NEC

GVT-187324-001-00 1.7

QX-W シリーズ

Web 認証(ポータル認証)

コマンドマニュアル

改版履歴

版数	日付	改版内容
1.0	2021/11	初版発行
1.1	2022/03	・「1 章 Web 認証(ポータル認証)」に、下記コマンドを追加しました。 ・**display portal rule** ・**portal free-rule** 誤記修正
1.2	2022/09	・「1 章 Web 認証(ポータル認証)」に、下記コマンドを追加しました。 ・**portal host-check enable** ・**url-parameter**
1.3	2023/06	・「3 章 SSL」の **ssl version disable** コマンドにパラメータを追加しました。
1.4	2023/09	・対象バージョンに QX-W610 を追加しました。
1.5	2023/12	・対象バージョンに QX-W1240、QX-W2120AC、QX-W2230AC を追加しました。 ・関連マニュアルに QX-W1240，QX-W2120AC、QX-W2230AC の情報を追加しました。 ・誤記訂正
1.6	2024/01	・「1 章 Web 認証(ポータル認証)」に、下記コマンドを追加しました。 ・**login failed-url** ・**login success-url**
1.7	2024/02	・対象バージョンに QX-W2330AC を追加しました。

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-W シリーズ Web 認証(ポータル認証)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-W シリーズ Web 認証(ポータル認証)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

バージョン

本マニュアルに対応する製品バージョンは以下の通りです。

対象装置	製品バージョン
QX-W1000 シリーズ	Version 7.2.47 を含む以降
QX-W1100 シリーズ	Version 7.2.47 を含む以降
QX-W610	初版より
QX-W1240	初版より
QX-W2120AC	Version 7.2.47 を含む以降
QX-W2230AC	Version 7.2.47 を含む以降
QX-W2330AC	初版より

関連マニュアル

マニュアル	内容
QX-W1000/W1100 シリーズアクセスポイント 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-W1000/W1100 シリーズアクセスポイント 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-W1000/W1100 シリーズアクセスポイント 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-W1000/W1100 シリーズアクセスポイント 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-W1000/W1100 シリーズアクセスポイント Anchor-AC オペレーションマニュアル	Anchor-AC として動作させる場合の機能設定について説明しています。
QX-W1000/W1100 シリーズアクセスポイント Anchor-AC コマンドマニュアル	Anchor-AC として動作させる場合の機能に関するコマンドについて説明しています。
QX-W1000/W1100 シリーズ アクセスポイント	Anchor-AC として動作させる場合の 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

Anchor-AC Web コンソール操作マニュアル	を記述しています。
QX-W610 シリーズアクセスポイント 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-W610 シリーズアクセスポイント 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-W610 シリーズアクセスポイント 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-W1240 アクセスポイント 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-W1240 アクセスポイント 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-W1240 アクセスポイント 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-W2120AC アクセスコントローラ 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-W2120AC アクセスコントローラ 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-W2120AC アクセスコントローラ 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-W2120AC アクセスコントローラ 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-W2230AC アクセスコントローラ 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-W2230AC アクセスコントローラ 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-W2230AC アクセスコントローラ 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-W2230AC アクセスコントローラ 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-W シリーズ Web 認証 (ポータル認証) オペレーションマニュアル	Web 認証の設定について説明しています。
QX-W シリーズ Web 認証 (ポータル認証) コマンドマニュアル	**Web 認証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. コマンド表記規則

表記規則	説明
太字体	コマンドラインを示すキーワードには**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、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。1 つあるいは複数選択することも、何も選択しないこともできます。
&<1-n>	&の前のキーワードと引数を組み合わせます。引数で指定した数までキーワードを繰り返し指定できます。
#	#で始まる行はコメントを示します。

II. GUI 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。例えば、<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。例えば、[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。例えば、[File/Create/Folder]。

III. キーボード操作

表記規則	説明
<KEY>	KEY のキーを押します。例えば、 <Enter>は Enter キーを押します。
<KEY1 + KEY2>	複数のキーを同時に押します。例えば、<Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<KEY1, KEY2>	複数のキーを順番に押します。例えば、 <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

表記規則	説明
クリック	マウスのボタンを素早く押します。特に指定がない場合は左ボタンを押します。
ダブルクリック	マウスの左ボタンを素早く 2 回押します。
ドラッグ	マウスの左ボタンを押したまま移動します。

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重要な情報を示します。
⚠ **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重要な情報を示します。
⚠ **重要**	注意を払う必要が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. ネットワークアイコン

表記規則	説明
	ルータ、スイッチ、またはファイアウォールなどの一般的なネットワークデバイスを表しています。
	ルータまたはレイヤ 3 スイッチなどのルーティング対応のデバイスを表しています。
	レイヤ 2、レイヤ 3 スイッチまたはレイヤ 2 転送機能に対応したルータなどの一般的なスイッチデバイスを表しています。

VII. 設定例

本マニュアルの設定例は各機能での代表的な設定例を示します。インタフェース番号、システム名の表記、display コマンドで表示される情報は、ご使用の装置と異なることがあります。

VIII. セキュリティ強化

セキュリティ強化のため、simple で設定されたパスワードも cipher や hash で登録されます。

本マニュアルは以下に示す 3 個のセクションで構成されています。

01-Web 認証(ポータル認証)

02-PKI

03-SSL

目次

1章 Web 認証(ポータル認証)

1.1 Web認証(ポータル認証)設定コマンド

1.1.1 default-logon-page

Syntax

default-logon-page *filename*

undo default-logon-page

デフォルト

設定なし

View

Local portal Web server view

定義済みユーザロール

network-admin

パラメータ

filename: 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なし)で指定します。設定範囲は 1～91 文字です。大文字、小文字を区別します。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、デバイスはファイルを解凍して認証ページを取得します。デバイスは、これらをローカルポータル認証のデフォルト認証ページとして設定します。

ローカルポータル認証を成功させるには、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-W シリーズ Web 認証(ポータル認証) オペレーションマニュアルの *“1.5 認証ページのカスタマイズ”* を参照してください。

例

ローカルポータル Web サーバのデフォルトの認証ページファイルとして、pagefile1.zip ファイルを指定します。

<AP> system-view

[AP] portal local-web-server http

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

関連コマンド

portal local-web-server

1.1.2 display portal

Syntax

display portal { **ap** *ap-name* [**radio** *radio-id*] | **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

ap ap-name: AP 名を指定します。設定範囲は 1~64 文字です。大文字、小文字は区別されません。有効な文字は、英字、数字、アンダースコア (_) 、左カッコ ([) 、右かっこ (])、スラッシュ (/) 、およびマイナス記号 (-) です。AP 名を指定しない場合、すべての AP のポータル設定、ポータルの実行状態を表示します。

radio *radio-id:* 指定した無線のポータル設定、ポータルの実行状態を表示します。*radio-id* の範囲は、デバイスモデルによって異なります。このオプションを指定しないと、指定した AP の無線すべてのポータル設定、ポータルの実行状態を表示します。

