



Hewlett Packard
Enterprise

HPE ArcSight Connectors

SmartConnector for Microsoft Windows Event Log
– Unified

Windows 2008/2012 Security Event Mappings

June 30, 2015

HP ArcSight SmartConnector for Microsoft Windows Event Log – Unified Security Event Mappings

June 30, 2015

Copyright © 2008 – 2015 Hewlett Packard Enterprise Development LP

Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise Development LP shall not be liable for technical or editorial omissions contained herein. The information contained herein is subject to change without notice. The network information used in the examples in this document (including IP addresses and hostnames) is for illustration purposes only. Hewlett Packard Enterprise Development LP products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices. This document is confidential.

Restricted Rights Legend

Confidential computer software. Valid license from Hewlett Packard Enterprise Development LP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Follow this link to see a complete statement of Hewlett Packard Enterprise Development LP copyrights, trademarks and acknowledgements:

<https://www.protect724.hpe.com/docs/DOC-13026>.

Revision History

Date	Description
06/30/2015	Updated Destination User Name mappings for security events 4704 and 4705.
05/15/2014	GA support for Windows Server 2012 R2 events.
03/31/2014	Added beta support for Windows Server 2012 R2 events.
11/15/2013	Added Windows 2008 mapping for Device Custom IPv6 Address 2 for events 4624, 4768, 4769, 4770, and to Common Security Events.
08/15/2013	Separated Windows XP/2000/2003 event mappings into its own document. Added Windows 2012 support to this document.
11/15/2010	Added mappings for Security Event 5145.
05/26/2010	Added Device Custom String 4 mapping for Security Event 5136.
03/31/2010	Added mappings for Security Event 536.
02/11/2010	Added support for Microsoft Windows Server 2008/Vista security events.

Contents

About This Book.....	11
Windows 2008/2012 Common Security Mappings.....	12
Specific 2008/2012 Windows Security Event Mappings	14
521 Unable to log events to security log.....	14
525 The connection authorization policy could not be updated.....	14
1101 Audit events have been dropped by the transport.....	14
1102 The audit log was cleared.....	14
1104 The security log is now full.....	14
1105 Event log automatic backup.....	14
4610 An authentication package has been loaded by the Local Security Authority.....	14
4611 A trusted logon process has been registered with the Local Security Authority.....	15
4612 Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.....	15
4614 A notification package has been loaded by the Security Account Manager.....	15
4615 Invalid use of LPC port.....	15
4616 The system time was changed.....	15
4618 A monitored security event pattern has occurred.....	15
4621 Administrator recovered system from CrashOnAuditFail.....	15
4622 A security package has been loaded by the Local Security Authority.....	16
4624 An account was successfully logged on.....	16
4625 An account failed to log on.....	16
4626 User/Device claims information.....	17
4634 An account was logged off.....	17
4647 User initiated logoff.....	17
4648 A logon was attempted using explicit credentials.....	17
4649 A replay attack was detected.....	17
4650 An IPsec Main Mode security association was established. Extended Mode was not enabled.....	17
4651 An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.....	18
4652 An IPsec Main Mode negotiation failed.....	18
4653 An IPsec Main Mode negotiation failed.....	18
4654 An IPsec Quick Mode negotiation failed.....	19
4655 An IPsec Main Mode security association ended.....	19
4656 A handle to an object was requested.....	19
4657 A registry value was modified.....	19
4658 The handle to an object was closed.....	19
4659 A handle to an object was requested with intent to delete.....	20
4660 An object was deleted.....	20
4661 A handle to an object was requested.....	20
4662 An operation was performed on an object.....	20
4663 An attempt was made to access an object.....	20
4664 An attempt was made to create a hard link.....	20
4665 An attempt was made to create an application client context.....	20
4666 An application attempted an operation.....	21
4667 An application client context was deleted.....	21
4668 An application was initialized.....	21
4670 Permissions on an object were changed.....	21
4671 An application attempted to access a blocked ordinal through the TBS.....	21

4672	Special privileges assigned to new logon.....	21
4673	A privileged service was called.	21
4674	An operation was attempted on a privileged object.....	21
4675	SIDs were filtered.....	22
4688	A new process has been created.....	22
4689	A process has exited.....	22
4690	An attempt was made to duplicate a handle to an object.....	22
4691	Indirect access to an object was requested.....	22
4692	Backup of data protection master key was attempted.....	23
4693	Recovery of data protection master key was attempted.....	23
4694	Protection of auditable protected data was attempted.....	23
4695	Unprotection of auditable protected data was attempted.....	23
4696	A primary token was assigned to process.....	23
4697	A service was installed in the system.....	23
4698	A scheduled task was created.....	24
4699	A scheduled task was deleted.....	24
4700	A scheduled task was enabled.....	24
4701	A scheduled task was disabled.....	24
4702	A scheduled task was updated.....	24
4704	A user right was assigned.....	24
4705	A user right was removed.....	25
4706	A new trust was created to a domain.....	25
4707	A trust to a domain was removed.....	25
4709	IPsec Services was started.....	25
4713	Kerberos policy was changed.....	25
4714	Encrypted data recovery policy was changed.....	25
4715	The audit policy (SACL) on an object was changed.....	26
4716	Trusted domain information was modified.....	26
4717	System security access was granted to an account.....	26
4718	System security access was removed from an account.....	26
4719	System audit policy was changed.....	26
4720	A user account was created.....	27
4722	A user account was enabled.....	27
4723	An attempt was made to change an account's password.....	27
4724	An attempt was made to reset an account's password.....	27
4725	A user account was disabled.....	28
4726	A user account was deleted.....	28
4727	A security-enabled global group was created.....	28
4728	A member was added to a security-enabled global group.....	28
4729	A member was removed from a security-enabled global group.....	29
4730	A security-enabled global group was deleted.....	29
4731	A security-enabled local group was created.....	29
4732	A member was added to a security-enabled local group.....	29
4733	A member was removed from a security-enabled local group.....	30
4734	A security-enabled local group was deleted.....	30
4735	A security-enabled local group was changed.....	30
4737	A security-enabled global group was changed.....	30
4738	A user account was changed.....	31
4739	Domain Policy was changed.....	31
4740	A user account was locked out.....	31

4741	A computer account was created.	32
4742	A computer account was changed.	32
4743	A computer account was deleted.	32
4744	A security-disabled local group was created.	32
4745	A security-disabled local group was changed.	33
4746	A member was added to a security-disabled local group.	33
4747	A member was removed from a security-disabled local group.	33
4748	A security-disabled local group was deleted.	33
4749	A security-disabled global group was created.	34
4750	A security-disabled global group was changed.	34
4751	A member was added to a security-disabled global group.	34
4752	A member was removed from a security-disabled global group.	34
4753	A security-disabled global group was deleted.	35
4754	A security-enabled universal group was created.	35
4755	A security-enabled universal group was changed.	35
4756	A member was added to a security-enabled universal group.	35
4757	A member was removed from a security-enabled universal group.	36
4758	A security-enabled universal group was deleted.	36
4759	A security-disabled universal group was deleted.	36
4760	A security-disabled universal group was changed.	36
4761	A member was added to a security-disabled universal group.	37
4762	A member was removed from a security-disabled universal group.	37
4763	A security-disabled universal group was deleted.	37
4764	A group's type was changed.	38
4765	SID History was added to an account.	38
4766	An attempt to add SID History to an account failed.	38
4767	A user account was unlocked.	38
4768	A Kerberos authentication ticket (TGT) was requested.	39
4769	A Kerberos service ticket was requested.	39
4770	A Kerberos service ticket was renewed.	40
4771	Kerberos pre-authentication failed.	40
4772	A Kerberos Authentication ticket request failed.	40
4773	A Kerberos service ticket request failed.	40
4774	An account was mapped for logon.	41
4775	An account could not be mapped for logon.	41
4776	The domain controller attempted to validate the credentials for an account.	41
4777	The domain controller failed to validate the credentials for an account.	41
4778	A session was reconnected to a Window Station.	41
4779	A session was disconnected from a Window Station.	41
4780	The ACL was set on accounts that are members of administrators groups.	42
4781	The name of an account was changed.	42
4782	The password hash account was accessed.	42
4783	A basic application group was created.	42
4784	A basic application group was changed.	43
4785	A member was added to a basic application group.	43
4786	A member was removed from a basic application group.	43
4787	A non-member was added to a basic application group.	43
4788	A non-member was removed from a basic application group.	44
4789	A basic application group was deleted.	44
4789	A basic application group was deleted.	44

4790	An LDAP query group was created.	44
4791	A basic application group was changed.	45
4792	An LDAP security group was deleted.	45
4793	The Password Policy Checking API was called.	45
4794	An attempt was made to set the Directory Services Restore Mode administrator password.	45
4797	An attempt was made to query the existence of a blank password for an account.	45
4800	The workstation was locked.	46
4801	The workstation was unlocked.	46
4802	The screen saver was invoked.	46
4803	The screen saver was dismissed.	46
4816	RPC detected an integrity violation while decrypting an incoming message.	46
4817	Auditing settings on object were changed.	46
4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy.	46
4819	Central Access policies on the machine have been changed.	47
4820	A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions.	47
4821	A Kerberos ticket was denied because the user, device, or both does not meet the access control restrictions.	48
4822	NTLM authentication failed because the account was a member of the Protected User group.	48
4823	NTLM authentication failed because access control restrictions are required.	48
4824	Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group.	49
4864	A namespace collision was detected.	49
4865	A trusted forest information entry was added.	49
4866	A trusted forest information entry was removed.	49
4867	A trusted forest information entry was modified.	49
4868	The certificate manager denied a pending certificate request.	50
4869	Certificate Services received a resubmitted certificate request.	50
4870	Certificate Services revoked a certificate.	50
4871	Certificate Services received a request to publish the certificate revocation list (CRL).	50
4872	Certificate Services published the certificate revocation list (CRL).	50
4873	A certificate request extension changed.	50
4874	One or more certificate request attributes changed.	50
4875	Certificate Services received a request to shutdown.	50
4876	Certificate Services backup started.	50
4877	Certificate Services backup completed.	50
4880	Certificate Services started.	51
4881	Certificate Services stopped.	51
4882	The security permissions for Certificate Services changed.	51
4883	Certificate Services retrieved an archived key.	51
4884	Certificate Services imported a certificate into its database.	51
4885	The audit filter for Certificate Services changed.	51
4886	Certificate Services received a certificate request.	51
4887	Certificate Services approved a certificate request and issued a certificate.	51
4888	Certificate Services denied a certificate request.	51
4889	Certificate Services set the status of a certificate request to pending.	51
4890	The certificate manager settings for Certificate Services changed.	51
4891	A configuration entry changed in Certificate Services.	51
4892	A property of Certificate Services changed.	51
4893	Certificate Services archived a key.	52

