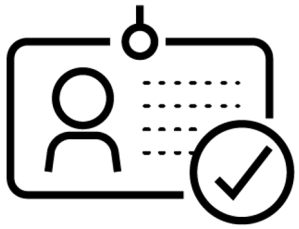
BLOCK THREATS BY IDENTIFYING USERS



KNOW THE WHO, CONTROL THE WHO

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

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 the Windows-based agent to probe IP addresses for username information
- Configure username-to-group name mapping
- Implement User-ID in Security policy

User-ID overview

User mapping methods overview

Configure User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configure group mapping

User-ID and Security policy

paloalto NETWORKS

User-ID Purposes

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

Policies > Security

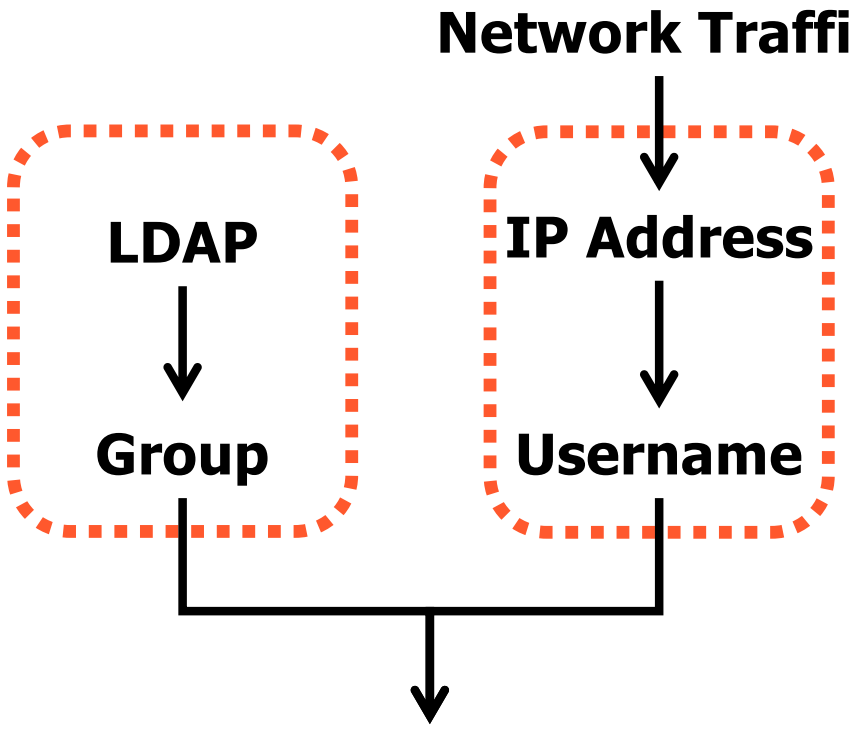
	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	Users_to_Extranet	Users_Net	universal	Users_Net	any	lab\lab users	any	Extranet	any	any	ssl web-browsing	application-default	Allow
2	Users_to_Internet	Users_Net	universal	Users_Net	any	lab\lab users	any	Internet	any	any	any	application-default	Allow
3	Danger-Simulated-Tr...	Danger	universal	Danger	any	lab\lab users	any	Danger	any	any	any	application-default	Allow

Monitor > Logs > Traffic

		RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	TO PORT	APPLICATION	ACTION	RULE
		07/22 22:39:12	end	Users_Net	Internet	192.168.1.254	lab\lab-user-id	107.178.249.217	443	paloalto-updates	allow	Users_to_Internet
		07/22 22:36:27	end	Users_Net	Internet	192.168.1.254	lab\lab-user-id	35.190.82.33	443	paloalto-updates	allow	Users_to_Internet
		07/22 22:34:06	end	Users_Net	Internet	192.168.1.254	lab\lab-user-id	107.178.249.217	443	paloalto-updates	allow	Users_to_Internet

User-ID Main Functions

Group Mapping:
Learn group names and member users from LDAP.



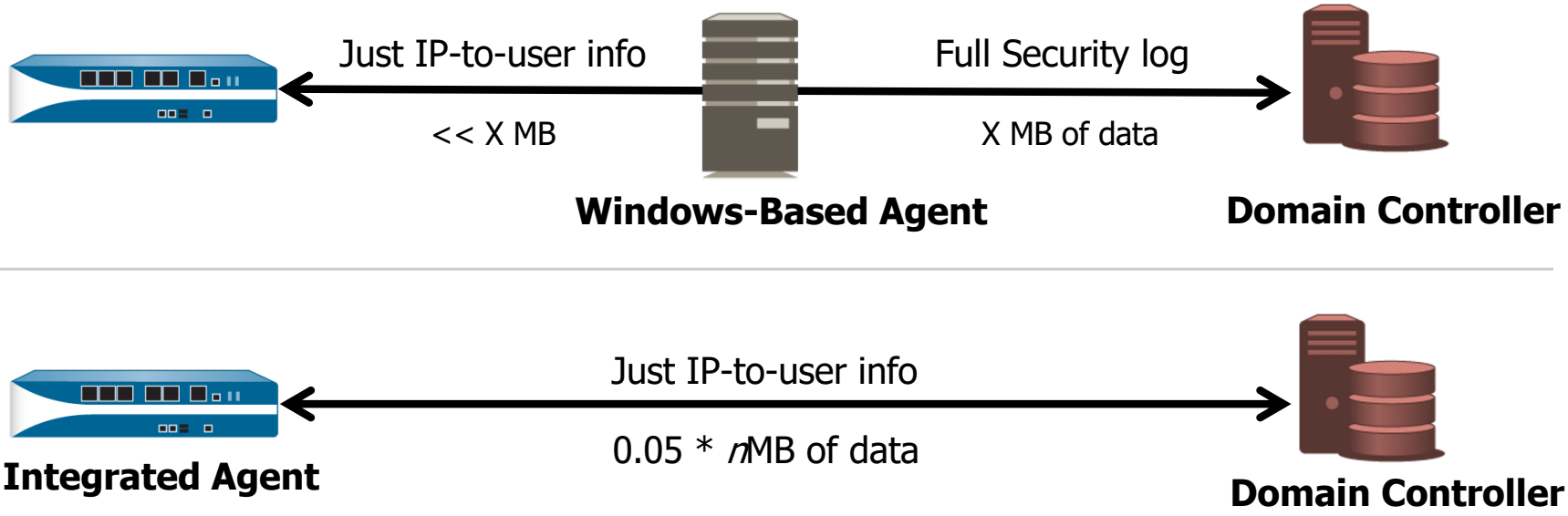
User Mapping:
Associate IP addresses with usernames.

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

Integrated Agent Versus Windows-Based Agent

- An integrated agent uses network bandwidth more efficiently.
- For remote sites:
  - Use an integrated agent at the local site, or
  - Install a Windows-based agent at the site.



User-ID overview

User mapping methods overview

Configure User-ID

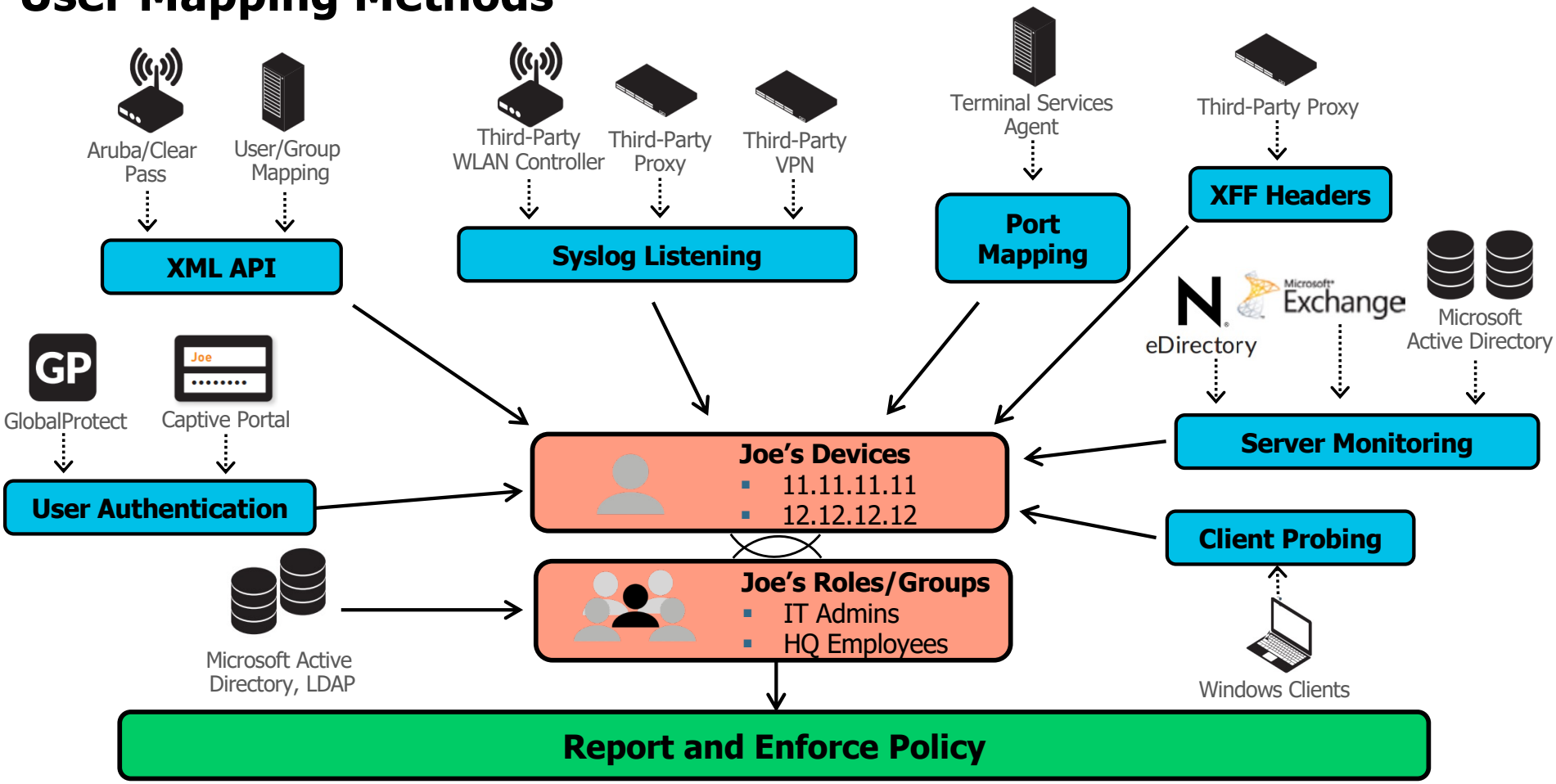
PAN-OS integrated agent configuration

Windows-based agent configuration

Configure group mapping

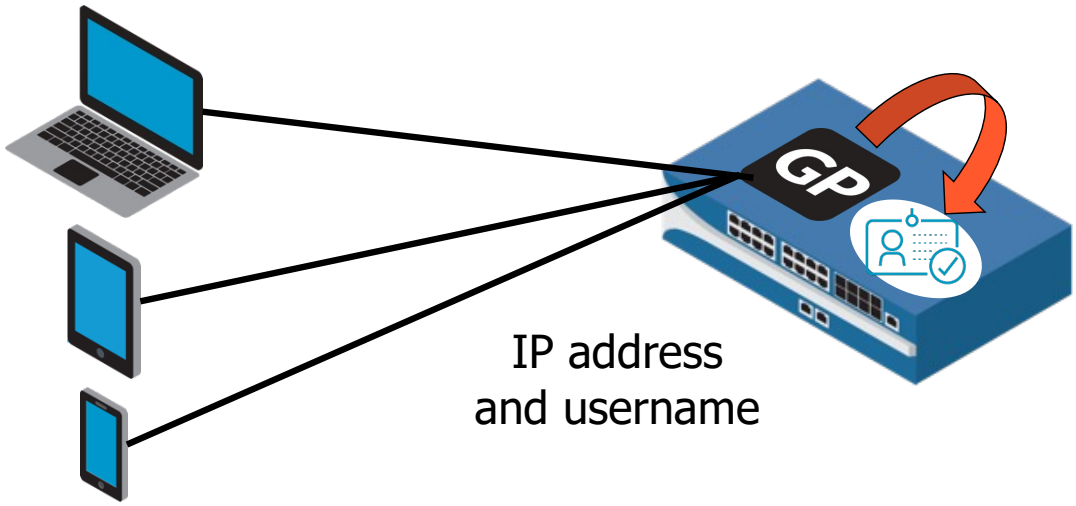
User-ID and Security policy

User Mapping Methods



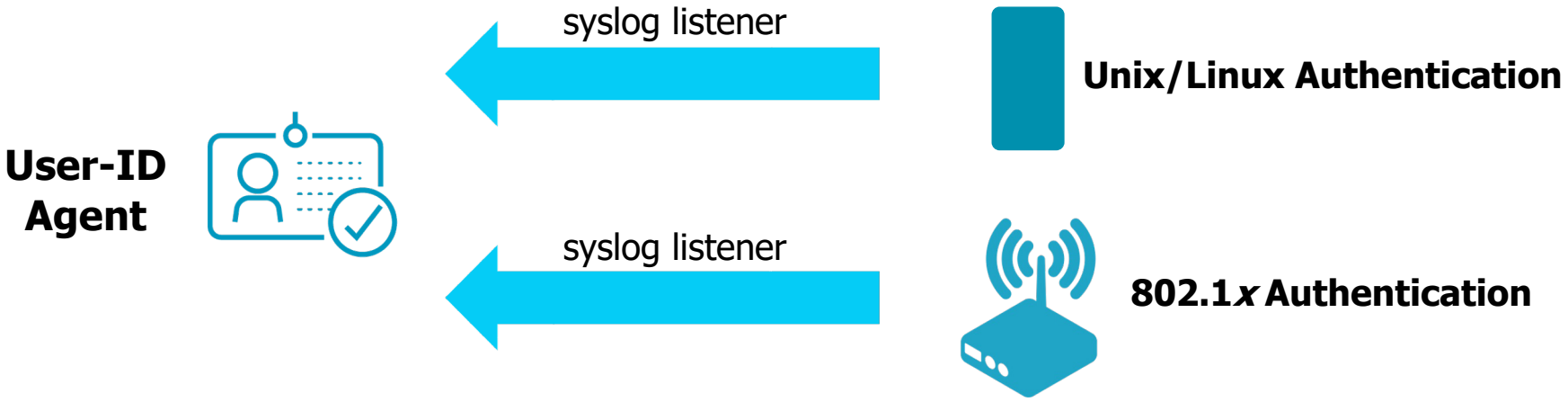
User Mapping Using GlobalProtect

- 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.

