PurpleSynapz™

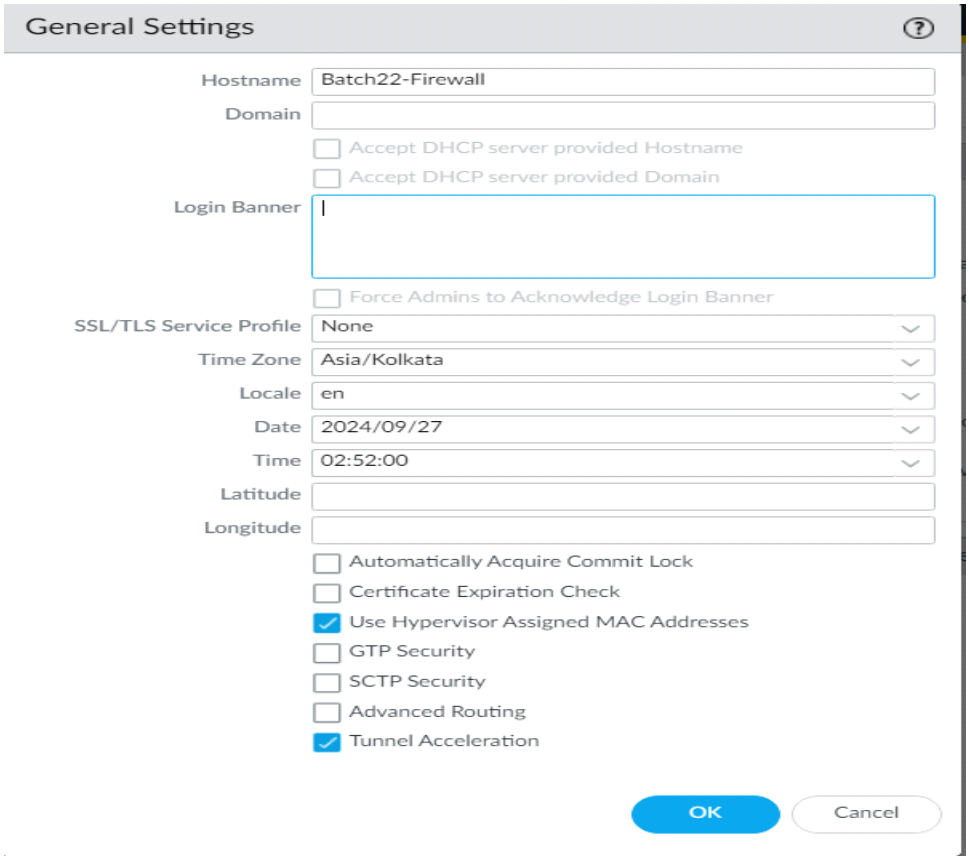
ASSIGNMENT

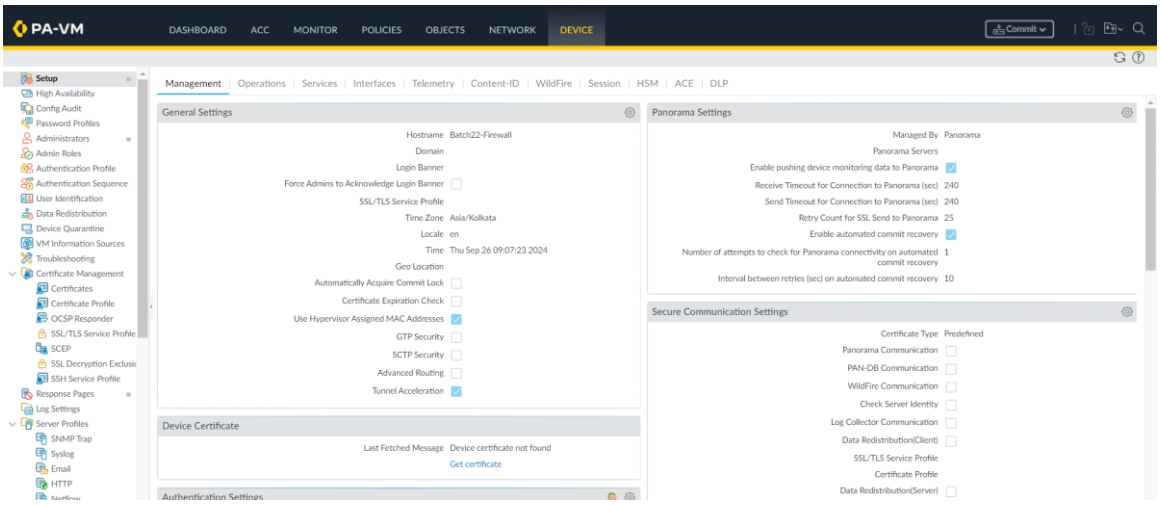
COURSE	PAN Firewall	**ASSIGNMENT NO**	3
MODULE	Firewall	**ASSIGNMENT DATE**	26-Sep-24
STUDENT NAME	Konganti Chaithanya Kumar	**SUBMIT DATE**	26-Sep-24

1. Change the Firewall Name and Time

- **Access the PAN Web Interface:**
  - Log in to the PAN firewall using the web interface with your credentials.
- **Navigate to:**
  - Device > Setup > Management tab.
- **Change Firewall Name:**
  - Under General Settings, click the gear icon to the right of Hostname.
  - Enter the new firewall name and click OK.
- **Change System Time:**
  - Under Operations in the same tab, click Set Time.
  - Update the time and time zone as needed.
  - Click OK to apply changes.

