

PA Firewall Configuration:

Navigate to **Device > Server Profile > Radius > Add**. Here to add the details of your RADIUS server. Don't forget to use the same secret key already in the RADIUS configuration. Profile Name: **ISE-RADIUS** can give any name you like. Choose Authentication Protocol: **PAP**, click **add** type any name you like for RADIUS Server I put **ISE-01**, type RADIUS Server IP: **192.168.100.210**, Type Share Secret Key in my case **Test123**, leave the Port 1812 default. Press **OK** to submit.

PA-VM POLICIES OBJECTS NETWORK **DEVICE**

User Identification
Data Redistribution
Device Quarantine
VM Information Sources
Troubleshooting
Certificate Management
Certificates
Certificate Profile
OCSP Responder
SCEP
SSL/TLS Service Profile
SSL Decryption Exclusion
SSH Service Profile
Response Pages
Log Settings
Server Profiles
SNMP Trap
Syslog
Email
HTTP
Netflow
RADIUS
TACACS+
LDAP

RADIUS Server Profile

Profile Name: **ISE-RADIUS**
☐ Administrator Use Only

Server Settings
Timeout (sec): 3
Retries: 3
Authentication Protocol: **PAP**

Servers

NAME	RADIUS SERVER	SECRET	PORT
ISE-01	192.168.100.210	*****	1812

[+ Add](#) [- Delete](#)

Enter the IP address or FQDN of the RADIUS server

OK Cancel

Click **Device** → **Authentication Profile** → **Add**. Here you want to make the type 'RADIUS' and choose the profile you created earlier. Give any name you like in my case **RADIUS-Auth**,

Authentication Profile

Name: RADIUS-Auth

Authentication | Factors | Advanced

Type: RADIUS

Server Profile: ISE-RADIUS

☒ Retrieve user group from RADIUS

User Domain:

Username Modifier: %USERINPUT%

Single Sign On

Kerberos Realm:

Kerberos Keytab: Click "Import" to configure this field X Import

OK Cancel

Navigate to **Advanced** tab click on **Add** button and choose **all** click **OK** to submit.

