



Micro Focus Security ArcSight Connectors

SmartConnector for Microsoft Windows Event Log – Native

Windows Security Event Mappings

Document Release Date: May 16, 2018

Software Release Date:

Legal Notices

Warranty

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Except as specifically indicated otherwise, a valid license from Micro Focus is 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.

Copyright Notice

© Copyright 2008-2018 Micro Focus or one of its affiliates.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://community.softwaregrp.com/t5/ArcSight-Product-Documents/ct-p/productdocs

Contents

About This Book	16
Windows Common Security Mappings	18
Specific Windows Security Event Mappings	21
1100	21
1101	21
1102	21
1104	21
1105	22
4608	22
4609	22
4610	22
4611	23
4612	23
4614	23
4615	24
4616	24
4618	25
4621	25
4622	25
4624	26
4625	27
4626	28
4627	29
4634	30
4646	30
4647	31
4648	31

4649	32
4650	32
4651	32
4652	33
4653	33
4654	33
4655	34
4656	34
4657	35
4658	35
4659	36
4660	36
4661	37
4662	37
4663	38
4664	38
4665	38
4666	39
4667	39
4668	39
4670	39
4671	40
4672	40
4673	40
4674	41
4675	41
4688	41
4689	42
4690	43
4691	43
4692	43
4693	44

4694	44
4695	44
4696	45
4697	45
4698	46
4699	46
4700	46
4701	47
4702	47
4703	47
4704	48
4705	48
4706	49
4707	49
4709	49
4710	49
4711	50
4712	50
4713	50
4714	50
4715	51
4716	51
4717	52
4718	52
4719	53
4720	53
4722	53
4723	54
4724	54
4725	55
4726	55
4727	55

4728	56
4729	56
4730	57
4731	57
4732	58
4733	58
4734	59
4735	59
4737	60
4738	60
4739	61
4740	61
4741	62
4742	62
4743	63
4744	63
4745	64
4746	64
4747	65
4748	65
4749	66
4750	66
4751	67
4752	67
4753	68
4754	68
4755	69
4756	69
4757	70
4758	70
4759	71
4760	71

4761	72
4762	72
4763	73
4764	73
4765	74
4766	74
4767	75
4768	75
4769	76
4770	76
4771	77
4772	77
4773	78
4774	78
4775	78
4776	78
4777	79
4778	79
4779	80
4780	80
4781	81
4782	81
4783	82
4784	82
4785	83
4786	83
4787	84
4788	84
4789	85
4790	85
4791	86
4792	86

4793	87
4794	87
4797	87
4798	88
4799	88
4800	89
4801	89
4802	89
4803	90
4816	90
4817	90
4818	91
4819	91
4820	92
4821	92
4822	93
4823	93
4824	94
4826	94
4864	95
4865	95
4866	96
4867	96
4868	96
4869	97
4870	97
4871	97
4872	98
4873	98
4874	98
4875	99
4876	99

4877	99
4878	99
4879	100
4880	100
4881	100
4882	100
4883	100
4884	101
4885	101
4886	101
4887	102
4888	102
4889	102
4890	102
4891	103
4892	103
4893	103
4894	103
4895	104
4896	104
4897	104
4898	104
4899	104
4900	105
4902	105
4904	105
4905	106
4906	106
4907	106
4908	107
4909	107
4910	107

4911	107
4912	108
4913	108
4928	109
4929	109
4930	109
4931	109
4932	110
4933	110
4934	110
4935	110
4936	110
4937	110
4944	111
4945	111
4946	111
4947	111
4948	111
4949	112
4950	112
4951	112
4952	112
4953	112
4954	113
4956	113
4957	113
4958	113
4960	114
4961	114
4962	114
4963	114
4964	115

4965	115
4976	115
4977	116
4978	116
4979	116
4980	116
4981	117
4982	117
4983	117
4984	118
4985	118
5024	118
5025	119
5027	119
5028	119
5029	119
5030	120
5031	120
5032	120
5033	120
5034	120
5035	121
5037	121
5038	121
5039	121
5040	122
5041	122
5042	122
5043	122
5044	122
5045	123
5046	123

5047	123
5048	123
5049	123
5050	124
5051	124
5056	124
5057	125
5058	125
5059	125
5060	126
5061	126
5062	126
5063	127
5064	127
5065	127
5066	128
5067	128
5068	128
5069	129
5070	129
5071	129
5120	130
5121	130
5122	130
5123	130
5124	131
5125	131
5126	131
5127	131
5136	131
5137	132
5138	132

5139	133
5140	133
5141	134
5142	134
5143	134
5144	135
5145	135
5146	136
5147	136
5152	136
5153	137
5154	137
5155	137
5156	138
5157	138
5158	138
5159	139
5168	139
5376	140
5377	140
5378	140
5440	141
5441	141
5442	141
5443	141
5444	142
5446	142
5447	142
5448	142
5449	142
5450	143
5451	143

5452	143
5453	143
5456	144
5457	144
5458	144
5459	144
5460	144
5461	145
5462	145
5463	145
5464	145
5465	145
5466	146
5467	146
5468	146
5471	146
5472	147
5473	147
5474	147
5477	147
5478	147
5479	148
5480	148
5483	148
5484	148
5632	149
5633	149
5712	149
5888	150
5889	150
5890	150
6144	151

6145	151
6272	151
6273	152
6274	152
6275	152
6276	153
6277	153
6278	153
6279	154
6280	154
6281	154
6409	154
6410	155
6416	155
8191	155
Windows Event Log Event Descriptions by Category	156
Send Documentation Feedback	180

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 and the SmartConnector for Microsoft Windows Event Log – Native 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 these Microsoft Windows versions:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016

Note that Security events are not audited by default. Be sure to specify the type of security events to be audited (see "Enable Microsoft Windows Event Log Audit Policies" in the configuration guide for the SmartConnector for Microsoft Windows Event Log -- Native).

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)

Revision History

Date	Description
05/16/2018	Updated mappings for Event 4625
03/15/2017	Updated mappings for Event 4624. Removed Windows Server 2003 due to end of support for that product.
11/30/2016	Added support for Windows Server 2016.
10/31/2016	Added mappings to Event 4738.
05/16/2016	Added mappings to Event 5156.
02/15/2016	Added Windows 10 support. Added fields to security event 4648 mappings.
02/16/2015	First generally available edition of this guide.

Windows Common Security Mappings

The following security event mappings generally apply to all Windows Server 2008, Windows Server 2012, Windows Server 2016, and Windows 10 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

Windows Security Event Mappings

Windows Common Security Mappings

HP ArcSight ESM Field	Device-Specific Field
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
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)

Windows Security Event Mappings

Windows Common Security Mappings

HP ArcSight ESM Field	Device-Specific Field
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 Windows Security Event Mappings

1100

HP ArcSight ESM Field	Device-Specific Field
Name	'The event logging service has shut down.'

1101

HP ArcSight ESM Field	Device-Specific Field
Name	'Audit events have been dropped by the transport. The real time backup file was corrupt due to improper shutdown.'
Device Custom Number 3	Reason

1102

HP ArcSight ESM Field	Device-Specific Field
Name	'The audit log was cleared.'
Destination NT Domain	SubjectDomainName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination User ID	SubjectLogonId

1104

HP ArcSight ESM Field	Device-Specific Field
Name	'The security log is now full.'

1105

HP ArcSight ESM Field	Device-Specific Field
Name	'Event log automatic backup.'
File Type	Channel
File Name	BackupPath

4608

HP ArcSight ESM Field	Device-Specific Field
Name	'Windows is starting up. This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.'

4609

HP ArcSight ESM Field	Device-Specific Field
Name	'Windows is shutting down. All logon sessions will be terminated by this shut down.'

4610

HP ArcSight ESM Field	Device-Specific Field
Name	'An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts.'
Device Custom String 5	AuthenticationPackageName

4611

HP ArcSight ESM Field	Device-Specific Field
Name	'A trusted logon process has been registered with the Local Security Authority. This logon process will be trusted to submit logon requests.'
Destination Process Name	LogonProcessName
Source Process Name	LogonProcessName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4612

HP ArcSight ESM Field	Device-Specific Field
Name	'Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.'
Device Custom Number 3	AuditsDiscarded
Message	'This event is generated when audit queues are filled and events must be discarded. This most commonly occurs when security events are being generated faster than they are being written to disk, or when the auditing system loses connectivity to the event log, such as when the event log service is stopped.'

4614

HP ArcSight ESM Field	Device-Specific Field
Name	'A notification package has been loaded by the Security Account Manager. This package will be notified of any account or password changes.'
Device Custom String 5	'NotificationPackageName'

4615

HP ArcSight ESM Field	Device-Specific Field
Name	'Invalid use of LPC port.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Message	'Windows Local Security Authority (LSA) communicates with the Windows kernel using Local Procedure Call (LPC) ports. If you see this event, an application has inadvertently or intentionally accessed this port which is reserved exclusively for LSA's use. The application (process) should be investigated to ensure that it is not attempting to tamper with this communications channel.'

