Firewall Configuration

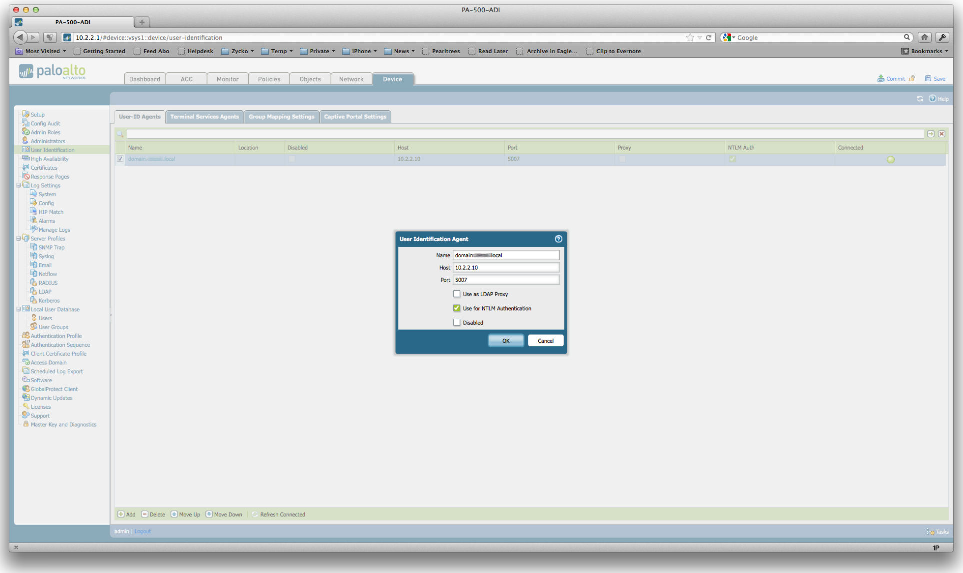
Version 4.1

After you installed the Agent the next step is to configure the firewall to be able to talk to the agent and retrieve the User/IP-Address mappings.

Since Version 4.1 you're not restricted to a single domain anymore, i.e. a single Agent installation can monitor several domains within a forrest.

Communication settings

The first thing to do is to configure the firewall so it can talk to the agent. Go to "Device" --> "User identification" and choose the tap "User-ID Agents" and click "Add".



Name	Location	Disabled	Host	Port	Proxy	NTLM Auth	Connected
☑ domain.[redacted].local		□	10.2.2.10	5007	□	☑	●

User Identification Agent

Name: domain[redacted]local
Host: 10.2.2.10
Port: 5007
□ Use as LDAP Proxy
☑ Use for NTLM Authentication
□ Disabled

OK | Cancel

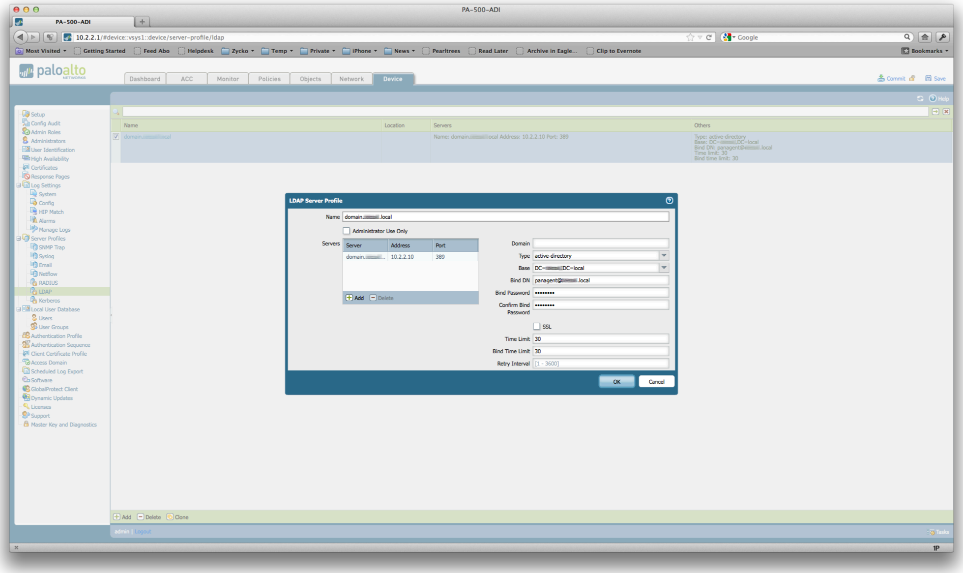
Give it a name and the TCP Port (see Agent Installation) for more details. TCP/5007 is the default setting. If the configured server acts as a LDAP proxy mark the check box. If you want to use this server for NTLM Authentication in the Portal as well, mark the NTLM check box. You can disable the server without deleting it if required.

