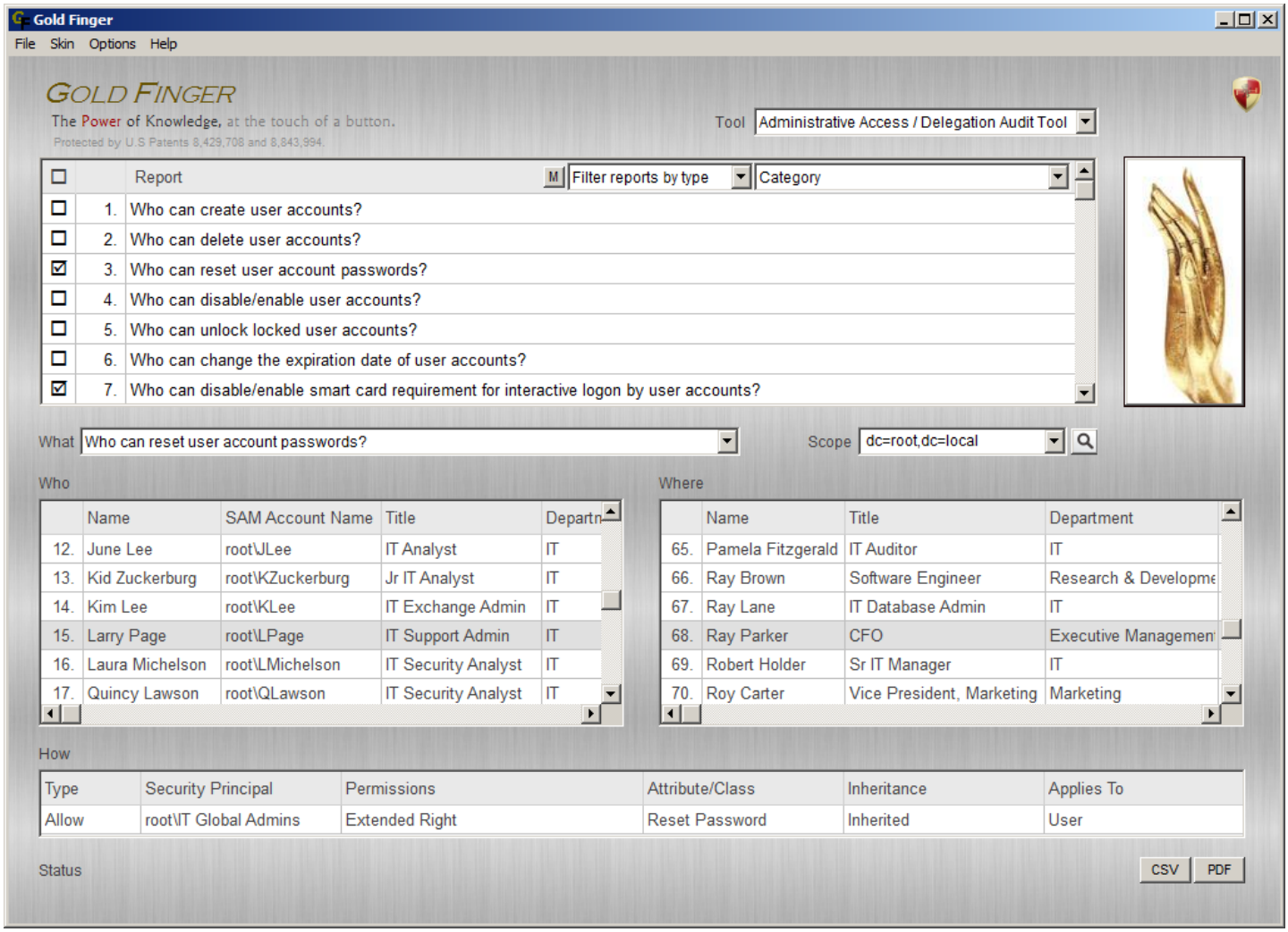
GOLD FINGER

Active Directory Administrative (Privileged) Access and Delegation Audit Tool



"We are very pleased to see Paramount Defenses, a valued Microsoft partner, offer an innovative security solution (in Gold Finger) that helps enhance security and compliance in Active Directory environments."

