmask* はネットワーク マスク アドレス、*gateway* は追加するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv4 add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv4 delete

指定した管理インターフェイスの IPv4 スタティック ルートを削除します。

構文

```
configure network static-routes ipv4 delete interface destination netmask gateway
```

interface は管理インターフェイス、*destination* は宛先 IP アドレス、*netmask* はネットワーク マスク アドレス、*gateway* は削除するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv4 delete eth1 10.115.24.0 255.255.255.0  
10.115.9.2
```

static-routes ipv6 add

指定した管理インターフェイスの IPv6 スタティック ルートを追加します。

構文

```
configure network static-routes ipv6 add interface destination prefix gateway
```

interface は管理インターフェイス、*destination* は宛先 IP アドレス、*prefix* は IPv6 プレフィックス長、*gateway* は追加するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv6 add eth1 2001:DB8:3ffe:1900:4545:3:200:  
f8ff:fe21:67cf 64
```

static-routes ipv6 delete

指定した管理インターフェイスの IPv6 スタティック ルートを削除します。

構文

```
configure network static-routes ipv6 delete interface destination prefix gateway
```

interface は管理インターフェイス、*destination* は宛先 IP アドレス、*prefix* は IPv6 プレフィックス長、*gateway* は削除するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv6 delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff:  
fe21:67cf 64
```

password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLIは現在の(古い)パスワードを入力するようユーザに要求し、その後で新しいパスワードを2回入力するよう要求します。

アクセス (Access)

基本

構文

```
configure password
```

例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

stacking disable

管理対象デバイスで、そのデバイスのスタッキング設定をすべて削除します。プライマリとして設定されているデバイスでは、スタックが完全に削除されます。セカンダリとして設定されているデバイスでは、デバイスはスタックから削除されます。このコマンドは、仮想デバイス、またはASA FirePOWER デバイスでは使用できません。また、このコマンドを使用して、クラスタ化されたスタックをクラスタ化解除することはできません。

スタッキング階層の上位アプライアンスとの通信を確立できない場合は、このコマンドを使用します。防御センターを通信で使用できる場合は、代わりに 防御センター Web インターフェイスを使用するよう伝えるメッセージが表示されます。同様に、プライマリ デバイスを使用できる場合に、セカンダリとして設定されているデバイス上で `stacking disable` を入力すると、プライマリ デバイスからコマンドを入力するよう伝えるメッセージが表示されます。

アクセス (Access)

設定 (Configuration)

構文

```
configure stacking disable
```

例

```
> configure stacking disable
```

user

仮想デバイスでのみ使用できます。`configure user` コマンドは、デバイスのローカルユーザデータベースを管理します。

アクセス (Access)

設定 (Configuration)

アクセス (Access)

指定したユーザのアクセス レベルを変更します。このコマンドは、指定されたユーザが次にログインするとき有効になります。

構文

```
configure user access username [basic | config]
```

例

```
> configure user access jdoe basic
```

username は、アクセスを変更するユーザの名前を表します。*basic* は **basic** アクセスを、*config* は **configuration** アクセスを表します。

追加

指定された名前とアクセス レベルで新しいユーザを作成します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

構文

```
configure user add username [basic | config]
```

ここで *username* は新しいユーザの名前を表します。*basic* は **basic** アクセス、*config* は **configuration** アクセスを表します。

例

```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

aging

ユーザ パスワードに有効期限を設定します。

構文

```
configure user aging username max_days warn_days
```

ここで *username* はユーザの名前を表します。*max_days* はパスワードが有効な最大日数、*warn_days* は、有効期限が切れるまでにパスワードを変更するためにユーザが使用できる日数を表します。

