CONTROLLING ACCESS TO NETWORK RESOURCES WITH USER-ID

KNOW THE WHO, CONTROL THE WHO

- User-ID overview
- User mapping methods overview
- Configure User-ID
- PAN-OS integrated agent configuration
- Configure group mapping
- User-ID and Security policy

EDU-210 Version A
PAN-OS® 10.2

paloalto NETWORKS

Learning Objectives

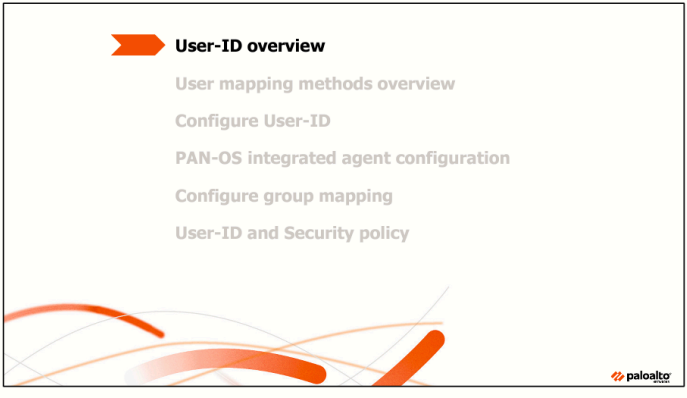
After you complete this module,
you should be able to:

- Identify the purpose and four main components of User-ID
- Identify available IP-to-username mapping methods
- Configure the PAN-OS® integrated agent to connect to monitored servers
- Configure username-to-group name mapping
- Implement User-ID in Security policy

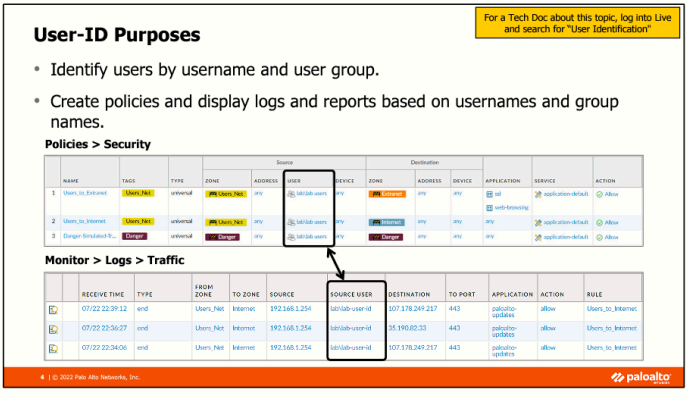
This module covers the topics listed here. Read through the list before proceeding.

After you complete this module, you should be able to:

- Identify the purpose and four main components of User-ID
- Identify available IP-to-username mapping methods
- Configure the PAN-OS® integrated agent to connect to monitored servers
- Configure username-to-group name mapping
- Implement User-ID in Security policy



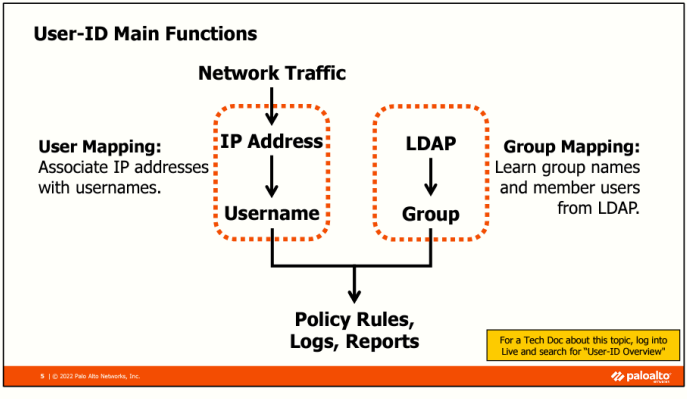
This section provides an overview of the purpose and function of User-ID.



As opposed to an IP address, the user identity is an integral component of an effective security infrastructure. Knowing who is using each application 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 ultimate purpose of User-ID is to give you the ability to write policy, display logs, and display reports by using usernames instead of using just IP addresses and port numbers. User-ID, combined with App-ID technology, provides you with very granular control over which users or user groups may access which applications from which network segments (zones). For example, unknown users can be treated differently from known users to accommodate network guests.

Multiple policy types support User-ID. You can use usernames or group names as matching criteria in Authentication policies, Decryption policies, DoS Protection policies, Policy-Based Forwarding policies, QoS policies, Security policies, SD-WAN policies, and Tunnel Inspection policies.



Before creating user-based and group-based policy rules, the firewall requires a list of all available users and their corresponding group mappings. The firewall uses group mapping and user mapping to collect this information.

The firewall collects Group Mapping information by connecting directly to your LDAP directory server or using XML API integration with your directory server. User-ID technology includes many methods to collect IP address-to-username mapping information. You can choose which user mapping methods to use to suit your environment and even use different methods at different sites.

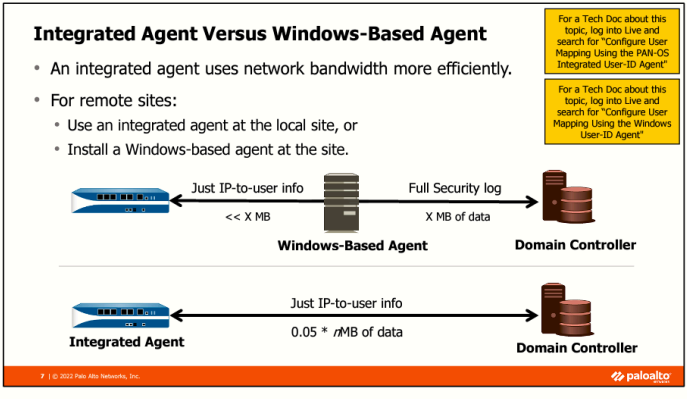
User-ID Components

Component	Characteristics
Palo Alto Networks firewall	• Maps IP addresses to usernames • Maps usernames to group names
PAN-OS integrated User-ID agent	• Runs on the firewall • Collects IP address-to-username information
Windows-based User-ID agent	• Runs on a domain member • Collects IP address-to-username information • Sends information to the firewall
Palo Alto Networks Terminal Services agent	• Runs on Microsoft and Citrix terminal servers • Collects IP and port number-to-username information • Sends information to firewall

User-ID technology has four main components. The table lists each component's name and primary characteristics.

