USER-ID

EDU-210 Version A
PAN-OS® 9.0

KNOW THE WHO; CONTROL THE WHO

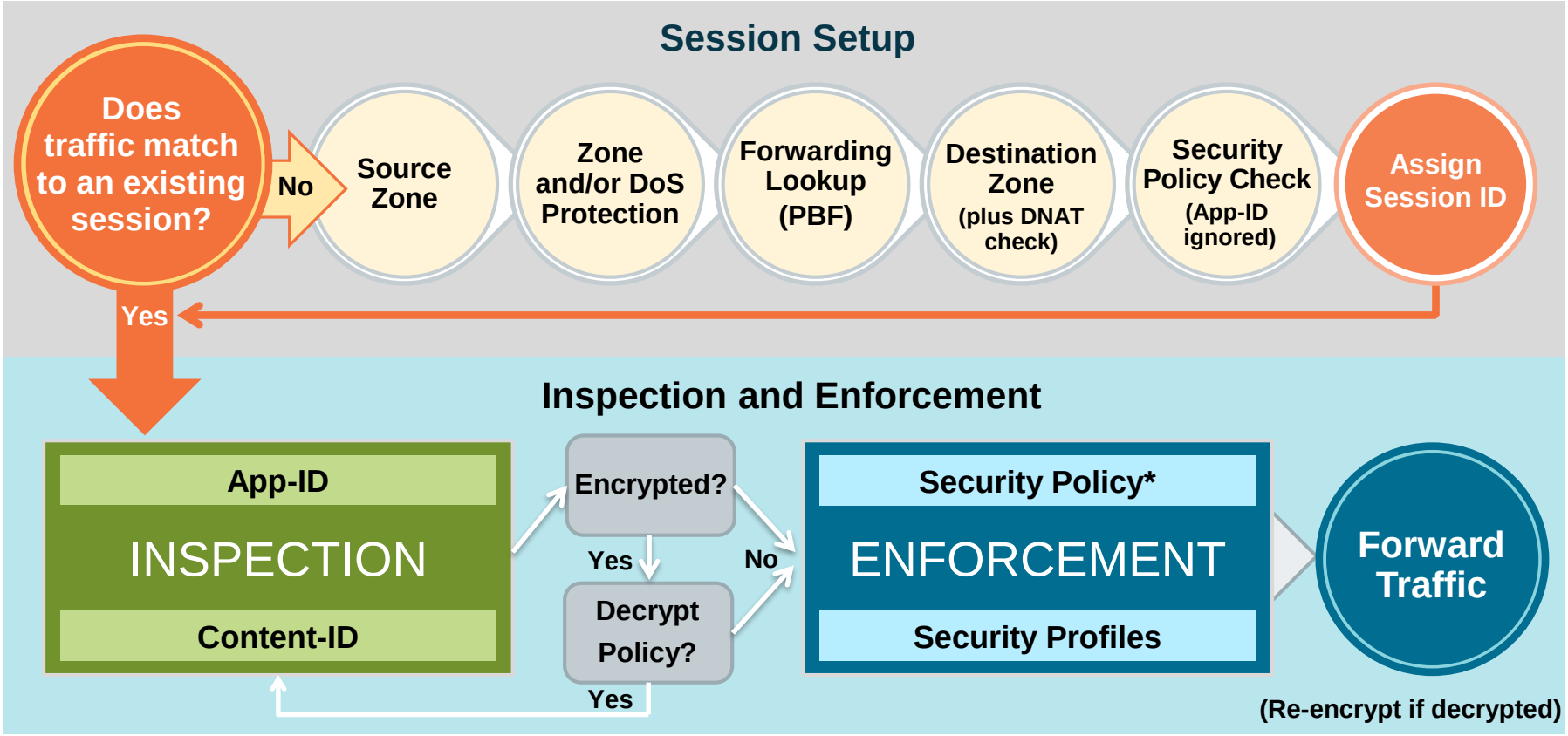
- User-ID overview
- User mapping methods overview
- Configuring User-ID
- PAN-OS® integrated agent configuration
- Windows-based agent configuration
- Configuring group mapping
- User-ID and security policy

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

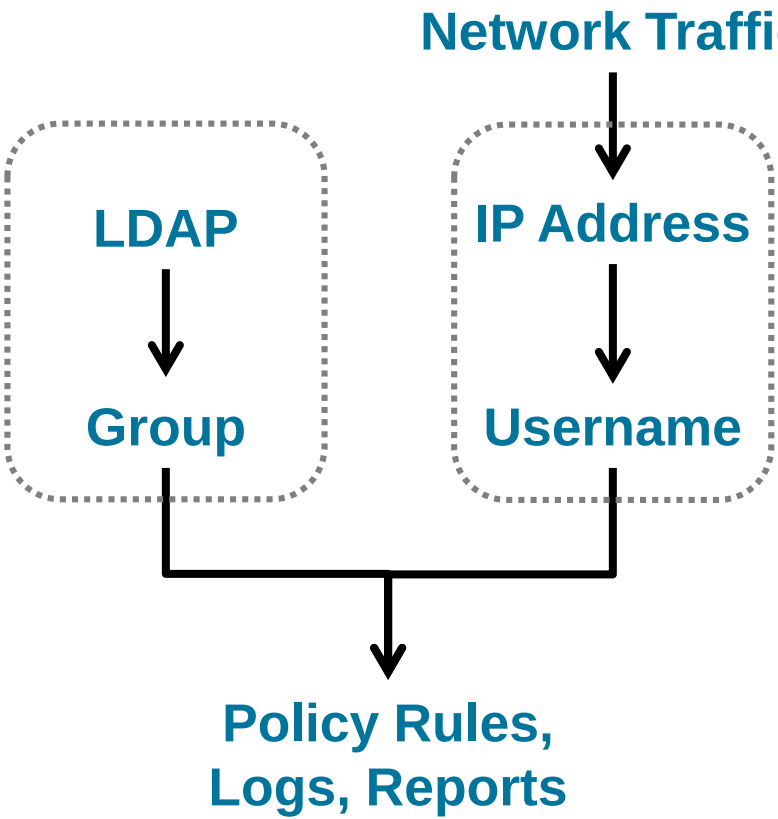
	Name	Tags	Type	Source				Destination		Application	Service	Action
				Zone	A...	User	HIP Pr...	Zone	Addr...			
1	egress-outside	egress	universal	inside	any	lab\lab users	any	outside	any	facebook-base	application-default	Deny
2	egress-public.ftp	egress	universal	inside	any	lab\lab users	any	outside	any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

Group mapping:
Learn group names and member users from LDAP



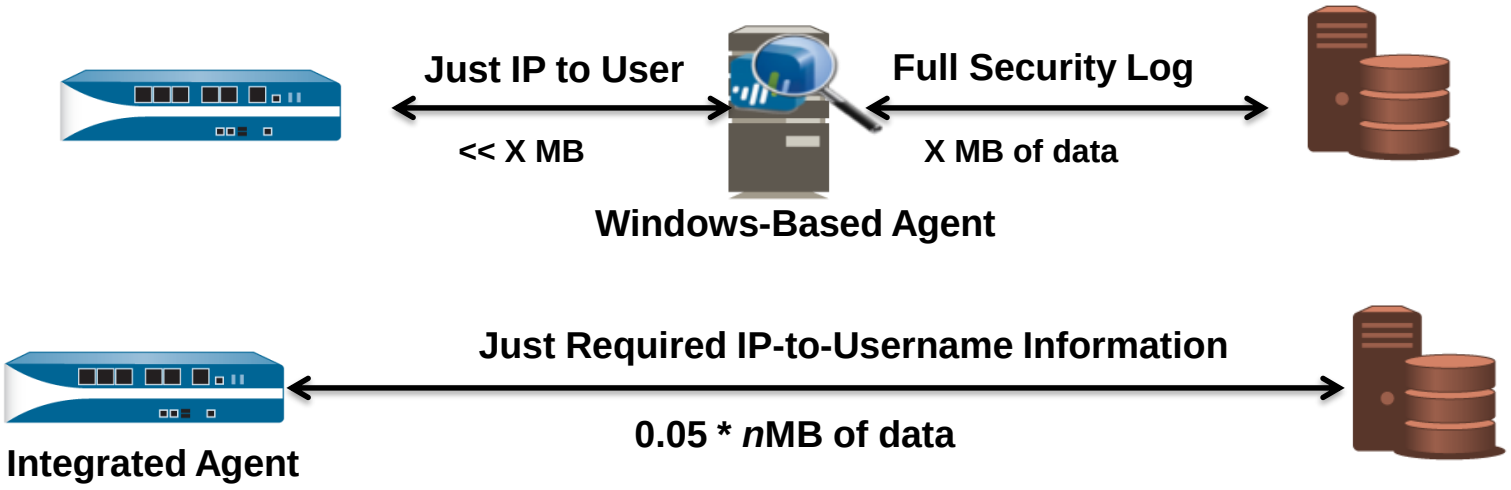
User mapping:
Associate IP addresses with usernames

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 or install a Windows-based agent at the site.



