Certificate auto-enrollment and renewal

Many certificates can be distributed without the client interaction. These can include most types of certificates issued to computers and services, as well as many certificates issued to users.

To enroll clients automatically for certificates in a domain environment, you must do the following:

- Configure a certificate template with auto-enroll permissions

- Configure an auto-enrollment policy for the domain

Membership in Domain Admins or Enterprise Admins, or equivalent, is the minimum required to complete this procedure. In Exercise 22.3 we are going to configure a group policy to support the auto-enrollment feature.

Right-click the Default Domain Policy GPO and click Edit.

In the Group Policy Management Console (GPMC), go to User Configuration ➤ Windows Settings ➤ Security Settings and click Public Key Policies.

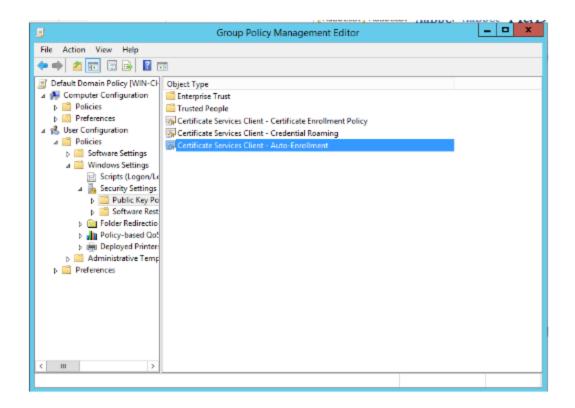Double-click Certificate Services Client – Auto-Enrollment.

Select the Enroll Certificates Automatically check box to enable auto-enrollment. If you want to block auto-enrollment from occurring, select the Do Not Enroll Certificates Automatically check box.

If you are enabling certificate auto-enrollment, you can select the following check boxes:

"Renew expired certificates, update pending certificates, and remove revoked certificates enables auto-enrollment for certificate renewal, issuance of pending certificate requests, and the automatic removal of revoked certificates from a user's certificate store."

"Update certificates that use certificate templates enables auto-enrollment for issuance of certificates that supersede issued certificates."

Click OK to accept your changes.