

USER-ID



EDU-210 Version A
PAN-OS® 9.0

KNOW THE WHO; CONTROL THE WHO

- User-ID overview
- User mapping methods overview
- Configuring User-ID
- PAN-OS® integrated agent configuration
- Windows-based agent configuration
- Configuring group mapping
- User-ID and security policy

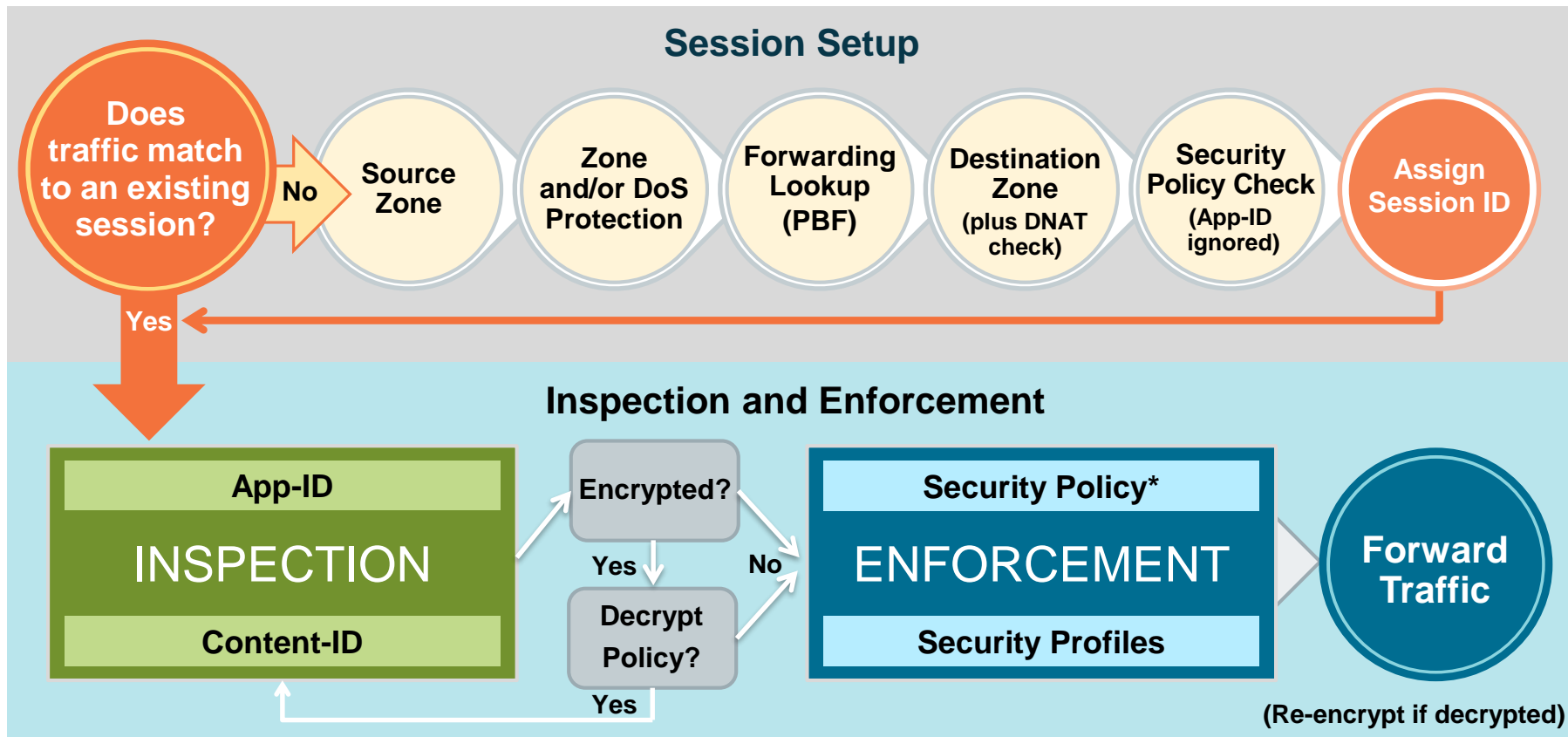
Agenda

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



- Describe the four main components of User-ID
- Describe the differences between the integrated agent and the Windows-based agent
- Define the methods to map IP addresses to users
- Configure the PAN-OS integrated agent to connect to monitored servers
- Configure the Windows-based agent to probe IP addresses for username information

Flow Logic of the Next-Generation Firewall



* Policy check relies on pre-NAT IP addresses



User-ID overview

User mapping methods overview

Configuring User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

User-ID and security policy

User-ID Purpose

- Identify users by username and user group.
- Create policies and display logs and reports based on usernames and group names.

Policies > Security

	Name	Tags	Type	Source			Destination		Application	Service	Action
				Zone	A...	User	Zone	Addr...			
1	egress-outside	egress	universal	inside	any	lab\lab users	outside	any	facebook-base	application-default	Deny
2	egress-public.ftp	egress	universal	inside	any	lab\lab users	outside	any	ftp	application-default	Allow
3	egress-ssl	egress	universal	inside	any	lab\lab users	outside	any	ssl	application-default	Allow

Monitor > Logs > Traffic

	Receive Time	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule
	02/26 20:14:02	inside	outside	192.168.1.20	lab\lab-user	8.8.8.8	53	dns	allow	egress-outside
	02/26 20:11:25	inside	outside	192.168.1.20	lab\lab-user	151.101.2.2	443	ssl	allow	egress-outside
	02/26 20:09:12	inside	outside	192.168.1.20	lab\lab-user	172.217.1.227	443	google-base	allow	egress-outside

User-ID Main Functions

Network Traffic

Group mapping:
Learn group names
and member users
from LDAP

LDAP



Group

IP Address



Username

User mapping:
Associate IP
addresses with
usernames

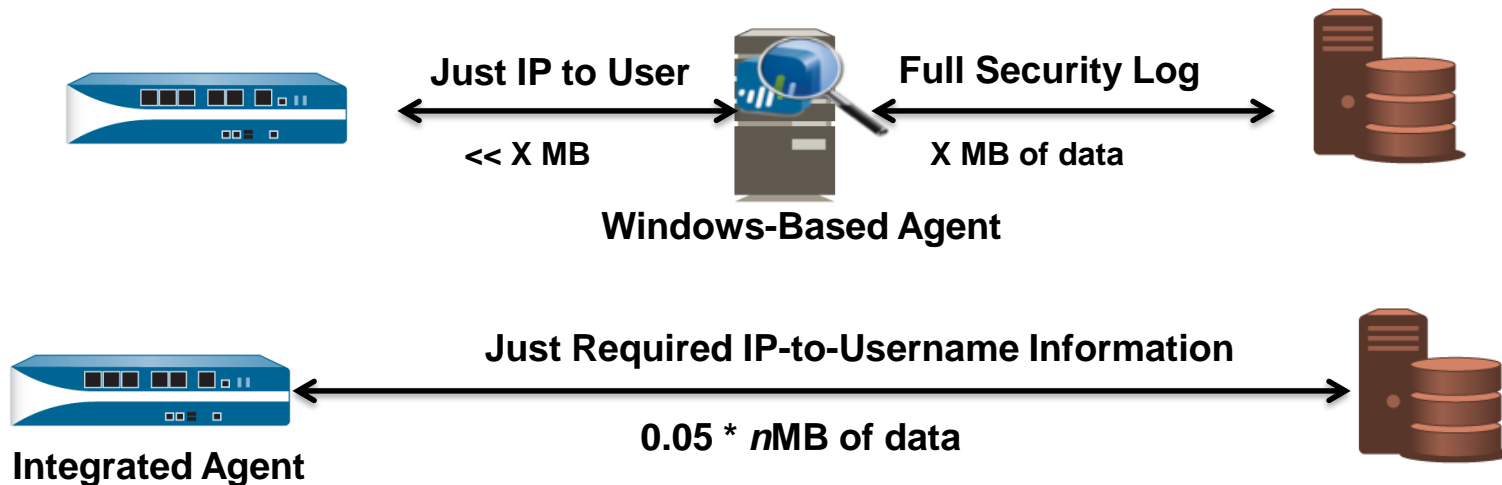
Policy Rules,
Logs, Reports

User-ID Components

Component	Characteristics
Palo Alto Networks firewall	<ul style="list-style-type: none">▪ Maps IP addresses to usernames▪ Maps usernames to group names
PAN-OS integrated User-ID agent	<ul style="list-style-type: none">▪ Runs on the firewall▪ Collects IP address-to-username information
Windows-based User-ID agent	<ul style="list-style-type: none">▪ Runs on a domain member▪ Collects IP address-to-username information▪ Sends information to the firewall
Palo Alto Networks Terminal Services agent	<ul style="list-style-type: none">▪ Runs on Microsoft and Citrix terminal servers▪ Collects IP and port number-to-username information▪ Sends information to firewall