User-ID overview

User mapping methods overview

Configuring User-ID

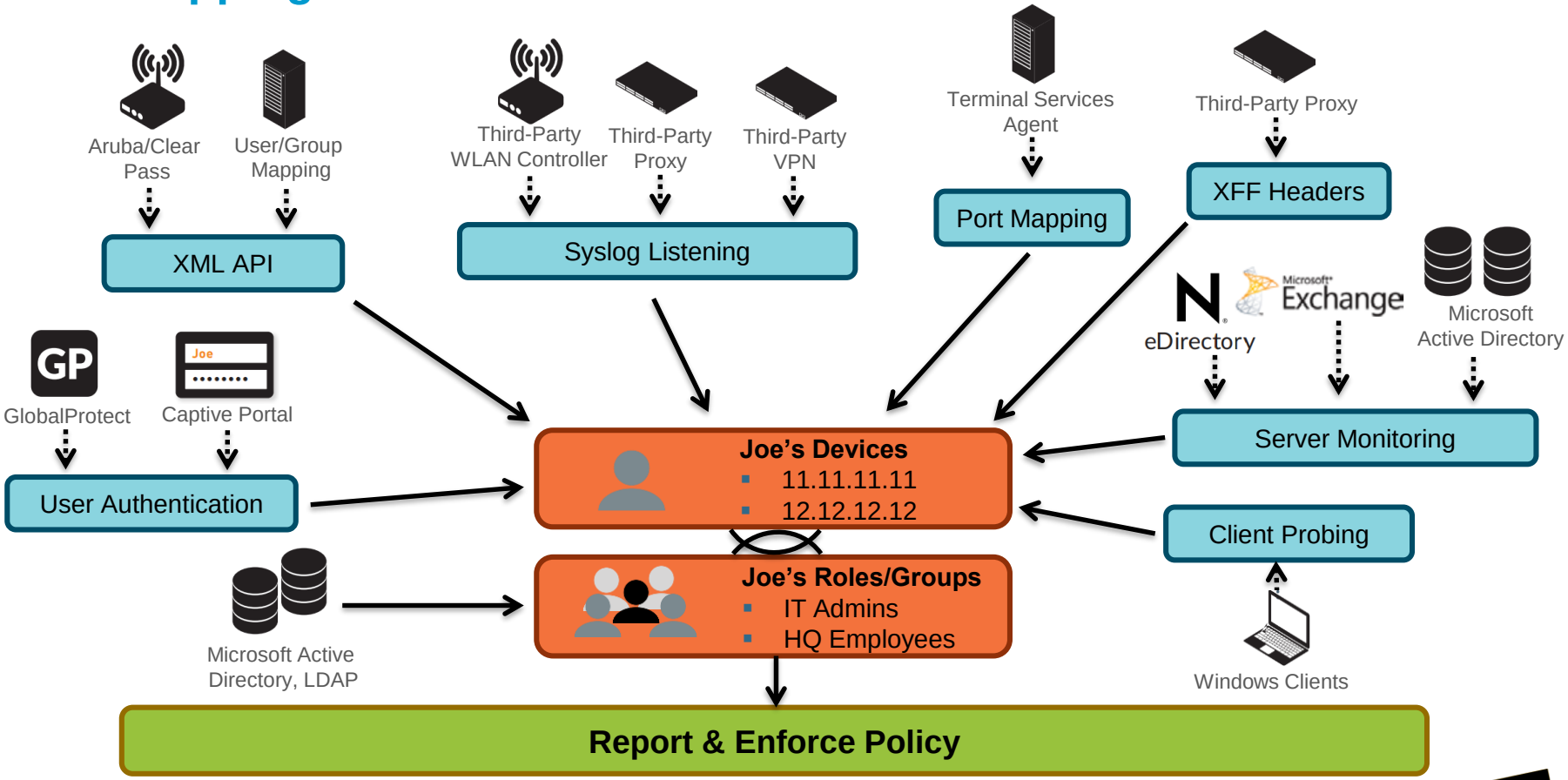
PAN-OS integrated agent configuration

Windows-based agent configuration

Configuring group mapping

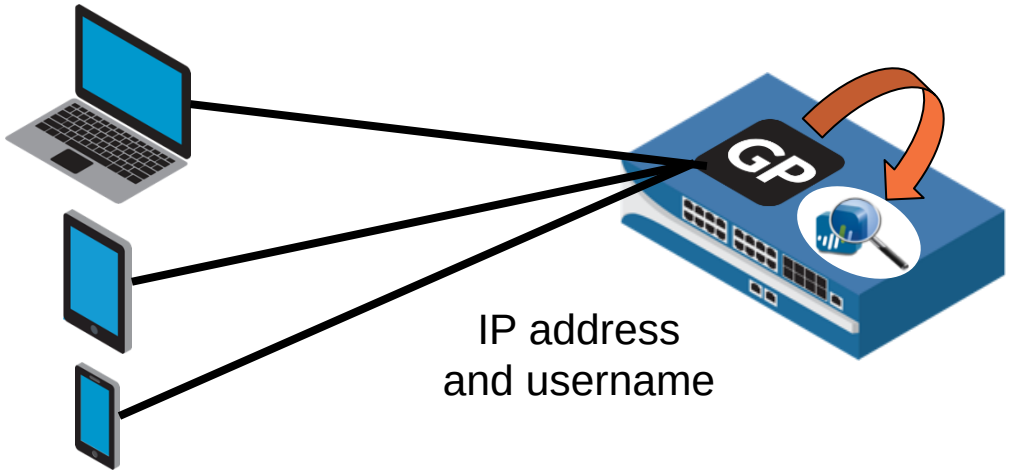
User-ID and security policy

User Mapping Methods



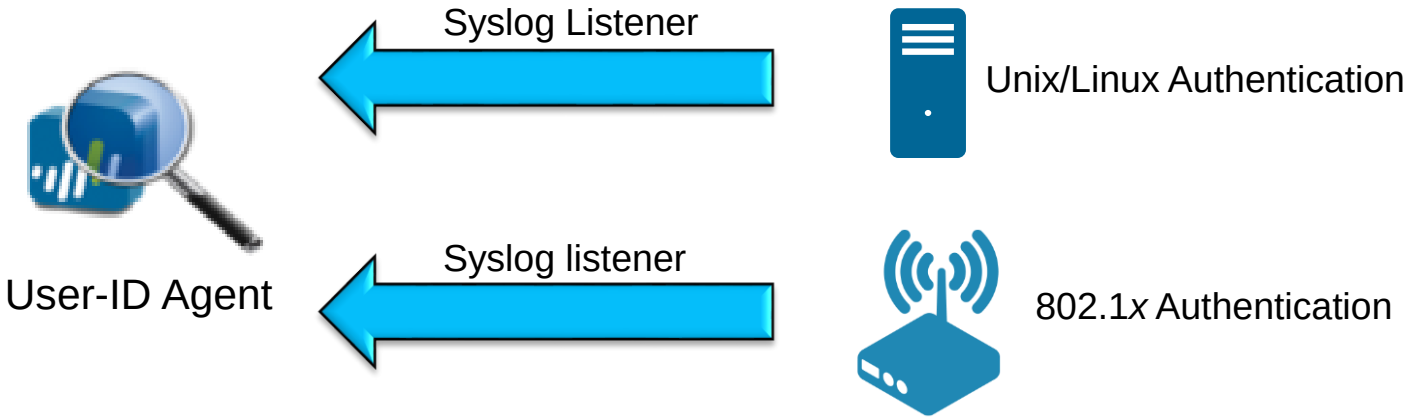
User Mapping Using GlobalProtect

- 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.

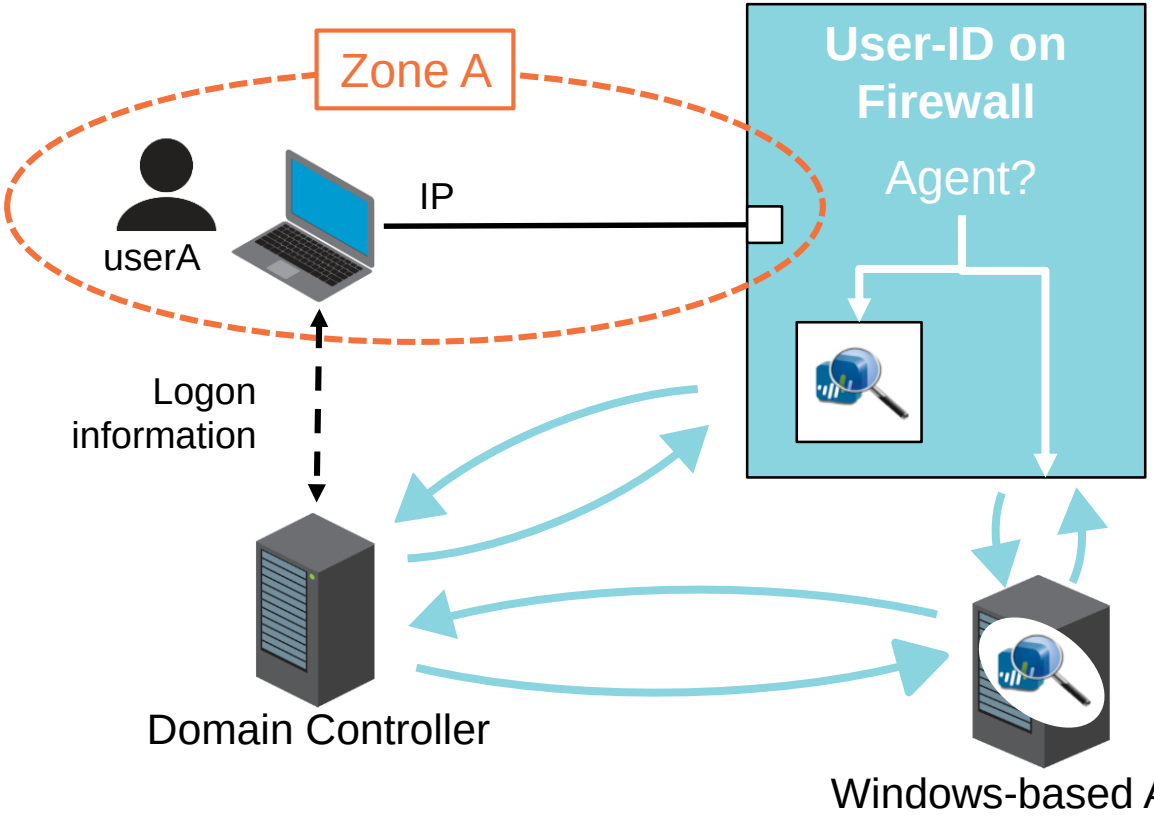


User-ID Syslog Monitoring

- 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.



