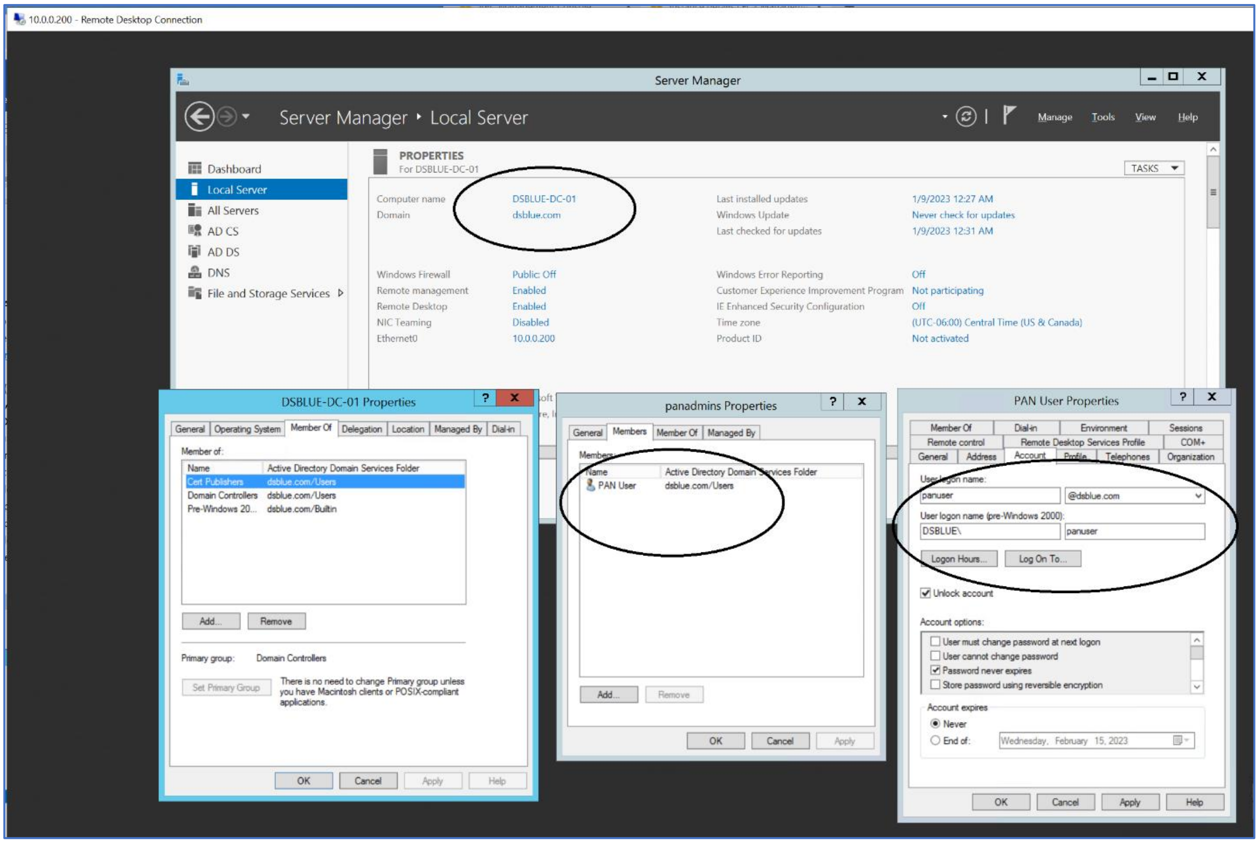
Palo Alto Networks Firewall Active Directory (LDAP) Integration

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 environment is an ESXi 6.7 host. This document's purpose is instructional, and other factors need to be considered for a production environment.

Step 1: Set Up Active Directory

First you need an Active Directory Domain Controller with groups and users set up. I built this previously in the DSBlue lab on ESXi 6.7 (documented separately). Here are some snapshots from this AD DC server.



