Micro Focus Security ArcSight Connectors

SmartConnector for Microsoft Windows Event Log – Native

Windows Event Mappings

Document Release Date: April 27, 2021
Software Release Date: April 27, 2021

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

ArcSight Product Documentation on the Micro Focus Security Community

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-Documentation/ct-p/productdocs

Revision History

Date	Description
04/27/2021	Updated the following event Ids: • 4625 • 5145
10/16/2020	Updated event Id 4769.
08/20/2020	Added mappings to the following events: 4673, 5058, 5376, and 5377. Added support for Microsoft OAlerts. Added support DNS Client Operational. Updated mappings for Event 4703
06/18/2020	Added mappings to Event 4950.
05/21/2020	Added mappings to Event 5145. Added the following new events: • Microsoft Windows Security Auditing: 5379 • Microsoft-Windows Security Auditing: 5380 • Microsoft Windows Security Auditing: 5381 • Microsoft Windows Security Auditing: 5382
02/20/2020	Added “Application" field mapping to the following audit events: 5152,5153,5154,5155,5156,5157, and 5158.
07/18/2018	Updated mappings for Event 1074
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.

Contents

About This Book 19

Windows Common Security Mappings 20

Specific Windows Security Event Mappings 22

- Event Id 1100 22
- Event Id 1101 22
- Event Id 1102 22
- Event Id 1104 22
- Event Id 1105 23
- Event Id 1074 23
- Event Id 4608 23
- Event Id 4609 24
- Event Id 4610 24
- Event Id 4611 24
- Event Id 4612 25
- Event Id 4614 25
- Event Id 4615 25
- Event Id 4616 26
- Event Id 4618 26
- Event Id 4621 27
- Event Id 4622 27
- Event Id 4624 27
- Event Id 4625 28
- Event Id 4626 29
- Event Id 4627 30
- Event Id 4634 31
- Event Id 4646 31
- Event Id 4647 32

Event Id 4648 32
Event Id 4649 33
Event Id 4650 33
Event Id 4651 33
Event Id4652 34
Event Id4653 34
Event Id 4654 34
Event Id 4655 35
Event Id 4656 35
Event Id 4657 36
Event Id 4658 36
Event Id 4659 37
Event Id 4660 37
Event Id 4661 38
Event Id 4662 38
Event Id 4663 39
Event Id 4664 39
Event Id 4665 39
Event Id 4666 40
Event Id 4667 40
Event Id 4668 40
Event Id 4670 40
Event Id 4671 41
Event Id 4672 41
Event Id 4673 41
Event Id 4674 42
Event Id 4675 42
Event Id 4688 42
Event Id 4689 43
Event Id 4690 44
Event Id 4691 44
Event Id 4692 44

Event Id 4693 45
Event Id 4694 45
Event Id 4695 45
Event Id 4696 46
Event Id 4697 46
Event Id 4698 47
Event Id 4699 47
Event Id 4700 47
Event Id 4701 48
Event Id 4702 48
Event Id 4703 48
Event Id 4704 49
Event Id 4705 49
Event Id 4706 50
Event Id 4707 50
Event Id 4709 50
Event Id 4710 50
Event Id 4711 51
Event Id 4712 51
Event Id 4713 51
Event Id 4714 51
Event Id 4715 52
Event Id 4716 52
Event Id 4717 53
Event Id 4718 53
Event Id 4719 54
Event Id 4720 54
Event Id 4722 54
Event Id 4723 55
Event Id 4724 55
Event Id 4725 56
Event Id 4726 56

Event Id 4727 56
Event Id 4728 57
Event Id 4729 57
Event Id 4730 58
Event Id 4731 58
Event Id 4732 59
Event Id 4733 59
Event Id 4734 60
Event Id 4735 60
Event Id 4737 61
Event Id 4738 61
Event Id 4739 62
Event Id 4740 62
Event Id 4741 63
Event Id 4742 63
Event Id 4743 64
Event Id 4744 64
Event Id 4745 65
Event Id 4746 65
Event Id 4747 66
Event Id 4748 66
Event Id 4749 67
Event Id 4750 67
Event Id 4751 68
Event Id 4752 68
Event Id 4753 69
Event Id 4754 69
Event Id 4755 70
Event Id 4756 70
Event Id 4757 71
Event Id 4758 71
Event Id 4759 72

