Wireless Active Testing with ThousandEyes

Feature history for wireless active testing with ThousandEyes

- This table provides release and related information for the feature explained in this module.
- This feature is also available in all the releases subsequent to the one in which they are introduced in, unless noted otherwise.

Table 1: Feature history for wireless active testing (WAT) with ThousandEyes

Feature Name	Release Information	Feature Description
Wireless active testing with ThousandEyes	Cisco IOS XE 17.18.2	Wireless Active Testing (WAT) proactively detects and reports Wi-Fi issues, integrating with the Cisco Catalyst 9800 Wireless LAN Controller and ThousandEyes for comprehensive network and application testing. It leverages APs as WAT devices to troubleshoot Wi-Fi network unpredictability and test network health directly from the edge.

Wireless active testing (WAT)

Wireless active testing (WAT) is a solution that

- proactively detects and reports Wi-Fi issues before end-users encounter them
- integrates the Cisco Catalyst 9800 Wireless LAN Controller with ThousandEyes for comprehensive network and application testing, and
- helps troubleshoot Wi-Fi network unpredictability by leveraging APs as WAT devices.

WAT functionality allows you to test wireless network health and application connectivity directly from the edge of your network, with the controller managing the onboarding and configuration of these active test APs to the ThousandEyes platform.

Key aspects of wireless active testing:

- Wireless onboarding test: This part of WAT performs Layer 2 onboarding tests, including 802.11 authentication, association, EAP, key exchange, and DHCP. It reports failures and collects metrics and telemetry for successful onboarding attempts, providing insights into the wireless client experience.
- Synthetic testing with ThousandEyes: This integrates with the ThousandEyes Endpoint Agent, deployed on Catalyst APs, to run synthetic tests over the wireless connection. It checks for success or failure to various web server applications and collects metrics for application performance, offering Layer 3 and above testing capabilities directly from the AP. The controller facilitates the connection and management of these agents with the ThousandEyes platform.

Supported controller and AP platforms

Wireless active testing (WAT) is supported on Cisco Catalyst Wireless LAN Controllers and APs, offering a range of features for network monitoring and assurance by integrating with ThousandEyes.

Supported controller Platforms:

- Cisco CW9800 Series (CW9800L, CW9800M, CW9800H1, CW9800H2).
- Cisco Catalyst 9800 Series (C9800-L, C9800-40, C9800-80).
- Catalyst 9800-CL (virtual controller).

- Embedded Wireless Controller (EWC) on Catalyst 9000 Series Switches.

Supported AP Platforms:

- Cisco Wireless 9172H Catalyst AP (Wi-Fi 7 wall-plate model).

Supported security types

WAT supports a variety of security configurations for testing wireless networks, enabling comprehensive assessment of different WLAN setups.

This table includes the supported and non supported WLAN security types.

WLAN types	Supported types	Non supported types
AKM Suites	• 802.1X • PSK • FT-802.1X • FT-PSK • 802.1X-SHA256 • PSK-SHA256 • SAE • FT-SAE • OWE, including OWE Transition Mode	• Suite-B (11) • Suite-B-192 (12) • SAE-EXT-KEY (24) • FT-SAE-EXT-KEY (25)
Ciphers	CCMP-128	• GCMP-128 • CCMP-256 • GCMP-256
PHY Mode / Wi-Fi versions	• HE (802.11ax / Wi-Fi 6 + 6E). • VHT (802.11ac / Wi-Fi 5). • HT (802.11n / Wi-Fi 4). • Legacy (802.11abg). **Note** All PHY modes up to Wi-Fi 6E are supported	EHT (802.11be or Wi-Fi 7)

WLAN types	Supported types	Non supported types
Bands	• 2.4 GHz • 5 GHz • 6 GHz	-

Note

- WPA Support: WPA2 and WPA3 are both supported, including PMF (disabled, optional, required).
- Beacon protection is not supported.
- WAT supports IPv4 for wireless connectivity tests, ThousandEyes agent tests, and HTTP(S) proxy for management traffic.
- Hidden SSIDs are not supported.

Guidelines of wireless active testing

- There is a download server used to obtain the ThousandEyes endpoint agent. There is also a telemetry server, known as the platform server, with which the ThousandEyes endpoint agent communicates. Both servers require internet connectivity, either through an HTTPS proxy or through a direct connection. Ensure that the required IP addresses and URLs are allowlisted to enable access through any firewall. For more information, check Network Connections.
- The Cisco Wireless 9172H Catalyst AP does not broadcast SSIDs when WAT is enabled on the AP. They do not broadcast WLANs and do not serve clients. Use these APs exclusively for monitoring and testing. As a result, all WLANs tagged to the WAT AP in its assigned policy profile are communicated to the TE Platform, allowing selection for SSID test configuration and credentials.
- Because WAT APs require a tag, assign a policy tag based on the location of your AP and tag it as you would for any other AP. If you do not tag at least one of the AP's slots in the RF Tag with a radio profile that has WAT enabled, the AP will not be able to test.