The User-ID agent comes in two forms: an integrated agent that resides on the firewall and a Windows-based agent:

- The PAN-OS integrated agent is included with PAN-OS software.
- The Windows-based agent is available for download from Palo Alto Networks and installed on one or more Windows systems.
- A firewall can communicate with both agent types at the same time.
- Both agent types monitor up to 100 domain controllers or Exchange servers.
- Both agent types can monitor users and domain controllers only from a single Active Directory (or AD) domain.
- The integrated agent is designed for small and midsize deployments such as small remote offices or lab environments.
- Multiple Windows-based agents can be deployed to handle larger environments or multi-forest domains.

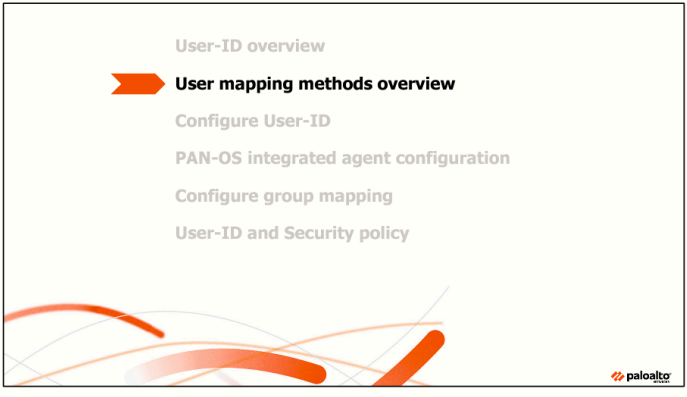


Although the Windows-based agent and the PAN-OS integrated agent perform the same basic tasks, they use different underlying communication protocols. This difference makes each agent more appropriate for particular environments.

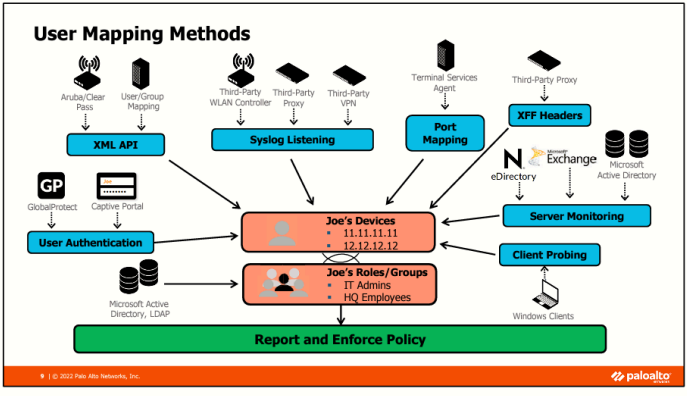
The Windows-based agent uses MS-RPC, which requires the full Windows Security logs to be sent to the agent, where they are filtered for the relevant User-ID information.

The PAN-OS integrated agent uses either the Windows Management Instrumentation (or WMI) or the Windows Remote Management Protocol (or WinRM) over HTTP/HTTPS, enabling the agent to retrieve only the relevant information User-ID information from the Windows Security logs.

The result is that, in infrastructure with remote networks separated by WAN links, the integrated agent is more appropriate for reading remote logs, and the Windows-based agent is more suitable for reading local logs. However, the use of the integrated agent is not without cost: It consumes more of the firewall's management plane resources. For this reason, deployment of the Windows agent at remote sites and having them forward the relevant User-ID information to a firewall on a central network often is beneficial.



This section describes the mapping and monitoring methods of User-ID.



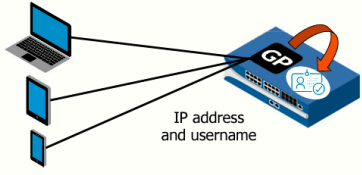
User-ID technology includes multiple methods to map IP addresses to users. The decision about which methods you employ depends on your organization's operating systems, applications, and network infrastructure. If any of the methods successfully maps an IP address to a user, the firewall can use the user's name for policy rule matches, logs, and reports.

The following list is a brief description of each method shown in the illustration:

- User-ID acquires username information from Captive Portal web forms and login events on GlobalProtect client machines.
- User-ID listens for Syslog login and logout messages from network access control (or NAC) systems, 802.1x devices, and wireless controllers.
- User-ID monitors Microsoft AD domain controllers, Microsoft Exchange servers, or Novell eDirectory servers for login or logout events recorded in Authentication logs. User-ID also reads session tables to confirm known IP address-to-username mappings based on current Windows file and printer shares.
- User-ID maps IP address and port number combinations to usernames for Microsoft Remote Desktop Services and Citrix Presentation Server or Citrix XenApp.
- User-ID probes Windows systems to verify current user mappings and discover new IP address-to-username mappings.
- When other methods cannot be used, User-ID can consume PAN-OS XML API user login and logout messages sent from terminal servers, NAC systems, and other network devices that can format and send XML over HTTP.

User Mapping Using GlobalProtect

- Every GlobalProtect user is required to enter login credentials to access the firewall.
- GlobalProtect directly adds the username to the firewall's User-ID mapping table.
- GlobalProtect is the best solution for high-security environments.



The GlobalProtect client provides the user mapping information to the firewall for remote roaming users. 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. The firewall adds this GlobalProtect login information to the User-ID user mapping table for visibility and user-based policy rule enforcement.

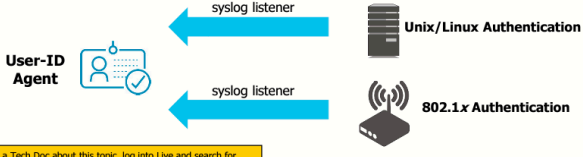
User-ID information can also be provided from clients connected to an internal network via an internal GlobalProtect gateway without establishing a VPN tunnel to a firewall. Every internal GlobalProtect user has an agent or app running on the internal client that requires the user to enter login credentials that the firewall can use.

