Configuring User Identification via Active Directory

Version 1.0

PAN-OS 5.0.1

Johan Loos

johan@accessdenied.be

User Identification Overview

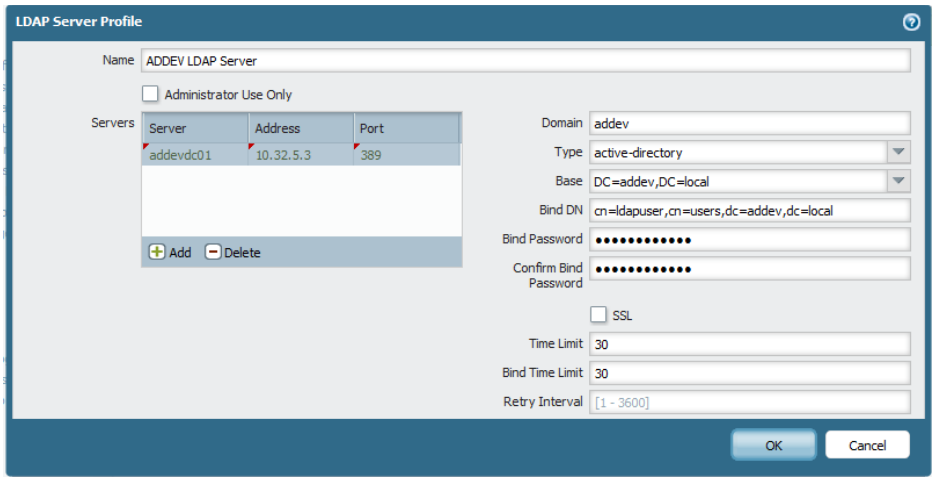
User Identification allows you to create security policies based on users or groups which are member of Active Directory. The firewall has a native agent which contacts the domain controller to retrieve a list of available groups.

User Identification Task List

- △ Create a LDAP server profile
- △ Add LDAP server profile to User-ID group mapping
- △ Map user name to IP address
- △ Enable User Identification for your zone
- △ Configure security policy based on group membership