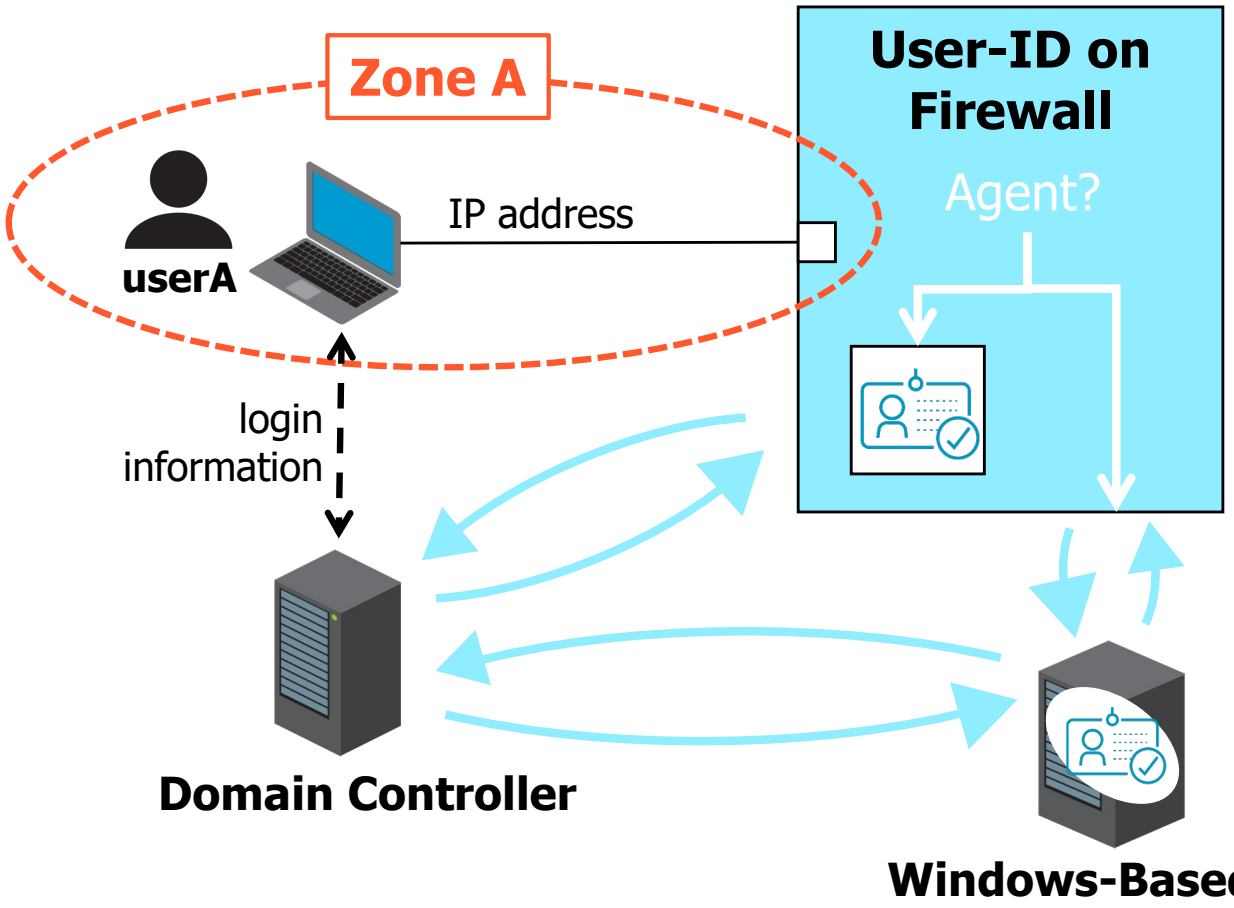


User-ID Syslog Monitoring

- 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.



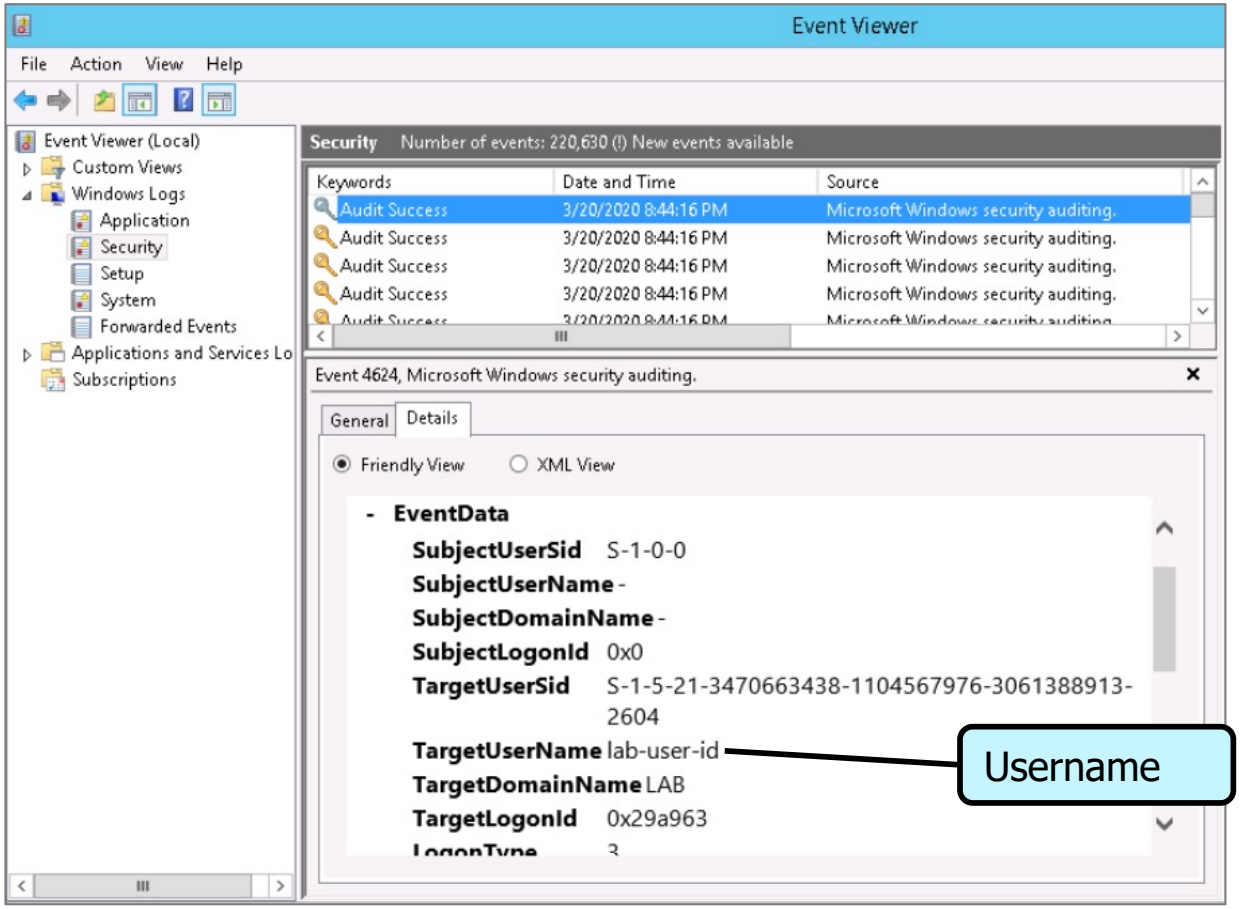
User-ID Operation Overview: Domain Controllers



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

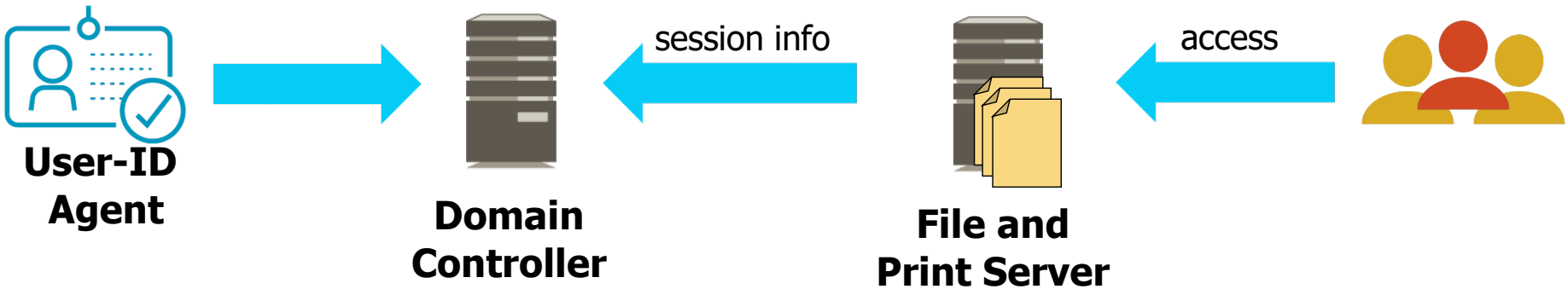
User-ID Domain Controller Monitoring

- Monitors Security logs of domain controllers
- Monitors all domain controllers per domain to get all login 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, 802.1*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

User-ID overview

User mapping methods overview

Configure User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configure group mapping

User-ID and Security policy

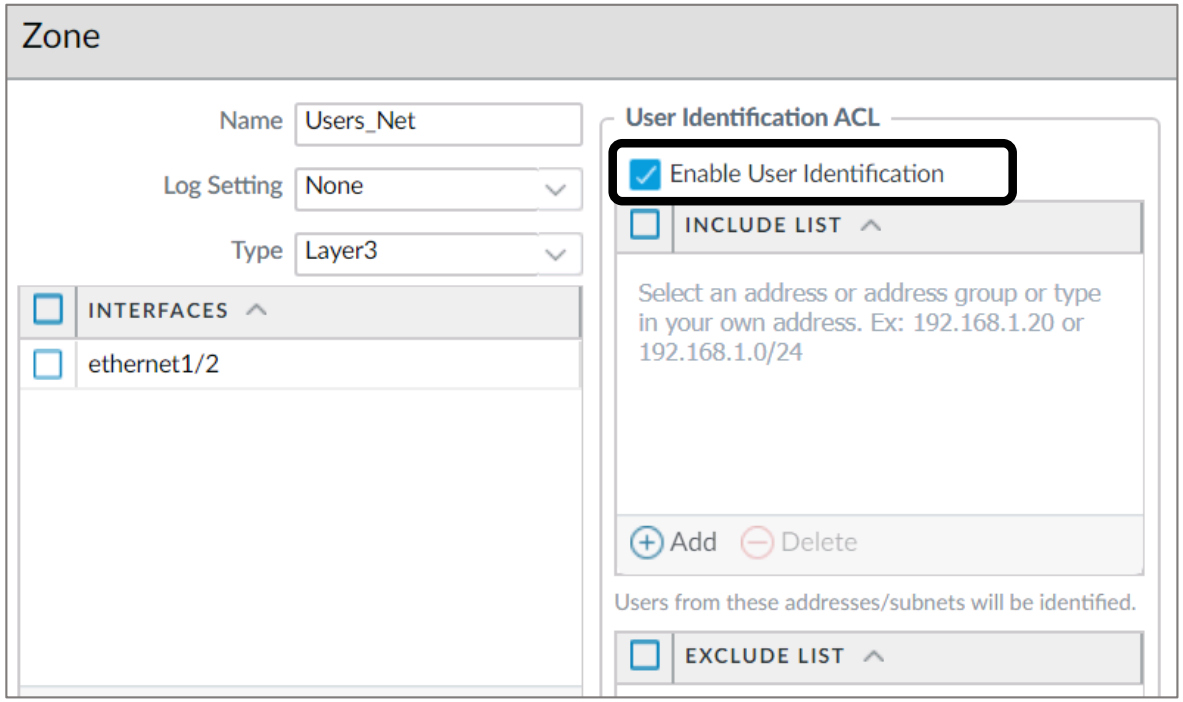
Configure User-ID

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.

Enable User-ID Per Zone

- 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>



User-ID overview

User mapping methods overview

Configure User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configure group mapping

User-ID and Security policy

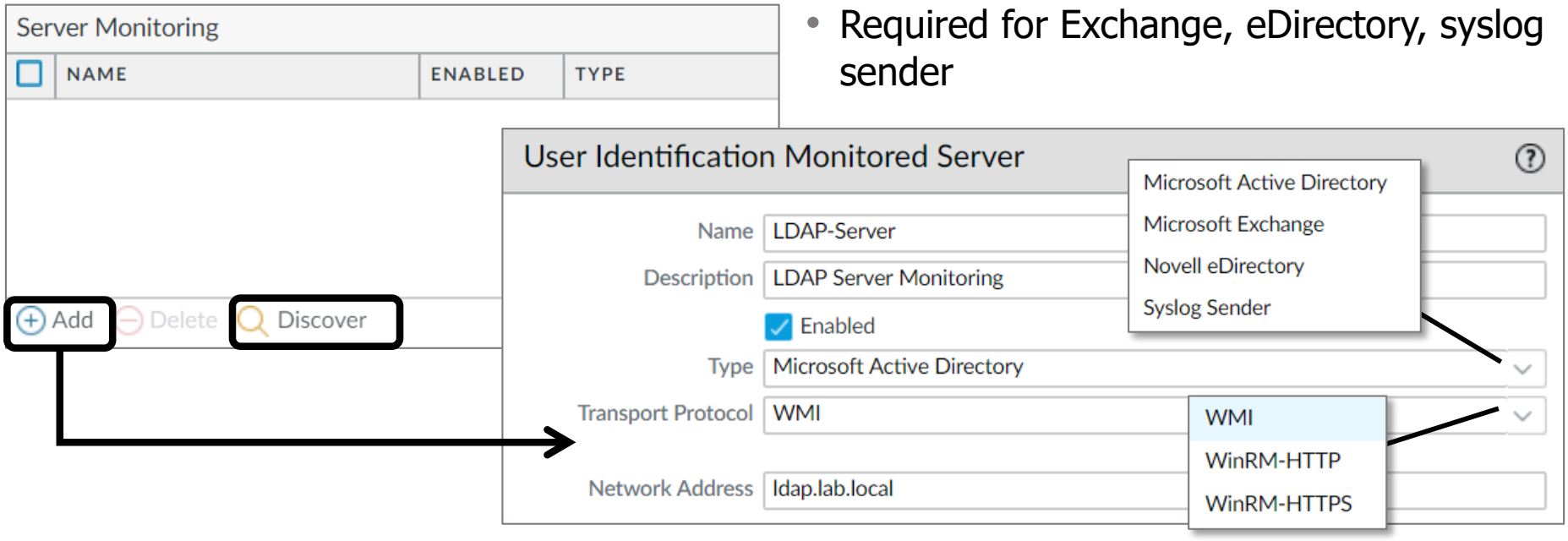
Configure the PAN-OS Integrated User-ID Agent

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. 

