



使用可能なコマンド

この章では、IPS 6.0 のコマンドをアルファベット順に示します。次の項があります。

- [anomaly-detection load](#) (P. 2-3)
- [anomaly-detection save](#) (P. 2-4)
- [banner login](#) (P. 2-5)
- [clear denied-attackers](#) (P. 2-6)
- [clear events](#) (P. 2-7)
- [clear line](#) (P. 2-8)
- [clear os-identification](#) (P. 2-10)
- [clock set](#) (P. 2-11)
- [configure](#) (P. 2-12)
- [copy](#) (P. 2-13)
- [copy ad-knowledge-base](#) (P. 2-16)
- [copy instance](#) (P. 2-17)
- [display serial](#) (P. 2-18)
- [downgrade](#) (P. 2-19)
- [end](#) (P. 2-20)
- [erase](#) (P. 2-21)
- [erase ad-knowledge-base](#) (P. 2-22)
- [exit](#) (P. 2-23)
- [iplog](#) (P. 2-24)
- [iplog-status](#) (P. 2-25)
- [list component-configurations](#) (P. 2-27)
- [more](#) (P. 2-28)
- [more begin](#) (P. 2-30)
- [more exclude](#) (P. 2-32)
- [more include](#) (P. 2-34)
- [packet](#) (P. 2-35)
- [password](#) (P. 2-37)
- [ping](#) (P. 2-39)
- [privilege](#) (P. 2-40)
- [recover](#) (P. 2-41)
- [rename ad-knowledge-base](#) (P. 2-42)
- [reset](#) (P. 2-43)

- service (P. 2-44)
- setup (P. 2-48)
- show ad-knowledge-base diff (P. 2-61)
- show ad-knowledge-base files (P. 2-63)
- show ad-knowledge-base thresholds (P. 2-64)
- show begin (P. 2-67)
- show clock (P. 2-69)
- show configuration (P. 2-70)
- show events (P. 2-71)
- show exclude (P. 2-73)
- show history (P. 2-74)
- show include (P. 2-75)
- show interfaces (P. 2-76)
- show inventory (P. 2-78)
- show os-identification (P. 2-79)
- show privilege (P. 2-80)
- show settings (P. 2-81)
- show ssh authorized-keys (P. 2-84)
- show ssh server-key (P. 2-85)
- show ssh host-keys (P. 2-86)
- show statistics (P. 2-87)
- show tech-support (P. 2-90)
- show tls fingerprint (P. 2-92)
- show tls trusted-hosts (P. 2-93)
- show users (P. 2-94)
- show version (P. 2-96)
- ssh authorized-key (P. 2-98)
- ssh generate-key (P. 2-99)
- ssh host-key (P. 2-100)
- terminal (P. 2-102)
- tls generate-key (P. 2-103)
- tls trusted-host (P. 2-104)
- trace (P. 2-106)
- upgrade (P. 2-107)
- username (P. 2-108)

anomaly-detection load

Knowledge Base (KB; 知識ベース) ファイルを、指定した仮想センサーの現行の KB として設定するには、特権 EXEC モードで **anomaly-detection load** コマンドを使用します。

anomaly-detection virtual-sensor load [initial | file name]

構文説明	パラメータ	説明
	<i>virtual-sensor</i>	仮想センサー。1 ~ 64 文字の大文字小文字を区別する文字列です。有効な文字は A ~ Z、a ~ z、0 ~ 9、「-」および「_」です。
	<i>name</i>	KB ファイル名。1 ~ 32 文字の大文字小文字を区別する文字列です。有効な文字は A ~ Z、a ~ z、0 ~ 9、「-」および「_」です。
	initial	初期の KB。
	file	既存の KB ファイル。

デフォルト デフォルトの動作または値はありません。

コマンド モード EXEC

サポートされるユーザロール 管理者

コマンド履歴	リリース	修正
	6.0(1)	このコマンドを導入。

使用上のガイドライン



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例 次の例は、現行の KB ファイルとして 2006-Mar-16-10_00_00 をロードします。

```
sensor# anomaly-detection vs0 load file 2006-Mar-16-10_00_00
sensor#
```

anomaly-detection save

現行の Anomaly Detection (AD; 異常検出) KB ファイルを取得してローカルに保存するには、特権 EXEC モードで **anomaly-detection save** コマンドを使用します。

anomaly-detection virtual-sensor save [*new-name*]

構文説明	
<i>virtual-sensor</i>	仮想センサー。1 ~ 64 文字の大文字小文字を区別する文字列です。有効な文字は A ~ Z、a ~ z、0 ~ 9、「-」および「_」です。
<i>new-name</i>	(オプション) 新しい KB ファイル名。最大 32 文字の大文字小文字を区別する文字列です。有効な文字は A ~ Z、a ~ z、0 ~ 9、「-」および「_」です。

デフォルト 生成されるデフォルトのファイル名は *YYYY-Mon-dd-hh_mm_ss* です。Mon は現在の月を示す 3 文字の省略形です。

コマンド モード EXEC

サポートされるユーザロール 管理者

コマンド履歴	リリース	修正
	6.0(1)	このコマンドを導入。

使用上のガイドライン このコマンドの実行時に AD がアクティブになっていないと、エラーが生成されます。初期の KB ファイルを上書きすることはできません。新しい名前を選択する場合でも、デフォルトの名前を使用する場合でも、KB ファイルの名前がすでに存在する場合は古い KB ファイルが上書きされます。

KB ファイルに使用できるサイズには、制限があります。新しい KB が生成されてこの制限に到達すると、最も古い KB (現行ファイルでも初期ファイルでもない場合) が削除されます。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例 次の例は、現行の KB を保存し、my-kb として保管します。

```
sensor# anomaly-detection vs0 save my-kb
sensor#
```

banner login

端末画面に表示するバナー メッセージを作成するには、グローバル コンフィギュレーション モードで **banner login** コマンドを使用します。ログイン バナーを削除するには、このコマンドの **no** 形式を使用します。バナー メッセージは、ユーザが CLI にアクセスしたときに、ユーザ名プロンプトとパスワード プロンプトの前に表示されます。

banner login

no banner login

構文説明

引数	CLI にログインする前に表示されるテキスト。メッセージの最大長は 2500 文字です。改行または疑問符 (?) を入力する場合は、その前にキーストローク Ctrl+V を入力する必要があります。
----	---

デフォルト

デフォルトの動作または値はありません。

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者

コマンド履歴

リリース	修正
5.0(1)	このコマンドを導入。

使用上のガイドライン

banner login コマンドによって、端末画面に表示される 2500 文字までのテキスト メッセージを作成できます。このメッセージは、CLI にアクセスしたときに表示されます。**Ctrl+V** を入力してから改行または疑問符 (?) を入力することによって、改行または疑問符をメッセージに含めることができます。改行は、作成したテキスト メッセージでは **^M** と表示されますが、ユーザに対してメッセージが表示されるときは、実際の改行として表示されます。

Message プロンプトで **Ctrl+C** を入力すると、メッセージの要求がキャンセルされます。



(注) このコマンドの形式は、Cisco IOS 12.0 の実装とは異なります。

例

次の例は、ログイン時に端末画面に表示されるメッセージを作成します。

```
sensor(config)# banner login
Banner[: This message will be displayed on login. ^M Thank you!
```

ログイン時に、次のメッセージが表示されます。

```
This message will be displayed on login.
```

```
Thank you!
password:
```

clear denied-attackers

現在の拒否 IP アドレスのリストを削除するには、特権 EXEC モードで **clear denied-attackers** コマンドを使用します。

clear denied-attackers [*virtual-sensor*] [*ip-address ip-address*]

構文説明	
<i>virtual-sensor</i>	(オプション) センサーに設定された仮想センサーの名前。クリア操作は、指定した仮想センサーに関連付けられているラーニングしたアドレスに制限されます。1～64文字の大文字小文字を区別する文字列です。有効な文字はA～Z、a～z、0～9、「-」および「_」です。仮想センサーの名前を指定しないと、拒否する攻撃者はすべてクリアされます。
<i>ip-address</i>	(オプション) クリアする IP アドレス。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者

コマンド履歴	リリース	修正
	5.0(1)	このコマンドを導入。
	6.0(1)	オプションの <i>virtual-sensor</i> パラメータおよび <i>ip-address</i> パラメータを追加。

使用上のガイドライン **clear denied-attackers** コマンドによって、拒否する攻撃者のリストをクリアし、以前拒否した IP アドレスとの通信を復元できます。このリストの IP アドレスを個別に選択し、削除することはできません。拒否する攻撃者のリストをクリアすると、リストからすべての IP アドレスが削除されます。

仮想センサーと IP アドレスはオプションです。仮想センサー名を指定すると、要求した仮想センサーだけを対象に IP アドレスがクリアされます。仮想センサー名を指定しないと、すべての仮想センサー上で IP アドレスがクリアされます。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、拒否する攻撃者のリストからすべての IP アドレスを削除します。

```
sensor# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of attackers
currently being denied by the system.
Continue with clear? []: yes
sensor#
```

関連コマンド	コマンド	説明
	show statistics denied-attackers	拒否する攻撃者のリストを表示します。

clear events

イベントストアをクリアするには、特権 EXEC モードで **clear events** コマンドを使用します。

clear events

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン

このコマンドを使用すると、イベントストアからすべてのイベントをクリアできます。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、イベントストアをクリアします。

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:yes
sensor#
```

clear line

別の CLI セッションを終了するには、特権 EXEC モードで **clear line** コマンドを使用します。

clear line *cli-id* [*message*]

構文説明

<i>cli-id</i>	ログインセッションに関連付けられている CLI ID 番号。 show users コマンドを参照してください。
<i>message</i>	(オプション) message を選択した場合、メッセージを受信するユーザに送信する内容を入力するように求めるプロンプトが表示されます。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

コマンド履歴

リリース	修正
5.0(1)	このコマンドを導入。

サポートされるユーザロール

管理者、オペレータ、ビューア



(注) オペレータとビューアは、現在のログインと同じユーザ名の回線のみをクリアできます。

使用上のガイドライン

clear line コマンドを使用して、別の回線で実行中の特定のセッションをログアウトさせます。終了しようとするログインセッションの端末に表示するメッセージ (オプション) を指定するには、**message** キーワードを使用します。**Ctrl+C** では要求がキャンセルされ、改行によって指定したメッセージとともに要求が送信されます。メッセージの最大長は 2550 文字です。**Ctrl+V** の後に改行を入力すると、メッセージテキストに改行を含めることができます。

clear line コマンドを使用して、サービス アカウントのログインをクリアすることはできません。



(注) **message** キーワードは、このコマンドの Cisco IOS 12.0 バージョンではサポートされていません。

例

次の例は、最大セッション数に達した後、管理者権限を持つユーザがログインしようとしたときに表示される出力を示します。

```
Error: The maximum allowed CLI sessions are currently open, would you like to
terminate one of the open sessions? [no] yes
CLI   ID       User Privilege
1253  admin1  administrator
1267  cisco   administrator
1398  test    operator

Enter the CLI ID to clear: 1253
Message:Sorry! I need access to the system, so I am terminating your session.
sensor#
```


次の例は、admin1 の端末に表示されるメッセージを示します。

```
sensor#  
***  
***  
Termination request from Admin0  
***  
Sorry! I need access to the system, so I am terminating your session.
```

次の例は、最大セッション数に達した後、オペレータまたはビューア権限を持つユーザがログインしようとしたときに表示される出力を示します。

```
Error: The maximum allowed CLI sessions are currently open, please try again later.
```

関連コマンド

コマンド	説明
show users	CLI にログインしているユーザに関する情報を表示します。

clear os-identification

センサーが受動分析によってラーニングした IP アドレスとの OS ID アソシエーションを削除するには、特権 EXEC モードで **clear os-identification** コマンドを使用します。

clear os-identification [*virtual-sensor*] learned [*ip-address*]

構文説明

<i>virtual-sensor</i>	(オプション) センサーに設定された仮想センサーの名前。クリア操作は、指定した仮想センサーに関連付けられているラーニングしたアドレスに制限されます。1 ~ 64 文字の大文字小文字を区別する文字列です。有効な文字は A ~ Z、a ~ z、0 ~ 9、「-」および「_」です。
<i>ip-address</i>	(オプション) クリアする IP アドレス。センサーは、指定された IP アドレスにマッピングされた OS ID をクリアします。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ

コマンド履歴

リリース	修正
6.0(1)	このコマンドを導入。

使用上のガイドライン

仮想センサーと IP アドレスはオプションです。IP アドレスを指定すると、指定した IP アドレスの OS ID だけがクリアされます。IP アドレスを指定しないと、ラーニングした OS ID がすべてクリアされます。

仮想センサーを指定すると、指定した仮想センサーの OS ID だけがクリアされます。仮想センサーを指定しないと、すべての仮想センサーのラーニングした OS ID がクリアされます。仮想センサーを指定せずに IP アドレスを指定した場合、すべての仮想センサーで IP アドレスがクリアされます。

例

次の例は、すべての仮想センサーを対象に IP アドレス 10.1.1.12 のラーニングした OS ID をクリアします。

```
sensor# clear os-identification learned 10.1.1.12
sensor#
```

clock set

アプライアンスのシステム クロックを手動で設定するには、特権 EXEC モードで **clock set** コマンドを使用します。

clock set *hh:mm[:ss] month day year*

構文説明		
<i>hh:mm[:ss]</i>	時 (24 時形式)、分、および秒形式の現在時間	
<i>month</i>	現在月 (月名)	
<i>day</i>	月の現在日 (日)	
<i>year</i>	現在年 (省略なし)	

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン 次の場合、システム クロックを設定する必要はありません。

- システムが、NTP または VINES クロック ソースなど、有効な外部タイミング機構と同期化されている場合
- カレンダ機能を持つルータを使用している場合

どの時刻源も使用できない場合に、**clock set** コマンドを使用します。このコマンドで指定する時間は、設定した時間帯での相対時間です。

例 次の例は、システム クロックを手動で 2002 年 7 月 29 日午後 1 時 32 分に設定します。

```
sensor# clock set 13:32 July 29 2002
sensor#
```

configure

グローバル コンフィギュレーション モードに入るには、特権 EXEC モードで **configure terminal** コマンドを使用します。

configure terminal

構文説明	terminal 端末からコンフィギュレーション コマンドを実行します。
デフォルト	デフォルトの動作または値はありません。
コマンド モード	EXEC
サポートされるユーザロール	管理者、オペレータ、ビューア
使用上のガイドライン	configure terminal コマンドを実行すると、グローバル コンフィギュレーション モードに入ることができます。
例	次の例は、モードを特権 EXEC モードからグローバル コンフィギュレーション モードに変更します。 <pre>sensor# configure terminal sensor(config)#</pre>

copy

IP ログおよびコンフィギュレーション ファイルをコピーするには、特権 EXEC モードで **copy** コマンドを使用します。

copy [/erase] *source-url destination-url*

copy iplog *log-id destination-url*

構文説明

/erase (オプション) コピーする前に宛先ファイルを消去します。



(注)

このキーワードは現行のコンフィギュレーションだけに適用され、バックアップ コンフィギュレーションは常に上書きされます。このキーワードが宛先の現行のコンフィギュレーションに対して指定されると、ソース コンフィギュレーションがシステムのデフォルト コンフィギュレーションに適用されます。宛先の現行のコンフィギュレーションに対して指定されない場合、ソース コンフィギュレーションは現行のコンフィギュレーションとマージされます。

<i>source-url</i>	コピーされるソース ファイルの場所。URL またはキーワードが一般的です。
<i>destination-url</i>	コピーされる宛先ファイルの場所。URL またはキーワードが一般的です。
<i>log-id</i>	コピーするファイルのログ ID。 iplog-status コマンドを使用して、 <i>log-id</i> を取得します。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ (copy iplog または packet-file のみ)、ビューア (copy iplog または packet-file のみ)

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン

ソースおよび宛先 URL の正確なフォーマットは、ファイルにより異なります。次の有効なタイプがサポートされています。

プレフィックス	ソースまたは宛先
ftp:	FTP ネットワーク サーバのソースまたは宛先 URL。このプレフィックスの構文は、次のとおりです。 ftp://[username@] location[/relativeDirectory]/filename ftp://[username@]location//absoluteDirectory/filename
scp:	SCP ネットワーク サーバのソースまたは宛先 URL。このプレフィックスの構文は、次のとおりです。 scp://[username@] location[/relativeDirectory]/filename scp://[username@] location//absoluteDirectory/filename

プレフィックス	ソースまたは宛先
http:	Web サーバのソース URL。このプレフィックスの構文は、次のとおりです。 http://[username@]location/directory/filename ソース URL のみを使用できます。
https:	Web サーバのソース URL。このプレフィックスの構文は、次のとおりです。 https://[username@]location/directory/filename ソース URL のみを使用できます。

センサーのファイルの場所を指定するには、キーワードを使用します。次のファイルがサポートされています。

キーワード	ソースまたは宛先
current-config	現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。
backup-config	コンフィギュレーションバックアップの保管場所。ファイルフォーマットは CLI コマンドです。
iplog	システムに組み込まれている iplog。IP ログはログ ID を基に検索されます。 iplog-status コマンドの出力を参照してください。IP ログはバイナリで保存され、ログ ビューアで表示されます。
license-key	加入ライセンス ファイル。
packet-file	packet capture コマンドを使用してキャプチャされ、ローカルに保管されている libpcap ファイル。

選択したプロトコルが FTP または SCP の場合、パスワードのプロンプトが表示されます。FTP セッションにパスワードが必要でない場合は、何も入力しないで Return キーを押します。

コマンドラインですべての必要なソースおよび宛先 URL 情報とユーザ名を入力するか、または **copy** コマンドを入力して、不足している情報をセンサーからプロンプトで要求させることができます。



警告

システム センシング インターフェイスと仮想センサーのコンフィギュレーションが異なる場合、別のセンサーからコンフィギュレーション ファイルをコピーすると、エラーが発生することがあります。



(注) Cisco IOS バージョン 12.0 の **copy** コマンドはさらに柔軟性があり、異なる宛先間でコピーできます。

例

次の例は、IP アドレスが 10.1.1.1 のセンサーのディレクトリ / ファイル名 ~csidsuser/configuration/cfg から現行のコンフィギュレーションにファイルをコピーします。ディレクトリとファイルは、csidsuser のホーム アカウントからの相対パスです。

