



The **Top-100 Reports** that Gold Finger can generate, on-demand, in real-time, at the touch of a button –

I. **Domain User Account Management Reports** (27 reports)

1. All domain user accounts, and who can change the security permissions protecting them
2. All administrative domain user accounts, and who can reset their passwords
3. All active domain user accounts, and who can disable them
4. All stale domain user accounts, and who can reset their passwords to login as them
5. All unused domain user accounts, and who can reset their passwords to login as them
6. All enabled domain user accounts, and who can disable them
7. All disabled domain user accounts, and who can enable them
8. All locked domain user accounts, and who can unlock them
9. All recently created domain user accounts, and who can delete them
10. All recently deleted domain user accounts, and who can create domain user accounts, and where*
11. All recently changed domain user accounts
12. All password-protected domain user accounts, and who can reset their passwords
13. All smart-card protected domain user accounts, and who can disable the requirement of smart cards on them
14. All domain-user accounts that do not require passwords to logon
15. All domain user accounts whose passwords never expire, and who can change this setting
16. All domain user accounts whose password must be changed at next logon, and who can change this setting
17. All domain-user accounts that do not have an expiration date, and who can set an expiration date on them
18. All domain-user accounts that are about to expire, and who can prevent them from expiring
19. All domain user accounts that are sensitive and cannot be delegated, and who can change their sensitivity
20. All domain user accounts that are not sensitive and can be delegated, and who can change their sensitivity
21. All domain user accounts that can logon to any workstation, and who can change this setting
22. All domain user accounts that can logon to specific workstations, and who can change the list of workstations
23. All domain user accounts that can logon anytime, and who can restrict logon to specific times only
24. All domain user accounts for which specific logon hours have been specified, and who can change the hours

25. All domain user accounts for which a logon-script is specified, and who can specify a logon-script
26. All domain user accounts for which a logon-script is not specified, and who can specify their logon-script
27. All domain user accounts that do not have a description specified, and who can specify their description

II. Domain Computer Account Management Reports (17 reports)

1. All domain computer accounts, and who can change the security permissions protecting them
2. All active domain computer accounts, and who can disable them
3. All stale domain computer accounts, and who can reset them
4. All unused domain computer accounts
5. All enabled domain computer accounts, and who can disable them
6. All disabled domain computer accounts, and who can enable them
7. All recently created domain computer accounts, and who can delete them
8. All recently deleted domain computer accounts, and who can create domain computer accounts, and where*
9. All recently changed domain computer accounts
10. All domain computer accounts that are trusted for delegation
11. All domain computer accounts that are trusted for unconstrained delegation
12. All domain computer accounts for which a manager is not designated, and who can designate their manager
13. All domain computer accounts for which a location is not specified, and who can specify their location
14. All domain computer accounts for which a description is not specified, and who can specify their description
15. Who can change the expiration date of a computer account, and of which accounts*
16. Who can change the DNS name of a computer account, and of which accounts*
17. Who can change the Service Principal Names (SPNs) of a computer account, and of which accounts*

III. Domain Security Group Management Reports (14 reports)

1. All domain security groups, and who can change the security permissions protecting them
2. All domain security groups of a specific scope, and who can change their scope
3. All administrative domain security groups, and who can change their memberships
4. All empty domain security groups, and who can change their memberships
5. All nested domain security groups, and who can un-nest them
6. All domain security groups with large memberships, and who can change their memberships
7. All domain security groups for which a manager is not designated, and who can designate their manager
8. All domain security groups for which a description is not specified, and who can specify their description

9. All recently created domain security groups, and who can delete them
10. All recently deleted domain security groups, and who can create domain security groups, and where*
11. All recently changed domain security groups
12. All direct and nested members of a security group, and who can change their memberships
13. Who can add/remove oneself to/from the membership of a security group, and to/from which groups*
14. Who can change a security group into a distribution group, and which groups*

IV. Organizational Unit Management Reports (11 reports)

1. All organizational units, and who can change the security permissions protecting them
2. All empty organizational units, and who can create accounts, groups, containers and OUs within them
3. All recently created organizational units, and who can delete them
4. All recently deleted organizational units, and who can create organizational units, and where*
5. All recently changed organizational units
6. All organizational units to which group policies are explicitly linked, and who can unlink linked policies
7. All organizational units to which group policies are not explicitly linked, and who can link policies to them
8. All organizational units for which a manager is not designated, and who can designate their manager
9. All organizational units for which a description is not specified, and who can specify their description
10. Who can generate resultant set of policy (logging-mode) for users/computers in an organizational unit
11. Who can generate resultant set of policy (planning-mode) for users/computers in an organizational unit

V. Container Management Reports (6 reports)

1. All containers, and who can change the security permissions protecting them
2. All empty containers, and who can create accounts, groups and containers within them
3. All recently created containers, and who can delete them
4. All recently deleted containers, and who can create containers, and where*
5. All recently changed containers
6. All containers for which a description is not specified, and who can specify their description

VI. Group Policy Management Reports (4 reports)

1. All group policy containers, and who can change the security permissions protecting them
2. All recently created group policy containers, and who can delete them
3. All recently deleted group policy containers, and who can create valid group policy containers

4. All recently changed group policy containers

VII. Service Connection Point Management Reports (7 reports)

1. All service connection points, and who can change the security permissions protecting them
2. All recently created service connection points, and who can delete them
3. All recently deleted service connection points, and who can create service connection points, and where*
4. All recently changed service connection points
5. All service connection points for which keywords are specified, and who can change their keywords
6. All service connection points for which DNS service names are specified, and who can change these names
7. All service connection points for which service bindings are specified, and who can change these bindings

VIII. Active Directory Permissions Analysis Reports (9 reports)

1. All objects on which a security principal has any permissions
2. All objects on which a security principal has explicit / inherited permissions
3. All objects on which a security principal has allow / deny permissions
4. All objects on which a security principal has read/modify permissions / modify owner permissions
5. All objects on which a security principal has read-property permissions
6. All objects on which a security principal has write-property permissions
7. All objects on which a security principal has create-child / delete / delete-child / delete tree permissions
8. All objects on which a security principal has extended right permissions
9. All objects on which a security principal has validated write permissions

IX. Domain Security Policy Management Reports (5 reports)

1. Who can change the maximum password age for domain user accounts
2. Who can change the minimum password age for domain user accounts
3. Who can change the lockout duration for domain user accounts
4. Who can change the lockout threshold for domain user accounts
5. Who can change the lockout observation window for domain user accounts

Trustworthy Insight

Gold Finger is developed by Paramount Defenses Inc, a valued Microsoft directory services partner. Architected by former Microsoft Program Manager for Active Directory Security, it is trusted worldwide and endorsed by Microsoft Corporation.

Report Categories

Gold Finger offers **100+** resultant-access and security reports that cover the following IT management categories –

1. Domain User and Computer Account Management
2. Domain Security Group and Policy Management
3. Organizational Unit and Container Management
4. SCP, Group Policy and Printer Management
5. Contact Management
6. Active Directory Security Permissions Management

Capabilities

Gold Finger offers the following **6** Active Directory security assessment capabilities –

1. Security-Audit Reports
2. Membership Reports
3. ACL Viewer & Exporter
4. Permission Analyzer
5. Effective Permissions
6. Effective Delegated Access

For a complete list of reports, features and editions and to download a free trial, please visit www.paramountdefenses.com.