Web Admin Settings

- Information About Web Admin Settings, on page 1
- Configuring HTTP/HTTPS Access , on page 1
- Configuring HTTP Trust Point, on page 2
- Configuring Netconf Yang, on page 3
- Configuring Timeout Policy , on page 3
- Configuring VTY, on page 4

Information About Web Admin Settings

This chapter outlines the various settings to access the controller's web interface. These include setting up the controller for communication with others in the network, configuring the management interface to connect over IP, setting up the number of users and protocols to access the controller remotely and configure the source interface for file transfers depending upon the preferred file transfer protocols.

Use the **Administration** > **Management** > **HTTP/HTTPS/Netconf/VTY** page to configure system-wide settings.

Configuring HTTP/HTTPS Access

HTTP/HTTPS access allows users to access the controller's WebUI using its IP address. You can either allow users to connect securely over HTTPS or over HTTP, which is not a secure connection.

Use the **Administration** > **Management** > **HTTP/HTTPs/Netconf/VTY** page to configure secure access to the controller.

Procedure

Step 1 Enable **HTTP Access** and enter the port that will listen for HTTP requests. The default port is 80. Valid values are 80, and ports between 1025 and 65535.

Step 2 Enable **HTTPS Access** on the device and enter the designated port to listen for HTTPS requests. The default port is 1025. Valid values are 443, and ports between 1025 and 65535.

Enabling HTTPs access allows users to access the controller's GUI using 'https://ip-address' . On a secure HTTP connection, data to and from an HTTP server is encrypted before being sent over the Internet. HTTP

with SSL encryption provides a secure connection to allow such functions as configuring a switch from a Web browser.

Step 3 Enable Personal Identity Verification (PIV) for two factor authentication.

This method of authentication allows users to access the WebUI using Personal Identity Verification (PIV) compatible smart cards, enabling login without password. For this to work, ensure that you have configured the trustpoint, CA server certificate on the device and the client certificate signed by the CA server on the browser. Failure to provide the client certificate would deny access to the UI.

Step 4 Set the **Personal Identity Verification Authorization only** option to *Enabled* for authorizing a user's permissions and restrictions based on a remote TACACS+/RADIUS security server.

Step 5 Click **Apply** to save the configuration.

Note In order to use Personal Identity Verification (PIV) for two factor authentication on Safari, perform the following steps.

a. Open Safari browser and go to **Settings > Advanced**

1. Check the **Show Develop in menu bar** check box. This enables the Develop option in the top menu bar.
2. Click **Develop**, and from the dropdown, select **Empty Caches**.

b. Open the web url to login.

Configuring HTTP Trust Point

Certificate authorities (CAs) manage certificate requests and issue certificates to participating network devices. These services provide centralized security key and certificate management for the participating devices. Specific CA servers are referred to as trustpoints. When a connection attempt is made, the HTTPS server provides a secure connection by issuing a certified X.509v3 certificate, obtained from a specified CA trustpoint, to the client. The client (usually a Web browser), in turn, has a public key that allows it to authenticate the certificate. For secure HTTP connections, we highly recommend that you configure a CA trustpoint. If a CA trustpoint is not configured for the device running the HTTPS server, the server certifies itself and generates the needed RSA key pair. Because a self-certified (self-signed) certificate does not provide adequate security, the connecting client generates a notification that the certificate is self-certified, and the user has the opportunity to accept or reject the connection. This option is useful for internal network topologies (such as testing). If you do not configure a CA trustpoint, when you enable a secure HTTP connection, either a temporary or a persistent self-signed certificate for the secure HTTP server (or client) is automatically generated. If the device is not configured with a hostname and a domain name, a temporary self-signed certificate is generated. If the switch reboots, any temporary self-signed certificate is lost, and a new temporary new self-signed certificate is assigned. If the device has been configured with a host and domain name, a persistent self-signed certificate is generated. This certificate remains active if you reboot the device or if you disable the secure HTTP server so that it will be there the next time you re-enable a secure HTTP connection.

Use the **Trust Point Configuration**section of the **Administration** > **Management** > **HTTP/HTTPs/Netconf/VTY** page to make these changes.

