# Implementing LDAP Authentication For Palo Alto Networks NGFWs

**Dan Edeen**
*dan@edeen.com*
*March 2023*

This document outlines the process to set up LDAP integration between a Palo Alto Networks firewall and an Active Directory environment. In this case the AD DC is Windows Server 2012r2, the Firewall is a VM-based NGFW running PANOS 10.1, and the host environment for both is ESXi 6.7. This document is demonstrative, and many other factors need to be considered for a production environment.

## Step 1: Set Up Active Directory

You will need an Active Directory Domain Controller with groups and users configured. I built and configured this separately, and have included snapshots of key configuration items below.

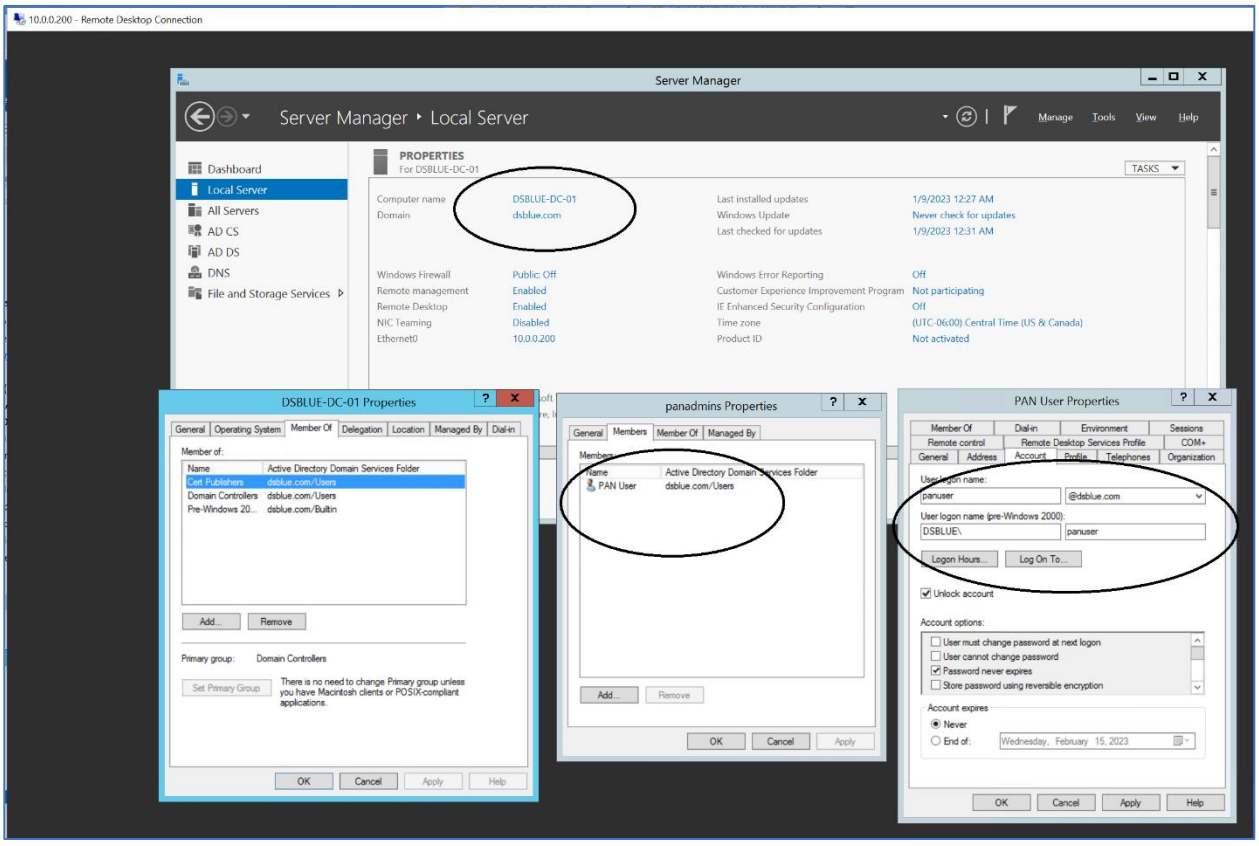


*Figure 1. PAN OS user account on Active Directory. Note the group is panadmins, the username is panuser, and the domain is dsblue.com. Certificate Services (CS) have been installed, a PKI created, and the certificates have been exported.*

## Step 2: Set Up Palo Alto Networks NGFW

For this project I am using a PA-VM, version 10.1.0, running as a VM on ESXi 6.7. This FW has four Ethernet interfaces mapped to two port groups on ESXI, with a pair of interfaces configured as a VWire to allow capturing other VM traffic on this system. Details are shown below.

