



Device Analytics

- [Device Analytics](#), on page 1
- [Adaptive 802.11r](#), on page 4

Device Analytics

Information About Device Analytics

The Device Analytics feature enhances the enterprise Wi-Fi experience for client devices to ensure seamless connectivity. This feature provides a set of data analytics tools for analyzing wireless client device behavior. With device profiling enabled on the controller, information is exchanged between the client device and the controller and AP. This data is encrypted using AES-256-CBC to ensure device security.



Note • From 17.1.1 release onwards, this feature is applicable to Samsung devices.



Note From Cisco IOS XE Dublin 17.12.1, MacBook Analytics is supported on the controller when the MacBook device sends 11k action frames along with the model information.



Note Apple clients such as iPhones and iPads use 802.11k action frames to send device information to the controller. When they fail to send 802.11k action frames, the controller will not perform device classification based on the 802.11 protocol. Hence, this falls back to legacy device classification which is based on HTTP and DHCP protocols.

Restrictions for Device Analytics

- This feature is applicable only for Cisco device ecosystem partners.
- This feature is supported only on the 802.11ax and Wave 2 APs.

- This feature is supported using central authentication in either local mode or FlexConnect mode.

Configuring Device Analytics (GUI)

Procedure

-
- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
- Step 2** On the **WLANs** page, click the name of the WLAN.
- Step 3** In the **Edit WLAN** window, click the **Advanced** tab.
- Step 4** In the **Device Analytics** section, select the **Advertise Support** check box.
- Step 5** (Optional) In the **Device Analytics** section, select the **Share Data with Client** check box.
- Step 6** Click **Update & Apply to Device**.
-

Configuring Device Analytics (CLI)

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 2	wlan wlan-name wlan-id SSID-name Example: Device(config)# wlan device_analytics 1 device_analytics	Enters the WLAN configuration sub-mode. <ul style="list-style-type: none"> • <i>wlan-name</i>—Enter the profile name. The range is from 1 to 32 alphanumeric characters. • <i>wlan-id</i>—Enter the WLAN ID. The range is from 1 to 512. • <i>SSID-name</i>—Enter the Service Set Identifier (SSID) for this WLAN. If the SSID is not specified, the WLAN profile name is set as the SSID. <p>Note If you have already configured WLAN, enter wlan wlan-name command.</p>
Step 3	client association limit {clients-per-wlan apclients-per-ap-per-wlan radio clients-per-ap-radio-per-wlan} Example:	Sets the maximum number of clients, clients per AP, or clients per AP radio that can be configured on a WLAN.

	Command or Action	Purpose
	Device(config)# client association limit 1 1	
Step 4	[no] device-analytics Example: Device(config)# device-analytics	This is enabled by default. Enables or disables device analytics. WLANs advertise analytics capability in beacons & probe responses.
Step 5	[no] device-analytics [export] Example: Device(config)# device-analytics export	When export option is set, the information from Cisco devices are shared with compatible clients (such as, Samsung devices). Here, information from Cisco devices refer to the Cisco controller details, AP version, and model number. This configuration is disabled by default.
Step 6	no shutdown Example: Device(config)# no shutdown	Enables the WLAN.
Step 7	end Example: Device(config)# end	Returns to privileged EXEC mode.

Verifying Device Analytics Configuration

To view the status of device analytics export, use the following command:

```
Device# show wlan 1 test-wlan

WLAN Profile Name      : test-wlan
=====
Identifier              : 1
Description             :
Network Name (SSID)    : test-open-ssid
Status                  : Enabled
Broadcast SSID         : Enabled
Advertise-Apname       : Disabled
Universal AP Admin     : Disabled

Device Analytics
  Advertise Support     : Enabled
  Share Data with Client : Disabled
```

To view client device information, use the following command:

```
Device# show device classifier mac-address 0040.96ae.xxx detail

Client Mac: 0040.96ae.xxxx
Device Type: Samsung Galaxy S10e(Phone)
Confidence Level: 40
Device Name: android-dhcp-9
Software Version(Carrier Code): SD7(TMB)
Device OS: Android 9
```

```
Device Vendor: android-dhcp-9
Country: US
```

To view the last disconnect reason, use the following command:

```
Device# show device classifier mac-address 0040.96ae.xxxx detail
```

```
Client MAC Address : 0040.96ae.xxxx
Client IPv4 Address : 12.1.0.52
Client IPv6 Addresses : fe80::631b:5b4f:f9b6:53cc
Client Username: N/A
AP MAC Address : 7069.5a51.53c0
AP Name: AP4C77.6D9E.61B2
AP slot : 1
Client State : Associated

Assisted Roaming Neighbor List
Nearby AP Statistics:
EoGRE : No/Simple client
Last Disconnect Reason : User initiated disconnection - Device was powered off or Wi-Fi
turned off
```

Adaptive 802.11r

Information About Adaptive 802.11r

The Cisco device ecosystem partner now supports 11r functionality on an adaptive 802.11r SSID. Samsung is one of the partners.



Note The Adaptive 802.11r is enabled by default. This means that when you create a WLAN, the adaptive 802.11r is configured by default.

Client device information such as its model number, supported operating system is shared with the controller and AP while the device receives information such as controller and AP type, software release, etc. Also, this enables 802.11r-compatible devices to benefit from adaptive 802.11r on Cisco networks. This ecosystem comes handy especially for troubleshooting device disconnection from the AP as the controller receives information such as the disconnect reason code from the client device.



Note Devices without 11r support cannot join an SSID where 11r is enabled.

To use the 11r functionality on devices, you need to create a separate SSID with 11r enabled and another with 11r disabled to support the non-11r devices in the network.

Adaptive dot11r is supported by Apple iPad, Apple iPhone, and Samsung S10 devices. However; some software update creates a MIC mismatch error in these devices. But these errors are transient and clients will successfully be able to associate to the SSID in subsequent results.

Configuring Adaptive 802.11r (GUI)

Procedure

- Step 1** Choose **Configuration > Tags & Profiles > WLANs**.
 - Step 2** On the **WLANs** page, click the name of the WLAN.
 - Step 3** In the **Edit WLAN** window, click the **Security > Layer2** tab.
 - Step 4** In the **WPA Parameters** section and **Fast Transition** drop-down list, choose **Adaptive Enabled**.
 - Step 5** Click **Update & Apply to Device**.
-

Verifying Adaptive 802.11r

To view the details, use the following command:

```
Device# show running-config all
wlan test-psk 2 test-psk
security ft adaptive
"adaptive" is optional
```



Note The following command is used to enable or disable adaptive 11r:

[no] security ft adaptive

The following command is used to enable or disable 802.11r:

[no] security ft