```
sensor# copy scp://csidsuser@10.1.1.1/configuration/cfg current-config
Password: *****
WARNING: Copying over the current configuration may leave the box in an unstable
state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
csidsuser@10.1.1.1's password:
cfg          100%
|*****| 36124
00:00
sensor#
```

次の例は、IP アドレスが 10.1.1.1 のセンサーのディレクトリ / ファイル名 ~csidsuser/iplog12345 に ID 12345 の iplog をコピーします。ディレクトリとファイルは、csidsuser のホーム アカウントからの相対パスです。

```
sensor# copy iplog 12345 scp://csidsuser@10.1.1.1/iplog12345
Password: *****
iplog          100%
|*****|
36124          00:00
sensor#
```

関連コマンド

コマンド	説明
iplog-status	使用可能な IP ログの内容の説明を表示します。
more	論理ファイルの内容を表示します。
packet	インターフェイス上のライブ トラフィックを表示またはキャプチャします。

copy ad-knowledge-base

KB ファイルをコピーするには、特権 EXEC モードで **copy ad-knowledge-base** コマンドを使用します。

copy ad-knowledge-base *virtual-sensor* [**current** | **initial** | **file name**] *destination-url*

copy ad-knowledge-base *virtual-sensor* *source-url* *new-name*

構文説明

<i>virtual-sensor</i>	KB ファイルが含まれる仮想センサー。1 ～ 64 文字の大文字小文字を区別する文字列です。有効な文字は A ～ Z、a ～ z、0 ～ 9、「-」および「_」です。
<i>name</i>	KB ファイル名。最大 32 文字の大文字小文字を区別する文字列です。有効な文字は A ～ Z、a ～ z、0 ～ 9、「-」および「_」です。
current	現在ロードされている KB。
file	既存の KB ファイル。
initial	初期の KB。
<i>new-name</i>	新しい KB ファイル名。1 ～ 32 文字の大文字小文字を区別する文字列です。有効な文字は A ～ Z、a ～ z、0 ～ 9、「-」および「_」です。
<i>source-url</i>	ソース URL には FTP、SCP、HTTP、または HTTPS を指定することができます。構文の詳細については、 P.2-13 の「copy」 を参照してください。
<i>destination-url</i>	宛先 URL には FTP、SCP、HTTP、または HTTPS を指定することができます。構文の詳細については、 P.2-13 の「copy」 を参照してください。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

リリース	修正
6.0(1)	このコマンドを導入。

使用上のガイドライン

すでに存在する名前にファイルをコピーすると、そのファイルは上書きされます。**current** キーワードを *new-name* として使用することはできません。**load** コマンドにより、新しい現行 KB が作成されます。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、IP アドレスが 10.1.1.1 のコンピュータの ~cidsuser/AD/my-kb に 2006-Mar-16-10_00_00 をコピーします。

```
sensor# copy ad-knowledge-base vs0 file 2006-Mar-16-10_00_00
scp://cidsuser@10.1.1.1/AD/my-kb
Password: *****
2006-Mar-16-10_00_00          100%   14920   0.0KB/s
00:00
sensor#
```


copy instance

コンフィギュレーション インスタンスをコピーするには、特権 EXEC モードで **copy instance** コマンドを使用します。

copy [**anomaly-detection** | **event-action-rules** | **signature-definition**] *source destination*

構文説明	<i>source</i>	コピーする既存のコンポーネント インスタンスの名前。
	<i>destination</i>	新規または既存のコンポーネント インスタンスの名前。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者

コマンド履歴	リリース	修正
	6.0(1)	このコマンドを導入。

使用上のガイドライン このコマンドを使用して、コンフィギュレーション インスタンスをコピーします。インスタンスがすでに存在する場合や、新しいインスタンスで使用する十分なスペースがない場合には、エラーが生成されます。

例 次の例は、「sig0」というシグニチャ定義を「mySig」という新しい定義にコピーします。

```
sensor# copy signature-definition sig0 mySig
sensor#
```

display serial

すべての出力をシリアル接続に転送するには、グローバル コンフィギュレーション モードで **display serial** コマンドを使用します。**no display-serial** コマンドを使用すると、ローカル端末への出力をリセットします。

display-serial

no display-serial

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの設定は、no display-serial です。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン **display-serial** コマンドによって、ブート処理中にリモート コンソール (シリアル ポートを使用) でシステム メッセージを参照できます。このオプションが有効である限り、ローカル コンソールは使用できません。シリアル ポートに接続したときに、このオプションが設定されていないと、Linux が完全に起動してシリアル接続のサポートが有効になるまで、フィードバックを得られません。

例 次の例は、出力をシリアル ポートにリダイレクトします。

```
sensor (config)# display-serial
sensor (config)#
```

downgrade

最後に適用したシグニチャ アップデートまたはサービス パックを削除するには、グローバル コンフィギュレーション モードで **downgrade** コマンドを使用します。

downgrade

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

管理者

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

例

次の例は、適用した最新のシグニチャ アップデートをセンサーから削除します。

```
sensor(config)# downgrade
Warning: Executing this command will reboot the system and downgrade to
IDS-K9-sp-4.1-4-S91.rpm. Configuration changes made since the last upgrade will be
lost and the system may be rebooted.
Continue with downgrade?: yes
sensor#
```

downgrade コマンドが使用できない場合 (たとえば、アップグレードが適用されていない場合)、次のメッセージが表示されます。

```
sensor# downgrade
Error: No downgrade available
sensor#
```

関連コマンド

コマンド	説明
show version	すべてのインストール済み OS パッケージ、シグニチャ パッケージ、およびシステムで実行中の IPS プロセスのバージョン情報を表示します。

end

コンフィギュレーション モードまたはコンフィギュレーション サブモードを終了するには、グローバル コンフィギュレーション モードで **end** コマンドを使用します。このコマンドは、最上位の EXEC メニューに戻ります。

end

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

すべてのモード

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

例

次の例は、コンフィギュレーション モードを終了する方法を示します。

```
sensor# configure terminal
sensor(config)# end
sensor#
```

erase

論理ファイルを削除するには、特権 EXEC モードで **erase** コマンドを使用します。

```
erase { backup-config | current-config | packet-file }
```

構文説明	backup-config	現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。
	current-config	コンフィギュレーション バックアップの保管場所。ファイル フォーマットは CLI コマンドです。
	packet-file	packet capture コマンドを使用してキャプチャされ、ローカルに保管されている libpcap ファイル。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン 現行のコンフィギュレーションを削除すると、コンフィギュレーションの値はデフォルトにリセットされます。 **service** コマンドで作成したコンフィギュレーションインスタンスは削除されません。

このコマンドの Cisco IOS 12.0 バージョンでは、ファイル システム全体を削除できます。IPS では、この概念はサポートされません。

例 次の例は、現行のコンフィギュレーション ファイルを削除してすべての設定をデフォルトに戻します。このコマンドは、センサーのリブートを必要とする場合があります。

```
sensor# erase current-config
Warning: Removing the current-config file will result in all configuration being reset
to default, including system information such as IP address.
User accounts will not be erased. They must be removed manually using the "no
username" command.
Continue? []: yes
sensor#
```

erase ad-knowledge-base

センサーから KB ファイルを削除するには、特権 EXEC モードで **erase ad-knowledge-base** コマンドを使用します。

erase ad-knowledge-base [*virtual-sensor* [*name*]]

構文説明

<i>virtual-sensor</i>	(オプション) KB ファイルが含まれる仮想センサー。1 ~ 64 文字の大文字小文字を区別する文字列です。有効な文字は A ~ Z、a ~ z、0 ~ 9、「-」および「_」です。
<i>name</i>	(オプション) KB ファイル名。最大 32 文字の大文字小文字を区別する文字列です。有効な文字は A ~ Z、a ~ z、0 ~ 9、「-」および「_」です。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

リリース	修正
6.0(1)	このコマンドを導入。

使用上のガイドライン

現行の KB ファイルとしてロードされている KB ファイルは削除できません。初期の KB ファイルを削除することはできません。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、仮想センサー vs0 から 2006-Mar-16-10_00_00 を削除します。

```
sensor# erase ad-knowledge-base vs0 2006-Mar-16-10_00_00
sensor#
```

次の例は、現行としてロードされたファイルおよび初期の KB を除く、すべての KB を仮想センサー vs0 から削除します。

```
sensor# erase ad-knowledge-base vs0
Warning: Executing this command will delete all virtual sensor 'vs0' knowledge bases
except the file loaded as current and the initial knowledge base.
Continue with erase? : yes
sensor#
```

次の例は、現行としてロードされたファイルおよび初期の KB を除く、すべての KB をすべての仮想センサーから削除します。

```
sensor# erase ad-knowledge-base
Warning: Executing this command will delete all virtual sensor knowledge bases except
the file loaded as current and the initial knowledge base.
Continue with erase? : yes
sensor#
```

exit

コンフィギュレーション モードを終了、またはアクティブなターミナル セッションを閉じて、特権 EXEC モードを終了するには、**exit** コマンドを使用します。

exit

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

すべてのモード

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン

exit コマンドを使用すると、直前のメニュー レベルに戻ります。中に含まれるサブモードで変更を行った場合、変更を適用するかどうかを尋ねられます。**no** を選択すると、親サブモードに戻ります。

例

次の例は、直前のメニュー レベルに戻る方法を示します。

```
sensor# configure terminal
sensor(config)# exit
sensor#
```

iplog

仮想センサーの IP ロギングを開始するには、特権 EXEC モードで **iplog** コマンドを使用します。このコマンドの **no** 形式を使用すると、仮想センサーのすべてのロギングセッション、**log-id** に基づく特定のロギングセッション、またはすべてのロギングセッションがディセーブルになります。

iplog name ip-address [duration minutes] [packets numPackets] [bytes numBytes]

no iplog [log-id log-id | name name]

構文説明

<i>name</i>	ロギングを開始および終了する仮想センサー。
<i>ip-address</i>	指定された IP アドレスが含まれるログ パケットのみをロギングします。パラメータの詳細については、P.2-48 の「 setup 」を参照してください。
<i>minutes</i>	ロギングがアクティブな期間（分単位）。有効範囲は 1 ～ 60 です。デフォルトは 10 分です。
<i>numPackets</i>	ロギングするパケットの合計数。有効範囲は 0 ～ 4294967295 です。デフォルトは 1000 パケットです。値 0 は、無制限を意味します。
<i>numBytes</i>	ロギングする合計バイト数。有効範囲は 0 ～ 4294967295 です。値 0 は、無制限を意味します。
<i>log-id</i>	停止するロギングセッションのログ ID。ログ ID は、 iplog-status コマンドを使用することで取得できます。

デフォルト

「構文説明」の表を参照してください。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン

パラメータを設定しないでこのコマンドを **no** 形式で使用すると、すべてのロギングが停止します。期間、パケット数、およびバイト数を入力すると、ロギングは最初のイベントが発生したときに終了します。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、仮想センサー vs0 で、ソースまたは宛先アドレスに 10.2.3.1 を含むすべてのパケットのロギングを開始します。

```
sensor# iplog vs0 10.2.3.1
Logging started for virtual sensor vs0, IP address 10.2.3.1, Log ID 2342
WARNING: IP Logging will affect system performance.
sensor#
```


関連コマンド	コマンド	説明
	iplog-status	使用可能な IP ログの内容の説明を表示します。
	packet	インターフェイス上のライブ トラフィックを表示またはキャプチャします。

iplog-status

使用可能な IP ログの内容の説明を表示するには、特権 EXEC モードで **iplog-status** コマンドを使用します。

```
iplog-status [log-id log-id] [brief] [reverse] [begin regular-expression | exclude regular-expression | include regular-expression | redirect destination-url]
```

構文説明		
	<i>log-id</i>	(オプション) ステータスを表示するファイルのログ ID。
	brief	(オプション) 各ログの iplog ステータス情報の概要を表示します。
	reverse	(オプション) 発生順とは逆の順序でリストを表示します (最新のログが先頭)。
		(オプション) 縦棒は、出力処理指定が続くことを意味します。
	<i>regular-expression</i>	iplog-status 出力に存在する任意の正規表現。
	begin	more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
	exclude	iplog-status コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
	include	iplog-status コマンドの出力をフィルタ処理して、特定の正規表現を含む行が表示されるようにします。
	redirect	iplog-status コマンドの出力を宛先 URL にリダイレクトします。
	<i>destination-url</i>	コピーされる宛先ファイルの場所。URL またはキーワードが一般的です。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	4.0(2)	このコマンドに status フィールドを追加。
	6.0(1)	log-id 、 brief 、 reverse 、 begin 、 exclude 、 include 、および redirect の各オプションを追加。

使用上のガイドライン

ログが作成されたときのステータスは added です。最初のエントリがログに挿入されると、ステータスは started に変更されます。パケット数の上限に達するなどの条件によってログが終了すると、ステータスは completed に変更されます。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、すべての IP ログのステータスを表示します。

```
sensor# iplog-status
Log ID:          2425
IP Address:      10.1.1.2
Virtual Sensor:  vs0
Status:          started
Start Time:      2003/07/30 18:24:18 2002/07/30 12:24:18 CST
Packets Captured: 1039438

Log ID:          2342
IP Address:      10.2.3.1
Virtual Sensor:  vs0
Status:          completed
Event ID:        209348
Start Time:      2003/07/30 18:24:18 2002/07/30 12:24:18 CST
End Time:        2003/07/30 18:34:18 2002/07/30 12:34:18 CST
sensor#
```

次の例は、すべての IP ログの概要リストを表示します。

```
sensor# iplog-status brief
Log ID  VS   IP Address1  Status      Event ID  Start Date
2425    vs0  10.1.1.2    started     N/A       2003/07/30
2342    vs0  10.2.3.1    completed   209348    2003/07/30
```

関連コマンド

コマンド	説明
iplog	仮想センサーで IP ロギングを開始します。

list component-configurations

コンポーネントの既存のコンフィギュレーション インスタンスを表示するには、特権 EXEC モードで **list component-configurations** コマンドを使用します。

list [anomaly-detection-configurations | event-action-rules-configurations | signature-definition-configurations]

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
6.0(1)	このコマンドを導入。

使用上のガイドライン

ファイルサイズの単位はバイトです。仮想センサーが N/A になっている場合、インスタンスは現在、仮想センサーに割り当てられていないことを示します。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、シグニチャ定義の既存のコンフィギュレーションを表示します。

```
sensor# list signature-definition-configurations
Signature Definition
  Instance   Size   Virtual Sensor
  sig0       2293   vs0
  mySig      3422   N/A
sensor#
```

more

論理ファイルの内容を表示するには、特権 EXEC モードで **more** コマンドを使用します。

more *keyword*

構文説明	current-config	現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。
	backup-config	コンフィギュレーション バックアップの保管場所。ファイル フォーマットは CLI コマンドです。

デフォルト デフォルトの動作または値はありません。

コマンド モード EXEC

サポートされるユーザロール 管理者、オペレータ (current-config のみ)、ビューア (current-config のみ)

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン IPS では、論理ファイルのみを表示できます。

パスワードなどの非表示フィールドは、管理者の場合にのみ表示されます。



(注) Cisco IOS バージョン 12.0 のこのコマンドでは、デバイス内のさまざまなパーティションに格納されたファイルの内容を表示できます。

例

次の例は、**more** コマンドの出力を示します。

```

sensor# more current-config
! -----
! Current configuration last modified Tue Jan 24 08:24:44 2006
! -----
! Version 6.0(0.9)
! Host:
!   Realm Keys          key1.0
! Signature Definition:
!   Signature Update    S212.0   2006-01-12
! -----
service interface
physical-interfaces FastEthernet0/1
admin-state enabled
exit
physical-interfaces FastEthernet1/0
admin-state enabled
exit
physical-interfaces FastEthernet1/1
admin-state enabled
exit
physical-interfaces FastEthernet1/2
admin-state enabled
exit
physical-interfaces FastEthernet1/3
admin-state enabled
exit
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-ip 10.89.149.118/25,10.89.149.126
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! -----
service logger
exit
! -----
service network-access
exit

```

関連コマンド

コマンド	説明
more begin	more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
more exclude	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
more include	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。

more begin

more コマンドの出力を検索するには、特権 EXEC モードで **more begin** コマンドを使用します。このコマンドは、指定された正規表現を含む最初の行で **more** コマンドの出力を開始します。フィルタ処理は行いません。

```
more keyword | begin regular-expression
```

構文説明	keyword	current-config	backup-config
		現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。	コンフィギュレーションバックアップの保管場所。ファイルフォーマットは CLI コマンドです。
			縦棒は、出力処理指定が続くことを意味します。
	regular expression	more コマンド出力に存在する任意の正規表現。	

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ (current-config のみ)、ビューア (current-config のみ)

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	4.0(2)	more コマンドの begin 拡張を導入。

使用上のガイドライン 正規表現の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

例 次の例は、**more** コマンドの出力を検索して、正規表現「ip」以降を表示する方法を示します。

```

sensor# more current-config | begin ip
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
exit
! -----
service interface
exit
! -----
service logger
exit
! -----
service network-access
user-profiles mona
enable-password foobar
exit
exit
! -----
service notification
--MORE--

```

関連コマンド

コマンド	説明
more exclude	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
more include	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。
show begin	特定の show コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
show exclude	show コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
show include	show コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。

more exclude

more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除するには、特権 EXEC モードで **more exclude** コマンドを使用します。

