Cisco Nexus 5000 シリーズ NX-OS TrustSec コマンド リファレンス

Cisco NX-OS Release 5.x

初版：2011 年 11 月
最終更新日：2011 年 12 月

Text Part Number: OL-25830-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Nexus 5000 シリーズ NX-OS TrustSec コマンド リファレンス

CONTENTS

はじめに

ここでは、『Cisco Nexus 5000 シリーズ NX-OS TrustSec コマンド リファレンス』の対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

この前書きは、次の項で構成されています。

対象読者

このマニュアルは、Cisco NX-OS デバイスを設定および管理する経験豊富なユーザの方を対象としています。

サポートされるスイッチ

ここでは、次の内容について説明します。

Cisco Nexus 5500 プラットフォーム スイッチ

表 1 に、Cisco Nexus 5500 プラットフォームでサポートされる Cisco スイッチを示します。

（注） これらのスイッチの詳細については、次の URL にある『*Cisco Nexus 5500 Platform and Cisco Nexus 5000 Platform Hardware Installation Guide*』を参照してください。
http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

表 1　サポートされる Cisco Nexus 5500 プラットフォーム スイッチ

スイッチ	説明
Cisco Nexus 5548P スイッチ	Cisco Nexus 5548P スイッチは、Cisco Nexus 5500 プラットフォームの最初のスイッチです。このスイッチは、1 Rack-Unit（1 RU）の 10 ギガビット イーサネットおよび Fibre Channel over Ethernet（FCoE）スイッチであり、最大 960 Gbps スループットおよび最大 48 ポートを提供します。
Cisco Nexus 5596P スイッチ	Cisco Nexus 5596P スイッチは、Top-of-Rack の 10 ギガビット イーサネットおよび FCoE スイッチであり、最大 1920 ギガビット スループットおよび最大 96 ポートを提供します。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章タイトル	説明
「新機能および変更された機能に関する情報」	新しい Cisco NX-OS ソフトウェア リリースの新機能および変更された機能について説明します。
「A コマンド」	A で始まる Cisco NX-OS TrustSec コマンドについて説明します。
「C コマンド」	C で始まる Cisco NX-OS TrustSec コマンドについて説明します。
「F コマンド」	F で始まる Cisco NX-OS TrustSec コマンドについて説明します。
「P コマンド」	P で始まる Cisco NX-OS TrustSec コマンドについて説明します。
「show コマンド」	Cisco NX-OS TrustSec の **show** コマンドについて説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[　]	角カッコの中の要素は、省略可能です。
{x | y | z}	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

出力例では、次の表記法を使用しています。

screen フォント	スイッチに表示される端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「*注釈*」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

Cisco Nexus 5000 シリーズ スイッチおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダ のマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

次に、Cisco Nexus 5000 シリーズおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダに関連するマニュアルを示します。

リリース ノート

『Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Release Notes』

『Cisco Nexus 5000 Series Switch Release Notes』

コンフィギュレーション ガイド

『Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 5.0(2)N1(1)』

『Cisco Nexus 5000 Series Configuration Limits for Cisco NX-OS Release 4.2(1)N1(1) and Release 4.2(1)N2(1)』

『Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Layer 2 Switching Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Multicast Routing Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide』

『Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Security Configuration Guide』

『Cisco Nexus 5000 Series NX-OS System Management Configuration Guide』

『Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide』

『Cisco Nexus 5000 Series Switch NX-OS Software Configuration Guide』

『Cisco Nexus 5000 Series Fabric Manager Configuration Guide, Release 3.4(1a)』

『Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide, Release 6.x』

『Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide』

メンテナンスおよび操作ガイド

『Cisco Nexus 5000 Series NX-OS Operations Guide』

インストレーション ガイドおよびアップグレード ガイド

『Cisco Nexus 5000 Series and Cisco Nexus 5500 Platform Hardware Installation Guide』

『Cisco Nexus 2000 Series Hardware Installation Guide』

『Cisco Nexus 5000 Series NX-OS Software Upgrade and Downgrade Guide, Release 4.2(1)N1(1)』

『Regulatory Compliance and Safety Information for the Cisco Nexus 5000 Series Switches and Cisco Nexus 2000 Series Fabric Extenders』

ライセンス ガイド

『Cisco NX-OS Licensing Guide』

コマンド リファレンス

『Cisco Nexus 5000 Series NX-OS FabricPath Command Reference』

『Cisco Nexus 5000 Series NX-OS Fabric Extender Command Reference』

『Cisco Nexus 5000 Series NX-OS Fibre Channel Command Reference』

『Cisco Nexus 5000 Series NX-OS Fundamentals Command Reference』

『Cisco Nexus 5000 Series NX-OS Layer 2 Interfaces Command Reference』

『Cisco Nexus 5000 Series NX-OS Multicast Routing Command Reference』

『Cisco Nexus 5000 Series NX-OS QoS Command Reference』

『Cisco Nexus 5000 Series NX-OS Security Command Reference』

『Cisco Nexus 5000 Series NX-OS System Management Command Reference』

『Cisco Nexus 5000 シリーズ NX-OS TrustSec コマンド リファレンス』

『Cisco Nexus 5000 Series NX-OS Unicast Routing Command Reference』

『Cisco Nexus 5000 Series NX-OS vPC Command Reference』

テクニカル リファレンス

『Cisco Nexus 5000 Series and Cisco Nexus 2000 Series Fabric Extender MIBs Reference』

