Knowledge Base

Default Permission Settings for an Enterprise Certificate Authority

PSS ID Number: 239706

Article Last Modified on 11/13/2003

The information in this article applies to:

- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server

This article was previously published under Q239706

SUMMARY

An Enterprise Certificate Authority (CA) provides certificate management for users and computers in Active Directory. The CA can issue and revoke certificates. This article describes basic information and the security settings necessary for the configuration of an Enterprise CA.

MORE INFORMATION

After installing an Enterprise CA, set the following permissions on the following Active Directory objects and folder shares:

- Certlog: located in the Winnt\System32 folder.
  - Domain Administrators - Full Control for this folder, subfolders, and files.
  - Enterprise Administrators - Full Control for this folder, subfolders, and files.
  - System - Full Control for this folder, subfolders, and files.

- CertSrv: located in the Winnt\System32 folder.
  - Authenticated Users - Read and Execute for this folder, subfolders, and files.
  - Server Operators - Modify for this folder, subfolders, and files.
  - Domain Administrators - Full Control for this folder, subfolders, and files.
  - System - Full Control for this folder, subfolders, and files.
  - Creator/Owner - Full Control for this folder, subfolders, and files.
  - Allow inheritable permissions on all child objects and enable propagation of inheritable permissions.

- Shared Folder (CertConfig share) - name and location specified by the administrator.
  - Domain Administrators - Full Control, Change, and Read for share permissions.
  - Everyone - Read for share permissions.
  - Domain Administrators - Full Control for this folder, subfolders, and files.
  - System - Full Control for this folder, subfolders, and files.
  - Enterprise Administrators- Full Control for this folder, subfolders, and files.
  - Everyone - Read for this folder, subfolders, and files.

Set permissions for Active Directory objects according to the following rules. You can set permissions using the **Security** tab in Adsiedit.msc or with the Active Directory Sites and Services snap-in under the Services container. To view the Services container, click **Show Services Node** on the **View** menu within the Microsoft Management Console (MMC).

- Certificate Templates Container - Located in the DC=Domain, CN=Configuration, CN=Services, CN=Public Key Services.
  - Authenticated Users - Special Permission (List Contents, Read All Properties, Read Permissions) for this object only.
  - Enterprise Administrators - Special Permission (List Contents, Read All Properties, Write All Properties, Read Permissions, Modify Permissions, Modify Owner, All Validated Writes, All Extended Rights, Create

All Child Objects, Create (for all objects)) for this object only.

- System- Full Control for This object only.
- Enterprise Administrators - Full Control for This object and all child objects.
- Domain Administrators - Special Permission (List Contents, Read All Properties, Read Permissions, Write All Properties, Delete, Read Permissions, Modify Permissions, Modify Owner, All Validated Writes, All Extended Rights, Create All Child Objects, Create (for all objects)) for This object and all child objects.
- Allow inheritable permission from the parent to propagate to this object.

- Certificate Templates in the Certificate Templates Folder
  - Authenticated Users - Special Permission (List Contents, Read All Properties, Read Permissions).
  - Domain Administrators - Full Control.
  - Domain Users - Special Permission (Enroll).
  - Depending on the certificate template to which the administrator wants the user to have access, the user must have Read permission to the template. The user must have Enroll permission on the template to make a request for the template.

- Certification Authority - Located in DC=Domain, CN=Configuration, CN=Services, CN=Public Key Services.
  - Authenticated Users - Special Permission (List Contents, Read All Properties, Read Permissions) for this object only.
  - Enterprise Administrators - Special Permission (List Contents, Read All Properties, Write All Properties, Read Permissions, Modify Permissions, Modify Owner, All Validated Writes, All Extended Rights, Create All Child Objects, Create (for all objects)) for this object only.
  - System - Full Control for this object only.
  - Enterprise Administrators - Full Control for this object and all child objects.
  - Domain Administrators - Special Permission (List Contents, Read All Properties, Read Permissions, Write All Properties, Delete, Read Permissions, Modify Permissions, Modify Owner, All Validated Writes, All Extended Rights, Create All Child Objects, Create (for all objects)) for this object and all child objects.
  - Allow inheritable permission from the parent to propagate to this object.

- Objects in Certification Authority Container
  - Enterprise Administrators - Full Control.
  - Domain Administrators - Full Control.
  - Cert Publishers - Full Control.
  - Administrators - Full Control.
  - Everyone - Special Permission (List Contents, Read All Properties, Read Permissions).

- Enrollment Services - Located in DC=Domain, CN=Configuration, CN=Services, CN=Public Key Services.
  - Authenticated Users - Special Permission (List Contents, Read All Properties, Read Permissions) for this object only.
  - Enterprise Administrators - Special Permission (List Contents, Read All Properties, Write All Properties, Read Permissions, Modify Permissions, Modify Owner, All Validated Writes, All Extended Rights, Create All Child Objects, Create (for all objects)) for this object only.
  - System - Full Control for this object only.
  - Enterprise Administrators - Full Control for this object and all child objects.
  - Domain Administrators - Special Permission (List Contents, Read All Properties, Read Permissions, Write All Properties, Delete, Read Permissions, Modify Permissions, Modify Owner, All Validated Writes, All Extended Rights, Create All Child Objects, Create (for all objects)) for this object and all child objects.
  - Allow inheritable permission from the parent to propagate to this object.

- Objects in Enrollment Services Container

- Authenticated Users - Special Permission (List Contents, Read All Properties, Write All Properties, Read Permissions) for this object and all child objects.
- Domain Administrators - Full Control.
- Enterprise Administrators - Full Control.
- Administrators - Full Control.

Keywords: kbenv kbinfo KB239706
Technology: kbwin2000AdvServ kbwin2000AdvServSearch kbwin2000DataServ kbwin2000DataServSearch kbwin2000Search kbwin2000Serv kbwin2000ServSearch kbWinAdvServSearch kbWinDataServSearch

---