4894	Certificate Services imported and archived a key.....	52
4895	Certificate Services published the CA certificate to Active Directory Domain Services.	52
4896	One or more rows have been deleted from the certificate database.	52
4897	Role separation enabled.	52
4898	Certificate Services loaded a template.	52
4899	A Certificate Services template was updated.	52
4900	Certificate Services template security was updated.	52
4902	The Per-user audit policy table was created.	52
4904	An attempt was made to register a security event source.	52
4905	A user right was removed.....	53
4906	The CrashOnAuditFail value has changed.....	53
4907	Auditing settings on object were changed.....	53
4908	Special Groups Logon table modified.....	53
4909	The local policy settings for the TBS were changed.....	53
4910	The group policy settings for the TBS were changed.....	53
4911	Resource attributes of the object were changed.	53
4912	Per User Audit Policy was changed.	54
4913	Central Access Policy on the object was changed.	54
4928	An Active Directory replica source naming context was established.....	54
4929	An Active Directory replica source naming context was removed.	54
4930	An Active Directory replica source naming context was modified.....	54
4931	An Active Directory replica destination naming context was modified.....	54
4932	Synchronization of a replica of an Active Directory naming context has begun.	54
4933	Synchronization of a replica of an Active Directory naming context has ended.	54
4934	Attributes of an Active Directory object were replicated.	54
4935	Replication failure begins.	54
4936	Replication failure ends.	54
4937	A lingering object was removed from a replica.....	55
4944	The following policy was active when the Windows Firewall started.	55
4945	A rule was listed when the Windows Firewall started.....	55
4946	A change has been made to Windows Firewall exception list. A rule was added.	55
4947	A change has been made to Windows Firewall exception list. A rule was modified.....	55
4948	A change has been made to Windows Firewall exception list. A rule was deleted.....	55
4950	A Windows Firewall setting has changed.....	55
4951	A rule has been ignored because its major version number was not recognized by Windows Firewall	55
4952	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall.....	55
4953	A rule has been ignored by Windows Firewall because it could not parse the rule.....	55
4956	Windows Firewall has changed the active profile.....	55
4957	Windows Firewall did not apply the following rule.	55
4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.....	56
4960	IPsec dropped an inbound packet that failed an integrity check.....	56
4961	IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.....	56
4962	IPsec dropped an inbound packet that failed a replay check. The inbound packet has too low a sequence number to ensure it was not a replay.	56
4963	IPsec dropped an inbound clear text packet that should have been secured.....	56
4964	Special groups have been assigned to a new logon.	56
4965	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI).....	56
4976	During Main Mode negotiation, IPsec received an invalid negotiation packet.....	56

4977	During Quick Mode negotiation, IPsec received an invalid negotiation packet.	56
4978	During Extended Mode negotiation, IPsec received an invalid negotiation packet.	57
4979	IPsec Main Mode and Extended Mode security associations were established.....	57
4980	IPsec Main Mode and Extended Mode security associations were established.....	57
4981	An IPsec Quick Mode security association was established.	57
4982	An IPsec Quick Mode security association was established.	57
4983	An IPsec Quick Mode security association was established.....	58
4984	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.	58
4985	The state of a transaction has changed.	58
5027	The Windows Firewall Service was unable to retrieve the security policy from the local storage.	58
5028	The Windows firewall Service was unable to parse the new security policy.	58
5029	The Windows Firewall Service failed to initialize the driver.	58
5030	The Windows Firewall Service failed to start.....	58
5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.	59
5032	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.	59
5035	The Windows Firewall Driver failed to start.	59
5037	The Windows Firewall Driver detected official runtime error. Terminating.	59
5038	Code integrity determined that the image hash of a file is not valid.	59
5039	A registry key was virtualized.	59
5040	A change has been made to IPsec settings. An Authentication Set was added.	59
5041	A change has been made to IPsec settings. An Authentication Set was modified.....	59
5042	A change has been made to IPsec settings. An Authentication Set was deleted.....	59
5043	A change has been made to IPsec settings. A Connection Security Rule was added.	59
5044	A change has been made to IPsec settings. A Connection Security Rule was modified.	59
5045	A change has been made to IPsec settings. A Connection Security Rule was deleted.	59
5046	A change has been made to IPsec settings. A Crypto Set was added.	60
5047	A change has been made to IPsec settings. A Crypto Set was modified.	60
5048	A change has been made to IPsec settings. A Crypto Set was deleted.....	60
5049	An IPsec Security Association was deleted.	60
5050	An attempt to programmatically disable the Windows Firewall using a call to INetFwProfile.	60
5051	A file was virtualized.	60
5056	A cryptographic self test was performed.	60
5057	A cryptographic primitive operation failed.	60
5058	Key file operation.	60
5059	Key migration operation.	61
5060	Verification operation failed.....	61
5061	Cryptographic operation.....	61
5062	A kernel-mode cryptographic self test was performed.	61
5063	A cryptographic provider operation was attempted.	61
5064	A cryptographic context operation was attempted.	61
5065	A cryptographic context modification was attempted.	61
5066	A cryptographic function operation was attempted.	61
5067	A cryptographic function modification was attempted.	61
5068	A cryptographic function provider operation was attempted.....	61
5069	A cryptographic function property operation was attempted.	61
5070	A cryptographic function property modification was attempted.	61
5071	Key access denied by Microsoft key distribution service.....	62
5122	A Configuration entry changed in the OCSF Responder Service.	62

5123	A configuration entry changed in the OCSP Responder Service.	62
5124	A security setting was updated on OCSP Responder Service.	62
5126	Signing Certificate was automatically updated by the OCSP Responder Service.	62
5127	The OCSP Revocation provider successfully updated the revocation information.	62
5136	A directory service object was modified.	62
5137	A directory service object was created.	62
5138	A directory service object was undeleted.	63
5139	A directory service object was moved.	63
5140	A network share object was accessed.	63
5141	A directory service object was deleted.	63
5142	A network share object was added.	64
5143	A network share object was modified.	64
5144	A network share object was deleted.	64
5145	A network share object was checked to see whether client can be granted desired access.	64
5146	The Windows Filtering Platform has blocked a packet.	65
5147	A more restrictive Windows Filtering Platform filter has blocked a packet.	65
5152	The Windows Filtering Platform blocked a packet.	65
5153	A more restrictive Windows Filtering Platform filter has blocked a packet.	65
5154	The Windows Filtering platform has permitted an application or service to listen on a port for incoming connections.	66
5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.	66
5156	The Windows Filtering Platform has allowed a connection.	66
5157	The Windows Filtering Platform has blocked a connection.	66
5158	The Windows Filtering Platform has permitted a bind to a local port.	66
5159	The Windows Filtering Platform has blocked a bind to a local port.	67
5168	Spn check for SMB/SMB2 fails.	67
5376	Credential Manager credentials were backed up.	67
5377	Credential Manager credentials were restored from a backup.	67
5378	The requested credentials delegation was disallowed by policy.	67
5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started.	68
5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started.	68
5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started.	68
5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.	68
5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.	68
5446	A Windows Filtering Platform callout has been changed.	68
5447	A Windows Filtering Platform filter has been changed.	68
5448	A Windows Filtering Platform provider has been changed.	68
5449	A Windows Filtering Platform provider context has been changed.	68
5450	A Windows Filtering Platform sub-layer has been changed.	68
5451	An IPsec Quick Mode security association was established.	69
5452	An IPsec Quick Mode security association ended.	69
5456	PAStore Engine applied Active Directory storage IPsec policy on the computer.	69
5457	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.	69
5458	PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.	69
5459	PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.	69
5460	PAStore Engine applied local registry storage IPsec policy on the computer.	69
5461	PAStore Engine failed to apply local registry storage IPsec policy on the computer.	70
5462	PAStore Engine failed to apply some rules of the active IPsec policy on the computer.	70

5471	PASStore Engine loaded local storage IPsec policy on the computer.....	70
5472	PASStore Engine failed to load local storage IPsec policy on the computer.	70
5473	PASStore Engine loaded directory storage IPsec policy on the computer.	70
5474	PASStore Engine failed to load directory storage IPsec policy on the computer.....	70
5477	PASStore Engine failed to add quick mode filter.	70
5483	IPsec Services failed to initialize RPC server. IPsec Services could not be started.....	70
5484	IPsec Services has experienced a critical failure and has been shut down.	70
5632	A request was made to authenticate to a wireless network.....	70
5633	A request was made to authenticate to a wired network.	71
5712	A Remote Procedure Call (RPC) was attempted.	71
5888	An object in the COM+ Catalog was attempted.	71
5889	An object was deleted from the COM+ Catalog.	71
5890	An object was added to the COM+ Catalog.	71
6144	Security policy In the group policy objects has been applied successfully.	71
6145	One or more errors occurred while processing security policy in the group policy objects.....	71
6272	Network Policy Server granted access to a user.....	72
6273	Network Policy Server denied access to a user.	72
6274	Network Policy Server discarded the request for a user.	72
6275	Network Policy Server discarded the accounting request for a user.	73
6276	Network Policy Server quarantined a user.	73
6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.	73
6278	Network Policy Server granted full access to a user because the host met the defined health policy.	73
6279	Network Policy Server locked the user account due to repeated failed authentication attempts.....	73
6280	Network Policy Server unlocked the user account.	74
6409	BranchCache: A service connection point object could not be parsed.....	74
6410	Code integrity determined that a file does not meet the security requirements to load into a process.....	74
8222	No fax devices were found.....	74
	Complete Windows 2012/Windows 8 Event Descriptions.....	75

About This Book

This guide provides the specific events generated by the various policies and their mappings to HP ArcSight fields.

The SmartConnector for Microsoft Windows Event Log – Unified can connect to local or remote machines, inside a single domain or from multiple domains, to retrieve events from all types of event logs. This connector supports event collection from Microsoft Windows 2003, 2008, 2008 R2, 2012, and 2012 R2. .



Note that Security events are not audited by default. Be sure to specify the type of security events to be audited (see "Enabling Auditing Policies" in this document).

There are three default Windows event logs:

- Application log (tracks events that occur in a registered application)
- Security log (tracks security changes and possible breaches in security)
- System log (tracks system events)

Note that security events are not audited by default. You must specify the type of system events to be audited. See the *SmartConnector for Microsoft Windows Event Log – Unified Configuration Guide*.

The configuration guide for the *SmartConnector for Microsoft Windows Event Log – Unified* also provides the following information:

- Configuring the Windows Machine
- Enabling Auditing Policies
- Deploying SmartConnectors for Microsoft Windows Event Log
- Installing, Upgrading, Rolling Back, and Uninstalling the SmartConnector
- Configuring the SmartConnector
- Configuring Windows Connectors to Capture Print Events



For complete information regarding Windows Security Events, see Randy Franklin Smith's comprehensive information at <http://www.ultimatewindowssecurity.com>

Windows 2008/2012 Common Security Mappings

The following security event mappings generally apply to all Windows Server 2008 and Windows Server 2012 Windows Event Log Security Events. For the cases in which specific security events have differing or extended mappings, see "Specific 2008 Windows Security Event Mappings."

HP ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Medium when Device Severity = Error or Warning; Low when Device Severity = Information or Audit_success
Destination Host Name	One of (Target Server Name, Computer Name, Target Server:Target Server Name)
Destination NT Domain	One of (Domain Name, Subject:Account Domain, New Token Information:Account Domain, Subject:Domain Name)
Destination Port	Network Information:Destination Port
Destination Process Name	One of (Process Information:New Process Name, Process Information:Process Name)
Destination Service Name	Service Information:Service Name
Destination User ID	One of (Subject:Logon ID, New Token Information:Logon ID)
Destination User Name	One of (Account Name, Subject:Account Name, Subject:Security ID, User, New Token Information:Account Name)
Destination User Privileges	One of (Additional Information:Privileges, New Right:User Right, Removed Right:User Right, Access Granted:Access Right, Access Removed:Access Right)
Device Action	One of (Account Action, Allowed, 'No', 'Blocked')
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom Number 1	Logon Type
Device Custom Number 2	Value of CrashOnAuditFail
Device Custom Number 3	Count
Device Custom String 1	One of (Access Request Information:Access Mask, Operation:Accesses, Operation:Access Mask)
Device Custom String 2	EventCategory
Device Custom String 4	One of (Error Code, Additional Information:Failure Code, Additional Information:Reason Code, Additional Information:Error Code, Failure Information:Failure Reason, Audit Events Dropped:Reason, Reason, Reason for Rejection, Error Information:Reason, Error Information:Error, Process Information:Exit Status)
Device Custom String 5	One of (Authentication Package Name, Authentication Package, Authentication, Detailed Authentication Information:authentication Package)
Device Event Category	Event logType
Device Event Class ID	Both (Event Source , Event ID)
Device Host Name	Computer Name
Device NT Domain	One of (Domain Name, Subject:Account Domain)
Device Product	'Microsoft Windows'
Device Receipt Time	DetectTime
Device Severity	EventType

HP ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
External ID	Event ID
File ID	One of (Object Handle ID, Object:Object Handle)
File Name	Object:Object Name
File Type	One of (Object Type, Object:Object Type)
Message	Message
Name	Description
Source Address	One of (Network Information:Source Network Address, Local Network Address, Additional Information:Client Address)
Source Host Name	One of (Subject:Client Name, Network Information:Workstation Name, Source Workstation, Additional Information:Client Name)
Source NT Domain	Subject:Client Domain
Source Port	One of (Network Information:Source Port, Network Information:Port, Network Information:Client Port)
Source Process Name	One of (Logon Process Name, process Information:Caller Process ID)

Specific 2008/2012 Windows Security Event Mappings

521 Unable to log events to security log.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 4	Status code
Device Custom Number 2	Value of CrashOnAuditFail
Device Custom Number 3	Number of failed audits

525 The connection authorization policy could not be updated.

HP ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	Value of CrashOnAuditFail

1101 Audit events have been dropped by the transport.

HP ArcSight ESM Field	Device-Specific Field
Device Custom Number 3	Audit Events Dropped:Reason

1102 The audit log was cleared.

This event is supported by common security event mappings. There are no specific mappings.