4616

HP ArcSight ESM Field	Device-Specific Field
Name	'The system time was changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Device Custom Date 1	Both (PreviousDate, PreviousTime)
Device Custom Date 2	Both (NewDate, NewTime)
Device Custom String 3	ProcessId
Destination process Name	ProcessName
Message	'This event is generated when the system time is changed. It is normal for the Windows Time Service, which runs with System privilege, to change the system time on a regular basis. Other system time changes may be indicative of attempts to tamper with the computer.'

4618

HP ArcSight ESM Field	Device-Specific Field
Name	'A monitored security event pattern has occurred.'
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetUserDomain
Device NT Domain	TargetUserDomain
Message	'This event is generated when Windows is configured to generate alerts in accordance with the Common Criteria Security Audit Analysis requirements (FAU_SAA) and an auditable event pattern occurs.'

4621

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'
Device Custom Number 2	CrashOnAuditFail value.
Message	'This event is logged after a system reboots following CarshOnAuditFail.'

4622

HP ArcSight ESM Field	Device-Specific Field
Name	'A security package has been loaded by the Local Security Authority.'
File Path	SecurityPackageName
Device Custom String 5	SecurityPackageName

4624

HP ArcSight ESM Field	Device-Specific Field
Name	'An account was successfully logged on.'
Additional data	TargetOutboundUserName
Additional data	TargetOutboundDomainName
Device NT Domain	SubjectDomainName
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Destination Process Name	ProcessName
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId
Device Custom String 1	ImpersonationLevel
Device Custom String 3	ProcessId
Device Custom String 4	RestrictedAdminMode
Device Process Name	LogonProcessName
Device Custom String 6	LogonGuid
Source Host Name	One of (IpAddress, 'localhost')
Source Port	IpPort
Device Custom String 5	AuthenticationPackageName
Device Custom Number 1	LogonType
File Type	VirtualAccount
File ID	TargetLinkedLogonId
File Name	ElevatedToken
Message	'This event is generated when a logon session is created. It is generated on the computer that was accessed.'

4625

HP ArcSight ESM Field	Device-Specific Field
Name	'An account failed to log on.'
Device NT Domain	SubjectDomainName
Source Address	IpAddress
Destination Process Name	ProcessName
Destination NT Domain	TargetDomainName
Device Custom String 1	SubStatus
Device Custom String 3	ProcessId
Reason	FailureReason
Device Process Name	LogonProcessName
Destination User ID	''
Source Host Name	WorkstationName
Source Port	IpPort
Source Process Name	ProcessId
Device Custom String 4	FailureReason
Device Custom String 5	AuthenticationPackageName

HP ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	LogonType
Destination UserName	TargetUserName
Message	<p>'This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request.</p> <ul style="list-style-type: none"> - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.'

4626

HP ArcSight ESM Field	Device-Specific Field
Name	'User/Device claims information.'
Device NT Domain	SubjectDomainName
Destination User Name	TargetUserName
Destination User ID	TargetLogonId

HP ArcSight ESM Field	Device-Specific Field
Destination NT Domain	TargetDomainName
Device Custom Number 1	LogonType
Message	<p>'The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. This event is generated when the Audit User/Device claims subcategory is configured and the user's logon token contains user/device claims information. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.'</p>

4627

HP ArcSight ESM Field	Device-Specific Field
Name	'Group membership information.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId
Device Custom Number 1	LogonType
Device Custom Number 2	EventIdx

HP ArcSight ESM Field	Device-Specific Field
Device Custom Number 3	EventCountTotal
Device Custom String 1	GroupMembership
Message	‘This event is generated when the Audit Group Membership subcategory is configured. The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network). The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on. The Logon ID field can be used to correlate this event with the corresponding user logon event as well as to any other security audit events generated during this logon session.’

4634

HP ArcSight ESM Field	Device-Specific Field
Name	‘An account was logged off.’
Destination User ID	TargetLogonId
Device Custom Number 1	LogonType
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName
Message	‘This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.’

4646

HP ArcSight ESM Field	Device-Specific Field
Name	‘IKE DoS-prevention mode started.’

4647

HP ArcSight ESM Field	Device-Specific Field
Name	'User initiated logoff.'
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName
Message	'This event is generated when a logoff is initiated but the token reference count is not zero and the logon session cannot be destroyed. No further user-initiated activity can occur. This event can be interpreted as a logoff event.'

4648

HP ArcSight ESM Field	Device-Specific Field
Name	'A logon was attempted using explicit credentials.'
Device NT Domain	SubjectDomainName
Source Address	IpAddress
Destination Process Name	ProcessName
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Device Custom String 6	TargetLogonGuid (Logon GUID)
Device Custom String 3	ProcessId (Process ID)
Source Port	IpPort
Destination User ID	SubjectLogonId
Source User Name	One of (SubjectUserName, SubjectUserSid)
Message	'This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.'
Device Custom String 5	TargetServerName

4649

HP ArcSight ESM Field	Device-Specific Field
Name	'A replay attack was detected.'
Source Host Name	WorkstationName
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Device Custom String 5	AuthenticationPackage
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Message	'This event indicates that a Kerberos replay attack was detected- a request was received twice with identical information. This condition could be caused by network misconfiguration.'

4650

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.'

4651

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.'
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort

4652

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Main Mode negotiation failed.'
Device Custom String 4	FailureReason
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort
Message	FailureReason

4653

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Main Mode negotiation failed.'
Device Custom String 4	FailureReason
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort
Message	FailureReason

4654

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Quick Mode negotiation failed.'
Device Custom String 4	FailureReason
Source Address	LocalAddress
Source Port	LocalPort

HP ArcSight ESM Field	Device-Specific Field
Destination Address	RemoteAddress
Destination Port	RemotePort
Message	FailureReason

4655

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Main Mode security association ended.'
Source Address	LocalAddress

4656

HP ArcSight ESM Field	Device-Specific Field
Name	'A handle to an object was requested.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom String 3	ProcessId
Device Custom String 1	AccessList
Device NT Domain	SubjectDomainName
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Privileges	PrivilegeList
File ID	HandleId
File Name	ObjectName
File Type	ObjectType

4657

HP ArcSight ESM Field	Device-Specific Field
Name	'A registry value was modified.'
Device Custom String 6	ObjectValueName
Device Action	OperationType
Old File Type	OldValueType
Device Custom String 4	OldValue
File Type	NewValueType
File ID	HandleId
File Name	ObjectName
Device Custom String 5	NewValue
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4658

HP ArcSight ESM Field	Device-Specific Field
Name	'The handle to an object was closed.'
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File ID	HandleId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4659

HP ArcSight ESM Field	Device-Specific Field
Name	'A handle to an object was requested with intent to delete.'
Device Custom String 1	AccessList
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
File Type	ObjectType
File ID	HandleId
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4660

HP ArcSight ESM Field	Device-Specific Field
Name	'An object was detected.'
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File ID	HandleId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4661

HP ArcSight ESM Field	Device-Specific Field
Name	'A handle to an object was requested.'
Device Custom String 1	AccessList
Destination User Privileges	PrivilegeList
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File ID	HandleId
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4662

HP ArcSight ESM Field	Device-Specific Field
Name	'An operation was performed on an object.'
Device Custom String 5	ObjectType
Destination User ID	SubjectLogonId
Device Custom String 1	One of (AccessList, AccessMask)
File Type	ObjectType
File ID	HandleId
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4663

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to access an object.'
Device Custom String 1	AccessList
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File ID	HandleId
File Name	ObjectName
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Name	One of (SubjectUserName, SubjectUserSid)

4664

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to create a hard link.'
Destination User ID	SubjectLogonId
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4665

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to create an application client context.'
Source Host Name	ClientName
Source NT Domain	ClientDomain

4666

HP ArcSight ESM Field	Device-Specific Field
Name	'An application attempted an operation.'
File Name	ObjectName

4667

HP ArcSight ESM Field	Device-Specific Field
Name	'An application client context was deleted.'
Source Host Name	ClientName
Source NT Domain	ClientDomain

4668

HP ArcSight ESM Field	Device-Specific Field
Name	'An application was initialized.'
Source Host Name	ClientName
Source NT Domain	ClientDomain

4670

HP ArcSight ESM Field	Device-Specific Field
Name	'Permissions on an object were changed.'
Device Custom String 4	OldSd
Device Custom String 5	NewSd
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
File Type	ObjectType
File ID	HandleId

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
File Name	ObjectName

4671

HP ArcSight ESM Field	Device-Specific Field
Name	'An application attempted to access a blocked ordinal through the TBS.'
Destination User ID	CallerLogonId
Destination User Name	One of (CallerUserName, CallerUserSid)
Destination NT Domain	CallerDomainName
Device NT Domain	CallerDomainName

4672

HP ArcSight ESM Field	Device-Specific Field
Name	'Special privileges assigned to new logon.'
Destination User privileges	PrivilegeList
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4673

HP ArcSight ESM Field	Device-Specific Field
Name	'A privileged service was called.'
Destination User ID	SubjectLogonId

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4674

HP ArcSight ESM Field	Device-Specific Field
Name	'An operation was attempted on a privileged object.'
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList
Device Custom String 3	ProcessId
File ID	HandleId

4675

HP ArcSight ESM Field	Device-Specific Field
Name	'SIDs were filtered.'

