



Configuration Guide for DPI, IPS/IDS, and Wireless IPS/IDS

This guide will introduce how to use the DPI, IPS/IDS, and wireless IPS/IDS functions of the Omada Controller.

CONTENTS

1. DPI.....	1
2. IDS/IPS	4
2.1 Configure IDS/IPS	4
2.2 Manage Threats in a Site.....	5
2.3 Manage Threats Globally	7
3. Wireless IDS/IPS.....	9

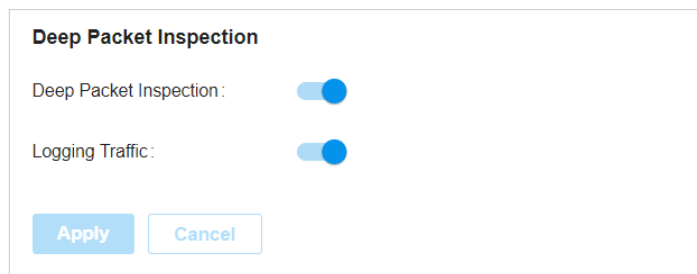
♥ 1. DPI

Overview

DPI (Deep Packet Inspection) helps you identify, analyze, and control the traffic at the application layer in the network. DPI engine includes the latest application identification signatures to track which applications are using the most bandwidth. You can better manage and distribute network traffic usage through DPI.

Configuration

1. Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Network Security](#) > [Application Control](#).
2. On the [Deep Packet Inspection](#) page, enable [Deep Packet Inspection](#) and [Logging Traffic](#), then apply the settings.



[Deep Packet Inspection](#)

When enabled, the device will send the forwarded traffic to a professional local DPI engine for analysis, so as to judge and identify the type of traffic.

[Logging Traffic](#)

When enabled, the device will collect and save the results of traffic analysis. You can check the results on the [Statistics](#) > [Application Analytics](#) page.

3. Apply the settings.

4. On the [Rules Management](#) page, click [Create New Rule](#). You can predefine one or more rules, and APP control strategy that can be referenced, and realize block or QoS actions for specified Apps within a specified time period.

Create New Rule

Rules Name:

Schedule: [Manage Time Range Entries](#)

QoS: ☐ Enable

Select Apps [?](#)

☐	NAME	CATEGORY	DESCRIPTION	ACTION
☐	1-clickshare-com	Sharehosting	The application 1-clickshare-com was used to classify traffic from the hoster with the same name. It was deprecated because the website is no longer reachable.	E
☐	1-upload-com	Sharehosting	The application 1-upload-com was used to classify traffic from the hoster with the same name. It was deprecated because the website is no longer reachable.	E
☐	1-upload-to	Sharehosting	The application 1-upload-to was used to classify traffic from the hoster with the same name. It was deprecated because the website is no longer reachable.	E
☐	10upload-com	Sharehosting	The application 10upload-com was used to classify traffic from the hoster with the same name. It was deprecated because the website is no longer reachable.	E
☐	123VPN	Tunnel	123VPN is a free VPN application provided by Amplusnet SRL.	E
☐	123upload	Sharehosting	The application 123upload was used for traffic from the hoster with the same name. It was deprecated because the website is no longer reachable.	E
☐	123upload-pl	Sharehosting	The application 123upload-pl was used to classify traffic from the hoster with the same name. It was deprecated because the website is no longer reachable.	E
☐	139pan-com	Sharehosting	The application 139pan-com was used to classify traffic from the hoster with the same name. It was deprecated because the website is no longer reachable.	E
☐	163pan-com	Sharehosting	The application 163pan-com was used to classify traffic from the hoster with the same name. It was deprecated because the website is no longer reachable.	E
☐	1clickshare-net	Sharehosting	The application 1clickshare-net was used to classify traffic from the hoster with the same name. It was deprecated because the website is no longer reachable.	E

Select 0 of 2085 items [Select All](#) Showing 1-10 of 2085 records [1](#) [2](#) [3](#) [4](#) [5](#) ... [209](#) [10 / page](#) Go To page: [Go](#)

[Apply](#) [Cancel](#)

Rule Name Specify the name of the rule.

Schedule Specify the time period when the rule takes effect. You can create new time range according to your needs.

QoS Enable this option and select QoS Class to configure the QoS strategy if needed.