Screenshot: After changing the firewall name and time, take a screenshot from the Management tab.



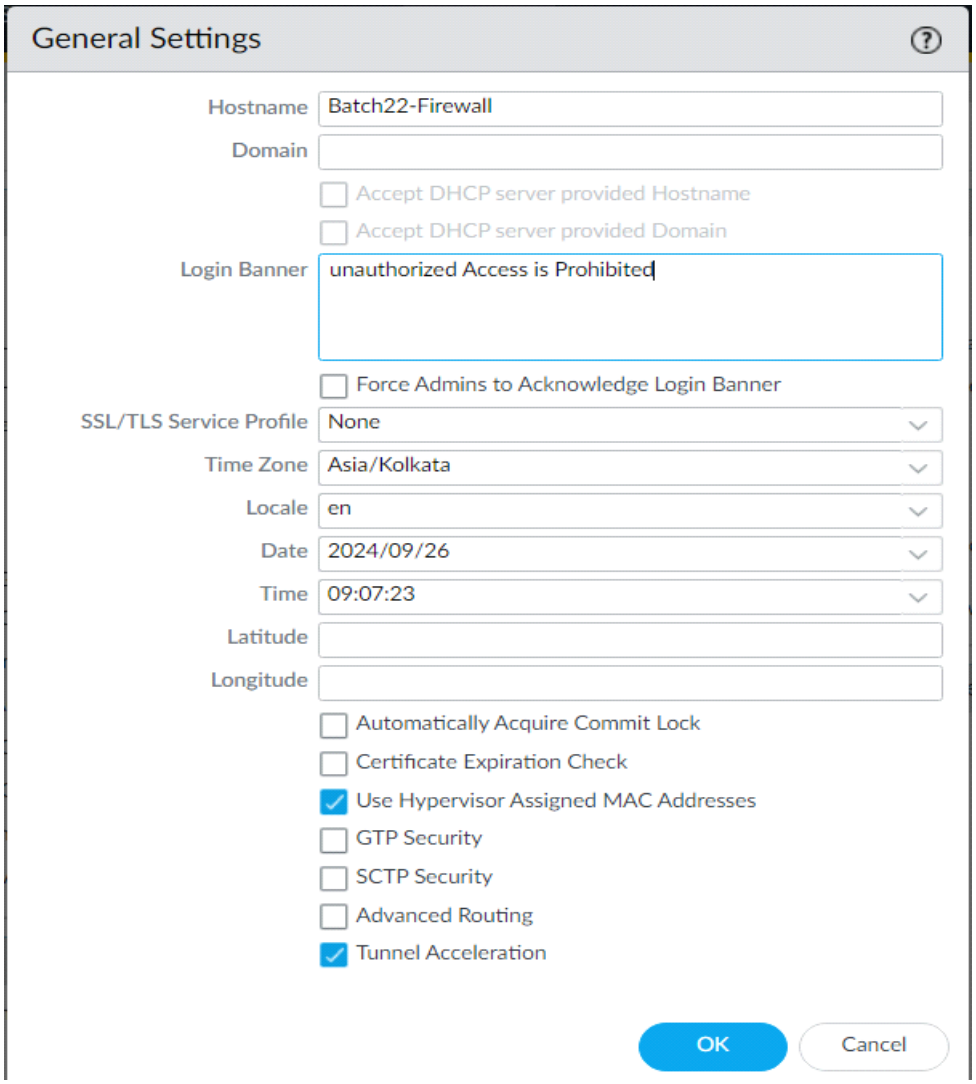


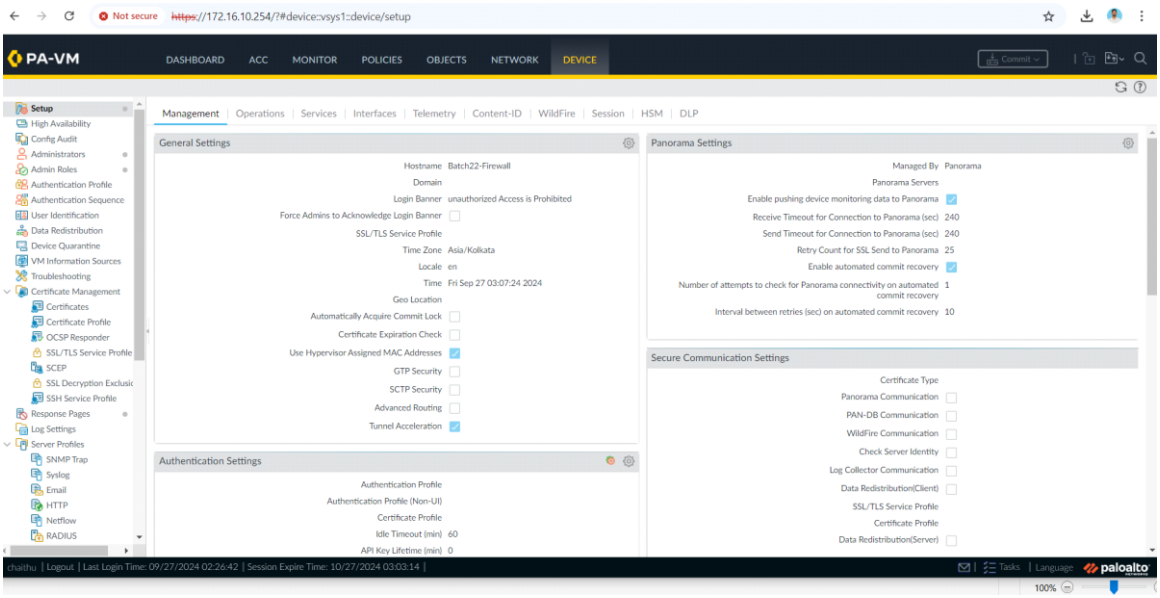
2. Write a Banner and Verify It

- **Access the PAN Web Interface:**
  - Log in to the PAN firewall using the web interface with your credentials.