エラー メッセージおよびシステム メッセージ

『Cisco NX-OS System Messages Reference』

トラブルシューティング ガイド

『Cisco Nexus 5000 Troubleshooting Guide』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

新機能および変更された機能に関する情報

この章では、『Cisco Nexus 5000 シリーズ NX-OS TrustSec コマンド リファレンス』の新機能および変更された機能に関するリリース固有の情報を示します。このマニュアルの最新バージョンは、次のシスコ Web サイトから入手できます。

http://www.cisco.com/en/US/products/ps9670/prod_command_reference_list.html

この Cisco NX-OS リリースに関する追加情報を確認するには、次のシスコ Web サイトから入手できる『*Cisco Nexus 5000 Series Switch Release Notes*』を参照してください。

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

Cisco NX-OS リリースの新機能および変更された機能に関する情報

ここでは、次の内容について説明します。

Cisco NX-OS Release 5.1(3)N1(1) の新機能および変更された機能に関する情報

表 1 では、Cisco NX-OS Release 5.1(3)N1(1) の新機能および変更された機能を要約し、その参照先を示しています。

表 1　　Release 5.1(3)N1(1) の新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
Cisco TrustSec	この機能が導入されました。	5.1(3)N1(1)	「A コマンド」 「C コマンド」 「D コマンド」 「F コマンド」 「P コマンド」 「show コマンド」

A コマンド

この章では、A で始まる Cisco NX-OS TrustSec コマンドについて説明します。

aaa authentication cts default group

Cisco TrustSec 認証のデフォルト AAA RADIUS サーバ グループを設定するには、**aaa authentication cts default group** コマンドを使用します。デフォルト AAA 認証サーバ グループ リストからサーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa authentication cts default group *group-list*

no aaa authentication cts default group *group-list*

構文の説明

group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。

コマンド デフォルト

なし

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバの名前付きグループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa groups** コマンドを使用します。これらのコマンドの詳細については、『*Cisco Nexus 5000 Series NX-OS Security Command Reference*』を参照してください。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec のデフォルト AAA 認証 RADIUS サーバ グループを設定する例を示します。

```
switch# configure terminal
swtich(config)# aaa authentication cts default group RadGroup
swtich(config)#
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証の設定を表示します。
show aaa groups	AAA サーバ グループを表示します。

aaa authorization cts default group

Cisco TrustSec 認可のデフォルト AAA RADIUS サーバ グループを設定するには、**aaa authorization cts default group** コマンドを使用します。デフォルト AAA 認可サーバ グループ リストからサーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa authorization cts default group *group-list*

no aaa authorization cts default group *group-list*

構文の説明

group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius**：設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。

コマンド デフォルト

なし

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

aaa authorization cts default group コマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバの名前付きグループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa groups** コマンドを使用します。これらのコマンドの詳細については、『*Cisco Nexus 5000 Series NX-OS Security Command Reference*』を参照してください。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに Cisco NX-OS ソフトウェアが各グループをチェックします。

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec のデフォルト AAA 認可 RADIUS サーバ グループを設定する例を示します。

```
switch# configure terminal
swtich(config)# aaa authorization cts default group RadGroup
swtich(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。
show aaa groups	AAA サーバ グループを表示します。

C コマンド

この章では、C で始まる Cisco NX-OS TrustSec コマンドについて説明します。

clear cts policy

Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）ポリシーをクリアするには、**clear cts policy** コマンドを使用します。

clear cts policy {**all** | **peer** *device-id* | **sgt** *sgt-value*}

構文の説明

all	ローカル デバイス上のすべての Cisco TrustSec SGACL をクリアします。
peer *device-id*	ローカル デバイス上のピア デバイスの Cisco TrustSec SGACL ポリシーをクリアします。
sgt *sgt-value*	ローカル デバイス上のセキュリティ グループ タグ（SGT）に対する Cisco TrustSec SGACL ポリシーをクリアします。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

SGACL ポリシーをクリアすると、動作は、インターフェイスがフラップするまで有効になりません。インターフェイスがスタティック SGT のインターフェイスである場合、SGT 値はフラッピングのあとにゼロ（0）に設定されます。この操作を取り消すには、次のコマンドを使用します。

```
switch(config-if-cts-manual)# no policy static
switch(config-if-cts-manual)# policy static sgt sgt-value
switch(config-if-cts-manual)#
```

インターフェイスがダイナミック SGT のインターフェイスである場合、SGT はフラッピングのあとに、RADIUS サーバから再ダウンロードされます。

このコマンドには、ライセンスは必要ありません。

例

次に、デバイスのすべての Cisco TrustSec SGACL ポリシーをクリアする例を示します。

```
switch# clear cts policy all
switch#
```

関連コマンド

コマンド	説明
cts role-based sgt	SGACL に SGT をマッピングします。
feature cts	Cisco TrustSec 機能をイネーブルにします。

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
policy	インターフェイスに認証ポリシーを設定します。
show cts role-based policy	Cisco TrustSec の SGACL ポリシー情報を表示します。

clear cts role-based counters

ロールベース アクセス コントロール リスト（RBACL）統計情報をすべてのカウンタが 0 にリセットされるようにクリアするには、**clear cts role-based counters** コマンドを使用します。

clear cts role-based counters

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

任意のコンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、RBACL 統計情報をクリアする例を示します。

```
switch# clear cts role-based counters
switch#
```

