NEC

D10-0000021610 1.8 版

QX シリーズ Ethernet スイッチ

Web 認証

コマンドマニュアル

改版履歴

版数	日付	改版内容
1.0	2011/08	・初版発行
1.1	2011/12	・「本マニュアルについて」の「適用装置」、「関連マニュアル」にQX-S4000シリーズEthernetスイッチ(QX-S4009P、QX-S4020P、QX-S4028P、QX-S4028P-PW)を追加
1.2	2012/02	・「本マニュアルについて」の「適用装置」、「関連マニュアル」にQX-S5300シリーズEthernetスイッチを追加 ・誤記訂正 ・「portal max-user」の設定範囲に関するメモ追加
1.3	2012/04	・「本マニュアルについて」の「適用装置」にQX-S4009P-PWに関する記述を追加
1.4	2012/07	・「本マニュアルについて」の「適用装置」にQX-S3800シリーズEthernetスイッチを追加
1.5	2012/12	・「本マニュアルについて」の「適用装置」にQX-S5700シリーズEthernetスイッチを追加
1.6	2015/09/18	・「3章 SSL設定」に **ssl version ssl3.0 disable**コマンドを追加 ・誤記訂正
1.7	2016/02/29	・「3章 SSL設定」の **ssl version ssl3.0 disable**コマンドにQX-S5700シリーズのソフトウェアを追加、SSL Version 3.0の設定を変更する場合に関する注記を追加 ・誤記訂正
1.8	2016/12/27	・「3章 SSL設定」の **ssl version ssl3.0 disable**コマンドにQX-S4000シリーズのソフトウェアを追加しました。 ・誤記訂正

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

- QX シリーズの Web 認証機能は *QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル*に記載されているコマンド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*に記載されていないコマンドを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。

装置	適用バージョン
QX-S5200シリーズEthernetスイッチ	Version 5.3.1を含む以降のソフトウェア
QX-S3300TPシリーズEthernetスイッチ	Version 5.1.5を含む以降のソフトウェア
QX-S4000シリーズEthernetスイッチ	Version 5.3.3を含む以降のソフトウェア (QX-S4009P-PWはVersion5.3.5を含む以降のソフトウェア)
QX-S5300シリーズEthernetスイッチ	Version 5.1.xを含む以降のソフトウェア
QX-S3800シリーズEthernetスイッチ	Version 5.1.xを含む以降のソフトウェア
QX-S5700シリーズEthernetスイッチ	Version 5.1.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	Web認証の設定について記述しています。
QXシリーズ EthernetスイッチWeb認証コマンドマニュアル	Web認証に関するコマンドを使用するときの参考になります。
QX-S5200シリーズ Ethernetスイッチオペレーションマニュアル	QX-S5200シリーズ Ethernetスイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S5200シリーズ Ethernetスイッチコマンドマニュアル	QX-S5200シリーズ Ethernetスイッチのユーザがさまざまなコマンドを使用するときの参考になります。
QX-S3100TP/S3300TPシリーズ Ethernetスイッチオペレーションマニュアル	QX-S3100TP/S3300TPシリーズ Ethernetスイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S3100TP/S3300TPシリーズ Ethernetスイッチコマンドマニュアル	QX-S3100TP/S3300TPシリーズ Ethernetスイッチのユーザがさまざまなコマンドを使用するときの参考になります。
QX-S4000シリーズ Ethernetスイッチオペレーションマニュアル	QX-S4000シリーズ Ethernetスイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S4000シリーズ Ethernetスイッチコマンドマニュアル	QX-S4000シリーズ Ethernetスイッチのユーザがさまざまなコマンドを使用するときの参考になります。

マニュアル	内容
QX-S5300シリーズ Ethernetスイッチオペレーションマニュアル	QX-S5300シリーズ Ethernetスイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S5300シリーズ Ethernetスイッチコマンドマニュアル	QX-S5300シリーズ Ethernetスイッチのユーザがさまざまなコマンドを使用するときの参考になります。
QX-S3800シリーズ Ethernetスイッチオペレーションマニュアル	QX-S3800シリーズ Ethernetスイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S3800シリーズ Ethernetスイッチコマンドマニュアル	QX-S3800シリーズ Ethernetスイッチのユーザがさまざまなコマンドを使用するときの参考になります。
QX-S5700シリーズ Ethernetスイッチオペレーションマニュアル	QX-S5700シリーズ Ethernetスイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S5700シリーズ Ethernetスイッチコマンドマニュアル	QX-S5700シリーズ Ethernetスイッチのユーザがさまざまなコマンドを使用するときの参考になります。

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。
[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

本マニュアルでは、以下のような記号も使用して、操作中に特に注意すべき点を強調しています。意味は次のとおりです。

⚠ 注意、警告、危険：操作中に特に注意すべきことを表します。

🕮 メモ、コメント、ヒント、ノウハウ、アイデア：補助的な説明を表します。

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 3 章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 Web認証設定コマンド

1.1.1 display portal free-rule

Syntax

display portal free-rule [*rule-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