Event Id 4760 72
Event Id 4761 73
Event Id 4762 73
Event Id 4763 74
Event Id 4764 74
Event Id 4765 75
Event Id 4766 75
Event Id 4767 76
Event Id 4768 76
Event Id 4769 77
Event Id 4770 77
Event Id 4771 78
Event Id 4772 78
Event Id 4773 79
Event Id 4774 79
Event Id 4775 79
Event Id 4776 79
Event Id 4777 80
Event Id 4778 80
Event Id 4779 81
Event Id 4780 81
Event Id 4781 82
Event Id 4782 82
Event Id 4783 83
Event Id 4784 83
Event Id 4785 84
Event Id 4786 84
Event Id 4787 85
Event Id 4788 85
Event Id 4789 86
Event Id 4790 86
Event Id 4791 87

Event Id 4792 87
Event Id 4793 88
Event Id 4794 88
Event Id 4797 88
Event Id 4798 89
Event Id 4799 89
Event Id 4800 90
Event Id 4801 90
Event Id 4802 90
Event Id 4803 91
Event Id 4816 91
Event Id 4817 91
Event Id 4818 92
Event Id 4819 92
Event Id 4820 92
Event Id 4821 93
Event Id 4822 94
Event Id 4823 94
Event Id 4824 95
Event Id 4826 95
Event Id 4864 96
Event Id 4865 96
Event Id 4866 96
Event Id 4867 97
Event Id 4868 97
Event Id 4869 97
Event Id 4870 98
Event Id 4871 98
Event Id 4872 98
Event Id 4873 99
Event Id 4874 99
Event Id 4875 99

Event Id 4876 100
Event Id 4877 100
Event Id 4878 100
Event Id 4879 100
Event Id 4880 101
Event Id 4881 101
Event Id 4882 101
Event Id 4883 101
Event Id 4884 102
Event Id 4885 102
Event Id 4886 102
Event Id 4887 102
Event Id 4888 103
Event Id 4889 103
Event Id 4890 103
Event Id 4891 103
Event Id 4892 104
Event Id 4893 104
Event Id 4894 104
Event Id 4895 104
Event Id 4896 104
Event Id 4897 105
Event Id 4898 105
Event Id 4899 105
Event Id 4900 105
Event Id 4902 105
Event Id 4904 106
Event Id 4905 106
Event Id 4906 106
Event Id 4907 107
Event Id 4908 107
Event Id 4909 107

Event Id 4910 108
Event Id 4911 108
Event Id 4912 108
Event Id 4913 109
Event Id 4928 109
Event Id 4929 109
Event Id 4930 109
Event Id 4931 110
Event Id 4932 110
Event Id 4933 110
Event Id 4934 110
Event Id 4935 110
Event Id 4936 110
Event Id 4937 111
Event Id 4944 111
Event Id 4945 111
Event Id 4946 111
Event Id 4947 111
Event Id 4948 112
Event Id 4949 112
Event Id 4950 112
Event Id 4951 112
Event Id 4952 112
Event Id 4953 113
Event Id 4954 113
Event Id 4956 113
Event Id 4957 113
Event Id 4958 113
Event Id 4960 114
Event Id 4961 114
Event Id 4962 114
Event Id 4963 114

Event Id 4964 115
Event Id 4965 115
Event Id 4976 115
Event Id 4977 116
Event Id 4978 116
Event Id 4979 116
Event Id 4980 116
Event Id 4981 117
Event Id 4982 117
Event Id 4983 117
Event Id 4984 118
Event Id 4985 118
Event Id 5024 118
Event Id 5025 118
Event Id 5027 119
Event Id 5028 119
Event Id 5029 119
Event Id 5030 119
Event Id 5031 120
Event Id 5032 120
Event Id 5033 120
Event Id 5034 120
Event Id 5035 120
Event Id 5037 121
Event Id 5038 121
Event Id 5039 121
Event Id 5040 121
Event Id 5041 122
Event Id 5042 122
Event Id 5043 122
Event Id 5044 122
Event Id 5045 122

Event Id 5046 123
Event Id 5047 123
Event Id 5048 123
Event Id 5049 123
Event Id 5050 123
Event Id 5051 124
Event Id 5056 124
Event Id 5057 124
Event Id 5058 125
Event Id 5059 125
Event Id 5060 126
Event Id 5061 126
Event Id 5062 126
Event Id 5063 126
Event Id 5064 127
Event Id 5065 127
Event Id 5066 127
Event Id 5067 128
Event Id 5068 128
Event Id 5069 128
Event Id 5070 129
Event Id 5071 129
Event Id 5120 129
Event Id 5121 129
Event Id 5122 130
Event Id 5123 130
Event Id 5124 130
Event Id 5125 130
Event Id 5126 131
Event Id 5127 131
Event Id 5136 131
Event Id 5137 131