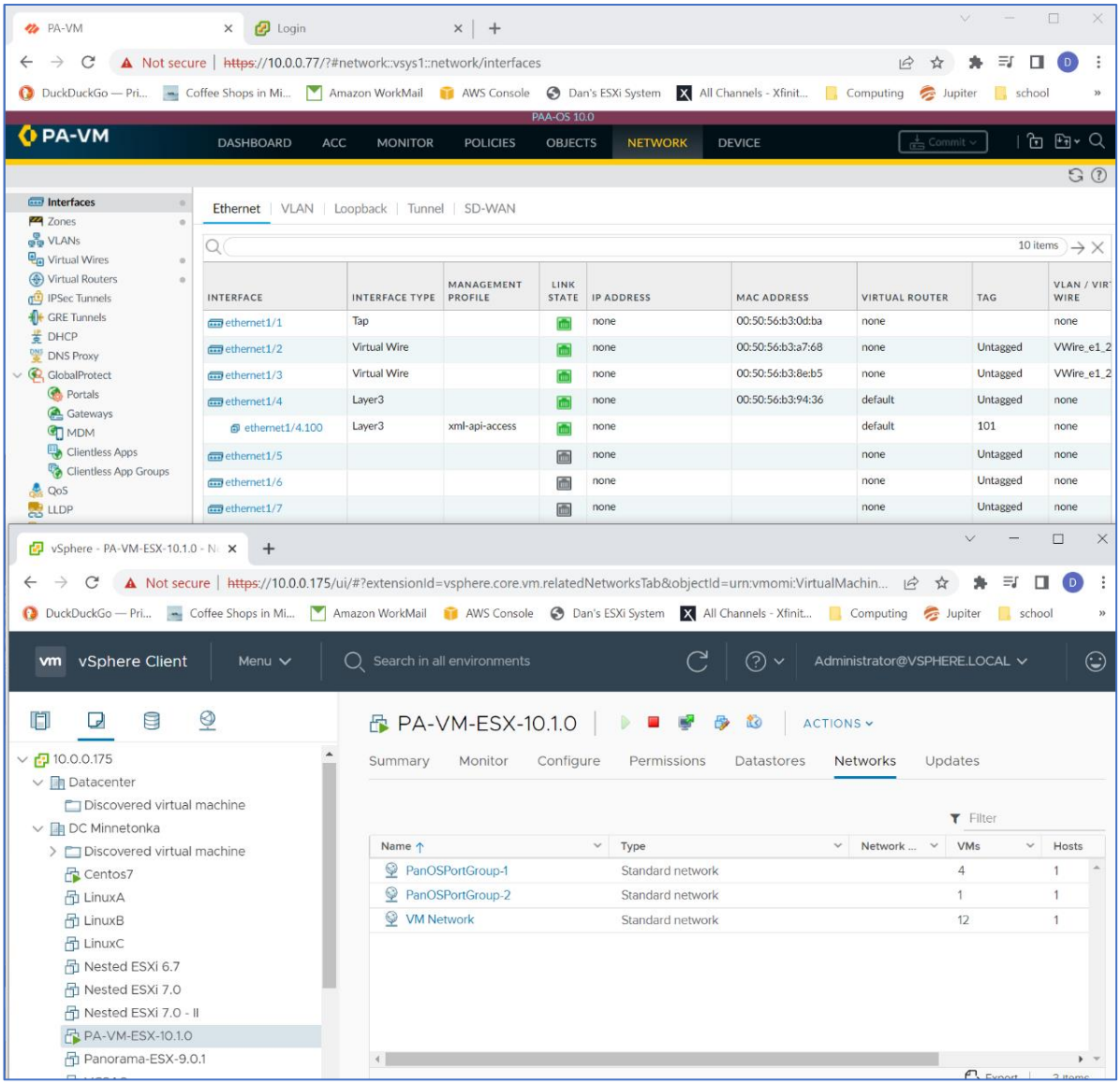


*Figure 2. Palo Alto Networks PA-VM running on ESXi 6.7.*

## Step 3: Configure Palo Alto Networks NGFW for Active Directory Integration

### 3.1 LDAP Server Profile

To integrate the NGFW with the AD, first create an LDAP Server Profile, a Group Mapping, and an Authentication Profile [Device > Server Profiles > LDAP]. These configurations are shown in the following figures.