PROPERTIES
For DSBLUE-DC-01

Computer name	DSBLUE-DC-01	Last installed updates	1/9/2023 12:27 AM
Domain	dsblue.com	Windows Update	Never check for updates
		Last checked for updates	1/9/2023 12:31 AM
Windows Firewall	Public: Off	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Enabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC-06:00) Central Time (US & Canada)
Ethernet0	10.0.0.200	Product ID	Not activated

DSBLUE-DC-01 Properties

Member of:

Name	Active Directory Domain Services Folder
Cert Publishers	dsblue.com/Users
Domain Controllers	dsblue.com/Users
Pre-Windows 20...	dsblue.com/Builtin

Primary group: Domain Controllers

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

panadmins Properties

Members:

Name	Active Directory Domain Services Folder
PAN User	dsblue.com/Users

PAN User Properties

User logon name:
panuser @dsblue.com

User logon name (pre-Windows 2000):
DSBLUE\ panuser

☑ Unlock account

Account options:
- ☐ User must change password at next logon
- ☐ User cannot change password
- ☑ Password never expires
- ☐ Store password using reversible encryption

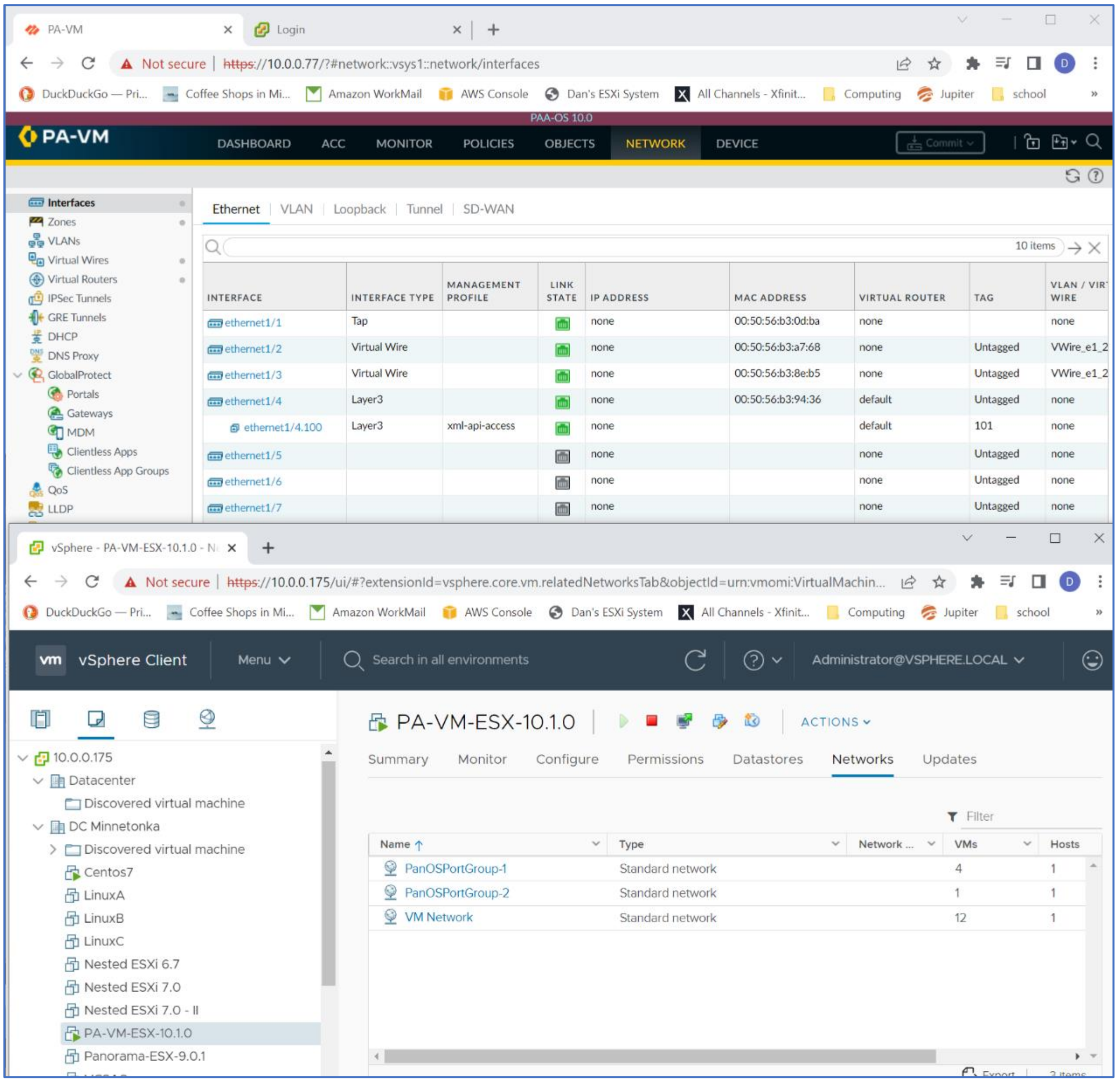
Account expires
- ● Never
- ○ End of: Wednesday, February 15, 2023

Figure 1. PAN OS user account on Active Directory. Note group is panadmins, username is panuser, domain is dsblue.com. Certificate Services (CS) installed, PKI setup and cert exported.