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。

説明

display portal コマンドはポータル設定と実行状態を表示します。

例

AP ap 1 上の設定およびポータルの実行状態を表示します。

<AP> display portal ap ap1

```
Portal information of ap1
Radio ID: 1
SSID: portal
   Authorization : Strict checking
   ACL           : Disable
   User profile  : Disable
IPv4:
```

```
    Portal status: Enabled
    Portal authentication method: Direct
    Portal Web server: wbs(active)
    Secondary portal Web server: wbs sec
    Portal mac-trigger-server: mts
    Authentication domain: my-domain
    User-dhcp-only: Enabled
    Max portal users: 1024
    Bas-ip: 2.2.2.2
    Action for sever detection:
       Server type     Server name         Action
       Web server      wbs                fail-permit
       Portal server   pts                fail-permit
    Destination authentication subnet:
       IP address                         Mask
       2.2.2.2                            255.255.0.0
IPv6:
    Portal status: Enabled
    Portal authentication method: Direct
    Portal Web server: wbsv6(active)
    Secondary portal Web server: Not configured
    Authentication domain: my-domain
    User-dhcp-only: Disabled
    Max portal users: 512
    Bas-ipv6: 2000::1
    Action for sever detection:
       Server type     Server name         Action
       Web server      wbsv6              fail-permit
       Portal server   ptsv6              fail-permit
    Destination authentication subnet:
       IP address                         Prefix length
       3000::1                            64
```

#VLAN インタフェース 30 上の設定およびポータルの実行状態を表示します。

<AP> display portal interface Vlan-interface 30

```
Portal information of Vlan-interface30
    NAS-ID profile: Not configured
    Authorization : Strict checking
    ACL         : Disable
    User profile  : Disable
IPv4:
    Portal status: Enabled
    Portal authentication method: Direct
```

```
    Portal Web server: pt
    Secondary portal Web server: wbs sec(active)
    Authentication domain: test
    Pre-auth domain: Not configured
    User-dhcp-only: Disabled
    Pre-auth IP pool: Not configured
    Max portal users: Not configured
    Bas-ip: Not configured
    User detection: Not configured
    Portal temp-pass: Enabled      Period: 30s
    Action for server detection:
       Server type    Server name                    Action
       --             --                          --
IPv6:
    Portal status: Disabled
    Portal authentication method: Disabled
    Portal Web server: Not configured
    Secondary portal Web server: Not configured
    Authentication domain: Not configured
    Pre-auth domain: Not configured
    User-dhcp-only: Disabled
    Pre-auth IP pool: Not configured
    Max portal users: Not configured
    Bas-ipv6: Not configured
    User detection: Not configured
    Portal temp-pass: Disabled
    Action for server detection:
       Server type    Server name                    Action
       --             --                          --
    Destination authentication subnet:
       IP address                                  Prefix length
```

表 1-1 コマンド出力

フィールド	説明
Portal information of interface	インタフェースの設定です。
Radio ID	無線のIDです。
SSID	SSIDです。
NAS-ID profile	インタフェースのNAS-IDプロファイルです。
VSRP instance	インタフェース上のVSRPインスタンスの名前です。

フィールド	説明
VSRP state	インタフェースのVSRP状態です。: ● Masterーデバイスは VSRPインスタンスのマスターとして機能します。 ● バックアップーデバイスは、VSRPインスタンスのバックアップとして機能します。 ● Downーデバイスは VSRPインスタンスで実行されていません。この状態は、次のいずれかの状況で発生します。 • 関連付けられたVRRPグループは初期状態です。 • VSRPインスタンスが存在しないか、デバイスに正しく設定されていません。 ● N/Aーインタフェースはどの VSRPインスタンスにも関連付けられていません。
Authorization	認可情報タイプ:です。 ● ACL ● ユーザープロファイル
Strict checking	ポータル認可情報の厳密なチェック設定が表示されます
IPv4	IPv 4ポータル設定です。
IPv6	IPv 6ポータル設定です。
Portal status	インタフェースでのポータル認証ステータスです。 ● Disabledーポータル認証は無効です。 ● Enabledーポータル認証は有効です。 ● Authorizedーポータル認証サーバまたはポータルWebサーバにアクセスできません。インタフェースを使用すると、ユーザは認証なしでネットワークにアクセスできます。

フィールド	説明
Portal VSRP status	インタフェース上のポータルVSRPのステータス: ● M_Initial－マスターデバイスは初期状態です。 ● M_Delay－マスターデバイスは遅延状態です。(遅延時間が経過すると、デバイスはマスター状態に切り替わります。) ● M_Alone－マスターデバイスはスタンドアロン状態です。この状態は、マスターデバイスとバックアップデバイスが相互に通信できない場合に発生します。一般的な理由は、フェールオーバーリンクが切断されていることです。 ● M_Hello－マスターデバイスは、バックアップデバイスとTCP接続を構築しています (インタフェース上のVSRPステートとポータルイネーブルステートをネゴシエートします) 。 ● M_Collect－マスターデバイスは、バックアップデバイスからのユーザ情報を待機しています。 ● M_Sync－マスターデバイスは、ユーザ情報をバックアップデバイスに送信します。 ● M_Synced－マスターデバイスは、ユーザ情報をバックアップデバイスに同期しました。 ● B_Initial－バックアップデバイスは初期状態です。 ● B_Alone－バックアップデバイスはスタンドアロン状態です。この状態は、バックアップデバイスとマスターデバイスが相互に通信できない場合に発生します。一般的な理由は、フェールオーバーリンクが切断されていることです。 ● B_Hello－バックアップデバイスは、マスターデバイスとTCP接続を構築します (インタフェース上のVSRPステートとポータルイネーブルステートをネゴシエートします) 。 ● B_Report－バックアップデバイスは、ユーザ情報をマスターデバイスに送信しています。 ● B_Sync－バックアップデバイスは、マスターデバイスからユーザ情報を受信しています。 ● B_Synced－バックアップデバイスは、ポータル情報をマスターデバイスと同期しました。 ● Down－デバイスはVSRPインスタンスで実行されていません。 インタフェースがポータルで有効になっていない場合、またはVSRPインスタンスに関連付けられていない場合、このフィールドは表示されません。

フィールド	説明
Portal authentication method	インタフェースで認証モードが有効になっている。 直接認証が有効になっている場合、このフィールドには Directと表示されます。
Portal Web server	インタフェース上で指定されたプライマリ・ポータルWeb サーバの名前です。 サーバが使用されている場合、このフィールドにはサーバ名の横に (アクティブ) フラグが表示されます。
Secondary portal Web server	インタフェース上で指定されたバックアップポータルWeb サーバの名前です。 サーバが使用されている場合、このフィールドにはサーバ名の横に (アクティブ) フラグが表示されます。
Portal mac-trigger-server	インタフェース上で指定されたMACバインディングサーバの名前です。
Authentication domain	インタフェース上の必須認証ドメインです。
Pre-auth domain	インタフェース上のポータルユーザの事前認証ドメインです。
User-dhcp-only	user-dhcp-only機能のステータスです。 ● Enabled－DHCPで取得したIPアドレスを持つユーザだけがポータル認証を実行できます。 ● Disabled－DHCPで取得したIPアドレスを持つユーザと静的IPアドレスを持つユーザの両方が、認証を通過してオンラインになることができます。
Pre-auth ip-pool	認証前のポータルユーザに指定されたIPアドレスプールの名前です。
Max portal users	インタフェースで許可されるポータルユーザの最大数です。
Bas-ip	ポータル認証サーバに送信されるポータルパケットの BAS-IP属性です。
Bas-ipv6	ポータル認証サーバに送信されるポータルパケットの BAS-IPv 6属性です。
User detection	検出方法(ARP、ICMP、ND、またはICMPv 6)、検出間隔、検出の最大試行回数、インタフェースアイドル時間など、オンラインユーザを上のポータルで検出するための設定です。
Portal temp-pass	一時パス機能のステータスです。 ● Enabled－一時パス機能は有効です。 ● Disabled－一時パス機能は無効です。 ● [Period] －ユーザが一時的にインターネットにアクセスできる一時的なパス期間。このフィールドは、一時パス機能が有効な場合にのみ表示されます。

