

Troubleshoot SSH Authentication Failure on ASA with RADIUS Using One-Time Password

Contents

Issue

The Secure Shell (SSH) access to Adaptive Security Appliance (ASA) software with Remote Authentication Dial-In User Service (RADIUS) using One-Time Password (OTP) fails when the CiscoSSH Stack is enabled.

These syslog messages are generated:

```
Nov 14 2025 16:28:35: %ASA-6-113010: AAA challenge received for user from server .  
Nov 14 2025 16:28:35: %ASA-4-109033: Authentication failed for admin user from . Interactive challenge
```

Environment

The symptoms are observed when all conditions match:

- Secure Firewall 1230 with ASA in single or multicontext mode. Other hardware platforms are also affected.
- RADIUS server is used for SSH authentication:

```
<#root>
```

```
device#
```

```
show run | i aaa
```

```
aaa-server RAD-OTP protocol radius  
aaa-server RAD-OTP (management) host 192.0.2.1  
aaa-server RAD-OTP (management) host 192.0.2.2  
aaa authentication ssh console RAD-OTP
```

- The RADIUS server requests and requires a valid OTP code or challenge for successful authentication.
- CiscoSSH stack is enabled on ASA.
- In versions 9.19.1 and later the CiscoSSH stack is enabled by default and can be optionally disabled using the **no ssh stack cisco** command. Use the **show ssh** command for verification:

```
<#root>
```

```
device#
```

```
show ssh
```

```
ssh secure copy : ENABLED
```

```
ciscoSSH stack : DISABLED
```

- In versions 9.23.1 and later this stack cannot be disabled or verified.

Resolution

The symptoms are successfully reproduced in the internal lab and tracked in the Cisco bug ID [CSCwt57790](#).

Use one of these workaround options in affected versions:

- Use local authentication for SSH connections.
- On the RADIUS server disable OTP requirement for ASA.
- In earlier than 9.23 disable the CiscoSSH stack using the **no ssh stack cisco** command. Ensure to review [Cisco Secure Firewall ASA Series Command Reference, S Commands](#) and assess the potential impact of disabling the CiscoSSH stack.

Cause

The cause of the authentication failure is the Cisco bug ID [CSCwt57790](#).

Related Content

- Cisco bug ID [CSCwi04513](#)
- Cisco bug ID [CSCwt57790](#)
- [Cisco Secure Firewall ASA Series Command Reference, S Commands](#)