4688

HP ArcSight ESM Field	Device-Specific Field
Name	'A new process has been created.'
Destination User Name	One of (SubjectUserName, SubjectUserSid, TargetUserName, TargetUserSid)

Windows Security Event Mappings

Specific Windows Security Event Mappings

HP ArcSight ESM Field	Device-Specific Field
Destination NT Domain	One of (SubjectDomainName, desinationNtDomain)
Destination User ID	One of (SubjectLogonId, TargetLogonId)
Device Custom String 1	MandatoryLabel
Device Custom String 3	NewProcessId
Device Custom String 6	TokenElevationType
Device Custom String 5	ProcessId
Device Custom String 4	CommandLine
Destination Process Name	NewProcessName
Device NT Domain	SubjectDomainName
File Path	ParentProcessName
Message	'Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.Type 1 is a full token with no privileges removed or groups disabled. Type 2 is an elevated token with no privileges removed or groups disabled.Type 3 is a limited token with administrative privileges removed and administrative groups disabled.'

4689

HP ArcSight ESM Field	Device-Specific Field
Name	'A process has exited.'
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Device Custom String 4	Status
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4690

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to duplicate a handle to an object.'
Old File ID	SourceHandleId
Device Custom String 5	SourceProcessId
File ID	TargetHandleId
Device Custom String 3	TargetProcessId
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4691

HP ArcSight ESM Field	Device-Specific Field
Name	'Indirect access to an object was requested.'
Destination User ID	SubjectLogonId
Device Custom String 1	AccessMask
File Type	ObjectType
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4692

HP ArcSight ESM Field	Device-Specific Field
Name	'Backup of data protection master key was attempted.'
Destination User ID	SubjectLogonId

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4693

HP ArcSight ESM Field	Device-Specific Field
Name	'Recovery of data protection master key was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4694

HP ArcSight ESM Field	Device-Specific Field
Name	'Protection of auditable protected data was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4695

HP ArcSight ESM Field	Device-Specific Field
Name	'Unprotection of auditable protected data was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4696

HP ArcSight ESM Field	Device-Specific Field
Name	'A primary token was assigned to process.'
Device Custom String 3	TargetProcessId
Destination Process Name	TargetProcessName
Device Custom String 5	ProcessId
Source Process Name	ProcessName
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId
Device NT Domain	SubjectDomainName

4697

HP ArcSight ESM Field	Device-Specific Field
Name	'A service was installed in the system.'
File Path	ServiceFileName
File Type	ServiceType
Device Custom String 5	ServiceStartType
Device Custom String 6	ServiceAccount
Destination User ID	SubjectLogonId
Destination Service Name	ServiceName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4698

HP ArcSight ESM Field	Device-Specific Field
Name	'A scheduled task was created.'
Device Custom String 6	TaskName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4699

HP ArcSight ESM Field	Device-Specific Field
Name	'A scheduled task was deleted.'
Device Custom String 6	TaskName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4700

HP ArcSight ESM Field	Device-Specific Field
Name	'A scheduled task was enabled.'
Device Custom String 6	TaskName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4701

HP ArcSight ESM Field	Device-Specific Field
Name	'A scheduled task was disabled.'
Device Custom String 6	TaskName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4702

HP ArcSight ESM Field	Device-Specific Field
Name	'A scheduled task was updated.'
Device Custom String 6	TaskName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4703

HP ArcSight ESM Field	Device-Specific Field
Name	'A user right was adjusted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId

HP ArcSight ESM Field	Device-Specific Field
Destination Process Name	ProcessName
Device Custom String 3	ProcessId
Device Custom String 1	EnabledPrivilegeList
Device Custom String 4	DisabledPrivilegeList
Message	'A user right was adjusted.'

4704

HP ArcSight ESM Field	Device-Specific Field
Name	'A user right was assigned.'
Source User Name	One of (SubjectUserSid, SubjectUserName)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetSid
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4705

HP ArcSight ESM Field	Device-Specific Field
Name	'A user right was removed.'
Source User Name	One of (SubjectUserSid, SubjectUserName)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetSid
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4706

HP ArcSight ESM Field	Device-Specific Field
Name	'A new trust was created to a domain.'
Device Custom String 6	One of (DomainName, DomainSid)
Device Custom String 5	TdoType (Trust Type)
Device Custom String 3	TdoDirection (Trust Direction)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4707

HP ArcSight ESM Field	Device-Specific Field
Name	'A trust to a domain was removed.'
Device Custom String 6	One of (DomainName, DomainSid)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4709

HP ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services was started.'

4710

HP ArcSight ESM Field	Device-Specific Field
Name	'The IPsec Policy Agent service was disabled.'

4711

HP ArcSight ESM Field	Device-Specific Field
Name	'PStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.'

4712

HP ArcSight ESM Field	Device-Specific Field
Name	'IPsec Policy Agent encountered a potentially serious failure.'

4713

HP ArcSight ESM Field	Device-Specific Field
Name	'Kerberos policy was changed.'
Message	All of ((KerberosPolicyChange, "", "(—" means no changes, otherwise each change is shown as: (Parameter Name): (new value) (old value))
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4714

HP ArcSight ESM Field	Device-Specific Field
Name	'Data Recovery Agent group policy for Encrypting File System (EFS) has changed. The new changes have been applied.'
Message	All of (EfsPolicyChange, "", "Changes Made('-' means no changes, otherwise each change is shown as: (Parameter Name): (new value) (old value))")

HP ArcSight ESM Field	Device-Specific Field
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4715

HP ArcSight ESM Field	Device-Specific Field
Name	'The audit policy (SACL) on an object was changed.'
Device Custom String 6	NewSd
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4716

HP ArcSight ESM Field	Device-Specific Field
Name	'Trusted domain information was modified.'
Device Custom String 6	One of (DomainName, DomainSid)
Device Custom String 5	TdoType (Trust Type)
Device Custom String 3	TdoDirection (Trust Direction)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4717

HP ArcSight ESM Field	Device-Specific Field
Name	'System security access was granted to an account.'
Source User ID	SubjectLogonId
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Destination User Name	TargetSid
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	AccessGranted

4718

HP ArcSight ESM Field	Device-Specific Field
Name	'System security access was removed from an account.'
Source User ID	SubjectLogonId
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Destination User Name	TargetSid
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	AccessRemoved

4719

HP ArcSight ESM Field	Device-Specific Field
Name	'System audit policy was changed.'
Device Custom String 5	SubcategoryId
Device Custom String 6	CategoryId
Device Action	AuditPolicyChanges
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4720

HP ArcSight ESM Field	Device-Specific Field
Name	'A user account was created.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4722

HP ArcSight ESM Field	Device-Specific Field
Name	'A user account was enabled.'
Source User Name	One of (SubjectUserName, SubjectUserSid)

HP ArcSight ESM Field	Device-Specific Field
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

4723

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to change an account's password.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4724

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to reset an account's password.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

4725

HP ArcSight ESM Field	Device-Specific Field
Name	'A user account was disabled.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

4726

HP ArcSight ESM Field	Device-Specific Field
Name	'A user account was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4727

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled global group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)

HP ArcSight ESM Field	Device-Specific Field
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	SubjectDomainName
Destination User Privilege	PrivilegeList

4728

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-enabled global group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4729

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-enabled global group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName

HP ArcSight ESM Field	Device-Specific Field
Source User ID	SubjectLogonId
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4730

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled global group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4731

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled local group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)

HP ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4732

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-enabled local group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4733

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-enabled local group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	MemberSid
Destination NT Domain	MemberSid

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4734

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled local group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4735

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled local group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom String 6	Both (TargetDomainName, TargetUserName)

HP ArcSight ESM Field	Device-Specific Field
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4737

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled global group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4738

HP ArcSight ESM Field	Device-Specific Field
Name	'A user account was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device Custom String 4	OldUacValue (Old User Account Control Value)
Device Custom String 5	NewUacValue (New User Account Control Value)