- **Navigate to:**
    - Device > Setup > Management tab.
- **Write the Banner:**
    - Click the gear icon to the right of Login Banner.
    - Enter the text for your banner and click OK.
- **Verify the Banner:**
    - Logout of the web interface and re-login to see if the banner is displayed correctly.

Screenshot: After logging back in, capture a screenshot showing the banner at the login page.





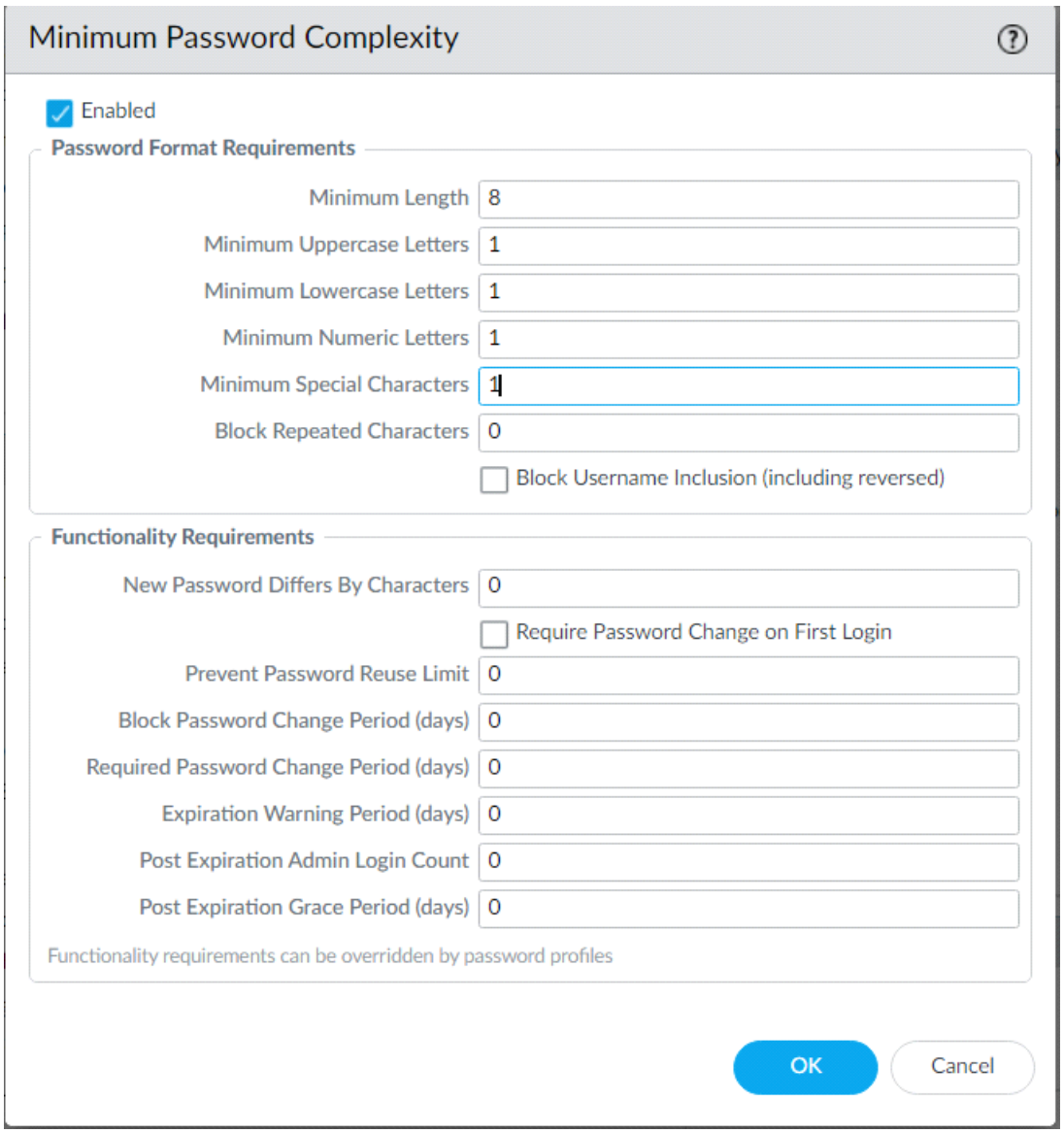
3. Configure a Complex Password Policy

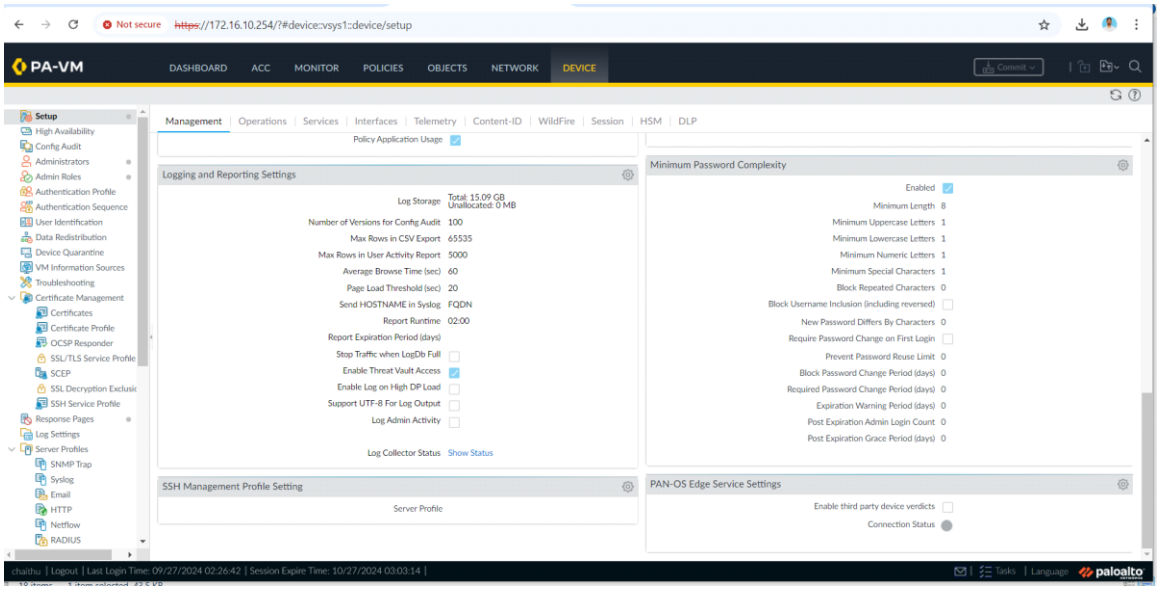
- **Access the PAN Web Interface:**
  - Log in to the PAN firewall using the web interface with your credentials.
- **Navigate to:**
  - Device > Setup > Management > Password Profile.
- **Create a Password Profile:**
  - Click Add and configure the following settings:
    - Minimum length: Set a value (8 characters).
    - Require at least one uppercase letter(1), one lowercase letter(1), one number(1), and one special character(1).
    - Set password expiration days (10).
    - Set the number of failed login attempts before lockout.

- Click OK.

- **Test the Validity:**
  - Create a test user and attempt to set a password that doesn't meet the complexity requirements, and then one that does.

Screenshot: After configuring the policy, capture a screenshot showing the Password Profile screen.