Select Apps Select the Apps for the rule.

5. On the [Application Filter](#) page, click [Create New Application Filter](#). You can apply the defined rules and divide multiple rules into one filter set for easy management.

Create New Application Filter

Name:

Description:

Select Rules [+ Add](#)

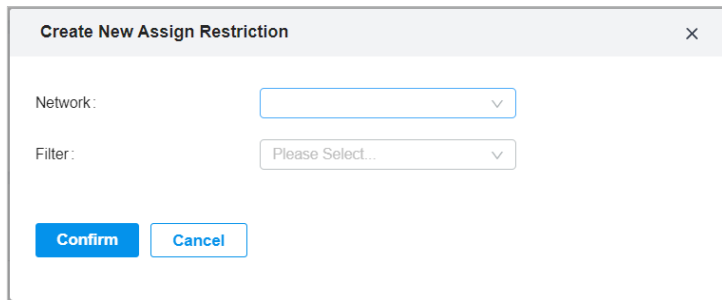
☐	RULES NAME	APP NUMBER	QOS STATUS	SCHEDULE	ACTION
☐	AD	144	Disabled	everyday	E

Select 0 of 1 items [Select All](#) Showing 1-1 of 1 records [1](#) [10 / page](#) Go To page: [Go](#)

[Create](#) [Cancel](#)

Name	Specify the name of the filter.
Description	Enter a description for identification.
Select Rules	Select the rules for the filter.

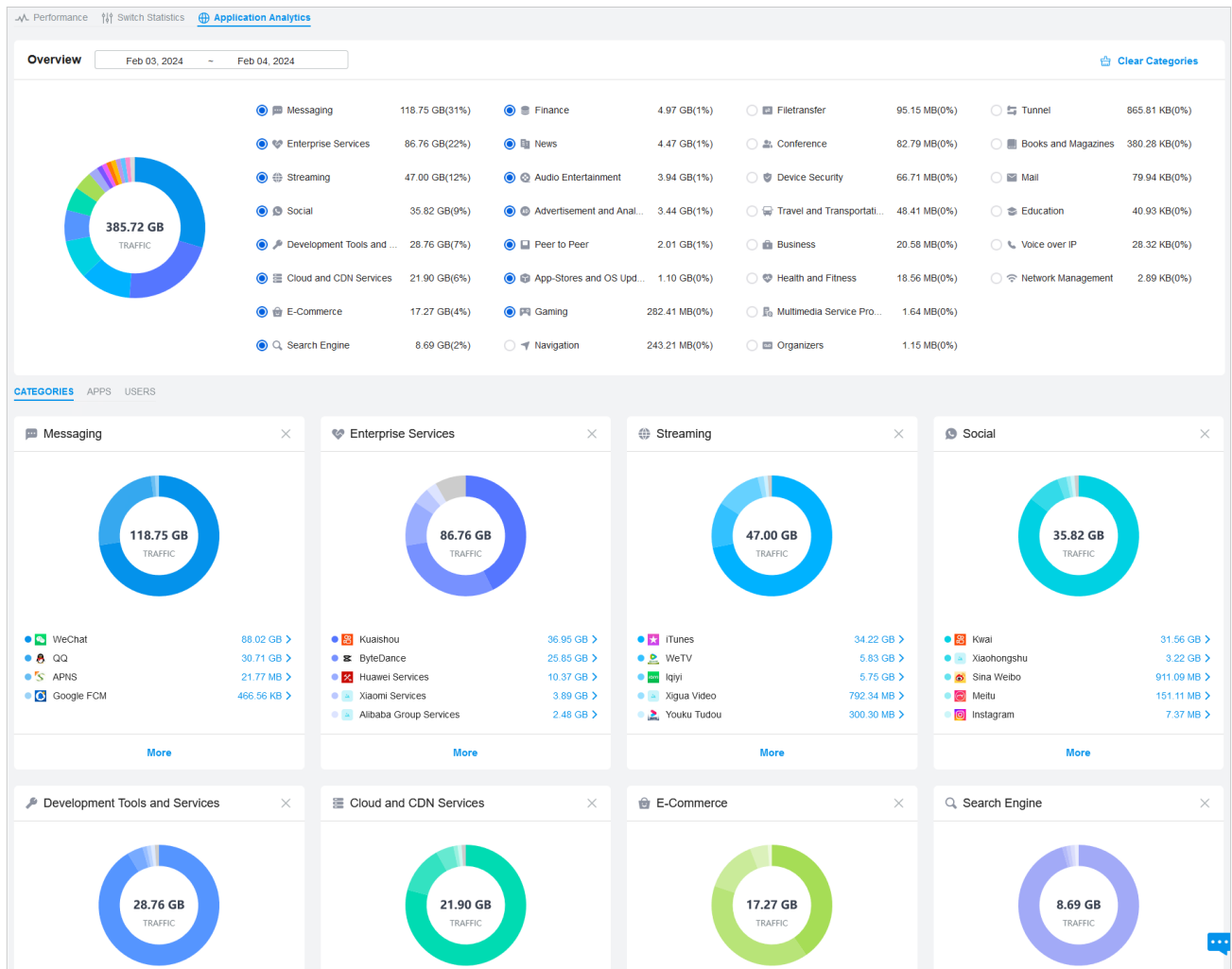
6. On the [DPI Packet Inspection](#) page, click [Create New Assign Restriction](#). Select a network to apply a pre-defined filter.