```
more keyword | exclude regular-expression
```

構文説明	keyword	current-config	backup-config
		現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。	コンフィギュレーションバックアップの保管場所。ファイルフォーマットは CLI コマンドです。
		縦棒は、出力処理指定が続くことを意味します。	
	regular expression	more コマンド出力に存在する任意の正規表現。	

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ (current-config のみ)、ビューア (current-config のみ)

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	4.0(2)	more コマンドに exclude 拡張を追加。

使用上のガイドライン 正規表現の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

例 次の例は、**more** コマンドの出力を検索して、正規表現「ip」を排除して表示する方法を示します。

```

sensor# more current-config | exclude ip
! -----
! Version 5.0(0.26)
! Current configuration last modified Thu Feb 17 04:25:15 2005
! -----
display-serial
! -----
service analysis-engine
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
--MORE--

```

関連コマンド

コマンド	説明
more begin	more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
more include	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。
show begin	特定の show コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
show exclude	show コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
show include	show コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。

more include

more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示するには、特権 EXEC モードで **more include** コマンドを使用します。

more keyword | include regular-expression

構文説明	keyword	current-config	現在実行中のコンフィギュレーション。このコンフィギュレーションは、Cisco IOS 12.0 の場合と異なり、コマンドが入力されると固定になります。ファイルフォーマットは CLI コマンドです。
		backup-config	コンフィギュレーションバックアップの保管場所。ファイルフォーマットは CLI コマンドです。
			縦棒は、出力処理指定が続くことを意味します。
	regular expression		more コマンド出力に存在する任意の正規表現。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ (current-config のみ)、ビューア (current-config のみ)

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	4.0(2)	more コマンドに include 拡張を追加。

使用上のガイドライン 正規表現の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

例 次の例は、**more** コマンドの出力を検索して、正規表現「ip」を含む行のみを表示する方法を示します。

```
sensor# more current-config | include ip
host-ip 10.89.147.31/25,10.89.147.126
sensor#
```

関連コマンド	コマンド	説明
	more begin	more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
	more exclude	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
	show begin	特定の show コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
	show exclude	show コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
	show include	show コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。

packet

インターフェイス上のライブ トラフィックを表示またはキャプチャするには、特権 EXEC モードで **packet** コマンドを使用します。**display** オプションを使用すると、ライブ トラフィックまたは以前にキャプチャしたファイル出力を画面に直接ダンプできます。**capture** オプションを使用すると、**libpcap** の出力をローカル ファイルにキャプチャできます。ローカル ファイルの保管場所は 1 か所だけなので、後続のキャプチャ要求によって既存のファイルは上書きされます。**copy** コマンドと **packet-file** キーワードを使用して、ローカル ファイルをマシンからコピーできます。ローカル ファイルを表示するには、**display packet-file** オプションを使用します。ローカル ファイルに関する情報がある場合は、**info** オプションを使用して表示できます。

```
packet display interface-name [snaplen length] [count count] [verbose] [expression expression]
```

```
packet display packet-file [verbose] [expression expression]
```

```
packet display iplog id [verbose] [expression expression]
```

```
packet capture interface-name [snaplen length] [count count] [expression expression]
```

```
packet display file-info
```

構文説明

<i>interface-name</i>	インターフェイス名、インターフェイス タイプ (GigabitEthernet、FastEthernet、Management) とその後続くスロット / ポート。システムに存在する有効なインターフェイス名のみを入力できます。
<i>id</i>	表示する既存の IP ログ ID。
file-info	保管されているパケット ファイルに関する情報を表示します。
verbose	(オプション) 1 行の要約ではなく、各パケットのプロトコル ツリーを表示します。
<i>length</i>	(オプション) スナップショットの長さ。デフォルトは 0 です。有効範囲は 0 ~ 1600 です。
<i>count</i>	(オプション) キャプチャするパケット数。指定しない場合は、最大ファイル サイズをキャプチャすると、キャプチャは終了します。有効範囲は 1 ~ 10000 です。
<i>expression</i>	(オプション) パケット キャプチャ フィルタ式。この式が tcpdump に直接渡されます。 tcpdump 式の構文と一致する必要があります。

デフォルト

「構文説明」の表を参照してください。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア (表示のみ)

コマンド履歴

リリース	修正
5.0(1)	このコマンドを導入。

使用上のガイドライン

ストレージは、1 つのローカル ファイルで使用可能です。このファイルのサイズは、プラットフォームによって異なります。可能な場合、要求したパケット カウントをキャプチャする前に最大ファイル サイズに達すると、メッセージが表示されます。**packet capture interface-name** コマンドは、同時

に1ユーザのみが使用できます。2番目のユーザが要求すると、キャプチャを実行しているユーザに関する情報が含まれたエラーメッセージが表示されます。インターフェイスに関わるコンフィギュレーションの変更を行うと、そのインターフェイスで実行中の `packet` コマンドが異常終了することがあります。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。



警告

このコマンドを実行すると、パフォーマンスが大幅に低下します。

ライブ表示またはファイル キャプチャを終了するには、**Ctrl+C** を押します。

式の構文については、`ethereal-filter` の `man` ページを参照してください。

`file-info` の表示は、次のとおりです。

Captured by: *user:id*, Cmd: *cliCmd*

Start: *yyyy/mm/dd hh:mm:ss zone*, End: *yyyy/mm/dd hh:mm:ss zone* or *in-progress*

ここで

user = キャプチャを開始したユーザのユーザ名

id = ユーザの CLI ID

cliCmd = キャプチャを実行するために入力したコマンド

例

次の例は、FastEthernet 0/0 で発生するライブ トラフィックを表示します。

```
sensor# packet display fastethernet0/0
Warning This command will cause significant performance degradation.
Executing command: tethereal -i fastethernet0/0
0.000000 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=56
0.000262 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470
Ack=2972370007 Win=9184 Len=0
0.029148 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.029450 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470
Ack=2972370231 Win=9184 Len=0
0.030273 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.030575 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470
Ack=2972370455 Win=9184 Len=0
0.031361 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.031666 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK] Seq=3844631470
Ack=2972370679 Win=9184 Len=0
0.032466 10.89.147.56 -> 64.101.182.20 SSH Encrypted response packet len=224
0.032761 64.101.182.20 -> 10.89.147.56 TCP 33053 > ssh [ACK]
```

次の例は、保管されているキャプチャ ファイルに関する情報を表示します。

```
sensor# packet display file-info
Captured by: raboyd:5292, Cmd: packet capture fastethernet0/0
Start: 2004/01/07 11:16:21 CST, End: 2004/01/07 11:20:35 CST
```

関連コマンド	コマンド	説明
	<code>iplog</code>	仮想センサーで IP ログインを開始します。
	<code>iplog-status</code>	使用可能な IP ログの内容の説明を表示します。

password

ローカル センサーのパスワードを更新するには、グローバル コンフィギュレーション モードで `password` コマンドを使用します。管理者は、`password` コマンドを使用して既存のユーザのパスワードを変更することもできます。管理者は、コマンドの `no` 形式を使用して、ユーザ アカウントをディセーブルにできます。

password

管理者用の構文 : `password [name [newPassword]]`

`no password name`

構文説明	パラメータ	説明
	<code>name</code>	ユーザ名を指定します。有効なユーザ名の長さは 1 ～ 64 文字です。ユーザ名の先頭は、英数字にする必要があります。その他の文字には、スペース以外のすべての文字を使用できます。
	<code>password</code>	このコマンドを入力すると、パスワードを要求されます。ユーザのパスワードを指定します。有効なパスワードの長さは 8 ～ 32 文字です。スペース以外のすべての文字を使用できます。

デフォルト cisco アカウントのデフォルト パスワードは `cisco` です。

コマンド モード グローバル コンフィギュレーション

サポートされるユーザ ロール 管理者、オペレータ（現行ユーザのパスワードのみ）、ビューア（現行ユーザのパスワードのみ）

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン `password` コマンドを使用すると、現行ユーザのログインパスワードを更新できます。管理者は、このコマンドを使用して既存のユーザのパスワードを変更できます。この場合、管理者に現行パスワードのプロンプトは表示されません。

最後の管理者アカウントをディセーブルにしようとする時、エラーが発生します。`password` コマンドを使用して、ディセーブルにしたユーザ アカウントを再びイネーブルにし、ユーザ パスワードをリセットします。

パスワードは IPS で保護されます。



(注) Cisco IOS バージョン 12.0 の password コマンドでは、パスワード行にクリア テキストで新規パスワードを入力できます。

例

次の例は、現行ユーザのパスワードの変更方法を示します。

```
sensor(config)# password
Enter Old Login Password: *****
Enter New Login Password: *****
Re-enter New Login Password: *****
sensor(config)#
```

次の例は、ユーザ tester のパスワードを変更します。このコマンドは、管理者のみが実行できます。

```
sensor(config)# password tester
Enter New Login Password: *****
Re-enter New Login Password: *****
sensor(config)#
```

関連コマンド

コマンド	説明
username	ローカル センサーのユーザを作成します。

ping

基本的なネットワーク接続を診断するには、特権 EXEC モードで **ping** コマンドを使用します。

ping *address* [*count*]

構文説明	<i>address</i>	<i>count</i>
	ping の対象のシステムの IP アドレス。	送信するエコー要求数。値を指定しない場合、4 要求が送信されます。有効範囲は 1 ~ 10000 です。

デフォルト 「構文説明」の表を参照してください。

コマンドモード EXEC

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

サポートされるユーザロール 管理者、オペレータ、ビューア

使用上のガイドライン このコマンドは、オペレーティング システムで用意されている **ping** コマンドを使用して実装されます。コマンドからの出力は、オペレーティング システムにより若干異なります。

例 次の例は、Solaris システムでの **ping** コマンドの出力を示します。

```
sensor# ping 10.1.1.1
PING 10.1.1.1: 32 data bytes
40 bytes from 10.1.1.1: icmp_seq=0. time=0. ms
40 bytes from 10.1.1.1: icmp_seq=1. time=0. ms
40 bytes from 10.1.1.1: icmp_seq=2. time=0. ms
40 bytes from 10.1.1.1: icmp_seq=3. time=0. ms

----10.1.1.1 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
sensor#
```

次の例は、Linux システムでの **ping** コマンドの出力を示します。

```
sensor# ping 10.1.1.1 2
PING 10.1.1.1 from 10.1.1.2 : 32(60) bytes of data.
40 bytes from 10.1.1.1: icmp_seq=0 ttl=255 time=0.2 ms
40 bytes from 10.1.1.1: icmp_seq=1 ttl=255 time=0.2 ms

--- 10.1.1.1 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.2 ms
sensor#
```

次の例は、到達不能アドレスに対する出力を示します。


```
sensor# ping 172.21.172.1
PING 172.21.172.1 (172.21.172.1) from 10.89.175.50 : 56(84) bytes of data.

--172.21.172.1 ping statistics--
5 packets transmitted, 0 packets received, 100% packet loss
sensor#
```

privilege

既存のユーザの権限レベルを変更するには、グローバル コンフィギュレーション モードで **privilege** コマンドを使用します。 **username** コマンドでユーザを作成するときに、権限を指定することもできます。


privilege user name [administrator | operator | viewer]

構文説明	<i>name</i>	ユーザ名を指定します。有効なユーザ名の長さは1～64文字です。ユーザ名の先頭は、英数字にする必要があります。その他の文字には、スペース以外のすべての文字を使用できます。
デフォルト		デフォルトの動作または値はありません。
コマンドモード		グローバル コンフィギュレーション
サポートされるユーザロール		管理者
コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
使用上のガイドライン		このコマンドを使用すると、ユーザの権限を変更できます。
		
(注)		このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。
例		次の例は、ユーザ「tester」の権限をオペレータに変更します。
		<pre>sensor(config)# privilege user tester operator Warning: The privilege change does not apply to current CLI sessions. It will be applied to subsequent logins. sensor(config)#</pre>
関連コマンド	コマンド	説明
	username	ローカル センサーのユーザを作成します。

recover

回復パーティションに保存されているアプリケーション イメージでアプリケーション パーティションのイメージを再作成するには、特権 EXEC モードで **recover** コマンドを使用します。センサーは複数回リブートされて、ほとんどのコンフィギュレーション（ネットワーク パラメータ、アクセスリスト パラメータ、時間パラメータ以外）がデフォルトの設定にリセットされます。

recover application-partition

構文説明	application-partition アプリケーションパーティションのイメージを再作成します。				
デフォルト	デフォルトの動作または値はありません。				
コマンドモード	グローバル コンフィギュレーション				
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>修正</th> </tr> </thead> <tbody> <tr> <td>4.0(1)</td> <td>このコマンドを導入。</td> </tr> </tbody> </table>	リリース	修正	4.0(1)	このコマンドを導入。
リリース	修正				
4.0(1)	このコマンドを導入。				
サポートされるユーザロール	管理者				
使用上のガイドライン	<p>回復を続行する質問への有効な応答は、yes または no です。Y または N は、有効な応答ではありません。</p> <p>コマンドを実行後、すぐにシャットダウンが開始されます。シャットダウンに少し時間がかかるため、CLI コマンドへのアクセスを続行できますが（アクセスは拒否されない）、アクセスは警告なしで終了します。必要であれば、アプリケーションがシャットダウンしている間、画面にピリオド（.）を1秒ごとに表示して進行を示すことができます。</p> <p> (注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。</p>				

例 次の例は、回復パーティションに保存されているバージョン 4.0(1)S29 のイメージを使用して、アプリケーションパーティションのイメージを再作成します。

```
sensor(config)# recover application-partition
Warning: Executing this command will stop all applications and re-image the node to
version 5.0(1)Sx. All configuration changes except for network settings will be reset
to default.
Continue with recovery? []:yes
Request Succeeded
sensor(config)#
```

rename ad-knowledge-base

既存の KB ファイルの名前を変更するには、特権 EXEC モードで **rename ad-knowledge-base** コマンドを使用します。

```
rename ad-knowledge-base virtual-sensor [current | file name] new-name
```

構文説明

<i>virtual-sensor</i>	KB ファイルが含まれる仮想センサー。1 ～ 64 文字の大文字小文字を区別する文字列です。有効な文字は A ～ Z、a ～ z、0 ～ 9、「-」および「_」です。
<i>name</i>	KB ファイル名。最大 32 文字の大文字小文字を区別する文字列です。有効な文字は A ～ Z、a ～ z、0 ～ 9、「-」および「_」です。
current	現在ロードされている KB。
file	既存の KB ファイル。
<i>new-name</i>	新しい KB ファイル名。1 ～ 32 文字の大文字小文字を区別する文字列です。有効な文字は A ～ Z、a ～ z、0 ～ 9、「-」および「_」です。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

リリース	修正
6.0(1)	このコマンドを導入。

使用上のガイドライン

current キーワードを使用すると、現在使用している KB の名前が変更されます。初期の KB ファイル名を変更することはできません。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、名前を 2006-Mar-16-10_00_00 から my-kb に変更します。

```
sensor# rename ad-knowledge-base vs0 file 2006-Mar-16-10_00_00 my-kb
sensor#
```

reset

センサーで実行中のアプリケーションをシャットダウンし、アプライアンスをリブートするには、特権 EXEC モードで **reset** コマンドを使用します。**powerdown** オプションを使用した場合は、アプライアンスの電源がオフ（可能な場合）、または電源をオフにできる状態になります。

reset[powerdown]

構文説明	powerdown	このオプションを指定すると、アプリケーションのシャットダウン後、センサーにより電源がオフになります。
-------------	------------------	--

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

サポートされるユーザロール 管理者

使用上のガイドライン リセットを続行する質問への有効な応答は、**yes** または **no** です。**Y** または **N** は、有効な応答ではありません。

コマンドを実行後、すぐにシャットダウンが開始されます。シャットダウン中の CLI コマンドへのアクセスは拒否されませんが、開いているセッションは、シャットダウンが完了すると同時に、警告なしに終了します。必要であれば、アプリケーションがシャットダウンしている間、画面にピリオド (.) を 1 秒ごとに表示して進行を示すことができます。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例 次の例は、センサーをリブートします。

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:yes
sensor#
```

service

さまざまなセンサー サービスのコンフィギュレーション メニューに入るには、グローバル コンフィギュレーション モードで **service** コマンドを使用します。このコマンドの **default** 形式を使用すると、アプリケーションのコンフィギュレーション全体が、工場出荷時のデフォルトにリセットされます。

service {authentication | analysis-engine | external-product-interface | host | interface | logger | network-access | notification | ssh-known-hosts | trusted-certificate | web-server}

default service {authentication | analysis-engine | external-product-interface | host | interface | logger | network-access | notification | ssh-known-hosts | trusted-certificate | web-server}