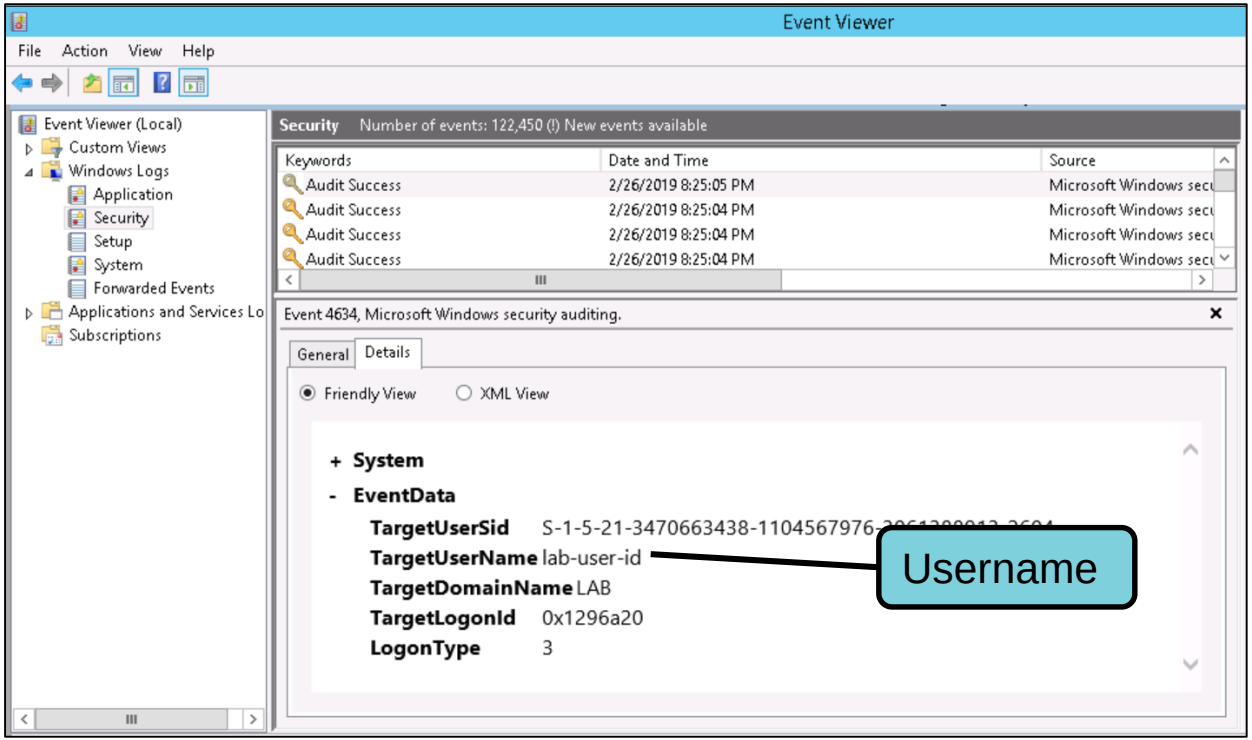
User-ID Operation Overview: Domain Controllers



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

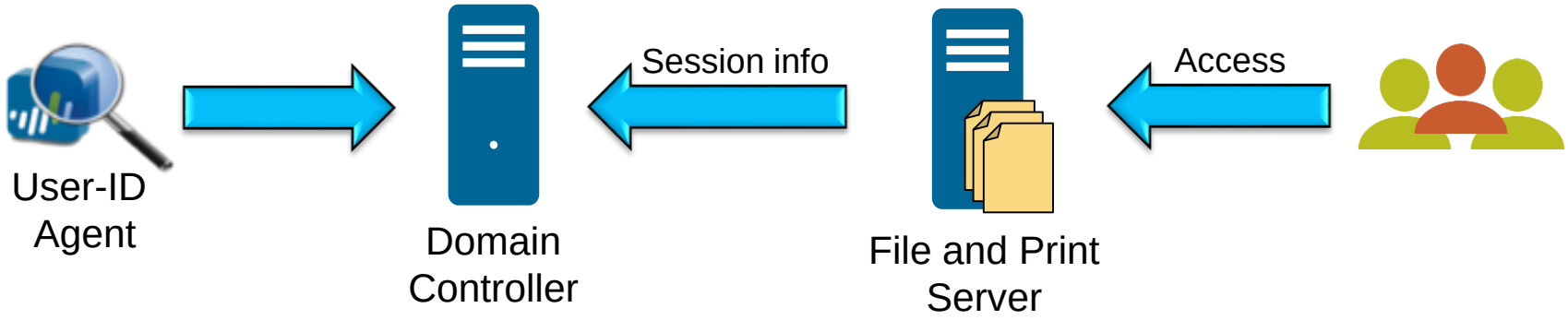
User-ID Domain Controller Monitoring

- 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, 802.1*x* 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

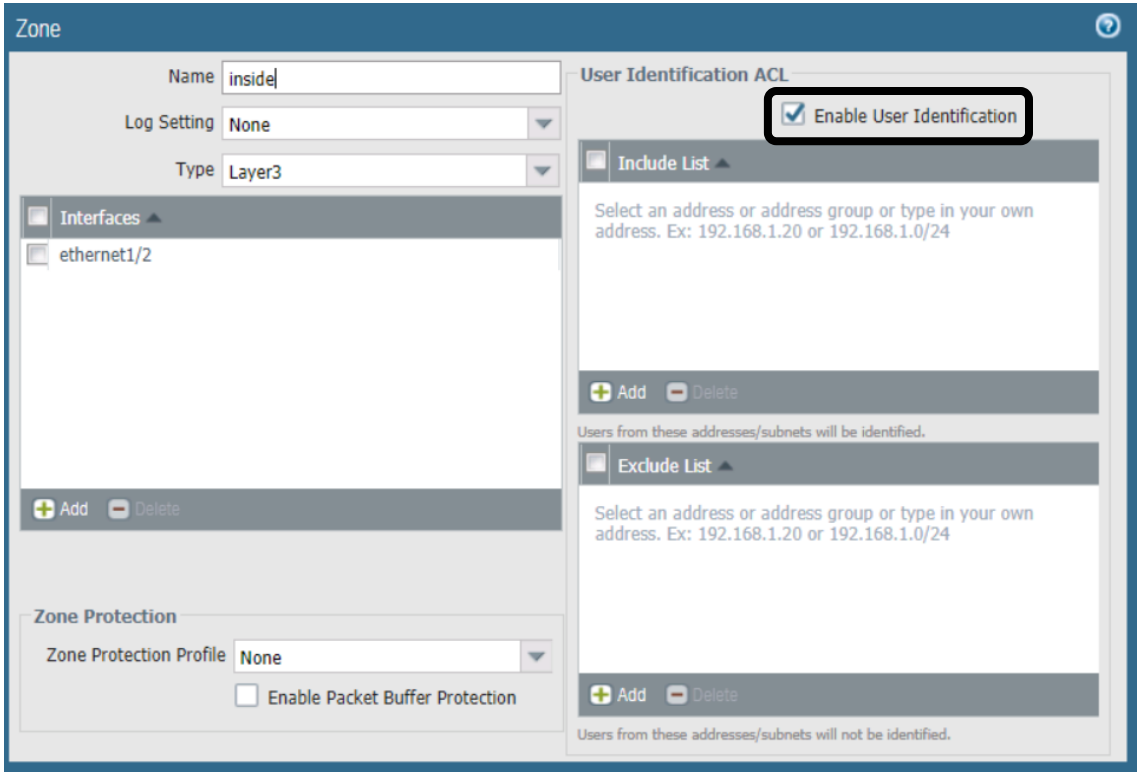
Configuring User-ID

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>



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

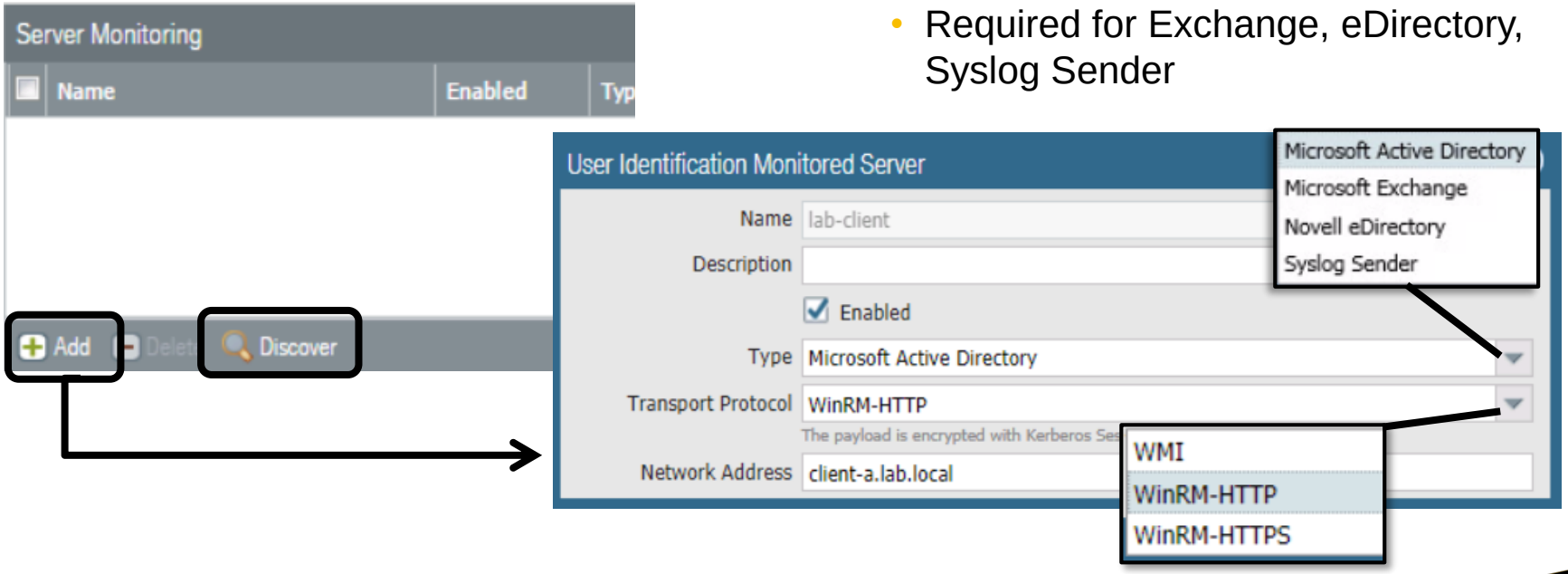
Configuring the PAN-OS Integrated User-ID Agent

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) *optional*
5. Configure WMI probing (optional) *optional*
6. Commit the configuration and verify agent connection status

Defining the Monitored Server(s)

