Next-Generation Firewall

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

Previous
Configure the Windows User-ID Agent for User Mapping

Next
Configure Server Monitoring Using WinRM

The following procedure describes how to configure the PAN-OS® integrated User-ID™ agent on the firewall for IP address-to-username mapping. The integrated User-ID agent performs the same tasks as the Windows-based agent.

STEP 1 - Create an Active Directory service account for the User-ID agent to access the services and hosts that the firewall will monitor for collecting user mapping information.

Create a Dedicated Service Account for the User-ID Agent.

STEP 2 - Define the servers that the firewall will monitor to collect user mapping information.

Within the total maximum of 100 monitored servers per firewall, you can define no more than 50 syslog senders for any single virtual system.

To collect all the required mappings, the firewall must connect to all servers that your users log in to so that the firewall can monitor the Security log files on all servers that contain login events.

1. Select **Device > User Identification > User Mapping**.
2. **Add** a server (Server Monitoring section).
3. Enter a **Name** to identify the server.
4. Select the **Type** of server.
   - **Microsoft Active Directory**
   - **Microsoft Exchange**
   - **Novell eDirectory**
   - **Syslog Sender**
5. (**Microsoft Active Directory and Microsoft Exchange only**) Select the **Transport Protocol** you want to use to monitor security logs and session information on the server.
   - **WMI**—The firewall and the monitored servers use Windows Management Instrumentation (WMI) to communicate.
   - **WinRM-HTTP**—The firewall and the monitored servers use Kerberos for mutual authentication and the monitored server encrypts the communication with the firewall using a negotiated Kerberos session key.
   - **WinRM-HTTPS**—The firewall and the monitored servers use HTTPS to communicate and use basic authentication or Kerberos for mutual authentication.

   If you select a Windows Remote Management (WinRM) option, you must Configure Server Monitoring Using WinRM.
6. (**Microsoft Active Directory, Microsoft Exchange, and Novell eDirectory only**) Enter the **Network Address** of the server.

   If you are using WinRM with Kerberos, you must enter a fully qualified domain name (FQDN). If you want to use WinRM with basic authentication or use **WMI** to monitor the server, you can enter an IP address or FQDN.

   To monitor servers using WMI, specify an IP address, the service account name (if all server monitoring is in the same domain), or a fully qualified domain name (FQDN). If you specify an FQDN, use the down-level logon name in the (DLN)\sAMAccountName format instead of the FQDN\sAMAccountName format. For example, use `example\user.services` not `example.com\user.services`. If you specify an FQDN, the firewall will attempt to authenticate using Kerberos, which does not support WMI.
7. (**Syslog Sender only**) If you select **Syslog Sender** as the server **Type**, Configure the PAN-OS Integrated User-ID Agent as a Syslog Listener.
8. (**Novell eDirectory only**) Make sure the **Server Profile** you select is **Enabled** and click **OK**.
9. (Optional) Configure the firewall to automatically **Discover** domain controllers on your network using DNS lookups.

   The auto-discovery feature is for domain controllers only; you must manually add any Exchange servers or eDirectory servers you want to monitor.

STEP 3 - (Optional) Specify the frequency at which the firewall polls Windows servers for mapping information. This is the interval between the end of the last query and the start of the next query.

If the domain controller is processing many requests, delays between queries may exceed the specified value.

1. **Edit** the **Palo Alto Networks User ID Agent Setup**.
2. Select the **Server Monitor** tab and specify the **Server Log Monitor Frequency** in seconds (range is 1 to 3,600; default is 2). In environments with older domain controllers or high-latency links, set this frequency to a minimum of five seconds.

   Ensure that the **Enable Session** option is not enabled. This option 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 control (NAC) devices.
3. Click **OK** to save your changes.

STEP 4 - Specify the subnetworks that the PAN-OS integrated User-ID agent should include in or exclude from user mapping.

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, optionally, which networks to exclude from User-ID to ensure that the agent is communicating only with internal resources and to prevent unauthorized users from being mapped. You should enable user mapping only on the subnetworks where users internal to your organization are logging in.

1. Select **Device > User Identification > User Mapping**.
2. **Add** an entry to the **Include/Exclude Networks** and enter a **Name** for the entry. Ensure that the entry is **Enabled**.
3. Enter the **Network Address** and then select whether to include or exclude it:
   - **Include**—Select this option to limit user mapping to only users logged in to the specified subnetwork. 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**—Select this option to configure 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 5 - Set the domain credentials for the account that the firewall will use to access Windows resources. This is required for monitoring Exchange servers and domain controllers as well as for WMI probing.

1. **Edit** the **Palo Alto Networks User-ID Agent Setup**.
2. Select the **Server Monitor Account** tab and enter the **User Name** and **Password** for the service account that the User-ID agent will use to probe the clients and monitor servers. Enter the username using the `domain\username` syntax.
3. If you are using WinRM to monitor servers, configure the firewall to authenticate with the server you are monitoring.
   - If you want to use WinRM with basic authentication, enable WinRM on the server, configure basic authentication, and specify the service account **Domain's DNS Name**.
   - If you want to use WinRM with Kerberos, Configure a Kerberos server profile if you have not already done so and then select the **Kerberos Server Profile**.

STEP 6 - (**Optional, not recommended**) Configure WMI probing.

Do not enable WMI probing on high-security networks. Client probing can generate a large amount of network traffic and can pose a security threat when misconfigured.

1. On the **Client Probing** tab, **Enable Probing**.
2. (**Optional**) Specify the **Probe Interval** to define the interval (in minutes) between the end of the last probe request and the start of the next request.

   If necessary, increase the value to ensure the User-ID agent has sufficient time to probe all the learned IP addresses (range is 1 to 1440; default is 20).

   If the request load is high, the observed delay between requests might significantly exceed the specified interval.
3. Click **OK**.
4. Make sure the Windows firewall will allow client probing by adding a remote administration exception to the Windows firewall for each probed client.

STEP 7 - (**Optional**) Define the set of user accounts that don't require IP address-to-username mappings, such as kiosk accounts.

Define the ignore user list on the firewall that is the User-ID agent, not the client. If you define the ignore user list on the client firewall, the users in the list are still mapped during redistribution.

On the **Ignore User List** tab, **Add** each username you want to exclude from user mapping. You can also use the ignore user list to identify the users you want to force to use Authentication Portal to authenticate. 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 add up to 5,000 entries to exclude from user mapping.

STEP 8 - Activate your configuration changes.

Click **OK** and **Commit**.

STEP 9 - Verify the configuration.

1. Access the firewall CLI.
2. Enter the following operational command:

```
> show user server-monitor state all
```

3. On the **Device > User Identification > User Mapping** tab in the web interface, verify that the Status of each server you configured for server monitoring is **Connected**.

Previous
Configure the Windows User-ID Agent for User Mapping

Next
Configure Server Monitoring Using WinRM

© 2026 Palo Alto Networks, Inc. All rights reserved.