



## システム管理コマンド

---

- arp (4 ページ)
- boot (5 ページ)
- cat (6 ページ)
- copy (7 ページ)
- copy startup-config tftp: (8 ページ)
- copy tftp: startup-config (9 ページ)
- debug voice diagnostics mac-address (10 ページ)
- debug platform condition feature multicast controlplane (11 ページ)
- debug platform condition mac (13 ページ)
- debug platform rep (15 ページ)
- debug ilpower powerman (17 ページ)
- delete (20 ページ)
- dir (21 ページ)
- exit (23 ページ)
- factory-reset (24 ページ)
- flash\_init (27 ページ)
- help (28 ページ)
- install (29 ページ)
- ip ssh bulk-mode (33 ページ)
- l2 traceroute (35 ページ)
- license air level (36 ページ)
- license boot level (38 ページ)
- license smart (グローバル コンフィギュレーション) (41 ページ)
- license smart (特権 EXEC) (52 ページ)
- line auto-consolidation (62 ページ)
- location (64 ページ)
- location plm calibrating (68 ページ)
- mac address-table move update (69 ページ)
- mgmt\_init (71 ページ)

- [mkdir \(72 ページ\)](#)
- [more \(73 ページ\)](#)
- [no debug all \(74 ページ\)](#)
- [rename \(75 ページ\)](#)
- [request consent-token accept-response shell-access \(76 ページ\)](#)
- [request consent-token generate-challenge shell-access \(77 ページ\)](#)
- [request consent-token terminate-auth \(78 ページ\)](#)
- [request platform software console attach switch \(79 ページ\)](#)
- [reset \(81 ページ\)](#)
- [rmdir \(82 ページ\)](#)
- [sdm prefer \(83 ページ\)](#)
- [service private-config-encryption \(84 ページ\)](#)
- [set \(85 ページ\)](#)
- [show avc client \(88 ページ\)](#)
- [show bootflash: \(89 ページ\)](#)
- [show consistency-checker mcast \(92 ページ\)](#)
- [show consistency-checker objects \(95 ページ\)](#)
- [show consistency-checker run-id \(97 ページ\)](#)
- [show debug \(99 ページ\)](#)
- [show env xps \(100 ページ\)](#)
- [show flow monitor \(104 ページ\)](#)
- [show idprom module \(106 ページ\)](#)
- [show install \(108 ページ\)](#)
- [show license all \(111 ページ\)](#)
- [show license authorization \(118 ページ\)](#)
- [show license data translation \(124 ページ\)](#)
- [show license eventlog \(125 ページ\)](#)
- [show license history message \(127 ページ\)](#)
- [show license reservation \(128 ページ\)](#)
- [show license status \(129 ページ\)](#)
- [show license summary \(139 ページ\)](#)
- [show license tech \(143 ページ\)](#)
- [show license udi \(161 ページ\)](#)
- [show license usage \(162 ページ\)](#)
- [show location \(166 ページ\)](#)
- [show logging onboard switch uptime \(168 ページ\)](#)
- [show mac address-table \(171 ページ\)](#)
- [show mac address-table move update \(176 ページ\)](#)
- [show parser encrypt file status \(177 ページ\)](#)
- [show platform hardware fpga \(178 ページ\)](#)
- [show platform integrity \(179 ページ\)](#)

- [show platform software audit](#) (180 ページ)
- [show platform software fed switch punt cause](#) (184 ページ)
- [show platform software fed switch punt cpuq](#) (186 ページ)
- [show platform software sl-infra](#) (190 ページ)
- [show platform sudi certificate](#) (191 ページ)
- [show running-config](#) (193 ページ)
- [show sdm prefer](#) (199 ページ)
- [show tech-support confidential](#) (201 ページ)
- [show tech-support monitor](#) (202 ページ)
- [show tech-support platform](#) (203 ページ)
- [show tech-support platform evpn\\_vxlan](#) (207 ページ)
- [show tech-support platform fabric](#) (210 ページ)
- [show tech-support platform igmp\\_snooping](#) (214 ページ)
- [show tech-support platform layer3](#) (217 ページ)
- [show tech-support platform mld\\_snooping](#) (225 ページ)
- [show tech-support port](#) (232 ページ)
- [show tech-support pvlan](#) (235 ページ)
- [show version](#) (236 ページ)
- [system env temperature threshold yellow](#) (244 ページ)
- [traceroute mac](#) (246 ページ)
- [traceroute mac ip](#) (249 ページ)
- [type](#) (252 ページ)
- [unset](#) (253 ページ)
- [upgrade rom-monitor capsule](#) (255 ページ)
- [version](#) (257 ページ)

# arp

Address Resolution Protocol (ARP) テーブルの内容を表示するには、ブートローダモードで **arp** コマンドを使用します。

**arp** [*ip\_address* ]

---

**構文の説明**      *ip\_address*    (任意) ARP テーブルまたは特定の IP アドレスのマッピングを表示します。

---

**コマンド デフォルト**      デフォルトの動作や値はありません。

**コマンド モード**          ブートローダ

---

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

---

**使用上のガイドライン**      ARP テーブルには、IP アドレスと MAC アドレスのマッピングが示されます。

## 例

次に、ARP テーブルを表示する例を示します。

```
Device: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

# boot

実行可能イメージをロードおよびブートして、コマンドラインインターフェイス (CLI) を表示するには、ブートローダモードで **boot** コマンドを使用します。

## 構文の説明

<i>filesystem:</i>	ファイルシステムのエイリアス。システム ボードフラッシュ デバイスには <b>flash:</b> を使用します。USB メモリスティックには <b>usbflash0:</b> を使用します。
<i>file-url</i>	ブート可能なイメージのパス (ディレクトリ) および名前。各イメージ名はセミコロンで区切ります。

## コマンドデフォルト

デフォルトの動作や値はありません。

## コマンドモード

ブートローダ

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

引数を何も指定しないで **boot** コマンドを入力した場合、デバイスは、BOOT 環境変数が設定されていればその中の情報を使用して、システムを自動的にブートしようとします。

*file-url* 変数にイメージ名を指定した場合、**boot** コマンドは指定されたイメージをブートしようとします。

ブートローダ **boot** コマンドのオプションを設定した場合は、このコマンドがただちに実行され、現在のブートローダセッションだけに適用されます。

これらの設定が保存されて次回のブート処理に使用されることはありません。

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

## 例

次の例では、*new-image.bin* イメージを使用してデバイスをブートする方法を示します。

```
Device: set BOOT flash:/new-images/new-image.bin
Device: boot
```

このコマンドを入力すると、セットアッププログラムを開始するように求められます。

# cat

1つ以上のファイルの内容を表示するには、ブートローダモードで**cat** コマンドを使用します。

**cat** *filesystem:/file-url...*

## 構文の説明

*filesystem:* ファイルシステムを指定します。

*/file-url* 表示するファイルのパス（ディレクトリ）と名前を指定します。ファイル名はスペースで区切ります。

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

ブートローダ

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

## 例

次の例では、イメージファイルの内容を表示する方法を示します。

```
Device: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

# copy

ファイルをコピー元からコピー先にコピーするには、ブートローダモードで **copy** コマンドを使用します。

**copy** *filesystem:/source-file-url filesystem:/destination-file-url*

## 構文の説明

*filesystem:* ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。

*/source-file-url* コピー元のパス（ディレクトリ）およびファイル名です。

*/destination-file-url* コピー先のパス（ディレクトリ）およびファイル名です。

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

ブートローダ

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スラッシュ (/) 間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大 127 文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

ファイルを別のディレクトリにコピーする場合は、そのディレクトリが存在していなければなりません。

## 例

次の例では、ルートにあるファイルをコピーする方法を示します。

```
Device: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

ファイルがコピーされたかどうかを確認するには、**dir filesystem:** ブートローダコマンドを入力します。

## copy startup-config tftp:

スイッチから TFTP サーバに設定をコピーするには、特権 EXEC モードで **copy startup-config tftp:** コマンドを使用します。

**copy startup-config tftp:** *remote host {ip-address}/{name}*

### 構文の説明

*remote host {ip-address}/{name}* リモートホストのホスト名または IP アドレス。

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

特権 EXEC

### コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

### 使用上のガイドライン

スイッチから現在の設定をコピーするには、**copy startup-config tftp:** コマンドを実行し、続く指示に従います。設定が TFTP サーバにコピーされます。

次に、別のスイッチへログインし、**copy tftp: startup-config** コマンドを実行して、続く指示に従います。これで、設定は別のスイッチにコピーされます。

### 例

次に、TFTP サーバに設定をコピーする例を示します。

```
Device: copy startup-config tftp:
Address or name of remote host []?
```



## copy tftp: startup-config

TFTP サーバから新しいスイッチに設定をコピーするには、新しいスイッチ上で、特権 EXEC モードで **copy tftp: startup-config** コマンドを使用します。

```
copy tftp: startup-config remote host {ip-address}/{name}
```

---

### 構文の説明

*remote host {ip-address}/{name}* リモートホストのホスト名または IP アドレス。

---

---

### コマンド デフォルト

デフォルトの動作や値はありません。

---

### コマンド モード

特権 EXEC

---

### コマンド履歴

リリース	変更内容
------	------

---

Cisco IOS XE リリース 16.1 このコマンドが導入されました。

---

---

### 使用上のガイドライン

設定をコピーした後、その設定を保存するには、**write memory** コマンドを使用し、その後スイッチをリロードするか、または **copy startup-config running-config** コマンドを実行します。

---

### 例

次に、TFTP サーバからスイッチに設定をコピーする例を示します。

```
Device: copy tftp: startup-config
Address or name of remote host []?
```

## debug voice diagnostics mac-address

音声クライアントの音声診断のデバッグを有効にするには、特権 EXEC モードで **debug voice diagnostics mac-address** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

**debug voice diagnostics mac-address mac-address1 verbose mac-address mac-address2 verbose**  
**nodebug voice diagnostics mac-address mac-address1 verbose mac-address mac-address2 verbose**

構文の説明	<b>voice diagnostics</b>	音声クライアントの音声のデバッグを設定します。
	<b>mac-address mac-address1 mac-address mac-address2</b>	音声クライアントの MAC アドレスを指定します。
	<b>verbose</b>	音声診断の冗長モードを有効にします。

コマンド デフォルト      デフォルトの動作や値はありません。

コマンド モード      特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

以下は、**debug voice diagnostics mac-address** コマンドの出力例で、MAC アドレスが 00:1f:ca:cf:b6:60 である音声クライアントの音声診断のデバッグを有効にする手順を示しています。

```
Device# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

## debug platform condition feature multicast controlplane

Internet Group Management Protocol (IGMP) およびマルチキャストリスナー検出 (MLD) のスヌーピング機能の放射線トレースを有効にするには、特権 EXEC モードで **debug platform condition feature multicast controlplane** コマンドを使用します。放射線トレースを無効にするには、このコマンドの **no** 形式を使用します。

```
debug platform condition feature multicast controlplane {{igmp-debug | pim} group-ip {ipv4 address / ipv6 address} | {mld-snooping | igmp-snooping} mac mac-address ip {ipv4 address / ipv6 address} vlan vlan-id } level {debug | error | info | verbose | warning}
no debug platform condition feature multicast controlplane {{igmp-debug | pim} group-ip {ipv4 address / ipv6 address} | {mld-snooping | igmp-snooping} mac mac-address ip {ipv4 address / ipv6 address} vlan vlan-id } level {debug | error | info | verbose | warning}
```

### 構文の説明

<b>igmp-debug</b>	IGMP制御の放射線トレースを有効にします。
<b>pim</b>	Protocol Independent Multicast (PIM) 制御の放射線トレースを有効にします。
<b>mld-snooping</b>	MLD スヌーピング制御の放射線トレースを有効にします。
<b>igmp-snooping</b>	IGMP スヌーピング制御の放射線トレースを有効にします。
<b>mac mac-address</b>	受信者の MAC アドレス。
<b>group-ip {ipv4 address / ipv6 address}</b>	igmp-debug または pim グループの IPv4 または IPv6 アドレス。
<b>ip {ipv4 address / ipv6 address}</b>	mld-snooping または igmp-snooping グループの IPv4 または IPv6 アドレス。
<b>vlan vlan-id</b>	VLAN ID。指定できる範囲は 1 ~ 4094 です。
<b>level</b>	デバッグの重大度レベルを有効にします。
<b>debug</b>	デバッグレベルを有効にします。
<b>error</b>	エラーデバッグを有効にします。

<b>info</b>	情報デバッグを有効化します。
<b>verbose</b>	詳細デバッグを有効にします。
<b>warning</b>	警告デバッグを有効にします。

## コマンドモード

特権 EXEC (#)

## コマンド履歴

リリース 変更内容

Cisco IOS XE Gibraltar 16.10.1 このコマンドが導入されました。

次に、IGMP スヌーピングの放射線トレース有効にする例を示します。

```
Device# debug platform condition feature multicast controlplane igmp-snooping mac
000a.f330.344a ip 10.1.1.10 vlan 550 level warning
```

## 関連コマンド

Command	Description
<b>clear debug platform condition all</b>	プラットフォームに適用されているデバッグ条件を削除します。
<b>debug platform condition</b>	指定した条件に基づいて <b>debug</b> コマンドのデバッグ出力をフィルタリングします。
<b>debug platform condition start</b>	システムの条件付きデバッグを開始します。
<b>debug platform condition stop</b>	システムの条件付きデバッグを停止します。
<b>show platform condition</b>	現在アクティブなデバッグ設定を表示します。

## debug platform condition mac

MAC ラーニングの放射線トレースを有効にするには、特権 EXEC モードで **debug platform condition mac** コマンドを使用します。MAC ラーニングの放射線トレースを無効にするには、このコマンドの **no** 形式を使用します。

**debug platform condition mac** {*mac-address* {**control-plane** | **egress** | **ingress**} | **access-list** *access-list name* {**egress** | **ingress**}}

**no debug platform condition mac** {*mac-address* {**control-plane** | **egress** | **ingress**} | **access-list** *access-list name* {**egress** | **ingress**}}

構文の説明	構文	説明
	<b>mac</b> <i>mac-address</i>	指定された MAC アドレスに基づいて出力をフィルタリングします。
	<b>access-list</b> <i>access-list name</i>	指定されたアクセスリストに基づいて出力をフィルタリングします。
	<b>control-plane</b>	コントロールプレーンのルーチンに関するメッセージを表示します。
	<b>egress</b>	発信パケットに基づいて出力をフィルタリングします。
	<b>ingress</b>	着信パケットに基づいて出力をフィルタリングします。

コマンドモード 特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、MAC アドレスに基づいてデバッグ出力をフィルタリングする例を示します。

```
Device# debug platform condition mac bc16.6509.3314 ingress
```

### 関連コマンド

Command	Description
<b>show platform condition</b>	現在アクティブなデバッグ設定を表示します。
<b>debug platform condition</b>	指定した条件に基づいて <b>debug</b> コマンドのデバッグ出力をフィルタリングします。

Command	Description
<b>debug platform condition start</b>	システムの条件付きデバッグを開始します。
<b>debug platform condition stop</b>	システムの条件付きデバッグを停止します。
<b>clear debug platform condition all</b>	プラットフォームに適用されているデバッグ条件を削除します。

## debug platform rep

Resilient Ethernet Protocol (REP) 機能のデバッグをイネーブルにするには、特権 EXEC モードで **debug platform rep** コマンドを使用します。指定した条件を削除するには、このコマンドの **no** 形式を使用します。

**debug platform rep {all | error | event | packet | verbose}**  
**no debug platform rep {all | error | event | packet | verbose}**

### 構文の説明

<b>all</b>	すべての REP デバッグ機能をイネーブルにします。
<b>error</b>	REP エラーデバッグをイネーブルにします。
<b>event</b>	REP イベントデバッグをイネーブルにします。
<b>packet</b>	REP パケットデバッグをイネーブルにします。
<b>verbose</b>	REP 詳細デバッグをイネーブルにします。

### コマンドモード

特権 EXEC (#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、すべての機能のデバッグをイネーブルにする例を示します。

```
Device# debug platform rep all

debug platform rep verbose debugging is on
debug platform rep control pkt handle debugging is on
debug platform rep error debugging is on
debug platform rep event debugging is on
```

### 関連コマンド

Command	Description
<b>show platform condition</b>	現在アクティブなデバッグ設定を表示します。
<b>debug platform condition</b>	指定した条件に基づいて <b>debug</b> コマンドのデバッグ出力をフィルタリングします。

Command	Description
<b>debug platform condition start</b>	システムの条件付きデバッグを開始します。
<b>debug platform condition stop</b>	システムの条件付きデバッグを停止します。
<b>clear debug platform condition all</b>	プラットフォームに適用されているデバッグ条件を削除します。



## debug ilpower powerman

電源コントローラおよびPoweroverEthernet (PoE) システムのデバッグをイネーブルにするには、特権EXECモードで **debug ilpower powerman** コマンドを使用します。デバッグをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**コマンドデフォルト** このコマンドには引数またはキーワードはありません。

**コマンドモード** 特権 EXEC

**コマンド履歴**

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

次に、Cisco IOS XE Gibraltar 16.10.1 よりも前のリリースの **debug ilpower powerman** コマンドの出力例を示します。

```
Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface
Gix/y/z: Power Controller reports power Imax error detected
Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign
is done by proto CDP
Port Gil/0/48: Selected Protocol CDP
Mar 8 16:35:17.801: Ilpowerinterface (Gil/0/48) process tlvfrom cdpINPUT:

Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1,
power_man_id= 2,
Mar 8 16:35:17.801: power_request_level[] = 2640 0 0 0 0
Mar 8 16:35:17.801:
Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: Ilpowerinterface (Gil/0/48) power negotiation:
consumption = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gil/0/48) setting ICUT_OFF
threshold to 2640.
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.115: ILP:: posting ilpslot 1 port 48 event 5 class 0
Mar 8 16:35:18.115: ILP:: Gil/0/48: State=NGWC_ILP_LINK_UP_S-6,
Event=NGWC_ILP_IMAX_FAULT_EV-5
Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdownGil/0/48
Mar 8 16:35:18.115: Ilpowerinterface (Gil/0/48), delete allocated power
2640
Mar 8 16:35:18.116: Ilpowerinterface (Gil/0/48) setting ICUT_OFF
threshold to 0.
Mar 8 16:35:18.116: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.116: ilpower_notify_lldp_power_via_mdi_tlvGil/0/48
```

```

pwralloc0
Mar 8 16:35:18.116: Gi1/0/48 AUTO PORT PWR Alloc130 Request 130
Mar 8 16:35:18.116: Gi1/0/48: LLDP NOTIFY TLV:
(curr/prev) PSE Allocation: 13000/0
(curr/prev) PD Request : 13000/0
(curr/prev) PD Class : Class 4/
(curr/prev) PD Priority : low/unknown
(curr/prev) Power Type : Type 2 PSE/Type 2 PSE
(curr/prev) mdi_pwr_support: 7/0
(curr/prevPower Pair) : Signal/
(curr/prev) PSE PwrSource : Primary/Unknown

```

次に、Cisco IOS XE Gibraltar 16.10.1 以降の **debug ilpower powerman** コマンドの出力例を示します。power\_request\_level、PSE Allocation、および PD Request に電力の単位 (mW) が追加されています。power\_request\_level にゼロ以外の値のみが表示されるようになりました。

```

Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface
Gix/y/z: Power Controller reports power Imax error detected
Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign
is done by proto CDP
Port Gi1/0/48: Selected Protocol CDP
Mar 8 16:35:17.801: Ilpowerinterface (Gi1/0/48) process tlvfrom cdpINPUT:

Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1,
power_man_id= 2,
Mar 8 16:35:17.801: power_request_level(mW) = 2640
<----- mW unit added, non-zero value display
Mar 8 16:35:17.801:
Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) power negotiation:
consumption = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF
threshold to 2640.
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.115: ILP:: posting ilpslot 1 port 48 event 5 class 0
Mar 8 16:35:18.115: ILP:: Gi1/0/48: State=NGWC_ILP_LINK_UP_S-6,
Event=NGWC_ILP_IMAX_FAULT_EV-5
Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdownGi1/0/48
Mar 8 16:35:18.115: Ilpowerinterface (Gi1/0/48), delete allocated power
2640
Mar 8 16:35:18.116: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF
threshold to 0.
Mar 8 16:35:18.116: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.116: ilpower_notify_lldp_power_via_mdi_tlvGi1/0/48
pwralloc0
Mar 8 16:35:18.116: Gi1/0/48 AUTO PORT PWR Alloc130 Request 130

```

```
Mar 8 16:35:18.116: Gi1/0/48: LLDP NOTIFY TLV:  
(curr/prev) PSE Allocation (mW): 13000/0  
<----- mW unit added  
(curr/prev) PD Request (mW) : 13000/0  
<----- mW unit added  
(curr/prev) PD Class : Class 4/  
(curr/prev) PD Priority : low/unknown  
(curr/prev) Power Type : Type 2 PSE/Type 2 PSE  
(curr/prev) mdi_pwr_support: 7/0  
(curr/prevPower Pair) : Signal/  
(curr/prev) PSE PwrSource : Primary/Unknown
```

# delete

指定されたファイルシステムから1つ以上のファイルを削除するには、ブートローダモードで **delete** コマンドを使用します。

**delete filesystem:/file-url...**

## 構文の説明

*filesystem*: ファイルシステムのエイリアス。USB メモリスティックの場合は、**usbflash0** を使用します。

*/file-url...* 削除するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

ブートローダ

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

各ファイルを削除する前に確認を求めるプロンプトがデバイスによって表示されます。

## 例

次の例では、2つのファイルを削除します。

```
Device: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

ファイルが削除されたことを確認するには、**dir usbflash0**: ブートローダコマンドを入力します。

# dir

指定されたファイルシステムのファイルおよびディレクトリのリストを表示するには、ブートローダモードで **dir** コマンドを使用します。

**dir** *filesystem:/file-url*

## 構文の説明

*filesystem:* ファイルシステムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。USB メモリスティックには **usbflash0:** を使用します。

*/file-url* (任意) 表示するコンテンツが格納されているパス (ディレクトリ) およびディレクトリの名前です。ディレクトリ名はスペースで区切ります。

## コマンドデフォルト

デフォルトの動作や値はありません。

## コマンドモード

ブートローダ  
特権 EXEC

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

ディレクトリ名では、大文字と小文字が区別されます。

## 例

次の例では、フラッシュメモリ内のファイルを表示する方法を示します。

```
Device: dir flash:
Directory of flash:/
  2  -rwx      561   Mar 01 2013 00:48:15  express_setup.debug
  3  -rwx    2160256   Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
  4  -rwx     1048   Mar 01 2013 00:01:39  multiple-fs
  6  drwx      512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
645 drwx      512   Mar 01 2013 00:01:11  dc_profile_dir
647 -rwx     4316   Mar 01 2013 01:14:05  config.text
648 -rwx        5   Mar 01 2013 00:01:39  private-config.text

96453632 bytes available (25732096 bytes used)
```

表 1: *dir* のフィールドの説明

フィールド	説明
2	ファイルのインデックス番号

フィールド	説明
-rwx	ファイルのアクセス権 (次のいずれか、またはすべて) <ul style="list-style-type: none"><li>• d : ディレクトリ</li><li>• r : 読み取り可能</li><li>• w : 書き込み可能</li><li>• x : 実行可能</li></ul>
1644045	ファイルのサイズ
<date>	最終変更日
env_vars	ファイル名

# exit

以前のモードに戻るか、CLI EXEC モードを終了するには、**exit** コマンドを使用します。

## exit

---

**構文の説明**

このコマンドには引数またはキーワードはありません。

---

**コマンド デフォルト**

デフォルトの動作や値はありません。

---

**コマンド モード**

特権 EXEC

グローバル コンフィギュレーション

---

**コマンド履歴**

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

次に、コンフィギュレーション モードを終了する例を示します。

```
Device(config)# exit  
Device#
```

# factory-reset

お客様固有のすべてのデータを消去し、デバイスを工場出荷時の設定に戻すには、特権 EXEC モードで **factory-reset** コマンドを使用します。



(注) NIST SP 800-88 Rev. 1 で説明されているように、消去は **clear** メソッドと一致します。

## Standalone Device

**factory-reset all [secure 3-pass] | boot-vars | config**

## Stacked Device

**factory-reset all [secure 3-pass] | boot-vars | config | switch switch\_number | all all [secure 3-pass] | boot-vars | config**

### 構文の説明

<b>all</b>	NVRAM のすべての内容、現在のブートイメージ、ブート変数、起動コンフィギュレーションと実行コンフィギュレーションのデータ、およびユーザデータを含むすべての Cisco IOS イメージを消去します。
<b>secure 3-pass</b>	3-pass 上書きでデバイスからすべての内容を消去します。 <ul style="list-style-type: none"> <li>• Pass 1 : すべてのアドレス可能な場所を 2 進数のゼロで上書きします。</li> <li>• Pass 2 : すべてのアドレス可能な場所を 2 進数の 1 で上書きします。</li> <li>• Pass 3 : すべてのアドレス可能な場所をランダムビットパターンで上書きします。</li> </ul>
<b>boot-vars</b>	ユーザによって追加されたブート変数のみを消去します。
<b>config</b>	スタートアップ コンフィギュレーションのみを消去します。
<b>switch</b> { <i>switch_number</i>   <b>all</b> }	選択したスイッチのコンテンツを消去します。 <ul style="list-style-type: none"> <li>• <i>switch-number</i> : スイッチ番号を指定します。指定できる範囲は 1 ~ 16 です。</li> <li>• <b>all</b> : スタック内のすべてのスイッチを選択します。</li> </ul>

コマンド デフォルト なし

コマンド モード 特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。



リリース	変更内容
Cisco IOS XE Amsterdam 17.2.1	<b>secure 3-pass</b> キーワードと <b>switch</b> キーワードが導入されました。

**使用上のガイドライン** **factory-reset** コマンドは、次のシナリオで使用されます。

- 返品許可（RMA）のためにデバイスをシスコに返送する必要がある場合は、このコマンドを使用してお客様固有のデータをすべて削除してからデバイスの RMA 証明書を取得します。
- デバイ스에保存されている重要な情報やクレデンシャルに不正にアクセスされた場合は、このコマンドを使用してデバイスを初期設定にリセットしてから再設定します。

工場出荷時の状態へのリセットプロセスが正常に完了すると、デバイスがリブートして ROMMON モードになります。

## 例

次に、**factory-reset all** コマンドを使用してデバイスのすべての内容を消去する例を示します。

```
Device> enable
Device# factory-reset all

The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, including the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units(USB/SSD/SATA)
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
You will need to load IOS image using USB/TFTP from rommon after
this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
```

次に、スタック構成デバイスで初期設定へのリセットを実行する例を示します。

```
Device> enable
Device# factory-reset switch all all

The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, including the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units(USB/SSD/SATA)
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
You will need to load IOS image using USB/TFTP from rommon after
this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
Chassis 1 reloading, reason - Factory Reset
```

```

Protection key not found
9300L#Oct 25 09:53:05.740: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting:
reload fp action requested
Oct 25 09:53:07.277: %PMAN-5-EXITACTION:vp: Process manager is exiting: rp processes
exit with reload switch code

Enabling factory reset for this reload cycle
Switch booted with
tftp://10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin

Switch booted via
//10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
% FACTORYRESET - Started Cleaning Up...

% FACTORYRESET - Unmounting sd1
% FACTORYRESET - Cleaning Up sd1 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...
% FACTORYRESET - finish erase

% FACTORYRESET - Making File System sd1 [0]
Discarding device blocks: done
Creating filesystem with 409600 4k blocks and 102544 inodes
Filesystem UUID: fcf01664-7c6f-41ce-99f0-6df1d941701e
Superblock backups stored on blocks:
 32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done

% FACTORYRESET - Mounting Back sd1 [0]
% FACTORYRESET - Handling Mounted sd1
% FACTORYRESET - Factory Reset Done for sd1

% FACTORYRESET - Unmounting sd3
% FACTORYRESET - Cleaning Up sd3 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...

Chassis 2 reloading, reason - Factory Reset
Dec 12 01:02:12.500: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload
fp action requested
De
Enabling factory reset for this reload cycle
Switch booted with
tftp://10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin

Switch booted via
//10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
% FACTORYRESET - Started Cleaning Up...
% FACTORYRESET - Unmounting sd1
% FACTORYRESET - Cleaning Up sd1 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...

After this the switch will come to boot prompt. Then the customer has to boot the device
from TFTP.

```

# flash\_init

flash: ファイルシステムを再初期化するには、ブートローダモードで **flash\_init** コマンドを使用します。

## flash\_init

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンドデフォルト

flash: ファイルシステムは、通常のシステム動作中に自動的に初期化されます。

### コマンドモード

ブートローダ

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

### 使用上のガイドライン

flash: ファイルシステムは、通常のブートプロセス中に自動的に初期化されます。

このコマンドは、**flash:** ファイルシステムを手動で初期化します。たとえば、パスワードを忘れた場合には、回復手順中にこのコマンドを使用します。

# help

利用可能なコマンドを表示するには、ブートローダモードで **help** コマンドを使用します。

## help

構文の説明	このコマンドには引数またはキーワードはありません。
コマンド デフォルト	デフォルトの動作や値はありません。
コマンド モード	ブートローダ

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 例

次に、利用可能なブートローダコマンドのリストを表示する例を示します。

```
Device:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

# install

ソフトウェア メンテナンス アップグレード (SMU) パッケージをインストールするには、特権 EXEC モードで **install** コマンドを使用します。

**install abort** | **activate** | **file bootflash:** | **flash:** | **harddisk:** | **webui:** [**auto-abort-timer timer timer prompt-level all | none**] | **add file bootflash:** | **flash:** | **ftp:** | **harddisk:** | **http:** | **https:** | **rcp:** | **scp:** | **ftftp:** | **webui:** [**activate [auto-abort-timer timer prompt-level all | none commit]**] | **commit** | **auto-abort-timer stop** | **deactivate file bootflash:** | **flash:** | **harddisk:** | **webui:** | **label id description description** | **label-name name** | **remove file bootflash:** | **flash:** | **harddisk:** | **webui:** | **inactive** | **rollback to base** | **committed** | **id install-ID** | **label label-name**

## 構文の説明

<b>abort</b>	現在のインストール操作を終了します。
<b>activate</b>	<p><b>install add</b> コマンドを通じて SMU が追加されているかどうかを検証します。</p> <p>このキーワードは、互換性チェックを実行し、パッケージステータスを更新します。パッケージを再起動できる場合はポストインストール スクリプトをトリガーして必要なプロセスを再起動するか、または再起動できないパッケージの場合はリロードをトリガーします。</p>
<b>file</b>	アクティブにするパッケージを指定します。
<b>{bootflash:   flash:   harddisk:   webui:}</b>	インストールしたパッケージのロケーションを指定します。
<b>auto-abort-timer timer</b>	(任意) 自動アボートタイマーをインストールします。
<b>prompt-level {all   none}</b>	<p>(任意) インストールアクティビティについてのプロンプトをユーザに表示します。</p> <p>たとえば、<b>activate</b> キーワードはリロードが必要なパッケージに対してリロードを自動的にトリガーします。パッケージをアクティブにする前に、続行するかどうかについてユーザに確認するプロンプトが表示されます。</p> <p><b>all</b> キーワードを使用するとプロンプトをイネーブルにすることができます。<b>none</b> キーワードはプロンプトをディセーブルにします。</p>

<b>add</b>	<p>ファイルをリモートロケーション（FTPまたはTFTP）からデバイスにコピーし、プラットフォームとイメージのバージョンのSMU互換性チェックを実行します。</p> <p>このキーワードは、指定したパッケージがプラットフォームで必ずサポートされるように基本の互換性チェックを実行します。</p>
<b>{ bootflash:   flash:   ftp:   harddisk:   http:   https:   rcp:   scp:   tftp:   webui: }</b>	追加するパッケージを指定します。
<b>commit</b>	<p>リロード後もSMUの変更が持続されるようにします。</p> <p>パッケージをアクティブにした後、システムがアップ状態にある間、または最初のリロード後にコミットを実行できます。パッケージがアクティブになっていてもコミットされていない場合は、最初のリロード後はアクティブの状態を保ちますが、2回目のリロード後はアクティブ状態を保ちません。</p>
<b>auto-abort-timer stop</b>	自動アボートタイマーを停止します。
<b>deactivate</b>	<p>インストールしたパッケージを非アクティブにします。</p> <p>(注) パッケージを非アクティブにすると、パッケージステータスも更新され、プロセスが再起動またはリロードされることがあります。</p>
<b>label <i>id</i></b>	ラベルを付けるインストールポイントのIDを指定します。
<b>description</b>	指定したインストールポイントに説明を追加します。
<b>label-name <i>name</i></b>	指定されたインストールポイントにラベル名を追加します。
<b>remove</b>	<p>インストールしたパッケージを削除します。</p> <p><b>remove</b> キーワードは、現在非アクティブ状態のパッケージでのみ使用できます。</p>
<b>inactive</b>	非アクティブ状態のすべてのパッケージをデバイスから削除します。

<b>rollback</b>	データモデルインターフェイス (DMI) パッケージ SMU をベースバージョン、最後にコミットされたバージョン、または既知のコミット ID にロールバックします。
<b>to base</b>	ベースイメージに戻します。
<b>committed</b>	最後のコミット操作が実行されたときのインストール状態に戻します。
<b>id install-ID</b>	特定のインストールポイントIDに戻します。有効な値は、1 ~ 4294967295 です。

**コマンド デフォルト** パッケージはインストールされません。

**コマンド モード** 特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが追加されました。

**使用上のガイドライン** SMUは、システムにインストールしてパッチ修正やセキュリティ解決をリリースされたイメージに提供ができるパッケージです。このパッケージには、パッケージの内容を記述するいくつかのメタデータとともに、リリースにパッチを適用するための最小限の一連のファイルが含まれています。

SMU をアクティブ化する前にパッケージを追加する必要があります。

パッケージは、フラッシュから削除する前に非アクティブにする必要があります。削除したパッケージは、もう一度追加する必要があります。

次に、インストールパッケージをデバイスに追加する例を示します。

```
Device# install add file
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin

install_add: START Mon Mar  5 21:48:51 PST 2018
install_add: Adding SMU

--- Starting initial file syncing ---
Info: Finished copying
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin to
the selected switch(es)
Finished initial file syncing

Executing pre scripts....

Executing pre scripts done.
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
  [1] SMU_ADD package(s) on switch 1
  [1] Finished SMU_ADD on switch 1
Checking status of SMU_ADD on [1]
```

```
SMU_ADD: Passed on [1]
Finished SMU Add operation

SUCCESS: install_add
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar 5 21:49:00 PST 2018
```

次に、インストールパッケージをアクティブにする例を示します。

```
Device# install activate file
flash:cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin

install_activate: START Mon Mar 5 21:49:22 PST 2018
install_activate: Activating SMU
Executing pre scripts....

Executing pre sripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
  [1] SMU_ACTIVATE package(s) on switch 1
  [1] Finished SMU_ACTIVATE on switch 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

SUCCESS: install_activate
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar 5 21:49:34 PST 2018
```

次に、インストールしたパッケージをコミットする例を示します。

```
Device# install commit

install_commit: START Mon Mar 5 21:50:52 PST 2018
install_commit: Committing SMU
Executing pre scripts....

Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
  [1] SMU_COMMIT package(s) on switch 1
  [1] Finished SMU_COMMIT on switch 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

SUCCESS: install_commit
/flash/cat9k_iosxe.BLD_SMU_20180302_085005_TWIG_LATEST_20180306_013805.3.SSA.smu.bin Mon
Mar 5 21:51:01 PST 2018
```

## 関連コマンド

コマンド	Description
<b>show install</b>	インストールパッケージに関する情報を表示します。



## ip ssh bulk-mode

セキュアシェル (SSH) バルクデータ転送モードをイネーブルにするには、グローバル コンフィギュレーションモードで **ip ssh bulk-mode** コマンドを使用します。このモードをディセーブルにするには、このコマンドの **no** 形式を使用します。

```
ip ssh bulk-mode [ window-size ]
no ip ssh bulk-mode [ window-size ]
```

構文の説明	<i>window-size</i> (任意) SSH ウィンドウサイズです。範囲は 131072 ~ 1073741824 です。デフォルトは 131072 です。						
コマンド デフォルト	SSH 一括モードが有効になっていません。						
コマンド モード	グローバル コンフィギュレーション (config)						
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Amsterdam 17.2.1</td> <td>このコマンドが導入されました。</td> </tr> <tr> <td>Cisco IOS XE Bengaluru 17.6.1</td> <td>このコマンドが変更されました。<i>window-size</i> 変数オプションが導入されました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。	Cisco IOS XE Bengaluru 17.6.1	このコマンドが変更されました。 <i>window-size</i> 変数オプションが導入されました。
リリース	変更内容						
Cisco IOS XE Amsterdam 17.2.1	このコマンドが導入されました。						
Cisco IOS XE Bengaluru 17.6.1	このコマンドが変更されました。 <i>window-size</i> 変数オプションが導入されました。						

**使用上のガイドライン** SSH 一括モードを使用すると、大量のデータ転送を伴うプロシージャのスループットパフォーマンスを最適化できます。一括モードの最適化を活用するために、セキュアコピー機能が強化されました。この操作は、他のファイル転送操作と比較して、CPU やメモリなどのシステムリソースをより多く消費するため、大きなファイルを転送するための **ip ssh bulk-mode** コマンドを有効にすることをお勧めします。システムリソースが大量にロードされている場合は、このコマンドを使用しないでください。必要なファイル転送が完了したら、このコマンドをディセーブルにします。



- (注)
- 一括データ転送モードは、時間ベースまたはボリュームベースの SSH キー再生成機能をサポートしていません。
  - 一括データ転送モードは、SSH バージョン 1 ではサポートされていません。

### 例

次に、SSH サーバで一括データ転送モードを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh bulk-mode
Device(config)# exit
```

## 関連コマンド

コマンド	Description
<b>ip ssh window-size</b>	Secure Copy Protocol のウィンドウサイズを変更します。

## l2 traceroute

レイヤ2 トレースルートサーバを有効にするには、グローバル コンフィギュレーション モードで **l2 traceroute** コマンドを使用します。レイヤ2 トレースルートサーバを無効にするには、このコマンドの **no** 形式を使用します。

**l2 traceroute**  
**no l2 traceroute**

---

**構文の説明**

このコマンドには引数またはキーワードはありません。

---

**コマンドモード**

グローバル コンフィギュレーション (config#)

---

**コマンド履歴**

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが追加されました。

---

**使用上のガイドライン**

レイヤ2 トレースルートはデフォルトでは有効になっており、ユーザ データグラム プロトコル (UDP) ポート 2228 でリスニングソケットが開きます。UDP ポート 2228 を閉じてレイヤ2 トレースルートが無効にするには、グローバルコンフィギュレーションモードで **no l2 traceroute** コマンドを使用します。

次に、**l2 traceroute** コマンドを使用してレイヤ2 トレースルートを設定する例を示します。

```
Device# configure terminal  
Device(config)# l2 traceroute
```

# license air level

Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチに接続されているワイヤレスコントローラで AIR ライセンスを設定するには、グローバル コンフィギュレーション モードで **license air level** コマンドを入力します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**license air level air-network-advantage [ addon air-dna-advantage ] | air-network-essentials [ addon air-dna-essentials ]**

**no license air level**

## 構文の説明

**air-network-advantage** AIR Network Advantage ライセンスレベルを設定します。

**addon air-dna-advantage** (任意) アドオンの AIR DNA の Advantage ライセンスレベルを設定します。

このアドオンオプションは AIR Network Advantage ライセンスで使用できる、デフォルトのライセンスです。

**air-network-essentials** AIR Network Essential ライセンスレベルを設定します。

**addon air-dna-essentials** (任意) アドオンの AIR DNA の Essential ライセンスレベルを設定します。

このアドオンオプションは AIR Network Essential ライセンスで使用できます。

## コマンド デフォルト

AIR DNA Advantage がデフォルトのライセンスです

## コマンド モード

グローバル コンフィギュレーション (Device(config)#)

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、このリリースで導入されるポリシーを使用したスマートライセンスで、引き続き使用および適用することができます。詳細については、「使用上のガイドライン」セクションを参照してください。

## 使用上のガイドライン

ポリシーを使用したスマートライセンスの環境では、**license air level** コマンドを使用して、製品インスタンスで使用されているライセンスレベルを変更したり、製品インスタンスでアドオンライセンスを追加設定したりすることができます。変更はリロード後に有効になります。

設定できるライセンスは次のとおりです。

- AIR Network Essential

- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

DNA ライセンスを更新しない場合は、AIR DNA Essential または AIR DNA Advantage ライセンスレベルを設定し、期限切れになった時点で Network Advantage または Network Essentials のライセンスレベルに移行することができます。

接続しているすべてのアクセスポイントにおいて、コントローラの一意的な値プロパティを利用するために、Cisco DNA Center ライセンスが必要です。

詳細については、「[Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide](#)」を参照してください。

## 例

次に、AIR DNA Essential ライセンスレベルを設定する例を示します。

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

次に、AIR DNA Advantage ライセンスレベルを設定する例を示します。

