Information About the 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. The management interface has the only consistently "pingable" in-band interface IP address on the controller. 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.

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.

If the service port is in use, the management interface must be on a different supernet from the service-port interface.

---

**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 must 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.
Do not configure wired clients in the same VLAN or subnet of the service port of the controller on the network. If you configure wired clients on the same subnet or VLAN as the service port, it is not possible to access the management interface of the controller.

**Caution**

Authentication Type for Management Interfaces

For any type of management access to the controller, be it SSH, Telnet, or HTTP, we recommend that you use any one authentication type, which can be TACACS+, RADIUS, or Local, and not a mix of these authentication types. Ensure that you take care of the following:

- Authentication type (TACACS+, RADIUS, or Local), must be the same for all management access and for all AAA authentication and authorization parameters.
- The method list must be explicitly specified in the HTTP authentication.

**Example**

Follow these steps to configure Telnet:

1. Configure TACACS+ server by entering these commands:
   - `tacacs server server-name`
   - `address ipv4 ip-address`
   - `key key-name`

2. Configure the server group name by entering these commands:
   - `aaa group server tacacs+ group-name`
   - `server name name`

3. Configure authentication and authorization by entering these commands:
   - `aaa authentication login method-list group server-group`
   - `aaa authorization exec method-list group server-group`

**Note**

These and all the other authentication and authorization parameters must be using the same database, be it RADIUS, TACACS+, or Local. For example, if command authorization has to be enabled, it also needs to be pointing to the same database.

4. Configure HTTP to use the above method lists:

   1. `ip http authentication aaa login-auth method-list`
      
         You must explicitly specify the method list, even if the method list is "default".

   2. `ip http authentication aaa exec-auth method-list`
• Do not configure any method-lists on the "line vty" configuration parameters. If the above steps and the line vty have different configurations, then line vty configurations take precedence.

• The database should be the same across all management configuration types such as SSH/Telnet and webui.

• You must explicitly define the method list for HTTP authentication.

Workaround

As a workaround, enter the following commands:

1. `aaa authentication login default group server-group local`
2. `aaa authorization exec default group server-group local`

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:

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

  • Quarantine and quarantine VLAN ID, if applicable

  Note Select the Quarantine check box if you want to configure this VLAN as unhealthy or you want to configure network access control (NAC) out-of-band integration. Doing so causes the data traffic of any client that is assigned to this VLAN to pass through the controller.

  • NAT address (only Cisco 2500 Series Controllers and Cisco 5500 Series Controllers are configured for dynamic AP management.)

  Note Select the Enable NAT Address check box and enter the external NAT IP address if you want to be able to deploy your Cisco 2500 Series Controllers or Cisco 5500 Series Controller 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 2500 Series Controllers or Cisco 5500 Series 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
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 Cisco WLC. As the IPv6 packets are always sent to the Gateway, if the AP and WLC 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).
- 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.
- In 8500 controller running a ha-pair, IPv6 primary gateway (link local) configured though 3600 AP joined with the IPv6 address tears down the capwap. Using the command test capwap though the AP joined with ipv6 address, it is seen that when the Link local address is not reachable capwap should not be formed.
  - If APs are joined on V6 tunnel and if IPv6 gateway is misconfigured then v6 tunnel will not be teared down. The APs will still be on v6 tunnel and will not fall back to v4 tunnel.

- Dynamic AP management (for Cisco 2500 Series Controllers or Cisco 5500 Series Controller only)

Note

- For Cisco 5500 Series Controllers, 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.
- Physical port assignment (for all controllers except the Cisco 2500 Series Controllers or Cisco 5500 Series Controller)
- 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}` (for Cisco 5500 Series Controllers only)  
  
  **Note** Use the `config interface ap-manager management {enable | disable}` command to enable or disable dynamic AP management for the management interface. For Cisco 5500 Series Controllers, 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 5500 series)

- `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 Cisco WLC. As the IPv6 packets are always sent to the Gateway, if the AP and WLC are in the 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}` (for Cisco 5500 Series Controllers only)  
  
  **Note** Use the `config interface ap-manager management {enable | disable}` command to enable or disable dynamic AP management for the management interface. For Cisco 5500 Series Controllers, 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 5500 series)
• 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 Cisco 5500 Series 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.