The dialog box titled "Create New Assign Restriction" contains two dropdown menus. The first is labeled "Network:" and the second is labeled "Filter:" with a placeholder text "Please Select...". At the bottom of the dialog are two buttons: "Confirm" and "Cancel".

Network	Select a network to apply the filter.
Filter	Select a pre-defined filter.

7. Save the settings. You can view the results of traffic analysis on the [Statistics > Application Analytics](#) page.



If you want to clear DPI data of a time period, go to the [Deep Packet Inspection](#) page, click the [Clear Data](#) button and specify the period.

♥ 2. IDS/IPS

Overview

IDS/IPS is a security mechanism that detects intrusions based on attack characteristics. It can detect malware, Trojan horses, worms, ActiveX and other attacks to protect the network security of users.

ⓘ Note:

Using Intrusion Detection/Prevention may reduce maximum throughput speeds.

2.1 Configure IDS/IPS

1. Select a site from the drop-down list of [Organization](#). Go to [Settings > Network Security > IDS/IPS](#).

2. Enable [Intrusion Detection/Prevention](#) and configure the parameters.

IDS/IPS ⓘ

Intrusion
 ☒

Detection/Prevention :

Type :
 ☒ Detect Only (IDS)
 ☐ Detect and Prevent (IPS)

⚠ Using Intrusion Detection/Prevention may reduce maximum throughput speeds.

GEO Enforcer :
 ☐ Enable ⓘ

Security Level :

High

 ⓘ

✓ 12 of 12 Threat Categories Enabled.

Effective Time :
 ☐ Enable

Apply Cancel

Type	Specify the working mode. In IDS mode, the system will only report the threat log. In IPS mode, the system will block the corresponding connection for 300s after a threat is detected.
GEO Enforcer	Enable geographic location identification of threat logs.
Security Level	Choose the protection level. A higher protection level means more threat types are detected, while a lower protection level only detects some important threats. You can also customize the protection level.
Effective Time	Specify the effective time period of the IDS/IPS module.

3. Apply the settings.

When the system discovers a threat, the corresponding threat log will be displayed on the [Insights > Threat Management](#) page.

2.2 Manage Threats in a Site

1. Select a site from the drop-down list of [Organization](#). Go to [Insights > Threat Management](#).

- Click a threat that the system discovered, then you can choose a specified response strategy for the corresponding attack IP: Block, Isolate Device, Signature Suppression, or Allow.

The screenshot displays the Threat Management interface. On the left is a sidebar with navigation options: Session Limit, Known Clients, Past Connections, Past Portal Authorizations, Switch Status, Port Forwarding Status, VPN Status, Routing Table, Dynamic DNS, Wireless IDS/IPS, Threat Management (selected), and QoS Data. The main area shows a table of threats with columns: DATE TIME, SOURCE LOCATION, THREAT DESCRIPTION, SEVERITY, and CATEGORY. Three threats are listed, all categorized as DNS. The first two have a severity of 'Major', and the third has a severity of 'Low'. Below the table is a pagination control showing 'Showing 1-3 of 3 records' and a 'Go to page' field. On the right, the 'Threat Management Detail' panel is open, showing an 'Overview' tab. It displays details for a selected threat: Date (Nov 21, 2023), Time (14:30:09), Source IP Location (United States), Destination IP Location (United States), Source IP (192.168.192.15), Destination IP (8.8.8.8), Threat Description (ET DNS Query to a * to...), Severity (Major), Category (DNS), Classification (bad-unknown), Activity (70 B), and Protocol (UDP). At the bottom of the detail panel are four buttons: Block, Isolate Device, Signature Suppression, and Allow.