```
Device# configure terminal
Device(config)# license air level air-network-advantage addon air-dna-advantage
```

# license boot level

デバイスで新しいソフトウェアライセンスを起動するには、グローバルコンフィギュレーションモードで **license boot level** コマンドを使用します。すべてのソフトウェアライセンスをデバイスから削除するには、このコマンドの **no** 形式を使用します。

**license boot level network-advantage [ addon dna-advantage ] | network-essentials [ addon dna-essentials ]**

**no license boot level**

## 構文の説明

**network-advantage [ addon dna-advantage ]** Network Advantage ライセンスを設定します。オプションで、デジタルネットワークアーキテクチャ (DNA) Advantage ライセンスを設定することもできます。

**network-essentials [ addon dna-essentials ]** Network Essential ライセンスを設定します。オプションで、デジタルネットワークアーキテクチャ (DNA) Essential ライセンスを設定することもできます。

## コマンド デフォルト

Network Essentials

## コマンド モード

グローバル コンフィギュレーション (config)

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、このリリースで導入されるポリシーを使用したスマートライセンスで、引き続き使用および適用することができます。詳細については、「使用上のガイドライン」セクションを参照してください。

## 使用上のガイドライン

Cisco Catalyst 9000 シリーズ スイッチで使用可能なソフトウェア機能は、次のように、基本またはアドオンのライセンスレベルに分類されます。

基本ライセンス :

- Network Advantage : Network Essentials ライセンスで使用可能な機能と追加機能が含まれます。

アドオンライセンス :

- DNA Advantage : Network Essentials ライセンスで使用可能な機能と追加機能が含まれます。

基本ライセンスは永続的または永久に効力を持つライセンスです。

アドオンライセンスはサブスクリプションまたは期間ライセンスであり、3年、5年、または7年の期間にわたって購入できます。基本ライセンスは、アドオンライセンスの前提条件です。詳細については、リリース ノートを参照してください。

以下のセクションでは、以前のスマートライセンス環境およびポリシーを使用したスマートライセンス環境での **license boot level** コマンドの使用について説明します。

**スマートライセンス**：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、スマートライセンスはデフォルトで有効になっており、次の目的で **license boot level** コマンドを使用できます。

- ライセンスのダウングレードとアップグレード
- 評価ライセンスと拡張ライセンスの有効化と無効化
- アップグレードライセンスのクリア

このコマンドは、特定のモジュールのライセンスインフラストラクチャで保持されているライセンス階層ではなく、設定されたライセンスレベルで起動するようにライセンスインフラストラクチャを設定します。

- スイッチをリロードすると、ライセンスインフラストラクチャでスタートアップコンフィギュレーションの設定にライセンスがあるかどうかを確認されます。設定にライセンスがある場合、そのライセンスでスイッチが起動します。ライセンスがない場合、ライセンスインフラストラクチャでイメージ階層に従ってライセンスが確認されます。
- 強制ブート評価ライセンスが期限切れの場合、ライセンスインフラストラクチャで通常の階層に従ってライセンスが確認されます。
- 設定されたブートライセンスがすでに期限切れになっている場合、ライセンスインフラストラクチャで階層に従ってライセンスが確認されます。

**ポリシーを使用したスマートライセンス**：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、ポリシーを使用したスマートライセンスはデフォルトで有効になっており、次の目的で **license boot level** コマンドを使用できます。

- 製品インスタンスで使用されている基本またはアドオンのライセンスレベルを変更します。  
たとえば、Network Essentials を使用していて、次のリロードで Network Advantage を使用する場合や、DNA Advantage を使用して次のリロードで DNA Essentials を使用する場合があります。
- 製品インスタンスで使用されているアドオンのライセンスレベルを追加または削除します。  
たとえば、Network Essentials のみを使用していて、次のリロードで DNA Essentials を使用する場合、または DNA Advantage を使用しており、次のリロード後にアドオンを使用しない場合があります。

評価ライセンスまたは期限切れライセンスの概念は、ポリシーを使用したスマートライセンスには存在しません。

コマンドを設定すると、設定したライセンスは次のリロード後に有効になります。ライセンスの使用状況は引き続きデバイスに記録され、この変更されたライセンス設定情報は、次のリソース使用率測定レポート（RUM レポート）を介して CSSM に送信する必要があります。レポートの要件と頻度は、適用されるポリシーによって決まります。**show license status** コマンド出力の「使用状況レポート」の項を参照してください。ポリシーを使用したスマートライセンスの詳細については、必要なリリースのソフトウェア設定ガイドで、「*System Management*」 > 「*Smart Licensing Using Policy*」を参照してください。

## 例

次に、次回のリロード時に Network Essentials ライセンスを設定する例を示します。

```
Device# configure terminal
Device(config)# license boot level network-essentials
Device(config)# exit
Device# copy running-config startup-config
Device# reload
```

次に、次回のリロード時に DNA Essentials ライセンスを設定する例を示します。

```
Device# configure terminal
Device(config)# license boot level network-essentials add-on dna-essentials
Device(config)# exit
Device# copy running-config startup-config
Device# reload
```



## license smart (グローバル コンフィギュレーション)

製品インスタンスが Cisco Smart Software Manager (CSSM) や Cisco Smart Licensing Utility (CSLU)、または Smart Software Manager オンプレミス (SSM オンプレミス) との通信に使用するトランスポートモードや URL などのライセンス関連の設定を行い、使用状況レポートの間隔を設定し、ライセンス使用状況レポート (RUM レポート) に含めるか、または除外する必要がある情報を設定するには、グローバルコンフィギュレーションモードで **license smart** コマンドを入力します。デフォルト値に戻すには、コマンドの **no** 形式を使用します。

```
license smart custom_id ID | enable | privacy all | hostname | version | proxy address
address_hostname | port port | reservation | server-identity-check | transport automatic | callhome
| cslu | off | smart | url url | cslu cslu_or_on-prem_url | default | smart smart_url | utility
secondary_url | usage customer-tags tag1 | tag2 | tag3 | tag4 tag_value | interval interval_in_days
| utility [ customer_info city city | country country | postalcode postalcode | state state | street
street ]
```

```
no license smart custom_id | enable | privacy all | hostname | version | proxy address
address_hostname | port port | reservation | server-identity-check | transport | url url | cslu
cslu_or_on-prem_url | default | smart smart_url | utility secondary_url | usage customer-tags tag1
| tag2 | tag3 | tag4 tag_value | interval interval_in_days | utility [ customer_info city city | country
country | postalcode postalcode | state state | street street ]
```

### 構文の説明

<b>custom_id ID</b>	このオプションは CLI では使用できませんがサポートされていません。
<b>enable</b>	このキーワードは CLI には表示されますが、設定しても効果はありません。スマートライセンスは常に有効になっています。

**privacy all | hostname | version**

製品インスタンスによって生成された RUM レポートから特定の情報を除外できます。

すべてのデータプライバシー設定はデフォルトで無効になっています。

RUM レポートから除外するオプションを設定します。

- **all** : すべての通信で最小限のライセンス情報のみを送信します。
- **hostname** : 通信からホスト名を除外します。
- **version** : 製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンを除外します。

上記のオプションのいずれかでコマンドの **no** 形式を入力すると、そのオプションのプライバシーが無効になり、対応する情報が RUM レポートに含まれます。

データプライバシーが有効かどうかに関係なく、製品 ID (PID) とシリアル番号が RUM レポートに含まれます。

**proxy address address\_hostname | port port**

CSLU または CSSM とライセンス使用状況を同期するためにプロキシを設定します。つまり、トランスポートモードが **license smart transport smart** (CSSM) または **license smart transport cslu** (CSLU) の場合にのみ、このオプションを使用してプロキシを設定できます。

ただし、トランスポートモードとして **license smart transport cslu** も使用する SSM オンプレミス展開では、ライセンス使用状況の同期にプロキシは設定できません。

次のオプションを設定します。

- **address address\_hostname** : プロキシアドレスを設定します。

*address\_hostname* には、プロキシの IP アドレスまたはホスト名を入力します。

- **port port** : プロキシポートを設定します。

*port* には、プロキシポート番号を入力します。

---

<b>reservation</b>	ライセンス予約機能を有効または無効にします。  (注) このオプションは、CLI で使用できますが、ライセンスの予約が適用されないため、ポリシーを使用したスマートライセンシングの環境では適用されません。
<b>server-identity-check</b>	HTTP セキュアサーバの ID チェックを有効または無効にします。
<b>transport automatic   callhome   cslu   off   smart</b>	製品インスタンスが CSSM との通信に使用する転送モードを設定します。次のオプションから選択します。 <ul style="list-style-type: none"><li>• <b>automatic</b> : 転送モード <b>cslu</b> を設定します。</li><li>• <b>callhome</b> : 転送モードとして Call Home を有効にします。</li><li>• <b>cslu</b> : 転送モードとして CSLU を有効にします。これがデフォルトの転送モードです。 CSLU と SSM オンプレミスの両方に同じキーワードが適用されますが、URL が異なります。次の行の <b>cslu</b><i>cslu_or_on-prem_url</i> を参照してください。</li><li>• <b>off</b> : 製品インスタンスからのすべての通信を無効にします。</li><li>• <b>smart</b> : スマート転送を有効にします。</li></ul>

---

---

**url** *url* | **cslu** *cslu\_url* | **default** | **smart**  
*smart\_url* | **utility** *secondary\_url*

---

設定された転送モードの URL を設定します。次のオプションから選択します。

- **url** : 転送モードとして **callhome** を設定している場合は、このオプションを設定します。  
CSSM URL を次のように正確に入力します。

`https://software.cisco.com/#module/SmartLicensing`

**no license smart url url** コマンドは、デフォルトの URL に戻ります。

- **cslu cslu\_or\_on-prem\_url** : トランスポートモードを **cslu** として設定している場合は、必要に応じて CSLU または SSM オンプレミスの URL を使用してこのオプションを設定します。

- CSLU を使用している場合は、次のように URL を入力します。

`http://<cslu_ip_or_host>:8182/cslu/v1/pi`

<cslu\_ip\_or\_host> には、CSLU をインストールした Windows ホストのホスト名や IP アドレスを入力します。8182 はポート番号であり、CSLU が使用する唯一のポート番号です。

**no license smart url cslu cslu\_or\_on-prem\_url** コマンドは

`http://cslu-local:8182/cslu/v1/pi` に戻ります。

- SSM オンプレミスを使用している場合は、次のように URL を入力します。

`http://<ip>/cslu/v1/pi/<tenant ID>`

<ip> には、SSM オンプレミスをインストールしたサーバのホスト名または IP アドレスを入力します。<tenantID> はデフォルトのローカルバーチャルアカウント ID にする必要があります。

**ヒント** SSM オンプレミスから URL 全体を取得できます。該当するリリース (17.3.x 以降) のソフトウェア コンフィギュレーション ガイドで、「System Management」> 「Smart Licensing Using Policy」> 「Task Library for Smart Licensing Using Policy」> 「Retrieving the

Transport URL (SSM On-Prem UI)」を参照してください。

**no license smart url cslu cslu\_or\_on-prem\_url**  
コマンドは

<http://cslu-local:8182/cslu/v1/pi> に戻ります。

- **default** : 設定されている転送モードによって異なります。このオプションでは、**smart** および **cslu** 転送モードのみがサポートされます。

転送モードが **cslu** に設定されている場合、**license smart url default** を設定すると、CSLU URL は自動的に設定されます

(<https://cslu-local:8182/cslu/v1/pi>)。

転送モードが **smart** に設定されている場合、**license smart url default** を設定すると、スマート URL は自動的に設定されます

(<https://smartreceiver.cisco.com/licservice/license>)。

- **smart smart\_url** : 転送タイプとして **smart** を設定している場合は、このオプションを設定します。URL を次のように正確に入力します。

<https://smartreceiver.cisco.com/licservice/license>

このオプションを設定すると、システムは **license smart url url** で自動的に URL の複製を作成します。重複するエントリは無視できません。これ以上の操作は必要ありません。

**no license smart url smartsmart\_url** コマンドは、デフォルトの URL に戻ります。

- **utility smart\_url** : このオプションは CLI では使用できませんがサポートされていません。

**usage** **customer-tags** **tag1** | **tag2** | **tag3** | **tag4** *tag\_value* | **interval** *interval\_in\_days* | 使用状況レポートの設定を構成します。次のオプションを設定できます。

- **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag\_value* : テレメトリ用のデータモデルに含める文字列を定義します。最大4つの文字列 (またはタグ) を定義できます。

*tag\_value* には、定義する各タグの文字列値を入力します。

- **interval** *interval\_in\_days* : レポート間隔の日数を設定します。デフォルトでは、RUM レポートは 30 日ごとに送信されます。有効な値の範囲は 1 ~ 3650 です。

この値をゼロに設定すると、適用されるポリシーの指定内容に関係なく、RUM レポートは送信されません。これは、CSLU または CSSM が受信側にある可能性があるトポロジに適用されます。

ゼロより大きい値を設定し、通信タイプが**オフ**に設定されている場合、*interval\_in\_days* と Ongoing reporting frequency(days) : のポリシー値の間で、値の小さい方が適用されます。たとえば、*interval\_in\_days* が 100 に設定され、ポリシーの値が Ongoing reporting frequency (days) : 90 の場合、RUM レポートは 90 日ごとに送信されます。

間隔を設定せず、デフォルトが有効な場合、レポート間隔は完全にポリシー値によって決定されます。たとえば、デフォルト値が有効で、不適用ライセンスのみが使用されている場合、ポリシーでレポートが不要と記述されていると、RUM レポートは送信されません。

**utility** [ **customer\_info** *city* *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* ] このオプションは CLI には表示されますが、サポートされていません。

#### コマンド デフォルト

Cisco IOS XE Amsterdam 17.3.1 以前 : スマートライセンスがデフォルトで有効になっていません。

Cisco IOS XE Amsterdam 17.3.2a 以降 : ポリシーを使用したスマートライセンシングはデフォルトで有効になっています。

コマンドモード	Global config (Device(config)#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.2a	<p>ポリシーを使用したスマートライセンスで、次のキーワードと変数が導入されました。</p> <ul style="list-style-type: none"> <li>• <b>url</b> キーワードの下に、次のオプションが導入されました。 <b>cslu cslu_url   smart smart_url</b></li> <li>• <b>transport</b> キーワードの下に、次のオプションが導入されました。 <b>cslu   off</b></li> </ul> <p>さらに、デフォルトの通信タイプが <b>callhome</b> から <b>cslu</b> に変更されました。</p> <ul style="list-style-type: none"> <li>• <b>usage customer-tags tag1   tag2   tag3   tag4 tag_value   interval interval_in_days</b></li> </ul> <p><b>license smart global</b> コマンドの次のキーワードと変数は廃止され、CLI では使用できなくなりました：<b>enable</b>、<b>conversion automatic</b>。</p>
	Cisco IOS XE Amsterdam 17.3.3	<p>SSM オンプレミスサポートが導入されました。SSM オンプレミス展開での製品インスタンス開始型通信の場合、既存の <b>[no ]license smart url cslucaclu_or_on-prem_url</b> コマンドは SSM オンプレミスの URL の設定もサポートします。ただし、SSM オンプレミスに必要な URL 形式は <code>http://&lt;ip&gt;/cslu/v1/pi/&lt;tenant ID&gt;</code> です。</p> <p>設定する必要がある対応するトランスポートモードも、既存のコマンド (<b>license smart transport cslu</b>) です。</p>
	Cisco IOS XE Cupertino 17.7.1	<p>バージョンプライバシーが無効になっている場合 (<b>no license smart privacy version</b> グローバル コンフィギュレーション コマンド)、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンが RUM レポートに含まれます。</p> <p>RUM レポートからバージョン情報を除外するには、バージョンプライバシーを有効にする必要があります (<b>license smart privacy version</b>)。</p>

## 使用上のガイドライン 通信障害とレポート

設定したレポート間隔 (**license smart usage interval interval\_in\_days** コマンド) によって、製品インスタンスが RUM レポートを送信する日時が決まります。スケジュールされた間隔が通信障害と一致する場合、製品インスタンスは、スケジュールされた時間が経過した後、最大 4 時間 RUM レポートの送信を試みます。(通信障害が続くために) それでもレポートを送信で



きない場合、システムは間隔を 15 分にリセットします。通信障害が解消されると、レポート間隔はユーザが最後に設定した値に戻ります。

通信障害の場合に表示される可能性があるシステムメッセージ

は、%SMART\_LIC-3-COMM\_FAILED です。このエラーを解決し、レポート間隔の値を復元する方法については、該当するリリース (17.3.x 以降) のソフトウェア設定ガイドで、「*System Management*」 > 「*Smart Licensing Using Policy*」 > 「*Troubleshooting Smart Licensing Using Policy*」を参照してください。

### プロキシサーバーの受け入れ

**license smart proxy {address address\_hostname | portport}** コマンドを設定するとき、Cisco IOS XE Bengaluru 17.6.1 以降、プロキシサーバーの受け入れ基準が変更されたことに注意してください。プロキシサーバーの応答のステータスコードのみがシステムによって検証され、理由フレーズは検証されません。RFC 形式は、status-line = HTTP-version SP status-code SP reason-phrase CRLF で、ステータスコードは 3 桁の数値コードになります。ステータス行の詳細については、[RFC 7230](#) の [セクション 3.1.2](#) を参照してください。

- [データプライバシーの例 \(49 ページ\)](#)
- [転送タイプと URL の例 \(50 ページ\)](#)
- [使用状況レポートのオプションの例 \(51 ページ\)](#)

### データプライバシーの例

次に、グローバル コンフィギュレーションモードで **license smart privacy** コマンドを使用してデータプライバシー関連情報を設定する例を示します。**show license status** 出力には、設定された情報が表示されます。

プライベート情報は送信されません。

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# license smart transport callhome
Device(config)# license smart url
https://tools.cisco.com/its/service/oddce/services/DDCEService
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
  Callhome hostname privacy: ENABLED
  Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

ホスト名が除外され、バージョン情報が RUM レポートに含まれます。

次の出力は、製品インスタンスで実行されているソフトウェアバージョンが Cisco IOS XE Cupertino 17.7.1 である製品インスタンスからのものです。バージョンプライバシーが無効に

なっているため、製品インスタンスで実行されている Cisco IOS-XE ソフトウェアバージョンとスマートエージェントのバージョンが RUM レポートに含まれます。

```
Device# configure terminal
Device(config)# license smart privacy hostname
Device(config)# no license smart privacy version
Device(config)# exit

Device# show license all
<output truncated>

Data Privacy:
  Sending Hostname: no
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

<output truncated>
```

### 転送タイプと URL の例

次に、グローバル コンフィギュレーション モードで **license smart transport** および **license smart url** コマンドを使用して、転送タイプの一部を設定する例を示します。**show license all** 出力には、設定された情報が表示されます。

トランスポート : **cslu** :

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
<output truncated>

Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>
```

トランスポート : **smart** :

```
Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>

Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
<output truncated>
```

### 使用状況レポートのオプションの例

次に、グローバルコンフィギュレーションモードで **license smart usage** コマンドを使用して、使用状況レポートの一部を設定する例を示します。 **show running-config** 出力には、設定された情報が表示されます。

#### customer-tag オプションの設定 :

```
Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01
```

#### 現在適用されているポリシーよりも絞り込んだレポート間隔の設定 :

```
Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

```
Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>
```

```
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

## license smart (特権 EXEC)

承認コードの要求または返却、リソース使用状況測定レポート (RUM レポート) の保存、製品インスタンスへのファイルのインポート、Cisco Smart Software Manager (CSSM) との信頼の確立、CSSM または Cisco Smart License Utility (CSLU)、あるいは Smart Software Manager オンプレミス (SSM オンプレミス) との製品インスタンスの同期、製品インスタンスからのライセンス情報の削除などのライセンス機能を設定するには、対応するキーワードまたは引数を指定して特権 EXEC モードで **license smart** コマンドを入力します。

**license smart authorization request add | replace | save path feature\_name all | local | return all | local offline [ path ] | online | clear eventlog | export return all | local feature\_name | factory reset | import file\_path | save trust-request filepath\_filename | usage all | days days | rum-id rum-ID | unreported file file\_path | sync all | local | trust idtoken id\_token\_value local | all [ force ]**

### 構文の説明

<b>smart</b>	スマートライセンスのオプションを提供します。
<b>authorization</b>	承認コードを要求する、または承認コードを返すオプションを提供します。  認証コードは、輸出規制または輸出規制の適用タイプのライセンスを使用する場合にのみ必要です。
<b>request</b>	承認コードを CSSM、CSLU (CSLU は CSSM から承認コードを取得)、または SSM オンプレミスから要求し、そのコードを製品インスタンスにインストールします。
<b>add</b>	要求されたライセンスを既存の承認コードに追加します。新しい承認コードには、既存の承認コードのすべてのライセンスと要求されたライセンスが含まれます。
<b>replace</b>	既存の承認コードを置き換えます。新しい承認コードには、要求されたライセンスのみが含まれます。現在の承認コードのすべてのライセンスが返されます。  このオプションを入力すると、製品インスタンスは、削除される承認コードに対応するライセンスが使用中であるかどうかを確認します。ライセンスが使用されている場合は、対応する機能を最初に無効にするようにエラーメッセージが表示されます。
<b>save filepath_filename</b>	承認コード要求をファイルに保存します。  <i>filepath_filename</i> には、ファイルの絶対パス (ファイル名を含む) を指定します。
<b>feature_name</b>	承認コードを要求するライセンスの名前。
<b>all</b>	高可用性セットアップまたはスタック構成セットアップで、すべての製品インスタンスに対してアクションを実行します。

<b>local</b>	アクティブな製品インスタンスに対してアクションを実行します。これがデフォルトのオプションです。
<b>return</b>	CSSM のライセンスプールに承認コードを返します。
<b>offline</b> <i>filepath_filename</i>	<p>製品インスタンスが CSSM に接続されていないことを意味します。承認コードはオフラインで返されます。このオプションでは、戻りコードをファイルに出力する必要があります。</p> <p>ファイルを保存するパスを指定することもできます。ファイル形式は、.txt などの読み取り可能な任意の形式にすることができます。</p> <p>オフラインオプションを選択する場合は、CLI や保存したファイルから戻りコードをコピーして CSSM に入力する、という追加の手順を実行する必要があります。</p>
<b>online</b>	製品インスタンスが接続モードであることを意味します。承認コードは、CSLU や CSSM に直接返されます。
<b>clear eventlog</b>	製品インスタンスからすべてのイベントログファイルをクリアします。
<b>export return</b>	このコマンドは、CLI で表示されますが、ポリシーを使用したスマートライセンスングの環境では適用されません。代わりに <b>license smart authorization return</b> 特権 EXEC コマンドを使用して承認コードを返します。
<b>factory reset</b>	製品インスタンスから保存されているすべてのライセンス情報をクリアします。
<b>import</b> <i>filepath_filename</i>	<p>製品インスタンスにファイルをインポートします。ファイルは、承認コード、信頼コード、またはポリシーのファイルである場合があります。</p> <p><i>filepath_filename</i> には、場所（ファイル名を含む）を指定します。</p>
<b>save</b>	RUM レポートや信頼コード要求を保存するオプションを提供します。
<b>trust-request</b> <i>filepath_filename</i>	<p>アクティブな製品インスタンスの信頼コード要求を指定した場所に保存します。</p> <p><i>filepath_filename</i> には、ファイルの絶対パス（ファイル名を含む）を指定します。</p>

<b>usage all   days</b> <i>days</i>   <b>rum-id</b> <i>rum-ID</i>   <b>unreported file</b> <i>file_path</i>	<p>RUM レポート (ライセンス使用状況情報) を指定した場所に保存します。次のいずれかのオプションを指定する必要があります。</p> <ul style="list-style-type: none"> <li>• <b>all</b> : すべての RUM レポートを保存します。</li> <li>• <b>days days</b> : 過去 <i>n</i> 日間 (現在の日を除く) の RUM レポートを保存します。番号を入力します。有効範囲は 0 ~ 4294967295 です。 たとえば、3 と入力すると、過去 3 日間の RUM レポートが保存されます。</li> <li>• <b>rum-Id rum-ID</b> : 指定した RUM ID を保存します。値の有効な範囲は 0 ~ 18446744073709551615 です。</li> <li>• <b>unreported</b> : すべての未報告の RUM レポートを保存します。</li> </ul> <p><b>file filepath_filename</b> : 指定した使用状況情報をファイルに保存します。ファイルの絶対パス (ファイル名を含む) を指定します。</p>
<b>sync all   local</b>	<p>CSSM または CSLU、あるいは SSM オンプレミスと同期して、保留中のデータを送受信します。これには、保留中の RUM レポートのアップロード、ACK 応答のダウンロード、および製品インスタンスの保留中の承認コード、信頼コード、ポリシーが含まれます。</p> <p>次のいずれかのオプションを入力して、製品インスタンスを指定します。</p> <ul style="list-style-type: none"> <li>• <b>all</b> : 高可用性セットアップまたはスタック構成セットアップで、すべての製品インスタンスに対して同期を実行します。このオプションを選択すると、製品インスタンスは同期要求内にあるすべての UDI のリストも送信します。</li> <li>• <b>local</b> : 要求を送信するアクティブな製品インスタンス、つまり自身の UDI に対してのみ同期を実行します。これがデフォルトのオプションです。</li> </ul>
<b>trust idtoken</b> <i>id_token_value</i>	<p>CSSM との信頼できる接続を確立します。</p> <p>このオプションを使用するには、最初に CSSM ポータルでトークンを生成する必要があります。<i>id_token_value</i> に生成されたトークン値を指定します。</p>
<b>force</b>	<p>信頼コードが製品インスタンスにすでに存在する場合でも、信頼コード要求を送信します。</p> <p>信頼コードは、製品インスタンスの UDI にノードロックされます。UDI がすでに登録されている場合、CSSM は同じ UDI の新規登録を許可しません。 <b>force</b> キーワードを入力すると、この動作が上書きされます。</p>

#### コマンド デフォルト

Cisco IOS XE Amsterdam 17.3.1 以前 : スマートライセンスがデフォルトで有効になっていません。

Cisco IOS XE Amsterdam 17.3.2a 以降：ポリシーを使用したスマートライセンスはデフォルトで有効になっています。

コマンドモード	特権 EXEC (Device#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.2a	<p>ポリシーを使用したスマートライセンスで、次のキーワードと変数が導入されました。</p> <ul style="list-style-type: none"> <li>• <b>authorization request add   replace <i>feature_name</i> all   local   return all   local offline [ <i>path</i> ]   online</b></li> <li>• <b>import <i>file_path</i></b></li> <li>• <b>save trust-request <i>filepath_filename</i>   usage all   days <i>days</i>   rum-id <i>rum-ID</i>   unreported file <i>file_path</i></b></li> <li>• <b>sync all   local</b></li> <li>• <b>trust idtoken <i>id_token_value</i> local   all [ force ]</b></li> </ul> <p><b>license smart</b> コマンドの次のキーワードと変数は廃止され、CLI では使用できなくなりました。</p> <ul style="list-style-type: none"> <li>• <b>register idtoken <i>token_id</i> [ force ]</b></li> <li>• <b>deregister</b></li> <li>• <b>renew id ID   auth</b></li> <li>• <b>debug error   debug   trace   all</b></li> <li>• <b>mfg reservation request   install   install file   cancel</b></li> <li>• <b>conversion start   stop</b></li> </ul>
	Cisco IOS XE Amsterdam 17.3.3	SSM オンプレミスのサポートが導入されました。リソース使用状況測定レポート (RUM レポート) の保存、製品インスタンスへのファイルのインポート、製品インスタンスの同期、認証コードの返却、SSM オンプレミス展開での製品インスタンスからのライセンス情報の削除など、ライセンス関連のタスクを実行できます。
	Cisco IOS XE Bengaluru 17.6.2	Export Control Key for High Security (HSECK9) のサポートが Cisco Catalyst 9300X シリーズスイッチに導入されました。承認コード関連のコマンド ( <b>license smart authorization request</b> および <b>license smart authorization return</b> ) は、サポートされているプラットフォームで、HSECK9 キーのスマートライセンス承認コード (SLAC) を要求して返すために使用できます。

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	<p>このリリースでは、次の機能拡張が導入されています。</p> <ul style="list-style-type: none"> <li>• <b>save path</b> キーワードと変数が <b>license smart authorization request</b> コマンド文字列に追加されました。このオプションを使用して、SLAC 要求を生成し、ファイルに保存できます。新しいオプションは次のように表示されます。</li> </ul> <pre>license smart authorization request add   replace   save path feature_name all   local request_count</pre> <ul style="list-style-type: none"> <li>• 既存の <b>license smart save usage</b> コマンドは、信頼コード要求がまだ存在しない場合に自動的に含めるように拡張されました。</li> </ul>

## 使用上のガイドライン エアーギャップネットワークでの信頼コードの要求

Cisco IOS XE Cupertino 17.7.1 以降、製品インスタンスで信頼コードが使用できない場合、**license smart save usage** コマンドを入力すると、製品インスタンスは自動的に RUM レポートに信頼コード要求を含めます。これは、スタンドアロンセットアップ、高可用性セットアップおよびスタック構成セットアップでサポートされます。高可用性セットアップおよびスタック構成セットアップでは、アクティブな製品インスタンスが、信頼コードが欠落しているすべてのメンバーまたはスタンバイの信頼コードを要求し、インストールします。CSSM の ACK には信頼コードが含まれており、CSSM Web UI からダウンロードできます。そして ACK を製品インスタンスにインストールする必要があります。信頼コードのインストールを確認するには、特権 EXEC モードで **show license status** コマンドを入力します。[Trust Code Installed] フィールドで更新されたタイムスタンプを確認します。

### 信頼コードの上書き

**license smart trust idtoken** コマンドを設定するときの **force** オプションの使用例：

- 1 つのバーチャルアカウントに属するすべての製品インスタンスに同じトークンを使用します。製品インスタンスが 1 つのアカウントから別のアカウントに移動した場合（たとえば、別のバーチャルアカウントの一部である高可用性設定に追加されたため）、既存の信頼コードを上書きすることが必要になる場合があります。
- 製品インスタンスに工場出荷時にすでにインストールされている信頼コードがありますが、製品インスタンスが CSSM に直接接続されているトポロジを実装する必要があります。工場出荷時にインストールされている信頼コードは、CSSM とのセキュア通信には使用できません。CSSM Web UI で ID トークンを生成し、信頼コードファイルをダウンロードする必要があります。この新しい信頼コードをインストールする場合は、工場出荷時にインストールされている既存の信頼コードを上書きする必要があります。

### ライセンス情報の削除

**license smart factory reset** コマンドを入力すると、承認コード、RUM レポートなど、すべてのライセンス情報（使用中のライセンスを除く）が製品インスタンスから削除されます。そのため、このコマンドは、製品インスタンスを返却する場合（Return Material Authorization



(RMA) )、または永続的にデコミットする場合にのみ使用することを推奨します。また、製品インスタンスからライセンス情報を削除する前に、承認コードを返却し CSSM に RUM レポートを送信することをお勧めします。これは、CSSM に最新の使用状況情報が含まれていることを確認するためです。

#### 承認コードの要求と返却：

- SLAC の要求と返却 - 製品インスタンスが CSSM、CSLU、または SSM オンプレミスに接続されている場合：
  - サポートされている製品インスタンスで SLAC を要求するには、次のコマンドを使用します。スタック構成セットアップでは、アクティブ (**local**) またはスタック全体 (**all**) のいずれかに SLAC を要求できます。1 つのメンバーまたはスタンバイに対してのみ SLAC を要求することはできません。ここでは、製品インスタンスは CSSM、CSLU または SSM オンプレミスに接続されています。エアギャップネットワークの場合、生成された SLAC に必要な詳細を CSSM に直接入力する必要があります。

**license smart authorization request add | replace *feature\_name* all | local**

- 次のコマンドを使用して、SLAC または SLR 承認コードを返します。

**license smart authorization return all | local online**

- 製品インスタンスがエアギャップネットワークにある場合に、SLAC を要求して返します。
  - Cisco IOS XE Cupertino 17.7.1 以降  
必要な PID を入力したり、CSSM Web UI で SLAC を生成したりせずに、SLAC を要求してインストールできます。代わりに、**license smart authorization request {add | replace} *feature\_name* {all | local}** に続けて **license smart authorization request save [path]** コマンドを設定して、SLAC 要求をファイルに保存します。  
SLAC 要求ファイルを CSSM Web UI (RUM レポートと同じ場所) にアップロードします。要求が処理されると、CSAC Web UI で SLAC ファイルを使用できるようになります。SLAC ファイルをダウンロードし、製品インスタンスにインポートします。  
同様に、SLAC を返すには、**offline [path]** オプションを指定して **license smart authorization return** コマンドを設定し、ファイルを保存します。ファイルを CSSM Web UI (RUM レポートと同じ場所) にアップロードします。
  - Cisco IOS XE Cupertino 17.7.1 より前：  
エアギャップネットワークの製品インスタンスで SLAC を要求するには、CSSM Web UI に必要な詳細を直接入力して、SLAC を生成する必要があります。  
SLAC または SLR 承認コードを返すには、次を実行します。

**license smart authorization return all | local offline [ path ] | online**

CLIに表示される戻りコードをコピーし、CSSMに入力します。戻りコードをファイルに保存する場合は、ファイルからコードをコピーし、CSSMに同じコードを入力できます。

ポリシーを使用したスマートライセンスの環境のSLR承認コードの場合、「予約」の概念が適用されないため、ポリシーを使用したスマートライセンスの環境で新しいSLRを要求できないことに注意してください。完全に外部との接続性がないネットワーク内にいる場合は、代わりにCSSMへの接続なし、CSLUなしのトポロジが適用されます。

### SSM オンプレミス展開の承認コード

SSM オンプレミス展開でSLACを要求する場合は、**license smart authorization request** コマンドを設定する前に、次の前提条件を満たしていることを確認してください。

- 製品インスタンスをSSM オンプレミスに追加する必要があります。追加のプロセスで、製品インスタンスを検証してCSSMの該当するスマートアカウントとバーチャルアカウントにマッピングします。
- 輸出規制ライセンスと適用済みライセンスに必要な承認コードは、CSSMで生成し、SSM オンプレミスにインポートする必要があります。

### 例

- [SLACの要求例 \(CSSMに直接接続\) \(58 ページ\)](#)
- [ライセンス使用状況情報の保存例 \(60 ページ\)](#)
- [信頼コードのインストールの例 \(60 ページ\)](#)
- [SLR承認コードを返す例 \(60 ページ\)](#)

### SLACの要求例 (CSSMに直接接続)

次の例は、CSSMに直接接続されている製品インスタンスにSLACを要求してインストールする方法を示しています。この例は、アクティブ、スタンバイ、およびメンバーのスタック構成セットアップです。スタック内のすべてのデバイスはC9300Xであり、HSECK9キーとIPSecをサポートします。IPsecはHSECK9キーを必要とする暗号化機能です。セットアップのすべての製品インスタンスに対してSLACが要求されます。

```
Device# license smart authorization request add hseck9 all
Device#
Oct 19 15:49:47.888: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code was successfully installed on PID:C9300X-24HX,SN:FOC2519L8R7
Oct 19 15:49:47.946: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code was successfully installed on PID:C9300X-48HX,SN:FOC2524L39P
Oct 19 15:49:48.011: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing
authorization code was successfully installed on PID:C9300X-48HX,SN:FOC2516LC92

Device# show license authorization
Overall status:
Active: PID:C9300X-24HX,SN:FOC2519L8R7
Status: SMART AUTHORIZATION INSTALLED on Oct 19 15:49:47 2021 UTC
```

```

Last Confirmation code: 4e740fb8
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
Status: SMART AUTHORIZATION INSTALLED on Oct 19 15:49:47 2021 UTC
Last Confirmation code: 086d28d7
Member: PID:C9300X-48HX,SN:FOC2516LC92
Status: SMART AUTHORIZATION INSTALLED on Oct 19 15:49:48 2021 UTC
Last Confirmation code: beb51aal

Authorizations:
C9K HSEC (Cat9K HSEC):
  Description: HSEC Key for Export Compliance on Cat9K Series Switches
  Total available count: 3
  Enforcement type: EXPORT RESTRICTED
  Term information:
    Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1
    Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1
    Member: PID:C9300X-48HX,SN:FOC2516LC92
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available

```

### 例：SLAC の要求と SLAC の返却（CSSM への接続なし、CSLU なし）

次の例は、製品インスタンスで SLAC 要求を生成して保存する方法と、エアギャップネットワーク内の製品インスタンスの SLAC を CSSM Web UI に返す方法を示しています。製品インスタンスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.7.1 です。これにより、エアギャップネットワークで SLAC を要求し、返却する方法がより簡単になりました。

#### SLAC の要求

```

Device# license smart authorization request add hseck9 local
Device# license smart authorization request save bootflash:slac-request.txt

```

上記の手順の後、CSSM Web UI にファイルをアップロードします。CSSM Web UI から、SLAC を含むファイルをダウンロードします。ファイルをインポートして製品インスタンスにインストールするには、次のコマンドを入力します。

```

Device# copy tftp://10.8.0.6/user01/slac_code.txt bootflash:
Device# license smart import bootflash:slac_code.txt

```

#### SLAC の返却

```

Device# license smart authorization return local offline bootflash:auth_return.txt

```

上記の手順の後、CSSM Web UI にファイルをアップロードします。この後、ファイルをダウンロードできますが、このファイルのインポートとインストールはオプションです。

### ライセンス使用状況情報の保存例

次の例は、製品インスタンスのライセンス使用状況情報を保存する方法を示しています。このオプションを使用して、エアギャップネットワークのレポート要件を満たすことができます。この例では、ファイルはまずフラッシュメモリに保存され、次に TFTP の場所にコピーされます。

```
Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

RUM レポートをファイルに保存した後、(インターネットに接続しているワークステーションや Cisco から) CSSM にアップロードする必要があります。

### 信頼コードのインストールの例

次の例は、信頼コードがすでに製品インスタンスにインストールされている場合に、信頼コードをインストールする方法を示しています。これには、CSSM への接続が必要です。正常なインストール後の **show license status** 出力例を次に示します。

信頼コードをインストールする前に、トークンを生成し、CSSM から対応するファイルをダウンロードする必要があります。

結果を確認するには、**show license status** コマンド (Trust Code Installed:) を使用します。

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzZmtgWm local force
Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9500-24Y4C,SN:CAT2344L4GH
          INSTALLED on Sep 04 01:01:46 2020 EDT
  Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ
           INSTALLED on Sep 04 01:01:46 2020 EDT
<output truncated>
```

### SLR 承認コードを返す例

次の例は、SLR 承認コードを削除して返す方法を示しています。ここでは、コードがオフラインで返されます (CSSM への接続なし)。正常に返された後の **show license all** 出力例を次に示します。

```
Device> enable
Device# license smart authorization return local offline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9500-16X,SN:FCW2233A5ZV
Return code: Cr9JHx-Llx5Rj-ftwzgl-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7
Device# configure terminal
Device(config)# no license smart reservation

Device# show license all
<output truncated>
License Authorizations
=====
```

Overall status:

Active: UDI: PID:C9500-16X,SN:FCW2233A5ZV

Status: NOT INSTALLED

**Last return code: Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7**

<output truncated>

製品インスタンスはエアギャップネットワーク内にあるため、CLIから戻りコードをコピーし、CSSM Web UI で製品インスタンスを見つけ、戻りコードを入力して戻りプロセスを完了する必要があります。

## line auto-consolidation

同じサブモードの複数回線の設定を単一回線に統合するには、グローバル コンフィギュレーション モードで **line auto-consolidation** コマンドを使用します。回線設定の自動統合はデフォルトで有効になっています。Cisco IOS XE Bengaluru 17.4.1 からこのコマンドの **no** 形式を使用して自動統合を無効化できます。

**line auto-consolidation**  
**no line auto-consolidation**

構文の説明	<b>auto-consolidation</b>	同じサブモードの複数回線の設定を単一回線に統合します。
コマンド デフォルト	自動統合はデフォルトで有効になっています。	
コマンド モード	グローバル コンフィギュレーション モード (config)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Bengaluru 17.4.1	このコマンドが追加されました。

次に、**line auto-consolidation** を設定した場合の不揮発性生成 (NVGEN) プロセスの出力例を示します。

```
Device# show run | sec line
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 9
transport input all
Device# configure terminal
Device(config)# line vty 10 15
Device(config-line)# transport input all
Device(config-line)# end
Device# show run | sec line
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 15
transport input all
```

次に、**no line auto-consolidation** を設定した場合の不揮発性生成 (NVGEN) プロセスの出力例を示します。

```
Device# show run | sec line
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 9
```

```
transport input all
Device# configure terminal
Device(config)#no line auto-consolidation
Device(config)# line vty 10 15
Device(config-line)# transport input all
Device(config-line)# end
Device# show run | sec line
no line auto-consolidation
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 9
transport input all
line vty 10 15
transport input all
```

# location

エンドポイントのロケーション情報を設定するには、グローバルコンフィギュレーションモードで **location** コマンドを使用します。ロケーション情報を削除するには、このコマンドの **no** 形式を使用します。

```
location admin-tag string | civic-location identifier hostid | civic-location identifier hostid |
elin-location {string | identifier id} | geo-location identifier hostid | prefer {cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
no location admin-tag string | civic-location identifier hostid | civic-location identifier hostid |
elin-location {string | identifier id} | geo-location identifier hostid | prefer {cdp weight
priority-value | lldp-med weight priority-value | static config weight priority-value}
```

## 構文の説明

<b>admin-tag</b> <i>string</i>	管理タグまたはサイト情報を設定します。英数字形式のサイト情報またはロケーション情報。
<b>civic-location</b>	都市ロケーション情報を設定します。
<b>identifier</b>	都市ロケーション、緊急ロケーション、地理的な場所の名前を指定します。
<b>host</b>	ホストの都市ロケーションや地理空間的な場所を定義します。
<i>id</i>	都市ロケーション、緊急ロケーション、地理的な場所の名前。  (注) LLDP-MED スイッチ TLV での都市ロケーションの ID は 250 バイト以下に制限されます。スイッチ設定中に使用できるバッファスペースに関するエラーメッセージを回避するには、各都市ロケーション ID に指定されたすべての都市ロケーション情報の全体の長さが 250 バイトを超えないようにします。
<b>elin-location</b>	緊急ロケーション情報 (ELIN) を設定します。
<b>geo-location</b>	地理空間的なロケーション情報を設定します。
<b>prefer</b>	ロケーション情報のソースのプライオリティを設定します。

コマンド デフォルト デフォルトの動作や値はありません。

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	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

**使用上のガイドライン** **location civic-location identifier** グローバル コンフィギュレーション コマンドを入力後、都市ロケーション コンフィギュレーション モードが開始されます。 **location geo-location identifier** グローバル コンフィギュレーション コマンドを入力後、ジオロケーション コンフィギュレーション モードが開始されます。

