How To Enable LDAP Authentication
Objective

This document explains the configuration of External Authentication to an LDAP (Active Directory) Server.

Details

Supported Versions

R75.40 to R77.xx
(This article was written using R77.)

Supported OS

- Security Management: Windows, SecurePlatform, GAIA
- Security Gateway: Windows, SecurePlatform, GAIA, IPSO

Before You Start

Prerequisites and Limitations

- Security Management requires the CPSB-UDIR license (R70 and higher) or CPFW-AM (below R70/legacy)
- This document does not enable or configure the Identity Awareness blade. Even though it uses LDAP, these features are separate from each other.
- LDAP Server already configured and running.

Impact on the Environment and Warnings

- None

Setting Up External Authentication

Enable User Directory in Global Properties:
1. Launch SmartDashboard and connect to the Security Management Server.
2. Click Policy menu > Global Properties > User Directory.
4. Click OK.
5. Install policy.
Create User Template:

When using LDAP Authentication, we need to map LDAP users to a user template.

1. Go to Users and Administrators object tab.
2. Right-click Templates and select New template.
3. Enter a name for the template.
4. Click Authentication > Check Point Password.
5. OPTIONAL: You can extend the configuration by assigning details on Groups, Location, or Time.
   The settings in the Encryption page are not relevant.
Create LDAP Account Unit:

The LDAP Account unit links the Security Gateway and the LDAP server.

1. Right-click Servers and OPSEC Applications and select New > LDAP Account Unit.

2. In the General tab, enter a name for the Account Unit.
3. From **Profile**, select the profile that best matches your LDAP architecture.
4. Enter the domain of the LDAP server.
5. Click **CRL retrieval** and **User management**.
6. Click **Enable Unicode support**, if necessary.
7. Open **Servers**.
8. Click Add and then New (unless there is a host object already defined).
9. In Username, enter the login name of the admin account.
10. In Login DN, enter the full DN of the admin account.
   For example: cn=UserAccount, cn=users, DC=Testdoamin, DC=org
   The Login DN is for the Firewall. It must have administrator privileges, to be able to fetch user data from the LDAP.
11. Enter the admin password.
12. OPTIONAL: You can enable SSL encryption between the Security Gateway and the LDAP server. If you do, you must configure the LDAP server for this too. See your LDAP documentation on enabling LDAPs (LDAP over SSL).
13. Make sure the port is the default 389.
14. Click OK.
   In versions R65 and earlier, select Early Versions Compatibility server.
15. Open Objects Management.
16. Select your LDAP Server and click **Fetch Branches**.
   These branches will be searched when this LDAP server is queried. You can add or modify the branches. Make sure to add all required branches that are not automatically fetched. If a user is in a branch that is not listed here, the Firewall will not be able to validate credentials for that user.

17. OPTIONAL: This account unit object can be locked with a password when accessed. Click **Prompt for password when opening this Account Unit**.

18. Open **Authentication**.
19. Make sure that **Use common group path for queries** is not selected.

20. Make sure that **Allowed authentication schemes > Check Point Password** is selected.

21. In **User's default values**, click **Use user template** and select the template created earlier.

22. **OPTIONAL**: Click **Limit login failures** and define the number of login attempts before account locking.

23. Click **OK**.

24. If you have multiple LDAP Servers (Domain controllers), repeat the steps to add your servers. For each LDAP server object, make sure that the **Default Priority** value is unique among the servers.

**Create an LDAP User Group:**

*This is required so that you can use the user group in the Security Policy.*

1. Right-click **Users and Administrators objects tab > LDAP Groups** and select **New LDAP Group**.
2. Enter a name for the group.
3. Select the LDAP Account unit from the drop-down list.
4. OPTIONAL: Assign scopes to this LDAP Group.
5. Click OK.

Create Security Rules that use External LDAP User Group in the Security Policy:
The most common use of this configuration is for Remote Access VPN. You can also create legacy Client Authentication rules with the same LDAP User Groups.

- For a Remote Access VPN, right-click the Source column and select Add Objects > Add Legacy Users Access. Make sure the LDAP group is in the Remote Access VPN community.
- For a Client Auth rule, right-click the Action column and select Legacy and Client Auth.

Completing the Procedure

- Install policy.
Verifying

Test communication between the gateway and the LDAP server. Run:

```
ldapsearch -h <LDAP server IP> -D "cn=<your CN>,cn=users,dc=<your DC>,dc=com" -b "dc=<your DC>,dc=com" -w <password> "cn=*" > ldap.out
```

See that the data is taken from the server and in the output file.

Test the features that you require users to authenticate. Users login with LDAP login name and password as normal.

For example, if you configured Remote Access VPN: When building the VPN site on the client machine, the authentication method is "Username and Password". When connecting, the user will use their LDAP credentials.

If you configured Client Auth rules, the user will use their LDAP credentials when prompted by the security gateway.