NEC

GVT-018493-001-00 1.16

QX シリーズ Ethernet スイッチ

Web 認証コマンドマニュアル

(V7)

改版履歴

版数	日付	改版内容
1.0	2016/10	初版発行
1.1	2017/05/18	・「本マニュアルについて」の「適用装置」に QX-S5500G シリーズ Ethernet スイッチを追加しました。 ・誤記訂正
1.2	2017/06/26	・「本マニュアルについて」の「適用装置」に QX-S4100G シリーズ Ethernet スイッチを追加しました。 ・誤記訂正
1.3	2017/10/06	・「本マニュアルについて」の「適用装置」に QX-S3400F シリーズ Ethernet スイッチを追加しました。 ・「2 章 PKI」の **display pki certificate** コマンドを 2 つのコマンドに分割しました。 ・「2 章 PKI」の **pki delete-certificate** コマンドの Syntax を変更しました。 ・「2 章 PKI」の **pki retrieval-certificate** コマンド名を **pki retrieve-certificate** に変更し、Syntax を変更しました。 ・「2 章 PKI」の **pki retrieval-crl domain** コマンド名を **pki retrieve-crl domain** に変更し、Syntax を変更しました。 ・「2 章 PKI」の **pki validate-certificate** コマンドの Syntax を変更しました。 ・誤記訂正
1.4	2018/06/07	・「2 章 PKI」に以下のコマンドをサポートしました。 **Attribute**、**certificate request mode**、**certificate request polling**、**display pki certificate access-control-policy**、 **display pki certificate attribute-group**、 **pki abort-certificate-request**、**pki certificate access-control-policy**、**pki certificate attribute-group**、**pki request-certificate**、 **pki storage**、 **public-key dsa**、 **public-key ecdsa**、 **public-key rsa**、 **root-certificate fingerprint** ・誤記訂正
1.5	2018/10/15	・「本マニュアルについて」の「適用装置」に QX-S5300G シリーズ、QX-S5600G シリーズ Ethernet スイッチを追加しました。 ・誤記訂正
1.6	2018/10/25	・「本マニュアルについて」の「適用装置」に QX-S5600G シリーズ Ethernet スイッチを追加しました。
1.7	2018/11/09	・「3 章 SSL」に **certificate-chain-sending enable** コマンドを追加しました。
1.8	2018/11/22	・「3 章 SSL」に QX-S3400F シリーズのサポートを追加しました。 ・誤記訂正

1.9	2019/02/15	・QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I、QX-S4508GT-4G-I をサポートしました。「本マニュアルについて」の「適用装置」に記載を追加しました（QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I は QX-S4100G シリーズに含みます）。 ・「関連マニュアル」に QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチの記載を追加しました。 ・「関連マニュアル」から QX-S3400F シリーズ、QX-S4100G シリーズの記載を削除しました。 ・「2 章 PKI」のメモ誤記訂正（QX-S3400F シリーズの削除） ・**certificate-chain-sending enable** コマンドの QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I、QX-S4508GT-4G-I のサポートバージョンを追加しました。 ・**web-auth max-user** コマンドにメモを追加しました。
1.10	2020/02/13	・QX-S5824XP-2Q2C をサポートしました。
1.11	2020/09/01	・QX-S4300X シリーズをサポートしました。 ・**default-logon-page** コマンドを追加しました。 ・**portal local-web-server** コマンドを追加しました。 ・誤記訂正
1.12	2021/03/16	・QX-S5100G シリーズをサポートしました。 ・誤記訂正
1.13	2021/07/02	・QX-S4800X シリーズをサポートしました。
1.14	2022/05	・「1 章 WebAuth」に **web-auth timer temp-entry-aging** コマンドを追加しました。
1.15	2025/04	・QX-S4200G シリーズをサポートしました。
1.16	2026/11	・QX-S4800X シリーズを適用装置と関連マニュアルに記載しました。 ・certificate-chain-sending enable コマンドのメモに QX-S5500G を追記しました。

Copyright © NEC Corporation 2016-2026

All Rights Reserved

事前に NEC の書面による許可なく、本マニュアルをいかなる形式または方法で複製または配布することを禁止します。

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- 本装置は *QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル(V7)*に記載されている機能の操作のみ使用することができます。*QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル(V7)*に記載されていない機能の操作に使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

適用装置

本マニュアルの適用装置は以下となります。

マニュアル	内容
QX-S3400F シリーズ Ethernet スイッチ	Version 7.2.X を含む以降のソフトウェア
QX-S4100G シリーズ Ethernet スイッチ	Version 7.2.X を含む以降のソフトウェア (QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I は Version7.2.30 を含む以降のソフトウェア)
QX-S4200G シリーズ Ethernet スイッチ	Version 7.1.X を含む以降のソフトウェア
QX-S4300X シリーズ Ethernet スイッチ	Version 7.1.6 を含む以降のソフトウェア
QX-S4508GT-4G-I Ethernet スイッチ	Version 7.2.30 を含む以降のソフトウェア
QX-S4800X シリーズ Ethernet スイッチ	Version 7.3.X を含む以降のソフトウェア
QX-S5100G シリーズ Ethernet スイッチ	Version 7.1.X を含む以降のソフトウェア
QX-S5200G シリーズ Ethernet スイッチ	Version 7.1.12 を含む以降のソフトウェア
QX-S5300G シリーズ Ethernet スイッチ	Version 7.1.X を含む以降のソフトウェア
QX-S5500G シリーズ Ethernet スイッチ	Version 7.2.11 を含む以降のソフトウェア
QX-S5600G シリーズ Ethernet スイッチ	Version 7.1.X を含む以降のソフトウェア
QX-S5800X シリーズ Ethernet スイッチ	Version 7.2.X を含む以降のソフトウェア

関連マニュアル

マニュアル	内容
QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル(V7)	Web 認証の設定について説明しています。
QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル(V7)	Web 認証に関するコマンドについて説明しています。
QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。

マニュアル	内容
QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S3400F/S4100G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-S4200G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S4200G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S4200G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S4200G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-S4300X シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S4300X シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S4300X シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S4800X シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S4800X シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S4800X シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S5100G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5100G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S5100G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-S5200G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5200G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5200G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S5200G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。

マニュアル	内容
QX-S5300G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5300G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5300G シリーズ Series Ethernet Switches Command References	機能に関するコマンドについて説明しています。
QX-S5300G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-S5500G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5500G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5500G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S5600G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5600G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5600G シリーズ Series Ethernet Switches Command References	機能に関するコマンドについて説明しています。
QX-S5800X シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5800X シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5800X シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンドの表記規則

表記規則	説明
太字体	コマンド行のキーワードには**太字体**を使用します。
イタリック体	コマンドの引数には*イタリック体*を使用します。
[]	大カッコに囲まれた項目(キーワードまたは引数)はオプションです。
{x|y|…}	選択する項目は中カッコに入れて、縦線で区切ってあります。1 つを選択します。

表記規則	説明
[x|y|…]	オプションの選択項目は大カッコに入れて、縦線で区切ってあります。１つまたは複数を選択します。
{x|y|…}*	選択する項目は中カッコに入れて、縦線で区切ってあります。少なくとも１つ、多い場合はすべてを選択できます。
[x|y|…]*	オプションの選択項目は大カッコに入れて、縦線で区切ってあります。複数選択することも、何も選択しないこともできます。
#	#で始まる行はコメントです。

II. GUI の表記規則

表記規則	説明
< >	ボタン名は三角カッコに入っています。たとえば、<OK>ボタンをクリックします。
[ ]	ウィンドウ名、メニュー項目、データ表、およびフィールド名は大カッコに入っています。たとえば、[New User]ウィンドウが表示されます。
/	複数レベルのメニューはスラッシュで区切ってあります。たとえば、[File/Create/Folder]。

III. キーボード操作

書式	説明
<キー>	三角カッコ内の名前のキーを押します。たとえば、<Enter>、<Tab>、<Backspace>、<A>となります。
<キー1 + キー2>	複数のキーを同時に押します。たとえば、<Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<キー1、キー2>	複数のキーを順番に押します。たとえば、 <Alt、A>は 2 つのキーを順に押すことを表します。

IV. マウス操作

動作	説明
クリック	左ボタンまたは右ボタンを素早く押します(特に記述がない場合は左ボタン)。
ダブルクリック	左ボタンを素早く 2 回続けて押します。
ドラッグ	左ボタンを押したまま、別の位置まで移動します。

V. 記号

表記規則	説明
⚠ **警告**	表示を無視したり指示に従わない場合、利用者が怪我などをする恐れのある情報を示します。
⚠ **注意**	表示を無視したり指示に従わない場合、データの損失や破損、ハードウェアやソフトウェアの損傷などが発生する恐れのある情報を示します。
⚠ **重要**	表示を無視したり指示に従わない場合、装置が正しく動作しない恐れのある情報を示します。
🕮 **メモ**	追加または補足となる情報を示します。
🕮 **ポイント**	参考となる情報を示します。

VI. 設定例

本マニュアルの設定例の記述は、各機能の設定例です。インタフェース番号、システム名の表記、display コマンドでの情報表示がご使用の装置と異なることがあります。

本マニュアルは以下に示すセクションで構成されています。

01-Web 認証

02-PKI

03-SSL

目次

1 章 Web 認証 1-1
1.1 Web 認証設定コマンド 1-1
1.1.1 default-logon-page 1-1
1.1.2 display web-auth 1-2
1.1.3 display web-auth free-ip 1-3
1.1.4 display web-auth server 1-4
1.1.5 display web-auth user 1-5
1.1.6 ip 1-6
1.1.7 portal local-web-server 1-8
1.1.8 url 1-10
1.1.9 web-auth auth-fail vlan 1-11
1.1.10 web-auth domain 1-12
1.1.11 web-auth enable 1-13
1.1.12 web-auth free-ip 1-13
1.1.13 web-auth max-user 1-14
1.1.14 web-auth offline-detect 1-16
1.1.15 web-auth proxy port 1-17
1.1.16 web-auth server 1-18
1.1.17 web-auth timer temp-entry-aging 1-19

1章 Web 認証

1.1 Web認証設定コマンド

1.1.1 default-logon-page

Syntax

default-logon-page *file-name*

undo default-logon-page

デフォルト

default.zip

View

Local portal Web service view

定義済みユーザロール

network-admin

パラメータ

file-name:デフォルトの認証ページファイルをファイル名(ファイル保管ディレクトリーなし)で指定します。ファイル名は、大文字と小文字が区別される 1 から 91 文字の文字列です。有効な文字は、文字、数字、ドット (。) とアンダースコア (_) です。

説明

default-logon-page コマンドを使用してファイルを指定すると、装置はファイルを解凍して認証ページを取得します。装置は、これらをローカル Web 認証のデフォルト認証ページとして設定します。

ローカル Web サービスを正しく操作するには、Flash のルートディレクトリにあるデフォルトの認証ページファイルを使用してください。カスタム認証ページを使用するには、独自の認証ページをカスタマイズするときに、関連する制限およびガイドラインに従う必要があります。制限およびガイドラインの詳細については QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル(V7)の *1 章 Web 認証の 1.4 認証ページのカスタマイズ*を参照してください。

例

ローカル Web 認証用のデフォルトの認証ページファイルとして、ファイル **pagefile 1.zip** を指定します。

<Switch> system-view

[Switch] portal local-web-server http

[Switch-portal-local-websvr-http] default-logon-page pagefile1.zip

関連コマンド

- **url**
- **tcp-port**

1.1.2 display web-auth

Syntax

display web-auth [**interface** *interface-type interface-number*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースの WebAuth の設定を表示します。

説明

display web-auth コマンドはインタフェースの WebAuth の設定を表示します。

例

GigabitEthernet 1/0/1 の WebAuth の設定を表示します。

<Switch> display web-auth interface gigabitethernet 1/0/1

```
Global Web-auth parameters:
  Proxy Port Numbers        : Not configured
   Online web-auth users: 0
Gigabitethernet 1/0/1 is link-up
   Port role                : Authenticator
   Web-auth domain           : my-domain
   Auth-Fail VLAN            : Not configured
   Offline-detect            : Not configured
   Max online users          : 1024
   Web authentication        : Enabled

   Online web-auth users: 0
```