Note the username, group, and domain settings used on the AD server (W2012r2).

Step 2: Set Up Palo Alto Networks NGFW

I am running a PA-VM, version 10.1.0, as a VM on the DSBlue lab on ESXi 6.7 system. This FW has four Ethernet interfaces mapped to two port groups on ESXI, with a pair in a VWire to capture other traffic on this host. Figure 2 illustrates.



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

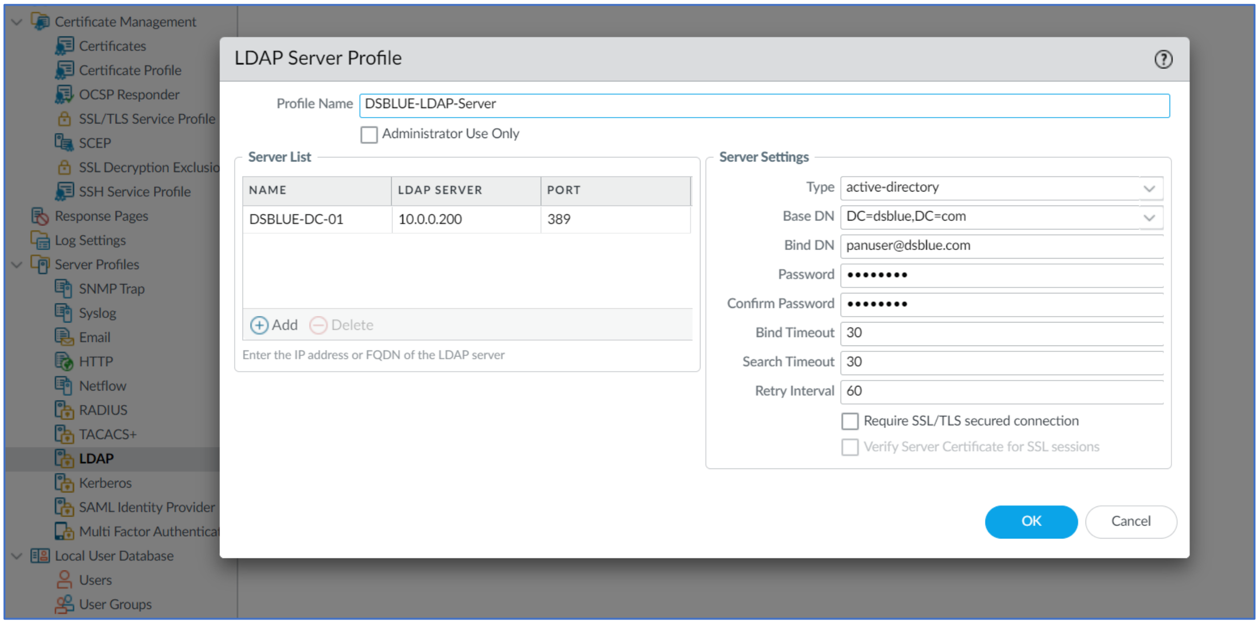
Name ↑	Type	Network ...	VMs	Hosts
PanOSPortGroup-1	Standard network		4	1
PanOSPortGroup-2	Standard network		1	1
VM Network	Standard network		12	1

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, you need to create an LDAP Server Profile, a Group Mapping, and an Authentication Profile [Device > Server Profiles > LDAP]. These are illustrated in the following figures.



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

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	••••••••
Confirm Password	••••••••
Bind Timeout	30
Search Timeout	30
Retry Interval	60