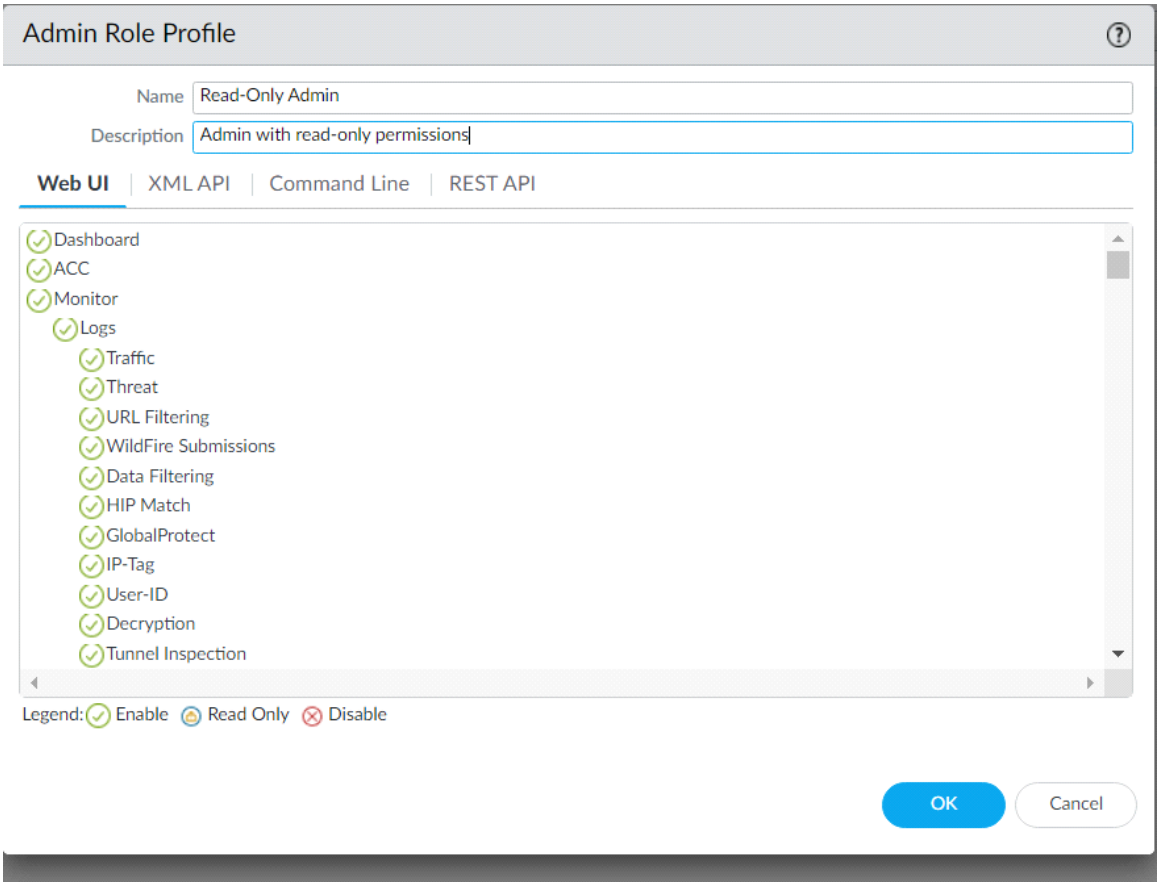


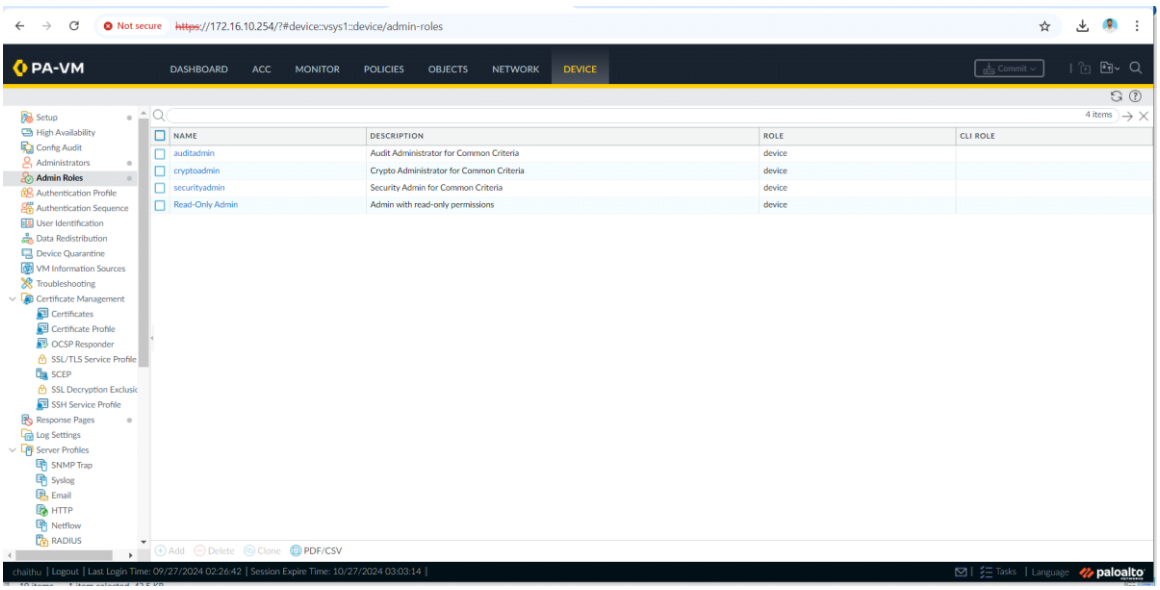


4. Create a Role-Based Profile

- **Access the PAN Web Interface:**
  - Log in to the PAN firewall using the web interface with your credentials.
- **Navigate to:**
  - Device > Admin Roles.
- **Create a New Role:**