表 1-1 コマンド出力

フィールド	説明
Interface is link-up	インタフェースの状態です。 • **link-up**—インタフェースが管理上および物理的にアップしています。 • **link-down**—インタフェースがダウンしています。
Offline-detect	Webユーザを検出する間隔です。
Max online users	インタフェースで許可されたWebAuthユーザの最大数です。
Web-auth domain	WebAuthで使用するISPドメインです。
Auth-fail VLAN	WebAuthの制限VLANです。
Web authentication	WebAuthの状態です。 • **Enabled**－有効です。 • **Disabled**－無効です。

関連コマンド

- **web-auth server**
- **web-auth max-user**
- **web-auth free-ip**
- **web-auth auth-fail**
- **web-auth domain**
- **web-auth offline-detect**
- **web-auth enable**

1.1.3 display web-auth free-ip

Syntax

display web-auth free-ip

View

すべての view

定義済みユーザロール

network-admin

説明

display web-auth free-ip コマンドは WebAuth-free サブネットを表示します。

例

WebAuth-free サブネットを表示します。

<Switch> display web-auth free-ip

```
Free IP
                : 1.1.0.0        255.255.0.0
                : 1.2.0.0        255.255.0.0
```

関連コマンド

web-auth free-ip

1.1.4 display web-auth server

Syntax

display web-auth server [*server-name*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

server-name: WebAuth サーバの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。指定しない場合、すべての WebAuth サーバの情報を表示します。

説明

display web-auth server コマンドは WebAuth サーバの情報を表示します。

例

WebAuth サーバ aaa の情報を表示します。

<Switch> display web-auth server aaa

```
Web-auth server: aaa
  IP                 : 8.8.8.8
  Port               : 80
  URL                : http://8.8.8.8/portal/
  URL parameters       : Not configured
```

表 1-2 コマンド出力

フィールド	説明
Web-auth server	WebAuthサーバの名前です。
IP	WebAuthサーバのIPアドレスです。
Port	WebAuthサーバのポート番号です。
URL	WebAuthサーバのリダイレクトを行うURLです。
URL parameters	リダイレクトを行うURLのパラメータです。

🕮 **メモ：**

URL parameters フィールドは現在のソフトウェアバージョンでサポートしていません。

関連コマンド

- **web-auth server**
- **ip**
- **url**

1.1.5 display web-auth user

Syntax

display web-auth user [**interface** *interface-type interface-number* | **slot** *slot-number*]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

interface *interface-type interface-number*: インタフェースのタイプと番号を指定します。指定しない場合、すべてのインタフェースのオンライン WebAuth ユーザの情報を表示します。

slot *slot-number*: IRF スタックメンバ装置の ID を指定します。指定しない場合、すべての IRF スタックメンバ装置のオンライン WebAuth ユーザの情報を表示します。

説明

display web-auth user コマンドはインタフェースのオンライン WebAuth ユーザの情報を表示します。

例

GigabitEthernet 1/0/1 のオンライン WebAuth ユーザの情報を表示します。

<Switch> display web-auth user interface gigabitethernet 1/0/1

```
User Name: user1
  MAC address: a036-9f5c-74b2
  Access interface: GigabitEthernet1/0/1
  Initial VLAN: 1
  Authorization VLAN: N/A
  Authorization ACL ID: N/A
  Authorization user profile: N/A

Total 1 users matched.
```

表 1-3 コマンド出力

フィールド	説明
User Name	オンラインWebAuthユーザの名前です。
MAC address	オンラインWebAuthユーザのMACアドレスです。
Access interface	オンラインWebAuthユーザのアクセスインタフェースです。
Authorization VLAN	オンラインWebAuthユーザの許可VLANのIDです。
Total 1 user matched	オンラインWebAuthユーザの総数です。

1.1.6 ip

Syntax

ip *ipv4-address* **port** *port-number*

undo ip

デフォルト

設定なし

View

Web authentication server view

定義済みユーザロール

network-admin

パラメータ

ipv4-address: WebAuth サーバの IPv4 アドレスを指定します。この IP アドレスはアクセス装置のレイヤ 3 インタフェースの IP アドレスです。WebAuth ユーザと通信可能である必要があります。

port *port-number*: WebAuth サーバのポート番号を指定します。設定範囲は 1～65535 です。

説明

ip コマンドは WebAuth サーバの IP アドレスとポート番号を設定します。

undo ip コマンドはデフォルトに戻します。

WebAuth サーバの IP アドレスとポート番号は **url** コマンドで設定されたリダイレクトを行う URL で使用する IP アドレスとポート番号と同一にする必要があります。また WebAuth サーバのポート番号はローカルポータル Web サーバで使用するポート番号と同一にする必要があります。ローカルポータル Web サーバの設定は QX シリーズ WebAuth オペレーションマニュアルを参照してください。

IP アドレスとしてループバックインタフェースの IP アドレスを設定することを推奨します。

- ループバックインタフェースは常にアップ状態です。インタフェースの障害によって認証ページへのアクセス障害が発生することはありません。
- ループバックインタフェースはパケットの送受信を行いません。多くのネットワークへのアクセス要求があるとき、システムのパフォーマンスに影響することを防ぎます。

複数回設定した場合、最後に入力した設定が適用されます。

例

WebAuth サーバ wbs の view に移行します。

<Switch> system-view

[Switch] web-auth server wbs

WebAuth サーバ wbs の IP アドレス 192.168.1.1、ポート番号 8080 を設定します。

[Switch-web-auth-server-wbs] ip 192.168.1.1 port 8080

関連コマンド

- **url**
- **tcp-port**

1.1.7 portal local-web-server

Syntax

portal local-web-server { **http** | **https ssl-server-policy** *policy-name* [**tcp-port** *port-number*] }

undo portal local-web-server { **http** | **https** }

デフォルト

無効

View

System view

定義済みユーザロール

network-admin

パラメータ

http:HTTP ベースのローカル Web サービスを指定します。HTTP を使用してクライアントと認証情報を交換します。

https:HTTPS ベースのローカル Web サービスを指定します。この Web サービスは、HTTPS を使用してクライアントと認証情報を交換します。

ssl-server-policy *policy-name*:HTTPS の既存の SSL サーバポリシーを指定します。ポリシー名は、1 から 31 文字の大文字と小文字を区別しない文字列です。

tcp-port *port-number*:HTTPS ベースのローカル Web サービスのリスニング TCP ポート番号を指定します。*port-number* 引数の値の範囲は 1~65535 です。デフォルトのポート番号は 443 です。

説明

ローカル Web サービスでは、装置は Web サーバおよび認証サーバとして機能します。

ローカル Web サービスを使用するには、ローカル Web サーバの URL が次の要件を満たしている必要があります。

- URL の IP アドレスは、装置のローカル IP アドレスである必要があります。
- URL は/portal/で終わる必要があります。例:http://1.1.1.1/portal/。

ポリシーが HTTPS に関連付けられている場合、**undo ssl server-policy** コマンドを使用して SSL サーバポリシーを削除することはできません。

HTTPS に新しい SSL サーバポリシーを指定するには、まずこのコマンドの **undo** コマンドを実行して、既存の HTTPS ベースローカル Web サービスを無効にします。

HTTPS ベースのローカル Web サービスのリスニング TCP ポート番号を指定する場合は、次の制限およびガイドラインに従ってください。

- HTTPS ベースのローカル Web サービスおよび HTTPS を使用するその他のサービスの場合:
  - 同じ SSL サーバポリシーを使用する場合は、HTTPS のリスニングポートに同じ TCP ポート番号を使用できます。
  - 異なる SSL サーバポリシーを使用する場合、HTTPS のリスニングポートに同じ TCP ポート番号を使用することはできません。
- HTTPS リスニング TCP ポート番号を、既知のプロトコル(HTTPS を除く)またはその他のサービスで使用されるポート番号として設定しないでください。たとえば、ポート番号 80 と 23 は、それぞれ HTTP と Telnet で使用されるため、指定しないでください。
- HTTP および HTTPS ローカル Web サービスには、同じ TCP ポート番号を構成しないでください。

例

HTTP ベースのローカル Web サービスを有効にして、そのビューに入ります。

<Switch> system-view

[Switch] portal local-web-server http

[Switch-portal-local-websvr-http] quit

HTTPS ベースのローカル Web サービスを使用可能にし、SSL サーバポリシー**policy1** を関連付けます。

<Switch> system-view

[Switch] portal local-web-server https ssl-server-policy policy1

[Switch-portal-local-websvr-https] quit

SSL サーバポリシーを **policy2** に変更します。

[Switch] undo portal local-web-server https

[Switch] portal local-web-server https ssl-server-policy policy2

[Switch-portal-local-websvr-https] quit

HTTPS ベースのローカル Web サービスを有効にします。関連する SSL サーバポリシーは **policy1** で、リスニングポート番号は **442** です。

<Switch> system-view

[Switch] portal local-web-server https ssl-server-policy policy1 tcp-port 442

[Switch-portal-local-websvr-https] quit

関連コマンド

- **default-logon-page**
- **ssl server-policy**

1.1.8 url

Syntax

url *url-string*

undo url

デフォルト

設定なし

View

Web authentication server view

定義済みユーザロール

network-admin

パラメータ

url-string: WebAuth サーバのリダイレクトを行う URL を指定します。設定範囲は 1～256 文字です。大文字、小文字を区別します。

説明

url コマンドは WebAuth サーバのリダイレクトを行う URL を設定します。

undo url コマンドはデフォルトに戻します。

リダイレクトを行う URL は標準 HTTP あるいは HTTPS を使用してアクセスできる URL です。

リダイレクトを行う URL の先頭は “http://” あるいは “https://” にする必要があります。URL で “http://” あるいは “https://” を指定しない場合、システムは文字列の先頭が “http://” であると認識します。

例

WebAuth サーバ wbs の view に移行します。

<Switch> system-view

[Switch] web-auth server wbs

WebAuth サーバ wbs のリダイレクトを行う URL として http://192.168.1.1:80/portal/を指定します。

[Switch-web-auth-server-wbs] url http://192.168.1.1:80/portal/

関連コマンド

- **ip**
- **tcp-port**

1.1.9 web-auth auth-fail vlan

Syntax

web-auth auth-fail vlan *authfail-vlan-id*

undo web-auth auth-fail vlan

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

authfail-vlan-id: 制限 VLAN の ID を指定します。設定範囲は 1～4094 です。あらかじめ VLAN を作成しておく必要があります。

説明

web-auth auth-fail vlan コマンドは WebAuth の制限 VLAN を設定します。

undo web-auth auth-fail vlan コマンドはデフォルトに戻します。

インタフェースで設定したのち、インタフェースで WebAuth に失敗したユーザは制限 VLAN のリソースにアクセスすることができます。WebAuth-free の IP アドレスとして、リソースを供給できるサーバの IP アドレスを設定する必要があります。

制限 VLAN を適用するため、インタフェースで MAC ベース VLAN を有効にし、WebAuth-free サブネットとして制限 VLAN のサブネットを設定する必要があります。

MAC ベース VLAN はハイブリッドポートでのみ有効であるため、制限 VLAN もハイブリッドポートでのみ有効です。

super VLAN として VLAN を指定した場合、インタフェースの制限 VLAN を設定することができません。VLAN をインタフェースの制限 VLAN として指定した場合、super VLAN を設定することができません。

制限 VLAN として設定されている VLAN を削除することはできません。VLAN を削除する場合、最初に **undo web-auth auth-fail vlan** コマンドで制限 VLAN の設定を削除してください。

例

GigabitEthernet 1/0/1 で WebAuth の制限 VLAN を 5 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch–GigabitEthernet1/0/1] port link-type hybrid