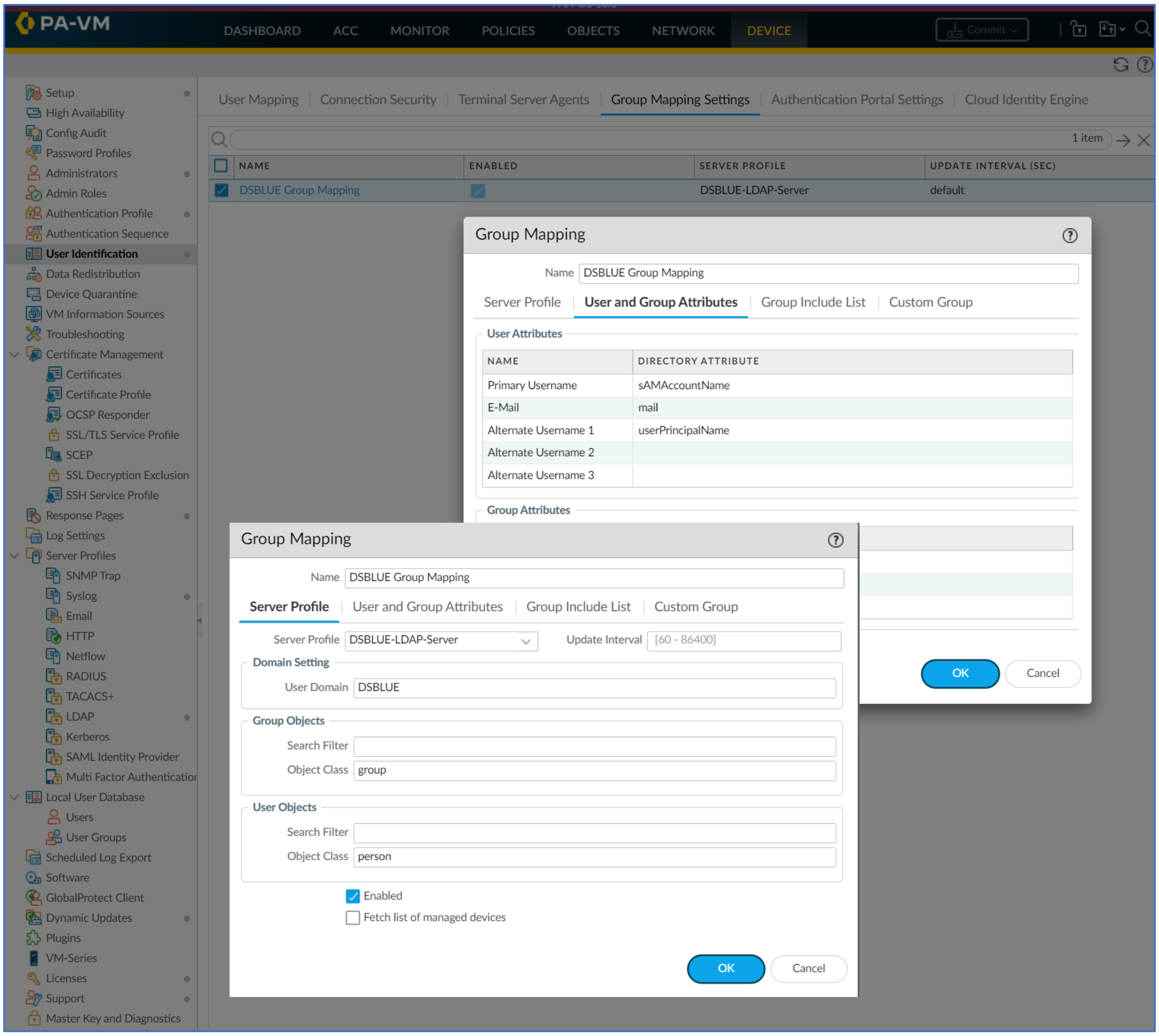
□ Require SSL/TLS secured connection

□ Verify Server Certificate for SSL sessions

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

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



NAME	ENABLED	SERVER PROFILE	UPDATE INTERVAL (SEC)
DSBLUE Group Mapping	☑	DSBLUE-LDAP-Server	default

Group Mapping

Name: DSBLUE Group Mapping

Server Profile | **User and Group Attributes** | Group Include List | Custom Group

User Attributes

NAME	DIRECTORY ATTRIBUTE
Primary Username	sAMAccountName
E-Mail	mail
Alternate Username 1	userPrincipalName
Alternate Username 2	
Alternate Username 3	

Group Attributes

Group Mapping

Name: DSBLUE Group Mapping

Server Profile | User and Group Attributes | Group Include List | Custom Group

Server Profile: DSBLUE-LDAP-Server
Update Interval: [60 - 86400]

