

Dsrevoke

Dsrevoke is a new command-line tool that can be used on domain controllers that are running Windows Server 2003 or Windows 2000 Server to report the existence of all permissions for a specific user or group on a set of OUs in a domain and optionally remove from the DACLs of a set of OUs all permissions specified for a particular user or group. Dsrevoke complements the functionality provided by Delegation of Control Wizard, which is used to delegate administrative authority, by providing the ability to revoke delegated administrative authority.

Dsrevoke usage:

```
Usage: dsrevoke /report|remove [/domain:<domainname>] [/username:<username>]
        [/password:<password>|*] [/root:<domain/OU>] <securityprincipal>
```

/report: Only reports the ACEs that have been set for the given principal on all domain and OU objects under root

/remove: Reports and then removes (after confirmation) the aces for the given principal

/domain: Dns OR Netbios name of domain
(must be specified when <securityprincipal> is in domain other than default or if alternate credentials are provided)

/username: Username if alternate credentials must be specified

/password: * will prompt for password

/root: Root OU to start search for ACEs. If not specified will default to the specified domain's default naming context (The root domain or OU must be specified using x500 format; if the dn must include spaces enclose the option in quotes, e.g. "/root:...")

<securityprincipal>: Domain\User or Domain\Group for the security principal being looked up

Best-Practices on using Dsrevoke when delegating administration in Active Directory

To maximize the benefits offered by Dsrevoke, follow these guidelines as much as possible when delegating administrative authority:

- Use roles to delegate administrative authority. When delegating roles, be sure to use a unique and specific security group to represent every unique and specific role instance.

- o Use inheritance to grant permissions to the security group representing a role instance, and grant permissions on OUs.

Delegating administrative authority by using roles involves the following tasks:

1. Create a specific and unique security group to represent the role.
2. Identify the highest level OU that represents the root of the smallest subtree that contains the subset of all objects the delegated user needs to access and modify in order to perform the delegated tasks.
3. Run the Delegation of Control Wizard on that OU and delegate the required administrative tasks to the unique and specific security group representing the unique and specific role.

If you follow these delegation guidelines, you can use Dsrevoke to easily and reliably undelegate authority. Simply run Dsrevoke in the domain, providing as input the name of the specific security group used to represent the delegated role, and use the **/report** switch to verify the existence of all explicit permissions for that security group that have been set on all OU objects in the domain . Once you have reviewed the reported permissions, you can use the **/remove** switch to revoke all permissions granted to that security group, thereby revoking the delegated authority.



Note

Dsrevoke removes only permissions; if a role has user rights applied, you must manually remove them by modifying the appropriate Group Policy. Also, because Dsrevoke works only on domain objects and OUs, you must manually remove ACEs if you set them on a container object or if you explicitly set permissions on an object within a container or OU. For this reason, it is recommended that you always apply permissions to OUs rather than to specific objects within OUs, and that you apply permissions to child OUs by using inheritance. Finally, because Dsrevoke works only on domain objects and OUs, you cannot use it to remove permissions from the Configuration and Schema directory partitions. Consequently, you typically cannot use Dsrevoke to revoke delegation of service management tasks.