論理名が付けられたイベント アクション ルール コンフィギュレーションのコンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **service event-action-rules name** コマンドを使用します。**default** キーワードを使用すると、コンフィギュレーションが工場出荷時の設定にリセットされます。**no** キーワードを使用すると、センサーからイベント アクション ルール コンフィギュレーションが削除されます。このコマンドは、コンフィギュレーションが仮想センサーに割り当てられていない場合にだけ、正常に実行されます。

service event-action-rules name

default service event-action-rules name

no service event-action-rules name

論理名が付けられたシグニチャ定義コンフィギュレーションのコンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **service signature-definition name** コマンドを使用します。**default** キーワードを使用すると、コンフィギュレーションが工場出荷時の設定にリセットされます。**no** キーワードを使用すると、センサーからシグニチャ定義コンフィギュレーションが削除されます。このコマンドは、コンフィギュレーションが仮想センサーに割り当てられていない場合にだけ、正常に実行されます。

service signature-definition name

default service signature-definition name

no service signature-definition name


論理名が付けられた異常検出コンフィギュレーションのコンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **service anomaly-detection name** コマンドを使用します。**default** キーワードを使用すると、コンフィギュレーションが工場出荷時の設定にリセットされます。**no** キーワードを使用すると、センサーから異常検出コンフィギュレーションが削除されます。このコマンドは、コンフィギュレーションが仮想センサーに割り当てられていない場合にだけ、正常に実行されます。

service anomaly-detection name

default anomaly-detection name

no service anomaly-detection name

構文説明

authentication	ユーザの認証に使用する方式の順序を設定します。
analysis-engine	グローバル分析エンジンパラメータを設定します。このコンフィギュレーションによって、仮想センサーを作成し、シグニチャ定義、イベントアクションルール、およびセンシング インターフェイスを仮想センサーに割り当てることができます。
anomaly-detection	異常検出のパラメータを設定します。
event-action-rules	イベントアクションルール コンフィギュレーションのパラメータを設定します。
external-product-interface	外部製品のインターフェイスのパラメータを設定します。
host	システム クロック設定、アップグレード、および IP アクセス リストを設定します。
logger	デバッグ レベルを設定します。
network-access	ARC に関するパラメータを設定します。
	
(注) Network Access Controller は、現在は Attack Response Controller (ARC) と言います。サービスは新しい名称になっていますが、変更は IPS 6.0 の CLI には反映されていません。CLI 全体にわたって network-access および nac と表示されます。	
notification	通知アプリケーションを設定します。
signature-definition	シグニチャ定義コンフィギュレーションのパラメータを設定します。
ssh-known-hosts	システムの既知のホスト キーを設定します。
trusted-certificate	信頼できる認証機関の X.509 証明書のリストを設定します。
web-server	Web サーバ ポートなど、Web サーバに関するパラメータを設定します。
name	イベントアクションルールまたはシグニチャ定義コンフィギュレーションの論理名。まだ論理名がない場合は、新しいコンフィギュレーション ファイルが作成されます。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者、オペレータ (ホストおよびインターフェイス以外)、ビューア (表示のみ)

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。
5.0(1)	default キーワードと、通知アプリケーションのサポートを追加。
6.0(1)	anomaly-detection 、 external-product-interface 、および os-identification の各コマンドを追加。

使用上のガイドライン

このコマンドで、サービス固有のパラメータを設定できます。このコンフィギュレーションの項目とメニューはサービスによって異なり、コマンドが実行されたときにサービスから取得したコンフィギュレーションに基づいて動的に作成されます。

**注意**

このモードおよびその中に含まれるすべてのサブモードで行われた変更は、サービス モードを終了するときにサービスに適用されます。

コマンドモードは、コマンドプロンプトに表示されるサービス名で示されます。たとえば、`service authentication` では、次のプロンプトが表示されます。

```
sensor(config-aut)#
```

**(注)**

このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次のコマンドは、認証サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service authentication
sensor(config-aut)#
```

次のコマンドは、分析エンジン サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service analysis-engine
sensor(config-ana)#
```

次のコマンドは、イベント アクションルール サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service event-action-rules rules0
sensor(config-rul)#
```

次のコマンドは、ホスト サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service host
sensor(config-hos)#
```

次のコマンドは、インターフェイス サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service interface
sensor(config-int)#
```

次のコマンドは、ロギング サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service logger
sensor(config-log)#
```

次のコマンドは、ARC サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service network-access
sensor(config-net)#
```

次のコマンドは、SNMP 通知サービスのコンフィギュレーション モードに入ります。

```
sensor(config)# service notification
sensor(config-not)#
```

次のコマンドは、シグニチャ定義サービスのコンフィギュレーションモードに入ります。

```
sensor(config)# service signature-definition sig0  
sensor(config-sig)#
```

次のコマンドは、SSH 既知のホスト サービスのコンフィギュレーションモードに入ります。

```
sensor(config)# service ssh-known-hosts  
sensor(config-ssh)#
```

次のコマンドは、信頼できる認証サービスのコンフィギュレーションモードに入ります。

```
sensor(config)# service trusted-certificate  
sensor(config-tru)#
```

次のコマンドは、Web サーバ サービスのコンフィギュレーションモードに入ります。

```
sensor(config)# service web-server  
sensor(config-web)#
```

setup

基本的なセンサー コンフィギュレーションを構成するには、特権 EXEC モードで **setup** コマンドを使用します。

setup

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

hostname : sensor

IP interface : 10.1.9.201/24,10.1.9.1

telnet-server : disabled

web-server port : 443

summer time : disabled

ユーザが summer time を enabled にした場合、デフォルトは次のとおりです。

- Summertime type : Recurring
- Start Month : april
- Start Week : first
- Start Day : sunday
- Start Time : 02:00:00
- End Month : october
- End Week : last
- End Day : sunday
- End Time : 02:00:00
- Offset : 60

システムの時間帯のデフォルトは、次のとおりです。

- Timezone : UTC
- UTC Offset : 0

コマンドモード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

リリース	修正
4.0(2)	アクセス リストおよび時間設定のコンフィギュレーションを追加。
5.0(1)	仮想センサー設定のコンフィギュレーションを追加。
5.1(1)	インライン VLAN ペアのコンフィギュレーションを追加。
6.0(1)	複数の仮想センサーおよび VLAN グループのコンフィギュレーションを追加。デフォルトで自動的に脅威を拒否するかどうかを尋ねるプロンプトを追加。

使用上のガイドライン

setup コマンドを使用すると、システム コンソール画面に System Configuration Dialog と呼ばれる対話型ダイアログが表示されます。System Configuration Dialog によって、コンフィギュレーションプロセスの手順が示されます。

各プロンプトの横のカッコ内に示される値が、最後に設定されたデフォルト値です。

System Configuration Dialog を終了してから、項目の変更に移る必要があります。変更しない項目についてデフォルトの設定を受け入れるには、**Enter** を押します。

変更せず、また System Configuration Dialog を終了せずに EXEC プロンプトに戻るには、**Ctrl+C** を押します。

この機能には、各プロンプトに関するヘルプ テキストも用意されています。ヘルプ テキストにアクセスするには、プロンプトで疑問符 (?) を入力します。

変更が完了すると、セットアップ セッションで作成されたコンフィギュレーションが表示されます。このコンフィギュレーションを保存するかどうかを尋ねるプロンプトが表示されます。**yes** と入力すると、コンフィギュレーションはディスクに保存されます。**no** と入力すると、コンフィギュレーションは保存されず、処理が再開されます。このプロンプトに対するデフォルトはありません。**yes** または **no** と入力する必要があります。

構成可能パラメータの有効な範囲は、次のとおりです。

IP Address/Netmask/Gateway : *X.X.X.X/mn,Y.Y.Y.Y*。ここで、*X.X.X.X* は、ピリオドで区切られた 4 オクテットの 32 ビット アドレスとしてセンサーの IP アドレスを指定します。*X*=0 ~ 255 です。

mn は、ネットマスクのビット数を指定します。

Y.Y.Y.Y は、ピリオドで区切られた 4 オクテットの 32 ビット アドレスとしてデフォルト ゲートウェイを指定します。*Y*=0 ~ 255 です。

Host Name : 最大 256 文字の大文字小文字を区別する文字列。数字、「_」、および「-」は有効ですが、スペースは使用できません。

システムが NTP を使用しない場合にのみ、**setup** モードでクロック設定を入力します。NTP コマンドは、別に用意されています。

夏時間は、**recurring** モードまたは **date** モードで設定できます。**recurring** モードを選択した場合、開始日と終了日は、週、曜日、月、時間に基づいて入力します。**date** モードを選択した場合、開始日と終了日は、月、日、年、時間に基づいて入力します。**disable** を選択すると、夏時間がオフになります。

表 2-1 に、クロック設定パラメータを示します。

表 2-1 クロック設定パラメータ

DST zone	サマータイムが有効なときに表示される時間帯の名前。
week	週 (1 ~ 5 または last)。
day	曜日 (Sunday、Monday など)。
date	日 (1 ~ 31)。
month	月 (January、February など)。
year	年。省略なし (2001 ~ 2035)。
hh:mm	開始 / 終了 DST (24 時形式) の時間と分。
offset	(オプション) サマータイム中に加算する時間 (分)。デフォルトは 60 です。
timezone	標準時が有効なときに表示される時間帯の名前。
hours	UTC からの時間差。
hh:mm:ss	時 (24 時形式)、分、および秒形式の現在時間。

デフォルトの仮想センサー vs0 の編集もできます。仮想センサーに、混合 / インラインのペアとインライン VLAN のペア（または、どちらか一方）を割り当て、割り当てたインターフェイスをイーネーブルにできます。セットアップが完了すると、仮想センサーはトラフィックを監視するように設定されます。

セットアップ時に、**deny-packet-inline** アクションに関連付けられた上書きルールを有効または無効にすることができます。仮想センサーに割り当てられたイベント アクション ルール コンフィギュレーションのすべてのインスタンスを変更できます。仮想センサーに割り当てられていないイベント アクション ルール コンフィギュレーションのインスタンスは、変更されません。

例

次の例は、**setup** コマンドと System Configuration プログラムを示します。

```
sensor# setup
```

```
--- System Configuration Dialog ---
```

```
At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
```

```
Current Configuration:
```

```
service host
network-settings
host-ip 172.21.172.25/8,172.21.172.1
host-name sensor
telnet-option disabled
access-list 10.0.0.0/24
access-list 172.0.0.0/24
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 8080
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 75-100
exit
exit
service event-action-rules myEvr
overrides deny-packet-inline
override-item-status Enabled
risk-rating-range 90-100
exit
exit
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
```

```
exit
physical-interfaces GigabitEthernet1/0
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user cisco
vlan1 2
vlan2 3
exit
subinterface 2
description Created via setup by user cisco
vlan1 344
vlan2 23
exit
subinterface 10
description Created via setup by user cisco
vlan1 20
vlan2 10
exit
exit
exit
physical-interfaces GigabitEthernet1/1
admin-state enabled
subinterface-type vlan-group
subinterface 3
description Created via setup by user cisco
vlans 5-7,9
exit
exit
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
exit
inline-interface foo
description Create via setup by user cisco
interface1 GigabitEthernet3/0
interface2 GigabitEthernet3/1
subinterface-type vlan-group
subinterface 3
vlans 200-299
exit
subinterface 8
vlans 300-399
exit
exit
exit
service analysis-engine
virtual-sensor vs0
anomaly-detection ad0
event-action-rules rules0
signature-definition sig0
physical-interface GigabitEthernet0/0
physical-interface GigabitEthernet1/0 subinterface-number 1
physical-interface GigabitEthernet1/0 subinterface-number 2
exit
virtual-sensor myVs
anomaly-detection myAd
event-action-rules myEvr
signature-definition mySigs
physical-interface GigabitEthernet2/0
physical-interface GigabitEthernet1/1 subinterface-number 3
logical-interface foo subinterface 3
logical-interface foo subinterface 8
exit
exit
```

Current time: Wed May 5 10:25:35 2004

Setup Configuration last modified: Mon May 3 15:34:30 2004

```

Continue with configuration dialog?[yes]:
Enter host name[sensor]:
Enter IP interface[172.21.172.25/8,172.21.172.1]:
Enter telnet-server status[enabled]:
Enter web-server port[8080]: 80
Modify current access list? [no]: yes
Current access list entries:
  [1] 10.0.0.0/24
  [2] 172.0.0.0/24
Delete: 1
Delete:
Permit: 173.0.0.0/24
Permit:
Modify system clock settings? [no]: yes
  Use NTP? [yes] no
  Modify summer time settings? [no]: yes
    Recurring, Date or Disable[recurring]:
    Start Month[apr]:
    Start Week[1]:
    Start Day[sun]:
    Start Time[02:00:00]:
    End Month[oct]:
    End Week[last]:
    End Day[sun]:
    End Time[02:00:00]:
    DST Zone[]: CDT
    Offset[60]:
  Modify system timezone? [no]: yes
    Timezone[UTC]: CST
    GMT Offset[-360]
Modify interface/virtual sensor configuration?[no]: yes
Current interface configuration
  Command control GigabitEthernet0/1
  Unassigned:
    Promiscuous:
      GigabitEthernet2/1
      GigabitEthernet4/0
      GigabitEthernet4/1
    Inline Vlan Pairs:
      GigabitEthernet1/0:10 (Vlans: 20, 10)

Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Promiscuous:
    GigabitEthernet0/0
  Inline Vlan Pairs:
    GigabitEthernet1/0:1 (Vlans: 2, 3)
    GigabitEthernet1/0:2 (Vlans: 344, 23)

Virtual Sensor: myVs
  Anomaly Detection: myAd
  Event Action Rules: myEvr
  Signature Definition: mySigs
  Promiscuous:
    GigabitEthernet2/0
  Promiscuous Vlan Groups:
    GigabitEthernet1/1:3 (Vlans: 5-7,9)
  Inline Interface Pair Vlan Groups:
    foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)

```

```
foo:8 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 300-399)
```

```
[1] Edit Interface Configuration
[2] Edit Virtual Sensor Configuration
[3] Display configuration
Option: 1
```

次のプロンプトでは、インターフェイスを作成または削除できます。Edit Virtual Sensor Configuration セクションで、インターフェイスを仮想センサーに割り当てることができます。混合モードで監視されているインターフェイスが VLAN によって細分化されていない場合、追加のコンフィギュレーションは必要ありません。仮想センサーのコンフィギュレーションに進み、仮想センサーにインターフェイスを割り当ててください。

```
[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 1
Inline Vlan Pairs:
  [1] GigabitEthernet1/0:1 (Vlans: 2, 3)
  [2] GigabitEthernet1/0:2 (Vlans: 344, 23)
  [3] GigabitEthernet1/0:10 (Vlans: 20, 10)
Promiscuous Vlan Groups:
  [4] GigabitEthernet1/1:3 (Vlans: 5-7,9)
Inline Interface Pair Vlan Groups:
  [5] foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)
  [6] foo:8 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 300-399)
Remove Interface: 6
Remove Interface:
```

```
[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 2
```

```
Available Interfaces
  [1] GigabitEthernet1/0
  [2] GigabitEthernet2/1
  [3] GigabitEthernet4/0
  [4] GigabitEthernet4/1
Interface to modify: 2
Inline Vlan Pairs for GigabitEthernet2/1:
  None
Subinterface number: 1
Description[Created via setup by user cisco]:
Vlan1: 5
Vlan2: 6
Subinterface number:
Available Interfaces
  [1] GigabitEthernet1/0
  [2] GigabitEthernet2/1
  [3] GigabitEthernet4/0
  [4] GigabitEthernet4/1
Interface to modify:
```

```

[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 3

```

```

Available Interfaces
  [1] GigabitEthernet1/1
  [2] GigabitEthernet4/0
  [3] GigabitEthernet4/1
Interface to modify: 1
Promiscuous Vlan Groups for GigabitEthernet1/1:
  GigabitEthernet1/1:3 (Vlans: 5-7,9)
Subinterface number: 1
Description[Created via setup by user cisco]:
  Vlans: 3,8,34-69
Subinterface number:
Available Interfaces
  [1] GigabitEthernet1/1
  [2] GigabitEthernet4/0
  [3] GigabitEthernet4/1
Interface to modify:

```

```

[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 4

```

```

Available Interfaces
  GigabitEthernet4/0
  GigabitEthernet4/1
Pair Name: test
Description[Created via setup by user cisco]:
  Interface1: GigabitEthernet4/0
  Interface2: GigabitEthernet4/1

```

```

[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.
[5] Add/Modify Inline Interface Pair Vlan Groups.
[6] Modify interface default-vlan.
Option: 5

```

```

Available inline interface pairs:
  [1] foo (GigabitEthernet3/0, GigabitEthernet3/1)
  [2] test (GigabitEthernet4/0, GigabitEthernet4/1)
Interface to modify: 1
Inline Interface Pair Vlan Groups for foo:
  Subinterface: 3; Vlans: 200-299
Subinterface number: 1
Description[Created via setup by user cisco]:
  Vlans: 100-199
Subinterface number:
Available inline interface pairs:
  [1] foo (GigabitEthernet3/0, GigabitEthernet3/1)
  [2] test (GigabitEthernet4/0, GigabitEthernet4/1)
Interface to modify:

```

```

[1] Remove interface configurations.
[2] Add/Modify Inline Vlan Pairs.
[3] Add/Modify Promiscuous Vlan Groups.
[4] Add/Modify Inline Interface Pairs.

```

```
[5] Add/Modify Inline Interface Pair Vlan Groups.  
[6] Modify interface default-vlan.  
Option: 6
```

```
GigabitEthernet0/0 default-vlan[0]:  
GigabitEthernet1/0 default-vlan[0]:  
GigabitEthernet1/1 default-vlan[0]:  
GigabitEthernet2/0 default-vlan[0]:  
GigabitEthernet2/1 default-vlan[0]:  
GigabitEthernet3/0 default-vlan[0]: 100  
GigabitEthernet3/1 default-vlan[0]: 100  
GigabitEthernet4/0 default-vlan[0]:  
GigabitEthernet4/1 default-vlan[0]:
```

```
[1] Remove interface configurations.  
[2] Add/Modify Inline Vlan Pairs.  
[3] Add/Modify Promiscuous Vlan Groups.  
[4] Add/Modify Inline Interface Pairs.  
[5] Add/Modify Inline Interface Pair Vlan Groups.  
[6] Modify interface default-vlan.  
Option:
```

```
[1] Edit Interface Configuration  
[2] Edit Virtual Sensor Configuration  
[3] Display configuration  
Option: 3
```