Because GlobalProtect users must authenticate to gain access to the network, the IP address-to-username mapping is explicitly known. GlobalProtect is the best solution in sensitive environments where you must be sure of who a user is to allow access to an application or service.

For more information about configuring GlobalProtect, log into Live and search Technical Documentation for "GlobalProtect Administrator's Guide" or see *GlobalProtect Administrator's Guide* at https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin.html.

User-ID Syslog Monitoring

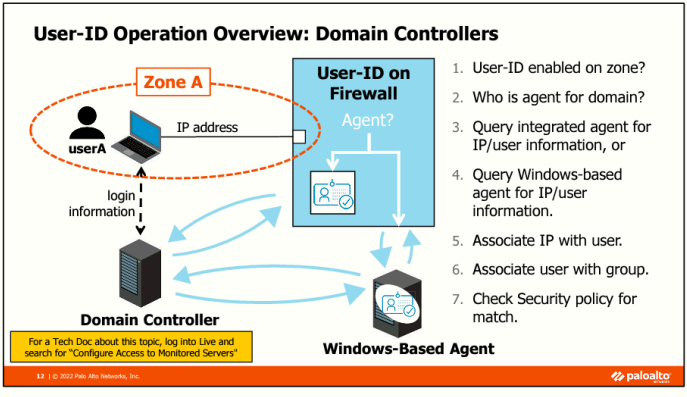
- Monitors syslog events for login and logout messages.
- Messages are used to update IP address-to-username mappings.
- Syslog Parse Profiles enable interoperability with diverse syslog types.



For a Tech Doc about this topic, log into Live and search for "Configure User-ID to Monitor Syslog Senders for User Mapping"

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 NAC mechanisms. You can configure these services to send Syslog messages that contain information about login and logout events and configure the User-ID agent to parse those messages. Both the integrated and Windows-based agents can retrieve Syslog messages. The User-ID agent can parse for login events to map IP addresses to usernames and parse for logout events so that the firewall deletes outdated mappings. Deleting outdated mappings is particularly useful in environments where IP address assignments often change.

The PAN-OS integrated User-ID agent and the 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 and associate multiple profiles with each sender. If you use the PAN-OS integrated User-ID agent, you also can use predefined Syslog Parse Profiles that Palo Alto Networks provides through Applications content updates.



The diagram and text provide an overview of the operation of User-ID technology in the scenario where userA logs in to their laptop. The laptop is an AD domain member, so userA's login information is recorded on the AD domain controller. The login information includes userA's username and IP address.

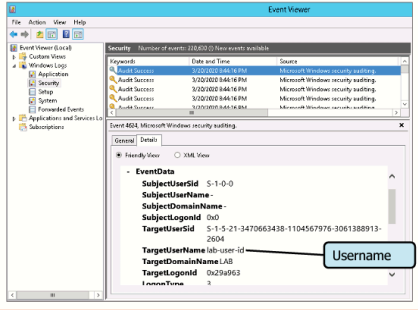
Before User-ID can operate, it must be enabled on the security zone. If User-ID is enabled, the firewall consults the administrator-defined User-ID configuration to determine which agents the firewall has available to gather IP address and username information. Depending on the configuration, user-ID on the firewall could query either an integrated agent or a Windows-based agent. The agent retrieves IP address and username information from the domain controller.

After User-ID has retrieved the IP address and username information from an agent, it can use the firewall's LDAP configuration to retrieve user-to-group mapping information from an LDAP server.

At this point, User-ID will have an IP address associated with a username and possibly a username associated with one or more group names. Suppose traffic arrives from the IP address associated with userA. In that case, the firewall can use the User-ID information to check its Security policy rules for a match and determine how to handle traffic from userA.

User-ID Domain Controller Monitoring

- Monitors Security logs of domain controllers
- Monitors all domain controllers per domain to get all login and logout events



For a Tech Doc about this topic, log into Live and search for "Create a Dedicated Service Account for the User-ID Agent"

With passive server monitoring, a User-ID agent (either a Windows-based or integrated User-ID agent) monitors the Security logs for user login or logout events for the specified Microsoft domain controllers:

- When the User-ID agent starts up, it will parse the security event logs and record all the user login events.
- Afterward, it will regularly check the Security logs for new login or logout events.
- User mappings are cached for an amount of time equal to the timeout value set in the User-ID agent interface.

To ensure that security events are recorded in the Security logs, note that the AD domain must be configured to log successful account login events.

Because users can authenticate to any domain controller in a domain and the Security logs are not replicated between domain controllers, you also must set up server monitoring for all domain controllers to capture all user login events. Each User-ID agent can monitor multiple domain controllers per domain. However, each User-ID agent can monitor only a single domain.

Because server monitoring requires very little overhead and because most users generally can be mapped using this method, Palo Alto Networks recommends it as the base user mapping method for most User-ID deployments.

User-ID Windows Session Monitoring

- The server logs session information when users connect to shared printers or files.
- Session monitoring is used to maintain known IP address-to-username mappings.

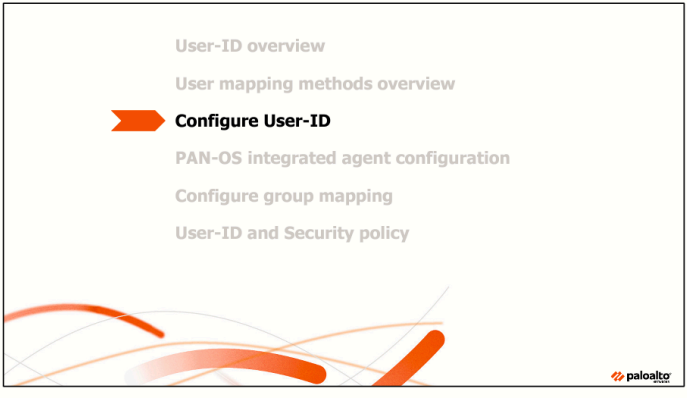
Clients connected to a shared file or print resource will have their session information stored on the domain controller. An additional Windows-based method to resolve IP addresses to users is to consult the shared resource session table recorded on the domain controller.