- Charles Coates, Senior Product Manager, Identity and Security Business Group, Microsoft

Capability Overview

Organizations have a paramount need to be able to perform effective privileged access audits in their IT environments to know exactly who has what effective administrative/privileged access, unrestricted as well as delegated, at all times.

The Gold Finger Active Directory Administrative (Privileged) Access and Delegation Audit Tool was designed to empower organizations to be able to efficiently, cost-effectively and trustworthily fulfill this paramount cyber security need.

The Active Directory Administrative (Privileged) Access and Delegation Audit Tool fully automates the accurate audit of effective administrative (privileged) access across an entire Active Directory domain. It is unique in its ability to do so. The tool also lets IT administrators, auditors, analysts and managers export data for analysis as well as generate reports that can be furnished as evidence to demonstrate regulatory compliance, delivering in minutes, what could take years.

Effective Privileged Access Audit Reports

Gold Finger offers the following 105 effective privileged (administrative) access and delegation audit reports –

Domain User Account Management Reports –

1. List of all individuals who can create user accounts
2. List of all individuals who can delete user accounts
3. List of all individuals who can reset user account passwords
4. List of all individuals who can disable/enable user accounts
5. List of all individuals who can unlock locked user accounts
6. List of all individuals who can change the expiration date of user accounts
7. List of all individuals who can disable/enable smart card requirement for interactive logon by user accounts
8. List of all individuals who can force users to change their user account passwords at next logon
9. List of all individuals who can prevent users from changing their user account passwords
10. List of all individuals who can change the logon name of user accounts
11. List of all individuals who can change the Pre-Windows 2000 logon name of user accounts
12. List of all individuals who can change the logon hours of user accounts
13. List of all individuals who can change the logon workstations of user accounts

14. List of all individuals who can change the profile path for user accounts
15. List of all individuals who can change the logon script for user accounts
16. List of all individuals who can change alternate security identities associated with user accounts
17. List of all individuals who can change whether or not user accounts are sensitive and cannot be delegated
18. List of all individuals who can change whether or not DES encryption types should be used for user accounts
19. List of all individuals who can change whether or not Kerberos pre-authentication is required for user accounts
20. List of all individuals who can change the first name of user accounts
21. List of all individuals who can change the last name of user accounts
22. List of all individuals who can change the display name of user accounts
23. List of all individuals who can change the description of user accounts
24. List of all individuals who can change the office location of user accounts
25. List of all individuals who can change the organizational title of user accounts
26. List of all individuals who can change the organizational department of user accounts
27. List of all individuals who can change the organizational manager for user accounts
28. List of all individuals who can change the picture associated with user accounts
29. List of all individuals who can change the security permissions protecting user accounts

Domain Computer Account Management Reports –

30. List of all individuals who can create computer accounts
31. List of all individuals who can delete computer accounts
32. List of all individuals who can reset computer accounts
33. List of all individuals who can disable/enable computer accounts
34. List of all individuals who can change the expiration date of computer accounts
35. List of all individuals who can change the computer name (Pre-Windows 2000) of computer accounts
36. List of all individuals who can change the DNS name of computer accounts
37. List of all individuals who can change the machine role of computer accounts
38. List of all individuals who can change the description of computer accounts
39. List of all individuals who can change the location of computer accounts

40. List of all individuals who can change the Service Principal Names (SPNs) of computer accounts
41. List of all individuals who can change alternate security identities associated with computer accounts
42. List of all individuals who can change the designated manager of computer accounts
43. List of all individuals who can change the picture associated with computer accounts
44. List of all individuals who can change the security permissions protecting computer accounts

Domain Security Group Management Reports –

45. List of all individuals who can create security groups
46. List of all individuals who can delete security groups
47. List of all individuals who can change security group memberships
48. List of all individuals who can add/remove oneself to/from the membership of security groups
49. List of all individuals who can change security group scopes
50. List of all individuals who can change security group types
51. List of all individuals who can change the group name (Pre-Windows 2000) of security groups
52. List of all individuals who can change the description of security groups
53. List of all individuals who can change the email-address of security groups
54. List of all individuals who can change notes annotated for security groups
55. List of all individuals who can change the designated manager of security groups
56. List of all individuals who can change the security permissions protecting security groups

