|  |  |  |
| --- | --- | --- |
| **Subject**: | **Subject**: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 | **4611, 4624, 4625, 4634,4647, 4656, 4672, 4673, 4674, 4688, 4689, 4696, 4715, 4717, 4718, 4719, ,4720, 4722, 4723, 4724, 4725, 4726, 4738, 4739, 4740, 4741, 4742, 4743, 4767, 4912** |
|  | **Subject:** Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon GUID: %5 | **4648** |
|  | **Subject:** Account Name: %1 Account Domain: %2 Logon ID: %3 | **4778, 4779,** |
| **Logon Process Name:** | Logon Process Name: %5 | **4611** |
| **Session:** | **Session:** Session Name: %4 | **4778, 4779** |
| **Additional Information:** | **Additional Information:** Client Name: %5 Client Address: %6 | **4778,4779** |
|  | **Additional Information:**  Weight: %14  Conditions: %15  Filter Action: %16 | **5447** |
|  | **Additional Information:** Privileges %8 | **4723, 4726,4743,** |
|  | **Additional Information:** Caller Computer Name: %2 | **4740** |
|  | **Additional Information:** Ticket Options: %6 Result Code: %7 Ticket Encryption Type: %8 Pre-Authentication Type: %9 | **4768** |
|  | **Additional Information:** Ticket Options: %5 Ticket Encryption Type: %6 Failure Code: %9 Transited Services: %11 | **4769** |
|  | **Additional Information:** Ticket Options: %5 Ticket Encryption Type: %6 | **4770** |
|  | **Additional Information:** Ticket Options: %4 Failure Code: %5 Pre-Authentication Type: %6 | **4771** |
|  | **Additional Information:** Ticket Options: %4 Failure Code: %5 | **4772, 4773** |
| **Notification Package Name:** | Notification Package Name: %1 | **4614** |
| **Task Information:** | **Task Information:**  Task Name: %5  Task New Content: %6 | **4702** |
| **Process Information:** | **Process Information:**  Process ID: %9  Name: %10 | **4624, 4648** |
|  | **Process Information:** Process ID: %14 Process Name: %15 | **4656, 4658, 4674, 4696** |
|  | **Process Information:** Caller Process ID: %18 Caller Process Name: %19 | **4625** |
|  | **Process Information:** New Process ID: %5 New Process Name: %6 Token Elevation Type: %7 Creator Process ID: %8 | 4668, 4688 |
|  | **Process Information:** Process ID: %6 Process Name: %7 Exit Status: %5 | **4**689 |
|  | **Process Information:**  New Process ID: %5  New Process Name: %6!S!  Token Elevation Type: %7  Mandatory Label: %15  Creator Process ID: %8  Creator Process Name: %14!S!  Process Command Line: %9!S! | **4688** |
| **Previous Time:** | **Previous Time: %6 %5** | **4616** |
| **New Time:** | **New Time: %8 %7** | **4616** |
| **Logon Type:** | **Logon Type: %9** | **4624, 4625, 4634,** |
| **New Logon:** | **New Logon:**  Security ID: %5  Account Name: %6  Account Domain: %7  Logon ID: %8  Logon GUID: %13 | **4624,** |
| **Service**: | **Service**:  Server: %5  Service Name: %6 | **4673** |
| **Network Information:** | **Network Information:**  Workstation Name: %12  Source Network Address: %19  Source Port: %20 | **4624, 4625** |
|  | **Network Information:**  Object Type: %5  Source Address: %6  Source Port: %7 | **5145** |
|  | **Network Information:**  Network Address: %13  Port: %14 | **4648** |
|  | **Network Information:** Client Address: %10 Client Port: %11 | **4768, 4769, 4770, 4771, 4772, 4773** |
| **Detailed Authentication Information:** | **Detailed Authentication Information:**  Logon Process: %10  Authentication Package: %11  Transited Services: %14  Package Name (NTLM only): %15  Key Length: %16 | **4624** |