Note If you use an HTTP(S) proxy with an FQDN, configure a DNS IP address on the AP, either statically or using DHCP. The AP must resolve the proxy FQDN using DNS to connect to the ThousandEyes server.

Configure wireless active testing (GUI)

Enable and configure wireless active testing (WAT) on your controller and associated APs for integration with ThousandEyes using the GUI.

This task involves setting up global WAT parameters on the controller, configuring AP-specific settings, and enabling WAT on selected APs. It allows APs to act as active test APs, performing wireless and application tests managed by the ThousandEyes platform.

Before you begin

Ensure your controller and APs are running compatible software versions (17.18.2 or later is required).

- You must have a ThousandEyes account and obtain the **ThousandEyes Endpoint Agent Connection String** found in the **Endpoint Experience** section from your ThousandEyes dashboard account settings. This string links your controller and APs to your ThousandEyes organization.

Procedure

Step 1 Choose **Configuration** > **Services** > **Cloud Services**.

Step 2 Click the **Thousand Eyes** tab.

Step 3 The **Wireless Active Testing (WAT) status** toggle is **Enabled** by default.

Step 4 Paste the **ThousandEyes Endpoint Agent Connection String** from the ThousandEyes platform.

Step 5 Click **Apply**.

Configure wireless active testing (CLI)

Enable and configure Wireless active testing (WAT) on your controller and associated APs for integration with ThousandEyes using commands.

Before you begin

Ensure your controller and APs are running compatible software versions (17.18.2 or later is required).

- You must have a ThousandEyes account and obtain the **ThousandEyes Endpoint Agent Connection String** found in the **Endpoint Experience** section from your ThousandEyes platform Endpoint Agent settings. This string links your controller and APs to your ThousandEyes organization.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure ThousandEyes endpoint agent connection string.

Example:

```
Device(config)# wireless active testing thousand-eyes connection-string STRING
```

This string associates the AP's ThousandEyes agent with your ThousandEyes organization. Use the **no** form of the command to remove the connection string.

Note
Removing the connection string unregisters all WAT APs from the ThousandEyes Platform.

Step 3 Exit the global configuration mode.

Example:

```
Device(config)# end
```

Configure HTTP(S) proxy for WAT (GUI)

Follow these steps to configure an HTTP(S) proxy for WAT management traffic to the ThousandEyes server, using GUI.

Before you begin

Unauthenticated HTTP forward proxy is supported.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **AP Join**.

Step 2 Click **Add**.
The **Add AP Join Profile** page appears.

Step 3 In the **General** tab, enter the **Name** and **Description** for the AP join profile.

Step 4 In the **Management** tab, go to the **HTTP Proxy Configuration** section.

Step 5 Enter the IPV4 or Hostname in the **Client Proxy Server** field.

Step 6 Enter a value in the **Client Proxy Port** field.

Step 7 Click **Apply to Device**.

Configure HTTP(S) proxy for WAT (CLI)

Follow these steps to configure an HTTP(S) proxy for WAT management traffic to the ThousandEyes server, using commands.

Before you begin

Unauthenticated HTTP forward proxy is supported.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Enter AP Join Profile configuration mode.

Example:

```
Device(config)# ap profile default-ap-profile
```

Step 3 Configure the HTTP(S) proxy.

Example:

```
Device(config-ap-profile)# ip http client proxy hostname URL PORT
```

The valid value range for the port number is 0 to 65535. The **URL** needs to be in the format of `{http|https}://<FQDN or IP>[/<path>]`.

Note
This proxy enables the ThousandEyes Agent IOx package download and manages all subsequent communications between the ThousandEyes Agent and the ThousandEyes platform.

Step 4 Exit AP Join Profile configuration mode.

Example:

```
Device(config-ap-profile)# end
```

Configure WAT radio selection and tag the RF profile (GUI)

Follow these steps to configure the radio profile and RF tag to designate AP radios for WAT using the GUI.

This process helps you to identity the APs that you want to become WAT APs.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **RF/Radio**.

Step 2 Create a new radio profile in the **Radio** tab and then select the profile.
The **Edit Radio Profile** tab appears.

Step 3 Select **Enabled (Always)** for the **Wireless Active Testing Radio Selection** field's drop-down list.

The options are **Enabled (Always)** and **Disabled**.

Step 4 Click **Update & Apply to Device**.

Step 5 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 6 In the **RF** tab, click the newly created and configured RF profile.
The **Edit RF Tag** page appears.