Block

Drop traffic to/from the external IP address and the specific internal IP address.

If you block an entry, it will be added to the [Block List](#) at [Settings > Network Security > IDS/IPS](#).

Isolate Device

Drop traffic to/from the external IP address and any internal IP address.

Signature Suppression

Mute the alerting on certain signatures. This will also disable blocking on traffic matching the designated suppression rule.

If you suppress the signature of an entry, it will be added to the [Signature Suppression](#) list at [Settings > Network Security > IDS/IPS](#).

Allow

Trust the IP address so that the traffic, depending on the direction selected, will not get blocked to or from the identified IP address.

If you allow an entry, it will be added to the [Allow List](#) at [Settings > Network Security > IDS/IPS](#).

- You can further check and edit processed entries at [Settings > Network Security > IDS/IPS](#).

■ Block List

The Block List page displays all block entries added through the [Threat Management](#) page. You can choose to block all traffic of the source IP in the threat log, or block all traffic between the source IP and the destination IP in the threat log.

■ Allow List

On the Allow List page, you can add, view, and edit the exemption entries of IDS/IPS detection, so that the specified objects will no longer trigger threat logs.

Click [Create New Allow List](#) and configure the parameters.

Create New Allow List [X]

Direction:

Track By:

IP Address:

Direction	Specify the location of the object (target) exempt from triggering the threat: source, destination, or both directions.
Track By	Specify the type of object (target) exempt from triggering the threat: IP address, Network, or Subnet.
IP Address/Network/Subnet	Specify the value of the object.

■ Signature Suppression

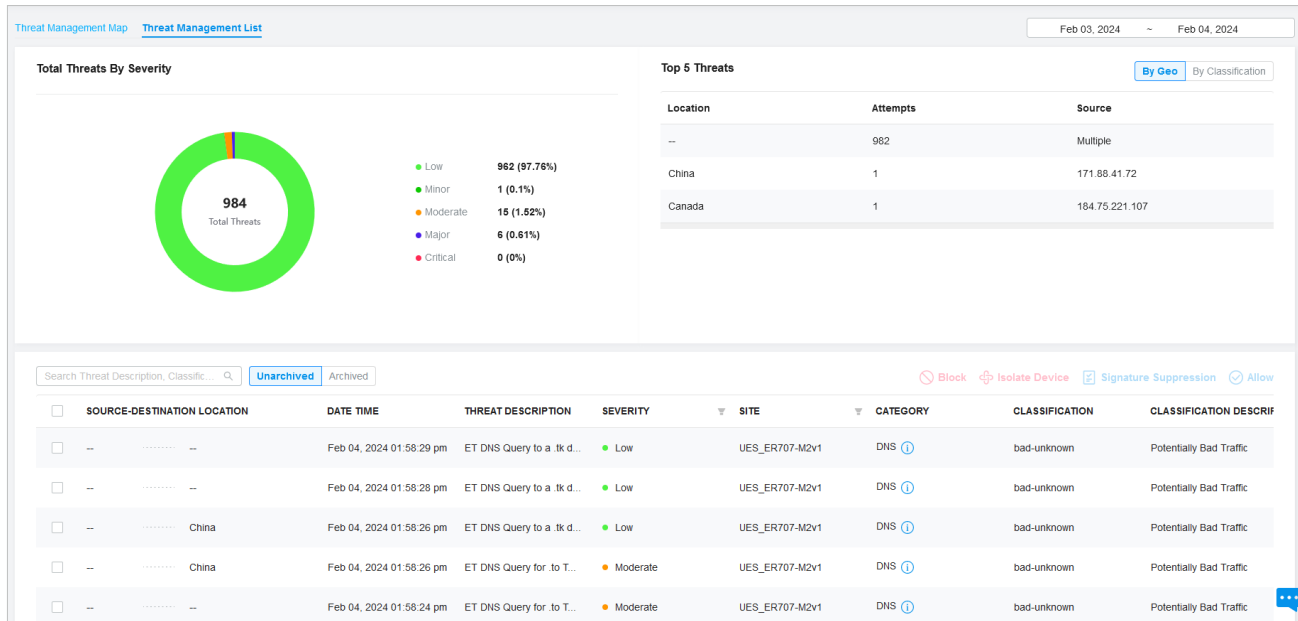
The Signature Suppression page displays all the signature suppression entries added through the Threat Management page, and the objects with signature suppressed will no longer trigger specific threat logs.

