

Preparing your Windows Server for AD LDAPS access

We recommend using **LDAPS** for your Active Directory connection to ensure your user data is encrypted in transit on your network between your Active Directory server and your DrawBridge.

However, while Windows Active Directory Server listens on port 636, it will reject all requests unless a security certificate has been configured for it.

(It is Not necessary to install an extra LDAPS function on your Windows Server to use the AD-LDAPS connection.)

Check if a security certificate has been configured

1. Go to Start and open Run. Enter `mmc` and click Run
2. Under the `File` menu, click `Add/Remove Snap-ins...`
3. In the wizard, under available snap-ins, select **Certificates**, and click Add, then OK
4. For the Certificates Snap-in, select `Computer account`, and click Next
5. For the Select Computer options, ensure `Local Computer` is selected, and click Finish
6. In the tree view on the left, under Certificates, expand out the Personal directory. If this directory, or a Certificates sub-directory is empty, *the AD server doesn't have a security certificate it can use for the LDAPS connection*. Proceed with the Setup steps below.

Set up a new CA and issue a security certificate

1. Go to Server Manager, and click **Add Roles and Features**
2. Click Next
3. Ensure `Role-based or feature-based installation` is selected, and click Next
4. Ensure `Select a server from the server pool` is selected, as well as a server in the Server Pool list, and click Next

5. Select the box for **Active Directory Certificate Services**, and click Next
6. Don't select anything under Features, and click Next
7. Read over comments in AD CS, and click Next
8. Select **Certification Authority** in Role Services, and click Next
9. Optionally select `Restart the destination server automatically if required` (or manually restart later), then click Install
10. After the installation is finished, click the link for **Configure Active Directory Certificate Services on the destination server**, and close the Add Roles and Features Wizard window.
11. In the AD CS Configuration window, click Next to proceed with the credentials of the user you're signed-in as (must have Administrator permissions)
12. Select **Certification Authority** under Role Services, and click Next
13. Ensure `Enterprise CA` is selected, and click Next
14. Select `Root CA`, and click Next
15. Select `Create a new private key`, and click Next
16. Select a minimum of `SHA256` for the hash algorithm, and click Next
17. Review the names suggested for the CA, and click Next
18. Use the default validity period of 5 years, and click Next
19. Review the database location, change if you wish, and click Next
20. Review what will be performed, and click Configure
21. It should report `Configuration Successful`, and you can close that window
22. Next, go to the Start Menu, open Run, and enter `certmpl.msc` and run it
23. In the **Certificate Templates Console**, right-click `Kerberos Authentication`, and click `Duplicate Template`
24. **Properties of new Template** will appear. Make the following changes:
 - General tab: set the Display Name to **DrawBridge LDAPS**
 - General tab: select `Publish certificate in Active Directory`
 - Request Handling tab: select `Allow private key to be exported`
 - Subject Name tab: ensure `Build from this Active Directory information` is selected, as well as the checkbox for `DNS name`
 - Click **Apply** and **OK**.
 - Close the Certificate Templates Console
25. Go to Start, and open **Certification Authority**
26. Right-click on `Certificate Templates`, then under `New`, click `Certificate Templates to Issue`
27. In the **Enable Certificate Templates** wizard, select `DrawBridge LDAPS` and click OK
28. Close the Certificate Authority window
29. Go to Start, open Run, and enter `mmc`, and Run
30. Under `File`, click `Add/Remove snap-in`
31. In the **Add/Remove Snap-in** window, select **Certificates**, then `Add >`, then click OK
32. Select `Computer account`, and click Next
33. Select `Local Computer`, and then click Finish
34. In the tree view on the left, expand the Personal folder
35. Under the Personal, right-click on `Certificates`, select `All Tasks`, then click `Request New Certificate...`
36. The **Certificate Enrollment** wizard will open, click Next
37. Under the Certificate Enrollment Policy, ensure `Active Directory Enrollment Policy` is selected, and then click Next

38. Under Request Certificates, select **DrawBridge LDAPS**, and click Enroll
 39. The wizard should support STATUS: Succeeded, click Finish
 40. That's it! If you opted to not automatically restart the server in step #9, restart the server now.
-

Revision #1

Created 26 March 2024 15:10:17 by Marvin M.

Updated 26 March 2024 15:41:20 by Marvin M.