802.1X Client Exclusion on an AireOS WLC

Contents

Introduction
Prerequisites
Requirements
Components Used
User Cases
How 802.1X Client Exclusion Works
Exclusion Settings to Protect RADIUS Servers from Overload
Problems That Prevent 802.1X Exclusion from Working
Clients Not Excluded Due to WLC EAP Timer Settings
Clients Not Excluded Due to ISE PEAP Settings
Related Information

Introduction

This document describes the 802.1X Client Exclusion on an AireOS Wireless LAN Controller (WLC). 802.1X Client Exclusion is an important option to have on a 802.1X authenticator such as a WLC. This is in order to prevent an overload of the authentication server infrastructure by Extensible Authentication Protocol (EAP) clients that are hyperactive or function improperly.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco AireOS WLC
- 802.1X Protocol
- Remote Authentication Dial-In User Service (RADIUS)
- Identity Service Engine (ISE)

Components Used

The information in this document is based on AireOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

User Cases

Example user cases include:
An EAP supplicant that is configured with incorrect credentials. Most supplicants, such as EAP supplicants, cease authentication attempts after a few successive failures. However, some EAP supplicants continue attempts to reauthenticate upon failure, possibly many times per second. Some clients overload RADIUS servers and cause a Denial of Service (DoS) for the whole network.

After a major network failover, hundreds or thousands of EAP clients might simultaneously attempt to authenticate. As a result, the authentication servers might be overloaded and provide a slow response. If the clients or authenticator time out before the slow response is processed, then a vicious cycle can occur where the authentication attempts continue to time out, and then try to process the response again.

Note: An admission control mechanism is required in order to allow authentication attempts to succeed.

How 802.1X Client Exclusion Works

802.1X Client Exclusion prevents clients from sending authentication attempts for a period of time after excessive 802.1X authentication failures. On an AireOS WLC 802.1X, client exclusion is globally enabled under Security > Wireless Protection Policies > Client Exclusion Policies by default and can be seen in this image.

Client Exclusion Policies

- Excessive 802.11 Association Failures
- Excessive 802.11 Authentication Failures
- Excessive 802.1X Authentication Failures
- IP Theft or IP Reuse
- Excessive Web Authentication Failures

Client Exclusion can be enabled or disabled on a per-WLAN basis. By default it is enabled with a timeout of 60 seconds before AireOS 8.5 and 180 seconds starting in AireOS 8.5.
Exclusion Settings to Protect RADIUS Servers from Overload

In order to validate that the RADIUS server is protected from overload due to wireless clients that function incorrectly, verify that these settings are in effect:

- **Excessive 802.1X Authentication Failures** is selected in the WLC's global Client Exclusion Policies.
- **Client Exclusion** is set to Enabled in the WLAN's advanced settings.
- **Client Exclusion Timeout Value** is set to 60 to 300 seconds.
  - Note: Values higher than 300 seconds provide better protection but might trigger user complaints.
- Configure AireOS EAP timers and ISE Protected Extensible Authentication Protocol (PEAP) settings

Problems That Prevent 802.1X Exclusion from Working

Several configuration settings, in the WLC and in the RADIUS server might prevent 802.1X Client Exclusion from working.

Clients Not Excluded Due to WLC EAP Timer Settings

By default, wireless clients are not excluded when **Client Exclusion** is set to Enabled on the WLAN. This is due to long default EAP timeouts of 30 seconds which cause a client that misbehaves never to hit enough successive failures to trigger an exclusion. Configure shorter EAP timeouts with increased numbers of retransmissions to allow the 802.1X Client Exclusion to take effect. See the timeout example.
Clients Not Excluded Due to ISE PEAP Settings

In order for 802.1X Client Exclusion to work, the RADIUS server must send an Access-Reject when authentication fails. If the RADIUS server is ISE and if PEAP is in use, then exclusion might not happen and it depends on the ISE PEAP settings. Within ISE, navigate to Policy > Results > Authentication > Allowed Protocols > Default Network Access as shown in the image.

If you set **Retries** (circled in red on the right) to 0, then ISE should send Access-Reject immediately to the WLC, which should enable the WLC in order to exclude the client (if it tries three times to authenticate).

**Note:** The setting of **Retries** is somewhat independent of the **Allow Password Change** checkbox, i.e. The **Retries** value will be honored, even if **Allow Password Change** is unchecked. However, if **Retries** is set to 0, then **Allow Password Change** will not work.

**Related Information**

- Cisco Bug ID: [CSCsq16858](https://supportforums.cisco.com/docs/DOC-10507)
- Prevent Large-Scale Wireless RADIUS Network Melt Downs
- Technical Support & Documentation - Cisco Systems