例

```
> configure user aging jdoe 100 3
```

削除

ユーザとユーザのホーム ディレクトリを削除します。

構文

```
configure user delete username
```

username はユーザの名前を表します。

例

```
> configure user delete jdoe
```

disable

ユーザを無効にします。無効なユーザはログインできません。

構文

```
configure user disable username
```

username はユーザの名前を表します。

例

```
> configure user disable jdoe
```

enable

ユーザを有効にします。

構文

```
configure user enable username
```

username はユーザの名前を表します。

例

```
> configure user enable jdoe
```

forcereset

ユーザが次にログインするときに、パスワードの変更を要求します。ユーザがログインしてパスワードを変更すると、強度のチェックが自動的に有効になります。

構文

```
configure user forcereset username
```

username はユーザの名前を表します。

例

```
> configure user forcereset jdoe
```

maxfailedlogins

指定したユーザが、ログインで失敗できる最大回数を設定します。

構文

```
configure user maxfailedlogins username number
```

username はユーザの名前、*number* は、ログインで失敗できる最大回数を表します。

例

```
> configure user maxfailedlogins jdoe 3
```

password

ユーザのパスワードを設定します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

構文

```
configure user password username
```

`username` はユーザの名前を表します。

例

```
> configure user password jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

strengthcheck

ユーザのパスワードに対する強度の要件を有効または無効にします。ユーザ パスワードの有効期限が切れた場合、または `configure user forcereset` コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

構文

```
configure user strengthcheck username {enable | disable}
```

`username` はユーザの名前を表します。`enable` は指定されたユーザのパスワードの要件を設定し、`disable` は、指定されたユーザのパスワードの要件を削除します。

例

```
> configure user strengthcheck jdoe enable
```

unlock

ログイン失敗の最大数を超過したユーザをロック解除します。

構文

```
configure user unlock username
```

`username` はユーザの名前を表します。

例

```
> configure user unlock jdoe
```

vmware-tools

仮想デバイス上で VMware Tools 機能を有効または無効にします。このコマンドは、仮想デバイスでのみ使用できます。

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティスイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- `guestInfo`
- `powerOps`

- スナップショット
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト (<http://www.vmware.com>) を参照してください。

アクセス (Access)

基本

構文

```
configure vmware-tools (enable | disable)
```

例

```
> configure vmware-tools enable
```

system コマンド

system コマンドを使用して、システム全体のファイルおよびアクセス コントロールの設定を管理することができます。Configuration CLI アクセス権を持つユーザのみが、システム モードでコマンドを発行できます。

以降の項で、system コマンドについて説明します。

- [access-control \(D-47 ページ\)](#)
- [disable-http-user-cert \(D-48 ページ\)](#)
- [file \(D-49 ページ\)](#)
- [generate-troubleshoot \(D-50 ページ\)](#)
- [ldapsearch \(D-50 ページ\)](#)
- [lockdown-sensor \(D-51 ページ\)](#)
- [nat rollback \(D-51 ページ\)](#)
- [reboot \(D-51 ページ\)](#)
- [restart \(D-52 ページ\)](#)
- [shutdown \(D-52 ページ\)](#)

access-control

system access-control コマンドは、ユーザがデバイス上でアクセス コントロールの設定を管理できるようにします。

アクセス (Access)

設定 (Configuration)

archive

現在適用されているアクセス コントロール ポリシーを、`/var/common` にテキスト ファイルとして保存します。

構文

```
system access-control archive
```

例

```
> system access-control archive
```

clear-rule-counts

アクセス コントロール ルールのヒット数を 0 にリセットします。

構文

```
system access-control clear-rule-counts
```

例

```
> system access-control clear-rule-counts
```

rollback

以前に適用していたアクセス コントロールの設定に、システムを戻します。クラスタ化されたデバイス、およびスタック デバイスではこのコマンドは使用できません。

構文

```
system access-control rollback
```

例

```
> system access-control rollback
```

disable-http-user-cert

システム上に存在するすべての HTTP ユーザ証明書を削除します。

アクセス (Access)

設定 (Configuration)

構文