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	UserAccountControl (Change in User Account Control)
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4739

HP ArcSight ESM Field	Device-Specific Field
Name	'Domain Policy was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination NT Domain	DomainName
Destination User Name	''
Destination User ID	''
Message	DomainPolicyChanged
Device Custom String 6	Changed Attributes
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4740

HP ArcSight ESM Field	Device-Specific Field
Name	'A user account was locked out.'
Destination User Name	TargetUserName
Source Host Name	TargetDomainName
Destination NT Domain	TargetSid
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

4741

HP ArcSight ESM Field	Device-Specific Field
Name	'A computer account was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4742

HP ArcSight ESM Field	Device-Specific Field
Name	'A computer account was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	' '
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4743

HP ArcSight ESM Field	Device-Specific Field
Name	'A computer account was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4744

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled local group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4745

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled local group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4746

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-disabled local group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User ID	MemberName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4747

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-disabled local group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4748

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled local group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4749

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled global group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4750

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled global group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4751

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-disabled global group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (MemberSid, MemberName)
Destination NT Domain	MemberSid
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4752

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-disabled global group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4753

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled global group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4754

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled universal group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4755

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled universal group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4756

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-enabled universal group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4757

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-enabled universal group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4758

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled universal group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4759

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled universal group was created.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4760

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled universal group was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4761

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a security-disabled universal group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4762

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a security-disabled universal group.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	MemberName
Destination User Name	MemberSid
Destination NT Domain	MemberSid
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4763

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-disabled universal group was deleted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4764

HP ArcSight ESM Field	Device-Specific Field
Name	'A group's type was changed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Device Custom String 5	GroupTypeChange
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4765

HP ArcSight ESM Field	Device-Specific Field
Name	'SID History was added to an account.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	SourceUserName
Destination User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4766

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt to add SID History to an account failed.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Device Custom String 6	SourceUserName
Destination User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4767

HP ArcSight ESM Field	Device-Specific Field
Name	'A user account was unlocked.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

4768

HP ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos authentication ticket (TGT) was requested.'
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom String 3	IpAddress (Client Address)
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Device Custom String 4	Status
Device Custom String 5	PreAuthType
Source Port	IpPort
Destination Service Name	ServiceName
Message	'Certificate information is only provided if a certificate was used for pre-authentication.Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.'

4769

HP ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos service ticket was requested.'
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom String 3	IpAddress (Client Address)
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination Service Name	ServiceName
Device Custom String 6	LogonGuid
Source Port	IpPort
Device Custom String 4	Status
Message	'This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.'

4770

HP ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos service ticket was renewed.'
Device Custom String 3	IpAddress (Client Address)
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName

HP ArcSight ESM Field	Device-Specific Field
Destination Service Name	ServiceName
Source Port	IpPort
Message	'Ticket options and encryption types are defined in RFC 4120.'

4771

HP ArcSight ESM Field	Device-Specific Field
Name	'Kerberos pre-authentication failed.'
Device Custom String 3	IpAddress (Client Address)
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Destination User Name	TargetUserName
Destination NT Domain	TargetSid
Destination Service Name	ServiceName
Reason	Status
Source Port	IpPort
Device Custom String 4	Status
Message	'Certificate information is only provided if a certificate was used for pre-authentication.Pre-authentication types, ticket options and failure codes are defined in RFC 4120.If the ticket was malformed or damaged during transit and could not be decrypted, then many fields in this event might not be present.'

4772

HP ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos authentication ticket request failed.'
Device Custom String 3	IpAddress (Client Address)
Source Port	IpPort
Destination Service Name	ServiceName
Device Custom String 4	FailureCode
Message	'Ticket options and failure codes are defined in RFC 4120.'

4773

HP ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos service ticket request failed.'
Device Custom String 3	IpAddress (Client Address)
Source Port	IpPort
Destination Service Name	ServiceName
Device Custom String 4	FailureCode
Message	'Ticket options and failure codes are defined in RFC 4120.'

4774

HP ArcSight ESM Field	Device-Specific Field
Name	'An account was mapped for logon.'
Destination User Name	MappedName
Device Custom String 5	One of (MappedName, MappingBy)

4775

HP ArcSight ESM Field	Device-Specific Field
Name	'An account could not be mapped for logon.'
Destination User Name	MappingBy
Device Custom String 5	ClientUserName

4776

HP ArcSight ESM Field	Device-Specific Field
Name	'The domain controller attempted to validate the credentials for an account.'
Destination User Name	TargetUserName

HP ArcSight ESM Field	Device-Specific Field
Reason	Status
Source Host Name	Workstation
Device Custom String 4	Status
Device Custom String 5	PackageName

4777

HP ArcSight ESM Field	Device-Specific Field
Name	'The domain controller failed to validate the credentials for an account.'
Destination User Name	TargetUserName
Source Host Name	Workstation
Device Custom String 4	Status
Device Custom String 5	ClientUserName

4778

HP ArcSight ESM Field	Device-Specific Field
Name	'A session was reconnected to a Window Station.'
Device Custom String 6	SessionName
Source Host Name	ClientName
Source Address	ClientAddress
Destination User ID	LogonID
Destination User Name	AccountName
Destination NT Domain	AccountDomain
Device NT Domain	Account Domain
Message	'This event is generated when a user reconnects to an existing Terminal Services session, or when a user switches to an existing desktop using Fast User Switching.'

4779

HP ArcSight ESM Field	Device-Specific Field
Name	'A session was disconnected from a Window Station.'
Device Custom String 6	SessionName
Source Host Name	ClientName
Source Address	ClientAddress
Destination User ID	LogonID
Destination User Name	AccountName
Destination NT Domain	AccountDomain
Device NT Domain	Account Domain
Message	'This event is generated when a user disconnects from an existing TerminalServices session, or when a user switches away from an existing desktop using Fast User Switching.'

4780

HP ArcSight ESM Field	Device-Specific Field
Name	'The ACL was set on accounts which are members of administrators group.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId

HP ArcSight ESM Field	Device-Specific Field
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList
Message	'Every hour, the Windows domain controller that holds the primary domain controller (PDC) Flexible Single Master Operation (FSMO) role compares the ACL on all security principal accounts (users, groups, and machine accounts) present for its domain in Active Directory and that are in administrative groups against the ACL on the AdminSDHolder object. If the ACL on the principal account differs from the ACL on the AdminSDHolder object, then the ACL on the principal account is reset to match the ACL on the AdminSDHolder object and this event is generated.'

4781

HP ArcSight ESM Field	Device-Specific Field
Name	'The name of an account was changed.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	OldTargetUserName
Device Custom String 6	NewTargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4782

HP ArcSight ESM Field	Device-Specific Field
Name	'The password hash account was accessed.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName

HP ArcSight ESM Field	Device-Specific Field
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName

4783

HP ArcSight ESM Field	Device-Specific Field
Name	'A basic application group was created.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetSid)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4784

HP ArcSight ESM Field	Device-Specific Field
Name	'A basic application group was changed.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetSid)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4785

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was added to a basic application group.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (MemberSid, MemberName)
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4786

HP ArcSight ESM Field	Device-Specific Field
Name	'A member was removed from a basic application group.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (MemberSid, MemberName)
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4787

HP ArcSight ESM Field	Device-Specific Field
Name	'A non-member was added to a basic application group.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (MemberSid, MemberName)
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList
Message	'A non-member is an account that is explicitly excluded from membership in a basic application group. Even if the account is specified as a member of the application group, either explicitly or through nested group membership, the account will not be treated as a group member if it is listed as a non-member.'

4788

HP ArcSight ESM Field	Device-Specific Field
Name	'A non-member was removed from a basic application group.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (MemberSid, MemberName)
Device Custom String 6	Both (TargetDomainName, TargetUserName)
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

HP ArcSight ESM Field	Device-Specific Field
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList
Message	'A non-member is an account that is explicitly excluded from membership in a basic application group. Even if the account is specified as a member of the application group, either explicitly or through nested group membership, the account will not be treated as a group member if it is listed as a non-member.'