  - Click Add and provide a name for the role.
  - Customize the permissions for various system components like Policies, Objects, Network, etc.
  - Save the role by clicking OK.

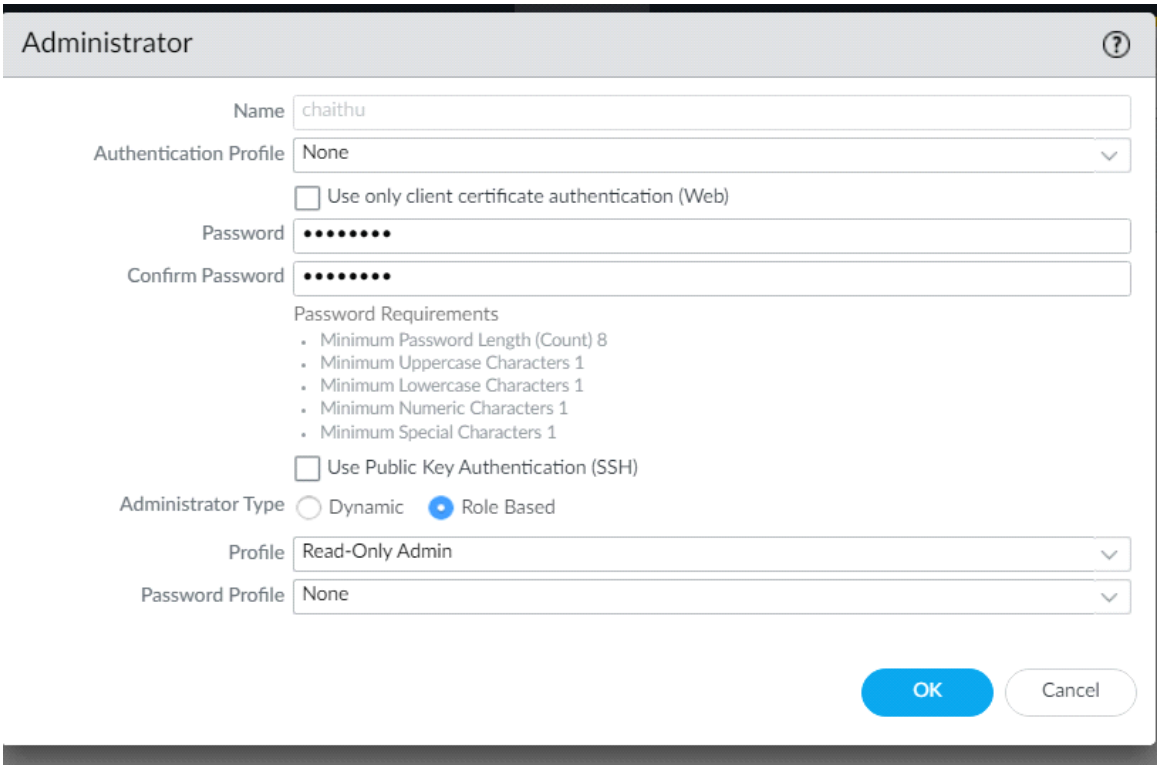
Screenshot: After creating the role, capture a screenshot showing the role settings.