Step 7 Tag the profile to **Slot 2** for the **6 GHz Radio Profile** band, to **Slot 1** for the **5 GHz Radio Profile** band and to **Slot 0** for the **2.4 GHz Radio Profile** band.

Step 8 Click **Update & Apply to Device**.

Configure wireless active testing radio selection (CLI)

Follow these steps to configure the radio profile and RF tag to designate AP radios for WAT using commands.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Create or modify a radio profile.

Example:

```
Device(config)# wireless profile radio RADIO_PROFILE_NAME
```

Step 3 Enable wireless active testing radio selection within the radio profile.

Example:

```
Device(config-wireless-radio-profile)# active testing radio-selection always
```

Step 4 Exit radio profile configuration mode and create or modify an RF tag.

Example:

```
Device(config)# wireless tag rf RF_TAG_NAME
```

Step 5 Tag the profile to **Slot 2** for the **6 GHz Radio Profile** band, to **Slot 1** for the **5 GHz Radio Profile** band and to **Slot 0** for the **2.4 GHz Radio Profile** band.

Example:

```
Device((config-wireless-rf-tag))# dot11 24ghz slot0 radio-profile RADIO_PROFILE_NAME
Device(config-wireless-rf-tag)# dot11 5ghz slot1 radio-profile RADIO_PROFILE_NAME
Device(config-wireless-rf-tag)# dot11 6ghz slot2 radio-profile RADIO_PROFILE_NAME
```

Step 6 Exit RF tag configuration mode.

Example:

```
Device(config)# end
```

Enable WAT management for an individual AP (GUI)

Follow these steps to enable or disable WAT Management on an individual AP using the GUI.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 Click the **AP** tab.

Step 3 Go to the **Static** tab for a per AP enablement. Click **Add.**

Step 4 Enter the MAC address in the **AP MAC Address** field.

Step 5 Select the policy-tag, site-tag and RF-tag in the **Policy Tag Name**, **Site Tag Name** and **RF Tag Name** fields as per preference.

Step 6 Click **Apply to Device**.

Enable WAT management for an individual AP (CLI)

Follow these steps to enable or disable WAT management on individual APs using commands.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure the Ethernet MAC address of the AP.

Example:

```
Device(config)# ap H.H.H
```

Step 3 Map a policy tag to the AP.

Example:

```
Device(config)# policy-tag default-policy-tag
```

Use the **no** form of this command to disable it.

Step 4 Map a RF tag to the AP.

Example:

```
Device(config)# rf-tag wat-rf-tag
```

Use the **no** form of this command to disable it.

Step 5 Map a site tag to the AP.

Example:

```
Device(config)# site-tag wat-site-tag
```

Use the **no** form of this command to disable it.

Step 6 Exit the global configuration mode.

Example:

```
Device(config)# end
```

Enable WAT management for multiple APs using location (GUI)

Follow these steps to enable or disable WAT Management on multiple APs using the location process from the GUI.

Before you begin

For multiple APs, follow these steps of enabling WAT management for multiple APs using location or by using the filter process.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 Click the **AP** tab.

Step 3 Go to the **Location** tab. Click **Add**.

Step 4 Enter a location name and description in the **Location** and **Description** fields.

Step 5 In the **General** tab, select the policy-tag, site-tag and RF-tag in the **Policy Tag Name**, **Site Tag Name** and **RF Tag Name** fields as per preference.

Step 6 Click **Apply to Device**.

Step 7 In the **AP Provisioning** tab, select or add APs in the **Import AP MAC**, **AP MAC Address**, **Available AP list** and **Associated AP list** fields to associate them with the location.

Step 8 Click **Apply to Device**.

Enable WAT management for multiple APs using location (CLI)

Follow these steps to enable or disable WAT Management on multiple APs using the location process from the console.

Before you begin

For multiple APs, follow these steps of enabling WAT management for multiple APs using location or by using the filter process.

Procedure

Step 1 Enter the global configuration mode and modify or create AP location configuration.

Example:

```
Device# configure terminal
Device(config)# ap location name wat-location
```

Step 2 Add AP to this location.

Example:

```
Device(config-ap-location)# ap-eth-mac H.H.H
```

Use the **no** form of this command to disable it.

Step 3 Configure tags based for this location, configure policy tag for this location and configure rf and site tag for this location.

Example:

```
Device(config-ap-location)# tag policy default-policy-tag
Device(config-ap-location)# tag rf wat-rf-tag
Device(config-ap-location)# tag site wat-site-tag
```

Use the **no** form of this command to disable it.

Step 4 Exit the global configuration mode.