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

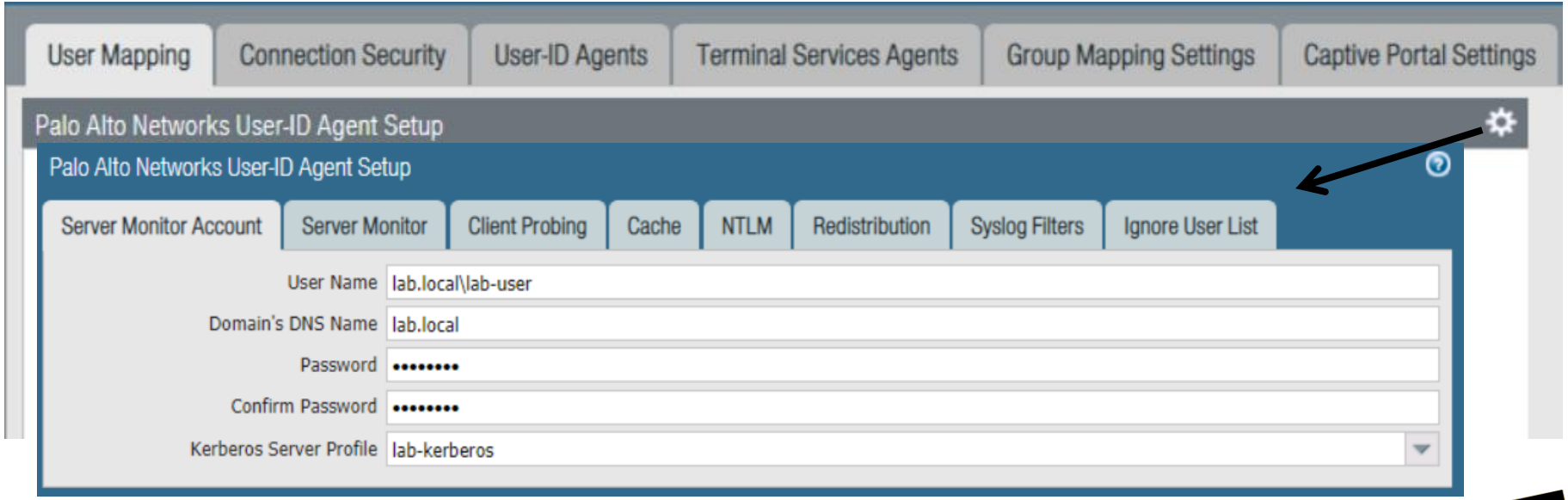
Device > User Identification > User Mapping



Defining the User-ID Agent Account

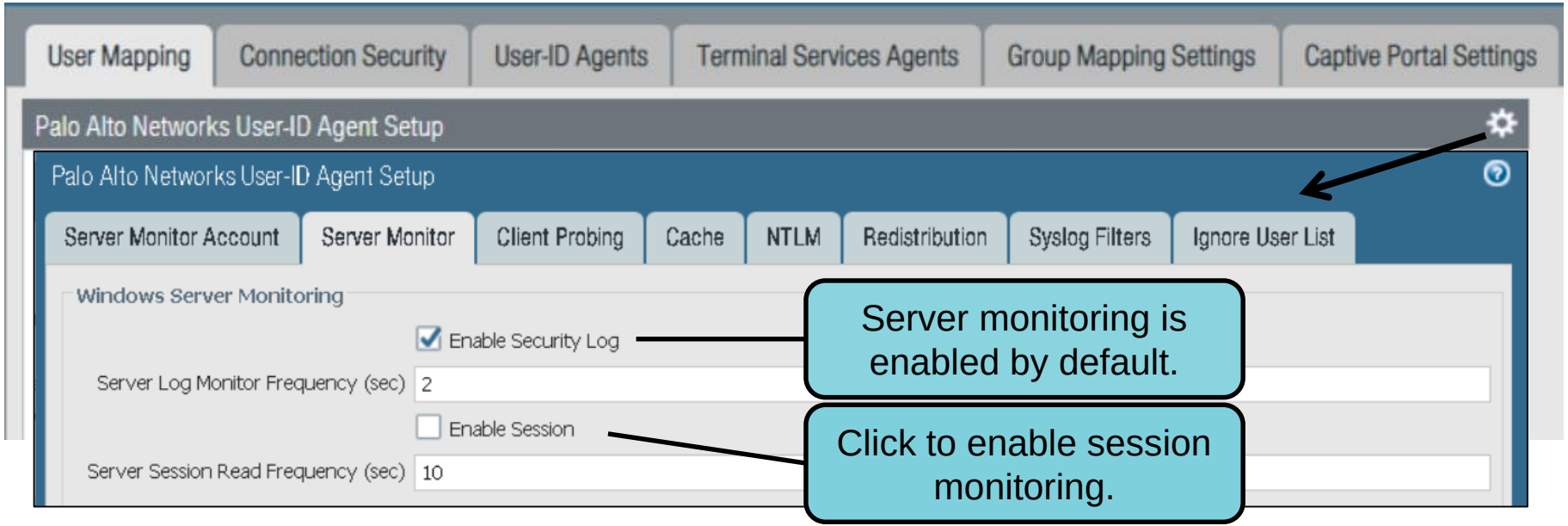
- Necessary permissions are provided if the agent account belongs to:
  - Domain Administrators group, or
  - Server Operators and Event Log Readers groups

Device > User Identification > User Mapping



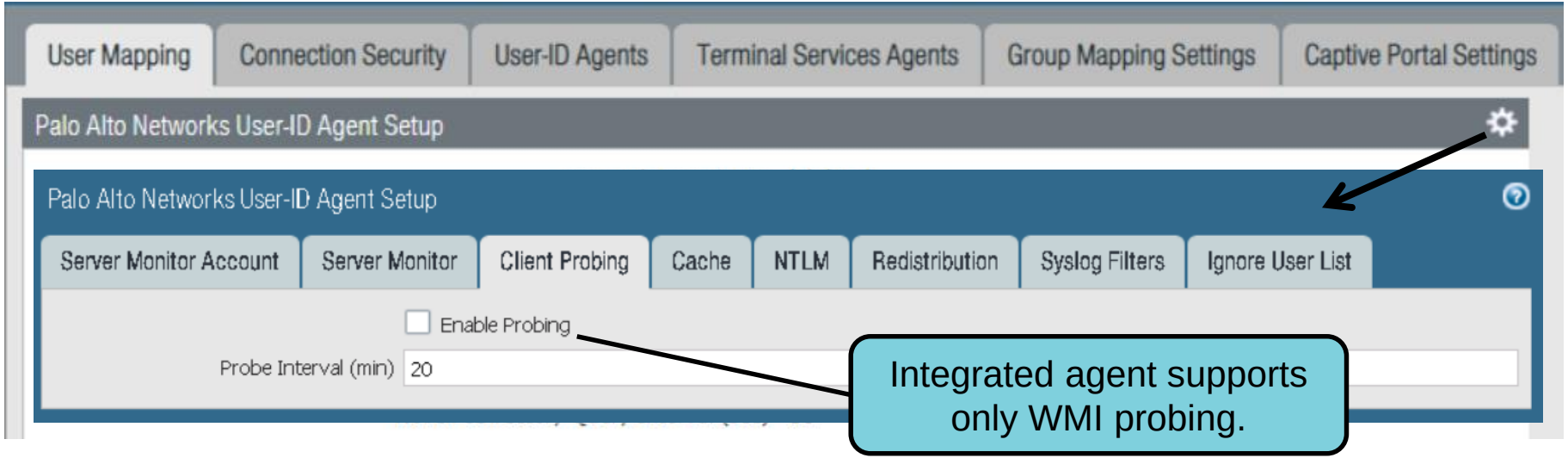
Optional Session Monitoring

Device > User Identification > User Mapping



Optional WMI Client Probing

Device > User Identification > User Mapping



Verifying Connection Status

Device > User Identification

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

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	☑	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

