LDAP Authentication on-premise

When hosting the system on-premise, additional configuration is required to enable LDAP / Active Directory authentication.

Tomcat Service Account

The application server (Tomcat) must run under a user account that has permission to query the Active Directory.

- Configure the Tomcat service to run as a dedicated **Active Directory user**
- Ensure this user has:
  - Read access to the directory
  - Permission to perform user lookups

LDAPS Certificate Configuration

If you are using **LDAPS (recommended)**, the LDAP server's SSL certificate must be trusted by Java.

You must import the LDAP server certificate into the Java **keystore (truststore)** used by Tomcat.

Steps to Import Certificate

1. Export the SSL certificate from your LDAP / Domain Controller
2. Import the certificate into the Java keystore using:

```
keytool -importcert \
-alias ldap-cert \
-file ldap_certificate.crt \
-keystore $JAVA_HOME/lib/security/cacerts
```

3. Restart Tomcat after importing the certificate

Steps Using Portecle

1. Download and start **Portecle**
2. Open the Java keystore:
   - Path:
     `$JAVA_HOME/lib/security/cacerts`
3. Enter the keystore password
   (Note: the default password `cacerts` is often changed in secure environments)
4. Import the LDAP / Active Directory certificate:
   - Go to **Tools → Import Trusted Certificate**
   - Select your exported certificate file (e.g., `.crt`)
5. Assign an alias (e.g., `ldap-cert`)
6. Save the keystore
7. Restart Tomcat

Important Notes

- The default Java keystore password (`cacerts`) is **often changed** in secure environments
  → Please confirm the correct password with your system administrator
- If the certificate is not trusted:
  - LDAPS connections will fail
  - Authentication will not work
- Ensure the correct Java runtime is used (the one running Tomcat)

Recommendation

- Always use **LDAPS (port 636)** instead of plain LDAP for secure communication
- Use a **dedicated service account** rather than a personal user account

---

Revision #1
Created 7 April 2026 15:58:21 by Admin
Updated 7 April 2026 17:22:56 by Admin