

Next-Generation Firewall

Configure the Windows User-ID Agent for User Mapping

Previous

Install the Windows-Based User-ID Agent

Next

Configure User Mapping Using the PAN-OS Integrated User-ID Agent

The Palo Alto Networks Windows User-ID agent is a Windows service that connects to servers on your network—for example, Active Directory servers, Microsoft Exchange servers, and Novell eDirectory servers—and monitors the logs for login events. The agent uses this information to map IP addresses to usernames. Palo Alto Networks firewalls connect to the User-ID agent to retrieve this user mapping information, enabling visibility into user activity by username rather than IP address and enables user- and group-based security enforcement.



For information about the server OS versions supported by the User-ID agent, refer to “Operating System (OS) Compatibility User-ID Agent” in the [User-ID Agent Release Notes](#).

STEP 1 - Define the servers the User-ID agent will monitor to collect IP address to user mapping information.

The User-ID agent can monitor up to 100 servers, of which up to 50 can be syslog senders.



To collect all of the required mappings, the User-ID agent must connect to all servers that your users log in to in order to monitor the security log files on all servers that contain login events.

1 Open the Windows **Start** menu and select **User-ID Agent**.

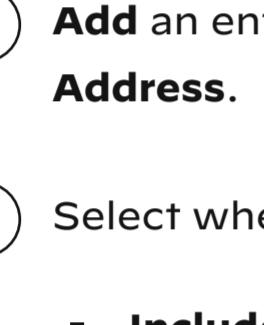
2 Select **User Identification > Discovery**.

3 In the **Servers** section of the screen, click **Add**.

4 Enter a **Name** and **Server Address** for the server to be monitored. The network address can be a FQDN or an IP address.

5 Select the **Server Type** (**Microsoft Active Directory**, **Microsoft Exchange**, **Novell eDirectory**, or **Syslog Sender**) and then click **OK** to save the server entry. Repeat this step for each server to be monitored.

6 **(Optional)** To enable the Windows User-ID agent to automatically discover domain controllers on your network using DNS lookups, click **Auto Discover**. If you have new domain controllers that you want the Windows User-ID agent to discover, click **Auto Discover** each time you want to discover the new domain controllers.



Auto-discovery locates domain controllers in the local domain only; you must manually add Exchange servers, eDirectory servers, and syslog senders.

7 **(Optional)** To tune the frequency at which the firewall polls configured servers for mapping information, select **User Identification > Setup** and **Edit** the **Setup** section. On the **Server Monitor** tab, modify the value in the **Server Log Monitor Frequency (seconds)** field. Increase the value in this field to 5 seconds in environments with older Domain Controllers or high-latency links.



Ensure that the **Enable Server Session Read** setting is not selected. This setting requires that the User-ID agent have an Active Directory account with Server Operator privileges so that it can read all user sessions. Instead, use a syslog or XML API integration to monitor sources that capture login and logout events for all device types and operating systems (instead of just Windows), such as wireless controllers and Network Access Controllers (NACs).

8 Click **OK** to save the settings.

STEP 2 - Specify the subnetworks the Windows User-ID agent should include in or exclude from User-ID.

By default, the User-ID maps all users accessing the servers you are monitoring.



As a best practice, always specify which networks to include and exclude from User-ID to ensure that the agent is only communicating with internal resources and to prevent unauthorized users from being mapped. You should only enable User-ID on the subnetworks where users internal to your organization are logging in.

1 Select **User Identification > Discovery**.

2 Add an entry to the Include/Exclude list of configured networks and enter a **Name** for the entry and enter the IP address range of the subnetwork in as the **Network Address**.

3 Select whether to include or exclude the network:

- **Include specified network**—Select this option if you want to limit user mapping to users logged in to the specified subnetwork only. For example, if you include 10.0.0.0/8, the agent maps the users on that subnetwork and excludes all others. If you want the agent to map users in other subnetworks, you must repeat these steps to add additional networks to the list.
- **Exclude specified network**—Select this option only if you want the agent to exclude a subset of the subnetworks you added for inclusion. For example, if you include 10.0.0.0/8 and exclude 10.2.50.0/22, the agent will map users on all the subnetworks of 10.0.0.0/8 except 10.2.50.0/22, and will exclude all subnetworks outside of 10.0.0.0/8.



If you add Exclude profiles without adding any Include profiles, the User-ID agent excludes all subnetworks, not just the ones you added.

4 Click **OK**.

STEP 3 - **(Optional)** If you configured the agent to connect to a Novell eDirectory server, you must specify how the agent should search the directory.

1 Select **User Identification > Setup** and click **Edit** in the **Setup** section of the window.

2 Select the **eDirectory** tab and then complete the following fields:

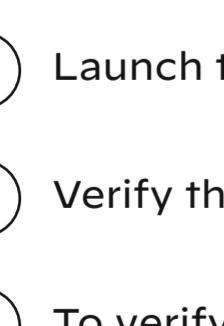
- **Search Base**—The starting point or root context for agent queries, for example: `dc=domain1,dc=example, dc=com`.
- **Bind Distinguished Name**—The account to use to bind to the directory, for example: `cn=admin,ou=IT, dc=domain1, dc=example, dc=com`.
- **Bind Password**—The bind account password. The agent saves the encrypted password in the configuration file.
- **Search Filter**—The search query for user entries (default is `objectClass=Person`).
- **Server Domain Prefix**—A prefix to uniquely identify the user. This is only required if there are overlapping name spaces, such as different users with the same name from two different directories.
- **Use SSL**—Select the check box to use SSL for eDirectory binding.
- **Verify Server Certificate**—Select the check box to verify the eDirectory server certificate when using SSL.

STEP 4 - **(Strongly recommended)** Disable client probing.



Palo Alto Networks strongly recommends disabling client probing on high-security networks. Client probing can pose a security threat if not correctly configured. For more information, see [client probing](#).

1 On the **Client Probing** tab, deselect the **Enable WMI Probing** check box if it is enabled.



Palo Alto Network strongly recommends that you collect user mapping information from isolated and trusted sources, such as domain controllers or integrations with [Syslog](#) or the [XML API](#), to safely capture user mapping information from any device type or operating system.

If you must enable client probing, select the **Enable WMI Probing** check box and on the **Client Probing** tab. Then add a remote administration exception to the Windows firewall for each probed client to ensure the Windows firewall will allow client probing. Each probed client PC must allow port 139 in the Windows firewall and must also have file and printer sharing services enabled.

STEP 5 - Save the configuration.

Click **OK** to save the User-ID agent setup settings and then click **Commit** to restart the User-ID agent and load the new settings.

STEP 6 - **(Optional)** Define the set of users for which you do not need to provide IP address-to-username mappings, such as kiosk accounts.

Save the **ignore-user** list as a text document on the agent host using the title **ignore_user_list** and use the **.txt** file extension to save it to the User-ID Agent folder on the domain server where the agent is installed.

List the user accounts to ignore; there is no limit to the number of accounts you can add to the list. Each user account name must be on a separate line. For example:



SPAdmin
SPInstall
TFSReport

You can use an asterisk as a wildcard character to match multiple usernames, but only as the last character in the entry. For example, `corpdomain\it-admin*` would match all administrators in the `corpdomain` domain whose usernames start with the string `it-admin`. You can also use the **ignore-user** list to identify users whom you want to force to authenticate using Authentication Portal.



After adding entries to the Ignore User list, you must stop and restart the connection to the service.

Previous

Install the Windows-Based User-ID Agent

Next

Configure User Mapping Using the PAN-OS Integrated User-ID Agent