



ヘルパーユーティリティ

ヘルパーユーティリティを使用すると、Cisco Security Packet Analyzer 2400 シリーズ アプライアンスで次のタスクを実行できます。



注

ヘルパーユーティリティへのアクセス方法については、[リカバリ インストール\(6-3 ページ\)](#)を参照してください。

図 E-1 ヘルパーユーティリティメニュー

```
=====
Cisco Systems, Inc.
Network Analysis Module (SEC-PA-2400-K9) helper utility
Version 1.1(0.25)

-----
Main menu
1 - Download application image and write to HDD
2 - Download application image and reformat HDD
3 - Install application image from CD and reformat HDD
4 - Display software versions
5 - Reset application image CLI passwords to default
6 - Send Ping
7 - Configure Capture RAID settings
8 - Install application image from flash and reformat HDD
f - Check for and fix file system errors on local disk
s - Show upgrade log
n - Configure network
r - Exit and reset Services Engine
h - Exit and shutdown Services Engine
```

次の項では、[ヘルパーユーティリティメニュー](#)、各オプションの内容、および特定のオプションの使用要件について説明します。

ヘルパー ユーティリティメニューの概要

表 E-1 ヘルパー ユーティリティメニューオプションの概要

メニュー オプション	説明	参照先
1	アプリケーションイメージをダウンロードし、ハードディスクドライブに書き込みます。	オプション 1: アプリケーションイメージをダウンロードし、HDD に書き込む (E-4 ページ)
2	アプリケーションイメージをダウンロードし、ハードディスクドライブを再フォーマットします。	オプション 2: アプリケーションイメージをダウンロードし、HDD を再フォーマットする (E-4 ページ)
3	CD からアプリケーションイメージをインストールします。	オプション 3: CD からアプリケーションイメージをインストールする (E-5 ページ)
4	ハードディスクに格納された現在の Cisco Security Packet Analyzer アプリケーションイメージのバージョンを表示します。	オプション 4: ソフトウェアバージョンを表示する (E-5 ページ)
5	ルートユーザと管理ユーザのパスワードをデフォルト値にリセットします。	オプション 5: アプリケーションイメージ CLI パスワードをデフォルト値にリセットする (E-5 ページ)
6	ping を実行して、ネットワーク接続が存在するかどうかを調べます。	オプション 6: ping を実行する (E-5 ページ)
7	キャプチャ RAID を設定します。	オプション 7: キャプチャ RAID を設定する (E-6 ページ)
8	フラッシュからアプリケーションイメージをインストールし、ハードディスクドライブを再フォーマットします。	オプション 8: フラッシュからアプリケーションイメージをインストールし、HDD を再フォーマットする (E-7 ページ)
f	ローカルディスクのファイルシステムエラーをチェックし、修正します。	オプション f: ローカルディスクのファイルシステムエラーをチェックし、修正する (E-7 ページ)
s	アップグレードログを表示します。	オプション s: アップグレードログを表示する (E-7 ページ)
n	アプライアンスのネットワークパラメータを設定します。	オプション n: ネットワークを設定する (E-3 ページ)
r	ヘルパー ユーティリティを終了し、電源を再投入して(リブートして)Cisco Security Packet Analyzer アプリケーションイメージを起動します。	オプション r: サービスエンジンを終了し、リセットする (E-7 ページ)
h	ヘルパー ユーティリティを終了し、Cisco Security Packet Analyzer アプライアンスをシャットダウンします。	オプション h: サービスエンジンを終了し、シャットダウンする (E-8 ページ)

オプション n: ネットワークを設定する

オプション n を使用して、アプライアンスのネットワーク パラメータを設定します。

- ステップ 1** [Configure Network Interface] メニューが表示されたら、**1** と入力してネットワークを手動で設定します。

```
-----
Configure Network interface:
1 - Configure network manually
2 - Show config
3 - Write config to application image
r - return to main menu
Selection [123r]: 1
```

- ステップ 2** ユーティリティで、アプライアンスの IP アドレス、ネットマスク、およびデフォルトゲートウェイを入力するよう求められます。

```
Enter IP configuration:
IP address []: 172.20.122.93
netmask []: 255.255.255.128
default gateway []: 172.20.122.1
```

```
-----
Configure Network interface:
1 - Configure network manually
2 - Show config
3 - Write config to application image
r - return to main menu
Selection [123r]:
```