Integrated Agent Versus Windows-Based Agent

- An integrated agent uses network bandwidth more efficiently.
- For remote sites, use an integrated agent or install a Windows-based agent at the site.





User-ID overview

User mapping methods overview

Configuring User-ID

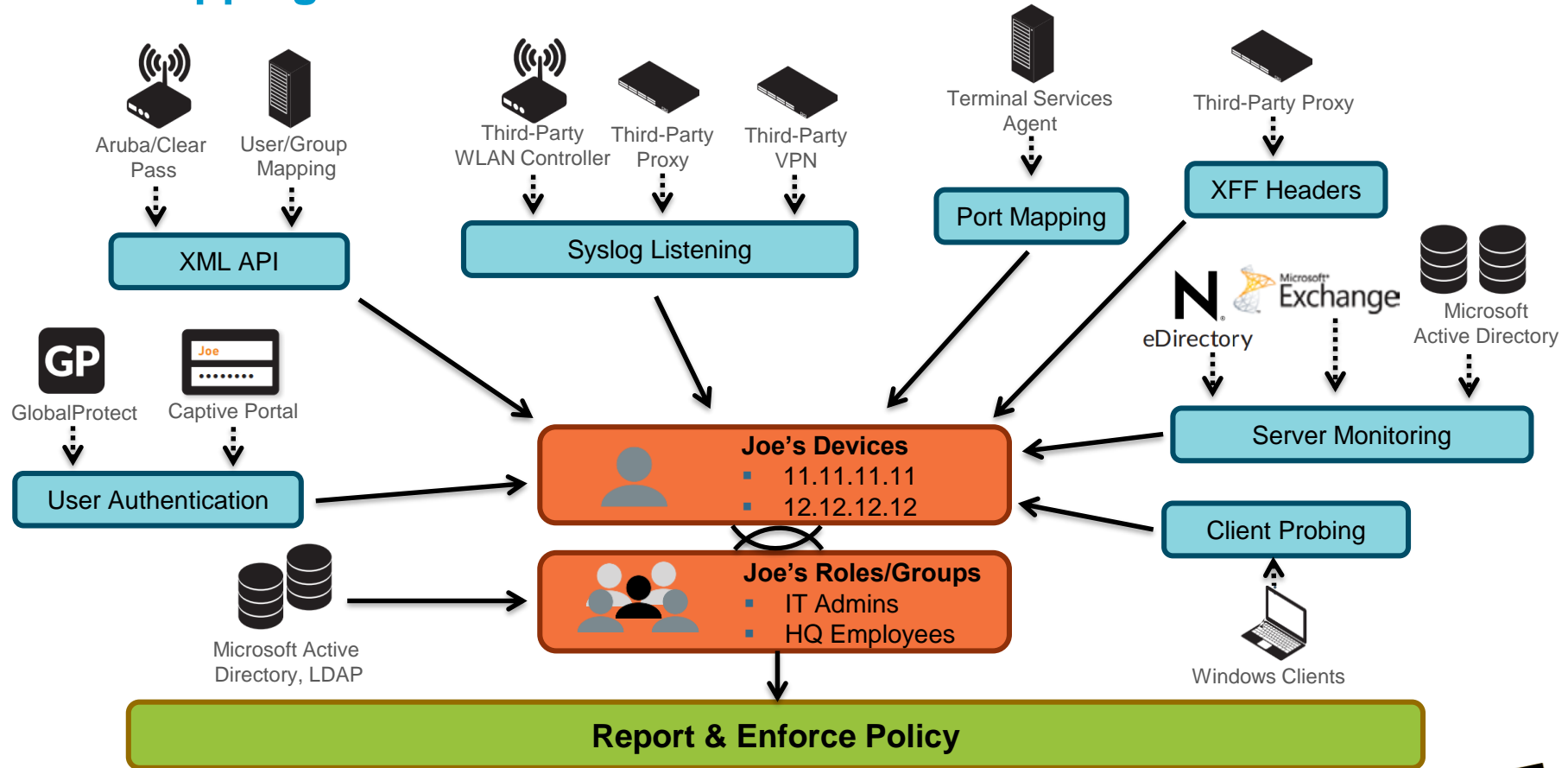
PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

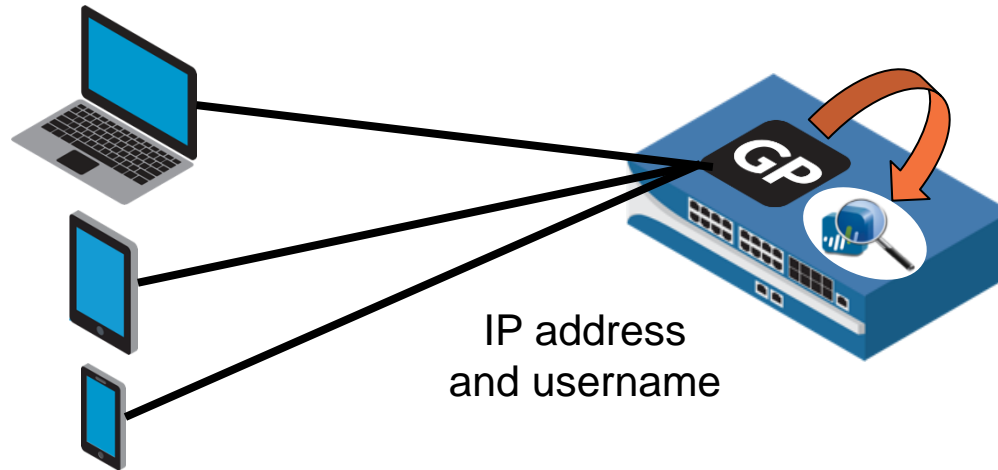
User-ID and security policy

User Mapping Methods



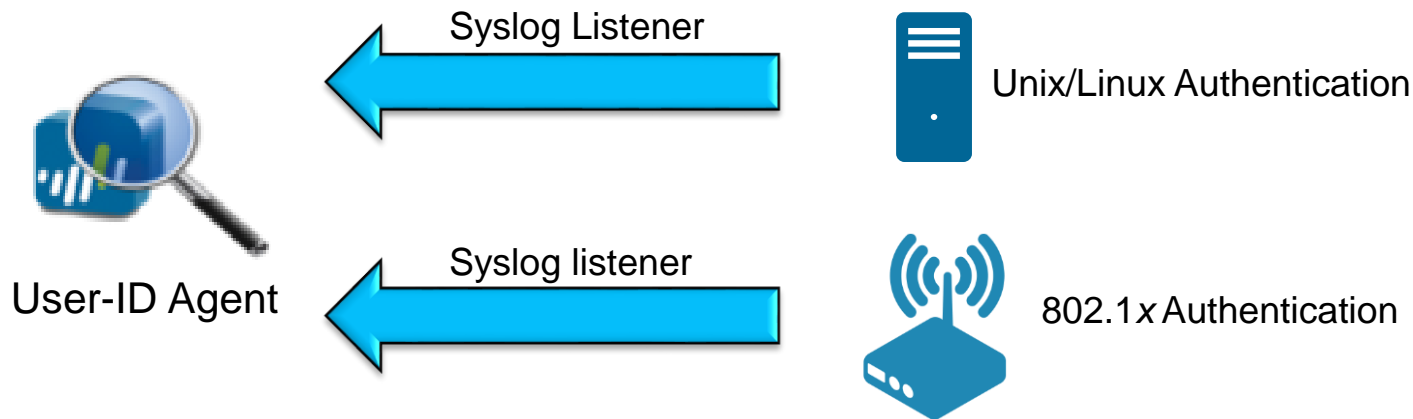
User Mapping Using GlobalProtect

- 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.