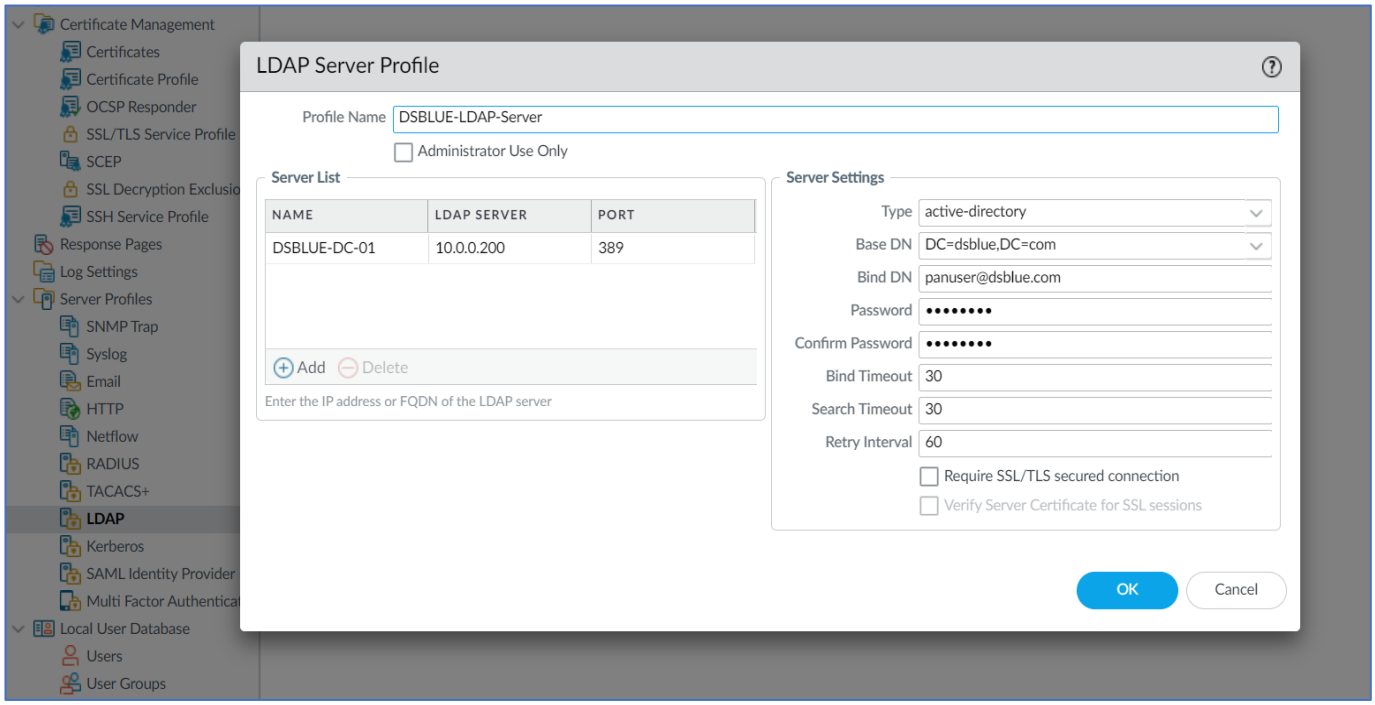


*Figure 3. NGFW LDAP Server Profile. Note that the password used is that which was created on the AD DC for the user 'panuser'.*

## 3.2 Group Mapping

Create a group mapping on the firewall matching the AD group *panadmins* that was created previously [Device > User Identification > Group Mapping Settings]. This allows configuring policy rules for groups instead of individual users.