Before you begin

You must have configured a trustpoint for web administration purposes.

Procedure

Step 1 Tap to enable the Trust Point.

Step 2 Select the appropriate Trust Point from the drop-down list to to be used for web admin purpose.

If you have not configured a trust point earlier, you can navigate to the appropriate page and first configure it.

Step 3 Click **Apply** to save the configuration.

Configuring Netconf Yang

NETCONF provides a mechanism to install, manipulate, and delete the configuration of network devices.

If the NETCONF connection is configured to use AAA for authentication purposes, it uses only the default Method List and cannot be pointed to use any other named Method List.

Use the **Netconf Yang Configuration** section of the **Administration** > **Management** > **HTTP/HTTPs/Netconf/VTY** page to make these changes.

Procedure

Step 1 Enable NETCONF.

Step 2 Enter the SSH port number that will be used to facilitate communication between a client and a server. The default port is 830.

Step 3 Click **Apply** to save the configuration.

Configuring Timeout Policy

The Timeout Policy Configuration allows you to configure the details of the interval that the management sessions can remain idle before they timeout. Once the time value is reached, you must log in again to be able to reestablish the connection.

Use the **Timeout Policy Configuration** section of the **Administration** > **Management** > **HTTP/HTTPs/Netconf/VTY** page to make these changes.

Procedure

Step 1 Enter the maximum number of seconds a connection to the HTTP server should remain open before they timeout in the **HTTP Timeout-policy** field. Once the time value is reached, you must log in again to be able to reestablish connection.

Step 2 Enter the maximum number of seconds the connection will be kept open if no data is received or if response data cannot be sent out on the connection in the **Session Idle Timeout**field

Note that a new value may not take effect on any already existing connections. If the server is too busy or the limit on the life time or the number of requests is reached, the connection may be closed sooner. The default value is 180 seconds (3 minutes).

Step 3 Enter the maximum number of seconds the connection will be kept open, from the time the connection is established in the **Server Life Time** field.

Note that the new value may not take effect on any already existing connections. If the server is too busy or the limit on the idle time or the number of requests is reached, it may close the connection sooner. Also, since the server will not close the connection while actively processing a request, the connection may remain open longer than the specified life time if processing is occurring when the life maximum is reached. In this case, the connection will be closed when processing finishes. The default value is 180 seconds (3 minutes). The maximum value is 86400 seconds (24 hours).

Step 4 Enter a value for the maximum limit on the number of requests processed on a persistent connection before it is closed in the **Max Number of Requests** field.

Note that the new value may not take effect on already existing connections. If the server is too busy or the limit on the idle time or the life time is reached, the connection may be closed before the maximum number of requests are processed. The default value is 1. The maximum value is 86400.

Step 5 Click **Apply** to save the configuration.

Configuring VTY

VTY is a virtual port used for Telnet or SSH access to the device. VTY is solely used for inbound connections to the device. You can configure the number of simultaneous connections to your device and add security to validate these connections.

Use the **VTY**section of the **Administration** > **Management** > **HTTP/HTTPs/Netconf/VTY** page to make these changes.

Procedure

Step 1 Set the number of vty lines to allow the number of simultaneous access to the device remotely.

Virtual Terminal Lines or Virtual TeleType (VTY) is a virtual way of accessing the controller 's CLI remotely, unlike physically connecting a laptop to the controller though a console. The number of VTY lines is the maximum number of simultaneous connections possible. 0-50 allows up to fifty simultaneous telnet or ssh sessions to the controller. Although the default is set at 15, we recommend that you to increase the number of VTY lines to 50 to avoid a disruption in connectivity when there are multiple connections to the device.

Step 2 Select the protocol for the remote connection from the **VTY Transport Mode** drop-down list. You can split the connections based on protocol. For e.g. 0-5 might allow for SSH and 10-20 might allow Telnet.

Step 3 (Optional) You can add security in the WebUI to validate login requests. To configure AAA authentication and authorization for inbound sessions to vty lines on your system you must first configure a Radius or a TACACS+ authentication server and select the authentication and authorization list from the corresponding drop-downs.

Step 4 Click **Apply** to save the configuration.