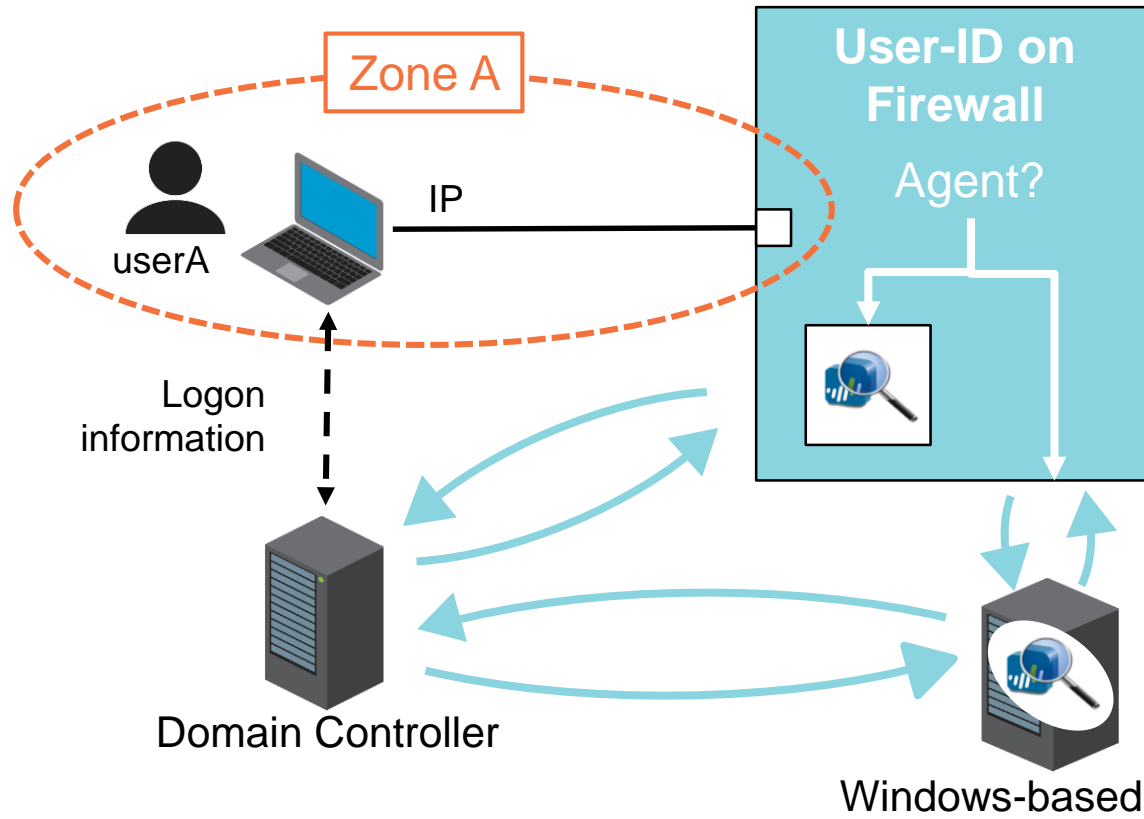


User-ID Syslog Monitoring

- 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.



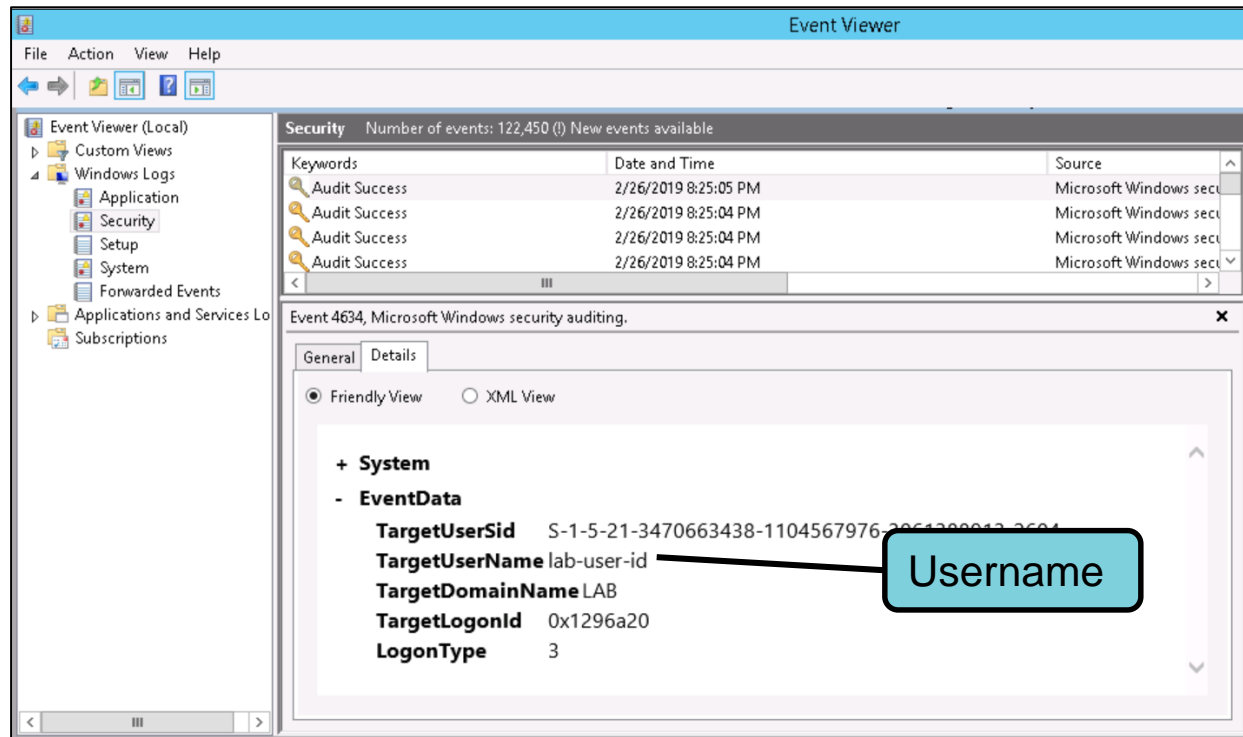
User-ID Operation Overview: Domain Controllers



1. User-ID enabled on zone?
2. Who is agent for domain?
3. Query integrated agent for IP/user information, or
3. Query Windows-based agent for IP/user information
4. Associate IP with user
5. Associate user with group
6. Check Security policy for match