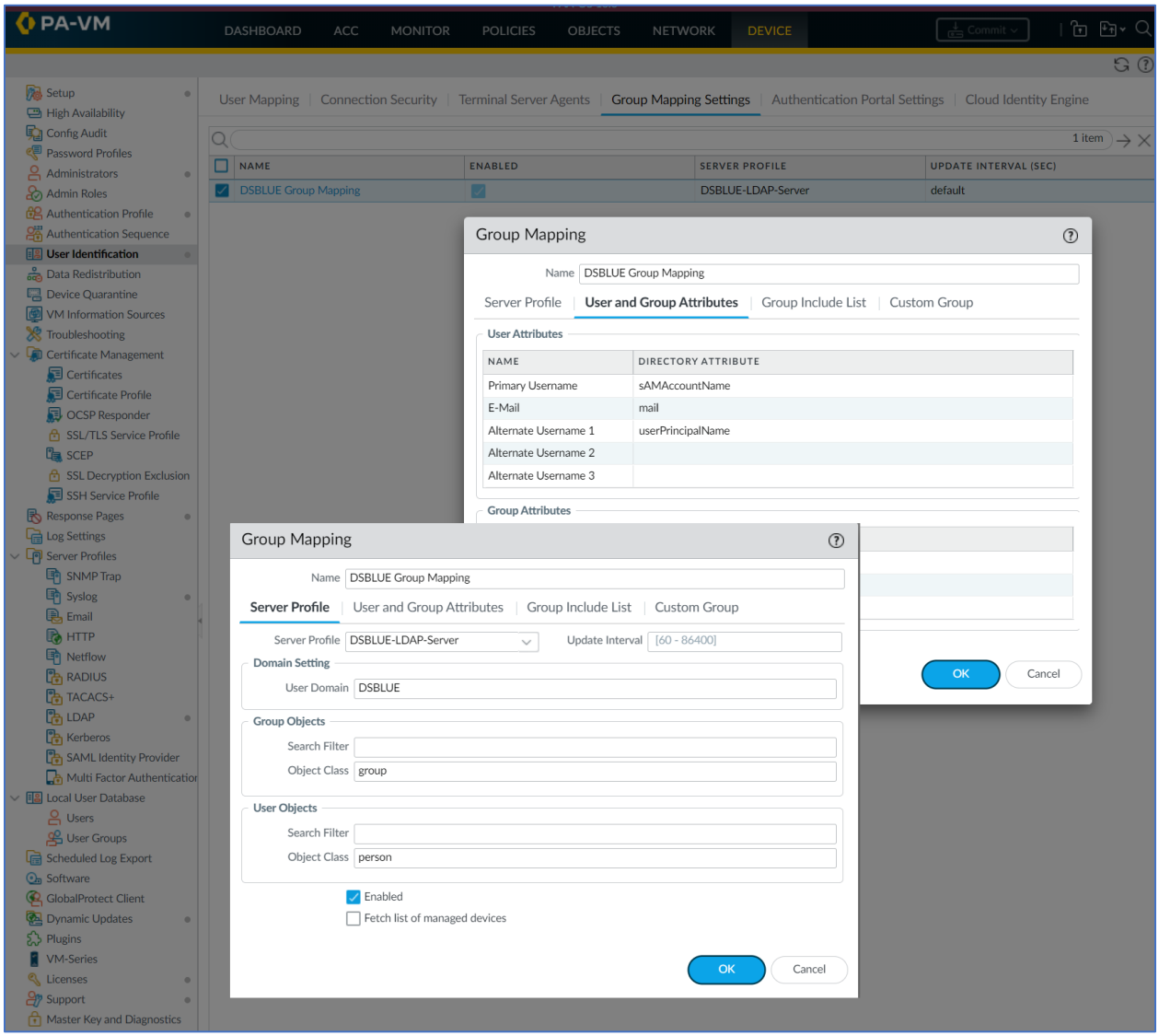


*Figure 4. Group Mapping Server Profile and User and Group Attributes. Note primary username 'sAMAccountName'.*

## 3.3 Authentication Profile

Next create an authentication profile on the firewall [Device > Authentication Profile].