フィールド	説明
Action for server detection	インタフェース上の設定のポータルサーバ検出: ● [Server type] ーサーバのタイプ。ポータルサーバはポータル認証サーバを表し、Webサーバはポータルwebサーバを表します。 ● [Server name] ーサーバの名前。 ● [Action] ーサーバ検出の結果によってトリガーされるアクション。ポータルのfail-permit機能がイネーブルの場合、このフィールドにはfail-permitが表示されます。
Destination authentication subnet	ポータル認証の宛先サブネットの情報です。
IP address	ポータル認証サブネットのIPアドレスです。
Mask	ポータル認証サブネットのサブネットマスクです。
Prefix length	IPv 6ポータル認証サブネットアドレスのプレフィクス長です。

1.1.3 display portal rule

Syntax

display portal rule { **all** | **dynamic** | **static** } { **ap** *ap-name* [**radio** *radio-id*] | **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

all:ダイナミックおよびスタティックポータルフィルタリングルールを含む、すべてのポータルフィルタリングルールを表示します。

dynamic: ユーザがポータル認証を通過した後に生成されるダイナミックポータルフィルタリングルールを表示します。これらのルールでは、特定の送信元 IP アドレスを持つパケットがインタフェースを通過できます。

static: ポータル認証がイネーブルになった後に生成されるスタティックポータルフィルタリングルールを表示します。インタフェース認証がイネーブルの場合、ポータルはこれらのルールによってパケットをフィルタリングします。

ap *ap-name*: AP 名を指定します。設定範囲は 1~64 文字です。大文字、小文字は区別しません。有効な文字は、英字、数字、アンダースコア (_) 、左カッコ ([) 、右かっこ (])、スラッシュ (/) 、およびマイナス記号 (-) です。

radio *radio-id*: 無線 ID を指定します。無線 ID の値の範囲は、デバイスモデルによって異なります。無線 ID を指定しない場合、このコマンドは AP のすべての無線のポータルフィルタリングルールを表示します。

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。

説明

display portal コマンドはポータル設定と実行状態を表示します。

例

AP1 のすべてのポータルフィルタリングルールを表示します。

<AP> display portal rule all ap ap1

```
Slot 1:
IPv4 portal rules on ap1:
Radio ID : 1
SSID    : portal
Rule 1:
 Type             : Static
 Action           : Permit
 Protocol         : Any
 Status           : Active
 Source:
   IP       : 0.0.0.0
   Mask     : 0.0.0.0
   Port     : 23
   MAC      : 0000-0000-0000
   Interface : WLAN-BSS1/0/1
   VLAN     : any
 Destination:
   IP       : 192.168.0.111
   Mask     : 255.255.255.255
   Port     : Any

Rule 2:
 Type             : Dynamic
 Action           : Permit
 Status           : Active
 Source:
   IP       : 2.2.2.2
   MAC      : 0a0d-0af8-0eab
   Interface : WLAN-BSS1/0/1
   VLAN     : 2
 Author ACL:
```

```
    Number    : N/A

Rule 3:
 Type              : Static
 Action            : Redirect
 Status            : Active
 Source:
    IP       : 0.0.0.0
    Mask     : 0.0.0.0
    Interface : WLAN-BSS1/0/1
    VLAN     : any
    Protocol  : TCP
 Destination:
    IP       : 0.0.0.0
    Mask     : 0.0.0.0
    Port     : 80

Rule 4:
 Type              : Static
 Action            : Deny
 Status            : Active
 Source:
    IP       : 0.0.0.0
    Mask     : 0.0.0.0
    Interface : WLAN-BSS1/0/1
    VLAN     : Any
 Destination:
    IP       : 0.0.0.0
    Mask     : 0.0.0.0
```

表 1-2 コマンド出力

フィールド	説明
Radio ID	無線のIDです。
SSID	SSIDです。
Rule	ポータルフィルタリングルールの番号です。
Type	ポータルフィルタリングルールのタイプ: ● [Static] :スタティックポータルフィルタリングルール。 ● [Dynamic] :ダイナミックポータルフィルタリングルール。

フィールド	説明
Action	ポータルフィルタリングルールによってトリガーとして使用されるアクション: ● Permit:インタフェースはパケットの通過を許可します。 ● Redirect:インタフェースはパケットをリダイレクトします。 ● Deny:インタフェースはパケットの通過を禁止します。 ● [Match pre-auth ACL] :インタフェースは、事前認証ドメイン内の許可されたACLルールとパケットを照合します。
Protocol	レイヤフィルタリング規則で許可されているトランスポートポータルプロトコル: ● [Any] :任意のトランスポートレイヤプロトコルを許可します。 ● [TCP] :TCPを許可します。 ● [UDP] :UDPを許可します。
Status	ポータルフィルタリングルールのステータス: ● Active:ポータルルールが有効です。 ● Unactated:ポータルルールはアクティブ化されていません。
Source	ポータルフィルタリングルールのソース情報です。
IP	送信元IPアドレスです。
Mask	送信元IPv 4アドレスのサブネットマスクです。
Prefix length	送信元IPv 6アドレスのプレフィクス長です。
Port	送信元トランスポートレイヤポート番号です。
MAC	送信元MACアドレスです。
Interface	ポータルフィルタリングルールが実装されるインターフェイスです。
VLAN	送信元VLAN IDです。
Protocol	ポータルフィルタリングルールのプロトコルタイプです。
Destination	ポータルフィルタリングルールの宛先情報です。
IP	宛先IPアドレスです。
Port	宛先トランスポートレイヤポート番号です。

フィールド	説明
Mask	宛先IPv 4アドレスのサブネットマスクです。
Prefix length	宛先IPv 6アドレスのプレフィクス長です。
Author ACL	認証されたポータルユーザに割り当てられた認可ACLです。このフィールドは、ダイナミックポータルフィルタリングルールの場合にのみ表示されます。
Pre-auth ACL	事前認証ポータルユーザに割り当てられた認可ACLです。このフィールドは、Match pre-auth ACLアクションの場合にだけ表示されます。
Number	許可されたACLの番号です。AAAサーバがACLを割り当てていない場合、このフィールドにはNoneと表示されます。

1.1.4 display portal user

Syntax

display portal user { **all** | **ap** *ap-name* [**radio** *radio-id*] | **auth-type local** | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **username** *username* } [**brief** | **verbose**]

View

すべての view

定義済みユーザロール

network-admin

パラメータ

all: すべてのポータルユーザに関する情報を表示します。

ap *ap-name*: AP 名を指定します。設定範囲は 1~64 文字です。大文字、小文字は区別しません。有効な文字は、英字、数字、アンダースコア (_) 、左カッコ ([) 、右かっこ (])、スラッシュ (/) 、およびマイナス記号 (-) です。

radio radio-id: 無線 ID を指定します。無線 ID の値の範囲は、デバイスモデルによって異なります。無線 ID を指定しない場合、このコマンドは AP のすべての無線のポータルユーザに関する情報を表示します。

auth-type: 認証タイプを指定します。

local: ローカル認証を指定します。ローカルポータル認証サーバは、ポータルユーザに対してポータル認証を実行します。

interface *interface-type interface-number*: 指定したインタフェース上のポータルユーザに関する情報を表示します。

ip *ipv4-address*: ユーザの IPv 4 アドレスを指定します。

mac *mac-address*: ユーザの MAC アドレスを H-H-H の形式で指定します。

username *username*: ユーザのユーザ名を指定します。大文字、小文字を区別します。1~253 文字の文字列で指定します。ユーザ名にドメイン名を含めることはできません。

brief: ポータルユーザに関する簡易情報を表示します。

verbose: ポータルユーザに関する詳細情報を表示します。

説明

display portal user コマンドはポータルユーザに関する情報を表示します。

例

#すべてのポータルユーザに関する情報を表示します。

<AP> display portal user all

```
Total portal users: 1
Username: def
  AP name: ap1
  Radio ID: 1
  SSID: portal
  Portal server: pts
  State: Online
  VPN instance: vpn1
  MAC             IP              VLAN   Interface
  000d-88f8-0eac    4.4.4.4          2    Bss1/2
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: 3000
```

