Booting the Controller and Accessing the Console

Day 0 WebUI Wizard for Public Cloud

Perform the following procedure to create a Day 0 configuration and push it to the controller:

Step 1 In the address bar of a web browser, enter the **IP address** of the controller.

Step 2 Enter the **Username** and **Password**.

The **Configuration Setup Wizard** window is displayed.

Enter the following details in the **General Settings** window:

a) Choose the **Deployment Mode**.
b) Choose the **Country**.
c) Choose the **Date**.
d) Enter the **Time** or choose the **Timezone** using the drop down list.
e) Enter the **NTP Servers** name.
f) Enter the **AAA Servers** name.

Step 3 Enter the **Wireless Management Settings**:

a) Choose **Port Number**.
b) Choose **IP Address**.

Step 4 Click **Next**.

Step 5 Enter the **Wireless Network Settings**:

a) Enter a **Network Name**.
b) Select the **Network Type**.
c) Select the **Security** option using the drop-down.
d) Enter the **Pre-Shared Key**.

e) Click **Add**.

Note Enter three wireless network settings, one for wireless management, another for device management and one more for guest management.

Step 6 Click **Next**.

This opens the Advanced Settings page.

Step 7 Enter the details in **Advanced Settings** page.

a) Select the **Client Density** using the slider.
b) Enter the **RF Group Name**.
c) Use the drop-down to select **Traffic Type**.
d) Enter the **Virtual IP Address**.
e) Use the **Generate Certificate** slider to generate certificates for APs.

This certificate is required for APs to join the controller.

f) Select the **RSA Key-Size** from the drop-down list.
g) Enter the **Signature Algorithm**.
h) Enter the **Password**.
i) Review the details in the **Summary** page.

Step 8 Click **Finish**.

Step 9 Click **Yes**.

This creates the configuration and pushes it to the controller.

Day 0 WebUI Wizard for Private Cloud

Perform the following procedure to create a Day 0 configuration and push it to the controller:

Step 1 In the address bar of a web browser, enter the **IP address** of the controller.

Step 2 Enter the **Username** and **Password**.

The **Configuration Setup Wizard** window is displayed.

Enter the details in the **General Settings** window.

a) Choose the **Deployment Mode**.
b) Choose the **Country**.
c) Choose the **Date**.
d) Enter the **Time** or choose the **Timezone** from the drop-down list.
e) Enter the **NTP Servers** name.
f) Enter the **AAA Servers** name.

Step 3 Enter the **Service Port Settings**:

a) Choose **DHCP**.
b) Enter the **Static IP** address.

c) Enter the **Subnet Mask**.

Step 4 Enter the **Static Route Settings (Optional)**:

a) Enter the **IP Address**.
b) Enter the **Subnet Mask**.
c) Enter the **Gateway** address.

Step 5 Enter the **Wireless Management Settings**:

a) Choose **Port Number**.
b) Enter the **VLAN**.
c) Choose **IPv4** or **IPv6**.
d) Enter the **Wireless Management IP** address.
e) Enter the **Subnet Mask**.
f) Enter the **Management VLAN DHCP Server**.

Step 6 Click **Next**.

This opens the **Wireless Network Settings** page.

Step 7 Enter the **Wireless Network Settings**:

a) Enter a **Network Name**.
b) Select the **Network Type**.
c) Select the **Security** option using the drop-down.
d) Enter the **Pre-Shared Key**.
e) Click **Add**.

Note Enter three wireless network settings, one for wireless management, another for device management and one more for guest management.

Step 8 Click **Next**.

The **Advanced Settings** page is displayed.

Step 9 Enter the details in **Advanced Settings** page.

a) Choose the **Client Density** using the slider.
b) Enter the **RF Group Name**.
c) Choose the **Traffic Type** from the drop-down list.
d) Enter the **Virtual IP Address**.
e) Enter the **Local IP**, **Subnet Mask**, **Remote IP** for High Availability.

Note Available only when the deployment mode is set to ACTIVE.

f) Use the **Generate Certificate** slider to generate certificates for APs.

