Agent Installation & Setup

Version 4.1

Overview

This document will outline the steps to install the 4.1.x version of the Palo Alto Networks User Identification (User-ID) Agent on a member server in a domain (can be installed on a Domain Controller as well). It assumes that no prior version of the User Identification agent has been installed. This guide is only applicable in on a Windows 2008 Server.

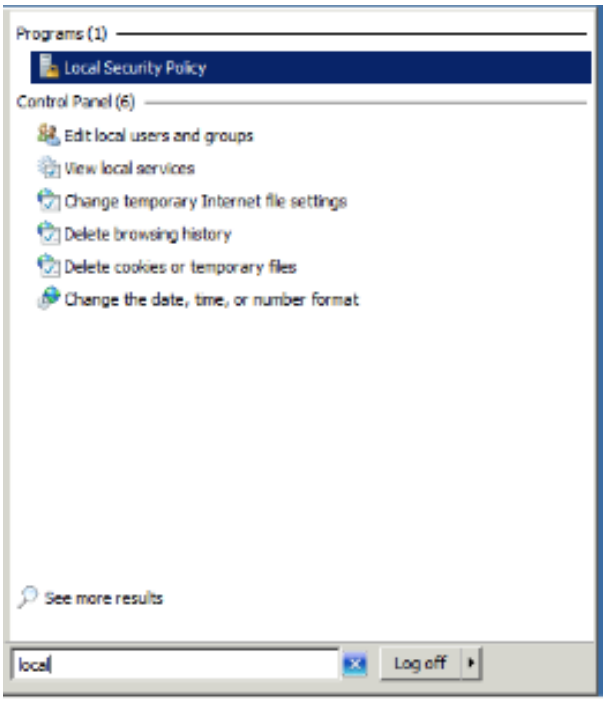
Prerequisites

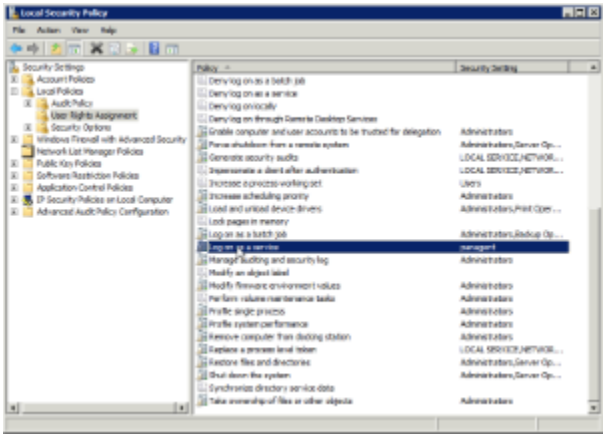
During installation of the User ID Agent, it'll be by default configured to login as a service under the username which it has been installed with. It it common and best practice to create a special service account with limited rights.

Create and configure a service Account

You should create a service account. In this example we call it "pan agent". Add this account to the local build in groups "Event Log Readers" and "Server Operators".

You can also give that user the right to logon as a service. This should be done automatically when you later chosse this account as the service account, but if that for whatever reason doesn't work, go to "Local Security Policy" --> Local Policies --> User Right Assignment and add the just created user account to the "Log on as a Service" setting.





After you've done this basic setup, don't forget to refresh the group policies throughout your domain. You can do this manually with "gpupdate" in an administrative command prompt, or wait 30 Minutes (default domain setting) for the automated replication.

Installation

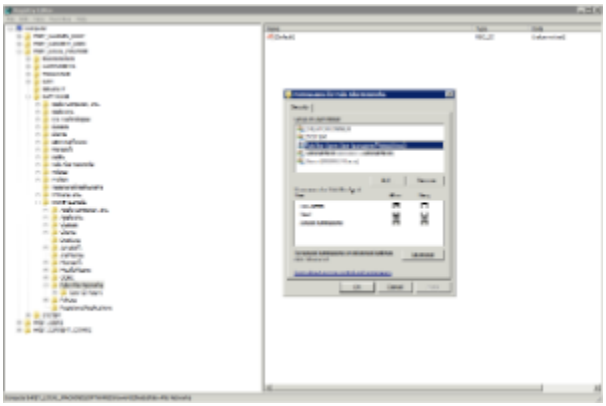
This example will describe the steps needed to install the User-ID Agent on a Windows 2008 member server that is part of the domain “corp.local”. The agent will be configured to use the service account “agent_user”, which is not an administrative account on the member server or in the domain.

1. Download the installer from support.paloaltonetworks.com. Make sure you have the right Version (32/64 Bit) and that the Version is compatible with your PanOS Version.
2. On the server you have two choices to install the Agent:
    a. If you are logged in as an administrator (or member of the admninistrator group), you can install directly by double clicking the installer icon
    b. if you are not a member of the administrator group, either right click the install and choose "Run as Administrator", or start the Installed from a Command Prompt you have launched as an administrator.