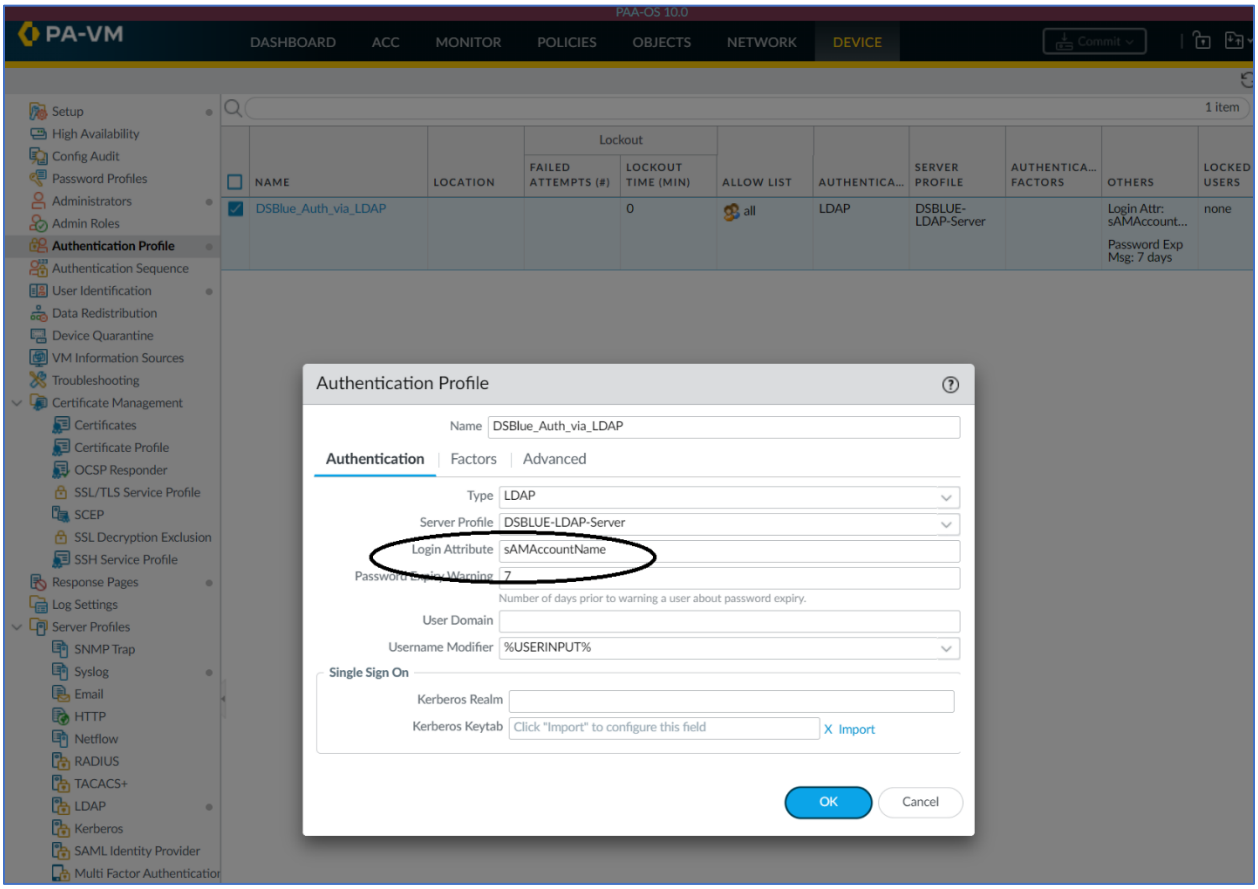


*Figure 5. Authentication Profile. Note the Login Attribute 'sAMAccountName'. You must spell this exactly the same, including the case.*

## 3.4 Administrator Access

Next assign the rights you want this user to have on the firewall [Device > Administrators]. Here I used the account name *panuser*, the authentication profile *DSBlue_Auth_via_LDAP*, and made the administrator a Superuser.