Define the Monitored Server(s)

- Use **Discover** for domain controllers.
- Use **Add** to manually add servers:
  - Required for Exchange, eDirectory, syslog sender

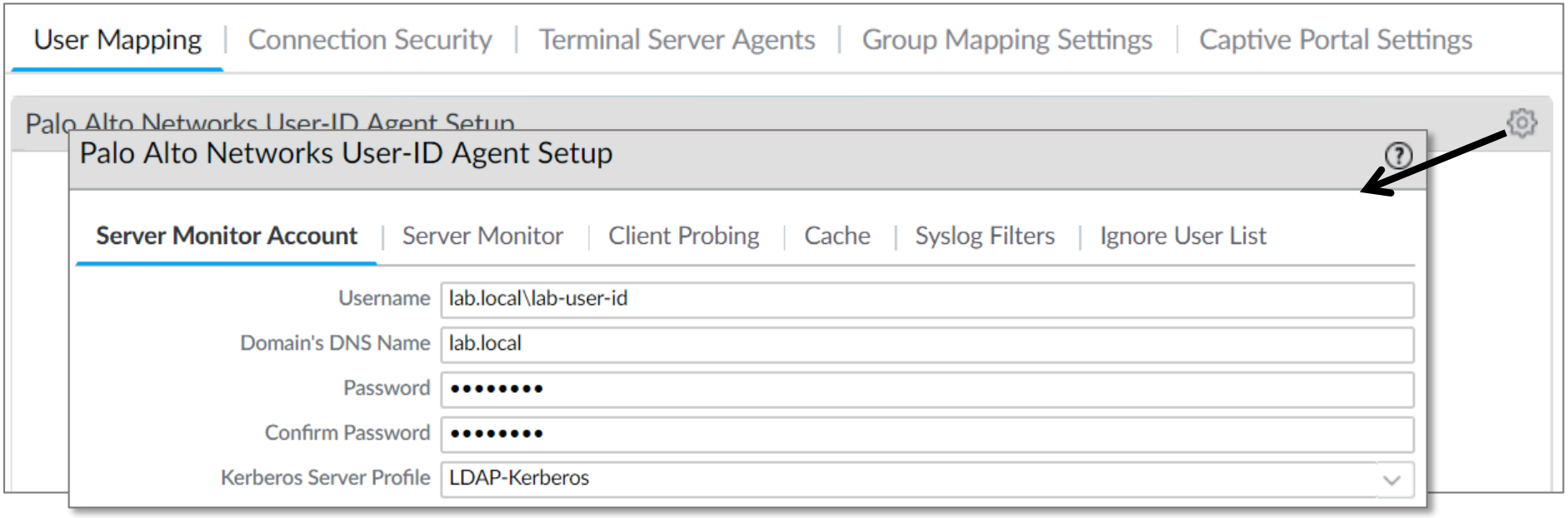
Device > User Identification > User Mapping



Define the User-ID Agent Account

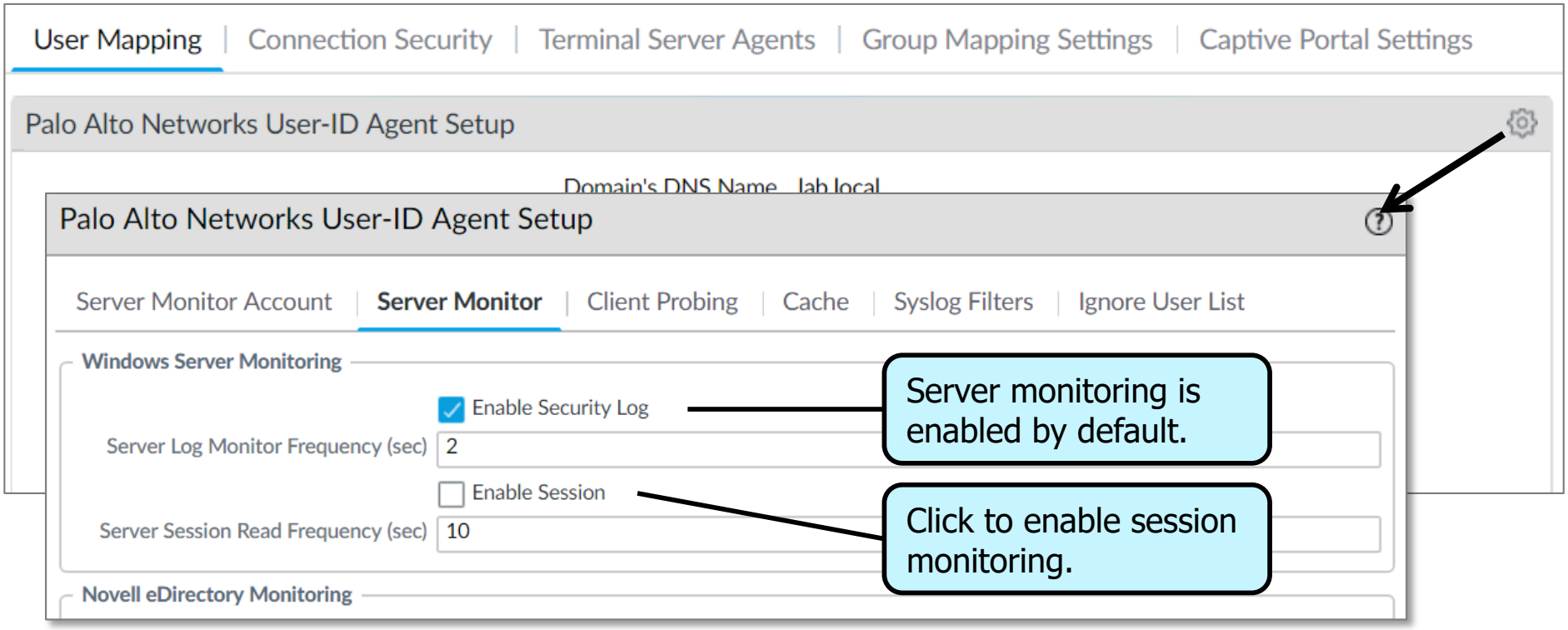
- Necessary permissions are provided if the agent account belongs to:
  - Domain Administrators group, or
  - Server Operators and Event Log Readers groups

Device > User Identification > User Mapping



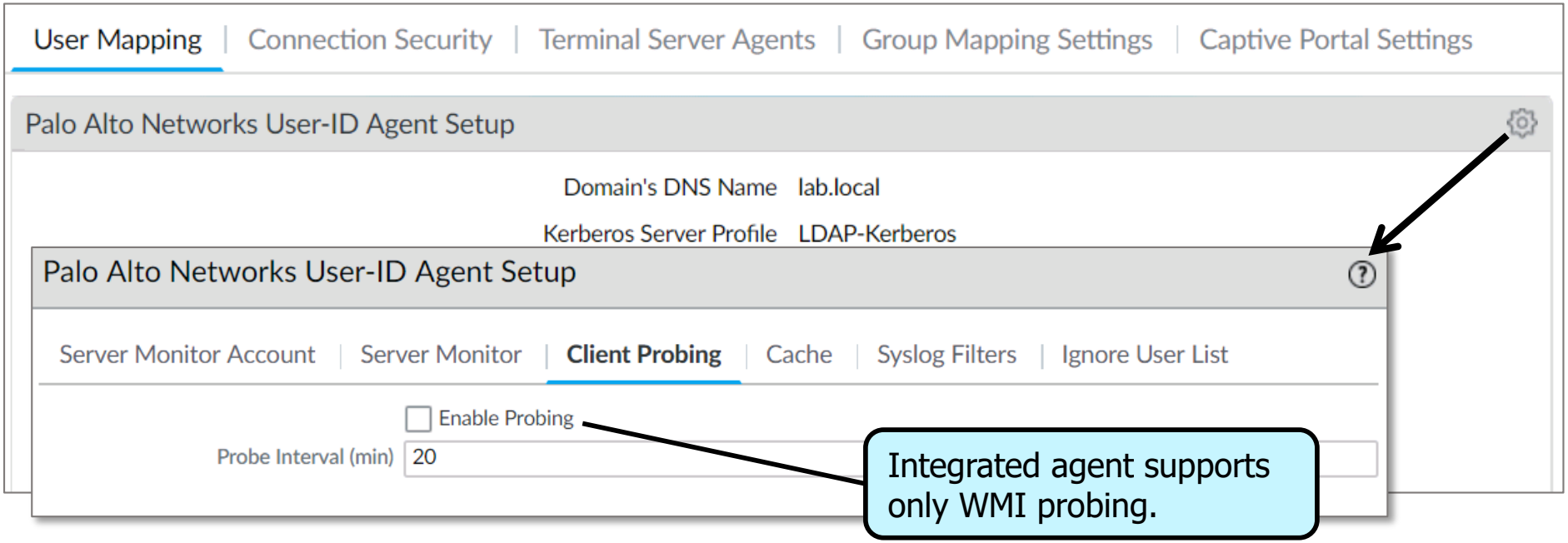
Optional Session Monitoring

Device > User Identification > User Mapping



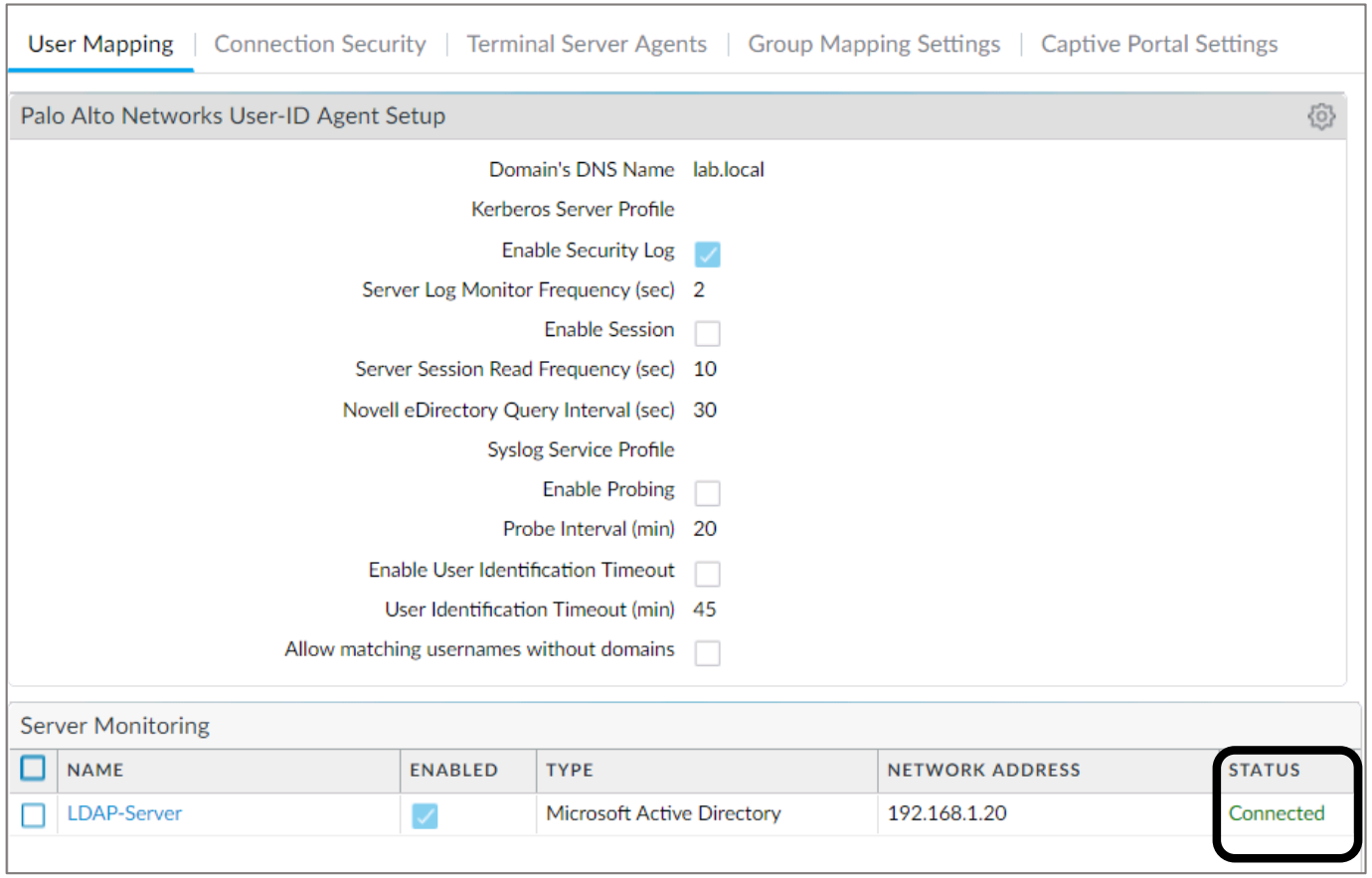
Optional WMI Client Probing

Device > User Identification > User Mapping



Verify Connection Status

Device > User Identification



User-ID overview

User mapping methods overview

Configure User-ID

PAN-OS integrated agent configuration

Windows-based agent configuration

Configure group mapping

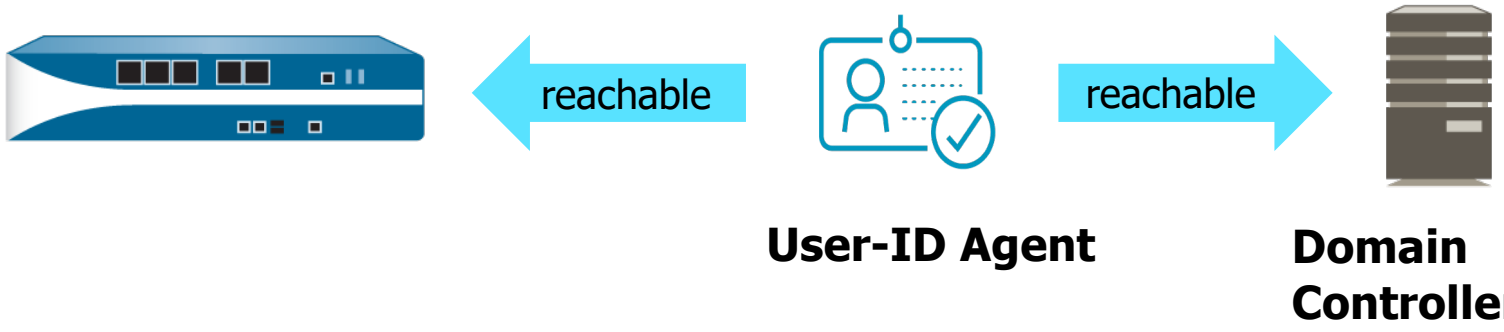
User-ID and Security policy

Configure 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.