[Switch–GigabitEthernet1/0/1] mac-vlan enable

[Switch–GigabitEthernet1/0/1] web-auth auth-fail vlan 5

関連コマンド

display web-auth

1.1.10 web-auth domain

Syntax

web-auth domain *domain-name*

undo web-auth domain

デフォルト

設定なし

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP 認証ドメインの名前を指定します。設定範囲は 1～24 文字です。大文字、小文字を区別しません。

説明

web-auth domain コマンドはインタフェースで WebAuth ユーザの認証ドメインを設定します。

undo web-auth domain コマンドはデフォルトに戻します。

設定したのち、装置はインタフェースで WebAuth ユーザの AAA（認証、許可、アカウンティング）の認証ドメインを使用することができます。

例

GigabitEthernet1/0/1 で WebAuth ユーザの認証ドメイン my-domain を設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch–GigabitEthernet1/0/1] web-auth domain my-domain

1.1.11 web-auth enable

Syntax

web-auth enable apply server *server-name*

undo web-auth enable

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

server-name: WebAuth サーバの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

説明

web-auth enable コマンドはインタフェースで WebAuth を有効にし、WebAuth サーバを指定します。

undo web-auth enable コマンドはインタフェースで WebAuth を無効にします。

WebAuth を正常に動作させるため、インタフェースでポートセキュリティを有効にしないでください。あるいはポートセキュリティのモードを設定しないでください。

例

GigabitEthernet1/0/1 で WebAuth を有効にし、WebAuth サーバ wbs を指定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] web-auth enable apply server wbs

関連コマンド

display web-auth

1.1.12 web-auth free-ip

Syntax

web-auth free-ip *ip-address* { *mask-length* | *mask* }

undo web-auth free-ip { *ip-address* { *mask-length* | *mask* } | **all** }

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

ip-address: WebAuth-free サブネットの IP アドレスを指定します。

mask-length: WebAuth-free サブネットのマスク長を指定します。設定範囲は 0～32 です。

mask: WebAuth-free サブネットのマスクを指定します。ドットで区切り、10 進数で指定します。

all: すべての WebAuth-free サブネットを指定します。

説明

web-auth free-ip コマンドは WebAuth-free サブネットを設定します。

undo web-auth free-ip コマンドはデフォルトに戻します。

WebAuth ユーザは、認証を行うことなく WebAuth-free サブネットのネットワークリソースにアクセスできます。

WebAuth-free サブネットの設定を複数回実行することで、複数の WebAuth-free サブネットを設定することができます。

例

WebAuth-free サブネット 192.168.0.0/24 を設定します。

<Switch> system-view

[Switch] web-auth free-ip 192.168.0.0 24

1.1.13 web-auth max-user

Syntax

web-auth max-user *max-number*

undo web-auth max-user

デフォルト

1024

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

max-number: インタフェースで許可される WebAuth ユーザの最大数を指定します。設定範囲は 1～2048 です。

説明

web-auth max-user コマンドはインタフェースで許可される WebAuth ユーザの最大数を設定します。

undo web-auth max-user コマンドはデフォルトに戻します。

設定する WebAuth ユーザの最大数を、現在のオンライン WebAuth ユーザ数より少ない数に設定した場合、最大数を正常に制限することができます。設定した制限はオンライン WebAuth ユーザに影響しません。しかしオンラインユーザがログアウトし、最大数より少ないユーザ数になるまで、装置はインタフェースから新しい WebAuth ユーザのログインを許可しません。

IPv4 WebAuth ユーザのみ最大数を設定することができます。

例

GigabitEthernet1/0/1 で WebAuth ユーザの最大数を 32 に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] web-auth max-user 32

関連コマンド

display web-auth

🕮 **メモ**:

- QX-S3400F シリーズ/S4100G シリーズ/S4200G シリーズ/S4508GT-4G-I/S5100G シリーズはポート当たり 512、装置当たり 512 まで認証動作が可能です。
- QX-S5200G シリーズはポート当たり 448、装置当たり 448 まで認証動作が可能です。
- QX-S5300G シリーズ/S5500G シリーズ/S5600G シリーズ/S4300X シリーズ/ S4800X シリーズ/S5800X シリーズはポート当たり 512、装置当たり 1024 まで認証動作が可能です。

1.1.14 web-auth offline-detect

Syntax

web-auth offline-detect interval *interval*

undo web-auth offline-detect interval

デフォルト

無効

View

Layer 2 Ethernet interface view

定義済みユーザロール

network-admin

パラメータ

interval: WebAuth ユーザを検出する間隔を指定します。設定範囲は 60～65535 秒です。

説明

web-auth offline-detect コマンドはオンライン WebAuth ユーザの検出を有効にします。

undo web-auth max-user コマンドは WebAuth ユーザの検出を無効にします。

この機能を有効にすることで、装置が定期的に指定した検出間隔でオンラインユーザの MAC アドレスエントリを検出します。

ユーザの MAC アドレスエントリが更新されていない、あるいはエージアウトした場合、ユーザの検出に失敗します。ユーザが 2 回連続で検出に失敗した場合、装置は強制的にユーザをログオフします。

検出間隔は MAC アドレスエントリのエージング時間と同一に設定してください。異なる場合、オンラインユーザはエージアウトした MAC アドレスエントリによってオフラインと認識される可能性があります。

例

GigabitEthernet1/0/1 で WebAuth ユーザの検出を有効にし、検出間隔を 3600 秒に設定します。

<Switch> system-view

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] web-auth offline-detect interval 3600

1.1.15 web-auth proxy port

Syntax

web-auth proxy port *port-number*

undo web-auth proxy port { *port-number* | **all** }

undo web-auth proxy { **all-port** | **port** *port-number* }

undo コマンドは使用する装置によって異なります。

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

all: すべての Web proxy サーバの TCP ポート番号を指定します。

all-port: すべての Web proxy サーバの TCP ポート番号を指定します。

port-number: Web proxy サーバの TCP ポート番号を指定します。設定範囲は 1～65535 です。TCP ポート番号 80 または 443 を指定しないでください。これらの番号は Web 認証に予約されています。

説明

web-auth proxy port コマンドは、Web proxy サーバによって転送された HTTP 要求によって WebAuth を開始できるように Web proxy サーバのポート番号を追加します。

undo web-auth proxy port コマンドは 1 つ、あるいはすべての Web proxy サーバのポート番号を削除します。

デフォルトで、proxy によって転送された HTTP 要求は WebAuth を開始することができず、HTTP 要求を廃棄します。転送された HTTP 要求によって WebAuth を開始するため、装置で Web proxy サーバのポート番号を指定します。

ユーザのブラウザが WPAD（Web Proxy Auto-Discovery）プロトコルを使用している場合、以下の作業を行う必要があります。

- 装置で Web proxy サーバのポート番号を追加します。
- 認証を行うことなく、WPAD サーバの IP アドレス向けのパケットを許可するように WebAuth-free サブネットの設定を行います。
- ユーザは、Web 認証のための Web サーバの IP アドレスをブラウザのプロキシ例外に追加する必要があります。すると、ユーザが Web 認証のために Web サーバに送信する HTTP パケットは Web プロキシサーバに送信されません。

このコマンドを繰り返して、Web 認証のための複数の Web プロキシサーバのポート番号を追加できます。

例

WebAuth のため、Web proxy サーバの TCP ポート番号 7777 を追加します。

<Switch> system-view

[Switch] web-auth proxy port 7777

1.1.16 web-auth server

Syntax

web-auth server *server-name*

undo web-auth server *server-name*

デフォルト

設定なし

View

System view

定義済みユーザロール

network-admin

パラメータ

server-name: WebAuth サーバの名前を指定します。設定範囲は 1～32 文字です。大文字、小文字を区別します。

説明

web-auth server コマンドは WebAuth サーバを作成し、その view に移行します。すでに WebAuth サーバが作成されている場合、その view に移行します。

undo web-auth server コマンドは WebAuth サーバを削除します。

WebAuth サーバの view で以下のパラメータと機能を設定することができます。

- サーバの IP アドレス
- リダイレクトを行う URL

例

WebAuth サーバを作成し、その view に移行します。

<Switch> system-view

[Switch] web-auth server wbs

[Switch-web-auth-server-wbs]

関連コマンド

web-auth enable apply server

1.1.17 web-auth timer temp-entry-aging

🕮 **メモ**:

web-auth timer temp-entry-aging コマンドは、QX-S5100G の Version 7.1.8 を含むそれ以降のバージョンでサポートしています。

Syntax

web-auth timer temp-entry-aging *aging-time-value*

undo web-auth timer temp-entry-aging

デフォルト

60 秒

View

System view

定義済みユーザロール

network-admin

パラメータ

ging-time-value:一時タイマアドレスエントリのエージング MAC を秒単位で指定します。指定できる範囲は 60~2147483647 です。

説明

一時タイマアドレスエントリのエージングタイマを設定するには、**web-auth timer temp-entry-aging** を使用します。

undo web-auth timer temp-entry-aging コマンドでデフォルトに戻ります。

Web 認証を有効にした場合、スイッチはユーザからトラフィックを検出すると、一時的なエントリアドレスを生成します。エントリは、ユーザのアドレス、アクセスインタフェース、VLAN ID、およびエントリのエージングタイムを記録します。

エージングタイマは次のように機能します。

- ユーザがエージングタイマの期限が切れるまでに認証を開始しなかった場合、装置は一時的なエントリを削除します。
- エージングタイマが期限切れになる前にユーザが認証をパスした場合、装置はエージングタイマを削除し、Web 認証ユーザのオンライン情報を記録します。

- ユーザがエージングタイマの期限が切れる前に認証に失敗し、かつ Auth-Fail VLAN が Web 認証用に指定されている場合、装置はユーザの MAC アドレスを Auth-Fail VLAN にバインドし、エージングタイマをリセットします。ユーザがエージングタイマの期限が切れるまでに再度認証に失敗した場合、装置はユーザの一時的なエントリを削除します。

次の場合は、タイマ値を拡大することをお勧めします。

- アクセス権のない Web 認証ユーザは、短時間でトラフィックを送信することがよくあります。その結果、アクセス装置は Web 認証プロセスを継続的に開始し、スイッチの負荷が増加します。
- ユーザが認証に失敗した場合、Auth-Fail VLAN からリソースを取得する時間が十分にないため、例えばウイルスパッチのダウンロードに失敗します。

例

#一時タイマアドレスエントリのエージングタイムを 500 秒に設定します。

<Switch> system-view

[Switch] web-auth timer temp-entry-aging 500

目次

2 章 PKI 2-1
2.1 PKI 設定コマンド 2-1
2.1.1 attribute 2-1
2.1.2 ca identifier 2-2
2.1.3 certificate request entity 2-3
2.1.4 certificate request from 2-4
2.1.5 certificate request mode 2-4
2.1.6 certificate request polling 2-6
2.1.7 certificate request url 2-7
2.1.8 common-name 2-7
2.1.9 country 2-8
2.1.10 crl check enable 2-9
2.1.11 crl url 2-10
2.1.12 display pki certificate access-control-policy 2-10
2.1.13 display pki certificate attribute-group 2-12
2.1.14 display pki certificate domain 2-13
2.1.15 display pki certificate request-status 2-17
2.1.16 display pki crl domain 2-18
2.1.17 fqdn 2-19
2.1.18 ip 2-20
2.1.19 locality 2-21
2.1.20 organization 2-22
2.1.21 organization-unit 2-22
2.1.22 pki abort-certificate-request 2-23
2.1.23 pki certificate access-control-policy 2-24
2.1.24 pki certificate attribute-group 2-25
2.1.25 pki delete-certificate 2-26
2.1.26 pki domain 2-27
2.1.27 pki entity 2-28
2.1.28 pki import 2-28
2.1.29 pki request-certificate 2-31
2.1.30 pki retrieve-certificate 2-33
2.1.31 pki retrieve-crl domain 2-34
2.1.32 pki storage 2-35
2.1.33 pki validate-certificate 2-36
2.1.34 public-key dsa 2-38
2.1.35 public-key ecdsa 2-39
2.1.36 public-key rsa 2-40
2.1.37 root-certificate fingerprint 2-42