都市ロケーション ID は 250 バイトを超えてはなりません。

ホスト ID はホストの都市ロケーションや地理空間的な場所を設定します。ID がホストではない場合、ID はインターフェイスで参照できる地理空間的なテンプレートまたは都市ロケーションだけを定義します。

**host** キーワードは、デバイスの場所を定義します。 **identifier** と **host** キーワードを使用して設定可能な都市ロケーション オプションは同じです。都市ロケーション コンフィギュレーション モードで次の都市ロケーション オプションを指定できます。

- **additional-code** : 追加都市ロケーション コードを設定します。
- **additional-location-information** : 追加都市ロケーション情報を設定します。
- **branch-road-name** : ブランチのロード名を設定します。
- **building** : 建物の情報を設定します。
- **city** : 都市名を設定します。
- **country** : 2 文字の ISO 3166 の国コードを設定します。
- **county** : 郡名を設定します。
- **default** : コマンドをデフォルト値に設定します。
- **division** : 市の地区の名前を設定します。
- **exit** : 都市ロケーション コンフィギュレーション モードを終了します。
- **floor** : 階数を設定します。
- **landmark** : 目印となる建物の情報を設定します。
- **leading-street-dir** : 町名番地に付与される方角を設定します。
- **name** : 居住者名を設定します。
- **neighborhood** : ネイバーフッド情報を設定します。
- **no** : 指定された都市ロケーション データを拒否し、デフォルト値を設定します。
- **number** : 町名番地を設定します。
- **post-office-box** : 私書箱を設定します。
- **postal-code** : 郵便番号を設定します。
- **postal-community-name** : 郵便コミュニティ名を設定します。
- **primary-road-name** : 主要道路の名前を設定します。
- **road-section** : 道路の区間を設定します。
- **room** : 部屋の情報を設定します。
- **seat** : 座席の情報を設定します。
- **state** : 州の名前を設定します。

- **street-group** : 町名番地のグループを設定します。
- **street-name-postmodifier** : 町名番地の名前のポストモディファイアを設定します。
- **street-name-premodifier** : 町名番地の名前のプレモディファイアを設定します。
- **street-number-suffix** : 町名番地の番号のサフィックスを設定します。
- **street-suffix** : 町名番地のサフィックスを設定します。
- **sub-branch-road-name** : 支線からさらに分岐した道路名を設定します。
- **trailing-street-suffix** : 後に続く町名番地のサフィックスを設定します。
- **type-of-place** : 場所のタイプを設定します。
- **unit** : 単位を設定します。

地理的ロケーション コンフィギュレーション モードで次の地理空間的なロケーション情報を指定できます。

- **altitude** : 高さの情報を階数、メートル、またはフィート単位で設定します。
- **latitude** : 度、分、秒の緯度情報を設定します。範囲は -90 ~ 90 度です。正の値は、赤道より北側の位置を示します。
- **longitude** : 度、分、秒の経度の情報を設定します。範囲は -180 ~ 180 度です。正の値は、グリニッジ子午線の東側の位置を示します。
- **resolution** : 緯度と経度の分解能を設定します。分解能値を指定しない場合、10m のデフォルト値が緯度と経度の分解能パラメータに適用されます。緯度と経度の場合、分解能の単位はメートルで測定されます。分解能の値は小数単位でも指定できます。
- **default** : デフォルトの属性によって、地理的位置を設定します。
- **exit** : 地理的ロケーション コンフィギュレーション モードを終了します。
- **no** : 指定された地理的パラメータを拒否し、デフォルト値を設定します。

ロケーション TLV をディセーブルにするには、**no lldp med-tlv-select location information** インターフェイス コンフィギュレーション コマンドを使用します。デフォルトでは、ロケーション TLV はイネーブルに設定されています。

次の例では、スイッチに都市ロケーション情報を設定する方法を示します。

```
Device(config)# location civic-location identifier 1
Device(config-civic)# number 3550
Device(config-civic)# primary-road-name "Cisco Way"
Device(config-civic)# city "San Jose"
Device(config-civic)# state CA
Device(config-civic)# building 19
Device(config-civic)# room C6
Device(config-civic)# county "Santa Clara"
Device(config-civic)# country US
Device(config-civic)# end
```

設定を確認するには、**show location civic-location** 特権 EXEC コマンドを入力します。

次の例では、スイッチ上で緊急ロケーション情報を設定する方法を示します。

```
Device(config)# location elin-location 14085553881 identifier 1
```

設定を確認するには、**show location elin** 特権 EXEC コマンドを入力します。

次に、スイッチに、地理空間ロケーション情報を設定する例を示します。

```
Device(config)# location geo-location identifier host  
Device(config-geo)# latitude 12.34  
Device(config-geo)# longitude 37.23  
Device(config-geo)# altitude 5 floor  
Device(config-geo)# resolution 12.34
```

設定された地理空間的な場所の詳細を表示するには、**show location geo-location identifier** コマンドを使用します。

# location plm calibrating

調整クライアントのパス損失測定（CCXS60）要求を設定するには、グローバルコンフィギュレーションモードで **location plm calibrating** コマンドを使用します。

## location plm calibrating multiband | uniband

### 構文の説明

**multiband** 関連付けられた 802.11a または 802.11b/g 無線での調整クライアントのパス損失測定要求を指定します。

**uniband** 関連付けられた 802.11a/b/g 無線での調整クライアントのパス損失測定要求を指定します。

### コマンド デフォルト

デフォルトの動作や値はありません。

### 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

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

### 使用上のガイドライン

単一の無線クライアントには、（無線がデュアルバンドで、2.4 GHz と 5 GHz の両方の帯域でも動作できるとしても）uniband が役立ちます。複数の無線クライアントには、multiband が役立ちます。

次に、関連付けられた 802.11a/b/g 無線での調整クライアントのパス損失測定要求を設定する例を示します。

```
Device# configure terminal
Device(config)# location plm calibrating uniband
Device(config)# end
```

## mac address-table move update

MAC アドレステーブル移行更新機能を有効にするには、スイッチスタックまたはスタンドアロンスイッチのグローバル コンフィギュレーション モードで **mac address-table move update** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**mac address-table move update receive | transmit**  
**no mac address-table move update receive | transmit**

### 構文の説明

<b>receive</b>	スイッチが MAC アドレス テーブル移行更新メッセージを処理するように指定します。
<b>transmit</b>	プライマリ リンクがダウンし、スタンバイ リンクが起動した場合、スイッチが MAC アドレステーブル移行更新メッセージをネットワークの他のスイッチに送信するように指定します。

### コマンド デフォルト

デフォルトでは、MAC アドレステーブル移行更新機能はディセーブルです。

### コマンド モード

グローバル コンフィギュレーション

### コマンド履歴

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

### 使用上のガイドライン

MAC アドレステーブル移行更新機能により、プライマリ（フォワーディング）リンクがダウンし、スタンバイリンクがトラフィックのフォワーディングを開始した場合、スイッチは高速双方向コンバージェンスを提供できます。

プライマリリンクがダウンし、スタンバイリンクが起動した場合、アクセススイッチが MAC アドレステーブル移行更新メッセージを送信するように設定できます。アップリンクスイッチが、MAC アドレステーブル移行更新メッセージを受信および処理するように設定できます。

### 例

次の例では、アクセス スイッチが MAC アドレス テーブル移行更新メッセージを送信するように設定する方法を示します。

```
Device# configure terminal
Device(config)# mac address-table move update transmit
Device(config)# end
```

次の例では、アップリンク スイッチが MAC アドレス テーブル移行更新メッセージを取得および処理するように設定する方法を示します。

```
Device# configure terminal
```

```
Device(config)# mac address-table move update receive  
Device(config)# end
```

設定を確認するには、**show mac address-table move update** 特権 EXEC コマンドを入力します。

# mgmt\_init

イーサネット管理ポートを初期化するには、ブートローダモードで **mgmt\_init** コマンドを使用します。

## mgmt\_init

---

### 構文の説明

このコマンドには引数またはキーワードはありません。

---

### コマンドデフォルト

デフォルトの動作や値はありません。

---

### コマンドモード

ブートローダ

---

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

---

### 使用上のガイドライン

イーサネット管理ポートのデバッグ中にのみ、**mgmt\_init** コマンドを使用します。

---

### 例

次の例では、イーサネット管理ポートを初期化する方法を示します。

```
Device: mgmt_init
```

# mkdir

指定されたファイルシステムに1つ以上のディレクトリを作成するには、ブートローダモードで **mkdir** コマンドを使用します。

**mkdir** *filesystem:/directory-url...*

## 構文の説明

*filesystem:* ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。

*/directory-url...* 作成するディレクトリの名前です。ディレクトリ名はスペースで区切ります。

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

ブートローダ

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

ディレクトリ名では、大文字と小文字が区別されます。

スラッシュ (/) 間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

## 例

次の例では、ディレクトリ **Saved\_Configs** を作成する方法を示します。

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```



## more

1つ以上のファイルの内容を表示するには、ブートローダモードで **more** コマンドを使用します。

**more** *filesystem:/file-url...*

### 構文の説明

*filesystem:* ファイルシステムのエイリアス。システム ボード フラッシュ デバイスには **flash:** を使用します。

*/file-url...* 表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

### コマンドデフォルト

デフォルトの動作や値はありません。

### コマンドモード

ブートローダ

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

### 使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定した場合は、各ファイルの内容が順に表示されます。

### 例

次に、ファイルの内容を表示する例を示します。

```
Device: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

## no debug all

スイッチのデバッグを無効にするには、特権 EXEC モードで **no debug all** コマンドを使用します。

### no debug all

コマンド デフォルト	デフォルトの動作や値はありません。	
コマンド モード	特権 EXEC	
コマンド履歴	リリース	変更内容
	Cisco IOS XE リリース 16.1 このコマンドが導入されました。	

### 例

次に、スイッチでデバッグを無効にする例を示します。

```
Device: no debug all
All possible debugging has been turned off.
```

# rename

ファイルの名前を変更するには、ブートコンフィギュレーションモードで **rename** コマンドを使用します。

**rename** *filesystem:/source-file-url filesystem:/destination-file-url*

## 構文の説明

*filesystem:* ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。

*/source-file-url* 元のパス（ディレクトリ）およびファイル名です。

*/destination-file-url* 新しいパス（ディレクトリ）およびファイル名です。

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

ブートローダ

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

スラッシュ (/) 間に指定できるディレクトリ名は最大 127 文字です。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

指定できるファイル名は最大 127 文字です。ファイル名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、コロンは使用できません。

## 例

次の例では、ファイル *config.text* の名前を *config1.text* に変更します。

```
Device: rename usbflash0:config.text usbflash0:config1.text
```

ファイルの名前が変更されたかどうかを確認するには、**dir filesystem:** ブートローダコマンドを入力します。

# request consent-token accept-response shell-access

以前に生成されたチャレンジに対する同意トークン応答を送信するには、**request consent-token accept-response shell-access** コマンドを使用します。

**request consent-token accept-response shell-access** *response-string*

## 構文の説明

構文	Description
<i>response-string</i>	応答を表す文字列を指定します。

## コマンドモード

特権 EXEC モード (#)

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

応答文字列は、チャレンジの生成から30分以内に入力する必要があります。入力しないとチャレンジが期限切れになり、新しいチャレンジの要求が必要になります。

## 例

次に、**request consent-token accept-response shell-access** *response-string* コマンドの出力例を示します。

```
Device# request consent-token accept-response shell-access
% Consent token authorization success
*Jan 18 02:51:37.807: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success:
Shell access 0).
```

# request consent-token generate-challenge shell-access

システムシェルアクセスに対する同意トークンチャレンジを生成するには、**request consent-token generate-challenge shell-access** コマンドを使用します。

**request consent-token generate-challenge shell-access auth-timeout *time-validity-slot***

## 構文の説明

構文	Description
<b>auth-timeout <i>time-validity-slot</i></b>	シェルアクセスを要求するタイムスロット (分) を指定します。

コマンドモード 特権 EXEC モード (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン システムシェルに対する要求したタイムスロットが期限切れになると、セッションは自動的に終了します。

システムシェルアクセスの最大承認タイムアウトは7日間です。

## 例

次に、**request consent-token generate-challenge shell-access auth-timeout *time-validity-slot*** コマンドの出力例を示します。

```
Device# request consent-token generate-challenge shell-access auth-timeout 900
Zs1wqB9QWNgPwMMwMh6csh1CBAQRd7cR1eDBAw7UBWAgBADEFHNEAGND9R1BN09S10SBX0WQCM0DAUM1L5Q10Q1E5E3R1E
Device#
*Jan 18 02:47:06.733: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation
attempt: Shell access 0).
```

## request consent-token terminate-auth

システムシェルに対する同意トークンベースの承認を終了するには、**request consent-token terminate-auth** コマンドを使用します。

### request consent-token terminate-auth

コマンドモード	特権 EXEC モード (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

**使用上のガイドライン** システムシェルアクセスのシナリオでは、シェルを終了しても、承認タイムアウトが発生するまで承認は終了しません。

システムシェルアクセスの目的を達成したら、**request consent-token terminate-auth** コマンドを明示的に発行することによって、システムシェルの承認を強制終了することを推奨します。

**request consent-token terminate-auth** コマンドを使用して現在の認証を終了した場合、ユーザがシステムシェルにアクセスする際に再度認証プロセスが必要になります。

### 例

次に、**request consent-token terminate-auth** コマンドの出力例を示します。

```
Device# request consent-token terminate-auth shell-access
% Consent token authorization termination success

Device#
*Mar 13 01:45:39.197: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate
authentication: Shell access 0).
Device#
```

# request platform software console attach switch

メンバスイッチでセッションを開始するには、特権 EXEC モードで **request platform software console attach switch** コマンドを使用します。



- (注) スタッキングスイッチ (Catalyst 3650/3850/9200/9300 スイッチ) では、このコマンドはスタンバイコンソールでセッションを開始する場合にのみ使用できます。Catalyst 9500 スイッチでは、このコマンドは Stackwise Virtual セットアップでのみサポートされます。メンバスイッチでセッションを開始することはできません。デフォルトでは、すべてのコンソールはすでにアクティブであるため、アクティブなコンソールでセッションを開始する要求はエラーになります。

**request platform software console attach switch** { *switch-number* | **active** | **standby** } { **0/0** | **R0** }

## 構文の説明

**switch-number** スイッチ番号を指定します。指定できる範囲は 1 ~ 9 です。

**active** アクティブスイッチを指定します。

(注) この引数は、Catalyst 9500 スイッチではサポートされていません。

**standby** スタンバイスイッチを指定します。

**0/0** SPA-Inter-Processor スロットが 0 で、ベイが 0 であることを指定します。

(注) このオプションをスタッキングスイッチとともに使用しないでください。それはエラーになります。

**R0** ルートプロセッサ スロットが 0 であることを指定します。

## コマンドデフォルト

デフォルトでは、スタック内のすべてのスイッチはアクティブです。

## コマンドモード

特権 EXEC (#)

## コマンド履歴

リリース 変更内容  
ス

このコマンドが導入されました。

## 使用上のガイドライン

スタンバイスイッチでセッションを開始するには、最初に設定で有効にする必要があります。

## 例

次に、スタンバイスイッチとのセッションを行う例を示します。

```
Device# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)# end
Device# request platform software console attach switch standby R0
#
# Connecting to the IOS console on the route-processor in slot 0.
# Enter Control-C to exit.
#
Device-stby> enable
Device-stby#
```



## reset

システムでハードリセットを実行するには、ブートローダモードで **reset** コマンドを実行します。ハードリセットを行うと、デバイスの電源切断後に電源を投入する手順と同様に、プロセッサ、レジスタ、およびメモリの内容が消去されます。

### reset

**構文の説明** このコマンドには引数またはキーワードはありません。

**コマンド デフォルト** デフォルトの動作や値はありません。

**コマンド モード** ブートローダ

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

### 例

次の例では、システムをリセットする方法を示します。

```
Device: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

# rmdir

指定されたファイルシステムから1つ以上の空のディレクトリを削除するには、ブートローダモードで **rmdir** コマンドを使用します。

**rmdir** *filesystem:/directory-url...*

## 構文の説明

*filesystem:* ファイルシステムのエイリアス。USB メモリ スティックの場合は、**usbflash0:** を使用します。

*/directory-url...* 削除する空のディレクトリのパス（ディレクトリ）および名前です。ディレクトリ名はスペースで区切ります。

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

ブートローダ

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

スラッシュ (/) 間に指定できるディレクトリ名は最大 45 文字で、大文字と小文字の区別があります。ディレクトリ名には制御文字、スペース、削除文字、スラッシュ、引用符、セミコロン、およびコロンは使用できません。

ディレクトリを削除する前に、まずディレクトリ内のファイルをすべて削除する必要があります。

デバイスは、各ディレクトリを削除する前に、確認を求めるプロンプトを出します。

## 例

次の例では、ディレクトリを 1 つ削除する方法を示します。

```
Device: rmdir usbflash0:Test
```

ディレクトリが削除されたかどうかを確認するには、**dir filesystem:** ブートローダコマンドを入力します。

## sdm prefer

スイッチで使用する SDM テンプレートを指定するには、グローバル コンフィギュレーション モードで **sdm prefer** コマンドを使用します。

**sdm prefer**  
{ **advanced** }

### 構文の説明

**advanced** NetFlow などの高度な機能をサポートします。

### コマンド デフォルト

デフォルトの動作や値はありません。

### 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

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

### 使用上のガイドライン

スタックでは、すべてのスタック メンバが、アクティブな に保存された同一の SDM テンプレートを使用する必要があります。

新規 がスタックに追加されると、アクティブ に保存された SDM コンフィギュレーションは、個々の に設定されているテンプレートを上書きします。

### 例

次に、高度なテンプレートを設定する例を示します。

```
Device(config)# sdm prefer advanced
Device(config)# exit
Device# reload
```

## service private-config-encryption

プライベート設定ファイルの暗号化を有効にするには、**service private-config-encryption** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

**service private-config-encryption**  
**no service private-config-encryption**

**構文の説明** このコマンドには引数またはキーワードはありません。

**コマンド デフォルト** デフォルトの動作や値はありません。

**コマンド モード** グローバル コンフィギュレーション (config)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

**例** 次に、プライベート設定ファイルの暗号化を有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# service private-config-encryption
```

関連コマンド	コマンド	説明
	<b>show parser encrypt file status</b>	プライベート設定の暗号化ステータスを表示します。

## set

環境変数を設定または表示するには、ブートローダモードで **set** コマンドを使用します。環境変数は、ブートローダまたはデバイスで稼働している他のソフトウェアを制御するために使用できます。

**set** *variable value*

### 構文の説明

変数 値 *variable* および *value* の適切な値には、次のいずれかのキーワードを使用します。

**MANUAL\_BOOT** : デバイスの起動を自動で行うか手動で行うかを決定します。

有効な値は 1/Yes と 0/No です。0 または No に設定されている場合、ブートローダはシステムを自動的に起動します。他の値に設定されている場合は、ブートローダモードから手動でデバイスを起動する必要があります。

**BOOT filesystem:/file-url** : 自動起動時にロードおよび実行される実行可能ファイルのセミコロン区切りリストを識別します。

BOOT 環境変数が設定されていない場合、システムは、フラッシュファイルシステム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。BOOT 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュファイルシステムで最初に検出した起動可能なファイルを起動しようとします。

**ENABLE\_BREAK** : ユーザがコンソールの **Break** キーを押すと自動起動プロセスを中断できるようになります。

有効な値は 1、Yes、On、0、No、および Off です。1、Yes、または On に設定されている場合は、フラッシュファイルシステムの初期化後にコンソール上で Break キーを押すことで、自動起動プロセスを中断できます。

**HELPER filesystem:/file-url** : ブートローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを識別します。ヘルパーファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。

**PS1 prompt** : ブートローダモードの場合に、コマンドラインプロンプトとして使用する文字列を指定します。

**CONFIG\_FILE flash:/file-url** : Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名を指定します。

**BAUD rate** : コンソールのボーレートに使用するビット数/秒 (b/s) を指定します。コンフィギュレーションファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブートローダからボーレート設定を継承し、この値を引き続き使用します。指定できる範囲は0～128000 b/sです。有効値は、50、75、110、150、300、600、1200、1800、2000、2400、3600、4800、7200、9600、14400、19200、28800、38400、56000、57600、115200、および128000です。

最も一般的な値は、300、1200、2400、9600、19200、57600、および115200です。

**SWITCH\_NUMBER** *stack-member-number* : スタックメンバのメンバ番号を変更します。

**SWITCH\_PRIORITY** *priority-number* : スタックメンバのプライオリティ値を変更します。

#### コマンド デフォルト

環境変数のデフォルト値は、次のとおりです。

MANUAL\_BOOT: No (0)

BOOT : ヌルストリング

ENABLE\_BREAK : No (Off または 0) (コンソール上で Break キーを押して自動起動プロセスを中断することはできません)。

HELPER: デフォルト値はありません (ヘルパーファイルは自動的にロードされません)。

PS1 デバイス :

CONFIG\_FILE: config.text

BAUD : 9600 b/s

SWITCH\_NUMBER: 1

SWITCH\_PRIORITY: 1



(注) 値が設定された環境変数は、各ファイルのフラッシュファイルシステムに保管されます。ファイルの各行には、環境変数名と等号に続いて、その変数の値が指定されます。

このファイルに表示されていない変数には値がありません。表示されていればヌルストリングであっても値があります。Null 文字列 (たとえば"") が設定されている変数は、値が設定された変数です。

多くの環境変数は事前に定義されており、デフォルト値が設定されています。

#### コマンド モード

ブートローダ

#### コマンド履歴

リリース

変更内容

Cisco IOS XE Gibraltar 16.11.1 このコマンドが導入されました。

**使用上のガイドライン** 環境変数は大文字と小文字の区別があり、指定どおりに入力する必要があります。

値を持つ環境変数は、フラッシュ ファイル システムの外にあるフラッシュ メモリに保管されます。

通常的环境では、環境変数の設定を変更する必要はありません。

MANUAL\_BOOT 環境変数は、**boot manual** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

BOOT 環境変数は、**boot system filesystem:/file-url** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

ENABLE\_BREAK 環境変数は、**boot enable-break** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

HELPER 環境変数は、**boot helper filesystem:/file-url** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

CONFIG\_FILE 環境変数は、**boot config-file flash:/file-url** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

SWITCH\_NUMBER 環境変数は、**switch current-stack-member-number renumber new-stack-member-number** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

SWITCH\_PRIORITY 環境変数は、**device stack-member-number priority priority-number** グローバル コンフィギュレーション コマンドを使用して設定することもできます。

ブート ロードのプロンプト文字列 (PS1) には、等号 (=) を除く、出力可能な文字列を 120 文字まで指定できます。

## 例

次に、SWITCH\_PRIORITY 環境変数を設定する例を示します。

```
Device: set SWITCH_PRIORITY 2
```

設定を確認するには、**set** ブートローダコマンドを使用します。

## show avc client

上位アプリケーションの数に関する情報を表示するには、特権 EXEC モードで **show avc client** コマンドを使用します。

**show avc client** *client-mac* **top n application** [**aggregate** | **upstream** | **downstream**]

### 構文の説明

**client** *client-mac* クライアントの MAC アドレスを指定します。

**top n application** 特定のクライアントの上位「N」個のアプリケーションの数を指定します。

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

特権 EXEC

### コマンド履歴

リリース 変更内容  
ス

このコマンドが導入されました。

次に、**show avc client** コマンドの出力例を示します。

```
# sh avc client 0040.96ae.65ec top 10 application aggregate
```

Cumulative Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	skinny	7343	449860	61	94
2	unknown	99	13631	137	3
3	dhcp	18	8752	486	2
4	http	18	3264	181	1
5	tftp	9	534	59	0
6	dns	2	224	112	0

Last Interval (90 seconds) Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	skinny	9	540	60	100



## show bootflash:

ファイルシステムに関する情報を表示するには、ユーザ EXEC または特権 EXEC モードで **show bootflash:** コマンドを使用します。

**show bootflash:** [all | filesys | namesort | sizesort | timesort ]

構文の説明	all	(任意) 可能なすべてのフラッシュ情報を表示します。
	<b>filesys</b>	(任意) フラッシュシステム情報を表示します。
	<b>namesort</b>	(任意) 出力をファイル名でソートします。
	<b>sizesort</b>	(任意) 出力をファイルサイズでソートします。
	<b>timesort</b>	(任意) 出力をタイムスタンプでソートします。

コマンドデフォルト	ユーザ EXEC (>)
	特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
	Cisco IOS XE Amsterdam 17.3.1	次のキーワードが導入されました。 <ul style="list-style-type: none"> <li>• <b>namesort</b></li> <li>• <b>sizesort</b></li> <li>• <b>timesort</b></li> </ul>

例 :

次に、**show bootflash: all** コマンドの出力例を示します。

```
Device# show bootflash: all
-#- --length-- -----date/time----- path
2      4096 May 11 2020 16:49:01.0000000000 +00:00 .installer
3      4096 Feb 27 2020 15:03:50.0000000000 +00:00 .installer/issu_crash
4          12 May 05 2020 22:06:48.0000000000 +00:00 .installer/issu_crash/fru_crash
5          50 May 11 2020 16:40:40.0000000000 +00:00 .installer/last_pkgconf_shasum
```

## show bootflash:

```

6          6 Feb 27 2020 16:33:59.0000000000 +00:00 .installer/install_issu_pid
7          13 Feb 27 2020 21:05:35.0000000000 +00:00 .installer/install_issu_prev_state
8          17 Feb 27 2020 21:05:36.0000000000 +00:00 .installer/install_issu_state
9          13 May 11 2020 16:41:12.0000000000 +00:00 .installer/watchlist
10         8 Feb 28 2020 18:04:31.0000000000 +00:00 .installer/crdu_frus
11         0 Mar 01 2020 18:01:09.0000000000 +00:00
.installer/.install_add_pkg_list.prev.txt
12        1729 Mar 01 2020 18:02:54.0000000000 +00:00 .installer/install_add_oper.log
13         5 May 11 2020 16:40:40.0000000000 +00:00 .installer/install_global_trans_lock
14        10 May 11 2020 16:40:40.0000000000 +00:00 .installer/install_state
15 33554432 May 11 2020 16:42:37.0000000000 +00:00 nvram_config
16        396 May 11 2020 16:41:02.0000000000 +00:00 boothelper.log
17       4096 May 11 2020 16:40:42.0000000000 +00:00 rpr
18        80 May 11 2020 16:40:42.0000000000 +00:00 rpr/RPR_log.txt
19        80 May 05 2020 22:10:45.0000000000 +00:00 rpr/RPR_log_prev.txt
20       2183 May 11 2020 16:40:42.0000000000 +00:00 bootloader_evt_handle.log
21       4096 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh
22        965 Dec 24 2019 15:23:55.0000000000 +00:00 .ssh/ssh_host_key
23        630 Dec 24 2019 15:23:55.0000000000 +00:00 .ssh/ssh_host_key.pub
24       1675 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_rsa_key
25        382 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_rsa_key.pub
26        668 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_dsa_key
27        590 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_dsa_key.pub
28        492 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ecdsa_key
29        162 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ecdsa_key.pub
30        387 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ed25519_key
31         82 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ed25519_key.pub
32       4096 Dec 24 2019 15:24:41.0000000000 +00:00 core
33       4096 May 11 2020 16:41:29.0000000000 +00:00 core/modules
34       4096 May 05 2020 22:11:47.0000000000 +00:00 .prst_sync
35       4096 Mar 01 2020 18:17:15.0000000000 +00:00 .rollback_timer
36       4096 Mar 06 2020 21:01:11.0000000000 +00:00 gs_script
37       4096 Mar 06 2020 21:01:11.0000000000 +00:00 gs_script/sss

```

```

38      4096 Apr 24 2020 18:56:40.0000000000 +00:00 tech_support
39      15305 May 11 2020 16:41:01.0000000000 +00:00 tech_support/igmp-snooping.tcl
40      1612 May 11 2020 16:41:01.0000000000 +00:00 tech_support/igmpsn_dump.tcl
.
.
.

```

次に、**show bootflash: sizesort** コマンドの出力例を示します。

```

Device# show bootflash: sizesort
-#- --length-- -----date/time----- path
126 968337890 Mar 27 2020 18:06:17.0000000000 +00:00 cat9k_iosxe.CSCvt37598.bin
136 967769293 May 05 2020 21:50:33.0000000000 +00:00 cat9k_iosxe.CSCvu05574
124 967321806 Mar 23 2020 18:48:45.0000000000 +00:00 cat9k_ts_2103.bin
133 951680494 Apr 13 2020 19:46:35.0000000000 +00:00
cat9k_iosxe.2020-04-13_17.34_rakoppak.SSA.bin
130 950434163 Apr 09 2020 09:03:47.0000000000 +00:00
cat9k_iosxe.2020-04-09_13.49_rakoppak.SSA.bin
132 950410332 Apr 09 2020 07:29:57.0000000000 +00:00
cat9k_iosxe.2020-04-09_12.28_rakoppak.SSA.bin
134 948402972 Apr 17 2020 23:02:04.0000000000 +00:00 cat9k_iosxe.tla.bin
77 810146146 Feb 27 2020 15:41:42.0000000000 +00:00 cat9k_iosxe.16.12.01c.SPA.bin
88 701945494 Feb 27 2020 16:23:55.0000000000 +00:00 cat9k_iosxe.16.09.03.SPA.bin
101 535442436 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-rpbase.16.12.01c.SPA.pkg
86 88884228 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-espbase.16.12.01c.SPA.pkg
104 60167172 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-sipspa.16.12.01c.SPA.pkg
102 43111770 Mar 01 2020 18:02:07.0000000000 +00:00 cat9k-rpboot.16.12.01c.SPA.pkg
15 33554432 May 11 2020 16:42:37.0000000000 +00:00 nvram_config
131 33554432 May 11 2020 16:42:39.0000000000 +00:00 nvram_config_bkup
103 31413252 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-sipbase.16.12.01c.SPA.pkg
105 22676484 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-srdriver.16.12.01c.SPA.pkg
85 14226440 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-cc_srdriver.16.12.01c.SPA.pkg
.
.
.

```

## show consistency-checker mcast

整合性チェックを実行し、レイヤ2 マルチキャスト転送テーブルおよびレイヤ3 マルチキャスト転送テーブルのソフトウェアエントリの不整合状態を検出するには、特権 EXEC モードで **show consistency-checker mcast** コマンドを実行します。

```
show consistency-checker mcast { l2m | l3m } start all | vlan vlan-id ipv4-address |
ipv6-address [ recursive ]
```

構文の説明		
<b>l2m</b>		整合性チェックを実行するために、レイヤ2 マルチキャスト転送テーブルが選択されます。
<b>l3m</b>		整合性チェックを実行するために、レイヤ3 マルチキャスト転送テーブルが選択されます。
<b>start</b>		レイヤ2 マルチキャストの整合性チェックを開始します。 <ul style="list-style-type: none"> <li>• <b>all</b> : テーブル全体のチェックを開始します。</li> <li>• <b>vlan vlan-id { ipv4-address   ipv6-address }</b> : 指定した VLAN のチェックを開始します。</li> </ul>
<b>all</b>		テーブル全体のチェックを開始します。
<b>vlan vlan-id { ipv4-address   ipv6-address }</b>		指定した VLAN のチェックを開始します。
<b>recursive</b>		再帰整合性チェックを実行します。

コマンド デフォルト      デフォルトの動作や値はありません。

コマンド モード          特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。
	Cisco IOS XE Cupertino 17.7.1	レイヤ3 マルチキャスト転送テーブルで整合性チェックを実行するために、 <b>l3m</b> キーワードが導入されました。

使用上のガイドライン      整合性チェックには次の制限事項があります。

- 整合性チェックを中断または終了するコマンドはありません。完全なレポートが表示されると停止します。
- FED ハードウェアチェックは部分的に実装されています。プログラミングハードウェアのエラーのみが報告されます。

- ・誤検出のケース：整合性チェッカが実行されており、多数の機能テーブルエントリの削除/追加/変更アクションが発生した場合（clear \* または relearn によってトリガーされた場合）、整合性チェッカはプロセス間で一貫性のないエントリまたは欠落したエントリを報告することがあります。また、テーブルエントリに多数の変更が加えられたために、古いレポートをオフにすることもあります。

## 例

次に、**show consistency-checker mcast l2m** コマンドの出力例を示します。

```
Device# show consistency-checker mcast l2m start vlan 900 229.1.1.1 recursive
Single entry scan started with Run_id: 2

*Feb 17 06:54:09.880: %IOSXE_FMANRP_CCK-6-FMANRP_COMPLETED: Consistency Check for Run-Id
2 is completed. Check 'show consistency-checker run-id 2'.
Device#
Device# show consistency-checker run 2
Process: IOSD
  Object-Type      Start-time          Entries      Exceptions
  12m_vlan         2021/02/17 06:54:01      1            0
  12m_group        2021/02/17 06:54:01      1            0

Process: FMAN-FP
*Statistics(A/I/M/S/O): Actual/Inherited/Missing/Stale/Others

  Object-Type      Start-time          State         A / I / M / S / O
  12m_vlan         1970/01/01 00:10:03      Consistent   0 / 0 / 0 / 0 / 0
  12m_group        1970/01/01 00:10:03      Consistent   0 / 0 / 0 / 0 / 0

Process: FED
*Statistics(A/I/M/S/HW/O): Actual/Inherited/Missing/Stale/Hardware/Others

  Object-Type      Start-time          State         A / I / M / S / HW / O
  12m_vlan         2021/02/17 06:54:01      Inconsistent 1 / 0 / 0 / 0 / 0 / 0
  12m_group        2021/02/17 06:54:01      Inconsistent 0 / 1 / 0 / 0 / 0 / 0

Device#
```

次に、**show consistency-checker mcast l3m** コマンドの出力例を示します。

```
Device# show consistency-checker mcast l2m start vlan 900 229.1.1.1 recursive
Single entry scan started with Run_id: 2

*Feb 17 06:54:09.880: %IOSXE_FMANRP_CCK-6-FMANRP_COMPLETED: Consistency Check for Run-Id
2 is completed. Check 'show consistency-checker run-id 2'.
Device#
Device# show consistency-checker run 2
Process: IOSD
  Object-Type      Start-time          Entries      Exceptions
  12m_vlan         2021/02/17 06:54:01      1            0
  12m_group        2021/02/17 06:54:01      1            0

Process: FMAN-FP
*Statistics(A/I/M/S/O): Actual/Inherited/Missing/Stale/Others

  Object-Type      Start-time          State         A / I / M / S / O
  12m_vlan         1970/01/01 00:10:03      Consistent   0 / 0 / 0 / 0 / 0
  12m_group        1970/01/01 00:10:03      Consistent   0 / 0 / 0 / 0 / 0
```

## show consistency-checker mcast

```
Process: FED
*Statistics (A/I/M/S/HW/O): Actual/Inherited/Missing/Stale/Hardware/Others

Object-Type      Start-time          State                A / I / M / S / HW/ O
l2m_vlan         2021/02/17 06:54:01 Inconsistent         1/ 0/ 0/ 0/ 0/ 0
l2m_group        2021/02/17 06:54:01 Inconsistent         0/ 1/ 0/ 0/ 0/ 0

Device#
```

## show consistency-checker objects

整合性チェッカを実行し、オブジェクトのソフトウェアエントリの不整合状態を検出するには、特権 EXEC モードで **show consistency-checker objects** コマンドを実行します。

```
show consistency-checker objects adjacency | interface | l2m_group | l2m_vlan |
l3_entry | l3m_entry [ run-id ] [ detail ]
```

### 構文の説明

**adjacency** 隣接関係エントリで整合性チェッカを実行します。

**interface** インターフェイスエントリで整合性チェッカを実行します。

**l2m\_group** レイヤ2マルチキャストグループエントリで整合性チェッカを実行します。

**l2m\_vlan** レイヤ2マルチキャストVLANエントリで整合性チェッカを実行します。

**l3\_entry** レイヤ3ユニキャストエントリで整合性チェッカを実行します。

**l3m\_entry** レイヤ3マルチキャストエントリで整合性チェッカを実行します。

**run-id** 実行IDごとに整合性チェッカを実行します。

**detail** 実行IDの詳細な出力を表示します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### コマンドモード

特権 EXEC (#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

### 使用上のガイドライン

整合性チェッカには次の制限事項があります。

- 整合性チェッカを中断または終了するコマンドはありません。完全なレポートが表示されると停止します。
- FEDハードウェアチェックは部分的に実装されています。プログラミングハードウェアのエラーのみが報告されます。
- 誤検出のケース：整合性チェッカが実行されており、多数の機能テーブルエントリの削除/追加/変更アクションが発生した場合（clear \* または relearn によってトリガーされた場合）、整合性チェッカはプロセス間で一貫性のないエントリまたは欠落したエントリを報告することがあります。また、テーブルエントリに多数の変更が加えられたために、古いレポートをオフにすることもあります。

## 例

次に、**show consistency-checker objects l2m\_group** コマンドの出力例を示します。

```
Device# show consistency-checker objects l2m_group
Process: IOSD
  Run-id   Start-time           Exception
  ----   -
  1       2021/02/17 05:20:42    0
  2       2021/02/17 06:19:05    0

Process: FMAN-FP
*Statistics (A/I/M/S/Oth): Actual/Inherited/Missing/Stale/Others

  Run-id   Start-time           State          A/  I/  M/  S/Oth
  ----   -
  1       2021/02/17 05:20:42    Consistent    0/  0/  0/  0/  0
  2       2021/02/17 06:19:05    Consistent    0/  0/  0/  0/  0

Process: FED
*Statistics (A/I/M/S/HW/Oth): Actual/Inherited/Missing/Stale/Hardware/Others

  Run-id   Start-time           State          A/  I/  M/  S/  HW/Oth
  ----   -
  1       2021/02/17 05:20:42    Consistent    0/  0/  0/  0/  0/  0
  2       2021/02/17 06:19:05    Inconsistent   4/  0/  2/  0/  0/  0

Device#
```



## show consistency-checker run-id

整合性チェッカを実行し、実行 ID によってソフトウェアエントリの不整合状態を検出するには、特権 EXEC モードで **show consistency-checker run-id run-id** コマンドを実行します。

**show consistency-checker run-id run-id [ detail | status ]**

### 構文の説明

*run-id* 実行 ID を指定します。

**detail** 実行 ID の詳細な出力を表示します。

**status** チェッカの完了ステータスを表示します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### コマンドモード

特権 EXEC (#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Bengaluru 17.6.1	このコマンドが導入されました。

### 使用上のガイドライン

整合性チェッカには次の制限事項があります。

- 整合性チェッカを中断または終了するコマンドはありません。完全なレポートが表示されると停止します。
- FEDハードウェアチェックは部分的に実装されています。プログラミングハードウェアのエラーのみが報告されます。
- 誤検出のケース：整合性チェッカが実行されており、多数の機能テーブルエントリの削除/追加/変更アクションが発生した場合（**clear \***または**relearn**によってトリガーされた場合）、整合性チェッカはプロセス間で一貫性のないエントリまたは欠落したエントリを報告することがあります。また、テーブルエントリに多数の変更が加えられたために、古いレポートをオフにすることもあります。

### 例

次に、**show consistency-checker run-id run-id** コマンドの出力例を示します。

```
Device# show consistency-checker run-id 6
Process: IOSD
Flags:    F - Full Table Scan, S - Single Entry Run
          RE - Recursive Check, GD - Garbage Detector
          Hw - Hardware Check, HS - Hardware Shadow Copy
Object-Type  Start-time           Entries  Exceptions  Flags
l2m_vlan    2021/07/19 15:19:41    30      0           F Hw HS
l2m_group   2021/07/19 15:19:42    10      0           F Hw HS

Process: FMAN-FP
```

## show consistency-checker run-id

\*Statistics (A/I/M/S/Oth) : Actual/Inherited/Missing/Stale/Others

Object-Type	Start-time	State	A/	I/	M/	S/Oth
l2m_vlan	2021/07/19 15:19:41	Consistent	0/	0/	0/	0/ 0
l2m_group	2021/07/19 15:19:42	Consistent	0/	0/	0/	0/ 0

Process: FED

\*Statistics (A/I/M/S/HW/Oth) : Actual/Inherited/Missing/Stale/Hardware/Others

Object-Type	Start-time	State	A/	I/	M/	S/	HW/Oth
l2m_vlan	2021/07/19 15:19:41	Consistent	0/	0/	0/	0/	0/ 0
l2m_group	2021/07/19 15:19:42	Consistent	0/	0/	0/	0/	0/ 0

Device#

次に、**show consistency-checker run-id run-id status** コマンドの出力例を示します。

Device# **show consistency-checker run-id 6 status**

Process: IOSD

Object-Type	Status	Time (sec)	Exceptions
l2m_vlan	Completed	13	No
l2m_group	Completed	13	No

Process: FMAN-FP

Object-Type	Status	Time (sec)	State
l2m_vlan	Completed	12	Consistent
l2m_group	Completed	11	Consistent

Process: FED

Object-Type	Status	Time (sec)	State
l2m_vlan	Completed	12	Consistent
l2m_group	Completed	11	Consistent

Device#

# show debug

スイッチで使用できるすべての debug コマンドを表示するには、特権 EXEC モードで **show debug** コマンドを使用します。

## show debug

**show debug condition** *Condition identifier* | *All conditions*

### 構文の説明

*Condition identifier* 使用される条件識別子の値を設定します。範囲は、1～1000です。

*All conditions* 使用可能なすべての条件付きデバッグ オプションを表示します。

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

特権 EXEC

### コマンド履歴

リリース	変更内容
Cisco IOS XE リリース 16.1	このコマンドが導入されました。

### 使用上のガイドライン

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。さらに、**debug** コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用するのが最良です。このような時間帯を選んでデバッグを実行すると、**debug** コマンドの処理の負担によってシステム利用が影響を受ける可能性が少なくなります。

### 例

次に、**show debug** コマンドの出力例を示します。

