

Implementing LDAP Authentication For Palo Alto Networks NGFWs

Dan Edeen

dan@eedeen.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.

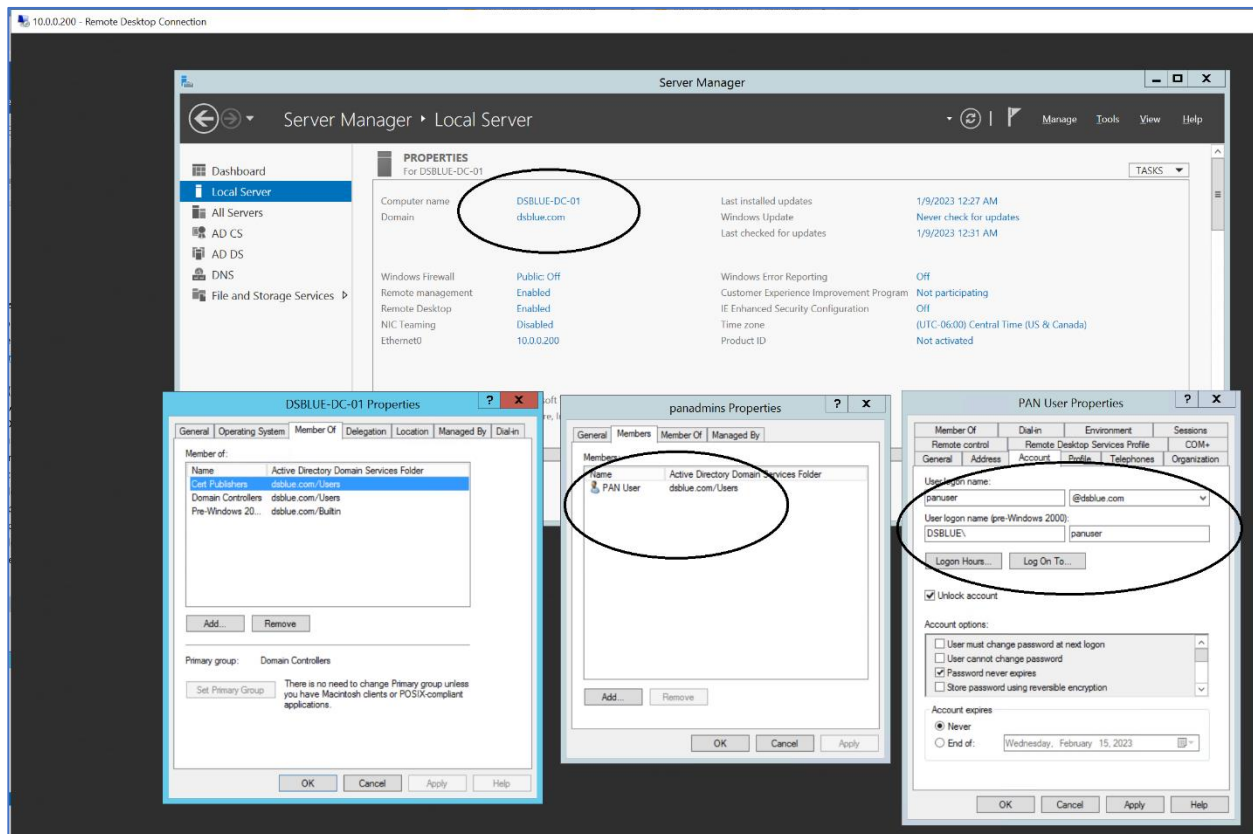


Figure 1. PAN OS user account on Active Directory. Note the group is panadmins, the username is panuser, and the domain is dsblue.com. Certificate Services (CS) have been installed, a PKI created, and the certificates have been exported.

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.

The screenshot displays two web interfaces. The top interface is the Palo Alto Networks PA-VM web UI, showing the 'Network' tab with a list of interfaces. The bottom interface is the vSphere Client, showing the 'Networks' tab for the PA-VM-ESX-10.1.0 VM.