1104 The security log is now full.

This event is supported by common security event mappings. There are no specific mappings.

1105 Event log automatic backup.

HP ArcSight ESM Field	Device-Specific Field
File Type	Log
File Name	File

4610 An authentication package has been loaded by the Local Security Authority.

This event is supported by common security event mappings. There are no specific mappings.

4611 A trusted logon process has been registered with the Local Security Authority.

HP ArcSight ESM Field	Device-Specific Field
Destination Process Name	Logon Process Name

4612 Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.

HP ArcSight ESM Field	Device-Specific Field
Device Custom Number 3	Number of audit messages discarded

4614 A notification package has been loaded by the Security Account Manager.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 5	Notification Package Name

4615 Invalid use of LPC port.

This event is supported by common security event mappings. There are no specific mappings.

4616 The system time was changed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	Previous Time
Device Custom Date 2	New Time
Device Custom String 3	Process Information:Process ID
Destination Process Name	Process Information:Name

4618 A monitored security event pattern has occurred.

This event is supported by common security event mappings. There are no specific mappings.

4621 Administrator recovered system from CrashOnAuditFail.

HP ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	Value of CrashOnAuditFail

4622 A security package has been loaded by the Local Security Authority.

HP ArcSight ESM Field	Device-Specific Field
File Path	Security Package Name
Device Custom String 5	Security Package Name

4624 An account was successfully logged on.

HP ArcSight ESM Field	Device-Specific Field
Device NT Domain	Subject:Account Domain
Source Address	Network Information:Source Network Address
Destination Process Name	Process Information:Process Name
Destination User Name	New Logon: Account Name
Destination NT Domain	New Logon: Account Domain
Destination User ID	New Logon: Logon ID
Device Custom IPv6 Address 2	Network Information:Network Address
Device Custom String 3	Process Information:Process ID
Device Process Name	Detailed Authentication Information:Logon Process
Device Custom String 6	New Logon: Logon GUID

Windows 2012 and 2012 R2 add the following field:

HP ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	Network Information:Source Network Address

4625 An account failed to log on.

HP ArcSight ESM Field	Device-Specific Field
Device NT Domain	Subject:Account Domain
Destination User Name	Account For Which Logon Failed: Account Name
Destination Process Name	Process Information:Caller Process Name
Destination NT Domain	Account For Which Logon Failed: Account Domain
Device Custom String 3	Process Information:Caller Process ID
Device Process Name	Detailed Authentication Information:Logon Process
Source Address	Network Information:Source Network Address
Destination User ID	' '
Reason	Failure Information:Failure Reason

4626 User/Device claims information.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Device NT Domain	Subject:Account Domain
Destination User Name	New Logon:Account Name
Destination NT Domain	New Logon:Account Domain
Destination User ID	New Logon:Logon ID

4634 An account was logged off.

This event is supported by common security event mappings. There are no specific mappings.

4647 User initiated logoff.

This event is supported by common security event mappings. There are no specific mappings.

4648 A logon was attempted using explicit credentials.

HP ArcSight ESM Field	Device-Specific Field
Device NT Domain	Subject:Account Domain
Source Address	Network Information:Network Address
Destination Process Name	Process Information:Process Name
Destination User Name	Account Whose Credentials Were Used:Account Name
Destination NT Domain	Account Whose Credentials Were Used:Account Domain
Device Custom String 6	Account Whose Credentials Were Used:Logon GUID
Device Custom String 3	Process Information:Process ID

4649 A replay attack was detected.

This event is supported by common security event mappings. There are no specific mappings.

4650 An IPsec Main Mode security association was established. Extended Mode was not enabled.

This event is supported by common security event mappings. There are no specific mappings.

4651 An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Local Endpoint:Network Address
Source Port	Local Endpoint:Keying Module Port
Destination Address	Remote Endpoint:Network Address
Destination Port	Remote Endpoint:Keying Module Port

4652 An IPsec Main Mode negotiation failed.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Local Endpoint:Network Address
Source Port	Local Endpoint:Keying Module Port
Destination Address	Remote Endpoint:Network Address
Destination Port	Remote Endpoint:Keying Module Port
Message	Failure Information:Failure Reason

4653 An IPsec Main Mode negotiation failed.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Local Endpoint:Network Address
Source Port	Local Endpoint:Keying Module Port
Destination Address	Remote Endpoint:Network Address
Destination Port	Remote Endpoint:Keying Module Port
Message	Failure Information:Failure Reason

4654 An IPsec Quick Mode negotiation failed.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Local Endpoint:Network Address
Source Port	Local Endpoint:Port
Destination Address	Remote Endpoint:Network Address
Destination Port	Remote Endpoint:Port
Message	Failure Information:Failure Reason

4655 An IPsec Main Mode security associated ended.

This event is supported by common security event mappings. There are no specific mappings.

4656 A handle to an object was requested.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Access Request Information:Accesses
Device Custom String 3	Process Information:Process ID
Destination User Privileges	Access Request Information:Privileges Used for Access Check

4657 A registry value was modified.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Object:Object Value Name
Device Action	Object:Operation Type
Old File Type	Change Information:Old Value Type
Device Custom String 4	Change Information:Old Value
File Type	Change Information:New Value Type
Device Custom String 5	Change Information:New Value
Device Custom String 3	Process Information:Process ID

4658 The handle to an object was closed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Process Information:Process ID

4659 A handle to an object was requested with intent to delete.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Access Request Information:Accesses
Device Custom String 3	Process Information:Process ID

4660 An object was deleted.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Process Information:Process ID

4661 A handle to an object was requested.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Access Request Information:Accesses
Destination User Privileges	Access Request Information:Privileges Used for Access Check
Device Custom String 3	Process Information:Process ID

4662 An operation was performed on an object.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 5	Object:Object Type

4663 An attempt was made to access an object.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Access Request Information:Accesses
Device Custom String 3	Process Information:Process ID

4664 An attempt was made to create a hard link.

This event is supported by common security event mappings. There are no specific mappings.

4665 An attempt was made to create an application client context.

This event is supported by common security event mappings. There are no specific mappings.

4666 An application attempted an operation.

This event is supported by common security event mappings. There are no specific mappings.

4667 An application client context was deleted.

This event is supported by common security event mappings. There are no specific mappings.

4668 An application was initialized.

This event is supported by common security event mappings. There are no specific mappings.

4670 Permissions on an object were changed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Process:Process ID
Device Custom String 4	Permissions Change:Original Security Descriptor
Device Custom String 5	Permissions Change:New Security Descriptor

4671 An application attempted to access a blocked ordinal through the TBS.

This event is supported by common security event mappings. There are no specific mappings.

4672 Special privileges assigned to new logon.

Windows 2008 only.

HP ArcSight ESM Field	Device-Specific Field
Destination User Privileges	Privileges

4673 A privileged service was called.

This event is supported by common security event mappings. There are no specific mappings.

4674 An operation was attempted on a privileged object.

HP ArcSight ESM Field	Device-Specific Field
Destination User Privileges	Requested Operation:Privileges
Device Custom String 3	Process Information:Process ID
Destination Process Name	Process Information:Process Name

4675 SIDs were filtered.

This event is supported by common security event mappings. There are no specific mappings.

4688 A new process has been created.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Process Information:New Process ID
Device Custom String 5	Process Information:Creator Process ID

Windows 2012 and 2012 R2 add the following fields:

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (Account Name, Subject:Account Name, Subject:Security ID, User, New Token Information:Account Name)
Source User Name	One of (Subject:Account Name, Subject"SecurityID)
Destination User ID	'One of (Subject:Logon ID, New Token Information:Logon ID)
Source User ID	Subject:Logon Id
Device Custom String 4	Process Information:Process Command Line
Device Custom String 6	Process Information:Token Elevation Type

4689 A process has exited.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Process Information:Process ID

4690 An attempt was made to duplicate a handle to an object.

HP ArcSight ESM Field	Device-Specific Field
Old File ID	Source Handle Information:Source Handle ID
File ID	New Handle Information:Target Handle ID
Device Custom String 3	New Handle Information:Target Process ID
Device Custom String 5	Source Handle Information:Source Process ID

4691 Indirect access to an object was requested.

This event is supported by common security event mappings. There are no specific mappings.

4692 Backup of data protection master key was attempted.

This event is supported by common security event mappings. There are no specific mappings.

4693 Recovery of data protection master key was attempted.

This event is supported by common security event mappings. There are no specific mappings.

4694 Protection of auditable protected data was attempted.

This event is supported by common security event mappings. There are no specific mappings.

4695 Unprotection of auditable protected data was attempted.

This event is supported by common security event mappings. There are no specific mappings.

4696 A primary token was assigned to process.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Target Process:Target Process ID
Destination Process Name	Target Process:Target Process Name
Source Process Name	Process Information:Process Name
Source NT Domain	Subject:Account Domain
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source User ID	Subject:Logon ID
Destination User Name	One of (New Token Information:Account Name, New Token Information:Security ID)
Destination NT Domain	New Token Information:Account Domain
Destination User ID	New Token Information:Logon ID
Device Custom String 5	Process Information:Process ID

4697 A service was installed in the system.

HP ArcSight ESM Field	Device-Specific Field
File Path	Service Information:Service File Name
File Type	Service Information:Service Type
Device Custom String 5	Service Information:Service Start Type
Device Custom String 6	Service Information:Service Account

4698 A scheduled task was created.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Task Information:Task Name
Additional Data	Task Information:Task Content

4699 A scheduled task was deleted.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Task Information:Task Name
Additional Data	Task Information:Task Content

4700 A scheduled task was enabled.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Task Information:Task Name
Additional Data	Task Information:Task Content

4701 A scheduled task was disabled.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Task Information:Task Name
Additional Data	Task Information:Task Content

4702 A scheduled task was updated.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Task Information:Task Name
Additional Data	Task Information:Task Content

4704 A user right was assigned.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Security ID, Subject:Account Name)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name

4705 A user right was removed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Security ID, Subject:Account Name)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name

4706 A new trust was created to a domain.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	One of (Trusted Domain:Domain Name, Trusted Domain:Domain ID)
Device Custom String 5	Trust Information:Trust Type (1 = The other domain is pre Win2k (NTLM only supported); 2 = The other domain is Win2k or later (Windows Kerberos supported); 3 = Other domain is actually an MIT Kerberos Realm (probably UNIX); 4 = The trusted domain is a DCE realm)
Device Custom String 3	Trust Information:Trust Direction (0=Disabled, 1=Inbound, 2=Outbound, 3=Bidirectional)

4707 A trust to a domain was removed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	One of (Domain Information:Domain Name, Domain Information:Domain ID)

4709 IPsec Services was started.

This event is supported by common security event mappings. There are no specific mappings.