User-ID Mapping Recommendations

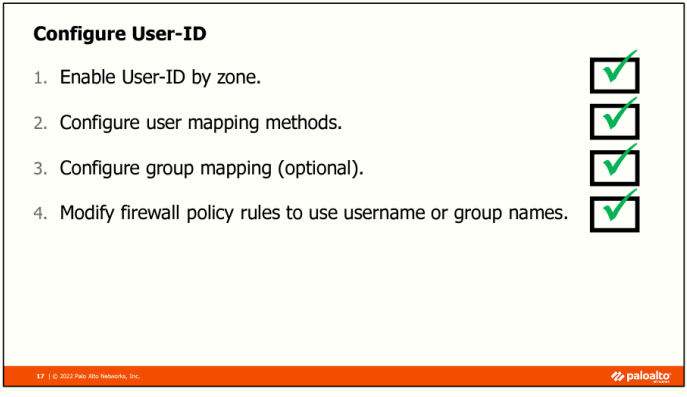
For a Tech Doc about this topic, log into Live and search for "Get Started with User-ID Best Practices"

If you have ...	Use
GlobalProtect VPN clients	GlobalProtect
Web clients that do not use the domain server	Captive Portal
Non-windows systems, NAC mechanisms such as wireless controllers, 802.1*x* devices, or proxy servers	syslog listener
Exchange servers, domain controllers, or eDirectory servers	User-ID agent: Server monitoring
Windows file and print shares	User-ID agent: Session monitoring
Multi-user systems such as Microsoft Remote Desktop Services or Citrix Metaframe Presentation Server (XenApp)	Terminal Services agent
Windows clients that often change IP addresses	User-ID agent: Client probing
Devices and applications not integrated with User-ID	XML API

The table shows the circumstances under which Palo Alto Networks recommend various User-ID components and mapping methods.



This section describes how to configure User-ID.



The list shows the four general steps to configure User-ID technology—the specific steps to configure group mapping, particularly user mapping, depending on your environment.

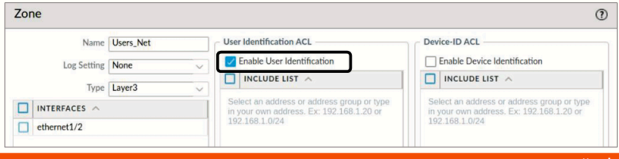
Definition of policy rules based on group names rather than individual usernames simplifies firewall administration. You do not have to update the rules or perform a commit whenever users are added to, or removed from, a group.

Enable User-ID Per Zone

For a Tech Doc about this topic, log into Live and search for "Enable User-ID"

- Enable User-ID on the source zone where user traffic originates.
- Enable User-ID only for internal zones.
- By default, all subnetworks in the source zone are mapped:
  - Modify using **Include List** or **Exclude List**.

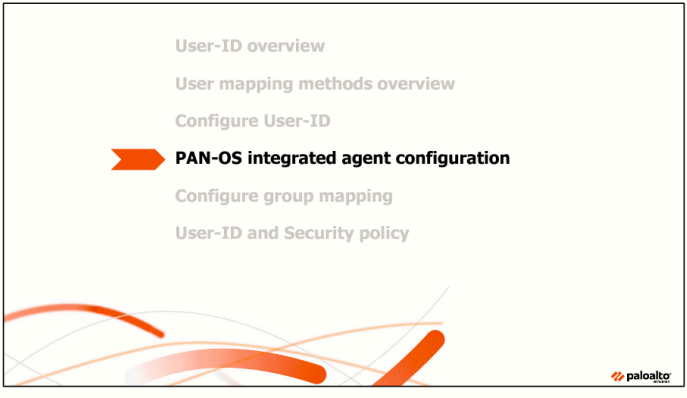
Network > Zones > <select_zone>



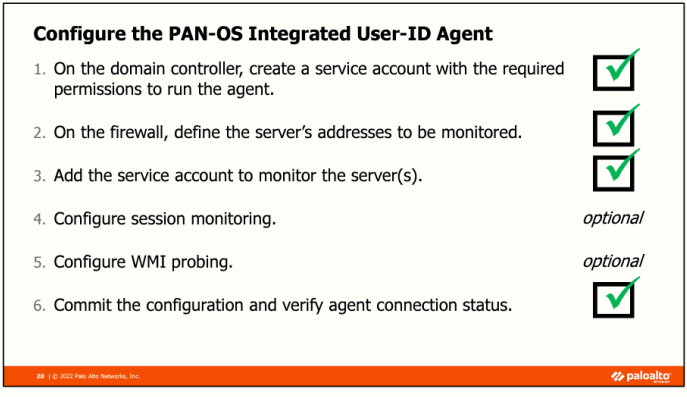
Enable User-ID technology per zone on the firewall. You must select the Enable User Identification check box for each zone to permit User-ID to probe for users on the zone. User-ID tracks only users associated with the source zone of a session. Never enable User-ID for a zone containing the internet, or your firewall will attempt to identify every user outside your network.

By default, User-ID will try to map users from all subnetworks found within a User-ID-enabled zone. Use the **Include List** to limit the subnetworks or specific addresses that the firewall will map to users. Use the **Exclude List** only to exclude user mapping information for a subset of the subnetworks you added to the **Include List**.

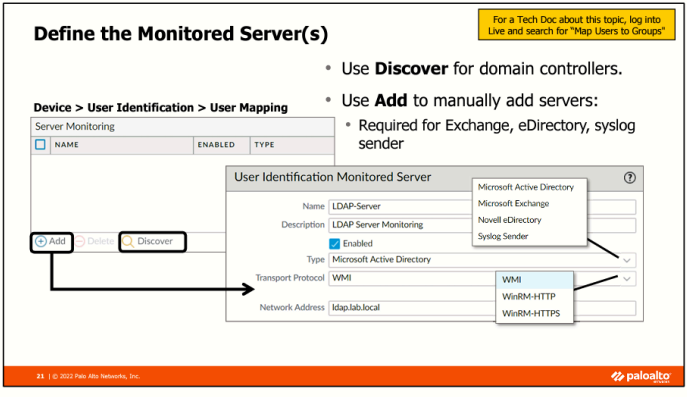
If WMI probing is enabled, WMI will probe private IP addresses but not probe public IP addresses by default. Private addresses are those found in the IP addresses ranges 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.255, and 192.168.0.0 to 192.168.255.255. To enable WMI probing to map public addresses, you must use the addresses or address ranges in the **Include List**.