4789

HP ArcSight ESM Field	Device-Specific Field
Name	'A basic application group was deleted.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetSid, TargetUserName)
Destination NT Domain	TargetDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4790

HP ArcSight ESM Field	Device-Specific Field
Name	'An LDAP query group was created.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetSid, TargetUserName)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4791

HP ArcSight ESM Field	Device-Specific Field
Name	'A basic application group was changed.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetSid, TargetUserName)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4792

HP ArcSight ESM Field	Device-Specific Field
Name	'An LDAP query group was deleted.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetSid, TargetUserName)
Destination NT Domain	TargetDomainName
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

4793

HP ArcSight ESM Field	Device-Specific Field
Name	'The Password Policy Checking API was called.'
Source Host Name	Workstation
Source User Name	TargetUserName
Device Custom String 4	Stataus
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4794

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to set the Directory Services Restore Modeadministrator password.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4797

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to query the existence of a blank password for an account.'
Source Host Name	Workstation
Destination User Name	One of (SubjectUserName, SubjectUserSid)

HP ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

4798

HP ArcSight ESM Field	Device-Specific Field
Name	'A user's local group membership was enumerated.'
Destination User Name	One of (TargetUserName, TargetSid)
Destination NT Domain	TargetDomainName
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
File Name	CallerProcessId
File Path	CallerProcessName
Message	'A user's local group membership was enumerated.'

4799

HP ArcSight ESM Field	Device-Specific Field
Name	'A security-enabled local group membership was enumerated.'
Destination User Name	One of (TargetUserName, TargetSid)
Destination NT Domain	TargetDomainName
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
File Name	CallerProcessId
File Path	CallerProcessName
Message	'A security-enabled local group membership was enumerated.'

4800

HP ArcSight ESM Field	Device-Specific Field
Name	'The workstation was locked.'
Device Custom String 6	SessionId
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName

4801

HP ArcSight ESM Field	Device-Specific Field
Name	'The workstation was unlocked.'
Device Custom String 6	SessionId
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName

4802

HP ArcSight ESM Field	Device-Specific Field
Name	'The screen saver was invoked.'
Device Custom String 6	SessionId
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName

4803

HP ArcSight ESM Field	Device-Specific Field
Name	'The screen saver was dismissed.'
Device Custom String 6	SessionId
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Device NT Domain	TargetDomainName

4816

HP ArcSight ESM Field	Device-Specific Field
Name	'RPC detected an integrity violation while decrypting an incoming message.'

4817

HP ArcSight ESM Field	Device-Specific Field
Name	'Auditing settings on object were changed.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File Type	ObjectType
File Name	ObjectName

4818

HP ArcSight ESM Field	Device-Specific Field
Name	'Proposed Central Access Policy does not grant in the same access permissions as the current Central Access Policy.'
Destination Process ID	ProcessId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File ID	HandleId
File Type	ObjectType
File Name	ObjectName
Destination Process Name	ProcessName

4819

HP ArcSight ESM Field	Device-Specific Field
Name	'Central Access Policies on the machine have been changed.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File Type	ObjectType
Device NT Domain	SubjectDomainName

4820

HP ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos Ticket-granting ticket \\(TGT\\) was denied because the device does not meet the access control restrictions.'
Source User Name	TargetUserName
Source DNS Domain	TargetDomainName
Source User ID	TargetSid
Device Custom String 5	ServiceSid
Device Custom String 1	All of (PreAuthType,, Status, TicketEncryptionType, TicketOptions)
Source Address	IpAddress
Device Custom String 4	All of (CertIssuerName,CertSerialNumber, CertThumbprint)
Device Custom String 3	SiloName
Device Custom String 6	PolicyName
Destination Service Name	ServiceName
Source Port	IpPort
Message	'Certificate information is only provided if a certificate was used for pre-authentication. Pre-authentication types, ticket options, encryption types and result codes are defined in RFC 4120.'

4821

HP ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions.'
Source User Name	TargetUserName
Source DNS Domain	TargetDomainName
Destination Process ID	ServiceSid
Device Custom String 1	All of (Status, TicketEncryptionType, TicketOptions, TransitedServices)

Windows Security Event Mappings

Specific Windows Security Event Mappings

HP ArcSight ESM Field	Device-Specific Field
Source Address	IpAddress
Source User ID	LogonGuid
Device Custom String 5	SiloName
Device Custom String 6	PolicyName
Source Port	IpPort
Destination Service Name	ServiceName
Device Custom String 4	Status
Message	<p>'This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.'</p>

4822

HP ArcSight ESM Field	Device-Specific Field
Name	'NTLM authentication failed because the account was a member of the Protected User group.'
Reason	Status
Device Custom String 4	Status
Destination User Name	AccountName

4823

HP ArcSight ESM Field	Device-Specific Field
Name	'NTLM authentication failed because access control restrictions are required.'
Reason	Status
Device Custom String 5	SiloName

HP ArcSight ESM Field	Device-Specific Field
Device Custom String 6	PolicyName
Device Custom String 4	Status
Destination User Name	AccountName

4824

HP ArcSight ESM Field	Device-Specific Field
Name	'Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group.'
Source User Name	TargetUserName
Source User ID	TargetSid
Device Custom String 1	All of (PreAuthType, Status, TicketOptions)
Source Address	IpAddress
Device Custom String 4	All of (CertIssuerName, CertSerialNumber, CertThumbprint)
Source Port	IpPort
Destination Service Name	ServiceName

4826

HP ArcSight ESM Field	Device-Specific Field
Name	'Boot Configuration Data loaded.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Message	'Boot Configuration Data loaded.'
Additional data	LoadOptions
Additional data	AdvancedOptions
Additional data	ConfigAccessPolicy
Additional data	RemoteEventLogging

HP ArcSight ESM Field	Device-Specific Field
Additional data	KernelDebug
Additional data	VsmLaunchType
Additional data	TestSigning
Additional data	FlightSigning
Additional data	DisableIntegrityChecks
Additional data	HypervisorLoadOptions
Additional data	HypervisorLaunchType
Additional data	HypervisorDebug

4864

HP ArcSight ESM Field	Device-Specific Field
Name	'A namespace collision was detected.'

4865

HP ArcSight ESM Field	Device-Specific Field
Name	'A trusted forest information entry was added.'
Device Custom String 6	ForestRoot
Device Custom String 3	OperationId
Device Custom String 5	TopLevelName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4866

HP ArcSight ESM Field	Device-Specific Field
Name	'A trusted forest information entry was removed.'
Device Custom String 6	ForestRoot
Device Custom String 3	OperationId
Device Custom String 5	TopLevelName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4867

HP ArcSight ESM Field	Device-Specific Field
Name	'A trusted forest information entry was modified.'
Device Custom String 6	ForestRoot
Device Custom String 3	OperationId
Device Custom String 5	TopLevelName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4868

HP ArcSight ESM Field	Device-Specific Field
Name	'The certificate manager denied a pending certificate request.'
Destination User ID	SubjectLogonId

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4869

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a resubmitted certificate request.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4870

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services revoked a certificate.'
Destination User ID	SubjectLogonId
Device Custom String 4	RevocationReason
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4871

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a request to publish the certificate revocation list (CRL).'
Destination User ID	SubjectLogonId

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4872

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a request to publish the certificate revocation list (CRL).'

4873

HP ArcSight ESM Field	Device-Specific Field
Name	'A certificate request extension changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4874

HP ArcSight ESM Field	Device-Specific Field
Name	'One or more certificate request attributes changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4875

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a request to shutdown.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4876

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services backup started.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4877

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services backup completed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4878

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services restore started.'

4879

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services restore completed.'

4880

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services started.'

4881

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services stopped.'

4882

HP ArcSight ESM Field	Device-Specific Field
Name	'The security permissions for Certificate Services changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4883

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services retrieved an archived key.'
Destination User ID	SubjectLogonId

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4884

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services imported a certificate into its database.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4885

HP ArcSight ESM Field	Device-Specific Field
Name	'The audit filter for Certificate Services changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4886

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a certificate request.'

4887

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services approved a certificate request and issued a certificate.'

4888

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services denied a certificate request.'

4889

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services set th status of a certificate request to pending.'

4890

HP ArcSight ESM Field	Device-Specific Field
Name	'The certificate manager settings for Certificate Services changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4891

HP ArcSight ESM Field	Device-Specific Field
Name	'A configuration entry changed in Certificate Services.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4892

HP ArcSight ESM Field	Device-Specific Field
Name	'A property of Certificate Services changed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4893

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services archived a key.'

4894

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services imported and archived a key.'

4895

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services published the CA certificate toActive Directory Domain Services.'

4896

HP ArcSight ESM Field	Device-Specific Field
Name	'One or more rows have been deleted from the certificate database.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4897

HP ArcSight ESM Field	Device-Specific Field
Name	'Role separation enabled.'

4898

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services loaded a template.'

4899

HP ArcSight ESM Field	Device-Specific Field
Name	'A Certificate Services template was updated.'

4900

HP ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services template security was updated.'