Event Id 5138 132
Event Id 5139 132
Event Id 5140 133
Event Id 5141 133
Event Id 5142 134
Event Id 5143 134
Event Id 5144 134
Event Id 5145 135
Event Id 5146 135
Event Id 5147 136
Event Id 5152 136
Event Id 5153 137
Event Id 5154 137
Event Id 5155 137
Event Id 5156 138
Event Id 5157 138
Event Id 5158 139
Event Id 5159 139
Event Id 5168 140
Event Id 5376 140
Event Id 5377 141
Event Id 5378 141
Event Id 5379 141
Event Id 5380 142
Event Id 5381 142
Event Id 5382 143
Event Id 5440 143
Event Id 5441 143
Event Id 5442 143
Event Id 5443 144
Event Id 5444 144
Event Id 5446 144

Event Id 5447 144
Event Id 5448 144
Event Id 5449 145
Event Id 5450 145
Event Id 5451 145
Event Id 5452 145
Event Id 5453 146
Event Id 5456 146
Event Id 5457 146
Event Id 5458 146
Event Id 5459 146
Event Id 5460 147
Event Id 5461 147
Event Id 5462 147
Event Id 5463 147
Event Id 5464 147
Event Id 5465 148
Event Id 5466 148
Event Id 5467 148
Event Id 5468 148
Event Id 5471 149
Event Id 5472 149
Event Id 5473 149
Event Id 5474 149
Event Id 5477 149
Event Id 5478 150
Event Id 5479 150
Event Id 5480 150
Event Id 5483 150
Event Id 5484 151
Event Id 5632 151
Event Id 5633 151

Event Id 5712 152
Event Id 5888 152
Event Id 5889 152
Event Id 5890 153
Event Id 6144 153
Event Id 6145 153
Event Id 6272 153
Event Id 6273 154
Event Id 6274 155
Event Id 6275 155
Event Id 6276 155
Event Id 6277 155
Event Id 6278 155
Event Id 6279 156
Event Id 6280 156
Event Id 6281 157
Event Id 6409 157
Event Id 6410 157
Event Id 6416 157
Event Id 8191 158

Mappings for Microsoft OAlerts 159
Event Id 300 159

Mappings for DNS Client Operational 160
Event Id 1015 160
Event Id 1016 160
Event Id 1017 160
Event Id 3006 161
Event Id 3008 161
Event Id 3009 161
Event Id 3010 162

Event Id 3011 162
Event Id 3012 162
Event Id 3013 163
Event Id 3014 163
Event Id 3016 163
Event Id 3018 163
Event Id 3019 164
Event Id 3020 164

Windows Event Log Event Descriptions by Category 165

Send Documentation Feedback 188

About This Book

This guide provides the specific events generated by the various policies and their mappings to Micro Focus 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 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

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)

Applications Supported

- Microsoft OAlerts
- DNS Client Operational

Windows Common Security Mappings

The following security event mappings generally apply to all Windows Server 2012, Windows Server 2016, and Windows 10 Windows Event Log Security Events.

Micro Focus ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Medium when Device Severity = Error or Warning; Low when Device Severity = Information or Audit_success
Destination Host Name	One of (Target Server Name, Computer Name, Target Server:Target Server Name)
Destination NT Domain	One of (Domain Name, Subject:Account Domain, New Token Information:Account Domain, Subject:Domain Name)
Destination Port	Network Information:Destination Port
Destination Process Name	One of (Process Information:New Process Name, Process Information:Process Name)
Destination Service Name	Service Information:Service Name
Destination User ID	One of (Subject:Logon ID, New Token Information:Logon ID)
Destination User Name	One of (Account Name, Subject:Account Name, Subject:Security ID, User, New Token Information:Account Name)
Destination User Privileges	One of (Additional Information:Privileges, New Right:User Right, Removed Right:User Right, Access Granted:Access Right, Access Removed:Access Right)
Device Action	One of (Account Action, Allowed, 'No', 'Blocked')
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom Number 1	Logon Type
Device Custom Number 2	Value of CrashOnAuditFail
Device Custom Number 3	Count
Device Custom String 1	One of (Access Request Information:Access Mask, Operation:Accesses, Operation:Access Mask)
Device Custom String 2	EventCategory