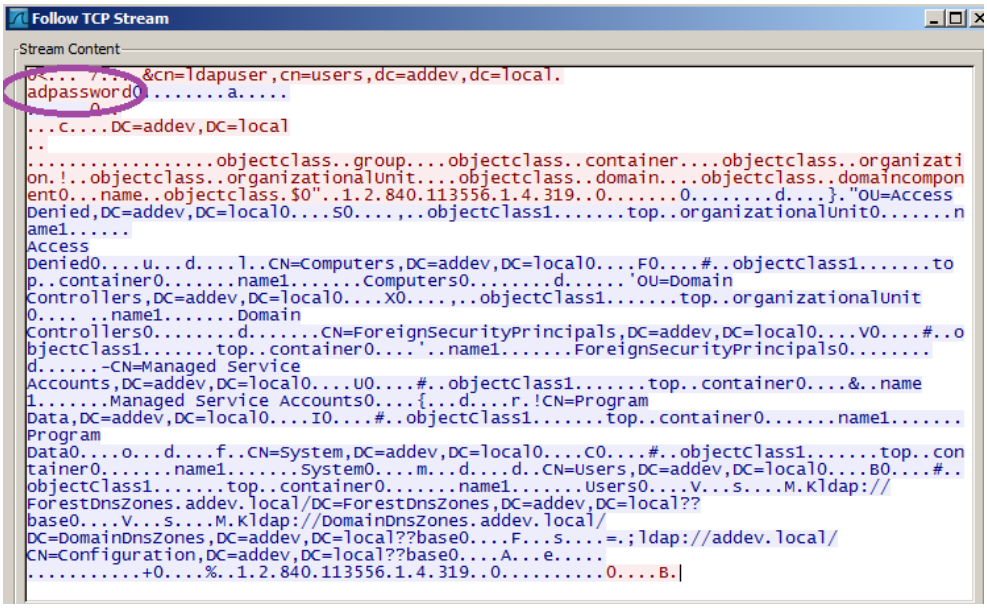
Create a LDAP server profile

- Navigate to **Device | Server Profiles | LDAP** and click **Add**
- On the **LDAP Server Profile** page, type a name for your profile, click **Add** to add LDAP servers from your domain.
- On **Servers**, specify a name for your server, IP address and port number
- Specify the type of LDAP server you are connecting to, for example Active Directory
- Type a base (this is the domain naming context of your domain), for example dc=addev,dc=local
- Type a Bind DN, this is a user account who is able to connect to the LDAP server. If you use the User Principal Name (UPN), your firewall performs a search against the Global Catalog Server in your domain. Type a password, select or clear the SSL checkbox



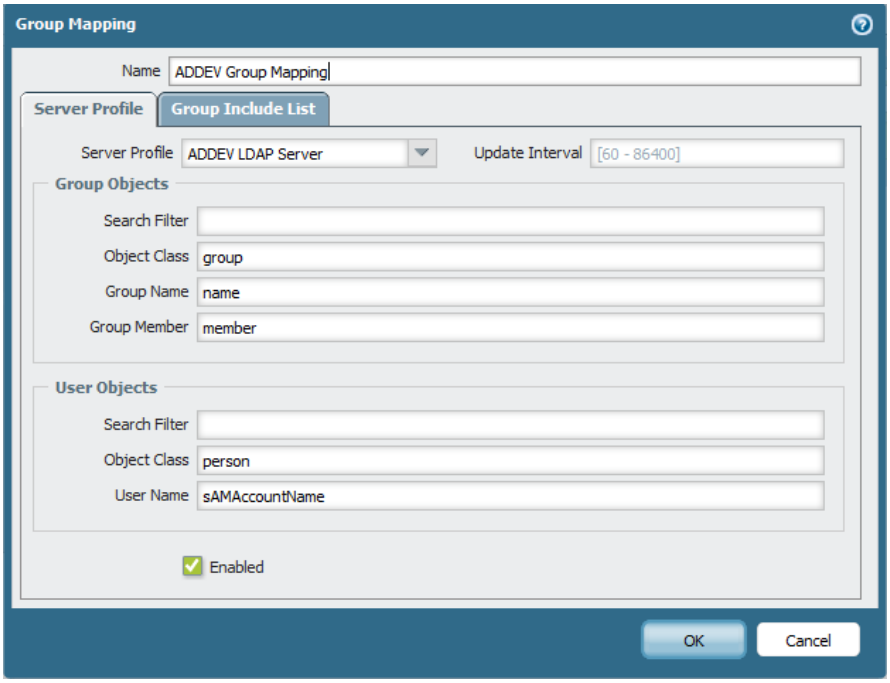
- Click **OK**

Try to avoid LDAP connection over port 389, because the password for your LDAP user account is send in clear text as you can see on the following screen:

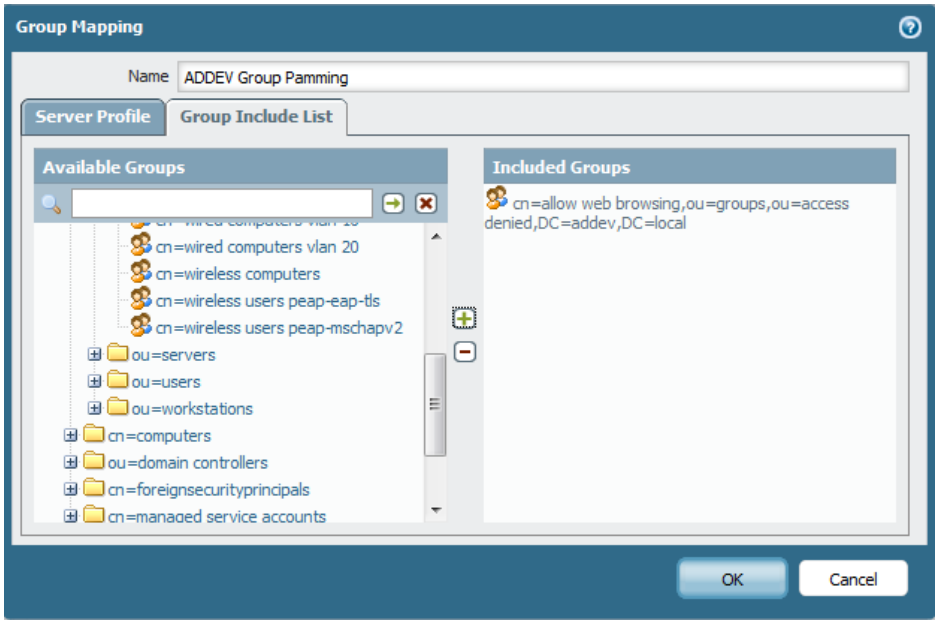


Add LDAP server profile to User-ID group mapping

- Navigate to **Device | User Identification | Group Mapping Settings** and click **Add**
- On the **Server Profile** page, select your LDAP server profile



- On the **Group Include List** page, include the required groups



- Click **OK**

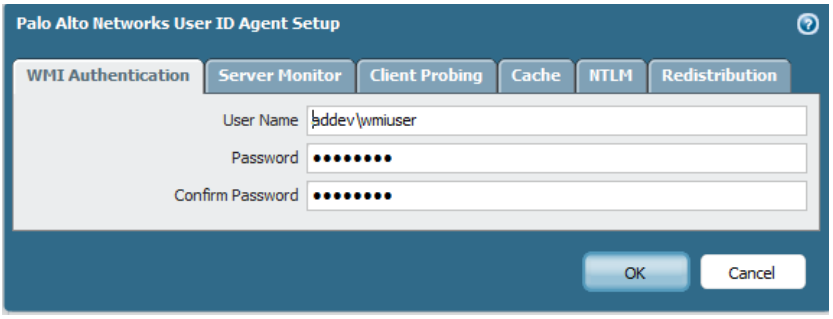
Map user name to IP address

You can install and configure a User-ID agent on a Windows server in your environment or by enabling the native agent on the firewall. You can use one of the following options:

Monitors security event logs: You have to configure your domain controllers to log successful account logon events. You have also to configure a user account that is able to read security event logs.

WMI: The specified user account must have permissions to access WMI

- Navigate to **Device | User Identification | User Mapping** and click **Edit**



- Type a username with appropriate permissions to read WMI and click **OK**

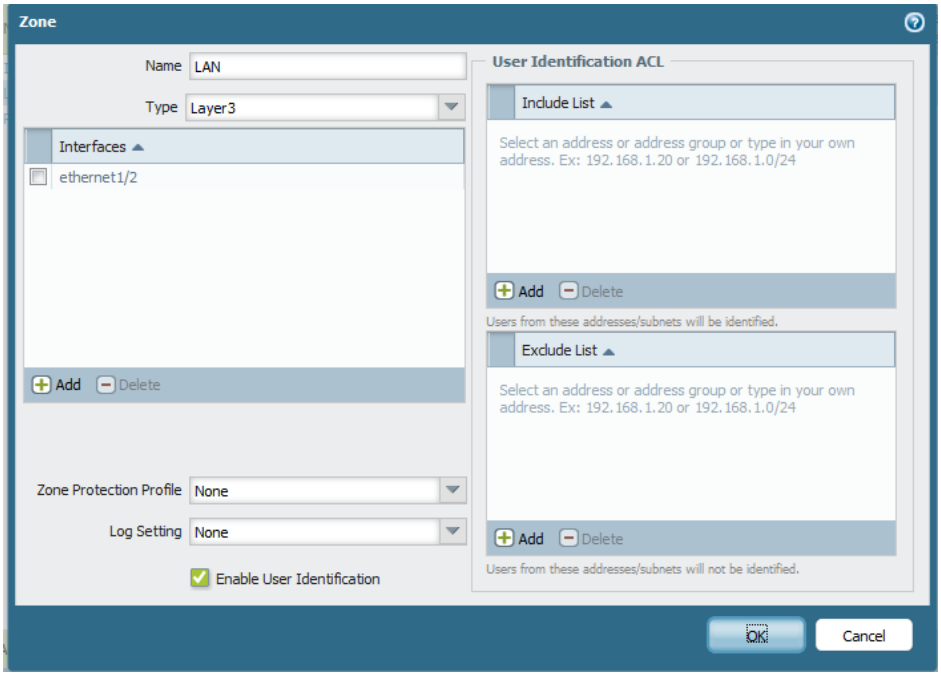
I've done some test, but authentication fails when the user is only a member of the Domain User group. After adding the user account as a member of the Domain Admins group, authentication was successful.