The section describes how to configure the PAN-OS integrated User-ID agent.



The list shows the main steps to configure a PAN-OS integrated User-ID agent to connect to monitored servers.



Each User-ID agent must be configured for the servers it needs to monitor. The agent includes an autodiscovery feature that, via DNS, automatically identifies available Microsoft Windows servers for event log monitoring. With the release of PAN-OS 9.0, the integrated agent supports WMI and WinRM protocols to map IP addresses to usernames.

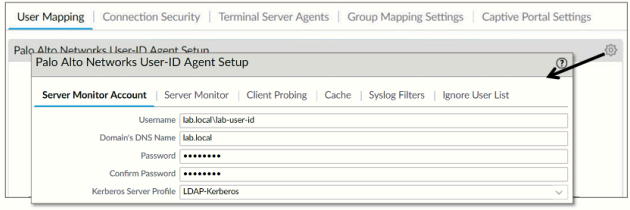
The firewall will discover domain controllers based on the domain name entered in the **Domain** field of the **Device > Setup > Management > General Settings** page.

Define the User-ID Agent Account

For a Tech Doc about this topic, log into Live and search for "Device > Server Profiles > LDAP"

- Necessary permissions are provided if the agent account belongs to:
  - Domain Administrators group, or
  - Server Operators and Event Log Readers groups

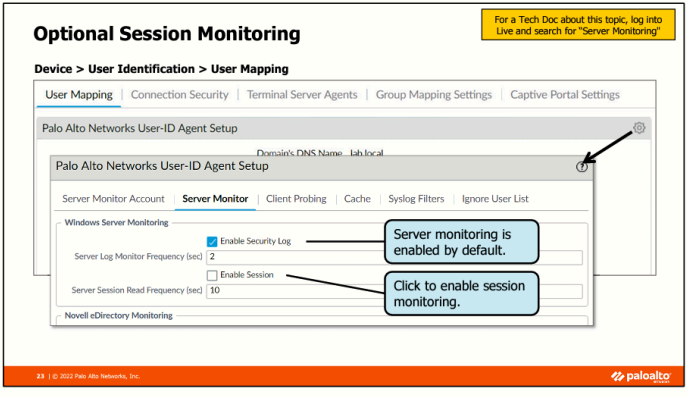
Device > User Identification > User Mapping



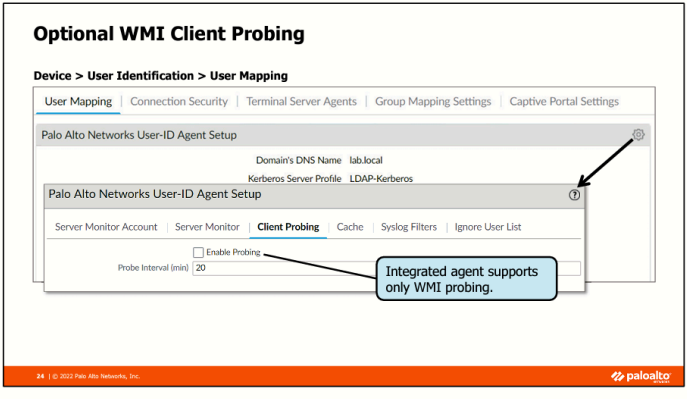
22 | © 2022 Palo Alto Networks, Inc.

Set the domain credentials for the account the firewall will use to access Windows resources. This setting is required for monitoring domain controllers and Exchange servers. The information in the **User Name** field must be entered using the format domain\username.

No special permissions configuration is necessary if the integrated agent runs as an account that belongs to the Domain Administrators group or belongs to the Server Operators and Event Log Readers groups. However, membership in these groups provides the account with more permissions than just the capability to perform server monitoring or client probing. Therefore, you might want to run the agent using a restricted account with minimal permissions. To create a Windows account with minimal permissions, see the permissions configuration instructions in the *PAN-OS Administrator's Guide* at https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin.html. The steps to configure an account with minimal Windows permissions depend on the Windows operating system version you have.

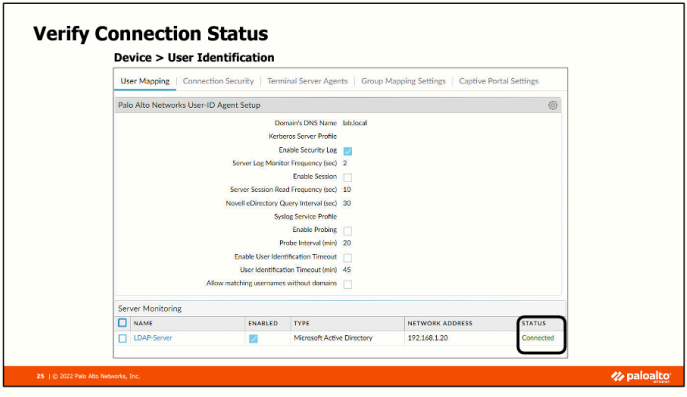


To enable session monitoring, select the **Enable Session** check box. This allows the integrated agent to use current file and print sharing information to verify current IP address-to-username mappings.

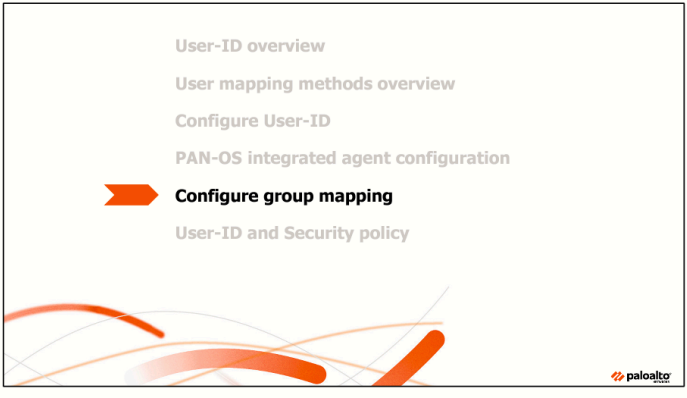


Client probing was designed for legacy networks where most users were on Windows workstations on the internal network. Still, it is not ideal for current networks that support roaming and mobile user base on various devices and operating systems.

