Active Directory Encryption

Contents

You can use the encryption when communicating with a Windows Active Directory server.
Set according to the following order when using the encryption for the first time.

Step 1. Installing Active Directory Certificate Services

To use Windows Active Directory server encryption communication, you must install the Active Directory Certificate Services.
The Active Directory Certificate Services can be installed as follows:

1) On the PC where the Windows Active Directory server is installed, run **Server Manager**, and then click **Manage** > **Add Roles and Features**.
2) On **Before You Begin**, click **Next**.
3) On **Select Installation Type**, select **Role-Based or feature-based installation** and then click **Next**.
4) On **Select destination server**, select **Select a server from the server pool**, check the server, and click **Next**.
5) On **Select Server Roles**, select **Active Directory Certificate Services** and click **Next**.
6) When a pop-up window appears, view the details and click **Add Features** > **Next**.
7) View the details of **Active Directory Certificate Services** and click **Next**.
8) On **Confirm installation selections**, click **Install**. When installation is complete, click **Configure Active Directory Certificate Services on the destination server**.
9) When **AD CS Configuration wizard** appears, view the details and click **Next**.
10) On **Role Services**, click **Certification Authority** > **Next**.
11) On the **Setup Type** page, select **Enterprise CA** and click **Next**.
12) On the **Specify the type of the CA** page, select **Root CA** and click **Next**.
13) On the **Specify the type of the private key** page, select **Create a new private key** and click **Next**.
14) Set the **Cryptography for CA**, **CA Name**, and **Validity Period**, and then click **Next**.
15) On the **CA Database** page, set the **folder location for the certificate database** and the **certificate database log** and then click **Next**.
16) On **Confirmation** page, view the details of Active Directory Certificate Services and click **Configure**.

Step 2. Connecting IDAPS

1) Click **Start** > **Run**.
2) Enter **ldp** in the input field.
3) When the **Ldp-disconnected** window appears, click **Connect**.
4) Fill in **Server** and **Port** fields and select **SSL**. And then click **OK**.

Step 3. Copying the root certificate

1) Run Command Prompt on the PC where the Windows Active Directory server is installed.
2) Enter **certutil -ca.cert client.crt** command to copy the root certificate.

3) Enter **keytool -import -keystore ad.jks -file client.crt** command to convert the server certificate to .jks format.
4) Save the .jks-formatted server certificate to the BioStar 2 installation path.