関連コマンド

コマンド	説明
cts role-based counters enable	RBACL 統計情報をイネーブルにします。
show cts role-based counters	RBACL 統計情報の設定ステータスを表示し、すべての RBACL ポリシーの統計情報を一覧表示します。

cts device-id

Cisco TrustSec デバイス ID を設定するには、**cts device-id** コマンドを使用します。

cts device-id *device-id* **password** [**7**] *password*

構文の説明

device-id	Cisco TrustSec デバイス ID 名。名前には英数字を使用します。大文字と小文字が区別され、最大長は 32 文字です。
password	EAP-FAST 処理中に使用するパスワードを（クリア テキストまたは暗号化で）指定します。
7	（任意）パスワードが暗号化されたテキストであること指定します。
password	Cisco TrustSec デバイスのパスワード。最大で 32 文字の英数字を使用でき、大文字と小文字が区別されます。

コマンド デフォルト

Cisco TrustSec デバイス ID なし
クリア テキスト パスワード

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec デバイス ID 名は固有でなければなりません。

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec デバイス ID を設定する例を示します。

```
switch# configure terminal
swtich(config)# cts device-id DeviceA password Cisco321
swtich(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	802.1X 機能をイネーブルにします。
show cts credentials	Cisco TrustSec クレデンシャル情報を表示します。

cts manual

インターフェイスの Cisco TrustSec 手動設定を開始するには、**cts manual** コマンドを使用します。手動設定を削除するには、このコマンドの **no** 形式を使用します。

cts manual

no cts manual

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

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、設定を有効にするには、**shutdown** と **no shutdown** コマンド シーケンスを使用することによってインターフェイスをイネーブルおよびディセーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、インターフェイスの Cisco TrustSec 手動コンフィギュレーション モードを開始する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)#
```

次に、インターフェイスから Cisco TrustSec 手動設定を削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# no cts manual
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	802.1X 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定情報を表示します。

cts role-based access-list

Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）を作成または指定して、ロールベース アクセス コントロール リスト コンフィギュレーション モードを開始するには、**cts role-based access-list** コマンドを使用します。SGACL を削除するには、このコマンドの **no** 形式を使用します。

cts role-based access-list *list-name*

no cts role-based access-list *list-name*

構文の説明

list-name	SGACL の名前。名前には英数字を使用します。大文字と小文字が区別され、最大長は 32 文字です。

コマンド デフォルト

なし

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

SGACL を削除すると、アクセス リストは、システム内の任意の SGT-DGT ペアから参照できなくなります。

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec SGACL を作成して、ロールベース アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)#
```

次に、Cisco TrustSec SGACL を削除する例を示します。

```
switch# configure terminal
switch(config)# no cts role-based access-list MySGACL
switch(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts role-based access-list	Cisco TrustSec SGACL の設定を表示します。

cts role-based counters enable

ロールベース アクセス コントロール リスト（RBACL）統計情報をイネーブルにするには、**cts role-based counters enable** コマンドを使用します。RBACL 統計情報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。

cts role-based counters enable

no cts role-based counters enable

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

ディセーブル

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用するには、VLAN での RBACL ポリシーの強制をイネーブルにする必要があります。

RBACL 統計情報をイネーブルにするには、ハードウェアのエントリが各ポリシーに 1 つずつ必要です。ハードウェアに十分な領域がない場合、エラー メッセージが表示され、統計情報をイネーブルにできません。

RBACL 統計情報は、ISSU 時またはアクセス コントロール エントリを RBACL に追加するか削除すると、失われます。

このコマンドには、ライセンスは必要ありません。

例

次に、RBACL 統計情報をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# cts role-based counters enable
Note: Clearing previously collected counters...
switch(config)#
```

次に、RBACL 統計情報をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no cts role-based counters enable
switch(config)#
```

関連コマンド

コマンド	説明
clear cts role-based counters	すべてのカウンタが 0 にリセットされるように、RBACL 統計情報をクリアします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts role-based counters	RBACL 統計情報の設定ステータスを表示し、すべての RBACL ポリシーの統計情報を一覧表示します。

cts role-based enforcement

VLAN のロールベース アクセス コントロール リスト（RBACL）の強制をイネーブルにするには、**cts role-based enforcement** コマンドを使用します。VLAN での RBACL の強制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。

cts role-based enforcement

no cts role-based enforcement

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

ディセーブル

コマンド モード

VLAN コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

RBACL の強制は VLAN 単位でイネーブルになります。RBACL の強制は、ルーテッド VLAN またはインターフェイスでイネーブルにできません。RBACL の強制の変更を有効にするには、VLAN コンフィギュレーション モードを終了する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、VLAN での RBACL の強制をイネーブルにし、ステータスを確認する例を示します。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# cts role-based enforcement
switch(config-vlan)# exit
switch(config)# show cts role-based enable
vlan:102
switch(config)#
```

次に、VLAN での RBACL の強制をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# vlan 5
switch(config-vlan)# no cts role-based enforcement
switch(config-vlan)#
```