PA-VM Network Interfaces Table:

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	MAC ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIR WIRE
ethernet1/1	Tap		none	none	00:50:56:b3:0d:ba	none		none
ethernet1/2	Virtual Wire		none	none	00:50:56:b3:a7:68	none	Untagged	VWire_e1_2
ethernet1/3	Virtual Wire		none	none	00:50:56:b3:8e:b5	none	Untagged	VWire_e1_2
ethernet1/4	Layer3		none	none	00:50:56:b3:94:36	default	Untagged	none
ethernet1/4.100	Layer3	xml-api-access	none	none		default	101	none
ethernet1/5			none	none		none	Untagged	none
ethernet1/6			none	none		none	Untagged	none
ethernet1/7			none	none		none	Untagged	none

vSphere Client Networks Table:

Name	Type	Network	VMs	Hosts
PanOSPortGroup-1	Standard network		4	1
PanOSPortGroup-2	Standard network		1	1
VM Network	Standard network		12	1

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.

The screenshot shows the Palo Alto Networks NGFW configuration interface. On the left is a sidebar with a tree view containing categories like Certificate Management, Log Settings, Server Profiles, Local User Database, and Users. The 'LDAP' option under 'Server Profiles' is selected. The main window displays the 'LDAP Server Profile' configuration dialog. The 'Profile Name' field is set to 'DSBLUE-LDAP-Server'. The 'Administrator Use Only' checkbox is unchecked. The 'Server List' table contains one entry: DSBLUE-DC-01, 10.0.0.200, 389. The 'Server Settings' section on the right is configured with Type: active-directory, Base DN: DC=dsblue,DC=com, Bind DN: panuser@dsblue.com, Password: [masked], Confirm Password: [masked], Bind Timeout: 30, Search Timeout: 30, and Retry Interval: 60. The 'Require SSL/TLS secured connection' and 'Verify Server Certificate for SSL sessions' checkboxes are unchecked. 'OK' and 'Cancel' buttons are at the bottom right.

LDAP Server Profile

Profile Name: DSBLUE-LDAP-Server

☐ Administrator Use Only

Server List

NAME	LDAP SERVER	PORT
DSBLUE-DC-01	10.0.0.200	389

+ Add - Delete

Enter the IP address or FQDN of the LDAP server

Server Settings

Type: active-directory

Base DN: DC=dsblue,DC=com

Bind DN: panuser@dsblue.com

Password: [masked]

Confirm Password: [masked]

Bind Timeout: 30

Search Timeout: 30

Retry Interval: 60

☐ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

OK Cancel

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.

