How to set up automatic certificate enrollment in Active Directory

Overview

This topic describes the procedure to set up automatic certificate enrollment in Active Directory.

Setting up automatic certificate enrollment in Active Directory consists of the following steps,

1. **Step 1 - Create a security group**
2. **Step 2 - Create a Certificate Template to enroll**
3. **Step 3 - Add Certificate Template to the Certification Authority**
4. **Step 4 - Create group policy for auto enrollment**

Before you begin

- Your user account must be part of Enterprise Admins and Cert Publishers group.
- You must logon to Active Directory Certificate Server (AD CS).

**Step 1 - Create a security group**

To create a security group on Active Directory

1. On DC1, click **Start > Administrative Tools**, and then click **Server Manager**.
2. In the navigation pane, expand **Roles**, expand **Active Directory Domain Services**, expand **Active Directory Users and Computers**, expand **contoso.com**, right-click **Users**, click **New**, and then click **Group**.
3. In the **New Object - Group** dialog box, in the **Group name** text box, type a name for the group. Example: **AutoEnrollGroup**.
4. Click **OK**, Leave Server Manager running with the Computers container shown in the results pane.

https://docs.druva.com/Knowledge_Base/inSync/How_To/How_to_set_up_automatic_certificate_enrollment_in_Active_Directory

Updated: Mon, 24 Jun 2019 20:17:29 GMT

Powered by
Step 2 - Create a certificate template to enroll

To create a certificate template

1. Open the Certificate Templates Console
   1. From the Start menu, click Run.
   2. Type `certtmpl.msc` in the text box and click OK. Certificate Templates Console window appears on the page.
2. Right-click the User template, and then click Duplicate Template.

3. Under General tab,
   1. Type a Template display name. For example, User Auto Enroll.
   2. (Optional) Modify the default Validity Period and Renewal Period as per your requirements.
   3. Select Publish certificate in Active Directory check box.
   4. Select Do not Automatically reenroll if duplicate certificate exists in Active Directory check box.
4. Under **Request Handling** tab,

1. Ensure **Allow private key to be exported** check box is clear.

   **Important**: This ensures that the downloaded user certificates are useless by preventing a possible compromise of the server's private key.

2. Select **Enroll Subject without requiring any user input** option.
5. Click the **Cryptography** tab, enter **Minimum key size** as 4096.
6. Under **Security** tab,

1. In the Group or user name, click **Add** and type the name or browse to select the security group. For example, Auto Enroll group.

2. Select the security group and under **Permissions** dialog box, select the **Read**, **Enroll**, and **Autoenroll** check boxes.
7. Under Extensions tab,

1. Select the Application Policies extension, and click Edit. 
   Edit Application Policies Extension dialog box appears on the page.
2. Select and remove all other application policies except the Client Authentication application policy.
3. Click OK.
8. Click **Apply** and then click **OK**.
9. Close the **Certificate Templates Console**.

**Step 3 - Add certificate template to the certification authority**

To add certificate template to the certification authority

1. Open the **Certificate Authority**.
   1. From the **Start** menu, click **Run**.
   2. Type `certsrv.msc` and click **OK**.
2. Right-click **Certificate Templates**, click **New**, and then click **Certificate Template to Issue**.
3. Select the certificate template, for example - 'User Auto Enroll' in this case, and click **OK**.

4. Ensure the certificate template is added to your Certification Authority.
Step 4 - Create group policy for auto enrollment

To create a group policy for auto enrollment

1. Launch the Group Policy Management console.
   1. From the Start menu, click Run.
   2. Type `gpmc.msc` in the text box, and click OK.
2. In the left pane, on the Domain Controller, right-click and select Create a Gpo in this domain, and Link it here. New GPO dialog box appears on the page.
3. Type a Name for the group policy and click OK.
4. Right-click on the newly created group policy, and click Edit.
5. Go to User Configuration > Windows Settings > Security Settings > Public Key Policies and then under Object Type section in the right pane, select Certificate Services Client - Auto-Enrollment.
6. Right-click on **Certificate Services Client - Auto-Enrollment** and click **Properties**.

7. Under Enrollment Policy Configuration tab,
   1. For Configuration Model, select **Enabled** from the drop-down list.
   2. Select the following check boxes,
      - Renew expired certificates, update pending certificates, and remove revoked certificates
      - Update certificates that use certificate templates
   3. Click **OK**.
8. Save your changes and close the Group Policy Management console.