関連コマンド

コマンド	説明
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts role-based enable	RBACL がイネーブルになっている VLAN を表示します。

cts role-based sgt

セキュリティ グループ アクセス コントロール リスト（SGACL）と Cisco TrustSec Security Group Tag（SGT; セキュリティ グループ タグ）のマッピングを手動で設定するには、**cts role-based sgt** コマンドを使用します。SGACL と SGT のマッピングを削除するには、このコマンドの **no** 形式を使用します。

cts role-based sgt {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list** *list-name*

no cts role-based sgt {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**}

構文の説明

sgt-value	送信元 SGT の値。範囲は 0 ～ 65519 です。
any	SGT または宛先 SGT を指定します。
unknown	未知の SGT を指定します。
dgt	宛先 SGT を指定します。
dgt-value	宛先 SGT の値。範囲は 0 ～ 65519 です。
access-list *list-name*	SGACL の名前を指定します。

コマンド デフォルト

なし

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

SGT のマッピングを設定する前に SGACL を設定する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、SGACL の SGT マッピングを設定する例を示します。

```
switch# configure terminal
switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL
switch(config)#
```

次に、宛先 SGT への SGT マッピングを設定する例を示します。

```
switch# configure terminal
switch(config)# cts role-based sgt any dgt any access-list MySGACL
switch(config)#
```

次に、SGACL の SGT マッピングを削除する例を示します。

```
switch# configure terminal
switch(config)# no cts role-based sgt 3 dgt 10
switch(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts role-based policy	SGACL の Cisco TrustSec SGT マッピングを表示します。

cts role-based sgt-map

IP アドレスと Cisco TrustSec セキュリティ グループ タグ（SGT）のマッピングを手動で設定するには、**cts role-based sgt-map** コマンドを使用します。SGT を削除するには、このコマンドの **no** 形式を使用します。

cts role-based sgt-map *ipv4-address sgt-value*

no cts role-based sgt-map *ipv4-address*

構文の説明

ipv4-address	IPv4 アドレス。形式は、*A.B.C.D* です。
sgt-value	SGT 値。指定できる範囲は 1 ～ 65519 です。

コマンド デフォルト

なし

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
VLAN コンフィギュレーション モード
VRF コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec SGT のマッピングを設定する例を示します。

```
switch# configure terminal
switch(config)# cts role-based sgt-map 10.10.1.1 3
switch(config)#
```

次に、Cisco TrustSec SGT のマッピングを削除する例を示します。

```
switch# configure terminal
switch(config)# no cts role-based sgt-map 10.10.1.1
switch(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

コマンド	説明
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts role-based sgt-map	Cisco TrustSec SGT のマッピングを表示します。

cts sgt

Cisco TrustSec セキュリティ グループ タグ（SGT）を設定するには、**cts sgt** 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。

cts sgt *tag*

no cts sgt

構文の説明

tag	**0x***hhhh* 形式の 16 進値であるデバイスのローカル SGT。指定できる範囲は 0x2 ～ 0xffef です。

コマンド デフォルト

なし

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、デバイスの Cisco TrustSec SGT を設定する例を示します。

```
switch# configure terminal
switch(config)# cts sgt 0x3
switch(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts environment-data	Cisco TrustSec 環境データを表示します。

cts sxp connection peer

Cisco TrustSec の SGT Exchange Protocol（SXP）ピア接続を設定するには、**cts sxp connection peer** コマンドを使用します。SXP 接続を削除するには、このコマンドの **no** 形式を使用します。

cts sxp connection peer *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** {*password*| **7** *encrypted-password*}} **mode listener** [**vrf** *vrf-name*]

no cts sxp connection peer *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** {**default** | **none** | **required** {*password* | **7** *encrypted-password*}} **mode listener** [**vrf** *vrf-name*]

構文の説明

peer-ipv4-addr	ピア デバイスの IPv4 アドレス
source *src-ipv4-addr*	（任意）送信元デバイスの IPv4 アドレスを指定します。
password	SXP 認証に使用するパスワード オプションを指定します。
default	SXP がピア接続のデフォルト SXP パスワードを使用するように指定します。
none	SXP がパスワードを使用しないように指定します。
required	SXP がこのピア接続で使用する必要があるパスワードを指定します。
password	テキスト パスワードをクリアします。パスワードには英数字を使用します。大文字と小文字が区別され、最大長は 32 文字です。
7 *encrypted-password*	暗号化パスワードを指定します。最大長は 32 文字です。
mode	ピア デバイスのモードを指定します。
listener	ピアがリスナーとなるように指定します。
vrf *vrf-name*	（任意）ピアの仮想ルーティングおよび転送（VRF）インスタンスを指定します。この VRF の名前には最大 32 文字までの英数字を指定できます。

コマンド デフォルト

デバイスに設定されたデフォルト SXP パスワード
デバイスに設定されたデフォルト SXP 送信元 IPv4 アドレス
デフォルト VRF

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

送信元 IPv4 アドレスを指定しない場合は、**cts sxp default source-ip** コマンドを使用してデフォルト SXP 送信元 IPv4 アドレスを設定する必要があります。

デフォルトをパスワード モードで指定する場合は、**cts sxp default password** コマンドを使用してデフォルト SXP パスワードを設定する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、SXP ピア接続を設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp connection peer 10.10.1.1 source 10.10.2.2 password default mode
listener
switch(config)#
```

次に、SXP ピア接続を削除する例を示します。

```
switch# configure terminal
switch(config)# no cts sxp connection peer 10.10.1.1
switch(config)#
```

