Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About this Guide

This guide takes you through the configuration and maintenance of your Palo Alto Networks next-generation firewall. For additional information, refer to the following resources:

- For information on how to configure other components in the Palo Alto Networks Next-Generation Security Platform, go to the Technical Documentation portal: https://docs.paloaltonetworks.com or search the documentation.

- For access to the knowledge base and community forums, refer to https://live.paloaltonetworks.com.

- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/services/solution-assurance.

- For the most current PAN-OS and Panorama 7.1 release notes, go to https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-release-notes

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.
User-ID

The user identity, as opposed to an IP address, is an integral component of an effective security infrastructure. Knowing who is using each of the applications on your network, and who may have transmitted a threat or is transferring files, can strengthen security policies and reduce incident response times. User-ID™, a standard feature on the Palo Alto Networks firewall, enables you to leverage user information stored in a wide range of repositories. The following topics provide more details about User-ID and how to configure it:

- User-ID Overview
- User-ID Concepts
- Enable User-ID
- Map Users to Groups
- Map IP Addresses to Users
- Enable User- and Group-Based Policy
- Enable Policy for Users with Multiple Accounts
- Verify the User-ID Configuration
- Deploy User-ID in a Large-Scale Network
User-ID™ enables you to identify all users on your network using a variety of techniques to ensure that you can identify users in all locations using a variety of access methods and operating systems, including Microsoft Windows, Apple iOS, Mac OS, Android, and Linux®/UNIX. Knowing who your users are instead of just their IP addresses enables:

- **Visibility**—Improved visibility into application usage based on users gives you a more relevant picture of network activity. The power of User-ID becomes evident when you notice a strange or unfamiliar application on your network. Using either ACC or the log viewer, your security team can discern what the application is, who the user is, the bandwidth and session consumption, along with the source and destination of the application traffic, as well as any associated threats.

- **Policy control**—Tying user information to Security policy rules improves safe enablement of applications traversing the network and ensures that only those users who have a business need for an application have access. For example, some applications, such as SaaS applications that enable access to Human Resources services (such as Workday or Service Now) must be available to any known user on your network. However, for more sensitive applications you can reduce your attack surface by ensuring that only users who need these applications can access them. For example, while IT support personnel may legitimately need access to remote desktop applications, the majority of your users do not.

- **Logging, reporting, forensics**—If a security incident occurs, forensics analysis and reporting based on user information rather than just IP addresses provides a more complete picture of the incident. For example, you can use the pre-defined User/Group Activity to see a summary of the web activity of individual users or user groups, or the SaaS Application Usage report to see which users are transferring the most data over unsanctioned SaaS applications.

To enforce user- and group-based policies, the firewall must be able to map the IP addresses in the packets it receives to usernames. User-ID provides many mechanisms to collect this User Mapping information. For example, the User-ID agent monitors server logs for login events and listens for syslog messages from authenticating services. To identify mappings for IP addresses that the agent didn’t map, you can configure the firewall to redirect HTTP requests to a Captive Portal login. You can tailor the user mapping mechanisms to suit your environment, and even use different mechanisms at different sites to ensure that you are safely enabling access to applications for all users, in all locations, all the time.

**Figure: User-ID**

![User-ID Diagram](image)
To enable user- and group-based policy enforcement, the firewall requires a list of all available users and their corresponding group memberships so that you can select groups when defining your policy rules. The firewall collects Group Mapping information by connecting directly to your LDAP directory server, or using XML API integration with your directory server.

See User-ID Concepts for information on how User-ID works and Enable User-ID for instructions on setting up User-ID.

User-ID does not work in environments where the source IP addresses of users are subject to NAT translation before the firewall maps the IP addresses to usernames.
User-ID Concepts

**Group Mapping**

To define policy rules based on user or group, first you create an LDAP server profile that defines how the firewall connects and authenticates to your directory server. The firewall supports a variety of directory servers, including Microsoft Active Directory (AD), Novell eDirectory, and Sun ONE Directory Server. The server profile also defines how the firewall searches the directory to retrieve the list of groups and the corresponding list of members. If you are using a directory server that is not natively supported by the firewall, you can integrate the group mapping function using the XML API. You can then create a group mapping configuration to Map Users to Groups and Enable User- and Group-Based Policy.

Defining policy rules based on group membership rather than on individual users simplifies administration because you don’t have to update the rules whenever new users are added to a group. When configuring group mapping, you can limit which groups will be available in policy rules. You can specify groups that already exist in your directory service or define custom groups based on LDAP filters. Defining custom groups can be quicker than creating new groups or changing existing ones on an LDAP server, and doesn't require an LDAP administrator to intervene. User-ID maps all the LDAP directory users who match the filter to the custom group. For example, you might want a security policy that allows contractors in the Marketing Department to access social networking sites. If no Active Directory group exists for that department, you can configure an LDAP filter that matches users for whom the LDAP attribute Department is set to Marketing. Log queries and reports that are based on user groups will include custom groups.

**User Mapping**

Knowing user and groups names is only one piece of the puzzle. The firewall also needs to know which IP addresses map to which users so that security rules can be enforced appropriately. Figure: User-ID illustrates the different methods that are used to identify users and groups on your network and shows how user mapping and group mapping work together to enable user- and group-based security enforcement and visibility. The following topics describe the different methods of user mapping:
Server Monitoring

With server monitoring a User-ID agent—either a Windows-based agent running on a domain server in your network, or the integrated PAN-OS User-ID agent running on the firewall—monitors the security event logs for specified Microsoft Exchange Servers, Domain Controllers, or Novell eDirectory servers for login events. For example, in an AD environment, you can configure the User-ID agent to monitor the security logs for Kerberos ticket grants or renewals, Exchange server access (if configured), and file and print service connections. Note that for these events to be recorded in the security log, the AD domain must be configured to log successful account login events. In addition, because users can log in to any of the servers in the domain, you must set up server monitoring for all servers to capture all user login events. See Configure User Mapping Using the Windows User-ID Agent or Configure User Mapping Using the PAN-OS Integrated User-ID Agent for details.

Port Mapping

In environments with multi-user systems—such as Microsoft Terminal Server or Citrix environments—many users share the same IP address. In this case, the user-to-IP address mapping process requires knowledge of the source port of each client. To perform this type of mapping, you must install the Palo Alto Networks Terminal Services Agent on the Windows/Citrix terminal server itself to intermediate the assignment of source ports to the various user processes. For terminal servers that do not support the Terminal Services agent, such as Linux terminal servers, you can use the XML API to send user mapping information from login and logout events to User-ID. See Configure User Mapping for Terminal Server Users for configuration details.

XFF Headers

User-ID can read the IPv4 or IPv6 addresses of users from the X-Forwarded-For (XFF) header in HTTP client requests when the firewall is deployed between the Internet and a proxy server that would otherwise hide the user IP addresses. User-ID matches the true user IP addresses with usernames. See Configure the firewall to obtain the user IP address from the X-Forwarded-For (XFF) header.

Captive Portal

If the firewall or the User-ID agent can't map an IP address to a username—for example, if the user isn't logged in or uses an operating system such as Linux that your domain servers don't support—you can configure Captive Portal. Any web traffic (HTTP or HTTPS) that matches a Captive Portal policy rule requires user authentication. You can base the authentication on a transparent browser-challenge (Kerberos single sign-on (SSO) or NT LAN Manager (NTLM) authentication), web form (for RADIUS, TACACS+, LDAP, Kerberos, or local database authentication), or client certificates. For details, see Map IP Addresses to Usernames Using Captive Portal.
Syslog

Your environment might have existing network services that authenticate users. These services include wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, and other Network Access Control (NAC) mechanisms. You can configure these services to send syslog messages and configure the User-ID agent to parse the messages for login events. The agent then maps IP addresses to usernames based on the login events.

Both the PAN-OS integrated User-ID agent and Windows-based User-ID agent use Syslog Parse profiles to parse syslog messages. In environments where services send the messages in different formats, you can create a custom profile for each format. If you use the PAN-OS integrated User-ID agent, you can also use predefined Syslog Parse profiles that Palo Alto Networks provides through Applications content updates.

Syslog messages must meet the following criteria for a User-ID agent to parse them:

- Each message must be a single-line text string. The allowed delimiters for line breaks are a new line (\n) or a carriage return plus a new line (\r\n).
- The maximum size for individual messages is 2,048 bytes.
- Messages sent over UDP must be contained in a single packet; messages sent over SSL can span multiple packets. A single packet might contain multiple messages.

See Configure User-ID to Receive User Mappings from a Syslog Sender for configuration details.
GlobalProtect

For mobile or roaming users, the GlobalProtect client provides the user mapping information to the firewall directly. In this case, every GlobalProtect user has an agent or app running on the client that requires the user to enter login credentials for VPN access to the firewall. This login information is then added to the User-ID user mapping table on the firewall for visibility and user-based security policy enforcement. Because GlobalProtect users must authenticate to gain access to the network, the IP address-to-username mapping is explicitly known. This is the best solution in sensitive environments where you must be certain of who a user is in order to allow access to an application or service. For more information on setting up GlobalProtect, refer to the GlobalProtect Administrator’s Guide.

XML API

Captive Portal and the other standard user mapping methods might not work for certain types of user access. For example, the standard methods cannot add mappings of users connecting from a third-party VPN solution or users connecting to a 802.1x-enabled wireless network. For such cases, you can use the PAN-OS XML API to capture login events and send them to the PAN-OS integrated User-ID agent. See Send User Mappings to User-ID Using the XML API for details.

Client Probing

In a Microsoft Windows environment, you can configure the User-ID agent to probe client systems using Windows Management Instrumentation (WMI) and/or NetBIOS probing at regular intervals to verify that an existing user mapping is still valid or to obtain the username for an IP address that is not yet mapped.

NetBIOS probing is only supported on the Windows-based User-ID agent; it is not supported on the PAN-OS integrated User-ID agent.

Client probing was designed for legacy networks where most users were on Windows workstations on the internal network, but is not ideal for today’s more modern networks that support a roaming and mobile user base on a variety of devices and operating systems. Additionally, client probing can generate a large amount of network traffic (based on the total number of mapped IP addresses) and can pose a security threat when misconfigured. Therefore, client probing is no longer a recommended method for user mapping. Instead collect user mapping information from more isolated and trusted sources, such as domain controllers and through integrations with Syslog or the XML API, which allow you to safely capture user mapping information from any device type or operating system. If you have sensitive applications that require you to know exactly who a user is, configure Captive Portal to ensure that you are only allowing access to authorized users.

Because WMI probing trusts data reported back from the endpoint, it is not a recommended method of obtaining User-ID information in a high-security network. If you are using the User-ID agent to parse AD security event logs, syslog messages, or the XML API to obtain User-ID mappings, Palo Alto Networks recommends disabling WMI probing.

If you do choose to use WMI probing, do not enable it on external, untrusted interfaces, as this would cause the agent to send WMI probes containing sensitive information such as the username, domain name, and password hash of the User-ID agent service account outside of your network. This information could potentially be exploited by an attacker to penetrate the network to gain further access.
If you do choose to enable probing in your trusted zones, the agent will probe each learned IP address periodically (every 20 minutes by default, but this is configurable) to verify that the same user is still logged in. In addition, when the firewall encounters an IP address for which it has no user mapping, it will send the address to the agent for an immediate probe.

Enable User-ID

The user identity, as opposed to an IP address, is an integral component of an effective security infrastructure. Knowing who is using each of the applications on your network, and who may have transmitted a threat or is transferring files, can strengthen your security policy and reduce incident response times. User-ID enables you to leverage user information stored in a wide range of repositories for visibility, user- and group-based policy control, and improved logging, reporting, and forensics:

> On PA-5060 and PA-7000 Series firewalls that have the multiple virtual systems capability disabled, you can base policies on up to 3,200 distinct user groups. If these platforms have multiple virtual systems, the limit is 640 groups. All other firewall platforms support up to 640 groups per virtual system or per firewall (if it doesn’t have multiple virtual systems).

Use the following workflow to configure User-ID.

**Configure User-ID**

**Step 1** Enable User-ID on the source zones that contain the users who will send requests that require user-based access controls.

- Enable User-ID on trusted zones only. If you enable User-ID and client probing on an external untrusted zone (such as the internet), probes could be sent outside your protected network, resulting in an information disclosure of the User-ID agent service account name, domain name, and encrypted password hash, which could allow an attacker to gain unauthorized access to protected resources.

1. Select **Network > Zones** and click the Name of the zone.
2. Select the **Enable User Identification** check box and click **OK**.

**Step 2** Create a Dedicated Service Account for the User-ID Agent.

- Create a service account with the minimum set of permissions required to support the User-ID options you enable to reduce your attack surface in the event that the service account is compromised.

This is required if you plan to use the Windows-based User-ID agent or the PAN-OS integrated User-ID agent to monitor domain controllers, Exchange servers, Windows clients for user login and logout events.

**Step 3** Map Users to Groups.

- This enables the firewall to connect to your LDAP directory and retrieve Group Mapping information so that you will be able to select usernames and group names when creating policy.
### Configure User-ID (Continued)

#### Step 4  Map IP Addresses to Users.

As a best practice, do not enable client probing as a user mapping method on high-security networks. Client probing can generate a large amount of network traffic and can pose a security threat when misconfigured.

The way you do this depends on where your users are located and what types of systems they are using, and what systems on your network are collecting login and logout events for your users. You must configure one or more User-ID agents to enable User Mapping:
- Configure User Mapping Using the Windows User-ID Agent.
- Configure User Mapping Using the PAN-OS Integrated User-ID Agent.
- Configure User-ID to Receive User Mappings from a Syslog Sender.
- Configure User Mapping for Terminal Server Users.
- Send User Mappings to User-ID Using the XML API.

#### Step 5  Specify the networks to include and exclude from user mapping.

As a best practice, always specify which networks to include and exclude from User-ID. This allows you to ensure that only your trusted assets are probed and that unwanted user mappings are not created unexpectedly.

Configure each agent that you configured for user mapping as follows:
- Specify the subnetworks the Windows User-ID agent should include in or exclude from User-ID.
- Specify the subnetworks the PAN-OS integrated User-ID agent should include in or exclude from user mapping.

#### Step 6  Enable user- and group-based policy enforcement.

Create rules based on group rather than user whenever possible. This prevents you from having to continually update your rules (which requires a commit) whenever your user base changes.

