



IP Theft

- [Introduction to IP Theft, on page 1](#)
- [Configuring IP Theft \(GUI\), on page 2](#)
- [Configuring IP Theft, on page 2](#)
- [Configuring the IP Theft Exclusion Timer, on page 2](#)
- [Adding Static Entries for Wired Hosts, on page 3](#)
- [Verifying IP Theft Configuration, on page 4](#)

Introduction to IP Theft

The IP Theft feature prevents the usage of an IP address that is already assigned to another device. If the controller finds that two wireless clients are using the same IP address, it declares the client with lesser precedence binding as the IP thief and allows the other client to continue. If blocked list is enabled, the client is put on the exclusion list and thrown out.

The IP Theft feature is enabled by default on the controller. The preference level of the clients (new and existing clients in the database) are also used to report IP theft. The preference level is a learning type or source of learning, such as Dynamic Host Configuration Protocol (DHCP), Address Resolution Protocol (ARP), data glean (looking at the IP data packet that shows what IP address the client is using), and so on. The wired clients always get a higher preference level. If a wireless client tries to steal the wired IP, that client is declared as a thief.



Note Some devices might use different MAC addresses but the same IPv6 link-local addresses, for different WLANs. If the devices switch WLANs when they are not in range of the APs, an IP theft event is triggered. To avoid this, we recommend that you lower the idle timeout for the devices. When the devices are out of the APs' range, the idle timeout takes effect and the old entries in the initial WLAN are deleted.

The order of preference for IPv4 clients are:

1. DHCPv4
2. ARP
3. Data packets

The order of preference for IPv6 clients are:

1. DHCPv6
2. NDP
3. Data packets



Note The static wired clients have a higher preference over DHCP.

Configuring IP Theft (GUI)

Procedure

-
- Step 1** Choose **Configuration > Security > Wireless Protection Policies > Client Exclusion Policies**.
 - Step 2** Check the **IP Theft or IP Reuse** check box.
 - Step 3** Click **Apply**.
-

Configuring IP Theft

Follow the procedure given below to configure the IP Theft feature:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless wps client-exclusion ip-theft Example: Device(config)# wireless wps client-exclusion ip-theft	Configures the client exclusion policy.

Configuring the IP Theft Exclusion Timer

Follow the procedure given below to configure the IP theft exclusion timer:

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wireless profile policy <i>profile-policy</i> Example: Device(config)# wireless profile policy default-policy-profile	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	exclusionlist timeout <i>time-in-seconds</i> Example: Device(config-wireless-policy)# exclusionlist timeout 5	Specifies the timeout, in seconds. The valid range is from 0-2147483647. Enter zero (0) for no timeout.

Adding Static Entries for Wired Hosts

Follow the procedure given below to create static wired bindings:



Note The statically configured wired bindings and locally configured SVI IP addresses have a higher precedence than DHCP.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	Use the first option to configure an IPv4 static entry or the second option to create an IPv6 static entry. <ul style="list-style-type: none"> • device-tracking binding vlan <i>vlan-id</i> <i>ipv4-address interface</i> gigabitEthernet<i>ge-intf-num</i> <i>hardware-or-mac-address</i> • device-tracking binding vlan <i>vlan-id</i> <i>ipv6-address interface</i> gigabitEthernet<i>ge-intf-num</i> <i>hardware-or-mac-address</i> Example:	Configures IPv4 or IPv6 static entry.

Command or Action	Purpose
<pre>Device(config)# device-tracking binding vlan 20 20.20.20.5 interface gigabitEthernet 1 0000.1111.2222</pre> <p>Example:</p> <pre>Device(config)# device-tracking binding vlan 20 2200:20:20::6 interface gigabitEthernet 1 0000.444.3333</pre>	

Verifying IP Theft Configuration

Use the following command to check if the IP Theft feature is enabled or not:

```
Device# show wireless wps summary
```

```
Client Exclusion Policy
Excessive 802.11-association failures : Enabled
Excessive 802.11-authentication failures: Enabled
Excessive 802.1x-authentication      : Enabled
IP-theft                            : Enabled
Excessive Web authentication failure  : Enabled
Cids Shun failure                     : Enabled
Misconfiguration failure              : Enabled
Failed Qos Policy                     : Enabled
Failed Epm                            : Enabled
```

Use the following commands to view additional details about the IP Theft feature:

```
Device# show wireless client summary
```

Number of Local Clients: 1

MAC Address	AP Name	WLAN State	Protocol	Method	Role
000b.bbb1.0001	SimAP-1	2 Run	11a	None	Local

Number of Excluded Clients: 1

MAC Address	AP Name	WLAN State	Protocol	Method
10da.4320.cce9	charlie2	2 Excluded	11ac	None

```
Device# show wireless device-tracking database ip
```

IP	VLAN	STATE	DISCOVERY	MAC
20.20.20.2	20	Reachable	Local	001e.14cc.cbff
20.20.20.6	20	Reachable	IPv4 DHCP	000b.bbb1.0001

```
Device# show wireless exclusionlist
```

Excluded Clients

MAC Address	Description	Exclusion Reason	Time Remaining
-------------	-------------	------------------	----------------

10da.4320.cce9

IP address theft

59



Note Client exclusion timer deletes the entry from exclusion list with a granularity of 10 seconds. The entry is checked to retain or delete after every 10 seconds. There are chances that the running timer value for excluded clients might display negative values upto 10 seconds.



Note When client exclusion is enabled, it adds the client to the exclusion list. It does not block the client from getting deleted.

```
Device# show wireless exclusionlist client mac 12da.4820.cce9 detail
```

```
Client State : Excluded
Client MAC Address : 12da.4820.cce9
Client IPv4 Address: 20.20.20.6
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason : IP address theft
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 58ac.780e.08f0
AP Name: charlie2
AP slot : 1
Wireless LAN Id : 2
Wireless LAN Name: mhe-ewlc
VLAN Id : 20
```