関連コマンド

コマンド	説明
cts sxp default password	デバイスのデフォルト SXP パスワードを設定します。
cts sxp default source-ip	デバイスのデフォルト SXP 送信元 IPv4 アドレスを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP ピア接続情報を表示します。

cts sxp default password

デバイスのデフォルト SGT Exchange Protocol（SXP）パスワードを設定するには、**cts sxp default password** コマンドを使用します。デフォルトを削除するには、このコマンドの **no** 形式を使用します。

cts sxp default password {*password* | **7** *encrypted-password*}

no cts sxp default password

構文の説明

password	テキスト パスワードをクリアします。パスワードには英数字を使用します。大文字と小文字が区別され、最大長は 32 文字です。
7 *encrypted-password*	暗号化パスワードを指定します。最大長は 32 文字です。

コマンド デフォルト

なし

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、デバイスのデフォルト SXP パスワードを設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp default password Cisco654
switch(config)#
```

次に、デフォルト SXP パスワードを削除する例を示します。

```
switch# configure terminal
switch(config)# no cts sxp default password
switch(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp default source-ip

デバイスのデフォルト SGT Exchange Protocol（SXP）送信元 IPv4 アドレスを設定するには、**cts sxp default source-ip** 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。

cts sxp default source-ip *ipv4-address*

no cts sxp default source-ip

構文の説明

ipv4-address	デバイスのデフォルト SXP IPv4 アドレス

コマンド デフォルト

なし

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、デバイスのデフォルト SXP 送信元 IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp default source-ip 10.10.3.3
switch(config)#
```

次に、デフォルト SXP 送信元 IP アドレスを削除する例を示します。

```
switch# configure terminal
switch(config)# no cts sxp default source-ip
switch(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp enable

デバイス上の SGT Exchange Protocol（SXP）ピアをイネーブルにするには、**cts sxp enable** 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。

cts sxp enable

no cts sxp enable

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

ディセーブル

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、SXP をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# cts sxp enable
switch(config)#
```

次に、SXP をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no cts sxp enable
switch(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp reconcile-period

SGT Exchange Protocol（SXP）復帰期間タイマーを設定するには、**cts sxp reconcile-period** 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。

cts sxp reconcile-period *seconds*

no cts sxp reconcile-period

構文の説明

seconds	秒数。範囲は 0 ～ 64000 です。

コマンド デフォルト

120 秒（2 分）

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

ピアが SXP 接続を終了すると、内部ホールドダウン タイマーが開始されます。内部ホールドダウン タイマーが終了する前にピアが再接続すると、SXP 復帰期間タイマーが開始されます。

（注） SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになります。

このコマンドには、ライセンスは必要ありません。

例

次に、SXP 復帰期間を設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp reconcile-period 120
switch(config)#
```

次に、SXP 復帰期間をデフォルト値に戻す例を示します。

```
switch# configure terminal
switch(config)# no cts sxp reconcile-period
switch(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP 設定情報を表示します。

cts sxp retry-period

SGT Exchange Protocol（SXP）リトライ期間タイマーを設定するには、**cts sxp retry-period** 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。

cts sxp retry-period *seconds*

no cts sxp retry-period

構文の説明

seconds	秒数。範囲は 0 ～ 64000 です。

コマンド デフォルト

60 秒（1 分）

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

SXP リトライ期間によって、Cisco NX-OS ソフトウェアが SXP 接続を再試行する頻度が決まります。SXP 接続が正常に確立されなかった場合、Cisco NX-OS ソフトウェアは SXP リトライ期間タイマーの終了後に、新たな接続の確立を試行します。

（注） SXP リトライ期間を 0 秒に設定すると、タイマーがディセーブルになり、再試行は実行されません。

このコマンドには、ライセンスは必要ありません。

例

次に、SXP リトライ期間を設定する例を示します。

```
switch# configure terminal
switch(config)# cts sxp retry-period 120
switch(config)#
```

次に、SXP リトライ期間をデフォルト値に戻す例を示します。

```
switch# configure terminal
switch(config)# no cts sxp retry-period
switch(config)#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP ピア接続情報を表示します。

D コマンド

この章では、D で始まる Cisco NX-OS TrustSec コマンドについて説明します。

deny

セキュリティ グループ アクセス コントロール リスト（SGACL）で拒否アクションを設定するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

deny {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

no deny {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

構文の説明

all	すべてのトラフィックを指定します。
icmp	インターネット制御メッセージ プロトコル（ICMP）トラフィックを指定します。
igmp	インターネット グループ管理プロトコル（IGMP）トラフィックを指定します。
ip	IP トラフィックを指定します。
tcp	TCP トラフィックを指定します。
udp	ユーザ データグラム プロトコル（UDP）トラフィックを指定します。
dest	宛先ポート番号を指定します。
dst	宛先ポート番号を指定します。
src	送信元ポート番号を指定します。
eq	ポート番号と同等の番号を指定します。
gt	ポート番号より大きい番号を指定します。
lt	ポート番号より小さい番号を指定します。
neq	ポート番号と同等ではない番号を指定します。
port-number	TCP または UDP のポート番号。指定できる範囲は 0 ～ 65535 です。
range	TCP または UDP のポート範囲を指定します。
port-number1	範囲の開始ポート。指定できる範囲は 0 ～ 65535 です。
port-number2	範囲の終了ポート。指定できる範囲は 0 ～ 65535 です。
log	（任意）この設定に一致するパケットをログに記録することを指定します。

コマンド デフォルト

なし

コマンド モード

ロールベース アクセス コントロール リスト（RBACL）

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

RBACL ロギングをイネーブルにするには、VLAN での RBACL ポリシーの強制をイネーブルにする必要があります。また **cts role-based counters enable** コマンドを使用して Cisco TrustSec カウンタをイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、SGACL に拒否アクションを追加し、RBACL ログをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# deny icmp log
switch(config-rbacl)#
```

次に、SGACL から拒否アクションを削除する例を示します。

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no deny icmp log
switch(config-rbacl)#
```