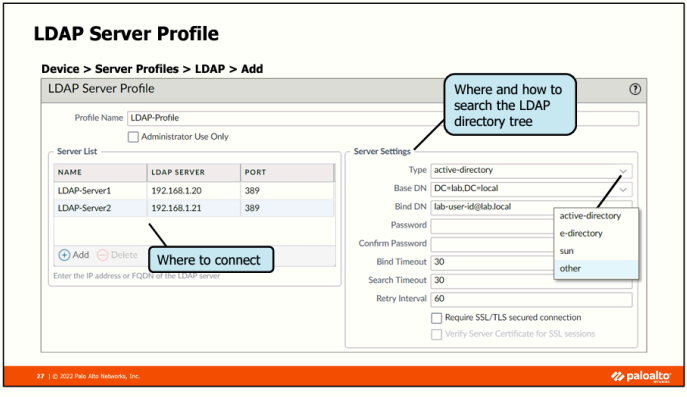
You can enable the integrated agent to perform WMI probing for each client system identified by the user mapping process. The integrated agent periodically probes each learned IP address to verify that the same user still is logged in. When a firewall encounters an IP address for which it has no user mapping, it sends the address to the integrated agent for an immediate probe.



After you commit your configuration changes, the status of each of your monitored servers should be **Connected**.



This section describes how to configure User-ID group mapping.



A Server Profile specifies which LDAP servers will be contacted, the order in which they are reached, and how and where to search the LDAP directory tree. By default, port 389 communicates to the LDAP server using TLS. To use SSL instead, specify port 636.

The **Type** menu specifies the LDAP server to which the firewall will connect.

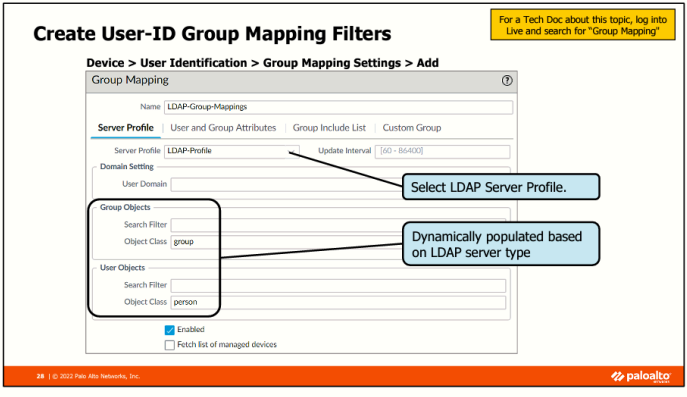
The **Base DN** field represents the point in the LDAP directory tree where the firewall will begin its search for users and groups. The **Base DN** information should auto-populate from the LDAP server when you click the **Base DN** drop-down arrow, but you can manually override the value. If you have difficulties identifying your directory base DN on the domain controller, open the **Active Directory Domains and Trusts** Microsoft Management Console snap-in and look at the name of the top-level domain.

The **Bind DN** and **Password** fields contain the LDAP username and password that the firewall uses to connect to the LDAP server. The format of this field must match what the LDAP server is expecting. For example, it could be either a fully qualified LDAP name (cn=administrator,cn=users,dc=cse,dc=local) or a user principal name (administrator@cse.local). The bind DN account must have sufficient LDAP permissions to read the LDAP directory.

If universal groups are used in AD, a global catalog (or GC) server must capture group memberships. The firewall can access a GC server only if the LDAP port is set to 3268.

The default timeout and interval settings can be overridden as necessary based on the performance of your network and LDAP server.

Ensure that the **Require SSL/TLS secured connection** check box is selected. By default, it should be. To have the firewall verify the LDAP server's certificate, select the **Verify Server Certificate for the SSL sessions** check box.

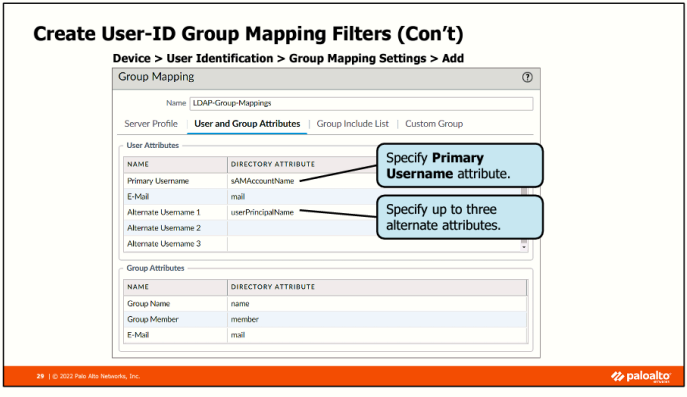


On the **Server Profile** tab, use the **Server Profile** menu to select your LDAP Server Profile.

The **User Domain** value normally is blank. Enter a NetBIOS domain name value only if you need to override the domain automatically detected on the LDAP server.

The **Group Objects** fields are dynamically populated. Modify the **Group Objects** fields to configure the firewall to look for group names in non-standard LDAP tree locations. The groups found by the firewall will be displayed in the **Available Groups** pane on the **Group Include List** tab.

The **User Objects** fields are dynamically populated. Modify the **User Objects** fields to configure the firewall to look for usernames in non-standard LDAP tree locations.



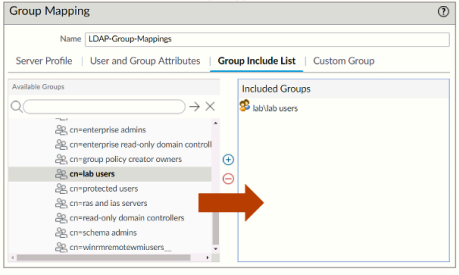
Starting with PAN-OS 8.1, the firewall can identify a user even if the User-ID sources send usernames in multiple formats. For example, the username format could be a SAM account name, email address, user principal name, or common name. As the firewall acquires usernames, the usernames are identified based on the user attributes that the firewall will read from the LDAP-compliant directory service. You can specify which attributes are used to collect usernames from the directory service using a Group Mapping Profile.