```
Current interface configuration  
Command control GigabitEthernet0/1  
Unassigned:  
Promiscuous:  
  GigabitEthernet2/1  
Inline Vlan Pairs:  
  GigabitEthernet1/0:10 (Vlans: 20, 10)  
Promiscuous Vlan Groups:  
GigabitEthernet1/1:1 (Vlans: 3,8,34-39)  
Inline Interface Pairs:  
  test (GigabitEthernet4/0, GigabitEthernet4/1)  
Inline Interface Pair Vlan Groups:  
  foo:1 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 100-199)  
Virtual Sensor: vs0  
Anomaly Detection: ad0  
Event Action Rules: rules0  
Signature Definitions: sig0  
Promiscuous:  
  GigabitEthernet0/0  
Inline Vlan Pairs:  
  GigabitEthernet1/0:1 (Vlans: 2, 3)  
  GigabitEthernet1/0:2 (Vlans: 344, 23)
```

```
Virtual Sensor: myVs  
Anomaly Detection: myAd  
Event Action Rules: myEvr  
Signature Definition: mySigs  
Promiscuous:  
  GigabitEthernet2/0  
Promiscuous Vlan Groups:  
  GigabitEthernet1/1:3 (Vlans: 5-7,9)  
Inline Interface Pair Vlan Groups:  
  foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)
```

```
[1] Edit Interface Configuration  
[2] Edit Virtual Sensor Configuration  
[3] Display configuration  
Option: 2
```

```
[1] Remove virtual sensor.  
[2] Modify "vs0" virtual sensor configuration.  
[3] Modify "myVs" virtual sensor configuration.
```

```

[4] Create new virtual sensor.
Option: 1

Virtual sensors
  [1] vs0
  [2] myVs
Remove: 2
Remove:

[1] Remove virtual sensor.
[2] Modify "vs0" virtual sensor configuration.
[3] Create new virtual sensor.
Option: 2

Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Promiscuous:
    GigabitEthernet0/0
  Inline Vlan Pairs:
    [1] GigabitEthernet1/0:1 (Vlans: 2, 3)
    [2] GigabitEthernet1/0:2 (Vlans: 344, 23)
Remove Interface: 2
Remove Interface:

Unassigned:
  Promiscuous:
    [1] GigabitEthernet2/1
    [2] GigabitEthernet2/0
  Inline Vlan Pairs:
    [3] GigabitEthernet1/0:2 (Vlans: 344, 23)
    [4] GigabitEthernet1/0:10 (Vlans: 20, 10)
  Promiscuous Vlan Groups:
    [5] GigabitEthernet1/1:1 (Vlans: 3,8,34-39)
    [6] GigabitEthernet1/1:3 (Vlans: 5-7,9)
  Inline Interface Pairs:
    [7] test (GigabitEthernet4/0, GigabitEthernet4/1)
  Inline Interface Pair Vlan Groups:
    [8] foo:1 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 100-199)
    [9] foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)
Add Interface: 4
Add Interface:

Current interface configuration
Command control GigabitEthernet0/1
Unassigned:
  Promiscuous:
    GigabitEthernet2/0
    GigabitEthernet2/1
  Inline Vlan Pairs:
    GigabitEthernet1/0:2 (Vlans: 344, 23)
  Promiscuous Vlan Groups:
    GigabitEthernet1/1:1 (Vlans: 3,8,34-39)
    GigabitEthernet1/1:3 (Vlans: 5-7,9)
  Inline Interface Pairs:
    test (GigabitEthernet4/0, GigabitEthernet4/1)
  Inline Interface Pair Vlan Groups:
    foo:1 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 100-199)
    foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)

Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Promiscuous:
    GigabitEthernet0/0
  Inline Vlan Pairs:

```



```

GigabitEthernet1/0:1 (Vlans: 2, 3)
GigabitEthernet1/0:10 (Vlans: 20, 10)

[1] Remove virtual sensor.
[2] Modify "myVs" virtual sensor configuration.
[3] Create new virtual sensor.
Option: 3
Name: newVs
Description[Created via setup by user cisco]:
Anomaly Detection Configuration:
  [1] ad0
  [2] myAd
  [3] Create a new anomaly detection configuration
Option[3]: 2
Signature Definition Configuration:
  [1] sig0
  [2] mySigs
  [3] Create new signature definition configuration
Option[3]: 2
Event Action Rules Configuration:
  [1] rules0
  [2] myEvr
  [3] newRules
  [4] Create new event action rules configuration
Option[4]: 2
Unassigned:
  Promiscuous:
    [1] GigabitEthernet2/0
    [2] GigabitEthernet2/1
  Inline Vlan Pairs:
    [3] GigabitEthernet1/0:1 (Vlans: 2, 3)
  Promiscuous Vlan Groups:
    [4] GigabitEthernet1/1:1 (Vlans: 3,8,34-39)
    [5] GigabitEthernet1/1:3 (Vlans: 5-7,9)
  Inline Interface Pairs:
    [6] test (GigabitEthernet4/0, GigabitEthernet4/1)
  Inline Interface Pair Vlan Groups:
    [7] foo:1 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 100-199)
    [8] foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)
Add Interface: 1
Add Interface: 2
Add Interface:

Current interface configuration
Command control GigabitEthernet0/1
Unassigned:
  Inline Vlan Pairs:
    GigabitEthernet1/0:1 (Vlans: 2, 3)
  Promiscuous Vlan Groups:
    GigabitEthernet1/1:1 (Vlans: 3,8,34-39)
    GigabitEthernet1/1:3 (Vlans: 5-7,9)
  Inline Interface Pairs:
    test (GigabitEthernet4/0, GigabitEthernet4/1)
  Inline Interface Pair Vlan Groups:
    foo:1 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 100-199)
    foo:3 (GigabitEthernet3/0, GigabitEthernet3/1 Vlans: 200-299)

Virtual Sensor: vs0
Anomaly Detection: ad0
Event Action Rules: rules0
Signature Definitions: sig0
Promiscuous:
  GigabitEthernet0/0
  Inline Vlan Pairs:
    GigabitEthernet1/0:1 (Vlans: 2, 3)
    GigabitEthernet1/0:2 (Vlans: 344, 23)
    GigabitEthernet1/0:10 (Vlans: 20, 10)

Virtual Sensor: newVs

```

```
Anomaly Detection: myAd
Event Action Rules: newRules
Signature Definition: mySigs
Promiscuous:
  GigabitEthernet2/0
  GigabitEthernet2/1
```

```
[1] Remove virtual sensor.
[2] Modify "vs0" virtual sensor configuration.
[3] Modify "newVs" virtual sensor configuration.
[4] Create new virtual sensor.
Option:
```

```
[1] Edit Interface Configuration
[2] Edit Virtual Sensor Configuration
[3] Display configuration
Option:
```

```
Modify default threat prevention settings? [no] yes
  Virtual sensor vs0 is NOT configured to prevent a modified range of threats in inline
  mode. (Risk Rating 75-100)
  Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
  Rating 90-100)
```

```
Do you want to enable automatic threat prevention on all virtual sensors? [no]
```



(注) 上記の質問への応答に **yes** を選択すると、その次の質問は表示されません。



(注) すべての仮想センサーが有効である場合、無効にするかどうかの質問だけが表示されます。



(注) すべての仮想センサーが無効である場合、有効にするかどうかの質問だけが表示されます。

```
Do you want to disable automatic threat prevention on all virtual sensors? [no] yes
The Event Action "overrides" rule for action "deny-packet-inline" has been Disabled
on all virtual sensors.
```

```
The following configuration was entered.
```

```
service host
network-settings
host-ip 172.21.172.25/8,172.21.172.1
host-name sensor
telnet-option enabled
access-list 172.0.0.0/24
access-list 173.0.0.0/24
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
summertime-option recurring
offset 60
```

```
summertime-zone-name CDT
start-summertime
month april
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
end-summertime
month october
week-of-month last
day-of-week sunday
time-of-day 02:00:00
exit
exit
ntp-option disabled
exit
service web-server
port 80
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 75-100
exit
exit
service event-action-rules myEvr
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit
service event-action-rules newRules
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit
service interface
service event-action-rules rules0
overrides deny-packet-inline
risk-rating-range 85-100
exit
exit
service event-action-rules newRules
overrides deny-packet-inline
risk-rating-range 85-100
exit
exit
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet1/0
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user cisco
vlan1 2
vlan2 3
exit
subinterface 2
description Created via setup by user cisco
vlan1 344
vlan2 23
exit
subinterface 10
description Created via setup by user cisco
vlan1 20
vlan2 10
```

```

exit
exit
exit
physical-interfaces GigabitEthernet1/1
subinterface-type vlan-group
subinterface 3
description Created via setup by user cisco
vlans 5-7,9
exit
subinterface 1
description Created via setup by user cisco
vlans 3,8,34-39
exit
exit
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
physical-interfaces GigabitEthernet3/0
default-vlan 100
exit
physical-interfaces GigabitEthernet3/1
default-vlan 100
exit
inline-interface foo
description Create via setup by user cisco
interface1 GigabitEthernet3/0
interface2 GigabitEthernet3/1
subinterface-type vlan-group
subinterface 3
vlans 200-299
exit
subinterface 1
vlans 100-199
exit
exit
exit
inline-interface test
description Created via setup by user cisco
interface1 GigabitEthernet4/0
interface2 GigabitEthernet4/1
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet1/0 subinterface-number 2
physical-interface GigabitEthernet1/0 subinterface-number 10
exit
virtual-sensor newVs
anomaly-detection myAd
event-action-rulse newRules
signature-definition mySigs
physical-interface GigabitEthernet2/0
physical-interface GigabitEthernet2/1
exit
exit

```

- [0] Go to the command prompt without saving this config.
- [1] Return back to the setup without saving this config.
- [2] Save this configuration and exit.

```

Enter your selection [2]:
Configuration Saved.
Modify system date and time? [no] yes
Local Date[]: 2003-01-18

```

```

Local Time[4:33:49]: 10:33:49
System Time Updated successfully
sensor#

```

show ad-knowledge-base diff

2つのKBの違いを表示するには、特権 EXEC モードで **show ad-knowledge-base diff** コマンドを使用します。

```

show ad-knowledge-base virtual-sensor diff [current | initial | file name1][current | initial | file name2]
diff-percentage

```

構文説明

<i>virtual-sensor</i>	比較する KB ファイルが含まれる仮想センサー。1～64文字の大文字小文字を区別する文字列です。有効な文字は A～Z、a～z、0～9、「-」および「_」です。
<i>name1</i>	比較する1つ目の既存 KB ファイルの名前。最大32文字の大文字小文字を区別する文字列です。有効な文字は A～Z、a～z、0～9、「-」および「_」です。
<i>name2</i>	比較する2つ目の既存 KB ファイルの名前。最大32文字の大文字小文字を区別する文字列です。有効な文字は A～Z、a～z、0～9、「-」および「_」です。
current	現在ロードされている KB。
initial	初期の KB。
file	既存の KB ファイル。
<i>diff-percentage</i>	(オプション) しきい値が指定されたパーセントより大きく異なるサービスを表示します。有効な値は1～100です。デフォルトは10%です。

デフォルト

「構文説明」の表を参照してください。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
6.0(1)	このコマンドを導入。

使用上のガイドライン



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例 次の例は、2006-Mar-16-10_00_00 と仮想センサー vs0 に現在ロードされている KB を比較します。

```
sensor# show ad-knowledge-base vs0 diff current file 2006-Mar-16-10_00_00
2006-Mar-17-10_00_00 Only Services/Protocols
  External Zone
    TCP Services
      Service = 30
      Service = 20
    UDP Services
      None
    Other Protocols
      Protocol = 1
  Illegal Zone
    None
  Internal Zone
    None
2006-Mar-16-10_00_00 Only Services/Protocols
  External Zone
    None
  Illegal Zone
    None
  Internal Zone
    None
Thresholds differ more than 10%
  External Zone
    None
  Illegal Zone
    TCP Services
      Service = 31
      Service = 22
    UDP Services
      None
    Other Protocols
      Protocol = 3
  Internal Zone
    None
sensor#
```

show ad-knowledge-base files

仮想センサーで使用できる異常検出 KB ファイルを表示するには、特権 EXEC モードで **show ad-knowledge-base files** コマンドを使用します。

show ad-knowledge-base *virtual-sensor* files

構文説明	<i>virtual-sensor</i> (オプション) KB ファイルが含まれる仮想センサー。1～64文字の大文字小文字を区別する文字列です。有効な文字は A～Z、a～z、0～9、「-」および「_」です。
-------------	--

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

コマンド履歴	リリース 修正
	6.0(1) このコマンドを導入。

使用上のガイドライン ファイル名の前にある * は、その KB ファイルが現在ロードされていることを示します。現行 KB は必ず存在します（インストール後は初期の KB です）。AD で現在ロードされている KB、または AD が現在アクティブになっていない場合はロードされている KB が示されます。

仮想センサーを指定しない場合、すべての仮想センサーですべての KB ファイルが取得されます。

初期の KB は、しきい値が工場出荷時の設定になっている KB です。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例 次の例は、すべての仮想センサーで使用できる KB ファイルを表示します。2006-Mar-16-10_00_00 ファイルは、仮想センサー vs0 にロードされた現行 KB ファイルです。

```
sensor# show ad-knowledge-base files
Virtual Sensor vs0
  Filename                Size   Created
  -----                -
  initial                  84    04:27:07 CDT Wed Jan 28 2006
* 2006-Jan-29-10_00_01    84    04:27:07 CDT Wed Jan 29 2006
  2006-Mar-17-10_00_00    84    10:00:00 CDT Fri Mar 17 2006
  2006-Mar-18-10_00_00    84    10:00:00 CDT Sat Mar 18 2006
sensor#
```

show ad-knowledge-base thresholds

KB のしきい値を表示するには、特権 EXEC モードで **show ad-knowledge-base thresholds** コマンドを使用します。

```
show ad-knowledge-base virtual-sensor thresholds {current | initial | file name} [zone {external |
illegal | internal}] [[protocol {tcp | udp}] [dst-port port] | [protocol other] [number
protocol-number]]
```

構文説明

<i>virtual-sensor</i>	比較する KB ファイルが含まれる仮想センサー。1 ~ 64 文字の大文字小文字を区別する文字列です。有効な文字は A ~ Z、a ~ z、0 ~ 9、「-」および「_」です。
current	現在ロードされている KB。
initial	初期の KB。
file	既存の KB ファイル。
<i>name</i>	KB ファイル名。最大 32 文字の大文字小文字を区別する文字列です。有効な文字は A ~ Z、a ~ z、0 ~ 9、「-」および「_」です。
zone	(オプション) 指定されたゾーンのしきい値だけを表示します。デフォルトでは、すべてのゾーンに関する情報が表示されます。
external	外部ゾーンを表示します。
illegal	無許可ゾーンを表示します。
internal	内部ゾーンを表示します。
protocol	(オプション) 指定されたプロトコルのしきい値だけを表示します。デフォルトでは、すべてのプロトコルに関する情報が表示されます。
tcp	TCP プロトコルを表示します。
udp	UDP プロトコルを表示します。
dst-port	(オプション) 指定されたポートのしきい値だけを表示します。デフォルトでは、すべての TCP ポートまたは UDP ポート、またはその両方に関する情報を表示します。
<i>port</i>	(オプション) 指定されたポートのしきい値だけを表示します。デフォルトでは、すべての TCP ポートまたは UDP ポート、またはその両方に関する情報を表示します。有効な値は 0 ~ 65535 です。
number	(オプション) 他の特定のプロトコル番号のしきい値だけを表示します。デフォルトでは、他のすべてのプロトコルに関する情報が表示されます。
other	TCP または UDP 以外の他のプロトコルを表示します。
<i>protocol-number</i>	プロトコル番号。有効な値は 0 ~ 255 です。

デフォルト

デフォルト値については、「構文説明」の表を参照してください。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
6.0(1)	このコマンドを導入。

使用上のガイドライン

表示されたしきい値は、KBに含まれるしきい値です。上書きされるユーザ コンフィギュレーションがある場合のしきい値は、知識ベースのしきい値とユーザ コンフィギュレーションの両方が表示されます。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、KB 2006-Mar-16-10_00_00 の無許可ゾーンに含まれるしきい値を表示します。

```

sensor# show ad-knowledge-base vs0 thresholds file 2006-Mar-16-10_00_00 zone illegal
2006-Mar-16-10_00_00
  Illegal Zone
    TCP Port 20
      Scanner Threshold
        >> User Configuration = 100
        >> Knowledge Base = 20
      Threshold Histogram
        Destination IP           5    10    100
        >> User Configuration: source IP 100 1    0
        >> Knowledge Base: source IP   10 1    0
    TCP Port 30
      Scanner Threshold
        Knowledge Base = 110
      Threshold Histogram
        Destination IP           5    10    100
        Knowledge Base: source IP 10 1    0
    TCP Port any
      Scanner Threshold
        Knowledge Base = 9
      Threshold Histogram
        Destination IP           5    10    100
        Knowledge Base: source IP 2 1    0
    UDP Port any
      Scanner Threshold
        Knowledge Base = 19
      Threshold Histogram
        Destination IP           5    10    100
        Knowledge Base: source IP 12 10   0
    Other Protocol any
      Scanner Threshold
        Knowledge Base = 1
      Threshold Histogram
        Destination IP           5    10    100
        Knowledge Base: source IP 1 1    0
    Other Protocol 1
      Scanner Threshold
        Knowledge Base = 10
      Threshold Histogram
        Destination IP           5    10    100
        Knowledge Base: source IP 10 10   0
sensor#

```

■ show ad-knowledge-base thresholds

次の例は、現行 KB の無許可ゾーンに含まれ、プロトコルが TCP で宛先ポートが 20 である場合のしきい値を表示します。