関連コマンド

コマンド	説明
cts role-based access-list	Cisco TrustSec SGACL を設定します。
cts role-based counters	RBACL カウンタをイネーブルにします。
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
permit	SGACL に許可ルールを設定します。
show cts role-based access-list	Cisco TrustSec SGACL の設定を表示します。

F コマンド

この章では、F で始まる Cisco NX-OS TrustSec コマンドについて説明します。

feature cts

Cisco TrustSec 機能をイネーブルにするには、**feature cts** 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。

feature cts

no feature cts

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

ディセーブル

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、**feature dot1x** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec 機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature cts
switch(config)#
```

次に、Cisco TrustSec 機能をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature cts
switch(config)#
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show cts	Cisco TrustSec のステータス情報を表示します。

feature dot1x

802.1X 機能をイネーブルにするには、**feature dot1x** 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。

feature dot1x

no feature dot1x

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

ディセーブル

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

feature cts コマンドを使用してスイッチの Cisco TrustSec 機能をイネーブルにする前に、**feature dot1x** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、802.1X をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature dot1x
switch(config)#
```

次に、802.1X をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no feature dot1x
switch(config)#
```

関連コマンド

コマンド	説明
show dot1x	802.1X のステータス情報を表示します。
feature cts	スイッチの Cisco TrustSec 機能をイネーブルにします。

P コマンド

この章では、P で始まる Cisco NX-OS TrustSec コマンドについて説明します。

permit

セキュリティ グループ アクセス コントロール リスト（SGACL）に許可ルールを設定するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

permit {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

no permit {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**dest** | **dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

構文の説明

all	すべてのトラフィックを指定します。
icmp	インターネット制御メッセージ プロトコル（ICMP）トラフィックを指定します。
igmp	インターネット グループ管理プロトコル（IGMP）トラフィックを指定します。
ip	IP トラフィックを指定します。
tcp	TCP トラフィックを指定します。
udp	ユーザ データグラム プロトコル（UDP）トラフィックを指定します。
dest	宛先ポート番号を指定します。
dst	宛先ポート番号を指定します。
src	送信元ポート番号を指定します。
eq	ポート番号と同等の番号を指定します。
gt	ポート番号より大きい番号を指定します。
lt	ポート番号より小さい番号を指定します。
neq	ポート番号と同等ではない番号を指定します。
port-number	TCP または UDP のポート番号。指定できる範囲は 0 ～ 65535 です。
range	TCP または UDP のポート範囲を指定します。
port-number1	範囲の開始ポート。指定できる範囲は 0 ～ 65535 です。
port-number2	範囲の終了ポート。指定できる範囲は 0 ～ 65535 です。
log	（任意）この設定に一致するパケットをログに記録することを指定します。

デフォルト

なし

コマンド モード

ロールベース アクセス コントロール リスト（RBACL）

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

RBACL ロギングをイネーブルにするには、VLAN での RBACL ポリシーの強制をイネーブルにする必要があります。また **cts role-based counters enable** コマンドを使用して Cisco TrustSec カウンタをイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、SGACL に許可アクションを追加し、RBACL ログをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# permit icmp log
switch(config-rbacl)#
```

次に、SGACL から許可ルールを削除する例を示します。

```
switch# configure terminal
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no permit icmp log
switch(config-rbacl)#
```

関連コマンド

コマンド	説明
cts role-based access-list	Cisco TrustSec SGACL を設定します。
cts role-based counters	RBACL カウンタをイネーブルにします。
deny	SGACL に拒否アクションを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts role-based access-list	Cisco TrustSec SGACL の設定を表示します。

policy

Cisco TrustSec デバイス識別情報または Security Group Tag（SGT; セキュリティ グループ タグ）を使用して、インターフェイス上に Cisco TrustSec 認証ポリシーを手動で設定するには、**policy** 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。

policy {**dynamic identity** *device-id* | **static sgt** *sgt-value* [**trusted**]}

no policy {**dynamic** | **static**}

構文の説明

dynamic identity	Cisco TrustSec デバイス識別情報を使用してダイナミック ポリシーを指定します。
device-id	Cisco TrustSec デバイス識別情報。デバイス識別情報は、大文字と小文字を区別して指定します。
static sgt	SGT を使用してスタティック ポリシーを指定します。
sgt-value	Cisco TrustSec SGT。形式は、**0x***hhhh* です。範囲は 0x2 ～ 0xffef です。
trusted	（任意）インターフェイス上で受信したトラフィックに SGT が設定されている場合、タグを上書きしません。

コマンド デフォルト

なし

コマンド モード

Cisco TrustSec 手動コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、設定を有効にするには、**shutdown** と **no shutdown** コマンド シーケンスを使用することによってインターフェイスをイネーブルおよびディセーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、インターフェイスにダイナミック Cisco TrustSec ポリシーを手動で設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

次に、手動で設定したダイナミック Cisco TrustSec ポリシーをインターフェイスから削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy dynamic
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

次に、インターフェイスにスタティック Cisco TrustSec ポリシーを手動で設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

次に、手動で設定したスタティック Cisco TrustSec ポリシーをインターフェイスから削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy static
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