- ステップ 3** 使用しているネットワーク設定を確認するには、**2** と入力します。

```
Selection [123r]: 2

eth0      Link encap:Ethernet HWaddr 00:0E:0C:EE:50:3E
          inet addr:172.20.122.93 Bcast:172.20.122.127 Mask:255.255.255.128
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:210 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13632 (13.3 KiB) TX bytes:0 (0.0 b)

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
172.20.122.0 0.0.0.0 255.255.255.128 U 0 0 eth0
0.0.0.0 172.20.122.1 0.0.0.0 UG 0 0 eth0
-----
Configure Network interface:
1 - Configure network manually
2 - Show config
3 - Write config to application image
r - return to main menu
Selection [123r]:
```

オプション1:アプリケーションイメージをダウンロードし、HDDに書き込む

オプション1を使用して、FTPサーバの場所から現在のアプリケーションイメージのバージョンをダウンロードし、イメージをハードディスクに書き込みます。



注

Cisco Security Packet Analyzer アプリケーションがすでにインストール済みで、ネットワークが設定されている場合、ネットワーク設定がヘルパーにより自動的に検出されます。検出されない場合は、このオプションを使用する前に、**オプション n** を使用してネットワークを設定する必要があります。

このオプションを使用すると、FTPサーバの場所または HTTP を使用してアクセスできる場所から現在のアプリケーションのバージョンがダウンロードされます。また、[最新の Cisco Security Packet Analyzer ソフトウェア バージョン](#) を Cisco.com からダウンロードすることもできます。

この URL を使用するには、シスコ サービス契約を締結している必要があり、zip 形式のソフトウェアをダウンロードするためにインターネットへのアクセスが必要です。

オプション2:アプリケーションイメージをダウンロードし、HDDを再フォーマットする

オプション2を使用して、現在のアプリケーションイメージをダウンロードし、イメージをハードディスクに書き込みます。



注意

このオプションを使用すると、アプリケーションイメージを書き込む前にハードディスクが再フォーマットされ、レポート、パケットキャプチャ、設定などのすべてのデータが破棄されます。ただし、ネットワーク接続設定は保持されます。



注

Cisco Security Packet Analyzer アプリケーションがすでにインストール済みで、ネットワークが設定されている場合、ネットワーク設定がヘルパーにより自動的に検出されます。検出されない場合は、このオプションを使用する前に、**オプション n** を使用してネットワークを設定する必要があります。

このオプションを使用すると、FTPサーバの場所または HTTP を使用してアクセスできる場所から現在のアプリケーションイメージのバージョンがダウンロードされます。また、[最新の Cisco Security Packet Analyzer ソフトウェア バージョン](#) を Cisco.com からダウンロードすることもできます。

この URL を使用するには、シスコ サービス契約を締結している必要があり、zip 形式のソフトウェアをダウンロードするためにインターネットへのアクセスが必要です。

オプション 3: CD からアプリケーションイメージをインストールする

オプション 3 を使用して、リカバリ CD から現在のアプリケーションイメージをインストールします。以前にアーカイブした Packet Analyzer ソフトウェアバージョンをダウンロードするためにネットワークに接続できない場合には、このオプションが必要になることがあります。



注意

このオプションを使用すると、アプリケーションイメージを書き込む前にハードディスクが再フォーマットされ、レポート、パケットキャプチャ、設定などのすべてのデータが破棄されます。ただし、ネットワーク接続設定は保持されます。



注

リカバリ CD で利用可能な Packet Analyzer ソフトウェアのバージョンは、そのソフトウェアの最初のリリースであり、パッチやアップグレードを含んでいません。このオプションを使用する場合は、[ソフトウェアのアップグレード\(6-2 ページ\)](#)を参照してください。

オプション 4: ソフトウェアバージョンを表示する

オプション 4 を使用すると、ハードディスクに保存されている現在の Cisco Security Packet Analyzer アプリケーションイメージバージョンが表示されます。

```
Selection [123456789dnfrh]:4
```

```
-----
```

```
SECFA application version: 6.2(2) RELEASE SOFTWARE
```

```
Selection [123456789dnfrh]:
```