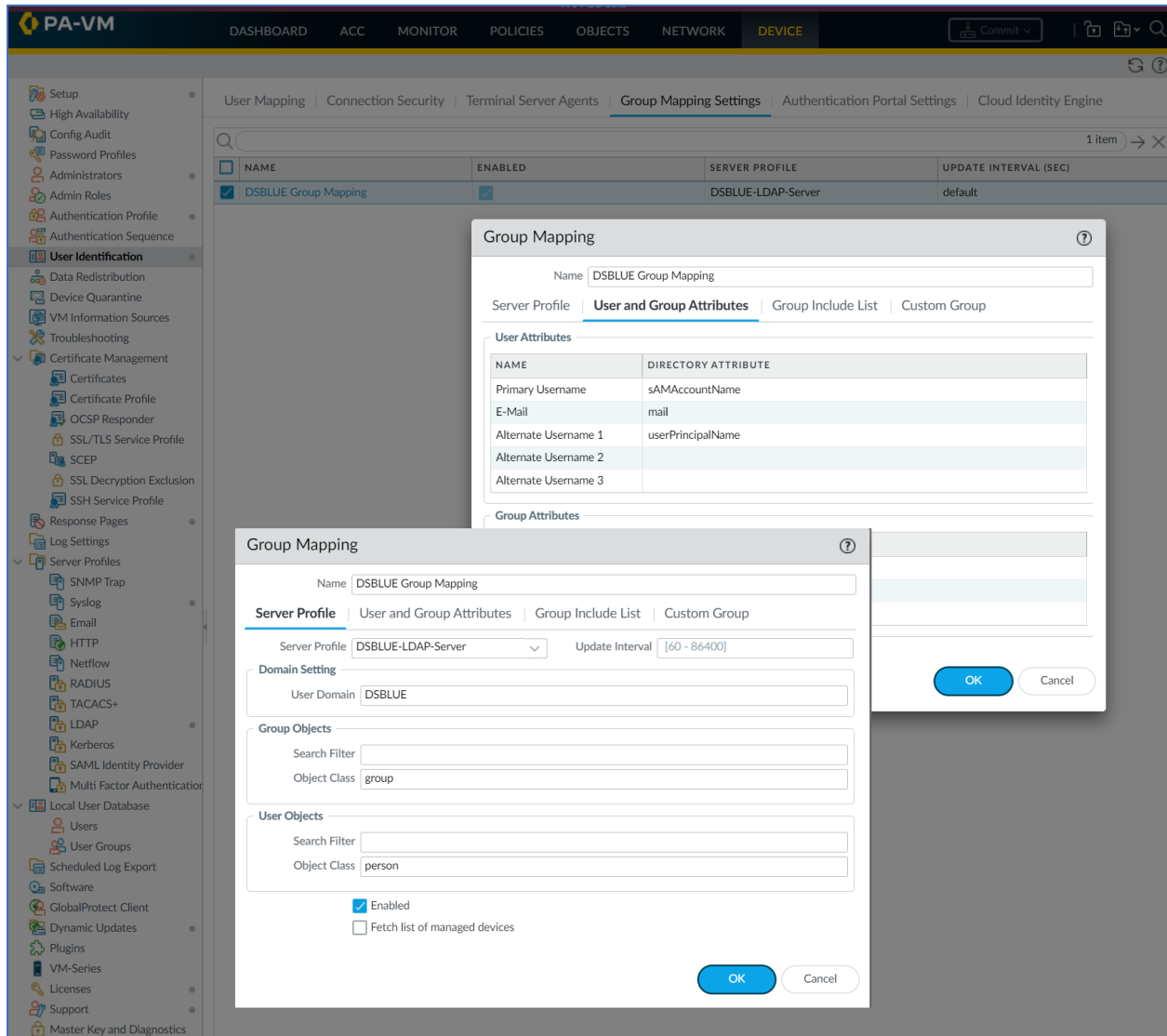


Figure 4. Group Mapping Server Profile and User and Group Attributes. Note primary username 'sAMAccountName'.