Example:

```
Device(config-ap-location)# end
```

Enable WAT management for multiple APs using filter (GUI)

Follow these steps to enable or disable WAT Management on multiple APs using the filter process from the GUI.

Before you begin

For multiple APs, follow these steps of enabling WAT management for multiple APs using location or by using the location process.

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Tags**.

Step 2 Click the **AP** tab.

Step 3 Go to the **Filter** tab for a regex on the AP name and select a WAT AP.
The **Edit Tags** page appears.

Step 4 Enter the **Rule Name** and the **AP name regex**.

This results in the tag going to only those selected APs.

Step 5 In the **Active** field, enable the toggle to **Yes**. Click **Update & Apply to Device**.

Note
Tags have a priority order. In the **Tag Source** tab, the default setting is static, so the per-AP priority is zero. If no per-AP tag exists, the system checks the location. If the location is not set, it checks for a filter. If there is no filter, the system checks whether the AP has an assigned tag and saves it. To enable this feature, check the **Enable AP Tag Persistency** checkbox. Click **Apply**.

Enable WAT management for multiple APs using filter (CLI)

Follow these steps to enable or disable WAT Management on multiple APs using the filter process from the console.

Before you begin

For multiple APs, follow these steps of enabling WAT management for multiple APs using location or by using the location process.

Procedure

Step 1 Enter the global configuration mode.

Example:

```
Device# configure terminal
```

Step 2 Configure ap filter and enter AP filter name.

Example:

```
Device(config-ap-filter)# ap filter name wat-aps
```

Step 3 Configure filter based on AP name regular expression match.

Example:

```
Device(config-ap-filter)# ap name-regex WAT-9172H
```

Use the **no** form of this command to disable it.

Step 4 Configure tags based for this filter, configure policy tag for this filter and configure rf and site tag for this filter.

Example:

```
Device(config-ap-filter)# tag policy default-policy-tag
Device(config-ap-filter)# tag rf wat-rf-tag
Device(config-ap-filter)# tag site wat-site-tag
```

Use the **no** form of this command to disable it.

Step 5 Exit the global configuration mode.

Example:

```
Device(config-ap-filter)# end
```

Verify wireless active testing

Use these commands to verify the status of WAT.

- **show run | sec wat-radio-profile**

- **show ap profile name wat-ap-profile detailed**
- **show wireless profile radio detailed wat-radio-profile**
- **show wireless tag rf detailed wat-rf-tag**
- **show wireless active testing configuration**

To verify the WAT radio profile, enter this command from the console:

```
Device# show run | sec wat-radio-profile

wireless profile radio wat-radio-profile
 active testing radio-selection always
Device# show run | sec wat-rf-tag

wireless tag rf wat-rf-tag
 dot11 24ghz slot0 radio-profile wat-radio-profile
 dot11 5ghz slot1 radio-profile wat-radio-profile
 dot11 6ghz slot2 radio-profile wat-radio-profile
```

To verify the WAT AP profile detailed, enter this command from the console:

```
Device# show ap profile name wat-ap-profile detailed
…
Proxy :
  Hostname                    : http://192.168.1.100
  Port                        : 80
  NO_PROXY list               : Not Configured
  Username                    : Not Configured
…
```

To verify the WAT radio profile detailed, enter this command from the console:

```
Device# show wireless profile radio detailed wat-radio-profile
…
Wireless Active Testing (WAT) Configuration
  WAT Admin State (Radio Selection)               : Enabled (Always)
…
```

To verify the WAT RF tag detailed, enter this command from the console:

```
Device# show wireless tag rf detailed wat-rf-tag

Tag Name                      : wat-rf-tag
Description                   :
---------------------------------------
6ghz RF Policy                : default-rf-profile-6ghz
5ghz RF Policy                : Global Config
2.4ghz RF Policy              : Global Config
2.4ghz slot 0 Radio Profile   : wat-radio-profile
5ghz slot 0 Radio Profile     : default-radio-profile
5ghz slot 1 Radio Profile     : wat-radio-profile
6ghz slot 1 Radio Profile     : default-radio-profile
5ghz slot 2 Radio Profile     : default-radio-profile
6ghz slot 2 Radio Profile     : wat-radio-profile
6ghz slot 3 Radio Profile     : default-radio-profile
AP Beam State                 : Boresight
URWB Profile                  :
```

To verify the WAT wireless active testing configuration, enter this command from the console:

```
Device# show wireless active testing configuration

Wireless Active Testing (WAT) Management - Configuration
============================================================
```

```
Administrative State                          : Enabled

ThousandEyes Endpoint Agent
---------------------------
  Connection String                           :
S3FD77CY+VOrk+************************************************************
  Download URL                                :
https://downloads.thousandeyes.com/endpointagent/iox/arm64/latest.tar
```