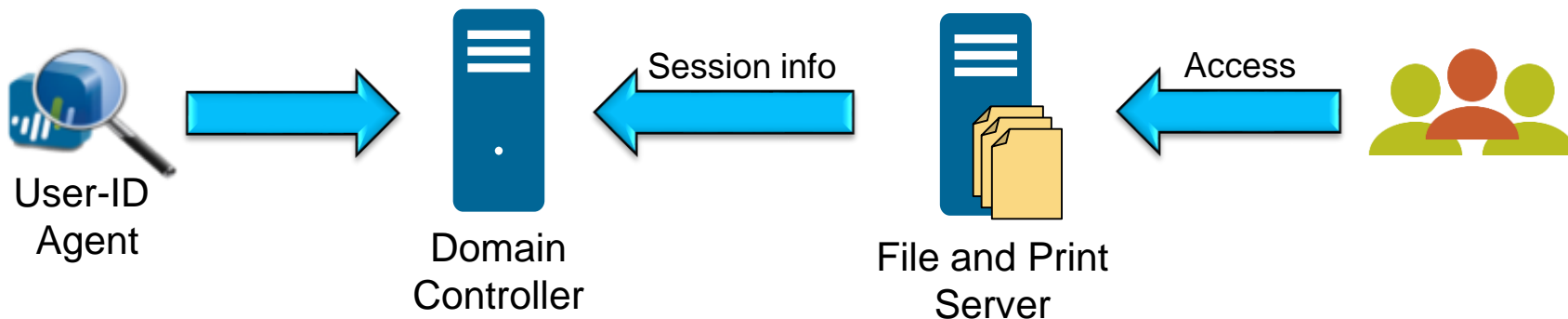
User-ID Domain Controller Monitoring

- Monitors Security logs of Domain Controllers
- Monitors all Domain Controllers per domain to get all logon and logout events



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.



User-ID Mapping Recommendations

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, 802.1x devices, or proxy servers	Syslog listener
Exchange servers, Domain Controllers, or eDirectory servers	User-ID agent: Session 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



User-ID overview

User mapping methods overview

Configuring User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

User-ID and security policy

Configuring User-ID

1. Enable User-ID by zone
2. Configure user mapping methods
3. Configure group mapping (optional)
4. Modify firewall policy rules to use username or group names



Enabling User-ID Per Zone

- Enable User-ID by 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 Lists or Exclude Lists

Network > Zones > <select_zone>

The screenshot shows the configuration page for a Zone named 'inside'. The 'Log Setting' is 'None' and the 'Type' is 'Layer3'. Under the 'Interfaces' section, 'ethernet1/2' is listed. The 'Zone Protection' section shows the 'Zone Protection Profile' set to 'None' and 'Enable Packet Buffer Protection' is unchecked. The 'User Identification ACL' section is highlighted with a red box, showing the 'Enable User Identification' checkbox checked. Below this, there are two lists: 'Include List' and 'Exclude List', both with instructions to select an address or address group. The 'Include List' and 'Exclude List' sections are currently empty.

Zone

Name: inside

Log Setting: None

Type: Layer3

Interfaces

- ethernet1/2

+ Add - Delete

Zone Protection

Zone Protection Profile: None

☐ Enable Packet Buffer Protection

User Identification ACL

☒ Enable User Identification

Include List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Users from these addresses/subnets will be identified.

Exclude List

Select an address or address group or type in your own address. Ex: 192.168.1.20 or 192.168.1.0/24

+ Add - Delete

Users from these addresses/subnets will not be identified.



User-ID overview

User mapping methods overview

Configuring User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

User-ID and security policy

Configuring the PAN-OS Integrated User-ID Agent

1. On the domain controller, create a service account with the required permissions to run the agent
2. On the firewall define the address of the server(s) to be monitored
3. Add the service account to monitor the server(s)
4. Configure session monitoring (optional)
5. Configure WMI probing (optional)
6. Commit the configuration and verify agent connection status



optional

optional



Defining the Monitored Server(s)

Device > User Identification > User Mapping

Server Monitoring			
<input type="checkbox"/>	Name	Enabled	Type



User Identification Monitored Server

Name lab-client

Description

☒ Enabled

Type Microsoft Active Directory

Transport Protocol WinRM-HTTP

The payload is encrypted with Kerberos Security

Network Address client-a.lab.local

Microsoft Active Directory
Microsoft Exchange
Novell eDirectory
Syslog Sender

WMI
WinRM-HTTP
WinRM-HTTPS

- Use **Discover** for domain controllers
- Use **Add** to manually add servers:
 - Required for Exchange, eDirectory, Syslog Sender

Defining the User-ID Agent Account

- 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

The screenshot shows the 'Palo Alto Networks User-ID Agent Setup' configuration page. The 'Server Monitor Account' tab is active. The configuration fields are as follows:

Field	Value
User Name	lab.local\lab-user
Domain's DNS Name	lab.local
Password	*****
Confirm Password	*****
Kerberos Server Profile	lab-kerberos

A gear icon in the top right corner of the configuration area is highlighted with a black arrow.

Optional Session Monitoring

Device > User Identification > User Mapping

The screenshot displays the Palo Alto Networks User-ID Agent Setup interface. At the top, there are tabs for User Mapping, Connection Security, User-ID Agents, Terminal Services Agents, Group Mapping Settings, and Captive Portal Settings. The 'User Mapping' tab is selected. Below the tabs, the page title is 'Palo Alto Networks User-ID Agent Setup'. A gear icon in the top right corner is pointed to by an arrow. Below the title bar, there are sub-tabs: Server Monitor Account, Server Monitor, Client Probing, Cache, NTLM, Redistribution, Syslog Filters, and Ignore User List. The 'Server Monitor' sub-tab is selected. Under the 'Windows Server Monitoring' section, there are two checkboxes: 'Enable Security Log' (checked) and 'Enable Session' (unchecked). The 'Enable Security Log' checkbox is pointed to by an arrow from a callout box stating 'Server monitoring is enabled by default.' The 'Enable Session' checkbox is pointed to by an arrow from a callout box stating 'Click to enable session monitoring.' Below the checkboxes, there are two input fields: 'Server Log Monitor Frequency (sec)' with a value of 2, and 'Server Session Read Frequency (sec)' with a value of 10.

User Mapping | Connection Security | User-ID Agents | Terminal Services Agents | Group Mapping Settings | Captive Portal Settings

Palo Alto Networks User-ID Agent Setup

Palo Alto Networks User-ID Agent Setup

Server Monitor Account | Server Monitor | Client Probing | Cache | NTLM | Redistribution | Syslog Filters | Ignore User List

Windows Server Monitoring

☒ Enable Security Log

Server Log Monitor Frequency (sec) 2

☐ Enable Session

Server Session Read Frequency (sec) 10

Server monitoring is enabled by default.

Click to enable session monitoring.

Optional WMI Client Probing

Device > User Identification > User Mapping

The screenshot displays the 'Palo Alto Networks User-ID Agent Setup' configuration page. At the top, a navigation bar includes tabs for 'User Mapping', 'Connection Security', 'User-ID Agents', 'Terminal Services Agents', 'Group Mapping Settings', and 'Captive Portal Settings'. The 'User Mapping' tab is active. Below this, a sub-header 'Palo Alto Networks User-ID Agent Setup' is followed by a row of configuration tabs: 'Server Monitor Account', 'Server Monitor', 'Client Probing', 'Cache', 'NTLM', 'Redistribution', 'Syslog Filters', and 'Ignore User List'. The 'Client Probing' tab is selected. In this tab, there is a checkbox labeled 'Enable Probing' which is currently unchecked. Below the checkbox is a text field for 'Probe Interval (min)' with the value '20'. A callout box with a black border and a light blue background points to the 'Enable Probing' checkbox, containing the text: 'Integrated agent supports only WMI probing.' Another arrow points from the top right of the configuration area to a gear icon.

User Mapping Connection Security User-ID Agents Terminal Services Agents Group Mapping Settings Captive Portal Settings

Palo Alto Networks User-ID Agent Setup

Palo Alto Networks User-ID Agent Setup

Server Monitor Account Server Monitor Client Probing Cache NTLM Redistribution Syslog Filters Ignore User List

☐ Enable Probing

Probe Interval (min) 20

Integrated agent supports only WMI probing.