After configuring User-ID, you will be able to choose a username or group name when defining the source or destination of a security rule:

1. Select **Policies > Security** and Add a new rule or click an existing rule name to edit.
2. Select the **User** tab and specify which users and groups to match in the rule in one of the following ways:
   - If you want to select specific users/groups as matching criteria, click the **Add** button in the Source User section to display a list of users and groups discovered by the firewall group mapping function. Select the users and/or groups to add to the rule.
   - If you want to match any user who has or has not authenticated and you don’t need to know the specific user or group name, select **known-user** or **unknown** from the drop-down above the Source User list.
3. Configure the rest of the rule as appropriate and then click **OK** to save it. For details on other fields in the security rule, see Set Up a Basic Security Policy.
### Configure User-ID (Continued)

**Step 7** Create the Security policy rules to safely enable User-ID within your trusted zones and prevent User-ID traffic from egressing your network.

Follow the [Best Practice Internet Gateway Security Policy](#) to ensure that the User-ID application (paloalto-userid-agent) is only allowed in the zones where your agents (both your Windows agents and your PAN-OS integrated agents) are monitoring services and distributing mappings to firewalls. Specifically:

- Allow the paloalto-userid-agent application between the zones where your agents reside and the zones where the monitored servers reside (or even better, between the specific systems that host the agent and the monitored servers).
- Allow the paloalto-userid-agent application between the agents and the firewalls that need the user mappings and between firewalls that are redistributing user mappings and the firewalls they are redistributing the information to.
- Deny the paloalto-userid-agent application to any external zone, such as your internet zone.

**Step 8** Configure Captive Portal.

Because Captive Portal authenticates users rather than relying on user mappings, it is useful for ensuring that you know exactly who is accessing your most sensitive applications and data. You can configure Captive Portal as the fall-back to identify users who have not yet been identified using another user mapping method before allowing access.

As a best practice, choose Kerberos transparent authentication over NTLM authentication when configuring Captive Portal. Kerberos is a stronger, more robust authentication method than NTLM and it does not require the firewall to have an administrative account to join the domain.

**Configure Captive Portal.**

1. Select **Policies > Captive Portal**.
2. Add a **Name** for the rule.
3. Define the matching criteria for the rule by completing the **Source**, **Destination**, and **Service/URL Category** tabs as appropriate to match the traffic you want to authenticate. The matching criteria on these tabs is the same as the criteria you define when creating a Security policy rule. See [Set Up a Basic Security Policy](#) for details.
4. Define the **Action** to take on traffic that matches the rule:
   - **no-captive-portal**—Allow traffic to pass without presenting a Captive Portal page for authentication.
   - **web-form**—Present a Captive Portal page for the user to explicitly enter authentication credentials or use client certificate authentication.
   - **browser-challenge**—Transparently obtain user authentication credentials. If you select this action, you must enable Kerberos single sign-on (SSO) or NT LAN Manager (NTLM) authentication when you Configure Captive Portal. If Kerberos SSO authentication fails, the firewall falls back to NTLM authentication. If you didn’t configure NTLM, or NTLM authentication fails, the firewall falls back to **web-form** authentication.
5. Click **OK** and **Commit**.
## Configure User-ID (Continued)

**Step 9** Configure the firewall to obtain the user IP address from the X-Forwarded-For (XFF) header. When the firewall is between the Internet and a proxy server, the IP address in the packet the firewall sees contains is for the proxy server rather than the user. To enable visibility of the user IP address instead, configure the firewall to use the XFF header for user mapping. With this option enabled, the firewall matches the IP addresses with usernames referenced in policy to enable control and visibility for the associated users and groups. For details, see Identify Users Connected through a Proxy Server.

1. Select **Device > Setup > Content-ID** and edit the X-Forwarded-For Headers settings.
2. Select the **X-Forwarded-For Header** in **User-ID** check box. Selecting the **Strip-X-Forwarded-For Header** check box doesn't disable the use of XFF headers for user attribution in policy rules; the firewall zeroes out the XFF value only after using it for user attribution.
3. Click **OK** to save your changes.

**Step 10** Verify the User-ID Configuration.

After you configure user mapping and group mapping, verify that it is working properly and that you can safely enable and monitor user and group access to the applications, resources, and services.
Map Users to Groups

Defining policy rules based on user group membership rather than individual users simplifies administration because you don’t have to update the rules whenever group membership changes. Use the following procedure to enable the firewall to connect to your LDAP directory and retrieve Group Mapping information. You can then Enable User- and Group-Based Policy.

The following are best practices for group mapping in an Active Directory (AD) environment:

- If you have a single domain, you need only one group mapping configuration with an LDAP server profile that connects the firewall to the domain controller with the best connectivity. You can add up to four domain controllers to the LDAP server profile for redundancy. Note that you cannot increase redundancy beyond four domain controllers for a single domain by adding multiple group mapping configurations for that domain.
- If you have multiple domains and/or multiple forests, you must create a group mapping configuration with an LDAP server profile that connects the firewall to a domain server in each domain/forest. Take steps to ensure unique usernames in separate forests.
- If you have Universal Groups, create an LDAP server profile to connect to the Global Catalog server.

<table>
<thead>
<tr>
<th>Map Users to Groups</th>
<th>Configure an LDAP Server Profile:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Add an LDAP server profile. The profile defines how the firewall connects to the directory servers from which it collects group mapping information. You can add up to four servers to the profile but they must be the same Type.</td>
<td>1. Select Device &gt; Server Profiles &gt; LDAP, click Add, and enter a Profile Name.</td>
</tr>
<tr>
<td></td>
<td>2. For each LDAP server, click Add and enter the server Name, IP address (LDAP Server), and Port (default is 389).</td>
</tr>
<tr>
<td></td>
<td>3. Based on your Type selection (for example, active-directory), the firewall automatically populates the correct LDAP attributes in the group mapping settings. However, if you customized your LDAP schema, you might need to modify the default settings.</td>
</tr>
<tr>
<td></td>
<td>4. In the Base DN field, enter the Distinguished Name (DN) of the LDAP tree location where you want the firewall to begin its search for user and group information.</td>
</tr>
<tr>
<td></td>
<td>5. Enter the authentication credentials for binding to the LDAP tree in the Bind DN, Password, and Confirm Password fields. The Bind DN can be a fully qualified LDAP name (for example, cn=administrator,cn=users,dc=acme,dc=local) or a user principal name (for example, <a href="mailto:administrator@acme.local">administrator@acme.local</a>).</td>
</tr>
<tr>
<td></td>
<td>6. Click OK to save the profile.</td>
</tr>
</tbody>
</table>
Configure the server settings in a group mapping configuration.

2. Select a virtual system (Location) if the firewall has multiple.
3. Click Add and enter a unique Name to identify the group mapping configuration.
4. Select the LDAP Server Profile you just created.
5. (Optional) By default, the User Domain field is blank: the firewall automatically detects the domain names for Active Directory (AD) servers. If you enter a value, it overrides any domain names that the firewall retrieves from the LDAP source. Your entry must be the NetBIOS domain name.
6. (Optional) To filter the groups that the firewall tracks for group mapping, in the Group Objects section, enter a Search Filter (LDAP query), Object Class (group definition), Group Name, and Group Member.
7. (Optional) To filter the users that the firewall tracks for group mapping, in the User Objects section, enter a Search Filter (LDAP query), Object Class (user definition), and User Name.
8. (Optional) To match User-ID information with email header information identified in the links and attachments of emails forwarded to WildFire™, enter the list of email domains in your organization in the Mail Domains section, Domain List field. Use commas to separate multiple domains (up to 256 characters). After you click OK, PAN-OS automatically populates the Mail Attributes field based on your LDAP server type (Sun/RFC, Active Directory, or Novell). When a match occurs, the username in the WildFire log email header section will contain a link that opens the ACC tab, filtered by user or user group.
9. Make sure the Enabled check box is selected.
### Map Users to Groups (Continued)

**Step 3**  
Limit which groups will be available in policy rules.  
Required only if you want to limit policy rules to specific groups. By default, if you don't specify groups, all groups are available in policy rules.  

Any custom groups you create will also be available in the Allow List of authentication profiles.

1. Add existing groups from the directory service:  
   a. Select the **Group Include List** tab.  
   b. In the Available Groups list, select the groups you want to appear in policy rules and click the Add icon.  
2. If you want to base policy rules on user attributes that don't match existing user groups, create custom groups based on LDAP filters:  
   a. Select the **Custom Group** tab and click **Add**.  
   b. Enter a group **Name** that is unique in the group mapping configuration for the current firewall or virtual system. If the **Name** has the same value as the Distinguished Name (DN) of an existing AD group domain, the firewall uses the custom group in all references to that name (for example, in policies and logs).  
   c. Specify an **LDAP Filter** of up to 2,048 UTF-8 characters and click **OK**. The firewall doesn't validate LDAP filters, so it's up to you to ensure they are accurate.  

To minimize the performance impact on the LDAP directory server, use only indexed attributes in the filter.

3. Click **OK** to save your changes.

**Step 4**  
Commit your changes.

Click **Commit**. A commit is necessary before you can use custom groups in policies and objects.  

After configuring the firewall to retrieve group mapping information from an LDAP server, but before configuring policies based on the groups it retrieves, you must either wait for the firewall to refresh its group mappings cache or refresh the cache manually. To verify which groups you can currently use in policies, access the firewall CLI and run the `show user group` command. To determine when the firewall will next refresh the group mappings cache, run the `show user group-mapping statistics` command and check the Next Action. To manually refresh the cache, run the `debug user-id refresh group-mapping all` command.
Map IP Addresses to Users

User-ID provides many different methods for mapping IP addresses to usernames. Before you begin configuring user mapping, consider where your users are logging in from, what services they are accessing, and what applications and data you need to control access to. This will inform which types of agents or integrations would best allow you to identify your users. For guidance, refer to Architecting User Identification Deployments.

Once you have your plan, you can begin configuring user mapping using one or more of the following methods as needed to enable user-based access and visibility to applications and resources:

- To map users as they log in to your Exchange servers, domain controllers, eDirectory servers, or Windows clients you must configure a User-ID agent:
  - Configure User Mapping Using the PAN-OS Integrated User-ID Agent
  - Configure User Mapping Using the Windows User-ID Agent

- If you have clients running multi-user systems in a Windows environment, such as Microsoft Terminal Server or Citrix Metaframe Presentation Server or XenApp, Configure the Palo Alto Networks Terminal Services Agent for User Mapping. For a multi-user system that doesn't run on Windows, you can Retrieve User Mappings from a Terminal Server Using the PAN-OS XML API.

- To obtain user mappings from existing network services that authenticate users—such as wireless controllers, 802.1x devices, Apple Open Directory servers, proxy servers, or other Network Access Control (NAC) mechanisms—Configure User-ID to Receive User Mappings from a Syslog Sender.

  While you can configure either the Windows agent or the PAN-OS integrated User-ID agent on the firewall to listen for authentication syslog messages from the network services, because only the PAN-OS integrated agent supports syslog listening over TLS, it is the preferred configuration.

- If you have users with client systems that aren’t logged in to your domain servers—for example, users running Linux clients that don’t log in to the domain—you can Map IP Addresses to Usernames Using Captive Portal.

- For other clients that you can’t map using the other methods, you can Send User Mappings to User-ID Using the XML API.

- A large-scale network can have hundreds of information sources that firewalls query for user and group mapping and can have numerous firewalls that enforce policies based on the mapping information. You can simplify User-ID administration for such a network by aggregating the mapping information before the User-ID agents collect it. You can also reduce the resources that the firewalls and information sources use in the querying process by configuring some firewalls to redistribute the mapping information. For details, see Deploy User-ID in a Large-Scale Network.
Create a Dedicated Service Account for the User-ID Agent

If you plan to use either the Windows-based User-ID agent or the PAN-OS integrated User-ID agent to map users as they log in to your Exchange servers, domain controllers, eDirectory servers, or Windows clients, you must create a dedicated service account for the User-ID agent on a domain controller in each domain that the agent will monitor.

The required permissions for the service account depend on what user mapping methods and settings you plan to use. For example, if you are using the PAN-OS integrated User-ID agent, the service account requires Server Operator privileges. If you are using the Windows-based User-ID agent, the service account does not require Server Operator privileges. To reduce the risk associated with compromise of the User-ID service account, always configure the account with the minimum set of permissions necessary for the agent to function properly.

User-ID provides many methods for safely collecting user mapping information. Some of the legacy features, which were designed for environments that only required mapping of users on Windows desktops attached to the local network, require privileged service accounts. In the event that the privileged service account is compromised, this would open your network to attack. As a best practice, avoid using these legacy features—such as client probing, NTLM authentication, and session monitoring—that require privileges that would pose a threat if compromised. The following workflow details all privileges required and provide guidance as to which User-ID features require privileges that could pose a threat so that you can decide how to best identify users without compromising your overall security posture.

Configure an Active Directory account for the User-ID Agent

| Step 1 | Create an AD account for the User-ID agent. You must create a service account in each domain the agent will monitor. |
|        | 1. Log in to the domain controller. |
|        | 2. Right-click the Windows icon ( ), Search for Active Directory Users and Computers, and launch the application. |
|        | 3. In the navigation pane, open the domain tree, right-click Managed Service Accounts and select New > User. |
|        | 4. Enter the First Name, Last Name, and User logon name of the user and click Next. |
|        | 5. Enter the Password and Confirm Password, and then click Next and Finish. |
## Configure an Active Directory account for the User-ID Agent (Continued)

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Add the account to the Builtin groups that have privileges for accessing the services and hosts the User-ID agent will monitor.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Right-click the service account you just added and <strong>Add to a group</strong>.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Enter the object names to select</strong> as follows to assign the account to groups. Separate each entry with a semicolon.</td>
</tr>
<tr>
<td>•</td>
<td><strong>Event Log Readers</strong> or a custom group that has privileges for reading Security log events. These privileges are required if the User-ID agent will collect mapping information by monitoring Security logs.</td>
</tr>
<tr>
<td>•</td>
<td><strong>(PAN-OS integrated agent only) Distributed COM Users</strong> group, which has privileges for launching, activating, and using Distributed Component Object Model (DCOM) objects.</td>
</tr>
<tr>
<td>•</td>
<td><strong>(PAN-OS integrated agent only - Not recommended) Server Operators</strong> group, which has privileges for opening sessions. The agent only requires these privileges if you plan to configure it to refresh existing mapping information by monitoring user sessions.</td>
</tr>
<tr>
<td></td>
<td>Because this group also has privileges for shutting down and restarting servers, assign the account to it only if monitoring user sessions is very important.</td>
</tr>
<tr>
<td>•</td>
<td><strong>(PAN-OS integrated agent only) If you plan to configure NTLM authentication for Captive Portal, the firewall where you've configured the agent will need to join the domain. To enable this, enter the name of a group that has administrative privileges to join the domain, write to the validated service principal name, and create a computer object within the <code>computers</code> organization unit (ou=computers).</strong></td>
</tr>
<tr>
<td></td>
<td>The PAN-OS integrated agent requires privileged operations to join the domain, which poses a security threat if the account is compromised. Consider configuring Kerberos authentication for Captive Portal instead of NTLM. Kerberos is a stronger, more secure authentication method and it does not require the firewall to join the domain. For a firewall with multiple virtual systems, only vsys1 can join the domain because of AD restrictions on virtual systems running on the same host.</td>
</tr>
</tbody>
</table>
| 3.     | **Check Names** to validate your entries and click **OK** twice. **


Step 3 If you plan to use WMI probing, enable the account to read the CIMV2 namespace and assign the required permissions on the client systems to be probed.