3.3 Authentication Profile

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

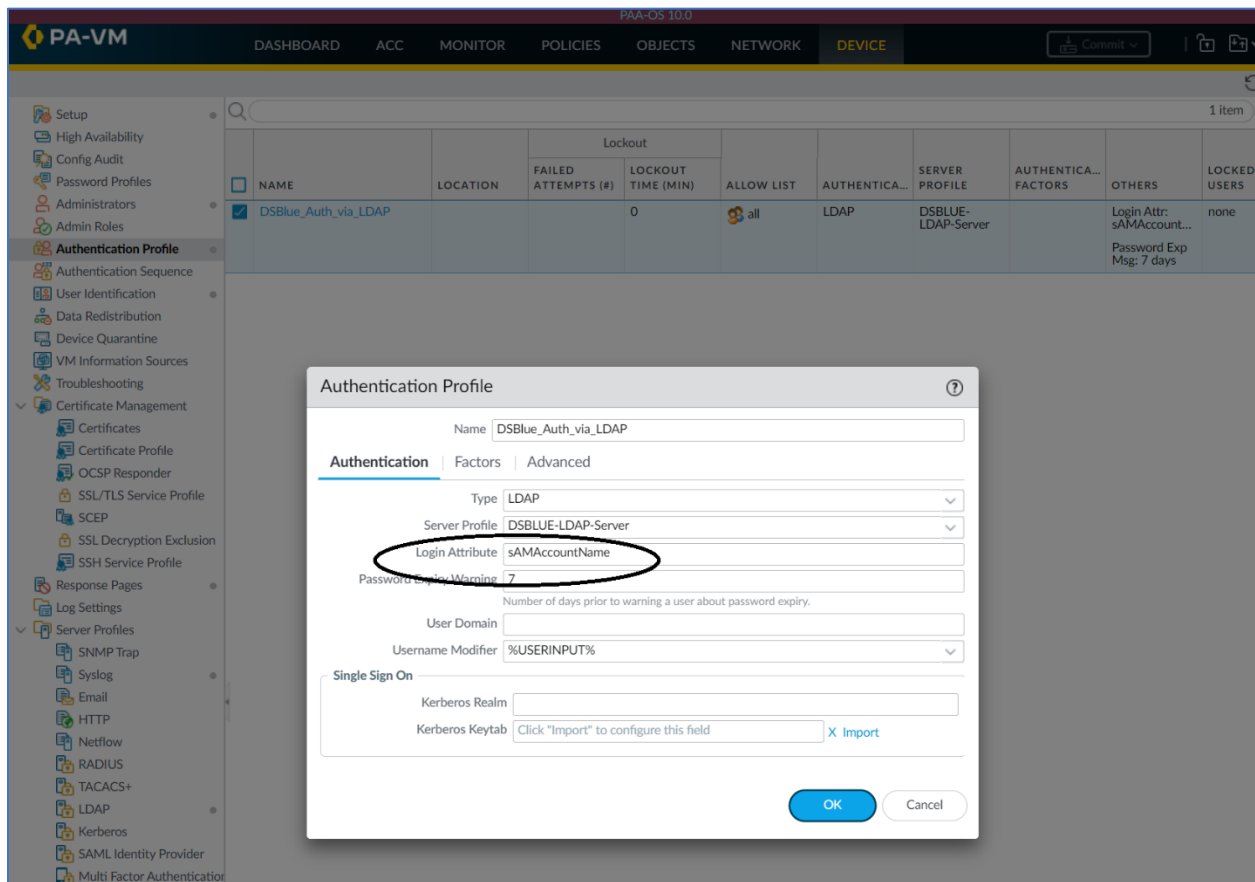


Figure 5. Authentication Profile. Note the Login Attribute 'sAMAccountName'. You must spell this exactly the same, including the case.

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.

The screenshot shows the PA-VM interface with the 'DEVICES' tab selected. On the left, the 'Administrators' section is expanded. The main table lists administrators with columns: NAME, ROLE, AUTHENTICATION PROFILE, PASSWORD PROFILE, CLIENT CERTIFICATE AUTHENTICATI... (WEB), PUBLIC KEY AUTHENTICATI... (SSH), and PROFILE. The 'panuser' entry is circled.

NAME	ROLE	AUTHENTICATION PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)	PUBLIC KEY AUTHENTICATI... (SSH)	PROFILE
admin	Superuser			<input type="checkbox"/>	<input type="checkbox"/>	
deviceadmin1	Device administrator			<input type="checkbox"/>	<input type="checkbox"/>	
devicesuperuser1	Superuser			<input type="checkbox"/>	<input type="checkbox"/>	
panuser	Superuser	DSBlue_Auth_via_LDAP		<input type="checkbox"/>	<input type="checkbox"/>	

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].

The screenshot shows the PA-VM interface with the 'MONITOR' tab selected. The left sidebar shows 'Logs' expanded. The main table displays log entries with columns: RECEIVE TIME, TYPE, SEVERITY, EVENT, OBJECT, and DESCRIPTION. The first entry shows a successful authentication for 'panuser'.

RECEIVE TIME	TYPE	SEVERITY	EVENT	OBJECT	DESCRIPTION
01/17 17:22:53	general	informational	general		User panuser logged in via Web from 10.0.0.137 using https
01/17 17:22:53	auth	informational	auth-success	DSBlue_Auth_vi...	authenticated for user 'panuser'. auth profile 'DSBlue_Auth_via_LDAP', vsys 'shared', server profile 'DSBLUE-LDAP-Server', server address '10.0.0.200', From: 10.0.0.137.
01/17 17:20:28	general	informational	general		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.0.0.77
01/17 17:05:39	general	informational	general		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.0.0.77
01/17 16:50:46	general	informational	general		Connection to Update server: updates.paloaltonetworks.com completed successfully, initiated by 10.0.0.77

Figure 7. Successful Authentication to PAN FW via LDAP.

The configuration is complete.