Admin Role Profile
Name
Read-Only Admin
Description
Admin with read-only permissions
Web UI
XML API
Command Line
REST API
Dashboard
ACC
Monitor
Logs
Traffic
Threat
URL Filtering
WildFire Submissions
Data Filtering
HIP Match
GlobalProtect
IP-Tag
User-ID
Decryption
Tunnel Inspection
Legend: Enable Read Only Disable
OK
Cancel


Not secure https://172.16.10.254/?#device:vsys1::device/admin-roles
PA-VM
DASHBOARD
ACC
MONITOR
POLICIES
OBJECTS
NETWORK
DEVICE
NAME
DESCRIPTION
ROLE
CLI ROLE
auditadmin
Audit Administrator for Common Criteria
device
cryptoadmin
Crypto Administrator for Common Criteria
device
securityadmin
Security Admin for Common Criteria
device
Read-Only Admin
Admin with read-only permissions
device

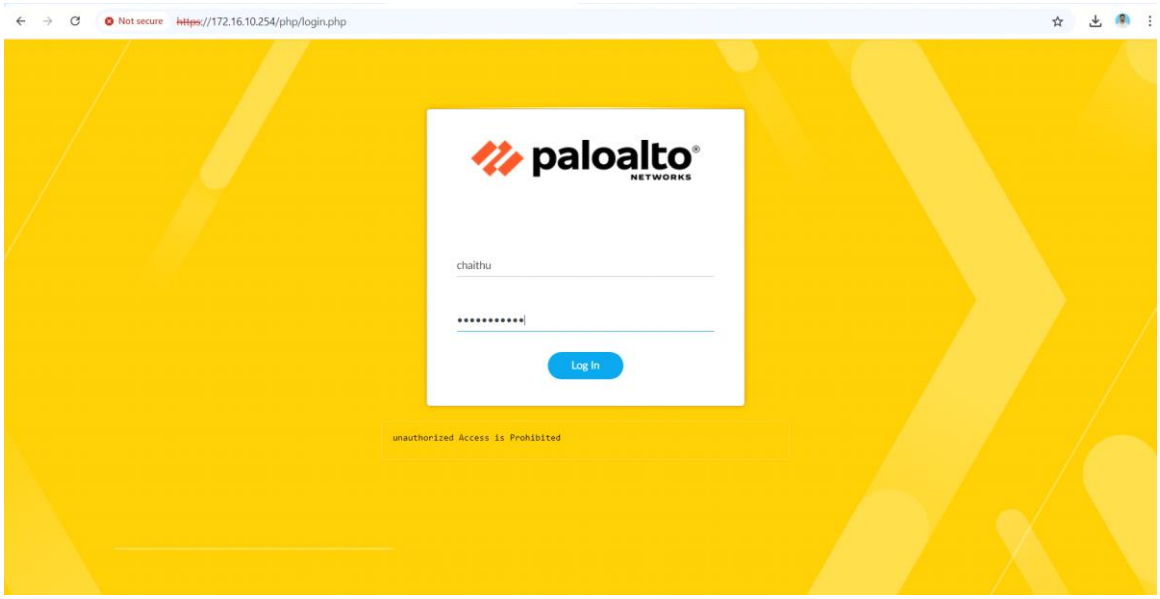
5. Create a User and Assign the Role-Based Profile

- **Access the PAN Web Interface:**
  - Log in to the PAN firewall using the web interface with your credentials.
- **Navigate to the Administrators Section:**
  - Go to the PAN firewall's Web UI.
  - Navigate to Device > Administrators.
- **Add a New Administrator:**
  - In the Administrators section, click the Add button to create a new administrator account.
- **Enter User Details:**
  - **Username:** Enter a username for the new admin (chaithu).
  - **Password:** Enter and confirm a strong password for the user. Ensure the password complies with the complex password policy if you've set one.
- **Assign the Role-Based Profile:**
  - In the Admin Role Profile dropdown, select the role profile you created earlier.
- **Set the Authentication Profile:**
  - In the Authentication Profile section, choose the default profile or any existing authentication profile that is configured.
- **Save the Configuration:**
  - Click OK to save the new administrator.