When the firewall supports multiple user attributes, you should specify an attribute as the **Primary Username** for users. This value represents the username in the logs, reports, and policy configuration.

In addition to configuring a **Primary Username**, you can configure an email address or up to three alternate usernames to identify users uniquely.

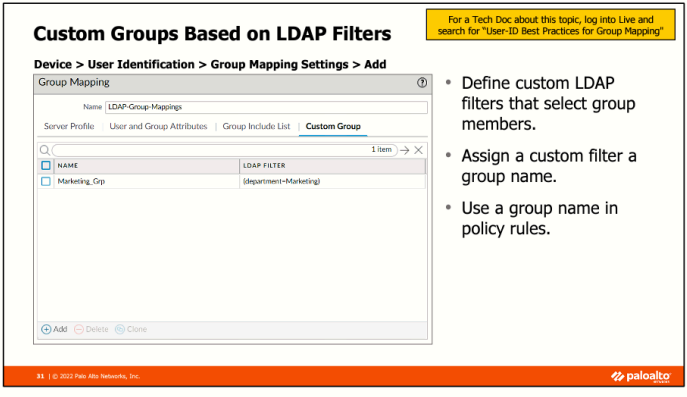
Filter Groups Sent to the Firewall

Device > User Identification > Group Mapping Settings > Add



- Only **Included Groups** are available on drop-down lists in policy rules.
- Shorter lists simplify firewall policy rule administration.

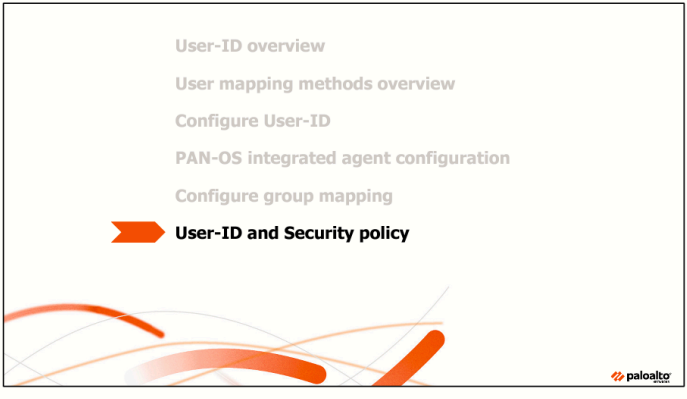
Use the **Group Include List** tab to filter which groups discovered on the LDAP server are displayed on the drop-down lists in firewall policy rules. By default, if you do not move groups to the **Included Groups** pane, all discovered groups are available in policy rules.



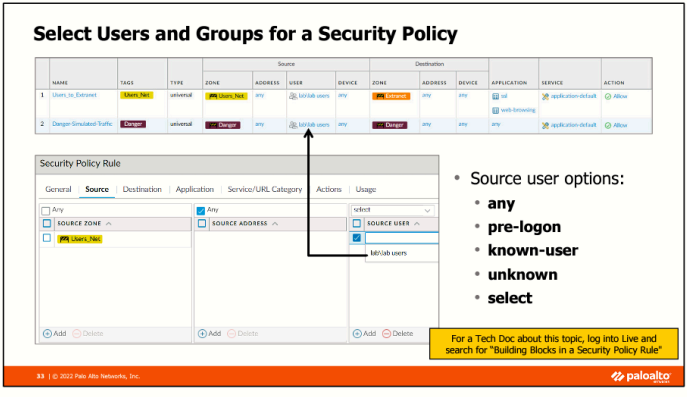
The **Custom Group** tab enables you to define custom groups based on LDAP filters to base firewall policy rules on user attributes that do not match existing LDAP user groups. Definition of a custom group using an LDAP filter on the firewall can be quicker than creating a new group or changing an existing group on an LDAP server. It does not require the assistance of an LDAP administrator. User-ID maps all the LDAP directory users who match your filter to the custom group. For example, you might want a Security policy rule that allows only users in the Marketing department to access social networking sites. If no LDAP group exists for that department, you can configure an LDAP filter that matches users the LDAP attribute department is set to Marketing.

Log queries and reports that are based on user groups include custom groups.

You can add custom groups to the **Allow List** of Authentication Profiles.



This section describes selecting users and groups for a Security policy.

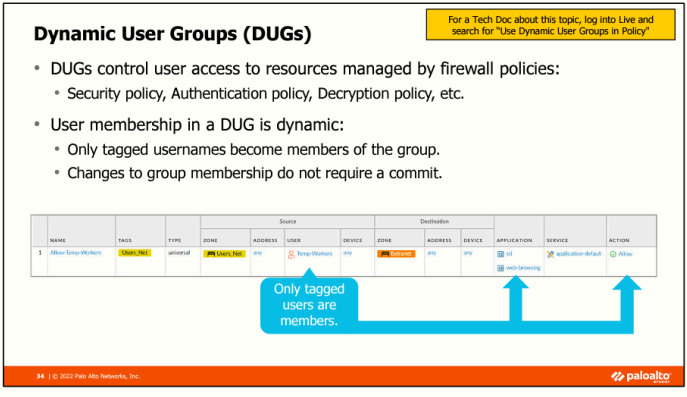


When you select users for a Security policy, these options are available:

- **any**: Matches any value for the user
- **pre-logon**: Used with certain GlobalProtect implementations
- **known-user**: Matches any user or group identified by User-ID
- **unknown**: Matches traffic where User-ID methods could not identify the user
- **select**: Matches a specific user or group identified by User-ID

When using a user or group in a policy rule, remember that the **Source Address** field and the **Source User** field are evaluated with a logical AND condition. The rule applies only if the specified user or group and the specified source addresses match. Be careful not to make the match conditions so specific that the policy eliminates permitted traffic.