By default, accounts in the Server Operators group have this permission. Do not enable client probing on high-security networks. Client probing can generate a large amount of network traffic and can pose a security threat when misconfigured. Instead collect user mapping information from more isolated and trusted sources, such as domain controllers and through integrations with Syslog or the XML API, which have the added benefit of allowing you to safely capture user mapping information from any device type or operating system, instead of just Windows clients.

Perform this task on each client system that the User-ID agent will probe for user mapping information:

1. Right-click the Windows icon ( ), Search for wmi.mgmt.msc, and launch the WMI Management Console.
2. In the console tree, right-click WMI Control and select Properties.
3. Select Security, select Root > CIMV2, and click Security. You might have to change the Locations or click Advanced to query for account names. See the dialog help for details.
4. Add the name of the service account you created, Check Names to verify your entry, and click OK.
5. In the Permissions for <Username> section, Allow the Enable Account and Remote Enable permissions.
6. Click OK twice.
7. Use the Local Users and Groups MMC snap-in (lusrmgr.msc) to add the service account to the local Distributed Component Object Model (DCOM) Users and Remote Desktop Users groups on the system that will be probed.

Step 4 Turn off account privileges that are not necessary.

By ensuring that the User-ID service account has the minimum set of account privileges, you can reduce the attack surface should the account be compromised.

To ensure that the User-ID account has the minimum privileges necessary, deny the following privileges on the account:

- **Deny interactive logon for the User-ID service account**—While the User-ID service account does need permission to read and parse Active Directory security event logs, it does not require the ability to logon to servers or domain systems interactively. You can restrict this privilege using Group Policies or by using a Managed Service account (refer to Microsoft TechNet for more information).
- **Deny remote access for the User-ID service account**—This prevents an attacker from using the account to access your network from the outside the network.

Step 5 Next steps...

You are now ready to:

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

In most cases, the majority of your network users will have logins to your monitored domain services. For these users, the Palo Alto Networks User-ID agent monitors the servers for login events and performs the IP address to username mapping. The way you configure the User-ID agent depends on the size of your environment and the location of your domain servers. As a best practice, locate your User-ID agents near the servers it will monitor (that is, the monitored servers and the Windows User-ID agent should not be across a WAN link from each other). This is because most of the traffic for user mapping occurs between the agent and the monitored server, with only a small amount of traffic—the delta of user mappings since the last update—from the agent to the firewall.

The following topics describe how to install and configure the User-ID Agent and how to configure the firewall to retrieve user mapping information from the agent:

▲ Install the User-ID Agent
▲ Configure the User-ID Agent for User Mapping

Install the User-ID Agent

The following procedure shows how to install the User-ID agent on a member server in the domain and set up the service account with the required permissions. If you are upgrading, the installer will automatically remove the older version, however, it is a good idea to back up the config.xml file before running the installer.

![For information about the system requirements for installing the Windows-based User-ID agent and for information on supported server OS versions, refer to “Operating System (OS) Compatibility User-ID Agent” in the User-ID Agent Release Notes.]

Install the Windows User-ID Agent

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Create a dedicated Active Directory service account for the User-ID agent to access the services and hosts it will monitor to collect user mappings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Create a Dedicated Service Account for the User-ID Agent.</td>
</tr>
<tr>
<td>2.</td>
<td>Add the service account to the Event Log Reader builtin group to enable privileges to read the security log events.</td>
</tr>
<tr>
<td>a.</td>
<td>Run the MMC and launch the Active Directory Users and Computers snap-in.</td>
</tr>
<tr>
<td>b.</td>
<td>Navigate to the Builtin folder for the domain, right-click the Event Log Reader group and select Add to Group to open the properties dialog.</td>
</tr>
<tr>
<td>c.</td>
<td>Click Add and enter the name of the service account that you configured the User-ID service to use, then click Check Names to validate that you have the proper object name.</td>
</tr>
<tr>
<td>d.</td>
<td>Click OK twice to save the settings.</td>
</tr>
<tr>
<td>3.</td>
<td>Enable the service account to log on as a service.</td>
</tr>
<tr>
<td>b.</td>
<td>Right-click Log on as a service, then select Properties.</td>
</tr>
<tr>
<td>c.</td>
<td>Add the service account username or builtin group (Administrators have this privilege by default.).</td>
</tr>
</tbody>
</table>
Step 2 Decide where to install the User-ID agent.
The User-ID agent queries the Domain Controller and Exchange server logs using Microsoft Remote Procedure Calls (MSRPCs), which require a complete transfer of the entire log at each query. Therefore, always install one or more User-ID agents at each site that has servers to be monitored.

For more detailed information on where to install User-ID agents, refer to Architecting User Identification (User-ID) Deployments.

- You must install the User-ID agent on a system running one of the supported OS versions: see “Operating System (OS) Compatibility User-ID Agent” in the User-ID Agent Release Notes.
- Make sure the system that will host the User-ID agent is a member of the same domain as the servers it will monitor.
- As a best practice, install the User-ID agent close to the servers it will be monitoring (there is more traffic between the User-ID agent and the monitored servers than there is between the User-ID agent and the firewall, so locating the agent close to the monitored servers optimizes bandwidth usage).
- To ensure the most comprehensive mapping of users, you must monitor all domain controllers that process authentication for users you want to map. You might need to install multiple User-ID agents to efficiently monitor all of your resources.

Step 3 Download the User-ID agent installer. Install the User-ID agent version that is the same as the PAN-OS version running on the firewalls. If there is not a User-ID agent version that matches the PAN-OS version, install the latest version that is closest to the PAN-OS version. For example, if you are running PAN-OS 7.1 on your firewalls, install User-ID agent version 7.0.

1. Log in to the Palo Alto Networks Customer Support web site.
2. Select Software Updates from the Manage Devices section.
3. Scroll to the User Identification Agent section of the screen and Download the version of the User-ID agent you want to install.
4. Save the UaInstall-x.x.x-xx.msi file on the system(s) where you plan to install the agent.

Step 4 Run the installer as an administrator.
1. Open the Windows Start menu, right-click the Command Prompt program, and select Run as administrator.
2. From the command line, run the .msi file you downloaded. For example, if you saved the .msi file to the Desktop you would enter the following:
   C:\Users\administrator.acme>cd Desktop
   C:\Users\administrator.acme\Desktop>UaInstall-6.0.0-1.msi
3. Follow the setup prompts to install the agent using the default settings. By default, the agent gets installed to the C:\Program Files (x86)\Palo Alto Networks\User-ID Agent folder, but you can Browse to a different location.
4. When the installation completes, Close the setup window.

Step 5 Launch the User-ID Agent application.
Open the Windows Start menu and select User-ID Agent.
### Install the Windows User-ID Agent (Continued)

**Step 6 (Optional)** Change the service account that the User-ID agent uses to log in.

By default, the agent uses the administrator account used to install the .msi file. However, you may want to switch this to a restricted account as follows:

1. Select **User Identification > Setup** and click **Edit**.
2. Select the **Authentication** tab and enter the service account name that you want the User-ID agent to use in the **User name for Active Directory** field.
3. Enter the **Password** for the specified account.
4. **Commit** the changes to the User-ID agent configuration to restart the service using the service account credentials.

**Step 7 (Optional)** Assign account permissions to the installation folder.

You only need to perform this step if the service account you configured for the User-ID agent is not either a domain administrator or a local administrator on the User-ID agent server host.

1. **Give the service account permissions to the installation folder:**
   a. From the Windows Explorer, navigate to `C:\Program Files\Palo Alto Networks` and right-click the folder and select **Properties**.
   b. On the **Security** tab, click **Edit**, then **Add** the User-ID agent service account and assign it permissions to **Modify**, **Read & execute**, **List folder contents**, **Read**, and **Write** and then click **OK** to save the account settings.
   2. **Give the service account permissions to the User-ID Agent registry sub-tree:**
      a. Run `regedit32` and navigate to the Palo Alto Networks sub-tree in one of the following locations:
         - **32-bit systems**—`HKEY_LOCAL_MACHINE\Software\Palo Alto Networks`
         - **64-bit systems**—`HKEY_LOCAL_MACHINE\Software\WOW6432Node\Palo Alto Networks`
      b. Right-click the Palo Alto Networks node and select **Permissions**.
      c. Assign the User-ID service account **Full Control** and then click **OK** to save the setting.
   3. **On the domain controller, add the service account to the builtin groups to enable privileges to read the security log events (Event Log Reader group) and open sessions (Server Operator group):**
      a. Run the MMC and Launch the Active Directory Users and Computers snap-in.
      b. Navigate to the Builtin folder for the domain and then right-click each group you need to edit (Event Log Reader and Server Operator) and select **Add to Group** to open the properties dialog.
      c. Click **Add** and enter the name of the service account that you configured the User-ID service to use and then click **Check Names** to validate that you have the proper object name.
      d. Click **OK** twice to save the settings.
Configure the User-ID Agent for User Mapping

The Palo Alto Networks 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.

Map IP Addresses to Users Using the Windows-based User-ID Agent

**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 firewall to automatically discover domain controllers on your network using DNS lookups, click **Auto Discover**.
   
   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 (XML API only) 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.
Map IP Addresses to Users Using the Windows-based User-ID Agent (Continued)

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 subnetworks for exclusion without adding any for inclusion, the agent will not perform user mapping in any subnetwork.
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.
Map IP Addresses to Users Using the Windows-based User-ID Agent (Continued)

| Step 4     | 1. On the Client Probing tab, select the Enable WMI Probing check box and/or the Enable NetBIOS Probing check box.  
|            | 2. Make sure the Windows firewall will allow client probing by adding a remote administration exception to the Windows firewall for each probed client.  
| Optional, not recommended | For NetBIOS probing to work effectively, each probed client PC must allow port 139 in the Windows firewall and must also have file and printer sharing services enabled. Although client probing is not recommended, if you plan to enable it, WMI probing is preferred over NetBIOS whenever possible.  
| Configure client probing. Do not enable client probing on high-security networks. Client probing can generate a large amount of network traffic and can pose a security threat when misconfigured. |  

| Step 5     | 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.  
|            | Save the configuration.  
| Optional   |  

| Step 6     | Save the ignore-user list as a text document 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.  
| (Optional) Define the set of users for which you do not need to provide IP address-to-username mappings, such as kiosk accounts. Use the ignore-user list to identify users whom you want to force to authenticate using Captive Portal. | 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. |  

| Step 7     | Complete the following steps on each firewall you want to connect to the User-ID agent to receive user mappings:  
| Configure the firewalls to connect to the User-ID agent. | 1. Select Device > User Identification > User-ID Agents and click Add.  
|            | 2. Enter a Name for the User-ID agent.  
|            | 3. Enter the IP address of the Windows Host on which the User-ID Agent is installed.  
|            | 4. Enter the Port number (1-65535) on which the agent will listen for user mapping requests. This value must match the value configured on the User-ID agent. By default, the port is set to 5007 on the firewall and on newer versions of the User-ID agent. However, some older User-ID agent versions use port 2010 as the default.  
|            | 5. Make sure that the configuration is Enabled, then click OK.  
|            | 6. Commit the changes.  
|            | 7. Verify that the Connected status displays as connected (a green light). |
Step 8  Verify that the User-ID agent is successfully mapping IP addresses to usernames and that the firewalls can connect to the agent.

1. Launch the User-ID agent and select **User Identification**.
2. Verify that the agent status shows **Agent is running**. If the Agent is not running, click **Start**.
3. To verify that the User-ID agent can connect to monitored servers, make sure the Status for each Server is **Connected**.
4. To verify that the firewalls can connect to the User-ID agent, make sure the Status for each of the Connected Devices is **Connected**.
5. To verify that the User-ID agent is mapping IP addresses to usernames, select **Monitoring** and make sure that the mapping table is populated. You can also **Search** for specific users, or **Delete** user mappings from the list.
Configure User Mapping Using the PAN-OS Integrated User-ID Agent

The following procedure shows 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 with the exception of NetBIOS client probing (WMI probing is supported).

<table>
<thead>
<tr>
<th>Map IP Addresses to Users Using the Integrated User-ID Agent</th>
<th>Create a Dedicated Service Account for the User-ID Agent.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Create an Active Directory service account for the User-ID agent to access the services and hosts it will monitor for collecting user mapping information.</td>
<td></td>
</tr>
</tbody>
</table>
| **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 it can monitor the Security log files on all servers that contain login events. | 1. Select Device > User Identification > User Mapping.  
2. Click Add in the Server Monitoring section.  
3. Enter a Name to identify the server.  
4. Select the Type of server.  
5. Enter the Network Address (an FQDN or IP address) of the server.  
6. Make sure the server profile is Enabled and click OK.  
7. (Optional) Click Discover if you want 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.  
8. (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 query load is high, the observed delay between queries might significantly exceed the specified frequency.  
   a. Edit the Palo Alto Networks User ID Agent Setup.  
   b. Select the Server Monitor tab and specify the Server Log Monitor Frequency in seconds (default is 2, range is 1-3600). Increase the value in this field to 5 seconds in environments with older domain controllers or high-latency links. Ensure that the Enable Session 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 NACs.  
   c. Click OK to save the changes. |
### Map IP Addresses to Users Using the Integrated User-ID Agent (Continued)

**Step 3** Specify the subnetworks 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, to 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 mapping on the subnetworks where users internal to your organization are logging in.