PA-VM

POLICIES OBJECTS NETWORK **DEVICE**

Setup

High Availability

Config Audit

Password Profiles

Administrators

Admin Roles

Authentication Profile

Authentication Sequence

User Identification

Data Redistribution

Device Quarantine

VM Information Sources

Troubleshooting

Certificate Management

Certificates

Certificate Profile

OCSP Responder

Authentication Profile

Name: RADIUS-Auth

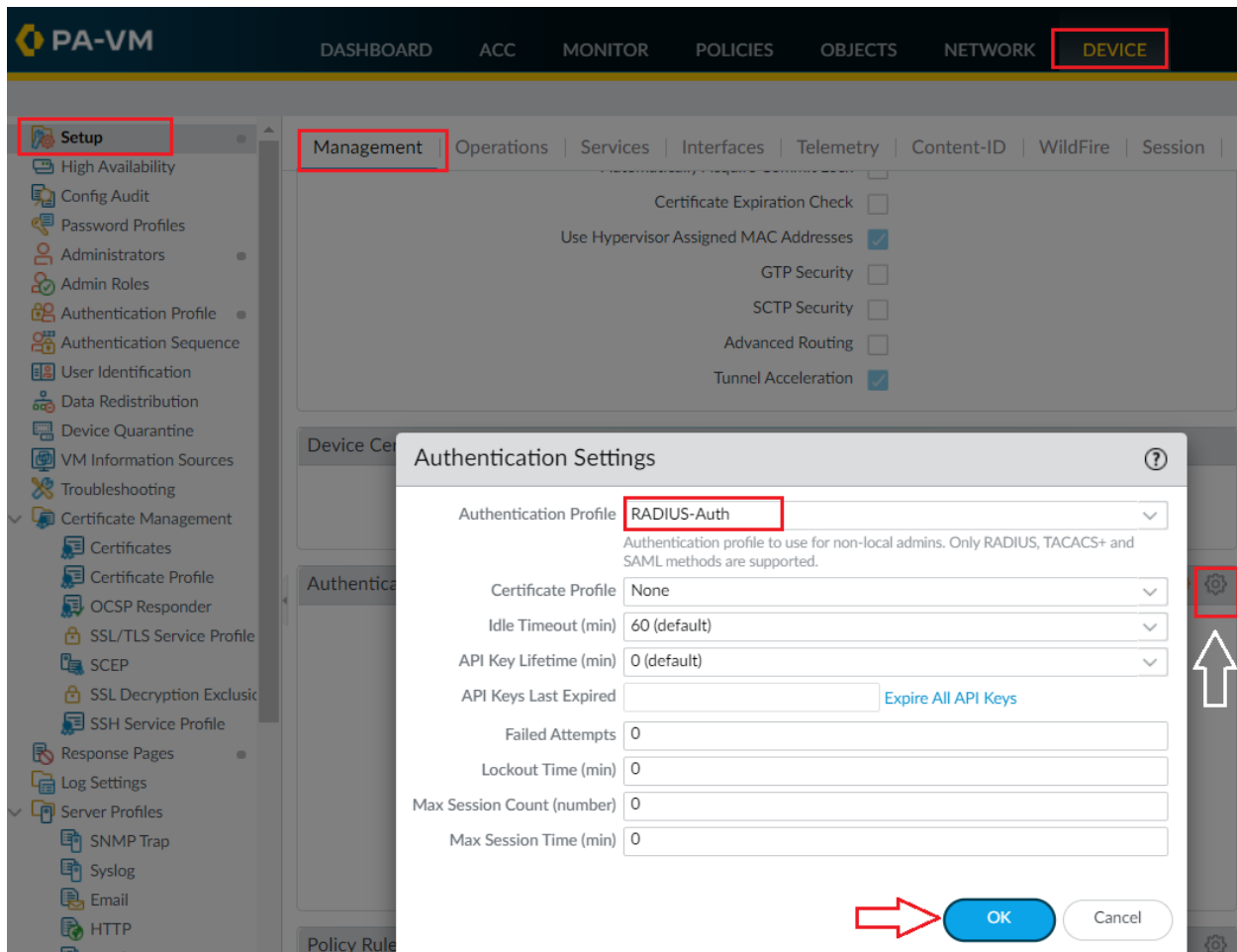
Authentication | Factors **Advanced**

Allow List

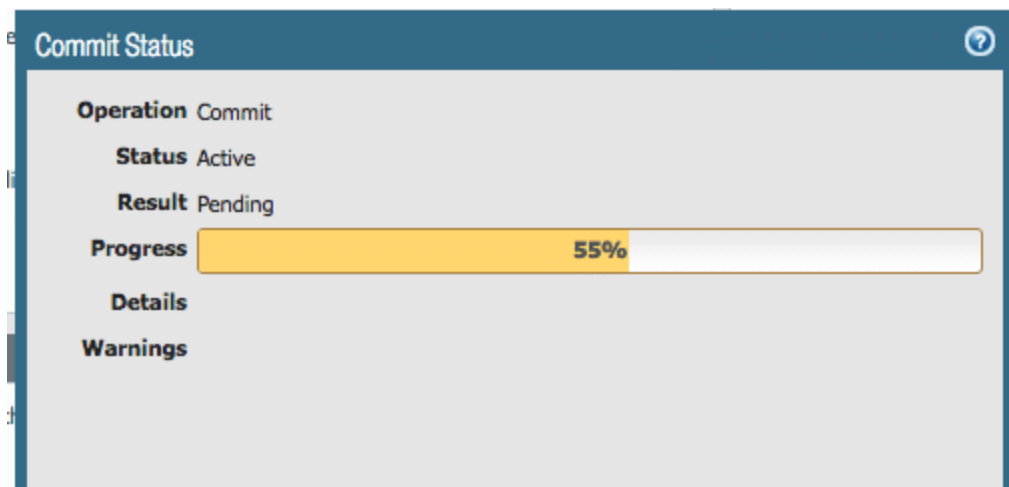
☒ ALLOW LIST

☒ all

Navigate to **Device > Setup > Management > Authentication Settings** click on Gear Icon choose Authentication Profile **RADIUS-Auth** which earlier created Click **OK**.



Commit the Changes by Clicking **Commit** on top right corner to save the configuration.



Testing and Verification:

We can test our configuration by login into the Palo Alto Firewall by SSH. Let's try using the **ad1** user credential.

