Configuring General Settings

Configuring HTTPS Access

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.

Step 1 Check the **HTTPS Access** check box to enable HTTPS 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. 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 2 In the **Trust Point Configuration** section, check the **Enable Trust Point** check box to use Certificate Authority servers as trustpoints.

Step 3 To keep track of hosts connecting to the device, check the **IP Device Tracking** check box.

Step 4 In the **Timeout Policy Configuration** section, enter the number of minutes of inactivity allowed before the session times out.

Step 5 Enter the server life time in seconds. Valid values can range from 1 to 86400 seconds.

Step 6 Enter the maximum number of requests the device can accept. Valid values range from 1 to 86400 requests.

Step 7 Click **Apply**.

Upgrading Device Software

Use the **General Settings > Software Upgrade** page to upgrade the software image on your device.

Step 1 Depending on whether you want to update only the WebUI image or the IOS bundle and WebUI image on your device, select the software from the **File Type** drop-down list.

Step 2 Browse to locate the file on your local device.

Step 3 Click **Start Update** to update the image.

Step 4 Click **Restart Switch** to boot your device after the device has been updated with the image.

Configuring System Settings

Setting Time Manually

Step 1 Choose **General Settings > System > Time > System Time**.

Step 2 In the **Set Date** and **Set Time** fields, set the date and the time for your device. This will override the time and date received from the NTP server (if configured).

Step 3 Choose the time zone associated with the location of the device.

Step 4 Coordinated Universal Time (UTC) is the 24-hour time standard and the basis for civil time today. Based on the time zone you selected, in the **Set Offset Hours** and **Set Offset Minutes** field, enter the number of hours and the number of minutes by which you want it offset from UTC, to arrive at your local time. For example, the offset for PST is -8 hours.

Step 5 Toggle to enable or disable **Daylight Savings Time**.

Step 6 Click **Apply** to save your changes. The system clock shows the device time and is refreshed every 30 seconds.

Setting Device Time Using NTP

A Network Time Protocol (NTP) network usually gets its time from an authoritative time source such as a radio clock or an atomic clock attached to a time server.

NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two machines to the accuracy of within a millisecond of one another. NTP

uses the concept of a stratum to describe how many NTP hops away a machine is from an authoritative time source. A stratum 1 time server typically has an authoritative time source (such as a radio or atomic clock, or a Global Positioning System (GPS) time source) directly attached, a stratum 2 time server receives its time via NTP from a stratum 1 time server, and so on.

Step 1 On the **General Settings > System > Time > NTP Server** page, click **Add**.

Step 2 Enter the Host name or the IP address of the server you want to add in the **Create NTP Server** window.

Step 3 Select the Interface to associate it with the NTP server. If you selected VLAN, select from the available list of VLANs. If you selected Interface , select the Interface from the drop-down list.

Step 4 Click **Save & Apply to Device**.

Transferring Configuration Files from the Device

Step 1 On the **General Settings > System > Config File** page, click **Add**.

Step 2 From the **Transfer** drop-down list, choose *From Switch*.

Step 3 From the **Src/Dest** drop-down list, choose either *TFTP* Server or a **Local Hard Drive** to indicate the location to which to transfer the configuration file.

Step 4 Type the name of the configuration file and provide the location of the file.

Step 5 If you choose TFTP server as the source, type the IP address of the server.

Step 6 Click **Apply**.

Transferring Configuration Files to the Device

Step 1 On the **General Settings > System > Config File** page, click **Add**.

Step 2 From the **Transfer** drop-down list, choose *To Switch*.

Step 3 From the **Src/Dest** drop-down list, choose either a TFTP server or a local directory to indicate the location from which to transfer the configuration file.

Step 4 Type the name of the configuration file and provide the location of the file.

Step 5 Enter the IP address of the TFTP server.

Step 6 Click **Apply**.

Creating DHCP Scopes

Network segments that do not have a separate DHCP server can have built-in DHCP scopes that assign IP addresses and subnet masks to hosts connecting to the device.

Step 1 Choose **General Settings > System > DHCP**.

Step 2 From the **DHCP Scopes** page, click Add. The **Create DHCP Scope** window is displayed.

Step 3 In the **Basic** section, enter a name for the new DHCP scope in the **DHCP Scope Name** field.

Step 4 In the **Network** field, enter the network served by this DHCP scope. This IP address is used by the management interface, as configured on the Interfaces page.

Step 5 In the **Subnet Mask** field, enter the subnet mask for the network.

Step 6 In the **Lease** fields, enter the amount of time that an IP address is granted to a client.

Step 7 In the **Default Router(s)** fields, type the IP address of the optional router or router(s) that connect to the device. Each router must include a DHCP forwarding agent that enables a single device to serve the clients of multiple devices.

Step 8 In the **Advanced** section, enter the IP address of the optional DNS server(s), in the **DNS Server(s)** field. Each DNS server must be able to update a client's DNS entry to match the IP address assigned by this DHCP scope.

Step 9 In the **NetBios Name Server(s)** field, enter the IP address of the optional Microsoft NetBIOS name servers, such as a Microsoft Windows Internet Naming Service (WINS) server.

Step 10 In the **Domain Name** field, enter the optional domain name of this DHCP scope for use with one or more DNS servers.

Step 11 To add DHCP options, click **Add**, in the **DHCP Options List** section. DHCP provides an internal framework for passing configuration parameters and other control information as DHCP options, to clients on your network. DHCP options carry parameters as tagged data stored within protocol messages exchanged between the DHCP server and its clients.

Step 12 Specify the DHCP option you want to add, and enter the option value.

Step 13 Click **Save**.

Configuring DHCP Excluded Addresses

Use the **General Settings > System > DHCP Excluded Address** section to specify IP addresses (excluded addresses) that the DHCP server should not assign to clients.

The IP address configured on the device interface is automatically excluded from the DHCP address pool. The DHCP server assumes that all other IP addresses in a DHCP address pool subnet are available to DHCP clients. If the DHCP server should not allocate some IP addresses to clients, add the IP addresses to the Excluded Addresses list. For example, if two DHCP servers are set up to service the same network segment (subnet) for redundancy. If the two servers do not coordinate their services with each other using a protocol such as DHCP failover, then each DHCP server must be configured to allocate from a non-overlapping set of addresses in the shared subnet.

Step 1 In the **DHCP Excluded Address** section, enter the IP address that you want to exclude, and the mask of the subnet to which the address belongs.

Step 2 Click **Apply**.

Creating Administrator Usernames and Passwords

You can configure administrator usernames and passwords to prevent unauthorized users from reconfiguring the switch and viewing configuration information.

Guidelines for Settings Passwords

- There should be at least three of the following categories—lowercase letters, uppercase letters, digits, and special characters.
- The new password should not be the same as the associated username or any close variant of the username.
- The characters in the password should not be repeated more than three times consecutively.
- The password should not be cisco, ocsic, admin, nimda, or any variant of the order of letters, or by substituting "1" "|" or "!" for i, and/or substituting "0" for "o", and/or substituting "$" for "s".
- The maximum number of characters accepted for the username and password is 32.

Creating a User Account

Step 1 On the **General Settings > User Administration** page, enter a user name for the new account.

Step 2 Specify the privilege level or you want to associate with the user. The privilege level defines what commands the user can enter using the CLI after they have logged into the device. Privilege 1 allows access in User Exec mode, privilege 15 allows access in Privileged Exec mode. To access the webUI, user should use highest privileged value i.e. 15.

Step 3 Enter a password with which to authenticate access to the device. Enter the password again to confirm it.

Step 4 Click **Done**.