4902

HP ArcSight ESM Field	Device-Specific Field
Name	'The Per-user audit policy table was created.'
Device Custom Number 3	PuaCount
Device Custom Number 6	PuaPolicyId

4904

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to register a security event source.'
Device Custom String 6	AuditSourceName
Device Custom String 5	EventSourceId
Device Custom String 3	ProcessId
Destination Process Name	ProcessName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4905

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt was made to unregister a security event source.'
Device Custom String 6	AuditSourceName
Device Custom String 5	EventSourceId
Device Custom String 3	ProcessId
Destination Process Name	ProcessName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4906

HP ArcSight ESM Field	Device-Specific Field
Name	'The CrashOnAuditFail value has changed.'
Device Custom Number 2	CrashOnAuditFailValue

4907

HP ArcSight ESM Field	Device-Specific Field
Name	'Auditing settings on object were changed.'
Device Custom String 5	ObjectType
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File ID	HandleId

HP ArcSight ESM Field	Device-Specific Field
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4908

HP ArcSight ESM Field	Device-Specific Field
Name	'Special Groups Logon table modified.'
Device Custom String 6	SidList
Message	'This event is generated when the list of special groups is updated in the registry or through security policy. The updated list of special groups is indicated in the event.'

4909

HP ArcSight ESM Field	Device-Specific Field
Name	'The local policy settings for the TBS were changed.'

4910

HP ArcSight ESM Field	Device-Specific Field
Name	'The group policy settings for the TBS were changed.'

4911

HP ArcSight ESM Field	Device-Specific Field
Name	'Resource attributes of the object were changed.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

HP ArcSight ESM Field	Device-Specific Field
Destination User ID	SubjectLogonId
File ID	HandleId
File Name	ObjectName
File Type	ObjectType
Destination Process ID	ProcessId
Destination Process Name	ProcessName

4912

HP ArcSight ESM Field	Device-Specific Field
Name	'Per User Audit Policy was changed.'
Device Custom String 6	TargetUserSid
Device Custom String 5	SubcategoryId
Device Action	AuditPolicyChanges
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

4913

HP ArcSight ESM Field	Device-Specific Field
Name	'Central Access Policy on the object was changed.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File ID	HandleId
File Name	ObjectName

HP ArcSight ESM Field	Device-Specific Field
File Type	ObjectType
Destination process ID	ProcessId
Destination process Name	ProcessName

4928

HP ArcSight ESM Field	Device-Specific Field
Name	'An Active Directory replica source naming context was established.'

4929

HP ArcSight ESM Field	Device-Specific Field
Name	'An Active Directory replica source naming context was removed.'

4930

HP ArcSight ESM Field	Device-Specific Field
Name	'An Active Directory replica source naming context was modified.'

4931

HP ArcSight ESM Field	Device-Specific Field
Name	'An Active Directory replica destination naming context was modified.'

4932

HP ArcSight ESM Field	Device-Specific Field
Name	'Synchronization of a replica of an Active Directory naming context has begun.'

4933

HP ArcSight ESM Field	Device-Specific Field
Name	'Synchronization of a replica of an Active Directory naming context has ended.'

4934

HP ArcSight ESM Field	Device-Specific Field
Name	'Attributes of an Active Directory object were replicated.'

4935

HP ArcSight ESM Field	Device-Specific Field
Name	'Replication failure begins.'

4936

HP ArcSight ESM Field	Device-Specific Field
Name	'Replication failure ends.'

4937

HP ArcSight ESM Field	Device-Specific Field
Name	'A lingering object was removed from a replica.'

4944

HP ArcSight ESM Field	Device-Specific Field
Name	'The following policy was active when the Windows Firewall started..'

4945

HP ArcSight ESM Field	Device-Specific Field
Name	'A rule was listed when the Windows Firewall started.'

4946

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to Windows Firewall exception list. A rule was added.'

4947

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to Windows Firewall exception list. A rule was modified.'

4948

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to Windows Firewall exception list. A rule was deleted.'

4949

HP ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall settings were restored to the default values.'

4950

HP ArcSight ESM Field	Device-Specific Field
Name	'A Windows Firewall setting has changed.'

4951

HP ArcSight ESM Field	Device-Specific Field
Name	'A rule has been ignored because its major version number was not recognized by Windows Firewall.'

4952

HP ArcSight ESM Field	Device-Specific Field
Name	'Parts of a rule have bween ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.'

4953

HP ArcSight ESM Field	Device-Specific Field
Name	'A rule has been ignored by Windows Firewall because it could not parse the rule.'
Device Custom String 4	ReasonForRejection

4954

HP ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall Group Policy settings has changed. The new settings have been applied.'

4956

HP ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall has changed the active profile.'

4957

HP ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall did not apply the following rule.'
Device Custom String 6	RuleName
Device Custom String 4	RuleAttr (Error Information)

4958

HP ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.'
Device Custom String 4	Error

4960

HP ArcSight ESM Field	Device-Specific Field
Name	'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

HP ArcSight ESM Field	Device-Specific Field
Name	'IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.'

4962

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'

4963

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'

4964

HP ArcSight ESM Field	Device-Specific Field
Name	'Special groups have been assigned to a new login.'
Source User Name	SubjectUserName
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	TargetUserName
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId
Device Custom String 3	TargetLogonGuid
Device Custom String 6	SidList
Device NT Domain	SubjectDomainName

4965

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'

4976

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'
Source Address	LocalAddress

4977

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'
Source Address	LocalAddress

4978

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'
Source Address	LocalAddress

4979

HP ArcSight ESM Field	Device-Specific Field
Name	'IPsec Main Mode and Extended Mode security associations were established.'

4980

HP ArcSight ESM Field	Device-Specific Field
Name	'IPsec Main Mode and Extended Mode security associations were established.'

4981

HP ArcSight ESM Field	Device-Specific Field
Name	'IPsec Main Mode and Extended Mode security associations were established.'
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort

4982

HP ArcSight ESM Field	Device-Specific Field
Name	'IPsec Main Mode and Extended Mode security associations were established.'
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort

4983

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.'
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort
Message	FailureReason
Device Custom String 4	Failure

4984

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.'
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort
Message	FailureReason
Device Custom String 4	Failure

4985

HP ArcSight ESM Field	Device-Specific Field
Name	'The state of a transaction has changed.'
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5024

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service has started successfully.'

5025

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service has been stopped.'

5027

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.'
Device Custom String 4	ErrorCode

5028

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.'
Device Custom String 4	ErrorCode

5029

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.'
Device Custom String 4	ErrorCode

5030

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service failed to start.'
Device Custom String 4	ErrorCode

5031

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Service blocked an application from accepting incoming connections on the network.'

5032

HP ArcSight ESM Field	Device-Specific Field
Name	'Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.'
Device Custom String 4	ErrorCode

5033

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Driver has started successfully.'
Message	" "

5034

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Driver has been stopped..'

5035

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Driver failed to start.'
Device Custom String 4	ErrorCode

5037

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Firewall Driver detected critical runtime error. Terminating.'
Device Custom String 4	ErrorCode

5038

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'

5039

HP ArcSight ESM Field	Device-Specific Field
Name	'A registry key was virtualized.'
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5040

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. An Authentication Set was added.'

5041

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. An Authentication Set was modified.'

5042

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. An Authentication Set was deleted.'

5043

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Connection Security Rule was added.'

5044

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Connection Security Rule was modified.'

5045

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Connection Security Rule was deleted.'

5046

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Crypto Set was added.'

5047

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Crypto Set was modified.'

5048

HP ArcSight ESM Field	Device-Specific Field
Name	'A change has been made to IPsec settings. A Crypto Set was deleted.'

5049

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Security Association was deleted.'

5050

HP ArcSight ESM Field	Device-Specific Field
Name	'An attempt to programmatically disable the Windows Firewall using a call to INetFwProfile.FirewallEnabled (FALSE) interface was rejected because this API is not supported on Windows Vista. This has most likely occurred due to a program which is incompatible with Windows Vista. Please contact the program's manufacturer to make sure you have a Windows Vista compatible program version.'

5051

HP ArcSight ESM Field	Device-Specific Field
Name	'A file was virtualized.'
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5056

HP ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic self test was performed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5057

HP ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic primitive operation failed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Message	Reason
Reason	ReturnCode

5058

HP ArcSight ESM Field	Device-Specific Field
Name	'Key file operation.'
File Name	KeyName
File Type	KeyType
File Path	KeyFilePath
Device Action	Operation
Device Custom String 4	ReturnCode
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5059

HP ArcSight ESM Field	Device-Specific Field
Name	'Key migration operation.'
File Name	KeyName

HP ArcSight ESM Field	Device-Specific Field
File Type	KeyType
Device Action	Operation
Device Custom String 4	ReturnCode
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5060

HP ArcSight ESM Field	Device-Specific Field
Name	'Verification operation failed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5061

HP ArcSight ESM Field	Device-Specific Field
Name	'Cryptographic operation.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5062

HP ArcSight ESM Field	Device-Specific Field
Name	'A kernel-mode cryptographic self test was performed.'

