To install AD CS

1. Log on as a member of both the Enterprise Admins group and the root domain's Domain Admins group.
2. Click **Server Manager** in the taskbar. The Server Manager console opens. Click **Add roles and features**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, ensure **Role-based or feature-based installation** is selected and click **Next**.
5. On the **Select destination server** page, ensure your server is selected and click **Next**.
6. On the **Select Server Roles** page, select **Active Directory Certificate Services**, and then click **Add Features** and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Active Directory Certificate Services** page, click **Next**.
9. On the **Select role services** page, ensure **Certification Authority** is selected and click **Next**.
10. On the **Confirm installation selections** page, click **Install**.

After installation completes, click close.

1. On the Server Manager Dashboard, click the Notifications flag icon and then click **Configure Active Directory Certificate Services on the destination server**.
2. On the **Credentials** page, ensure the default user account is a member of both the local Administrators group and the Enterprise Admins group and then click **Next**.
3. On the **Role Services** page, click **Certification Authority**, and click **Next**.
4. On the **Setup Type** page, ensure **Enterprise CA** is selected, and click **Next**.
5. On the **CA Type** page, ensure **Root CA** is selected, and then click **Next**.
6. On the **Private Key** page, ensure **Create a new private key** is selected, and then click **Next**.
7. On the **Cryptography for CA** page, keep the default settings for CSP (**RSA#Microsoft Software Key Storage Provider**) and hash algorithm (**sha1**), and determine the best key character length for your deployment. Large key character lengths provide optimal security, but they can affect server performance. It is recommended that you keep the default setting of 2048 or, if appropriate for your deployment, reduce key character length to 1024. Click **Next**.
8. On the **CA Name** page, keep the suggested common name for the CA or change the name according to your requirements, and then click **Next**.
9. On the **Validity Period** page, in **Specify the validity period**, type the number and select a time value (Years, Months, Weeks, or Days). The default setting of five years is recommended. Click **Next**.
10. On the **CA Database** page, in **Certificate database location** and **Certificate database log location**, specify the folder location for these items. If you specify locations other than the default locations, make sure that the folders are secured with access control lists (ACLs) that prevent unauthorized users or computers from accessing the CA database and log files.
11. Click **Next**, click **Configure**, and then click **Close**.

Screen shots are attached in last