4713 Kerberos policy was changed.

HP ArcSight ESM Field	Device-Specific Field
Message	Both (Changes Made, Message)

4714 Encrypted data recovery policy was changed.

Windows 2008 mappings

HP ArcSight ESM Field	Device-Specific Field
Message	Both (Changes Made, Message)

4715 The audit policy (SACL) on an object was changed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Audit Policy Change:New Security Descriptor

4716 Trusted domain information was modified.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	One of (Trusted Domain:Domain Name, Trusted Domain:Domain ID)
Device Custom String 5	New Trust Information: Trust Type (1 = The other domain is pre Win2K (NTLM only supported); 2 = The other domain is Win2K or later (Windows Kerberos supported); 3 = Other domain is actually an MIT Kerberos Realm (probably UNIX); 4 = The trusted domain is a DCE realm)
Device Custom String 3	New Trust Information:Trust Direction (0=Disabled, 1=Inbound, 2=Outbound, 3=Bidirectional)

4717 System security access was granted to an account.

HP ArcSight ESM Field	Device-Specific Field
Source User ID	Subject:Logon ID
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Destination User Name	Account Modified:Account Name

4718 System security access was removed from an account.

HP ArcSight ESM Field	Device-Specific Field
Source User ID	Subject:Logon ID
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Destination User Name	Account Modified:Account Name

4719 System audit policy was changed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 5	Audit Policy Change:Subcategory
Device Action	Audit Policy Change:Changes
Device Custom String 6	Audit Policy Change:Category

4720 A user account was created.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	New Account:Account Name
Destination NT Domain	New Account:Account

4722 A user account was enabled.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Security ID, Subject:Account Name)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Target Account:Security ID, Target Account:Account Name)
Destination NT Domain	Target Account:Account Domain

4723 An attempt was made to change an account's password.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain

4724 An attempt was made to reset an account's password.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain

4725 A user account was disabled.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain

4726 A user account was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain

4727 A security-enabled global group was created.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (New Group:Group Domain, New Group:Group Name)

4728 A member was added to a security-enabled global group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)
Destination User ID	Member:Account Name

4729 A member was removed from a security-enabled global group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)
Destination User ID	Member:Account Name

4730 A security-enabled global group was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Deleted Group:Group Domain, Deleted Group:Group Name)

4731 A security-enabled local group was created.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (New Group:Group Domain, New Group:Group Name)

4732 A member was added to a security-enabled local group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)
Destination User ID	Member:Account Name

4733 A member was removed from a security-enabled local group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Member:Security ID extracted from NTUser
Destination NT Domain	Member:Security ID extracted from NTDomain
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)
Destination User ID	Member:Account Name

4734 A security-enabled local group was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4735 A security-enabled local group was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4737 A security-enabled global group was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4738 A user account was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain

4739 Domain Policy was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination NT Domain	Domain: Domain Name
Message	Change Type
Device Custom String 6	Both (Changed Attributes:Min. Password Age,Changed Attributes:Max. Password Age,Changed Attributes:Force Logoff,Changed Attributes:Lockout Threshold,Changed Attributes:Lockout Observation Window,Changed Attributes:Lockout Duration,Changed Attributes:Password Properties,Changed Attributes:Min. Password Length,Changed Attributes:Machine Account Quota,Changed Attributes:Mixed Domain Mode,Changed Attributes:Domain Behavior Version,Changed Attributes:OEM Information)

4740 A user account was locked out.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Account That Was Locked Out:Account Name
Source Host Name	Additional Information:Caller Computer Name
Destination NT Domain	Account that was locked out: Security ID

4741 A computer account was created.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (New Computer Account:Account Domain, New Computer Account:Account Name)

4742 A computer account was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Computer Account That Was Changed:Account Domain, Computer Account That Was Changed:Account Name)
Destination User Name	One of (Subject:Account Name, Subject:Security ID)

4743 A computer account was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Target Computer:Account Domain, Target Computer:Account Name)

4744 A security-disabled local group was created.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (New Group:Group Domain, New Group:Group Name)

4745 A security-disabled local group was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4746 A member was added to a security-disabled local group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID
Destination User ID	Member:Account Name
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4747 A member was removed from a security-disabled local group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Destination User Name	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID
Destination User ID	Member:Account Name
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4748 A security-disabled local group was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4749 A security-disabled global group was created.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4750 A security-disabled global group was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4751 A member was added to a security-disabled global group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Member:Security ID, Member:Account Name)
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4752 A member was removed from a security-disabled global group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4753 A security-disabled global group was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4754 A security-enabled universal group was created.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4755 A security-enabled universal group was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4756 A member was added to a security-enabled universal group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)
Destination User ID	Member:Account Name

4757 A member was removed from a security-enabled universal group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)
Destination User ID	Member:Account Name

4758 A security-enabled universal group was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4759 A security-disabled universal group was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4760 A security-disabled universal group was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4761 A member was added to a security-disabled universal group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID
Destination User ID	Member:Account Name
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4762 A member was removed from a security-disabled universal group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID
Destination User ID	Member:Account Name
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4763 A security-disabled universal group was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)

4764 A group's type was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)
Device Custom String 5	Change Type

4765 SID History was added to an account.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain
Device Custom String 6	Source Account:Account Name

4766 An attempt to add SID History to an account failed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain
Device Custom String 6	Source Account:Account Name

4767 A user account was unlocked.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain

4768 A Kerberos authentication ticket (TGT) was requested.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Network Information:Client Address
Destination User Name	Account Information:Account Name
Destination NT Domain	Account Information:Supplied Realm Name
Device Custom String 4	Additional Information:Result Code
Device Custom String 5	Additional Information:Pre-Authentication Type
Source Address	Network Information:Client Address
Device Custom IPv6 Address 2	Network Information:Network Address

Windows 2012 and 2012 R2 add the following field:

HP ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	Network Information:Client Address

4769 A Kerberos service ticket was requested.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	One of (Network Information:Client Address, 'Client Address')
Destination User Name	Account Information:Account Name
Destination NT Domain	Account Information:Account Domain
Destination Service Name	Service Information:Service Name
Device Custom String 6	Account Information:Logon GUID
Source Address	Network Information:Client Address
Device Custom IPv6 Address 2	Network Information:Network Address

Windows 2012 and 2012 R2 add the following field:

HP ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	Network Information:Client Address

4770 A Kerberos service ticket was renewed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Network Information:Client Address
Destination User Name	Account Information:Account Name
Destination NT Domain	Account Information:Account Domain
Destination Service Name	Service Information:Service Name
Device Custom IPv6 Address 2	Network Information:Network Address

Windows 2012 and 2012 R2 add the following field:

HP ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	Network Information:Client Address

4771 Kerberos pre-authentication failed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Network Information:Client Address
Destination User Name	Account Information:Account Name
Destination NT Domain	Account Information:Security ID
Destination Service Name	Service Information:Service Name
Reason	Additional Information:Failure Code

Windows 2012 and 2012 R2 add the following field:

HP ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	Network Information:Client Address

4772 A Kerberos Authentication ticket request failed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Network Information:Client Address

4773 A Kerberos service ticket request failed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Network Information:Client Address

4774 An account was mapped for logon.

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	Mapped Name

4775 An account could not be mapped for logon.

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	Account Name

4776 The domain controller attempted to validate the credentials for an account.

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	Logon Account
Reason	Error Code

4777 The domain controller failed to validate the credentials for an account.

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	Logon Account

4778 A session was reconnected to a Window Station.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Session:Session Name

4779 A session was disconnected from a Window Station.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Session:Session Name

4780 The ACL was set on accounts that are members of administrators groups.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain

4781 The name of an account was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Old Account Name
Destination NT Domain	Target Account:Account Domain
Device Custom String 6	Target Account:New Account Name

4782 The password hash account was accessed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain

4783 A basic application group was created.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Group:Security ID, Group:Account Name)
Destination NT Domain	Group:Account Domain

4784 A basic application group was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Group:Security ID, Group:Account Name)
Destination NT Domain	Group:Account Domain

4785 A member was added to a basic application group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Member:Security ID,Member:Account Name)
Device Custom String 6	Both (Group:Group Domain,Group:Group Name)

4786 A member was removed from a basic application group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Member:Security ID,Member:Account Name)
Device Custom String 6	Both (Group:Group Domain,Group:Group Name)

4787 A non-member was added to a basic application group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Member:Security ID,Member:Account Name)
Device Custom String 6	Both (Group:Account Domain, Group:Account Name)

4788 A non-member was removed from a basic application group.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Member:Security ID,Member:Account Name)
Device Custom String 6	Both (Group:Account Domain, Group:Account Name)

4789 A basic application group was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Group:Security ID, Group:Account Name)
Destination NT Domain	Group:Account Domain

4789 A basic application group was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Group:Security ID, Group:Account Name)
Destination NT Domain	Group:Account Domain

4790 An LDAP query group was created.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Group:Security ID, Group:Account Name)
Destination NT Domain	Group:Account Domain

4791 A basic application group was changed.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Group:Security ID, Group:Account Name)
Destination NT Domain	Group:Account Domain

4792 An LDAP security group was deleted.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	One of (Group:Security ID, Group:Account Name)
Destination NT Domain	Group:Account Domain

4793 The Password Policy Checking API was called.

HP ArcSight ESM Field	Device-Specific Field
Source Host Name	Additional Information:Caller Workstation
Source User Name	Additional Information:Provided Account Name (unauthenticated)
Device Custom String 4	Additional Information:Status Code

4794 An attempt was made to set the Directory Services Restore Mode administrator password.

This event is supported by common security event mappings. There are no specific mappings.

4797 An attempt was made to query the existence of a blank password for an account.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Additional Information:Caller Workstation
Destination User Name	Additional Information:Target Account Name
Destination NT Domain	Additional Information:Target Account Domain

4800 The workstation was locked.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Subject:Session ID

4801 The workstation was unlocked.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Subject:Session ID

4802 The screen saver was invoked.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Subject:Session ID

4803 The screen saver was dismissed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Subject:Session ID

4816 RPC detected an integrity violation while decrypting an incoming message.

This event is supported by common security event mappings. There are no specific mappings.

4817 Auditing settings on object were changed.

Windows 2012 and 2012 R2 Only

This event is supported by common security event mappings. There are no specific mappings.

4818 Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Destination Process ID	Process Information:Process ID

4819 Central Access policies on the machine have been changed.

Windows 2012 and 2012 R2 Only

This event is supported by common security event mappings. There are no specific mappings.

4820 A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions.

Windows 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 1	All of ('Pre-Authentication Type:', Additional Information:Pre-Authentication Type, 'Result Code:', Additional Information:Result Code, 'Ticket Encryption Type:', Additional Information:Ticket Encryption Type, 'Ticket Options:', Additional Information:Ticket Options)
Device Custom String 3	Authentication Policy Information:Silo Name
Device Custom String 4	All of ('Certificate Issuer Name:', Certificate Information:Certificate Issuer Name, 'Certificate Serial Number:', Certificate Information:Certificate Serial Number, 'Certificate Thumbprint:', Certificate Information:Certificate Thumbprint)
Device Custom String 5	Service Information:Service ID
Device Custom String 6	Authentication Policy Information:Policy Name
Source Address	Network Information:Client Address
Source DNS Domain	Account Information:Supplied Realm Name
Source User ID	Account Information:User ID
Source User Name	Account Information:Account Name (from NTUser)
Additional data	Device Information:DeviceName
Additional data	Authentication Policy Information:TGT Lifetime

4821 A Kerberos ticket was denied because the user, device, or both does not meet the access control restrictions.

Windows 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Destination Process ID	Service Information:Service ID
Device Custom String 1	All of ('Result Code:', Additional Information:Failure Code, 'Ticket Encryption Type:', Additional Information:Ticket Encryption Type, 'Ticket Options:', Additional Information:Ticket Options, 'Transited Services', Additional Information:Transited Services)
Device Custom String 5	Authentication Policy Information:Silo Name
Device Custom String 6	Authentication Policy Information:Policy Name
Source Address	Network Information:Client Address
Source DNS Domain	Account Information:Account Domain
Source User ID	Account Information:Logon GUID
Source User Name	Account Information:Account Name (from NTUser)
Additional data	Device Information:DeviceName

4822 NTLM authentication failed because the account was a member of the Protected User group.

Windows 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Additional data	Device Name
Reason	Error Code

4823 NTLM authentication failed because access control restrictions are required.

Windows 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Additional data	Device Name
Reason	Error Code
Device Custom String 5	Authentication Policy Information:Silo Name
Device Custom String 6	Authentication Policy Information:PolicyName

4824 Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group.