5063

HP ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic provider operation was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5064

HP ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic context operation was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5065

HP ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic context modification was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5066

HP ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function operation was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5067

HP ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function modification was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5068

HP ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function provider operation was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5069

HP ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function property operation was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5070

HP ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function property modification was attempted.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5071

HP ArcSight ESM Field	Device-Specific Field
Name	'Key access denied by Microsoft key distribution service.'
Device Custom String 5	SecurityDescriptor
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5120

HP ArcSight ESM Field	Device-Specific Field
Name	'OCSP Responder Service Started.'

5121

HP ArcSight ESM Field	Device-Specific Field
Name	'OCSP Responder Service Stopped.'

5122

HP ArcSight ESM Field	Device-Specific Field
Name	'A Configuration entry changed in the OCSP Responder Service.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5123

HP ArcSight ESM Field	Device-Specific Field
Name	'A configuration entry changed in the OCSP Responder Service.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5124

HP ArcSight ESM Field	Device-Specific Field
Name	'A security setting was updated on OCSP Responder Service.'

5125

HP ArcSight ESM Field	Device-Specific Field
Name	'A request was submitted to OCSP Responder Service.'

5126

HP ArcSight ESM Field	Device-Specific Field
Name	'Signing Certificate was automatically updated by the OCSP Responder Service.'

5127

HP ArcSight ESM Field	Device-Specific Field
Name	'The OCSP Revocation provider successfully updated the revocation information.'

5136

HP ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was modified.'
Device Custom String 6	ObjectDN
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)

HP ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Device Custom String 4	OperationType

5137

HP ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was created.'
Device Custom String 6	ObjectDN
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5138

HP ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was undeleted.'
Device Custom String 6	NewObjectDN
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5139

HP ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was moved.'
Device Custom String 6	NewObjectDN
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5140

HP ArcSight ESM Field	Device-Specific Field
Name	'A network share object was accessed.'
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
File Path	ShareName
File Type	ObjectType
Device Custom String 6	ShareName
Device Custom String 1	AccessList
Source Port	IpPort
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5141

HP ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was deleted.'
Device Custom String 6	ObjectDN
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5142

HP ArcSight ESM Field	Device-Specific Field
Name	'A network share object was added.'
File Path	ShareName
Device Custom String 6	ShareName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

5143

HP ArcSight ESM Field	Device-Specific Field
Name	'A network share object was modified.'
File Path	ShareName
Device Custom String 5	ObjectType
Device Custom String 6	ShareName
Destination User Name	One of (SubjectUserName, SubjectUserSid)

HP ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

5144

HP ArcSight ESM Field	Device-Specific Field
Name	'A network share object was deleted.'
File Path	ShareName
Device Custom String 6	ShareName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

5145

HP ArcSight ESM Field	Device-Specific Field
Name	'A network share object was checked to see whether client can be granted desired access.'
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom String 1	AccessList
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Source Port	IpPort

5146

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has blocked a packet.'
Device Direction	Direction
Source Address	SourceAddress
Device Custom IPv6 Address 2	SourceAddress (Source IPv6 Address)
Destination Address	DestAddress
Device Custom IPv6 Address 3	DestAddress (Destination IPv6 Address)
Source Port	SourceSwitchPort
Destination Port	DestinationvSwitchPort

5147

HP ArcSight ESM Field	Device-Specific Field
Name	'A more restrictive Windows Filtering Platform filter has blocked a packet.'
Device Direction	Direction
Source Address	SourceAddress
Device Custom IPv6 Address 2	SourceAddress (Source IPv6 Address)
Destination Address	DestAddress
Device Custom IPv6 Address 3	DestAddress (Destination IPv6 Address)
Source Port	SourceSwitchPort
Destination Port	DestinationvSwitchPort

5152

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform blocked a packet.'
Source Address	SourceAddress

HP ArcSight ESM Field	Device-Specific Field
Source Port	SourcePort
Destination Address	DestAddress
Destination Port	DestPort

5153

HP ArcSight ESM Field	Device-Specific Field
Name	'A more restrictive Windows Filtering Platform filter has blocked a packet.'
Source Port	SourcePort
Destination Port	DestPort

5154

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering platform has permitted an application or service to listen on a port for incoming connections.'
Source Address	SourceAddress
Device Custom IPv6 Address 2	SourceAddress (Source IPv6 Address)
Source Port	SourcePort

5155

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.'
Source Port	SourcePort

5156

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has allowed a connection.'
Device Direction	Direction
Source Address	One of (SourceAddress)
Device Custom IPv6 Address 2	SourceAddress (Source IPv6 Address)
Source Port	SourcePort
Destination Address	One of (DestAddress)
Device Custom IPv6 Address 3	DestAddress (Destination IPv6 Address)
Destination Port	DestPort
Transport Protocol	Protocol

5157

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has blocked a connection.'
Source Port	SourcePort
Destination Port	DestPort

5158

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has permitted a bind to a local port.'
Source Address	SourceAddress
Device Custom IPv6 Address 2	SourceAddress (Source IPv6 Address)
Source Port	SourcePort

5159

HP ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has blocked a bind to a local port.'
Source Process ID	ProcessId
File Name	Application
File Path	Application
File Type	Application
Source Address	SourceAddress
Destination Address	SourceAddress
Transport Protocol	Protocol
Device Custom Number 2	FilterRTID
Device Custom String 6	LayerName
Device Custom Number 3	LayerRTID
Source Port	SourcePort

5168

HP ArcSight ESM Field	Device-Specific Field
Name	'Spn check for SMB/SMB2 fails.'
Destination User Name	' '
Source User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	' '
Source NT Domain	SubjectDomainName
Destination User ID	' '
Source User ID	SubjectLogonId
Destination Service Name	SpnName
Device Custom String 4	ErrorCode
Device NT Domain	SubjectDomainName
Reason	ErrorCode

5376

HP ArcSight ESM Field	Device-Specific Field
Name	'Credential Manager credentials were backed up.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Message	'This event occurs when a user backs up their own Credential Manager credentials. A user (even an Administrator) cannot back up the credentials of an account other than his own.'

5377

HP ArcSight ESM Field	Device-Specific Field
Name	'Credential Manager credentials were restored from a backup.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Message	'This event occurs when a user restores his Credential Manager credentials from a backup. A user (even an Administrator) cannot restore the credentials of an account other than his own.'

5378

HP ArcSight ESM Field	Device-Specific Field
Name	'The requested credentials delegation was disallowed by policy.'
Destination User ID	SubjectLogonId

HP ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5440

HP ArcSight ESM Field	Device-Specific Field
Name	'The following callout was present when the Windows Filtering Platform Base Filtering Engine started.'

5441

HP ArcSight ESM Field	Device-Specific Field
Name	'The following filter was present when the Windows Filtering Platform Base Filtering Engine started.'

5442

HP ArcSight ESM Field	Device-Specific Field
Name	'The following provider was present when the Windows Filtering Platform Base Filtering Engine started.'

5443

HP ArcSight ESM Field	Device-Specific Field
Name	'The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.'

5444

HP ArcSight ESM Field	Device-Specific Field
Name	'The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.'

5446

HP ArcSight ESM Field	Device-Specific Field
Name	'A Windows Filtering Platform callout has been changed.'
Destination User Name	One of (UserName, UserSid)

5447

HP ArcSight ESM Field	Device-Specific Field
Name	'A Windows Filtering Platform filter has been changed.'
Destination User Name	One of (UserName, UserSid)

5448

HP ArcSight ESM Field	Device-Specific Field
Name	'A Windows Filtering Platform provider has been changed.'
Destination User Name	One of (UserName, UserSid)

5449

HP ArcSight ESM Field	Device-Specific Field
Name	'A Windows Filtering Platform provider context has been changed.'
Destination User Name	One of (UserName, UserSid)

5450

HP ArcSight ESM Field	Device-Specific Field
Name	'A Windows Filtering Platform sub-layer has been changed.'
Destination User Name	One of (UserName, UserSid)

5451

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Quick Mode security association was established.'
Source Address	LocalAddress
Source Port	LocalPort
Destination Address	RemoteAddress
Destination Port	RemotePort

5452

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Quick Mode security association ended.'
Source Address	LocalAddress
Source Port	LocalPort
Destination Address	RemoteAddress
Destination Port	RemotePort

5453

HP ArcSight ESM Field	Device-Specific Field
Name	'An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.'

5456

HP ArcSight ESM Field	Device-Specific Field
Name	'PASTore Engine applied Active Directory storage IPsec policy on the computer.'

5457

HP ArcSight ESM Field	Device-Specific Field
Name	'PASTore Engine failed to apply Active Directory storage IPsec policy on the computer.'