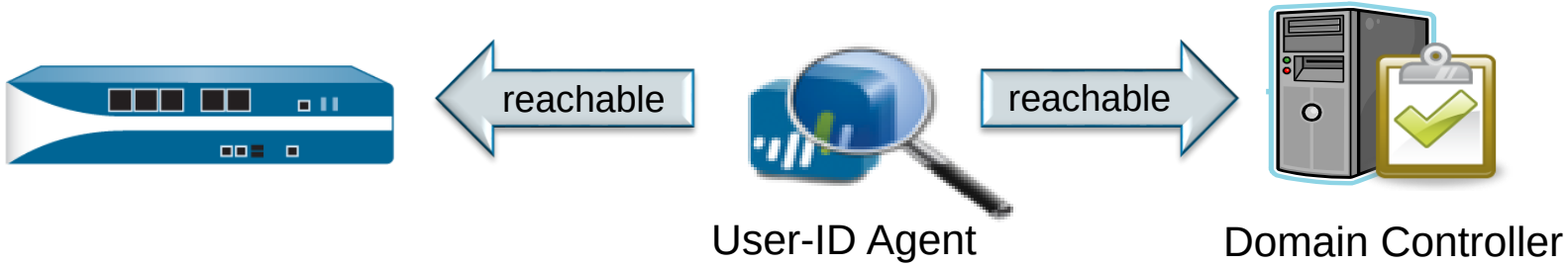
User-ID and security policy

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

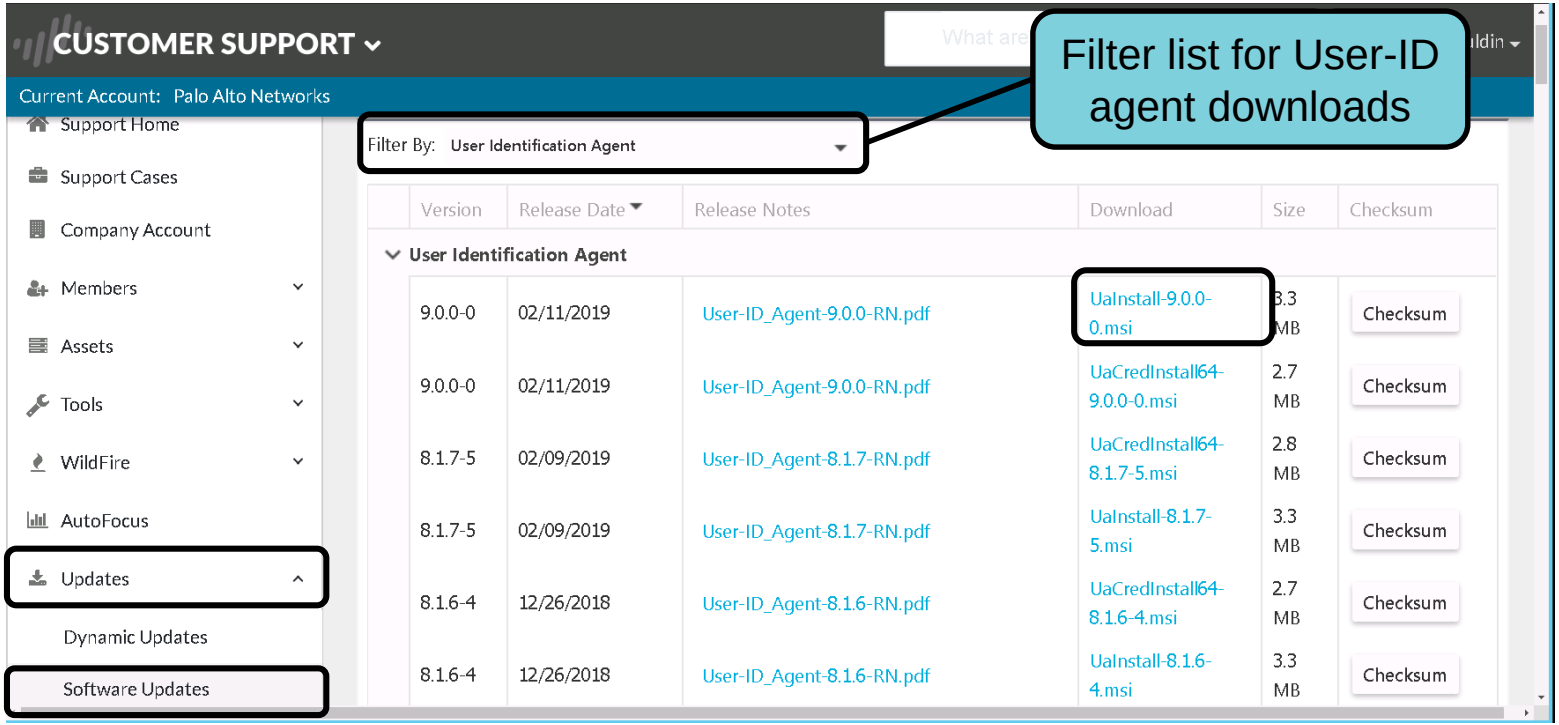
Selecting the Installation Location

- 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

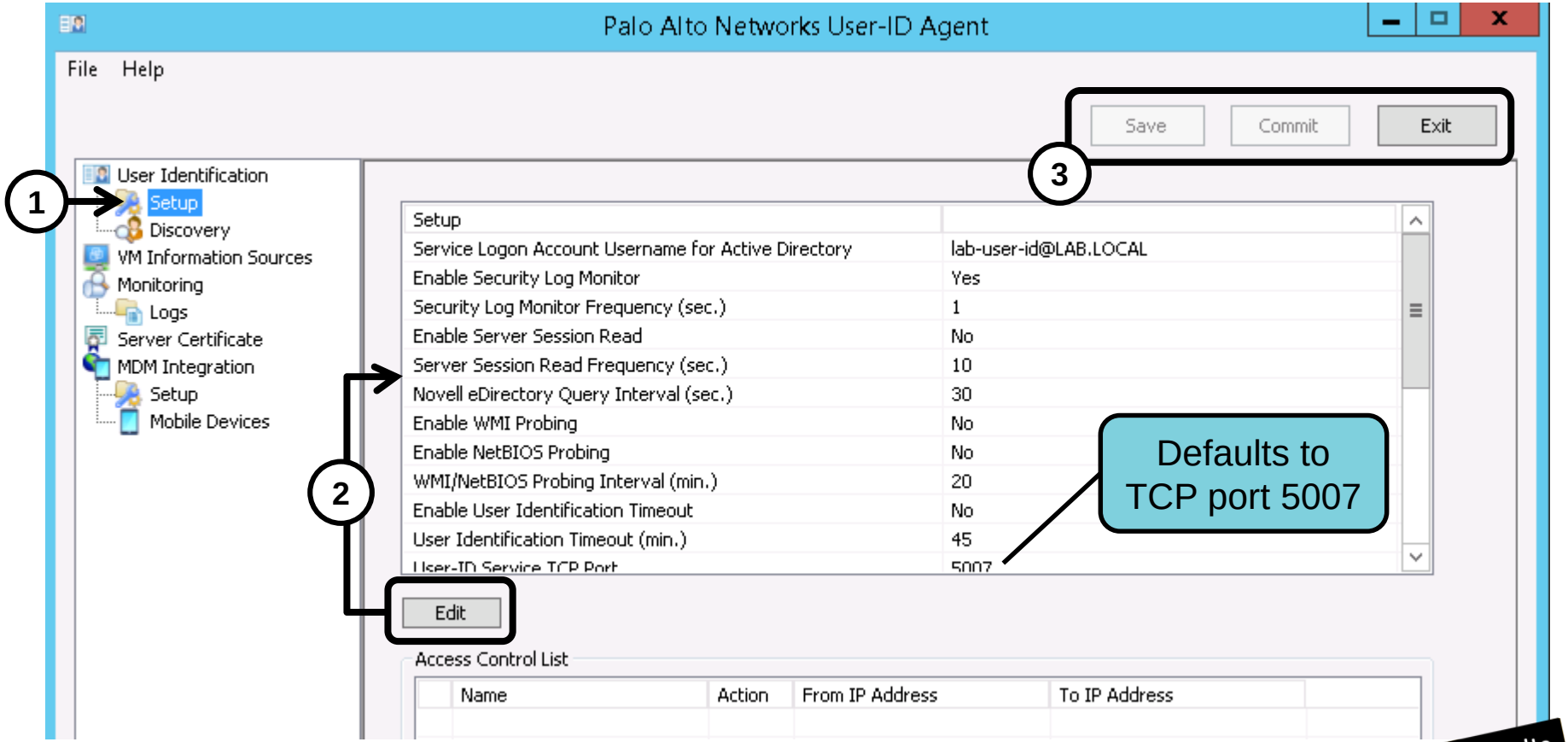


Download User-ID Agent Software

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



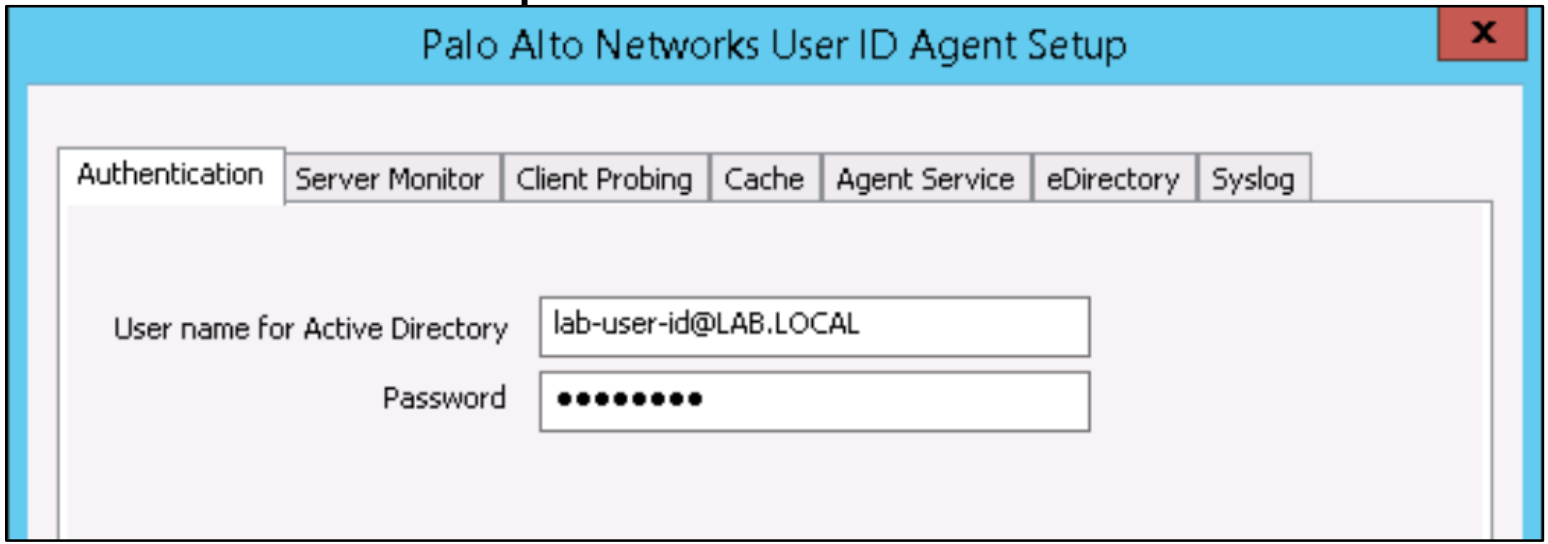
Agent Setup Process



Configuring the User-ID Agent Account

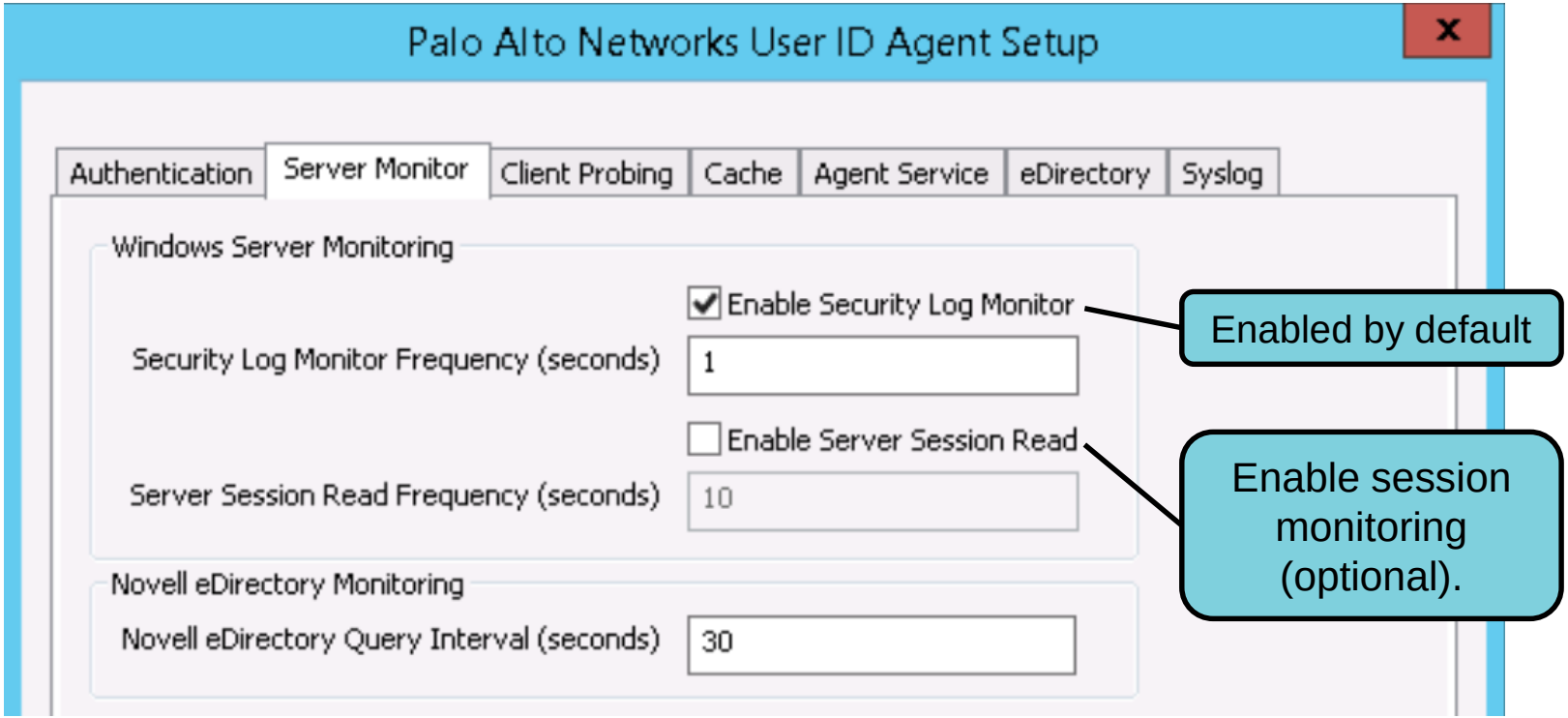
- Necessary permissions are provided if the agent account belongs to:
  - Domain Administrators group, or
  - Server Operators and Event Log Readers groups