Windows 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 1	All of ('Pre-Authentication Type:', Additional Information:Pre-Authentication Type, ' Failure Code:', Additional Information:Failure Code, ' Ticket Options:', Additional Information:Ticket Options)
Device Custom String 4	All of ('Certificate Issuer Name:', Certificate Information:Certificate Issuer Name, ' Certificate Serial Number:', Certificate Information:Certificate Serial Number, ' Certificate Thumbprint:', Certificate Information:Certificate Thumbprint)
Source Address	Network Information:Client Address
Source User Name	Account Information:Account Name (from NTUser)

4864 A namespace collision was detected.

This event is supported by common security event mappings. There are no specific mappings.

4865 A trusted forest information entry was added.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Trust Information:Operation ID
Device Custom String 5	Trust Information:Top Level Name
Device Custom String 6	Trust Information:Forest Root

4866 A trusted forest information entry was removed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Trust Information:Operation ID
Device Custom String 5	Trust Information:Top Level Name
Device Custom String 6	Trust Information:Forest Root

4867 A trusted forest information entry was modified.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Trust Information:Operation ID
Device Custom String 5	Trust Information:Top Level Name
Device Custom String 6	Trust Information:Forest Root

4868 The certificate manager denied a pending certificate request.

This event is supported by common security event mappings. There are no specific mappings.

4869 Certificate Services received a resubmitted certificate request.

This event is supported by common security event mappings. There are no specific mappings.

4870 Certificate Services revoked a certificate.

This event is supported by common security event mappings. There are no specific mappings.

4871 Certificate Services received a request to publish the certificate revocation list (CRL).

This event is supported by common security event mappings. There are no specific mappings.

4872 Certificate Services published the certificate revocation list (CRL).

This event is supported by common security event mappings. There are no specific mappings.

4873 A certificate request extension changed.

This event is supported by common security event mappings. There are no specific mappings.

4874 One or more certificate request attributes changed.

This event is supported by common security event mappings. There are no specific mappings.

4875 Certificate Services received a request to shutdown.

Windows 2012 and 2012 R2 Only

This event is supported by common security event mappings. There are no specific mappings.

4876 Certificate Services backup started.

This event is supported by common security event mappings. There are no specific mappings.

4877 Certificate Services backup completed.

Windows 2012 and 2012 R2 Only

This event is supported by common security event mappings. There are no specific mappings.

4880 Certificate Services started.

This event is supported by common security event mappings. There are no specific mappings.

4881 Certificate Services stopped.

This event is supported by common security event mappings. There are no specific mappings.

4882 The security permissions for Certificate Services changed.

Windows 2012 and 2012 R2 Only

This event is supported by common security event mappings. There are no specific mappings.

4883 Certificate Services retrieved an archived key.

This event is supported by common security event mappings. There are no specific mappings.

4884 Certificate Services imported a certificate into its database.

This event is supported by common security event mappings. There are no specific mappings.

4885 The audit filter for Certificate Services changed.

This event is supported by common security event mappings. There are no specific mappings.

4886 Certificate Services received a certificate request.

This event is supported by common security event mappings. There are no specific mappings.

4887 Certificate Services approved a certificate request and issued a certificate.

This event is supported by common security event mappings. There are no specific mappings.

4888 Certificate Services denied a certificate request.

This event is supported by common security event mappings. There are no specific mappings.

4889 Certificate Services set the status of a certificate request to pending.

This event is supported by common security event mappings. There are no specific mappings.

4890 The certificate manager settings for Certificate Services changed.

This event is supported by common security event mappings. There are no specific mappings.

4891 A configuration entry changed in Certificate Services.

This event is supported by common security event mappings. There are no specific mappings.

4892 A property of Certificate Services changed.

This event is supported by common security event mappings. There are no specific mappings.

4893 Certificate Services archived a key.

This event is supported by common security event mappings. There are no specific mappings.

4894 Certificate Services imported and archived a key.

This event is supported by common security event mappings. There are no specific mappings.

4895 Certificate Services published the CA certificate to Active Directory Domain Services.

This event is supported by common security event mappings. There are no specific mappings.

4896 One or more rows have been deleted from the certificate database.

This event is supported by common security event mappings. There are no specific mappings.

4897 Role separation enabled.

Windows 2012 and 2012 R2 Only

This event is supported by common security event mappings. There are no specific mappings.

4898 Certificate Services loaded a template.

This event is supported by common security event mappings. There are no specific mappings.

4899 A Certificate Services template was updated.

This event is supported by common security event mappings. There are no specific mappings.

4900 Certificate Services template security was updated.

This event is supported by common security event mappings. There are no specific mappings.

4902 The Per-user audit policy table was created.

HP ArcSight ESM Field	Device-Specific Field
Device Custom Number 3	Number of Elements
Device Custom String 6	Policy ID

4904 An attempt was made to register a security event source.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Process:Process ID
Device Custom String 5	Event Source:Event Source ID
Device Custom String 6	Event Source:Source Name
Destination Process Name	Process:Process Name

4905 A user right was removed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Process:Process ID
Device Custom String 5	Event Source:Event Source ID
Device Custom String 6	Event Source:Source Name
Destination Process Name	Process:Process Name

4906 The CrashOnAuditFail value has changed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	New Value of CrashOnAuditFail

4907 Auditing settings on object were changed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 5	Object:Object Type
Device Custom String 3	Process Information:Process ID

4908 Special Groups Logon table modified.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Special Groups

4909 The local policy settings for the TBS were changed.

This event is supported by common security event mappings. There are no specific mappings.

4910 The group policy settings for the TBS were changed.

This event is supported by common security event mappings. There are no specific mappings.

4911 Resource attributes of the object were changed.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Destination Process ID	Process Information:Process ID

4912 Per User Audit Policy was changed.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Policy for Account:Security ID
Device Custom String 5	Policy Change Details:Subcategory
Device Action	Policy Change Details:Changes

4913 Central Access Policy on the object was changed.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Destination Process ID	Process Information:Process ID

4928 An Active Directory replica source naming context was established.

This event is supported by common security event mappings. There are no specific mappings.

4929 An Active Directory replica source naming context was removed.

This event is supported by common security event mappings. There are no specific mappings.

4930 An Active Directory replica source naming context was modified.

This event is supported by common security event mappings. There are no specific mappings.

4931 An Active Directory replica destination naming context was modified.

This event is supported by common security event mappings. There are no specific mappings.

4932 Synchronization of a replica of an Active Directory naming context has begun.

This event is supported by common security event mappings. There are no specific mappings.

4933 Synchronization of a replica of an Active Directory naming context has ended.

This event is supported by common security event mappings. There are no specific mappings.

4934 Attributes of an Active Directory object were replicated.

This event is supported by common security event mappings. There are no specific mappings.

4935 Replication failure begins.

This event is supported by common security event mappings. There are no specific mappings.

4936 Replication failure ends.

This event is supported by common security event mappings. There are no specific mappings.

4937 A lingering object was removed from a replica.

This event is supported by common security event mappings. There are no specific mappings.

4944 The following policy was active when the Windows Firewall started.

This event is supported by common security event mappings. There are no specific mappings.

4945 A rule was listed when the Windows Firewall started.

This event is supported by common security event mappings. There are no specific mappings.

4946 A change has been made to Windows Firewall exception list. A rule was added.

This event is supported by common security event mappings. There are no specific mappings.

4947 A change has been made to Windows Firewall exception list. A rule was modified.

This event is supported by common security event mappings. There are no specific mappings.

4948 A change has been made to Windows Firewall exception list. A rule was deleted.

This event is supported by common security event mappings. There are no specific mappings.

4950 A Windows Firewall setting has changed.

This event is supported by common security event mappings. There are no specific mappings.

4951 A rule has been ignored because its major version number was not recognized by Windows Firewall

This event is supported by common security event mappings. There are no specific mappings.

4952 Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall.

This event is supported by common security event mappings. There are no specific mappings.

4953 A rule has been ignored by Windows Firewall because it could not parse the rule.

This event is supported by common security event mappings. There are no specific mappings.

4956 Windows Firewall has changed the active profile.

This event is supported by common security event mappings. There are no specific mappings.

4957 Windows Firewall did not apply the following rule.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 4	Both (Error Information:Reason," resolved to an empty set.")
Device Custom String 6	Rule Information:Name

4958 Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.

This event is supported by common security event mappings. There are no specific mappings.

4960 IPsec dropped an inbound packet that failed an integrity check.

This event is supported by common security event mappings. There are no specific mappings.

4961 IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.

This event is supported by common security event mappings. There are no specific mappings.

4962 IPsec dropped an inbound packet that failed a replay check. The inbound packet has too low a sequence number to ensure it was not a replay.

This event is supported by common security event mappings. There are no specific mappings.

4963 IPsec dropped an inbound clear text packet that should have been secured.

This event is supported by common security event mappings. There are no specific mappings.

4964 Special groups have been assigned to a new logon.

HP ArcSight ESM Field	Device-Specific Field
Source User Name	Subject:Account Name
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Destination User Name	New Logon:Account Name
Destination NT Domain	New Logon:Account Domain
Destination User ID	New Logon:Logon ID
Device Custom String 3	New Logon:Logon GUID
Device Custom String 6	New Logon:Special Groups Assigned

4965 IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI).

This event is supported by common security event mappings. There are no specific mappings.

4976 During Main Mode negotiation, IPsec received an invalid negotiation packet.

This event is supported by common security event mappings. There are no specific mappings.

4977 During Quick Mode negotiation, IPsec received an invalid negotiation packet.

This event is supported by common security event mappings. There are no specific mappings.

4978 During Extended Mode negotiation, IPsec received an invalid negotiation packet.

This event is supported by common security event mappings. There are no specific mappings.

4979 IPsec Main Mode and Extended Mode security associations were established.

This event is supported by common security event mappings. There are no specific mappings.

4980 IPsec Main Mode and Extended Mode security associations were established.

This event is supported by common security event mappings. There are no specific mappings.

4981 An IPsec Quick Mode security association was established.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Local Endpoint:Network Address
Source Port	Local Endpoint:Keying Module Port
Destination Address	Remote Endpoint:Network Address
Destination Port	Remote Endpoint:Keying Module Port

4982 An IPsec Quick Mode security association was established.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Local Endpoint:Network Address
Source Port	Local Endpoint:Keying Module Port
Destination Address	Remote Endpoint:Network Address
Destination Port	Remote Endpoint:Keying Module Port

4983 An IPsec Quick Mode security association was established

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Local Endpoint:Network Address
Source Port	Local Endpoint:Keying Module Port
Destination Address	Remote Endpoint:Network Address
Destination Port	Remote Endpoint:Keying Module Port

4984 An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Local Endpoint:Network Address
Source Port	Local Endpoint:Keying Module Port
Destination Address	Remote Endpoint:Network Address
Destination Port	Remote Endpoint:Keying Module Port
Message	Failure Information:Failure Reason

4985 The state of a transaction has changed.

This event is supported by common security event mappings. There are no specific mappings.

5027 The Windows Firewall Service was unable to retrieve the security policy from the local storage.

This event is supported by common security event mappings. There are no specific mappings.

5028 The Windows firewall Service was unable to parse the new security policy.

This event is supported by common security event mappings. There are no specific mappings.

5029 The Windows Firewall Service failed to initialize the driver.

This event is supported by common security event mappings. There are no specific mappings.

5030 The Windows Firewall Service failed to start.

This event is supported by common security event mappings. There are no specific mappings.

5031 The Windows Firewall Service blocked an application from accepting incoming connections on the network.

This event is supported by common security event mappings. There are no specific mappings.

5032 Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.

This event is supported by common security event mappings. There are no specific mappings.

5035 The Windows Firewall Driver failed to start.

This event is supported by common security event mappings. There are no specific mappings.