デフォルトレベル

1： Monitor level

パラメータ

rule-number：ポータルフリールールの番号を表示します。 設定範囲は 0～255 です。

|： 表示される情報を正規表現で指定した文字列でフィルタします。

begin： 指定した正規表現の文字列を含む行以降を表示します。

exclude： 指定した正規表現の文字列を含まない行を表示します。

include： 指定した正規表現の文字列を含む行を表示します。

regular-expression： 正規表現を指定します。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

指定されたポータルフリールールまたはすべてのポータルフリールールについての情報を表示するには、**display portal free-rule** コマンドを使用してください。

関連コマンド： **portal free-rule**

例

portal free-rule 1 についての情報を表示します。

<QX> display portal free-rule 1

```
Rule-Number  1:
Source:
  IP       : 2.2.2.0
  Mask     : 255.255.255.0
```

```
  MAC      : 0000-0000-0000
  Interface : any
  Vlan     : 0
Destination:
  IP       : 0.0.0.0
  Mask     : 0.0.0.0
```

表1-1 **display portal free-rule** コマンドのフィールドについて

フィールド	説明
Rule-Number	ポータルフリールールの番号です。
Destination	ポータルフリールールの宛先情報です。
IP	ポータルフリールールの宛先IPアドレスです。
Mask	ポータルフリールールの宛先IPアドレスのサブネットマスクです。

1.1.2 display portal interface

Syntax

display portal interface *interface-type interface-number* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

デフォルトレベル

1： Monitor level

パラメータ

interface-type interface-number：タイプと番号によるインタフェースを示します。

|: 表示される情報を正規表現で指定した文字列でフィルタします。

begin： 指定した正規表現の文字列を含む行以降を表示します。

exclude： 指定した正規表現の文字列を含まない行を表示します。

include： 指定した正規表現の文字列を含む行を表示します。

regular-expression: 正規表現を指定します。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

インタフェースの Web 認証設定を表示するためには、**display portal interface** コマンドを利用してください。

例

GigabitEthernet1/0/1 の Web 認証設定を表示します。

<QX> display portal interface gigabitethernet1/0/1

```
Interface portal configuration:
GigabitEthernet1/0/1: Portal running
Portal server: local-server
Portal backup-group: N/A
Authentication type: Direct
Authentication domain: aaa
Authentication network:
```

表1-2 **display portal interface** コマンドのフィールドについて

フィールド	説明
Interface portal configuration	インタフェース上でのWeb認証設定です。
GigabitEthernet1/0/1	インタフェース上でのWeb認証のステータスです。 • disabled –Web認証が無効です。 • enabled –Web認証が有効ですが機能していません。 • running–Web認証が機能しています。
Authentication domain	インタフェースの認証ドメインです。

1.1.3 display portal local-server

Syntax

display portal local-server [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

デフォルトレベル

1： Monitor level

パラメータ

|： 表示される情報を正規表現で指定した文字列でフィルタします。

begin： 指定した正規表現の文字列を含む行以降を表示します。

exclude： 指定した正規表現の文字列を含まない行を表示します。

include： 指定した正規表現の文字列を含む行を表示します。

regular-expression： 正規表現を指定します。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

display portal local-server コマンドを使用して、ローカルポータルサーバの設定情報を表示します。ローカルポータルサーバの設定情報には、サポートされたプロトコルタイプや、SSL サーバのポリシー情報を含みます。

関連コマンド： **portal local-server**、**portal local-server bind**

例

ローカルポータルサーバの認証情報を表示します。

<QX> display portal local-server

```
Protocol: HTTPS
Server policy: policy1
```

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

フィールド	説明
Protocol	ローカルポータルサーバでサポートされたプロトコルです。HTTPもしくはHTTPSがあります。
Server policy	SSLサーバポリシーはHTTPSサービスに関連づけられています。 HTTPが構成されている場合、このフィールドはnullになります。

1.1.4 display portal user

Syntax

display portal user { **all** | **interface** *interface-type interface-number* } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

デフォルトレベル

1： Monitor level

パラメータ

all： すべてのインタフェースを示します。

interface *interface-type interface-number*：タイプと名前によるインタフェースを示します。

|： 表示される情報を正規表現で指定した文字列でフィルタします。

begin： 指定した正規表現の文字列を含む行以降を表示します。

exclude： 指定した正規表現の文字列を含まない行を表示します。

include： 指定した正規表現の文字列を含む行を表示します。

regular-expression： 正規表現を指定します。設定版には 1～256 文字です。大文字、小文字を区別します。

説明

指定したインタフェースもしくはすべてのインタフェースにポータルユーザの情報を表示するためには、**display portal user** コマンドを使用してください。

例

すべてのインタフェース上のポータルユーザ情報を表示します。

<QX> display portal user all

```
Index：2
State：ONLINE
SubState：INVALID
ACL：NONE
Work-mode：Stand-alone
MAC              IP              Vlan   Interface
------------------------------------------------------------------------
000d-88f8-0eab   2.2.2.2         0      GigabitEthernet1/0/1
Total 1 user(s) matched, 1 listed.
```

表1-4 **display portal user** コマンドのフィールドについて

フィールド	説明
Index	ポータルユーザのインデックスです。
State	ポータルユーザの状態です。
MAC	ポータルユーザのMACアドレスです。
IP	ポータルユーザのIPアドレスです。
Vlan	ポータルユーザが属しているVLANです。
Interface	ポータルユーザが接続されているインタフェースです。
Total 1 user(s) matched, 1 listed	ポータルユーザの総数です。