2.3 Manage Threats Globally

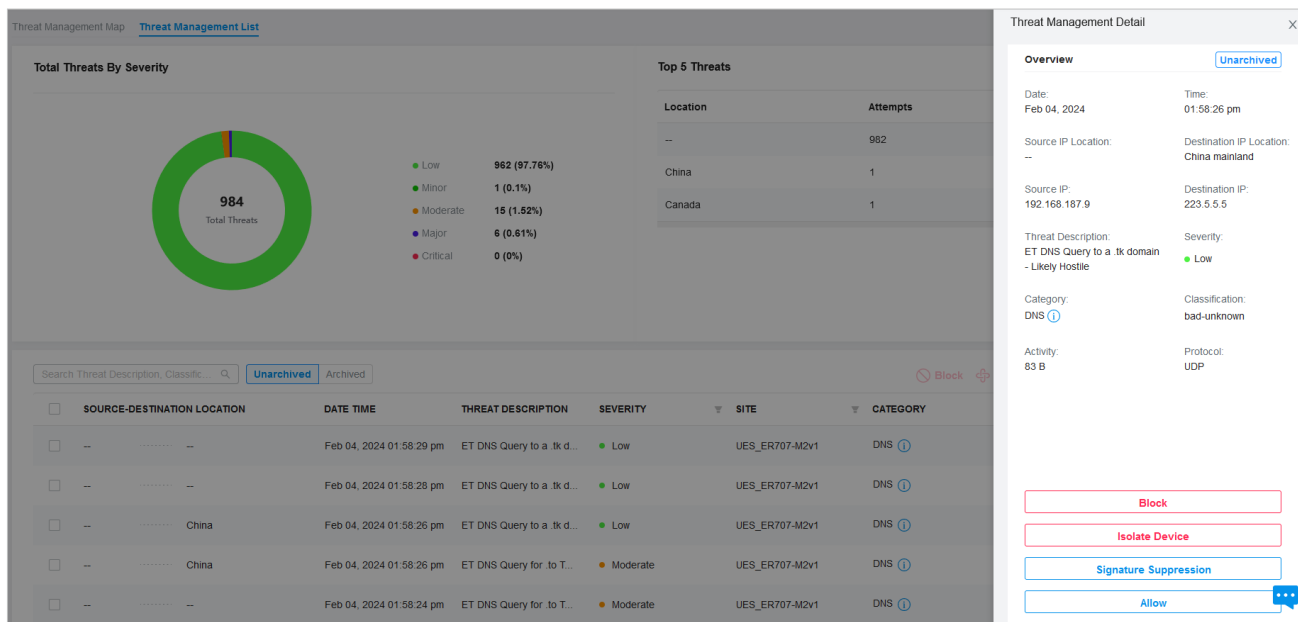
In Global view, go to [Security](#).

■ Threat Management List

In the [Threat Management List](#), you can check top threats by severity, locations of top threats, and unarchived and archived threats.



In the unarchived threat list, click an entry, then you can choose a specified response strategy for the corresponding attack IP: Block, Isolate Device, Signature Suppression, or Allow.



Block

Drop traffic to/from the external IP address and the specific internal IP address.

If you block an entry, it will be added to the [Block List](#) at [Settings > Network Security > IDS/IPS](#).

Isolate Device

Drop traffic to/from the external IP address and any internal IP address.

Signature Suppression

Mute the alerting on certain signatures. This will also disable blocking on traffic matching the designated suppression rule.