2.1.38 state..... 2-43

2章 PKI

🕮 メモ：

PKI は QX-S5500G シリーズではサポートしていません。

2.1 PKI設定コマンド

2.1.1 attribute

Syntax

attribute *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ** } *attribute-value*

undo attribute *id*

View

Certificate attribute group view

定義済みユーザロール

network-admin

パラメータ

id: 1～16 でルール ID を指定します。

alt-subject-name: alternative subject name field(代名のフィールド)を指定します。

fqdn: FQDN 属性を指定します。

ip: IP アドレス属性を指定します。

dn: DN 属性を指定します。

issuer-name: issuer name field(発行人名フィールド)を指定します。

subject-name: subject name field を指定します。

ctn: contain operation を指定します。

equ: equal operation を指定します。

nctn: not-contain operation を指定します。

nequ: not-equal operation を指定します。

attribute-value: 属性値(1～128 文字)を設定します。

説明

attribute に基づいた証明書を、certificate issuer name、subject name、alternative subject name field においてフィルタ規則を設定するために、**attribute** コマンドを使ってください。

例

#証明書属性グループを作成し、その view に入ります。

<Switch> system-view

[Switch] pki certificate attribute-group mygroup

#対象 DN で、”abc”含んでいる証明書とマッチする、属性ルールを設定します。

[Switch-pki-cert-attribute-group-mygroup] attribute 1 subject-name dn ctn abc

issuer name field に FQDN "abc"を含んでいない証明書とマッチする属性ルールを設定します。

[Switch-pki-cert-attribute-group-mygroup] attribute 2 issuer-name fqdn nequ abc

alternative subject name field に IP アドレス"10.0.0.1"を含んでいない証明書とマッチする属性ルールを設定します。

[Switch-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-name ip nequ 10.0.0.1

2.1.2 ca identifier

Syntax

ca identifier *name*

undo ca identifier

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

name： trusted-CA の識別子を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。

説明

Trusted-CA を指定し、CA にデバイスを結合させるには **ca identifier** コマンドを使用してください。

設定を削除するには **undo ca identifier** コマンドを使用してください。

デフォルト：trusted-CA は PKI ドメインに指定されていません。

証明書要求、取得、取り消しおよびクエリのすべては trusted-CA に依存しています。

例

new-ca として trusted-CA を指定します。

<Switch> system-view

[Switch] pki domain 1

[Switch-pki-domain-1] ca identifier new-ca

2.1.3 certificate request entity

Syntax

certificate request entity *entity-name*

undo certificate request entity

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

entity-name：証明書要求のエンティティの名前を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別します。

説明

証明書要求のエンティティを指定するには **certificate request entity** コマンドを使用してください。

設定を削除するには **undo certificate request entity** コマンドを使用してください。

デフォルト：すべてのエンティティは証明書要求に指定されていません。

関連コマンド： **pki entity**

例

証明書要求のエンティティを entity1 として指定します。

<Switch> system-view

[Switch] pki domain 1

[Switch-pki-domain-1] certificate request entity entity1

2.1.4 certificate request from

Syntax

certificate request from { **ca** | **ra** }

undo certificate request from

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

ca： エンティティが CA に証明書を要求することを指定します。

ra： エンティティが RA に証明書を要求することを指定します。

説明

証明書要求の権限を指定するには **certificate request from** コマンドを使用してください。

設定を削除するには **undo certificate request from** コマンドを使用してください。

デフォルト：証明書要求に指定された権限はありません。

例

エンティティが CA に証明書を要求することを指定します。

<Switch> system-view

[Switch] pki domain 1

[Switch-pki-domain-1] certificate request from ca

2.1.5 certificate request mode

Syntax

certificate request mode { **auto** [**password** { **cipher** | **simple** } *string*] | **manual** }

undo certificate request mode

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

auto: オート証明書要求モードを指定します。

password: 証明書取消し用のパスワードを指定します。

cipher: 暗号化された形でパスワードを指定します。

simple: 平文形でパスワードを指定します。セキュリティ向上のために、平文で指定したパスワードは暗号化されます。

string: パスワードを指定します。その平文では 1～31 文字、暗号化では 1～73 文字で設定します。大文字小文字は区別されます

manual: マニュアルの証明書要求モードを指定します。

説明

証明書要求モードを設定するために、**certificate request mode** を使ってください。

undo certificate request mode でデフォルトに戻ります。

証明書要求はオフラインまたはオンラインのモードの中の CA に提出することができます。オンラインモードでは、証明書要求を自動もしくは手動で提出が可能です。

- **オート要求モード**–PKI エンティティは自動的に CA 証明書を取得して、以下の条件の両方が存在しているときに、証明書要求を CA に提出します:
  - 関連したアプリケーション(例：IKE)は identity 認証を実行します。
  - どの証明書も機器のアプリケーションで利用可能ではありません。

  オート要求モードで、CA ポリシによって必要とされている、証明書取消し用のパスワードを指定してください。
- **マニュアル要求モード**–手動で CA 証明書を得て、証明書要求を提出しなければなりません。

デフォルト：マニュアル要求モード

例

証明書要求モードを”auto"に設定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] certificate request mode auto

証明書要求モードをオートにして、証明書取消しパスワードを"123456"に設定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] certificate request mode auto password simple 123456

2.1.6 certificate request polling

Syntax

certificate request polling { **count** *count* | **interval** *interval* }

undo certificate request polling { **count** | **interval** }

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

count *count*:クエリの最大数を 1～100 の範囲で指定します。

interval *interval*:ポーリング間隔(分)を 5～168 範囲で指定します。

説明

certificate request polling で、ポーリング間隔と証明書要求ステータスの最大リトライ数を設定します。

undo certificate request polling でデフォルトに戻ります。

PKI エンティティが証明書要求を提出した後に、CA 管理者が手動で証明書要求を承認しなければならない場合、CA サーバが証明書を出すのに、しばらく時間がかかる可能性があります。この期間の間、PKI エンティティは周期的に CA サーバに要求をします。PKI エンティティが証明書を得るか、証明書要求ステータスの最大リトライ数に達すると、周期的な要求が止まります。証明書要求ステータスの最大リトライ数に達しても承認されなければ、証明書要求は失敗します。

CA サーバが自動的に証明書要求を承認できるならば、証明書要求を提出したすぐ後に、PKI エンティティは証明書を得ることができます。

デフォルト： ポーリング間隔：20 分、証明書要求ステータス最大リトライ数：50

例

ポーリングインターバルを 15 分、証明書要求ステータス最大リトライ数を 40 回に設定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] certificate request polling interval 15

[Switch-pki-domain-aaa] certificate request polling count 40

2.1.7 certificate request url

Syntax

certificate request url *url-string*

undo certificate request url

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

url-string : 証明書を要求するサーバの URL を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

証明書を要求するサーバの URL のフォーマットは、サーバの位置情報と CGI コマンドインタフェースクリプトの位置情報から構成される http://*server_location*/*ca_script_location* です。*server_location* は IP アドレスでなければならず、ドメイン名解決をサポートしていません。

説明

SCEP を用いて証明書を要求するサーバの URL を指定するには **certificate request url** コマンドを使用してください。

設定を削除するには **undo certificate request url** コマンドを使用してください。

デフォルト : PKI ドメインに指定された URL はありません。

例

証明書要求サーバの URL を指定します。

<Switch> system-view

[Switch] pki domain 1

[Switch-pki-domain-1] certificate request url http://169.254.0.100/certsrv/mscep/mscep.dll

2.1.8 common-name

Syntax

common-name *name*

undo common-name

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

name：エンティティの共通名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。コンマは含まれません。

説明

エンティティの共通名を設定するには **common-name** コマンドを使用してください。たとえば、ユーザ名です。

設定を削除するには **undo common-name** コマンドを使用してください。

デフォルト：指定された共通名はありません。

例

#エンティティの共通名を test として設定します。

<Switch> system-view

[Switch] pki entity 1

[Switch-pki-entity-1] common-name test

2.1.9 country

Syntax

country *country-code-str*

undo country

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

country-code-str： エンティティの国コードを指定します。2 文字で指定します。大文字、小文字を区別します。

説明

エンティティに属する国コードを指定するには **country** コマンドを使用してください。国コードはスタンダードな 2 文字のコードです。たとえば日本の場合は JP です。

設定を削除するには **undo country** コマンドを使用してください。

デフォルト：国コードは指定されていません。

例

エンティティの国コードを JP に設定します。

<Switch> system-view

[Switch] pki entity 1

[Switch-pki-entity-1] country JP

2.1.10 crl check enable

Syntax

crl check enable

undo crl check enable

View

PKI domain view

定義済みユーザロール

network-admin

説明

CRL チェックを無効または有効にするためには **crl check** コマンドを使用してください。

デフォルト：CRL チェックは有効です。

CRL は取り消したすべての証明書を公開するために CA によって発行されたファイルです。

証明書の取り消しは証明書失効以前に起こります。CRL チェックは証明書が取り消しされたかどうかをチェックすることを目的としています。

例

CRL チェックを無効にします。

<Switch> system-view

[Switch] pki domain 1

[Switch-pki-domain-1] undo crl check enable

2.1.11 crl url

Syntax

crl url *url-string*

undo crl url

View

PKI domain view

定義済みユーザロール

network-admin

パラメータ

url-string：CRL 配布ポイントの URL を指定します。ldap://*server_location* または http://*server_location* のフォーマットで指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。*server_location* は IP アドレスでなければならず、ドメイン名解決をサポートしません。

説明

CRL 配布ポイントの URL を指定するには **crl url** コマンドを使用してください。

設定を削除するには **undo crl url** コマンドを使用してください。

デフォルト：CRL 配布ポイントの URL は指定されていません。

CRL 配布ポイントの URL が設定されていないときは、CA 証明書とローカル証明書を取得し、SCEP により CRL を取得してください。

例

CRL 配布ポイントの URL を指定します。

<Switch> system-view

[Switch] pki domain 1

[Switch-pki-domain-1] crl url ldap://169.254.0.30

2.1.12 display pki certificate access-control-policy

Syntax

display pki certificate access-control-policy [*policy-name*]

Views

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy-name: ポリシ名を 1～31 文字で指定します。

説明

display pki certificate access-control-policy コマンドで、証明書ベースのアクセス制御ポリシ情報を表示します。

ポリシ名を指定しなければ、すべての証明書ベースのアクセス制御ポリシの情報を表示します。

例

ポリシ名 mypolicy の証明書ベース アクセス制御ポリシ情報を表示します。

<Switch> display pki certificate access-control-policy mypolicy

```
Access control policy name: mypolicy
    Rule 1  deny    mygroup1
    Rule 2  permit  mygroup2
```

すべての証明書ベース アクセス制御ポリシ情報を表示します。

<Switch> display pki certificate access-control-policy

```
Total PKI certificate access control policies: 2
Access control policy name: mypolicy1
    Rule 1  deny    mygroup1
    Rule 2  permit  mygroup2
Access control policy name: mypolicy2
    Rule 1  deny    mygroup3
    Rule 2  permit  mygroup4
```

表2-1 **display pki certificate access-control-policy** の出力情報

フィールド	説明
Total PKI certificate access control policies	証明書ベースのアクセス制御ポリシの総数。
permit	許可しているアクセス制御ルール
deny	制限されているアクセス制御ルール

2.1.13 display pki certificate attribute-group

Syntax

display pki certificate attribute-group [*group-name*]

Views

Any view

定義済みユーザロール

network-admin

network-operator

パラメータ

group-name:証明書属性グループ名を 1～31 文字で指定します。

説明

display pki certificate attribute-group コマンドで、証明書属性グループの情報を表示します。

証明書属性グループ名を指定しないならば、すべての証明書属性グループについての情報を表示します。

例

#証明書属性グループ”mygroup”についての情報を表示します。

<Switch> display pki certificate attribute-group mygroup

```
Attribute group name: mygroup
     Attribute  1 subject-name    dn    ctn   abc
     Attribute  2 issuer-name     fqdn  nctn  app
```