This certificate is required for APs to join the controller.

g) Choose **RSA Key-Size** from thr drop-down list.
h) Enter the **Signature Algorithm**.
i) Enter the **AP password**.
j) Review the details in the **Summary** page.

Step 10 Click **Finish**.

Step 11 Click **Yes**.

This creates the configuration and pushes it to the controller.

Booting the Controller

The controller boots when the VM is powered on. Depending on your configuration, you can monitor the installation process on the virtual VGA console.

Perform the following procedure to boot the controller:

1. Power up the VM. Within 5 seconds of powering up the VM, choose a console described from Step 2 to Step 4 to view the device's bootup and to access the controller CLI.
2. (Optional) Click **Auto Console** to use automatic console detection. This is the default setting, and the controller will boot using automatic console detection if another option is not selected within 5 seconds.
3. (Optional) Click **Virtual Console** to use the virtual VGA console. If you choose to use the virtual console, the rest of the steps in this procedure do not apply. The controller starts the boot process.
4. Use one of the following commands to Telnet to the VM:
   - **telnet:**//*host-ipaddress:portnumber*
   - **telnet***host-ipaddress portnumber* (from a UNIX xTerm terminal)
5. After booting, the system displays the main software image and the Golden image, with an instruction that the highlighted entry is booted automatically in 3 seconds. Do not select the option for the Golden image, and allow the main software image to boot.

Note While doing backup restore of configs, make sure you do not have **platform console serial**, as it could make the controller boot into grub mode and recovery is not possible.

Accessing the Controller Through the Virtual VGA Console

You will be prompted for wireless configuration after the Day 0 banner.

For information on modifying the configuration after you create it, see the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide and the Cisco Catalyst 9800 Series Wireless Controller Command Reference Guide.

This section covers the following:

- Configuring the device management interface.
- Configuring the device management IP.
- [Optional] Setting a static route.

- Configuring the management credentials.
- Configuring the wireless management interface.
- Choosing the deployment mode.
- Configuring the system name or hostname.
- Configuring credentials for management access on access points.
- Configuring the country code.
- Configuring the time using an NTP server or manually.
- [Optional] Configuring a time zone.
- [Optional] Configuring the wireless client density.
- [Optional] Configuring AAA servers.
- [Optional] Configuring the wireless network settings.
- [Optional] Configuring a network name or SSID.
- [Optional] Configuring a virtual IP.
- [Optional] Configuring an RF network name.
- [Optional] Configuring a self-signed certificate.
- [Optional] Configuring high avalability.

Note Presently, there is no direct method to get back to your previous configuration. Press **Ctrl-C** to restart the configuration and return to the setup without saving the configuration.

Day 0 CLI Wizard for the Controller

Step 1 You can get into the Day 0 setup wizard using the **write erase** command or directly on the Day 0 device.

Step 2 Device management interface setup configures the device management or service port. This interface enables the basic configuration to access the device using the GUI. This is an optional configuration where you can opt to configure only the wireless management interface and not the device management.

```
Configure device management interface?[yes]:
```

Note There is no dedicated device management port for Cisco Catalyst 9800-CL Cloud Wireless Controller. So, you are prompted to select one of the options from the given range.

```
Select interface to be used for device management
1. GigabitEthernet1 [Up]
2. GigabitEthernet2 [Up]
3. GigabitEthernet3 [Up]
Choose the interface to config [1]:
```

Step 3 Device management IP helps access the device using the GUI.

```
 Configure static IP address? [yes]:
    Enter the interface IP [GigabitEthernet1]: 192.168.1.10
    Enter the subnet mask [GigabitEthernet1] [255.0.0.0]: 255.255.255.0
```

Step 4 [Optional] Setting a static route to access the device using the GUI.

```
Configure static route? [yes]:
Enter the destination prefix: 192.168.1.0
Enter the destination mask: 255.255.255.0
Enter the forwarding router IP: 192.168.1.1
```

Step 5 Enter the management username and password. This is a mandatory step.

```
Enter the management username: cisco
  Enter the password: ********
  Reenter the password: ********
```

Step 6 Configure the wireless management if you haven't configured a device management interface.

```
Basic management setup is now complete. At this point, it is possible to save the above and
continue wireless setup using the webUI (for this, choose 'no' below)

Would you like to continue with the wireless setup? [yes]: yes
```

Note This prompt is not applicable for 17.4 release.