```

sensor# show ad-knowledge-base vs0 thresholds current zone illegal protocol tcp
dst-port 20
2006-Mar-16-10_00_00
  Illegal Zone
    TCP Port 20
      Scanner Threshold
        >> User Configuration = 100
        >> Knowledge Base = 50
      Threshold Histogram
        Destination IP           5    10    100
        >> User Configuration: source IP 100  1    0
        >> Knowledge Base: source IP   10   1    0
sensor#

```

次の例は、現行 KB の無許可ゾーンに含まれ、プロトコルがその他で宛先ポート番号が 1 である場合のしきい値を表示します。

```

sensor# show ad-knowledge-base vs0 thresholds current zone illegal protocol other
number 1
2006-Mar-16-10_00_00
  Illegal Zone
    Other Protocol 1
      Scanner Threshold
        >> User Configuration = 79
        >> Knowledge Base = 50
      Threshold Histogram
        Destination IP           5    10    100
        >> User Configuration: source IP 100  5    0
        >> Knowledge Base: source IP   12   1    0
sensor#

```

show begin

show コマンドの出力を検索するには、特権 EXEC モードで **show begin** コマンドを使用します。このコマンドは、指定された正規表現を含む最初の行で **show** コマンドの出力を開始します。フィルタ処理は行いません。

show [configuration | events | settings | tech-support] | begin regular-expression

構文説明		縦棒は、出力処理指定が続くことを意味します。
	regular-expression	show コマンド出力に存在する任意の正規表現。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザーロール 管理者、オペレータ (current-config のみ)、ビューア (current-config のみ)

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	4.0(2)	show コマンドの begin 拡張を追加。
	5.1(1)	tech-support オプションを追加。

使用上のガイドライン 正規表現の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

例 次の例は、正規表現「ip」から始まる出力を示します。

```
sensor# show configuration | begin ip
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
exit
! -----
service interface
exit
! -----
service logger
exit
! -----
service network-access
user-profiles mona
enable-password foobar
exit
exit
! -----
service notification
--MORE--
```

関連コマンド

コマンド	説明
more begin	more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
more exclude	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
more include	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。
show exclude	show コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
show include	show コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。

show clock

システムクロックを表示するには、特権 EXEC モードで **show clock** コマンドを使用します。

show clock [detail]

構文説明	<i>detail</i> (オプション) クロック ソース (NTP またはシステム) および現行のサマータイム設定 (設定されている場合) を示します
-------------	---

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン システムクロックは「保証」フラグを保持して、時間が保証されるか (正確と見なされるか) どうかを示します。システムクロックが NTP などのタイミングソースで設定された場合、このフラグがセットされます。表 2-2 に保証フラグを示します。

表 2-2 保証フラグ

記号	説明
*	時間は保証されない。
(ブランク)	時間は保証される。
.	時間は保証されるが、NTP は同期化されない。

例 次の例は、設定され、同期化された NTP を示します。

```
sensor# show clock detail
12:30:02 CST Tues Dec 19 2002
Time source is NTP
Summer time starts 03:00:00 CDT Sun Apr 7 2003
Summer time ends 01:00:00 CST Sun Oct 27 2003
sensor#
```

次の例は、時刻源が設定されていないことを示します。

```
sensor# show clock
*12:30:02 EST Tues Dec 19 2002
sensor#
```

次の例は、時刻源が設定されていないことを示します。

```
sensor# show clock detail
*12:30:02 CST Tues Dec 19 2002
No time source
Summer time starts 02:00:00 CST Sun Apr 7 2003
Summer time ends 02:00:00 CDT Sun Oct 27 2003
```

show configuration

`more` コマンドの `more current-config` コマンドを参照してください。

コマンド履歴


リリース	修正
4.0(2)	このコマンドを追加。

show events

ローカル イベント ログの内容を表示するには、特権 EXEC モードで **show events** コマンドを使用します。

```
show events [{alert [informational] [low] [medium] [high] [include-traits traits] [exclude-traits traits]
[min-threat-rating min-rr] [max-threat-rating max-rr] error [warning] [error] [fatal] | log | NAC
| status}] [hh:mm:ss [month day [year]] | past hh:mm:ss]
```

構文説明

alert	アラートを表示します。侵入攻撃が行われている、または試みられた可能性のある動作を通知します。アラートイベントは、IPS シグニチャがネットワーク アクティビティでトリガーされると、常に分析エンジンによって生成されます。レベル（情報、低、中、高）が選択されていない場合、すべてのアラートイベントが表示されます。
include-traits	指定された <i>traits</i> のあるアラートを表示します。
exclude-traits	指定された <i>traits</i> のあるアラートを表示しません。
<i>traits</i>	10 進（0 ～ 15）の特性ビット位置。
min-threat-rating	脅威評価がこの値以上であるイベントを表示します。有効範囲は 0 ～ 100 です。デフォルトは 0 です。
max-threat-rating	脅威評価がこの値以下であるイベントを表示します。有効範囲は 0 ～ 100 です。デフォルトは 100 です。
error	エラー イベントを表示します。エラー イベントは、エラー条件が発生したときにサービスによって生成されます。レベル（警告、エラー、重大）が選択されていない場合、すべてのエラー イベントが表示されます。
log	ログ イベントを表示します。これらのイベントは、トランザクションが受信され、アプリケーションによって応答されたときに常に生成されます。要求、応答、およびトランザクションの成功または失敗についての情報が含まれます。
NAC	ARC 要求（ブロック要求）を表示します。
	 <p>(注) Network Access Controller は、現在は Attack Response Controller (ARC) と言います。サービスは新しい名称になっていますが、変更は IPS 6.0 の CLI には反映されていません。CLI 全体にわたって network-access および nac と表示されます。</p>
status	状況イベントを表示します。
<i>hh:mm:ss</i>	時（24 時形式）、分、および秒形式の開始時間。
<i>day</i>	月の開始日（日）。
<i>month</i>	開始月（月の名前）。
<i>year</i>	開始年（省略なし）。
past	今までに開始したイベントを表示します。 <i>hh:mm:ss</i> に表示を開始する過去の時間を指定します。

デフォルト

デフォルト値については、「構文説明」の表を参照してください。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。
4.0(2)	複数のエラーイベント レベルを同時に選択できる機能を追加。
4.1(1)	include-traits 、 exclude-traits 、および past オプションを追加。
6.0(1)	min-threat-rating および max-threat-rating オプションを追加。

使用上のガイドライン

show events コマンドを使用すると、要求された開始時間に始まる要求イベント タイプを表示できます。開始時間が入力されていない場合、現行時間に開始する選択されたイベントが表示されます。イベント タイプが入力されていない場合、すべてのイベントが表示されます。イベントは、ライブ フィードとして表示されます。ライブ フィードをキャンセルするには、**Ctrl+C** を押します。

show events コマンドで正規表現 | **include shunInfo** を使用すると、イベントのソース アドレスなどのブロッキング情報を表示できます。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、2004 年 12 月 25 日午前 10 時に開始したブロック要求を表示します。

```
sensor# show events NAC 10:00:00 Dec 25 2004
```

次の例は、現行時間に開始するエラーおよび重大エラー メッセージを表示します。

```
sensor# show events error fatal error
```

次の例は、2004 年 12 月 25 日 10 時に開始したすべてのイベントを表示します。

```
sensor# show events 10:00:00 Dec 25 2004
```

次の例は、過去 30 秒に開始したすべてのイベントを表示します。

```
sensor# show events past 00:00:30
```

次の出力は、XML コンテンツから取得されます。

```
evAlert: eventId=1025376040313262350 severity=high
  originator:
    deviceName: sensor1
    appName: sensorApp
  time: 2002/07/30 18:24:18 2002/07/30 12:24:18 CST
  signature: sigId=4500 subSigId=0 version=1.0 IOS Embedded SNMP Community Names
  participants:
    attack:
      attacker: proxy=false
      addr: 132.206.27.3
      port: 61476
    victim:
      addr: 132.202.9.254
      port: 161
  protocol: udp
```


show exclude

show コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除するには、特権 EXEC モードで **show exclude** コマンドを使用します。

show [**configuration** | **events** | **settings** | **tech-support**] | **exclude** *regular-expression*

構文説明		縦棒は、出力処理指定が続くことを意味します。
	regular-expression	show コマンド出力に存在する任意の正規表現。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ (*current-config* のみ)、ビューア (*current-config* のみ)

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	4.0(2)	show コマンドの exclude 拡張を追加。
	5.1(1)	tech-support オプションを追加。

使用上のガイドライン *正規表現* の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

例 次の例は、正規表現「ip」を排除した出力を示します。

```
sensor# show configuration | exclude ip
! -----
! Version 5.0(0.26)
! Current configuration last modified Thu Feb 17 04:25:15 2005
! -----
display-serial
! -----
service analysis-engine
exit
! -----
service authentication
exit
! -----
service event-action-rules rules0
exit
! -----
service host
network-settings
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on user login.
exit
time-zone-settings
offset -360
standard-time-zone-name CST
--MORE-
```

関連コマンド	コマンド	説明
	more begin	more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
	more exclude	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
	more include	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。
	show begin	特定の show コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
	show include	show コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。

show history

現行のメニューで入力したコマンドのリストを表示するには、すべてのモードで **show history** コマンドを使用します。

show history

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

すべてのモード

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン

show history コマンドでは、現行メニューで入力したコマンドの記録が表示されます。履歴バッファに記録されるコマンド数は 50 です。

例

次の例は、**show history** コマンドで表示されるコマンドの記録を示します。

```
sensor# show history
show users
show events
sensor#
```

show include

show コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示するには、特権 EXEC モードで **show include** コマンドを使用します。

show [configuration | events | settings | tech-support] | include regular-expression

構文説明

	縦棒は、出力処理指定が続くことを意味します。
regular-expression	show コマンド出力に存在する任意の正規表現。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ (current-config のみ)、ビューア (current-config のみ)

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。
4.0(2)	show コマンドの include 拡張を追加。
5.1(1)	tech-support オプションを追加。

使用上のガイドライン

正規表現の引数は大文字小文字を区別し、複雑な照合の要件を指定できます。

show settings コマンドの出力では、照合要求のヘッダー情報も表示され、照合コンテキストを判別できます。

例

次の例は、正規表現「ip」を含む行のみの出力を示します。

```
sensor# show configuration | include ip
host-ip 10.89.147.31/25,10.89.147.126
sensor#
```

関連コマンド

コマンド	説明
more begin	more コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
more exclude	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。
more include	more コマンドの出力をフィルタ処理して、特定の正規表現を含む行のみを表示します。
show begin	特定の show コマンドの出力を検索し、指定した文字列が最初に出現した位置から表示します。
show exclude	show コマンドの出力をフィルタ処理して、特定の正規表現を含む行を排除します。


show interfaces

すべてのシステムインターフェイスの統計情報を表示するには、特権 EXEC モードで `show interfaces` コマンドを使用します。このコマンドでは、**show interfaces management**、**show interfaces fastethernet**、および **show interfaces gigabithernet** を表示します。

show interfaces [**clear**] [**brief**]

show interfaces {**FastEthernet** | **GigabitEthernet** | **Management**} [*slot/port*]

構文説明

clear	(オプション) 診断をクリアします。
brief	(オプション) 各インターフェイスのユーザビリティ ステータス情報の概要を表示します。
FastEthernet	FastEthernet インターフェイスの統計情報を表示します。
GigabitEthernet	GigabitEthernet インターフェイスの統計情報を表示します。
Management	Management インターフェイスの統計情報を表示します。
	
	(注) このキーワードは、Management とマークされた外部ポートを持つプラットフォームでのみサポートされます。その他のプラットフォームの管理インターフェイスは、インターフェイスの種類 (通常、FastEthernet) に基づいて、 show interfaces の出力で表示されます。
<i>slot/port</i>	スロットとポートの情報については、適切なハードウェア マニュアルを参照してください。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
5.0(1)	show interfaces group 、 show interfaces sensing 、および show interfaces command-control の各コマンドを削除。 show interfaces FastEthernet 、 show interfaces GigabitEthernet 、および show interfaces Management の各コマンドを追加。
6.0(1)	brief キーワードを追加。

使用上のガイドライン

このコマンドは、コマンド、コントロール、およびセンシング インターフェイスに関する統計情報を表示します。**clear** オプションで統計情報をクリアしてリセットすることもできます。

インターフェイスの種類を指定してこのコマンドを使用すると、その種類のすべてのインターフェイスに関する統計情報が表示されます。スロット番号やポート番号を追加すると、その特定のインターフェイスに関する統計情報が表示されます。

エントリの横にある * は、そのインターフェイスがコマンド/コントロール インターフェイスであることを示します。

例

次の例は、インターフェイス統計情報を示します。

```
sensor# show interfaces
Interface Statistics
  Total Packets Received = 0
  Total Bytes Received = 0
  Missed Packet Percentage = 0
  Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/0
  Media Type = TX
  Missed Packet Percentage = 0
  Inline Mode = Unpaired
  Pair Status = N/A
  Link Status = Down
  Link Speed = N/A
  Link Duplex = N/A
  Total Packets Received = 0
  Total Bytes Received = 0
  Total Multicast Packets Received = 0
  Total Broadcast Packets Received = 0
  Total Jumbo Packets Received = 0
  Total Undersize Packets Received = 0
  Total Receive Errors = 0
  Total Receive FIFO Overruns = 0
  Total Packets Transmitted = 0
  Total Bytes Transmitted = 0
  Total Multicast Packets Transmitted = 0
--MORE--
```

次の例は、インターフェイス統計情報の概要出力を示します。

```
sensor# show interfaces brief
CC  Interface          Sensing State  Link  Inline Mode  Pair Status
*   GigabitEthernet0/0  Enabled       Up    Unpaired    N/A
    GigabitEthernet0/1  Enabled       Up    Unpaired    N/A
    GigabitEthernet2/1  Disabled      Up    Subdivided  N/A
sensor#
#
```

show inventory

PEP 情報を表示するには、特権 EXEC モードで **show inventory** コマンドを使用します。このコマンドは、センサーの PID、VID および SN で構成された UDI 情報を表示します。

show inventory

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

コマンド履歴	リリース	修正
	5.0(1)	このコマンドを導入。

使用上のガイドライン これは、Cisco PEP ポリシーで要求される **show inventory** Cisco IOS コマンドと同じです。**show inventory** の出力は、ハードウェアによって異なります。

例 次の例は、**show inventory** コマンドの出力例を示します。

```
sensor# show inventory
NAME: "Chassis", DESCR: "Chasis-4240"
PID: 4240-515E , VID: V04, SN: 639156

NAME: "slot 0", DESCR: "4 port I/O card"
PID: 4240-4IOE , VID: V04, SN: 4356785466
sensor#
```

show os-identification

センサーが受動分析によってラーニングした IP アドレスと関連付けられた OS ID を表示するには、特権 EXEC モードで **show os-identification** コマンドを使用します。

```
show os-identification [name] learned [ip-address]
```

構文説明

<i>name</i>	(オプション) センサーに設定された仮想センサーの名前。表示操作は、指定した仮想センサーに関連付けられているラーニングした IP アドレスに制限されます。
<i>ip-address</i>	(オプション) 照会する IP アドレス。センサーは、指定された IP アドレスにマッピングされた OS ID を表示します。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
6.0(1)	このコマンドを導入。

使用上のガイドライン

IP アドレスと仮想センサーはオプションです。IP アドレスを指定すると、指定した IP アドレスの OS ID だけが表示されます。IP アドレスを指定しないと、ラーニングした OS ID がすべて表示されます。

仮想センサーを指定すると、指定した仮想センサーの OS ID だけが表示されます。仮想センサーを指定しないと、すべての仮想センサーのラーニングした OS ID が表示されます。仮想センサーを指定せずに IP アドレスを指定した場合、要求された IP アドレスが含まれるすべての仮想センサーが表示されます。

例

次の例は、特定の IP アドレスの OS ID を表示します。

```
sensor# show os-identification learned 10.1.1.12
Virtual Sensor vs0:
  10.1.1.12 windows
```

次の例は、すべての仮想センサーの OS ID を表示します。

```
sensor# show os-identification learned
Virtual Sensor vs0:
  10.1.1.12 windows
Virtual Sensor vs1:
  10.1.0.1  unix
  10.1.0.2  windows
  10.1.0.3  windows
sensor#
```

■ show privilege

関連コマンド	コマンド	説明
	show statistics os-identification	OS ID に関する統計情報を表示します。
	clear os-identification	センサーが受動分析によってラーニングした IP アドレスとの OS ID アソシエーションを削除します。

show privilege

現行の権限レベルを表示するには、特権 EXEC モードで **show privilege** コマンドを使用します。

```
show privilege
```

構文説明 このコマンドには、引数またはキーワードはありません。

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン このコマンドを使用して、現行の権限レベルを表示します。権限レベルは、管理者だけが変更できます。詳細については、**username** コマンドを参照してください。

例 次の例は、ユーザの権限を示します。


```
sensor# show privilege
Current privilege level is viewer
sensor#
```

関連コマンド	コマンド	説明
	username	ローカル センサーのユーザを作成します。

show settings

現行のサブモードに含まれるコンフィギュレーションの内容を表示するには、サービス コマンドモードで **show settings** コマンドを使用します。

show settings [terse]

構文説明	<i>terse</i>	出力を簡潔に表示します。
デフォルト		デフォルトの動作または値はありません。
コマンドモード		すべての サービス コマンド モード
サポートされるユーザロール		管理者、オペレータ、ビューア（最上位コマンドツリーの表示のみ）
コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	4.0(2)	terse キーワードを追加。
使用上のガイドライン	 (注)	このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。
例		次の例は、ARC コンフィギュレーション モードでの show settings コマンドの出力を示します。



(注) Network Access Controller は、現在は Attack Response Controller (ARC) と言います。サービスは新しい名称になっていますが、変更は IPS 6.0 の CLI には反映されていません。CLI 全体にわたって **network-access** および **nac** と表示されます。