Micro Focus ArcSight ESM Field	Device-Specific Field
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)
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

Event Id 1100

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

Event Id 1101

Micro Focus 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

Event Id 1102

Micro Focus 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

Event Id 1104

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

Event Id 1105

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

Event Id 1074

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	The process has initiated the shutdown/restart of computer.
Message	concatenate(The process ",%1," has initiated the ",%5," of computer ",%2," on behalf of user ",%7," for the following reason: ",%3)
Source Process Name	%1
Destination Host Name	%2
Reason	%3
Device Custom String4	Reason Code
Device Custom String5	Shutdown Type
Device Custom String6	Comment

Event Id 4608

Micro Focus 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.'

Event Id 4609

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

Event Id 4610

Micro Focus 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

Event Id 4611

Micro Focus 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

Event Id 4612

Micro Focus 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.'

Event Id 4614

Micro Focus 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'

Event Id 4615

Micro Focus 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.'

Event Id 4616

Micro Focus 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.'

Event Id 4618

Micro Focus 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.'

Event Id 4621

Micro Focus 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.'

Event Id 4622

Micro Focus 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

Event Id 4624

Micro Focus 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

Micro Focus ArcSight ESM Field	Device-Specific Field
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.'

Event Id 4625

Micro Focus 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

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom String 5	AuthenticationPackageName
Device Custom String 6	Status
Device Custom String 6 Label	"Status"
Device Custom Number 1	LogonType
Destination UserName	TargetUserName
Message	‘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. - 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.’

Event Id 4626

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	‘User/Device claims information.’
Device NT Domain	SubjectDomainName
Destination User Name	TargetUserName
Destination User ID	TargetLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination NT Domain	TargetDomainName
Device Custom Number 1	LogonType
Message	'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.'

Event Id 4627

Micro Focus 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

Micro Focus 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.'

Event Id 4634

Micro Focus 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.'

Event Id 4646

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IKE DoS-prevention mode started.'

Event Id 4647

Micro Focus 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.'

Event Id 4648

Micro Focus 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

Event Id 4649

Micro Focus 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.'

Event Id 4650

Micro Focus 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.'

Event Id 4651

Micro Focus 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

Event Id4652

Micro Focus 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

Event Id4653

Micro Focus 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

Event Id 4654

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

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

Event Id 4655

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

Event Id 4656

Micro Focus 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

Event Id 4657

Micro Focus 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

Event Id 4658

Micro Focus 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

Event Id 4659

Micro Focus 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

Event Id 4660

Micro Focus 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

Event Id 4661

Micro Focus 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

Event Id 4662

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User ID	SubjectLogonId
Destination NT Domain	SubjectDomainName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom String 1	One of (AccessList, AccessMask)
Device Custom String 5	ObjectType
Device Custom String 6	Properties
Device NT Domain	SubjectDomainName
File ID	HandleId
File Name	ObjectName
File Type	ObjectType
Name	'An operation was performed on an object.'

Event Id 4663

Micro Focus 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)

Event Id 4664

Micro Focus 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

Event Id 4665

Micro Focus 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

Event Id 4666

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

Event Id 4667

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

Event Id 4668

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

Event Id 4670

Micro Focus 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

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

Event Id 4671

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

Event Id 4672

Micro Focus 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

Event Id 4673

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A privileged service was called.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination Process Name	ProcessName

Event Id 4674

Micro Focus 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

Event Id 4675

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

Event Id 4688

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A new process has been created.'
Destination User Name	One of (SubjectUserName, SubjectUserSid, TargetUserName, TargetUserSid)
Destination NT Domain	One of (SubjectDomainName, desinationNtDomain)

Micro Focus ArcSight ESM Field	Device-Specific Field
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.'

Event Id 4689

Micro Focus 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

Event Id 4690

Micro Focus 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

Event Id 4691

Micro Focus 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

Event Id 4692

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

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

Event Id 4693

Micro Focus 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

Event Id 4694

Micro Focus 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

Event Id 4695

Micro Focus 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

Event Id 4696

Micro Focus 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

Event Id 4697

Micro Focus 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

Event Id 4698

Micro Focus 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

Event Id 4699

Micro Focus 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

Event Id 4700

Micro Focus 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

Event Id 4701

Micro Focus 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

Event Id 4702

Micro Focus 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

Event Id 4703

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A token 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

Micro Focus 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 token right was adjusted.'