関連コマンド

コマンド	説明
cts manual	インターフェイスの Cisco TrustSec 手動コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

propagate-sgt

レイヤ 2 Cisco TrustSec インターフェイス上でセキュリティ グループ タグ（SGT）伝搬をイネーブルにするには、**propagate-sgt** コマンドを使用します。SGT 伝搬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。

propagate-sgt

no propagate-sgt

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

手動設定がインターフェイスでイネーブルにされている場合、イネーブルになります。

手動設定がインターフェイスでディセーブルにされている場合、ディセーブルになります。

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

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、まず **feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにしてから、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

インターフェイスに接続しているピア デバイスで SGT がタグ付けされた Cisco TrustSec パケットを制御できない場合は、そのインターフェイスで SGT 伝搬機能をディセーブルにすることができます。

このコマンドを使用したあと、設定を有効にするには、**shutdown** と **no shutdown** コマンド シーケンスを使用することによってインターフェイスをイネーブルおよびディセーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、SGT 伝搬をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts manual
switch(config-if-cts-manual)# no propagate-sgt
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

次に、SGT 伝搬をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts manual
switch(config-if-cts-manual)# propagate-sgt
```

```
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
switch(config-if)#
```

関連コマンド

コマンド	説明
cts manual	インターフェイスの Cisco TrustSec 手動設定をイネーブルにします。
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

show コマンド

この章では、Cisco NX-OS TrustSec の **show** コマンドについて説明します。

show cts

グローバル Cisco TrustSec 設定を表示するには、**show cts** コマンドを使用します。

show cts

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec グローバル設定を表示する例を示します。

```
switch# show cts
CTS Global Configuration
================================
  CTS support           : enabled
  CTS device identity   : not configured
  SGT                   : 0
  CTS caching support   : disabled

  Number of CTS interfaces in
    DOT1X mode : 0
    Manual mode : 1

switch#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts credentials

Cisco TrustSec デバイスのクレデンシャルの設定を表示するには、**show cts credentials** コマンドを使用します。

show cts credentials

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec のクレデンシャルの設定を表示する例を示します。

```
switch# show cts credentials
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts environment-data

グローバル Cisco TrustSec 環境データを表示するには、**show cts environment-data** コマンドを使用します。

show cts environment-data

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

Cisco NX-OS デバイスは、デバイスで Cisco TrustSec のクレデンシャルを設定し、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を設定したあと、ACS から Cisco TrustSec 環境データをダウンロードします。

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec 環境データを表示する例を示します。

```
switch# show cts environment-data
CTS Environment Data
============================
  Current State           : CTS_ENV_DNLD_ST_INIT_STATE
  Last Status             : CTS_ENV_INCOMPLETE
  Local Device SGT        : 0x0000
  Transport Type          : CTS_ENV_TRANSPORT_DIRECT
  Data loaded from cache  : FALSE
  Env Data Lifetime       :
  Last Update Time        : Never
  Server List             :
     AID: IP: Port:

switch#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts interface

インターフェイスの Cisco TrustSec 情報を表示するには、**show cts interface** コマンドを使用します。

show cts interface {**all** | **ethernet** *slot*/*port* | **vethernet** *veth-num*}

構文の説明

all	すべてのインターフェイスの Cisco TrustSec 情報を表示します。
ethernet *slot*/*port*	特定のイーサネット インターフェイスの Cisco TrustSec 情報を表示します。スロット番号は 1 ～ 255、ポート番号は 1 ～ 48 です。
vethernet *veth-num*	特定の仮想イーサネット（vEthe）インターフェイスの Cisco TrustSec 情報を表示します。仮想イーサネット インターフェイス番号は 1 ～ 1048575 です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

vethernet キーワードを表示するには、**feature-set virtualization** コマンドを使用してスイッチの Cisco 仮想マシン機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、特定のインターフェイスの Cisco TrustSec 設定を表示する例を示します。

```
switch# show cts interface ethernet 1/5
CTS Information for Interface Ethernet1/5:
    CTS is enabled, mode:   CTS_MODE_MANUAL
    IFC state:              Unknown
    Authentication Status:  CTS_AUTHC_INIT
      Peer Identity:
      Peer is:              Unknown in manual mode
      802.1X role:          CTS_ROLE_UNKNOWN
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_INIT
      PEER SGT:             3
      Peer SGT assignment:  Not Trusted
    SAP Status:             CTS_SAP_INIT
      Configured pairwise ciphers:
      Replay protection:
      Replay protection mode:
      Selected cipher:
      Current receive SPI:
      Current transmit SPI:
    Propagate SGT: Enabled
```

```
switch#
```

次に、すべてのインターフェイスの Cisco TrustSec 設定を表示する例を示します。

```
switch# show cts interface all
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
feature-set virtualization	スイッチで Cisco 仮想マシン機能をイネーブルにします。

show cts pacs

EAP-FAST によってプロビジョニングされた Cisco TrustSec Protect Access Credentials（PAC）を表示するには、**show cts pacs** コマンドを使用します。

show cts pacs

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec グローバル設定を表示する例を示します。

```
switch# show cts pacs
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts role-based access-list

グローバル Cisco TrustSec Security Group Access Control List（SGACL）設定を表示するには、**show cts role-based access-list** コマンドを使用します。

show cts role-based access-list [*list-name*]

