

ISE Admin GUI Login Fails with PingID Federation RADIUS Token

Contents

Issue

Administrator GUI login to Cisco ISE fails when using PingID federation as a RADIUS token, despite packet captures showing that Ping Federate returns an Access-Accept response. The login failure occurs even though the RADIUS authentication appears successful from a network perspective, preventing administrative access to the ISE interface. Network packet analysis confirms that the PingID server (10.32.154.200) sends the expected Access-Accept response to ISE (10.2.200.241), but the ISE admin login process still fails to complete successfully.

Environment

- Cisco Identity Services Engine (ISE) version 3.3 Patch 7
- 4-node VM deployment
- PingID federation configured as RADIUS token authentication
- ISE IP address: 10.2.200.241
- PingID server IP address: 10.32.154.200
- Admin Access configuration reviewed under Administration > Admin Access

Resolution

The issue was resolved through the application of a workaround that enabled successful admin login functionality. The steps described in the next sections were taken to address the problem.

Step 1: Evidence Collection and Analysis

Packet capture evidence was collected and analyzed to confirm the RADIUS authentication flow between ISE and the PingID server. The analysis verified that Ping Federate was correctly sending Access-Accept responses.

Step 2: Evidence from prrt-server.log

###

prrt-server.log

```
RadiusTokenIDStore,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/  
RadiusClient,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/183397  
RadiusClient,2026-03-27 13:25:05,074,DEBUG,0x7f490d6b9700,NIL-CONTEXT,onProcessResponse: Processing Res  
RadiusClient,2026-03-27 13:25:05,074,WARN ,0x7f49444c6700,cntx=0180887321,sesn=SIT2194/554866250/183397
```

###

Step 3: What is the Message-Authenticator?

The Message-Authenticator is a security attribute used in RADIUS packets to ensure the integrity and authenticity of the messages exchanged between network devices and the RADIUS server. It is a cryptographic signature computed using HMAC-MD5 over the entire RADIUS packet with a shared secret key. This attribute helps protect against tampering and spoofing of RADIUS messages, especially those involving Extensible Authentication Protocol (EAP) authentication flows.

Step 4: Workaround Implementation

Disable "Message Authenticator Required On Response": Administration / Identity Management / External Identity Sources / RADIUS Token. Click on the RADIUS Token name, then go to Authentication. Uncheck "Message Authenticator Required On Response."

Step 5: Validation Testing

After applying the workaround, admin login tests were executed to validate the resolution. These tests confirmed successful authentication and access to the ISE admin GUI using PingID federation as the RADIUS token.

Step 6: Monitoring Period

A monitoring and validation period was established to ensure the stability of the workaround. During this period, continued admin login testing was performed with no errors or failures reported.

Cause

The ISE Admin GUI login failure was caused by a RADIUS protocol security enforcement mismatch between Cisco ISE 3.3 Patch 7 and PingID (Ping Federate) during MFA authentication.

Specifically:

- Cisco ISE **required the RADIUS** Message-Authenticator **attribute** to be present in the **Access-Accept** response from the external RADIUS token server.
- PingID was returning **Access-Accept** responses **without the** Message-Authenticator **attribute**.
- Because ISE had the setting **Message Authenticator Required On Response** enabled, it silently rejected the RADIUS response as invalid, even though the authentication itself succeeded on the PingID side.
- This enforcement is part of Cisco ISE's security hardening to mitigate the Blast-RADIUS vulnerability (CVE-2024-3596).

Related Content

- [Blast-RADIUS Protocol Spoofing Mitigation \(CVE-2024-3596\)](#)