Event Id 4704

Micro Focus 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

Event Id 4705

Micro Focus 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

Event Id 4706

Micro Focus 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

Event Id 4707

Micro Focus 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

Event Id 4709

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

Event Id 4710

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

Event Id 4711

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

Event Id 4712

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

Event Id 4713

Micro Focus 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

Event Id 4714

Micro Focus 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))")
Destination User ID	SubjectLogonId

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

Event Id 4715

Micro Focus 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

Event Id 4716

Micro Focus 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

Event Id 4717

Micro Focus 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

Event Id 4718

Micro Focus 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

Event Id 4719

Micro Focus 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

Event Id 4720

Micro Focus 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

Event Id 4722

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

Micro Focus 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

Event Id 4723

Micro Focus 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

Event Id 4724

Micro Focus 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

Event Id 4725

Micro Focus 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

Event Id 4726

Micro Focus 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

Event Id 4727

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

Micro Focus 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

Event Id 4728

Micro Focus 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

Event Id 4729

Micro Focus 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
Source User ID	SubjectLogonId

Micro Focus ArcSight ESM Field	Device-Specific Field
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

Event Id 4730

Micro Focus 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

Event Id 4731

Micro Focus 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)
Destination NT Domain	SubjectDomainName

Micro Focus 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

Event Id 4732

Micro Focus 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

Event Id 4733

Micro Focus 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
Device Custom String 6	Both (TargetDomainName, TargetUserName)

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User ID	MemberName
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4734

Micro Focus 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

Event Id 4735

Micro Focus 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)
Destination User ID	SubjectLogonId
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4737

Micro Focus 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

Event Id 4738

Micro Focus 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)
Device Custom String 6	UserAccountControl (Change in User Account Control)
Device NT Domain	SubjectDomainName
Destination User Privileges	PrivilegeList

Event Id 4739

Micro Focus 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

Event Id 4740

Micro Focus 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

Event Id 4741

Micro Focus 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

Event Id 4742

Micro Focus 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
Device Custom Date1	PasswordLastSet
Device Custom Date1 Label	Password Last Set

Event Id 4743

Micro Focus 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

Event Id 4744

Micro Focus 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

Event Id 4745

Micro Focus 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

Event Id 4746

Micro Focus 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

Event Id 4747

Micro Focus 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

Event Id 4748

Micro Focus 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

Event Id 4749

Micro Focus 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

Event Id 4750

Micro Focus 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

Event Id 4751

Micro Focus 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

Event Id 4752

Micro Focus 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

Event Id 4753

Micro Focus 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

Event Id 4754

Micro Focus 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

Event Id 4755

Micro Focus 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

Event Id 4756

Micro Focus 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

Event Id 4757

Micro Focus 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

Event Id 4758

Micro Focus 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

Event Id 4759

Micro Focus 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

Event Id 4760

Micro Focus 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

Event Id 4761

Micro Focus 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

Event Id 4762

Micro Focus 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

Event Id 4763

Micro Focus 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

Event Id 4764

Micro Focus 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

Event Id 4765

Micro Focus 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

Event Id 4766

Micro Focus 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

Event Id 4767

Micro Focus 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

Event Id 4768

Micro Focus 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.'

Event Id 4769

Micro Focus 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
Device Custom String 5	TicketEncryptionType ("Ticket Encryption Type")
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.’
File Name	ServiceSid
Device Custom String 1	TicketOptions ("Ticket Options")

Event Id 4770

Micro Focus 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

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

Event Id 4771

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Kerberos pre-autheitication 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.'

Event Id 4772

Micro Focus 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."

Event Id 4773

Micro Focus 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.'

Event Id 4774

Micro Focus 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)

Event Id 4775

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

Event Id 4776

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

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

Event Id 4777

Micro Focus 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

Event Id 4778

Micro Focus 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.'

Event Id 4779

Micro Focus 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 Terminal Services session, or when a user switches away from an existing desktop using Fast User Switching.'

Event Id 4780

Micro Focus 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

Micro Focus 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.'

Event Id 4781

Micro Focus 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

Event Id 4782

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

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

Event Id 4783

Micro Focus 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

Event Id 4784

Micro Focus 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

Event Id 4785

Micro Focus 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

Event Id 4786

Micro Focus 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

Event Id 4787

Micro Focus 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.'