2. Add an entry to the Include/Exclude Networks and enter a Name for the entry and make sure to keep the Enabled check box selected.
3. Enter the Network Address and then select whether to include or exclude it:
   - **Include**—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**—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 subnetworks for exclusion without adding any for inclusion, the agent will not perform user mapping in any subnetwork.

4. Click OK.

**Step 4** Set the domain credentials for the account 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 WMI Authentication tab and enter the User Name and Password for the account that the User-ID agent will use to probe the clients and monitor servers. Enter the username using the domain\username syntax.

**Step 5** *(Optional, not recommended)* Configure WMI probing (the PAN-OS integrated User-ID agent does not support NetBIOS 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. Select the Client Probing tab and select the Enable Probing check box.
2. *(Optional)* Modify the Probe Interval (in minutes) if necessary to ensure it is long enough for the User-ID agent to probe all the learned IP addresses (default is 20, range is 1-1440). This is the interval between the end of the last probe request and the start of the next request.
   - 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.
Configure User-ID to Receive User Mappings from a Syslog Sender

To obtain IP address-to-username mappings from existing network services that authenticate users, you can configure the PAN-OS integrated User-ID agent or Windows-based User-ID agent to parse Syslog messages from those services.

▲ Configure the Integrated User-ID Agent as a Syslog Listener
▲ Configure the Windows User-ID Agent as a Syslog Listener

Configure the Integrated User-ID Agent as a Syslog Listener

To configure the PAN-OS Integrated User-ID agent to create new user mappings based on syslog monitoring, start by defining Syslog Parse profiles. The User-ID agent uses the profiles to find login events in syslog messages. In environments where syslog senders (the network services that authenticate users) deliver syslog messages in different formats, configure a profile for each syslog format. Syslog messages must meet certain criteria for a User-ID agent to parse them (see Syslog). This procedure uses examples with the following format:

Source:192.168.3.212

After configuring the Syslog Parse profiles, you specify syslog senders for the User-ID agent to monitor.
The PAN-OS integrated User-ID agent accepts sylogs over SSL and UDP only. However, you must use caution when using UDP to receive syslog messages because it is an unreliable protocol and as such there is no way to verify that a message was sent from a trusted syslog server. Although you can restrict syslog messages to specific source IP addresses, an attacker can still spoof the IP address, potentially allowing the injection of unauthorized syslog messages into the firewall. As a best practice, always use SSL to listen for syslog messages. However, if you must use UDP, make sure that the syslog server and client are both on a dedicated, secure VLAN to prevent untrusted hosts from sending UDP traffic to the firewall.

<table>
<thead>
<tr>
<th>Collect User Mappings from Syslog Senders</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Determine whether there is a predefined Syslog Parse profile for your particular syslog senders. Palo Alto Networks provides several predefined profiles through Application content updates. The predefined profiles are global to the firewall, whereas custom profiles apply to a single virtual system only. Any new Syslog Parse profiles in a given content release is documented in the corresponding release note along with the specific regex used to define the filter.</td>
</tr>
<tr>
<td><strong>Step 2</strong> Define custom Syslog Parse profiles to extract IP address-to-username mapping information from syslog messages.</td>
</tr>
</tbody>
</table>

| 1. Install the latest Applications or Applications and Threats update:  
  a. Select **Device > Dynamic Updates** and **Check Now**.  
  b. **Download** and **Install** any new update.  |
|---|
| 2. Determine which predefined Syslog Parse profiles are available:  
  a. Select **Device > User Identification > User Mapping** and click **Add** in the Server Monitoring section.  
  b. Set the **Type** to **Syslog Sender** and click **Add** in the Filter section. If the Syslog Parse profile you need is available, skip the steps for defining custom profiles.  |
| 1. Review the syslog messages that the syslog sender generates to identify the syntax for successful login events. This enables you to define the matching patterns when creating Syslog Parse profiles.  
  While reviewing syslog messages, also determine whether they include the domain name. If they don’t, and your user mappings require domain names, enter the **Default Domain Name** when defining the syslog senders that the User-ID agent monitors (later in this procedure).  |
| 2. Select **Device > User Identification > User Mapping** and edit the Palo Alto Networks User-ID Agent Setup.  
  3. Select **Syslog Filters** and **Add** a Syslog Parse profile.  
  4. Enter a name to identify the **Syslog Parse Profile**.  
  5. Specify the **Type** of parsing to extract user mapping information:  
    - **Regex Identifier**—Regular expressions.  
    - **Field Identifier**—Text strings.  
  The following steps describe how to configure these parsing types. |
Collect User Mappings from Syslog Senders (Continued)

Step 3  (Regex Identifier parsing only) Define the regex matching patterns.

If the syslog message contains a standalone space or tab as a delimiter, use \s for a space and \t for a tab.

1. Enter the Event Regex for the type of events you want to find. For the example message, the regex (authentication\nsuccess){1} extracts the first \{1\} instance of the string authentication success. The backslash (\) before the space is a standard regex escape character that instructs the regex engine not to treat the space as a special character.

2. Enter the Username Regex to identify the start of the username. In the example message, the regex User:([a-zA-Z0-9\._\-]+) matches the string User:johndoe1 and identifies johndoe1 as the username.

3. Enter the Address Regex to identify the IP address portion of syslog messages. In the example message, the regular expression Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}) matches the IPv4 address Source:192.168.3.212.

The following is an example of a completed Syslog Parse profile that uses regex:

4. Click OK twice to save the profile.
Map IP Addresses to Users

Collect User Mappings from Syslog Senders  (Continued)

**Step 4** *(Field Identifier parsing only) Define string matching patterns.*

1. Enter an **Event String** to identify successful login events. For the example message, the string `authentication success` identifies login events.

2. Enter a **Username Prefix** to identify the start of the username field in syslog messages. The field does not support regex expressions such as `\s` (for a space) or `\t` (for a tab). In the example messages, `User:` identifies the start of the username field.

3. Enter the **Username Delimiter** that indicates the end of the username field in syslog messages. Use `\s` to indicate a standalone space (as in the sample message) and `\t` to indicate a tab.

4. Enter an **Address Prefix** to identify the start of the IP address field in syslog messages. The field does not support regex expressions such as `\s` (for a space) or `\t` (for a tab). In the example messages, `Source:` identifies the start of the address field.

5. Enter the **Address Delimiter** that indicates the end of the IP address field in syslog messages. For example, enter `\n` to indicate the delimiter is a line break.

The following is an example of a completed Syslog Parse profile that uses string matching:

![Syslog Parse Profile](image)

6. Click **OK** twice to save the profile.
### Collect User Mappings from Syslog Senders (Continued)

**Step 5** Specify the syslog senders that the firewall monitors.

Within the total maximum of 100 monitored servers per firewall, you can define no more than 50 syslog senders for any single virtual system. The firewall discards any syslog messages received from senders that are not on this list.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Select <strong>Device &gt; User Identification &gt; User Mapping</strong> and Add an entry to the Server Monitoring list.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter a <strong>Name</strong> to identify the sender.</td>
</tr>
<tr>
<td>3.</td>
<td>Make sure the sender profile is <strong>Enabled</strong> (default is enabled).</td>
</tr>
<tr>
<td>4.</td>
<td>Set the <strong>Type</strong> to <strong>Syslog Sender</strong>.</td>
</tr>
<tr>
<td>5.</td>
<td>Enter the <strong>Network Address</strong> of the syslog sender (IP address or FQDN).</td>
</tr>
<tr>
<td>6.</td>
<td>Select a custom or predefined Syslog Parse profile as a <strong>Filter</strong>.</td>
</tr>
<tr>
<td>7.</td>
<td>Select <strong>UDP</strong> or <strong>SSL</strong> (default) as the <strong>Connection Type</strong>.</td>
</tr>
</tbody>
</table>

**WARNING** Use caution when using UDP to receive syslog messages because it is an unreliable protocol and as such there is no way to verify that a message was sent from a trusted syslog server. Although you can restrict syslog messages to specific source IP addresses, an attacker can still spoof the IP address, potentially allowing the injection of unauthorized syslog messages into the firewall. As a best practice, always use SSL to listen for syslog messages when using agentless User Mapping on a firewall. However, if you must use UDP, make sure that the syslog server and client are both on a dedicated, secure VLAN to prevent untrusted hosts from sending UDP traffic to the firewall. A syslog server using SSL to connect will show a Status of Connected only when there is an active SSL connection. Syslog servers using UDP will not show a Status value.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td><em>(Optional)</em> If the syslog messages don't contain domain information and your user mappings require domain names, enter a <strong>Default Domain Name</strong> to append to the mappings.</td>
</tr>
<tr>
<td>9.</td>
<td>Click <strong>OK</strong> to save the settings.</td>
</tr>
</tbody>
</table>
### Collect User Mappings from Syslog Senders (Continued)

**Step 6** Enable syslog listener services in the management profile associated with the interface used for user mapping.

1. Select **Network > Network Profiles > Interface Mgmt** and edit an existing Interface Management profile or **Add** a new profile.
2. Select **User-ID Syslog Listener-SSL** or **User-ID Syslog Listener-UDP** or both, based on the protocols you defined for the syslog senders in the Server Monitoring list.
   - The listening ports (514 for UDP and 6514 for SSL) are not configurable; they are enabled through the management service only.
3. Click **OK** to save the interface management profile.
   - Even after enabling the User-ID Syslog Listener service on the interface, the interface only accepts syslog connections from senders that have a corresponding entry in the User-ID monitored servers configuration. The firewall discards connections or messages from senders that are not on the list.
4. Assign the Interface Management profile to the interface that the firewall uses to collect user mappings:
   a. Select **Network > Interfaces** and edit the interface.
   b. Select **Advanced > Other info**, select the Interface Management Profile you just added, and click **OK**.
5. **Commit** your changes.
Configure the Windows User-ID Agent as a Syslog Listener

To configure the Windows-based User-ID agent to create new user mappings based on syslog monitoring, start by defining Syslog Parse profiles. The User-ID agent uses the profiles to find login events in syslog messages. In environments where syslog senders (the network services that authenticate users) deliver syslog messages in different formats, configure a profile for each syslog format. Syslog messages must meet certain criteria for a User-ID agent to parse them (see Syslog). This procedure uses examples with the following format:


After configuring the Syslog Parse profiles, you specify syslog senders for the User-ID agent to monitor.
Map IP Addresses to Users

The Windows User-ID agent accepts syslogs over TCP and UDP only. However, you must use caution when using UDP to receive syslog messages because it is an unreliable protocol and as such there is no way to verify that a message was sent from a trusted syslog server. Although you can restrict syslog messages to specific source IP addresses, an attacker can still spoof the IP address, potentially allowing the injection of unauthorized syslog messages into the firewall. As a best practice, use TCP instead of UDP. In either case, make sure that the syslog server and client are both on a dedicated, secure VLAN to prevent untrusted hosts from sending syslogs to the User-ID agent.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Define custom Syslog Parse profiles to filter syslog messages for successful login events. &lt;br&gt;While reviewing syslog messages, determine whether they include the domain name. If they don’t, and your user mappings require domain names, enter the Default Domain Name when defining the syslog senders that the User-ID agent monitors (later in this procedure).</td>
</tr>
<tr>
<td>2.</td>
<td>Open the Windows Start menu and select User-ID Agent.</td>
</tr>
<tr>
<td>3.</td>
<td>Select User Identification &gt; Setup and Edit the Setup.</td>
</tr>
<tr>
<td>4.</td>
<td>Select Systlog, Enable Syslog Service, and Add a Syslog Parse profile.</td>
</tr>
<tr>
<td>5.</td>
<td>Enter a Profile Name and Description.</td>
</tr>
<tr>
<td>6.</td>
<td>Select the Type of parsing to find login events in syslog messages: &lt;br&gt;• Regex—Regular expressions. &lt;br&gt;• Field—Text strings. &lt;br&gt;The following steps describe how to configure these parsing types.</td>
</tr>
</tbody>
</table>
Step 2  (Regex parsing only) Define the regex matching patterns.
If the syslog message contains a standalone space or tab as a delimiter, use \s for a space and \t for a tab.

1. Enter the **Event Regex** to identify successful login events.
   For the example message, the regex `(authentication\nsuccess){1}` extracts the first \{1\} instance of the string authentication success. The backslash before the space is a standard regex escape character that instructs the regex engine not to treat the space as a special character.

2. Enter the **Username Regex** to identify the start of the username.
   In the example message, the regex
   ```regex
   User:([a-zA-Z0-9\.\._\+]+)  
   ```
   matches the string
   ```regex
   User:johndoe1  
   ```
   and identifies johndoe1 as the username.
   If you want to override the current domain in the username of your syslog message or prepend the domain to the username if your syslog message doesn’t contain a domain, enter a **Default Domain Name** when defining the monitored server entry in Step 5.

3. Enter the **Address Regex** to identify the IP address portion of syslog messages.
   In the example message, the regular expression
   ```regex
   Source:\([0-9]{1,3}\\.\[0-9]{1,3}\\.\[0-9]{1,3}\\.\[0-9]{1,3}\)  
   ```
   matches the IPv4 address Source:192.168.3.212.
   The following is an example of a completed Syslog Parse profile that uses regex to identify login events:

4. Click **OK** twice to save the profile.
Configure the Windows User-ID Agent to Collect User Mappings from Syslog Senders (Continued)

<table>
<thead>
<tr>
<th>Step 3</th>
<th>(Field Identifier parsing only) Define string matching patterns.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter an <strong>Event String</strong> to identify successful login events. For the example message, the string <code>authentication success</code> identifies login events.</td>
</tr>
<tr>
<td>2.</td>
<td>Enter a <strong>Username Prefix</strong> to identify the start of the username field in syslog messages. The field does not support regex expressions such as \s (for a space) or \t (for a tab). In the example messages, <code>User:</code> identifies the start of the username field.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter the <strong>Username Delimiter</strong> that indicates the end of the username field in syslog messages. Use \s to indicate a standalone space (as in the sample message) and \t to indicate a tab.</td>
</tr>
<tr>
<td>4.</td>
<td>Enter an <strong>Address Prefix</strong> to identify the start of the IP address field in syslog messages. The field does not support regex expressions such as \s (for a space) or \t (for a tab). In the example messages, <code>Source:</code> identifies the start of the address field.</td>
</tr>
<tr>
<td>5.</td>
<td>Enter the <strong>Address Delimiter</strong> that indicates the end of the IP address field in syslog messages. For example, enter \n to indicate the delimiter is a line break. The following is an example of a completed Syslog Parse profile that uses string matching to identify login events:</td>
</tr>
</tbody>
</table>

![Profile Name: Successful Login, Description: Filter for successful login events, Type: @Field, Event String: authentication success, Username Prefix: User:, Username Delimiter: \s, Address Prefix: Source:, Address Delimiter: \n]  

6. Click **OK** twice to save the profile.
Configure the Windows User-ID Agent to Collect User Mappings from Syslog Senders  (Continued)

Step 4  Specify the syslog senders that the User-ID agent monitors.
Within the total maximum of 100 servers of all types that the User-ID agent can monitor, up to 50 can be syslog senders. The User-ID agent discards any syslog messages received from senders that are not on this list.