Verifying Connection Status

Device > User Identification

Configuration page for User Identification settings. The page includes tabs for User Mapping, Connection Security, User-ID Agents, Terminal Services Agents, Group Mapping Settings, and Captive Portal Settings. The main configuration area lists various settings for User-ID Agents, including Domain's DNS Name, Kerberos Server Profile, Enable Security Log, Server Log Monitor Frequency, Enable Session, Server Session Read Frequency, Novell eDirectory Query Interval, Syslog Service Profile, Enable Probing, Probe Interval, Enable User Identification Timeout, User Identification Timeout, Allow matching usernames without domains, Enable NTLM, NTLM Domain, and User-ID Collector Name. A Server Monitoring table at the bottom shows the status of connected devices.

Domain's DNS Name: lab.local
Kerberos Server Profile: lab-kerberos
Enable Security Log: ☒
Server Log Monitor Frequency (sec): 2
Enable Session: ☒
Server Session Read Frequency (sec): 10
Novell eDirectory Query Interval (sec): 30
Syslog Service Profile
Enable Probing: ☒
Probe Interval (min): 20
Enable User Identification Timeout: ☒
User Identification Timeout (min): 45
Allow matching usernames without domains: ☐
Enable NTLM: ☐
NTLM Domain
User-ID Collector Name

Server Monitoring

Name	Enabled	Type	Network Address	Status
lab-client	<input checked="" type="checkbox"/>	Microsoft Active Directory	client-a.lab.local	Connected



User-ID overview

User mapping methods overview

Configuring User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

User-ID and security policy

Configuring the Windows-Based User-ID Agent

1. On the Domain Controller, create a service account with the required permissions to run the agent
2. Select a Windows domain member
3. Download and install User-ID agent software
4. Run the User-ID agent installer
5. Configure the User-ID agent
6. Configure the firewall to connect to the User-ID agent
7. Verify connection status



Selecting the Installation Location

- Install on the domain member:
 - Microsoft Windows XP SP3 or later
 - 32-bit and 64-bit are supported
 - Install close to the servers it will be monitoring to optimize bandwidth use
 - Install agents on two domain members for redundancy



Download User-ID Agent Software

- Download the Windows agent from <https://support.paloaltonetworks.com>
- Install the agent

CUSTOMER SUPPORT ▾

What are you looking for?

Current Account: Palo Alto Networks

Support Home

Support Cases

Company Account

Members ▾

Assets ▾

Tools ▾

WildFire ▾

AutoFocus

Updates ▴

Dynamic Updates

Software Updates

Filter By: User Identification Agent ▾

Filter list for User-ID agent downloads

Version	Release Date ▾	Release Notes	Download	Size	Checksum
▾ User Identification Agent					
9.0.0-0	02/11/2019	User-ID_Agent-9.0.0-RN.pdf	UaInstall-9.0.0-0.msi	3.3 MB	Checksum
9.0.0-0	02/11/2019	User-ID_Agent-9.0.0-RN.pdf	UaCredInstall64-9.0.0-0.msi	2.7 MB	Checksum
8.1.7-5	02/09/2019	User-ID_Agent-8.1.7-RN.pdf	UaCredInstall64-8.1.7-5.msi	2.8 MB	Checksum
8.1.7-5	02/09/2019	User-ID_Agent-8.1.7-RN.pdf	UaInstall-8.1.7-5.msi	3.3 MB	Checksum
8.1.6-4	12/26/2018	User-ID_Agent-8.1.6-RN.pdf	UaCredInstall64-8.1.6-4.msi	2.7 MB	Checksum
8.1.6-4	12/26/2018	User-ID_Agent-8.1.6-RN.pdf	UaInstall-8.1.6-4.msi	3.3 MB	Checksum

Agent Setup Process

The screenshot shows the 'Palo Alto Networks User-ID Agent' application window. The interface includes a menu bar with 'File' and 'Help'. On the left is a navigation pane with icons for 'User Identification', 'Discovery', 'VM Information Sources', 'Monitoring', 'Logs', 'Server Certificate', 'MDM Integration', 'Setup', and 'Mobile Devices'. The 'Setup' option is highlighted. In the center is a table of configuration settings. To the right of the table are 'Save', 'Commit', and 'Exit' buttons. Below the table is an 'Edit' button and an 'Access Control List' section with a table header. A callout box points to the 'User-ID Service TCP Port' value.

1 → User Identification Setup

2 → Edit

3 → Save, Commit, Exit

Setup	
Service Logon Account Username for Active Directory	lab-user-id@LAB.LOCAL
Enable Security Log Monitor	Yes
Security Log Monitor Frequency (sec.)	1
Enable Server Session Read	No
Server Session Read Frequency (sec.)	10
Novell eDirectory Query Interval (sec.)	30
Enable WMI Probing	No
Enable NetBIOS Probing	No
WMI/NetBIOS Probing Interval (min.)	20
Enable User Identification Timeout	No
User Identification Timeout (min.)	45
User-ID Service TCP Port	5007

Defaults to TCP port 5007

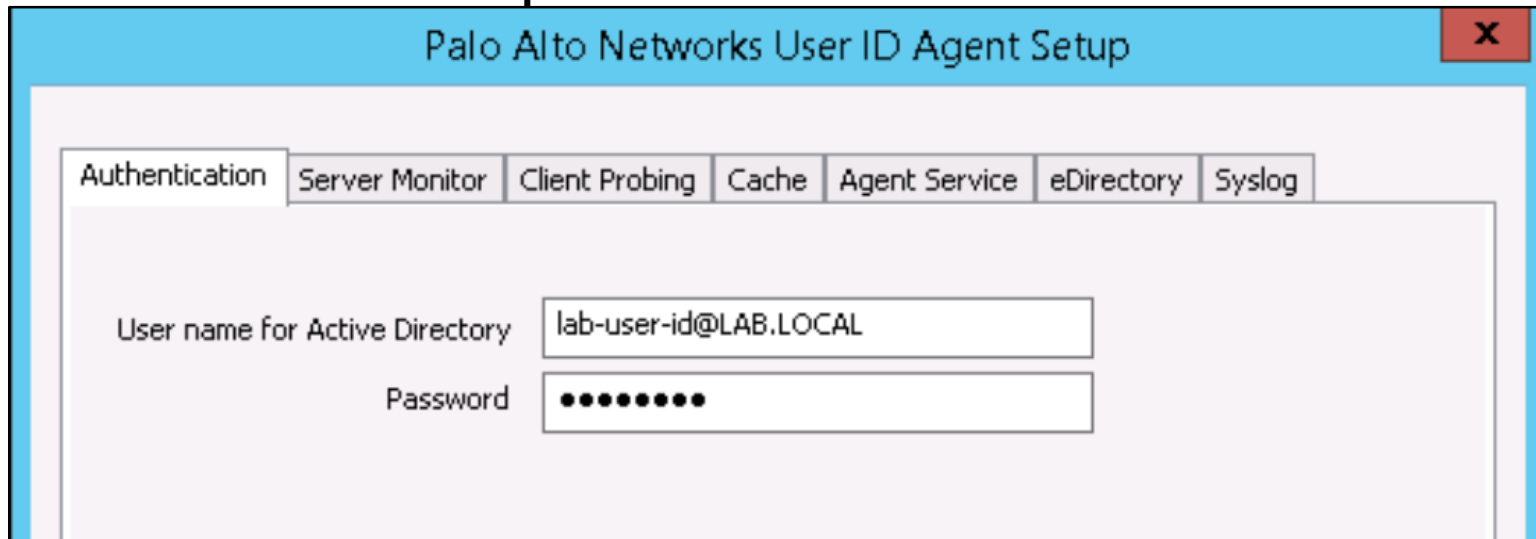
Access Control List

Name	Action	From IP Address	To IP Address

Configuring the User-ID Agent Account

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

User Identification > Setup > Edit



The screenshot shows the 'Palo Alto Networks User ID Agent Setup' window with the 'Edit' tab selected. The window has a blue title bar and a red close button. Below the title bar is a tabbed interface with the following tabs: Authentication (selected), Server Monitor, Client Probing, Cache, Agent Service, eDirectory, and Syslog. The 'Authentication' tab contains two input fields: 'User name for Active Directory' with the value 'lab-user-id@LAB.LOCAL' and 'Password' with a masked value represented by ten dots.