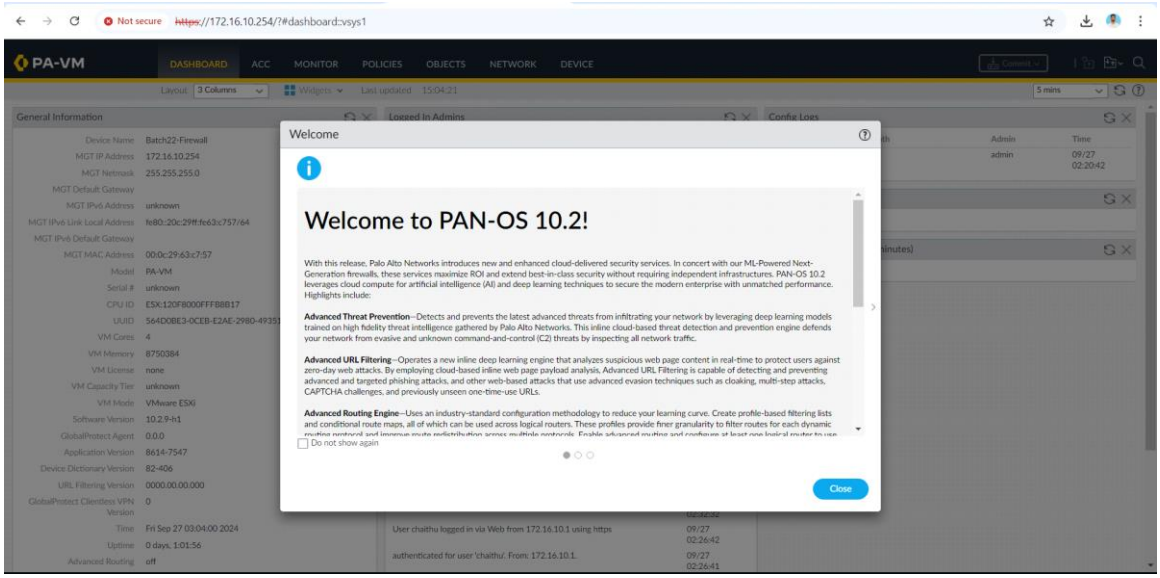


- **Test the Login:**
  - Logout of the web interface and login using the new user's credentials to confirm it works.

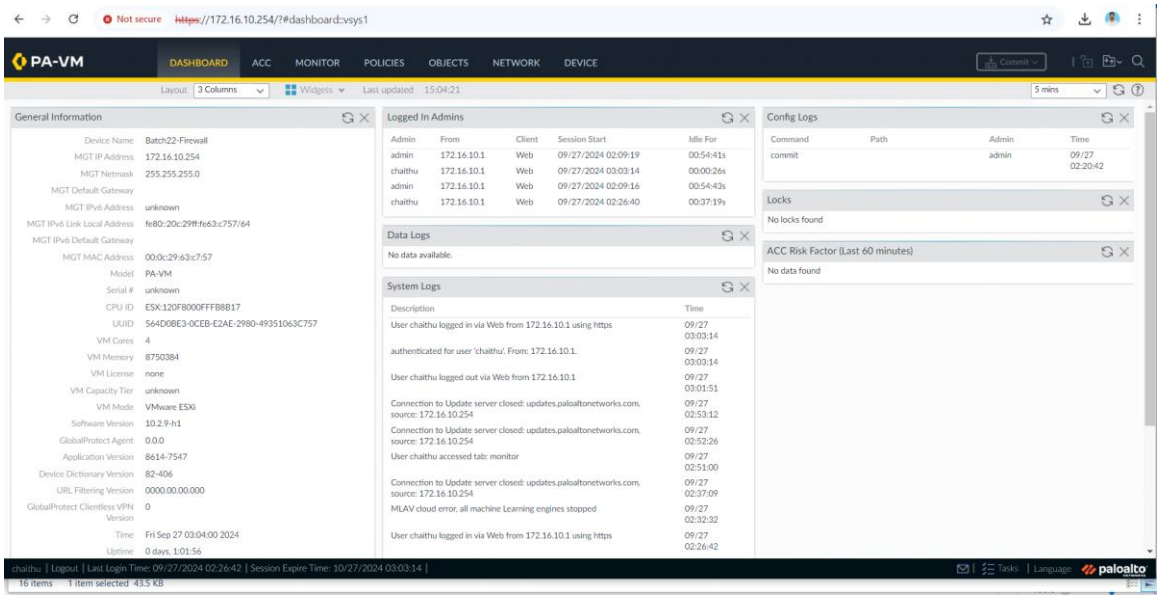
Screenshot: Capture a screenshot after logging in with the new user.



A successful login with the new user's credentials.



Verify the Role:

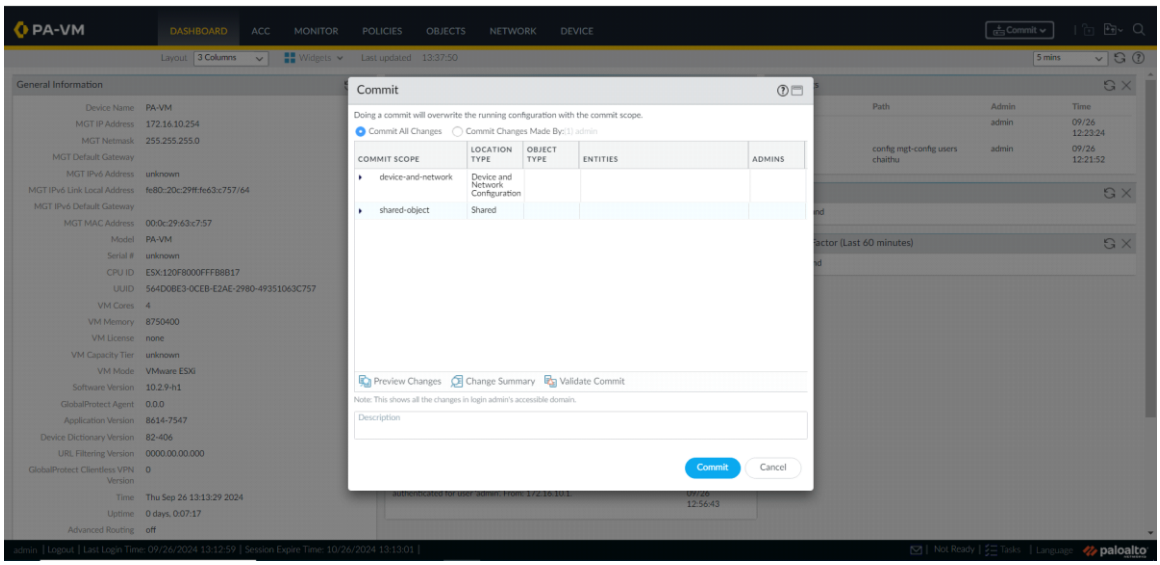


6. Commit the Changes

- **Access the PAN Web Interface:**
  - Log in to the PAN firewall using the web interface with your credentials.
- **Navigate to:**
  - Click Commit in the top-right corner of the web interface.
  - Review the changes and click Commit to apply.

