



Configuring the Management Interface

- [Management Interface, on page 1](#)
- [Configuring the Management Interface \(GUI\), on page 2](#)
- [Configuring the Management Interface \(CLI\), on page 3](#)

Management Interface

The management interface is the default interface for in-band management of the controller and connectivity to enterprise services such as AAA servers. It is also used for communications between the controller and access points, for all CAPWAP or intercontroller mobility messaging and tunneling traffic. You can access the GUI of the controller by entering the management interface IP address of the controller in the address field of your browser. The AP management is enabled by default on the management interface.

For CAPWAP, the controller requires one management interface to control all inter-controller communications and one AP-manager interface to control all controller-to-access point communications, regardless of the number of ports.



Note

To prevent or block a wired or wireless client from accessing the management network on a controller (from the wireless client dynamic interface or VLAN), the network administrator should ensure that only authorized clients gain access to the management network through proper CPU ACLs, or use a firewall between the client dynamic interface and the management network.



Caution

Do not map a guest WLAN to the management interface. If the EoIP tunnel breaks, the client could obtain an IP and be placed on the management subnet.

In a High Availability environment with Release 8.0 or a later release, ensure that the management interface and the redundancy management interface (RMI) are tagged for the HA-SSO to work as expected.

This section contains the following subsections:

Configuring the Management Interface (GUI)

Step 1 Choose **Controller > Interfaces** to open the Interfaces page.

Step 2 Click the management link.

The **Interfaces > Edit** page appears.

Step 3 Set the management interface parameters:

Note The management interface uses the controller's factory-set distribution system MAC address.

- Quarantine and quarantine VLAN ID, if applicable
- NAT address (only Cisco 2504 and 5508 controllers are configured for dynamic AP management.)

Note Check the **Enable NAT Address** check box and enter the external NAT IP address if you want to be able to deploy your Cisco 2504 and 5508 controllers behind a router or other gateway device that is using one-to-one mapping network address translation (NAT). NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller's intranet IP addresses to a corresponding external address. The controller's dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

Note If a Cisco 2504 or 5508 controller is configured with an external NAT IP address under the management interface, the APs in local mode cannot associate with the controller. The workaround is to either ensure that the management interface has a globally valid IP address or ensure that external NAT IP address is valid internally for the local APs.

Note The NAT parameters are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. The NAT parameters do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

- VLAN identifier

Note Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface.

- Configuring Management Interface using IPv4—Fixed IP address, IP netmask, and default gateway.

- Configuring Management Interface using IPv6—Fixed IPv6 address, prefix-length (interface subnet mask for IPv6) and the link local address of the IPv6 gateway router.

Note

- In a setup where IPv6 is used, we recommend the APs to be at least one hop away from the controller. As the IPv6 packets are always sent to the Gateway, if the AP and controller are in the same subnet, it increases the packet hops and impacts the performance.
- Once the primary IPv6 Address, prefix length, and primary IPv6 gateway are configured on the management interface, they cannot be changed back to default values (:: /128).
- In a setup where IPv6 CAPWAP is used, we recommend that the APs are at least 1 hop away from the controller because all IPv6 traffic is first forwarded to the gateway.
- A configuration backup must be carried out before configuring IPv6 in case the user wants to revert back to IPv4 only management interface.
- When more than 1300 IPv6 APs are in use, on a single Catalyst 6000 Switch, then assign APs on multiple VLANs.

- Dynamic AP management (for Cisco 2504 or 5508 controllers only)

Note

For Cisco 5508 controllers, the dynamic AP management parameter is enabled by default. If needed, this function can be disabled on the management interface and enabled for another dynamic interface.

- Physical port assignment (for all controllers except the Cisco 2504 or 5508 controllers)
- Primary and secondary DHCP servers
- Access control list (ACL) setting, if required

Step 4 Click **Save Configuration**.

Step 5 If you made any changes to the management or virtual interface, reboot the controller so that your changes take effect.

Configuring the Management Interface (CLI)

Step 1 Enter the **show interface detailed management** command to view the current management interface settings.

Note The management interface uses the controller's factory-set distribution system MAC address.

Step 2 Enter the **config wlan disable wlan-number** command to disable each WLAN that uses the management interface for distribution system communication.

Step 3 Enter these commands to define the management interface:

a) **Using IPv4 Address**

- **config interface address management ip-addr ip-netmask gateway**
- **config interface quarantine vlan management vlan_id**

Note

Use the **config interface quarantine vlan management vlan_id** command to configure a quarantine VLAN on the management interface.

- **config interface vlan management {vlan-id | 0}**

Note Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface.

- **config interface ap-manager management {enable | disable}**

Note Use the **config interface ap-manager management {enable | disable}** command to enable or disable dynamic AP management for the management interface. For Cisco 5508 controllers, the management interface acts like an AP-manager interface by default. If required, you can disable the management interface as an AP-manager interface and create another dynamic interface as an AP manager.

- **config interface port management primary-port [secondary-port]** (for all controllers except the 5508 controller)
- **config interface dhcp management ip-address-of-primary-dhcp-server [ip-address-of-secondary-dhcp-server]**
- **config interface acl management access-control-list-name**

b) Using IPv6 Address

Note we recommend the APs to be at least one hop away from the controller. As the IPv6 packets are always sent to the Gateway, if the AP and controller are in same subnet, it increases the packet hops and impacts the performance.

- **config ipv6 interface address management primary ip-address prefix-length IPv6_Gateway_Address**

Note Once the Primary IPv6 Address, Prefix Length, and Primary IPv6 Gateway are configured on the management interface, they cannot be changed back to default values (::/128). A configuration backup must be carried out before configuring IPv6 in case the user wants to revert back to IPv4 only management interface.

- **config interface quarantine vlan management vlan_id**

Note Use the **config interface quarantine vlan management vlan_id** command to configure a quarantine VLAN on the management interface.

- **config interface vlan management {vlan-id | 0}**

Note Enter 0 for an untagged VLAN or a nonzero value for a tagged VLAN. We recommend using tagged VLANs for the management interface.

- **config interface ap-manager management {enable | disable}**

Note Use the **config interface ap-manager management {enable | disable}** command to enable or disable dynamic AP management for the management interface. For Cisco 5508 WLCs, the management interface acts like an AP-manager interface by default. If desired, you can disable the management interface as an AP-manager interface and create another dynamic interface as an AP manager.

- **config interface port management physical-ds-port-number** (for all controllers except the 5508 WLC)
- **config interface dhcp management ip-address-of-primary-dhcp-server [ip-address-of-secondary-dhcp-server]**
- **config ipv6 interface acl management access-control-list-name**

Step 4 Enter these commands if you want to be able to deploy your controller behind a router or other gateway device that is using one-to-one mapping network address translation (NAT):

- **config interface nat-address management {enable | disable}**
- **config interface nat-address management set public_IP_address**

NAT allows a device, such as a router, to act as an agent between the Internet (public) and a local network (private). In this case, it maps the controller's intranet IP addresses to a corresponding external address. The controller's dynamic AP-manager interface must be configured with the external NAT IP address so that the controller can send the correct IP address in the Discovery Response.

Note These commands are supported for use only with one-to-one-mapping NAT, where each private client has a direct and fixed mapping to a global address. These commands do not support one-to-many NAT, which uses source port mapping to enable a group of clients to be represented by a single IP address.

Step 5 Enter the **save config** command.

Step 6 Enter the **show interface detailed management** command to verify that your changes have been saved.

Step 7 If you made any changes to the management interface, enter the **reset system** command to reboot the controller in order for the changes to take effect.