In this configuration, I did not install the User ID Agent onto the domain controller, but I use the native User Mapping Agent on the firewall.

Enable User Identification for your zone

Before you can use security policies based on user or groups, you need to configure your zone for user identification. You can then create security policies to allow or deny traffic based on user or group membership.

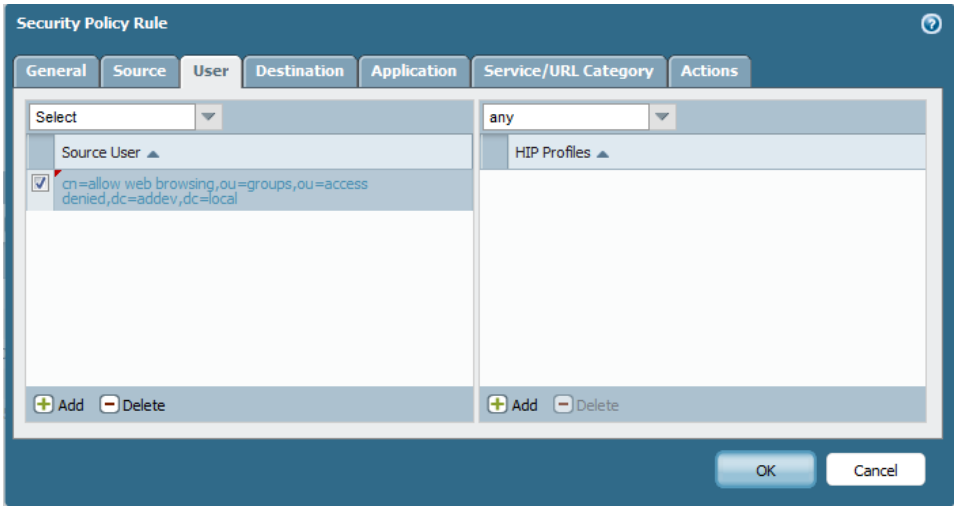
- Navigate to **Network | Zones**
- Click on the zone you want to enable user identification for
- On the **Zone** page, select **Enable User Identification**



- Click **OK**

Configure security policy based on group membership

- You can edit an existing security policy or you can create a new one.
- Navigate to **Policies | Security**, click on the security policy you want to perform user/group membership
- On the **Security Policy Rule** page, click on **User** page, click **Add** and select the required groups



- Click **OK**

When the user access resources on the internet, user identification is performed on the firewall:

Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application
02/02 19:39:51	start	LAN	Internet	10.32.5.52	addev\johan	95.211.20.91	80	web-browsing
02/02 19:39:51	start	LAN	Internet	10.32.5.52	addev\johan	95.211.20.91	80	web-browsing
02/02 19:39:51	start	LAN	Internet	10.32.5.52	addev\johan	95.211.20.91	80	web-browsing
02/02 19:39:51	start	LAN	Internet	10.32.5.52	addev\johan	95.211.20.91	80	web-browsing