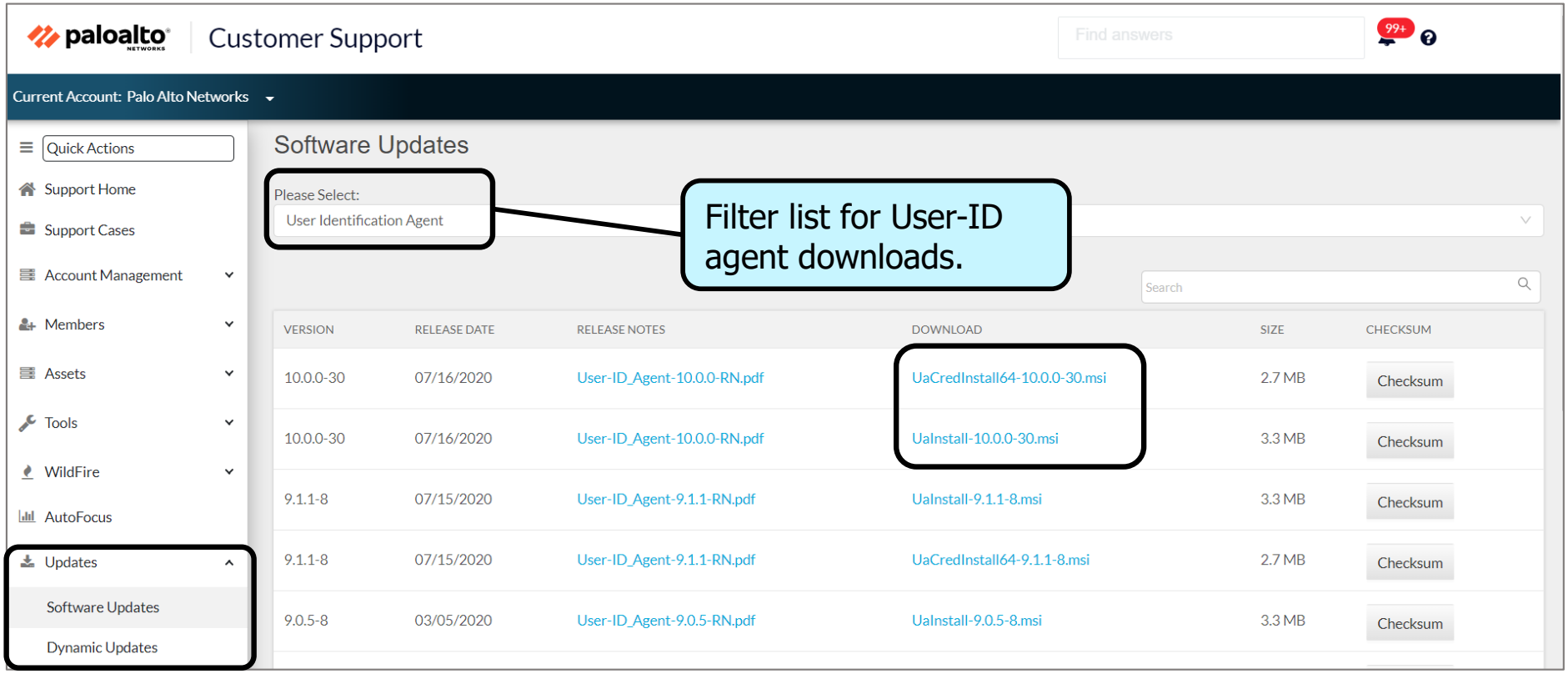
Select the Installation Location

- Install on the domain member:
  - Microsoft Windows Server 2008 or later.
  - Install close to the servers that the User-ID agent will be monitoring to optimize bandwidth use.
  - Install agents on two domain members for redundancy.

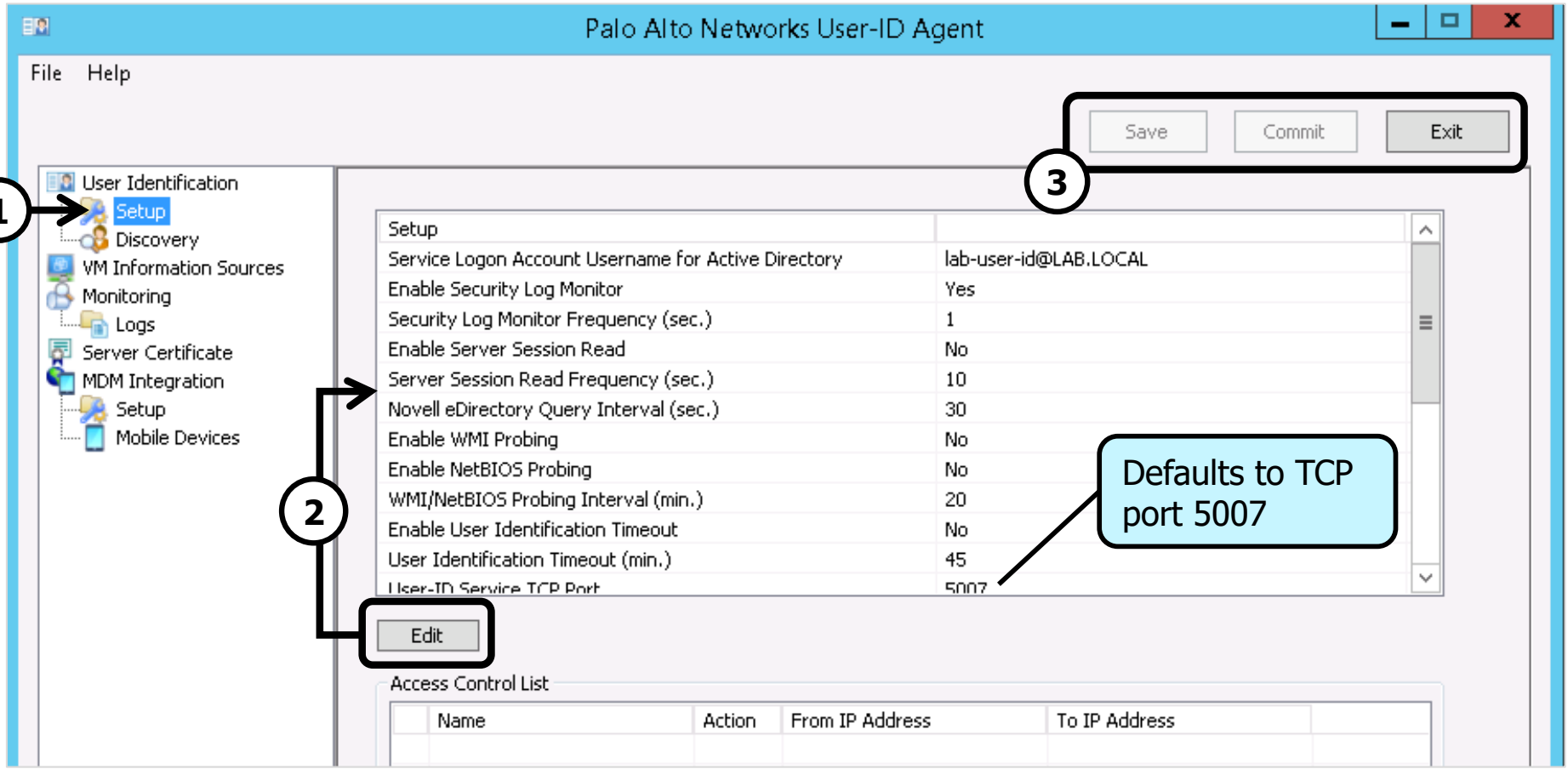


Download User-ID Agent Software

Download the Windows agent from https://support.paloaltonetworks.com/Support/Index and then install it.



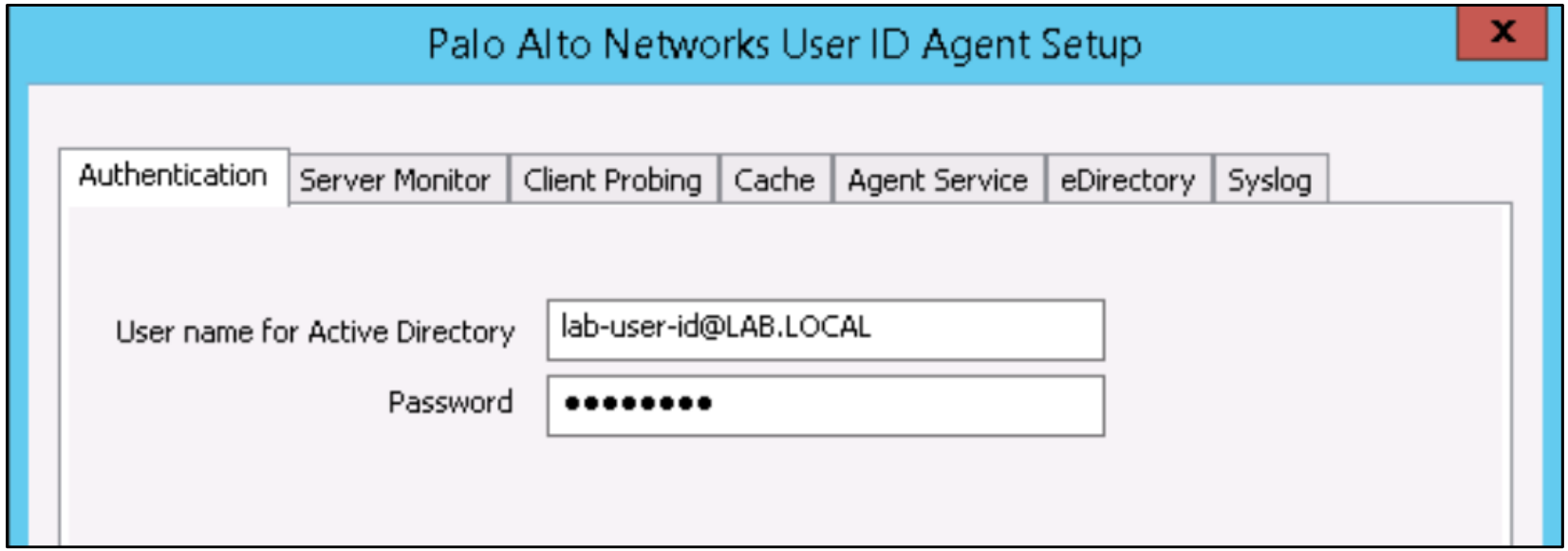
Agent Setup Process



Configure the User-ID Agent Account

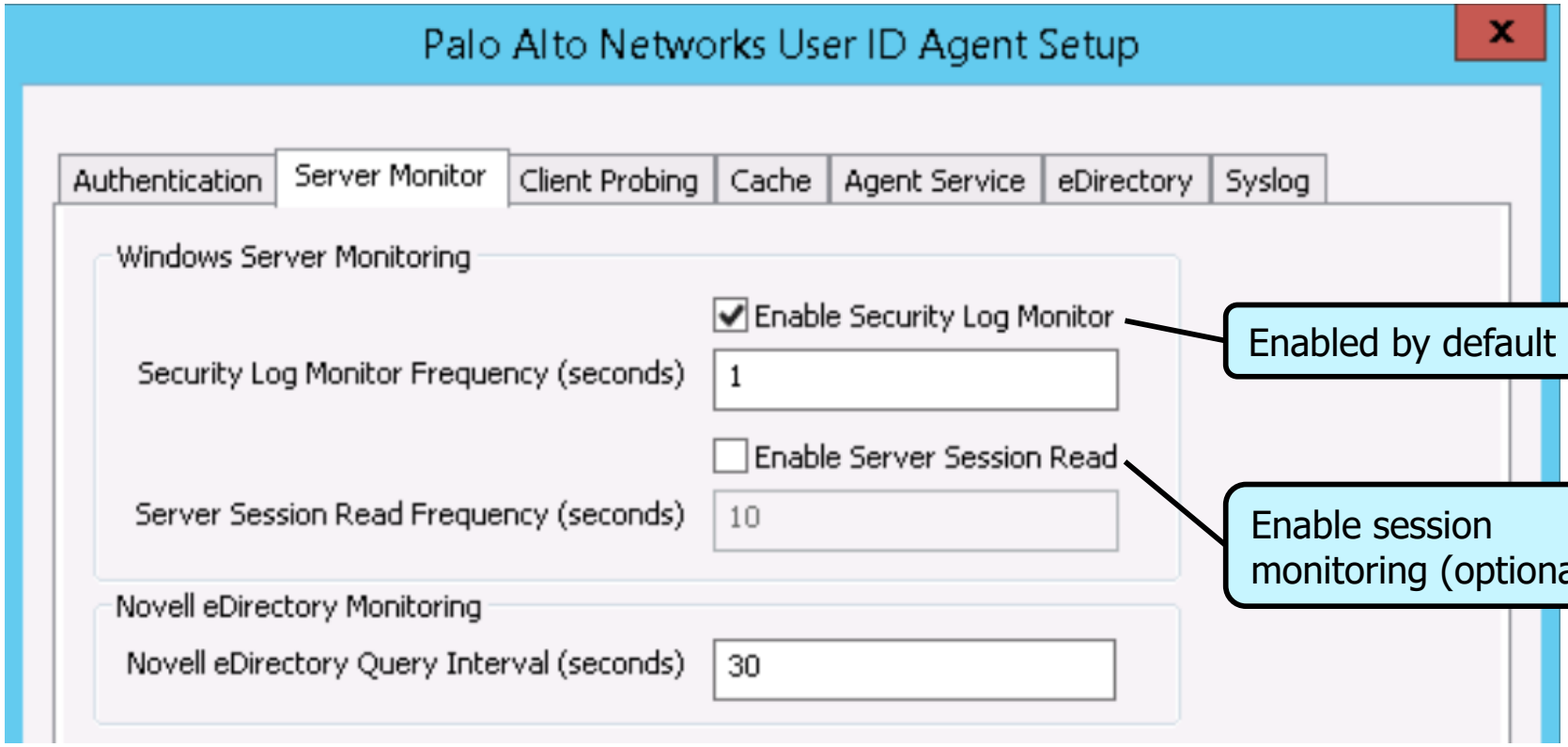
- Necessary permissions are provided if the agent account belongs to:
  - Domain Administrators group, or
  - Server Operators and Event Log Readers groups