User Identification > Setup > Edit



Configuring Server Monitoring

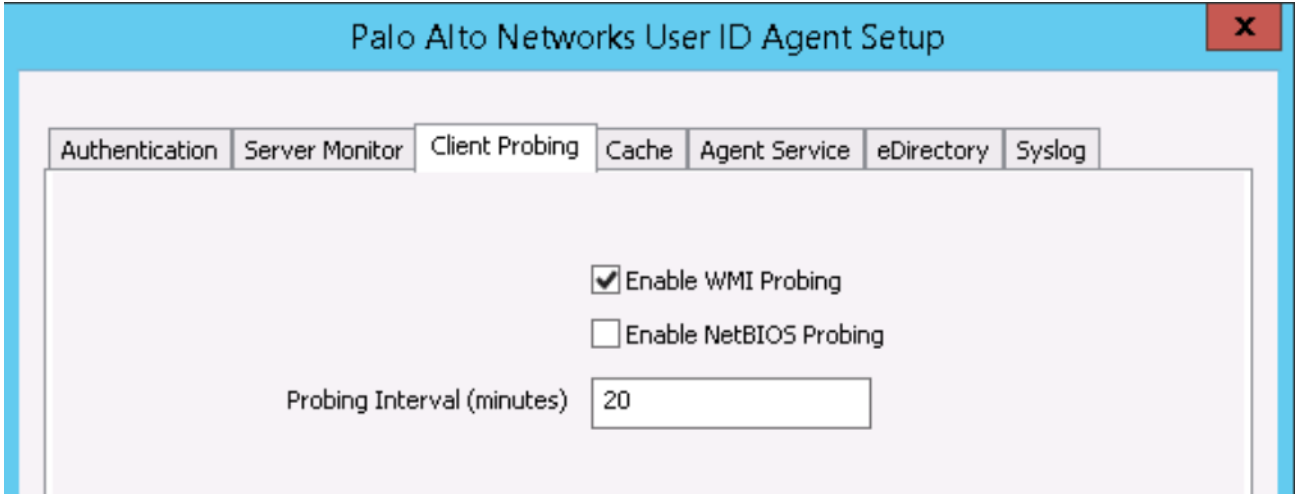
User Identification > Setup > Edit



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



Configuring the Monitored Servers

Palo Alto Networks User-ID Agent

File Help

Save Commit Exit

- User Identification
  - Setup
  - Discovery
- VM Information Sources
- Monitoring
  - Logs
- Server Certificate
- MDM Integration

Servers

	Name	Type	Network Address
☐	lab-client	active-directory	192.168.1.20
☐	lab-client1	edirectory	192.168.1.21
☐	mail-server	exchange	192.168.1.22

Add Edit Delete Auto Discover

Include / Exclude list of configured networks

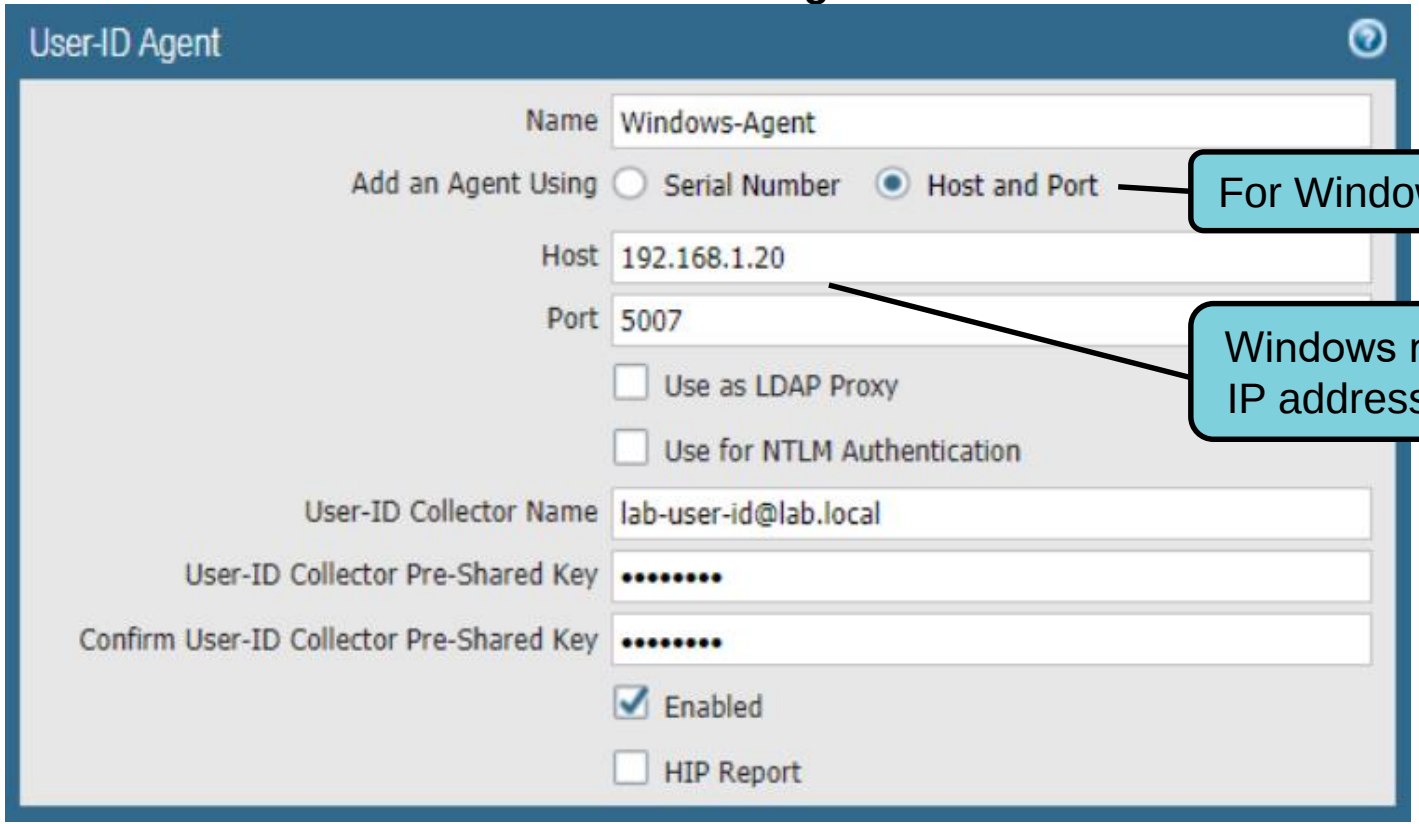
Name	Discovery	Network Address

Manually add Domain Controllers, Exchange, eDirectory, and syslog senders.

Domain Controllers only

Configuring the Firewall to Connect to the Agent

Device > User Identification > User-ID Agents > Add



For Windows agents

Windows machine's IP address and port

Confirm Connection to the User-ID Agent

Device > User Identification

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

1 item

Name	Enabled	Serial Number	Host	Port	User-ID Collector Name	Proxy	NTLM Auth	Connected
Windows-Agent	✓		192.168.1.20	5007	lab-user-id@lab.local			●