Note If you have not configured the device management, the setup moves to **Step 7** before displaying the above banner.

In 17.3 release, you will be allowed to exit the wizard after configuring at least one of the interfaces, that is, device or wireless management.

This banner is no longer available in 17.4. You cannot exit the wizard without completing the configuration.

If you select **Yes**, you need to follow the upcoming steps. Also, you can access the device using the IP configured in **Step 4**.

Step 7 Wireless management interface is a mandatory configuration:

```
Configuring wireless management interface
  Select interface to be used for wireless management
   1. GigabitEthernet2 [Up]
   2. GigabitEthernet3 [Up]
  Choose the interface to config [1]:
```

Note If GigabitEthernet1 is used for device management interface then the remaining GigabitEthernet interfaces will be displayed.

Step 8 Enter a VLAN ID:

```
Enter the vlan ID (1-4094): 112
```

Step 9 Configure an IPv4 or IPv6 address:

```
  Configure IPv4 address? [yes]:
```

```
    Enter the interface IP [GigabitEthernet1]: 9.11.112.40
    Enter the subnet mask [GigabitEthernet1] [255.0.0.0]: 255.255.255.0
  Configure IPv6 address? [yes]: no
```

Step 10 Configure a VLAN DHCP server and IP address:

```
 Do you want to configure a VLAN DHCP Server? [yes]: yes
   Enter the VLAN DHCP Server IP [GigabitEthernet1]: 9.11.112.45
```

Step 11 [Optional] Setting a static route to attach an AP client to the controller. The default options for static route prompts you to configure a default route. However, you can specify a different route as well.

```
 Configure static route? [yes/no]: yes
  Enter the destination prefix [0.0.0.0]:
  Enter the destination mask [0.0.0.0]:
  Enter the forwarding router IP: 9.11.112.1
```

Note If you configure the device as HA RMI and you haven't configured a default route (that is, source and destination as 0.0.0.0), the wizard asks for the default route information.

```
Basic management setup is now complete. At this point, it is possible to save the above and
continue wireless setup using the webUI(for this, choose 'no' below)

Would you like to continue with the wireless setup? [yes]
```

Step 12 Choose the deployment mode:

```
 Choose the deployment mode
    1. Standalone
    2. Active
    3. Standby
 Enter your selection [1]:
```

Note You can choose from one of the following deployment modes:

- **Standalone**: In this mode, you do not get to view any high availability pairing information.
- **Active**: In this mode, the controller needs to be configured with all the Day 0 information.
- **Standby**: In this mode, the configuration proceeds to the **High Availability** configuration.

Step 13 Configure the system name or hostname:

```
Enter the hostname [WLC]: ciscowlc
```

Note This is a mandatory step. The hostname needs to confirm to the RFC standards.

Step 14 [Optional] Configure the login credentials for an AP.

```
Configure credentials for management access on Access Points? [yes]:
  Enter the management username: cisco
  Enter the management password: ****
    Reenter the password: ****
  Enter the privileged mode access password: ****
    Reenter the password: ****
```

Step 15 Configure the country code. You can specify multiple country codes by separating them with a comma.

```
Configure country code for wireless operation in ISO format ? [US]:
```

Step 16 Configure the date and NTP to allow access points to join the controller. You can configure time using an NTP server or manually.