#ユーザアドレスが 0b0d-0bf8-0eab のポータル MAC に関する情報を表示します。

<AP> display portal user mac 0b0d-0bf8-0eab

```
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC             IP              VLAN   Interface
  0b0d-0bf8-0eab    2.2.2.2          2     WLAN-BSS1/0/1
  Authorization information:
    DHCP IP pool: N/A
    User profile: abc (active)
    Session group profile: cd (inactive)
    ACL number: N/A
```

#ユーザ名が abc のユーザに関する情報を表示します。

<AP> display portal user username abc

```
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC              IP               VLAN   Interface
  0b0d-0bf8-0eab    2.2.2.2           2     WLAN-BSS1/0/1
  Authorization information:
    DHCP IP pool: N/A
    User profile: abc (active)
    Session group profile: cd (inactive)
    ACL number: N/A
```

#IP アドレスが 18.18.0.20 のユーザに関する詳細情報を表示します

<AP> display portal user ip 18.18.0.20 verbose

```
Basic:
AP name: ap1
  Radio ID: 1
  SSID: portal
  Current IP address: 18.18.0.20
  Original IP address: 18.18.0.20
  Username: chap1
  User ID: 0x10000001
  Access interface: WLAN_BSS1/0/1
  Service-VLAN/Customer-VLAN: 50/-
  MAC address: 7854-2e1c-c59e
  Authentication type: Normal
  Domain name: portal
  VPN instance: N/A
  Status: Online
  Portal server: pt
  Vendor: Apple
  Portal authentication method: Direct
AAA:
  Realtime accounting interval: 720s, retry times: 5
  Idle cut: N/A
  Session duration: 0 sec, remaining: 0 sec
  Remaining traffic: N/A
  Login time: 2014-12-25 10:47:53 UTC
  Online duration (hh:mm:ss): 1:53:7
  DHCP IP pool: N/A
ACL&Multicast:
```

```
  ACL number: N/A
  User profile: N/A
  Session group profile: N/A
  Max multicast addresses: 4
Flow statistic:
  Uplink packets/bytes: 6/412
  Downlink packets/bytes: 0/0
```

#すべてのポータルユーザに関する簡易情報を表示します

<AP> display portal user all brief

```
IP address      MAC address      Online duration      Username
4.4.4.4         0b0d-0bf8-0eac   1:53:7              def
```

関連コマンド

portal enable

1.1.5 display portal user count

Syntax

display portal user count

View

すべての view

定義済みユーザロール

network-admin

network-operator

説明

display portal user count コマンドはポータルユーザ数を表示します。

例

#ポータルユーザの数を表示します。

<AP> display portal user count

```
Total number of users: 1
```

関連コマンド

- **portal enable**
- **portal delete-user**

1.1.6 display portal web-server

Syntax

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

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

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

説明

display portal web-server コマンドはポータル Web サーバの情報を表示します。

例

#ポータル Web サーバ wbs に関する情報を表示します。

<AP0> display portal web-server wbs

```
Portal Web server: wbs
   Type           : IMC
   URL            : http://www.test.com/portal
   URL parameters   : userurl=http://www.test.com/welcome
                    userip=source-address
   VPN instance     : Not configured
   Server detection : Interval: 120s  Attempts: 5  Action: log, trap
   IPv4 status      : Up
   IPv6 status      : N/A
   Captive-bypass   : Enabled
   If-match                :  original-url:   http://2.2.2.2,  redirect-url:
http://192.168.56.2
```

表 1-3 コマンド出力

フィールド	説明
Type	ポータルWebサーバの種類: ● CMCC― CMCCサーバ。 ● IMC― IMCサーバ。

フィールド	説明
Portal Web server	ポータルWebサーバの名前
URL	ポータルWebサーバのURL。
URL parameters	ポータルWebサーバのURLパラメータ。
VPN instance	ポータルWebサーバが属するVPNインスタンスの名前。 このフィールドは、現在のソフトウェアバージョンではサポートされていません。
Server detection	ポータルWebサーバ検出のパラメータ: ● 検出間隔 (秒単位) 。 ● 検出の最大試行回数。 ● ポータルWebサーバの到達可能性ステータスの変更によってトリガーされるアクション (ログおよびトラップ) 。
IPv4/IPv6 status	ポータルWebサーバの現在の状態: ● [N/A] ー ポータルWebサーバの検出は無効です。サーバの到達可能性ステータスが不明です。 ● [Up] ーポータルWebサーバ検出が有効です。サーバは到達可能です。 ● Down ーポータルWebサーバの検出が有効です。サーバに到達できません。
Captive-bypass	captive-bypass機能のステータス。 ● Disabled ー Captive-bypassは無効です。 ● Enabled ー Captive-bypassは有効です。 ● Optimize Enabled ー Optimized captive-bypassは有効です。
If-match	URLリダイレクション用に設定された一致ルール。

関連コマンド

- **portal enable**
- **portal web-server**
- **server-detect (portal Web server view)**

1.1.7 login failed-url

Syntax

login failed-url *url-string*

undo login failed-url *url-string*

デフォルト

設定なし

View

local portal web service view

定義済みユーザロール

network-admin

パラメータ

url-string：認証失敗時のリダイレクト URL を指定します。大文字小文字を区別する 1～256 文字の文字列が使用可能です。url-string 引数の場所に「?」を入力すると、CLI はこの引数のヘルプ情報を表示しません。

説明

login failed-url *url-string* コマンドはログイン失敗時のリダイレクト URL を設定します。

デバイスは、ポータルユーザが認証に失敗した後、指定された URL にリダイレクトします。

undo login failed-url *url-string* コマンドはログイン失敗時のリダイレクト URL の設定を解除します。

例

認証失敗時のリダイレクト URL を https://1.1.1.1/portal/login.html に設定します。

<AP> system-view

[AP] portal local-web-server https

[AP-portal-loca-websvr-https] login failed-url https://1.1.1.1/portal/login.html

1.1.8 login success-url

Syntax

login success-url *url-string*

undo login success-url *url-string*

デフォルト

設定なし

View

local portal web service view

定義済みユーザロール

network-admin

パラメータ

url-string：認証失敗時のリダイレクト URL を指定します。大文字小文字を区別する 1～256 文字の文字列が使用可能です。url-string 引数の場所に「?」を入力すると、CLI はこの引数のヘルプ情報を表示しません。

説明

login success-url *url-string* コマンドはログイン失敗時のリダイレクト URL を設定します。

デバイスは、ポータルユーザが認証に失敗した後、指定された URL にリダイレクトします。

undo login success-url *url-string* コマンドはログイン失敗時のリダイレクト URL の設定を解除します。

例

認証失敗時のリダイレクト URL を https://1.1.1.1/portal/login.html に設定します。

<AP> system-view

[AP] portal local-web-server https

[AP-portal-loca-websvr-https] login success-url https://1.1.1.1/portal/login.html