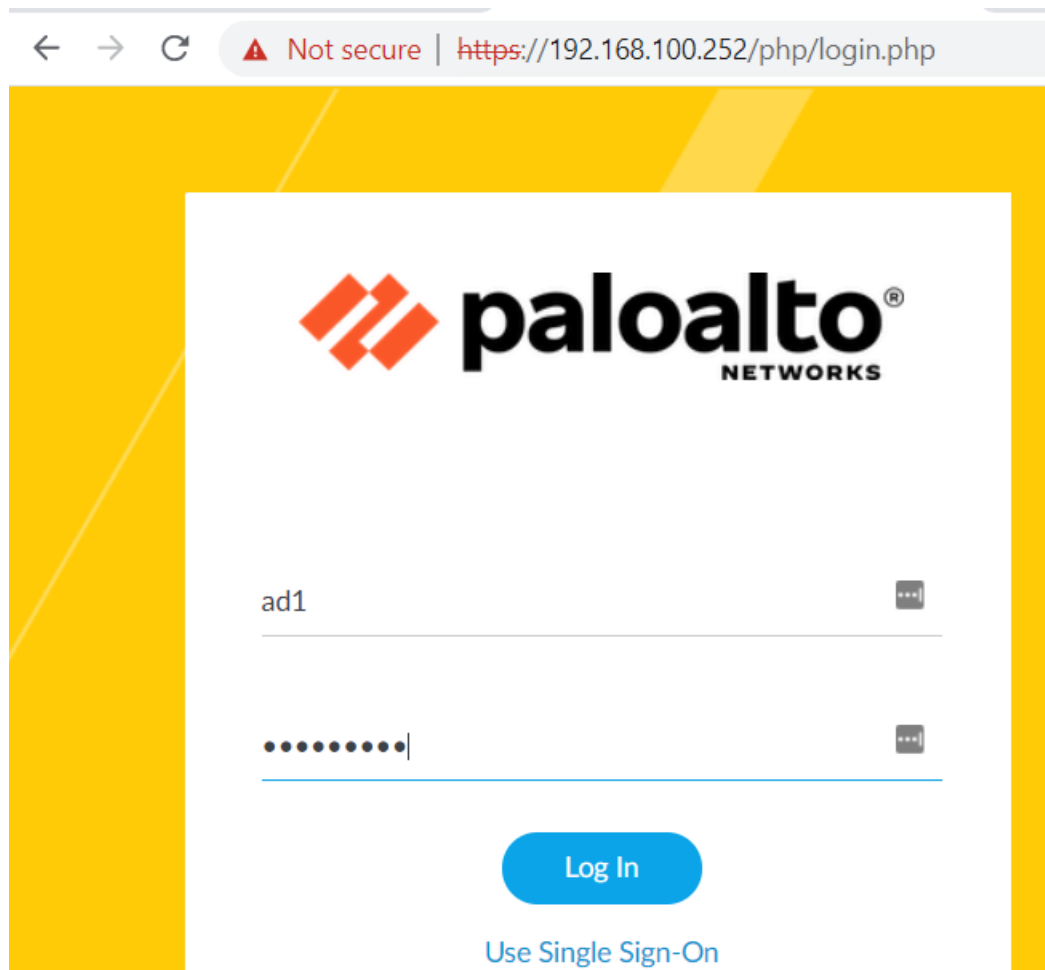
```
192.168.100.252 - PuTTY
login as: ad1
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

Number of failed attempts since last successful login: 0

ad1@PA-VM> configure
Entering configuration mode
[edit]
ad1@PA-VM#
```

```
192.168.100.252 - PuTTY
[edit]
ad1@PA-VM#
  check      Check configuration status
  commit     Commit current set of changes
  copy       Copy a statement
  delete     Delete a data element
  edit       Edit a sub-element
  exit       Exit from this level
  find       Find CLI commands with keyword
  load       Load configuration from disk
  move       Move a node within an ordered collection
  override   Override a template element
  quit       Quit from this level
  rename     Rename a statement
  revert     Revert changes from configuration
  run        Run an operational-mode command
  save       Save configuration to disk
  set        Set a parameter
  show       Show a parameter
  top        Exit to top level of configuration
  up         Exit one level of configuration
  validate   Validate current set of changes

ad1@PA-VM#
```



We can monitor the authentication/authorization logs on ISE **Operations > RADIUS > Live Logs**. The **ad1** user was successfully authenticated and authorized to run privileged commands.