1.1.5 portal auth-fail vlan

Syntax

portal auth-fail vlan *authfail-vlan-id*

undo portal auth-fail vlan

View

Layer 2 Ethernet interface view

デフォルトレベル

2：System level

パラメータ

authfail-vlan-id： Auth-Fail VLAN ID を指定します。Auth-Fail VLAN が指定されると、Web 認証 Web 認証に失敗したクライアントは Auth-Fail VLAN に加えられます。

説明

Web 認証を設定してあるポートに Auth-Fail VLAN を指定する場合は、**portal auth-fail vlan** コマンドを使用してください。

デフォルト設定に戻すには **undo portal auth-fail vlan** コマンドを使用してください。

デフォルト：ポートの Web 認証に指定されている Auth-Fail VLAN はありません。

🕮 **メモ：**

- 指定された VLAN が存在しなければなりません。
- Auth-Fail VLAN を有効にするには、ポート上で MAC VLAN 機能を有効にする必要があります。
- 別のポート上での Web 認証用に、別の Auth-Fail VLAN を指定することができます。Web 認証の Auth-Fail VLAN だけをポートに指定することができます。

例

Web 認証に失敗したら、VLAN5 にユーザを追加するように、GigabitEthernet1/0/1 上で Web 認証の Auth-Fail VLAN を設定してください。

<QX> system-view

[QX] vlan 5

[QX-vlan5] quit

[QX] interface gigabitethernet 1/0/1

[QX-GigabitEthernet1/0/1] port link-type hybrid

[QX-GigabitEthernet1/0/1] mac-vlan enable

[QX-GigabitEthernet1/0/1] portal auth-fail vlan 5

1.1.6 portal delete-user

Syntax

portal delete-user { *ip-address* | **all** | **interface** *interface-type interface-number* }

View

System view

デフォルトレベル

2： System level

パラメータ

ip-address：指定された IP アドレスを持つユーザをログオフします。

all：すべてのユーザをログオフします。

interface *interface-type interface-number*：指定されたインタフェース上のすべてのユーザをログオフします。

説明

ユーザをログオフするには、**portal delete-user** コマンドを使用してください。

関連コマンド： **display portal user**

例

IP アドレス 1.1.1.1.のユーザをログアウトします。

<QX> system-view

[QX] portal delete-user 1.1.1.1

1.1.7 portal domain

Syntax

portal domain *domain-name*

undo portal domain

View

Layer 2 Ethernet interface view

デフォルトレベル

2： System level

パラメータ

domain-name： Web 認証ドメイン名を指定します。設定範囲は 1～24 文字です。大文字、小文字を区別しません。この引数で指定されたドメインは既に存在する必要があります。

説明

インタフェース上に認証ドメインを指定するには、**portal domain** コマンドを利用してください。それから、デバイスはインタフェース上でポータルユーザの認証、許可およびアカウンティング(AAA)の認証ドメインを利用します。

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

デフォルト：インタフェースに指定されている認証ドメインはありません。

関連コマンド: **display portal interface**

例

GigabitEthernet1/0/1 上でポータルユーザが使用する認証ドメインを my-domain として設定します。

<QX> system-view

[QX] interface gigabitethernet1/0/1

[QX-GigabitEthernet1/0/1] portal domain my-domain

1.1.8 portal free-rule

Syntax

portal free-rule *rule-number* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *netmask* } | **any** } } }

undo portal free-rule { *rule-number* | **all** }

View

System view

デフォルトレベル

2：System level

パラメータ

rule-number: ポータルフリールール番号を指定します。設定範囲は 0～255 です。

any：前キーワードの制限がないことを指定します。

ip *ip-address*： IP アドレスを指定します。

mask { *mask-length* | *netmask* }：IP アドレスマスクを指定します。IP アドレスマスクの設定範囲は 0～32 です。ドット付き 10 進数もしくは整数です。

mac *mac-address*：フォーマット H-H-H での送信元 MAC アドレスを指定します。

all： すべてのポータルフリールールを指定します。

説明

ポータルフリールールの設定や、宛先フィルタリング条件のどちらか一方もしくは両方を指定するには、**portal free-rule** コマンドを使用してください。

指定されたポータルフリールールもしくはすべてのポータルフリールールを削除するには、**undo portal free-rule** コマンドを使用してください。

- 既存のものと同じフィルタリング規則を持つポータルフリールールを設定することはできません。
- Web 認証がインタフェース上で有効かどうかに関係なく、ポータルフリールールを追加、削除を行うことができます。ポータルフリールールの変更はできません。
- Web 認証では、すべての送信元アドレスから、すべてもしくは指定された宛先アドレスまでのポータルフリールールのみ設定することができます。そのようなポータルフリールールが設定されれば、ユーザは Web 認証無しに指定されたアドレスへアクセスすることができます。