Palo Alto Networks User ID Agent Setup

Authentication | Server Monitor | Client Probing | Cache | Agent Service | eDirectory | Syslog

User name for Active Directory: lab-user-id@LAB.LOCAL

Password: ••••••••••

Configuring Server Monitoring

User Identification > Setup > Edit

Palo Alto Networks User ID Agent Setup

Authentication | **Server Monitor** | Client Probing | Cache | Agent Service | eDirectory | Syslog

Windows Server Monitoring

☒ Enable Security Log Monitor Enabled by default

Security Log Monitor Frequency (seconds)

☐ Enable Server Session Read Enable session monitoring (optional).

Server Session Read Frequency (seconds)

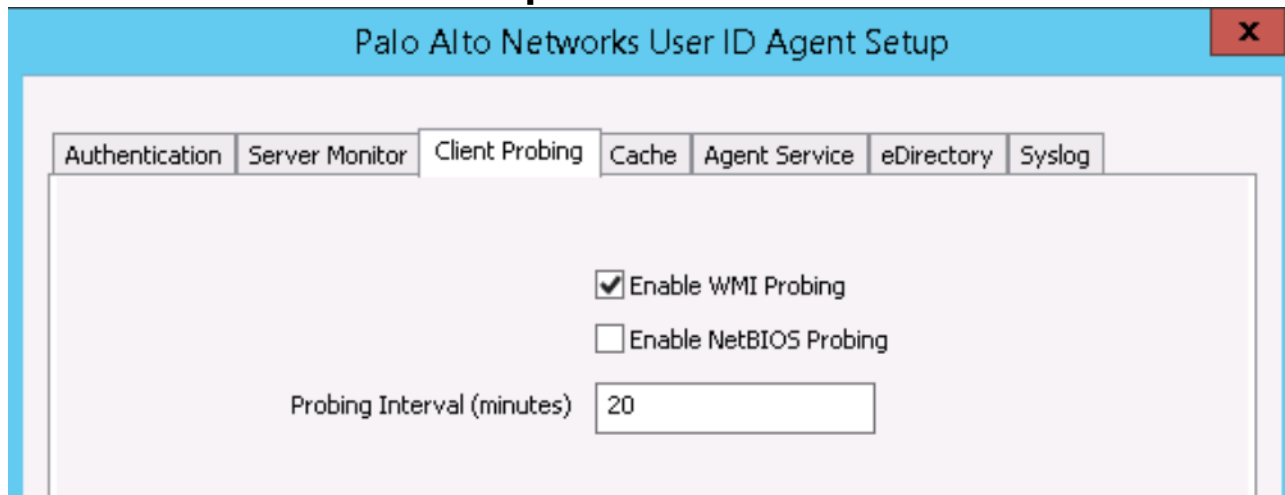
Novell eDirectory Monitoring

Novell eDirectory Query Interval (seconds)

Configuring Client Probing

- Optional NetBIOS client probing requires:
 - Access through Windows firewall to port 139
 - File and print services enabled
- NetBIOS does not require Windows authentication.

User Identification > Setup > Edit



The screenshot shows the 'Palo Alto Networks User ID Agent Setup' window with the 'Client Probing' tab selected. The window has a blue title bar and a red close button. The 'Client Probing' tab is active, showing two checkboxes: 'Enable WMI Probing' (checked) and 'Enable NetBIOS Probing' (unchecked). Below these is a text field for 'Probing Interval (minutes)' with the value '20'.

Authentication	Server Monitor	Client Probing	Cache	Agent Service	eDirectory	Syslog
		<input checked="" type="checkbox"/> Enable WMI Probing				
		<input type="checkbox"/> Enable NetBIOS Probing				
		Probing Interval (minutes) 20				

Configuring the Monitored Servers

The screenshot shows the Palo Alto Networks User-ID Agent configuration window. The left sidebar contains a tree view with the following items: User Identification, Setup, Discovery, VM Information Sources, Monitoring, Logs, Server Certificate, and MDM Integration. The main area is titled 'Servers' and contains a table with the following data:

Name	Type	Network Address
<input type="checkbox"/> lab-client	active-directory	192.168.1.20
<input type="checkbox"/> lab-client1	edirectory	192.168.1.21
<input type="checkbox"/> mail-server	exchange	192.168.1.22

Below the table are buttons for 'Add', 'Edit', 'Delete', and 'Auto Discover'. At the bottom, there is a section titled 'Include / Exclude list of configured networks' with a table that has columns for 'Name', 'Discovery', and 'Network Address'.

Annotations:

- A callout box on the left says: "Manually add Domain Controllers, Exchange, eDirectory, and syslog senders." with an arrow pointing to the 'Add' button.
- A callout box on the right says: "Domain Controllers only" with an arrow pointing to the 'lab-client' and 'lab-client1' entries in the table.

Configuring the Firewall to Connect to the Agent

Device > User Identification > User-ID Agents > Add

User-ID Agent

Name

Add an Agent Using ☐ Serial Number ☒ Host and Port

Host

Port

☐ Use as LDAP Proxy

☐ Use for NTLM Authentication

User-ID Collector Name

User-ID Collector Pre-Shared Key

Confirm User-ID Collector Pre-Shared Key

☒ Enabled

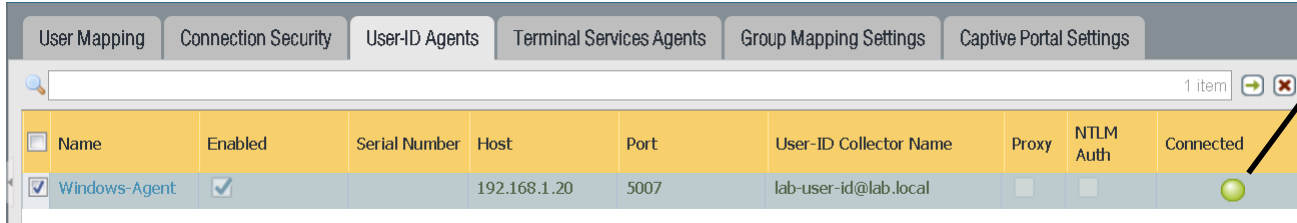
☐ HIP Report

For Windows agents

Windows machine's
IP address and port

Confirm Connection to the User-ID Agent

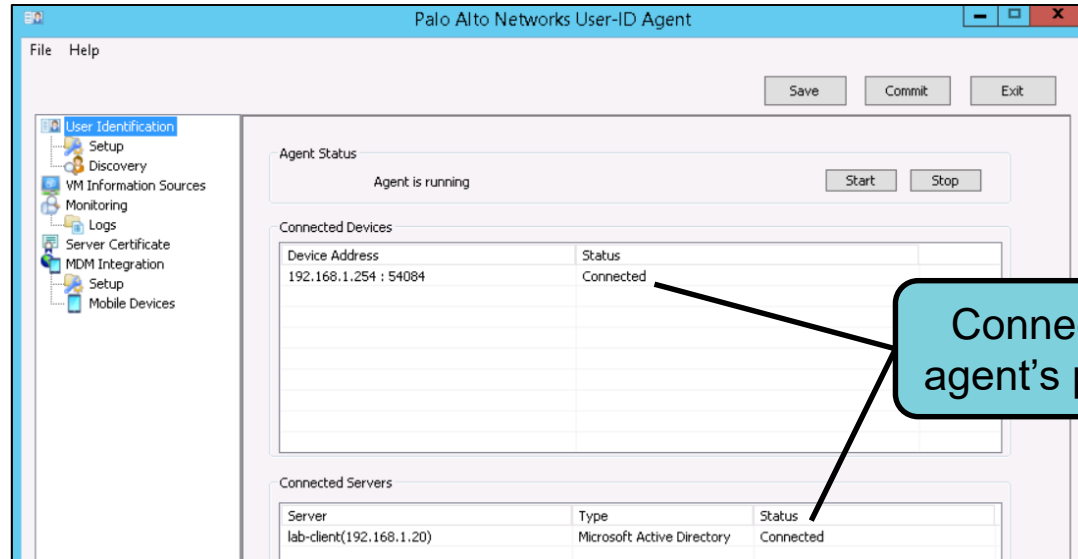
Device > User Identification



The screenshot shows the 'User-ID Agents' tab in the Palo Alto Networks configuration interface. A table lists the configured agents. One agent, 'Windows-Agent', is shown with a green status indicator in the 'Connected' column, signifying a successful connection from the firewall's perspective.