| **Object:** | **Object:**  Object Server: %5  Object Type: %6  Object Name: %7  Handle ID: %8 Resource Attributes: %17 | **4656** |
|  | **Object:** Object Server: %5 Object Type: %6 Object Name: %7 Handle ID: %8 | **4**656 |
|  | **Object:** Object Server: %5 Handle ID: %6 | **4**658 |
|  | **Object:** Object Server: %5 Object Type: %6 Object Name: %7 Object Handle: %8 | **4**674 |
| **Permissions Change:** | **Permissions Change:**  Original Security Descriptor: %9  New Security Descriptor: %10 | **4670** |
| **Privileges**: | **Privileges**: %5 | **4672** |
| **Event Source:** | **Event Source:**  Source Name: %5  Event Source ID: %6 |  |
| **Rule Information:** | **Rule Information:**  ID: %1  Name: %2 | **4957** |
| **Error Information:** | **Error Information:**  Reason: %3 resolved to an empty set. | **4957** |
| **Transaction Information:** | **Transaction Information:**  RM Transaction ID: %5  New State: %6  Resource Manager: %7 | **4985** |
| **Share Information:** | **Share Information:**  Share Name: %8  Share Path: %9  Relative Target Name: %10 | **5145** |
| **Access Request Information:** | **Access Request Information:** Transaction ID: %9 Accesses: %10 Access Mask: %11 Privileges Used for Access Check: %12 Restricted SID Count: %13 | **4**656 |
|  | **Access Request Information:**  Access Mask: %11  Accesses: %12  Access Check Results: %13 | **5145** |
| **Provider Information:** | **Provider Information:**  ID: %4  Name: %5 | **5440, 5441, 5446, 5447, 5449, 5450** |
|  | **Provider Information:**  ID: %5  Name: %6  Type: %7 | **5448** |
| **Change Information:** | **Change Information:**  Change Type: %6 | **5446, 5447, 5448, 5449, 5450,** |
| **Change Type:** | Change Type: %1 modified | **4739** |
| **Filter Information:** | **Filter Information:**  ID: %7  Name: %8  Type: %9  Run-Time ID: %10 |  |
| **Layer Information:** | **Layer Information:**  ID: %11  Name: %12  Run-Time ID: %13 | **5446, 5447,** |
| **Callout Information:** | **Callout Information:**  ID: %17  Name: %18 |  |
| **Target Server:** | **Target Server:**  Target Server Name: %9  Additional Information: %10 | **4648** |
| **Share Name:** | **Share Name:** %7 | **5140,** |
| **Requested Operation:** | **Requested Operation:**  Desired Access: %9  Privileges: %10 | **4674** |
| **Target Account:** | **Target Account:**  Security ID: %3  Account Name: %1  Account Domain: %2 | **4722** |
| **Service Information:** | **Service Information:**  Service Name: %4  Service ID: %5 | **4768, 4769, 4770,** |
|  | **Service Information:** Service Name: %3 | **4771, 4772, 4773,** |
| **Account Whose Credentials Were Used:** | **Account Whose Credentials Were Used:**  Account Name: %6  Account Domain: %7  Logon GUID: %8 | **4648,** |
| **Target Server:** | **Target Server:**  Target Server Name: %9  Additional Information: %10 | **4648** |
| **Creator Subject:** | **Creator Subject:**  Security ID: %1  Account Name: %2  Account Domain: %3  Logon ID: %4 | **4668, 4688** |
| **Target Subject:** | **Target Subject:**  Security ID: %10  Account Name: %11  Account Domain: %12  Logon ID: %13 | **4668, 4688** |
| **Target Process:** | **Target Process:**  Target Process ID: %9  Target Process Name: %10 | **4696** |
| **New Token Information:** | **New Token Information:**  Security ID: %5  Account Name: %6  Account Domain: %7  Logon ID: %8 | **4696** |