1. Select User Identification > Discovery and Add an entry to the Servers list.
2. Enter a Name to identify the sender.
3. Enter the Server Address of the syslog sender (IP address or FQDN).
4. Set the Server Type to Syslog Sender.
5. (Optional) If the syslog messages don't contain domain information and your user mappings require domain names, enter a Default Domain Name to append to the mappings.
6. Select the Syslog Parse profile you configured as a Filter.
7. Click OK to save the settings.
8. Commit your changes to the User-ID agent configuration.

Step 5  Verify the configuration by logging in to the firewall CLI and running the following commands:

To see the status of a particular syslog sender:

```
admin@PA-5050> show user server-monitor state Syslog2
UDP Syslog Listener Service is enabled
SSL Syslog Listener Service is enabled
Proxy: Syslog2(vsys: vsys1) Host: Syslog2(10.5.204.41)
   number of log messages            : 1000
   number of auth. success messages  : 1000
   number of active connections      : 0
   total connections made            : 4
```

To see how many log messages came in from syslog senders and how many entries were successfully mapped:

```
admin@PA-5050> show user server-monitor statistics
Directory Servers:
Name     TYPE     Host            Vsys    Status
--        ----     ------            ----    ------
AD        AD       10.2.204.43     vsys1   Connected

Syslog Servers:
Name                      Connection Host    Vsys    Status
-------------------------        ----------    ----    ------
Syslog1                       UDP        10.5.204.40     vsys1   N/A
Syslog2                    SSL        10.5.204.41     vsys1   Not connected
```

To see how many user mappings were discovered through syslog senders:

```
admin@PA-5050> show user ip-user-mapping all type SYSLOG
IP             Vsys     From    User                        IdleTimeout(s) M
--------------- ------     ------- -------------------------------- -------------- -
192.168.3.8   vsys1    SYSLOG  acme\jreddick               2476           2
476
192.168.5.39  vsys1    SYSLOG  acme\jdonaldson              2480           2
480
192.168.2.147 vsys1    SYSLOG  acme\ccrisp                  2476           2
476
192.168.2.175 vsys1    SYSLOG  acme\jjaso                   2476           2
476
192.168.4.196 vsys1    SYSLOG  acme\jblevins                2480           2
480
192.168.4.103 vsys1    SYSLOG  acme\bmoss                   2480           2
480
192.168.2.193 vsys1    SYSLOG  acme\esogard                 2476           2
476
192.168.2.119 vsys1    SYSLOG  acme\acallaspo               2476           2
476
192.168.3.176 vsys1    SYSLOG  acme\jlowrie                  2478           2
478
Total: 9 users
Map IP Addresses to Usernames Using Captive Portal

If the firewall receives a request from a security zone that has User-ID enabled and the source IP address does not have any user data associated with it yet, the firewall checks its Captive Portal policy rules for a match to determine whether to perform authentication. This is useful in environments where you have clients that are not logged in to your domain servers, such as Linux clients. The firewall triggers this user mapping method only for web traffic (HTTP or HTTPS) that matches a Captive Portal rule but has not been mapped using a different method.

- **Captive Portal Authentication Methods**
- **Captive Portal Modes**
- **Configure Captive Portal**

**Captive Portal Authentication Methods**

Captive Portal uses the following methods to obtain user information from the client when a web request matches a Captive Portal rule:

<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Description</th>
</tr>
</thead>
</table>
| Kerberos SSO                 | The firewall uses Kerberos single sign-on (SSO) to transparently obtain user credentials. To use this method, your network requires a Kerberos infrastructure, including a key distribution center (KDC) with an authentication server and ticket granting service. The firewall must have a Kerberos account, including a principal name and password.  
As a best practice, choose Kerberos transparent authentication over NTLM authentication. Kerberos is a stronger, more robust authentication method than NTLM and it does not require the firewall to have an administrative account to join the domain.  
If Kerberos SSO authentication fails, the firewall falls back to NT LAN Manager (NTLM) authentication. If you don’t configure NTLM, or NTLM authentication fails, the firewall falls back to web form or client certificate authentication, depending on your Captive Portal configuration. |
| NT LAN Manager (NTLM)        | The firewall uses an encrypted challenge-response mechanism to obtain the user credentials from the browser. When configured properly, the browser will transparently provide the credentials to the firewall without prompting the user, but will prompt for credentials if necessary.  
If you use the Windows-based User-ID agent, NTLM responses go directly to the domain controller where you installed the agent.  
If you configure Kerberos SSO authentication, the firewall tries that method first before falling back to NTLM authentication. If the browser can’t perform NTLM or if NTLM authentication fails, the firewall falls back to web form or client certificate authentication, depending on your Captive Portal configuration.  
Microsoft Internet Explorer supports NTLM by default. You can configure Mozilla Firefox and Google Chrome to also use NTLM but you can’t use NTLM to authenticate non-Windows clients. |
<table>
<thead>
<tr>
<th>Authentication Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Form</td>
<td>The firewall redirects web requests to a web form for authentication. You can configure Captive Portal to use a local user database, RADIUS server, TACACS+ server, LDAP server, or Kerberos server to authenticate users (or an authentication sequence). Although the firewall always prompts users for credentials, this method works with all browsers and operating systems.</td>
</tr>
<tr>
<td>Client Certificate Authentication</td>
<td>The firewall prompts the browser to present a valid client certificate to authenticate the user. To use this method, you must provision client certificates on each user system and install the trusted certificate authority (CA) certificate used to issue those certificates on the firewall.</td>
</tr>
</tbody>
</table>
Captive Portal Modes

The Captive Portal mode defines how the firewall captures web requests for authentication:

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparent</td>
<td>The firewall intercepts the browser traffic per the Captive Portal rule and impersonates the original destination URL, issuing an HTTP 401 to invoke authentication. However, because the firewall does not have the real certificate for the destination URL, the browser displays a certificate error to users attempting to access a secure site. Therefore, you should only use this mode when absolutely necessary, such as in Layer 2 or virtual wire deployments.</td>
</tr>
<tr>
<td>Redirect</td>
<td>The firewall intercepts unknown HTTP or HTTPS sessions and redirects them to a Layer 3 interface on the firewall using an HTTP 302 redirect to perform authentication. This is the preferred mode because it provides a better end-user experience (no certificate errors). However, it does require additional Layer 3 configuration. Another benefit of the Redirect mode is that it provides for the use of session cookies, which enable the user to continue browsing to authenticated sites without requiring re-mapping each time the time outs expire. This is especially useful for users who roam from one IP address to another (for example, from the corporate LAN to the wireless network) because they won’t need to re-authenticate when the IP address changes as long as the session stays open. If you use Kerberos SSO or NTLM authentication, you must use Redirect mode because the browser will provide credentials only to trusted sites.</td>
</tr>
</tbody>
</table>
Configure Captive Portal

The following procedure shows how to configure Captive Portal using the PAN-OS integrated User-ID agent to redirect web requests that match a Captive Portal rule to a redirect host. A redirect host is the intranet hostname (a hostname with no period in its name) that resolves to the IP address of the Layer 3 interface on the firewall to which the firewall will redirect requests.

If you use Captive Portal without the other User-ID functions (user mapping and group mapping), you don't need to configure a User-ID agent.

### Configure Captive Portal Using the PAN-OS Integrated User-ID Agent

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Configure the interfaces that the firewall will use for redirecting web requests, authenticating users, and communicating with directory servers to map usernames to IP addresses. The firewall uses the management (MGT) interface for all these functions by default, but you can configure other interfaces. In redirect mode, you must use a Layer 3 interface for redirecting requests.</th>
</tr>
</thead>
</table>
| **Step 1** | **1. (MGT interface only)** Select Device > Setup > Management, edit the Management Interface Settings, select the User-ID check box, and click OK.  
**2. (Non-MGT interface only)** Assign an Interface Management profile to the Layer 3 interface that the firewall will use to redirect web requests and communicate with directory servers. You must enable Response Pages and User-ID in the Interface Management profile.  
**3. (Non-MGT interface only)** Configure a service route for the interface that the firewall will use to authenticate users. If the firewall has more than one virtual system (vsys), the service route can be global or vsys-specific. The services must include LDAP and potentially the following:  
- **Kerberos, RADIUS, or TACACS+**—Configure a service route for one of these services only if you will use it for external authentication.  
- **UID Agent**—Configure this service only if you will enable NT LAN Manager (NTLM) authentication or if you will enable User- and Group-Based Policy.  
**4. (Redirect mode only)** Create a DNS address (A) record that maps the IP address on the Layer 3 interface to the redirect host. If you will use Kerberos SSO, you must also add a DNS pointer (PTR) record that performs the same mapping. If your network doesn't support access to the directory servers from any firewall interface, you must Configure User Mapping Using the Windows User-ID Agent. |
| Step 2 | Make sure Domain Name System (DNS) is configured to resolve your domain controller addresses.  
To verify proper resolution, ping the server FQDN. For example:  
admin@PA-200> ping host dc1.acme.com |
| Step 3 | Create a Kerberos keytab for the redirect host.  
Required for Kerberos SSO authentication.  
Create a Kerberos keytab. A keytab is a file that contains Kerberos account information (principal name and hashed password) for the redirect host (the firewall).  
To support Kerberos SSO, your network must have a Kerberos infrastructure, including a key distribution center (KDC) with an authentication server and ticket granting service. |
### Configure Captive Portal Using the PAN-OS Integrated User-ID Agent (Continued)

#### Step 4
Configure clients to trust Captive Portal certificates.
Required for redirect mode—to transparently redirect users without displaying certificate errors. You can generate a self-signed certificate or import a certificate that an external certificate authority (CA) signed.

To use a self-signed certificate, create a root CA certificate and use it to sign the certificate you will use for Captive Portal:

1. Select **Device > Certificate Management > Certificates > Device Certificates**.
2. Create a Self-Signed Root CA Certificate or import a CA certificate (see Import a Certificate and Private Key).
3. Generate a Certificate to use for Captive Portal. Be sure to configure the following fields:
   - **Common Name**—Enter the DNS name of the intranet host for the Layer 3 interface.
   - **Signed By**—Select the CA certificate you just created or imported.
   - **Certificate Attributes**—Click **Add**, for the **Type** select **IP**, and, for the **Value**, enter the IP address of the Layer 3 interface to which the firewall will redirect requests.
4. Configure an SSL/TLS Service Profile. Assign the Captive Portal certificate you just created to the profile.
5. Configure clients to trust the certificate:
   a. Export the CA certificate you created or imported.
   b. Import the certificate as a trusted root CA into all client browsers, either by manually configuring the browser or by adding the certificate to the trusted roots in an Active Directory (AD) Group Policy Object (GPO).

#### Step 5
Configure an authentication server profile.
Required for external authentication. If you enable Kerberos SSO or NTLM authentication, the firewall uses the external service only if those methods fail.

As a best practice, choose Kerberos transparent authentication over NTLM authentication. Kerberos is a stronger, more robust authentication method than NTLM and it does not require the firewall to have an administrative account to join the domain.

- Configure a RADIUS Server Profile.
- Configure a TACACS+ Server Profile
- Configure an LDAP Server Profile
- Configure a Kerberos Server Profile

The PAN-OS web server timeout (default is 3 seconds) must be the same as or greater than the server profile timeout multiplied by the number of servers in the profile. For RADIUS and TACACS+, the default server profile timeout is 3 seconds. For LDAP, the timeout is the total of the **Bind Timeout** (default is 30 seconds) and **Search Timeout** (default is 30 seconds) for each server. For Kerberos, the non-configurable timeout can take up to 17 seconds for each server. Also, the Captive Portal session timeout (default is 30 seconds) must be greater than the web server timeout.

To change the web server timeout, enter the following firewall CLI command, where `<value>` is 3-30 seconds: `set deviceconfig setting l3-service timeout <value>`. To change the Captive Portal session timeout, select **Device > Setup > Session**, edit the Session Timeouts, and enter a new **Captive Portal** value in seconds (range is 1-1,599,999).

Keep in mind that the more you raise the web server and Captive Portal session timeouts, the slower Captive Portal will respond to users.
## Configure Captive Portal Using the PAN-OS Integrated User-ID Agent (Continued)

### Step 6  Add an authentication profile

The profile defines the authentication methods to use (Kerberos SSO, external service, or local database) when a Captive Portal rule invokes Web Form authentication. Even if you enable NTLM, you must define a secondary authentication method in case NTLM authentication fails or the User-ID agent doesn't support NTLM.

If you set the authentication **Type** to RADIUS, specify a RADIUS **User Domain** in case users don’t enter the domain at login.

### Step 7 (Optional) Configure Client Certificate Authentication.

You don’t need an authentication profile or sequence for client certificate authentication. If you configure both an authentication profile/sequence and certificate authentication, users must authenticate using both.

### Step 8 (Optional) Enable NT LAN Manager (NTLM) authentication.

As a best practice, choose Kerberos transparent authentication over NTLM authentication. Kerberos is a stronger, more robust authentication method than NTLM and it does not require the firewall to have an administrative account to join the domain. If you do configure NTLM, the PAN-OS integrated User-ID agent must be able to successfully resolve the DNS name of your domain controller to join the domain.

### Configure an authentication profile:

1. **If** the authentication **Type** is an external service (RADIUS, TACACS+, LDAP, or Kerberos), select the authentication **Server Profile** you created.
2. **If** you use Kerberos SSO, enter the **Kerberos Realm** (usually the DNS domain of the users, except that the realm is uppercase), and import the **Kerberos Keytab** you created.
3. **Select** Advanced and Add the users and user groups that can authenticate using this profile. If the authentication **Type** is **Local Database**, add the Captive Portal users or user groups you created. You can select all to allow every user to authenticate. After completing the **Allow List**, click **OK**.

If your users are in multiple domains or Kerberos realms, you can create an authentication profile for each domain or realm, assign all the profiles to the authentication sequence, and assign the sequence to the Captive Portal configuration.

### Step 7 (Optional) Configure Client Certificate Authentication.

1. Use a root CA certificate to generate a client certificate for each user who will authenticate to Captive Portal. The CA in this case is usually your enterprise CA, not the firewall.
2. **Export the CA certificate** in PEM format to a system that the firewall can access.
3. **Import the CA certificate** onto the firewall: see Import a Certificate and Private Key. After the import, click the imported certificate, select **Trusted Root CA**, and click **OK**.
4. **Configure a Certificate Profile.**
   - In the **Username Field** drop-down, select the certificate field that contains the user identity information.
   - In the **CA Certificates** list, click **Add** and select the CA certificate you just imported.

### Step 8 (Optional) Enable NT LAN Manager (NTLM) authentication.

1. **If** you haven’t already done so, Create a Dedicated Service Account for the User-ID Agent.
2. Select **Device > User Identification > User Mapping** and edit the Palo Alto Networks User ID Agent Setup section.
3. On the **NTLM** tab, select the **Enable NTLM authentication processing** check box.
4. Enter the **NTLM Domain** against which the User-ID agent on the firewall will check NTLM credentials.
5. In the **Admin User Name**, **Password**, and **Confirm Password** fields, enter the username and password of the Active Directory account you created for the User-ID agent.
   - Do not include the domain in the **Admin User Name** field. Otherwise, the firewall will fail to join the domain.
   - Palo Alto Networks recommends that you use a User-ID agent account that is separate from your firewall administrator account.
6. Click **OK**.
Configure User Mapping for Terminal Server Users

Individual terminal server users appear to have the same IP address and therefore an IP address-to-username mapping is not sufficient to identify a specific user. To enable identification of specific users on Windows-based terminal servers, the Palo Alto Networks Terminal Services agent (TS agent) allocates a port range to each user. It then notifies every connected firewall about the allocated port range, which allows the firewall to create an IP address-port-user mapping table and enable user- and group-based security policy enforcement. For non-Windows terminal servers, you can configure the PAN-OS XML API to extract user mapping information.

The following sections describe how to configure user mapping for terminal server users:

1. Configure the Palo Alto Networks Terminal Services Agent for User Mapping
2. Retrieve User Mappings from a Terminal Server Using the PAN-OS XML API

Configure the Palo Alto Networks Terminal Services Agent for User Mapping

Use the following procedure to install and configure the TS agent on the terminal server. To map all your users, you must install the TS agent on all terminal servers that your users log in to.

For information about the supported terminal servers supported by the TS Agent, refer to “Operating System (OS) Compatibility TS Agent” in the Terminal Services Agent Release Notes.
# User-ID

## Map IP Addresses to Users

### Configure the Palo Alto Networks Terminal Services Agent for User Mapping

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Download the TS agent installer.</th>
<th>1. Log in to the <a href="https://www.paloaltonetworks.com/support">Palo Alto Networks Customer Support web site</a>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2. Select <a href="https://www.paloaltonetworks.com/support">Software Updates</a> from the Manage Devices section.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Scroll to the <a href="https://www.paloaltonetworks.com/support">Terminal Services Agent</a> section and <strong>Download</strong> the version of the agent you want to install.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Save the <code>TaInstall64.x64-x.x-x.x.x.x.msi</code> or <code>TaInstall-x.x.x-xx.msi</code> file (be sure to select the appropriate version based on whether the Windows system is running a 32-bit OS or a 64-bit OS) on the systems where you plan to install the agent.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 2</th>
<th>Run the installer as an administrator.</th>
<th>1. Open the Windows <strong>Start</strong> menu, right-click the <a href="https://www.paloaltonetworks.com/support">Command Prompt</a> program, and select <strong>Run as administrator</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2. From the command line, run the .msi file you downloaded. For example, if you saved the .msi file to the Desktop you would enter the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>```</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C:\Users\administrator.acme&gt;cd Desktop</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C:\Users\administrator.acme\Desktop&gt;TaInstall-6.0.0-1.msi</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Follow the setup prompts to install the agent using the default settings. By default, the agent gets installed to the <code>C:\Program Files (x86)\Palo Alto Networks\Terminal Server Agent</code> folder, but you can <strong>Browse</strong> to a different location.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. When the installation completes, <strong>Close</strong> the setup window. If you are upgrading to a TS Agent version that has a newer driver than the existing installation, the installation wizard prompts you to reboot the system after upgrading in order to use the new driver.</td>
</tr>
</tbody>
</table>
### Step 3 Define the range of ports for the TS Agent to allocate to end users.

1. Open the Windows **Start** menu and select **Terminal Server Agent** to launch the Terminal Services agent application.
2. Select **Configure** in the side menu.
3. Enter the **Source Port Allocation Range** (default 20000-39999). This is the full range of port numbers that the TS agent will allocate for user mapping. The port range you specify cannot overlap with the **System Source Port Allocation Range**.
4. (Optional) If there are ports/port ranges within the source port allocation that you do not want the TS Agent to allocate to user sessions, specify them as **Reserved Source Ports**. To include multiple ranges, use commas with no spaces, for example: 2000-3000,3500,4000-5000.
5. Specify the number of ports to allocate to each individual user upon login to the terminal server in the **Port Allocation Start Size Per User** field (default 200).
6. Specify the **Port Allocation Maximum Size Per User**, which is the maximum number of ports the Terminal Services agent can allocate to an individual user.
7. Specify whether to continue processing traffic from the user if the user runs out of allocated ports. By default, the **Fail port binding when available ports are used up** is selected, which indicates that the application will fail to send traffic when all ports are used. To enable users to continue using applications when they run out of ports, clear this check box. Keep in mind that this traffic may not be identified with User-ID.

### Step 4 Configure the firewalls to connect to the Terminal Services agent.

Complete the following steps on each firewall you want to connect to the Terminal Services agent to receive user mappings:

1. Select **Device > User Identification > Terminal Server Agents** and click **Add**.
2. Enter a **Name** for the Terminal Services agent.
3. Enter the IP address of the Windows **Host** on which the Terminal Services agent is installed.
   - When you configure a TS agent connection, use a static IP address or an FQDN that resolves to a static IP address for the **Host** and any **Alternative IP Addresses**. DHCP is not supported.
4. Enter the **Port** number on which the agent will listen for user mapping requests. This value must match the value configured on the Terminal Services agent. By default, the port is set to 5009 on the firewall and on the agent. If you change it here, you must also change the **Listening Port** field on the Terminal Services agent **Configure** screen.
5. Make sure that the configuration is **Enabled** and then click **OK**.
6. **Commit** the changes.
7. Verify that the **Connected** status displays as connected (a green light).
Retrieve User Mappings from a Terminal Server Using the PAN-OS XML API

The PAN-OS XML API uses standard HTTP requests to send and receive data. API calls can be made directly from command line utilities such as cURL or using any scripting or application framework that supports RESTful services.

To enable a non-Windows terminal server to send user mapping information directly to the firewall, create scripts that extract the user login and logout events and use them for input to the PAN-OS XML API request format. Then define the mechanisms for submitting the XML API request(s) to the firewall using cURL or wget and providing the firewall’s API key for secure communication. Creating user mappings from multi-user systems such as terminal servers requires use of the following API messages:

- **<multiusersystem>**—Sets up the configuration for an XML API Multi-user System on the firewall. This message allows for definition of the terminal server IP address (this will be the source address for all users on that terminal server). In addition, the `<multiusersystem>` Setup message specifies the range of source port numbers to allocate for user mapping and the number of ports to allocate to each individual user upon login (called the **block size**). If you want to use the default source port allocation range (1025-65534) and block size (200), you do not need to send a `<multiusersystem>` setup event to the firewall. Instead, the firewall will automatically generate the XML API Multi-user System configuration with the default settings upon receipt of the first user login event message.

- **<blockstart>**—Used with the `<login>` and `<logout>` messages to indicate the starting source port number allocated to the user. The firewall then uses the block size to determine the actual range of port numbers to map to the IP address and username in the login message. For example, if the `<blockstart>` value is 13200 and the block size configured for the multi-user system is 300, the actual source port range allocated to the user is 13200 through 13499. Each connection initiated by the user should use a unique source port number within the allocated range, enabling the firewall to identify the user based on its IP address-port-user mappings for enforcement of user- and group-based security rules. When a user exhausts all the ports allocated, the terminal server must send a new `<login>` message allocating a new port range for the user so that the firewall can update the IP address-port-user mapping. In addition, a
single username can have multiple blocks of ports mapped simultaneously. When the firewall receives a <logout> message that includes a <blockstart> parameter, it removes the corresponding IP address-port-user mapping from its mapping table. When the firewall receives a <logout> message with a username and IP address, but no <blockstart>, it removes the user from its table. And, if the firewall receives a <logout> message with an IP address only, it removes the multi-user system and all mappings associated with it.

The XML files that the terminal server sends to the firewall can contain multiple message types and the messages do not need to be in any particular order within the file. However, upon receiving an XML file that contains multiple message types, the firewall will process them in the following order: multiusersystem requests first, followed by logins, then logouts.

The following workflow provides an example of how to use the PAN-OS XML API to send user mappings from a non-Windows terminal server to the firewall.

### Use the PAN-OS XML API to Map Non-Windows Terminal Services Users

**Step 1** Generate the API key that will be used to authenticate the API communication between the firewall and the terminal server. To generate the key you must provide login credentials for an administrative account; the API is available to all administrators (including role-based administrators with XML API privileges enabled).

Any special characters in the password must be URL/percent-encoded.

| Step 1 | Generate the API key that will be used to authenticate the API communication between the firewall and the terminal server. To generate the key you must provide login credentials for an administrative account; the API is available to all administrators (including role-based administrators with XML API privileges enabled). | From a browser, log in to the firewall. Then, to generate the API key for the firewall, open a new browser window and enter the following URL: https://<Firewall-IPaddress>/api/?type=keygen&user=<username>&password=<password>

Where **<Firewall-IPaddress>** is the IP address or FQDN of the firewall and **<username>** and **<password>** are the credentials for the administrative user account on the firewall. For example: https://10.1.2.5/api/?type=keygen&user=admin&password=admin

The firewall responds with a message containing the key, for example:

```xml
<response status="success">
    <result>
        <key>k7J335J6hI7nBxIqyfa62sZugWx7ot%2BgzEA9UOnlZRg=</key>
    </result>
</response>
```
### Use the PAN-OS XML API to Map Non-Windows Terminal Services Users (Continued)

#### Step 2  (Optional) Generate a setup message that the terminal server will send to specify the port range and block size of ports per user that your terminal services agent uses.

If the terminal services agent does not send a setup message, the firewall will automatically create a Terminal Services agent configuration using the following default settings upon receipt of the first login message:

- Default port range: 1025 to 65534
- Per user block size: 200
- Maximum number of multi-user systems: 1,000

The following shows a sample setup message:

```xml
<uid-message>
  <payload>
    <multiusersystem>
      <entry ip="10.1.1.23" startport="20000" endport="39999" blocksize="100">
      </entry>
    </multiusersystem>
  </payload>
  <type>update</type>
  <version>1.0</version>
</uid-message>
```

Where `entry` specifies the IP address assigned to terminal server users, `startport` and `endport` specify the port range to use when assigning ports to individual users, and `blocksize` specifies the number of ports to assign to each user. The maximum blocksize is 4000 and each multi-user system can allocate a maximum of 1000 blocks.

If you define a custom blocksize and or port range, keep in mind that you must configure the values such that every port in the range gets allocated and that there are no gaps or unused ports. For example, if you set the port range to 1000–1499, you could set the block size to 100, but not to 200. This is because if you set it to 200, there would be unused ports at the end of the range.

#### Step 3  Create a script that will extract the login events and create the XML input file to send to the firewall.

Make sure the script enforces assignment of port number ranges at fixed boundaries with no port overlaps. For example, if the port range is 1000–1999 and the block size is 200, acceptable blockstart values would be 1000, 1200, 1400, 1600, or 1800. Blockstart values of 1001, 1300, or 1850 would be unacceptable because some of the port numbers in the range would be left unused.

The login event payload that the terminal server sends to the firewall can contain multiple login events.

The following shows the input file format for a PAN-OS XML login event:

```xml
<uid-message>
  <payload>
    <login>
      <entry name="acme\jjaso" ip="10.1.1.23" blockstart="20000">
      </entry>
      <entry name="acme\jparker" ip="10.1.1.23" blockstart="20100">
      </entry>
      <entry name="acme\ccrisp" ip="10.1.1.23" blockstart="21000">
      </entry>
    </login>
  </payload>
  <type>update</type>
  <version>1.0</version>
</uid-message>
```

The firewall uses this information to populate its user mapping table. Based on the mappings extracted from the example above, if the firewall received a packet with a source address and port of 10.1.1.23:20101, it would map the request to user jparker for policy enforcement.

Each multi-user system can allocate a maximum of 1,000 port blocks.
Map IP Addresses to Users

Use the PAN-OS XML API to Map Non-Windows Terminal Services Users (Continued)

Step 4 Create a script that will extract the logout events and create the XML input file to send to the firewall.
Upon receipt of a logout event message with a blockstart parameter, the firewall removes the corresponding IP address-port-user mapping. If the logout message contains a username and IP address, but no blockstart parameter, the firewall removes all mappings for the user. If the logout message contains an IP address only, the firewall removes the multi-user system and all associated mappings.

The following shows the input file format for a PAN-OS XML logout event:

```
<uid-message>
  <payload>
    <logout>
      <entry name="acme\jjaso" ip="10.1.1.23" blockstart="20000">
      <entry name="acme\ccrisp" ip="10.1.1.23">
      <entry ip="10.2.5.4">
    </logout>
  </payload>
  <type>update</type>
  <version>1.0</version>
</uid-message>
```

You can also clear the multiuser system entry from the firewall using the following CLI command: `clear xml-api multiusersystem`

Step 5 Make sure that the scripts you create include a way to dynamically enforce that the port block range allocated using the XML API matches the actual source port assigned to the user on the terminal server and that the mapping is removed when the user logs out or the port allocation changes.

One way to do this would be to use netfilter NAT rules to hide user sessions behind the specific port ranges allocated via the XML API based on the uid. For example, to ensure that a user with the user ID jjaso is mapped to a source network address translation (SNAT) value of 10.1.1.23:20000-20099, the script you create should include the following:

```
[root@ts1 ~]# iptables -t nat -A POSTROUTING -m owner --uid-owner jjaso -p tcp --dport jnat --source 10.1.1.23:20000-20099
```

Similarly, the scripts you create should also ensure that the IP table routing configuration dynamically removes the SNAT mapping when the user logs out or the port allocation changes:

```
[root@ts1 ~]# iptables -t nat -D POSTROUTING 1
```

Step 6 Define how to package the XML input files containing the setup, login, and logout events into wget or cURL messages for transmission to the firewall.

To apply the files to the firewall using wget:

```
> wget --post file <filename>
"https://<Firewall-IPaddress>/api/?type=user-id&key=<key>&file-name=<input_filename.xml>&client=wget&vsys=<VSYS_name>
```

For example, the syntax for sending an input file named login.xml to the firewall at 10.2.5.11 using key k7J335J6hI7nBxIqyfa62s2ugwx7ot%2BgzEA9U0n1ZRg using wget would look as follows:

```
> wget --post file login.xml
"https://10.2.5.11/api/?type=user-id&key=k7J335J6hI7nBxIqyfa62s2ugwx7ot%2BgzEA9U0n1ZRg&file-name=login.xml&client=wget&vsys=vsys1"
```

To apply the file to the firewall using cURL:

```
> curl --form file=@<filename>
https://<Firewall-IPaddress>/api/?type=user-id&key=<key>&vsys=<VSYS_name>
```

For example, the syntax for sending an input file named login.xml to the firewall at 10.2.5.11 using key k7J335J6hI7nBxIqyfa62s2ugwx7ot%2BgzEA9U0n1ZRg using cURL would look as follows:

```
> curl --form file@login.xml
"https://10.2.5.11/api/?type=user-id&key=k7J335J6hI7nBxIqyfa62s2ugwx7ot%2BgzEA9U0n1ZRg&vsys=vsys1"
```
User-ID provides many out-of-the-box methods for obtaining user mapping information. However, you might have applications or devices that capture user information but cannot natively integrate with User-ID. For example, you might have a custom, internally developed application or a device that no standard user mapping method supports. In such cases, you can use the PAN-OS XML API to create custom scripts that send the information to the PAN-OS integrated User-ID agent or directly to the firewall. The PAN-OS XML API uses standard HTTP requests to send and receive data. API calls can be made directly from command line utilities such as cURL or using any scripting or application framework that supports POST and GET requests.

To enable an external system to send user mapping information to the PAN-OS integrated User-ID agent, create scripts that extract user login and logout events and use the events as input to the PAN-OS XML API request. Then define the mechanisms for submitting the XML API requests to the firewall (using cURL, for example) and use the API key of the firewall for secure communication. For more details, refer to the PAN-OS XML API Usage Guide.

### Send User Mappings to User-ID Using the XML API

Verify the configuration by opening an SSH connection to the firewall and then running the following CLI commands:

**To verify if the terminal server is connecting to the firewall over XML:**

```
admin@PA-5050> show user xml-api multiusersystem
Host     Vsys   Users   Blocks
----------------------------------------
10.5.204.43 vsys1 5 2
```

**To verify that the firewall is receiving mappings from a terminal server over XML:**

```
admin@PA-5050> show user ip-port-user-mapping all

Global max host index 1, host hash count 1

XML API Multi-user System 10.5.204.43
Vsys 1, Flag 3
Port range: 20000 - 39999
Port size: start 200; max 2000
Block count 100, port count 20000
20000-20199: acme\administrator

Total host: 1
```
Enable User- and Group-Based Policy

After you Enable User-ID, you will be able to configure Security Policy that applies to specific users and groups. User-based policy controls can also include application information (including which category and subcategory it belongs in, its underlying technology, or what the application characteristics are). You can define policy rules to safely enable applications based on users or groups of users, in either outbound or inbound directions.

Examples of user-based policies include:

- Enable only the IT department to use tools such as SSH, telnet, and FTP on standard ports.
- Allow the Help Desk Services group to use Slack.
- Allow all users to read Facebook, but block the use of Facebook apps, and restrict posting to employees in marketing.
Enable Policy for Users with Multiple Accounts

If a user in your organization has multiple responsibilities, that user might have multiple usernames (accounts), each with distinct privileges for accessing a particular set of services, but with all the usernames sharing the same IP address (the client system of the user). However, the User-ID agent can map any one IP address (or IP address and port range for terminal server users) to only one username for enforcing policy, and you can't predict which username the agent will map. To control access for all the usernames of a user, you must make adjustments to the rules, user groups, and User-ID agent.

For example, say the firewall has a rule that allows username corp_user to access email and a rule that allows username admin_user to access a MySQL server. The user logs in with either username from the same client IP address. If the User-ID agent maps the IP address to corp_user, then whether the user logs in as corp_user or admin_user, the firewall identifies that user as corp_user and allows access to email but not the MySQL server. On the other hand, if the User-ID agent maps the IP address to admin_user, the firewall always identifies the user as admin_user regardless of login and allows access to the MySQL server but not email. The following steps describe how to enforce both rules in this example.

### Enable Policy for a User with Multiple Accounts

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>Step 1</strong></td>
<td>Configure a user group for each service that requires distinct access privileges. In this example, each group is for a single service (email or MySQL server). However, it is common to configure each group for a set of services that require the same privileges (for example, one group for all basic user services and one group for all administrative services).</td>
</tr>
<tr>
<td>If your organization already has user groups that can access the services that the user requires, simply add the username that is used for less restricted services to those groups. In this example, the email server requires less restricted access than the MySQL server, and corp_user is the username for accessing email. Therefore, you add corp_user to a group that can access email (corp_employees) and to a group that can access the MySQL server (network_services).</td>
<td></td>
</tr>
<tr>
<td>If adding a username to a particular existing group would violate your organizational practices, you can create a custom group based on an LDAP filter. For this example, say network_services is a custom group, which you configure as follows:</td>
<td></td>
</tr>
<tr>
<td>1. Select Device &gt; User Identification &gt; Group Mapping Settings and Add a group mapping configuration with a unique Name.</td>
<td></td>
</tr>
<tr>
<td>2. Select an LDAP Server Profile and ensure the Enabled check box is enabled.</td>
<td></td>
</tr>
<tr>
<td>3. Select the Custom Group tab and Add a custom group with network_services as a Name.</td>
<td></td>
</tr>
<tr>
<td>4. Specify an LDAP Filter that matches an LDAP attribute of corp_user and click OK.</td>
<td></td>
</tr>
<tr>
<td>5. Click OK and Commit.</td>
<td></td>
</tr>
</tbody>
</table>

Later, if other users that are in the group for less restricted services are given additional usernames that access more restricted services, you can add those usernames to the group for more restricted services. This scenario is more common than the inverse; a user with access to more restricted services usually already has access to less restricted services.
Enable Policy for Users with Multiple Accounts

Step 2 Configure the rules that control user access based on the groups you just configured.

Enable User- and Group-Based Policy:
1. Configure a security rule that allows the corp_employees group to access email.
2. Configure a security rule that allows the network_services group to access the MySQL server.

Step 3 Configure the ignore list of the User-ID agent.
This ensures that the User-ID agent maps the client IP address only to the username that is a member of the groups assigned to the rules you just configured. The ignore list must contain all the usernames of the user that are not members of those groups.

In this example, you add admin_user to the ignore list of the Windows-based User-ID agent to ensure that it maps the client IP address to corp_user. This guarantees that, whether the user logs in as corp_user or admin_user, the firewall identifies the user as corp_user and applies both rules that you configured because corp_user is a member of the groups that the rules reference.

1. Create an `ignore_user_list.txt` file.
2. Open the file and add admin_user. If you later add more usernames, each must be on a separate line.
3. Save the file to the User-ID agent folder on the domain server where the agent is installed.

If you use the PAN-OS integrated User-ID agent, see Configure User Mapping Using the PAN-OS Integrated User-ID Agent for instructions on how to configure the ignore list.

Step 4 Configure endpoint authentication for the restricted services.
This enables the endpoint to verify the credentials of the user and preserves the ability to enable access for users with multiple usernames.

In this example, you have configured a firewall rule that allows corp_user, as a member of the network_services group, to send a service request to the MySQL server. You must now configure the MySQL server to respond to any unauthorized username (such as corp_user) by prompting the user to enter the login credentials of an authorized username (admin_user).

If the user logs in to the network as admin_user, the user can then access the MySQL server without it prompting for the admin_user credentials again.

In this example, both corp_user and admin_user have email accounts, so the email server won’t prompt for additional credentials regardless of which username the user entered when logging in to the network.

The firewall is now ready to enforce rules for a user with multiple usernames.
Verify the User-ID Configuration

After you configure group mapping and user mapping and enable User-ID on your security rules and Captive Portal rules, you should verify that it is working properly.

<table>
<thead>
<tr>
<th>Verify the User-ID Configuration</th>
<th>From the CLI, enter the following operational command:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Verify that group mapping is working.</td>
<td>&gt; show user group-mapping statistics</td>
</tr>
<tr>
<td>Step 2 Verify that user mapping is working.</td>
<td>If you are using the PAN-OS integrated User-ID agent, you can verify this from the CLI using the following command:</td>
</tr>
<tr>
<td></td>
<td>&gt; show user ip-user-mapping-mp all</td>
</tr>
<tr>
<td>IP Vsys From User Timeout (sec)</td>
<td>Vsys From User Timeout (sec)</td>
</tr>
<tr>
<td>192.168.201.1 vsys1 UIA acme\george 210</td>
<td>192.168.201.1 vsys1 UIA acme\duane 210</td>
</tr>
<tr>
<td>192.168.201.11 vsys1 UIA acme\duane 210</td>
<td>192.168.201.10 vsys1 UIA acme\betsy 210</td>
</tr>
<tr>
<td>192.168.201.50 vsys1 UIA acme\betsy 210</td>
<td>192.168.201.100 vsys1 AD acme\administrator 748</td>
</tr>
<tr>
<td>Total: 5 users *: WMI probe succeeded</td>
<td></td>
</tr>
</tbody>
</table>

Step 3 Test your security rule.

- From a machine in the zone where User-ID is enabled, attempt to access sites and applications to test the rules you defined in your policy and ensure that traffic is allowed and denied as expected.
- You can also use the `test security-policy-match` operational command to determine whether the policy is configured correctly. For example, suppose you have a rule that blocks user duane from playing World of Warcraft; you could test the policy as follows:

  ```plaintext
  > test security-policy-match application worldofwarcraft source-user acme\duane source any destination any destination-port any protocol 6
  "deny worldofwarcraft" {
    from corporate;
    source any;
    source-region any;
    to internet;
    destination any;
    destination-region any;
    user acme\duane;
    category any;
    application/service worldofwarcraft;
    action deny;
    terminal no;
  }
  ```
### Verify the User-ID Configuration (Continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Instructions</th>
</tr>
</thead>
</table>
| Step 4 | Test your Captive Portal configuration. | 1. From the same zone, go to a machine that is not a member of your directory, such as a Mac OS system, and try to ping to a system external to the zone. The ping should work without requiring authentication.  
2. From the same machine, open a browser and navigate to a web site in a destination zone that matches a Captive Portal rule you defined. The Captive Portal web form should display and prompt you for login credentials.  
3. Log in using the correct credentials and confirm that you are redirected to the requested page.  
4. You can also test your Captive Portal policy using the `test cp-policy-match` operational command as follows:  
   ```
   > test cp-policy-match from corporate to internet  
   source 192.168.201.10 destination 8.8.8.8  
   ```  
   Matched rule: 'captive portal' action: web-form |
| Step 5 | Verify that the log files display usernames. | Select a logs page (for example, Monitor > Logs > Traffic) and verify that the Source User column displays usernames. |
| Step 6 | Verify that reports display usernames. | 1. Select Monitor > Reports.  
2. Select a report type that includes usernames. For example, the Denied Applications report, Source User column, should display a list of the users who attempted to access the applications. |
Deploy User-ID in a Large-Scale Network

A large-scale network can have hundreds of information sources that firewalls query to map IP addresses to usernames and to map usernames to user groups. You can simplify User-ID administration for such a network by aggregating the user mapping and group mapping information before the User-ID agents collect it, thereby reducing the number of required agents.

A large-scale network can also have numerous firewalls that use the mapping information to enforce policies. You can reduce the resources that the firewalls and information sources use in the querying process by configuring some firewalls to acquire mapping information through redistribution instead of direct querying. Redistribution also enables the firewalls to enforce user-based policies when users rely on local sources for authentication (for example, regional directory services) but need access to remote resources (for example, global data center applications).

- Deploy User-ID for Numerous Mapping Information Sources
- Configure Firewalls to Redistribute User Mapping Information

Deploy User-ID for Numerous Mapping Information Sources

You can use Windows Log Forwarding and Global Catalog servers to simplify user mapping and group mapping in a large-scale network of Microsoft Active Directory (AD) domain controllers or Exchange servers. These methods simplify User-ID administration by aggregating the mapping information before the User-ID agents collect it, thereby reducing the number of required agents.

- Windows Log Forwarding and Global Catalog Servers
- Plan a Large-Scale User-ID Deployment
- Configure Windows Log Forwarding
- Configure User-ID for Numerous Mapping Information Sources

Windows Log Forwarding and Global Catalog Servers

Because each User-ID agent can monitor up to 100 servers, the firewall needs multiple User-ID agents to monitor a network with hundreds of AD domain controllers or Exchange servers. Creating and managing numerous User-ID agents involves considerable administrative overhead, especially in expanding networks where tracking new domain controllers is difficult. Windows Log Forwarding enables you to minimize the administrative overhead by reducing the number of servers to monitor and thereby reducing the number of User-ID agents to manage. When you configure Windows Log Forwarding, multiple domain controllers export their login events to a single domain member from which a User-ID agent collects the user mapping information.


To collect group mapping information in a large-scale network, you can configure the firewall to query a Global Catalog server that receives account information from the domain controllers.
The following figure illustrates user mapping and group mapping for a large-scale network in which the firewall uses a Windows-based User-ID agent. See Plan a Large-Scale User-ID Deployment to determine if this deployment suits your network.

Plan a Large-Scale User-ID Deployment

When deciding whether to use Windows Log Forwarding and Global Catalog servers for your User-ID implementation, consult your system administrator to determine:

- Bandwidth required for domain controllers to forward login events to member servers. The bandwidth is a multiple of the login rate (number of logins per minute) of the domain controllers and the byte size of each login event.

  Note that domain controllers won’t forward their entire security logs; they forward only the events that the user mapping process requires per login: three events for Windows Server 2003 or four events for Windows Server 2008/2012 and MS Exchange.

- Whether the following network elements support the required bandwidth:
  - Domain controllers—Must support the processing load associated with forwarding the events.
  - Member Servers—Must support the processing load associated with receiving the events.
  - Connections—The geographic distribution (local or remote) of the domain controllers, member servers, and Global Catalog servers is a factor. Generally, a remote distribution supports less bandwidth.
Configure Windows Log Forwarding

To configure Windows Log Forwarding, you need administrative privileges for configuring group policies on Windows servers. Configure Windows Log Forwarding on all the Windows Event Collectors—the member servers that collect login events from domain controllers. The following is an overview of the tasks; consult your Windows Server documentation for the specific steps.

### Configure Windows Log Forwarding

**Step 1** On each Windows Event Collector, enable event collection, add the domain controllers as event sources, and configure the event collection query (subscription). The events you specify in the subscription vary by domain controller platform:

- **Windows Server 2003**—The event IDs for the required events are 672 (Authentication Ticket Granted), 673 (Service Ticket Granted), and 674 (Ticket Granted Renewed).
- **Windows Server 2008/2012 (including R2) or MS Exchange**—The event IDs for the required events are 4768 (Authentication Ticket Granted), 4769 (Service Ticket Granted), 4770 (Ticket Granted Renewed), and 4624 (Logon Success).

To forward events as quickly as possible, **Minimize Latency** when configuring the subscription.

User-ID agents monitor the Security log, not the default forwarded events location, on Windows Event Collectors. Therefore, perform the following steps on each Windows Event Collector to change the event logging path to the Security log.

1. Open the Event Viewer.
2. Right-click the **Security** log and select **Properties**.
3. Copy the **Log path** (default `%SystemRoot%\System32\Winevt\Logs\security.evtx`) and click **OK**.
4. Right-click the **Forwarded Events** folder and select **Properties**.
5. Replace the default **Log path** (%SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx) by pasting the value from the **Security** log, and then click **OK**.

**Step 2** Configure a group policy to enable Windows Remote Management (WinRM) on the domain controllers.

**Step 3** Configure a group policy to enable Windows Event Forwarding on the domain controllers.

### Configure User-ID for Numerous Mapping Information Sources

**Step 1** Configure Windows Log Forwarding on the member servers that will collect login events.

**Step 2** Install the Windows-based User-ID agent.

**Configure Windows Log Forwarding.** This step requires administrative privileges for configuring group policies on Windows servers.

**Install the User-ID Agent** on a Windows server that can access the member servers. Make sure the system that will host the User-ID agent is a member of the same domain as the servers it will monitor.
Step 3 Configure the User-ID agent to collect user mapping information from the member servers.

2. Select User Identification > Discovery and perform the following steps for each member server that will receive events from domain controllers:
   a. In the Servers section, click Add and enter a Name to identify the member server.
   b. In the Server Address field, enter the FQDN or IP address of the member server.
   c. For the Server Type, select Microsoft Active Directory.
   d. Click OK to save the server entry.
3. Configure the remaining User-ID agent settings: see Configure the User-ID Agent for User Mapping.

Step 4 Configure an LDAP server profile to specify how the firewall connects to the Global Catalog servers (up to four) for group mapping information.

1. Select Device > Server Profiles > LDAP, click Add, and enter a Name for the profile.
2. In the Servers section, for each Global Catalog, click Add and enter the server Name, IP address (LDAP Server), and Port. For a plaintext or Start Transport Layer Security (Start TLS) connection, use Port 3268. For an LDAP over SSL connection, use Port 3269. If the connection will use Start TLS or LDAP over SSL, select the Require SSL/TLS secured connection check box.
3. In the Base DN field, enter the Distinguished Name (DN) of the point in the Global Catalog server where the firewall will start searching for group mapping information (for example, DC=acbdomain,DC=com).
4. For the Type, select active-directory.
5. Configure the remaining fields as necessary: see Add an LDAP server profile.

Step 5 Configure an LDAP server profile to specify how the firewall connects to the servers (up to four) that contain domain mapping information. User-ID uses this information to map DNS domain names to NetBIOS domain names. This mapping ensures consistent domain/username references in policy rules.

1. Select Device > Server Profiles > LDAP, click Add, and enter a Name for the profile.
2. In the Servers section, for each Global Catalog, click Add and enter the server Name, IP address (LDAP Server), and Port. For a plaintext or Start TLS connection, use Port 389. For an LDAP over SSL connection, use Port 636. If the connection will use Start TLS or LDAP over SSL, select the Require SSL/TLS secured connection check box.
3. In the Base DN field, enter the Distinguished Name (DN) of the point in the Global Catalog server where the firewall will start searching for group mapping information. The value must start with the string: cn=partitions,cn=configuration (for example, cn=partitions,cn=configuration,DC=acbdomain,DC=com).
### Configure User-ID for Numerous Mapping Information Sources (Continued)

#### Step 6
Create a group mapping configuration for each LDAP server profile you created.

1. Select **Device > User Identification > Group Mapping Settings**.
2. Click **Add** and enter a **Name** to identify the group mapping configuration.
3. Select the **LDAP Server Profile** and ensure the **Enabled** check box is selected.
4. Configure the remaining fields as necessary: see **Map Users to Groups**.
   - If the Global Catalog and domain mapping servers reference more groups than your security rules require, configure the **Group Include List** and/or **Custom Group** list to limit the groups for which User-ID performs mapping.
5. Click **OK** and **Commit**.

### Configure Firewalls to Redistribute User Mapping Information

Every firewall that enforces user-based policy requires user mapping information. However, a large-scale network where numerous firewalls directly query the mapping information sources requires both the firewalls and sources to use considerable resources. To improve resource efficiency, you can configure some firewalls to acquire mapping information through redistribution instead of direct querying. Redistribution also enables the firewalls to enforce user-based policies when users rely on local sources for authentication (for example, regional directory services) but need access to remote resources (for example, global data center applications).

#### Firewall Deployment for User-ID Redistribution

You can organize the redistribution sequence in layers, where each layer has one or more firewalls. In the bottom layer, PAN-OS integrated User-ID agents running on firewalls and Windows-based User-ID agents running on Windows servers perform the IP address-to-username mapping. Each higher layer has firewalls that receive the mapping information from up to 100 User-ID agents in the layer beneath it. The top-layer firewalls aggregate the mapping information from all layers. This deployment provides the option to configure global policies for all users (in top-layer firewalls) and region- or function-specific policies for a subset of users in the corresponding domains (in lower-layer firewalls).

**Figure: User-ID-Redistribution** shows a deployment with three layers of firewalls that redistribute mapping information from local information sources (directory servers, in this example) to regional offices and then to a global data center. The data center firewall that aggregates all the mapping information shares it with other data center firewalls so that they can all enforce global policy. Only the bottom layer firewalls use PAN-OS integrated User-ID agents and Windows-based User-ID agents to query the directory servers.

The information sources from which User-ID agents collect mapping information do not count towards the maximum of ten hops in the sequence. However, Windows-based User-ID agents that forward mapping information to firewalls do count. Therefore, in this example, redistribution from the European region to all the data center firewalls requires only three hops, while redistribution from the North American region...
requires four hops. Also in this example, the top layer has two hops: the first to aggregate mapping information in one data center firewall and the second to share the information with other data center firewalls.

Figure: User-ID-Redistribution
## Configure User-ID Redistribution

| Step 1 | Plan the redistribution architecture. | Decide which User-ID agents and methods to use for mapping IP addresses to usernames. You can redistribute user mapping information collected through any method except Terminal Services (TS) agents. You cannot redistribute Group Mapping or HIP match information. | Determine the most efficient Firewall Deployment for User-ID Redistribution. Some factors to consider are:  
- Which firewalls will enforce global policies for all users and which firewalls will enforce region- or function-specific policies for a subset of users?  
- How many hops does the redistribution sequence require to aggregate mapping information for firewalls in different functional or regional layers to enforce policy?  
- How can you minimize the number of firewalls that query the information sources? The fewer the number of querying firewalls, the lower the processing load is on both the firewalls and sources. |
| Step 2 | Configure the User-ID agents to perform the user mapping. | Configure User Mapping Using the PAN-OS Integrated User-ID Agent.  
Configure User Mapping Using the Windows User-ID Agent. |
| Step 3 | Enable each bottom-layer firewall to forward mapping information to firewalls in the layer above. | 1. Configure the firewall to function as a User-ID agent.  
b. [Firewalls with multiple virtual systems only] Select the Location. You must configure the User-ID settings for each virtual system.  
You can redistribute mapping information among virtual systems on different firewalls or on the same firewall. In both cases, each virtual system counts as one hop in the redistribution sequence.  
c. Edit the Palo Alto Networks User-ID Agent Setup and select Redistribution.  
d. Enter a Collector Name to identify this firewall as a User-ID agent.  
e. Enter and confirm a Pre-Shared Key to secure communication between this firewall and the higher-layer firewalls. On a multi-vsyst firewall, each vsys requires a unique pre-shared key.  
f. Click OK.  
2. Configure an Interface Management profile with the User-ID service enabled and assign the profile to the interface you want the firewall to use when responding to mapping information queries from firewalls in the layer above.  
3. (Optional) Configure policies that are specific to the user accounts for which you want this firewall to collect mapping information.  
4. Commit your changes. |
Deploy User-ID in a Large-Scale Network

Step 4: Enable each middle layer firewall to receive mapping information from the layer below and forward it to the layer above.

You must also perform this task for any firewall that redistributes mapping information to other firewalls in the same layer. For example, Figure: User-ID-Redistribution shows one data center firewall that redistributes to other data center firewalls.

Each firewall can receive mapping information from up to 100 User-ID agents.

Figure: User-ID-Redistribution shows only one middle layer of firewalls but you can deploy as many layers as the redistribution limit of ten hops allows.

<table>
<thead>
<tr>
<th>Table: Configure User-ID Redistribution (Continued)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Configure the firewall to receive mapping information from firewalls acting as User-ID agents in the layer below.</td>
</tr>
<tr>
<td>b. Enter a Name to identify the lower-layer firewall.</td>
</tr>
<tr>
<td>c. Enter the Host name or IP address of the interface that you configured on the lower-layer firewall to respond to mapping information queries.</td>
</tr>
<tr>
<td>d. Enter the Port number (default is 5007) on which the lower-layer firewall will listen for User-ID queries.</td>
</tr>
<tr>
<td>e. Enter the Collector Name you specified when configuring the lower-layer firewall to act as a User-ID agent.</td>
</tr>
<tr>
<td>f. Enter and confirm the Collector Pre-Shared Key you specified on the lower-layer firewall.</td>
</tr>
<tr>
<td>g. Ensure the configuration is Enabled (default) and click OK.</td>
</tr>
<tr>
<td>h. Check the Connected column to confirm the firewall you just added as a User-ID agent is connected ( ).</td>
</tr>
<tr>
<td>2. Configure a service route for the firewall to use for sending mapping information queries to firewalls in the layer below.</td>
</tr>
<tr>
<td>a. Select Device &gt; Setup &gt; Services.</td>
</tr>
<tr>
<td>b. (Firewalls with multiple virtual systems only) Select Global (for a firewall-wide service route) or Virtual Systems (for a virtual system-specific service route). For details, refer to Customize Service Routes to Services for Virtual Systems.</td>
</tr>
<tr>
<td>c. Click Service Route Configuration, select Customize, and select IPv4 or IPv6 depending on your network protocols. Configure the service route for both protocols if your network uses both.</td>
</tr>
<tr>
<td>d. Select UID Agent and then select the Source Interface and Source Address.</td>
</tr>
<tr>
<td>e. Click OK twice to save the service route.</td>
</tr>
<tr>
<td>3. Enable the firewall to forward the mapping information to firewalls in the layer above.</td>
</tr>
<tr>
<td>a. Configure the firewall to function as a User-ID agent.</td>
</tr>
<tr>
<td>b. Configure an Interface Management profile with the User-ID service enabled and assign the profile to the interface you want the firewall to use when responding to mapping information queries from firewalls in the layer above.</td>
</tr>
<tr>
<td>4. (Optional) Configure policies specific to user accounts for which you want this firewall to aggregate mapping information from lower layers.</td>
</tr>
</tbody>
</table>
| 5. Commit your changes.
Configure User-ID Redistribution (Continued)

**Step 5** Enable each top-layer firewall to receive mapping information from all other layers.
You must also perform this task for any firewall that is an end point in the redistribution sequence within a layer.
In the example of Figure: User-ID-Redistribution, you would perform this task for the two data center firewalls that receive mapping information from another data center firewall.

1. Configure the firewall to receive mapping information from firewalls acting as User-ID agents in the layer below.
2. Configure a service route for the firewall to use for sending mapping information queries to firewalls in the layer below.
3. **(Optional)** Configure policies that are global to all user accounts.
4. **Commit** your changes.

**Step 6** Verify that the top-layer firewalls are aggregating mapping information from all other layers.
This step samples a single user mapping that is collected in a bottom-layer firewall and forwarded to a top-layer firewall. Repeat the step for several user mappings and several firewalls to ensure your configuration is successful.

1. Access the CLI of a bottom-layer firewall and run the following operational command:
   ```
   > show user ip-user-mapping all
   ```
2. Record the IP address associated with any username.
3. Access the CLI of a top-layer firewall and run the following command, where `<address>` is the IP address you recorded in the previous step:
   ```
   > show user ip-user-mapping ip <address>
   ```
   If the firewall successfully received the user mapping from the bottom-layer firewall, it displays output similar to the following and displays the same username as you recorded in the bottom-layer firewall.

   ```
   IP address: 192.0.2.0 (vsys1)
   User: corpdomain\username1
   From: AD
   Idle Timeout: 2643s
   Max. TTL: 2643s
   Groups that the user belongs to (used in policy)
   ```