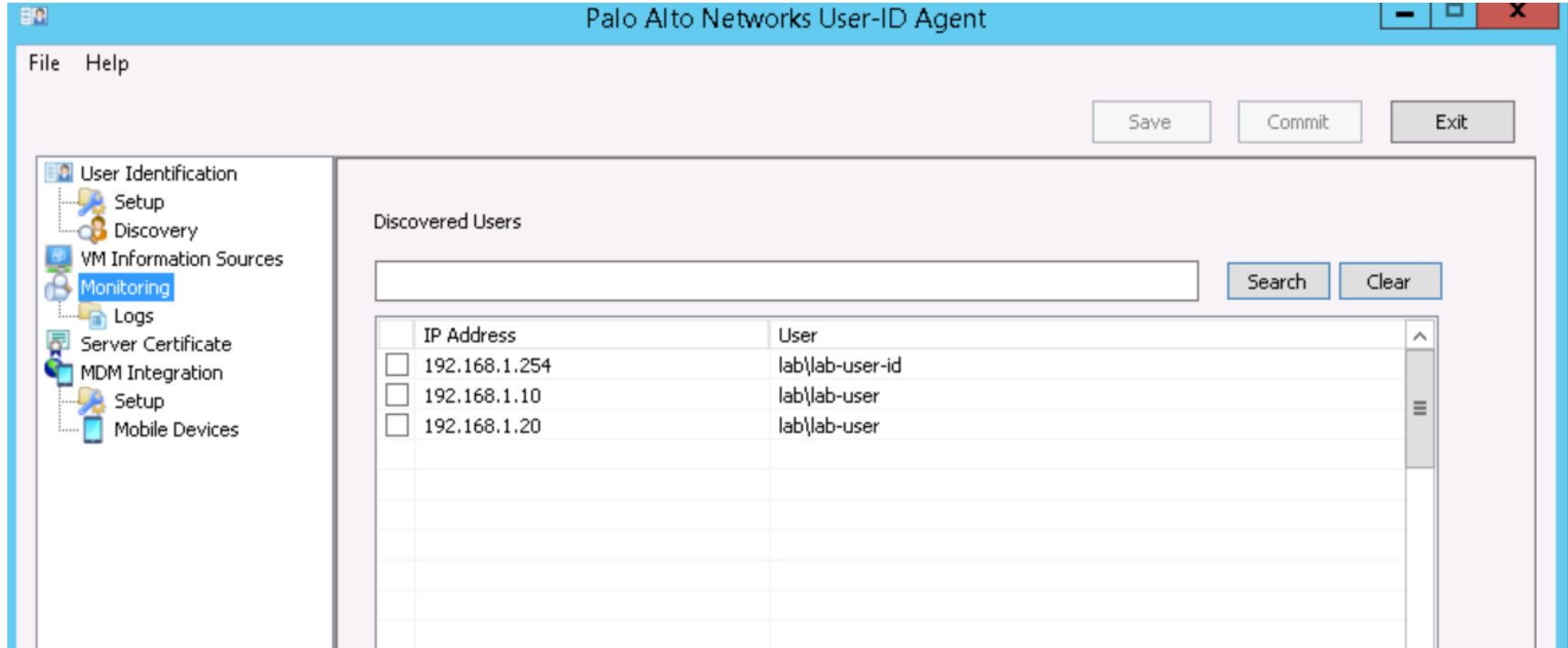
<input type="checkbox"/>	Name	Enabled	Serial Number	Host	Port	User-ID Collector Name	Proxy	NTLM Auth	Connected
<input checked="" type="checkbox"/>	Windows-Agent	<input checked="" type="checkbox"/>		192.168.1.20	5007	lab-user-id@lab.local	<input type="checkbox"/>	<input type="checkbox"/>	

Connection from
firewall's
perspective –
green is good



Connection from
agent's perspective

Display Mappings from the Windows Agent



The screenshot displays the Palo Alto Networks User-ID Agent application window. The title bar reads "Palo Alto Networks User-ID Agent". The menu bar includes "File" and "Help". On the right side of the window, there are three buttons: "Save", "Commit", and "Exit".

The left sidebar contains a tree view with the following items:

- User Identification
 - Setup
 - Discovery
- VM Information Sources
- Monitoring (highlighted)
- Logs
- Server Certificate
- MDM Integration
 - Setup
- Mobile Devices

The main area is titled "Discovered Users". It features a search bar with a "Search" button and a "Clear" button. Below the search bar is a table with two columns: "IP Address" and "User".

	IP Address	User
<input type="checkbox"/>	192.168.1.254	lab\lab-user-id
<input type="checkbox"/>	192.168.1.10	lab\lab-user
<input type="checkbox"/>	192.168.1.20	lab\lab-user
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		
<input type="checkbox"/>		

Display Mappings from the Firewall CLI

- Show mapping for all or specific IP addresses

```
admin@FW-08> show user ip-user-mapping all
```

IP	Vsys	From	User	IdleTimeout (s)	MaxTimeout (s)
10.5.5.13	vsys1	UIA	edupanw\student03	585	585
10.5.5.17	vsys1	UIA	edupanw\student07	2440	2440
172.16.1.8	vsys1	UIA	edupanw\useridagent	1336	1336
10.5.5.7	vsys1	UIA	edupanw\useridagent	2660	2660
192.168.8.254	vsys1	Unknown	unknown	1	4
10.5.5.11	vsys1	UIA	edupanw\student01	1367	1367
10.5.5.16	vsys1	UIA	edupanw\student07	1417	1417
10.5.5.18	vsys1	UIA	edupanw\student08	2573	2573
10.5.5.19	vsys1	UIA	edupanw\administrator	1366	1366
10.5.5.8	vsys1	UIA	edupanw\pwdap	902	902
Total: 10 users					

User-ID overview

User mapping methods overview

Configuring User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration



Configuring group mapping

User-ID and security policy

LDAP Server Profile

Device > Server Profiles > LDAP > Add



LDAP Server Profile

Profile Name: PAN-Training-AD

☐ Administrator Use Only

Server list

Name	LDAP Server	Port
DC1	10.5.5.60	389

 Add  Del

Enter the IP address or FQDN of the LDAP server

Server settings

Type: active-directory

Base DN: DC=edupanw,DC=com

Bind DN: pwldap@edupanw.com

Password:

Confirm Password:

Bind Timeout: 30

Search Timeout: 30

Retry Interval: 60

☒ Require SSL/TLS secured connection

☐ Verify Server Certificate for SSL sessions

Where and how to search the LDAP directory tree

Where to connect

active-directory
e-directory
sun
other

Creating User-ID Group Mapping Filters

Device > User Identification > Group Mapping Settings > Add

The screenshot shows the 'Group Mapping' configuration window. At the top, the 'Name' field is set to 'LDAP Username Formats'. Below this are three tabs: 'Server Profile', 'User and Group Attributes', 'Group Include List', and 'Custom Group'. The 'Server Profile' tab is active, showing a dropdown menu for 'Server Profile' with 'lab-active-directory' selected, and an 'Update Interval' field with the value '[60 - 86400]'. A callout box points to the 'Server Profile' dropdown with the text 'Select LDAP Server Profile.'.