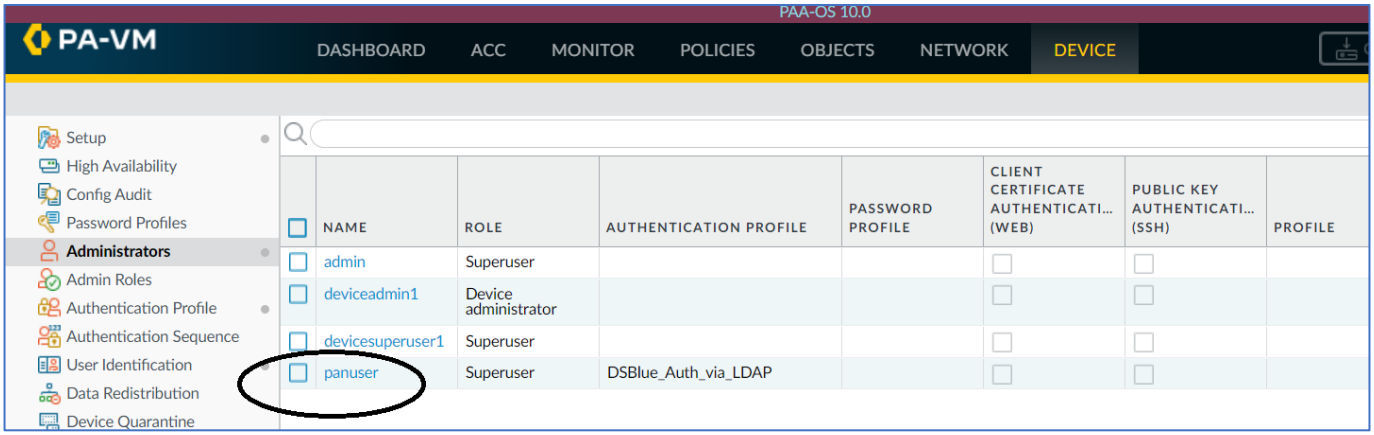


*Figure 6. Set Up Firewall Administrator for AD Account.*

### 3.5 Test The Configuration

After committing the changes to the firewall configuration, you should be able to log in to the PAN FW Management Interface using the account created on the AD DC (panuser in this case). Log in and check that the admin account works as expected. Check the logs at [Monitor > System].

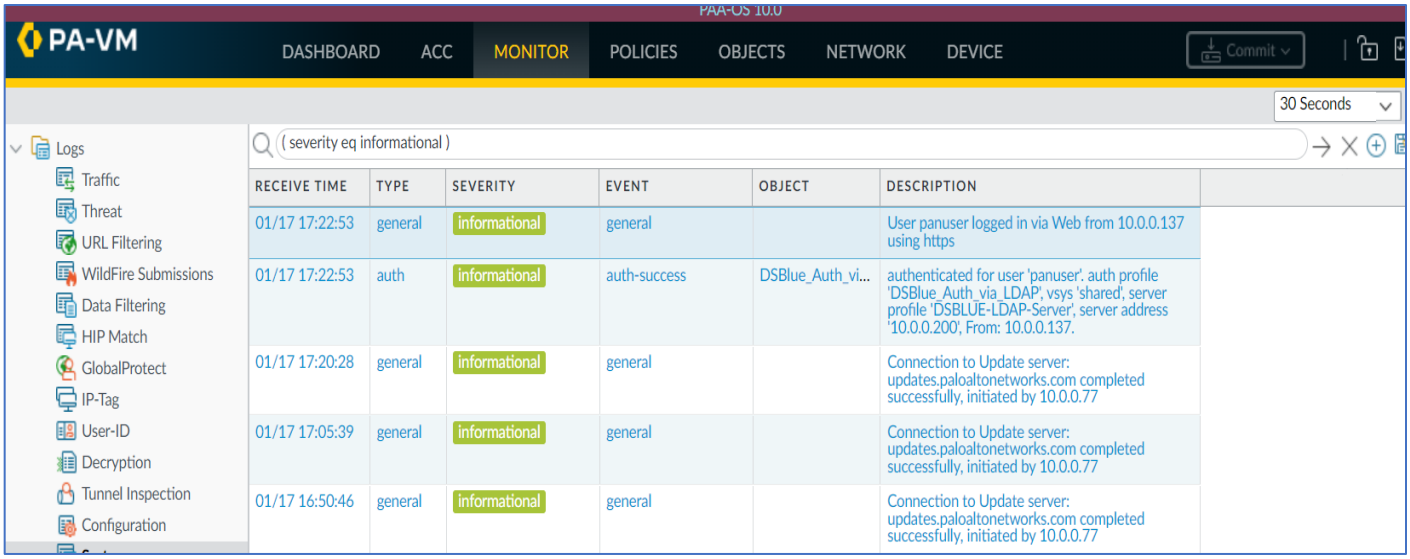


*Figure 7. Successful Authentication to PAN FW via LDAP.*

The configuration is complete.