```
Device# show debug condition all
```

デバッグを無効にするには、**no debug all** コマンドを使用します。

## show env xps

Cisco eXpandable Power System (XPS) 2200 のバジェット配分、設定、電力、およびシステム電源情報を表示するには、特権 EXEC モードで **show env xps** コマンドを使用します。

```
show env xps { budgeting | configuration | port [ all | number ] | power | system
| thermal | upgrade | version }
```

### 構文の説明

<b>budgeting</b>	XPS 電力バジェットの配分（電源スタックに含まれるすべてのスイッチに対する電力の割り当て量とバジェット量）を表示します。
<b>configuration</b>	power xps 特権 EXEC コマンドを実行した結果の設定を表示します。XPS 設定は XPS に保存されます。show env xps configuration コマンドを入力すると、デフォルト以外の設定が取得されます。
<b>port</b> [all   number ]	すべてのポートまたは指定の XPS ポートの設定とステータスを表示します。ポート番号は、1～9 です。
<b>power</b>	XPS 電源装置のステータスを表示します。
<b>system</b>	XPS システム ステータスを表示します。
<b>thermal</b>	XPS 温度ステータスを表示します。
<b>upgrade</b>	XPS アップグレード ステータスを表示します。
<b>version</b>	XPS バージョンの詳細を表示します。

### コマンドモード

特権 EXEC

### コマンド履歴

リリース 変更内容

12.2(55)SE1 このコマンドが導入されました。

### 使用上のガイドライン

XPS 2200 の情報を表示するには、**show env xps** 特権 EXEC コマンドを使用します。

### 例

次に、show env xps budgeting コマンドの出力例を示します。

```
Switch#
=====
```

```
XPS 0101.0100.0000 :
=====
```

```

Data          Current   Power   Power Port  Switch #  PS A  PS B  Role-State
Committed
Budget
-----  -----  -----  -----  -----  -    -    715  SP-PS
      223
      1543
2      -      -      -      SP-PS      223      223
3      -      -      -      -          -          -
4      -      -      -      -          -          -
5      -      -      -      -          -          -
6      -      -      -      -          -          -
7      -      -      -      -          -          -
8      -      -      -      -          -          -
9      1      1100  -      RPS-NB     223      070
XPS   -      -      1100  -          -          -

```

次に、show env xps configuration コマンドの出力例を示します。

```

Switch# show env xps configuration
=====
XPS 0101.0100.0000 :
=====
power xps port 4 priority 5
power xps port 5 mode disable
power xps port 5 priority 6
power xps port 6 priority 7
power xps port 7 priority 8
power xps port 8 priority 9
power xps port 9 priority 4

```

次に、show env xps port all コマンドの出力例を示します。

```

Switch#
XPS 010

-----
Port name      : -
Connected      : Yes
Mode           : Enabled (On)
Priority       : 1
Data stack switch # : - Configured role      : Auto-SP
Run mode       : SP-PS : Stack Power Power-Sharing Mode
Cable faults   : 0x0 XPS 0101.0100.0000 Port 2
-----
Port name      : -
Connected      : Yes
Mode           : Enabled (On)
Priority       : 2
Data stack switch # : - Configured role      : Auto-SP
Run mode       : SP-PS : Stack Power Power-Sharing Mode
Cable faults   : 0x0 XPS 0101.0100.0000 Port 3
-----
Port name      : -
Connected      : No
Mode           : Enabled (On)
Priority       : 3
Data stack switch # : - Configured role      : Auto-SP Run mode      : -
Cable faults   :
<output truncated>

```

次に、show env xps power コマンドの出力例を示します。

```

=====
XPS 0101.0100.0000 :
=====
Port-Supply SW PID                               Serial#      Status      Mode Watts
-----
XPS-A                Not present
XPS-B                NG3K-PWR-1100WAC  LIT13320NTV OK           SP   1100
1-A                  - -              -            -
1-B                  - -              -            -           SP   715
2-A                  - -              -            -
2-B                  - -              -            -
9-A                  100WAC          LIT141307RK OK           RPS  1100
9-B                  esent

```

次に、show env xps system コマンドの出力例を示します。

```

Switch#
=====

XPS 0101.0100.0000 :
=====
XPS                Cfg Cfg      RPS Switch Current  Data Port  XPS Port Name
-----
Mode Role      Pri Conn  Role-State Switch #
-----
1    -          -          On  Auto-SP  1  Yes  SP-PS  -
2    -          -          On  Auto-SP  2  Yes  SP-PS  -
3    -          -          On  Auto-SP  3  No   -      -
4    none       -          On  Auto-SP  5  No   -      -
5    -          -          Off Auto-SP  6  No   -      -
6    -          -          On  Auto-SP  7  No   -      -
7    -          -          On  Auto-SP  8  No   -      -
8    -          -          On  Auto-SP  9  No   -      -
9    test       -          On  Auto-SP  4  Yes  RPS-NB

```

次に、show env xps thermal コマンドの出力例を示します。

```

Switch#
=====

XPS 0101.0100.0000 :
=====
Fan  Status
----  -----
1    OK
2    OK
3    NOT PRESENT PS-1  NOT PRESENT PS-2  OK Temperature is OK

```

次に、アップグレードが実行されていない場合の show env xps upgrade コマンドの出力例を示します。

```

Switch# show env xps upgrade
No XPS is connected and upgrading.

```

次に、アップグレードが進行中の場合の show env xps upgrade コマンドの出力例を示します。

```

Switch# show env xps upgrade
XPS Upgrade Xfer

SW Status Prog
--  -----  ----

```

```

1 Waiting 0%
Switch#
*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has
started through the Service Port.
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- -----
1 Receiving 1%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- -----
1 Receiving 5%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- -----
1 Reloading 100%
Switch#
*Mar 22 03:16:01.733: %PLATFORM_XPS-6-UPGRADE_DONE: XPS 0022.bdd7.9b14 upgrade has
completed and the XPS is reloading.

```

次に、show env xps version コマンドの出力例を示します。

```

Switch# show env xps version
=====
XPS 0022.bdd7.9b14:
=====
Serial Number: FDO13490KUT
Hardware Version: 8
Bootloader Version: 7
Software Version: 18

```

表 2: 関連コマンド

コマンド	説明
power xps (グローバル コンフィギュレーション コマンド)	XPS と XPS ポートの名前を設定します。
power xps (特権 EXEC コマンド)	XPS ポートとシステムを設定します。

# show flow monitor

フローモニタのステータスと統計情報を表示するには、特権 EXEC モードで **show flow monitor** コマンドを使用します。

## 構文の説明

<b>name</b>	(任意) フローモニタの名前を指定します。
<b>monitor-name</b>	(任意) 事前に設定されたフローモニタの名前。
<b>cache</b>	(任意) フローモニタのキャッシュの内容を表示します。
<b>format</b>	(任意) ディスプレイ出力のフォーマットオプションのいずれかを使用することを指定します。
<b>csv</b>	(任意) フローモニタのキャッシュの内容をカンマ区切り値 (CSV) 形式で表示します。
<b>record</b>	(任意) フローモニタのキャッシュの内容をレコード形式で表示します。
<b>table</b>	(任意) フローモニタのキャッシュの内容を表形式で表示します。
<b>statistics</b>	(任意) フローモニタの統計情報を表示します。

## コマンドモード

特権 EXEC

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

**cache** キーワードでは、デフォルトでレコード形式が使用されます。

**show flowmonitor monitor-name cache** コマンドのディスプレイ出力に含まれる大文字のフィールド名は、フローの識別に使用するキーフィールドです。**show flow monitor monitor-name cache** コマンドのディスプレイ出力に含まれる小文字のフィールド名は、がキャッシュの追加データとして値を収集する非キーフィールドです。

## 例

次の例では、フローモニタのステータスを表示します。

```
# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:      Used for basic traffic analysis
  Flow Record:      flow-record-1
  Flow Exporter:    flow-exporter-1
                   flow-exporter-2

Cache:
  Type:             normal
  Status:           allocated
  Size:             4096 entries / 311316 bytes
  Inactive Timeout: 15 secs
```



```
Active Timeout: 1800 secs
```

次の表で、この出力に表示される重要なフィールドを説明します。

表 3: *show flow monitor monitor-name* フィールドの説明

フィールド	Description
Flow Monitor	設定したフロー モニタの名前。
Description	モニタに設定した説明、またはユーザ定義のデフォルトの説明。
Flow Record	フロー モニタに割り当てられたフロー レコード。
Flow Exporter	フロー モニタに割り当てられたエクスポータ。
Cache	フロー モニタのキャッシュに関する情報。
Type	フロー モニタのキャッシュ タイプ。この値は常に <b>normal</b> となります。これが唯一サポートされているキャッシュ タイプです。
Status	フロー モニタのキャッシュのステータス。 次の値が可能です。 <ul style="list-style-type: none"> <li>• <b>allocated</b> : キャッシュが割り当てられています。</li> <li>• <b>being deleted</b> : キャッシュが削除されています。</li> <li>• <b>not allocated</b> : キャッシュが割り当てられていません。</li> </ul>
Size	現在のキャッシュ サイズ。
Inactive Timeout	非アクティブ タイムアウトの現在の値 (秒単位)。
Active Timeout	アクティブ タイムアウトの現在の値 (秒単位)。

次の例では、**FLOW-MONITOR-1** という名前のフロー モニタのステータス、統計情報、およびデータを表示します。

次の表で、この出力に表示される重要なフィールドを説明します。

次の例では、**FLOW-MONITOR-1** という名前のフロー モニタのステータス、統計情報、およびデータを表形式で表示します。

次の例では、**FLOW-MONITOR-IPv6** という名前のフロー モニタ (キャッシュに IPv6 データを格納) のステータス、統計情報、およびデータをレコード形式で表示します。

次の例では、フロー モニタのステータスと統計情報を表示します。

# show idprom module

特定のモジュールの識別プログラム可能読み取り専用メモリ (IDPROM) 情報を表示するには、特権 EXEC モードで **show idprom module** コマンドを使用します。

**show idprom module** *slot-number* **eprom** [ **detail** | **dump** ]

構文の説明	<i>slot-number</i>	スロット番号を指定します。
	<b>eprom</b>	EEPROM 情報を指定します。
	<b>detail</b>	(任意) 詳細な EEPROM 情報を指定します。
	<b>dump</b>	(任意) EEPROM 情報を 16 進数または ASCII の形式で指定します。
コマンドモード	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

次に、**show idprom module** コマンドの出力例を示します。

```
Device# show idprom module 1 eeprom detail
Slot 1 EEPROM data:

EEPROM version           : 4
Compatible Type          : 0xFF
Controller Type          : 3481
Hardware Revision         : 0.5
PCB Part Number           : 73-18351-03
Board Revision            : 03
Deviation Number          : 0
Fab Version               : 03
PCB Serial Number         : CAT2232L0ND
RMA Test History          : 00
RMA Number                 : 0-0-0-0
RMA History                : 00
Top Assy. Part Number     : 068-101548-01
Top Assy. Revision        : 11
CLEI Code                  : UNDEFINED
ECI Number                 : 0
Product Identifier (PID)  : C9600-LC-48YL
Version Identifier (VID)  : V00
Base MAC Address           : 78 72 5D EC 6C 00
MAC Address block size    : 128
Environment Monitor Data  : 06 00 00 00 0E 60 E6 00
                           A6
Environment Monitor Data  : 00 06 00 FA
Manufacturing Test Data   : 00 00 00 00 00 00 00 00
Field Diagnostics Data    : 00 00 00 00 00 00 00 00
Platform features         : 00 00 00 00 00 00 00 00
                           00 00 00 00 00 00 00 00
```

```
00 00 00 00 00 00 00 00 00
Environment Monitor Data :
Description                : InltFrnt
Shutdown threshold        : 060
Critical threshold        : 055
Major threshold           : 050
Minor threshold           : 045
Environment Monitor Data :
Description                : InltRear
Shutdown threshold        : 060
Critical threshold        : 055
Major threshold           : 050
Minor threshold           : 045
Environment Monitor Data :
Description                : OtltFrnt
Shutdown threshold        : 090
Critical threshold        : 085
Major threshold           : 080
Minor threshold           : 075
Environment Monitor Data :
Description                : OtltRear
Shutdown threshold        : 090
Critical threshold        : 085
Major threshold           : 080
Minor threshold           : 075
```

# show install

インストールパッケージに関する情報を表示するには、特権 EXEC モードで **show install** コマンドを使用します。

**show install active | committed | inactive | log | package bootflash: | flash: | webui: | rollback | summary | uncommitted**

構文の説明	<b>active</b>	アクティブなパッケージに関する情報を表示します。
	<b>committed</b>	永続的なパッケージのアクティベーションを表示します。
	<b>inactive</b>	非アクティブなパッケージを表示します。
	<b>log</b>	ログインストールバッファに格納されているエントリを表示します。
	<b>package</b>	説明、再起動情報、パッケージ内のコンポーネントなど、パッケージに関するメタデータ情報を表示します。
	<b>{bootflash:   flash:   harddisk:   webui:}</b>	インストールパッケージのロケーションを指定します。
	<b>rollback</b>	保存されているインストールに関連付けられたソフトウェアセットを表示します。
	<b>summary</b>	アクティブ、非アクティブ、コミット済み、廃止されたパッケージのリストに関する情報を表示します。
	<b>uncommitted</b>	非永続的なパッケージのアクティベーションを表示します。
コマンドモード	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが追加されました。

使用上のガイドライン インストールパッケージのステータスを表示するには、**show** コマンドを使用します。

## 例

次に、**show install package** コマンドの出力例を示します。

```
Device# show install package bootflash:cat3k-universalk9.2017-01-10_13.15.1.
CSCxxx.SSA.dmp.bin
Name: cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SS
Version: 16.6.1.0.199.1484082952..Everest
Platform: Catalyst3k
Package Type: dmp
Defect ID: CSCxxx
Package State: Added
Supersedes List: {}
Smu ID: 1
```

次に、**show install summary** コマンドの出力例を示します。

```
Device# show install summary

Active Packages:
  bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Inactive Packages:
  No packages
Committed Packages:
  bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Uncommitted Packages:
  No packages
Device#
```

下の表に、ディスプレイ内に表示される重要なフィールドのリストを示します。

表 4: *show install summary* フィールドの説明

フィールド	Description
Active Packages	アクティブなインストールパッケージの名前。
Inactive Packages	非アクティブなパッケージのリスト。
Committed Packages	変更がリロード以降も存続するように、ハードディスクに変更を保存またはコミットしたインストールパッケージ。
Uncommitted Packages	非永続的なインストールパッケージのアクティベーション。

次に、**show install log** コマンドの出力例を示します。

```
Device# show install log

[0|install_op_boot]: START Fri Feb 24 19:20:19 Universal 2017
[0|install_op_boot]: END SUCCESS Fri Feb 24 19:20:23 Universal 2017
[3|install_add]: START Sun Feb 26 05:55:31 UTC 2017
[3|install_add( FATAL)]: File path (scp) is not yet supported for this command
[4|install_add]: START Sun Feb 26 05:57:04 UTC 2017
[4|install_add]: END SUCCESS
/bootflash/cat3k-universalk9.2017-01-10_13.15.1.CSCvb12345.SSA.dmp.bin
Sun Feb 26 05:57:22 UTC 2017
```

## show install

```
[5|install_activate]: START Sun Feb 26 05:58:41 UTC 2017
```

## 関連コマンド

コマンド	Description
<b>install</b>	SMUパッケージをインストールします。

## show license all

すべてのライセンス情報を表示するには、特権 EXEC モードで **show license all** コマンドを入力します。このコマンドは、ステータス、承認、UDI、および使用状況の情報をすべて組み合わせて表示します。

### show license all

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンド デフォルト

特権 EXEC (#)

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	<p>コマンド出力が更新され、ポリシーを使用したスマートライセンスに関する情報が表示されるようになりました。</p> <p>コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。</p>
Cisco IOS XE Cupertino 17.7.1	<p>コマンドの出力が強化され、次の情報が表示されるようになりました。</p> <ul style="list-style-type: none"> <li>• RUM レポートの統計情報 ([Usage Report Summary] セクション)。</li> <li>• [Account Information] セクションにあるスマートアカウントとバーチャルアカウントの情報。</li> </ul>

#### 使用上のガイドライン

このコマンドは、他の **show license** コマンドの出力を連結して、さまざまな種類のライセンス情報をまとめて表示できるようにします。フィールドの説明については、対応するコマンドを参照してください。

**スマートライセンス**：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されず（スマートライセンスが有効になっているかどうか、関連するすべてのライセンス証明書、コンプライアンスステータスなど）。

**ポリシーを使用したスマートライセンス**：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

- [Smart Licensing Status] セクションは、**show license status** コマンドの出力に対応しています。
- [License Usage] セクションは、**show license usage** コマンドの出力に対応しています。
- [Product Information] セクションは、**show license udi** コマンドの出力に対応しています。
- **show license all** コマンドの [Agent Version] セクションには、スマートエージェントのバージョンが表示され、このコマンドでのみ使用できます。
- [License Authorizations] セクションは、**show license authorization** コマンドの出力に対応しています。
- [Usage Report Summary] セクションは、**show license tech** コマンドの出力に対応しています。

### 例

- [ポリシーを使用したスマートライセンスの show license all \(Cisco Catalyst 9300 シリーズスイッチ\) \(112 ページ\)](#)
- [ポリシーを使用したスマートライセンスの show license all \(Cisco Catalyst 9500 シリーズスイッチ\) \(115 ページ\)](#)
- [#unique\\_961 unique\\_961\\_Connect\\_42\\_section\\_zlh\\_2xn\\_nnb](#)

### ポリシーを使用したスマートライセンスの show license all (Cisco Catalyst 9300 シリーズスイッチ)

次に、スタック構成セットアップの **show license all** コマンドの出力例を示します。スタック内のすべての製品インスタンスは C9300X スイッチであり、Cisco IOS XE Bengaluru 17.6.2 以降、Export Control Key for High Security (HSECK9) をサポートしています。ここでは HSECK9 キーが使用され、必要なスマートライセンス承認コード (SLAC) がインストールされています (SMART AUTHORIZATION は 2021 年 10 月 29 日 17:45:28 UTC にインストールされました)。

```
Device# show license all

Smart Licensing Status
=====

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
```



```
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: cslu
Cslu address: <empty>
Proxy:
Not Configured

Miscellaneous:
Custom Id: <empty>

Policy:
Policy in use: Installed On Oct 29 17:44:15 2021 UTC
Policy name: Custom Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 365 (Customer Policy)
Reporting frequency (days): 0 (Customer Policy)
Report on change (days): 90 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 90 (Customer Policy)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)

Usage Reporting:
Last ACK received: Oct 29 17:48:51 2021 UTC
Next ACK deadline: Jan 27 17:48:51 2022 UTC
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Oct 29 18:32:43 2021 UTC
Last report push: Oct 29 17:44:50 2021 UTC
Last report file write: <none>

Trust Code Installed:
Active: PID:C9300X-24HX,SN:FOC2519L8R7
INSTALLED on Oct 29 17:44:15 2021 UTC
Standby: PID:C9300X-48HXN,SN:FOC2524L39P
INSTALLED on Oct 29 17:44:15 2021 UTC
Member: PID:C9300X-48HX,SN:FOC2516LC92
INSTALLED on Oct 29 17:44:15 2021 UTC

License Usage
=====

network-advantage (C9300-24 Network Advantage):
Description: C9300-24 Network Advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: C9300-24 Network Advantage
Enforcement type: NOT ENFORCED
License type: Perpetual
```

```
dna-advantage (C9300-24 DNA Advantage):
  Description: C9300-24 DNA Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9300-24 DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription

network-advantage (C9300-48 Network Advantage):
  Description: C9300-48 Network Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9300-48 Network Advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual

dna-advantage (C9300-48 DNA Advantage):
  Description: C9300-48 DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9300-48 DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription

hseck9 (Cat9K HSEC):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual

Product Information
=====
UDI: PID:C9300X-24HX,SN:FOC2519L8R7

HA UDI List:
  Active:PID:C9300X-24HX,SN:FOC2519L8R7
  Standby:PID:C9300X-48HXN,SN:FOC2524L39P
  Member:PID:C9300X-48HX,SN:FOC2516LC92

Agent Version
=====
Smart Agent for Licensing: 5.1.23_rel/104

License Authorizations
=====
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
    Status: SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC
    Last Confirmation code: 6746c5b5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
```

```
Status: NOT INSTALLED
Member: PID:C9300X-48HX,SN:FOC2516LC92
Status: NOT INSTALLED

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

### ポリシーを使用したスマートライセンスの **show license all** (Cisco Catalyst 9500 シリーズスイッチ)

次に、Cisco Catalyst 9500 スイッチでの **show license all** コマンドの出力例を示します。この製品インスタンスで実行されているソフトウェアバージョンは、Cisco IOS XE Cupertino 17.7.1 です。同様の出力が、すべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license all

Smart Licensing Status
=====

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: <none>
  Virtual Account: <none>

Data Privacy:
  Sending Hostname: no
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured
```

## show license all

```

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Mar 30 22:32:22 2020 EST
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Oct 19 04:39:08 2021 EST
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>

License Usage
=====

network-advantage (C9500 Network Advantage):
  Description: C9500 Network Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9500 Network Advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual

dna-advantage (C9500-40X DNA Advantage):
  Description: C9500-40X DNA Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9500-40X DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription

Product Information
=====
UDI: PID:C9500-40X,SN:FCW2227A4NC

Agent Version

```

```

=====
Smart Agent for Licensing: 5.3.9_rel/22

License Authorizations
=====
Overall status:
  Active: PID:C9500-40X,SN:FCW2227A4NC
         Status: NOT INSTALLED

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
  regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c

  Entitlement Tag:
  regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9

Usage Report Summary:
=====
Total: 26, Purged: 0
Total Acknowledged Received: 0, Waiting for Ack: 0
Available to Report: 26 Collecting Data: 2

```

## 関連コマンド

コマンド	Description
<b>show license status</b>	ライセンスのコンプライアンスステータスを表示します。
<b>show license authorization</b>	許可コード関連情報を表示します。
<b>show license summary</b>	すべてのアクティブなライセンスの要約を表示します。
<b>show license udi</b>	UDI を表示します。
<b>show license usage</b>	ライセンス使用情報を表示します。
<b>show license tech support</b>	デバッグ出力を表示します。

# show license authorization

ライセンス（輸出規制および適用）の承認関連情報を表示するには、特権 EXEC モードで **show license authorization** コマンドを入力します。

## show license authorization

このコマンドには引数またはキーワードはありません。

コマンドモード	特権 EXEC (Device#)
---------	-------------------

コマンド履歴	リリース	変更内容
	Cisco IOS XE Amsterdam 17.3.2a	このコマンドが導入されました。

使用上のガイドライン	承認コードに関する情報を表示するには、このコマンドを使用します。これには、SLR 承認コードとスマートライセンス承認コード (SLAC) が含まれます。
------------	--

## 例

ディスプレイに表示されるフィールドについては、[表 5 : show license authorization のフィールドの説明 \(119 ページ\)](#) を参照してください。

出力例については、次を参照してください。

- [SLAC の表示 \(122 ページ\)](#)
- [SLR 承認コードの表示 \(122 ページ\)](#)。

表 5: show license authorization のフィールドの説明

フィールド	説明
Overall Status	設定内にあるすべての製品インスタンスの UDI 情報のヘッダー、インストールされている承認のタイプ、および設定エラー（存在する場合）。高可用性設定では、設定内にあるすべての UDI がリストされます。
Active: ステータス :	アクティブ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
Standby: ステータス :	スタンバイ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
Member: ステータス :	メンバー製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。 承認コードがインストールされていることを示すステータスであり、確認コードがある場合は、これも表示されます。
ERROR:	高可用性設定の設定エラーまたは不一致（存在する場合）。

フィールド	説明
承認	<p>詳細なライセンス承認情報のヘッダー。すべてのライセンス、その適用タイプ、および有効期間が表示されます。承認またはモードがアクティブにインストールされているものと一致しない場合、製品インスタンスごとにエラーが表示されます。</p> <p>このセクションは、製品インスタンスが承認コードを必要とするライセンスを使用している場合にのみ表示されます。</p>
():	ライセンス名およびライセンス名の短縮形。
説明	ライセンスの説明。
Total available count:	<p>使用可能なライセンスの合計数。</p> <p>これには、高可用性設定のすべての製品インスタンスに関して、期限切れのサブスクリプションライセンスを含む、すべての期間のライセンス（永久ライセンスおよびサブスクリプション）が含まれます。</p>
Enforcement type	<p>ライセンスの適用タイプ。これは、次のいずれかです。</p> <ul style="list-style-type: none"> <li>• 適用</li> <li>• 非適用</li> <li>• 輸出規制</li> </ul>
Term information:	



フィールド	説明												
	<p>ライセンス期間情報を提供するヘッダー。このヘッダーには、次のフィールドが含まれることがあります。</p> <ul style="list-style-type: none"> <li>• <b>Active</b> : アクティブ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。</li> <li>• <b>Authorization type</b> : インストールされている承認コードのタイプとインストール日。タイプは、SLAC、UNIVERSAL、SPECIFIED、PAK、RTU です。</li> <li>• <b>Start Date</b> : ライセンスが特定の期間または時間の場合に、有効期間の開始日を表示します。</li> <li>• <b>Start Date</b> : ライセンスが特定の期間または時間の場合に、有効期間の終了日を表示します。</li> <li>• <b>Term Count</b> : ライセンス数。</li> <li>• <b>Subscription ID</b> : ライセンスが特定の期間または時間の場合に、ID を表示します。</li> <li>• <b>License type</b> : ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。</li> <li>• <b>Standby</b> : スタンバイ製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。</li> <li>• <b>Member</b> : メンバー製品インスタンス UDI と、それに続いてこの UDI の承認コードインストールのステータス。</li> </ul>												
Purchased Licenses	<p>ライセンス購入情報のヘッダー。</p> <table border="1" data-bbox="639 1423 1515 1814"> <tbody> <tr> <td data-bbox="639 1423 860 1484">Active:</td> <td data-bbox="860 1423 1515 1484">アクティブ製品インスタンスとその UDI。</td> </tr> <tr> <td data-bbox="639 1484 860 1545">Count:</td> <td data-bbox="860 1484 1515 1545">ライセンス数。</td> </tr> <tr> <td data-bbox="639 1545 860 1606">Description:</td> <td data-bbox="860 1545 1515 1606">ライセンスの説明。</td> </tr> <tr> <td data-bbox="639 1606 860 1707">License type:</td> <td data-bbox="860 1606 1515 1707">ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。</td> </tr> <tr> <td data-bbox="639 1707 860 1768">Standby:</td> <td data-bbox="860 1707 1515 1768">スタンバイ製品インスタンスの UDI。</td> </tr> <tr> <td data-bbox="639 1768 860 1814">Member:</td> <td data-bbox="860 1768 1515 1814">メンバー製品インスタンスの UDI。</td> </tr> </tbody> </table>	Active:	アクティブ製品インスタンスとその UDI。	Count:	ライセンス数。	Description:	ライセンスの説明。	License type:	ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。	Standby:	スタンバイ製品インスタンスの UDI。	Member:	メンバー製品インスタンスの UDI。
Active:	アクティブ製品インスタンスとその UDI。												
Count:	ライセンス数。												
Description:	ライセンスの説明。												
License type:	ライセンス継続期間。これは、SUBSCRIPTION または PERPETUAL です。												
Standby:	スタンバイ製品インスタンスの UDI。												
Member:	メンバー製品インスタンスの UDI。												

## SLAC の表示

次に、C9300X モデルスイッチでの **show license authorization** コマンドの出力例を示します。ここで、SLAC はスタック構成セットアップのアクティブな製品インスタンスにのみインストールされます。

```
Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
    Status: SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC
    Last Confirmation code: 6746c5b5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
    Status: NOT INSTALLED
  Member: PID:C9300X-48HX,SN:FOC2516LC92
    Status: NOT INSTALLED

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Authorization type: SMART AUTHORIZATION INSTALLED
      License type: PERPETUAL
      Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

## SLR 承認コードの表示

次に、SLR 承認コード（最終確認コード:）を示す **show license authorization** コマンドの出力例を示します。SLR 承認コードは、Smart Licensing Using Policy へのアップグレード後にサポートされます。既存の SLR はアップグレード後に引き継がれますが、ポリシーを使用したスマートライセンシング環境で新しい SLR を要求することはできません。完全に外部との接続性がないネットワーク内にいる場合は、代わりに CSSM への接続なし、CSLU なしのトポロジが適用されます。

```
Device# show license authorization

Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
    Status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
    Last Confirmation code: 184ba6d6
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
    Status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
    Last Confirmation code: 961d598f

Specified license reservations:
  C9500 Network Advantage (C9500 Network Advantage):
    Description: C9500 Network Advantage
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Term Count: 1
```

```
Standby: PID:C9500-16X,SN:FCW2233A5ZY
  Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
  License type: PERPETUAL
  Term Count: 1
C9500-DNA-16X-A (C9500-16X DNA Advantage):
  Description: C9500-DNA-16X-A
  Total reserved count: 2
  Enforcement type: NOT ENFORCED
  Term information:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
    Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
    License type: PERPETUAL
    Term Count: 1
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
    Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
    License type: PERPETUAL
    Term Count: 1

Purchased Licenses:
  No Purchase Information Available

Derived Licenses:
  Entitlement Tag:
  regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c

  Entitlement Tag:
  regid.2017-07.com.cisco.C9500-DNA-16X-A,1.0_ef3574d1-156b-486a-864f-9f779ff3ee49
```

# show license data translation

ライセンスデータ転換情報を表示するには、特権 EXEC モードで **show license data** コマンドを入力します。

## show license data conversion

### 構文の説明

このコマンドには、引数またはキーワードはありません。

### コマンドモード

特権 EXEC (Device#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに関する情報が表示されるようになりました。 コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。

### 使用上のガイドライン

**スマートライセンス**：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

**ポリシーを使用したスマートライセンス**：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

デバイス主導の変換は、Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチではサポートされていません。

## show license eventlog

ポリシーを使用したスマートライセンスに関連するイベントログを表示するには、特権 EXEC モードで **show license eventlog** コマンドを入力します。

**show license eventlog** [ *days* ]

### 構文の説明

*days* イベントログを表示する日数を入力します。0 ~ 2147483647 の範囲の値を指定できません。

### コマンドモード

特権 EXEC (Device#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	<p>ポリシーを使用したスマートライセンスの導入により、次のイベントが追加されました。</p> <ul style="list-style-type: none"> <li>• ポリシーのインストールと削除</li> <li>• 承認コードの要求、インストール、および削除。</li> <li>• 信頼コードのインストールと削除。</li> <li>• ライセンス使用状況に関する承認ソース情報の追加。</li> </ul>

### 使用上のガイドライン

**スマートライセンス**：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

**ポリシーを使用したスマートライセンス**：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

#### 例

ポリシーを使用したスマートライセンスの [show license eventlog for One Day](#) (125 ページ)

ポリシーを使用したスマートライセンスの [show license eventlog for All Events](#) (126 ページ)

#### ポリシーを使用したスマートライセンスの show license eventlog for One Day

次に、Cisco Catalyst 9500 スイッチでの **show license eventlog** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。このコマンドは、1 日分のイベントを表示するように設定されています。

```

Device# show license eventlog 1
**** Event Log ****

2020-09-11 00:50:17.693 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
air-network-advantage,air-dna-advantage"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 00:50:50.175 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-11 08:50:17.694 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
air-network-advantage,air-dna-advantage"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 08:50:52.804 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"

```

### ポリシーを使用したスマートライセンスの show license eventlog for All Events

次に、Cisco Catalyst 9500 スイッチでの **show license eventlog** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。このコマンドは、すべてのイベントを表示するように設定されています。

```

Device# show license eventlog
**** Event Log ****

2020-09-01 15:43:42.300 UTC SAEVT_INIT_START version="4.13.14_rel/41"
2020-09-01 15:43:42.301 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization
has not been completed"
2020-09-01 15:43:42.301 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHarmfRegister"
2020-09-01 15:43:45.055 UTC SAEVT_READY
2020-09-01 15:43:45.055 UTC SAEVT_ENABLED
2020-09-01 15:43:45.088 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_LICENSE_USAGE count="0" type="destroy"
entitlementTag="regid.2018-01.com.cisco.C9500-24Y4C-A,1.0_6b065611-6552-472a-8859-ab3339550166"
2020-09-01 15:43:45.098 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"

```

## show license history message

製品インスタンスと CSSM または CSLU（該当する場合）の間の通信履歴を表示するには、特権 EXEC モードで **show license history message** コマンドを入力します。このコマンドの出力は、テクニカルサポートチームがトラブルシューティングに使用します。

### show license history message

#### 構文の説明

このコマンドにはキーワードまたは引数はありません。

#### コマンドモード

特権 EXEC (Device#)

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.2a	このコマンドが導入されました。

#### 使用上のガイドライン

解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra all** 特権 EXEC コマンドの出力例を提供してください。

## show license reservation

ライセンス予約情報を表示するには、特権 EXEC モードで **show license reservation** コマンドを入力します。

### show license reservation

このコマンドには引数またはキーワードはありません。

#### コマンドモード

特権 EXEC (Device#)

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンドは CLI で引き続き使用できますが、予約の概念がポリシーを使用したスマートライセンス環境に存在しないため、適用できません。

#### 使用上のガイドライン

コマンドは CLI で引き続き使用可能であり、対応する出力が表示されますが、ポリシーを使用したスマートライセンシングの導入により、予約の概念は適用されなくなりました。代わりに、特権 EXEC モードで **show license all** コマンドを使用して、移行された SLR ライセンスを表示します (SLR 承認コードはポリシーを使用してスマートライセンスに移行されます)。



## show license status

データプライバシー、ポリシー、転送、使用状況レポート、信頼コードなどのライセンス設定に関する情報を表示するには、特権 EXEC モードで **show license status** コマンドを入力します。

### show license status

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンドデフォルト

特権 EXEC (#)

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに適用可能な新しいフィールドが反映されました。これには、Trust code installed:、Policy in use、Policy name: 、ポリシーと同様のレポート要件、および使用状況レポートに関連するフィールドが含まれます。  コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。
Cisco IOS XE Cupertino 17.7.1	コマンド出力が更新され、スマートアカウントと仮想アカウントの情報が表示されるようになりました。

#### 使用上のガイドライン

**スマートライセンス** : デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

**ポリシーを使用したスマートライセンス** : デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

#### 出力のアカウント情報

Cisco IOS XE Cupertino 17.7.1 以降、すべての ACK には、CSSM で報告されたスマートアカウントとバーチャルアカウントが含まれています。ACK を受信すると、製品インスタンスにはこの情報の最新バージョンのみが安全に保存されます。これは、ACK のタイムスタンプによって決定されます。したがって、このコマンドの出力の [Account Information] セクションに表示されるスマートアカウントとバーチャルアカウントの情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。

製品インスタンスが1つのスマートアカウントとバーチャルアカウントから別のアカウントに移動された場合、移動後の次のACKにはこの更新された情報が含まれます。このACKが製品インスタンスで使用可能になると、このコマンドの出力が更新されます。

ACKは、直接的に（製品インスタンスがCSSMに接続されている場合）または間接的に（製品インスタンスがCSLU、Cisco DNA Center、またはSSM On-Premを介してCSSMに接続されている場合）、あるいは手動でACKをインポートすることによって（製品インスタンスがエアギャップネットワークにある場合）受信することができます。

## 例

ディスプレイに表示されるフィールドについては、[表 6: ポリシーを使用したスマートライセンスの show license status のフィールドの説明 \(130 ページ\)](#) を参照してください。

出力例については、次を参照してください。

- [ポリシーを使用したスマートライセンスの show license status \(136 ページ\)](#)
- [スマートライセンスの show license status \(137 ページ\)](#)

表 6: ポリシーを使用したスマートライセンスの *show license status* のフィールドの説明

フィールド	説明
ユーティリティ	製品インスタンスで設定されているユーティリティ設定のヘッダー。
ステータス :	Status
ユーティリティレポート :	最後の試行結果 :
顧客情報 :	次のフィールドが表示されます。 <ul style="list-style-type: none"> <li>• ID:</li> <li>• Name:</li> <li>• Street</li> <li>• City:</li> <li>• State:</li> <li>• Country:</li> <li>• Postal Code:</li> </ul>

フィールド	説明
ポリシーを使用したスマートライセンス	製品インスタンスのポリシー設定のヘッダー。
	<p>ステータス：</p> <p>ポリシーを使用したスマートライセンスが有効になっているかどうかを示します。</p> <p>ポリシーを使用したスマートライセンスは、Cisco IOS XE Amsterdam 17.3.2 以降でサポートされ、サポートされているソフトウェアイメージでは常に有効になっています。</p>
アカウント情報：	<p>製品インスタンスが属するアカウント情報のヘッダー（CSSM 内）。</p> <p>このセクションは、製品インスタンスのソフトウェアバージョンが Cisco IOS XE Cupertino 17.7.1 以降のリリースの場合にのみ表示されます。</p> <p>製品インスタンスに ACK がインストールされていない場合、次のフィールドには &lt;none&gt; が表示されます。</p>
	<p>スマートアカウント：</p> <p>製品インスタンスが属するスマートアカウント。この情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。</p>
	<p>バーチャルアカウント：</p> <p>製品インスタンスが属するバーチャルアカウント。この情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。</p>
データプライバシー：	製品インスタンスで設定されているプライバシー設定のヘッダー。
	<p>送信ホスト名：</p> <p>ホスト名が使用状況レポートで送信されるかどうかを示す <i>yes</i> または <i>no</i> の値。</p>
	<p>Callhome ホスト名のプライバシー：</p> <p>Call Home 機能がレポートの転送モードとして設定されているかどうかを示します。設定されている場合、次のいずれかの値が表示されます。</p> <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>
	<p>スマートライセンスホスト名のプライバシー：</p> <p>次のいずれかの値が表示されます。</p> <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>
<p>バージョンプライバシー：</p> <p>次のいずれかの値が表示されます。</p> <ul style="list-style-type: none"> <li>• ENABLED</li> <li>• DISABLED</li> </ul>	

フィールド	説明
トランスポート :	製品インスタンスで設定されているトランスポート設定のヘッダー。
Type:	使用中の転送モード。 特定の転送モードでは、追加のフィールドが表示されます。たとえば、通信タイプが CSLU に設定されている場合、CSLU アドレスも表示されます。

フィールド	説明
ポリシー :	製品インスタンスに適用されるポリシー情報のヘッダー。
使用中のポリシー :	適用されるポリシー これは、Cisco default、Product default、Permanent License Reservation、Specific License Reservation、PAK license、Installed on <date>、Controller のいずれかです。
ポリシー名 :	ポリシーの名前
レポートの ACK が必要 :	この製品インスタンスのレポートに CSSM 確認応答 (ACK) が必要かどうかを指定する <i>yes</i> または <i>no</i> の値。デフォルトポリシーは常に「 <i>yes</i> 」に設定されます。
Unenforced/Non-Export Perpetual 属性	永久ライセンスのポリシー値を表示します。  <ul style="list-style-type: none"> <li>• 最初のレポート要件 (日) : 最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。</li> <li>• レポート頻度 (日) : 次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。</li> <li>• 変化レポート (日) : ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます</li> </ul>
Unenforced/Non-Export Subscription 属性	サブスクリプション ライセンスのポリシー値を表示します。  <ul style="list-style-type: none"> <li>• 最初のレポート要件 (日) : 最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。</li> <li>• レポート頻度 (日) : 次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。</li> <li>• 変化レポート (日) : ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます</li> </ul>
Enforced (Perpetual/Subscription) ライセンス属性	

フィールド		説明
		<p>適用されたライセンスのポリシー値を表示します。</p> <ul style="list-style-type: none"> <li>最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。</li> <li>レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。</li> <li>変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます</li> </ul>
	Export (PerpetualSubscription) ライセンス属性	<p>輸出規制ライセンスのポリシー値を表示します。</p> <ul style="list-style-type: none"> <li>最初のレポート要件（日）：最初のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。</li> <li>レポート頻度（日）：次のレポートを送信するまでに使用可能な最大時間。その後にポリシー名が続きます。</li> <li>変化レポート（日）：ライセンスの使用状況が変化した場合にレポートを送信できる最大時間。その後にポリシー名が続きます</li> </ul>
その他	カスタム ID のヘッダー。	
	カスタム ID :	ID

フィールド	説明
使用状況レポート :	使用状況レポート (RUM レポート) 情報のヘッダー。
最後に受信した ACK :	最後に受信したACKの日時 (ローカルタイムゾーン)。
次の ACK 期限 :	次の ACK の日時。ACK が不要であることがポリシーで示されている場合、このフィールドには <code>none</code> と表示されます。  (注) ACKが必要で、この期限までに受信されない場合、 <code>syslog</code> が表示されます。
レポート間隔 :	日単位のレポート間隔  ここに表示される値は、 <b>license smart usage intervalinterval_in_days</b> とポリシー値の設定によって異なります。詳細については、 <a href="#">表 6: ポリシーを使用したスマートライセンスの show license status のフィールドの説明 (130 ページ)</a> で対応する構文の説明を参照してください。
次の ACK プッシュチェック :	製品インスタンスが ACK の次のポーリング要求を送信する日時。日時はローカルタイムゾーンで表示されます。  これは、CSSM または CSLU への製品インスタンスによって開始された通信にのみ適用されます。レポート間隔がゼロの場合、または ACK ポーリングが保留されていない場合、このフィールドには <code>none</code> と表示されます。
次のレポートプッシュ :	製品インスタンスが次の RUM レポートを送信する日時。日時はローカルタイムゾーンで表示されます。レポート間隔がゼロの場合、または保留中の RUM レポートがない場合、このフィールドには <code>none</code> と表示されます。
最後のレポートプッシュ :	製品インスタンスが最後の RUM レポートを送信した日時。日時はローカルタイムゾーンで表示されます。
最後のレポートファイル書き込み :	製品インスタンスが最後にオフライン RUM レポートを保存した日時。日時はローカルタイムゾーンで表示されます。
最後のレポートプル :	データモデルを使用して使用状況レポート情報が取得された日時。日時はローカルタイムゾーンで表示されます。