#すべての証明書属性グループ情報を表示します。

<Switch> display pki certificate attribute-group

```
Total PKI certificate attribute groups: 2.
Attribute group name: mygroup1
     Attribute  1 subject-name    dn    ctn   abc
     Attribute  2 issuer-name     fqdn  nctn  app
Attribute group name: mygroup2
     Attribute  1 subject-name    dn    ctn   def
     Attribute  2 issuer-name     fqdn  nctn  fqd
```

表2-2 **display pki certificate attribute-group** の出力情報

フィールド	説明
Total PKI certificate attribute groups	証明書属性グループ数

フィールド	説明
ctn	Contain operation.
nctn	Not-contain operation.
equ	Equal operation.
nequ	Not-equal operation.
Attribute 1 subject-name dn ctn abc	属性ルール: • **alt-subject-name** – Alternative subject name. • **issuer-name** – Certificate issuer name. • **subject-name** – Certificate subject name. • **fqdn**–PKI entity の FQDN. • **ip**–PKI entity の IP アドレス • **dn**–PKI entity の DN • **ctn**–contain operation を示します。 • **equ**–equal operation を示します。 • **nctn**–not-contain operation を示します。 • **nequ**–not-equal operation を示します。

2.1.14 display pki certificate domain

Syntax

display pki certificate domain *domain-name* { **ca** | **local** }

View

すべての view

定義済みユーザロール

network-admin

パラメータ

domain-name： PKI ドメイン名を指定します。設定範囲は 1～15 文字です。ドメイン名は表 2-3 に示す指定記号を設定することができません。

表2-3 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

ca： CA 証明書を表示します。

local： ローカル証明書を表示します。

説明

証明書の内容を表示させるには **display pki certificate** コマンドを使用してください

ca パラメータを指定した場合、ドメインのすべての証明書の内容を表示します。

local パラメータを指定した場合、ドメインのすべてのローカル証明書の内容を表示します。

関連コマンド： **pki retrieval-certificate**、**pki domain**

例

PKI ドメイン aaa の CA 証明書を表示します。

<Switch> display pki certificate local domain aaa ca

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            5c:72:dc:c4:a5:43:cd:f9:32:b9:c1:90:8f:dd:50:f6
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=cn, O=docm, OU=rnd, CN=rootca
        Validity
            Not Before: Jan  6 02:51:41 2011 GMT
            Not After : Dec  7 03:12:05 2013 GMT
        Subject: C=cn, O=ccc, OU=ppp, CN=rootca
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c4:fd:97:2c:51:36:df:4c:ea:e8:c8:70:66:f0:
                    28:98:ec:5a:ee:d7:35:af:86:c4:49:76:6e:dd:40:
                    4a:9e:8d:c0:cb:d9:10:9b:61:eb:0c:e0:22:ce:f6:
```

```
                57:7c:bb:bb:1b:1d:b6:81:ad:90:77:3d:25:21:e6:
                7e:11:0a:d8:1d:3c:8e:a4:17:1e:8c:38:da:97:f6:
                6d:be:09:e3:5f:21:c5:a0:6f:27:4b:e3:fb:9f:cd:
                c1:91:18:ff:16:ee:d8:cf:8c:e3:4c:a3:1b:08:5d:
                84:7e:11:32:5f:1a:f8:35:25:c0:7e:10:bd:aa:0f:
                52:db:7b:cd:5d:2b:66:5a:fb
            Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
        6d:b1:4e:d7:ef:bb:1d:67:53:67:d0:8f:7c:96:1d:2a:03:98:
        3b:48:41:08:a4:8f:a9:c1:98:e3:ac:7d:05:54:7c:34:d5:ee:
        09:5a:11:e3:c8:7a:ab:3b:27:d7:62:a7:bb:bc:7e:12:5e:9e:
        4c:1c:4a:9f:d7:89:ca:20:46:de:c5:b3:ce:36:ca:5e:6e:dc:
        e7:c6:fe:3f:c5:38:dd:d5:a3:36:ad:f4:3d:e6:32:7f:48:df:
        07:f0:a2:32:89:86:72:22:cd:ed:e5:0f:95:df:9c:75:71:e7:
        fe:34:c5:a0:64:1c:f0:5c:e4:8f:d3:00:bd:fa:90:b6:64:d8:
        88:a6
```

PKI ドメイン aaa のローカル証明書を表示します。

<Switch> display pki certificate domain aaa local

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            bc:05:70:1f:0e:da:0d:10:16:1e
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, O=sec, OU=software, CN=abdfdc
        Validity
            Not Before: Jan  7 20:05:44 2011 GMT
            Not After : Jan  7 20:05:44 2012 GMT
        Subject: O=OpenCA Labs, OU=Users, CN=fips fips-sec
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:b2:38:ad:8c:7d:78:38:37:88:ce:cc:97:17:39:
                    52:e1:99:b3:de:73:8b:ad:a8:04:f9:a1:f9:0d:67:
                    d8:95:e2:26:a4:0b:c2:8c:63:32:5d:38:3e:fd:b7:
                    4a:83:69:0e:3e:24:e4:ab:91:6c:56:51:88:93:9e:
                    12:a4:30:ad:ae:72:57:a7:ba:fb:bc:ac:20:8a:21:
                    46:ea:e8:93:55:f3:41:49:e9:9d:cc:ec:76:13:fd:
                    a5:8d:cb:5b:45:08:b7:d1:c5:b5:58:89:47:ce:12:
                    bd:5c:ce:b6:17:2f:e0:fc:c0:3e:b7:c4:99:31:5b:
                    8a:f0:ea:02:fd:2d:44:7a:67
```

```
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Cert Type:
                SSL Client, S/MIME
            X509v3 Key Usage:
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication, E-mail Protection, Microsoft
Smartcardlogin
            Netscape Comment:
                User Certificate of OpenCA Labs
            X509v3 Subject Key Identifier:

91:95:51:DD:BF:4F:55:FA:E4:C4:D0:10:C2:A1:C2:99:AF:A5:CB:30
            X509v3 Authority Key Identifier:

keyid:DF:D2:C9:1A:06:1F:BC:61:54:39:FE:12:C4:22:64:EB:57:3B:11:9F

            X509v3 Subject Alternative Name:
                email:fips@ccc.com
            X509v3 Issuer Alternative Name:
                email:pki@openca.org
            Authority Information Access:
                CA Issuers - URI:http://titan/pki/pub/cacert/cacert.crt
                OCSP - URI:http://titan:2560/
                1.3.6.1.5.5.7.48.12 - URI:http://titan:830/

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://titan/pki/pub/crl/cacrl.crl

    Signature Algorithm: sha256WithRSAEncryption
        94:ef:56:70:48:66:be:8f:9d:bb:77:0f:c9:f4:65:77:e3:bd:
        ea:9a:b8:24:ae:a1:38:2d:f4:ab:e8:0e:93:c2:30:33:c8:ef:
        f5:e9:eb:9d:37:04:6f:99:bd:b2:c0:e9:eb:b1:19:7e:e3:cb:
        95:cd:6c:b8:47:e2:cf:18:8d:99:f4:11:74:b1:1b:86:92:98:
        af:a2:34:f7:1b:15:ee:ea:91:ed:51:17:d0:76:ec:22:4c:56:
        da:d6:d1:3c:f2:43:31:4f:1d:20:c8:c2:c3:4d:e5:92:29:ee:
        43:c6:d7:72:92:e8:13:87:38:9a:9c:cd:54:38:b2:ad:ba:aa:
        f9:a4:68:b5:2a:df:9a:31:2f:42:80:0c:0c:d9:6d:b3:ab:0f:
```

```
dd:a0:2c:c0:aa:16:81:aa:d9:33:ca:01:75:94:92:44:05:1a:
65:41:fa:1e:41:b5:8a:cc:2b:09:6e:67:70:c4:ed:b4:bc:28:
04:50:a6:33:65:6d:49:3c:fc:a8:93:88:53:94:4c:af:23:64:
cb:af:e3:02:d1:b6:59:5f:95:52:6d:00:00:a0:cb:75:cf:b4:
50:c5:50:00:65:f4:7d:69:cc:2d:68:a4:13:5c:ef:75:aa:8f:
3f:ca:fa:eb:4d:d5:5d:27:db:46:c7:f4:7d:3a:b2:fb:a7:c9:
de:18:9d:c1
```

2.1.15 display pki certificate request-status

Syntax

display pki certificate request-status

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

証明書の状態を要求するには **display pki certificate** コマンドを使用してください

関連コマンド: **pki retrieval-certificate**、**pki domain**、**certificate request polling**

例

すべての PKI ドメインの状態を要求します。

<Switch> display pki certificate request-status

```
Certificate Request Transaction 1
   Domain name: domain1
   Status: Pending
   Key usage: General
   Remain polling attempts: 10
   Next polling attempt after : 1191 seconds
Certificate Request Transaction 2
   Domain name: domain2
   Status: Pending
   Key usage: Signature
   Remain polling attempts: 10
   Next polling attempt after : 188 seconds
```

表2-4 **display pki certificate** コマンドのフィールドについて

フィールド	説明
Certificate Request Transaction number	証明書要求の処理番号です。1から開始します。
Status	証明書要求の状態です。接続状態のみが含まれます。
Key usage	証明書の目的です。 • **General**–署名と暗号化です。 • **Signature**–署名のみです。 • **Encryption**–暗号のみです。
Remain polling attempts	証明書要求の状態を要求できる残り回数です。
Next polling attempt after	次の要求状態の確認を行う前の残り時間です。

2.1.16 display pki crl domain

Syntax

display pki crl domain *domain-name*

View

すべての view

定義済みユーザロール

network-admin

パラメータ

domain-name： PKI ドメイン名を指定します。設定範囲は 1～15 文字です。

説明

ローカル的に保存された CRL を表示するには **display pki crl domain** コマンドを使用してください。

関連コマンド： **pki retrieval-crl** 、 **pki domain**

例

ローカル的に保存された CRL を表示します。

<Switch> display pki crl domain 1

```
Certificate Revocation List (CRL):
      Version 2 (0x1)
      Signature Algorithm: sha1WithRSAEncryption
      Issuer:
          C=JP
```

```
    O=abc
    OU=soft
    CN=A Test Root
Last Update: Jan  5 08:44:19 2004 GMT
Next Update: Jan  5 21:42:13 2004 GMT
CRL extensions:
    X509v3 Authority Key Identifier:
    keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
    Revoked Certificates:
    Serial Number: 05a234448E…
    Revocation Date: Sep 6 12:33:22 2004 GMT
    CRL entry extensions:…
    Serial Number: 05a278445E…
    Revocation Date: Sep 7 12:33:22 2004 GMT
    CRL entry extensions:…
```

表2-5 **display pki crl domain** コマンドのフィールドについて

フィールド	説明
Version	CRLのバージョンです。
Signature Algorithm	CRLで使用される署名アルゴリズムです。
Issuer	CRLを発行するCAです。
Last Update	最新のアップデート時間です。
Next Update	次のアップデート時間です。
CRL extensions	CRLの拡張です。
X509v3 Authority Key Identifier	CRLを発行するCAです。証明書バージョンは X.509 v3 です。
keyid	公開鍵IDです。CAは複数の鍵ペアを持っている可能性があります。このフィールドはCRLの署名で使用される鍵ペアを示します。
Revoked Certificates	取り消された証明書です。
Serial Number	取り消された証明書のシリアル番号です。
Revocation Date	証明書を取り消した日時です。

2.1.17 fqdn

Syntax

fqdn *name-str*

undo fqdn

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

name-str：エンティティのドメイン名をすべて省略しない記述形式(FQDN、Fully qualified domain name)を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。

説明

エンティティの FQDN を設定するには **fqdn** コマンドを使用してください。

設定を削除するには **undo fqdn** コマンドを使用してください。

デフォルト：FQDN はエンティティに指定されていません。

FQDN はネットワーク上のエンティティの固有な識別子です。その固有な識別子はホスト名とドメイン名から構成されており、IP アドレスを解決できます。

例

エンティティの FQDN を pki.domain-name.com として設定します。

<Switch> system-view

[Switch] pki entity 1

[Switch-pki-entity-1] fqdn pki.domain-name.com

2.1.18 ip

Syntax

ip *ip-address* { *ip-address* | **interface** *interface-type interface-number* }

undo ip

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

ip-address： エンティティの IP アドレスを指定します。

interface *interface-type interface-number*:インタフェースのタイプと番号を指定します。インタフェースのプライマリ IPv4 アドレスは PKI エンティティの IP アドレスとして使われます。