Event Id 4788

Micro Focus 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

Micro Focus 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.'

Event Id 4789

Micro Focus 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

Event Id 4790

Micro Focus 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

Event Id 4791

Micro Focus 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

Event Id 4792

Micro Focus 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

Event Id 4793

Micro Focus 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

Event Id 4794

Micro Focus 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

Event Id 4797

Micro Focus 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)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

Event Id 4798

Micro Focus 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.'

Event Id 4799

Micro Focus 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.'

Event Id 4800

Micro Focus 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

Event Id 4801

Micro Focus 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

Event Id 4802

Micro Focus 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

Event Id 4803

Micro Focus 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

Event Id 4816

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

Event Id 4817

Micro Focus 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

Event Id 4818

Micro Focus 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

Event Id 4819

Micro Focus 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

Event Id 4820

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A Kerberos Ticket-granting ticket \\(TGT\\) was denied because the devicwe does not meet the access control restrictions.'
Source User Name	TargetUserName

Micro Focus ArcSight ESM Field	Device-Specific Field
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.'

Event Id 4821

Micro Focus 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)
Source Address	IpAddress
Source User ID	LogonGuid
Device Custom String 5	SiloName
Device Custom String 6	PolicyName
Source Port	IpPort

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination Service Name	ServiceName
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.'

Event Id 4822

Micro Focus 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

Event Id 4823

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'NTLM authentication failed because access control restrictions are required.'
Reason	Status
Device Custom String 5	SiloName
Device Custom String 6	PolicyName
Device Custom String 4	Status
Destination User Name	AccountName

Event Id 4824

Micro Focus 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

Event Id 4826

Micro Focus 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
Additional data	KernelDebug
Additional data	VsmLaunchType
Additional data	TestSigning
Additional data	FlightSigning
Additional data	DisableIntegrityChecks

Micro Focus ArcSight ESM Field	Device-Specific Field
Additional data	HypervisorLoadOptions
Additional data	HypervisorLaunchType
Additional data	HypervisorDebug

Event Id 4864

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

Event Id 4865

Micro Focus 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

Event Id 4866

Micro Focus 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

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

Event Id 4867

Micro Focus 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

Event Id 4868

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The certificate manager denied a pending certificate request.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4869

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a resubmitted certificate request.'
Destination User ID	SubjectLogonId

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

Event Id 4870

Micro Focus 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

Event Id 4871

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services received a request to publish the certificate revocation list (CRL).'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4872

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

Event Id 4873

Micro Focus 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

Event Id 4874

Micro Focus 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

Event Id 4875

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Cerftificate 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

Event Id 4876

Micro Focus 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

Event Id 4877

Micro Focus 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

Event Id 4878

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

Event Id 4879

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

Event Id 4880

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

Event Id 4881

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

Event Id 4882

Micro Focus 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

Event Id 4883

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services retrieved an archived key.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4884

Micro Focus 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

Event Id 4885

Micro Focus 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

Event Id 4886

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

Event Id 4887

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

Event Id 4888

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

Event Id 4889

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

Event Id 4890

Micro Focus 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

Event Id 4891

Micro Focus 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

Event Id 4892

Micro Focus 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

Event Id 4893

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

Event Id 4894

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

Event Id 4895

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

Event Id 4896

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'One or more rows have been deleted from the certificate database.'
Destination User ID	SubjectLogonId

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

Event Id 4897

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

Event Id 4898

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

Event Id 4899

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

Event Id 4900

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

Event Id 4902

Micro Focus 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

Event Id 4904

Micro Focus 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

Event Id 4905

Micro Focus 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

Event Id 4906

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

Event Id 4907

Micro Focus 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
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 4908

Micro Focus 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.'

Event Id 4909

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

Event Id 4910

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

Event Id 4911

Micro Focus 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
Destination User ID	SubjectLogonId
File ID	HandleId
File Name	ObjectName
File Type	ObjectType
Destination Process ID	ProcessId
Destination Process Name	ProcessName

Event Id 4912

Micro Focus 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

Event Id 4913

Micro Focus 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
File Type	ObjectType
Destination process ID	ProcessId
Destination process Name	ProcessName

Event Id 4928

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

Event Id 4929

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

Event Id 4930

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

Event Id 4931

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

Event Id 4932

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

Event Id 4933

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

Event Id 4934

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

Event Id 4935

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

Event Id 4936

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

Event Id 4937

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

Event Id 4944

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

Event Id 4945

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

Event Id 4946

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

Event Id 4947

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

Event Id 4948

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

Event Id 4949

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

Event Id 4950

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom String 4	SettingType
Device Custom String 5	SettingValue
Name	'A Windows Firewall setting has changed.'