1.1.9 portal apply web-server

Syntax

portal apply web-server *server-name*

undo portal apply web-server [*server-name*]

デフォルト

設定なし

View

VLAN interface view

Service template view

定義済みユーザロール

network-admin

パラメータ

server-name: インタフェース上で指定するポータル Web 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。名前はすでに存在している必要があります。

説明

portal apply web-server コマンドは VLAN インタフェースまたはサービステンプレートのポータル Web サーバを指定します

undo portal apply web-server コマンドは VLAN インタフェースまたはサービステンプレートのポータル Web サーバ指定を削除します。

undo portal apply web-server コマンドを *server-name* を省略して実行した場合、インタフェースまたはサービステンプレート上のすべてのポータル Web サーバ指定の設定が削除されます。

例

#ポータル Web サーバ wbs をポータル認証用のポータル Web サーバとして VLAN インタフェース 100 で指定します。

<AP> system-view

[AP] interface vlan-interface 100

[AP–Vlan-interface100] portal apply web-server wbs

#ポータル Web サーバ wbs をポータル認証用のポータル Web サーバとしてサービステンプレート service1 で指定します。

<AP> system-view

[AP] wlan service-template service1

[AP] portal apply web-server wbs

関連コマンド

- **display portal**
- **portal fail-permit server**
- **portal web-server**
- **server-detect (portal web-server view)**

1.1.10 portal domain

Syntax

portal domain *domain-name*

undo portal domain

デフォルト

設定なし

View

VLAN interface view

Service template view

定義済みユーザロール

network-admin

パラメータ

domain-name: ISP ドメイン名を指定します。設定範囲は 1～255 文字です。大文字、小文字は区別しません。

説明

portal domain コマンドは VLAN インタフェースまたはサービステンプレートにポータル認証の為の認証ドメインを指定します。

undo portal domain コマンドはデフォルトに戻します。

例

VLAN インタフェース 100 で、ポータル認証ユーザのための認証ドメインとして my-domain を指定します。

<AP> system-view

[AP] interface vlan-interface 100

[AP–Vlan-interface100] portal domain my-domain

サービステンプレート service1 で、ポータル認証ユーザのための認証ドメインとして my-domain を指定します。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] portal domain my-domain

1.1.11 portal enable

Syntax

portal enable method direct

undo portal enable

デフォルト

無効

View

VLAN interface view

Service template view

定義済みユーザロール

network-admin

説明

portal enable method direct コマンドは、ポータル認証を有効化します。

undo portal enable コマンドはデフォルトに戻します。

🕮 **メモ：**

- VLAN インタフェースとサービステンプレートの両方でポータル認証を有効にしないでください

例

#VLAN インタフェース 100 でポータル認証を有効にします。

<AP> system-view

[AP] interface vlan-interface 100

[AP–Vlan-interface100] portal enable method direct

#VLAN インタフェース 100 でポータル認証を有効にします。

<AP> system-view

[AP] wlan service-template service1

[AP-wlan-st-service1] portal enable method direct

関連コマンド

display portal

1.1.12 portal free-rule

🕮 **メモ**:

認証前のクライアントは、ポータル Web サーバとだけ通信が可能です。認証前の無線端末で DNS サーバ等と通信させる場合は、ポータルフリールールを設定してください。

Syntax

portal free-rule *rule-number* **{ destination ip {** *ip-address* **{** *mask-length* **|** *mask* **} | any }** **[tcp** *tcp-port-number* **| udp** *udp-port-number* **] | source ip {** *ip-address* **{** *mask-length* **|** *mask* **} | any } [tcp** *tcp-port-number* **| udp** *udp-port-number* **] } * [interface** *interface-type interface-number* **]**

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

rule-number: ポータルフリールール番号を 0~4294967295 の範囲で指定します。

destination: 宛先情報を指定します。

source: ソース情報を指定します。

ip *ip-address*: ポータルフリールールの IPv 4 アドレスを指定します。

{ mask-length | mask }: IPv4 アドレスのサブネットマスクを指定します。mask-length 引数の値の範囲は 0~32 です。mask 引数はドット付き 10 進表記です。

ip any: 任意の IPv 4 アドレスを表します。

tcp *tcp-port-number*: ポータルフリールールの TCP ポート番号を 0~65535 の範囲で指定します。

udp *udp-port-number*: ポータルフリールールの UDP ポート番号を 0~65535 の範囲で指定します。

all: すべてのポータルフリールールを指定します。

interface *interface-type interface-number*: ポータルフリールールが有効になる VLAN インタフェースを指定します。

説明

portal free-rule コマンドは、IP ベースのポータルフリールールを設定します。

undo portal free-rule コマンドはポータルフリールールを削除します。

ポータルフリールールには、source キーワードと destination キーワードの両方を指定できます。キーワードを 1 つだけ指定した場合、もう 1 つのキーワードはフィルタリング基準として機能しません。

ポータルフリールールの送信元ポート番号と宛先ポート番号の両方を指定する場合、2 つのポート番号は同じトランスポートレイヤプロトコルに属している必要があります。

VLAN インタフェースを指定しない場合、ポータルフリールールはすべてのポータル対応 VLAN インタフェースで有効になります。

同じフィルタリング基準で 2 つのポータルフリールールを設定することはできません。

例

#ルール番号を 1、送信元 IP アドレスを 10.10.10.1/24、宛先 IP アドレスを 20.20.20.1、宛先 TCP ポート番号を 23、インタフェースを VLAN インタフェース 100 としてポータルフリールールを設定します。

<AP> system-view

[AP] portal free-rule 1 destination ip 20.20.20.1 32 tcp 23 source ip 10.10.10.1 24 interface vlan-interface 100

関連コマンド

display portal rule

1.1.13 portal host-check enable

🕮 メモ：

ローカル転送モードの AP でポータル認証を行う場合は、このコマンドを有効にしてください。

Syntax

portal host-check enable

undo portal host-check enable

デフォルト

無効(ソフトウェアバージョン 7.2.47 を含む以前)

有効(ソフトウェアバージョン 7.2.49 を含む以降)

View

System view

定義済みユーザロール

network-admin

説明

portal host-check enable コマンドは、ワイヤレスポータルクライアントの有効性チェックを有効にします。

undo portal host-check enable コマンドはデフォルトに戻します。

ローカル転送モードの AP で構成されたワイヤレスネットワークでは、AC にクライアントの ARP エントリはありません。したがって、AC は ARP エントリを使用してポータルクライアントの有効性をチェックできません。ユーザがポータル認証を実行できるようにするには、AC でワイヤレスクライアントの有効性チェックを有効にする必要があります。

この機能により、AC は WLAN スヌーピングテーブル、DHCP スヌーピングテーブル、および ARP テーブル内のクライアント情報を検索することで、クライアントを検証できます。クライアント情報が存在する場合、AC はそのクライアントのポータル認証が有効であると判断します。