関連コマンド： **display portal free-rule**

例

宛先 IP アドレスが 10.10.10.1/24 であるすべてのパケットで Web 認証を不要にするポータルフリールールを設定します。

<QX> system-view

[QX] portal free-rule 15 destination ip 10.10.10.1 mask 24

1.1.9 portal local-server

Syntax

portal local-server { **http** | **https server-policy** *policy-name* }

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

View

System view

デフォルトレベル

2： System level

パラメータ

http: クライアントと認証パケットをやりとりするためにローカルポータルサーバが HTTP を使用するように指定します。

https:クライアントと認証パケットをやりとりするためにローカルポータルサーバが HTTPS を使用するように指定します。

server-policy *policy-name*: HTTPS サーバと関連づけるように SSL サーバポリシーを指定します。設定範囲は 1～16 文字です。大文字、小文字を区別しません。

説明

ローカルポータルサーバによってサポートされるプロトコルタイプを設定し、デフォルト認証ページを読み込むには **portal local-server** コマンドを使用してください。

設定をキャンセルするには **undo portal local-server** コマンドを使用してください。

デフォルト：ローカルポータルサーバは HTTP、HTTPS ともに設定されていません。

- このコマンドを実行するとき、ローカルポータルサーバはデフォルト認証ページファイルを読み込みます。これはデバイスのルートディレクトリに保存されることになっています。ローカルポータルサーバがユーザ定義のデフォルト認証ページを使用することを確認するためには、このコマンドを実行する前に適切に編集と保存を行ってください。さもなければ、システムデフォルト認証ページが使用されます。
- このコマンドで HTTP が指定されたら、HTTP パケットのリダイレクション URL は http:// *デバイスの IP address*/portal/logon.htm のような形式で、クライアントとポータルサーバは HTTP を通じて認証情報をやりとりします。
- このコマンドで HTTPS を指定したら、HTTP パケットのリダイレクション URL は https:// *デバイスの IP address*/portal/logon.htm のような形式で、クライアントとポータルサーバは HTTPS を通じて認証情報をやりとりします。
- ポリシーが HTTPS サービスから参照されている場合、**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。
- デバイスでは、HTTPS サーバで参照しているすべての SSL サーバポリシーは同一にする必要があります。
- オンラインポータルユーザがデバイス上に存在しているならば、認証されたプロトコルタイプの削除、変換および参照された SSL サーバポリシーを変更できません。
- HTTPS サービスによって指定された SSL サーバポリシーを変更するためには、**undo portal local-server https** コマンドを使用して HTTPS 設定をキャンセルしなければなりません。そして目的の SSL サーバポリシーを指定してください。

関連コマンド： **display portal local-server**、**ssl server-policy**

例

HTTP をサポートするためにローカルポータルサーバを設定します。

<QX> system-view

[QX] portal local-server http

HTTPS をサポートし、SSL サーバポリシーpolicy1 を参照するためにローカルポータルサーバを設定します。policy1 は既に設定されているものとします。

[QX] portal local-server https server-policy policy1

参照された SSL サーバポリシーを policy2 に変更します。

[QX] undo portal local-server https

[QX] portal local-server https server-policy policy2

1.1.10 portal local-server enable

Syntax

portal local-server enable

undo portal

View

Layer 2 Ethernet interface view

デフォルトレベル

2： System level

パラメータ

なし

説明

カレントポートで Web 認証を有効にするには、**portal local-server enable** コマンドを使用してください。

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

デフォルト：Web 認証はレイヤ 2 ポート上で無効

- Web 認証における一般的な操作では、ポートセキュリティおよび 802.1X のゲスト VLAN を無効にすることを推奨します。ポートセキュリティと 802.1X 機能についての情報は各装置のマニュアルを参照してください。
- レイヤ 2 ポートの Web 認証を有効にする前に、ローカルポータルサーバのリスニング IP アドレスを指定することを確認してください。

関連コマンド： **portal local-server ip**

例

GigabitEthernet 1/0/1 の Web 認証を有効にします。

<QX> system-view

[QX] interface gigabitethernet 1/0/1

[QX-GigabitEthernet1/0/1] portal local-server enable

1.1.11 portal local-server ip

Syntax

portal local-server ip *ip-address*

undo portal local-server ip

View

System view

デフォルトレベル

2： System level

パラメータ

ip-address： ローカルポータルサーバのリスニング IP アドレスを指定します。この IP アドレスはアクセスデバイス上のレイヤ 3 インタフェースであり、ポータルクライアントからルーティングします。

説明

Web 認証のためのローカルポータルサーバのリスニング IP アドレスを指定するには、**portal local-server ip** コマンドを使用してください。

リスニング IP アドレスを指定する際、デバイスはポータルクライアントからリスニング IP アドレスの認証ページまで Web リクエストをリダイレクトします。

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

デフォルト：ローカルポータルサーバに指定されたリスニング IP アドレスはありません。

以下の理由により、リスニング IP アドレスとしてループバック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の状態は安定しています。よってインタフェースの障害に起因する認証ページのアクセス障害を回避することができます。

- ループバックインタフェースは受信したパケットを転送しません。よって多くのネットワーク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を与えることを避けることができます。