Event Id 4951

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

Event Id 4952

Micro Focus 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.'

Event Id 4953

Micro Focus 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

Event Id 4954

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

Event Id 4956

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

Event Id 4957

Micro Focus 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)

Event Id 4958

Micro Focus 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

Event Id 4960

Micro Focus 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.'

Event Id 4961

Micro Focus 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.'

Event Id 4962

Micro Focus 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.'

Event Id 4963

Micro Focus 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.'

Event Id 4964

Micro Focus 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

Event Id 4965

Micro Focus 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 interoperabiolity problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.'

Event Id 4976

Micro Focus 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

Event Id 4977

Micro Focus 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

Event Id 4978

Micro Focus 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

Event Id 4979

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

Event Id 4980

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

Event Id 4981

Micro Focus 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

Event Id 4982

Micro Focus 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

Event Id 4983

Micro Focus 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

Event Id 4984

Micro Focus 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

Event Id 4985

Micro Focus 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

Event Id 5024

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

Event Id 5025

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

Event Id 5027

Micro Focus 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

Event Id 5028

Micro Focus 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

Event Id 5029

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

Event Id 5030

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

Event Id 5031

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

Event Id 5032

Micro Focus 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

Event Id 5033

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

Event Id 5034

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

Event Id 5035

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

Event Id 5037

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

Event Id 5038

Micro Focus 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.'

Event Id 5039

Micro Focus 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

Event Id 5040

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

Event Id 5041

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

Event Id 5042

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

Event Id 5043

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

Event Id 5044

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

Event Id 5045

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

Event Id 5046

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

Event Id 5047

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

Event Id 5048

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

Event Id 5049

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

Event Id 5050

Micro Focus 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.'

Event Id 5051

Micro Focus 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

Event Id 5056

Micro Focus 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

Event Id 5057

Micro Focus 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

Event Id 5058

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'Key file operation.'
File Name	KeyName
File Type	KeyType
File Path	KeyFilePath
Device Action	Operation
Device Custom Date 1	ClientCreationTime
Device Custom String 1	ProviderName
Device Custom String 3	AlogorithmName
Device Custom String 4	ReturnCode
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Source Process Id	ClientProcessId

Event Id 5059

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

Event Id 5060

Micro Focus 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

Event Id 5061

Micro Focus 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

Event Id 5062

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

Event Id 5063

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

Event Id 5064

Micro Focus 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

Event Id 5065

Micro Focus 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

Event Id 5066

Micro Focus 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

Event Id 5067

Micro Focus 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

Event Id 5068

Micro Focus 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

Event Id 5069

Micro Focus 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

Event Id 5070

Micro Focus 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

Event Id 5071

Micro Focus 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

Event Id 5120

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

Event Id 5121

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

Event Id 5122

Micro Focus 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

Event Id 5123

Micro Focus 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

Event Id 5124

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

Event Id 5125

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

Event Id 5126

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

Event Id 5127

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

Event Id 5136

Micro Focus 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)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Device Custom String 4	OperationType

Event Id 5137

Micro Focus 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

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

Event Id 5138

Micro Focus 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

Event Id 5139

Micro Focus 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

Event Id 5140

Micro Focus 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

Event Id 5141

Micro Focus 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	SubjetDomainName
Device NT Domain	SubjectDomainName

Event Id 5142

Micro Focus 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

Event Id 5143

Micro Focus 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)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId

Event Id 5144

Micro Focus 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)

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

Event Id 5145

Micro Focus 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
Device Custom String 6	ShareName
File Path	ShareLocalPath
File Name	RelativeTargetName
File Type	ObjectType

Event Id 5146

Micro Focus 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)

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination Address	DestAddress
Device Custom IPv6 Address 3	DestAddress (Destination IPv6 Address)
Source Port	SourceSwitchPort
Destination Port	DestinationvSwitchPort

Event Id 5147

Micro Focus 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

Event Id 5152

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform blocked a packet.'
Source Address	SourceAddress
Source Port	SourcePort
Destination Address	DestAddress
Destination Port	DestPort
File Name	Application
File Path	Application
File Type	Application