例

#ワイヤレスポータルクライアントの有効性チェックを有効にします。

<AC> system-view

[AC] portal host-check enable

関連コマンド

display ip source binding

1.1.14 portal ipv4-max-user

Syntax

portal ipv4-max-user *max-number*

undo portal ipv4-max-user

デフォルト

VLAN インタフェースまたはサービステンプレート上のポータルユーザの最大数に制限はありません。

View

VLAN interface view

Service template view

定義済みユーザロール

network-admin

パラメータ

max-number: VLAN インタフェースまたはサービステンプレート上で許可されるポータルユーザの最大数を 1~4294967295 の範囲で指定します。

説明

portal ipv4-max-user コマンドは VLAN インタフェースまたはサービステンプレート上のポータルユーザ最大数を設定します。

undo ipv4-max-user コマンドは VLAN インタフェースまたはサービステンプレート上のポータルユーザ最大数をデフォルトに戻します。

VLAN インタフェースまたはサービステンプレート上でオンライン状態のポータルユーザの数よりも小さい値を指定した場合でも、設定は成功します。

この時、オンライン状態のポータルユーザには影響ありません。

ただし、新しいポータルユーザが VLAN インタフェース、またはサービステンプレートからログインするには、オンラインユーザ数が制限値を下回る必要があります。

すべての VLAN インタフェースまたはサービステンプレートで指定されているポータルユーザの最大合計数が、システムで許可されている最大数を超えないように設定してください。システムで許可されている最大数を超過したポータルユーザがデバイスにログインできなくなります。

例

#VLAN インタフェース 100 で IPv 4 ポータルユーザの最大数を 100 に設定します。

<AP> system-view

[AP] interface vlan-interface 100

[AP–Vlan-interface100] portal ipv4-max-user 100

#サービステンプレート service 1 で IPv 4 ポータルユーザの最大数を 100 に設定します。

<AP> system-view

[AP] wlan service-template service1

[AP–wlan-st-service1] portal ipv4-max-user 100

関連コマンド

- **display portal user**
- **portal max-user**

1.1.15 portal local-web-server

Syntax

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

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。

このオプションを指定しない場合、HTTPS は自己署名証明書を使用する SSL サーバポリシーに関連付けられます。このポリシーではすべての暗号スイートをサポートします。

説明

portal local-web-server コマンドは、ローカルポータル Web サーバを作成し、その View に移行します。既にローカルポータル Web サーバが作成されている場合、その View に移行します。

undo portal local-web-server コマンドは、ローカルポータル Web サーバを削除します

ローカルポータル Web サーバの View で以下のパラメータを設定することができます。

- tcp-port
- default-logon-page

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。

外部ポータル Web サーバーおよびポータル認証サーバーは必要ありません。

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、デバイスのローカル 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。

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。

<AP> system-view

[AP] portal local-web-server http

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

HTTPS ベースのローカル Web サービスを有効にして、SSL サーバポリシーpolicy1 を関連付けます。

<AP> system-view

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

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

SSL サーバポリシーを policy2 に変更します。

[AP] undo portal local-web-server https

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

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

関連コマンド

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

1.1.16 portal max-user

Syntax

portal max-user *max-number*

undo portal max-user

デフォルト

システムで許可されるポータルユーザの最大数に制限はありません。

View

System view

定義済みユーザロール

network-admin

パラメータ

max-number: システムで許可されるポータルユーザの最大数を 1~4294967295 の範囲で指定します。

説明

portal max-user コマンドはシステムで許可されるポータルユーザ最大数を設定します。

undo max-user コマンドはシステムで許可されるポータルユーザ最大数をデフォルトに戻します。

デバイス上で現在オンライン状態のポータルユーザの数よりも小さい値を指定した場合でも、設定は成功します。

この時、オンライン状態のポータルユーザには影響ありません。

ただし、新しいポータルユーザがログインするには、オンラインユーザ数が制限値を下回る必要があります。

すべての VLAN インタフェースまたはサービステンプレートで指定されているポータルユーザの最大合計数が、システムで許可されている最大数を超えないように設定してください。システムで許可されている最大数を超過したポータルユーザがデバイスにログインできなくなります。

例

システムで許可されるオンライン・ポータル・ユーザの最大数を 100 に設定します。

<AP> system-view

[AP] portal max-user 100

関連コマンド

- **display portal user**
- **portal max-user**

1.1.17 portal web-server

Syntax

portal web-server *server-name*

undo portal web-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: ポータル Web 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

portal web-server コマンドはポータル Web サーバを作成し、その view に移行します。すでにポータル Web サーバが作成されている場合、その view に移行します。

undo portal web-server コマンドはポータル Web サーバを削除します。

portal web-server view で以下のパラメータを設定することができます。

- ポータル Web サーバの URL

例

#ポータル Web サーバを作成し、そのビューに移行します。.

<AP> system-view

[AP] portal web-server wbs

[AP-portal-websvr-wbs]

関連コマンド

- **display portal web-server**
- **portal apply web-server**

1.1.18 tcp-port

Syntax

tcp-port *port-number*

undo tcp-port

デフォルト

HTTP のリスニング TCP ポート番号は 80、HTTPS のリスニング TCP ポート番号は 443 です。

View

Local portal Web server view

定義済みユーザロール

network-admin

パラメータ

port-number: リスニング TCP ポート番号を 1~65535 の範囲で指定します。

説明

ローカルポータル Web サーバを使用するには、このコマンドで指定するポート番号を、ポータル Web サーバの URL のポート番号と同じ設定にしてください。

ローカルポータル認証を使用する場合は、次のガイドラインに従ってください。

- ローカルポータル Web サーバのリスニング TCP ポート番号に、既知のプロトコルまたはその他のサービスで使用されるポート番号を設定しないでください。たとえば、FTP と Telnet でそれぞれ使用されるポート番号 21 と 23 は指定しないでください。
- HTTP リスニング TCP ポート番号に、デフォルトの HTTPS TCP ポート番号 443 を設定しないでください。
- HTTPS リスニングポート番号に、デフォルトの HTTP TCP ポート番号 80 を設定しないでください。
- HTTP と HTTPS に同じリスニング TCP ポート番号を設定しないでください。

例

#ローカルポータル Web サーバの HTTP リスニング TCP ポート番号を 2331 に設定します。

<AP> system-view

[AP] portal local-web-server http

[AP-portal-local-websvr-http] tcp-port 2331

関連コマンド

portal local-web-server

1.1.19 url

Syntax

url *url-string*

undo url

デフォルト

設定なし

View

Portal Web server view

定義済みユーザロール

network-admin

パラメータ

url-string: ポータル Web サーバの 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 コマンドはポータル Web サーバの URL を設定します。

undo url コマンドはデフォルトに戻します。

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。

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

#ポータル Web サーバ wbs の URL を http://www.test.com/portal に設定します。

<AP> system-view

[AP] portal web-server wbs

[AP-portal-websvr-wbs] url http://www.test.com/portal

関連コマンド

display portal web-server

1.1.20 url-parameter

Syntax

url-parameter *param-name* **{ nas-id | nas-port-id | original-url | source-address | ssid | { ap-mac | source-mac } [encryption { aes | des } key { cipher | simple }** *string* **] | value** *expression* **| vlan }**

undo url-parameter *param-name*

デフォルト

設定なし

View

Portal Web server view

定義済みユーザロール

network-admin

パラメータ

param-name: パラメータ名を指定します。大文字と小文字が区別され、1~32 文字の文字列になります。パラメータの内容は、指定する次のキーワードによって決まります。