例

Web 認証のローカルポータルサーバのリスニング IP アドレスとして 1.1.1.1 を指定します。

<QX> system-view

[QX] interface loopback 1

[QX-LoopBack1] ip address 1.1.1.1 32

[QX-LoopBack1] quit

[QX] portal local-server ip 1.1.1.1

1.1.12 portal max-user

Syntax

portal max-user *max-number*

undo portal max-user

View

System view

デフォルトレベル

2： System level

パラメータ

max-number：システムで許可されたオンラインポータルユーザの最大数を指定します。

🕮 **メモ：**

max-number の設定範囲は装置によって異なります。

- QX-S5200 シリーズ、QX-S5300 シリーズ：1～1000 です。
- QX-S3800 シリーズ：1～1024 です。
- QX-S3300TP シリーズ、QX-S4000 シリーズ：1～512 です。
- QX-S5700 シリーズ：1～3000 です。

説明

システムで許可されたオンラインポータルユーザの最大数を設定するには、**portal max-user** コマンドを使用してください。

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

デフォルト：各装置の設定可能最大数

コマンドで指定されたポータルユーザの最大数が最新のオンラインポータルユーザ数よりも少なくても、コマンドは正常に実行することができ、オンラインポータルユーザに影響を与えません。しかし、システムはオンラインポータルユーザ数が最大数未満になるまで、新しいポータルユーザのログインを許可しません。

例

システムでポータルユーザ数の最大値として 100 を設定します。

<QX> system-view

[QX] portal max-user 100

1.1.13 portal move-mode auto

Syntax

portal move-mode auto

undo portal move-mode

View

System view

デフォルトレベル

2： System level

パラメータ

なし

説明

移動ポータルユーザ機能を有効にするためには **portal move-mode auto** コマンドを使用してください。また、認証されたユーザがデバイスのポートからログオフをせずに移動した場合、ユーザは次の状態を満たしていればネットワークに(再認証無しで)接続し続けることができます。

- 新しいポートがアップされています。
- 移動前のポートと新しいポートが同じ VLAN に属しています。
- ユーザの認証情報がどのような場合でも新しいポートに割り当てられています。

- 新しいポートに MAC 認証が設定されていません。

すべての状態が満たされていなければ、新しいポートではユーザは再認証が必要となります。

移動ポータルユーザ機能を無効にするためには、 **undo portal move-mode** コマンドを使用してください。

デフォルト：移動ポータルユーザ機能は無効。認証ユーザがあるポートから他のポートへログオフせずに移動した場合、移動前のポートがまだ接続しているときはオンラインに繋ぐことができません。なぜなら、移動前のポートはユーザの認証情報をまだ保持しているからです。

- ユーザがあるポートから他のポートへ移動した後に移動前のポートがダウンした場合、ユーザの認証情報は失われ、ユーザは再認証しなければなりません。
- ポータルユーザ移動のサポートは、ユーザとアクセスデバイスの間にハブ、レイヤ 2 スイッチおよび AP が存在するといった場合に適用してください。

例

#移動ポータルユーザ機能を有効にします。

<QX> system-view

[QX] portal move-mode auto

1.1.14 portal offline-detect interval

Syntax

portal offline-detect interval *offline-detect-interval*

undo portal offline-detect interval

View

Layer 2 Ethernet interface view

デフォルトレベル

2： System level

パラメータ

offline-detect-value：オンラインポータルユーザ検出間隔です。設定範囲は 60～65535 です。

説明

ポータルユーザ検出間隔を設定するためには **portal offline-detect interval** コマンドを使用してください。ポータルユーザがオンラインになった後からユーザの検出タイマーを開始し、ユーザがその指定した間隔でデバイスにパケットを送信して

いるかどうかを確認します。デバイスが 2 回の検出間隔の間でユーザからパケットを何も受信しなかった、もしくはユーザの MAC アドレスがエージアウトしていたことを発見した場合、デバイスはユーザがオフラインになりユーザ認証情報を消去したものとみなします。

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

デフォルト：オンラインポータルユーザ検出間隔は 300 秒です。

この検出間隔は MAC アドレスのエージングタイムより等しいかまたは短くない場合は、ポータルユーザは MAC アドレスのエージアウトが原因でオフラインとみなされます。

例

オンラインポータルユーザ検出間隔を GigabitEthernet 1/0/1 ポートへ 3600 秒と設定します。

<QX> system-view

[QX] interface gigabitethernet 1/0/1

[QX-GigabitEthernet1/0/1] portal offline-detect interval 3600

1.1.15 portal redirect-url

Syntax

portal redirect-url *url-string* [**wait-time** *period*]

undo portal redirect-url

View

System view

デフォルトレベル

2： System level

パラメータ

url-string：認証ポータルユーザの自動リダイレクト URL です。設定範囲は 1～127 文字です。http:// もしくは https:// で表されなければならず、十分に限定された URL でなければなりません。

period： デバイスが自動リダイレクト URL へ Web 認証をリダイレクトするまでの時間です設定範囲は 1～90 秒です。デフォルトは 5 秒です。

説明

認証ポータルユーザの自動リダイレクト URL を指定するためには **portal redirect-url** コマンドを使用してください。

設定をデフォルトに戻すには **undo portal redirect-url** コマンドを使用してください。

デフォルト：認証されたユーザは、リダイレクト先の指定がされていない場合、認証が行われる前に、アドレスバーで入力された URL にリダイレクトされます。ただし、認証が行われる前にアドレスバーで入力した URL が 255 文字以上の場合、ユーザが認証にパスした後の URL ページへのリダイレクトができません。