If you suppress the signature of an entry, it will be added to the [Signature Suppression](#) list at [Settings](#) > [Network Security](#) > [IDS/IPS](#).

Allow

Trust the IP address so that the traffic, depending on the direction selected, will not get blocked to or from the identified IP address.

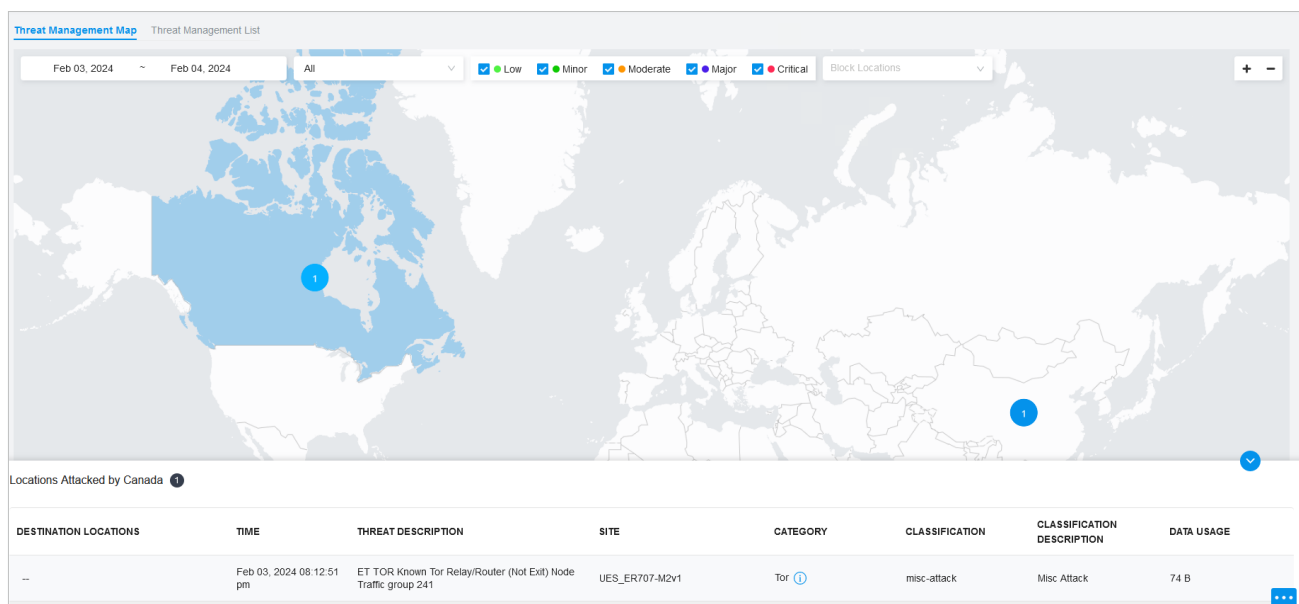
If you allow an entry, it will be added to the [Allow List](#) at [Settings](#) > [Network Security](#) > [IDS/IPS](#).

■ Threat Management Map

In the [Threat Management Map](#), you can view the threat sources and numbers of attacks that the system has discovered. You can click a number in the map to view attack details.

You can right-click a location to block its attack events and manage the Block Locations list.

If excessive attacks have been detected, you can choose specific severity levels to display.



♥ 3. Wireless IDS/IPS

Overview

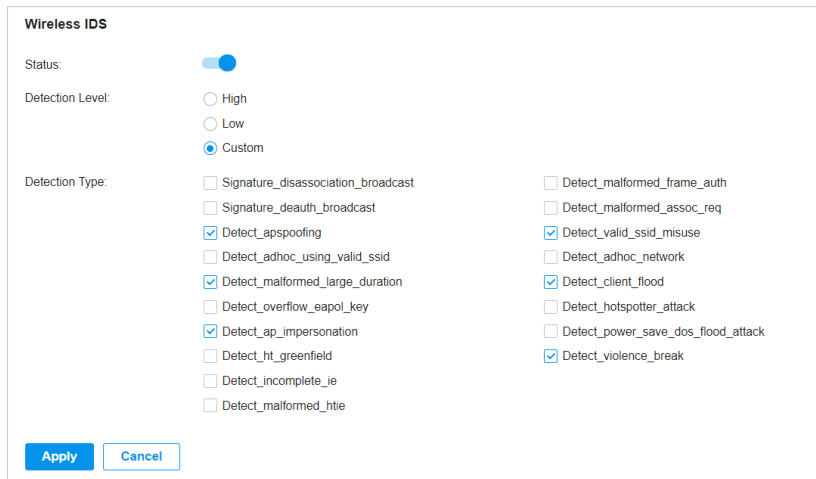
With Wireless IDS (Intrusion Detection System), APs will regularly detect wireless signals of the devices in the network to check for malicious or illegal network behaviors.