User Identification > Setup > Edit



Configure Server Monitoring

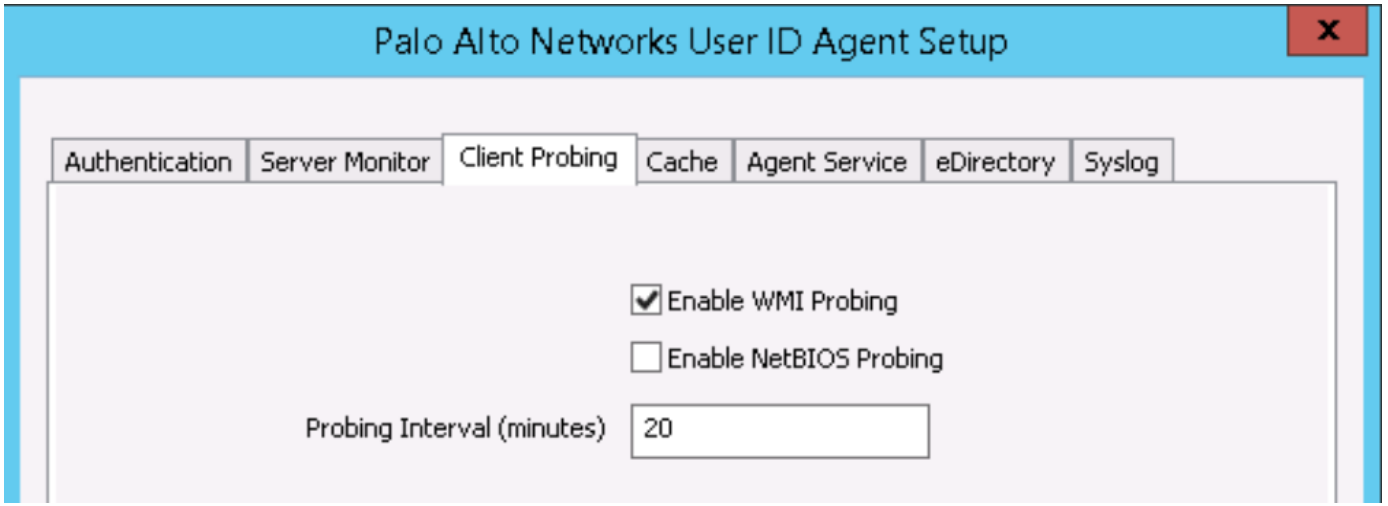
User Identification > Setup > Edit



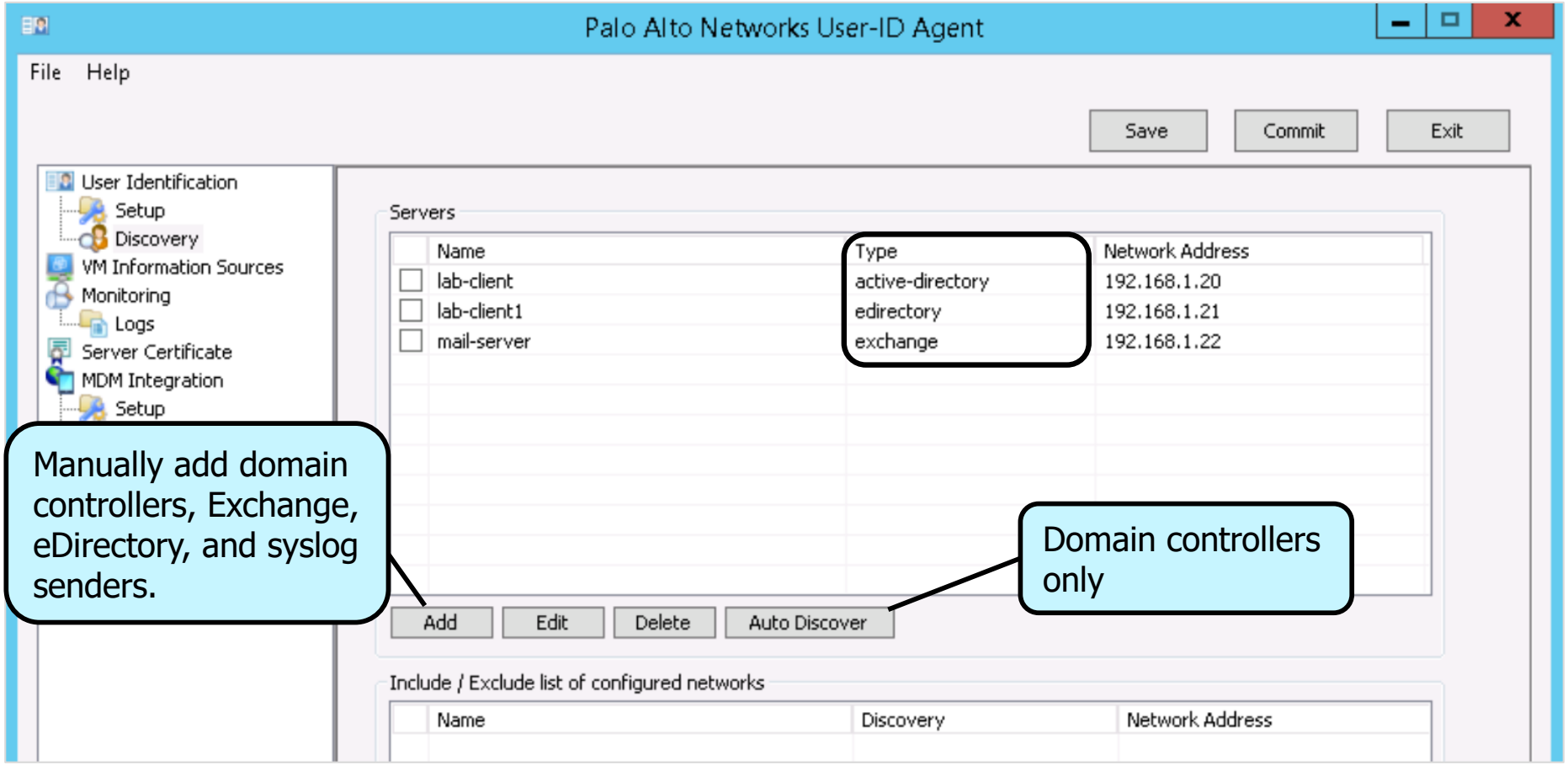
Configure Client Probing

- 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

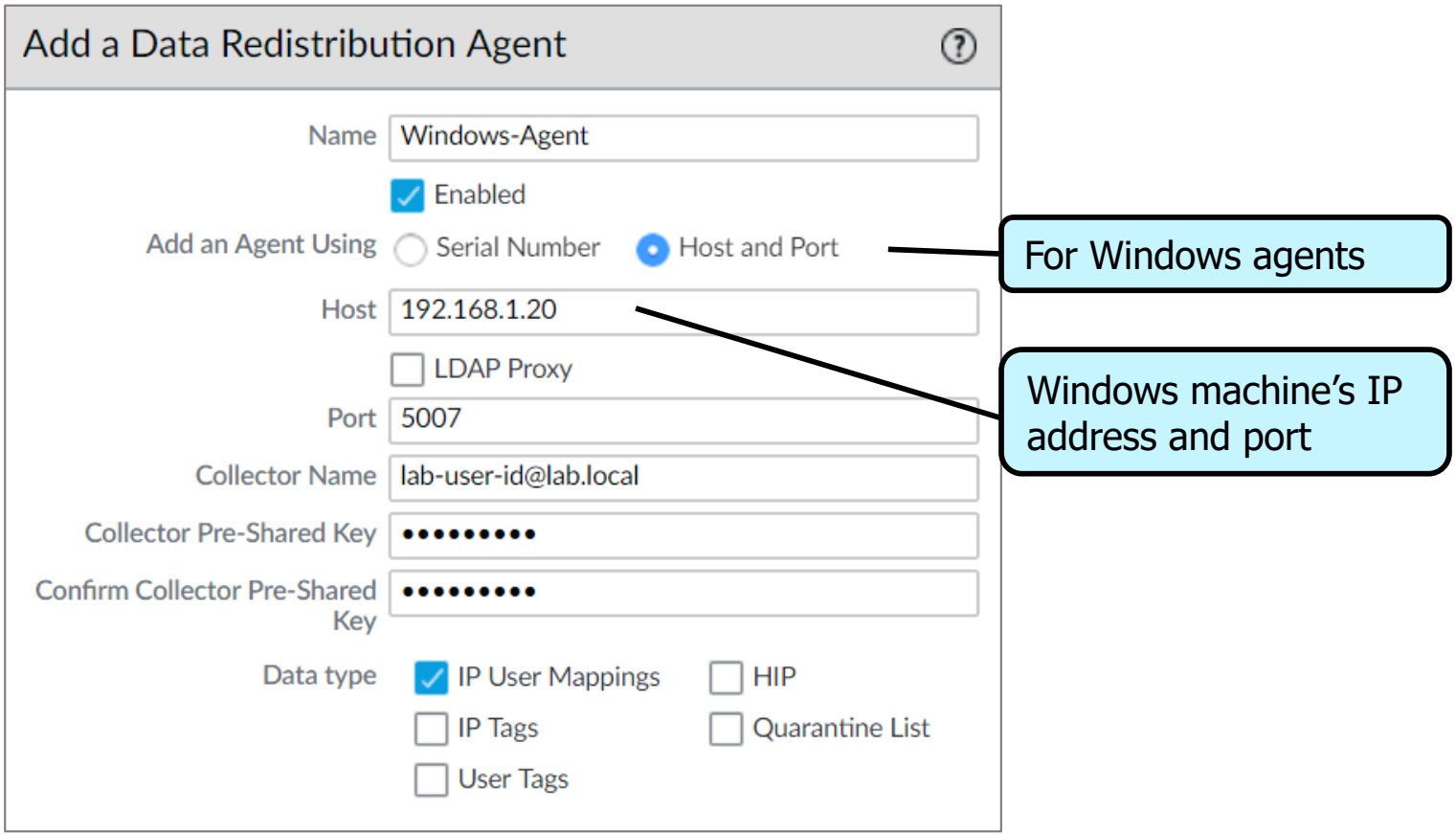


Configure the Monitored Servers



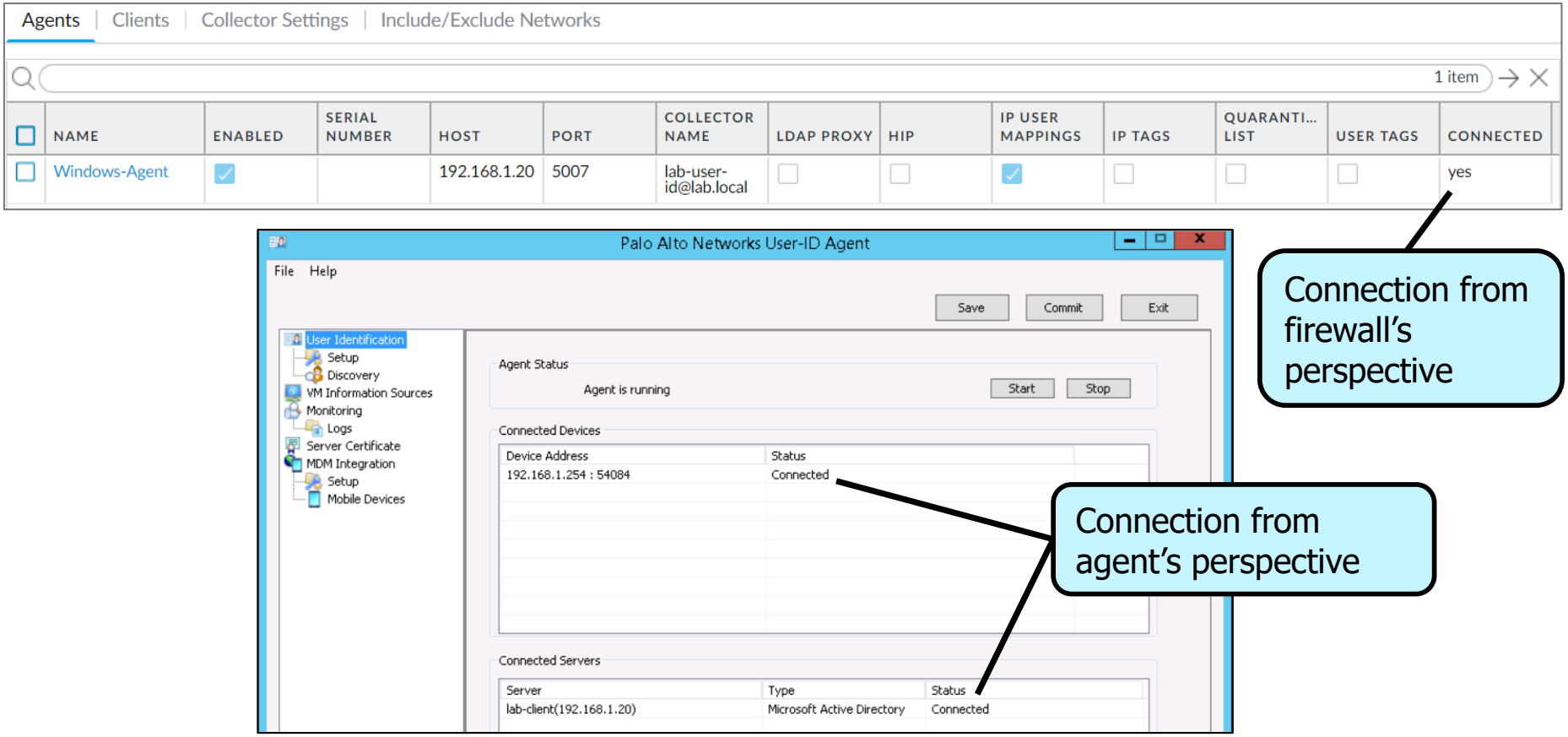
Configure the Firewall to Connect to the Agent