Domain Setting
User Domain: DSBLUE

Group Objects
Search Filter:
Object Class: group

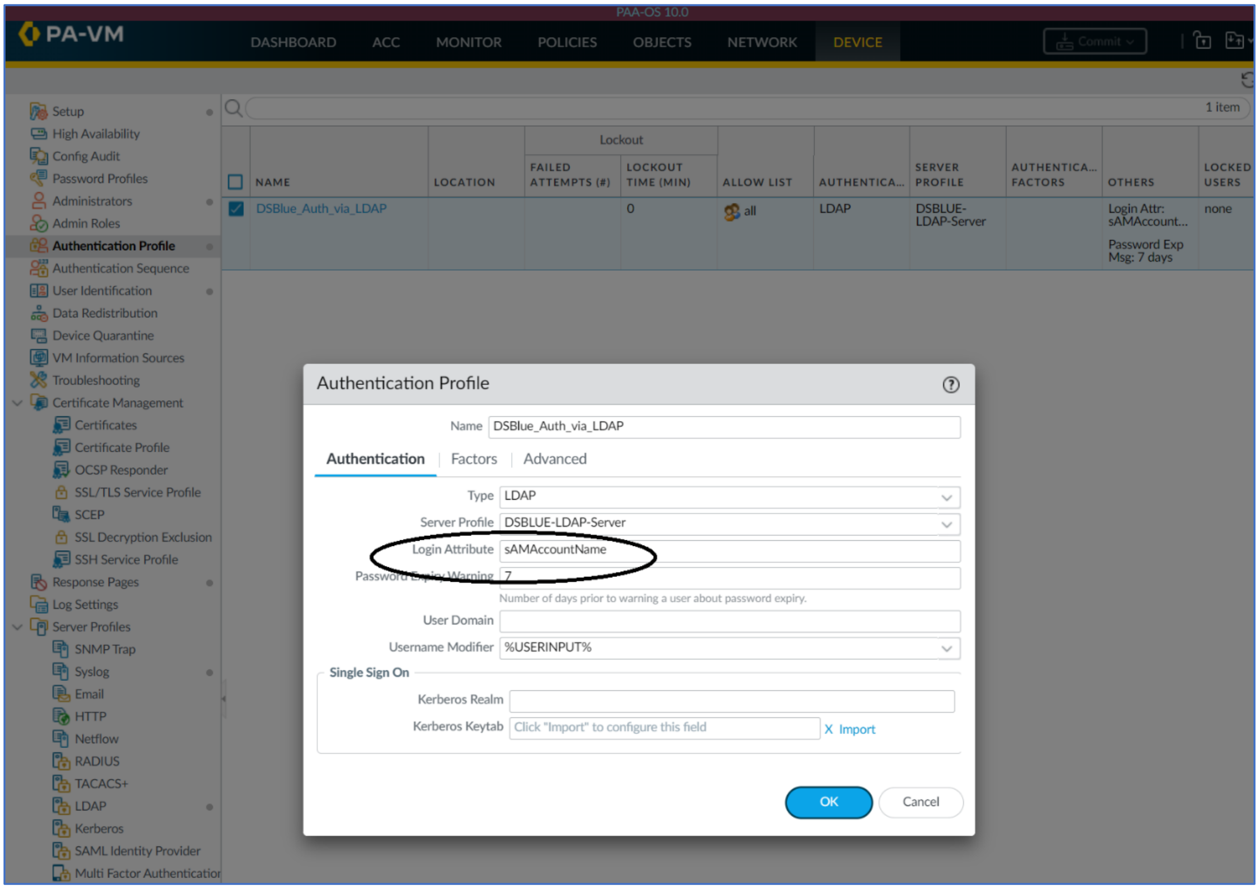
User Objects
Search Filter:
Object Class: person

☑ Enabled
☐ Fetch list of managed devices

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].



		Lockout							
NAME	LOCATION	FAILED ATTEMPTS (#)	LOCKOUT TIME (MIN)	ALLOW LIST	AUTHENTICA...	SERVER PROFILE	AUTHENTICA... FACTORS	OTHERS	LOCKED USERS
☑ DSBlue_Auth_via_LDAP			0	all	LDAP	DSBLUE-LDAP-Server		Login Attr: sAMAccount... Password Exp Msg: 7 days	none

Authentication Profile

Name: DSBlue_Auth_via_LDAP

Type: LDAP

Server Profile: DSBLUE-LDAP-Server

Login Attribute: sAMAccountName

Password Expiry Warning: 7

Number of days prior to warning a user about password expiry.