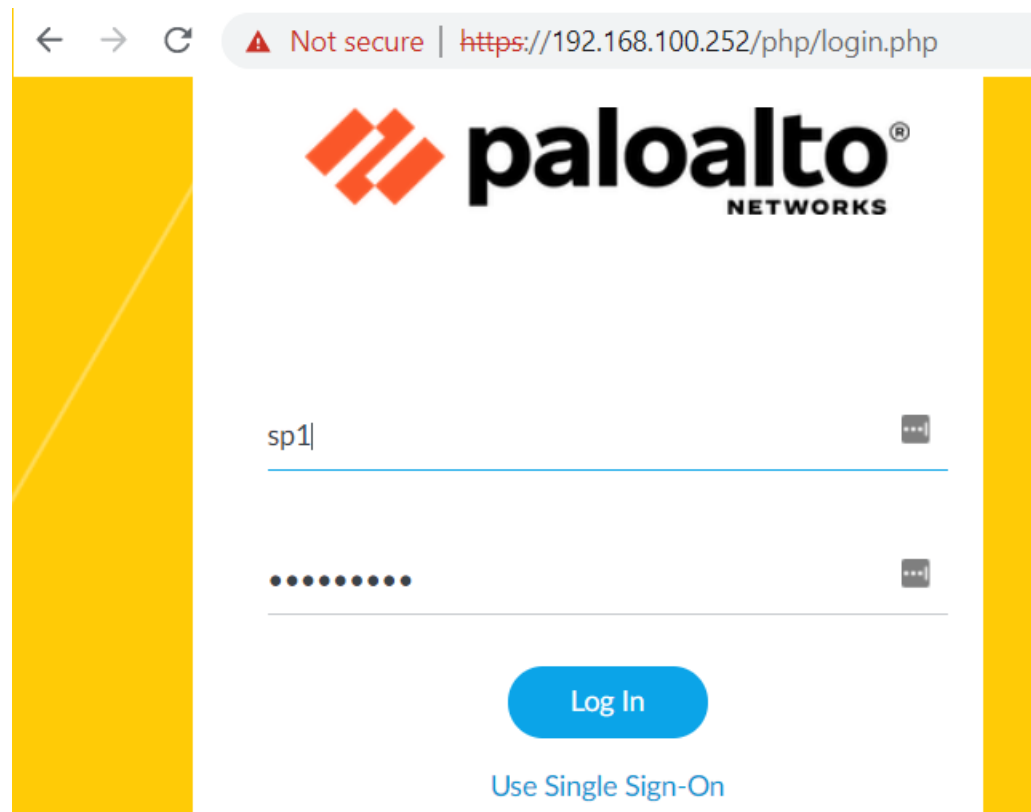
Time	Status	Details	Repeat ...	Identity	Authenticat...	Authorizati...	Authorizati...	IP Address
Dec 07, 2021 03:49:02.236 PM	✓			ad1	PaloAlto-Poli...	PaloAlto-Poli...	PA-AdminGr...	

Now let's try again using support account users **sp1**. The user **sp1** was successfully authenticated but wasn't authorized to run more commands.

```
192.168.100.252 - PuTTY
Keyboard-interactive authentication prompts from server:
| Password:
| End of keyboard-interactive prompts from server

Number of failed attempts since last successful login: 0

sp1@PA-VM> configure
Entering configuration mode
[edit]
sp1@PA-VM#
  check    Check configuration status
  edit     Edit a sub-element
  exit     Exit from this level
  find     Find CLI commands with keyword
  quit     Quit from this level
  run      Run an operational-mode command
  show     Show a parameter
  top      Exit to top level of configuration
  up       Exit one level of configuration
```



We can monitor the authentication/authorization logs on ISE **Operations > RADIUS > Live Logs**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

RADIUS Threat-Centric NAC Live Logs TACACS Troubleshoot Adaptive Network Control Reports

Live Logs Live Sessions

Misconfigured Supplicants 0 Misconfigured Network Devices 0 RADIUS Drops 0 Client 0

Refresh Reset Repeat Counts Export To

Time	Status	Identity	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device
Dec 10, 2021 03:22:07.571 AM	✓	sp1	PaloAlto-Poli...	PaloAlto-Poli...	PA-Support...		PaloAltoFW
Dec 10, 2021 03:21:17.220 AM	✓	ad1	PaloAlto-Poli...	PaloAlto-Poli...	PA-AdminGr...		PaloAltoFW

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Addresses

- Address Groups
- Regions
- Dynamic User Groups
- Applications
- Application Groups
- Application Filters
- Security Profile Groups
- Log Forwarding
- Authentication

NAME	LOCATION	TYPE
abc		IP Netmask

Readonly account Add, Delete and Clone is gray

+ Add - Delete Clone PDF/CSV

PA-VM DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

Logs

- Traffic
- Threat
- URL Filtering
- WildFire Submissions
- Data Filtering
- HIP Match
- GlobalProtect
- IP-Tag
- User-ID
- Decryption
- Tunnel Inspection
- Configuration
- System
- Alarms
- Authentication

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
12/07 10:49:59	general	informational	general		User ad1 accessed Monitor tab
12/07 10:49:03	general	informational	general		User ad1 logged in via Web from 192.168.100.6 using https
12/07 10:49:03	auth	informational	auth-success	RADIUS-Auth	authenticated for user 'ad1', auth profile 'RADIUS-Auth', vsys 'shared', server profile 'ISE-RADIUS', server address '192.168.100.210', auth protocol 'PAP', admin role 'superuser', From: 192.168.100.6.
12/07 10:49:03	auth	informational	auth-success	RADIUS-Auth	When authenticating user 'ad1' from '192.168.100.6', a less secure authentication method PAP is used. Please migrate to PEAP or EAP-TTLS. Authentication Profile 'RADIUS-Auth', vsys 'shared', Server Profile 'ISE-RADIUS', Server Address '192.168.100.210'
12/07 10:48:46	general	informational	general		User admin logged out via Web from 192.168.100.6
12/07 10:41:34	general	informational	general		Connection to Update server closed: updates.paloaltonetworks.com, source: 192.168.100.252