Device > Data Redistribution > Agents > Add

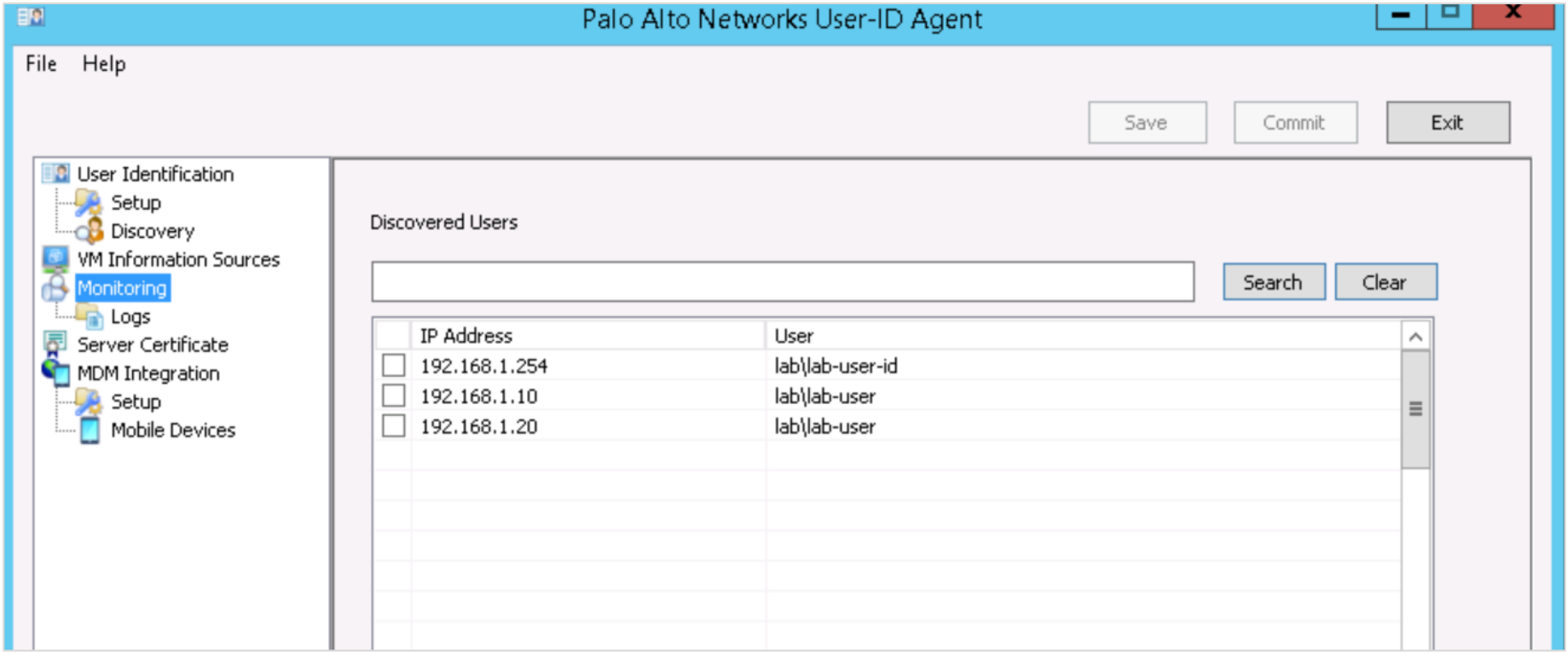


Confirm Connection to the User-ID Agent

Device > Data Redistribution > Agents



Display Mappings from the Windows Agent



Display Mappings from the Firewall CLI

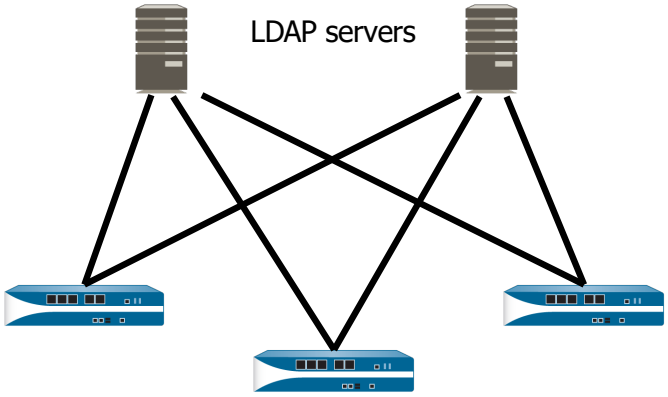
Show mapping for all or specific IP addresses.

```
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\pwldap                   902             902
Total: 10 users
```

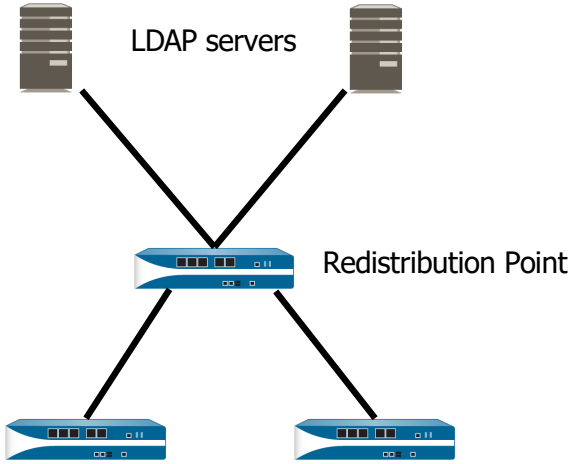
Data Redistribution

- Without Data Redistribution



Each firewall must connect directly to each mapping source to obtain User-ID data.

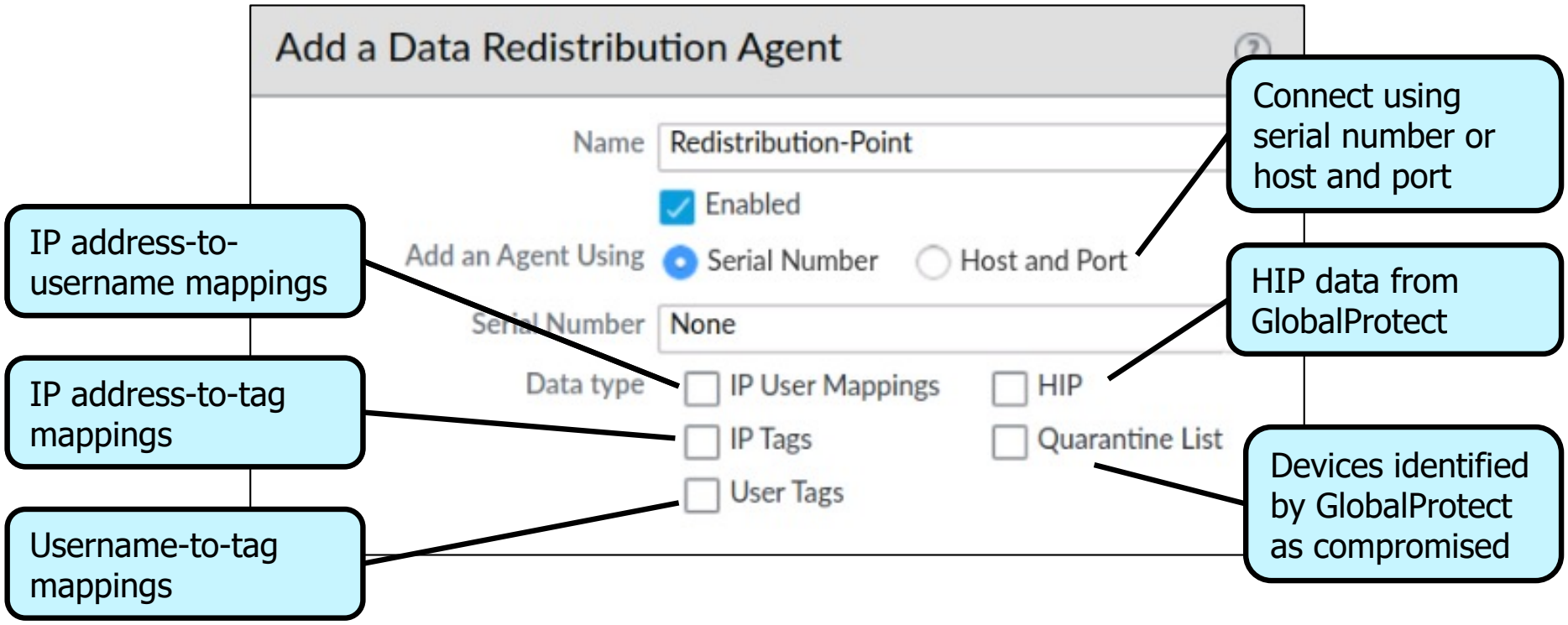
- With Data Redistribution



One firewall connects to each mapping source to obtain User-ID data. The remaining firewalls connect to a source firewall to obtain User-ID data.

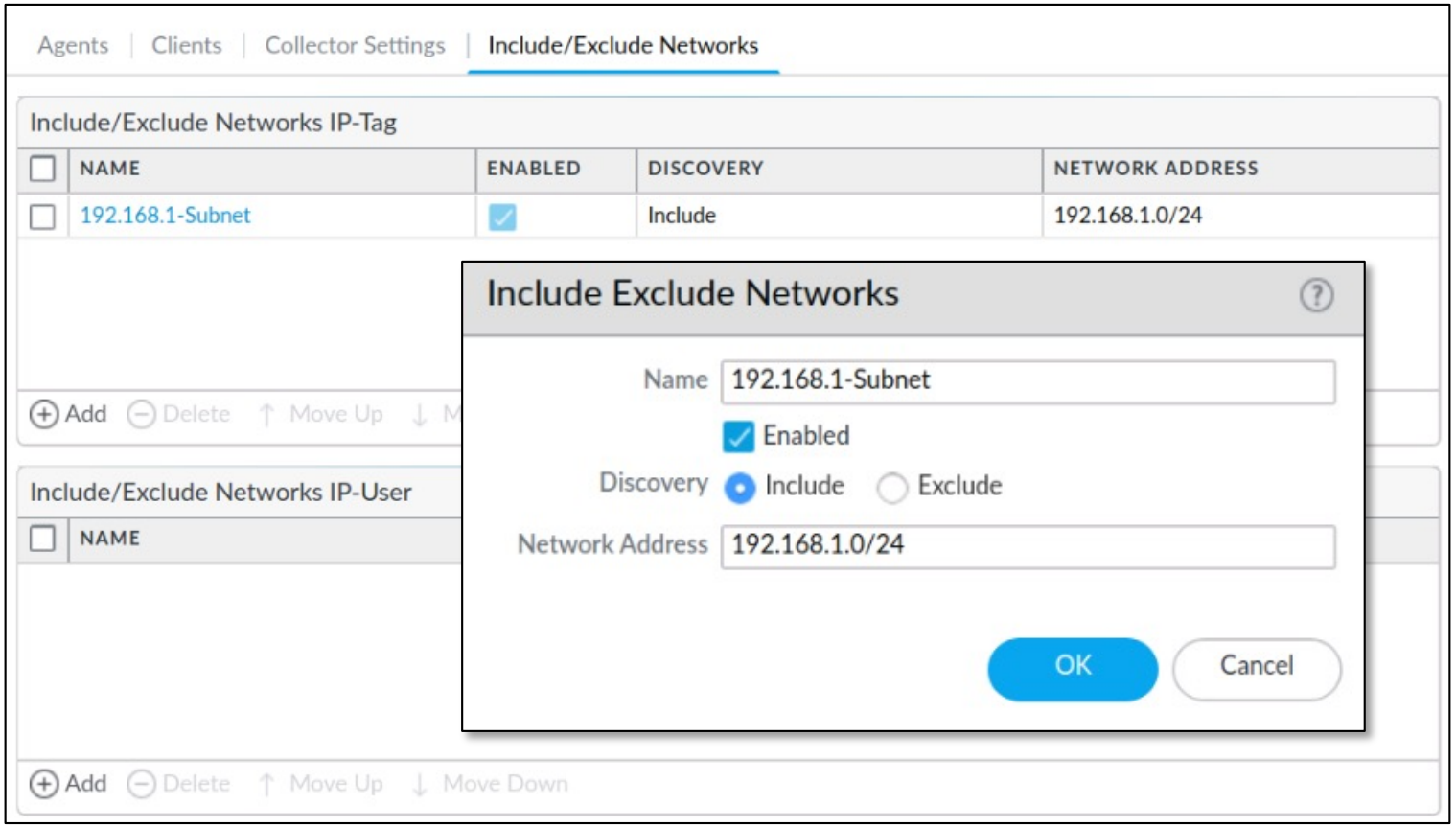
Configure the Firewall to Connect to the Redistribution Point

Device > Data Redistribution > Agents > Add



Configure the Firewall to Connect to the Redistribution Point (Cont.)