フィールド	説明
インストール済み の信頼コード:	信頼コード関連情報のヘッダー。 信頼コードがインストールされている場合は、日時が表示されます。日時はローカルタイムゾーンで表示されます。 信頼コードがインストールされていない場合、このフィールドには <code>none</code> と表示されます。
Active:	アクティブ製品インスタンス。 高可用性セットアップでは、セットアップ内のすべての製品インスタンスの UDI と、対応する信頼コードのインストール日時が表示されます。
Standby:	スタンバイ製品インスタンス。
Member:	メンバー製品インスタンス。

### ポリシーを使用したスマートライセンスの `show license status`

次に、Cisco Catalyst 9500 スイッチでの `show license status` コマンドの出力例を示します。ここで、製品インスタンスで実行されているソフトウェアバージョンは Cisco IOS XE Cupertino 17.7.1 です。このリリース以降、出力の [Smart Account] フィールドと [Virtual Account] フィールドに注意してください。

ACKがこの製品インスタンスにインストールされていません（最後に受信したACK:<none>）。したがって、アカウント情報フィールドに <none> が表示されます。

```
Device# show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: <none>
  Virtual Account: <none>

Data Privacy:
  Sending Hostname: no
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: ENABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Configured
  VRF:
    Not Configured

Policy:
```



```
Policy in use: Merged from multiple sources.
Reporting ACK required: yes (CISCO default)
Unenforced/Non-Export Perpetual Attributes:
  First report requirement (days): 365 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 90 (CISCO default)
Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 90 (CISCO default)
  Reporting frequency (days): 90 (CISCO default)
  Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Mar 30 22:32:22 2020 EST
  Reporting push interval: 30 days
  Next ACK push check: <none>
  Next report push: Oct 21 04:39:08 2021 EST
  Last report push: <none>
  Last report file write: <none>

Trust Code Installed: <none>
```

## スマートライセンスの show license status

次に、**show license status** コマンドの出力例を示します。

```
Device# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: Cisco Systems
  Virtual Account: NPR
  Export-Controlled Functionality: Allowed
  Initial Registration: First Attempt Pending
  Last Renewal Attempt: SUCCEEDED on Jul 19 14:49:49 2018 IST
  Next Renewal Attempt: Jan 15 14:49:47 2019 IST
  Registration Expires: Jul 19 14:43:47 2019 IST

License Authorization:
```

## show license status

```
Status: AUTHORIZED on Jul 28 07:02:56 2018 IST
Last Communication Attempt: SUCCEEDED on Jul 28 07:02:56 2018 IST
Next Communication Attempt: Aug 27 07:02:56 2018 IST
Communication Deadline: Oct 26 06:57:50 2018 IST
```

## 関連コマンド

コマンド	説明
<b>show license all</b>	権限付与情報を表示します。
<b>show license authorization</b>	許可コード関連情報を表示します。
<b>show license summary</b>	すべてのアクティブなライセンスの要約を表示します。
<b>show license udi</b>	UDI を表示します。
<b>show license usage</b>	ライセンス使用情報を表示します。
<b>show tech-support license</b>	デバッグ出力を表示します。

## show license summary

使用されているライセンス、カウント、およびステータスに関する情報を含む、ライセンス使用状況の概要を表示するには、特権 EXEC モードで **show license summary** コマンドを使用します。

### show license summary

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンドデフォルト

特権 EXEC (#)

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	<p>コマンド出力が更新され、ポリシーを使用したスマートライセンスの有効なライセンスステータスが反映されました。有効なライセンスステータスは、IN USE、NOT IN USE、NOT AUTHORIZED のみになりました。</p> <p>コマンド出力が更新され、登録および承認情報が削除されました。</p> <p>コマンド出力にスマートアカウントとバーチャルアカウントの情報が表示されなくなりました。</p>
Cisco IOS XE Cupertino 17.7.1	コマンド出力が更新され、スマートアカウントと仮想アカウントの情報が表示されるようになりました。

#### 使用上のガイドライン

**スマートライセンス**：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

**ポリシーを使用したスマートライセンス**：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

#### ライセンスステータス

- Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで使用可能な**不適用ライセンス**は、NOT AUTHORIZED または NOT IN USE にはなりません。
- Cisco IOS XE Bengaluru 17.6.2 以降の Cisco Catalyst 9300X シリーズスイッチで使用可能な、**輸出規制ライセンス**である Export Control Key for High Security (HSECK9) は、HSECK9

キーが製品インスタンスで使用可能で、必要なスマートライセンス承認コード (SLAC) がインストールされているが、HSECK9 キーを必要とする暗号化機能が設定されていない場合、NOT IN USE にできます。カウントフィールドとステータスフィールドの暗号化機能をそれぞれ 1 と IN USE に変更するように設定します。

SLAC を複数のデバイス (高可用性セットアップまたはスタック構成セットアップ) にインストールする場合、使用カウントは1のままです。これは、特定の時点でアクティブな HSECK9 キーが1つだけ使用されるためです。スイッチオーバーが発生すると、スタンバイのライセンスが有効になります。使用されている HSECK9 キーは1つだけであるため、新しいアクティブでもカウントは1のままです。

ライセンスの使用方法の詳細については、**show license usage** 特権 EXEC コマンドを参照してください。

### 出力のアカウント情報

Cisco IOS XE Cupertino 17.7.1 以降、すべての ACK には、CSSM で報告されたスマートアカウントとバーチャルアカウントが含まれています。ACK を受信すると、製品インスタンスにはこの情報の最新バージョンのみが安全に保存されます。これは、ACK のタイムスタンプによって決定されます。したがって、このコマンドの出力の [Account Information] セクションに表示されるスマートアカウントとバーチャルアカウントの情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。

製品インスタンスが1つのスマートアカウントとバーチャルアカウントから別のアカウントに移動された場合、移動後の次の ACK にはこの更新された情報が含まれます。この ACK が製品インスタンスで使用可能になると、このコマンドの出力が更新されます。

ACK は、直接的に (製品インスタンスが CSSM に接続されている場合) または間接的に (製品インスタンスが CSLU、Cisco DNA Center、または SSM On-Prem を介して CSSM に接続されている場合)、あるいは手動で ACK をインポートすることによって (製品インスタンスがエアギャップネットワークにある場合) 受信することができます。

### 例

ディスプレイに表示されるフィールドについては、[表 7: ポリシーを使用したスマートライセンスの show license summary のフィールドの説明 \(141 ページ\)](#) を参照してください。

出力例については、次を参照してください。

- [show license summary \(Cisco Catalyst 9500 シリーズ スイッチ\) \(141 ページ\)](#)
- [show license summary \(Cisco Catalyst 9300X シリーズ スイッチ\) \(142 ページ\)](#)

表 7: ポリシーを使用したスマートライセンスの *show license summary* のフィールドの説明

フィールド	説明
アカウント情報 : Smart Account: Virtual Account:	製品インスタンスが属するスマートアカウントとバーチャルアカウント。この情報は、常に製品インスタンスで使用可能な最新の ACK に基づいています。  このフィールドは、製品インスタンスのソフトウェアバージョンが Cisco IOS XE Cupertino 17.7.1 以降のリリースの場合にのみ表示されません。  製品インスタンスに ACK がインストールされていない場合、次のフィールドには <none> が表示されます。
License	使用中のライセンスの名前
Entitlement Tag	ライセンスの短縮名
Count	ライセンス数
Status	ライセンスのステータスは次のいずれかになります。  <ul style="list-style-type: none"> <li>• In-Use : 有効なライセンスかつ使用中。</li> <li>• Not In-Use : HSECK9 キーが製品インスタンスで使用可能で、必要なスマートライセンス承認コード (SLAC) がインストールされていますが、HSECK9 キーを必要とする暗号化機能が無効になっているか、設定されていません。  このステータスは、HSECK9 ライセンスの SLAC を CSSM に返す場合の前提条件です。</li> <li>• Not Authorized : ライセンスを使用する前に SLAC のインストールが必要であることを意味します。</li> </ul>

**show license summary (Cisco Catalyst 9500 シリーズ スイッチ)**

次に、ソフトウェアバージョンが Cisco IOS XE cupertino 17.7.1 である製品インスタンスの **show license summary** コマンドの出力例を示します。このリリース以降に表示されるアカウント情報フィールドに注意してください。

```
Device# show license summary
```

```
Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA
```

```
License Usage:
  License                               Entitlement Tag                Count Status
  -----
  network-advantage_250M (ESR_P_250M_A)                1 IN USE
  dna-advantage_250M      (DNA_P_250M_A)                1 IN USE
```

**show license summary (Cisco Catalyst 9300X シリーズ スイッチ)**

次に、C9300X スタックでの **show license summary** コマンドの出力例を示します。

この **Status** 列と **Count** 列には、HSECK9 キーの **NOT IN USE** と 0 が表示されます。これは、HSECK9 キーが使用可能で、SLAC がインストールされているが、ライセンスを必要とする暗号化機能が設定されていないことを意味します。

```
Device# show license summary
License Usage:
  License                               Entitlement Tag                Count Status
  -----
network-advantage (C9300-24 Network Advan...) 1 IN USE
dna-advantage     (C9300-24 DNA Advantage)      1 IN USE
network-advantage (C9300-48 Network Advan...) 2 IN USE
dna-advantage     (C9300-48 DNA Advantage)      2 IN USE
C9K HSEC (Cat9K HSEC) 0 NOT IN USE
```

この **Status** 列と **Count** 列には、HSECK9 キーの **IN USE** と 1 が表示されます。これは、HSECK9 キーを必要とする暗号化機能が設定されていることを意味します。

```
Device# show license summary
License Usage:
  License                               Entitlement Tag                Count Status
  -----
network-advantage (C9300-24 Network Advan...) 1 IN USE
dna-advantage     (C9300-24 DNA Advantage)      1 IN USE
network-advantage (C9300-48 Network Advan...) 2 IN USE
dna-advantage     (C9300-48 DNA Advantage)      2 IN USE
hseck9 (Cat9K HSEC) 1 IN USE
```

## show license tech

テクニカルサポートチームが問題をトラブルシューティングするのに役立つライセンス情報を表示するには、特権 EXEC モードで **show license tech** コマンドを入力します。このコマンドの出力には、他のいくつかの **show license** コマンドの出力などが含まれます。

**show license tech message | rum feature license\_name | all | id rum\_id | all [ detail ] [ save path ] | support**

### 構文の説明

<b>message</b>	信頼の確立、使用状況レポート、結果のポーリング、承認コードの要求と返却、および信頼の同期に関するメッセージを表示します。  これは、 <b>show license history message</b> コマンドの出力に表示される情報と同じです。
<b>rum feature license_name   all   id rum_id   all [ detail ] [ save path ]</b>	製品インスタンスのリソース使用率測定レポート (RUM レポート) に関する情報を表示します。これには、レポート ID、レポートの現在の処理状態、エラー情報 (ある場合)、および表示された RUM レポート情報を保存するオプションが含まれます。  (注) このオプションでは、RUM レポートに関する情報が保存され、レポート用ではありません。使用状況情報を含む XML ファイルである RUM レポートは保存されません。
<b>support</b>	テクニカルサポートチームが問題をデバッグするのに役立つライセンス情報を表示します。

### コマンドモード

特権 EXEC (Device#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに適用可能な新しいフィールドが反映されました。

リリース	変更内容
Cisco IOS XE Cupertino 17.7.1	<p><b>rum</b> キーワードおよびこのキーワードの下に追加のオプションが追加されました。</p> <p><b>feature license_name   all   id rum_id   all</b></p> <p><b>show license tech support</b> コマンドの出力が強化され、次の情報が表示されるようになりました。</p> <ul style="list-style-type: none"> <li>• [License Usage] と [Usage Report Summary] セクションに記載されている RUM レポート情報。</li> <li>• [Account Information:] セクションにあるスマートアカウントとバーチャルアカウント情報。</li> </ul> <p><b>data conversion</b>、<b>eventlog</b>、および <b>reservation</b> キーワードがこのコマンドから削除されました。これらは引き続き、個別の <b>show</b> コマンド、つまり、<b>show license data</b>、<b>show license eventlog</b>、および <b>show license reservation</b> として使用できます。</p>

## 使用上のガイドライン

**スマートライセンス**：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます（スマートライセンスが有効になっているかどうか、関連するすべてのライセンス証明書、コンプライアンスステータスなど）。

**ポリシーを使用したスマートライセンス**：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

- サポート担当者によるトラブルシューティング

解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージとともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra all** 特権 EXEC コマンドの出力例を提供してください。

- 出力の RUM レポート情報

- **show license tech support** コマンドの出力には、RUM レポートに関する次のセクションが表示されます。

表 8 : show license tech support : ヘッダー「ライセンスの使用状況」のフィールドの説明 (145 ページ)

```
License Usage
=====
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 1
    Current Report: 1574560510      Previous: 1574560508
```



表 8 : show license tech support : ヘッダー「ライセンスの使用状況」のフィールドの説明

フィールド名	説明
Interval:	これは固定の測定時間で、常に 15 分です。
Current Value:	現在のライセンス数に関する情報。
Current Report:	ライセンスの現在 OPEN レポートの ID。
Previous:	ライセンスの最後の OPEN レポートの ID。このレポートのステータスは現在 CLOSED です。

表 9 : show license tech support : ヘッダー「使用状況レポートの概要」のフィールドの説明 (145 ページ)

```
Usage Report Summary:
=====
Total: 26, Purged: 0(0)
Total Acknowledged Received: 0, Waiting for Ack: 0(26)
Available to Report: 26 Collecting Data: 2
Maximum Display: 26 In Storage: 26, MIA: 0(0)
```

表 9 : show license tech support : ヘッダー「使用状況レポートの概要」のフィールドの説明

フィールド名	説明
Total:	製品インスタンスが生成したレポートの合計数。  (注) この合計は、製品インスタンスで現在使用可能であり、追跡されているレポートの合計数を示すものではありません。このためには、[Total Acknowledged Received:] フィールドと [Available to Report] フィールドを合計する必要があります。
Purged:	システムリソースの制限により削除されたレポートの数。この数には、製品インスタンスにトラッキング情報がない RUM レポートが含まれます。
Total Acknowledged Received:	この製品インスタンスで確認された RUM レポートの数。
Waiting for Ack:	ACK を待機している RUM レポートの数。これは、UNACK 状態のレポートの総数です。この場合、製品インスタンスにはトラッキング情報があります。
Available to Report:	CSSM に送信可能な RUM レポートの数。これは、OPEN または CLOSED 状態のレポートの総数です。この場合、製品インスタンスにはトラッキング情報があります。

フィールド名	説明
Collecting Data:	製品インスタンスが現在測定値を収集しているレポートの数。
Maximum Display:	<b>show</b> コマンドの出力に表示できるレポートの数。
In Storage:	ディスクに現在保存されているレポートの数。
MIA:	欠落しているレポートの数。

- **show license tech rum** コマンドの出力には、RUM レポートに関する次のフィールドが表示されます。表 10 : **show license tech rum** : ヘッダー「スマートライセンスの使用状況レポート詳細」のフィールドの説明 (146 ページ)

**show license tech rum** キーワードで使用できるオプションは、**show license rum** 特権 EXEC コマンドで使用できるオプションと同じです。簡易ビューに表示される出力例も同じです。ただし、**detail** キーワードを使用する場合（たとえば、**show license tech rum feature license\_name detail** を入力する場合）、詳細ビューが表示され、**show license rum** と比較していくつかの追加フィールドがあります。

```
Smart Licensing Usage Report Detail:
=====
Report Id: 1574560509
  Metric Name: ENTITLEMENT
  Feature Name: dna-advantage
  Metric Value:
regid.2017-07.com.cisco.C9500-DNA-40X-A,1.0_7eb18f4c-2d44-4077-8346-818defbd9ad9

UDI: PID:C9500-40X,SN:FCW2227A4NC
Previous Report Id: 1574560507,   Next Report Id: 1574560511
Version: 2.0
State: CLOSED,           State Change Reason: REPORTING
Start Time: Aug 05 16:15:14 2021 EST,   End Time: Aug 05 19:38:43 2021 EST

Storage State: EXIST,   Storage State Change Reason: None
Transaction ID: 0
Transaction Message: <none>
Report Size: 1086(1202)
```

表 10 : **show license tech rum** : ヘッダー「スマートライセンスの使用状況レポート詳細」のフィールドの説明

フィールド名	説明
Version:	送信中のレポートの形式を表示します。  Cisco IOS XE Cupertino 17.7.1 以降、RUM レポートは処理時間を短縮する新しい形式で保存されます。このフィールドは、製品インスタンスが古い形式を使用しているか、新しい形式を使用しているかを示します。

フィールド名	説明
Storage State:	<p>特定のレポートが現在ストレージにあるかどうかを示します。</p> <p>RUM レポートの現在のストレージ状態の表示に加えて、EXIST、DELETED、PURGED、MISSING の各値が表示されます。ラベルの横に「(1)」が表示されている場合 (Storage State (1))、RUM レポートは古い (17.7.1 より前の) 形式であり、それに応じて処理されます。RUM レポートが新しい形式の場合、フィールドは [Storage State] として表示され、追加情報はありません。</p>
Storage State Change Reason:	<p>ストレージの状態が変化した理由を表示します。すべての状態変更が理由を示すわけではありません。</p> <ul style="list-style-type: none"> <li>• NONE : これは、ストレージの状態変更の理由が記録されなかったことを意味します。</li> <li>• PROCESSED : これは、CISCO がデータを処理した後に RUM レポートが削除されたことを意味します。</li> <li>• LIMIT_STORAGE : これは、製品インスタンスがストレージ制限に達したため、RUM レポートが削除されたことを意味します。</li> <li>• LIMIT_TIME : これは、レポートが永続的な時間制限に達したため、RUM レポートが削除されたことを意味します。</li> </ul>
Transaction ID: Transaction Message:	<p>トランザクション ID に関連 ID が表示され、エラーステータスが表示される場合、製品インスタンスのこのセクションにエラーコードフィールドが表示されます。エラーがない場合、データはここに表示されません。</p>
Report Size	<p>このフィールドには 2 つの数字が表示されます。最初の数値は、通信の raw レポートのサイズ (バイト単位) です。2 番目の数値は、レポートの保存に使用されるディスク容量 (バイト単位) です。2 番目の数値は、レポートが新しい形式で保存されている場合にのみ表示されます。</p>

## 例

## 例 : show license tech support (Cisco Catalyst 9400 シリーズ スイッチ)

次に、ソフトウェアバージョン Cisco IOS XE Cupertino 17.7.1 を実行している Cisco Catalyst 9400 スイッチでの **show license tech support** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license tech support

Smart Licensing Tech Support info

Smart Licensing Status
=====

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Account Information:
  Smart Account: Eg-SA
  Virtual Account: Eg-VA

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Address: <empty>
    Port: <empty>
    Username: <empty>
    Password: <empty>
  Server Identity Check: True
  VRF: <empty>

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Nov 20 12:10:02 2021 PDT
  Policy name: SLE Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 30 (Customer Policy)
    Reporting frequency (days): 60 (Customer Policy)
    Report on change (days): 60 (Customer Policy)
```

```
Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 120 (Customer Policy)
  Reporting frequency (days): 111 (Customer Policy)
  Report on change (days): 111 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 30 (Customer Policy)
  Reporting frequency (days): 90 (Customer Policy)
  Report on change (days): 60 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 30 (Customer Policy)
  Reporting frequency (days): 30 (Customer Policy)
  Report on change (days): 30 (Customer Policy)

Usage Reporting:
  Last ACK received: Dec 03 12:12:10 2021 PDT
  Next ACK deadline: Feb 01 12:12:10 2022 PDT
  Reporting push interval: 30 days State(4) InPolicy(60)
  Next ACK push check: Dec 04 04:12:06 2021 PDT
  Next report push: Dec 03 20:08:05 2021 PDT
  Last report push: Dec 03 12:08:08 2021 PDT
  Last report file write: <none>

License Usage
=====
Handle: 1
  License: network-advantage
  Entitlement Tag:
  regid.2017-05.com.cisco.advantagek9-C9400,1.0_61a546cd-1037-47cb-bbe6-7cad3217a7b3
  Description: C9400 Network Advantage
  Count: 2
  Version: 1.0
  Status: IN USE(15)
  Status time: Nov 20 19:07:28 2021 PDT
  Request Time: Nov 20 19:08:05 2021 PDT
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9400 Network Advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 2
      Current Report: 1637348082          Previous: 1637348080
  Soft Enforced: True

Handle: 2
  License: dna-essentials
  Entitlement Tag:
  regid.2017-05.com.cisco.dna_essentials-C9400,1.0_74d47865-1bf3-4f00-a06b-edbe18b049b3
  Description: C9400 DNA Essentials
  Count: 1
  Version: 1.0
  Status: IN USE(15)
  Status time: Nov 20 19:07:28 2021 PDT
  Request Time: Nov 20 19:07:28 2021 PDT
  Export status: NOT RESTRICTED
  Feature Name: dna-essentials
  Feature Description: C9400 DNA Essentials
  Enforcement type: NOT ENFORCED
  License type: Subscription
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
```

```

Current Value: 1
Current Report: 1637348083      Previous: 1637348081
Soft Enforced: True

Handle: 7
License: air-network-advantage
Entitlement Tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
Description: air-network-advantage
Count: 0
Version: 1.0
Status: NOT IN USE(1)
Status time: Dec 03 20:07:35 2021 PDT
Request Time: None
Export status: NOT RESTRICTED
Feature Name: air-network-advantage
Feature Description: air-network-advantage
Enforcement type: NOT ENFORCED
License type: Perpetual
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 0
    Current Report: 0      Previous: 0
Soft Enforced: True

Handle: 8
License: air-dna-advantage
Entitlement Tag:
regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
Description: air-dna-advantage
Count: 0
Version: 1.0
Status: NOT IN USE(1)
Status time: Dec 03 20:07:35 2021 PDT
Request Time: None
Export status: NOT RESTRICTED
Feature Name: air-dna-advantage
Feature Description: air-dna-advantage
Enforcement type: NOT ENFORCED
License type: Subscription
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 0
    Current Report: 0      Previous: 0
Soft Enforced: True

Product Information
=====
UDI: PID:C9407R,SN:FXS2119Q2U7

HA UDI List:
  Active:PID:C9407R,SN:FXS2119Q2U7
  Standby:PID:C9407R,SN:FXS2119Q2U7

Agent Version
=====
Smart Agent for Licensing: 5.3.16_rel/55

Upcoming Scheduled Jobs
=====
Current time: Dec 03 22:58:47 2021 PDT
Daily: Dec 04 19:07:31 2021 PDT (20 hours, 8 minutes, 44 seconds remaining)

```

```
Authorization Renewal: Expired Not Rescheduled
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Expired Not Rescheduled
Retrieve data processing result: Dec 04 04:12:06 2021 PDT (5 hours, 13 minutes, 19 seconds
remaining)
Start Utility Measurements: Dec 03 23:08:06 2021 PDT (9 minutes, 19 seconds remaining)
Send Utility RUM reports: Dec 04 20:08:05 2021 PDT (21 hours, 9 minutes, 18 seconds
remaining)
Save unreported RUM Reports: Dec 03 23:53:16 2021 PDT (54 minutes, 29 seconds remaining)
Process Utility RUM reports: Dec 04 12:17:10 2021 PDT (13 hours, 18 minutes, 23 seconds
remaining)
Data Synchronization: Expired Not Rescheduled
External Event: Jan 19 11:53:19 2022 PDT (46 days, 12 hours, 54 minutes, 32 seconds
remaining)
Operational Model: Expired Not Rescheduled

Communication Statistics:
=====
Communication Level Allowed: DIRECT
Overall State: <empty>
Trust Establishment:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Acknowledgement:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Usage Reporting:
  Attempts: Total=45, Success=22, Fail=23 Ongoing Failure: Overall=1 Communication=1
  Last Response: NO REPLY on Dec 03 20:08:05 2021 PDT
  Failure Reason: <none>
  Last Success Time: Dec 03 12:08:07 2021 PDT
  Last Failure Time: Dec 03 20:08:05 2021 PDT
Result Polling:
  Attempts: Total=85, Success=25, Fail=60 Ongoing Failure: Overall=3 Communication=3
  Last Response: NO REPLY on Dec 03 20:12:19 2021 PDT
  Failure Reason: <none>
  Last Success Time: Dec 03 12:29:18 2021 PDT
  Last Failure Time: Dec 03 20:12:19 2021 PDT
Authorization Request:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Confirmation:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Return:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Sync:
  Attempts: Total=5, Success=1, Fail=4 Ongoing Failure: Overall=0 Communication=0
```

```
Last Response: OK on Nov 20 19:17:37 2021 PDT
  Failure Reason: <none>
Last Success Time: Nov 20 19:17:37 2021 PDT
Last Failure Time: Nov 20 19:17:02 2021 PDT
Hello Message:
  Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>

License Certificates
=====
Production Cert: True
Not registered. No certificates installed

HA Info
=====
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
=====
License reservation: DISABLED

Overall status:
  Active: PID:C9407R,SN:FXS2119Q2U7
    Reservation status: NOT INSTALLED
    Request code: <none>
    Last return code: <none>
    Last Confirmation code: <none>
    Reservation authorization code: <none>
  Standby: PID:C9407R,SN:FXS2119Q2U7
    Reservation status: NOT INSTALLED
    Request code: <none>
    Last return code: <none>
    Last Confirmation code: <none>
    Reservation authorization code: <none>

Specified license reservations:

Purchased Licenses:
  No Purchase Information Available

Usage Report Summary:
=====
Total: 137, Purged: 0(0)
Total Acknowledged Received: 98, Waiting for Ack: 34(39)
Available to Report: 4 Collecting Data: 2
Maximum Display: 137 In Storage: 59, MIA: 0(0)
Report Module Status: Ready

Other Info
=====
Software ID: regid.2017-05.com.cisco.C9400,v1_ad928212-d182-407e-ac85-29e213602efa
Agent State: authorized
TS enable: True
Transport: Smart
Default URL: https://smartreceiver.cisco.com/licservice/license
```



```
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char) : 1
sizeof(int) : 4
sizeof(long) : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: True
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN, POLICY_USAGE
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPPluginMgmtInterfaceMutex: True
SAPPluginMgmtIPDomainName: True
SmartTransportVRFSupport: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: True
SmartTransportProxySupport: True
SmartAgentPolicyDisplayFormat: 0
SmartAgentReportOnUpgrade: False
SmartAgentIndividualRUMEncrypt: 2
SmartAgentMaxRumMemory: 50
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: False
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
```

```

HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: SmartAgentSystemDataListChanged
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 58 KB
P:C9407R,S:FXS2119Q2U7: P:C9407R,S:FXS2119Q2U7, state[2], Trust Data INSTALLED TrustId:412
P:C9407R,S:FXS2119Q2U7: P:C9407R,S:FXS2119Q2U7, state[2], Trust Data INSTALLED TrustId:412
Overall Trust: INSTALLED (2)
Clock sync-ed with NTP: True

Platform Provided Mapping Table
=====
C9407R: Total licenses found: 198
Enforced Licenses:
P:C9407R,S:FXS2119Q2U7:
No PD enforced licenses

```

### ポリシーを使用したスマートライセンスの **show license tech support** (Cisco Catalyst 9500 シリーズ スイッチ)

次に、Cisco Catalyst 9500 スイッチでの **show license tech support** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```

Device# show license tech support
Smart Licensing Tech Support info

Smart Licensing Status
=====

Smart Licensing is ENABLED
License Reservation is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
  Callhome hostname privacy: DISABLED
  Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Miscellaneous:

```

```
Custom Id: <empty>

Policy:
Policy in use: Merged from multiple sources.
Reporting ACK required: yes (CISCO default)
Unenforced/Non-Export Perpetual Attributes:
  First report requirement (days): 365 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 90 (CISCO default)
Unenforced/Non-Export Subscription Attributes:
  First report requirement (days): 90 (CISCO default)
  Reporting frequency (days): 90 (CISCO default)
  Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
  First report requirement (days): 0 (CISCO default)
  Reporting frequency (days): 0 (CISCO default)
  Report on change (days): 0 (CISCO default)

Usage Reporting:
Last ACK received: <none>
Next ACK deadline: Jan 27 09:49:33 2021 PST
Reporting push interval: 30 days State(2) InPolicy(90)
Next ACK push check: <none>
Next report push: Oct 29 09:51:33 2020 PST
Last report push: <none>
Last report file write: <none>

License Usage
=====
Handle: 1
  License: network-advantage
  Entitlement Tag:
regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c

  Description: network-advantage
  Count: 2
  Version: 1.0
  Status: IN USE(15)
  Status time: Oct 29 09:48:54 2020 PST
  Request Time: Oct 29 09:49:18 2020 PST
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 2
    Soft Enforced: True

Handle: 2
  License: dna-advantage
  Entitlement Tag:
regid.2017-07.com.cisco.C9500-DNA-16X-A,1.0_ef3574d1-156b-486a-864f-9f779ff3ee49
  Description: C9500-16X DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE(15)
  Status time: Oct 29 09:48:54 2020 PST
  Request Time: Oct 29 09:49:18 2020 PST
  Export status: NOT RESTRICTED
```

```
Feature Name: dna-advantage
Feature Description: C9500-16X DNA Advantage
Measurements:
  ENTITLEMENT:
    Interval: 00:15:00
    Current Value: 2
  Soft Enforced: True

Handle: 7
  License: air-network-advantage
  Entitlement Tag:
  regid.2018-06.com.cisco.DNA_NWstack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
  Description: air-network-advantage
  Count: 0
  Version: 1.0
  Status: IN USE(15)
  Status time: Oct 29 10:49:09 2020 PST
  Request Time: None
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 0
    Soft Enforced: True

Handle: 8
  License: air-dna-advantage
  Entitlement Tag:
  regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790
  Description: air-dna-advantage
  Count: 0
  Version: 1.0
  Status: IN USE(15)
  Status time: Oct 29 10:49:09 2020 PST
  Request Time: None
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 0
    Soft Enforced: True

Product Information
=====
UDI: PID:C9500-16X,SN:FCW2233A5ZV

HA UDI List:
  Active:PID:C9500-16X,SN:FCW2233A5ZV
  Standby:PID:C9500-16X,SN:FCW2233A5ZY

Agent Version
=====
Smart Agent for Licensing: 5.0.5_rel/42

Upcoming Scheduled Jobs
=====
Current time: Oct 29 11:04:46 2020 PST
Daily: Oct 30 09:48:56 2020 PST (22 hours, 44 minutes, 10 seconds remaining)
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Nov 05 09:52:25 2020 PST
```

```
(6 days, 22 hours, 47 minutes, 39 seconds remaining)
Start Utility Measurements: Oct 29 11:19:09 2020 PST (14 minutes, 23 seconds remaining)
Send Utility RUM reports: Oct 30 09:53:10 2020 PST (22 hours, 48 minutes, 24 seconds remaining)
Save unreported RUM Reports: Oct 29 12:04:19 2020 PST (59 minutes, 33 seconds remaining)
Process Utility RUM reports: Oct 30 09:49:33 2020 PST (22 hours, 44 minutes, 47 seconds remaining)
Data Synchronization: Expired Not Rescheduled
External Event: Nov 28 09:49:33 2020 PST (29 days, 22 hours, 44 minutes, 47 seconds remaining)
Operational Model: Expired Not Rescheduled
```

## Communication Statistics:

=====

Communication Level Allowed: INDIRECT

Overall State: &lt;empty&gt;

## Trust Establishment:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: &lt;none&gt;

Failure Reason: &lt;none&gt;

Last Success Time: &lt;none&gt;

Last Failure Time: &lt;none&gt;

## Trust Acknowledgement:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: &lt;none&gt;

Failure Reason: &lt;none&gt;

Last Success Time: &lt;none&gt;

Last Failure Time: &lt;none&gt;

## Usage Reporting:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: &lt;none&gt;

Failure Reason: &lt;none&gt;

Last Success Time: &lt;none&gt;

Last Failure Time: &lt;none&gt;

## Result Polling:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: &lt;none&gt;

Failure Reason: &lt;none&gt;

Last Success Time: &lt;none&gt;

Last Failure Time: &lt;none&gt;

## Authorization Request:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: &lt;none&gt;

Failure Reason: &lt;none&gt;

Last Success Time: &lt;none&gt;

Last Failure Time: &lt;none&gt;

## Authorization Confirmation:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: &lt;none&gt;

Failure Reason: &lt;none&gt;

Last Success Time: &lt;none&gt;

Last Failure Time: &lt;none&gt;

## Authorization Return:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: &lt;none&gt;

Failure Reason: &lt;none&gt;

Last Success Time: &lt;none&gt;

Last Failure Time: &lt;none&gt;

## Trust Sync:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: &lt;none&gt;

Failure Reason: &lt;none&gt;

Last Success Time: &lt;none&gt;

Last Failure Time: &lt;none&gt;

```

Hello Message:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
  Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>

License Certificates
=====
Production Cert: True
Not registered. No certificates installed

HA Info
=====
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
=====
License reservation: ENABLED

Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
    Reservation status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
    Request code: <none>
    Last return code: <none>
    Last Confirmation code: 184ba6d6
    Reservation authorization code:
    Network Advantage</displayName><tagDescription>C9500 Network

  Standby: PID:C9500-16X,SN:FCW2233A5ZY
    Reservation status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
    Request code: <none>
    Last return code: <none>
    Last Confirmation code: 961d598f
    Reservation authorization code:
    Network Advantage</displayName><tagDescription>C9500 Network

Specified license reservations:
  C9500 Network Advantage (C9500 Network Advantage):
    Description: C9500 Network Advantage
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
        License type: PERPETUAL
        Start Date: <none>
        End Date: <none>
        Term Count: 1
        Subscription ID: <none>
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
        License type: PERPETUAL

```

```
        Start Date: <none>
        End Date: <none>
        Term Count: 1
        Subscription ID: <none>
C9500-DNA-16X-A (C9500-16X DNA Advantage):
  Description: C9500-DNA-16X-A
  Total reserved count: 2
  Enforcement type: NOT ENFORCED
  Term information:
    Active: PID:C9500-16X,SN:FCW2233A5ZV
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Start Date: <none>
      End Date: <none>
      Term Count: 1
      Subscription ID: <none>
    Standby: PID:C9500-16X,SN:FCW2233A5ZY
      Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      License type: PERPETUAL
      Start Date: <none>
      End Date: <none>
      Term Count: 1
      Subscription ID: <none>

Purchased Licenses:
  No Purchase Information Available

Other Info
=====
Software ID: regid.2017-05.com.cisco.C9500,v1_7435cf27-0075-4bfb-b67c-b42f3054e82a
Agent State: authorized
TS enable: True
Transport: Transport Off
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)   : 1
sizeof(int)    : 4
sizeof(long)   : 4
sizeof(char *) : 8
sizeof(time_t) : 4
sizeof(size_t) : 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN, POLICY_USAGE
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPuginMgmtInterfaceMutex: True
```

```

SAPuginMgmtIPDomainName: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: False
SmartTransportProxySupport: False
SmartAgentMaxRunMemory: 50
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: False
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: SmartAgentSystemDataListChanged
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 109 KB
P:C9500-16X,S:FCW2233A5ZV: No Trust Data
P:C9500-16X,S:FCW2233A5ZY: No Trust Data
Overall Trust: No ID

```

Platform Provided Mapping Table

=====

C9500-16X: Total licenses found: 143

Enforced Licenses:

P:C9500-16X,S:FCW2233A5ZV:

No PD enforced licenses

P:C9500-16X,S:FCW2233A5ZY:

No PD enforced licenses



## show license udi

製品インスタンスの Unique Device Identifier (UDI) 情報を表示するには、特権 EXEC モードで **show license udi** コマンドを入力します。高可用性セットアップでは、接続されたすべての製品インスタンスの UDI 情報が出力に表示されます。

### show license udi

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンド デフォルト

特権 EXEC (#)

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	このコマンドは、ポリシーを使用したスマートライセンスの環境で引き続き使用できます。

#### 使用上のガイドライン

**スマートライセンス**：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

**ポリシーを使用したスマートライセンス**：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

高可用性セットアップまたはスタック構成セットアップでは、接続されたすべての製品インスタンスの UDI 情報が **show license udi** コマンドの出力に表示されます。

#### 例

[ポリシーを使用したスマートライセンスの show licensing udi \(161 ページ\)](#)

#### ポリシーを使用したスマートライセンスの show licensing udi

次に、Catalyst 9500 スイッチでのハイアベイラビリティ設定の **show license udi** コマンドの出力例を示します。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license udi

UDI: PID:C9500-16X, SN:FCW2233A5ZV
HA UDI List:
Active:PID:C9500-16X, SN:FCW2233A5ZV
Standby:PID:C9500-16X, SN:FCW2233A5ZY
```

## show license usage

ステータス、使用中のライセンス数、適用タイプなどのライセンス使用状況の情報を表示するには、特権 EXEC モードで **show license usage** コマンドを入力します。

### show license usage

このコマンドには引数またはキーワードはありません。

コマンド デフォルト 特権 EXEC (#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Amsterdam 17.3.2a	コマンド出力が更新され、ポリシーを使用したスマートライセンスに適用可能な新しいフィールドが反映されました。これには、Status、Enforcement type フィールドが含まれます。  コマンド出力が更新され、予約関連情報、承認ステータス情報、および輸出ステータス情報が削除されました。

### 使用上のガイドライン

**スマートライセンス**：デバイス上のソフトウェアバージョンが Cisco IOS XE Amsterdam 17.3.1 以前のリリースの場合、コマンド出力にはスマートライセンスに関連するフィールドが表示されます。

**ポリシーを使用したスマートライセンス**：デバイス上のソフトウェアバージョン（製品インスタンスとも呼ばれる）が Cisco IOS XE Amsterdam 17.3.2a 以降のリリースの場合、コマンド出力にはポリシーを使用したスマートライセンスに関連するフィールドが表示されます。

- Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで使用可能な**不適用ライセンス**は、NOT AUTHORIZED または NOT IN USE にはなりません。
- Cisco IOS XE Bengaluru 17.6.2 以降の Cisco Catalyst 9300X シリーズスイッチで使用可能な、**輸出規制ライセンス**である Export Control Key for High Security (HSECK9) は、HSECK9 キーが製品インスタンスで使用可能で、必要なスマートライセンス承認コード (SLAC) がインストールされているが、HSECK9 キーを必要とする暗号化機能が設定されていない場合、NOT IN USE にできます。カウントフィールドとステータスフィールドの暗号化機能をそれぞれ 1 と IN USE に変更するように設定します。

SLAC を複数のデバイス（高可用性セットアップまたはスタック構成セットアップ）にインストールする場合、使用カウントは1のままです。これは、特定の時点でアクティブな HSECK9 キーが1つだけ使用されるためです。スイッチオーバーが発生すると、スタンバイのライセンスが有効になります。使用されている HSECK9 キーは1つだけであるため、新しいアクティブでもカウントは1のままです。

## 例

ディスプレイに表示されるフィールドについては、[表 11: ポリシーを使用したスマートライセンス用 show license usage のフィールドの説明 \(163 ページ\)](#) を参照してください。

[ポリシーを使用したスマートライセンスの show license usage \(164 ページ\)](#)

表 11: ポリシーを使用したスマートライセンス用 *show license usage* のフィールドの説明

フィールド	Description
License Authorization: Status:	全体的な承認ステータスを表示します。
():	CSSM におけるようなライセンスの名前。 このライセンスが承認コードを必要とする場合、ライセンスの名前はコードから取得されます。
Description	CSSM におけるようなライセンスの説明。
Count	ライセンス数。ライセンスが使用中でない場合、カウントはゼロとして反映されます。
Version	バージョン。
Status	<p>ライセンスのステータスは次のいずれかになります。</p> <ul style="list-style-type: none"> <li>• In-Use : 有効なライセンスかつ使用中。</li> <li>• Not In-Use : HSECK9 キーが製品インスタンスで使用可能で、必要なスマートライセンス承認コード (SLAC) がインストールされていますが、HSECK9 キーを必要とする暗号化機能が無効になっているか、設定されていません。</li> </ul> <p>このステータスは、HSECK9 キーの SLAC を CSSM に返す場合の前提条件です。</p> <ul style="list-style-type: none"> <li>• Not Authorized : ライセンスを使用する前に SLAC のインストールが必要です。</li> </ul>

フィールド	Description
Export Status:	ライセンスが輸出規制されているかどうかを示します。それに応じて次のステータスのいずれかが表示されます。 <ul style="list-style-type: none"> <li>• RESTRICTED - ALLOWED</li> <li>• RESTRICTED - NOT ALLOWED</li> <li>• NOT RESTRICTED</li> </ul>
Feature name	このライセンスを使用する機能の名前。
Feature Description:	このライセンスを使用する機能の説明。
ユーティリティのサブスクリプション ID :	ID 対応する設定オプションがサポートされていないため、該当しません。
Enforcement type	ライセンスの適用タイプのステータス。これは、次のいずれかです。 <ul style="list-style-type: none"> <li>• ENFORCED：使用前に承認が必要なライセンス。</li> <li>• NOT ENFORCED：使用前に承認を必要としないライセンス。</li> <li>• EXPORT RESTRICTED - ALLOWED：必要な承認がある輸出規制ライセンス、つまり SLAC がインストールされています。</li> <li>• EXPORT RESTRICTED - NOT ALLOWED：必要な承認がない輸出規制ライセンス。輸出規制ライセンスは、使用前に承認が必要です。</li> </ul>

### ポリシーを使用したスマートライセンスの show license usage

次に、Cisco Catalyst 9500 スイッチでの **show license usage** コマンドの出力例を示します。ここでは、不適用ライセンスを使用中です。同様の出力が、サポートされているすべての Cisco Catalyst アクセス、コア、およびアグリゲーションスイッチで表示されます。