構文の説明

list-name	（任意）SGACL 名です。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec SGACL 設定を表示する例を示します。

```
switch# show cts role-based access-list
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts role-based counters

ロールベース アクセス コントロール リスト（RBACL）統計情報の設定ステータスを表示し、すべての RBACL ポリシーの統計情報を一覧表示するには、**show cts role-based counters** コマンドを使用します。

show cts role-based counters

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。また **cts role-based counters enable** コマンドを使用して Cisco TrustSec カウンタをイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、RBACL 統計情報の設定ステータスを表示する例を示します。

```
switch# show cts role-based counters

RBACL policy counters enabled
Counters last cleared: Never
rbacl:ACS_1101_15
        permit icmp log                                 [0]
        permit tcp log                                  [0]
        deny udp log                                  [0]

switch#
```

関連コマンド

コマンド	説明
feature cts	スイッチの Cisco TrustSec 機能をイネーブルにします。
clear cts role-based counters	すべてのカウンタが 0 にリセットされるように、RBACL 統計情報をクリアします。
cts role-based counters enable	RBACL 統計情報をイネーブルにします。

show cts role-based enable

VLAN に対する Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）イネーブル ステータスを表示するには、**show cts role-based enable** コマンドを使用します。

show cts role-based enable

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec SGACL 強制ステータスを表示する例を示します。

```
switch# show cts role-based enable
vlan:102
switch#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
cts role-based enforcement	VLAN でのロールベース アクセス コントロール リスト（RBACL）の強制をイネーブルにします。

show cts role-based policy

グローバル Cisco TrustSec Security Group Access Control List（SGACL）ポリシーを表示するには、**show cts role-based policy** コマンドを使用します。

show cts role-based policy

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec SGACL ポリシーを表示する例を示します。

```
switch# show cts role-based policy
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts role-based sgt-map

グローバル Cisco TrustSec Security Group Tag（SGT）マッピング設定を表示するには、**show cts role-based sgt-map** コマンドを使用します。

show cts role-based sgt-map

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec SGT マッピング設定を表示する例を示します。

```
switch# show cts role-based sgt-map
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts sxp

Cisco TrustSec Security Group Tag（SGT）Exchange Protocol（SXP）設定を表示するには、**show cts sxp** コマンドを使用します。

show cts sxp

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec SXP 設定を表示する例を示します。

```
switch# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120
switch#
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts sxp connection

Cisco TrustSec Security Group Tag（SGT）Exchange Protocol（SXP）接続情報を表示するには、**show cts sxp connection** コマンドを使用します。

show cts sxp connection

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、Cisco TrustSec Security Group Tag（SGT）Exchange Protocol（SXP）接続情報を表示する例を示します。

```
switch# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE
192.0.2.1       default         listener        speaker         initializing
switch#
```

関連コマンド

コマンド	説明
cts sxp connection peer	SXP ピア接続を設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。

show running-config cts

実行コンフィギュレーションの Cisco TrustSec 設定を表示するには、**show running-config cts** コマンドを使用します。

show running-config cts

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、実行コンフィギュレーションの Cisco TrustSec 設定を表示する例を示します。

```
switch# show running-config cts

!Command: show running-config cts
!Time: Thu Jan  1 05:33:03 2009

version 6.0(0)N1(1)
feature cts
cts role-based counters enable
cts sxp enable
cts sxp connection peer 192.0.2.1 password none mode listener


interface Ethernet1/5
  cts manual
    policy static sgt 0x3

switch#
```

関連コマンド

コマンド	説明
copy running-config startup-config	実行コンフィギュレーション情報をスタートアップ コンフィギュレーション ファイルにコピーします。
feature cts	Cisco TrustSec 機能をイネーブルにします。

show running-config dot1x

実行コンフィギュレーションの 802.1X 設定情報を表示するには、**show running-config dot1x** コマンドを使用します。

show running-config dotx1 [**all**]

構文の説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

コマンド デフォルト

なし

コマンド モード

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用する前に、**feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、実行コンフィギュレーションの設定済み 802.1X 情報を表示する例を示します。

```
switch# show running-config dot1x
```

関連コマンド

コマンド	説明
copy running-config startup-config	スタートアップ コンフィギュレーション ファイルに実行システム コンフィギュレーション情報をコピーします。
feature cts	スイッチの Cisco TrustSec 機能をイネーブルにします。
feature dot1x	スイッチ上で 802.1X 機能をイネーブルにします。

show startup-config cts

スタートアップ コンフィギュレーションの Cisco TrustSec 設定情報を表示するには、**show startup-config cts** コマンドを使用します。

show startup-config cts

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドには、ライセンスは必要ありません。

例

次に、スタートアップ コンフィギュレーションの Cisco TrustSec 情報を表示する例を示します。

```
switch# show startup-config cts
```

関連コマンド

コマンド	説明
copy running-config startup-config	実行コンフィギュレーション情報をスタートアップ コンフィギュレーション ファイルにコピーします。

show startup-config dot1x

スタートアップ コンフィギュレーションの 802.1X 設定情報を表示するには、**show startup-config dot1x** コマンドを使用します。

show startup-config dot1x

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

任意のコマンド モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

このコマンドを使用する前に、**feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、スタートアップ コンフィギュレーションの 802.1X 情報を表示する例を示します。

```
switch# show startup-config dot1x
```

関連コマンド

コマンド	説明
copy running-config startup-config	実行コンフィギュレーション情報をスタートアップ コンフィギュレーション ファイルにコピーします。