Click "OK" and commit. After that, the "connected" indicator should become green. If not, check the Firewall settings on the server where the agent is installed for allowing TCP/5007 communication and also check whether the User-ID Agent service runs properly.

Add LDAP Server

The next step is to configure the LDAP Server Object. Go to "Device" --> "Server Profiles" --> "LDAP" and click

"Add"



PA-500-ADI

10.2.2.1/#device::vsys1::device/server-profile/ldap

Name	Location	Servers	Others
☑ domain.[redacted]ocal		Name: domain.[redacted]ocal Address: 10.2.2.10 Port: 389	Type: active-directory Base: DC=[redacted],DC=local Bind DN: panagent@[redacted].local Time limit: 30 Bind time limit: 30

LDAP Server Profile

Name: domain.[redacted].local

□ Administrator Use Only

Servers:

Server	Address	Port
domain.[redacted]...	10.2.2.10	389

Domain:
Type: active-directory
Base: DC=[redacted]DC=local
Bind DN: panagent@[redacted].local
Bind Password: ••••••••
Confirm Bind Password: ••••••••
□ SSL
Time Limit: 30
Bind Time Limit: 30
Retry Interval: [1 - 3600]

- Give it a name and add any Windows AD Server to the list. The default Port for LDAP is 389.
- Leave the "Domain" filed black if you want to be able to work with more than one domain in a forrest. Choose "active-directory" as the type.
- Configure the BIND-DN and Password. Here you can use the ID of the user created for the User-ID Agent service in the form of userid@domain.tld (you do not need the LDAP syntax like cn=Administrator, dc=domain, dc=tld)
- Check or uncheck the SSL tick box depending on whether you need encrypted communication or not.
- **Do not configure anything in "Base" yet**. (it'll not work, as the config with Bind DN and password has not been committed yet)

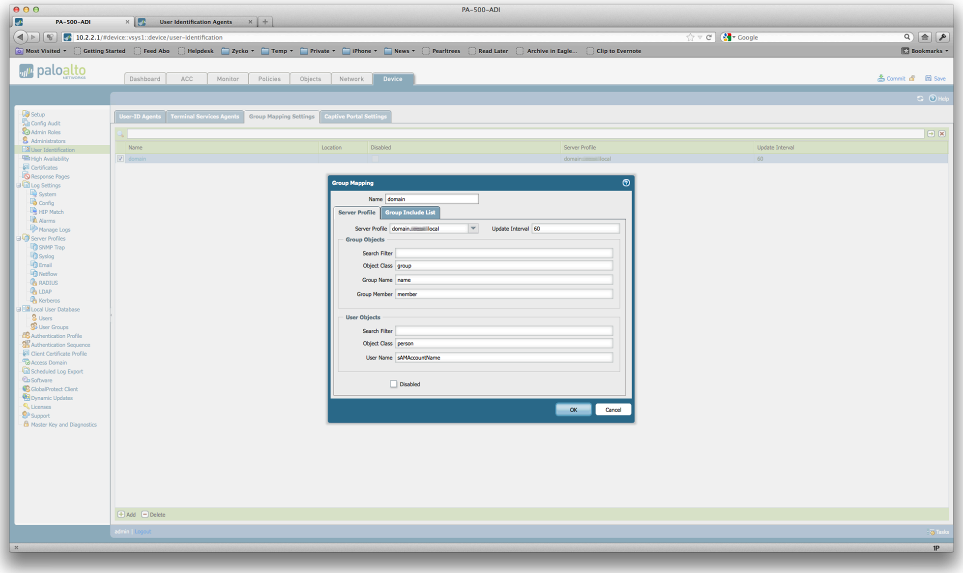
Click OK and commit the configuration.