5037 The Windows Firewall Driver detected official runtime error. Terminating.

This event is supported by common security event mappings. There are no specific mappings.

5038 Code integrity determined that the image hash of a file is not valid.

This event is supported by common security event mappings. There are no specific mappings.

5039 A registry key was virtualized.

This event is supported by common security event mappings. There are no specific mappings.

5040 A change has been made to IPsec settings. An Authentication Set was added.

This event is supported by common security event mappings. There are no specific mappings.

5041 A change has been made to IPsec settings. An Authentication Set was modified.

This event is supported by common security event mappings. There are no specific mappings.

5042 A change has been made to IPsec settings. An Authentication Set was deleted.

This event is supported by common security event mappings. There are no specific mappings.

5043 A change has been made to IPsec settings. A Connection Security Rule was added.

This event is supported by common security event mappings. There are no specific mappings.

5044 A change has been made to IPsec settings. A Connection Security Rule was modified.

This event is supported by common security event mappings. There are no specific mappings.

5045 A change has been made to IPsec settings. A Connection Security Rule was deleted.

This event is supported by common security event mappings. There are no specific mappings.

5046 A change has been made to IPsec settings. A Crypto Set was added.

This event is supported by common security event mappings. There are no specific mappings.

5047 A change has been made to IPsec settings. A Crypto Set was modified.

This event is supported by common security event mappings. There are no specific mappings.

5048 A change has been made to IPsec settings. A Crypto Set was deleted.

This event is supported by common security event mappings. There are no specific mappings.

5049 An IPsec Security Association was deleted.

This event is supported by common security event mappings. There are no specific mappings.

5050 An attempt to programmatically disable the Windows Firewall using a call to INetFwProfile.

This event is supported by common security event mappings. There are no specific mappings.

5051 A file was virtualized.

This event is supported by common security event mappings. There are no specific mappings.

5056 A cryptographic self test was performed.

This event is supported by common security event mappings. There are no specific mappings.

5057 A cryptographic primitive operation failed.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Message	Failure Information:Reason
Reason	Failure Information:Return Code

5058 Key file operation.

HP ArcSight ESM Field	Device-Specific Field
File Name	Cryptographic Parameters:Key Name
File Type	Cryptographic Parameters:Key Type
File Path	Key File Operation Information:File Path
Device Action	Key File Operation Information:Operation
Device Custom String 4	Key File Operation Information:Return Code

5059 Key migration operation.

HP ArcSight ESM Field	Device-Specific Field
File Name	Cryptographic Parameters:Key Name
File Type	Cryptographic Parameters:Key Type
Device Action	Additional Information:Operation
Device Custom String 4	Additional Information:Return Code

5060 Verification operation failed.

This event is supported by common security event mappings. There are no specific mappings.

5061 Cryptographic operation.

This event is supported by common security event mappings. There are no specific mappings.

5062 A kernel-mode cryptographic self test was performed.

This event is supported by common security event mappings. There are no specific mappings.

5063 A cryptographic provider operation was attempted.

This event is supported by common security event mappings. There are no specific mappings.

5064 A cryptographic context operation was attempted.

This event is supported by common security event mappings. There are no specific mappings.

5065 A cryptographic context modification was attempted.

This event is supported by common security event mappings. There are no specific mappings.

5066 A cryptographic function operation was attempted.

This event is supported by common security event mappings. There are no specific mappings.

5067 A cryptographic function modification was attempted.

This event is supported by common security event mappings. There are no specific mappings.

5068 A cryptographic function provider operation was attempted.

This event is supported by common security event mappings. There are no specific mappings.

5069 A cryptographic function property operation was attempted.

This event is supported by common security event mappings. There are no specific mappings.

5070 A cryptographic function property modification was attempted.

This event is supported by common security event mappings. There are no specific mappings.

5071 Key access denied by Microsoft key distribution service.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Source Host Name	Additional Information:Caller Workstation
Device Custom String 5	Security Descriptor

5122 A Configuration entry changed in the OCSP Responder Service.

This event is supported by common security event mappings. There are no specific mappings.

5123 A configuration entry changed in the OCSP Responder Service.

This event is supported by common security event mappings. There are no specific mappings.

5124 A security setting was updated on OCSP Responder Service.

This event is supported by common security event mappings. There are no specific mappings.

5126 Signing Certificate was automatically updated by the OCSP Responder Service.

This event is supported by common security event mappings. There are no specific mappings.

5127 The OCSP Revocation provider successfully updated the revocation information.

This event is supported by common security event mappings. There are no specific mappings.

5136 A directory service object was modified.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Object: DN
Device Custom String 5	Object: Class
Device Custom String 4	Operation:Type

5137 A directory service object was created.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Object: DN
Device Custom String 5	Object: Class

5138 A directory service object was undeleted.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Object: New DN
Device Custom String 5	Object: Class

5139 A directory service object was moved.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Object: New DN
Device Custom String 5	Object: Class

5140 A network share object was accessed.

Windows 2008 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Network Information:Source Address
File Path	Share Name
Device Custom String 6	Share Name

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Network Information:Source Address
Device Custom IPv6 Address 2	Network Information:Source Address
File Path	Share Information:Share Name
File Type	Network Information:Object Type
Device Custom String 1	Access Request Information:Accesses
Device Custom String 6	Share Information:Share Name

5141 A directory service object was deleted.

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Object: DN
Device Custom String 5	Object: Class

5142 A network share object was added.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
File Path	Share Information:Share Name
Device Custom String 6	Share Information:Share Name

5143 A network share object was modified.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
File Path	Share Information:Share Name
Device Custom String 6	Share Information:Share Name
Device Custom String 5	Object:Object Type

5144 A network share object was deleted.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
File Path	Share Information:Share Name
Device Custom String 6	Share Information:Share Name
Device Custom String 5	Object:Object Type

5145 A network share object was checked to see whether client can be granted desired access

HP ArcSight ESM Field	Device-Specific Field
Source NT Domain	Subject:Account Domain
Source User ID	Subject:Logon ID
Source Address	Network Information:Source Address
Device Custom String 1	Access Request Information:Accesses

Windows 2012 adds this field:

HP ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	Network Information:Source Address

5146 The Windows Filtering Platform has blocked a packet.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Device Direction	Network Information:Direction
Device Custom IPv6 Address 2	Network Information:Source Address
Source Address	Network Information:Source Address
Destination Address	Network Information:Destination Address
Device Custom IPv6 Address 3	Network Information:Destination Address
Source Port	Network Information:Source vSwitch Port
Destination Port	Network Information:Destination vSwitch Port

5147 A more restrictive Windows Filtering Platform filter has blocked a packet.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
Device Direction	Network Information:Direction
Device Custom IPv6 Address 2	Network Information:Source Address
Source Address	Network Information:Source Address
Destination Address	Network Information:Destination Address
Device Custom IPv6 Address 3	Network Information:Destination Address
Source Port	Network Information:Source vSwitch Port
Destination Port	Network Information:Destination vSwitch Port

5152 The Windows Filtering Platform blocked a packet.

This event is supported by common security event mappings. There are no specific mappings.

5153 A more restrictive Windows Filtering Platform filter has blocked a packet.

This event is supported by common security event mappings. There are no specific mappings.

5154 The Windows Filtering platform has permitted an application or service to listen on a port for incoming connections.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Network Information:Source Address
Device Custom IPv6 Address 2	Network Information:Source Address

5155 The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.

This event is supported by common security event mappings. There are no specific mappings.

5156 The Windows Filtering Platform has allowed a connection.

This event is supported by common security event mappings. There are no specific mappings.

5157 The Windows Filtering Platform has blocked a connection.

This event is supported by common security event mappings. There are no specific mappings.

5158 The Windows Filtering Platform has permitted a bind to a local port.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Network Information:Source Address
Device Custom IPv6 Address 2	Network Information:Source Address

5159 The Windows Filtering Platform has blocked a bind to a local port.

Windows 2008 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Process ID	Application Information:Process ID
File Name	Application Information:Application Name
File Path	Application Information:Application Name
File Type	One of (Application Information:Application Name, 'Application')
Source Address	Network Information:Source Address
Destination Address	Network Information:Source Address
Transport Protocol	Network Information:Protocol
Device Custom Number 2	Filter Information:Filter Run-Time ID
Device Custom String 6	Filter Information:Layer Name
Device Custom Number 3	Filter Information:Layer Run-Time ID

Windows 2012 and 2012 R2 mappings:

This event is supported by common security event mappings. There are no specific mappings.

5168 Spn check for SMB/SMB2 fails.

Windows 2008 only

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	' '
Source User Name	One of (Subject:Account Name, Subject:Security KD)
Destination User ID	' '
Source User ID	Subject:Logon ID
Destination Service Name	SPN:SPN Name
Device Custom String 4	SPN:Error Code
Reason	SPN:Error Code

5376 Credential Manager credentials were backed up.

This event is supported by common security event mappings. There are no specific mappings.

5377 Credential Manager credentials were restored from a backup.

This event is supported by common security event mappings. There are no specific mappings.

5378 The requested credentials delegation was disallowed by policy.

This event is supported by common security event mappings. There are no specific mappings.

5440 The following callout was present when the Windows Filtering Platform Base Filtering Engine started.

This event is supported by common security event mappings. There are no specific mappings.

5441 The following filter was present when the Windows Filtering Platform Base Filtering Engine started.

This event is supported by common security event mappings. There are no specific mappings.

5442 The following provider was present when the Windows Filtering Platform Base Filtering Engine started.

This event is supported by common security event mappings. There are no specific mappings.

5443 The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.

This event is supported by common security event mappings. There are no specific mappings.

5444 The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.

This event is supported by common security event mappings. There are no specific mappings.

5446 A Windows Filtering Platform callout has been changed.

This event is supported by common security event mappings. There are no specific mappings.

5447 A Windows Filtering Platform filter has been changed.

This event is supported by common security event mappings. There are no specific mappings.

5448 A Windows Filtering Platform provider has been changed.

This event is supported by common security event mappings. There are no specific mappings.

5449 A Windows Filtering Platform provider context has been changed.

This event is supported by common security event mappings. There are no specific mappings.

5450 A Windows Filtering Platform sub-layer has been changed.

This event is supported by common security event mappings. There are no specific mappings.

5451 An IPsec Quick Mode security association was established.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Local Endpoint:Network Address
Source Port	Local Endpoint:Port
Destination Address	Remote Endpoint:Network Address
Destination Port	Remote Endpoint:Port

5452 An IPsec Quick Mode security association ended.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Source Address	Local Endpoint:Network Address
Source Port	Local Endpoint:Port
Destination Address	Remote Endpoint:Network Address
Destination Port	Remote Endpoint:Port

5456 PASTore Engine applied Active Directory storage IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5457 PASTore Engine failed to apply Active Directory storage IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5458 PASTore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5459 PASTore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5460 PASTore Engine applied local registry storage IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5461 PAStore Engine failed to apply local registry storage IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5462 PAStore Engine failed to apply some rules of the active IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5471 PAStore Engine loaded local storage IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5472 PAStore Engine failed to load local storage IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5473 PAStore Engine loaded directory storage IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5474 PAStore Engine failed to load directory storage IPsec policy on the computer.

This event is supported by common security event mappings. There are no specific mappings.

5477 PAStore Engine failed to add quick mode filter.

This event is supported by common security event mappings. There are no specific mappings.

5483 IPsec Services failed to initialize RPC server. IPsec Services could not be started.

This event is supported by common security event mappings. There are no specific mappings.

5484 IPsec Services has experienced a critical failure and has been shut down.

This event is supported by common security event mappings. There are no specific mappings.

5632 A request was made to authenticate to a wireless network.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Reason	One of (Additional Information:EAP Error Code, Additional Information:EAP Reason Code, Additional Information:Error Code, both (Additional Information:Reason Code2, Additional Information:Reason Code))

5633 A request was made to authenticate to a wired network.

Windows 2008 mappings:

This event is supported by common security event mappings. There are no specific mappings.

