LDAP TLS setup

You can integrate Teamwork Cloud (TWCloud) with TLS-enabled Microsoft Windows Active Directory.

To complete this integration successfully, the following requirements should be passed:

- Windows Server Active Directory should have TLS enabled. This includes a valid Certificate Authority (CA) and a valid certificate for Active Directory (AD) server certificate (for more information on installing and configuring Certificate Services for Windows Server, see Microsoft documentation).
- Any TLS-aware LDAP client should be able to connect to your AD server port 636 with TLS-enabled and should have access to its contents (for more information on setting TLS-enabled connections to AD, refer to the specific LDAP client documentation).

Warning

Do not include private keys while exporting.

To export TLS certificates to be used for communication with TLS-Enabled Active Directories (LDAP) in TWAdmin console

---

- Export the CA and AD server certificates to the DER encoded binary.cer files using the Microsoft Management Console, the Certificates Snap-in.

The subsequent steps for the TWCloud integration with TLS-enabled Active Directory are the same as for the integration with any other LDAP server. This procedure is described in TWCloud documentation, section Enabling a secure connection.