```
system disable-http-user-cert
```

例

```
> system disable-http-user-cert
```


file

system file コマンドを使用すると、ユーザは、デバイス上の **common** ディレクトリにあるファイルを管理することができます。

アクセス (Access)

設定 (Configuration)

copy

FTP を使用して、ログイン ユーザ名を使用しているホスト上のリモート ロケーションへファイルを転送します。ローカル ファイルは **common** ディレクトリに配置する必要があります。

構文

```
system file copy hostname username path filenames filenames ...
```

hostname はターゲットのリモート ホストの名前または IP アドレスを表します。*username* はリモート ホスト上のユーザの名前、*path* はリモート ホスト上の宛先パス、*filenames* は転送するローカル ファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file copy sfrocks jdoe /pub *
```

削除

common ディレクトリから、指定したファイルを削除します。

構文

```
system file delete filenames filenames ...
```

filenames は削除するファイルを指定します。複数のファイル名はスペースで区切って指定します。

例

```
> system file delete *
```

list

ファイル名が指定されていない場合は、**common** ディレクトリ内のすべてのファイルについて変更の時刻、サイズ、およびファイル名が表示されます。ファイル名が指定されている場合は、指定されたファイル名と一致したファイルで、変更の時刻、サイズ、およびファイル名が表示されます。

構文

```
system file list {filenames filenames ...}
```

filenames は表示するファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file list
```

secure-copy

SCP を使用して、ログイン ユーザ名を使用しているホスト上のリモート ロケーションへファイルを転送します。ローカル ファイルは /var/common ディレクトリに配置する必要があります。

構文

```
system file secure-copy hostname username path filenames filenames ...
```

hostname はターゲットのリモート ホストの名前または IP アドレスを表します。*username* はリモート ホスト上のユーザの名前、*path* はリモート ホスト上の宛先パス、*filenames* は転送するローカル ファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

generate-troubleshoot

シスコが解析に使用するトラブルシューティング データを生成します。

アクセス (Access)

設定 (Configuration)

構文

```
system generate-troubleshoot
```

この構文は、どのトラブルシューティング データを表示するかを指定するための、オプションのパラメータのリストを表示します。

例

```
> system generate-troubleshoot
```

ldapsearch

ユーザが、指定された LDAP サーバのクエリを実行できるようにします。すべてのパラメータが必須であることに注意してください。

アクセス (Access)

設定 (Configuration)

構文

```
system ldapsearch host port baseDN userDN basefilter
```

host は LDAP サーバのドメイン、*port* は LDAP サーバのポート、*baseDN* は検索する DN (識別名)、*userDN* は LDAP ディレクトリへバインドするユーザの DN、*basefilter* は検索するレコードを表します。

例

```
> system ldapsearch ldap.example.com 389 cn=users,
dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

lockdown-sensor

expert コマンドを削除し、デバイス上の bash シェルへアクセスします。



注意

このコマンドは、サポートからのホットフィックスがない場合は取り消すことはできません。使用には注意が必要です。

アクセス (Access)

設定 (Configuration)

構文

```
system lockdown-sensor
```

例

```
> system lockdown-sensor
```

nat rollback

以前に適用していた NAT の設定に、システムを戻します。このコマンドは、仮想デバイスと ASA FirePOWER デバイスでは使用できません。クラスタ化されたデバイス、およびスタック デバイスではこのコマンドは使用できません。

アクセス (Access)

設定 (Configuration)

構文

```
system nat rollback
```

例

```
> system nat rollback
```

reboot

デバイスをリブートします。

アクセス (Access)

設定 (Configuration)

構文

```
system reboot
```

例

```
> system reboot
```

restart

デバイス アプリケーションを再起動します。

アクセス (Access)

設定 (Configuration)

構文

```
system restart
```

例

```
> system restart
```

shutdown

デバイスをシャットダウンします。このコマンドは ASA FirePOWER モジュールでは使用できません。

アクセス (Access)

設定 (Configuration)

構文

```
system shutdown
```

例

```
> system shutdown
```