

sshd[3167]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"

306 admin July 22, 2025 [Common Errors & Troubleshooting](#) 24355

How to solve the error sshd[3167]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root" ?

A promotional banner for EZEELOGIN. On the left, the logo 'EZEELOGIN' is displayed above the text 'Record, monitor and track SSH sessions of your employees'. Below this, a white button contains the text '30 Days Free Trial'. On the right, there is an isometric illustration of a large laptop with a person sitting on it, surrounded by various server racks, a cloud, and other network-related icons, all set against a dark green background.

Overview: This article explains, how to resolve the error "**sshd[3167]: pam_succeed_if(sshd:auth): requirement "uid >= 1000" not met by user "root"**" that appears in the log when root login to a remote server via SSH fails.

Step 1: Check for the logs on the remote server using **tail -f /var/log/secure** or **tail -f /var/log/auth.log**

```
[root@remote_server ~]# tail -f /var/log/secure

Apr 27 13:41:29 otp sshd[3384]: pam_unix(sshd:session): session
closed for user root

Apr 27 13:41:32 otp sshd[3403]: pam_unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.29.43
user=root

Apr 27 13:41:32 otp sshd[3403]: pam_succeed_if(sshd:auth):
requirement "uid >= 1000" not met by user "root"

Apr 27 13:41:34 otp sshd[3401]: error: PAM: Authentication failure
for root from 192.168.29.43

Apr 27 13:41:34 otp sshd[3401]: Received disconnect from
192.168.29.43 port 50064:11: Auth failed [preauth]

Apr 27 13:41:34 otp sshd[3401]: Disconnected from 192.168.29.43 port
50064 [preauth]
```

Step 2: To resolve the issue, make sure that "**PermitRootLogin**" is set to "**yes**" in the **SSHD** configuration file of the remote server. After making this change, **restart** the **sshd** service.

```
[root@remote_server ~]# vi /etc/ssh/sshd_config

PermitRootLogin yes

[root@remote_server ~]# service sshd restart
```

Step 3: To enable root login for localhost and for a specific IP address, use the following configuration in **/etc/ssh/sshd_config**:

```
Match host localhost

    PermitRootLogin yes

    PubkeyAuthentication yes

    PasswordAuthentication yes
```

```
Match Address 192.168.29.74
```

```
    PermitRootLogin yes
```

```
    PubkeyAuthentication yes
```

```
    PasswordAuthentication no
```

Related Articles

[Failed to establish SSH session](#)

[sshd\[902\]: debug1:PAM: password authentication failed for an illegal user: Authentication failure](#)

[Could not connect or access the remote servers/devices](#)

Online URL:

https://www.ezeelogin.com/kb/article/sshd3167-pam_succeed_if-40;sshdauth-41;-requirement-uid=-1000-not-met-by-user-root-306.html