5458

HP ArcSight ESM Field	Device-Specific Field
Name	'PASTore Engine applied locally cached copy of Active Directory storage IPsec on the computer.'

5459

HP ArcSight ESM Field	Device-Specific Field
Name	'PASTore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.'
Device Custom String 4	Error

5460

HP ArcSight ESM Field	Device-Specific Field
Name	'PASTore Engine applied local registry storage IPsec policy on the computer.'

5461

HP ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine failed to apply local registry storage IPsec policy on the computer.'
Device Custom String 4	Error

5462

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'
Device Custom String 4	Error

5463

HP ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine Polled for changes to the active IPsec policy and detected no changes.'

5464

HP ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.'

5465

HP ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.'

5466

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'

5467

HP ArcSight ESM Field	Device-Specific Field
Name	'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

HP ArcSight ESM Field	Device-Specific Field
Name	'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

HP ArcSight ESM Field	Device-Specific Field
Name	'PASTore Engine loaded local storage IPsec policy on the computer.'

5472

HP ArcSight ESM Field	Device-Specific Field
Name	'PASTore Engine failed to load local storage IPsec policy on the computer.'
Device Custom String 4	Error

5473

HP ArcSight ESM Field	Device-Specific Field
Name	'PASTore Engine loaded directory storage IPsec policy on the computer.'

5474

HP ArcSight ESM Field	Device-Specific Field
Name	'PASTore Engine failed to load directory storage IPsec policy on the computer.'
Device Custom String 4	Error

5477

HP ArcSight ESM Field	Device-Specific Field
Name	'PASTore Engine failed to add quick mode filter.'
Device Custom String 4	Error

5478

HP ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services has started successfully.'

5479

HP ArcSight ESM Field	Device-Specific Field
Name	'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

HP ArcSight ESM Field	Device-Specific Field
Name	'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

HP ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services failed to initialize RPC server. IPsec Services could not be started.'
Device Custom String 4	Error

5484

HP ArcSight ESM Field	Device-Specific Field
Name	'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.'
Device Custom String 4	Error

5632

HP ArcSight ESM Field	Device-Specific Field
Name	'A request was made to authenticate to a wireless network.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, Identity)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Device Custom String 4	One of (ReasonCode, ErrorCode)
Reason	One of (EAPErrorCode, EAPReasonCode, ErrorCode, both (ReasonText, ReasonCode))

5633

HP ArcSight ESM Field	Device-Specific Field
Name	'A request was made to authenticate to a wired network.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, Identity)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Device Outbound Interface	InterfaceName
Device Custom String 4	One of (ReasonCode, ErrorCode)
Reason	One of (ErrorCode, both (ReasonText, ReasonCode))

5712

HP ArcSight ESM Field	Device-Specific Field
Name	'A Remote Procedure Call (RPC) was attempted.'
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

5888

HP ArcSight ESM Field	Device-Specific Field
Name	'An object in the COM+ Catalog was modified.'
Destination User ID	SubjectLogonId
File Name	ObjectIdentifyingProperties
Destination user Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectUserDomainName
Device NT Domain	SubjectUserDomain Name

5889

HP ArcSight ESM Field	Device-Specific Field
Name	'An object was deleted from the COM+ Catalog.'
Destination User ID	SubjectLogonId
File Name	ObjectIdentifyingProperties
Destination user Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectUserDomainName
Device NT Domain	SubjectUserDomain Name
Message	'This event occurs when an object is deleted from the COM+ catalog.'

5890

HP ArcSight ESM Field	Device-Specific Field
Name	'An object was added to the COM+ Catalog.'
Destination User ID	SubjectLogonId
File Name	ObjectIdentifyingProperties
Destination user Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectUserDomainName
Device NT Domain	SubjectUserDomain Name

6144

HP ArcSight ESM Field	Device-Specific Field
Name	'Security policy in the group policy objects has been applied successfully.'

6145

HP ArcSight ESM Field	Device-Specific Field
Name	'One or more errors occurred while processing security policy in the group policy objects.'
Device Custom String 4	ErrorCode

6272

HP ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server granted access to a user.'
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName
Destination Address	NASIPv4Address
Destination Port	NASPort
Source User Name	SubjectMachineName
Source User ID	FullyQualifiedSubjectMachineName
Source Address	CallingStationID
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIPAddress
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier
Destination User Privileges	QuarantineState

6273

HP ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server denied access to a user. Contact the Network Policy Server administrator for more information.'
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName
Destination Address	NASIPv4Address
Destination Port	NASPort
Source User Name	SubjectMachineName
Source User ID	FullyQualifiedSubjectMachineName
Source Address	CallingStationID
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIPAddress
Device Custom String 4	Reason
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier

6274

HP ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server discarded the request for a user. . Contact the Network Policy Server administrator for more information.'

6275

HP ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server discarded the accounting request for a user. . Contact the Network Policy Server administrator for more information.'

6276

HP ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server quarantined a user.. Contact the Network Policy Server administrator for more information.'

6277

HP ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy . Contact the Network Policy Server administrator for more information.'

6278

HP ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server granted full access to a user because the host met the defined health policy.'
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName
Source User Name	SubjectMachineName
Source User ID	FullyQualifiedSubjectMachineName
Source Address	CallingStationID
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIPAddress
Destination Address	NASIPv4Address
Destination Port	NASPort
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier
Destination User Privileges	QuarantineState

6279

HP ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server locked the user account due to repeated failed authentication attempts.'
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName

6280

HP ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server unlocked the user account.'
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName

6281

HP ArcSight ESM Field	Device-Specific Field
Name	'Code Integrity determined that the page hashes or an image file are not valid.'
File Path	Param1
Message	'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.'

6409

HP ArcSight ESM Field	Device-Specific Field
Name	'BranchCache: A service connection point object could not be parsed.'

6410

HP ArcSight ESM Field	Device-Specific Field
Name	'Code integrity determined that a file does not meet the security requirements to load into a process.'
Message	'This could be due to the use of shared sections or other issues.'
File Name	param1

6416

HP ArcSight ESM Field	Device-Specific Field
Name	'A new external device was recognized by the system.'
Source UJser Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
File ID	ClassId
Device Custom String 1	VendorIds
Device Custom String 4	CompatibleIds
Device Custom String 5	LocationInformation
Message	'A new external device was recognized by the system.'

8191

HP ArcSight ESM Field	Device-Specific Field
Name	'Highest System-Defined Audit Message Value.'

Windows Event Log Event Descriptions by Category

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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

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.
		4799	A security-enabled local group membership was enumerated
Account Management	User Account Management	4758	A security-enabled universal group was deleted.
		4764	A group's type was changed.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
		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.
		4798	A user's local group membership was enumerated.
		5376	Credential Manager credentials were backed up.
		5377	Credential Manager credentials were restored from a backup.
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.
		4688	A new process has been created.
	Process Creation	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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
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	

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
		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.
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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
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.
		4627	Group membership 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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

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.
	Special Logon	4964	Special groups have been assigned to a new logon.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
Object Access	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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
Object Access	Detailed File Share	5145	A network share object was checked to see whether the client can be granted desired access.
		5140	A network share object was accessed.
	File Share	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.
		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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
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.
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.
		4703	A user right was adjusted.
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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
Policy Change	Filtering Platform Policy Change	4711	<p>May contain any one of the following: PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.</p> <p>PAStore Engine applied Active Directory storage IPsec policy on the computer.</p> <p>PAStore Engine applied local registry storage IPsec policy on the computer.</p> <p>PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.</p> <p>PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.</p> <p>PAStore Engine failed to apply local registry storage IPsec policy on the computer.</p> <p>PAStore Engine failed to apply some rules of the active IPsec policy on the computer.</p> <p>PAStore Engine failed to load directory storage IPsec policy on the computer.</p> <p>PAStore Engine loaded directory storage IPsec policy on the computer.</p> <p>PAStore Engine failed to load local storage IPsec policy on the computer.</p> <p>PAStore Engine loaded local storage IPsec policy on the computer.</p> <p>PAStore Engine polled for changes to the active IPsec policy and detected no changes.</p>

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
		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.
		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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

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:

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
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.
		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.
System	Other System Events	4820	A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions.
		4821	A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
		4822	NTLM authentication failed because the account was a member of the Protected User group.
System	Other System Events	4823	NTLM authentication failed because access control restrictions are required.
		4824	Kerberos preauthentication by using DES or RC4 failed because the account was a member of the Protected User group
		4826	Boot Configuration Data Loaded.
		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.
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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
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. Native Connector: An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts.
		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.

Windows Security Event Mappings

Windows Event Log Event Descriptions by Category

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

Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Windows Security Event Mappings (Connectors)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to arc-doc@hpe.com.

We appreciate your feedback!