



Release Notes for Cisco Aironet 1800S Active Sensor, Cisco Wireless Release 2.2.1.0 and 2.2.1.3

First Published: 2021-02-08

Last Modified: 2021-03-11

About the Release Notes

This release notes document describes what is new or changed in this release. The document is updated as needed to provide information about new features, caveats, potential software deferrals, and related documents for the Cisco Aironet 1800S Active Sensor for this release.

We recommend that you view the field notices for this release to check whether your software or hardware platforms are affected. If you have an account on Cisco.com, you can find the field notices at http://www.cisco.com/en/US/customer/support/tsd_products_field_notice_summary.html.

However, if you do not have a Cisco.com account, you can find the field notices at http://www.cisco.com/en/US/support/tsd_products_field_notice_summary.html.

Overview of Cisco Aironet 1800S Active Sensor

The Cisco Aironet 1800S Active Sensor is a part of the Cisco DNA Center Assurance solution. The DNA Center Assurance platform has three components—Wireless Performance Analytics, Real-time Client Troubleshooting, and Proactive Health Assessment.

In this document, the term *Network Sensor* or *sensor* refers to the Cisco Aironet 1800S Active Sensor.

The Cisco Aironet 1800S Active Sensor is an 802.11a/b/g/n/ac (Wave 2) sensor with internal antennas. The sensor can be mounted, in a vertical orientation, on a wall or a desk, and supports 2x2:2 SS. The sensor is capable of joining an infrastructure access point as a client. The sensor can be used to monitor, measure, and troubleshoot a wireless network's overall performance.

For more information about the sensor, including mounting instructions and limited troubleshooting procedures, setup, and configuration, see the [Cisco Aironet 1800S Active Sensor Getting Started Guide](#).

What's New in Release 2.2.1.3

There are no new features that are introduced in this release. For more information about updates in this release, see the Caveats section in this document.

What's New in Release 2.2.1.0

This section provides a brief introduction to the new features and enhancements introduced in this release.

Support for EAP Methods

In this release, the 1800S sensor's support for the Extensible Authentication Protocol (EAP) authentication method extends to support the following security methods for Dot1x enabled WLAN and Dot1x enabled Wired Port:

- EAP-TTLS-MSCHAPv2
- EAP-TTLS-PAP
- EAP-TTLS-CHAP
- EAP-FAST-GTC
- EAP-PEAP-GTC

This release also supports the Sensor's ability to identify, onboard, and test a TKIP enabled WLAN.

IP–Service Level Agreement (SLA) Enhancements

In this release, the IP SLA scheduling has been modified in the Cisco DNA Center to minimize the impact on the inventory collection.

IPerf Test Enhancements

- More locations from the template get tested because of better allocation of IPerf instances. However, only one sensor, which is a combination of server and port, gets tested.



Note Limiting the number of sensors tested simultaneously reduces test failures.

- The following warnings are introduced on the GUI to inform users that IPerf instances are present in multiple test templates:
 - Warning during template creation: This warning is displayed when there is an existing template with the same IPerf instance.
 - Warning during template deployment: This warning is displayed when an already deployed template contains the same Iperf instance.

Network Diagnostics Test (NDT)

In this release,

In this release, limitations are applied to the NDT tests to avoid NDT Server overload when scheduled synthetic tests are performed. The shortest interval allowed over the GUI between the tests is one hour.



Note In general, performance tests are not allowed to run continuously.

Device–Onboarding Test Error–Reporting Improvements

If a device onboarding test fails, the GUI displays an error code. In this release, the error codes are enhanced to give you a better understanding of the issue and help you resolve it.

Limitations and Caveats

This section provides information about known limitations and caveats relating to this release.

Known Limitations

- The sensor fails to detect broadcasted beacons by other APs while scanning its RF environment. However, this behavior occurs intermittently with low probability. It does not associate with the target SSID when it cannot see the beacons and skips the test. The DNAC logs show the detection success rates. For more information, see [CSCwa25257](#).
- **Problem** If you configure the Hexadecimal password option on the controller for pre-shared key (PSK) authentication on the WLAN, the sensor might fail to onboard. As a result, the sensor performs a synthetic test on the WLAN.
Solution To avoid this issue in the WLAN, configure the ASCII password (passphrase) corresponding to the Hex password (PSK).
- **Problem** If you enable P2P blocking on the controller, or set it to forward upstream, you might observe IP Service-Level Agreement (SLA) test failures on the Cisco DNA Center sensor dashboard.
Solution To avoid this issue, disable P2P on the controller.
- **Problem** If the sensor runs on Cisco wireless software, such as Cisco Wireless Release 8.5 that supports Cisco IOS-based (Wave 1) APs, you might experience IP SLA test failure.
Solution To avoid this issue, disable the IP SLA test for Cisco Wave 1 APs.

Caveats

Caveats describe unexpected behavior in the Cisco Wireless Network Sensor software. Severity 1 caveats are the most serious, while Severity 2 caveats are less severe.

The Open Caveats and Resolved Caveats sections list the caveats for this release.

Each caveat contains the following information:

- Identifier: Each caveat is assigned a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z), and N is any number (0-9). Cisco documentation such as Security Advisories, Field Notices and other Cisco support documents frequently refer to these caveat IDs. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific caveat.
- Description: A description is a brief of the issue observed when the caveat occurs.

Cisco Bug Search Tool

The [Cisco Bug Search Tool](#) (BST), the online successor to the Bug Toolkit, is designed to improve network risk management and device troubleshooting effectiveness. The BST allows partners and customers to search for software bugs based on product, release, and keyword and aggregates vital data, such as bug details,

product, and version. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

For more information about using the [Cisco Bug Search Tool](#) effectively, including setting email alerts for bugs, filtering bugs, and saving bugs and searches, see the [Bug Search Tool Help & FAQ](#) page.

You can access the listed bugs through the BST. This web-based tool provides you access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in the Cisco Wireless Network Sensor software and other Cisco hardware and software products.

Click the Caveat Identifier number in the table. The corresponding BST page gets displayed with the details of the bug.



Note If you are not logged in, you will be redirected to a **Log In** page where you need to enter your registered Cisco.com username and password to log in. If you do not have a Cisco.com account, you can [register](#) for one.

If the defect that you have selected cannot be displayed, this may be due to one or more of the following reasons:

- The defect number does not exist
- The defect does not have a customer-visible description yet
- The defect is marked Cisco Confidential

Open Caveats

There are no open caveats in Releases 2.2.1.0 and 2.2.1.3.

Resolved Caveats

There are no resolved caveats in release 2.2.1.0.

Table 1: Resolved Caveats for Release 2.2.1.3

Caveat ID Number	Description
CSCvx40520	Functional: 2.1.360.70270, sensor test failed on DHCP, DNS

Service and Support

For all support-related information, see <http://www.cisco.com/c/en/us/support/index.html>.

Related Documentation

- [Cisco Aironet 1800S Active Sensor Getting Started Guide](#)
- [Cisco Aironet Sensor Deployment Guide](#)

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.