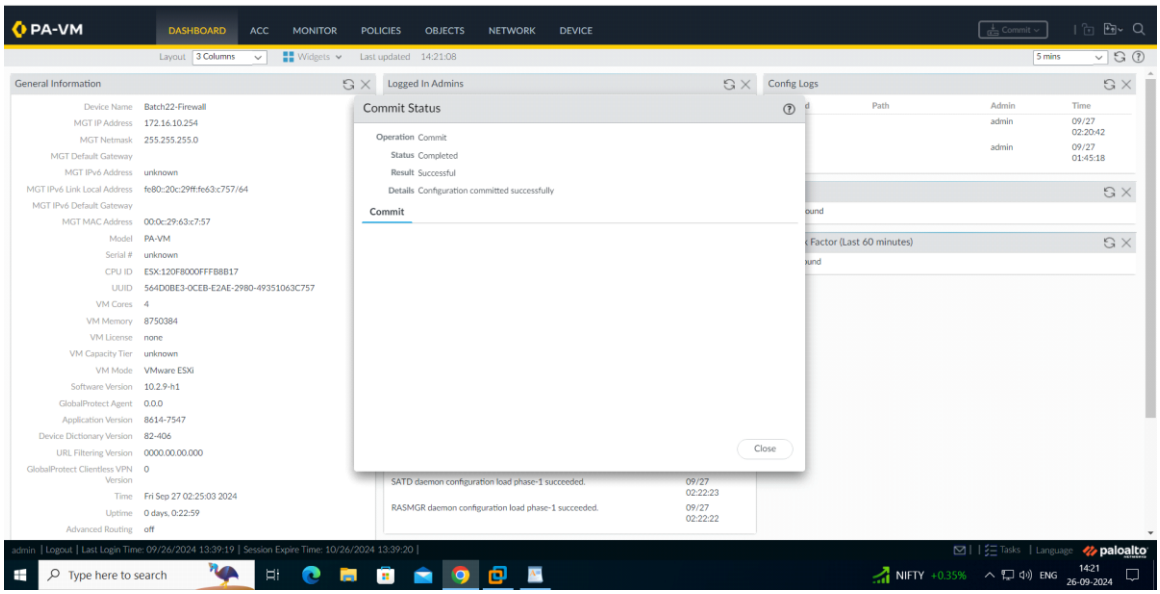
Screenshot: After committing the changes, take a screenshot of the Commit status.

Wait for the Commit to Complete:

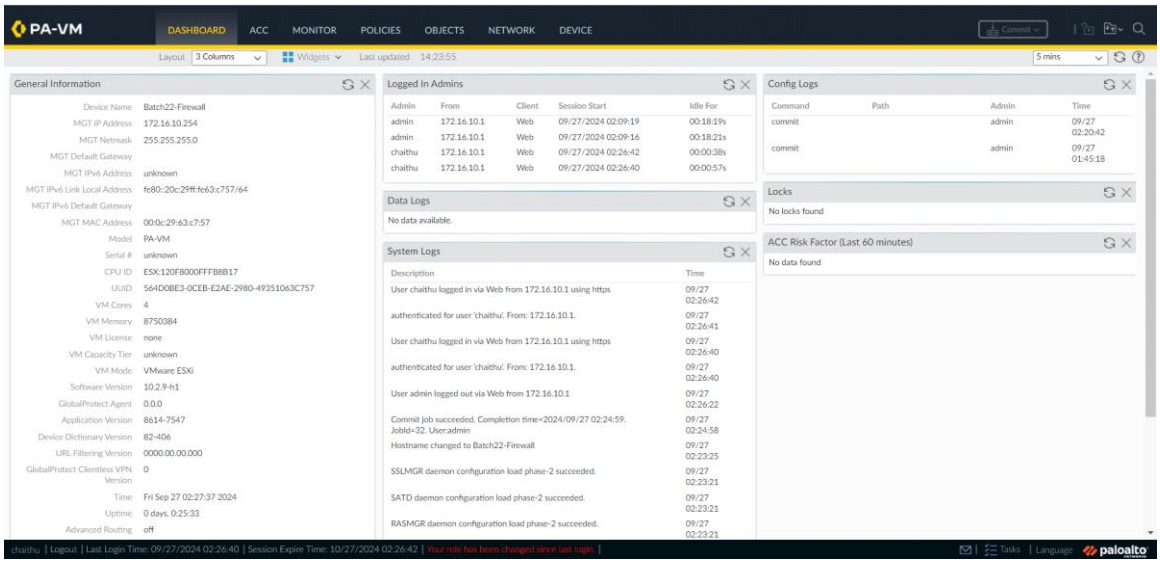


Successfully completed commit:

- **The commit process will take a few seconds to complete, depending on the size and complexity of the changes.**
- **You will see a notification when the commit is successful.**



After Completed welcome page:



Thank You