ポータルユーザが Web 認証承認後に VLAN を割り当てられると、ユーザはオンライン接続後に IP アドレスをアップデートしなければならないことがあります。この場合、リダイレクト待ち時間はユーザ IP アドレスのアップデート時間より長くなければなりません。リダイレクト待ち時間がユーザ IP アドレスのアップデート時間より短い場合、目的の IP アドレスアップデートが完了していないため、ユーザは URL を開くことができないことがあります。

例

ユーザの Web 認証承認後、ポータルユーザが http://www.testpt.jp へ 3 秒後にリダイレクトされるようにデバイスの設定をします。

<QX> system-view

[QX] portal redirect-url http://www.testpt.jp wait-time 3

1.1.16 portal server banner

Syntax

portal server banner *banner-string*

undo portal server banner

View

System view

デフォルトレベル

2： System level

パラメータ

banner-string：Web ページのウェルカムバナーです。設定範囲は 1～50 文字です。大文字、小文字を区別します。未満記号(<)もしくはアンド記号(&)を含めることはできません。連続する複数のスペースが文字列に存在する場合、ブラウザはそのスペースを一文字分として認識します。

説明

ローカルポータルサーバによってデフォルト Web ページのウェルカムバナーを表示させるには **portal server banner** コマンドを使用してください。

デフォルトに戻すためには **undo portal server banner** コマンドを使用してください。

デフォルト：Web ページウェルカムバナーは表示されていません。

設定されたウェルカムバナーは、カスタマイズされた認証ページではなく、デフォルト認証ページでのみ適用されています。

例

#ローカルポータルサーバで表示されるデフォルト Web ページのウェルカムバナーを Welcome to Portal Authentication として設定します。

<QX> system-view

[QX] portal server banner Welcome to Portal Authentication

1.1.17 portal web-proxy port

Syntax

portal web-proxy port *port-number*

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

View

System view

デフォルトレベル

2： System level

パラメータ

port-number： Web プロキシサーバポート番号です。設定範囲は 1～65535 です。

all： すべての web プロキシサーバポート番号を指定します。

説明

HTTP リクエストの宛先である Web 認証のトリガとなるポート番号に web プロキシサーバのポート番号を追加する場合に **portal web-proxy port** コマンドを使用してください。

一つもしくはすべてのプロキシサーバポート番号を削除するためには **undo portal web-proxy port** コマンドを使用してください。

デフォルト：プロキシサーバポート番号は設定されておらず、デバイスはポート 80 の HTTP リクエストのみリダイレクトします。

- 最大 4 つの web プロキシサーバポート番号を追加することができます。
- web プロキシサーバポート番号が 80 であったら、デバイス上のサーバのポート番号を設定する必要はありません。
- ユーザのブラウザが web プロキシサーバを探すために Web Proxy Auto-Discovery (WPAD)プロトコルを使用した場合、デバイス上の web プロキシサーバのポート番号を追加する必要があります。そして WPAD サーバの IP アドレス行きユーザパケットが認証無しで承認されるように、ポータルフリールールを設定してください。
- Web 認証では、デバイス上の web プロキシサーバのポート番号を追加する必要があり、ユーザは web プロキシを使用しているブラウザがローカルポータルサーバの IP アドレスをリスニングするためのプロキシサーバを使用しない、ということを保証する必要があります。したがって、ポータルユーザがローカルポータルサーバへ送信する HTTP パケットは web プロキシサーバへ送信しません。

例

ポート番号 8080 の web プロキシサーバを使用しているユーザが Web 認証ページへリダイレクトできるように、デバイスに web プロキシサーバポート番号 8080 を追加します。

<QX> system-view

[QX] portal web-proxy port 8080

目次

2章 PKI

2.1 PKI設定コマンド

2.1.1 ca identifier

Syntax

ca identifier *name*

undo ca identifier

View

PKI domain view

デフォルトレベル

2: System level

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ーのすべては trusted-CA に依存しています。

例

new-ca として trusted-CA を指定します。

<QX> system-view

[QX] pki domain 1

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

2.1.2 certificate request entity

Syntax

certificate request entity *entity-name*

undo certificate request entity

View

PKI domain view

デフォルトレベル

2: System level

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。

<QX> system-view

[QX] pki domain 1

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

2.1.3 certificate request from

Syntax

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

undo certificate request from

View

PKI domain view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki domain 1

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

2.1.4 certificate request url

Syntax

certificate request url *url-string*

undo certificate request url

View

PKI domain view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki domain 1

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

2.1.5 common-name

Syntax

common-name *name*

undo common-name

View

PKI entity view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki entity 1

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

2.1.6 country

Syntax

country *country-code-str*

undo country

View

PKI entity view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki entity 1

[QX-pki-entity-1] country JP

2.1.7 crl check

Syntax

crl check { **disable** | **enable** }

View

PKI domain view

デフォルトレベル

2： System level

パラメータ

disable： CRL チェックを無効にします。

enable： CRL チェックを有効にします。

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。

<QX> system-view

[QX] pki domain 1

[QX-pki-domain-1] crl check disable

2.1.8 crl update-period

Syntax

crl update-period *hours*

undo crl update-period

View

PKI domain view

デフォルトレベル

2： System level

パラメータ

hours： CRL の時間単位によるアップデート期間を指定します設定範囲は 1～720 です。

説明

CRL アップデート期間を設定するには **crl update-period** コマンドを使用してください。つまり、証明書付き PKI エンティティが LDAP サーバから最新の CRL をダウンロードする間隔です。