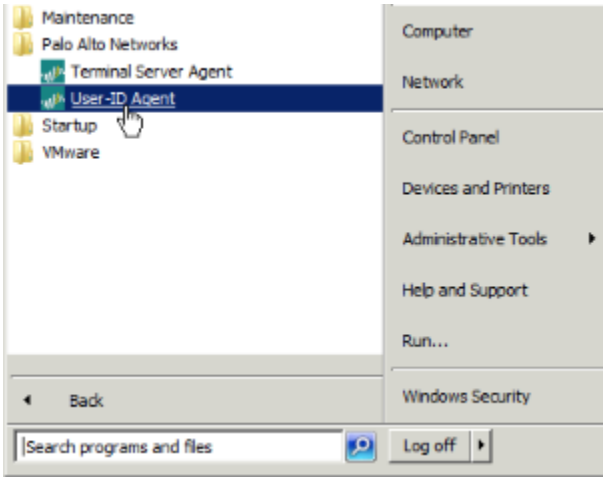
3. Do not start the agent yet.

After Installation you need to assign the correct permissions to the installation directory. Using the Windows Explorer navigate to the "Palo Alto Networks" folder within the "Programs" folder and right click on the "Palo Alto Networks" folder to go to it's properties. On the security tab add you "panagent" user account and grant it "modify" permissions on the folder and it's content.

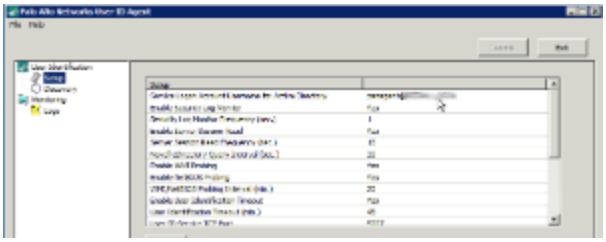
The next step is to assign proper permission in the registry settings for the agent. Launch "regedt32" to edit the Windows Registry and search for "User-ID Agent" which is nested in a folder called "Palo Alto Networks". Assign "full permissions" to the "Palo Alto Networks" folder to your service account (right click on the folder and choose "Properties"). According to Palo Alto the folder should be at "Computer\HKEY_LOCAL_MACHINE\Software\Palo Alto Networks" but I figured out that the exact location depends on your settings and whether it's a Domain Controller or Member Server, so searching for it might be the best way.



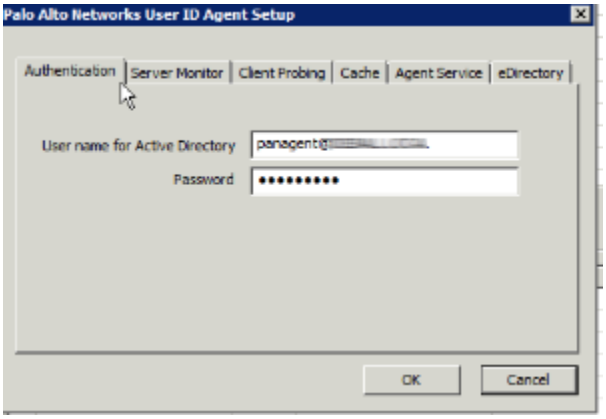
After these basic settings have been done, start the Palo Alto Networks User-ID Agent.



Here we need to change the user account the agent is using to logon as a service. We need to take the account we setup and assigned the proper permissions:



Click on "Edit" or double click on the setting in order to be able to change it:



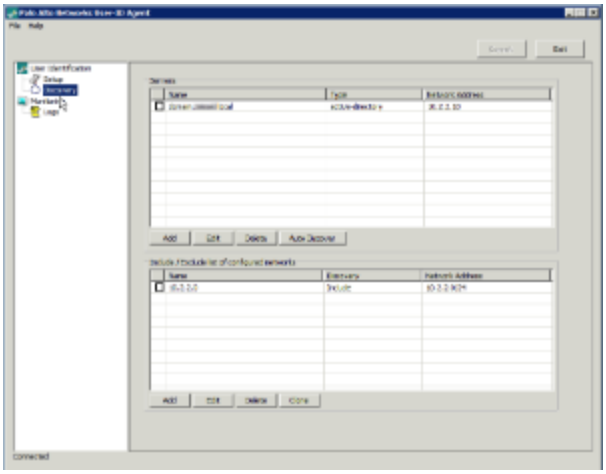
Now click on OK and on "commit" on the upper right corner of the main window.

You should be able to start the agent now.

> **Windows Firewall Settings**
>
> After installations the Agent is listening on TCP/5007 for connections from configured Palo Alto Firewalls. If you run the build in or any 3rd party firewalls, you need to make sure that this communication is allowed.

Since Version 4.x of the User-ID Agent, most of the configurations settings are done in the Firewall now instead of the Agent. This includes e.g. IP Address Ranges to include in user/IP mapping, group settings out of Active Directory, etc.

There are only two settings one needs to configure on the Agent: Servers and IP Networks



The "Servers" filed needs to include all your domain controllers. Clicking on "Auto Discovery" should bring them all up in the list, but one should double check and add any not automatically added servers.

The "Configured Networks" list should include all your internal IP Address ranges you want to include in the User/IP Address mapping. If you do not configure any Network here, The Firewall will not be able to display any user names.

After the installation has been completed and the service starts correctly you need to configure your firewall(s) to communicate with the agent.