Domain Security Policy Management Reports –

57. List of all individuals who can change the maximum password age for domain user accounts
58. List of all individuals who can change the minimum password age for domain user accounts
59. List of all individuals who can change the lockout duration for domain user accounts
60. List of all individuals who can change the lockout threshold for domain user accounts
61. List of all individuals who can change the lockout observation window for domain user accounts

Domain Organizational Unit Management Reports –

62. List of all individuals who can create organizational units
63. List of all individuals who can delete organizational units
64. List of all individuals who can disable group policies linked to organizational units
65. List of all individuals who can change the list of group policies linked to organizational units
66. List of all individuals who can change the precedence of group policies linked to organizational units
67. List of all individuals who can generate resultant set of policy (logging-mode) for users/computers in an OU
68. List of all individuals who can generate resultant set of policy (planning-mode) for users/computers in an OU
69. List of all individuals who can change the description of organizational units
70. List of all individuals who can change the street address of organizational units
71. List of all individuals who can change the city of organizational units
72. List of all individuals who can change the state/province of organizational units
73. List of all individuals who can change the zip/postal-code of organizational units
74. List of all individuals who can change the country of organizational units
75. List of all individuals who can change the designated manager of organizational units
76. List of all individuals who can change the security permissions protecting organizational units

Domain Container Management Reports –

77. List of all individuals who can create containers
78. List of all individuals who can delete containers
79. List of all individuals who can change the description of containers
80. List of all individuals who can change the security permissions protecting containers

Service Connection Point Management Reports –

81. List of all individuals who can create service connection points
82. List of all individuals who can delete service connection points
83. List of all individuals who can change the keywords of service connection points
84. List of all individuals who can change the description of service connection points
85. List of all individuals who can change the binding information of service connection points

86. List of all individuals who can change the service DNS name of service connection points
87. List of all individuals who can change the service DNS name type of service connection points
88. List of all individuals who can change the vendor of service connection points
89. List of all individuals who can change the version number of service connection points
90. List of all individuals who can change the hi version number of service connection points
91. List of all individuals who can change the low version number of service connection points
92. List of all individuals who can change the class-name of service connection points
93. List of all individuals who can change the security permissions protecting service connection points

Group Policy Management Reports –

94. List of all individuals who can create group policy containers
95. List of all individuals who can delete group policy containers
96. List of all individuals who can change the security permissions protecting group policy containers

Contact Management Reports –

97. List of all individuals who can create contacts
98. List of all individuals who can delete contacts
99. List of all individuals who can change the security permissions protecting contacts

Print Queue Management Reports –

100. List of all individuals who can create (publish) printers
101. List of all individuals who can delete published printers
102. List of all individuals who can change the description of published printers
103. List of all individuals who can change the share name of published printers
104. List of all individuals who can change the designated manager of published printers
105. List of all individuals who can change the security permissions protecting published printers

Trustworthy Insight

When it comes to your security, accurate, trustworthy insight is paramount, because a single inaccuracy can mean the difference between security and compromise. At Paramount Defenses, we set the industry bar for trustworthiness.

Gold Finger is architected by none other than former Microsoft Program Manager for Active Directory Security so you have the assurance that it embodies authoritative expertise that you can rely on to deliver accurate, trustworthy insight. It is also 100% built in the United States, developed and tested over almost a decade, by highly proficient, experienced and trustworthy developers, 100% of whom are U.S. citizens, so you know you're running the world's most secure code. Finally, it is specially engineered to ensure that its use does not require any elevated/privileged/administrative access.

Perhaps that's why today the world's most important organizations in six continents worldwide use Gold Finger.

Licensing and Pricing

Gold Finger also offers the industry's most flexible licensing model. The Active Directory Administrative (Privileged) Access and Delegation Audit Tool can be licensed individually or in combination with other tools in the Gold Finger suite on a long-term (single/multi-year) basis. Long-term licenses are intended for and ideal for organizational use. Pricing is available upon request.

For details, visit - http://www.paramountdefenses.com/active-directory-administrative-access-and-delegation-audit-tool