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

デフォルト：CRL アップデート期間は CRL ファイルの次のアップデートフィールドに依存します。

例

CRL アップデート期間を 20 時間に設定します。

<QX> system-view

[QX] pki domain 1

[QX-pki-domain-1] crl update-period 20

2.1.9 crl url

Syntax

crl url *url-string*

undo crl url

View

PKI domain view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki domain 1

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

2.1.10 display pki certificate

Syntax

display pki certificate { { **ca** | **local** } **domain** *domain-name* | **request-status** } [| { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

デフォルトレベル

2： System level

パラメータ

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。

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。

request-status： 証明書要求の状態を表示します。

|： 表示される情報を正規表現で指定した文字列でフィルタします。

begin： 指定した正規表現の文字列を含む行以降を表示します。

exclude： 指定した正規表現の文字列を含まない行を表示します。

include： 指定した正規表現の文字列を含む行を表示します。

regular-expression： 正規表現を指定します。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

証明書の内容を表示させるまたは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

ローカル証明書を表示します。

<QX> display pki certificate local domain 1

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            10B7D4E3 00010000 0086
        Signature Algorithm: md5WithRSAEncryption
        Issuer:
            emailAddress=myca@aabbcc.net
            C=JP
            ST=Country A
            L=City X
            O=abc
            OU=bjs
            CN=new-ca
        Validity
            Not Before: Jan 13 08:57:21 2004 GMT
            Not After : Jan 20 09:07:21 2005 GMT
        Subject:
            C=JP
            ST=Country B
            L=City Y
            CN=pki test
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00D41D1F …
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
            DNS: hyf.xxyyzz.net
            X509v3 CRL Distribution Points:
            URI:http://1.1.1.1:447/myca.crl
            …          …
    Signature Algorithm: md5WithRSAEncryption
        A3A5A447 4D08387D …
```

表2-1 **display pki certificate** コマンドのフィールドについて

フィールド	説明
Version	証明書のバージョンです。
Serial Number	証明書のシリアル番号です。

フィールド	説明
Signature Algorithm	署名アルゴリズムです。
Issuer	証明書発行人です。
Validity	証明書有効期間です。
Subject	証明書申請者のエンティティ名です。
Subject Public Key Info	エンティティの公開鍵情報です。
X509v3 extensions	X.509 (version 3)証明書の拡張機能です。
X509v3 CRL Distribution Points	X.509 (version 3) CRLの配布ポイントです。

2.1.11 display pki crl domain

Syntax

display pki crl domain *domain-name* [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

デフォルトレベル

2： System level

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。

|： 表示される情報を正規表現で指定した文字列でフィルタします。

begin： 指定した正規表現の文字列を含む行以降を表示します。

exclude： 指定した正規表現の文字列を含まない行を表示します。

include： 指定した正規表現の文字列を含む行を表示します。

regular-expression： 正規表現を指定します。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

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。

<QX> 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2-2 **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。

2.1.12 fqdn

Syntax

fqdn *name-str*

undo fqdn

View

PKI entity view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki entity 1

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

2.1.13 ip (PKI entity view)

Syntax

ip *ip-address*

undo ip

View

PKI entity view

デフォルトレベル

2： System level

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。

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。

<QX> system-view

[QX] pki entity 1

[QX-pki-entity-1] ip 11.0.0.1

2.1.14 locality

Syntax

locality *locality-name*

undo locality

View

PKI entity view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki entity 1

[QX-pki-entity-1] locality city

2.1.15 organization

Syntax

organization *org-name*

undo organization

View

PKI entity view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki entity 1

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

2.1.16 organization-unit

Syntax

organization-unit *org-unit-name*

undo organization-unit

View

PKI entity view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki entity 1

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

2.1.17 pki delete-certificate

Syntax

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

View

System view

デフォルトレベル

2： System level

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。

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。

<QX> system-view

[QX] pki delete-certificate local domain cer

2.1.18 pki domain

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

View

System view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki domain 1

[QX-pki-domain-1]

2.1.19 pki entity

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

View

System view

デフォルトレベル

2： System level

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。

<QX> system-view

[QX] pki entity en

[QX-pki-entity-en]

2.1.20 pki import-certificate

Syntax

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

View

System view

デフォルトレベル

2: System level

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。

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。

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**

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。

<QX> system-view

[QX] pki import-certificate ca domain cer pem

2.1.21 pki request-certificate domain

Syntax

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

View

System view

デフォルトレベル

2： System level

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。

password：証明書を取り消すパスワードを指定します。設定範囲は 1～31 文字です。大文字、小文字を区別します。

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 証明書要求を保存しているローカル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。

説明

SCEP を用いて CA からローカル証明書を要求するには **pki request-certificate** ドメインを使用してください。SCEP ができない場合、BASE64 フォーマットのローカル証明書要求を記録し、そのローカル証明書要求を電話、ディスク、e-mail のような方法によって CA に送るために pkcs10 キーワードを使用できます。

この操作はコンフィグファイルに保存されません。

関連コマンド： **pki domain**

例

PKCS#10 証明書要求情報を表示します。

<QX> system-view

[QX] pki request-certificate domain 1 pkcs10

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBTDCBtgIBADANMQswCQYDVQQDEwJqajCBnzANBgkqhkiG9w0BAQEFAAOBjQAw
gYkCgYEAw5Drj8ofs9THA4ezkDcQPBy8pvH1kumampPsJmx8sGG52NFtbrDTnTT5
ALx3LJijB3d/ndKpcHT/DfbJVDCn5gdw32tBZyCkEwMHZN3ol2z7Nvdu5TED6iN8
4m+hfp1QWoV6lty3o9pxAXuQl8peUDcfN6WV3LBXYyl1WCtkLkECAwEAAaAAMA0G
CSqGSIb3DQEBBAUAA4GBAA8E7BaIdmT6NVCZgv/I/1tqZH3TS4e4H9Qo5NiCKiEw
R8owVmA0XVtGMbyqBNcDTG0f5NbHrXZQT5+MbFJOnm5K/mn1ro5TJKMTKV46PlCZ
JUjsugaY02GBY0BVcylpC9iIXLuXNIqjh1MBIqVsa1lQOHS7YMvnop6hXAQlkM4c
-----END CERTIFICATE REQUEST-----
```