Windows 2012 and 2012 R2 mappings:

HP ArcSight ESM Field	Device-Specific Field
Reason	One of (Additional Information:Error Code, both (Additional Information:Reason Code2, Additional Information:Reason Code))
Device Outbound Interface	Interface:Name

5712 A Remote Procedure Call (RPC) was attempted.

This event is supported by common security event mappings. There are no specific mappings.

5888 An object in the COM+ Catalog was attempted.

This event is supported by common security event mappings. There are no specific mappings.

5889 An object was deleted from the COM+ Catalog.

This event is supported by common security event mappings. There are no specific mappings.

5890 An object was added to the COM+ Catalog.

This event is supported by common security event mappings. There are no specific mappings.

6144 Security policy In the group policy objects has been applied successfully.

This event is supported by common security event mappings. There are no specific mappings.

6145 One or more errors occurred while processing security policy in the group policy objects.

This event is supported by common security event mappings. There are no specific mappings.

6272 Network Policy Server granted access to a user.

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	User:Account Name
Destination NT Domain	User:Account Domain
Destination User ID	User:Fully Qualified Account Name
Source User Name	Client Machine:Account Name
Source User ID	Client Machine:Fully Qualified Account Name
Source Address	Client Machine:Calling Station Identifier
Device Custom String 1	Authentication Details:Proxy Policy Name
Device Custom String 3	RADIUS Client:Client IP Address
Destination Address	NAS:NAS IPv4 Address
Destination Port	NAS:NAS Port
Device Custom String 5	Authentication Details:Authentication Type
Device Custom String 6	Authentication Details:Account Session Identifier
Destination User Privileges	Quarantine Information:Result

6273 Network Policy Server denied access to a user.

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	User: Account Name
Destination NT Domain	User: Account Domain
Destination User ID	User: Fully Qualified Account Name
Source User Name	Client Machine:Account Name
Source User ID	Client Machine:Fully Qualified Account Name
Source Address	Client Machine:Calling Station Identifier
Destination Address	NAS:NAS IPv4 Address
Destination Port	NAS:NAS Port
Device Custom String 1	Authentication Details:Proxy Policy Name
Device Custom String 3	RADIUS Client:Client IP Address
Device Custom String 4	Authentication Details:Reason
Device Custom String 5	Authentication Details:Authentication Type
Device Custom String 6	Authentication Details:Account Session Identifier

6274 Network Policy Server discarded the request for a user.

This event is supported by common security event mappings. There are no specific mappings.

6275 Network Policy Server discarded the accounting request for a user.

This event is supported by common security event mappings. There are no specific mappings.

6276 Network Policy Server quarantined a user.

This event is supported by common security event mappings. There are no specific mappings.

6277 Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.

This event is supported by common security event mappings. There are no specific mappings.

6278 Network Policy Server granted full access to a user because the host met the defined health policy.

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	User:Account Name
Destination NT Domain	User:Account Domain
Destination User ID	User:Fully Qualified Account Name
Source User Name	Client Machine:Account Name
Source User ID	Client Machine:Fully Qualified Account Name
Source Address	Client Machine:Calling Station Identifier
Device Custom String 1	Authentication Details:Proxy Policy Name
Device Custom String 3	RADIUS Client:Client IP Address
Destination Address	NAS:NAS IPv4 Address
Destination Port	NAS:NAS Port
Device Custom String 5	Authentication Details:Authentication Type
Device Custom String 6	Authentication Details:Account Session Identifier
Destination User Privileges	Quarantine Information:Result

6279 Network Policy Server locked the user account due to repeated failed authentication attempts.

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	User:Account Name
Destination NT Domain	User:Account Domain
Destination User ID	User:Fully Qualified Account Name

6280 Network Policy Server unlocked the user account.

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	User:Account Name
Destination NT Domain	User:Account Domain
Destination User ID	User:Fully Qualified Account Name

6409 BranchCache: A service connection point object could not be parsed.

Windows 2012 and 2012 R2 Only

This event is supported by common security event mappings. There are no specific mappings.

6410 Code integrity determined that a file does not meet the security requirements to load into a process.

Windows 2012 and 2012 R2 Only

HP ArcSight ESM Field	Device-Specific Field
File Name	File Name

8222 No fax devices were found

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	User Name
Device Custom String 3	Process ID

Complete Windows 2012/Windows 8 Event Descriptions

Category	Subcategory	ID	Message Summary
Account Logon	Credential Validation	4774	An account was mapped for logon.
	Credential Validation	4775	An account could not be mapped for logon.
	Credential Validation	4776	The domain controller attempted to validate the credentials for an account.
	Credential Validation	4777	The domain controller failed to validate the credentials for an account.
	Kerberos Authentication Service	4768	A Kerberos authentication ticket (TGT) was requested.
	Kerberos Authentication Service	4771	Kerberos pre-authentication failed.
	Kerberos Authentication Service	4772	A Kerberos authentication ticket request failed.
	Kerberos Service Ticket Operations	4769	A Kerberos service ticket was requested.
	Kerberos Service Ticket Operations	4770	A Kerberos service ticket was renewed.
Account Management	Application Group Management	4783	A basic application group was created.
		4784	A basic application group was changed.
		4785	A member was added to a basic application group.
		4786	A member was removed from a basic application group.
		4787	A non-member was added to a basic application group.
		4788	A non-member was removed from a basic application group.
		4789	A basic application group was deleted.
		4790	An LDAP query group was created.
	Computer Account Management	4742	A computer account was changed.
		4743	A computer account was deleted.
Account Management	Distribution Group Management	4744	A security-disabled local group was created.
		4745	A security-disabled local group was changed.
		4746	A member was added to a security-disabled local group.
		4747	A member was removed from a security-disabled local group.
		4748	A security-disabled local group was deleted.
		4749	A security-disabled global group was created.
		4750	A security-disabled global group was changed.
		4751	A member was added to a security-disabled global group.
		4752	A member was removed from a security-disabled global group.
		4753	A security-disabled global group was deleted.
		4759	A security-disabled universal group was created.
		4760	A security-disabled universal group was changed.
		4761	A member was added to a security-disabled universal group.
		4762	A member was removed from a security-disabled universal group.
		4763	A security-disabled universal group was deleted.

Category	Subcategory	ID	Message Summary
Account Management	Other Account Management Events	4782	The password hash an account was accessed.
		4793	The Password Policy Checking API was called.
		4797	An attempt was made to query the existence of a blank password for an account.
Account Management	Security Group Management	4727	A security-enabled global group was created.
		4728	A member was added to a security-enabled global group.
		4729	A member was removed from a security-enabled global group.
		4730	A security-enabled global group was deleted.
		4731	A security-enabled local group was created.
		4732	A member was added to a security-enabled local group.
		4733	A member was removed from a security-enabled local group.
		4734	A security-enabled local group was deleted.
		4735	A security-enabled local group was changed.
		4737	A security-enabled global group was changed.
		4754	A security-enabled universal group was created.
		4755	A security-enabled universal group was changed.
		4756	A member was added to a security-enabled universal group.
		4757	A member was removed from a security-enabled universal group.
Account Management	User Account Management	4758	A security-enabled universal group was deleted.
		4764	A group's type was changed.
		4720	A user account was created.
		4722	A user account was enabled.
		4723	An attempt was made to change an account's password.
		4724	An attempt was made to reset an account's password.
		4725	A user account was disabled.
		4726	A user account was deleted.
		4738	A user account was changed.
		4740	A user account was locked out.
		4765	SID History was added to an account.
		4766	An attempt to add SID History to an account failed.
		4767	A user account was unlocked.
		4780	The ACL was set on accounts which are members of administrators groups.
		4781	The name of an account was changed:
		4794	An attempt was made to set the Directory Services Restore Mode.
		5376	Credential Manager credentials were backed up.
		5377	Credential Manager credentials were restored from a backup.

Category	Subcategory	ID	Message Summary
Detailed Tracking	DPAPI Activity	4692	Backup of data protection master key was attempted.
		4693	Recovery of data protection master key was attempted.
		4694	Protection of auditable protected data was attempted.
		4695	Unprotection of auditable protected data was attempted.
	Process Creation	4688	A new process has been created.
		4696	A primary token was assigned to process.
	Process Termination	4689	A process has exited.
	RPC Events	5712	A Remote Procedure Call (RPC) was attempted.
DS Access	Detailed Directory Service Replication	4928	An Active Directory replica source naming context was established.
		4929	An Active Directory replica source naming context was removed.
		4930	An Active Directory replica source naming context was modified.
		4931	An Active Directory replica destination naming context was modified.
		4934	Attributes of an Active Directory object were replicated.
		4935	Replication failure begins.
		4936	Replication failure ends.
		4937	A lingering object was removed from a replica.
DS Access	Directory Service Access	4662	An operation was performed on an object.
	Directory Service Changes	5136	A directory service object was modified.
		5137	A directory service object was created.
		5138	A directory service object was undeleted.
		5139	A directory service object was moved.
		5141	A directory service object was deleted.
	Directory Service Replication	4932	Synchronization of a replica of an Active Directory naming context has begun.
		4933	Synchronization of a replica of an Active Directory naming context has ended.
Logon/Logoff	Account Lockout	4625	An account failed to logon
	IPsec Extended Mode	4978	During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
		4979	IPsec Main Mode and Extended Mode security associations were established.
		4980	
		4981	
		4982	
		4983	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.
		4984	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.

Category	Subcategory	ID	Message Summary
Logon/Logoff	IPsec Main Mode	4646	IKE DoS-prevention mode started.
		4650	An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.
		4651	An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.
	IPsec Main Mode	4652	An IPsec Main Mode negotiation failed.
		4653	An IPsec Main Mode negotiation failed.
		4655	An IPsec Main Mode security association ended.
		4976	During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
		5049	An IPsec Security Association was deleted.
		5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.
	IPsec Quick Mode	4654	An IPsec Quick Mode negotiation failed.
		4977	During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
		5451	An IPsec Quick Mode security association was established.
		5452	An IPsec Quick Mode security association ended.
Logon/Logoff	Logoff	4634	An account was logged off.
		4647	User initiated logoff.
	Logon	4624	An account was successfully logged on.
		4625	An account failed to log on.
		4626	User/Device claims information.
		4648	A logon was attempted using explicit credentials.
		4675	SIDs were filtered.
	Network Policy Server	6272	Network Policy Server granted access to a user.
		6273	Network Policy Server denied access to a user.
		6274	Network Policy Server discarded the request for a user.
		6275	Network Policy Server discarded the accounting request for a user.
		6276	Network Policy Server quarantined a user.
		6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
		6278	Network Policy Server granted full access to a user because the host met the defined health policy.
		6279	Network Policy Server locked the user account due to repeated failed authentication attempts.
		6280	Network Policy Server unlocked the user account.

Category	Subcategory	ID	Message Summary
Logon/Logoff	Other Logon/Logoff Events	4649	A replay attack was detected.
		4778	A session was reconnected to a Window Station.
		4779	A session was disconnected from a Window Station.
		4800	The workstation was locked.
		4801	The workstation was unlocked.
		4802	The screen saver was invoked.
		4803	The screen saver was dismissed.
	Other Logon/Logoff Events	5378	The requested credentials delegation was disallowed by policy.
		5632	A request was made to authenticate to a wireless network.
		5633	A request was made to authenticate to a wired network.
Object Access	Special Logon	4964	Special groups have been assigned to a new logon.
	Application Generated	4665	An attempt was made to create an application client context.
		4666	An application attempted an operation:
		4667	An application client context was deleted.
		4668	An application was initialized.
	Central Policy Staging	4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy
	Certification Services	4868	The certificate manager denied a pending certificate request.
		4869	Certificate Services received a resubmitted certificate request.
		4870	Certificate Services revoked a certificate.
		4871	Certificate Services received a request to publish the certificate revocation list (CRL).
		4872	Certificate Services published the certificate revocation list (CRL).
		4873	A certificate request extension changed.
		4874	One or more certificate request attributes changed.
		4875	Certificate Services received a request to shutdown.
		4876	Certificate Services backup started.
		4877	Certificate Services backup completed.
		4878	Certificate Services restore started.
		4879	Certificate Services restore completed.
		4880	Certificate Services started.
		4881	Certificate Services stopped.
		4882	The security permissions for Certificate Services changed.