User Domain:

Username Modifier: %USERINPUT%

Single Sign On

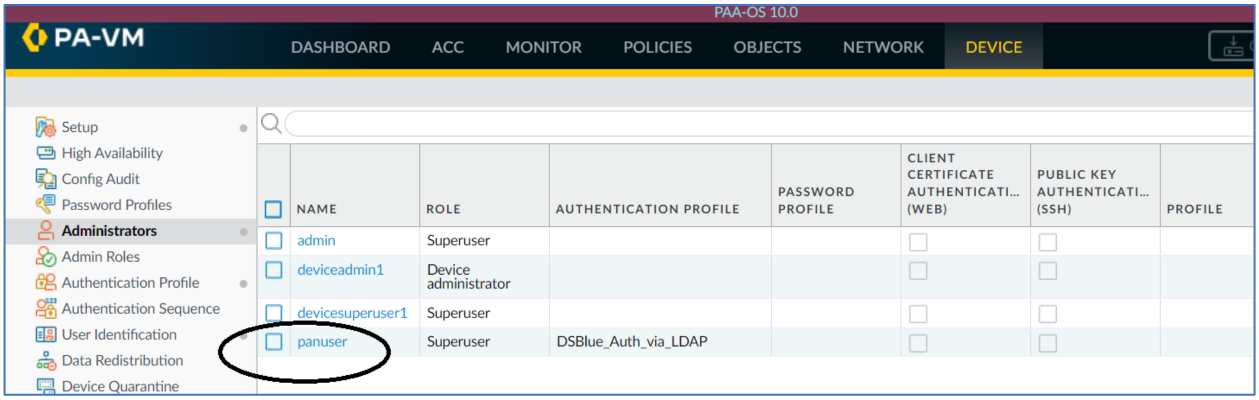
Kerberos Realm:

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

Figure 5. Authentication Profile. Note Login Attribute ‘sAMAccountName’, you must use this as spelled here and with the same 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.

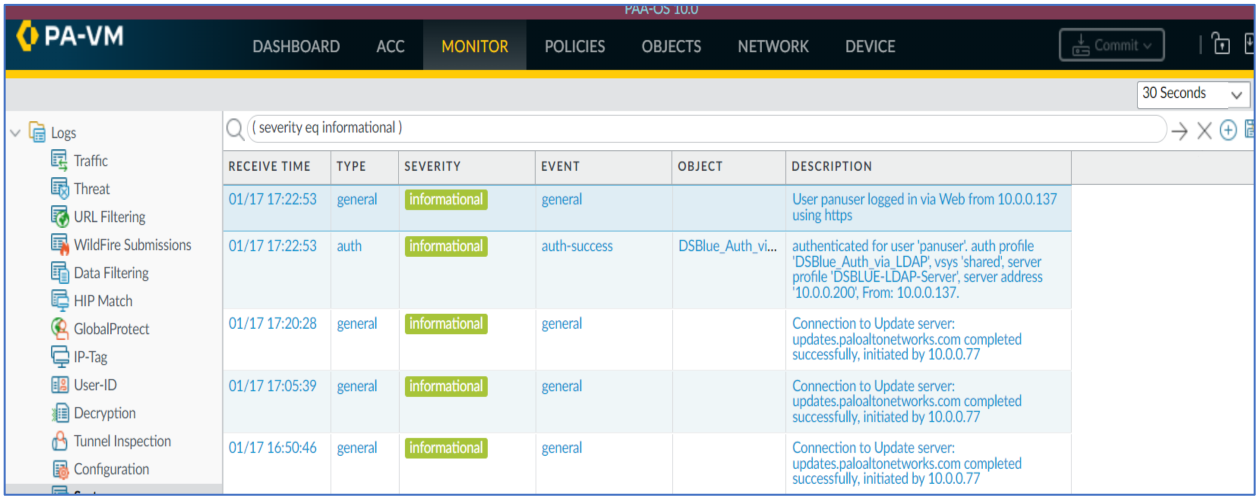


☐	NAME	ROLE	AUTHENTICATION PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)	PUBLIC KEY AUTHENTICATI... (SSH)	PROFILE
☐	admin	Superuser			☐	☐	
☐	deviceadmin1	Device administrator			☐	☐	
☐	devicesuperuser1	Superuser			☐	☐	
☐	panuser	Superuser	DSBlue_Auth_via_LDAP		☐	☐	

Figure 6. Set Up Firewall Administrator for AD Account.

3.5 Test

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].



(severity eq informational)

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.

END OF DOCUMENT