2.1.22 pki retrieval-certificate

Syntax

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

View

System view

デフォルトレベル

2： System level

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。

説明

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

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。

<QX> system-view

[QX] pki retrieval-certificate ca domain 1

2.1.23 pki retrieval-crl domain

Syntax

pki retrieval-crl domain *domain-name*

View

System view

デフォルトレベル

2： System level

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

CRL 配布サーバから最新の CRL を読み出すには **pki retrieval-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。

<QX> system-view

[QX] pki retrieval-crl domain 1

2.1.24 pki validate-certificate

Syntax

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

View

System view

デフォルトレベル

2： System level

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。

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。

証明書有効検証は証明書が CA によってサインされていることと、証明書が失効も削除もされていないことをチェックすることです。

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。

<QX> system-view

[QX] pki validate-certificate local domain 1

2.1.25 state

Syntax

state *state-name*

undo state

View

PKI entity view

デフォルトレベル

2： System level

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：州または領域の指定無し

例

エンティティが属する州を指定します。

<QX> system-view

[QX] pki entity 1

[QX-pki-entity-1] state country

目次

3章 SSL

3.1 SSL設定コマンド

3.1.1 display ssl server-policy

Syntax

display ssl server-policy { *policy-name* | **all** } [**|** { **begin** | **exclude** | **include** } *regular-expression*]

View

すべての view

デフォルトレベル

1： Monitor level

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 1～16 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。

|： 表示される情報を正規表現で指定した文字列でフィルタします。

begin： 指定した正規表現の文字列を含む行以降を表示します。

exclude： 指定した正規表現の文字列を含まない行を表示します。

include： 指定した正規表現の文字列を含む行を表示します。

regular-expression： 正規表現を指定します。設定範囲は 1～256 文字です。大文字と小文字を区別します。

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。

<QX> display ssl server-policy policy1

```
SSL Server Policy: policy1
    PKI Domain: domain1
    Ciphersuite:
        RSA_RC4_128_MD5
```

```
    RSA_RC4_128_SHA
    RSA_DES_CBC_SHA
    RSA_3DES_EDE_CBC_SHA
    RSA_AES_128_CBC_SHA
    RSA_AES_256_CBC_SHA
Handshake Timeout: 3600
Close-mode: wait disabled
Session Timeout: 3600
Session Cachesize: 500
Client-verify: disabled
```

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
SSL Server Policy	SSLサーバポリシー名です。
PKI Domain	SSLサーバポリシーに使用されるPKIドメインです。
Ciphersuite	SSLサーバポリシーにサポートされる暗号スイートです。
Session Timeout	SSLサーバポリシーのセッションタイムアウト時間です(秒)。
Session Cachesize	SSLサーバポリシーのバッファリングされたセッションの最大数です。

3.1.2 pki-domain

Syntax

pki-domain *domain-name*

undo pki-domain

View

SSL server policy view、 SSL client policy view

デフォルトレベル

2： System level

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

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。

<QX> system-view

[QX] ssl server-policy policy1

[QX-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。

<QX> system-view

[QX] ssl client-policy policy1

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

3.1.3 ssl server-policy

Syntax

ssl server-policy *policy-name*

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

View

System view

デフォルトレベル

2： System level

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 1～16 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。

<QX> system-view

[QX] ssl server-policy policy1

[QX-ssl-server-policy-policy1]

3.1.4 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。

🕮 **メモ：**

ssl version ssl3.0 disable コマンドは、以下のソフトウェアでサポートしています。

- QX-S4000 シリーズ：Version 5.4.14 を含む以降のソフトウェア
- QX-S5300 シリーズ：Version 5.1.11 を含む以降のソフトウェア
- QX-S5700 シリーズ：Version 5.1.12 を含む以降のソフトウェア

Syntax

ssl version ssl3.0 disable

undo ssl version ssl3.0 disable

View

System view

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。

<QX> system-view

[QX] ssl version ssl3.0 disable