```
Device# show license usage
License Authorization:
  Status: Not Applicable
network-advantage (C9500 Network Advantage):
  Description: network-advantage
  Count: 2
  Version: 1.0
  Status: IN USE
```

```

Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: network-advantage
Enforcement type: NOT ENFORCED
License type: Perpetual
dna-advantage (C9500-16X DNA Advantage):
Description: C9500-16X DNA Advantage
Count: 2
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9500-16X DNA Advantage
Enforcement type: NOT ENFORCED
License type: Subscription

```

## 関連コマンド

コマンド	Description
<b>show license all</b>	権限付与情報を表示します。
<b>show license status</b>	ライセンスのコンプライアンスステータスを表示します。
<b>show license summary</b>	すべてのアクティブなライセンスの要約を表示します。
<b>show license udi</b>	UDI を表示します。
<b>show tech-support license</b>	デバッグ出力を表示します。

# show location

エンドポイントのロケーション情報を表示するには、特権 EXEC モードで **show location** コマンドを使用します。

## show location

[**admin-tag** | **civic-location***identifier identifier-string* | **interface** *type number* | **static** | **custom-location***identifier identifier-string* | **interface** *type number* | **static** | **elin-location***identifier identifier-string* | **interface** *type number* | **static** | **geo-location***identifier identifier-string* | **interface** *type number* | **static** | **host**]

構文の説明		
<b>admin-tag</b>		管理タグまたはサイト情報を表示します。
<b>civic-location</b>		都市ロケーション情報を指定します。
<b>identifier</b> <i>identifier-string</i>		シビックロケーション、カスタムロケーション、または地理空間的なロケーションの情報識別子。
<b>interface</b> <i>type number</i>		インターフェイスのタイプと番号  デバイスに対する番号付け構文については、疑問符 (?) のオンラインヘルプ機能を使用してください。
<b>static</b>		設定されたシビック、カスタム、または地理空間的ロケーション情報を表示します。
<b>custom-location</b>		カスタムロケーション情報を指定します。
<b>elin-location</b>		緊急ロケーション情報 (ELIN) を指定します。
<b>geo-location</b>		地理空間的なロケーション情報を指定します。
<b>host</b>		シビック、カスタム、または地理空間的なホストロケーション情報を指定します。

コマンド デフォルト      デフォルトの動作や値はありません。

コマンド モード          特権 EXEC

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

次の **show location civic-location** コマンドの出力例は、指定された識別子 (*identifier* 1) のシビックロケーション情報を表示します。

```
Device# show location civic-location identifier 1
Civic location information
-----
```

```
Identifier          : 1
County              : Santa Clara
Street number      : 3550
Building            : 19
Room                : C6
Primary road name   : Example
City                : San Jose
State               : CA
Country             : US
```

## 関連コマンド

コマンド	Description
<b>location</b>	エンドポイントにロケーション情報を設定します。

# show logging onboard switch uptime

システム内のすべてのモジュールまたはスイッチのすべてのリセット理由の履歴を表示するには、**show logging onboard switch uptime** コマンドを使用します。

**show logging onboard switch** { *switch-number* | **active** | **standby** } **uptime** [[[**continuous** | **detail**]] [**start** *hour day month* [*year*] [**end** *hour day month year*]]] | **summary**]

構文の説明	switch <i>switch-number</i>	スイッチを指定します。スイッチ番号を入力します。
	<b>active</b>	アクティブ インスタンスを指定します。
	<b>standby</b>	スタンバイ インスタンスを指定します。
	<b>continuous</b>	(任意) 連続データを表示します。
	<b>detail</b>	(任意) 詳細データを表示します。
	<b>start</b> <i>hour day month year</i>	(任意) データを表示する開始時刻を指定します。
	<b>end</b> <i>hour day month year</i>	(任意) データを表示する終了時刻を指定します。
	<b>summary</b>	(任意) 要約データを表示します。
コマンドモード	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
		このコマンドが以下に実装されました。
	Cisco IOS XE Gibraltar 16.10.1	このコマンドの出力が更新され、スタック内のメンバのリロード理由が表示されるようになりました。

次に例を示します。

次に、**show logging onboard switch active uptime continuous** コマンドの出力例を示します。

```
Device# show logging onboard switch active uptime continuous
-----
UPTIME CONTINUOUS INFORMATION
-----
Time Stamp           | Reset                | Uptime
MM/DD/YYYY HH:MM:SS | Reason              | years weeks days hours minutes
-----
06/17/2018 19:42:56  | Reload              | 0    0    0    0    5
06/17/2018 19:56:31  | Reload              | 0    0    0    0    5
```



```

06/17/2018 20:10:46 Reload 0 0 0 0 5
06/17/2018 20:23:48 Reload 0 0 0 0 5
06/17/2018 20:37:20 Reload Command 0 0 0 0 5
06/18/2018 17:09:23 Reload Command 0 0 0 20 5
06/18/2018 17:18:39 redundancy force-switchover 0 0 0 0 5
06/18/2018 18:33:33 Reload 0 0 0 1 5
06/18/2018 19:03:05 Reload 0 0 0 0 5
06/18/2018 19:40:30 Reload 0 0 0 0 5
06/18/2018 20:37:47 Reload 0 0 0 0 5
06/18/2018 20:51:13 Reload 0 0 0 0 5
06/18/2018 21:04:08 Reload 0 0 0 0 5
06/18/2018 21:18:23 Reload 0 0 0 0 5
06/18/2018 21:31:25 Reload 0 0 0 0 5
06/18/2018 21:45:15 Reload 0 0 0 0 5
06/18/2018 21:59:02 Reload 0 0 0 0 5
06/18/2018 22:11:41 Reload 0 0 0 0 5
06/18/2018 22:24:27 Reload 0 0 0 0 5
06/18/2018 22:39:14 Reload Command 0 0 0 0 4
06/19/2018 00:01:59 Reload Command 0 0 0 1 5
06/19/2018 00:13:21 redundancy force-switchover 0 0 0 0 5
06/19/2018 01:05:42 redundancy force-switchover 0 0 0 0 5
06/20/2018 02:37:16 redundancy force-switchover 0 0 1 1 5
06/20/2018 02:50:03 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:02:13 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:14:26 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:26:44 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:38:58 redundancy force-switchover 0 0 0 0 5
06/20/2018 03:52:43 redundancy force-switchover 0 0 0 0 5
06/20/2018 04:05:16 redundancy force-switchover 0 0 0 0 5
.
.
.

```

次に、**show logging onboard switch active uptime detail** コマンドの出力例を示します。

```
Device# show logging onboard switch active uptime detail
```

```
-----
UPTIME SUMMARY INFORMATION
-----
```

```

First customer power on : 06/10/2017 09:28:22
Total uptime           : 0 years 50 weeks 4 days 13 hours 38 minutes
Total downtime        : 0 years 15 weeks 4 days 11 hours 52 minutes
Number of resets      : 75
Number of slot changes : 9
Current reset reason   : PowerOn
Current reset timestamp : 09/17/2018 10:59:57
Current slot          : 1
Chassis type          : 0
Current uptime        : 0 years 0 weeks 0 days 0 hours 0 minutes
-----

```

```
-----
UPTIME CONTINUOUS INFORMATION
-----
```

```

Time Stamp | Reset | Uptime
MM/DD/YYYY HH:MM:SS | Reason | years weeks days hours minutes
-----|-----|-----
06/10/2017 09:28:22 | Reload | 0 0 0 0 0
<snip>
09/17/2018 09:07:44 | PowerOn | 0 0 3 15 5
09/17/2018 10:16:26 | Reload Command | 0 0 0 1 5
09/17/2018 10:59:57 | PowerOn | 0 0 0 0 5

```

次に、**show logging onboard switch standby uptime detail** コマンドの出力例を示します。

```
Device# show logging onboard switch standby uptime detail
```

```
-----
UPTIME SUMMARY INFORMATION
-----
```

```
First customer power on : 06/10/2017 11:51:26
Total uptime           : 0 years 46 weeks 0 days 11 hours 44 minutes
Total downtime        : 0 years 20 weeks 1 days 10 hours 45 minutes
Number of resets      : 79
Number of slot changes : 13
Current reset reason   : PowerOn
Current reset timestamp : 09/17/2018 10:59:57
Current slot          : 2
Chassis type          : 0
Current uptime        : 0 years 0 weeks 0 days 0 hours 5 minutes
-----
```

```
-----
UPTIME CONTINUOUS INFORMATION
-----
```

Time Stamp MM/DD/YYYY HH:MM:SS	Reset Reason	Uptime years weeks days hours minutes
06/10/2017 11:51:26	Reload	0 0 0 0 0
<snip>		
08/10/2018 09:13:58	LocalSoft	0 0 2 5 4
08/28/2018 14:21:42	Reload Slot Command	0 0 0 3 5
08/28/2018 14:34:29	System requested reload	0 0 0 0 0
09/11/2018 09:08:15	Reload	0 0 1 8 5
09/11/2018 19:15:06	redundancy force-switchover	0 0 0 9 4
09/13/2018 16:50:18	Reload Command	0 0 1 21 6
09/17/2018 10:55:09	PowerOn	0 0 0 0 5

次に、**show logging onboard switch active uptime summary** コマンドの出力例を示します。

```
Device# show logging onboard switch active uptime summary
```

```
-----
UPTIME SUMMARY INFORMATION
-----
```

```
First customer power on : 04/26/2018 21:45:39
Total uptime           : 0 years 20 weeks 2 days 12 hours 22 minutes
Total downtime        : 0 years 2 weeks 2 days 8 hours 40 minutes
Number of resets      : 1900
Number of slot changes : 18
Current reset reason   : Reload Command
Current reset timestamp : 09/26/2018 20:43:15
Current slot          : 1
Chassis type          : 91
Current uptime        : 0 years 0 weeks 5 days 22 hours 5 minutes
-----
```

## show mac address-table

MAC アドレステーブルを表示するには、**show mac address-table** コマンドを特権 EXEC モードで使用します。

```
show mac address-table [ address mac-addr [ interface type/number | vlan vlan-id ] | aging-time
[ routed-mac | vlan vlan-id ] | control-packet-learn | count [ summary | vlan vlan-id ] |
dynamic | secure | static ][ address mac-addr ][ interface type/number | vlan vlan-id ] | interface
type/number | learning [ vlan vlan-id ] | multicast [ count ][ igmp-snooping | mld-snooping |
user ][ vlan vlan-id ] | notification change [ interface [ type/number ] ] | mac-move | threshold
| vlan vlan-id ]
```

### 構文の説明

<b>address mac-addr</b>	(任意) 特定の MAC アドレスの MAC アドレス テーブルに関する情報を表示します。
<b>interface type/number</b>	(任意) 特定のインターフェイスのアドレスを表示します。
<b>vlan vlan-id</b>	(任意) 特定の VLAN のアドレスを表示します。
<b>aging-time [routed-mac   vlan vlan-id]</b>	(任意) ルーテッド MAC または VLAN のエージングタイムを表示します。
<b>control-packet-learn</b>	(任意) 制御パケットの MAC 学習パラメータを表示します。
<b>count</b>	(任意) MAC アドレス テーブル内の現在のエントリ数を表示します。
<b>dynamic</b>	(任意) ダイナミックアドレスのみを表示します。
<b>secure</b>	(任意) セキュア アドレスだけを表示します。
<b>static</b>	(任意) スタティックアドレスのみを表示します。
<b>learning</b>	(任意) VLAN またはインターフェイスの学習を表示します。
<b>multicast</b>	(任意) マルチキャスト MAC アドレス テーブル エントリに関する情報を表示します。
<b>igmp-snooping</b>	(任意) Internet Group Management Protocol (IGMP) スヌーピングによって学習されたアドレスを表示します。
<b>mld-snooping</b>	(任意) Multicast Listener Discover version 2 (MLDv2) スヌーピングによって学習されたアドレスを表示します。
<b>user</b>	(任意) 手動で入力した (スタティック) アドレスを表示します。
<b>notification change</b>	MAC 通知パラメータおよび履歴テーブルを表示します。

<b>notification mac-move</b>	MAC 移動通知ステータスを表示します。
<b>notification threshold</b>	連想メモリ (CAM) テーブル利用通知ステータスを表示します。

コマンドモード 特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
	Cisco IOS XE Gibraltar 16.12.4	シスコのソフトウェアデファインドアクセス (SD-Access) ソリューションに使用される MAC アドレスを表示するように <b>show mac address-table vlan vlan-id</b> コマンドが更新されました。

使用上のガイドライン *mac-addr* の値は 48 ビットの MAC アドレスです。有効なフォーマットは H.H.H です。

*interface-number* 引数では、モジュールとポート番号を指定します。有効値は、指定されたインターフェイスタイプ、および使用されるシャーシとモジュールによって異なります。たとえば、13 スロットシャーシに 48 ポート 10/100BASE-T イーサネット モジュールが搭載されている場合に、ギガビット イーサネット インターフェイスを指定すると、モジュール番号の有効値は 1 ~ 13、ポート番号の有効値は 1 ~ 48 になります。

次に、**show mac address-table** コマンドの出力例を示します。

```
Device# show mac address-table

          Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
All     0100.0ccc.cccc  STATIC   CPU
All     0100.0ccc.cccd  STATIC   CPU
All     0180.c200.0000  STATIC   CPU
All     0180.c200.0001  STATIC   CPU
All     0180.c200.0002  STATIC   CPU
All     0180.c200.0003  STATIC   CPU
All     0180.c200.0004  STATIC   CPU
All     0180.c200.0005  STATIC   CPU
All     0180.c200.0006  STATIC   CPU
All     0180.c200.0007  STATIC   CPU
All     0180.c200.0008  STATIC   CPU
All     0180.c200.0009  STATIC   CPU
All     0180.c200.000a  STATIC   CPU
All     0180.c200.000b  STATIC   CPU
All     0180.c200.000c  STATIC   CPU
All     0180.c200.000d  STATIC   CPU
All     0180.c200.000e  STATIC   CPU
All     0180.c200.000f  STATIC   CPU
All     0180.c200.0010  STATIC   CPU
All     0180.c200.0021  STATIC   CPU
All     ffff.ffff.ffff  STATIC   CPU
1       780c.f0e1.1dc3  STATIC   V11
51      0000.1111.2222  STATIC   V151
```

```

51      780c.f0e1.1dc6    STATIC    V151
1021   0000.0c9f.f45c    STATIC    V11021
1021   0002.02cc.0002    STATIC    Gi6/0/2
1021   0002.02cc.0003    STATIC    Gi6/0/3
1021   0002.02cc.0004    STATIC    Gi6/0/4
1021   0002.02cc.0005    STATIC    Gi6/0/5
1021   0002.02cc.0006    STATIC    Gi6/0/6
1021   0002.02cc.0007    STATIC    Gi6/0/7
1021   0002.02cc.0008    STATIC    Gi6/0/8
1021   0002.02cc.0009    STATIC    Gi6/0/9
1021   0002.02cc.000a    STATIC    Gi6/0/10

```

<output truncated>

次に、特定の MAC アドレスの MAC アドレステーブルを表示する例を示します。

```
Device# show mac address-table address fc58.9a02.7382
```

```

                Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1       fc58.9a02.7382   DYNAMIC     Te1/0/1
Total Mac Addresses for this criterion: 1

```

次に、特定の VLAN に現在設定されているエージングタイムを表示する例を示します。

```
Device# show mac address-table aging-time vlan 1
```

```

Global Aging Time: 300
Vlan    Aging Time
----    -
1       300

```

次に、特定のインターフェイスの MAC アドレステーブルに関する情報を表示する例を示します。

```
Device# show mac address-table interface TenGigabitEthernet1/0/1
```

```

                Mac Address Table
-----
Vlan    Mac Address      Type        Ports
----    -
1       fc58.9a02.7382   DYNAMIC     Te1/0/1
Total Mac Addresses for this criterion: 1

```

次に、MAC 移動通知ステータスを表示する例を示します。

```
Device# show mac address-table notification mac-move
```

```
MAC Move Notification: Enabled
```

次に、CAM テーブル利用通知ステータスを表示する例を示します。

```
Device# show mac address-table notification threshold
```

```

                Status      limit      Interval
-----+-----+-----

```

```
enabled          50          120
```

次に、特定のインターフェイスの MAC 通知パラメータと履歴テーブルを表示する例を示します。

```
Device# show mac address-table notification change interface tenGigabitEthernet1/0/1
```

```
MAC Notification Feature is Disabled on the switch
Interface                               MAC Added Trap MAC Removed Trap
-----                               -
TenGigabitEthernet1/0/1                 Disabled       Disabled
```

次に、特定の VLAN の MAC アドレステーブルに関する情報を表示する例を示します。



(注) シスコの SD-Access ソリューションを使用している場合は、CP\_LEARN タイプの MAC アドレスが表示されます。

```
Device# show mac address-table vlan 1021
```

```
Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1021    0000.0c9f.f45c   STATIC    Vl1021
1021    0002.02cc.0002   STATIC    Gi6/0/2
1021    0002.02cc.0003   STATIC    Gi6/0/3
1021    0002.02cc.0004   STATIC    Gi6/0/4
1021    0002.02cc.0005   STATIC    Gi6/0/5
1021    0002.02cc.0006   STATIC    Gi6/0/6
1021    0002.02cc.0007   STATIC    Gi6/0/7
1021    0002.02cc.0008   STATIC    Gi6/0/8
1021    0002.02cc.0009   STATIC    Gi6/0/9
1021    0002.02cc.000a   STATIC    Gi6/0/10
1021    0002.02cc.000b   STATIC    Gi6/0/11
1021    0002.02cc.000c   STATIC    Gi6/0/12
1021    0002.02cc.000d   STATIC    Gi6/0/13
1021    0002.02cc.000e   STATIC    Gi6/0/14
1021    0002.02cc.000f   STATIC    Gi6/0/15
1021    0002.02cc.0010   STATIC    Gi6/0/16
1021    0002.02cc.0011   STATIC    Gi6/0/17
1021    0002.02cc.0012   STATIC    Gi6/0/18
1021    0002.02cc.0013   STATIC    Gi6/0/19
1021    0002.02cc.0014   STATIC    Gi6/0/20
.
.
.
1021    0002.0100.0001   CP_LEARN  Tu0
1021    0002.0100.0002   CP_LEARN  Tu0
1021    0002.0100.0003   CP_LEARN  Tu0
1021    0002.0100.0004   CP_LEARN  Tu0
1021    0002.0100.0005   CP_LEARN  Tu0
1021    0002.0100.0006   CP_LEARN  Tu0
1021    0002.0100.0007   CP_LEARN  Tu0
1021    0002.0100.0008   CP_LEARN  Tu0
1021    0002.0100.0009   CP_LEARN  Tu0
```

```
1021    0002.0100.000a    CP_LEARN    Tu0
Total Mac Addresses for this criterion: 114
```

次の表で、**show mac address-table** の出力に表示される重要なフィールドを説明します。

表 12: **show mac address-table** フィールドの説明

フィールド	説明
VLAN	VLAN 番号。
Mac Address	エントリの MAC アドレス。
タイプ	アドレスのタイプ。
ポート	ポートタイプ。
Total MAC addresses	MAC アドレステーブルの合計 MAC アドレス数。

#### 関連コマンド

コマンド	説明
<b>clear mac address-table</b>	MAC アドレス テーブルからダイナミック エントリを削除します。

# show mac address-table move update

デバイス上の MAC アドレステーブル移動更新情報を表示するには、EXEC モードで **show mac address-table move update** コマンドを使用します。

## show mac address-table move update

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンド デフォルト

デフォルトの動作や値はありません。

### コマンド モード

ユーザ EXEC

特権 EXEC

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

### 例

次に、**show mac address-table move update** コマンドの出力例を示します。

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```



## show parser encrypt file status

プライベート設定の暗号化ステータスを表示するには、**show parser encrypt file status** コマンドを使用します。

### show parser encrypt file status

#### 構文の説明

このコマンドには引数またはキーワードはありません。

#### コマンドデフォルト

なし

#### コマンドモード

ユーザ EXEC

#### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

#### 例

次のコマンド出力は、機能が使用可能で、ファイルが暗号化されていることを示します。ファイルは「暗号テキスト」形式です。

```
Device> enable
Device# show parser encrypt file status
Feature:           Enabled
File Format:       Cipher text
Encryption Version: ver1
```

#### 関連コマンド

コマンド	説明
<b>service private-config-encryption</b>	プライベート設定ファイルの暗号化を有効にします。

# show platform hardware fpga

システムのフィールドプログラマブルゲートアレイ（FPGA）の設定を表示するには、特権 EXEC モードで **show platform hardware fpga** コマンドを使用します。

## show platform hardware fpga

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンド デフォルト

なし

### コマンド モード

特権 EXEC (#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Fuji 16.9.1	このコマンドが導入されました。

### 例

次に、Cisco Catalyst 9300 シリーズ スイッチでの **show platform hardware fpga** コマンドの出力例を示します。

```
Device# show platform hardware fpga
```

```
Register Addr          FPGA Reg Description          Value
-----
0x00000000             Board ID                      0x00006053
0x00000004             FPGA Version                  0x00000206
0x00000008             Reset Reg1                    0x00010204
0x0000000c             Reset Reg2                    0x00000000
0x00000028             FRU LED DATA Reg1           0x00001008
0x0000002c             FRU LED DATA Reg2           0x00001008
0x00000030             FRU Control Reg              0x0000c015
0x00000034             Doppler Misc Reg             0x00000311
0x00000010             SBC Enable                    0x0000000f
<snip>
```

次に、Cisco Catalyst 9500 シリーズ スイッチでの **show platform hardware fpga** コマンドの出力例を示します。

```
Device# show platform hardware fpga
```

```
Register Addr          FPGA Reg Description          Value
-----
0x00000000             FPGA Version                  0x00000110
0x00000040             FRU Power Cntrl Reg          0x00000112
0x00000020             System Reset Cntrl Reg       0x00000000
0x00000024             Beacon LED Cntrl Reg         0x00000000
0x00000044             1588 Sync Pulse Reg         0x00000000
0x00000048             Mainboard Misc Cntrl Reg     0x0000000a
0x00000038             DopplerD Misc Cntrl Reg     0x000000ff
<snip>
```

## show platform integrity

起動段階のチェックサムレコードを表示するには、特権 EXEC モードで **show platform integrity** コマンドを使用します。

**show platform integrity** [**sign** [**nonce** <nonce>]]

### 構文の説明

**sign** (任意) 署名を表示します。

**nonce** (任意) ナンス値を入力します。

### コマンドモード

特権 EXEC (#)

### コマンド履歴

リリース 変更内容  
ス

このコマンドが導入されました。

### 例

次に、起動段階のチェックサムレコードを表示する例を示します。

```
Device# show platform integrity sign
```

```
PCR0: EE47F8644C2887D9BD4DE3E468DD27EB93F4A606006A0B7006E2928C50C7C9AB
PCR8: E7B61EC32AFA43DA1FF4D77F108CA266848B32924834F5E41A9F6893A9CB7A38
Signature version: 1
Signature:
816C5A29741BBAC1961C109FFC36DA5459A44DBF211025F539AFB4868EF91834C05789
5DAFBC7474F301916B7D0D08ABE5E05E66598426A73E921024C21504383228B6787B74
8526A305B17DAD3CF8705BACFD51A2D55A333415CABC73DAFDEEFD8777AA77F482EC4B
731A09826A41FB3EFFC46DC02FBA666534DBEC7DCC0C029298DB8462A70DBA26833C2A
1472D1F08D721BA941CB94A418E43803699174572A5759445B3564D8EAE57D64AE304
EE1D2A9C53E93E05B24A92387E261199CED8D8A0CE7134596FF8D2D6E6DA773757C70C
D3BA91C43A591268C248DF32658999276FB972153ABE823F0ACFE9F3B6F0AD1A00E257
4A4CC41C954015A59FB8FE
Platform: WS-C3650-12X48UZ
```

# show platform software audit

SE Linux 監査ログを表示するには、特権 EXEC モードで **show platform software audit** コマンドを使用します。

```
show platform software audit {all | summary | [switch {switch-number | active | standby}]
{0 | F0 | R0 | {FP | RP} {active}}}
```

構文の説明		
	<b>all</b>	すべてのスロットからの監査ログを表示します。
	<b>summary</b>	すべてのスロットからの監査ログの要約カウントを表示します。
	<b>switch</b>	特定のスイッチのスロットについての監査ログを表示します。
	<i>switch-number</i>	指定したスイッチ番号のスイッチを選択します。
	<b>switch active</b>	スイッチのアクティブインスタンスを選択します。
	<b>standby</b>	スイッチのスタンバイインスタンスを選択します。
	<b>0</b>	SPA インターフェイス プロセッサ スロット 0 の監査ログを表示します。
	<b>F0</b>	Embedded-Service-Processor スロット 0 の監査ログを表示します。
	<b>R0</b>	Route-Processor スロット 0 の監査ログを表示します。
	<b>FP active</b>	アクティブな Embedded-Service-Processor スロットの監査ログを表示します。
	<b>RP active</b>	アクティブな Route-Processor スロットの監査ログを表示します。

コマンドモード 特権 EXEC (#)

## コマンド履歴

使用上のガイドライン このコマンドは、Cisco IOS XE Gibraltar 16.10.1 で SELinux 許可モード機能の一部として導入されました。**show platform software audit** コマンドは、アクセス違反イベントを含むシステムログを表示します。

Cisco IOS XE Gibraltar 16.10.1 では、許可モードでの操作は、IOS XE プラットフォームの特定のコンポーネント（プロセスまたはアプリケーション）を制限する目的で利用できます。許可モードでは、アクセス違反イベントが検出され、システムログが生成されますが、イベントまたは操作自体はブロックされません。このソリューションは、主にアクセス違反検出モードで動作します。

次に、**show software platform software audit summary** コマンドの出力例を示します。

```
Device# show software platform software audit summary
```

```
=====
AUDIT LOG ON switch 1
-----
AVC Denial count: 58
=====
```

次に、**show software platform software audit all** コマンドの出力例を示します。

```
Device# show software platform software audit all
```

```
=====
AUDIT LOG ON switch 1
-----
===== START =====
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438600.896:119): avc: denied { execute } for pid=8300 comm="sh"
name="id" dev="loop0" ino=6982
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438600.897:120): avc: denied { execute_no_trans } for pid=8300
comm="sh"
path="/tmp/sw/mount/cat9k-rpbase.2018-10-02_00.13_mhungund.SSA.pkg/nyquist/usr/bin/id"
dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438615.535:121): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
```

```

tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc: denied { execute_no_trans } for pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc: denied { execute_no_trans } for pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539440246.697:149): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539440299.119:150): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
===== END =====
=====

```

次に、**show software platform software audit switch** コマンドの出力例を示します。

```
Device# show platform software audit switch active R0
```

```

===== START =====
type=AVC msg=audit(1539222292.584:100): avc: denied { read } for pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc: denied { getattr } for pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sdal" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc: denied { getattr } for pid=14028 comm="ls"
path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc: denied { read } for pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438624.916:122): avc: denied { execute_no_trans } for pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc: denied { execute_no_trans } for pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc: denied { name_connect } for pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc: denied { execute_no_trans } for pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0

```

```
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc: denied { execute_no_trans } for pid=10858
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc: denied { execute_no_trans } for pid=11579
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc: denied { name_connect } for pid=26421
 comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc: denied { execute_no_trans } for pid=12451
 comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438860.907:130): avc: denied { name_connect } for pid=26421
 comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
===== END =====
=====
```

# show platform software fed switch punt cause

インターフェイスで受信したパケットがルータプロセッサ（RP）にパントされている理由に関する情報を表示するには、特権 EXEC モードで **show platform software fed switch punt cpuq cause** コマンドを使用します。

**show platform software fed switch** *switch-number* | **active** | **standby** *puntcause\_id* | **clear** | **summary**

## 構文の説明

**switch** {*switch-number* | **active** | **standby**}

スイッチに関する情報を表示します。次の選択肢があります。

- *switch-number*。
- **active** : アクティブなスイッチに関する情報を表示します。
- **standby** : 存在する場合、スタンバイスイッチに関する情報を表示します。

(注) このキーワードはサポートされていません。

*cause\_id* 詳細を表示する必要がある原因の ID を指定します。

**clear** すべての原因の統計をクリアします。原因をクリアすると、統計に矛盾が生じる可能性があります。

**summary** パント理由の概要を表示します。

コマンド デフォルト なし

コマンド モード 特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

使用上のガイドライン なし

## 例

次に、**show platform software fed switch active punt cause summary** コマンドの出力例を示します。

```
Device# show platform software fed switch active punt cause summary
Statistics for all causes
```

Cause	Cause Info	Rcvd	Dropped
7	ARP request or response	1	0
21	RP<->QFP keepalive	22314	0



```
55    For-us control                12          0
60    IP subnet or broadcast packet  21          0
96    Layer2 control protocols      133808     0
-----
```

次に、**show platform software fed switch active punt cause *cause-id*** コマンドの出力例を示します。

```
Device# show platform software fed switch active punt cause 21
Detailed Statistics
```

```
Sub Cause      Rcvd          Dropped
-----
0              22363         0
-----
```

## show platform software fed switch punt cpuq

CPU キューのパントトラフィックに関する情報を表示するには、特権 EXEC モードで **show platform software fed switch punt cpuq** コマンドを使用します。

```
show platform software fed switch switch-number | active | standby punt cpuq cpuq_id |
all | brief | clear | rates
```

構文の説明		
	<b>switch</b> { <i>switch-number</i> <b>active</b> <b>standby</b> }	スイッチに関する情報を表示します。次の選択肢があります。 <ul style="list-style-type: none"> <li>• <i>switch-number</i>。</li> <li>• <b>active</b> : アクティブなスイッチに関する情報を表示します。</li> <li>• <b>standby</b> : 存在する場合、スタンバイスイッチに関する情報を表示します。</li> </ul> <p>(注) このキーワードはサポートされていません。</p>
	<b>punt</b>	パント情報を表示します。
	<b>cpuq</b>	CPU 受信キューに関する情報を表示します。
	<i>cpuq_id</i>	特定の CPU キューに固有の詳細を指定します。
	<b>all</b>	すべての CPU キューの統計を表示します。
	<b>brief</b>	受信およびドロップされたパントパケットの詳細など、すべてのキューの要約された統計を表示します。
	<b>clear</b>	すべての CPU キューの統計をクリアします。CPU キューをクリアすると、統計に矛盾が生じる可能性があります。
	<b>rates</b>	パケットのパントレートを表示します。
コマンド デフォルト	なし	
コマンド モード	特権 EXEC (#)	

コマンド履歴	リリース	変更内容
	Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

使用上のガイドライン なし

## 例

次に、**show platform software fed switch active punt cpuq brief** コマンドの出力例を示します。

```
Device#show platform software fed switch active punt cpuq brief
```

```
Punt CPU Q Statistics Brief
```

Q no	Queue Name	Rx prev	Rx cur	Rx delta	Drop prev	Drop cur	Drop delta
0	CPU_Q_DOT1X_AUTH	0	0	0	0	0	0
1	CPU_Q_L2_CONTROL	0	6772	6772	0	0	0
2	CPU_Q_FORUS_TRAFFIC	0	0	0	0	0	0
3	CPU_Q_ICMP_GEN	0	0	0	0	0	0
4	CPU_Q_ROUTING_CONTROL	0	12	12	0	0	0
5	CPU_Q_FORUS_ADDR_RESOLUTION	0	1	1	0	0	0
6	CPU_Q_ICMP_REDIRECT	0	0	0	0	0	0
7	CPU_Q_INTER_FED_TRAFFIC	0	0	0	0	0	0
8	CPU_Q_L2LVX_CONTROL_PKT	0	0	0	0	0	0
9	CPU_Q_EWLC_CONTROL	0	0	0	0	0	0
10	CPU_Q_EWLC_DATA	0	0	0	0	0	0
11	CPU_Q_L2LVX_DATA_PKT	0	0	0	0	0	0
12	CPU_Q_BROADCAST	0	21	21	0	0	0
13	CPU_Q_LEARNING_CACHE_OVFL	0	0	0	0	0	0
14	CPU_Q_SW_FORWARDING	0	0	0	0	0	0
15	CPU_Q_TOPOLOGY_CONTROL	0	127300	127300	0	0	0
16	CPU_Q_PROTO_SNOOPING	0	0	0	0	0	0
17	CPU_Q_BFD_LOW_LATENCY	0	0	0	0	0	0
18	CPU_Q_TRANSIT_TRAFFIC	0	0	0	0	0	0
19	CPU_Q_RPF_FAILED	0	0	0	0	0	0
20	CPU_Q_MCAST_END_STATION_SERVICE	0	0	0	0	0	0

## show platform software fed switch punt cpuq

```

21 CPU_Q_LOGGING          0      0      0      0      0      0
22 CPU_Q_PUNT_WEBAUTH     0      0      0      0      0      0
23 CPU_Q_HIGH_RATE_APP    0      0      0      0      0      0
24 CPU_Q_EXCEPTION        0      0      0      0      0      0
25 CPU_Q_SYSTEM_CRITICAL  0      0      0      0      0      0
26 CPU_Q_NFL_SAMPLED_DATA 0      0      0      0      0      0
27 CPU_Q_LOW_LATENCY      0      0      0      0      0      0
28 CPU_Q_EGR_EXCEPTION    0      0      0      0      0      0
29 CPU_Q_FSS              0      0      0      0      0      0
30 CPU_Q_MCAST_DATA       0      0      0      0      0      0
31 CPU_Q_GOLD_PKT         0      0      0      0      0      0

```

次の表で、この出力に表示される重要なフィールドを説明します。

表 13: *show platform software fed switch active punt cpuq brief* フィールドの説明

フィールド	Description
Q no	キューの ID。
Queue Name	キューの名前。
Rx	受信されたパケット数。
ドロップ	ドロップされたパケットの数

次に、**show platform software fed switch active punt cpuq cpuq\_id** コマンドの出力例を示します。

```
Device#show platform software fed switch active punt cpuq 1
```

```

Punt CPU Q Statistics
=====
CPU Q Id          : 1
CPU Q Name        : CPU_Q_L2_CONTROL
Packets received from ASIC : 6774
Send to IOSd total attempts : 6774
Send to IOSd failed count  : 0
RX suspend count   : 0
RX unsuspend count : 0
RX unsuspend send count : 0
RX unsuspend send failed count : 0
RX consumed count  : 0
RX dropped count   : 0
RX non-active dropped count : 0

```

```
RX conversion failure dropped : 0
RX INTACK count               : 6761
RX packets dq'd after intack  : 0
Active RxQ event               : 6761
RX spurious interrupt         : 0
```

```
Replenish Stats for all rxq:
```

```
-----
Number of replenish           : 61969
Number of replenish suspend   : 0
Number of replenish un-suspend : 0
-----
```

## show platform software sl-infra

トラブルシューティング情報を表示し、デバッグに関する情報を表示するには、特権 EXEC モードで **show platform software sl-infra** コマンドを入力します。このコマンドの出力は、テクニカルサポートチームがトラブルシューティングとデバッグに使用します。

**show platform software sl-infra all | current | debug | stored**

### 構文の説明

**all** 現在の情報、デバッグ情報、および保存されている情報を表示します。

**current** 現在のライセンス関連情報を表示します。

**debug** デバッグを有効にします。

**stored** 製品インスタンスに保存されている情報を表示します。

### コマンドモード

特権 EXEC (Device#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.3.2a	このコマンドが導入されました。

### 使用上のガイドライン

解決できないエラーメッセージが表示された場合は、コンソールまたはシステムログに表示されるメッセージとともに、シスコのテクニカルサポート担当者に **show license tech support**、**show license history message**、および **show platform software sl-infra all** 特権 EXEC コマンドの出力例を提供してください。

# show platform sudi certificate

特定の SUDI のチェックサムレコードを表示するには、特権 EXEC モードで **show platform sudi certificate** コマンドを使用します。

**show platform sudi certificate** [**sign** [**nonce** <nonce>]]

構文の説明	<b>sign</b>	(任意) 署名を表示します。
	<b>nonce</b>	(任意) ナンス値を入力します。
コマンドモード	特権 EXEC (#)	
コマンド履歴	リリー	変更内容
	ス	
	このコマンドが導入されました。	

## 例

次に、特定の SUDI のチェックサムレコードを表示する例を示します。

```
# show platform sudi certificate

-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBqkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwGgEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5j0AmaHBKeN8hF570YQXJ
FcjPFto1YmUQ6iEqDGYeJu5Tm8sUxJsZr2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUL4F1pyXOWWQCZe+36ufijXWLBvLd6ZeYpzPEApk0E5tziVmw/VgpSdh
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1a06g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
olEwTzALBgNVHQ8EBAMCAyYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFbi71R803UXHOjgxkhLtv5MOhmBVRBW7hmW
Yqpa02TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+fffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YaretIpsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEblfJU9u6ju7AQ7L4
CYNu/2bPPu8XslgYJQk0XuPL1hs27PKSb3TkL4Eq1ZKR4OCXPDJoBYVl0fdX4lId
kxpUnwVwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----
MIIEPDCAySgAwIBAgIKYQ1ufQAAAAADDANBqkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTvURJIENBMTIBIjANBqkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAm5l3THIXa9tN/hs5qR/6UZRpdd+9aE2JbFknjht6gfHKd477AkS
5XAtUs5oxDYvt/zEbs1Zq3+LR6grqKQVu6JYvh05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYzo3qPCpxzprWJDPclM4iYKHumMQmqmgmg+
xghHl0oWS80BocdiynEbeP5rZ7qRuewKmp11TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXDgJ13oVeF+EyFwLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAyVwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBRR12PhxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAwBQn
```

## show platform sudi certificate

```

88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRWoi8vd3d3
LmNpc2NvLmNvbS9zZW50cm10eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
BQcBAQREMEIwQAYIKwYBBQUHMAKGNgh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEAAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2l2Y28uY29tL3N1Y3VyXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGAlUdEwEB/wQIMAYBAf8CAQAwdQYJ
KoZlIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIffi9b9+GbMSJbi
ZHc/CcC101Ju0a9zTXA9w47H9/t61eduGxb4WeLxcwCiUgvFtCa51Ikl8nNbcKY
/4dwlex+7amATUQO4QggIE67wVlPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjoNpK/urSRI14WdIlplR1nH7KND15618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfy8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIDctWkMA0GCSqGSIb3DQEBCwUAMCcxDjAMBgNVBAoTBUNp
c2NvMRUwEwYDQDEwxBQ1QyIFNVREkgQ0EwHhcNMTUwODA2MDgwODI5WhcNMjUw
ODA2MDgwODI5WjBzMSwwKgYDVQQFEyNQSUQ6V1MtQzM2NTAtMTJYNdhVWVlBTtjP
RE8xOTMyWDAwQzEOMAwGA1UEChMFQ2l2Y28xGDAwBGNVBAStD0FDVC0yIEExpdGUg
U1VESTeZMBcGA1UEAxMQV1MtQzM2NTAtMTJYNdhVWVjCCASlWdQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANZxOGYI0eU14HcSwjL4HO75qTj19C2BHG3ufce9ikkN
xwGXi8qg8vKxub9tRYRaJC5bP1Wmoq7+ZJtQA079xE4X14soNbkq5NaUhh7RB1wD
iRUJvTfCozVICbNfbzvtB30I75tCarFNmpd0K6AFrIa41U988QGqaCj7R1JrYNa
jnc73UXXM/hc0HtNR5mhyqer5Y2qjjzo6tHZYqrrx2eS1XOa262ZSQriAxmaH/KLC
K97ywyRbdJlxBRX3hGtKlog8nASB8WpXqB9NVCERzUajwU3L/kg2BsCqw9Y2m7HW
U1cerTxgthuyUkdNI+Jg6iGAp2+s8E9hsHPBPMCdIsCAwEAAANvMG0wDgYDVR0P
AQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwTQYDVR0RBEEYwRKBCBgkrBgEEAQkVAgOg
NRMzQ2hpcE1EPVVZSk5ORmRRR1FvN1ZlVmxJRTlqZENBeU9DQXhPRG93TlRveE1T
QVg5eWc9MA0GCSqGSIb3DQEBCwUAA4IBAQBKicTRZbVCRjVIR5MQcWXUT086v6Ej
HahDHTts3YpQoyAvfioNg2x8J6EXcEau4voyVu+eMUuoNL4szPhmmDcULfiCGBcA
/R3EFuoVMIzNT0gezIytsCf728KGw1oGuosgvjNGOOahUELu4+F/My7bIJNBH+PD
KjIFmhJpJg0F3q17yClAeXvd13g3W393i35d00Lm5L1WbBfQTyBaOLAbxsHvutrX
ulVZ5sdqSTwTkk09vKMaQjh7a8J/AmJi93jvzM69pe5711P1zqZfYfpiJ3cyJ0xf
I4brQ1smdczloFD4asF7A+1vor5e4VDBP0ppmeFAJvcQ52Jtpj0M0o1D
-----END CERTIFICATE-----

```



## show running-config

現在実行されている設定ファイルまたは特定のモジュールのレイヤ 2 VLAN、クラスマップ、インターフェイス、マップクラス、ポリシーマップ、または仮想回線（VC）クラスの設定の内容を表示するには、**show running-config** コマンドを特権 EXEC モードで使用します。

**show running-config** [*options*]

### 構文の説明

オプション（任意）出力のカスタマイズに使用されるキーワード。複数のキーワードを入力できません。

- **aaa** [**accounting** | **attribute** | **authentication** | **authorization** | **diameter** | **group** | **ldap** | **miscellaneous** | **radius-server** | **server** | **tacacs-server** | **user-name** | **username**] : AAA の設定を表示します。
- **all** : デフォルトパラメータで設定されたコマンドを含むように出力を展開します。**all** キーワードを使用しない場合、デフォルトパラメータで設定されたコマンドは出力に表示されません。
- **bridge-domain** {**id** | **parameterized vlan**} : ブリッジドメインの実行中コンフィギュレーションを表示します。
- **brief** : 認定データや暗号化されたフィルタの詳細なしで設定を表示します。
- **class-map** [*name*] [**linenum**] : クラスマップ情報を表示します。
- **cts** [**interface** | **policy-server** | **rbm-rbac** | **server** | **sxp**] : Cisco TrustSec の設定を表示します。
- **deprecated** : 実行中コンフィギュレーションとともに廃止された設定を表示します。
- **eap** {**method** | **profiles**} : EAP 方式の設定とプロファイルを表示します。
- **flow** {**exporter** | **monitor** | **record**} : グローバル フロー コンフィギュレーション コマンドを表示します。
- **full** : 完全な設定を表示します。
- **identity** {**policy** | **profile**} : アイデンティティ プロファイルまたはポリシー情報を表示します。

- **interface** *type number* : インターフェイス固有の設定情報を表示します。**interface** キーワードを使用する場合は、インターフェイスタイプとインターフェイス番号（たとえば、**interface GigabitEthernet 1/0/1** など）を指定する必要があります。システムで使用できるインターフェイスを特定するには、**show run interface ?** コマンドを使用します。
- **ip dhcp pool** [*name*] : IPv4 DHCP プールの設定を表示します。
- **ipv6 dhcp pool** [*name*] : IPv6 DHCP プールの設定を表示します。
- **linenum** [**brief** | **full** | **partition**] : 出力の行番号を表示します。
- **map-class** [**atm** | **dialer** | **frame-relay**] [*name*] : マップクラス情報を表示します。
- **mdns-sd** [**gateway** | **location-group** | **service-definition** | **service-list** | **service-peer** | **service-policy**] : マルチキャスト DNS サービス検出 (mDNS-SD) の設定を表示します。
- **partition** {**access-list** | **class-map** | **common** | **global-cdp** | **interface** | **ip-as-path** | **ip-community** | **ip-prefix-list** | **ip-static-routes** | **line** | **policy-map** | **route-map** | **router snmp** | **tacacs**} : パーティションに対応する設定を表示します。
- **policy-map** [*name*] [**linenum**] : ポリシーマップ情報を表示します。
- **switch** *number* : 指定したスイッチの設定を表示します。
- **view** [**full**] : 完全な実行中のコンフィギュレーションを表示可能にします。これは、通常、特定のビューにアクセスする権限がある設定コマンドのみを表示できるビューベースのユーザ向けです。
- **vlan** [*vlan-id*] : 特定の VLAN 情報を表示します。有効な値は 1 ~ 4094 です。
- **vrf** [*vrf-name*] : 仮想ルーティングおよび転送 (VRF) 対応設定のモジュール番号を表示します。

## コマンド デフォルト

デフォルトシンタックスの **show running-config** では、デフォルトパラメータを使用して設定されたコマンドを除き、実行中コンフィギュレーションの内容を表示します。

## コマンド モード

特権 EXEC (#)

## コマンド履歴

リリース

変更内容

Cisco IOS XE Gibraltar 16.11.1 このコマンドが導入されました。

## 使用上のガイドライン

**show running-config** コマンドは、技術的には **more system:running-config** コマンドのコマンドエイリアス（代替シンタックスまたは置換シンタックス）です。より多くのコマンドを使用することを推奨しますが（プラットフォーム間で構造が統一されており、拡張可能なシンタックスであるため）、**show running-config** コマンドは、幅広く使用し、**show run** などのショートカットを入力できるように有効のままになっています。

**show running-config interface** コマンドは、複数のインターフェイスがある場合に特定のインターフェイスの設定を確認する際に役立ちます。

**linenum** キーワードを指定すると、行番号が出力に表示されます。このオプションは、非常に大規模な設定の特定の部分を識別するのに役立ちます。

オプションのキーワードの後にパイプ文字 (|) を含めることで、コマンドシンタックスに追加の出力修飾子を入力できます。たとえば、**show running-config interface GigabitEthernet 1/0/1 linenum | begin 3** などです。キーワードに使用可能な出力修飾子を表示するには、キーワードの後に **|?** を入力します。使用しているプラットフォームによって、*options* 引数のキーワードと引数は異なる場合があります。

**show running-config all** コマンドは、デフォルト設定や値を含めて、完全な設定情報を表示します。たとえば、Cisco Discovery Protocol (出力では CDP と省略) の保留時間の値がデフォルトの 180 に設定されているとします。

- **show running-config** コマンドではこの値が表示されません。
- **show running-config all** では `cdp holdtime 180` を出力します。

Cisco Discovery Protocol の保留時間をデフォルト以外の値 (100 など) に変更すると、**show running-config** コマンドと **show running-config all** コマンドの出力は同じになります。つまり、設定したパラメータが出力されます。

**show running-config** コマンドは ACL 情報を表示します。出力から ACL 情報を除外するには、**show running | section exclude ip access | access list** コマンドを使用します。

## 例

次に、GigabitEthernet0/0 インターフェイスを設定する例を示します。フィールドの説明は自明です。

```
Device# show running-config interface gigabitEthernet0/0

Building configuration...