```

sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# show settings
  general
  -----
    log-all-block-events-and-errors: true <defaulted>
    enable-nvram-write: false <defaulted>
    enable-acl-logging: false <defaulted>
    allow-sensor-block: true default: false
    block-enable: true <defaulted>
    block-max-entries: 250 <defaulted>
    max-interfaces: 250 <defaulted>
    master-blocking-sensors (min: 0, max: 100, current: 0)
    -----
    never-block-hosts (min: 0, max: 250, current: 0)
    -----
    never-block-networks (min: 0, max: 250, current: 0)
    -----
    block-hosts (min: 0, max: 250, current: 0)
    -----
    block-networks (min: 0, max: 250, current: 0)
    -----
    -----
    user-profiles (min: 0, max: 250, current: 0)
    -----
    cat6k-devices (min: 0, max: 250, current: 0)
    -----
    router-devices (min: 0, max: 250, current: 0)
    -----
    firewall-devices (min: 0, max: 250, current: 0)
    -----
  sensor(config-net)#

```

次の例は、シグニチャ定義サブモードでの **show settings terse** の出力を示します。

```

sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# show settings terse
  variables (min: 0, max: 256, current: 2)
-----
  <protected entry>
  variable-name: WEBPORTS
  variable-name: user2
-----
application-policy
-----
  http-policy
-----
  http-enable: false <defaulted>
  max-outstanding-http-requests-per-connection: 10 <defaulted>
  aic-web-ports: 80-80,3128-3128,8000-8000,8010-8010,8080-8080,8888-8888,
24326-24326 <defaulted>
-----
  ftp-enable: true default: false
-----
fragment-reassembly
-----
  ip-reassemble-mode: nt <defaulted>
-----
stream-reassembly
-----
  tcp-3-way-handshake-required: true <defaulted>
  tcp-reassembly-mode: strict <defaulted>
--MORE--

```

次の例は、フィルタ処理された **show settings** の出力を示します。このコマンドは、HTTP が含まれる行のみを出力します。

```

sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# show settings | include HTTP
Searching:
  sig-string-info: Bagle.Q HTTP propagation (jpeg) <defaulted>
  sig-string-info: Bagle.Q HTTP propagation (php) <defaulted>
  sig-string-info: GET ftp://@@@:/pub HTTP/1.0 <defaulted>
  sig-name: IMail HTTP Get Buffer Overflow <defaulted>
  sig-string-info: GET shellcode HTTP/1.0 <defaulted>
  sig-string-info: ..%c0%af..*HTTP <defaulted>
  sig-string-info: ..%c1%9c..*HTTP <defaulted>
  sig-name: IOS HTTP Unauth Command Execution <defaulted>
  sig-name: Null Byte In HTTP Request <defaulted>
  sig-name: HTTP tunneling <defaulted>
  sig-name: HTTP tunneling <defaulted>
  sig-name: HTTP tunneling <defaulted>
  sig-name: HTTP tunneling <defaulted>
  sig-name: HTTP CONNECT Tunnel <defaulted>
  sig-string-info: CONNECT.*HTTP/ <defaulted>
  sig-name: HTTP 1.1 Chunked Encoding Transfer <defaulted>
  sig-string-info: INDEX / HTTP <defaulted>
  sig-name: Long HTTP Request <defaulted>
  sig-string-info: GET \x3c400+ chars>? HTTP/1.0 <defaulted>
  sig-name: Long HTTP Request <defaulted>
  sig-string-info: GET .....?\x3c400+ chars> HTTP/1.0 <defaulted>
  sig-string-info: /mod_ssl:error:HTTP-request <defaulted>
  sig-name: Dot Dot Slash in HTTP Arguments <defaulted>
  sig-name: HTTPBench Information Disclosure <defaulted>
--MORE--

```

show ssh authorized-keys

現行ユーザの公開 RSA キーを表示するには、特権 EXEC モードで **show ssh authorized-keys** コマンドを使用します。

```
show ssh authorized-keys [ id]
```

構文説明	<i>id</i>	許可されたキーを一意に特定する 1 ~ 256 文字の文字列。数字、「_」、および「-」は有効ですが、スペースと「?」は使用できません。
-------------	-----------	--

デフォルト	デフォルトの動作または値はありません。
--------------	---------------------

コマンドモード	EXEC
----------------	------

サポートされるユーザロール	管理者、オペレータ、ビューア
----------------------	----------------

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン	オプションの ID を指定せずにこのコマンドを実行すると、システムで設定済みの ID のリストが表示されます。特定の ID を指定してコマンドを実行すると、その ID に関連付けられたキーが表示されます。
-------------------	--



(注)	このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。
------------	--

例	次の例は、SSH 認証キーのリストを表示します。
----------	--------------------------

```
sensor# show ssh authorized-keys
system1
system2
system3
system4
```

次の例は、system1 の SSH キーを表示します。

```
sensor# show ssh authorized-keys system1

1023 37
66022272955660983338089706716372943357082868686000817201780243492180421420781303592082
95091017013584805250399939321125031474527683786209111899866537160898131479220860447399
11341369642870682319361928148521864094557416306138786468335115835910404940213136954353
39616344979349705016792583146548622146467421997057
sensor#
```

関連コマンド	コマンド	説明
	ssh authorized-key	現行ユーザに公開キーを追加し、クライアントが RSA 認証を使用してローカル SSH サーバにログインできるようにします。

show ssh server-key

SSH サーバのホスト キーとホスト キーのフィンガープリントを表示するには、特権 EXEC モードで **show ssh server-key** コマンドを使用します。

```
show ssh server-key
```

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、**show ssh server-key** コマンドの出力を示します。

```
sensor# show ssh server-key
1024 35 144719237233791547030730646600884648599022074867561982783071499320643934
48734496072779375489584407249259840037709354850629125941930828428605183115777190
69953460097510388011424663818234783053872210554889384417232132153750963283322778
52374794118697053304026570851868326130246348580479834689461788376232451955011
MD5: F3:10:3E:BA:1E:AB:88:F8:F5:56:D3:A6:63:42:1C:11
Bubble Babble: xucis-hehon-kizog-nedeg-zunom-kolyn-syzec-zasyk-symuf-rykum-sexyx
sensor#
```

関連コマンド

コマンド	説明
ssh generate-key	センサーで SSH サーバが使用するサーバ ホスト キーを変更します。

show ssh host-keys

センサーが接続に使用できるリモート SSH サーバの公開キーを含む既知のホスト テーブルを表示するには、特権 EXEC モードで **show ssh host-keys** を使用します。

```
show ssh host-keys [ ipaddress]
```

構文説明	<i>ipaddress</i>	ピリオドで区切られた 4 オクテットの 32 ビットアドレス。X.X.X.X、ここで X は 0 ~ 255。
-------------	------------------	---

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	4.1(1)	コマンドへの Bubble Babble および MD5 の出力を追加。

使用上のガイドライン オプションの IP アドレス ID を指定せずにこのコマンドを実行すると、公開キーで設定済みの IP アドレスのリストが表示されます。特定の IP アドレスを指定してコマンドを実行すると、その IP アドレスに関連付けられたキーが表示されます。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例 次の例は、**show ssh host-keys** コマンドの出力を示します。

```
sensor# show ssh host-keys 10.1.2.3
1024 35 144719237233791547030730646600884648599022074867561982783071499320643934
48734496072779375489584407249259840037709354850629125941930828428605183115777190
69953460097510388011424663818234783053872210554889384417232132153750963283322778
52374794118697053304026570851868326130246348580479834689461788376232451955011
MD5: F3:10:3E:BA:1E:AB:88:F8:F5:56:D3:A6:63:42:1C:11
Bubble Babble: xucis-hehon-kizog-nedeg-zunom-kolyn-syzec-zasyk-symuf-rykum-sexyx
sensor#
```

関連コマンド	コマンド	説明
	ssh host-key	既知のホスト テーブルにエントリを追加します。

show statistics

要求した統計情報を表示するには、特権 EXEC モードで **show statistics** コマンドを使用します。

```
show statistics {analysis-engine | authentication | event-server | event-store |
external-product-interface | host | logger | network-access | notification | sdee-server |
transaction-server | web-server} [clear]
```

show statistics anomaly-detection、**denied-attackers**、**virtual-sensor**、および **os-identification** コマンドは、センサーに含まれるすべての仮想センサーに関する統計情報を表示します。オプションの名前を指定すると、その仮想センサーに関する統計情報が表示されます。

```
show statistics {anomaly-detection | denied-attackers | os-identification | virtual-sensor} [name]
[clear]
```

構文説明

clear	統計情報が取得された後、統計情報をクリアします。
	 <p>(注) このオプションは、分析エンジン、異常検出、ホスト、OS ID、またはネットワーク アクセスの統計情報には使用できません。</p>
analysis-engine	分析エンジン統計情報を表示します。
anomaly-detection	異常検出統計情報を表示します。
authentication	許可および認証統計情報を表示します。
denied-attackers	拒否する IP アドレスおよび各攻撃者からのパケット数のリストを表示します。
event-server	イベントサーバ統計情報を表示します。
event-store	イベントストア統計情報を表示します。
external-product-interface	外部製品のインターフェイス統計情報を表示します。
host	ホスト（メイン）統計情報を表示します。
logger	ログ機能統計情報を表示します。
network-access	ARC 統計情報を表示します。
	 <p>(注) Network Access Controller は、現在は Attack Response Controller (ARC) と言います。サービスは新しい名称になっていますが、変更は IPS 6.0 の CLI には反映されていません。CLI 全体にわたって network-access および nac と表示されます。</p>
notification	通知統計情報を表示します。
os-identification	OS ID 統計情報を表示します。
sdee-server	SDEE サーバ統計情報を表示します。
transaction-server	トランザクションサーバ統計情報を表示します。
web-server	Web サーバ統計情報を表示します。
virtual-sensor	仮想センサー統計情報を表示します。
<i>name</i>	仮想センサーの論理名。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

■ show statistics

サポートされるユーザロール 管理者、オペレータ、ビューア

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	5.0(1)	analysis-engine 、 virtual-sensor 、および denied-attackers を追加。
	6.0(1)	anomaly-detection 、 external-product-interface 、および os-identification を追加。

使用上のガイドライン



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、認証統計情報を表示します。

```
sensor# show statistics authentication
General
  totalAuthenticationAttempts = 9
  failedAuthenticationAttempts = 0
sensor#
```

次の例は、イベントストア統計情報を表示します。

```
sensor# show statistics event-store
Event store statistics
  General information about the event store
    The current number of open subscriptions = 1
    The number of events lost by subscriptions and queries = 0
    The number of queries issued = 1
    The number of times the event store circular buffer has wrapped = 0
  Number of events of each type currently stored
    Debug events = 0
    Status events = 129
    Log transaction events = 0
    Shun request events = 0
    Error events, warning = 8
    Error events, error = 13
    Error events, fatal = 0
    Alert events, informational = 0
    Alert events, low = 0
    Alert events, medium = 0
    Alert events, high = 0
sensor#
```


次の例は、ログ機能統計情報を表示します。

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 27
The number of <evError> events written to the event store by severity
  Fatal Severity = 0
  Error Severity = 13
  Warning Severity = 35
  TOTAL = 48
The number of log messages written to the message log by severity
  Fatal Severity = 0
  Error Severity = 13
  Warning Severity = 8
  Timing Severity = 0
  Debug Severity = 0
  Unknown Severity = 26
  TOTAL = 47
sensor#
```

次の例は、ARC 統計情報を表示します。

```
sensor# show statistics network-access
Current Configuration
  LogAllBlockEventsAndSensors = true
  EnableNvramWrite = false
  EnableAclLogging = false
  AllowSensorBlock = false
  BlockMaxEntries = 250
  MaxDeviceInterfaces = 250
State
  BlockEnable = true
sensor#
```

show tech-support

現行システムの状況を表示するには、特権 EXEC モードで **show tech-support** コマンドを使用します。

show tech-support [page] [destination-url destination url]

構文説明	page	(オプション) 出力は一度に 1 ページの情報が表示されます。Enter キーを押して次の出力行を表示するか、スペースバーを押して次ページの情報を表示します。page を使用しない場合、出力は改ページなしで表示されます
	destination-url	(オプション) 情報を HTML でフォーマット化し、このタグに続く宛先に送信することを示すタグ。このオプションを選択した場合、出力は画面に表示されません。
	destination url	(オプション) レポート ファイルの宛先。URL を指定すると、出力は HTML ファイルにフォーマット化されて、指定された宛先に送信されます。指定しない場合は画面に表示されます

デフォルト 「構文説明」の表を参照してください。

コマンドモード EXEC

サポートされるユーザロール 管理者

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	6.0(1)	password オプションを削除。パスワードは暗号化されて表示されます。



使用上のガイドライン (注) Cisco IOS バージョン 12.0 では、このコマンドの宛先部分はサポートされません。

宛先 URL の正確なフォーマットはファイルにより異なります。ファイル名を選択できますが、.html で終了する必要があります。次の有効なタイプがサポートされています。

プレフィックス	ソースまたは宛先
ftp:	FTP ネットワーク サーバの宛先 URL。このプレフィックスの構文は、次のとおりです。 ftp://[username@] location[/relativeDirectory]/filename ftp://[username@]location[/absoluteDirectory]/filename
scp:	SCP ネットワーク サーバの宛先 URL。このプレフィックスの構文は、次のとおりです。 scp://[username@] location[/relativeDirectory]/filename scp://[username@] location[/absoluteDirectory]/filename

レポートには、次のコマンドからの HTML リンク出力が含まれています。

- **show interfaces**
- **show statistics network-access**
- **cidDump**

例

次の例は、tech-support の出力を ~csidsuser/reports/sensor1Report.html ファイルに保存します。パスは、csidsuser のホーム アカウントを基準とします。

```
sensor# show tech-support destination-url  
ftp://csidsuser@10.2.1.2/reports/sensor1Report.html  
password:*****
```

次の例は、tech-support の出力を /absolute/reports/sensor1Report.html ファイルに保存します。

```
sensor# show tech-support destination-url  
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html  
password:*****
```

show tls fingerprint

サーバの TLS 証明書のフィンガープリントを表示するには、特権 EXEC モードで **show tls fingerprint** を使用します。

show tls fingerprint

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、**show tls fingerprint** コマンドの出力を示します。

```
sensor# show tls fingerprint
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor#
```

関連コマンド

コマンド	説明
tls generate-key	サーバの自己署名 X.509 証明書を再生成します。

show tls trusted-hosts

センサーの信頼できるホストを表示するには、特権 EXEC モードで **show tls trusted-hosts** コマンドを使用します。

```
show tls trusted-hosts [id]
```

構文説明	<i>id</i>	許可されたキーを一意に特定する 1 ~ 32 文字の文字列。数字、「_」、および「-」は有効ですが、スペースと「?」は使用できません。
-------------	-----------	---

デフォルト	デフォルトの動作または値はありません。
--------------	---------------------

コマンドモード	EXEC
----------------	------

サポートされるユーザロール	管理者、オペレータ、ビューア
----------------------	----------------

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン	オプションの ID を指定せずにこのコマンドを実行すると、システムで設定済みの ID のリストが表示されます。特定の ID を指定してコマンドを実行すると、その ID に関連付けられた証明書のフィンガープリントが表示されます。
-------------------	---



(注)	このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。
------------	--

例	次の例は、 show tls trusted-hosts コマンドの出力を示します。
----------	---

```
sensor# show tls trusted-hosts 172.21.172.1
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA
sensor#
```

関連コマンド	コマンド	説明
	tls trusted-host	信頼できるホストをシステムに追加します。

show users

現在 CLI にログインしているユーザに関する情報を表示するには、特権 EXEC モードで **show users** コマンドを使用します。

```
show users [ all ]
```

構文説明	all	(オプション) ログイン状況に関係なく、システムで構成されているすべてのユーザアカウントのリストを表示します
------	------------	--

デフォルト デフォルトの動作または値はありません。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア（自分のログインの表示のみ）

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。
	4.1(1)	ロックされたアカウントを表示するようにアップデート。 show users all のビューアの表示を制限。

使用上のガイドライン CLI でこのコマンドを使用すると、ID、ユーザ名、および権限を表示できます。説明の横の「*」は現行ユーザを示します。カッコ「()」で囲まれたユーザ名は、アカウントがロックされていることを示します。アカウントは、ユーザが連続して X 回、不正なパスワードを入力するとロックされます。ロックされたユーザのパスワードを **password** コマンドでリセットすると、アカウントのロックが解除されます。

同時にログインできる CLI ユーザの最大数は、プラットフォームによって異なります。



(注) このコマンドの出力は、Cisco IOS 12.0 コマンドの場合とは異なります。

例 次の例は、**show users** コマンドの出力を示します。

```
sensor# show users

      CLI ID      User           Privilege
-----
      1234        notheruser    viewer
*     9802        curuser       operator
      5824        tester        administrator
```

次の例は、tester2 のユーザアカウントがロックされていることを示します。

```
sensor# show users all

      CLI ID      User          Privilege
-----
      1234        notheruser    viewer
*     9802        curuser       operator
      5824        tester        administrator
                          (tester2)     viewer
                          foobar           operator
```

次の例は、ビューアに対する **show users all** の出力を示します。

```
sensor# show users all

      CLI ID      User          Privilege
-----
*     9802        tester        viewer
      5824        tester        viewer
```

