Release Notes for Cisco Aironet 1800S Active Sensor, Cisco Wireless Release 2.1.2.0 and 2.1.2.7

First Published: 2020-08-31

Last Modified: 2021-06-10

Introduction

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 2.1.2.7

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 Cisco Wireless Release 2.1.2.0

The following section provides a brief introduction to the new features and enhancements that are introduced in this release.

ClearPass Support for Sensor

Beginning with Cisco Wireless Release 2.1.2.0, Aruba ClearPass is supported as an additional external web authentication server on the Cisco Aironet 1800s Active Sensor. Support for Cisco Identity Services Engine (ISE) as a login portal and authentication server existed prior to Cisco Wireless Release 2.1.2.0.

802.1x Wired Port Authentication Support

Beginning with Cisco Wireless Release 2.1.2.0, a wired Cisco Aironet 1800s Active Sensor can authenticate itself with a AAA Server using specified 802.1x EAP authentication methods when the wired port on the switch is a closed port. Depending on the EAP method selected, the sensor can use the certificate provisioned through Secure Certificate Enrollment Profile (SCEP).

This feature enhances the security of devices connected to the network. You can specify your choice of EAP method for the wired interface using the Cisco DNA Center GUI. You can add the EAP method, during provisioning, while configuring the wireless and wired backhaul profile for the sensor. If you choose EAP-TLS as the authentication method, then you can add SCEP enrollment. Once staging is complete, the sensor is moved to a closed port on the production switch where 802.1x EAP authentication is used to connect to the wired backhaul.

Support for PEAP-TLS EAP

Beginning with Cisco Wireless Release 2.1.2.0, Cisco Aironet 1800s Active Sensor supports the PEAP-TLS EAP authentication method. This enables the use of this method for onboarding and tests of the following:

- 802.1x-enabled WLAN
- 802.1x-enabled backhaul WLAN
- 802.1x-wired port authentication

Sensor Error State Recovery After Provisioning

Beginning with Cisco Wireless Release 2.1.2.0, enhancements in post-provisioning error state recovery have been enabled on the Cisco Aironet 1800s Active Sensor.

Limitations and Caveats

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 configure the Wi-Fi Protected Access-Temporal Key Integrity Protocol (WPA-TKIP) on the WLAN, you may face issues during wireless network onboarding resulting in the sensor failing the synthetic tests.

Solution To avoid this issue, disable TKIP.

- **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. The severity categories are: Severity 1 caveats are the most serious, Severity 2 caveats are less serious and Severity 3 caveats are moderately serious and only select severity 3 caveats are listed here.

The Open Caveats and Resolved Caveats sections in this release notes list the caveats for this release. The following information is provided for each caveat:

- 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). These IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific caveat.
- Description—A description of what is observed when the caveat occurs.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST), which is the online successor to the Bug Toolkit, is designed to improve the effectiveness in network risk management and device troubleshooting. The BST allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key 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 how to use the Cisco Bug Search Tool effectively, including how to set email alerts for bugs, filter bugs, and save 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 is displayed with 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 has been marked Cisco Confidential

Open Caveats

There are no open caveats in Release 2.1.2.0 and 2.1.2.7.

.

Resolved Caveats

This section lists the caveats that have been resolved in Cisco Wireless Release 2.1.2.0 and 2.1.2.7.

Table 1: Resolved Caveats for Release 2.1.2.7

Caveat Identifier	Caveat Description
CSCvw84662	Webauth tests failing with clearpass after passing for several hours

Table 2: Resolved Caveats for Release 2.1.2.0

Caveat Identifier	Caveat Description
CSCvt18455	Outlook sensor test says `enter URL` but test fails if `http://` or `https://` is prefixed to the URL.
CSCvt32126	Sensor fails to enroll with ISE via SCEP. Displays error: `sscep: wrong MIME content type`
CSCvu16462	Cisco Aironet 1800s Active Sensor cannot PnP through wireless
CSCvu48137	Sensor EAP-TLS tests fail if the SSID contains spaces
CSCvu23069	Cisco Aironet 1800s Active Sensor: Sensor time is not sync'ing with NTP

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

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.

- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.