Current configuration : 130 bytes
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 ip address 10.5.20.10 255.255.0.0
 negotiation auto
 ntp broadcast
end
```

次に、コマンド出力に行番号を設定し、出力修飾子を使用して 10 行目から表示を開始する例を示します。フィールドの説明は自明です。

```
Device# show running-config linenum | begin 10

 10 : boot-start-marker
 11 : boot-end-marker
 12 : !
 13 : no logging buffered
 14 : enable password #####
 15 : !
 16 : spe 1/0 1/7
 17 : firmware location bootflash:mica-modem-pw.10.16.0.0.bin
```

```

18 : !
19 : !
20 : resource-pool disable
21 : !
22 : no aaa new-model
23 : ip subnet-zero
24 : ip domain name cisco.com
25 : ip name-server 172.16.11.48
26 : ip name-server 172.16.2.133
27 : !
28 : !
29 : isdn switch-type primary-5ess
30 : !
.
.
.
126 : end

```

**show running-config** コマンドの次の出力例では、**shape average** コマンドによって ATM のトラフィックシェーピングのオーバーヘッドアカウンティングが有効になっていることが示されています。BRAS-DSLAM のカプセル化タイプは **qinq** で、加入者回線のカプセル化タイプは ATM アダプテーション層 5 (AAL5) に基づき **snap-rbe** になります。フィールドの説明は自明です。

```

Device# show running-config
.
.
.
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average percent 10 account qinq aal5 snap-rbe
!

```

次に、**show running-config class-map** コマンドの出力例を示します。出力にはフィールドの説明も表示されます。

```

Device# show running-config class-map

Building configuration...

Current configuration : 2157 bytes
!
class-map match-any system-cpp-police-ewlc-control
  description EWLC Control
class-map match-any system-cpp-police-topology-control
  description Topology control
class-map match-any system-cpp-police-sw-forward
  description Sw forwarding, L2 LVX data packets, LOGGING, Transit Traffic
class-map match-any system-cpp-default
  description EWLC Data, Inter FED Traffic

```

```
class-map match-any system-cpp-police-sys-data
  description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any system-cpp-police-high-rate-app
  description High Rate Applications
class-map match-any system-cpp-police-multicast
  description MCAST Data
class-map match-any system-cpp-police-l2-control
  description L2 control
class-map match-any system-cpp-police-dot1x-auth
  description DOT1X Auth
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
  description Stackwise Virtual OOB
...
```

次に、teletype (tty) 回線 2 が 2 番目のコアとの通信用に予約されている例を示します。

```
Device# show running

Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname device
!
enable password lab
!
no ip subnet-zero
!
!
!
interface Ethernet0
 ip address 10.25.213.150 255.255.255.128
 no ip directed-broadcast
 no logging event link-status
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip default-gateway 10.25.213.129
```

```

ip classless
ip route 0.0.0.0 0.0.0.0 10.25.213.129
!
!
line con 0
  transport input none
line 1 6
  no exec
  transport input all
line 7
  no exec
  exec-timeout 300 0
  transport input all
line 8 9
  no exec
  transport input all
line 10
  no exec
  transport input all
  stopbits 1
line 11 12
  no exec
  transport input all
line 13
  no exec
  transport input all
  speed 115200
line 14 16
  no exec
  transport input all
line aux 0
line vty 0 4
  password cisco
  login
!
end

```

## 関連コマンド

Command	Description
<b>copy running-config startup-config</b>	実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします ( <b>copy system:running-config nvram:startup-config</b> コマンドのコマンドエイリアス)。
<b>show startup-config</b>	NVRAM の内容を表示するか (存在していて有効な場合)、または CONFIG_FILE 環境変数によって指定されている設定ファイルを表示します ( <b>more:nvram startup-config</b> コマンドのコマンドエイリアス)。

## show sdm prefer

特定の機能用のシステムリソースを最大にするために使用できるテンプレートに関する情報を表示するには、特権 EXEC モードで **show sdm prefer** コマンドを使用します。現在のテンプレートを表示するには、キーワードを指定せずにコマンドを使用します。

**show sdm prefer** [ advanced ]

構文の説明	<b>advanced</b> (任意) 高度なテンプレートに関する情報を表示します。
コマンドデフォルト	デフォルトの動作や値はありません。
コマンドモード	特権 EXEC
コマンド履歴	リリース <span style="float: right;">変更内容</span> Cisco IOS XE Gibraltar 16.11.1 このコマンドが導入されました。

**使用上のガイドライン** **sdm prefer** グローバル コンフィギュレーション コマンドを入力後にデバイスをリロードしていない場合、**show sdm prefer** 特権 EXEC コマンドでは、新しく設定されたテンプレートではなく現在使用中のテンプレートが表示されます。

各テンプレートで表示される番号は、各機能のリソースにおけるおおよその最大数になります。他に設定された機能の実際の数字にもよるため、実際の数字とは異なる場合があります。たとえば、デバイスに 16 を超えるルーテッドインターフェイス (サブネット VLAN) がある場合、デフォルトのテンプレートでは、可能なユニキャスト MAC アドレスの数は 6000 未満になることがあります。

### 例

次に、**show sdm prefer** コマンドの出力例を示します。

```
Device# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
Number of VLANs:          4094
Unicast MAC addresses:    32768
Overflow Unicast MAC addresses:  512
IGMP and Multicast groups:  8192
Overflow IGMP and Multicast groups:  512
Directly connected routes:  32768
Indirect routes:          7680
Security Access Control Entries:  3072
QoS Access Control Entries:  3072
Policy Based Routing ACEs:  1024
Netflow ACEs:             1024
Input Microflow policer ACEs:  256
```

```
Output Microflow policer ACEs: 256
Flow SPAN ACEs: 256
Tunnels: 256
Control Plane Entries: 512
Input Netflow flows: 8192
Output Netflow flows: 16384
SGT/DGT entries: 4096
SGT/DGT Overflow entries: 512
```

These numbers are typical for L2 and IPv4 features.  
Some features such as IPv6, use up double the entry size;  
so only half as many entries can be created.



# show tech-support confidential

**show tech-support** の機密情報を非表示にするには、特権 EXEC モードで **show tech-support confidential** コマンドを使用します。

**show tech-support confidential output** *file-name*

構文の説明	<b>output</b> <i>file-name</i>	テクニカルサポートデータを保存する出力ファイルを指定します。
コマンドデフォルト	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

**show tech-support confidential** コマンドは、MAC アドレス、IP アドレス、パスワードなどの機密データを非表示にします。出力は、すべての顧客固有のデータがマスクされた **show tech-support** コマンドの出力と同じです。

**show tech-support confidential** コマンドの出力は非常に長くなります。この出力を効率よく処理するには、**show tech-support confidential output location:filename** を使用してローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします。ファイルに出力をリダイレクトすると、出力を Cisco Technical Assistance Center (TAC) の担当者に送信することも容易になります。

```
Device# show tech-support confidential output flash:tech_confidential
Collecting tech-support without confidential info, it will take few min..
```

リダイレクトされたファイルの出力を表示するには、**more location:filename** コマンドを使用します。

# show tech-support monitor

SPAN モニタの情報を表示するには、特権 EXEC モードで **show tech-support monitor** コマンドを使用します。

**show tech-support monitor** [**switch** *switch-number* | **active** | **standby**]

構文の説明	<i>switch-number</i>	スイッチを指定します。
	<b>active</b>	スイッチのアクティブインスタンスを指定します。
	<b>standby</b>	スイッチのスタンバイインスタンスを指定します。
コマンド デフォルト	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

**使用上のガイドライン** **show tech-support monitor** コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします（たとえば、**show tech-support monitor** [**switch** *switch-number* | **active** | **standby**] | **redirect location:filename**）。ファイルに出力をリダイレクトすると、出力を Cisco Technical Assistance Center (TAC) の担当者に送信することも容易になります。

リダイレクトされたファイルの出力を表示するには、**more location:filename** コマンドを使用します。

# show tech-support platform

テクニカルサポートに使用するプラットフォームに関する詳細情報を表示するには、特権EXECモードで **show tech-support platform** コマンドを使用します。

## show tech-support platform

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンドモード

特権 EXEC (#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

### 使用上のガイドライン

このコマンドは、プラットフォーム固有のデバッグに使用されます。出力には、CPU使用率、Ternary Content Addressable Memory (TCAM) の使用率、容量、メモリ使用率など、プラットフォームに関する詳細情報が表示されます。

**show tech-support platform** コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform | redirect flash:filename**）。

**show tech-support platform** コマンドの出力には、一連のコマンドとその出力が表示されます。これらのコマンドは、プラットフォームによって異なる場合があります。

### 例

次に、**show tech-support platform** コマンドの出力例を示します。

```
Device# show tech-support platform
.
.
.
----- show platform hardware capacity -----

Load Average
Slot Status 1-Min 5-Min 15-Min
1-RP0 Healthy 0.25 0.17 0.12

Memory (kB)
Slot Status Total Used (Pct) Free (Pct) Committed (Pct)
1-RP0 Healthy 3964428 2212476 (56%) 1751952 (44%) 3420472 (86%)

CPU Utilization
Slot CPU User System Nice Idle IRQ SIRQ IOwait
1-RP0 0 1.40 0.90 0.00 97.60 0.00 0.10 0.00
1 2.00 0.20 0.00 0.00 97.79 0.00 0.00 0.00
2 0.20 0.00 0.00 0.00 99.80 0.00 0.00 0.00
3 0.79 0.19 0.00 99.00 0.00 0.00 0.00
4 5.61 0.50 0.00 93.88 0.00 0.00 0.00
5 2.90 0.40 0.00 96.70 0.00 0.00 0.00
```

```

*: interface is up
IHQ: pkts in input hold queue      IQD: pkts dropped from input queue
OHQ: pkts in output hold queue     OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)           RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)           TXPS: tx rate (pkts/sec)
TRTL: throttle count

```

Interface	TXBS	TXPS	TRTL	IHQ	IQD	OHQ	OQD	RXBS	RXPS
Vlan1	0	0	0	0	0	0	0	0	0
* GigabitEthernet0/0	0	0	0	0	10179	0	0	2000	4
GigabitEthernet1/0/1	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/2	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/3	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/4	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/5	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/6	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/7	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/8	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/9	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/10	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/11	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/12	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/13	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/14	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/15	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/16	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/17	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/18	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/19	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/20	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/21	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/22	0	0	0	0	0	0	0	0	0
GigabitEthernet1/0/23	0	0	0	0	0	0	0	0	0

```

GigabitEthernet1/0/24      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/25      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/26      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/27      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/28      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/29      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/30      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/31      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/32      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/33      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/34      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/35      0      0      0      0      0      0
  0      0      0
GigabitEthernet1/0/36      0      0      0      0      0      0
  0      0      0
Tel/0/37                    0      0      0      0      0      0
  0      0      0
Tel/0/38                    0      0      0      0      0      0
  0      0      0
Tel/0/39                    0      0      0      0      0      0
  0      0      0
Tel/0/40                    0      0      0      0      0      0
  0      0      0
Tel/0/41                    0      0      0      0      0      0
  0      0      0
Tel/0/42                    0      0      0      0      0      0
  0      0      0
Tel/0/43                    0      0      0      0      0      0
  0      0      0
Tel/0/44                    0      0      0      0      0      0
  0      0      0
Tel/0/45                    0      0      0      0      0      0
  0      0      0
Tel/0/46                    0      0      0      0      0      0
  0      0      0
Tel/0/47                    0      0      0      0      0      0
  0      0      0
Tel/0/48                    0      0      0      0      0      0
  0      0      0
Tel/1/1                    0      0      0      0      0      0
  0      0      0
Tel/1/2                    0      0      0      0      0      0
  0      0      0
Tel/1/3                    0      0      0      0      0      0
  0      0      0
Tel/1/4                    0      0      0      0      0      0
  0      0      0
ASIC 0 Info
-----
ASIC 0 HASH Table 0 Software info: FSE 0
MAB 0: Unicast MAC addresses srip 0 1
MAB 1: Unicast MAC addresses srip 0 1
MAB 2: Unicast MAC addresses srip 0 1

```

## show tech-support platform

```

MAB 3: Unicast MAC addresses srip 0 1
MAB 4: Unicast MAC addresses srip 0 1
MAB 5: Unicast MAC addresses srip 0 1
MAB 6: Unicast MAC addresses srip 0 1
MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 1 Software info: FSE 0
MAB 0: Unicast MAC addresses srip 0 1
MAB 1: Unicast MAC addresses srip 0 1
MAB 2: Unicast MAC addresses srip 0 1
MAB 3: Unicast MAC addresses srip 0 1
MAB 4: Unicast MAC addresses srip 0 1
MAB 5: Unicast MAC addresses srip 0 1
MAB 6: Unicast MAC addresses srip 0 1
MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 2 Software info: FSE 1
MAB 0: L3 Multicast entries srip 2 3
MAB 1: L3 Multicast entries srip 2 3
MAB 2: SGT_DGT          srip 0 1
MAB 3: SGT_DGT          srip 0 1
MAB 4: (null)           srip
MAB 5: (null)           srip
MAB 6: (null)           srip
MAB 7: (null)           srip
.
.
.

```

出力フィールドの意味は自明です。

## 関連コマンド

コマンド	説明
<b>show tech-support platform evpn_vxlan</b>	EVPN-VXLAN 関連のプラットフォーム情報を表示します。
<b>show tech-support platform fabric</b>	スイッチファブリックに関する詳細情報を表示します。
<b>show tech-support platform igmp_snooping</b>	グループに関する IGMP スヌーピング情報を表示します。
<b>show tech-support platform layer3</b>	レイヤ3プラットフォーム転送情報を表示します。
<b>show tech-support platform mld_snooping</b>	グループに関する MLD スヌーピング情報を表示します。

# show tech-support platform evpn\_vxlan

テクニカルサポートに使用するイーサネット VPN (EVPN) Virtual Extensible LAN (VXLAN) 関連のプラットフォーム情報を表示するには、特権 EXEC モードで **show tech-support platform evpn\_vxlan** コマンドを使用します。

**show tech-support platform evpn\_vxlan switch** *switch-number*

構文の説明	<b>switch</b> <i>switch-number</i>	指定されたスイッチに関する情報を表示します。有効な値は 1 ~ 9 です。
コマンドモード	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

**使用上のガイドライン** このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします (たとえば、**show tech-support platform evpn\_vxlan switch 1 | redirect flash:filename**)。

## 例

次に、**show tech-support platform evpn\_vxlan** コマンドの出力例を示します。

```
Device# show tech-support platform evpn_vxlan switch 1
.
.
.
  "show clock"
  "show version"
  "show running-config"switch no: 1

----- sh sdm prefer -----

Showing SDM Template Info

This is the Advanced template.
  Number of VLANs:                               4094
  Unicast MAC addresses:                          32768
  Overflow Unicast MAC addresses:                 512
  L2 Multicast entries:                           4096
  Overflow L2 Multicast entries:                   512
  L3 Multicast entries:                           4096
  Overflow L3 Multicast entries:                   512
  Directly connected routes:                      16384
  Indirect routes:                                7168
  STP Instances:                                  4096
  Security Access Control Entries:                 3072
  QoS Access Control Entries:                      2560
  Policy Based Routing ACEs:                       1024
```

## show tech-support platform evpn\_vxlan

```

Netflow ACEs: 768
Flow SPAN ACEs: 512
Tunnels: 256
LISP Instance Mapping Entries: 256
Control Plane Entries: 512
Input Netflow flows: 8192
Output Netflow flows: 16384
SGT/DGT (or) MPLS VPN entries: 4096
SGT/DGT (or) MPLS VPN Overflow entries: 512
Wired clients: 2048
MACSec SPD Entries: 256
MPLS L3 VPN VRF: 127
MPLS Labels: 2048
MPLS L3 VPN Routes VRF Mode: 7168
MPLS L3 VPN Routes Prefix Mode: 3072
MVPN MDT Tunnels: 256
L2 VPN EOMPLS Attachment Circuit: 256
MAX VPLS Bridge Domains : 64
MAX VPLS Peers Per Bridge Domain: 8
MAX VPLS/VPWS Pseudowires : 256

```

These numbers are typical for L2 and IPv4 features.  
Some features such as IPv6, use up double the entry size;  
so only half as many entries can be created.  
\* values can be modified by sdm cli.

```
----- show platform software fed switch 1 ifm interfaces nve -----
```

```
----- show platform software fed switch 1 ifm interfaces efp -----
```

```
----- show platform software fed switch 1 matm macTable -----
```

```

Total Mac number of addresses:: 0
*a_time=aging_time(secs) *e_time=total_elapsed_time(secs)
Type:
MAT_DYNAMIC_ADDR          0x1  MAT_STATIC_ADDR          0x2  MAT_CPU_ADDR
    0x4  MAT_DISCARD_ADDR          0x8
MAT_ALL_VLANS              0x10 MAT_NO_FORWARD            0x20  MAT_IPMULT_ADDR
    0x40  MAT_RESYNC                0x80
MAT_DO_NOT_AGE             0x100 MAT_SECURE_ADDR          0x200  MAT_NO_PORT
    0x400  MAT_DROP_ADDR                0x800
MAT_DUP_ADDR               0x1000 MAT_NULL_DESTINATION      0x2000  MAT_DOT1X_ADDR
    0x4000  MAT_ROUTER_ADDR                0x8000
MAT_WIRELESS_ADDR          0x10000 MAT_SECURE_CFG_ADDR       0x20000  MAT_OPQ_DATA_PRESENT
0x40000  MAT_WIRED_TUNNEL_ADDR          0x80000
MAT_DLR_ADDR               0x100000 MAT_MRP_ADDR              0x200000  MAT_MSRRP_ADDR
0x400000  MAT_LISP_LOCAL_ADDR            0x800000
MAT_LISP_REMOTE_ADDR      0x1000000 MAT_VPLS_ADDR             0x2000000
Device#

```

出力フィールドの意味は自明です。



## 関連コマンド

コマンド	Description
<b>show tech-support platform</b>	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

# show tech-support platform fabric

スイッチファブリックに関する情報を表示するには、特権 EXEC モードで **show tech-support platform fabric** コマンドを使用します。

```
show tech-support platform fabric [display-cli | vrf vrf-name ipv4 display-cli | ipv6 display-cli |
source instance-id instance-id ipv4 ip-address/ip-prefix | ipv6 ipv6-address/ipv6-prefix | mac
mac-address dest instance-id instance-id ipv4 ip-address/ip-prefix | ipv6 ipv6-address/ipv6-prefix |
mac mac-address [display-cli]]
```

構文の説明	<b>display-cli</b>	(任意) このコマンドの出力で使用可能な show コマンドのリストを表示します。
	<b>vrf vrf-name</b>	(任意) 指定した Virtual Routing and Forwarding (VRF) インスタンスのファブリック関連情報を表示します。
	<b>ipv4 ip-address/ip-prefix</b>	(任意) 送信元または宛先 IP VRF のファブリック関連情報を表示します。
	<b>ipv6 ipv6-address/ipv6-prefix</b>	(任意) 送信元または宛先 IPv6 VRF のファブリック関連情報を表示します。
	<b>source</b>	(任意) 送信元 VRF のファブリック関連情報を表示します。
	<b>instance-id instance-id</b>	(任意) 送信元のエンドポイント識別子 (EID) に関する情報を表示します。
	<b>mac mac-address</b>	(任意) レイヤ2拡張展開の送信元および宛先 MAC VRF のファブリック関連情報を表示します。
コマンドモード	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

## 使用上のガイドライン

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support platform fabric | redirect flash:filename**）。

このコマンドの出力には、一連のコマンドとその出力が表示されます。これらのコマンドは、プラットフォームによって異なる場合があります。

## 例

次に、**show tech-support platform fabric vrf source instance-id ipv4 dest instance-id ipv4** コマンドの出力例を示します。

```
Device# show tech-support platform fabric vrf DEFAULT_VN source instance-id
4098 ipv4 10.1.1.1/32 dest instance-id 4098 ipv4 10.12.12.12/32

.
.
.
-----show ip lisp eid-table vrf DEFAULT_VN forwarding eid remote 10.12.12.12-----

Prefix          Fwd action  Locator status bits  encap_iid
10.12.12.12/32  encap      0x00000001             N/A
  packets/bytes  1/576
  path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwcn]
  ifnums:
    LISP0.4098(78): 192.0.2.2
  1 path
    path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
      nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
  1 output chain
    chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
      IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378

-----show lisp instance-id 4098 ipv4 map-cache-----

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Encapsulating to proxy ETR
10.1.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
  Locator  Uptime   State    Pri/Wgt   Encap-IID
  192.0.2.2 02:45:54  up      10/10    -

-----show lisp instance-id 4098 ipv4 map-cache detail-----

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Sources: static-send-map-request
  State: send-map-request, last modified: 02:46:01, map-source: local
  Exempt, Packets out: 2(676 bytes) (~ 02:45:38 ago)
  Configured as EID address space
  Encapsulating to proxy ETR
101.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Sources: NONE
```

```

State: send-map-request, last modified: 02:46:01, map-source: local
Exempt, Packets out: 0(0 bytes)
Configured as EID address space
Configured as dynamic-EID address space
Encapsulating dynamic-EID traffic
Encapsulating to proxy ETR
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
Sources: map-reply
State: complete, last modified: 02:45:54, map-source: 10.0.1.2
Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
Locator Uptime State Pri/Wgt Encap-IID
192.0.2.2 02:45:54 up 10/10 -
Last up-down state change: 02:45:54, state change count: 1
Last route reachability change: 02:45:54, state change count: 1
Last priority / weight change: never/never
RLOC-probing loc-status algorithm:
Last RLOC-probe sent: 02:45:54 (rtt 1ms)

```

```
-----show lisp instance-id 4098 ipv4 map-cache 10.12.12.12/32-----
```

```

LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
Sources: map-reply
State: complete, last modified: 02:45:54, map-source: 10.0.1.2
Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
Locator Uptime State Pri/Wgt Encap-IID
192.0.2.2 02:45:54 up 10/10 -
Last up-down state change: 02:45:54, state change count: 1
Last route reachability change: 02:45:54, state change count: 1
Last priority / weight change: never/never
RLOC-probing loc-status algorithm:
Last RLOC-probe sent: 02:45:54 (rtt 1ms)

```

```
-----show ip cef vrf DEFAULT_VN 10.12.12.12/32 internal-----
```

```

10.12.12.12/32, epoch 1, flags [sc, lisp elig], refcnt 6, per-destination sharing
sources: LISP, IPL
feature space:
Broker: linked, distributed at 1st priority
subblocks:
SC owned,sourced: LISP remote EID - locator status bits 0x00000001
LISP remote EID: 1 packets 576 bytes fwd action encap, cfg as EID space
LISP source path list
path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwn]
ifnums:
LISP0.4098(78): 192.0.2.2
1 path
path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
1 output chain
chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
Dependent covered prefix type LISP, cover 0.0.0.0/0
2 IPL sources [no flags]
ifnums:
LISP0.4098(78): 192.0.2.2
path list 7F44EEC2C188, 3 locks, per-destination, flags 0x49 [shble, rif, hwn]
path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4

```

```

        nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
    output chain:
        PushCounter(LISP:10.12.12.12/32) 7F44F3C8B8D8
        IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
        IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
switch no: 1
.
.
.

```

```

Device# show tech-support platform fabric vrf Campus_VN source instance-id 8189
mac 00b7.7128.00a1 dest instance-id 8189 mac 00b7.7128.00a0 | i show

```

```

----- show clock -----
----- show version -----
----- show running-config -----
----- show device-tracking database -----
----- show lisp site -----
----- show mac address-table address 00B7.7128.00A0-----
----- show ip arp vrf Campus_VN-----
Device#

```

出力フィールドの意味は自明です。

#### 関連コマンド

コマンド	説明
<b>show tech-support platform</b>	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

# show tech-support platform igmp\_snooping

グループに関する Internet Group Management Protocol (IGMP) スヌーピング情報を表示するには、特権 EXEC モードで **show tech-support platform igmp\_snooping** コマンドを使用します。

**show tech-support platform igmp\_snooping** [**Group\_ipAddr** *ipv4-address* | [**vlan** *vlan-ID*]]

構文の説明	Group_ipAddr	(任意) 指定したグループアドレスに関するスヌーピング情報を表示します。
	<i>ipv4-address</i>	(任意) グループの IPv4 アドレス。
	<b>vlan</b> <i>vlan-ID</i>	(任意) IGMP スヌーピング VLAN 情報を表示します。有効な値は 1 ~ 4094 です。

コマンドモード 特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします (たとえば、**show tech-support platform igmp\_snooping | redirect flash:filename**)。

例

次に、**show tech-support platform igmp\_snooping** コマンドの出力例を示します。

```
Device# show tech-support platform igmp_snooping GroupIPAddr 226.6.6.6 vlan
.
.
.
----- show ip igmp snooping groups | i 226.6.6.6 -----
5          226.6.6.6          user          Gi1/0/8, Gi1/0/27, Gi1/0/28,

----- show ip igmp snooping groups count -----
Total number of groups:  2

----- show ip igmp snooping mrouter -----
```

```
Vlan    ports
-----
    23    Router
    24    Router
    25    Router
```

```
----- show ip igmp snooping querier -----
```

Vlan	IP Address	IGMP Version	Port
23	10.1.1.1	v2	Router
24	10.1.2.1	v2	Router
25	10.1.3.1	v2	Router

```
----- show ip igmp snooping vlan 5 -----
```

```
Global IGMP Snooping configuration:
```

```
-----
IGMP snooping           : Enabled
Global PIM Snooping    : Disabled
IGMPv3 snooping        : Enabled
Report suppression     : Enabled
TCN solicit query     : Disabled
TCN flood query count  : 2
Robustness variable    : 2
Last member query count : 2
Last member query interval : 1000
```

```
Vlan 5:
```

```
-----
IGMP snooping           : Enabled
Pim Snooping           : Disabled
IGMPv2 immediate leave : Disabled
Explicit host tracking  : Enabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode : IGMP_ONLY
Robustness variable    : 2
Last member query count : 2
Last member query interval : 1000
```

```
----- show ip igmp snooping groups vlan 5 -----
```

Vlan	Group	Type	Version	Port List
5	226.6.6.6	user		Gi1/0/8, Gi1/0/27, Gi1/0/28, Gi2/0/7, Gi2/0/8, Gi2/0/27, Gi2/0/28
5	238.192.0.1	user		Gi2/0/28

```
----- show platform software fed active ip igmp snooping vlan 5 -----
```

## show tech-support platform igmp\_snooping

```

Vlan 5
-----
IGMPSN Enabled   : On
PIMSN Enabled    : Off
Flood Mode       : On
I-Mrouter        : Off
Oper State       : Up
STP TCN Flood    : Off
Routing Enabled  : Off
PIM Enabled      : Off
PVLAN            : No
In Retry         : 0x0
L3mcast Adj      :
Mrouter PortQ    :
Flood PortQ     :

----- show platform software fed active ip igmp snooping groups | begin 226.6.6.6 -----

Vlan:5 Group:226.6.6.6
-----
Member ports      :
CAPWAP ports     :
Host Type Flags  : 0
Failure Flags    : 0
DI handle        : 0x7f11151cbad8
REP RI handle    : 0x7f11151cc018
SI handle        : 0x7f11151cd198
HTM handle       : 0x7f11151cd518

si hdl : 0x7f11151cd198 rep ri hdl : 0x7f11151cc018 di hdl : 0x7f11151cbad8 htm hdl :
0x7f11151cd518
.
.
.
Device#

```

出力フィールドの意味は自明です。

## 関連コマンド

コマンド	説明
<b>ip igmp snooping</b>	IGMP スヌーピングをグローバルまたはインターフェイスで有効にします。
<b>show ip igmp snooping</b>	デバイスの IGMP スヌーピング設定を表示します。
<b>show tech-support platform</b>	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。



## show tech-support platform layer3

レイヤ 3 プラットフォーム転送情報を表示するには、特権 EXEC モードで **show tech-support platform layer3** コマンドを使用します。

```
show tech-support platform layer3 multicast Group_ipAddr ipv4-address switch switch-number srcIP
ipv4-address | unicast dstIP ipv4-address srcIP ipv4-address | vrf vrf-name destIP ipv4-address srcIP
ipv4-address
```

構文の説明	<b>multicast</b>	マルチキャスト情報を表示します。
	<b>Group_ipv6Addr</b> <i>ipv4-address</i>	指定したマルチキャストグループアドレスに関する情報を表示します。
	<b>switch</b> <i>switch-number</i>	指定したスイッチに関する情報を表示します。有効な値は 1 ～ 9 です。
	<b>srcIP</b> <i>ipv4-address</i>	指定した送信元アドレスに関する情報を表示します。
	<b>unicast</b>	ユニキャスト関連の情報を表示します。
	<b>dstIP</b> <i>ipv4-address</i>	指定した宛先アドレスに関する情報を表示します。
	<b>vrf</b> <i>vrf-name</i>	ユニキャスト関連の Virtual Routing and Forwarding (VRF) 情報を表示します。
コマンドモード	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。
使用上のガイドライン	このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、 <b>show tech-support platform layer3 multicast group 224.1.1.1 switch 1 srcIP 10.10.0.2   redirect flash:filename</b> ）。	

## 例

次に、**show tech-support platform layer3 multicast group** コマンドの出力例を示します。

```
Device# show tech-support platform layer3 multicast group_ipAddr 224.1.1.1
switch 1 srcIp 10.10.0.2

.
.
.
destination IP: 224.1.1.1
source IP: 10.10.0.2
switch no: 1

----- show ip mroute 224.1.1.1 10.10.0.2 -----

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(10.10.0.2, 224.1.1.1), 00:00:22/00:02:37, flags: LFT
  Incoming interface: GigabitEthernet1/0/10, RPF nbr 0.0.0.0, Registering
  Outgoing interface list:
    Vlan20, Forward/Sparse, 00:00:22/00:02:37, A

----- show ip mfib 224.1.1.1 10.10.0.2 -----

Entry Flags:   C - Directly Connected, S - Signal, IA - Inherit A flag,
               ET - Data Rate Exceeds Threshold, K - Keepalive
               DDE - Data Driven Event, HW - Hardware Installed
               ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
               MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
               MS - MoFRR Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:  FS Pkt Count/PS Pkt Count
Default
(10.10.0.2,224.1.1.1) Flags: HW
  SW Forwarding: 0/0/0/0, Other: 1/1/0
  HW Forwarding:  NA/NA/NA/NA, Other: NA/NA/NA
```

```

GigabitEthernet1/0/10 Flags: A
Vlan20 Flags: F IC
Pkts: 0/0
Tunnel0 Flags: F
Pkts: 0/0

----- show platform software fed switch 1 ip multicast interface summary -----
Multicast Interface database

VRF Interface          IF ID          PIM Status  State          RI
Handle          SVI
-----
0    GigabitEthernet1/0/10    0x000000000000005f    enabled    0x0000000000000010
0x000007fb414b1f108    false
0    Vlan20                    0x0000000000000060    enabled    0x0000000000000010
0x000007fb414b31a98    true

----- show platform software fed switch 1 ip multicast groups summary -----
Multicast Groups database

Mvrf_id: 0 Mroute: (*, 224.0.1.40/32) Flags: C IC
Htm: 0x00007fb414b23ce8 Si: 0x00007fb414b23a08 Di: 0x00007fb414b240e8 Rep_ri:
0x00007fb414b245f8

Mvrf_id: 0 Mroute: (*, 224.0.0.0/4) Flags: C
Htm: 0x00007fb4143549e8 Si: 0x00007fb414b20a48 Di: 0x00007fb414b1fe78 Rep_ri:
0x00007fb414b20428

Mvrf_id: 0 Mroute: (*, 224.1.1.1/32) Flags: C IC
Htm: 0x00007fb414b2cc98 Si: 0x00007fb414b2b678 Di: 0x00007fb414b2ab98 Rep_ri:
0x00007fb414b2b0c8

Mvrf_id: 0 Mroute: (10.10.0.2, 224.1.1.1/32) Flags: IC
Htm: 0x00007fb414b2f348 Si: 0x00007fb414b321d8 Di: 0x00007fb414b2dba8 Rep_ri:
0x00007fb414b30ed8

----- show platform software fed switch 1 ip multicast groups count -----

Total Number of entries:4

----- show platform software fed switch 1 ip multicast groups 224.1.1.1/32
source 10.10.0.2 detail -----

MROUTE ENTRY vrf 0 (10.10.0.2, 224.1.1.1/32)
HW Handle: 140411418055080 Flags: IC
RPF interface: GigabitEthernet1/0/10(95)):
HW Handle:140411418055080 Flags:A
Number of OIF: 3
Flags: 0x4 Pkts : 0
OIF Details:
Tunnel0 Adj: 0xf8000636 F

```

## show tech-support platform layer3

```

Vlan20      Adj: 0xf8000601  F IC
GigabitEthernet1/0/10      A
Htm: 0x7fb414b2f348  Si: 0x7fb414b321d8  Di: 0x7fb414b2dba8  Rep_ri: 0x7fb414b30ed8

```

## DI details

```

-----
Handle:0x7fb414b2dba8 Res-Type:ASIC_RSC_DI Res-Switch-Num:255 Asic-Num:255
Feature-ID:AL_FID_L3_
MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x538e
mtu_index/l3u_ri_index0:0x0 index1:0x538e mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00
00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
-----

```

```

Destination Index (DI) [0x538e]
portMap = 0x00000000          0
cmil = 0x385
rcpPortMap = 0

```

```

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
-----

```

```

Destination Index (DI) [0x538e]
portMap = 0x00000000          0
cmil = 0x385
rcpPortMap = 0

```

```

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0

```

## RI details

```

-----
Handle:0x7fb414b30ed8 Res-Type:ASIC_RSC_RI_REP Res-Switch-Num:255 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x5
mtu_index/l3u_ri_index0:0x0
index1:0x5 mtu_index/l3u_ri_index1:0x0

```

```

Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00
00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
-----

Detailed Resource Information (ASIC# 1)
-----

=====

SI details
-----
Handle:0x7fb414b321d8 Res-Type:ASIC_RSC_SI_STATS Res-Switch-Num:255 Asic-Num:255
Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x4004
mtu_index/l3u_ri_index0:
0x0 sm handle 0:0x7fb414b2df98 index1:0x4004 mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00 00
00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
-----

Detailed Resource Information (ASIC# 1)
-----

=====

HTM details
-----
Handle:0x7fb414b2f348 Res-Type:ASIC_RSC_HASH_TCAM Res-Switch-Num:0 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_SG ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: handle0:0x7fb414b2f558
Detailed Resource Information (ASIC# 0)
-----

Number of HTM Entries: 1

Entry #0: (handle 0x7fb414b2f558)

KEY - src_addr:10.10.0.2 starg_station_index: 16387
MASK - src_addr:0.0.0.0 starg_station_index: 0
AD: use_starg_match: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0 rpf_valid: 1 rpf_le_ptr:
0
afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1 cpp_type: 0 dest_mod_index: 0
rp_index:
0 priority: 5 rpf_le: 36 station_index: 16388 capwap_mgid_present: 0 mgid 0

```

次に、**show tech-support platform layer3 unicast vrf** コマンドの出力例を示します。

```

Device# show tech-support platform layer3 unicast vrf vr1 dstIP 10.0.0.20
srcIP 10.0.0.10

.
.
.
destination IP: 10.0.0.20
source IP: 10.0.0.10
vrf name :

```

## show tech-support platform layer3

```
Switch/Stack Mac Address : 5006.ab89.0280 - Local Mac Address
Mac persistency wait time: Indefinite
```

Switch#	Role	Mac Address	Priority	H/W Version	Current State
*1	Active	5006.ab89.0280	1	V02	Ready

```
----- show switch -----
```

```
10.0.0.10 -> 10.0.0.20 =>IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20
```

```
----- show ip cef exact-route platform 10.0.0.10 10.0.0.20 -----
```

```
nexthop is 10.0.0.20
```

```
Protocol Interface Address
IP GigabitEthernet1/0/7 10.0.0.20(8)
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 0
Encap length 14
00211BFDE6495006AB8902C00800
L2 destination address byte offset 0
L2 destination address byte length 6
Link-type after encap: ip
ARP
```

```
----- show adjacency 10.0.0.20 detail -----
```

```
Routing entry for 10.0.0.0/24
```

```
Known via "connected", distance 0, metric 0 (connected, via interface)
```

```
Routing Descriptor Blocks:
```

```
* directly connected, via GigabitEthernet1/0/7
```

```
Route metric is 0, traffic share count is 1
```

```
----- show ip route 10.0.0.20 -----
```

```
10.0.0.20/32, epoch 3, flags [attached]
```

```
Adj source: IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20 FF90E67820
```

```
Dependent covered prefix type adjfib, cover 10.0.0.0/24
```

```
attached to GigabitEthernet1/0/7
```

```
----- show ip cef 10.0.0.20 detail -----
```

```
ip prefix: 10.0.0.20/32
```

```
Forwarding Table
```

```
10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30  
Connected Interface: 31  
Prefix Flags: Directly L2 attached  
OM handle: 0x10205416d8
```

```
----- show platform software ip switch 1 R0 cef prefix 10.0.0.20/32 detail -----
```