関連コマンド

コマンド	説明
clear line	別の CLI セッションを終了します。

show version

すべてのインストールされている OS パッケージ、シグニチャ パッケージ、およびシステムで実行している IPS プロセスに関するバージョン情報を表示するには、特権 EXEC モードで **show version** コマンドを使用します。

show version

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン

show version コマンドの出力は IPS 固有で、Cisco IOS コマンドの出力とは異なります。

シリアル番号の後ろに、次のいずれかのライセンス情報が表示されます。

No license present

Expired license: <expiration-date>

Valid license, expires: <expiration-date>

Valid demo license, expires: <expiration-date>

<expiration-date> の形式は *dd-mon-yyyy* です (04-dec-2004 など)。



(注)

アップグレード履歴パッケージ名の前の * は、ダウングレードが実行された後の残りのバージョンを示します。* のマークが付いたパッケージがない場合、ダウングレードはできません。

例 次の例は、**show version** コマンドの出力を示します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 6.0(0.2)S184.0

Host:
  Realm Keys          key1.0
Signature Definition:
  Signature Update    S184.0          2005-11-09
OS Version:          2.4.30-IDS-smp-bigphys
Platform:            ASA-SSM-20
Serial Number:       021
No license present

Using 546975744 out of 2115760128 bytes of available memory (25% usage)

MainApp              2005_Nov_16_05.00  (Release)  2005-11-16T05:54:13-0600  Running
AnalysisEngine       2005_Nov_16_05.00  (Release)  2005-11-16T05:54:13-0600  Running
CLI                  2005_Nov_16_05.00  (Release)  2005-11-16T05:54:13-0600

Upgrade History:

  IPS-K9-maj-6.0-0.2  05:00:00 UTC Wed Nov 16 2005

Recovery Partition Version /var/idstmp

sensor#
```

ssh authorized-key

現行ユーザに公開キーを追加し、クライアントが RSA 認証を使用してローカル SSH サーバにログインできるようにするには、グローバル コンフィギュレーション モードで **ssh authorized-key** コマンドを使用します。このコマンドを **no** 形式で使用すると、システムから許可されたキーを削除できます。

ssh authorized-key *id* *key-modulus-length* *public-exponent* *public-modulus*

no **ssh authorized-key** *id*

構文説明

<i>id</i>	許可されたキーを一意に特定する 1 ～ 256 文字の文字列。数字、「_」、および「-」は有効ですが、スペースと「?」は使用できません。
<i>key-modulus-length</i>	511 ～ 2048 の範囲の ASCII 10 進整数。
<i>public-exponent</i>	3 ～ 2 ³² の範囲の ASCII 10 進整数。
<i>public-modulus</i>	ASCII 10 進整数。(2 ^(キーモジュラス長)) < x < (2 ^(キーモジュラス長)) の x 値。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者、オペレータ、ビューア

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン

このコマンドにより、現行ユーザの既知のホスト テーブルにエントリが追加されます。キーを変更するには、エントリを削除し、再作成する必要があります。

このコマンドは IPS 固有です。



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例

次の例は、既知のホスト テーブルにエントリを追加する方法を示します。

```
sensor(config)# ssh authorized-key system1 1023 37
66022272955660983338089706716372943357082868686000817201780243492180421420781303592082
95091017013584805250399939321125031474527683786209111899866537160898131479220860447399
11341369642870682319361928148521864094557416306138786468335115835910404940213136954353
39616344979349705016792583146548622146467421997057
sensor(config)#
```

関連コマンド

コマンド	説明
ssh authorized-keys	現行ユーザの公開 RSA キーを表示します。

ssh generate-key

センサーで SSH サーバが使用するサーバ ホスト キーを変更するには、特権 EXEC モードで **ssh generate-key** コマンドを使用します。

ssh generate-key

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン

表示されるキーのフィンガープリントは、このセンサーと今後接続されるリモート SSH クライアントが SSH プロトコルバージョン 1.5 を使用している場合、リモートクライアントで表示されるフィンガープリントと一致します。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

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ます。

```
sensor# ssh generate-key
MD5: 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
Bubble Babble: xebiz-vykyk-fekuh-rukuh-cabaz-paret-gosym-serum-korus-fypop-huxyx
sensor#
```

関連コマンド

コマンド	説明
show ssh server-key	SSH サーバのホスト キーとホスト キーのフィンガープリントを表示します。

ssh host-key

既知のホスト テーブルにエントリを追加するには、グローバル コンフィギュレーション モードで **ssh host-key** コマンドを使用します。モジュラス、指数、および長さを指定しない場合、要求された IP アドレスの MD5 フィンガープリントおよび Bubble Babble がシステムに表示されて、テーブルにキーを追加できます。このコマンドを **no** 形式で使用すると、既知のホスト テーブルからエントリを削除できます。

```
ssh host-key ipaddress [ key-modulus-length public-exponent public-modulus ]
```

```
no ssh host-key ipaddress
```

構文説明

<i>ipaddress</i>	ピリオドで区切られた 4 オクテットの 32 ビット アドレス。X.X.X.X、ここで X は 0 ～ 255。
<i>key-modulus-length</i>	511 ～ 2048 の範囲の ASCII 10 進整数。
<i>public-exponent</i>	3 ～ 2 ³² の範囲の ASCII 10 進整数。
<i>public-modulus</i>	ASCII 10 進整数。(2 ^x (キーモジュラス長) < x < (2 ^x (キーモジュラス長))) の x 値。

デフォルト

デフォルトの動作または値はありません。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者、オペレータ

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン

ssh host-key コマンドを使用すると、既知のホスト テーブルにエントリを追加できます。IP アドレスのキーを変更するには、エントリを削除し、再作成する必要があります。

モジュラス、指数、および長さを指定しない場合、指定された IP アドレスの SSH サーバに接続して、要求されたキーをネットワーク経由で取得します。指定するホストは、コマンドを発行した時点でアクセス可能である必要があります。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、10.1.2.3 の既知のホスト テーブルにエントリを追加する方法を示します。

```
sensor(config)# ssh host-key 10.1.2.3
1024 35
13930621354183524038533292225396881468568452352006413199783990511364012021781686969670
87217046313228442920738517305650448790826706775541579370584852039955721146312966045521
61309712601068614812749969593513740598331393154884988302302182922353335152653860589163
651944997842874583627883277460138506084043415861927
sensor(config)#
```

次の例は、10.1.2.3 の既知のホスト テーブルにエントリを追加する方法を示します。

```
sensor(config)# ssh host-key 10.1.2.3
MD5 fingerprint is 49:3F:FD:62:26:58:94:A3:E9:88:EF:92:5F:52:6E:7B
Bubble Babble is xebiz-vykyk-fekuh-rukuh-cabaz-paret-gosym-serum-korus-fypop-huxyx
Would you like to add this to the known hosts table for this host? [yes]
sensor(config)#
```

関連コマンド

コマンド	説明
<code>show ssh host-key</code>	センサーが接続できるリモート SSH サーバの公開キーを含む既知のホスト テーブルを表示します。

terminal

ログインセッションのターミナルプロパティを変更するには、特権 EXEC モードで **terminal** コマンドを使用します。

terminal [length screen-length]

構文説明	<i>screen-length</i>	画面の行数を設定します。マルチ画面出力時に一時停止する行数を指定するには、この値を使用します。値ゼロの場合は、出力が画面長を超えても一時停止しません。デフォルトは 24 行です。この値は、ログインセッション間で保存されません。
-------------	----------------------	---

デフォルト 「構文説明」の表を参照してください。

コマンドモード EXEC

サポートされるユーザロール 管理者、オペレータ、ビューア

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン **terminal length** コマンドを使用すると、`--more--` プロンプトが表示される前に、表示される行数を設定できます。

例 次の例は、マルチ画面表示の画面間で一時停止しないように CLI を設定します。

```
sensor# terminal length 0
sensor#
```

次の例は、マルチ画面表示の各画面について 10 行表示するように CLI を設定します。

```
sensor# terminal length 10
sensor#
```

tls generate-key

サーバの自己署名 X.509 証明書を再生成するには、特権 EXEC モードで **tls generate-key** を使用します。ホストで自己署名証明書を使用しない場合は、エラーが返されます。

tls generate-key

構文説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトの動作または値はありません。

コマンドモード

EXEC

サポートされるユーザロール

管理者

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次の例は、サーバの自己署名証明書を生成する方法を示します。

```
sensor(config)# tls generate-key  
MD5: 1F:94:6F:2E:38:AD:FB:2C:42:0C:AE:61:EC:29:74:BB  
SHA1: 16:AC:EC:AC:9D:BC:84:F5:D8:E4:1A:05:C4:01:BB:65:7B:4F:FC:AA  
sensor(config)#
```

関連コマンド

コマンド	説明
show tls fingerprint	サーバの TLS 証明書のフィンガープリントを表示します。

tls trusted-host

信頼できるホストをシステムに追加するには、グローバル コンフィギュレーション モードで `tls trusted-host` コマンドを使用します。このコマンドを `no` 形式で使用すると、信頼できるホスト証明書を削除できます。

```
tls trusted-host ip-address ip-address [port port]
```

```
no tls trusted-host ip-address ip-address [ port port ]
```

```
no tls trusted-host id id
```

構文説明

<code>ip-address</code>	追加または削除するホストの IP アドレス。
<code>port</code>	(オプション) 接続するホストのポート番号。デフォルトはポート 443 です。

デフォルト

「構文説明」の表を参照してください。

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者、オペレータ

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。
4.0(2)	オプションのポートを追加。ID に基づいた削除をサポートするため <code>no</code> コマンドを追加。

使用上のガイドライン

このコマンドを使用すると、要求されたホスト / ポートの現行のフィンガープリントを取得して、その結果を表示できます。追加が要求されているホストから直接取得した情報に基づいて、フィンガープリントを受け入れるか拒否するかを選択できます。

各証明書は、ID フィールド付きで保存されます。IP アドレスおよびデフォルト ポートの ID フィールドは `ipaddress` で、IP アドレスおよび指定ポートの ID フィールドは `ipaddress:port` です。



(注) このコマンドは IPS 固有です。12.0 以前のバージョンに、関連する IOS コマンドはありません。

例

次のコマンドは、信頼できるホスト テーブルに、IP アドレス 172.21.172.1、ポート 443 のエントリを追加します。

```
sensor(config)# tls trusted-host ip-address 172.21.172.1
Certificate MD5 fingerprint is D4:C2:2F:78:B5:C6:30:F2:C4:6A:8E:5D:6D:C0:DE:32
Certificate SHA1 fingerprint is
36:42:C9:1B:9F:A4:A8:91:7F:DF:F0:32:04:26:E4:3A:7A:70:B9:95
Would you like to add this to the trusted certificate table for this host? [yes]
Certificate ID: 172.21.172.1 successfully added to the TLS trusted host table.
sensor(config)#
```




(注) コマンドが正常に終了すると、要求された証明書に関して保存された証明書 ID が表示されます。

次のコマンドは、IP アドレス 172.21.172.1、ポート 443 の信頼できるホストエントリーを削除します。

```
sensor(config)# no tls trusted-host ip-address 172.21.172.1
sensor(config)#
```

または、次のコマンドを使用して、IP アドレス 172.21.172.1、ポート 443 の信頼できるホストエントリーを削除できます。

```
sensor(config)# no tls trusted-host id 172.21.172.1
sensor(config)#
```

次のコマンドは、信頼できるホスト テーブルに、IP アドレス 10.1.1.1、ポート 8000 のエントリーを追加します。

```
sensor(config)# tls trusted-host ip-address 10.1.1.1 port 8000
Certificate MD5 fingerprint is D4:C2:2F:78:B5:C6:30:F2:C4:6A:8E:5D:6D:C0:DE:32
Certificate SHA1 fingerprint is
36:42:C9:1B:9F:A4:A8:91:7F:DF:F0:32:04:26:E4:3A:7A:70:B9:95
Would you like to add this to the trusted certificate table for this host? [yes]
Certificate ID: 10.1.1.1:8000 successfully added to the TLS trusted host table.
sensor(config)#
```



(注) コマンドが正常に終了すると、要求された証明書に関して保存された証明書 ID が表示されます。

次のコマンドは、IP アドレス 10.1.1.1、ポート 8000 の信頼できるホストエントリーを削除します。

```
sensor(config)# no tls trusted-host ip-address 10.1.1.1 port 8000
sensor(config)#
```

または、次のコマンドを使用して、IP アドレス 10.1.1.1、ポート 8000 の信頼できるホストエントリーを削除できます。

```
sensor(config)# no tls trusted-host id 10.1.1.1:8000
sensor(config)#
```

関連コマンド

コマンド	説明
<code>show tls trusted-hosts</code>	センサーの信頼できるホストを表示します。

trace

IP パケットが宛先に送信されるルートを表示するには、特権 EXEC モードで **trace** コマンドを使用します。

```
trace address [count]
```

構文説明	<i>address</i>	ルートをトレースするシステムのアドレス。
	<i>count</i>	使用するホップ数。デフォルトは 4 です。有効な値は 1 ~ 256 です。

デフォルト 「構文説明」の表を参照してください。

コマンドモード EXEC

コマンドタイプ 管理者、オペレータ、ビューア

コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン **trace** コマンドには、コマンド割り込みはありません。コマンドは完了するまで実行する必要があります。

例 次の例は、**trace** コマンドの出力を示します。

```
sensor# trace 10.1.1.1
traceroute to 172.21.172.24 (172.21.172.24), 30 hops max, 40 byte packets 1
171.69.162.2 (171.69.162.2) 1.25 ms 1.37 ms 1.58 ms 2 172.21.172.24 (172.21.172.24)
0.77 ms 0.66 ms 0.68 ms
sensor#
```

upgrade

サービス パック、シグニチャ アップデート、またはイメージアップグレードを適用するには、グローバル コンフィギュレーション モードで **upgrade** コマンドを使用します。

upgrade *source-url*

構文説明	<i>source-url</i>	取得するアップグレードの場所。
デフォルト	デフォルトの動作または値はありません。	
コマンド モード	グローバル コンフィギュレーション	
サポートされるユーザロール	管理者	
コマンド履歴	リリース	修正
	4.0(1)	このコマンドを導入。

使用上のガイドライン コマンドラインから、すべての必要なソースおよび宛先 URL 情報とユーザ名を入力できます。コマンド (**upgrade**) の後にプレフィックス (**ftp:** または **scp:**) だけを入力した場合は、適用されるパスワードを含む、不足している情報についてのプロンプトが表示されます。

ディレクトリは、必要なファイルへの絶対パスで指定する必要があります。アップグレードを繰り返す場合は、ファイル名を指定しないでください。指定した曜日の指定した時間に、繰り返しアップグレードを行うようにセンサーを設定できます。または、最初のアップグレードから指定した時間が経過した後で繰り返しアップグレードを行うように設定できます。

ソース URL の正確なフォーマットはファイルにより異なります。次の有効なタイプがサポートされています。

プレフィックス	ソースまたは宛先
ftp:	FTP ネットワーク サーバのソース URL。このプレフィックスの構文は、次のとおりです。 ftp://[username@] location]/relativeDirectory]/filename ftp://[username@]location]/absoluteDirectory]/filename
scp:	SCP ネットワーク サーバのソース URL。このプレフィックスの構文は、次のとおりです。 scp://[username@] location]/relativeDirectory]/filename scp://[username@] location]/absoluteDirectory]/filename
http:	Web サーバのソース URL。このプレフィックスの構文は、次のとおりです。 http://[username@]location]/directory]/filename
https:	Web サーバのソース URL。このプレフィックスの構文は、次のとおりです。 https://[username@]location]/directory]/filename



(注) このコマンドは、Cisco IOS 12.0 以前にはありません。

例 次の例は、センサーに対して、指定されたアップグレードをすぐに確認するよう指示します。ディレクトリとパスは `tester` のユーザアカウントを基準とします。

```
sensor(config)# upgrade scp://tester@10.1.1.1/upgrade/sp.rpm
Enter password: *****
Re-enter password: *****
```

username

ローカル センサーのユーザを作成するには、グローバル コンフィギュレーション モードで **username** コマンドを使用します。ユーザを作成するには、管理者になる必要があります。このコマンドを **no** 形式で使用すると、センサーからユーザを削除できます。この場合、ユーザは CLI と Web アクセスの両方から削除されます。

username *name* [**password** *password*] [**privilege** *privilege*]

no username *name*

構文説明

name	ユーザ名を指定します。有効なユーザ名の長さは 1 ～ 64 文字です。ユーザ名の先頭は、英数字にする必要があります。その他の文字には、すべての文字を使用できます。
password	ユーザのパスワードを指定します。有効なパスワードの長さは 8 ～ 32 文字です。スペース以外のすべての文字を使用できます。
privilege	ユーザの権限レベルを指定します。使用できるレベルは、サービス、管理者、オペレータ、ビューアで、デフォルトはビューアです。

デフォルト

「構文説明」の表を参照してください。

コマンドモード

グローバル コンフィギュレーション

サポートされるユーザロール

管理者

コマンド履歴

リリース	修正
4.0(1)	このコマンドを導入。

使用上のガイドライン

username コマンドを使用すると、ログインだけを目的としたユーザ名またはパスワード、またはその両方を認証できます。このコマンドを実行しているユーザは、自分自身を削除できません。

コマンドラインでパスワードを指定しなかった場合は、プロンプトが表示されます。**password** コマンドを使用すると、現行ユーザまたはシステムの既存のユーザのパスワードを変更できます。**privilege** コマンドを使用すると、システムの既存のユーザの権限を変更できます。

例 次の例は、ビューア レベルの権限とパスワード testpassword を持つユーザ tester を追加します。

```
sensor(config)# username tester password testpassword
```

次の例は、入力パスワードが保護されていることを示します。

```
sensor(config)# username tester
Enter Login Password: *****
Re-enter Login Password: *****
```

次の例は、ユーザ「tester」の権限をオペレータに変更します。

```
sensor(config)# username tester privilege operator
```

関連コマンド

コマンド	説明
password	ローカル センサーのパスワードを更新します。
privilege	既存のユーザの権限レベルを変更します。

■ username