Note Enter the date in the following format:

MM/DD/YYYY

```
Configure a NTP server now ? [yes]: no

Configure the system time now? [yes]: yes

Enter the date in MM/DD/YYYY format: 10/05/2021
Enter the time in HH:MM:SS format: 10:22:13
```

Step 17 [Optional] Configure a timezone:

```
 Configure timezone? [yes]:
  Enter name of timezone: ind
  Enter hours offset from UTC (-23,23): 5
  Enter mins offset from UTC (0,59) [0]: 30
```

Step 18 [Optional] Configure the expected client density:

```
 Configure Wireless client density? [yes]:
  Choose the client density
    1. Low
    2. Typical
    3. High
  Enter your selection [2]: 3
```

Step 19 [Optional] Configure AAA servers:

Note You can configure a maximum of 6 servers during Day 0 configuration.

```
 Configure AAA servers? [yes]:
  Enter the AAA server address: 9.11.112.46
  Enter the AAA key: ***
Do you want to add more AAA servers? [yes]:
  Enter the AAA server address: 9.11.112.47
  Enter the AAA key: ***
Do you want to add more AAA servers? [yes]: no
```

Note The AAA servers are required for WPA2 Enterprise. In 17.4 release, you need to configure AAA only in one place. If you follow **Step 21**, WPA2 Enterprise will not ask for AAA servers in **Step 22**.

Step 20 [Optional] Configure wireless network settings to configure WLAN information for an AP and client join:

```
Configure Wireless network settings? [yes]:
```

Step 21 [Optional] Configure an SSID for client join:

```
Enter the network name or service set identifier (SSID):
Choose the network type
    1. Employee
    2. Guest
```

If you choose **Employee** as the network type, the following options are displayed:

```
Choose the security type
    1. WPA Personal
    2. WPA Enterprise
   Enter your selection [2]:
```

If you choose **WPA2 Personal**, you will need to enter a pre-shared key (ASCII).

```
Enter the pre-shared key (ASCII):
```

If you choose **WPA2 Enterprise**, you will be able to add multiple AAA servers.

```
Enter the AAA server address:
Enter the AAA key:
Enter more AAA server details? [yes]
```

If you choose **Guest**, you get to view the following options:

```
Please choose the security type:
1. Webauth
2. Authbypass
3. Consent
4. Webconsent
Enter the security type:
```

Step 22 [Optional] Configure a virtual IP address. The default virtual IP address is 192.0.6.1.

```
 Configure virtual IP? [yes]:
  Enter the virtual IP [192.0.6.1]:
```

Step 23 [Optional] Configure an RF network name.

```
 Configure RF-Network Name? [yes]:
  Enter the RF-Network Name: ciscorf
```

Step 24 [Optional] Configure a self-signed certificate.

```
Auto generate certificate for AP join? [yes]:
Choose key size
1.2048
2.3072
3.4096
Enter your selection [1]:
Choose the signature algorithm
1.SHA256
2.SHA384
Enter your selection [1]:
Enter secret key(minimum 8 characters): ********
Self Signed Certificate generation will be done after system boots up.
```

Step 25 [Optional] Configure high availability.

If you choose the deployment mode as Active or Standby, you will need to choose from one of the HA pairing type:

a. RMI

b. RP-RP

Note For information on HA pairing types, see **Part: High Availability (High Availability > Information About Redundancy Management Interface)** in *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.4.x*.

```
High Availability configuration
 Please choose the HA pairing type
   1. RMI
   2. RP-RP
 Enter your selection [1]:
```

If you choose RMI+RP, you need to select an interface to be used as redundancy port:

```
Select interface to be used as redundancy port
  1. GigabitEthernet3 [Up]
 Choose the interface to config [1]: 2
 Enter the RMI IP for local chassis: 9.11.112.50
 Enter the RMI IP for remote chassis: 9.11.112.51
 Enter the gateway IP of the last resort: 9.11.112.1
```

If you choose the deployment mode as Standby, you need to specify the VLAN ID for completing the pairing:

```
 Enter the RMI IP for local chassis: 9.11.112.51
 Enter the RMI IP for remote chassis: 9.11.112.50
 Enter the wireless management VLAN: 112
```

If you choose RP, you need to select an interface to be used as redundancy port:

```
Select interface to be used as redundancy port
  1. GigabitEthernet3 [Up]
 Choose the interface to config [1]: 2
 Enter the local IP:
Enter the subnet mask:
Enter the remote IP:
```

Note It is recommended to use GigabitEthernet1 for device managemt interface, GigabitEthernet2 for wireless management interface, and GigabitEthernet3 for HA.