Connection from firewall's perspective – green is good

Palo Alto Networks User-ID Agent

File Help

Save | Commit | Exit

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

Agent Status

Agent is running — Start | Stop

Connected Devices

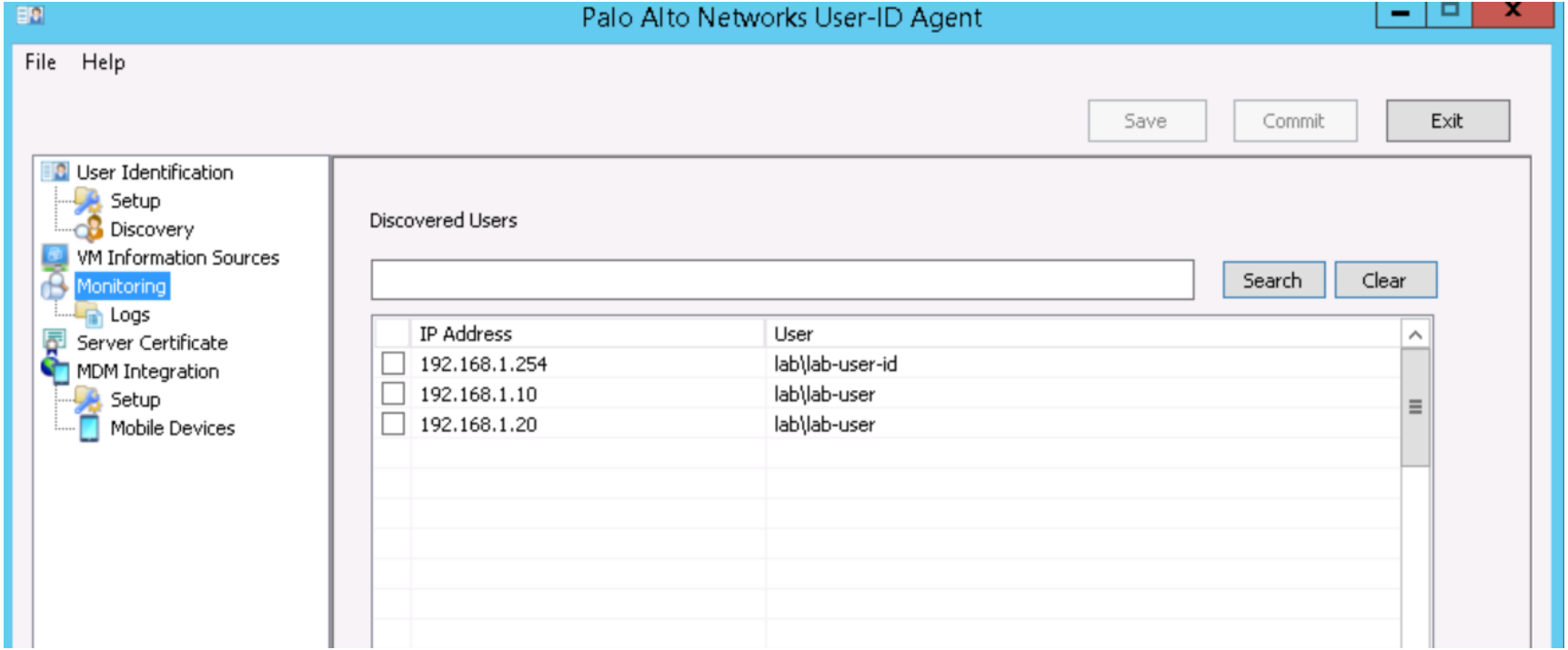
Device Address	Status
192.168.1.254 : 54084	Connected

