
eSCOP IT SECURITY EVENTS

- 512 Server Startup
- 513 Server Shutdown
- 514 Authentication package was located by the Local Security Agent (LSA)
- 515 Trusted Logon Process was registered by the Local Security Agent
- 516 Audit Log was exhausted
- 517 Event Log was cleared
- 518 Notification package was loaded on the Security Accounts Manager
- 519 Process is using an invalid located procedure call (LPC) port to impersonate a client and reply or read from or write to a client address space
- 520 The system time was change
- 521 Security log auditing failed
- 522 Audit Collection failed
- 523 Audit Log Capacity
- 528 Logon was successful
- 529 Logon failure from unknown user name or bad password
- 530 Logon failed by user outside allocated time
- 531 Logon to disabled account failed
- 532 Logon to expired account failed
- 533 Logon by unauthorized computer user failed
- 534 Logon by non-allowed type failed
- 535 Logon due to expired password failed
- 536 Logon failed due to inactive logon service
- 537 Logon for other reasons failed
- 538 Logoff by user was completed
- 539 Logon during account lock-out failed
- 540 Logon to network was successful
- 541 Main Mode IKE Connection to peer was complete
- 542 Data channel was terminated
- 543 Main mode was terminated
- 544 Main mode failed due to peer invalid certificate or signature
- 545 Main mode failed due to Kerberos failure or invalid password
- 546 IKE security establishment failed due to invalid peer proposal
- 547 IKE handshake failed
- 548 Logon failure due to SID difference with trusted domain and account domain
- 549 Logon from untrusted forest namespace failed
- 550 Notification of possible denial of service attack was sent
- 551 User log off process was initiated
- 552 User logon with explicit credentials while logged on as different user
- 560 Access was granted to an already existing object
- 561 Handle allocated
- 562 Handle to an object was closed
- 563 Attempt to open an object with the intent to delete it was made
- 564 A protect object was deleted
- 565 Access was granted to an already existing object type
- 566 A generic object operation took place
- 567 Permission associated with a handled was used
- 568 Attempt to create a hard link to a file being audited was made
- 569 Resource Manager of Authorization Manager attempted to create a client context
- 570 The client attempted to access an object
- 571 The client context was deleted by the Authorization Manager

572 Administrator Manager initialized the application
573 Process generates nonsystem audit event with Authorization API
577 Privilege Service Called
578 Privileges were used on an already open handle to a protected object
592 New Process was created
593 Process Exit
594 Object handle was duplicated
595 Object was indirectly accessed
596 Data Protection Master Key was backed up
597 Data Protection Master Key was recovered from a recovery server
598 Audible Data was protected
599 Audible Data was unprotected
600 Primary Token was assigned to an object
601 User attempted to install a service
602 Schedule job was created
608 User right was assigned
609 User right was removed
610 Trust Relationship with another domain was created
611 Trust Relationship with another domain was removed
612 Audit policy was changed
613 IPsec Policy Agent was started
614 IPsec Policy Agent was disabled
615 IPsec Policy was changed
616 IPsec Policy agent encountered a potentially serious failure
617 Kerberos policy was changed
618 Encrypted Data Policy was changed
619 Quality of Service Policy Changed
620 Trust Relationship with another domain is changed
621 System access was granted
622 System access was removed
623 Auditing policy was set on a per-user basis
624 User Account was created
625 User Account type was changed
625 Per User Audit Policy was changed
626 User Account was enabled
627 User Account password was changed
628 User Account password was set
629 User Account was disabled
630 User Account was deleted
631 Global Group was created
631 Global Group was created
632 Global Group member was added
633 Global Group member was removed
634 Global Group was deleted
635 Local Group was created
636 Local Group member was added
637 Local Group member was deleted
638 Local group was deleted
639 Local group account was changed
640 General account database was changed
641 Global Group was changed
642 User Account was changed
643 Domain Policy was changed
644 User Account was locked
645 Computer Account was created
646 Computer Account was changed
647 Computer Account was deleted

648 Local Security Group with Security Disabled was Created
649 Local Security Group with Security Disabled was Changed
650 Local Security Group Member Added
651 Security Disabled Local Group Member Removed
652 Security disabled local group was deleted
653 Security-disabled Global Group was created
654 Security-disabled Global Group was changed
655 Member of a Security-disabled Global Group was added
656 Member of Global Security-disabled Group was removed
657 Security-disable Global Group was deleted
658 Universal Group was created
659 Universal Group was changed
660 Member of a Universal Group security-enabled was added
661 Member of Universal Group security-enabled was removed
662 Universal Group was delete
663 Universal Security-disabled group was created
664 Universal Security-disabled group was changed
665 Member of Universal Security-disabled group was added
666 Member of Universal Security-disabled group was removed
667 Member of Universal Security-disabled group was deleted
668 Group type was changed
669 Add SID History (Success)
670 Add SID History(Failure)
671 User Account Unlocked
672 Authentication Service (AS) ticket was issued and validate
673 Ticket Granting Service (TGS) ticket was issued
674 Security Principal was renewed as AS or TGS Ticket
675 Preauthorization failed
676 Authorization ticket failed
677 TGS ticket was not granted
678 An account was successfully mapped to a domain account
680 NTLM Successfully Authenticates User
681 NTLM failed when login attempt to a domain
682 User reconnected to a disconnected terminal server connection
683 User disconnected terminal services connection without logging off
684 Set the security redirector for administrative groups
685 Name of an account was changed
686 Password for the user accessed
697 Password Policy Checking API Called
768 Collision detected between a namespace element in one forest and namespace element in another forest
769 Trusted forest information was added
770 Trusted forest information was deleted
771 Trusted forest information was modified
772 Certificate Manager denied a pending certificate request
773 Certificate Services received a resubmitted certificate request
774 Certificate Services revoked a certificate
775 Certificate Services received a request to publish the certificated revocation list (CRL)
776 Certificate Services publish the CRL
777 A certificate request extension was made
778 One or more certificate request attributes changed
779 Certificate Services received a request to shutdown
780 Certificate Services backup started
781 Certificate Services backup completed
782 Certificate Services restore started
783 Certificate Services restore completed
784 Certificate Services started

785 Certificate Services stopped
786 The security permissions for Certificate Services changed
787 Certificate Services retrieved an archival file
788 Certificate Services imported a certificate into the database
789 The audit filter for Certificate Services changed
790 Certificate Services received a certificate request
791 Certificate Services approved a certificate request
792 Certificate Services denied a certificate request
793 Certificate Services set the status of a certificate request to pending
794 The certificate manager settings for Certificate Services change
795 A Configuration entry changed in Certificate Services
796 A property of Certification Services change
797 Certificate Services archived a log
798 Certificate Services imported and archived a key
799 Certification services published the certificate authority (CA) certificate to AD
800 One or more rows have been deleted from certificate database
801 Role separation enabled
805 Event log service read the security log configuration for a session