

# Problemen oplossen met SSH-verificatie op ASA met RADIUS met behulp van een eenmalig wachtwoord

## Inhoud

---

---

## uitgeven

De toegang tot Adaptive Security Appliance (ASA)-software met de Remote Authentication Dial-In User Service (RADIUS) met behulp van het eenmalige wachtwoord (OTP) mislukt wanneer de CiscoSSH-stapel is ingeschakeld.

Deze syslog berichten worden gegenereerd:

```
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
```

## milieu

De symptomen worden waargenomen wanneer alle omstandigheden overeenkomen:

- Beveiligde Firewall 1230 met ASA in single- of multicontextmodus. Ook andere hardwareplatforms worden getroffen.
- RADIUS-server wordt gebruikt voor SSH-verificatie:

```
<#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
```

- De RADIUS-server vraagt en vereist een geldige OTP-code of uitdaging voor een succesvolle verificatie.
- CiscoSSH-stack is ingeschakeld op ASA.
- In versie 9.19.1 en hoger is de Cisco SSH-stack standaard ingeschakeld en kan deze optioneel worden uitgeschakeld met de opdracht `no ssh-stack cisco`. Gebruik de opdracht `show ssh` voor verificatie:

```
<#root>
```

```
device#
```

```
show ssh
```

```
ssh secure copy : ENABLED
```

```
ciscoSSH stack : DISABLED
```

- In versie 9.23.1 en hoger kan deze stapel niet worden uitgeschakeld of geverifieerd.

## resolutie

De symptomen worden succesvol gereproduceerd in het interne lab en gevolgd in de Cisco bug ID [CSCwt57790](#).

Gebruik een van deze opties voor een tijdelijke oplossing in de betreffende versies:

- Gebruik lokale verificatie voor SSH-verbindingen.
- Schakel op de RADIUS-server de OTP-vereiste voor ASA uit.
- In eerder dan 9.23 schakelt u de Cisco SSH-stack uit met de opdracht `no ssh-stack cisco`. Zorg ervoor dat u [Cisco Secure Firewall ASA Series Command Reference, S Commands](#)

bekijkt en de potentiële impact van het uitschakelen van de Cisco SSH-stack beoordeelt.

## Oorzaak

De oorzaak van de verificatiefout is de Cisco-bug-ID [CSCwt57790](#).

## Verwante inhoud

- Cisco bug ID [CSCwi04513](#)
- Cisco bug ID [CSCwt57790](#)
- [Cisco Secure Firewall ASA Series, opdrachtverwijzing, S-opdrachten](#)

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.