Connected Servers

Server	Type	Status
lab-client(192.168.1.20)	Microsoft Active Directory	Connected

Connection from agent's perspective

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
```


User-ID overview

User mapping methods overview

Configuring User-ID

PAN-OS integrated agent configuration

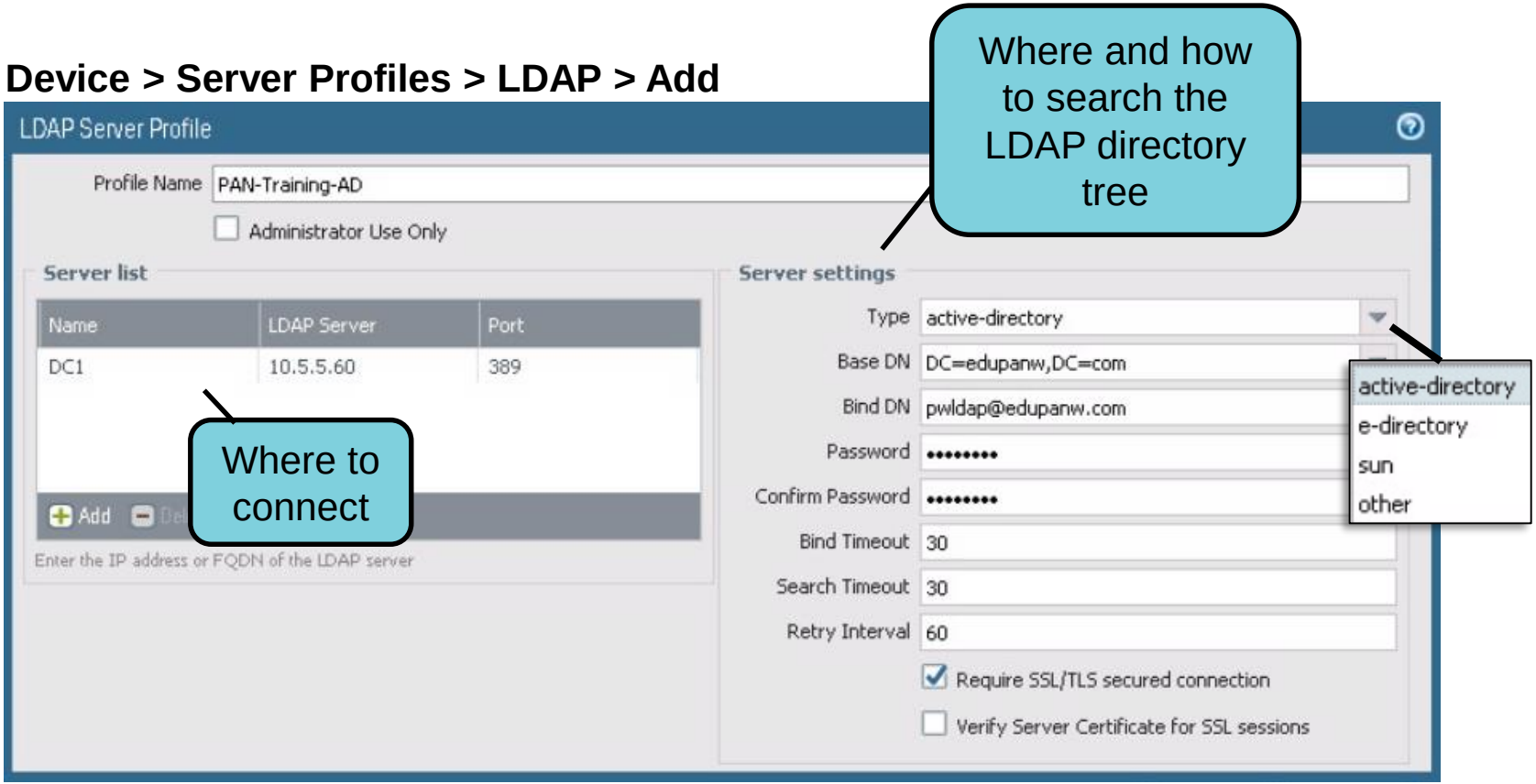
Windows-based agent configuration

Configuring group mapping

User-ID and security policy

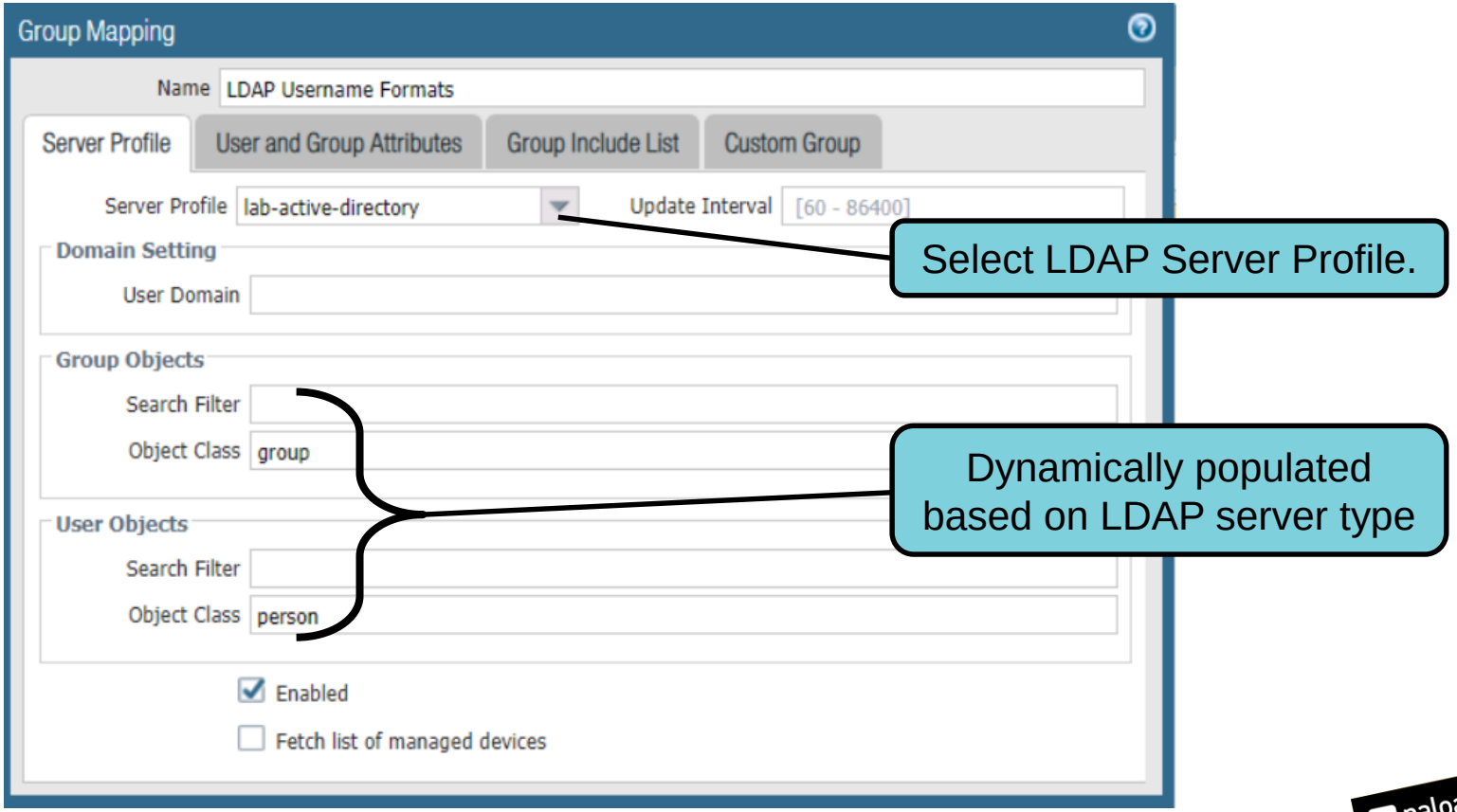
LDAP Server Profile

Device > Server Profiles > LDAP > Add



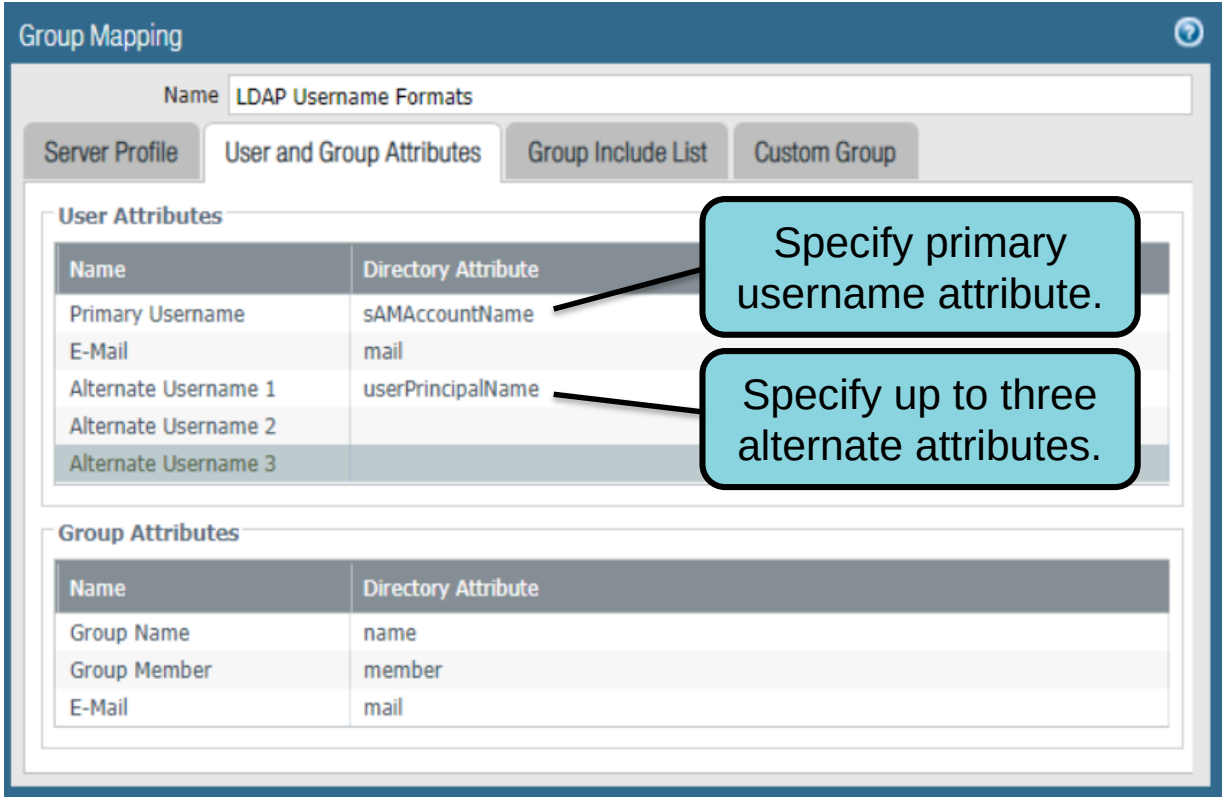
Creating User-ID Group Mapping Filters

Device > User Identification > Group Mapping Settings > Add



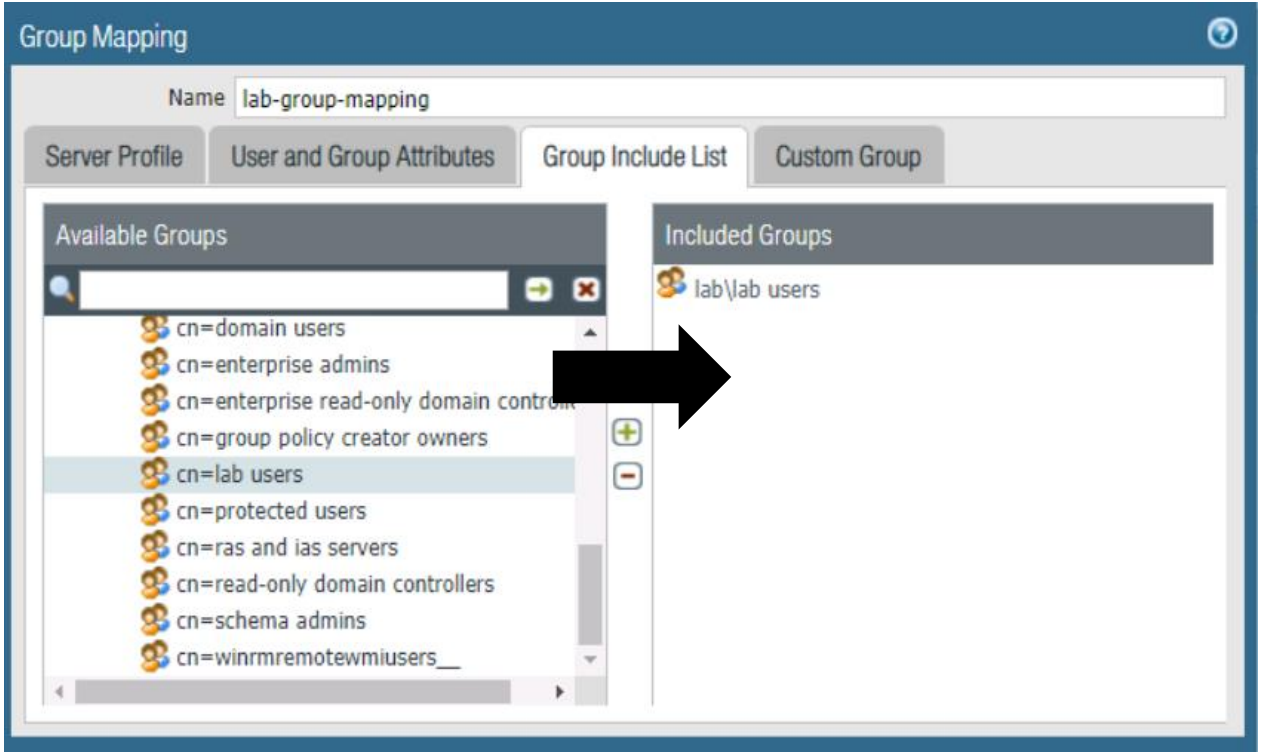
Multiple Username Formats

Device > User Identification > Group Mapping



Filtering Groups Sent to the Firewall

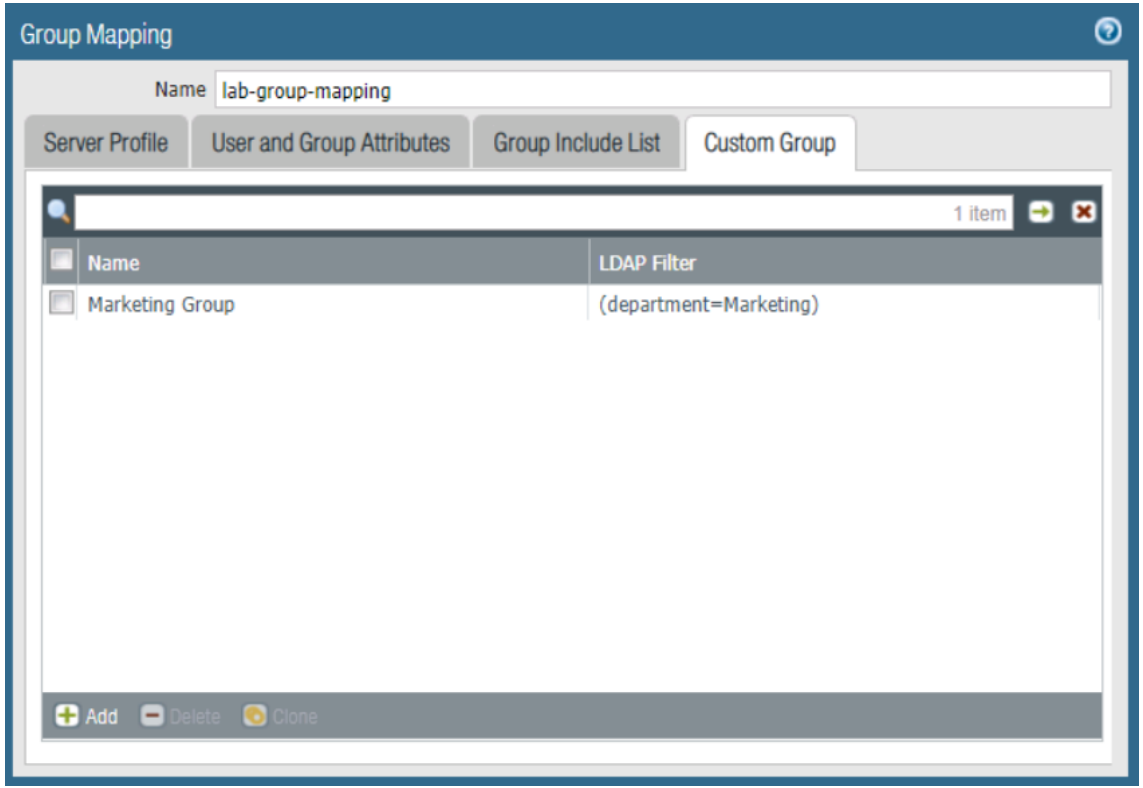
Device > User Identification > Group Mapping Settings > Add



- 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



- 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

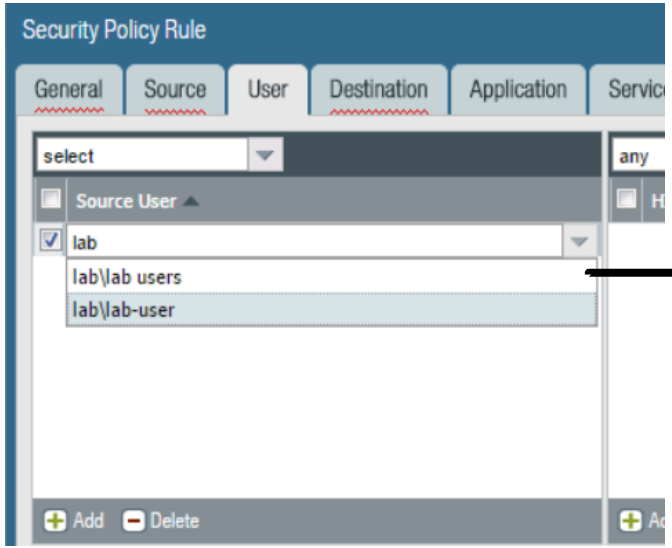
Windows-based agent configuration

Configuring group mapping

User-ID and security policy

Selecting Users and Groups for a Security Policy

				Source				Destination		Rule Usage						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Hit Co...	L... Hit	First Hit	URL Cate...	Application	Service	Action
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-logon
  - 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.

paloalto NETWORKS®

This page intentionally left blank