説明

エンティティの IP アドレスを設定するには **ip** コマンドを使用してください。

設定を削除するには **undo ip** コマンドを使用してください。

デフォルト：IP アドレスはエンティティに指定されていません。

例

エンティティの IP アドレスを 11.0.0.1.として設定します。

<Switch> system-view

[Switch] pki entity 1

[Switch-pki-entity-1] ip 11.0.0.1

2.1.19 locality

Syntax

locality *locality-name*

undo locality

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

locality-name： 所在地を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。コンマは含まれません。

説明

エンティティの所在地を設定するには **locality** コマンドを使用してください。たとえば都市名などです。

設定を削除するには **undo locality** コマンドを使用してください。

デフォルト：所在地はエンティティに指定されていません。

例

エンティティの所在地を city として設定します。

<Switch> system-view

[Switch] pki entity 1

[Switch-pki-entity-1] locality city

2.1.20 organization

Syntax

organization *org-name*

undo organization

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

org-name：組織名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。その文字列にコンマは含まれません。

説明

エンティティが属する組織の名前を設定するには **organization** コマンドを使用してください。

設定を削除するには **undo organization** コマンドを使用してください。

デフォルト：組織名はエンティティに指定されていません。

例

エンティティが属する組織の名前を test-lab として設定します。

<Switch> system-view

[Switch] pki entity 1

[Switch-pki-entity-1] organization test-lab

2.1.21 organization-unit

Syntax

organization-unit *org-unit-name*

undo organization-unit

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

org-unit-name： 異なる組織単位を区別する組織単位名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。その文字列にコンマは含まれません。

説明

このエンティティが属する組織単位名を指定するには **organization-unit** コマンドを使用してください。

設定を削除するには **undo organization-unit** コマンドを使用してください。

デフォルト：組織単位名はエンティティに指定されていません。

例

エンティティが属する組織単位名を group1 として設定します。

<Switch> system-view

[Switch] pki entity 1

[Switch-pki-entity-1] organization-unit group1

2.1.22 pki abort-certificate-request

Syntax

pki abort-certificate-request domain *domain-name*

Views

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を 1～31 文字で指定します。表 2-6 に記載している指定記号は使用できません.

表2-6 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

説明

pki abort-certificate-request コマンドで、PKI ドメインの証明書要求を中止します。

証明書要求を中止し、証明書要求の名前、国コード、または FQDN などのいくつかのパラメータを変更することができます。証明書要求ステータスを表示するには、**display pki certificate request-status** コマンドを使ってください。

例

PKI domain 1 の証明書要求を中止します。

<Switch> system-view

[Switch] pki abort-certificate-request domain 1

```
The certificate request is in process.
Confirm to abort it? [Y/N]:y
```

2.1.23 pki certificate access-control-policy

Syntax

pki certificate access-control-policy *policy-name*

undo pki certificate access-control-policy *policy-name*

Views

System view

定義済みユーザロール

network-admin

パラメータ

policy-name: ポリシ名を 1～31 文字で指定します。

説明

pki certificate access-control-policy コマンド で、証明書ベースのアクセス制御ポリシを作成し、その View に入るか、既存の証明書ベースのアクセス制御ポリシ view に入ります。

undo pki certificate access-control-policy コマンドで証明書ベースのアクセス制御ポリシを削除します。

証明書ベースのアクセス制御ポリシは、属性に基づいて許可もしくは、否定するアクセス制御ポリシを含んでいます。

デフォルト：なし

例

”mypolicy”という名の証明書ベースのアクセス制御ポリシを作成し、その view に入ります。

<Switch> system-view

[Switch] pki certificate access-control-policy mypolicy

[Switch-pki-cert-acp-mypolicy]

2.1.24 pki certificate attribute-group

Syntax

pki certificate attribute-group *group-name*

undo pki certificate attribute-group *group-name*

Views

System view

定義済みユーザロール

network-admin

パラメータ

group-name: グループ名を 1～31 文字で指定します。

説明

pki certificate attribute-group コマンドで、証明書属性グループを作成し、その View に入るか、既存の証明書属性グループの View に入ります。

undo pki certificate attribute-group コマンドで、証明書属性グループを削除します。

証明書属性グループは、**attribute** コマンドを使って設定された属性規則のセットです。各属性規則は発行人名、証明書の対象の名前、または代わりの対象の名前のフィールドにおいて属性を定義します。

証明書属性グループはアクセスコントロールルールと関連しなければなりません（**rule** コマンドを使って設定された許可証または否定ステートメント）。証明書属性グループが属性ルールを持っていないならば、システムは、すべての証明書が関連したアクセス制御ルールとマッチしていると判断します。

デフォルト：なし

例

"mygroup"という名の証明書属性グループを作成し、その View に入ります。

<Switch> system-view

[Switch] pki certificate attribute-group mygroup

[Switch-pki-cert-attribute-group-mygroup]

2.1.25 pki delete-certificate

Syntax

pki delete-certificate domain *domain-name* { **ca** | **local** }

View

System view

定義済みユーザロール

network-admin

パラメータ

ca： ローカルに記録された CA 証明書を削除します。

local： ローカルに記録されたローカル証明書を削除します。

domain-name： 証明書が削除されている PKI ドメインの名前を指定します。設定範囲は 1～15 文字です。ドメイン名は表 2-7 に示す指定記号を設定することができません。

表2-7 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"

名前	記号	名前	記号
コロン	:	アポストロフィー	'

説明

PKI ドメインのためにローカルに記録された証明書を削除するには **pki delete-certificate** コマンドを使用してください。

例

PKI ドメイン cer のローカル証明書を削除します。

<Switch> system-view

[Switch] pki delete-certificate domain cer local

2.1.26 pki domain

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name： PKI ドメイン名を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別します。

説明

PKI ドメインを作成し、PKI domain view へ移行する、または既存の PKI domain view へ移行するには **pki domain** コマンドを使用してください。

PKI ドメインを削除するには **undo pki domain** コマンドを使用してください。

デフォルト：PKI ドメインはありません。

例

PKI ドメインを作成し、その view へ移行します。

<Switch> system-view

[Switch] pki domain 1

[Switch-pki-domain-1]

2.1.27 pki entity

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

entity-name: エンティティ名を指定します。設定範囲は 1～15 文字です。大文字、小文字を区別します。

説明

PKI エンティティを作成し、その view へ移行するには **pki entity** コマンドを使用してください。

PKI エンティティを削除するには **undo pki entity** コマンドを使用してください。

デフォルト：エンティティはありません。

PKI entity view でエンティティの属性の多様性を設定することができます。エンティティは他コマンドによる参照の利便性だけを意図されています。

例

PKI エンティティ名を作成し、その view へ移行します。

<Switch> system-view

[Switch] pki entity en

[Switch-pki-entity-en]

2.1.28 pki import

Syntax

pki import domain *domain-name* { **der** { **ca** | **local** | **peer** } **filename** *filename* | **p12** **local filename** *filename* | **pem** { **ca** | **local** | **peer** } [**filename** *filename*] }

View

System view

定義済みユーザロール

network-admin

パラメータ

ca： CA 証明書を指定します。

local： local 証明書を指定します。

domain-name： PKI ドメイン名を指定します。設定範囲は 1～15 文字です。ドメイン名は表 2-8 に示す指定記号を設定することができません。

表2-8 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

der： DER フォーマットの証明書を指定します。

p12： P12 フォーマットの証明書を指定します。

pem： PEM フォーマットの証明書を指定します。

filename *filename*：しない文字列で表される証明書ファイル名を指定します。設定範囲は 1～127 文字です。大文字、小文字を区別します。デフォルトでは *domain-name*_ca.cer または *domain-name*_local.cer です。このファイルの名前はインポートされた証明書を保存するためにつくられます。

domain *domain-name*: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別しません。ドメイン名は以下の指定記号を含めることができません。チルダ（～）、アスタリスク（*）、バックスラッシュ（¥）、垂直バー（|）、コロン（:）、ドット（.）、左アングルブラケット（<）、右アングルブラケット（>）、ダブルクォーテーション（”）、アポロストフィー（’）

der: PKCS#7 を含んだ DER フォーマットの証明書を指定します。

p12: PKCS12 フォーマットの証明書を指定します。

pem: PEM フォーマットの証明書を指定します。

ca: CA 証明書を指定します。

local: local 証明書を指定します。

peer: ピア証明書を指定します。

filename *filename*:大文字小文字を区別しない証明書ファイル名を指定します。PEM フォーマットの証明書のために、ファイルからインポートせずにターミナルの上に証明書内容を貼りつけることもできます。

説明

CA 証明書またはローカル証明書をファイルからインポートし、ローカルに保存するには **pki import-certificate** コマンドを使用してください。

関連コマンド： **pki domain**

以下の状況で証明書をインポートするために、**pki import** コマンドを使います。

- CRL リポジトリを指定しない CA サーバは、SCEP をサポートしません。
- 証明書がサーバで一杯にした使用は 1 つのファイルの中で重要なペアを生成しました。PKCS12 だけを含む証明書であるか、PEM フォーマットは重要なペアを含むかもしれません。

証明書をインポートする前に、以下を完了させてください。

- 機器のフラッシュメモリに証明書ファイルをアップロードしてください。この場合に、PEM フォーマットの証明書だけがインポートできるので、証明書が PEM フォーマットであることを確かめてください。
- ローカル証明書またはインポートするピア証明書のために、対応する CA 証明書チェーンが存在しなければなりません。CA 証明書チェーンは機器に蓄えられるか、ローカル証明書またはピア証明書に含まれて運ばれることができます。PKI ドメイン、ローカル証明書、またはピア証明書が CA 証明書チェーンを持っていないならば、最初に CA 証明書をインポートする必要があります。

ローカル証明書またはピア証明書をインポートするとき

- ローカル証明書またはインポートされるピア証明書が CA 証明書チェーンを含んでいれば、同時に CA 証明書とローカル証明書またはピア証明書のインポートができます。すでに CA 証明書が PKI ドメインで存在している場合、既存の CA 証明書を上書きするか、システムはプロンプトを表示します。
- ローカルな証明書またはインポートするピア証明書が CA 証明書チェーンを含まないが、すでに CA 証明書が PKI ドメインで存在しているならば、直接ローカル証明書またはピア証明書をインポートできます。

CA 証明書をインポートするとき

- インポートされる CA 証明書が CA ルート証明書であるか、ルート証明書チェーンを含んでいる場合、CA 証明書をインポートができます。
- インポートされる CA 証明書がルート証明書なしで証明書チェーンを含んでいるが、機器の CA 証明書によって完全な証明書チェーンを形成することができる場合は、CA 証明書をインポートすることができます。

以下のシナリオで情報を得るために、CA サーバ管理者に連絡してください。

- インポートする証明書ファイルがルート証明書を含んでいるけれどもルート証明書とフィンガープリントが指定されない。

- インポートするローカル証明書が重要なペアを含んでいるならば、システムは秘密鍵を暗号化するためにチャレンジパスワードの入力を要求します。

重要なペアを含むローカル証明書ファイルをインポートする場合、重要なペアによってドメインをアップデートすることができます。重要なペアの目的に依存して、以下の条件があてはまります。

- 重要なペアの目的が一般的ならば、機器は重要なペアを使います：汎用キーペア、サインキーペア、および暗号化キーペア。
- 重要なペアの目的がサインであるならば、機器は重要なペアを使います：汎用キーペア、サインキーペア。
- 重要なペアの目的が暗号化であるならば、機器はドメインで暗号化キーペアを探します。