Category	Subcategory	ID	Message Summary
Object Access	Certification Services	4883	Certificate Services retrieved an archived key.
		4884	Certificate Services imported a certificate into its database.
		4885	The audit filter for Certificate Services changed.
		4886	Certificate Services received a certificate request.
		4887	Certificate Services approved a certificate request and issued a certificate.
		4888	Certificate Services denied a certificate request.
		4889	Certificate Services set the status of a certificate request to pending.
		4890	The certificate manager settings for Certificate Services changed.
		4891	A configuration entry changed in Certificate Services.
		4892	A property of Certificate Services changed.
		4893	Certificate Services archived a key.
		4894	Certificate Services imported and archived a key.
	Certification Services	4895	Certificate Services published the CA certificate to Active Directory Domain Services.
		4896	One or more rows have been deleted from the certificate database.
		4897	Role separation enabled.
		4898	Certificate Services loaded a template.
Object Access	Detailed File Share	5145	A network share object was checked to see whether the client can be granted desired access.
	File Share	5140	A network share object was accessed.
		5142	A network share object was added.
		5143	A network share object was modified.
		5144	A network share object was deleted.
		5168	Spn check for SMB/SMB2 failed.
	File System	4664	An attempt was made to create a hard link.
		4985	The state of a transaction has changed.
		5051	A file was virtualized.
	Filtering Platform Connection	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
		5146	The Windows Filtering Platform has blocked a packet.
		5147	A more restrictive Windows Filtering Platform filter has blocked a packet.
		5150	The Windows Filtering Platform has blocked a packet.
		5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
		5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
		5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
		5156	The Windows Filtering Platform has allowed a connection.
		5157	The Windows Filtering Platform has blocked a connection.
		5158	The Windows Filtering Platform has permitted a bind to a local port.

Category	Subcategory	ID	Message Summary
		5159	The Windows Filtering Platform has blocked a bind to a local port.
Object Access	Filtering Platform Packet Drop	5152	The Windows Filtering Platform blocked a packet.
		5153	A more restrictive Windows Filtering Platform filter has blocked a packet.
Object Access	Handle Manipulation	4656	A handle to an object was requested.
		4658	The handle to an object was closed.
		4690	An attempt was made to duplicate a handle to an object.
Object Access	Other Object Access Events	4671	An application attempted to access a blocked ordinal through the TBS.
		4691	Indirect access to an object was requested.
		4698	A scheduled task was created.
		4699	A scheduled task was deleted.
		4700	A scheduled task was enabled.
		4701	A scheduled task was disabled.
		4702	A scheduled task was updated.
Object Access	Other Object Access Events	5148	The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.
		5149	The DoS attack has subsided and normal processing is being resumed.
		5888	An object in the COM+ Catalog was modified.
		5889	An object was deleted from the COM+ Catalog.
		5890	An object was added to the COM+ Catalog.
Object Access	Registry	4657	A registry value was modified.
		5039	A registry key was virtualized.
Object Access	Special	4659	A handle to an object was requested with intent to delete.
		4660	An object was deleted.
		4661	A handle to an object was requested.
		4663	An attempt was made to access an object.
Policy Change	Audit Policy Change	4715	The audit policy (SACL) on an object was changed.
		4719	System audit policy was changed.
		4817	Auditing settings on an object were changed.
		4902	The Per-user audit policy table was created.
		4904	An attempt was made to register a security event source.
		4905	An attempt was made to unregister a security event source.
		4906	The CrashOnAuditFail value has changed.
		4907	Auditing settings on object were changed.
		4908	Special Groups Logon table modified.
		4912	Per User Audit Policy was changed.

Category	Subcategory	ID	Message Summary
Policy Change	Authentication Policy Change	4713	Kerberos policy was changed.
		4716	Trusted domain information was modified.
		4717	System security access was granted to an account.
		4718	System security access was removed from an account.
		4739	Domain Policy was changed.
		4864	A namespace collision was detected.
		4865	A trusted forest information entry was added.
		4866	A trusted forest information entry was removed.
		4867	A trusted forest information entry was modified.
Policy Change	Authorization Policy Change	4704	A user right was assigned.
		4705	A user right was removed.
		4706	A new trust was created to a domain.
		4707	A trust to a domain was removed.
		4714	Encrypted data recovery policy was changed.
		4911	Resource attributes of the object were changed.
		4913	Central Access Policy on the object was changed.
Policy Change	Filtering Platform Policy Change	4709	IPsec Services was started.
		4710	IPsec Services was disabled.
Policy Change	Filtering Platform Policy Change	4711	May contain any one of the following: PASTore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer. PASTore Engine applied Active Directory storage IPsec policy on the computer. PASTore Engine applied local registry storage IPsec policy on the computer. PASTore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer. PASTore Engine failed to apply Active Directory storage IPsec policy on the computer. PASTore Engine failed to apply local registry storage IPsec policy on the computer. PASTore Engine failed to apply some rules of the active IPsec policy on the computer. PASTore Engine failed to load directory storage IPsec policy on the computer. PASTore Engine loaded directory storage IPsec policy on the computer. PASTore Engine failed to load local storage IPsec policy on the computer. PASTore Engine loaded local storage IPsec policy on the computer. PASTore Engine polled for changes to the active IPsec policy and detected no changes.

Category	Subcategory	ID	Message Summary
Policy Change	Filtering Platform Policy Change	4712	IPsec Services encountered a potentially serious failure.
		5040	A change has been made to IPsec settings. An Authentication Set was added.
		5041	A change has been made to IPsec settings. An Authentication Set was modified.
		5042	A change has been made to IPsec settings. An Authentication Set was deleted.
		5043	A change has been made to IPsec settings. A Connection Security Rule was added.
		5044	A change has been made to IPsec settings. A Connection Security Rule was modified.
		5045	A change has been made to IPsec settings. A Connection Security Rule was deleted.
		5046	A change has been made to IPsec settings. A Crypto Set was added.
		5047	A change has been made to IPsec settings. A Crypto Set was modified.
		5048	A change has been made to IPsec settings. A Crypto Set was deleted.
Policy Change	Filtering Platform Policy Change	5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started.
		5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started.
		5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started.
		5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.
		5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.
		5446	A Windows Filtering Platform callout has been changed.
Policy Change	Filtering Platform Policy Change	5448	A Windows Filtering Platform provider has been changed.
		5449	A Windows Filtering Platform provider context has been changed.
		5450	A Windows Filtering Platform sub-layer has been changed.
		5456	PAStore Engine applied Active Directory storage IPsec policy on the computer.
		5457	PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.
		5458	PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.
		5459	PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.
		5460	PAStore Engine applied local registry storage IPsec policy on the computer.
		5461	PAStore Engine failed to apply local registry storage IPsec policy on the computer.
		5462	PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.

Category	Subcategory	ID	Message Summary
		5463	PAStore Engine polled for changes to the active IPsec policy and detected no changes.
		5464	PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.
		5465	PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.
		5466	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.
Policy Change	Filtering Platform Policy Change	5467	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.
		5468	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.
		5471	PAStore Engine loaded local storage IPsec policy on the computer.
		5472	PAStore Engine failed to load local storage IPsec policy on the computer.
		5473	PAStore Engine loaded directory storage IPsec policy on the computer.
		5474	PAStore Engine failed to load directory storage IPsec policy on the computer.
		5477	PAStore Engine failed to add quick mode filter.

Category	Subcategory	ID	Message Summary
Policy Change	MPSSVC Rule-Level Policy Change	4944	The following policy was active when the Windows Firewall started.
		4945	A rule was listed when the Windows Firewall started.
		4946	A change has been made to Windows Firewall exception list. A rule was added.
		4947	A change has been made to Windows Firewall exception list. A rule was modified.
		4948	A change has been made to Windows Firewall exception list. A rule was deleted.
		4949	Windows Firewall settings were restored to the default values.
		4950	A Windows Firewall setting has changed.
		4951	A rule has been ignored because its major version number was not recognized by Windows Firewall.
		4952	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.
		4953	A rule has been ignored by Windows Firewall because it could not parse the rule.
		4954	Windows Firewall Group Policy settings have changed. The new settings have been applied.
		4956	Windows Firewall has changed the active profile.
		4957	Windows Firewall did not apply the following rule:
		4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer:
Policy Change	Other Policy Change Events	4819	Central Access Policies on the machine have been changed.
		4909	The local policy settings for the TBS were changed.
		4910	The group policy settings for the TBS were changed.
		5063	A cryptographic provider operation was attempted.
		5064	A cryptographic context operation was attempted.
		5065	A cryptographic context modification was attempted.
		5066	A cryptographic function operation was attempted.
		5067	A cryptographic function modification was attempted.
		5068	A cryptographic function provider operation was attempted.
		5069	A cryptographic function property operation was attempted.
		5070	A cryptographic function property modification was attempted.
		5447	A Windows Filtering Platform filter has been changed.
		6144	Security policy in the group policy objects has been applied successfully.
		6145	One or more errors occurred while processing security policy in the group policy objects.
Policy Change	Subcategory (special)	4670	Permissions on an object were changed.
Privilege Use	Sensitive Privilege Use / Non Sensitive Privilege Use	4672	Special privileges assigned to new logon.
		4673	A privileged service was called.
		4674	An operation was attempted on a privileged object.

Category	Subcategory	ID	Message Summary
System	IPsec Driver	4960	IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.
		4961	IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.
		4962	IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.
System	IPsec Driver	4963	IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.
		4965	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.
		5478	IPsec Services has started successfully.
		5479	IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
		5480	IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
		5483	IPsec Services failed to initialize RPC server. IPsec Services could not be started.
		5484	IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
System	Other System Events	5485	IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
		5024	The Windows Firewall Service has started successfully.
		5025	The Windows Firewall Service has been stopped.
		5027	The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.

Category	Subcategory	ID	Message Summary
System	Other System Events	5028	The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.
		5029	The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.
		5030	The Windows Firewall Service failed to start.
		5032	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.
		5033	The Windows Firewall Driver has started successfully.
		5034	The Windows Firewall Driver has been stopped.
		5035	The Windows Firewall Driver failed to start.
		5037	The Windows Firewall Driver detected critical runtime error. Terminating.
		5058	Key file operation.
		5059	Key migration operation.
		6400	BranchCache: Received an incorrectly formatted response while discovering availability of content.
		6401	BranchCache: Received invalid data from a peer. Data discarded.
		6402	BranchCache: The message to the hosted cache offering it data is incorrectly formatted.
System	Other System Events	6403	BranchCache: The hosted cache sent an incorrectly formatted response to the client.
		6404	BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.
		6405	BranchCache: %2 instance(s) of event id %1 occurred.
		6406	%1 registered to Windows Firewall to control filtering for the following: %2
		6407	1%
		6408	Registered product %1 failed and Windows Firewall is now controlling the filtering for %2
System	Security State Change	4608	Windows is starting up.
		4609	Windows is shutting down.
		4616	The system time was changed.
		4621	Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.
System	Security System Extension	4610	An authentication package has been loaded by the Local Security Authority.
		4611	This logon process will be trusted to submit logon requests.
		4614	A notification package has been loaded by the Security Account Manager.
		4622	A security package has been loaded by the Local Security Authority.
		4697	A service was installed in the system.

Category	Subcategory	ID	Message Summary
System	System Integrity	4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
		4615	Invalid use of LPC port.
		4618	A monitored security event pattern has occurred.
		4816	RPC detected an integrity violation while decrypting an incoming message.
		5038	Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
		5056	A cryptographic self test was performed.
		5057	A cryptographic primitive operation failed.
		5060	Verification operation failed.
		5061	Cryptographic operation.
		5062	A kernel-mode cryptographic self test was performed.
		6281	Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error