Click on the created LDAP Server and the click on the selector at the "Base DN" field. If anything is properly confirgured you should get a list of OUs of your domain. If you want to restrict user-ID/IP Address mapping to a Base DN you can do that here otherwise live the field blank.

Configure Group Mappings

The last step is to configure the group mappings. This is helpful when you want NTLM authentication for e.g. Portal or redirect pages and want to use Active Directory Groups instead of single users.

Go to "Device" --> "User Identification" and click on the tap "Group Mapping Settings". Click on "Add".



Group Mapping

Name: domain

Server Profile | Group Include List

Server Profile: domain.[redacted]local
Update Interval: 60

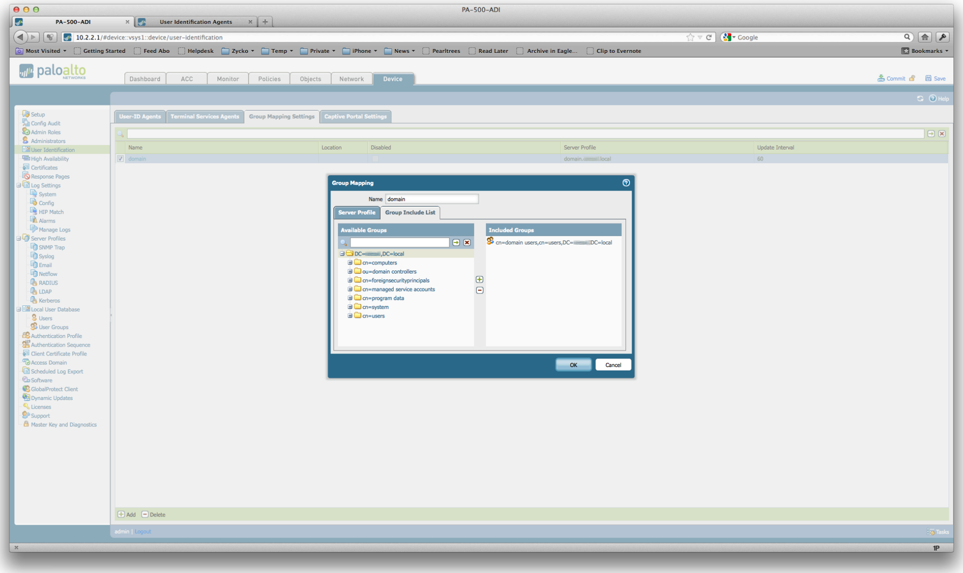
Group Objects
Search Filter:
Object Class: group
Group Name: name
Group Member: member

User Objects
Search Filter:
Object Class: person
User Name: sAMAccountName

□ Disabled

- Give the Element a name (you can freely choose)
- Select the just created LDAP Server for "Server Profile"
  - As the LDAP Server has been configured for active-directory, all required fields get populated automatically.
  - You can leave the Update Interval at 60 unless you have frequent changes in your domain.

Now click on the "Group Include List" tap:



Group Mapping

Name: domain

Server Profile | Group Include List

Available Groups
- DC=[redacted],DC=local
  - cn=computers
  - ou=domain controllers
  - cn=foreignsecurityprincipals
  - cn=managed service accounts
  - cn=program data
  - cn=system
  - cn=users

Included Groups
- cn=domain users,cn=users,DC=[redacted]DC=local

If you have configured the LDAP Server correctly, you'll see the Base DN in the "Available Groups" filed. Here you can choose OUs / DNs you want to include in the User/IP-Address Mapping. In order to lower the workload you should be as specific as possible, especially if you have a quite big domain.