Device > Data Redistribution > Include/Exclude Networks



 |

User-ID overview

User mapping methods overview

Configure User-ID

PAN-OS integrated agent configuration

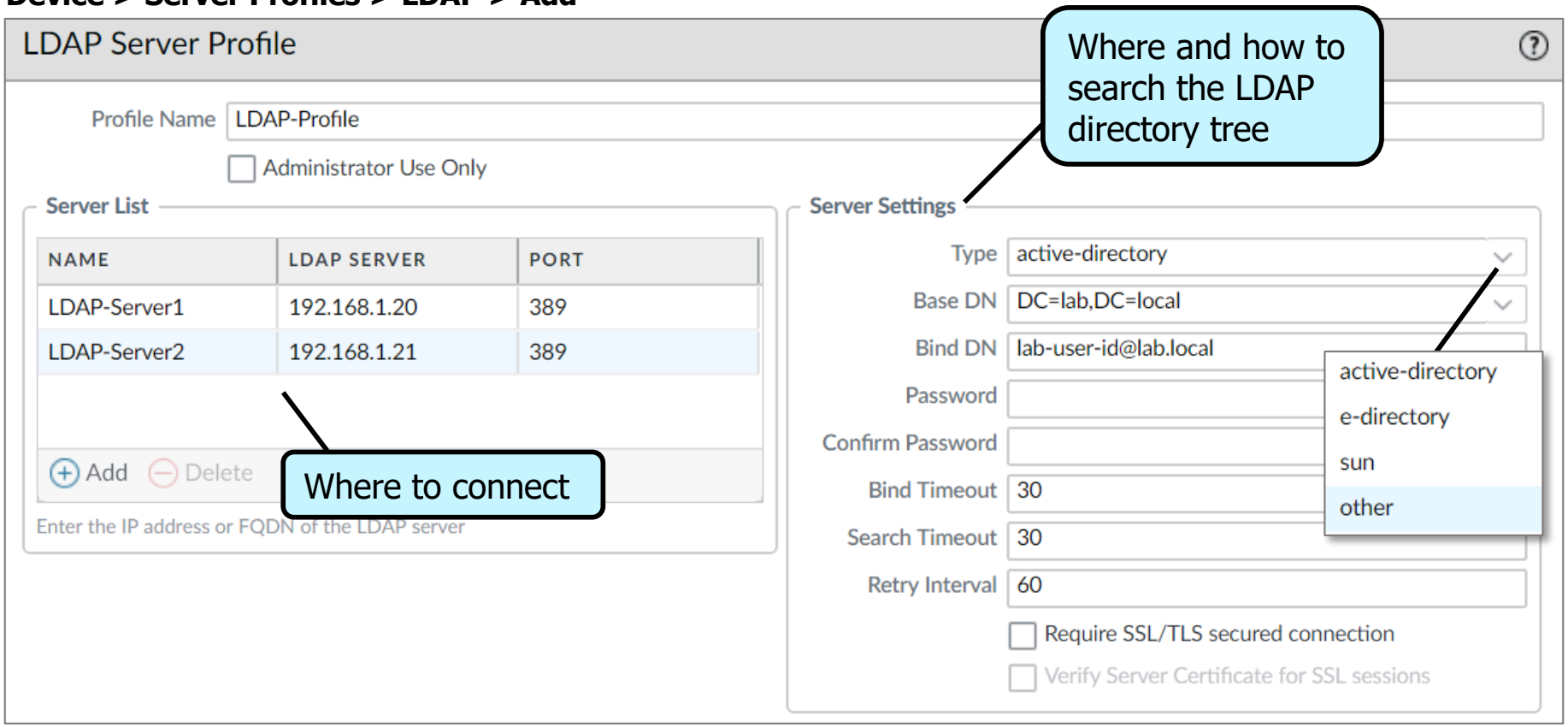
Windows-based agent configuration

Configure group mapping

User-ID and Security policy

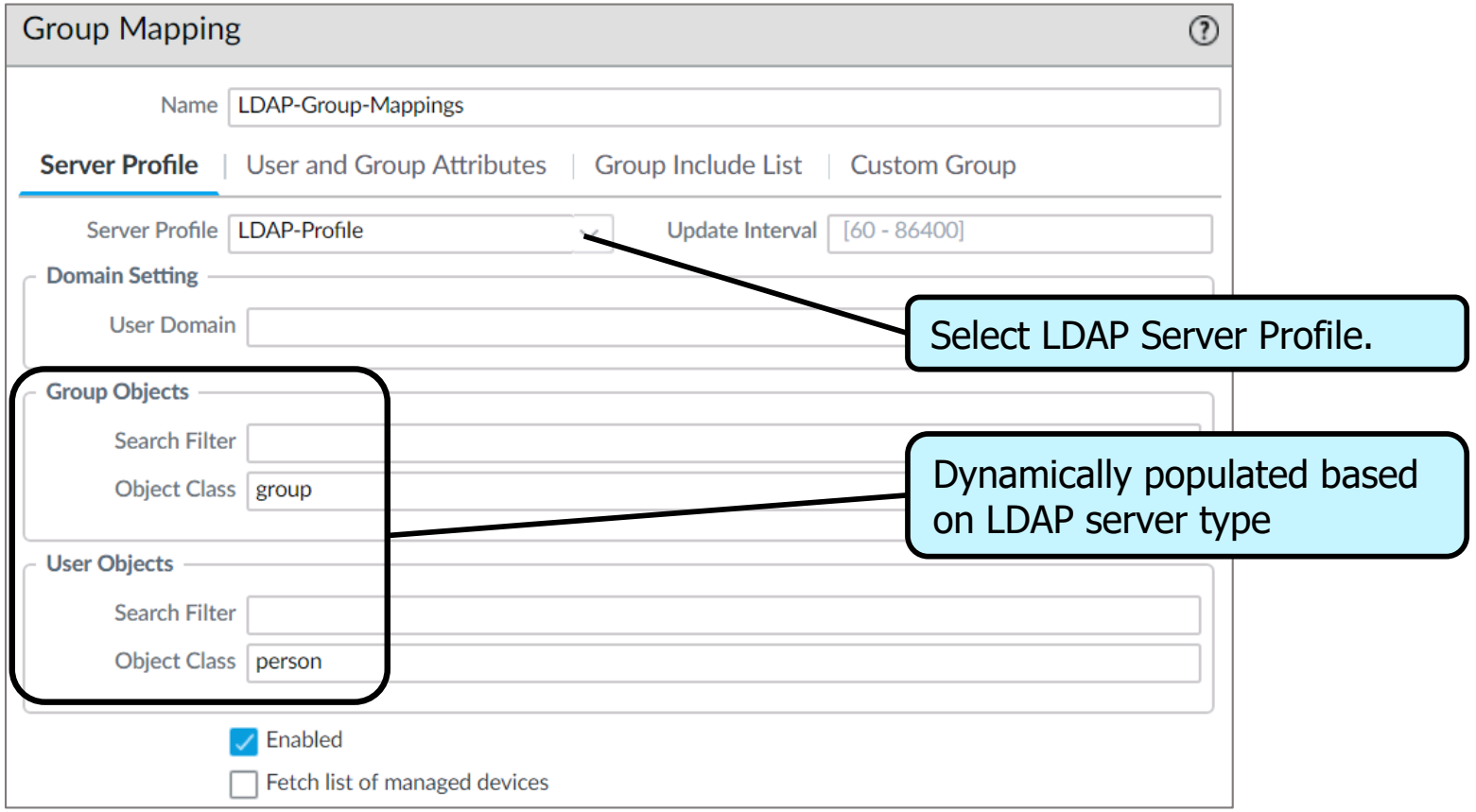
LDAP Server Profile

Device > Server Profiles > LDAP > Add



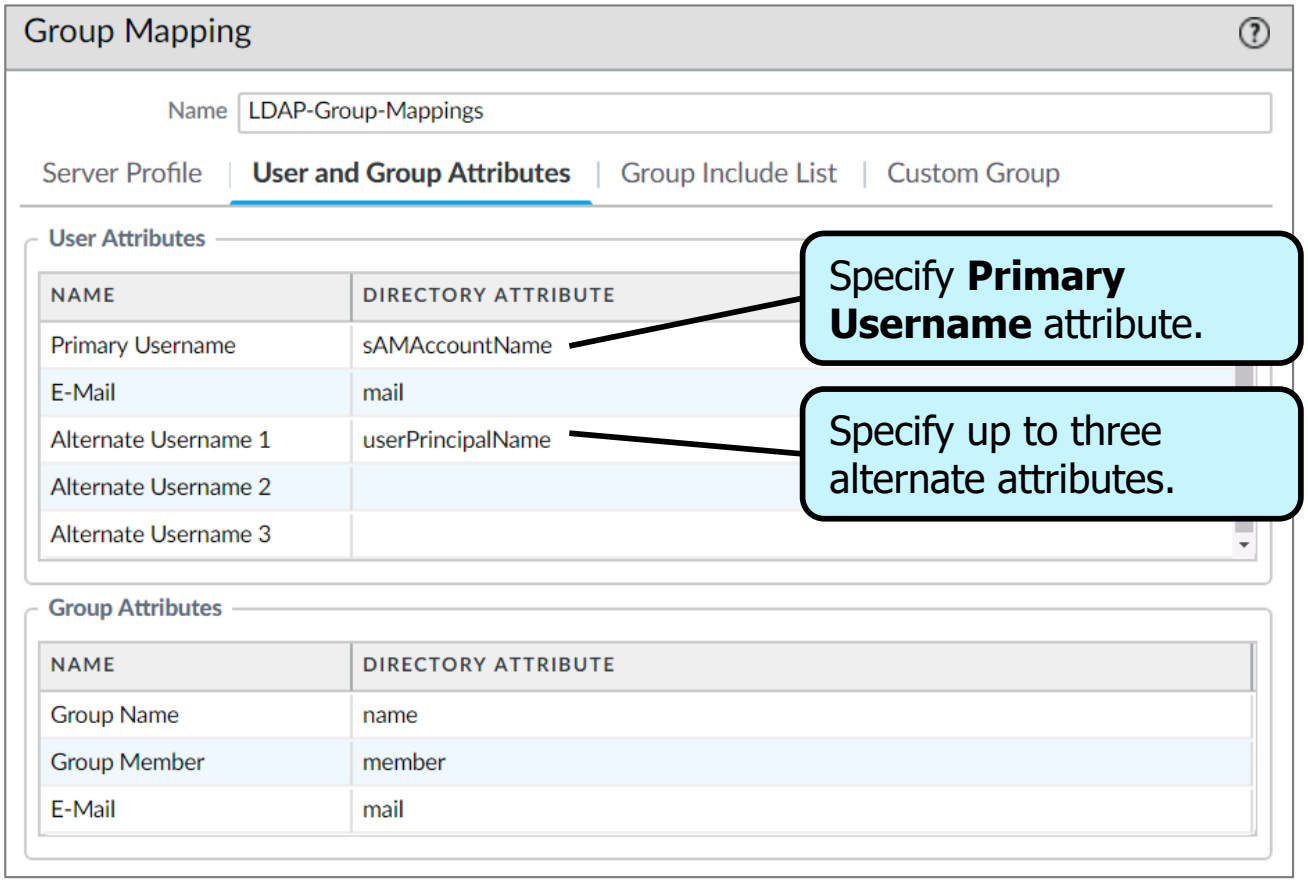
Create User-ID Group Mapping Filters

Device > User Identification > Group Mapping Settings > Add



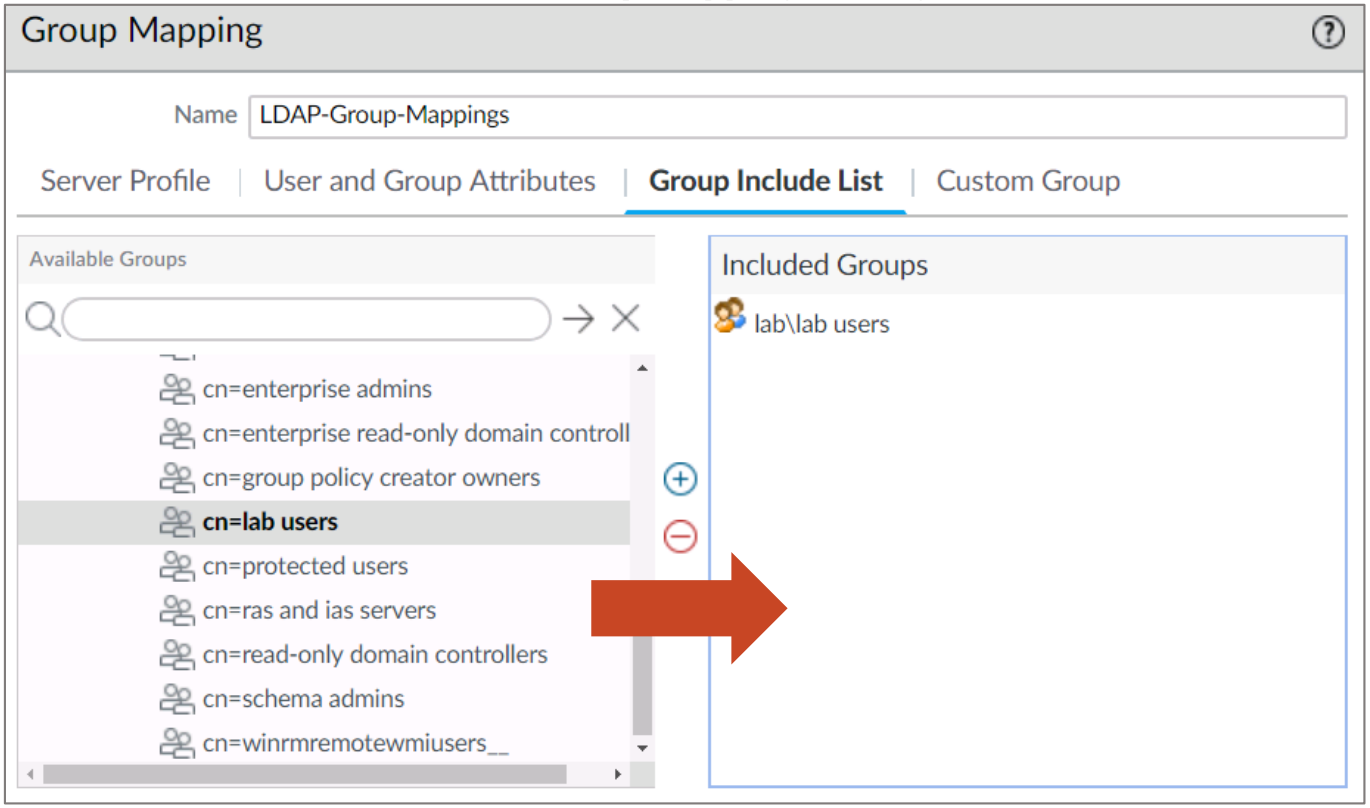
Create User-ID Group Mapping Filters (Con't)