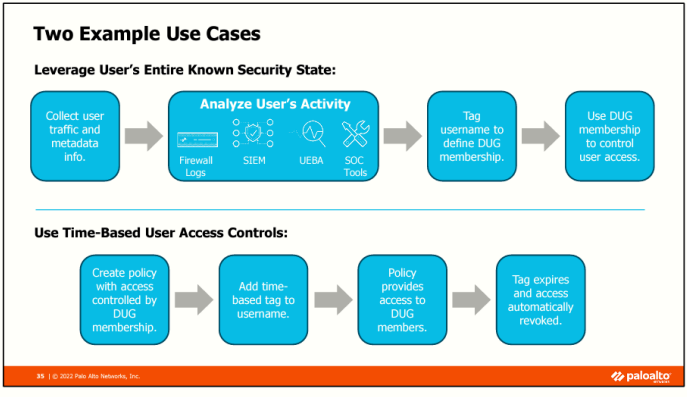
Users and groups can only be used in a policy rule if they are known on the firewall. For larger environments, a best practice is to configure policy rules based on groups rather than individual users. The number of users often becomes more unwieldy for defining policy as the number of users in an environment increases.



Dynamic user groups (or DUGs) are a new PAN-OS 9.1. DUGs control access to resources managed by firewall policies, including the Security policy, Authentication policy, and Decryption policy. When creating a policy rule, you add a DUG to the **Source User** field as a match criterion. In past PAN-OS releases, you would have been able to add only a username or a static group name to the **Source User** field.

You must commit your firewall configuration after configuring a DUG name and adding it to a policy rule. However, you do not have to perform a commit when users are added or removed from the DUG. User membership in a DUG is dynamic, and it is controlled by tagging and untagging usernames.

You can manually tag and untag usernames using the web interface. Usernames can also be tagged and untagged by using the auto-tagging feature in a log forwarding profile or programming another utility to invoke PAN-OS XML API commands.



Here we show two use case examples.

The first example illustrates the use of a user's entire known security state, derived from various sources, to determine how the firewall will control or affect the user's access to network resources. In this case, the user's network traffic is logged to be analyzed. User metadata also might be collected from other resources such as an LDAP server.

All of the data can be analyzed in the firewall's logs, on a Security Information and Event Management (SIEM), in a user and entity behavior analytics system, or using various tools available to a security operations center (SOC). Any of these tools can be configured to tag or untag a username, depending on the analysis results. Tagging and untagging of a username determine whether it is a member of a DUG. Then DUG membership and policy configuration determines how the firewall should treat the user's network traffic.

The second example illustrates how to use a DUG to implement time-based access controls for workers who require short-term access to network resources. In this case, you create a DUG and add it to policies that control user access to network resources. You can then add a time-based tag to a username. If the username is tagged, it is a member of the DUG, and the DUG permits network access. When the time-based tag expires, the user's membership in the DUG is terminated along with the network access that the DUG provided.

Module Summary

Now that you have completed this module, you should be able to:

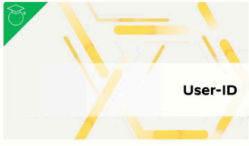
- Identify the purpose and four main components of User-ID
- Identify available IP-to-username mapping methods
- Configure the PAN-OS® integrated agent to connect to monitored servers
- Configure username-to-group name mapping
- Implement User-ID in Security policy

Now that you have completed the module, you should be able to perform the tasks listed.

Additional Resources

For a digital review of this module, log into Beacon and search for:

"User-ID"



Review Questions

1. Which two statements are true regarding User-ID and firewall configuration? (Choose two.)
   a. Communications between the firewall and the User-ID agent are sent over an encrypted SSL connection.
   b. The firewall needs to have information for every User-ID agent to which it will connect.
   c. NetBIOS is the only client-probing method supported by the User-ID agent.
   d. The User-ID agent must be installed on the domain controller.

2. Which three items are valid choices when the **Source User** field is configured in a Security policy rule? (Choose three.)
   a. all
   b. known-user
   c. any
   d. unknown
   e. none

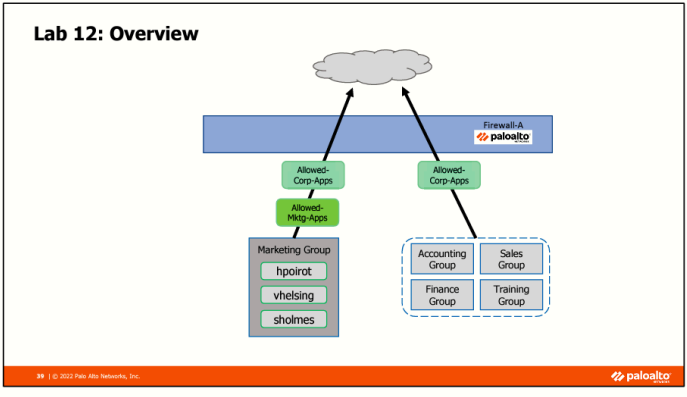
3. Which statement is true regarding User-ID and Security policy rules?
   a. If the user associated with an IP address cannot be determined, all traffic from that address will be dropped.
   b. The **Source User** field can match only users, not groups.
   c. The **Source IP** and **Source User** fields cannot be used in the same policy.
   d. Users can only be used in policy rules if the firewall knows them.

Review Questions

1. Which two statements are true regarding User-ID and firewall configuration? (Choose two.)
   a. Communications between the firewall and the User-ID agent are sent over an encrypted SSL connection.
   b. The firewall needs to have information for every User-ID agent to which it will connect.
   c. NetBIOS is the only client-probing method supported by the User-ID agent.
   d. The User-ID agent must be installed on the domain controller.

2. Which three items are valid choices when the **Source User** field is configured in a Security policy rule? (Choose three.)
   a. all
   b. known-user
   c. any
   d. unknown
   e. none

3. Which statement is true regarding User-ID and Security policy rules?
   a. If the user associated with an IP address cannot be determined, all traffic from that address will be dropped.
   b. The **Source User** field can match only users, not groups.
   c. The **Source IP** and **Source User** fields cannot be used in the same policy.
   d. Users can only be used in policy rules if the firewall knows them.



Your instructor can provide an overview of the lab environment and the details needed for this lab. See the following page for a list of tasks that you will carry out in this lab.

Lab 12: Controlling Access to Network Resources with User-ID

- Examine current configuration
- Enable User-ID technology on the Acquisition zone.
- Generate traffic
- Modify Security policy to meet requirements

Answers to Review Questions

1. a, b
2. b, c, d
3. b (false)
4. d