Below the 'Server Profile' section are three expandable sections: 'Domain Setting', 'Group Objects', and 'User Objects'. The 'Domain Setting' section has a 'User Domain' field. The 'Group Objects' section has a 'Search Filter' field and an 'Object Class' dropdown set to 'group'. The 'User Objects' section has a 'Search Filter' field and an 'Object Class' dropdown set to 'person'. A large callout box with a bracket spanning the 'Group Objects' and 'User Objects' sections contains the text 'Dynamically populated based on LDAP server type'.

At the bottom of the window, there are two checkboxes: 'Enabled' (checked) and 'Fetch list of managed devices' (unchecked).

Multiple Username Formats

Device > User Identification > Group Mapping

Group Mapping

Name: LDAP Username Formats

Server Profile | User and Group Attributes | Group Include List | Custom Group

User Attributes

Name	Directory Attribute
Primary Username	sAMAccountName
E-Mail	mail
Alternate Username 1	userPrincipalName
Alternate Username 2	
Alternate Username 3	

Specify primary username attribute.

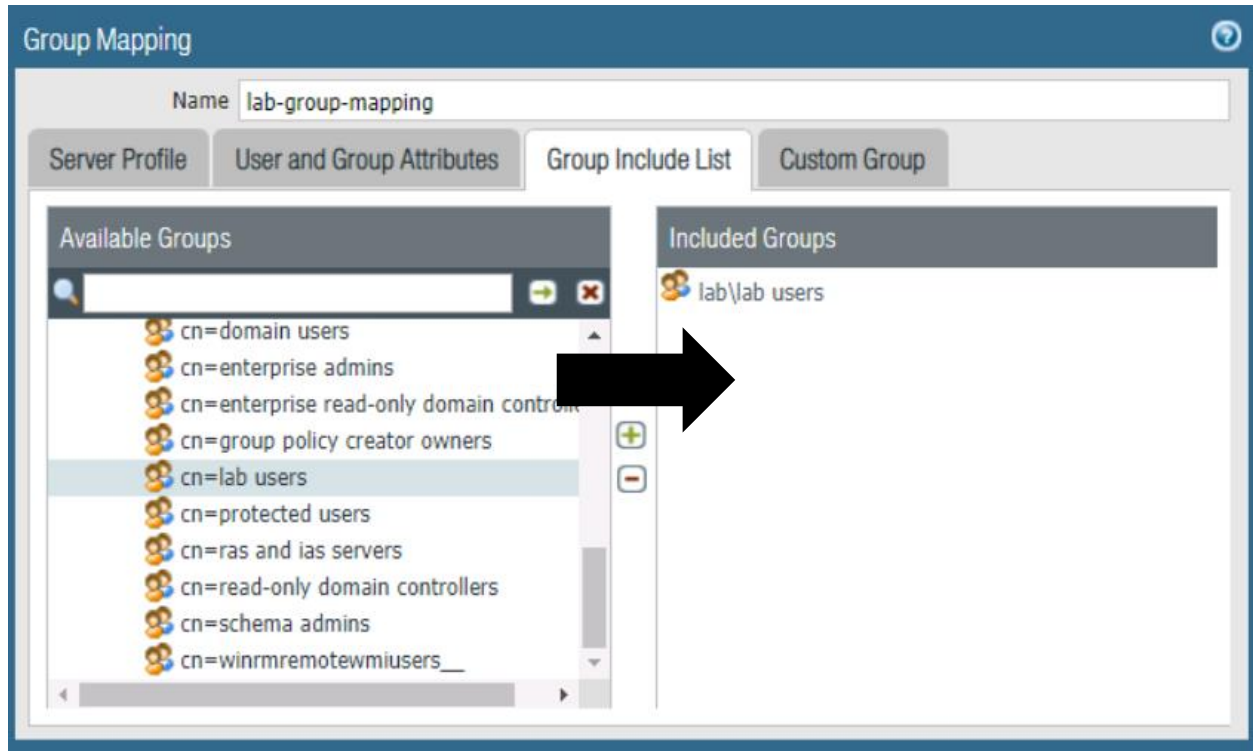
Specify up to three alternate attributes.

Group Attributes

Name	Directory Attribute
Group Name	name
Group Member	member
E-Mail	mail

Filtering 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.

Custom Groups Based on LDAP Filters

Device > User Identification > Group Mapping Settings > Add

The screenshot shows the 'Group Mapping' configuration window. At the top, the 'Name' field is set to 'lab-group-mapping'. Below this are four tabs: 'Server Profile', 'User and Group Attributes', 'Group Include List', and 'Custom Group'. The 'Custom Group' tab is selected. Inside this tab, there is a table with two columns: 'Name' and 'LDAP Filter'. The table contains one item: 'Marketing Group' with the LDAP filter '(department=Marketing)'. At the bottom of the window, there are three buttons: 'Add', 'Delete', and 'Clone'.

Name	LDAP Filter
Marketing Group	(department=Marketing)

- Define custom LDAP filters that select group members.
- Assign a custom filter a group name.
- Use a group name in policy rules.

User-ID overview

User mapping methods overview

Configuring User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

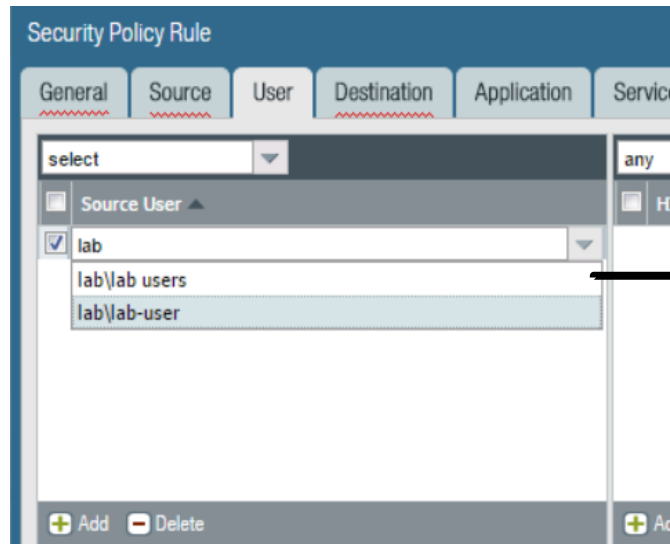
Configuring group mapping

User-ID and security policy



Selecting Users and Groups for a Security Policy

	Name	Tags	Type	Source				Destination		Rule Usage				Application	Service	Action
				Zone	Address	User	HIP Profile	Zone	Address	Hit Co...	L... Hit	First Hit	URL Cate...			
1	egress-public	inter...	unive...	🏠 inside	any	👤 lab\lab-user	any	🏠 outside	💻 203.0.1...	-	-	-	any	📘 facebook	any	🚫 Deny
2	egress-public-ftp	inter...	unive...	🏠 inside	any	👤 lab\lab-user	any	🏠 outside	any	-	-	-	any	📘 ftp	🔧 applicatio...	✅ Allow



- Source User options:
 - any
 - pre-logout
 - known-user
 - unknown
 - select

Module Summary



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

- Describe the four main components of User-ID
- Describe the differences between the integrated agent and the Windows-based agent
- Define the methods to map IP addresses to users
- Configure the PAN-OS integrated agent to connect to monitored servers
- Configure the Windows-based agent to probe IP addresses for username information

Questions?



User-ID Lab (Pages 170-182 in the Lab Guide)

- Load a firewall lab configuration
- Enable User-ID on a security zone
- Configure group mapping
- Configure an integrated User-ID agent
- Configure a Security policy rule to use User-ID

PROTECTION. DELIVERED.



This page intentionally left blank