Device > User Identification > Group Mapping Settings > Add



Filter Groups Sent to the Firewall

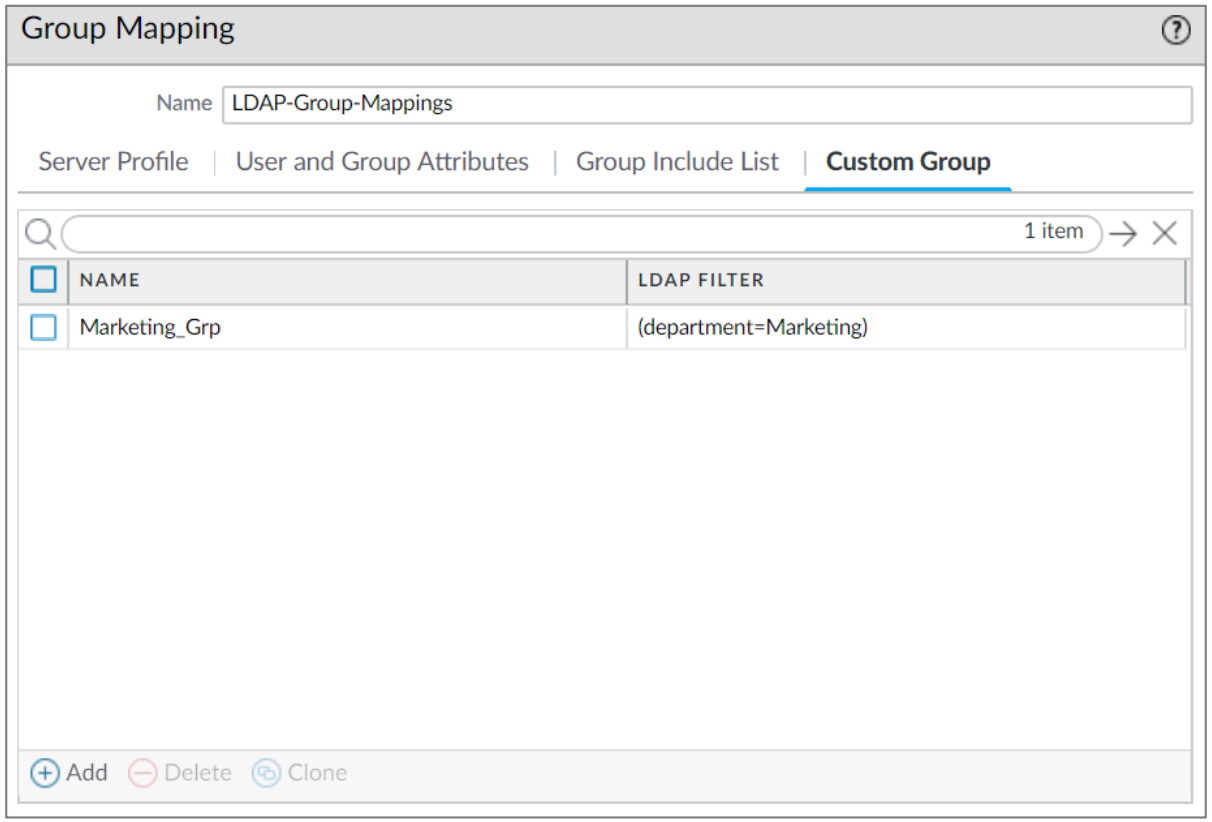
Device > User Identification > Group Mapping Settings > Add



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

Custom Groups Based on LDAP Filters

Device > User Identification > Group Mapping Settings > Add



- 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

Configure User-ID

PAN-OS integrated agent configuration

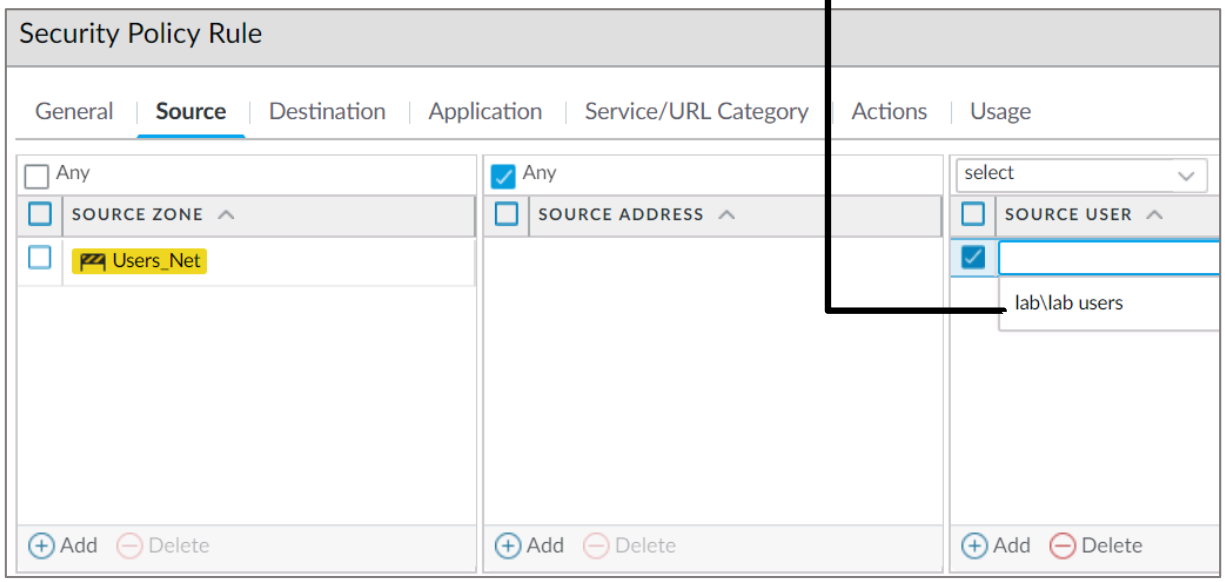
Windows-based agent configuration

Configure group mapping

User-ID and Security policy

Select Users and Groups for a Security Policy

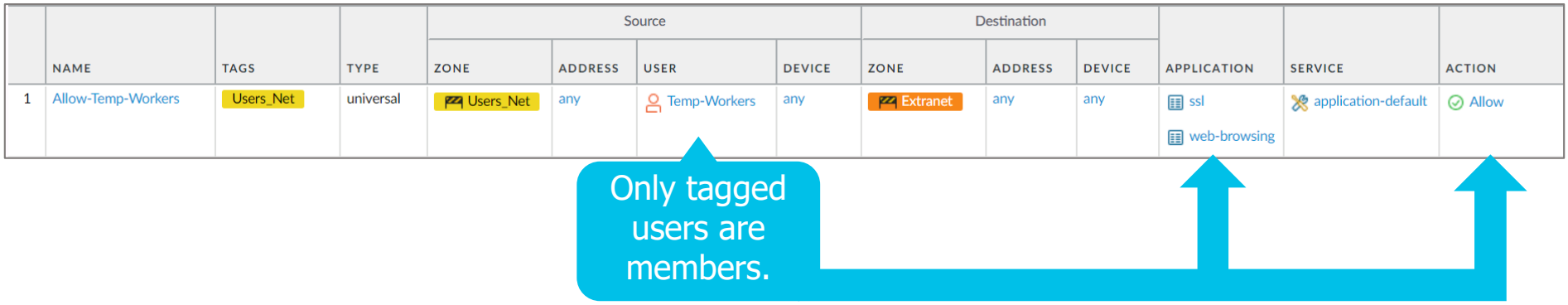
	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			
1	Users_to_Extranet	Users_Net	universal	Users_Net	any	lab\lab users	any	Extranet	any	any	ssl web-browsing	application-default	Allow
2	Danger-Simulated-Traffic	Danger	universal	Danger	any	lab\lab users	any	Danger	any	any	any	application-default	Allow



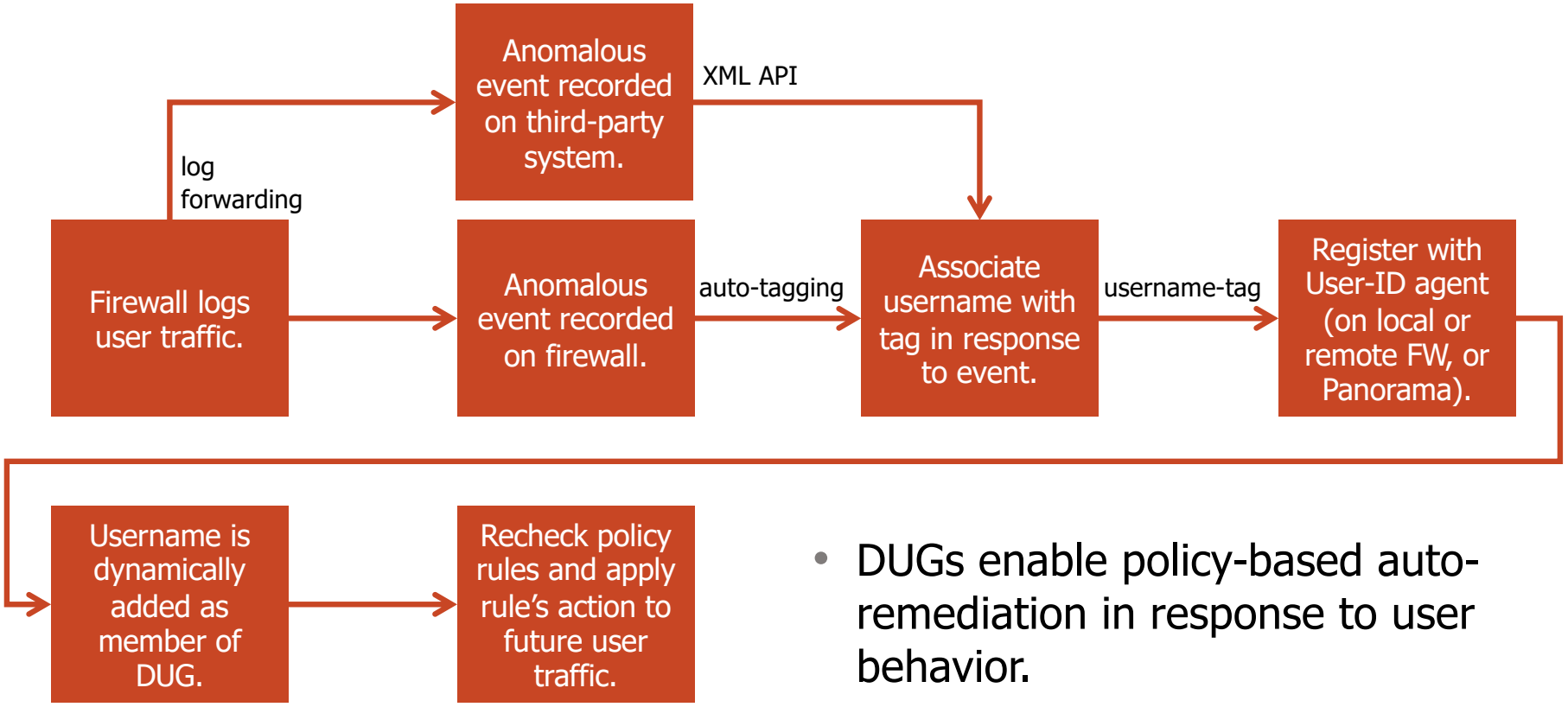
- Source user options:
  - **any**
  - **pre-logon**
  - **known-user**
  - **unknown**
  - **select**

Dynamic User Groups (DUGs)

- DUGs control user access to resources managed by firewall policies:
  - Security policy, Authentication policy, Decryption policy, etc.
- User membership in a DUG is dynamic:
  - Only tagged usernames become members of the group.
  - Changes to group membership do not require a commit.



Dynamic User Group Operation

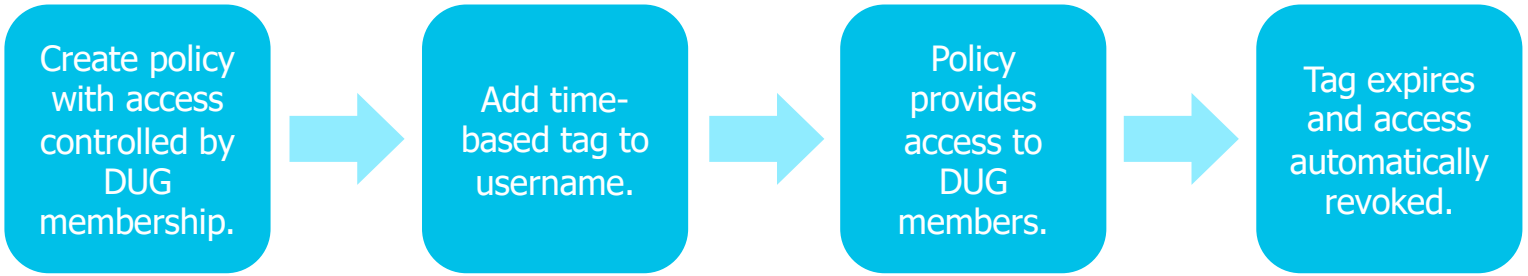


- DUGs enable policy-based auto-remediation in response to user behavior.

Two Example Use Cases

Leverage User's Entire Known Security State:

Use Time-Based User Access Controls:



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 the Windows-based agent to probe IP addresses for username information
- Configure username-to-group name mapping
- Implement User-ID in Security policy

Questions

Lab 13: Blocking Threats with User-ID

- Enable User-ID on Zone
- Modify the Security Policy Rule
- Create a Marketing Apps Rule
- Create a Deny Rule
- Generate Traffic from the Acquisition Zone
- Examine User-ID Logs
- Examine a Firewall Traffic Log

Protecting our digital way of life.