nas-id: NAS-ID を指定します

nas-port-id: NAS-Port-Id を指定します。

original-url:ユーザがアクセスする元の Web ページの URL を指定します。

source-address: ユーザ IP アドレスを指定します。

ssid: AP の SSID を指定します。

ap-mac: AP の MAC アドレスを指定します。

source-mac:ユーザ MAC アドレスを指定します。

aes:指定した URL パラメータを暗号化する AES を指定します。

des:指定した URL パラメータを暗号化する DES を指定します。

cipher:暗号化形式で鍵を指定します。

simple:プレーンテキストで共有鍵を設定します。セキュリティ上の理由から、平文形式で指定されたキーは暗号化された形式で保存されます。

string: 大文字と小文字を区別する鍵文字列を指定します。文字列の長さは、選択した暗号化方式によって異なります。

- DES 暗号化された暗号文鍵の場合、文字列の長さは 41 文字です。
- DES 暗号化された平文鍵の場合、文字列の長さは 8 文字です。
- AES で暗号化される暗号テキスト鍵の場合、文字列の長さは 1 から 73 文字です。
- AES で暗号化されたプレーンテキスト鍵の場合、文字列の長さは 1 から 31 文字です。

value *expression*:大文字と小文字を区別する 1~256 文字のカスタム文字列を指定します。

vlan:ユーザ VLAN ID を指定します。

説明

url-parameter コマンドはポータル Web サーバの URL に含まれるパラメータを設定します。

undo url parameter コマンドはデフォルトに戻します。

複数の URL パラメータを設定できます。

URL パラメータを複数回設定すると、最新の設定が有効になります。

URL パラメータを設定すると、アクセスデバイスは、これらのパラメータを含むポータル Web サーバ URL をポータルユーザに送信します。たとえば、ポータル Web サーバの URL が http://www.test.com/portal,で、url-parameter userip source-address コマンドと url-parameter userurl value http://www.abc.com/welcome コマンドを実行するとします。

次に、IP アドレスが 1.1.1.1 のユーザに

URL http://www.test.com/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome

を送信します。

このコマンドで param-name 引数を設定する場合は、実際のポータルサーバでサポートされている URL パラメータ名を使用する必要があります。ポータルサーバの種類によって、サポートされる URL パラメータ名が異なります。

たとえば、IMC サーバは、キーワード original-url、source-address、および source-mac に対して、それぞれパラメータ名 userurl、userip、および usermac をサポートします。ポータル Web サーバ URL でユーザ IP 情報を伝送するには、パラメータ名を userip に設定し、source-address キーワードを指定する必要があります。

パラメータに暗号化アルゴリズムを指定した場合、リダイレクト URL はパラメータの暗号化された値を伝送します。

url-parameter usermac source-mac encryption des 鍵 simple 12345678 コマンドを実行します。

次に、アクセスデバイスはユーザアドレス 1111-1111-1111 を持つ URL

http://www.test.com/portal?usermac=xxxxxxxxx&userip=1.1.1.1&userurl=
http://www.test.com/welcome,をユーザに送信します。xxxxxxxxx は暗号化された MAC アドレスです。

例

#ポータル Web サーバ wbs の URL パラメータとして userip および userurl を設定します。userip パラメータの値を source-address (ユーザの IP アドレス) とし、userurl パラメータの値を http://www.abc.com/welcome とします。

<AP> system-view

[AP] portal web-server wbs

[AP-portal-websvr-wbs] url-parameter userip source-address

[AP-portal-websvr-wbs] url-parameter userurl value http://www.abc.com/welcome

#ポータル Web サーバ wbs の URL パラメータとして usermac を設定します。usermac パラメータとして source-mac (ユーザの MAC アドレス)の値を使用し、MAC アドレスを DES で暗号化します。

<AP> system-view

[AP] portal web-server wbs

[AP-portal-websvr-wbs] url-parameter usermac source-mac encryption des key simple 12345678

#ポータル Web サーバ wbs の URL パラメータとして uservlan を設定します。uservlan パラメータとして、vlan(ユーザの VLAN ID)を指定します。

<AP> system-view

[AP] portal web-server wbs

[AP-portal-websvr-wbs] url-parameter uservlan vlan

関連コマンド

display portal web-server

url

目次

2章 PKI

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。

<AP> system-view

[AP] 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。

[AP-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。

[AP-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。

[AP-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

デフォルト

trusted-CA は PKI ドメインに指定されていません。

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。

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。

<AP> system-view

[AP] pki domain 1

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

2.1.3 certificate request entity

Syntax

certificate request entity *entity-name*

undo certificate request entity

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。

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 1～31 文字です。大文字、小文字を区別しません。

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。

例

証明書要求のエンティティを entity1 として指定します。

<AP> system-view

[AP] pki domain 1

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

関連コマンド

pki entity

2.1.4 certificate request from

Syntax

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

undo certificate request from

デフォルト

証明書要求に指定された権限はありません。

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。

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。

<AP> system-view

[AP] pki domain 1

[AP-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

デフォルト

マニュアル要求モード

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。平文指定では 1～31 文字、暗号化指定では 1～73 文字で設定します。大文字小文字を区別します

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。

例

証明書要求モードを”auto"に設定します。

<AP> system-view

[AP] pki domain aaa

[AP-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。

<AP> system-view

[AP] pki domain aaa

[AP-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** }

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

Views

PKI domain view

定義済みユーザロール

network-admin

パラメータ

count *count*: 証明書要求ステータス最大リトライ数を 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。

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。

<AP> system-view

[AP] pki domain aaa

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

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

2.1.7 certificate request url

Syntax

certificate request url *url-string*

undo certificate request url

デフォルト

PKI ドメインに指定された URL はありません。

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 1～511 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。

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。

例

証明書要求サーバの URL を指定します。

<AP> system-view

[AP] pki domain 1

[AP-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

デフォルト

指定された共通名はありません。

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 1～63 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。

例

#エンティティの共通名を test として設定します。

<AP> system-view

[AP] pki entity 1

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

2.1.9 country

Syntax

country *country-code-str*

undo country

デフォルト

国コードは指定されていません。

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。

例

エンティティの国コードを JP に設定します。

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] country JP

2.1.10 crl check enable

Syntax

crl check enable

undo crl check enable

デフォルト

CRL チェックは有効です。

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。

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。

<AP> system-view

[AP] pki domain 1

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

2.1.11 crl url

Syntax

crl url *url-string*

undo crl url

デフォルト

CRL 配布ポイントの URL は指定されていません。

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 1～511 文字です。大文字、小文字を区別します。*server_location* は IP アドレスまたはドメイン名を指定できます。URL の長さは、CLI 文字列制限または url-string パラメータのいずれか小さい方によって制限されます。

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。

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。

<AP> system-view

[AP] pki domain 1

[AP-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。大文字、小文字は区別しません。

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。

<AP> 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。

<AP> 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。大文字と小文字は区別しません。

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。

<AP> 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。

<AP> 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
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 1～31 文字です。大文字、小文字は区別しません。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。