オプション 5: アプリケーションイメージ CLI パスワードをデフォルト値にリセットする

オプション 5 を使用して、ルートユーザと管理ユーザのパスワードをデフォルト値にリセットします。

オプション 6: ping を実行する

オプション 7 を使用して、ping を実行し、ネットワーク接続が存在するかどうかを調べます。要求された場合は、ping を実行する対象の IP アドレスまたは完全ドメイン名を入力します。

```
IP address to ping []: 172.20.122.91
```

```
Sending 5 ICMP ECHO_REQUEST packets to 172.20.122.91.
```

```
PING 172.20.122.91 (172.20.122.91) 56(84) bytes of data.
```

```
64 bytes from 172.20.122.91: icmp_seq=1 ttl=64 time=0.151 ms
```

```
64 bytes from 172.20.122.91: icmp_seq=2 ttl=64 time=0.153 ms
```

■ オプション7:キャプチャ RAID を設定する

```

64 bytes from 172.20.122.91: icmp_seq=3 ttl=64 time=0.125 ms
64 bytes from 172.20.122.91: icmp_seq=4 ttl=64 time=0.102 ms
64 bytes from 172.20.122.91: icmp_seq=5 ttl=64 time=0.166 ms

--- 172.20.122.91 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.102/0.139/0.166/0.025 ms

```

オプション7:キャプチャ RAID を設定する

オプション8を使用して、キャプチャ RAID を設定します。このオプションには、次のサブオプションが含まれます。

```

-----
Capture RAID Menu
1 - Rebuild all failed disks
2 - Add all new disks to the Capture RAID
3 - Decommission the Capture RAID (destructive)
4 - Construct the Capture RAID (destructive)
c - Show current Capture RAID configuration
p - Show all progress of Capture RAID reconfiguration
r - return to main menu
-
Selection [1234cpr]:

```

次の表で、これらの各サブオプションについて説明します。

表 E-2 キャプチャ RAID メニュー オプション

メニュー オプション	説明
1	障害が発生したすべてのディスクを再構築します。
2	新しいディスクをキャプチャ RAID に追加します。Cisco Security Packet Analyzer アプリケーションの再フォーマット インストールが最後に実行された以降にディスクが取り付けられた場合、RAID はそれらのディスクを含むように拡張されます。
3	キャプチャ RAID を解放します。このオプションを使用すると、ハードディスクがクリーンアップされ、キャプチャ データのみが破棄されます。他のすべてのデータはシステム RAID に保持されます。
4	キャプチャ RAID を構築します。
c	現在のキャプチャ RAID 設定を表示します。
p	キャプチャ RAID 再設定の進行状況を表示します。
r	メイン メニューに戻ります。

オプション 8:フラッシュからアプリケーションイメージをインストールし、HDDを再フォーマットする

オプション9を使用して、フラッシュからアプリケーションイメージをインストールし、ハードディスクを再フォーマットします。



注意

このオプションを使用すると、アプリケーションイメージを書き込む前にハードディスクが再フォーマットされ、レポート、パケットキャプチャ、設定などのすべてのデータが破棄されます。ただし、ネットワーク接続設定は保持されます。



注

Cisco Security Packet Analyzer アプリケーションがすでにインストール済みで、ネットワークが設定されている場合、ネットワーク設定がヘルパーにより自動的に検出されます。検出されない場合は、このオプションを使用する前に、オプション n を使用してネットワークを設定する必要があります。

オプション f:ローカルディスクのファイルシステムエラーをチェックし、修正する

オプション f を使用して、ローカルディスクのファイルシステムエラーを見つけ、修正します。パーティションサイズによっては、このオプションを実行するのに時間がかかることがあります。

オプション s:アップグレードログを表示する

オプション s を使用してアップグレードログを表示します。

オプション r:サービスエンジンを終了し、リセットする

オプション r を使用して、ヘルパーユーティリティを終了し、電源を再投入して(リブートして)、新しくインストールされたアプリケーションイメージを起動します。

オプション h: サービス エンジンを終了し、シャットダウンする

オプション h を使用して、ヘルパー ユーティリティを終了し、Cisco Security Packet Analyzer アプライアンスをシャットダウンします。

```
-----  
Selection [12345678fsnrh]: h  
About to exit and shutdown SECPA.  
Are you sure? [y/N] y  
Stopping internet superserver: inetd.  
Stopping OpenBSD Secure Shell server: sshd.  
Stopping internet superserver: xinetd.  
Stopping internet superserver: xinetd-ipv4.  
: done.  
Shutting down SECPA (SECPA2400-K9), part 1:  
Stopping klogd ...  
Stopping syslogd ...  
Sending all processes the TERM signal... done.  
Sending all processes the KILL signal... done.  
Unmounting remote filesystems... done.  
Deactivating swap...done.  
Unmounting local filesystems...done.  
Starting halt command: halt  
Power down.  
-----
```