マッチが見つかった場合、機器の既存の重要なペアに上書きするかどうかを確認するために、プロンプトを表示します。マッチが見つからないならば、機器は重要なペアの名(デフォルト：PKI ドメインネーム)を入力するように頼みます。そして、証明書ファイルの中で定義された重要なペアのアルゴリズムと目的に従ってそれは重要なペアを生成します。

インポート操作は自動的に正しい重要なペアをアップデートするか、生成します。インポート操作を実行する前に、必ずコンフィギュレーションファイルを保存してください。

例

PEM のフォーマットの CA 証明書を PKI ドメイン cer へインポートします。

<Switch> system-view

[Switch] pki import-certificate ca domain cer pem

2.1.29 pki request-certificate

Syntax

pki request-certificate domain *domain-name* [**password** *password*] [**pkcs10** [**filename** *filename*]]

Views

System view

定義済みユーザロール

network-admin

パラメータ

domain-name: PKI ドメイン名を指定します。設定範囲は 1～31 文字です。ドメイン名は表 2-9 に示す指定記号を設定することができません。

表2-9 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

password *password*: 証明書の取り消しパスワードを、1～31 文字で設定します。パスワードは証明書要求に含まれ、証明書の取り消しをするならば、設定をしてください。

pkcs10: BASE64 でエンコードされた PKCS#10 証明書要求情報を表示します

filename *filename*: PKCS#10 フォーマットの証明書要求を保存する、ローカルファイルを指定します。

説明

pki request-certificate で、ローカル証明書要求の提出もしくは、PKCS#10 フォーマットの証明書要求を行います。

SCEP が失敗する場合は、以下のタスクのいずれかを実行することができます:

- BASE64 でエンコードされた要求情報を表示するために、**pkcs10** キーワードを使用する。
- 要求情報をローカルファイルに保存し、out-of-band を使ってファイルを CA に転送するために、**pkcs10 filename** *filename* オプションを使ってください。ファイル名は絶対パスを含むことができます。指定されたパスが存在しているならば、要求情報は保存されることができません。

このコマンドはコンフィギュレーションに保存されません。

例

証明書要求の情報を PKCS#10 フォーマットで表示させます。

<Switch> system-view

[Switch] pki request-certificate domain aaa pkcs10

```
*** Request for general certificate ***
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
```

```
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nmdcu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END NEW CERTIFICATE REQUEST-----
```

ローカル証明書をリクエストします。

[Switch] pki request-certificate domain openca

```
Start to request general certificate ...
...
Request certificate of domain openca successfully
```

2.1.30 pki retrieve-certificate

Syntax

pki retrieve-certificate domain *domain-name* { **ca** | **local** }

View

System view

定義済みユーザロール

network-admin

パラメータ

ca： CA 証明書を読み出します。

local： ローカル証明書を読み出します。

domain-name： 証明書要求に利用される PKI ドメイン名を指定します。 ドメイン名は表 2-10 に示す指定記号を設定することができません。

表2-10 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

説明

証明書配布サーバから証明書を読み出すには **pki retrieve-certificate** コマンドを使用してください。

オンラインモードでは、以下となります。

- SCEP プロトコルを通して CA 証明書を取得することができます。ローカルですでに CA 証明書がある場合、再度 CA 証明書を取得しません。新しい証明書を取得する場合、**pki delete-certificate** コマンドを使用して、CA 証明書、ローカル証明書を削除します。そして再度 CA 証明書を取得します。
- PKI ドメインですでにローカル証明書がある場合、処理を実行し続けます。ローカル証明書は既存の証明書に上書きします。RSA を使用した場合、PKI ドメインは 2 つのローカル証明書を持つことができます。1 つは署名用で、もう一つは暗号化用です。異なる目的のための証明書は上書きされません。

取得した CA 証明書、ローカル証明書は保存する前に自動で確認されます。確認に失敗した場合、保存されません。

このコマンドは設定ファイルに保存されません。

関連コマンド: **pki domain**

例

証明書発行サーバから CA 証明書を読み出します。（この処理はルート CA 証明局のフィンガープリントを確認することをユーザに要求します。）

<Switch> system-view

[Switch] pki retrieve-certificate domain aaa ca

```
The trusted CA's finger print is:
   MD5  fingerprint:5C41 E657 A0D6 ECB4 6BD6 1823 7473 AABC
   SHA1 fingerprint:1616 E7A5 D89A 2A99 9419 1C12 D696 8228 87BC C266
Is the finger print correct?(Y/N):y
```

証明書発行サーバからローカル証明書を読み出します。

<Switch> system-view

[Switch] pki retrieve-certificate domain aaa local

2.1.31 pki retrieve-crl domain

Syntax

pki retrieve-crl domain *domain-name*

View

System view

定義済みユーザロール

network-admin

パラメータ

domain-name： PKI ドメイン名を指定します。設定範囲は 1～15 文字です。ドメイン名は表 2-10 に示す指定記号を設定することができません。

表2-11 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

説明

CRL 配布サーバから最新の CRL を読み出すには **pki retrieve-crl domain** コマンドを使用してください。

CRL は証明書の有効性を検証します。

関連コマンド： **pki domain**

例

CRL を読み出します。

<Switch> system-view

[Switch] pki retrieve-crl domain 1

2.1.32 pki storage

Syntax

pki storage { **certificates** | **crls** } *dir-path*

undo pki storage { **certificates** | **crls** }

Views

System view

定義済みユーザロール

network-admin

パラメータ

certificates: 証明書を保存するストレージパスを指定します。

crls: CRL を保存するストレージパスを指定します。

dir-path: ストレージパスを指定します。スラッシュ(/)もしくは、2 つのドット+スラッシュ(../)を含むことはできません。dir-path は絶対パスまたは相対パスで指定し、存在しなければなりません。

説明

pki storage コマンドで、証明書または CRL のストレージパスを指定します。

undo pki storage コマンドで、デフォルトに戻ります。

指定されたストレージパスはマスタデバイス上になければなりません。

指定するパスが存在していないならば、最初に **mkdir** コマンドを使ってパスを作成してください。証明書ファイルは.cer または.p12 拡張子を使います。CRL ファイルは.crl ファイル拡張子を使います。

証明書または CRL にストレージパスを変更した後に、証明書ファイルと CRL ファイルは新しいパスに移動します。

デフォルト：証明書と CRL は flash:の PKI ディレクトリに保存します。

例

証明書のストレージパスとして **flash:/pki-new** を指定します。

<Switch> system-view

[Switch] pki storage certificates flash:/pki-new

CRL のストレージパスとして **pki-new** を指定します。

<Switch> system-view

[Switch] pki storage crls pki-new

2.1.33 pki validate-certificate

Syntax

pki validate-certificate domain *domain-name* { **ca** | **local** }

View

System view

定義済みユーザロール

network-admin

パラメータ

ca： CA 証明書を検証します。

local：ローカル証明書を検証します。

domain-name： 検証する証明書が属する PKI ドメイン名を指定します。設定範囲は 1～15 文字です。ドメイン名は表 2-12 に示す指定記号を設定することができません。

表2-12 指定記号

名前	記号	名前	記号
チルダ	~	ドット	.
アスタリスク	*	左アングルブラケット	<
バックスラッシュ	¥	右アングルブラケット	>
垂直バー	|	ダブルクォーテーション	"
コロン	:	アポストロフィー	'

説明

証明書の有効性を検証するには **pki validate-certificate** コマンドを使用してください。

通常、証明書は要求、取得、インポートした場合、あるいは PKI を使用している場合、自動で確認されます。

コマンドを使用して証明書の以下の項目を手動で確認することができます。

- 証明書がトラステッド CA であるかを確認します。
- 証明書の有効期限があるかどうかを確認します。
- 証明書が廃止されたかどうかを確認します。CRL の確認が有効な場合のみ、実行します。

CRL チェックが有効な場合、以下のことを行います。

- ローカル証明書を確認する際、PKI ドメインに CRL がない場合、装置はローカルに保存された CRL を確認します。CRL が正しい場合、PKI ドメインに CRL を読み込みます。CRL が正しくない場合、CA サーバから正しい CRL を取得し、ローカルに保存します。
- CA 証明書を確認する際、CRL チェックは、現在の CA からルート CA までの連続した CA 証明書の確認を行います。

関連コマンド： **pki domain**

例

ローカル証明書の有効性を検証します。

<Switch> system-view

[Switch] pki validate-certificate local domain 1

2.1.34 public-key dsa

Syntax

public-key dsa name *key-name* [**length** *key-length*]

undo public-key

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

name *key-name*:キーペアの名前を 1～64 文字で指定します。キーペアの名はアルファベット, 数字、およびハイフン(-)だけを含むことができます。

length *key-length*:キー長を指定します。値範囲は 512～2048 で、デフォルトは 1024 です。

説明

public-key dsa コマンドで、証明書要求のために DSA キーペアを指定します。

undo public-key コマンドで、デフォルトに戻ります。

このコマンドで存在しないキーペアを指定することができます。キーペアは以下の方法でも得られることができます。:

- **public-key local create** コマンドでキーペアを生成します。
- アプリケーションは、デジタル署名認証を使っている IKE のように、機器を引き起こして、キーペアを生成します。
- **pki import** コマンドでキーペアを含んでいる証明書をインポートします。

PKI ドメインは、DSA、ECDSA、RSA のいずれかの暗号アルゴリズムを使って、キーペアを持ちます。

複数回 PKI ドメインの DSA キーペアを設定するならば、最後に実行したコンフィギュレーションだけが有効です。

存在しないキーペアを指定した場合に、**length** *key-length* オプションが効果します。機器は、証明書要求を提出する前に指定された name と length を使って自動的にキーペアを作成します。指定したキーペアがすでに存在していると **length** *key-length* オプションは無視されるか、インポート済み証明書に含まれています。

デフォルト：なし

例

2048-bit の DSA キーペア abc の証明書要求をします。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] public-key dsa name abc length 2048

2.1.35 public-key ecdsa

Syntax

public-key ecdsa name *key-name* [**secp192r1** | **secp256r1** | **secp384r1** | **secp521r1**]

undo public-key

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

name *key-name*: キーペアの名前を 1～64 文字で指定します。キーペアの名はアルファベット, 数字、およびハイフン(-)だけを含むことができます。

secp192r1:キーペアの生成に、secp192r1 を使います。

secp256r1:キーペアの生成に、secp256r1 を使います。

secp384r1: キーペアの生成に、secp384r1 を使います。

secp521r1:キーペアの生成に、secp521r1 を使います。

説明

public-key ecdsa コマンドで、証明書要求の ECDSA キーペアを指定します。

undo public-key コマンドで、デフォルトに戻ります。

PKI ドメインに存在しないキーペアを指定することができます。

キーペアは以下のどの方法でも得ることができます。:

- **public-key local create** コマンドでキーペアを生成します。
- アプリケーションは、デジタル署名認証を使っている IKE のように、機器を引き起こして、キーペアを生成します。
- **pki import** コマンドでキーペアを含んでいる証明書をインポートします。

PKI ドメインは、DSA、ECDSA、RSA のいずれかの暗号アルゴリズムを使って、キーペアを持ちます。

存在しないキーペアを指定するならば、指定された設定が効果を生じます。機器は、指定された名前を使って自動的にキーペアを作成し、証明書要求を提出する前に変

化させるでしょう。指定された重要なペアがすでに存在しているならば、パラメータは無視されるか、インポート済の証明書にすでに含まれています。

デフォルト：なし

例

#証明書要求に、384bit の ECDSA キーペア"abc"を指定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] public-key ecdsa name abc secp384r1