With Wireless IPS (Intrusion Prevention System), APs can take corresponding preventions and countermeasures against detected malicious devices and attackers.

■ Wireless IDS

1. Select a site from the drop-down list of [Organization](#). Go to [Settings](#) > [Network Security](#) > [Wireless IDS/IPS](#).

- On the [Wireless IDS](#) page, enable the function and configure the detection settings.



Wireless IDS

Status: ☒

Detection Level:
☐ High
☐ Low
☒ Custom

Detection Type:

☐ Signature_disassociation_broadcast
☐ Signature_deauth_broadcast
☒ Detect_apspoofing
☐ Detect_adhoc_using_valid_ssid
☒ Detect_malformed_large_duration
☐ Detect_overflow_eapol_key
☒ Detect_ap_impersonation
☐ Detect_ht_greenfield
☐ Detect_incomplete_ie
☐ Detect_malformed_htie

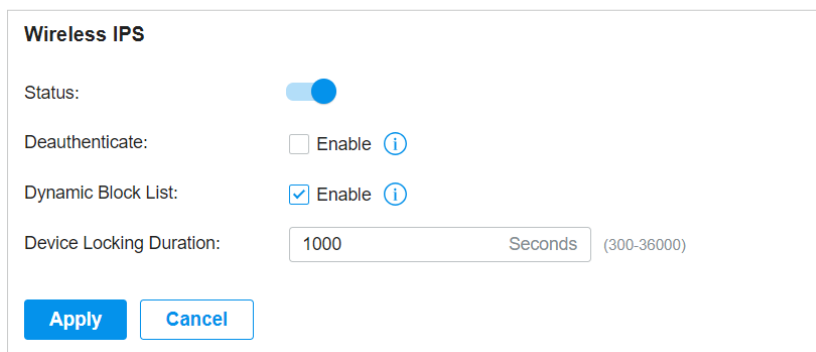
☐ Detect_malformed_frame_auth
☐ Detect_malformed_assoc_req
☒ Detect_valid_ssid_misuse
☐ Detect_adhoc_network
☒ Detect_client_flood
☐ Detect_hotspotter_attack
☐ Detect_power_save_dos_flood_attack
☒ Detect_violence_break

[Apply](#) [Cancel](#)

- Save the settings. When the device discovers a threat, the corresponding threat log will be displayed on the [Insights > Threat Management](#) page.

■ Wireless IPS

- Select a site from the drop-down list of [Organization](#). Go to [Settings > Network Security > Wireless IDS/IPS](#).
- On the [Wireless IPS](#) page, enable the function and configure the parameters.



Wireless IPS

Status: ☒

Deauthenticate: ☐ Enable ⓘ

Dynamic Block List: ☒ Enable ⓘ

Device Locking Duration: Seconds (300-36000)

[Apply](#) [Cancel](#)

Deauthenticate

When enabled, Omada APs will counteract the detected malicious APs, so that clients will disconnect from those APs. To use this function, make sure you have enabled detection of events **Detect_adhoc_using_valid_ssid** and **Detect_valid_ssid_misuse**. Otherwise the configuration will not take effect.

Dynamic Block List

When enabled, once an AP detects a malicious attack such as brute force cracking, it will add the attacker to the block list and will not deal with packets from this attacker for a period of time. To use this function, make sure you have enabled detection of events **Detect_client_flood**, **Detect_violence_break**, and **Detect_power_save_dos_flood_attack**. Otherwise the configuration will not take effect.

Device Locking Duration

Specify the duration for the attacker to stay in the dynamic block list after being added.

3. Save the settings. When the device discovers a threat, it will take corresponding preventions and countermeasures against detected malicious devices and attackers.