



The Gold Finger, powered by Microsoft-endorsed, patent-pending access assessment technology, is the world's only solution that can instantly and accurately assess and reveal exactly **Who can do What** in Active Directory, **Where and How** so.

Its patent-pending access assessment capabilities can accurately determine resultant-access provisioned in Active Directory.

An Active Directory resultant-access assessment involves determining the effective access actually provisioned for security principals in an organization's Active Directory deployment. The accurate determination of resultant-access in Active Directory is a very difficult, time-consuming and error-prone process because it involves the precise and methodical assessment of numerous security components and the inclusion of numerous security factors such as those listed below.

Here are **some** factors that influence an accurate resultant access assessment in Active Directory –

- **Detailed Security Permission Analysis** – This involves a comprehensive assessment of security permissions and includes factors such as applicability, effectiveness, precedence order inclusions, overlap conflict resolution etc.
- **Security Group Membership Expansions** – Permissions are often specified for security groups, many of which may be nested i.e. have other groups as members, which in turn might themselves have other groups as members. All such groups need to be transitively expanded while avoiding circular loops, resolving membership conflicts etc.
- **Dynamic Well-Known SID Expansions** – Permissions can also be specified for well-known SIDs such as Domain Users, Authenticated Users, Everyone etc. Should a single such pertinent permission be encountered, there is a need to accurately and dynamically evaluate and include the cumulative membership of all such well-known SIDs.
- **Special Object Specific Constraints** – This involves the inclusion of all relevant object specific constraints such as *Disallow Delete* flags, multiple deletion avenues, special encoded rules, all pertinent Schema constraints etc.
- **Large Number of Objects** – There typically exist a large number of objects in an Active Directory, and in order to determine a security principal's resultant access, one needs to assess resultant access on all objects of interest.

The only way to accurately assess resultant access in Active Directory is to take all factors involved in a real Active Directory authorization check into account in a manner identical to how they are taken into account during a real access check.

Only Gold Finger's unique Microsoft-endorsed patent-pending access assessment capabilities automate the simulation of real Active Directory access checks to assess and report resultant access in Active Directory with 100% accuracy.