2.1.36 public-key rsa

Syntax

public-key rsa { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] }

undo public-key

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

encryption:暗号化のためのキーペアを指定します。

name *encryption-key-name*:キーペアの名前を 1～64 文字で指定します。キーペアの名はアルファベット，数字、およびハイフン(-)だけを含むことができます。

signature:サインする、キーペアを指定します。

name *signature-key-name*:キーペアの名前を 1～64 文字で指定します。キーペアの名はアルファベット，数字、およびハイフン(-)だけを含むことができます。

general:サインと暗号化の両方のキーペアを指定します。

name *key-name*: キーペアの名前を 1～64 文字で指定します。キーペアの名はアルファベット，数字、およびハイフン(-)だけを含むことができます。

length *key-length*: キー長を指定します。値範囲は 512～2048 で、デフォルトは 1024 です。

🕮 **メモ：**

- QX-S3400F シリーズ/QX-S4100G シリーズは Ver7.3.37 を含む以降のバージョンで、**length** の範囲が最大 4096 までサポートしています。
- QX-S4508GT-4G-I は、Ver7.3.39 を含む以降のバージョンで、**length** の範囲が最大 4096 までサポートしています。

説明

public-key rsa コマンドで、証明書要求のために RSA キーペアを指定します。

undo public-key コマンドで、デフォルトに戻ります。

このコマンドで存在しないキーペアを指定することができます。キーペアは以下の方法でも得られることができます。:

- **public-key local create** コマンドでキーペアを生成します。
- アプリケーションは、デジタル署名認証を使っている IKE のように、機器を引き起こして、キーペアを生成します。
- **pki import** コマンドでキーペアを含んでいる証明書をインポートします。

PKI ドメインは、DSA、ECDSA、RSA のいずれかの暗号アルゴリズムを使って、キーペアを持ちます。

PKI ドメインは、異なる目的の 2 つの RSA キーペアを持つことができます。:一つはサインキーペアであり、もう一つは暗号化キーペアです。複数回サインキーペアまたは RSA 暗号化キーペア設定するならば、最後のコンフィギュレーションだけが効果します。RSA サインキーペアと暗号化キーペアは互いに上書きしません。

サインキーペアと暗号化キーペアを別々に指定する場合、それらのキー長は違うかもしれません。

存在しないキーペアを指定するならば、「**length** *key-length*」オプションは効果を生じます。機器は、証明書要求を提出する前に指定された名前と長さを使って自動的にキーペアを作成するでしょう。指定されたキーペアがすでに存在しているならば、「**length** *key-length*」オプションは無視されるか、輸入証明書の中にすでに含まれています。

デフォルト：なし

例

証明書要求で 2048bit の汎用 RSA キーペア "abc"を指定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] public-key rsa general name abc length 2048

証明書要求に以下の RSA キーペアを指定します。:

- 2048bit の RSA 暗号化キーペア "rsa1"

- 2048bit の RSA サインキーペア "sig1"

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] public-key rsa encryption name rsa1 length 2048

[Switch-pki-domain-aaa] public-key rsa signature name sig1 length 2048

2.1.37 root-certificate fingerprint

Syntax

root-certificate fingerprint { **md5** | **sha1** } *string*

undo root-certificate fingerprint

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

md5:フィンガープリントを指定します。

sha1:フィンガープリントを指定します。

string: フィンガープリントを 16 進数で指定します。 MD5 を指定した場合は 32 文字、SHA1 指定した場合は、40 文字のフィンガープリントを設定します。

説明

root-certificate fingerprint コマンドで、ルート CA 証明書を確認するフィンガープリントを設定します。

undo root-certificate fingerprint コマンドで、デフォルトに戻ります。

CA 証明書を持っていない PKI ドメインのために、証明書要求モードをオートに設定したならば、ルート CA 証明書立証のためにフィンガープリントを設定しなければなりません。ローカル証明書を要求するために、アプリケーション(例えば IKE)をトリガとして機器は自動的に以下を実行します。:

1) CA 証明書を CA サーバから得ます。
2) ルート CA 証明書の中に含まれているフィンガープリントを、以下の条件のどちらかが存在してれば PKI ドメインで設定されたフィンガープリントと比較します。:
   - 得られた CA 証明書がルート証明書
   - 得られた CA 証明書は証明書チェーンであり、機器の上に存在していないルート証明書を含んでいます。

2 つのフィンガープリントがマッチしていない、または PKI ドメインでフィンガープリントが設定されないならば、機器は CA 証明書を拒絶し、ローカル証明書要求が失敗します。

機器が以下の操作を実行するときに、このコマンドによって設定されたフィンガープリントはルート CA 証明書立証のために使われます。:

- **pki import** コマンドで CA 証明書をインポートします。
- pki retrieve-certificate コマンドで、CA 証明書の取得要求をします。

機器はルート CA 証明書に含まれているフィンガープリントを、以下の条件のどちらかが存在していれば PKI ドメインで設定されたフィンガープリントと比較します。:

- インポート、もしくは得られた CA 証明書は、機器上に存在していないルート証明書
- インポート、もしくは得られた CA 証明書は証明書チェーンであり、機器上に存在していないルート証明書を含んでいます。

2 つのフィンガープリントがマッチしていないならば、機器は CA 証明書を拒絶します。PKI ドメインにフィンガープリントが設定されないならば、機器は、手動でルート CA 証明書のフィンガープリントを確認するように促します。

デフォルト：なし

例

#ルート CA 証明書を確認するために、MD5 フィンガープリントを指定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] root-certificate fingerprint md5 12EF53FA355CD23E12EF53FA355CD23E

#ルート CA 証明書を確認するために、SHA1 フィンガープリントを指定します。

<Switch> system-view

[Switch] pki domain aaa

[Switch-pki-domain-aaa] root-certificate fingerprint sha1 D1526110AAD7527FB093ED7FC037B0B3CDDDAD93

2.1.38 state

Syntax

state *state-name*

undo state

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

state-name： 州または領域の名前を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。コンマは含まれません。

説明

エンティティが属する州または領域の名前を指定するには **state** コマンドを使用してください。

設定を削除するには **undo state** コマンドを使用してください。

デフォルト：なし

例

エンティティが属する州を指定します。

<Switch> system-view

[Switch] pki entity 1

[Switch-pki-entity-1] state country

目次

3 章 SSL 3-1
3.1 SSL 設定コマンド 3-1
3.1.1 certificate-chain-sending enable 3-1
3.1.2 display ssl server-policy 3-2
3.1.3 pki-domain 3-3
3.1.4 ssl server-policy 3-4
3.1.5 ssl version ssl3.0 disable 3-5

3章 SSL

🕮 メモ：

SSL は QX-S5500G シリーズではサポートしていません。

3.1 SSL設定コマンド

3.1.1 certificate-chain-sending enable

🕮 メモ：

- QX-S3400F シリーズ、QX-S4100G シリーズでは Version 7.2.26 を含む以降のソフトウェアからサポートしています（QX-S4108GT-2G-I 、QX-S4108GT-2G-PW-I を除く）。
- QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I、QX-S4508GT-4G-I では Version 7.2.30 を含む以降のソフトウェアからサポートしています。
- QX-S5200G シリーズ、QX-S5300G シリーズ、QX-S5500G シリーズ、QX-S5600G シリーズでは **certificate-chain-sending enable** コマンドをサポートしていません。

Syntax

certificate-chain-sending enable

undo certificate-chain-sending enable

デフォルト

SSL ネゴシエーションの実行中、SSL サーバは、完全な証明書チェーンではなくサーバ証明書をクライアントに送信します。

View

SSL server policy view

定義済みユーザロール

network-admin

mdc-admin

説明

certificate-chain-sending enable コマンドは SSL ネゴシエーションの実行中に SSL サーバが完全な証明書チェーンをクライアントに送信できるようにします。

undo certificate-chain-sending enable コマンドはデフォルトに戻します。

この機能により、SSL ネゴシエーションプロセスで追加の処理が発生します。SSL クライアントがサーバ証明書を確認するための完全な証明書チェーンを持っていない場合のみ、有効にします。

例

SSL サーバが SSL ネゴシエーションの実行中に完全な証明書チェーンをクライアントに送信できるようにします。

<Switch> system-view

[Switch] ssl server-policy policy1

[Switch-ssl-server-policy-policy1] certificate-chain-sending enable

3.1.2 display ssl server-policy

Syntax

display ssl server-policy { *policy-name* | **all** }

View

すべての view

定義済みユーザロール

network-admin

network-operator

パラメータ

policy-name： SSL クライアントポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

all： すべての SSL サーバポリシーについての情報を表示します。

説明

指定された SSL サーバポリシーまたはすべての SSL サーバポリシーについての情報を表示する場合、**display ssl server-policy** コマンドを使用します。

例

SSL サーバポリシーpolicy1 についての情報を表示します。

<Switch> display ssl server-policy policy1

```
SSL server policy: policy1
    PKI domain: server-domain
    Ciphersuites:
       DHE_RSA_AES_128_CBC_SHA
```

```
    RSA_AES_128_CBC_SHA
Session cache size: 600
Caching timeout: 3600 seconds
Client-verify: Enabled
Certificate chain sending: Enabled
```

表3-1 **display ssl server-policy** コマンドのフィールドについて

フィールド	説明
Caching timeout	セッションキャッシュのタイムアウト時間（秒）です。
PKI domain	SSLサーバポリシーで使用されるPKIドメインです。
Client-verify	SSLクライアント認証モードには以下があります。 • **Disabled**–SSL クライアント認証が無効です。 • **Enabled**–SSL クライアント認証が必須です。 • **Optional**–SSL クライアント認証は任意です。
Certificate chain sending	SSLサーバがSSLネゴシエーション中にクライアントへ完全な証明書チェーンを送信するかどうかを有効にするかどうかを示します。

3.1.3 pki-domain

Syntax

pki-domain *domain-name*

undo pki-domain

View

SSL server policy view、 SSL client policy view

定義済みユーザロール

network-admin

パラメータ

domain-name： PKI ドメイン名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

説明

SSL サーバポリシーまたは SSL クライアントポリシーの PKI ドメインを指定するには **pki-domain** コマンドを使用してください。

デフォルトに戻すには **undo pki-domain** コマンドを使用してください。

デフォルト：PKI ドメインは SSL サーバポリシーも SSL クライアントポリシーも設定されていません。

関連コマンド： **display ssl server-policy**

例

PKI ドメイン server-domain を使うために、SSL サーバポリシーpolicy1 を設定します。

<Switch> system-view

[Switch] ssl server-policy policy1

[Switch-ssl-server-policy-policy1] pki-domain server-domain

PKI ドメイン client-domain を使うために、SSL クライアントポリシーpolicy1 を設定します。

<Switch> system-view

[Switch] ssl client-policy policy1

[Switch-ssl-client-policy-policy1] pki-domain client-domain

3.1.4 ssl server-policy

Syntax

ssl server-policy *policy-name*

undo ssl server-policy { *policy-name* | **all** }

View

System view

定義済みユーザロール

network-admin

パラメータ

policy-name： SSL サーバポリシー名を指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。“a”、“al”、または “all”にはできません。

all： すべての SSL サーバポリシーを指定します。

説明

SSL サーバポリシーを作成し、その view へ移行するには **ssl server-policy** コマンドを使用してください。

指定された SSL サーバポリシーまたはすべての SSL サーバポリシーを削除するには **undo ssl server-policy** コマンドを使用してください。

ひとつ以上のアプリケーションレイヤープロトコルに関連付けられた SSL サーバポリシーを削除することはできません。

関連コマンド： **display ssl server-policy**

例

SSL サーバポリシーpolicy1 を作成し、その view へ移行します。

<Switch> system-view

[Switch] ssl server-policy policy1

[Switch-ssl-server-policy-policy1]

3.1.5 ssl version ssl3.0 disable

注意:

SSL Version 3.0 の設定を変更する場合、**ssl version ssl3.0 disable** コマンドあるいは **undo ssl version ssl3.0 disable** コマンドを設定したのち、HTTPS サービスを有効にする必要があります。すでに HTTPS サービスが有効である場合、無効にしたのち、再度有効にしてください。

Syntax

ssl version ssl3.0 disable

undo ssl version ssl3.0 disable

View

System view

定義済みユーザロール

network-admin

パラメータ

なし

説明

ssl version ssl3.0 disable コマンドは装置で SSL 3.0 を無効にします。コマンドはデフォルトに戻します。

デフォルトで装置は SSL 3.0 をサポートします。

例

装置で SSL 3.0 を無効にします。

<Switch> system-view

[Switch] ssl version ssl3.0 disable