例

PKI ドメイン aaa の CA 証明書を表示します。

<AP> 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。

<AP> 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
```

関連コマンド

- **pki retrieval-certificate**
- **pki domain**

2.1.15 display pki certificate request-status

Syntax

display pki certificate request-status [domain *domain-name***]**

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

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、小文字は区別しません。ドメイン名は表 2-4 に示す指定記号を設定することができません。

表 2-4 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

例

すべての PKI ドメインの状態を要求します。

<AP> 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 2-5 **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。

関連コマンド

- **pki retrieval-certificate**
- **pki domain**
- **certificate request polling**

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 1～31 文字です。大文字、小文字は区別しません。

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。

例

ローカル的に保存された CRL を表示します。

<AP> 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 2-6 **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。

フィールド	説明
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。

関連コマンド

- **pki retrieval-crl**
- **pki domain**

2.1.17 fqdn

Syntax

fqdn *name-str*

undo fqdn

デフォルト

FQDN はエンティティに指定されていません。

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 1～255 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。

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。

<P> system-view

[AP] pki entity 1

[AP-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

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。

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。

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。

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] ip 11.0.0.1

2.1.19 locality

Syntax

locality *locality-name*

undo locality

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。

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 1～63 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。

例

エンティティの所在地を city として設定します。

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] locality city

2.1.20 organization

Syntax

organization *org-name*

undo organization

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。

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 1～63 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。

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。

<AP> system-view

[AP] pki entity 1

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

2.1.21 organization-unit

Syntax

organization-unit *org-unit-name*

undo organization-unit

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。

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 1～63 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。

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。

<AP> system-view

[AP] pki entity 1

[AP-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 2-7 に記載している指定記号は使用できません.

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	"
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。

<AP> system-view

[AP] 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*

デフォルト

設定なし

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。大文字、小文字は区別しません。

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。

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。

<AP> system-view

[AP] pki certificate access-control-policy mypolicy

[AP-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*

デフォルト

設定なし

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。大文字、小文字は区別しません。

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。

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。

<AP> system-view

[AP] pki certificate attribute-group mygroup

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

2.1.25 pki delete-certificate

Syntax

pki delete-certificate domain *domain-name* { **ca** | **local | peer [serial** *serial-num***]** }

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: 証明書を削除する PKI ドメインの名前を指定します。設定範囲は 1～127 文字です。大文字、小文字は区別しません。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	'

peer： ローカルに記録されたピア証明書を削除します。

serial *serial-num*： ピア証明書をシリアル番号で指定します。設定範囲は 1～127 文字です。大文字、小文字は区別しません。シリアル番号を指定しない場合、このコマンドは PKI ドメイン内のすべてのピア証明書を削除します。

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。

<AP> system-view

[AP] pki delete-certificate domain cer local

2.1.26 pki domain

Syntax

pki domain *domain-name*

undo pki domain *domain-name*

デフォルト

PKI ドメインはありません。

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 1～31 文字です。大文字、小文字を区別します。ドメイン名には表 2-8 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	'

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。

例

PKI ドメインを作成し、その view へ移行します。

<AP> system-view

[AP] pki domain 1

[AP-pki-domain-1]

2.1.27 pki entity

Syntax

pki entity *entity-name*

undo pki entity *entity-name*

デフォルト

エンティティはありません。

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 1～31 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。

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。

<AP> system-view

[AP] pki entity en

[AP-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。

peer: ピア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 1～31 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 2-10 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	'

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*：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、小文字は区別しません。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。

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。

<AP> system-view

[AP] pki import-certificate ca domain cer pem

関連コマンド

pki domain

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。大文字、小文字は区別しません。ドメイン名は表 2-11 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	'

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。大文字、小文字を区別します。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。

<AP> system-view

[AP] 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。

[AP] 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** | **peer** *entity-name* }

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。

peer *entity-name*： ピアエンティティ名を指定します。設定範囲は 1～31 文字です。大文字、小文字は区別しません。

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。設定範囲は 1～31 文字です。大文字、小文字は区別しません。 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。

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。）

<AP> system-view

[AP] 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。

<AP> system-view

[AP] pki retrieve-certificate domain aaa local

関連コマンド

pki domain

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 1～31 文字です。ドメイン名は表 2-13 に示す指定記号を設定することができません。

表 2-13 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。

例

CRL を読み出します。

<AP> system-view

[AP] pki retrieve-crl domain 1

関連コマンド

pki domain

2.1.32 pki storage

Syntax

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

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

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。

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。

例

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

<AP> system-view

[AP] 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。

<AP> system-view

[AP] 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 1～31 文字です。大文字、小文字は区別しません。ドメイン名は表 2-14 に示す指定記号を設定することができません。

表 2-14 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。

例

ローカル証明書の有効性を検証します。

<AP> system-view

[AP] pki validate-certificate local domain 1

関連コマンド

pki domain

2.1.34 public-key dsa

Syntax

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

undo public-key

デフォルト

設定なし

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。大文字、小文字は区別しません。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。

例

2048-bit の DSA キーペア abc の証明書要求をします。

<AP> system-view

[AP] pki domain aaa

[AP-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

デフォルト

設定なし

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。大文字、小文字は区別しません。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。

例

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

<AP> system-view

[AP] pki domain aaa

[AP-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

デフォルト

設定なし

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。大文字、小文字は区別しません。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。大文字、小文字は区別しません。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。大文字、小文字は区別しません。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 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。

例

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

<AP> system-view

[AP] pki domain aaa

[AP-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"

<AP> system-view

[AP] pki domain aaa

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

[AP-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

デフォルト

設定なし

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。

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。

<AP> system-view

[AP] pki domain aaa

[AP-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。

<AP> system-view

[AP] pki domain aaa

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

2.1.38 state

Syntax

state *state-name*

undo state

デフォルト

設定なし

View

PKI entity view

定義済みユーザロール

network-admin

パラメータ

state-name：都道府県名または州を指定します。設定範囲は 1～63 文字です。大文字、小文字を区別します。コンマは含まれません。

説明

エンティティが属する都道府県名または州を指定するには **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。

例

エンティティが属する州を指定します。

<AP> system-view

[AP] pki entity 1

[AP-pki-entity-1] state country

目次

3章 SSL

3.1 SSL設定コマンド

3.1.1 certificate-chain-sending enable

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

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。

<AP> system-view

[AP] ssl server-policy policy1

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

3.1.2 display ssl server-policy

Syntax

display ssl server-policy *policy-name*

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、小文字は区別しません。

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。

<AP> 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。

3.1.3 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、小文字は区別しません。

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。

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。

<AP> system-view

[AP] ssl server-policy policy1

[AP-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。

<AP> system-view

[AP] ssl client-policy policy1

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

関連コマンド

display ssl server-policy

3.1.4 ssl server-policy

Syntax

ssl server-policy *policy-name*

undo ssl server-policy *policy-name*

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、小文字は区別しません。

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。

例

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

<AP> system-view

[AP] ssl server-policy policy1

[AP-ssl-server-policy-policy1]

関連コマンド

display ssl server-policy

3.1.5 ssl version 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 disable コマンドの tls1.0、tls1.1、tls1.2 のパラメータはソフトウェアバージョン 7.2.59 を含む以降のソフトウェアからサポートしています。

Syntax

ssl version { **ssl3.0 | tls1.0** | **tls1.1** | **tls1.2** } **disable**

undo ssl version ssl3.0 disable

デフォルト

SSL サーバは、SSL3.0、TLS1.0、TLS1.1、TLS1.2 をサポートします。

View

System view

定義済みユーザロール

network-admin

パラメータ

ssl3.0: SSL3.0 を指定します。

tls1.0: TLS1.0 を指定します。

tls1.1: TLS1.1 を指定します。

tls1.2: TLS1.2 を指定します。

説明

ssl version disable コマンドは SSL サーバがセッションネゴシエーションに特定の SSL プロトコルバージョンを使用しないようにします。

undo ssl version disable コマンドはデフォルトに戻します。

システムセキュリティを強化するために、SSL サーバがセッションネゴシエーションに特定の SSL プロトコルバージョン(SSL3.0、TLS1.0、TLS1.1 および TLS1.2) を使用しないよう にすることができます。

例

装置で SSL 3.0 を無効にします。

<AP> system-view

[AP] ssl version ssl3.0 disable