```
OBJ_ADJACENCY found: 29
```

```
Number of adjacency objects: 5
```

```
Adjacency id: 0x1d (29)  
Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP  
Encap: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0  
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500  
Flags: no-l3-inject  
Incomplete behavior type: None  
Fixup: unknown  
Fixup_Flags_2: unknown  
Nexthop addr: 10.0.0.20  
IP FRR MCP_ADJ_IPFRR_NONE 0  
OM handle: 0x1020541348
```

```
----- show platform software adjacency switch 1 R0 index 29 -----
```

```
Forwarding Table
```

```
10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30  
Connected Interface: 31  
Prefix Flags: Directly L2 attached  
aom id: 393, HW handle: (nil) (created)
```

```
----- show platform software ip switch 1 F0 cef prefix 10.0.0.20/32 detail -----
```

```
OBJ_ADJACENCY found: 29
```

```
Number of adjacency objects: 5
```

```
Adjacency id: 0x1d (29)  
Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP  
Encap: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0  
Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500  
Flags: no-l3-inject  
Incomplete behavior type: None
```

## show tech-support platform layer3

```

Fixup: unknown
Fixup_Flags_2: unknown
Nexthop addr: 10.0.0.20
IP FRR MCP_ADJ_IPFRR_NONE 0
aom id: 391, HW handle: (nil) (created)

```

```
----- show platform software adjacency switch 1 F0 index 29 -----
```

```
found aom id: 391
```

```

Object identifier: 391
  Description: adj 0x1d, Flags None
  Status: Done, Epoch: 0, Client data: 0xc6a747a8

```

```
----- show platform software object-manager switch 1 F0 object 391 -----
```

```

Object identifier: 66
  Description: intf GigabitEthernet1/0/7, handle 31, hw handle 31, HW dirty: NONE AOM
  dirty NONE
  Status: Done

```

```
----- show platform software object-manager switch 1 F0 object 391 parents -----
```

```

Object identifier: 393
  Description: PREFIX 10.0.0.20/32 (Table id 0)
  Status: Done

```

```

.
.
.

```

出力フィールドの意味は自明です。

## 関連コマンド

コマンド	説明
<b>show tech-support platform</b>	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。



## show tech-support platform mld\_snooping

グループに関するマルチキャストリスナー検出 (MLD) スヌーピング情報を表示するには、特権 EXEC モードで **show tech-support platform mld\_snooping** コマンドを使用します。

**show tech-support platform mld\_snooping** [**Group\_ipv6Addr** *ipv6-address*][**vlan** *vlan-ID*]

構文の説明	Group_ipv6Addr	(任意) 指定したグループアドレスに関するスヌーピング情報を表示します。
	<i>ipv6-address</i>	(任意) グループの IPv6 アドレス。
	<b>vlan</b> <i>vlan-ID</i>	(任意) MLD スヌーピング VLAN 情報を表示します。有効な値は 1 ~ 4094 です。

コマンドモード 特権 EXEC (#)

コマンド履歴

リリース	変更内容
Cisco IOS XE ジブラルタル 16.10.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします (たとえば、**show tech-support platform mld\_snooping | redirect flash:filename**)。

例

次に、**show tech-support platform mld\_snooping** コマンドの出力例を示します。

```
Device# show tech-support platform mld_snooping GroupIPv6Addr FF02::5:1
```

```
.
.
.
```

```
----- show running-config -----
```

```
Building configuration...
```

```
Current configuration : 11419 bytes
```

```
!
```

```
! Last configuration change at 09:17:04 UTC Thu Sep 6 2018
```

```
!
```

```
version 16.10
```

```
no service pad
```

```
service timestamps debug datetime msec
```

```
service timestamps log datetime msec
```

```
service call-home
```

## show tech-support platform mld\_snooping

```

no platform punt-keepalive disable-kernel-core
!
hostname Switch
!
!
vrf definition Mgmt-vrf
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
!
no aaa new-model
switch 1 provision ws-c3650-12x48uq
!
!
!
!
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact
email address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "profile-1"
active
destination transport-method http
no destination transport-method email
!
!
!
!
!
ip admission watch-list expiry-time 0
!
!
!
login on-success log
!
!
!
!
!
no device-tracking logging theft
!
crypto pki trustpoint TP-self-signed-559433368
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-559433368
revocation-check none
rsa-keypair TP-self-signed-559433368
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-559433368
certificate self-signed 01
30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 35353934 33333336 38301E17 0D313531 32303331 32353432
325A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3535 39343333

```

```

33363830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
AD8C9C3B FEE7FFC8 986837D2 4C126172 446C3C53 E040F798 4BA61C97 7506FDCE
46365D0A E47E3F4F C774CA5B 73E2A8DD B72A2E98 C66DB196 94E8150F 0B669CF6
AA5BC4CD FC2E02F6 FE08B17F 0164FC19 7DC84ABB C99D91D6 398233FF 814EF6DA
6DC8FC20 CA12C0D6 1CB28EDA 6ADD6DFA 7E3E8281 4A189A9A AA44FCC0 BA9BD8A5
02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
23041830 16801448 668D668E C92914BB 69E9BA64 F61228DE 132E2030 1D060355
1D0E0416 04144866 8D668EC9 2914BB69 E9BA64F6 1228DE13 2E20300D 06092A86
4886F70D 01010505 00038181 0000F1D3 3DD1E5F1 EB714A95 D5819933 CAD0C943
59927D55 9D70CAD0 D64830EB D54380AD D2B5B613 F8AF7A5B 1F801134 246F760D
5E5515DB D098304F 5086F6CE 88E8B576 F6B93A88 F458FDCF 91A42D7E FA741908
5C892D78 600FB655 E6C5A4D0 6C1F1B9A 3AECA550 E3DC0881 01C4D004 7AB65BC3
88CF24DE DAA19474 51B535A5 0C
quit
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
!
!
!
diagnostic bootup level minimal
diagnostic monitor syslog
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
redundancy
mode sso
!
!
!
!
!
class-map match-any system-cpp-police-topology-control
description Topology control

```

```

class-map match-any system-cpp-police-sw-forward
  description Sw forwarding, L2 LVX data, LOGGING
class-map match-any system-cpp-default
  description EWLC control, EWLC data, Inter FED
class-map match-any system-cpp-police-sys-data
  description Learning cache ovfl, High Rate App, Exception, EGR Exception, NFL SAMPLED
  DATA, RPF Failed
class-map match-any AutoQos-4.0-RT1-Class
  match dscp ef
  match dscp cs6
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
class-map match-any AutoQos-4.0-RT2-Class
  match dscp cs4
  match dscp cs3
  match dscp af41
class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any system-cpp-police-multicast
  description Transit Traffic and MCAST Data
class-map match-any system-cpp-police-l2-control
  description L2 control
class-map match-any system-cpp-police-dot1x-auth
  description DOT1X Auth
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
  description Stackwise Virtual
class-map match-any system-cpp-police-control-low-priority
  description ICMP redirect and general punt
class-map match-any system-cpp-police-wireless-priority1
  description Wireless priority 1
class-map match-any system-cpp-police-wireless-priority2
  description Wireless priority 2
class-map match-any system-cpp-police-wireless-priority3-4-5
  description Wireless priority 3,4 and 5
class-map match-any non-client-nrt-class
class-map match-any system-cpp-police-routing-control
  description Routing control and Low Latency
class-map match-any system-cpp-police-protocol-snooping
  description Protocol snooping
class-map match-any system-cpp-police-dhcp-snooping
  description DHCP snooping
class-map match-any system-cpp-police-system-critical
  description System Critical and Gold Pkt
!
policy-map system-cpp-policy
  class system-cpp-police-data
    police rate 200 pps
  class system-cpp-police-routing-control
    police rate 500 pps
  class system-cpp-police-control-low-priority
  class system-cpp-police-wireless-priority1
  class system-cpp-police-wireless-priority2
  class system-cpp-police-wireless-priority3-4-5
policy-map port_child_policy
  class non-client-nrt-class
    bandwidth remaining ratio 10
  !
  !

```

```
!  
!  
!  
!  
!  
!  
!  
!  
interface GigabitEthernet0/0  
  vrf forwarding Mgmt-vrf  
  no ip address  
  speed 1000  
  negotiation auto  
!  
interface GigabitEthernet1/0/1  
  switchport mode access  
  macsec network-link  
!  
interface GigabitEthernet1/0/2  
!  
interface GigabitEthernet1/0/3  
!  
interface TenGigabitEthernet1/1/1  
!  
interface TenGigabitEthernet1/1/2  
!  
interface TenGigabitEthernet1/1/3  
!  
interface TenGigabitEthernet1/1/4  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
ip forward-protocol nd  
ip http server  
ip http authentication local  
ip http secure-server  
!  
ip access-list extended AutoQos-4.0-wlan-Acl-Bulk-Data  
  permit tcp any any eq 22  
  permit tcp any any eq 465  
  permit tcp any any eq 143  
  permit tcp any any eq 993  
  permit tcp any any eq 995  
  permit tcp any any eq 1914  
  permit tcp any any eq ftp  
  permit tcp any any eq ftp-data  
  permit tcp any any eq smtp  
  permit tcp any any eq pop3  
ip access-list extended AutoQos-4.0-wlan-Acl-MultiEnhanced-Conf  
  permit udp any any range 16384 32767  
  permit tcp any any range 50000 59999  
ip access-list extended AutoQos-4.0-wlan-Acl-Scavenger  
  permit tcp any any range 2300 2400  
  permit udp any any range 2300 2400  
  permit tcp any any range 6881 6999  
  permit tcp any any range 28800 29100  
  permit tcp any any eq 1214  
  permit udp any any eq 1214  
  permit tcp any any eq 3689  
  permit udp any any eq 3689  
  permit tcp any any eq 11999  
ip access-list extended AutoQos-4.0-wlan-Acl-Signaling
```

```

permit tcp any any range 2000 2002
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-wlan-Acl-Transactional-Data
permit tcp any any eq 443
permit tcp any any eq 1521
permit udp any any eq 1521
permit tcp any any eq 1526
permit udp any any eq 1526
permit tcp any any eq 1575
permit udp any any eq 1575
permit tcp any any eq 1630
permit udp any any eq 1630
permit tcp any any eq 1527
permit tcp any any eq 6200
permit tcp any any eq 3389
permit tcp any any eq 5985
permit tcp any any eq 8080
!
!
!
ipv6 access-list preauth_ipv6_acl
permit udp any any eq domain
permit tcp any any eq domain
permit icmp any any nd-ns
permit icmp any any nd-na
permit icmp any any router-solicitation
permit icmp any any router-advertisement
permit icmp any any redirect
permit udp any eq 547 any eq 546
permit udp any eq 546 any eq 547
deny ipv6 any any
!
control-plane
service-policy input system-cpp-policy
!
!
line con 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
login
line vty 5 15
login
!
!
mac address-table notification mac-move
!
!
!
!
end

```

```
-----show switch | Include Ready-----
```

```
*1      Active   188b.9dfc.eb00    1      V00     Ready
```

```
----- show ipv6 mld snooping address | i FF02::5:1 -----
```

Vlan	Group	Type	Version	Port List
------	-------	------	---------	-----------

```
-----  
123          FF02::5:1          mld          v2          Gi2/0/1
```

Device#

出力フィールドの意味は自明です。

#### 関連コマンド

コマンド	Description
<b>ipv6 mld snooping</b>	MLDv2 プロトコルスヌーピングをグローバルに有効にします。
<b>show ipv6 mld snooping</b>	MLDv2 スヌーピング情報を表示します。
<b>show tech-support platform</b>	テクニカルサポートに使用するプラットフォームに関する詳細情報を表示します。

# show tech-support port

テクニカルサポートに使用するポート関連の情報を表示するには、特権 EXEC モードで **show tech-support port** コマンドを使用します。

## show tech-support port

### 構文の説明

このコマンドには引数またはキーワードはありません。

### コマンドモード

特権 EXEC (#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.10.1	このコマンドが導入されました。

### 使用上のガイドライン

**show tech-support port** コマンドの出力は非常に長くなります。この出力を効率よく処理するには、ローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力を外部ファイルにリダイレクトします（たとえば、**show tech-support port | redirect flash:filename**）。

このコマンドの出力には次のコマンドが表示されます。

- **show clock**
- **show version**
- **show module**
- **show inventory**
- **show interface status**
- **show interface counters**
- **show interface counters errors**
- **show interfaces**
- **show interfaces capabilities**
- **show controllers**
- **show controllers utilization**
- **show idprom interface**
- **show controller ethernet-controller phy detail**
- **show switch**
- **show platform software fed switch active port summary**
- **show platform software fed switch ifm interfaces ethernet**
- **show platform software fed switch ifm mappings**



- **show platform software fed switch ifm mappings lpn**
- **show platform software fed switch ifm mappings gpn**
- **show platform software fed switch ifm mappings port-le**
- **show platform software fed switch ifm if-id**
- **show platform software fed switch active port if\_id**

## 例

次に、**show tech-support port** コマンドの出力例を示します。

```
Device# show tech-support port
.
.
.
----- show controllers utilization -----

Port          Receive Utilization  Transmit Utilization
Gi1/0/1        0 0
Gi1/0/2        0 0
Gi1/0/3        0 0
Gi1/0/4        0 0
Gi1/0/5        0 0
Gi1/0/6        0 0
Gi1/0/7        0 0
Gi1/0/8        0 0
Gi1/0/9        0 0
Gi1/0/10       0 0
Gi1/0/11       0 0
Gi1/0/12       0 0
Gi1/0/13       0 0
Gi1/0/14       0 0
Gi1/0/15       0 0
Gi1/0/16       0 0
Gi1/0/17       0 0
Gi1/0/18       0 0
Gi1/0/19       0 0
Gi1/0/20       0 0
Gi1/0/21       0 0
Gi1/0/22       0 0
Gi1/0/23       0 0
Gi1/0/24       0 0
Gi1/0/25       0 0
Gi1/0/26       0 0
Gi1/0/27       0 0
Gi1/0/28       0 0
Gi1/0/29       0 0
Gi1/0/30       0 0
Gi1/0/31       0 0
Gi1/0/32       0 0
Gi1/0/33       0 0
Gi1/0/34       0 0
Gi1/0/35       0 0
Gi1/0/36       0 0
Te1/0/37       0 0
Te1/0/38       0 0
Te1/0/39       0 0
Te1/0/40       0 0
Te1/0/41       0 0
Te1/0/42       0 0
```

```
Tel/0/43      0  0
Tel/0/44      0  0
Tel/0/45      0  0
Tel/0/46      0  0
Tel/0/47      0  0
Tel/0/48      0  0
Tel/1/1       0  0
Tel/1/2       0  0
Tel/1/3       0  0
Tel/1/4       0  0
```

```
Total Ports : 52
Total Ports Receive Bandwidth Percentage Utilization : 0
Total Ports Transmit Bandwidth Percentage Utilization : 0
```

```
Average Switch Percentage Utilization : 0
```

```
----- show idprom interface Gi1/0/1 -----
```

```
*Sep  7 08:57:24.249: No module is present
```

```
.
.
.
```

出力フィールドの意味は自明です。

## show tech-support pvlan

プライベート VLAN に関する情報を表示するには、特権 EXEC モードで **show tech-support pvlan** コマンドを使用します。

**show tech-support pvlan [pvlan\_id pvlan-id]**

構文の説明	<b>pvlan_id pvlan-id</b>	プライベート VLAN ID を指定します。
コマンド デフォルト	特権 EXEC (#)	
コマンド履歴	リリース	変更内容
	Cisco IOS XE Amsterdam 17.3.1	このコマンドが導入されました。

**使用上のガイドライン** **show tech-support pvlan** コマンドの出力は非常に長くなります。この出力を効率よく処理するには、**show tech-support pvlan [ pvlan\_id vlan-id ] | redirect location:filename** を使用してローカルの書き込み可能なストレージ、またはリモートファイルシステムで、この出力をファイルにリダイレクトします。ファイルに出力をリダイレクトすると、出力を Cisco Technical Assistance Center (TAC) の担当者に送信することも容易になります。

リダイレクトされたファイルの出力を表示するには、**more location:filename** コマンドを使用します。

# show version

現在ロードされているソフトウェアの情報とハードウェアおよびデバイス情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show version** コマンドを使用します。

**show version** [**switch** ノード][**installed** | **provisioned** | **running**]

構文の説明	switch ノード	(任意) 1つのスイッチのみを指定できます。デフォルトは、スタック構成のシステム内のすべてのスイッチです。
	<b>running</b>	(任意) 現在実行されているファイルに関する情報を指定します。
	<b>provisioned</b>	(任意) プロビジョニングされているソフトウェアファイルに関する情報を指定します。
	<b>installed</b>	RP にインストールされているソフトウェアに関する情報を指定します。
	<b>user-interface</b>	ユーザインターフェイスに関連するファイルに関する情報を指定します。

コマンド デフォルト      デフォルトの動作や値はありません。

コマンド モード      ユーザ EXEC (>)  
 特権 EXEC (#)

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

**使用上のガイドライン**      このコマンドでは、デバイスで現在実行中の Cisco IOS ソフトウェアのバージョン、ROM モニタとブートフラッシュ ソフトウェアのバージョン、およびシステムメモリの量を含むハードウェア構成についての情報が表示されます。このコマンドではソフトウェアとハードウェアの両方の情報が表示されるため、このコマンドの出力は **show hardware** コマンドの出力と同じです (**show hardware** コマンドは **show version** コマンドのコマンドエイリアスです)。

**show version** コマンドは、具体的には次の情報を提供します。

- ソフトウェア情報
  - メインの Cisco IOS イメージのバージョン
  - メインの Cisco IOS イメージの機能 (フィーチャセット)
  - ROM 内のブートファイルの場所と名前
  - ブートフラッシュイメージのバージョン (プラットフォームによって異なる)
- デバイス固有の情報
  - デバイス名

- システムの動作期間
  - システムのリロードの理由
  - config-register 設定
  - 次回のリロード後の config-register 設定（プラットフォームによって異なる）
- ハードウェア情報
    - プラットフォームタイプ
    - プロセッサ タイプ
    - プロセッサ ハードウェア リビジョン
    - 搭載されているメイン（プロセッサ）メモリの容量
    - 搭載されている I/O メモリの容量
    - 搭載されている各タイプのフラッシュメモリの容量（プラットフォームによって異なる）
    - プロセッサボード ID

このコマンドの出力の形式は次のとおりです。

```
Cisco IOS Software, <platform> Software (<image-id>), Version <software-version>,
<software-type>

Technical Support: http://www.cisco.com/techsupport
Copyright (c) <date-range> by Cisco Systems, Inc.
Compiled <day> <date> <time> by <compiler-id>

ROM: System Bootstrap, Version <software-version>, <software-type>
BOOTLDR: <platform> Software (image-id), Version <software-version>, <software-type>

<router-name> uptime is <w> weeks, <d> days, <h> hours,
<m> minutes
System returned to ROM by reload at <time> <day> <date>
System image file is "<filesystem-location>/<software-image-name>"
Last reload reason: <reload-reason>Cisco <platform-processor-type>
processor (revision <processor-revision-id>) with <free-DRAM-memory>
K/<packet-memory>K bytes of memory.
Processor board ID <ID-number>

<CPU-type> CPU at <clock-speed>Mhz, Implementation <number>, Rev <
Revision-number>, <kilobytes-Processor-Cache-Memory>KB <cache-Level> Cache
```

この出力のフィールドの説明については、「例」を参照してください。

**show version** を入力すると、IOS XE ソフトウェアのバージョンと IOS XE ソフトウェアバンドルが表示されます。このバンドルには、スイッチで実行されるソフトウェアの完全なセットを構成する一連の個別パッケージが含まれています。

**show version running** コマンドは、スイッチで現在実行されている個々のパッケージのリストを表示します。インストールモードで起動した場合、通常は起動したプロビジョニングファイルにリストされているパッケージのセットになります。バンドルモードで起動した場合、通常はバンドルに含まれているパッケージのセットになります。

**show version provisioned** コマンドは、プロビジョニングされたパッケージセットに関する情報を表示します。

次に、Cisco Catalyst 9300 シリーズスイッチでの **show version** コマンドの出力例を示します。

```
Device# show version
Cisco IOS XE Software, Version BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2
Cisco IOS Software [Fujil], Catalyst L3 Switch Software (CAT9K_IOSXE), Experimental Version
 16.10.20180903:072347
[v1610_throttle-/nobackup/mcpre/BLD-BLD_V1610_THROTTLE_LATEST_20180903_070602 183]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 03-Sep-18 11:53 by mcpre
```

```
Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.
```

```
ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 16.10.1r, RELEASE SOFTWARE (P)
```

```
C9300 uptime is 20 hours, 7 minutes
Uptime for this control processor is 20 hours, 8 minutes
System returned to ROM by Image Install
System image file is "flash:packages.conf"
Last reload reason: Image Install
```

```
This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
```

```
If you require further assistance please contact us by sending email to
export@cisco.com.
```

Technology Package License Information:

```
-----
Technology-package
Current                                Type                                Technology-package
Next reboot
-----
network-advantage                      Smart License                      network-advantage
dna-advantage                          Subscription Smart License        dna-advantage
```

```

Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco C9300-24U (X86) processor with 1415813K/6147K bytes of memory.
Processor board ID FCW2125L0BH
8 Virtual Ethernet interfaces
56 Gigabit Ethernet interfaces
16 Ten Gigabit Ethernet interfaces
4 TwentyFive Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
1638400K bytes of Crash Files at crashinfo-2:.
11264000K bytes of Flash at flash:.
11264000K bytes of Flash at flash-2:.
0K bytes of WebUI ODM Files at webui:.

Base Ethernet MAC Address       : 70:d3:79:be:6c:80
Motherboard Assembly Number     : 73-17954-06
Motherboard Serial Number       : FOC21230KPX
Model Revision Number           : A0
Motherboard Revision Number     : A0
Model Number                    : C9300-24U
System Serial Number            : FCW2125L0BH

Switch Ports Model          SW Version  SW Image        Mode
-----
*   1 40    C9300-24U    16.10.1    CAT9K_IOSXE    INSTALL
   2 40    C9300-24U    16.10.1    CAT9K_IOSXE    INSTALL

Switch 02
-----
Switch uptime                : 20 hours, 8 minutes

Base Ethernet MAC Address     : 70:d3:79:84:85:80
Motherboard Assembly Number   : 73-17954-06
Motherboard Serial Number     : FOC21230KPK
Model Revision Number         : A0
Motherboard Revision Number   : A0
Model Number                  : C9300-24U
System Serial Number          : FCW2125L03W
Last reload reason            : Image Install

Configuration register is 0x102

次に、Cisco Catalyst 9300 シリーズ スイッチで show version running コマンドを入力して、2 メンバスタックの両方のスイッチで現在実行されているパッケージに関する情報を表示する例を示します。

Device# show version running
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: /flash/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 6a43991bae5b94de0df8083550f827a3c01756c5

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
  Role: rp_base

```

```
File:
/flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpboot, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
Role: rp_boot
File:
/flash/cat9k-rpboot.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: n/a

Package: guestshell, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
Role: guestshell
File:
/flash/cat9k-guestshell.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 10827f9f9db3b016d19a926acc6be0541440b8d7

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
Role: rp_daemons
File:
/flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
Role: rp_iosd
File:
/flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
Role: rp_security
File:
/flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: webui, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
active
Role: rp_webui
File:
/flash/cat9k-webui.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on:
RP0/0
Built: 2018-09-03_13.11, by: mcpre
File SHA1 checksum: 5112d7749b38fale122ce6ee1bfb266ad7eb553a

Package: srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
Role: srdriver
File:
```



```
/flash/cat9k-srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: aff411e981a8dfc8de14005cc33462dc69f8bfaf

Package: cc_srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
  Role: cc_srdriver
  File:
/flash/cat9k-cc_srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: e3da784f3e61ef1e153028e53d9dc94b2c9b1bf7
```

次に、2 メンバスタックのアクティブスイッチである Cisco Catalyst 9300 シリーズ スイッチで **show version provisioned** コマンドを入力した場合の例を示します。 **show version provisioned** コマンドは、プロビジョニングされたパッケージセットに含まれているパッケージに関する情報を表示します。

```
Device# show version provisioned
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: /flash/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 6a43991bae5b94de0df8083550f827a3c01756c5

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: rp_base
  File:
/flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: guestshell, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: guestshell
  File:
/flash/cat9k-guestshell.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 10827f9f9db3b016d19a926acc6be0541440b8d7

Package: rpboot, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: rp_boot
  File:
/flash/cat9k-rpboot.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: n/a

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: rp_daemons
  File:
/flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885
```

```
Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: rp_iosd
  File:
/flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: rp_security
  File:
/flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: webui, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_webui
  File:
/flash/cat9k-webui.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on:
RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 5112d7749b38fa1e122ce6ee1bfb266ad7eb553a

Package: wlc, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_wlc
  File: /flash/cat9k-wlc.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: ada21bb3d57e1b03e5af2329503ed6caa7236d6e

Package: srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: srdriver
  File:
/flash/cat9k-srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: aff411e981a8dfc8de14005cc33462dc69f8bfaf

Package: espbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: fp
  File:
/flash/cat9k-espbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: ESP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 1a2317485f285a3945b31ae57aa64c56ed30a8c0

Package: sipbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: cc
  File:
/flash/cat9k-sipbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: ce821195f0c0bd5e44f21e32fca76cf9b2eed02b

Package: sipspa, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
```

```

Role: cc_spa
File:
/flash/cat9k-sipspa.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 54645404860b662d72f8ff7fa5e6e88cb0960e20

Package: cc_srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: cc_srdriver
  File:
/flash/cat9k-cc_srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: e3da784f3e61ef1e153028e53d9dc94b2c9b1bf7

```

表 14 : show version running のフィールドの説明

フィールド	説明
Package:	個々のサブパッケージの名前。
version:	個々のサブパッケージのバージョン。
status :	特定のスーパーバイザモジュールに対してパッケージがアクティブであるか非アクティブであるか。
File:	個々のパッケージファイルのファイル名。
on:	このパッケージが実行されているアクティブまたはスタンバイのスーパーバイザのロット番号。
Built:	個々のパッケージが作成された日付。

## system env temperature threshold yellow

イエローのしきい値を決定する、イエローとレッドの温度しきい値の差を設定するには、グローバル コンフィギュレーション コマンドで **system env temperature threshold yellow** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**system env temperature threshold yellow value**  
**no system env temperature threshold yellow value**

### 構文の説明

*value* イエローとレッドのしきい値の差を指定します (摂氏)。指定できる範囲は 10 ~ 25 です。

### コマンド デフォルト

デフォルト値は次のとおりです。

表 15: 温度しきい値のデフォルト値

デバイス	イエローとレッドの差	レッド <sup>1</sup>
	14 °C	60 °C

<sup>1</sup> レッドの温度しきい値を設定することはできません。

### 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

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

### 使用上のガイドライン

グリーンとレッドのしきい値を設定することはできませんが、イエローのしきい値を設定することはできます。イエローとレッドのしきい値の差を指定して、イエローのしきい値を設定するには、**system env temperature threshold yellow value** グローバル コンフィギュレーション コマンドを使用します。たとえば、レッドしきい値が 66 °C の場合に、イエローしきい値を 51 °C に設定するには、しきい値の差を 15 に設定するために、**system env temperature threshold yellow 15** コマンドを使用します。たとえば、レッドしきい値が 60 °C の場合に、イエローしきい値を 51 °C に設定するには、しきい値の差を 9 に設定するために、**system env temperature threshold yellow 9** コマンドを使用します。



(注) デバイス内部の温度センサーでシステム内の温度を測定するため、±5 °C の差が生じる可能性があります。

### 例

次の例では、イエローとレッドのしきい値の差を 15 に設定する方法を示します。

```
Device(config)# system env temperature threshold yellow 15  
Device(config)#
```

## tracert mac

指定の送信元 MAC アドレスから指定の宛先 MAC アドレスまでをパケットが通過するレイヤ 2 パスを表示するには、特権 EXEC モードで **tracert mac** コマンドを使用します。

```
tracert mac [interface interface-id] source-mac-address [interface interface-id]
destination-mac-address [vlan vlan-id] [detail]
```

構文の説明	<b>interface</b> <i>interface-id</i> (任意) 送信元または宛先デバイス上のインターフェイスを指定します。						
	<i>source-mac-address</i> 送信元デバイスの 16 進形式の MAC アドレス。						
	<i>destination-mac-address</i> 宛先デバイスの 16 進形式の MAC アドレス。						
	<b>vlan</b> <i>vlan-id</i> (任意) 送信元デバイスから宛先デバイスまでをパケットが通過するレイヤ 2 のパスをトレースする VLAN を指定します。指定できる VLAN ID の範囲は 1 ~ 4094 です。						
	<b>detail</b> (任意) 詳細情報を表示するよう指定します。						
コマンド デフォルト	デフォルトの動作や値はありません。						
コマンド モード	特権 EXEC						
コマンド履歴	<table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>Cisco IOS XE Gibraltar 16.11.1</td> <td>このコマンドが導入されました。</td> </tr> <tr> <td>Cisco IOS XE Bengaluru 17.5.1</td> <td><b>tracert mac</b> コマンドの出力エラーメッセージで、<b>aborted</b> は <b>terminated</b> に置き換えられました。</td> </tr> </tbody> </table>	リリース	変更内容	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。	Cisco IOS XE Bengaluru 17.5.1	<b>tracert mac</b> コマンドの出力エラーメッセージで、 <b>aborted</b> は <b>terminated</b> に置き換えられました。
リリース	変更内容						
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。						
Cisco IOS XE Bengaluru 17.5.1	<b>tracert mac</b> コマンドの出力エラーメッセージで、 <b>aborted</b> は <b>terminated</b> に置き換えられました。						
使用上のガイドライン	<p>レイヤ 2 のトレースルートを適切に機能させるには、Cisco Discovery Protocol (CDP) がネットワークのすべてのデバイスでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。</p> <p>デバイスがレイヤ 2 パス内でレイヤ 2 トレースルートをサポートしていないデバイスを検知した場合、デバイスはレイヤ 2 トレースクエリを送信し続け、タイムアウトにします。</p> <p>パス内で識別可能な最大ホップ数は 10 です。</p> <p>レイヤ 2 <b>tracert</b> はユニキャストトラフィックだけをサポートします。マルチキャストの送信元または宛先 MAC アドレスを指定しても、物理的なパスは識別されず、エラーメッセージが表示されます。</p> <p>指定された送信元および宛先アドレスが同じ VLAN にある場合、<b>tracert mac</b> コマンド出力はレイヤ 2 パスを表示します。</p>						

異なる VLAN にある送信元および宛先アドレスを指定した場合、レイヤ 2 パスは識別されず、エラーメッセージが表示されます。

送信元または宛先 MAC アドレスが複数の VLAN に属する場合は、送信元および宛先 MAC アドレスの両方が属している VLAN を指定する必要があります。

VLAN を指定しないと、パスは識別されず、エラーメッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 traceroute 機能はサポートされません。

複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラーメッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

## 例

次の例では、送信元および宛先 MAC アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5          (2.2.5.5      ) : Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1      ) : Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2      ) : Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

次の例では、**detail** キーワードを使用することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 / WS-C3750E-24PD / 2.2.6.6 :
    Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先デバイスのインターフェイスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
```

```

con5          (2.2.5.5      ) : Gi0/0/3 => Gi0/0/1
con1          (2.2.1.1      ) : Gi0/0/1 => Gi0/0/2
con2          (2.2.2.2      ) : Gi0/0/2 => Gi0/0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed

```

次の例では、デバイスが送信元デバイスに接続されていない場合のレイヤ 2 のパスを示します。

```

Device# tracert mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
con5 / WS-C3750E-24TD / 2.2.5.5 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.

```

次の例では、デバイスが送信元 MAC アドレスの宛先ポートを検出できない場合のレイヤ 2 のパスを示します。

```

Device# tracert mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace terminated.

```

次の例では、送信元および宛先デバイスが異なる VLAN にある場合のレイヤ 2 のパスを示します。

```

Device# tracert mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace terminated.

```

次の例では、宛先 MAC アドレスがマルチキャストアドレスの場合のレイヤ 2 のパスを示します。

```

Device# tracert mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address

```

次の例では、送信元および宛先デバイスが複数の VLAN にある場合のレイヤ 2 のパスを示します。

```

Device# tracert mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace terminated.

```



## traceroute mac ip

指定の送信元 IP アドレスまたはホスト名から、指定の宛先 IP アドレスまたはホスト名を通過するパケットのレイヤ 2 パスを表示するには、特権 EXEC モードで **traceroute mac ip** コマンドを使用します。

```
traceroute mac ip source-ip-address source-hostname destination-ip-address
destination-hostname [detail]
```

### 構文の説明

<i>source-ip-address</i>	32 ビットの値（ドット付き 10 進表記）で指定された送信元デバイスの IP アドレス。
<i>source-hostname</i>	送信元デバイスの IP ホスト名。
<i>destination-ip-address</i>	32 ビットの値（ドット付き 10 進表記）で指定された宛先デバイスの IP アドレス。
<i>destination-hostname</i>	宛先デバイスの IP ホスト名。
<b>detail</b>	（任意）詳細情報を表示するよう指定します。

### コマンドデフォルト

デフォルトの動作や値はありません。

### コマンドモード

特権 EXEC

### コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。
Cisco IOS XE Bengaluru 17.5.1	<b>traceroute mac ip</b> コマンドの出力エラーメッセージで、 <b>aborted</b> は <b>terminated</b> に置き換えられました。

### 使用上のガイドライン

レイヤ 2 のトレーズルートを適切に機能させるには、Cisco Discovery Protocol (CDP) がネットワークの各デバイスでイネーブルになっている必要があります。CDP をディセーブルにすることは避けてください。

デバイスがレイヤ 2 パス内でレイヤ 2 トレーズルートをサポートしていないデバイスを検知した場合、デバイスはレイヤ 2 トレーズクエリを送信し続け、タイムアウトにします。

パス内で識別可能な最大ホップ数は 10 です。

指定された送信元および宛先の IP アドレスが同一のサブネット内にある場合、**traceroute mac ip** コマンド出力はレイヤ 2 パスを表示します。

IP アドレスを指定した場合、デバイスは Address Resolution Protocol (ARP) を使用し、IP アドレスとそれに対応する MAC アドレスおよび VLAN ID を対応させます。

- 指定の IP アドレスの ARP のエントリが存在している場合、デバイスは関連付けられた MAC アドレスを使用し、物理パスを識別します。
- ARP のエントリが存在しない場合、デバイスは ARP クエリを送信し、IP アドレスを解決しようと試みます。IP アドレスは同一のサブネットにある必要があります。IP アドレスが解決されない場合は、パスは識別されず、エラーメッセージが表示されます。

複数の装置がハブを介して 1 つのポートに接続されている場合（たとえば、複数の CDP ネイバーがポートで検出されるなど）、レイヤ 2 tracert 機能はサポートされません。

複数の CDP ネイバーが 1 つのポートで検出された場合、レイヤ 2 パスは特定されず、エラーメッセージが表示されます。

この機能は、トークンリング VLAN ではサポートされません。

## 例

次の例では、**detail** キーワードを使用して、送信元と宛先の IP アドレスを指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# tracert mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
    Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
    Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
    Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
    Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

次の例では、送信元および宛先ホスト名を指定することで、レイヤ 2 のパスを表示する方法を示します。

```
Device# tracert mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5           (2.2.5.5)   ) : Gi0/0/3 => Gi0/1
con1           (2.2.1.1)   ) : Gi0/0/1 => Gi0/2
con2           (2.2.2.2)   ) : Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

次の例では、ARP が送信元 IP アドレスと対応する MAC アドレスを関連付けられない場合の、レイヤ 2 のパスを示します。

```
Device# traceroute mac ip 2.2.66.66 2.2.77.77  
Arp failed for destination 2.2.77.77.  
Layer2 trace terminated.
```

# type

1 つ以上のファイルの内容を表示するには、ブートローダモードで **type** コマンドを使用します。

**type** *filesystem:/file-url...*

## 構文の説明

*filesystem:* ファイルシステムのエイリアス。システム ボードフラッシュ デバイスには **flash:** を使用します。USB メモリスティックには **usbflash0:** を使用します。

*/file-url...* 表示するファイルのパス（ディレクトリ）および名前です。ファイル名はスペースで区切ります。

## コマンド デフォルト

デフォルトの動作や値はありません。

## コマンド モード

ブートローダ

## コマンド履歴

リリース	変更内容
Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

## 使用上のガイドライン

ファイル名およびディレクトリ名は、大文字と小文字を区別します。

ファイルのリストを指定すると、各ファイルの内容が順次表示されます。

## 例

次に、ファイルの内容を表示する例を示します。

```
Device: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

# unset

1つ以上の環境変数をリセットするには、ブートローダモードで**unset** コマンドを使用します。

**unset variable...**

## 構文の説明

<i>variable</i>	<i>variable</i> には、次に示すキーワードのいずれかを使用します。  <b>MANUAL_BOOT</b> : デバイスの起動を自動で行うか手動で行うかどうかを指定します。  <b>BOOT</b> : 自動起動時に、実行可能ファイルのリストをリセットして、ロードおよび実行します。 <b>BOOT</b> 環境変数が設定されていない場合、システムは、フラッシュファイルシステム全体に再帰的な縦型検索を行って、最初に検出された実行可能イメージをロードして実行を試みます。 <b>BOOT</b> 変数が設定されていても、指定されたイメージをロードできなかった場合、システムはフラッシュファイルシステムで最初に検出した起動可能なファイルを起動しようとします。  <b>ENABLE_BREAK</b> : フラッシュファイルシステムの初期化後に、コンソール上の <b>Break</b> キーを使用して自動ブートプロセスを中断できるかどうかを指定します。  <b>HELPER</b> : ブートローダの初期化中に動的にロードされるロード可能ファイルのセミコロン区切りリストを識別します。ヘルパーファイルは、ブートローダの機能を拡張したり、パッチを当てたりします。  <b>PS1</b> : ブートローダモードの場合に、コマンドラインプロンプトとして使用する文字列を指定します。  <b>CONFIG_FILE</b> : Cisco IOS がシステム設定の不揮発性コピーの読み書きに使用するファイル名をリセットします。  <b>BAUD</b> : コンソールで使用される速度（ビット/秒 (b/s) 単位）をリセットします。コンフィギュレーションファイルに別の設定が指定されていない限り、Cisco IOS ソフトウェアはブートローダからボーレート設定を継承し、この値を引き続き使用します。
-----------------	---

コマンドデフォルト デフォルトの動作や値はありません。

コマンドモード ブートローダ

コマンド履歴	リリース	変更内容
	Cisco IOS XE Gibraltar 16.11.1	このコマンドが導入されました。

使用上のガイドライン 通常的环境では、環境変数の設定を変更する必要はありません。

MANUAL\_BOOT 環境変数は、**no boot manual** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

BOOT 環境変数は、**no boot system** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

ENABLE\_BREAK 環境変数は、**no boot enable-break** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

HELPER 環境変数は、**no boot helper** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

CONFIG\_FILE 環境変数は、**no boot config-file** グローバル コンフィギュレーション コマンドを使用してリセットすることもできます。

### 例

次に、SWITCH\_PRIORITY 環境変数をリセットする例を示します。

```
Device: unset SWITCH_PRIORITY
```

## upgrade rom-monitor capsule

カプセル方式を使用して読み取り専用メモリモニタ（ROMMON）をアップグレードするには、特権 EXEC モードで **upgrade rom-monitor capsule** コマンドを使用します。

スタンドアロン デバイス

**upgrade rom-monitor capsule golden | primary[R0 | RP active]**

ハイ アベイラビリティ対応デバイス

**upgrade rom-monitor capsule golden | primary[R0 | R1 | RP active | standby]**

StackWise Virtual 対応デバイス

**upgrade rom-monitor capsule golden | primary[R0 | R1 | RP active | standby | switch *switch\_number* | active | standbyR0 | R1 | RP active | standby]**

### 構文の説明

<b>golden</b>	アップグレードするゴールド ROMMON を指定します。
<b>primary</b>	アップグレードするプライマリ ROMMON を指定します。
<b>R0</b>	ルートプロセッサ（RP）スロット 3 の ROMMON をアップグレードします。
<b>R1</b>	RP スロット 4 の ROMMON をアップグレードします。
<b>RP {active   standby}</b>	RP スロット 1 およびスロット 2 の ROMMON をアップグレードします。  <ul style="list-style-type: none"> <li>• <b>active</b> : アクティブインスタンスを指定します。</li> <li>• <b>standby</b> : スタンバイインスタンスを指定します。</li> </ul>
<b>switch {<i>switch_number</i>   active   standby}</b>	スイッチを指定します。  <ul style="list-style-type: none"> <li>• <i>switch_number</i> : スイッチの ID。有効な範囲は 1 ～ 2 です。</li> <li>• <b>active</b> : アクティブスイッチを指定します。</li> <li>• <b>standby</b> : スタンバイスイッチを指定します。</li> </ul>

### コマンド デフォルト

このコマンドには、デフォルト設定がありません。

### コマンド モード

特権 EXEC (#)

### コマンド履歴

リリース	変更内容
Cisco IOS XE Amsterdam 17.1.1	このコマンドが導入されました。

**使用上のガイドライン** ROMMONバージョンのアップグレードがソフトウェアバージョンに適用可能かどうかを確認するには、対応するソフトウェアリリースのリリースノートを参照してください。

<https://www.cisco.com/c/en/us/support/switches/catalyst-9600-series-switches/products-release-notes-list.html>

**例**

次に、StackWise Virtual 対応デバイスでゴールデン ROMMON をアップグレードする例を示します。

```
Device# upgrade rom-monitor capsule golden switch active R0

This operation will reload the switch and take a few minutes to complete.
Do you want to proceed (y/n)? [confirm]y

Device#

Initializing Hardware .....

!
!
!

Warning : New region (type 2) access rights will be modified

Updating Block at FFFFF000h 100%

Restarting switch to complete capsule upgrade

<output truncated>
```





