Converged Access: Management

This chapter describes the switch configuration that is required to enable access for Web GUI and Cisco Prime.

You can manage converged access platforms using the following methods:

- Web GUI–A web browser or GUI is built into each switch.
- Cisco Prime–Cisco Network management software
- Simple Network Management Protocol (SNMP)
- CLI

Web GUI Access

The Web GUI uses HTTPS, by default. However, you can configure HTTP access using the **ip http server** command in global configuration mode.

To access the Web GUI, configure an IP address and a user with privilege 15. Configure an IP address on the management port, on a regular interface, or a Switch Virtual Interface (SVI); this IP address should be reachable through the network.

Note For information about configuring IP on the management interface, see Chapter 4, Basic Configuration.

To create a user with privilege level 15 and to use the credentials from an authentication server, use the **username user_name privilege 15 password password** command in global configuration mode.

For Web GUI access, perform the following procedure:

Step 1 Open a browser, type your management IP address, and press **Enter**.

Step 2 Enter the configured username and password.

Step 3 On the Home window, click the **Wireless Web GUI** hyperlink.
The Wireless Web GUI home page is displayed.

Converged Access Web GUI

The Web GUI supports the following features:

- The following tasks can be performed from the Configuration tab:
  - Configure a switch for all initial operations using the web Configuration wizard. The wizard allows you to configure user details, management interface, and so on.
  - Configure system, internal DHCP server, management, and mobility management parameters.
  - Configure the switch, WLAN, and radios.
  - Configure and set security policies on the switch.
  - Access the software management commands of the operating system.

- The Configuration wizard–After the initial configuration of an IP address and a local username and password, or authentication through an authentication server (privilege 15), the wizard provides a method to complete the initial wireless configuration.

  Start the wizard by choosing **Configuration** > **Wizard**, and then configure the following:
  - Admin Users
  - SNMP System Summary
  - Management Port
  - Wireless Management
  - RF Mobility and Country Code
  - Mobility Configuration
  - WLANs
  - 802.11 Configuration
  - Set Time

- The Monitor tab displays the following information:
  - Summary details of switch, clients, and access points.
  - All radio and AP join statistics.

- Air quality on access points.
- List of all the Cisco Discovery Protocol neighbors on all the interfaces and the Cisco Discovery Protocol traffic information.
- All the rogue access points based on their classification — friendly, malicious, ad hoc, classified, and unclassified.

• The Administration tab enables you to configure system logs.

Enabling Cisco Prime

To enable Cisco Prime, enable SNMP.

Enabling SNMP v2

To enable SNMP on a switch, configure SNMPv2 or SNMPv3. You can configure read-only or read-write community strings, depending on the requirement.

To configure a Read Only (RO) SNMP community string, use the following command:

```
Device# configure terminal
Device(config)# snmp-server community name RO
Device(config)# end
```

To configure a Read Write (RW) SNMP community string, use the following command:

```
Device# configure terminal
Device(config)# snmp-server community name RW
Device(config)# end
```

To check the SNMP community string, use the following command:

```
Device# show running-config | in snmp-server community
```

Enabling SNMP v3

To enable SNMP v3, perform the following procedure:

Step 1 To create a new group and select a security model, use the following commands:

```
Device# configure terminal
Device(config)# snmp-server group grp-name v3 privilege write write_name
Device(config)# end
```

Step 2 To create a user account, use the following commands:

```
Device# configure terminal
Device(config)# snmp-server user user-name-grp-name v3 auth md5 password privilege aes 128 password
Device(config)# end
Configuring snmpv3 USM user, persisting snmpEngineBoots. Please Wait...
```

Step 3 To verify SNMPv3 configuration, use the following commands:

```
Device# show running-config | in snmp-server group
Device# show snmp user
Device# show snmp group
```