Event Id 5153

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'A more restrictive Windows Filtering Platform filter has blocked a packet.'
Source Port	SourcePort
Destination Port	DestPort
File Name	Application
File Path	Application
File Type	Application

Event Id 5154

Micro Focus 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
File Name	Application
File Path	Application
File Type	Application

Event Id 5155

Micro Focus 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
File Name	Application
File Path	Application
File Type	Application

Event Id 5156

Micro Focus 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
File Name	Application
File Path	Application
File Type	Application

Event Id 5157

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform has blocked a connection.'
Source Port	SourcePort
Destination Port	DestPort
File Name	Application
File Path	Application
File Type	Application

Event Id 5158

Micro Focus 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
File Name	Application
File Path	Application
File Type	Application

Event Id 5159

Micro Focus 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

Event Id 5168

Micro Focus 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

Event Id 5376

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom Date 1	ProcessCreationTime
Device NT Domain	SubjectDomainName
File Path	BackupFileName
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.'
Name	'Credential Manager credentials were backed up.'
Source Process ID	ClientProcessId

Event Id 5377

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	ProcessCreationTime
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
File Path	BackupFileName
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.'
Name	'Credential Manager credentials were restored from a backup.'
Source Process ID	ClientProcessId

Event Id 5378

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'The requested credentials delegation was disallowed by policy.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event Id 5379

Micro Focus ArcSight ESM Field	Device-Specific Field
Destination Process Name	TargetName
Device Custom Date 1	ProcessCreationTime
Device Custom Number 1	Type

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	CountOfCredentialsReturned
Device Custom String 3	ReadOperation
Reason	ReturnCode
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName or SubjectUserSid
Source User Id	SubjectLogonId
Source Process Id	ClientProcessId

Event Id 5380

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	ProcessCreationTime
Device Custom Number 2	CountOfCredentialsReturned
Device Custom String 4	SchemaFriendlyName
Request Context	SearchString
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName or SubjectUserSid
Source User Id	SubjectLogonId
Source Process Id	ClientProcessId

Event Id 5381

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	ProcessCreationTime
Device Custom Number 2	CountOfCredentialsReturned
Device Custom Number 3	Flags
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName or SubjectUserSid
Source User Id	SubjectLogonId
Source Process Id	ClientProcessId

Event Id 5382

Micro Focus ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	ProcessCreationTime
Device Custom Number 3	Flags
Device Custom String 4	SchemaFriendlyName
Device Custom String 5	PackageSid
Device Custom String 6	Identity
Reason	ReturnCode
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName or SubjectUserSid
Source User Id	SubjectLogonId
Source Process Id	ClientProcessId

Event Id 5440

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

Event Id 5441

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

Event Id 5442

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

Event Id 5443

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

Event Id 5444

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

Event Id 5446

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

Event Id 5447

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

Event Id 5448

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

Event Id 5449

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

Event Id 5450

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

Event Id 5451

Micro Focus 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

Event Id 5452

Micro Focus 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

Event Id 5453

Micro Focus 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.'

Event Id 5456

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine applied Active Directory storage IPsec policy on the computer.'

Event Id 5457

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

Event Id 5458

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

Event Id 5459

Micro Focus 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

Event Id 5460

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine applied local registry storage IPsec policy on the computer.'

Event Id 5461

Micro Focus 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

Event Id 5462

Micro Focus 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

Event Id 5463

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

Event Id 5464

Micro Focus 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.'

Event Id 5465

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

Event Id 5466

Micro Focus 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.'

Event Id 5467

Micro Focus 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.'

Event Id 5468

Micro Focus 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.'

Event Id 5471

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine loaded local storage IPsec policy on the computer.'

Event Id 5472

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

Event Id 5473

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine loaded directory storage IPsec policy on the computer.'

Event Id 5474

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

Event Id 5477

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

Event Id 5478

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

Event Id 5479

Micro Focus 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.'

Event Id 5480

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services fialed 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.'

Event Id 5483

Micro Focus 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

Event Id 5484

Micro Focus 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

Event Id 5632

Micro Focus 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)

Event Id 5633

Micro Focus 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)

Event Id 5712

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

Event Id 5888

Micro Focus 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

Event Id 5889

Micro Focus 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.'

Event Id 5890

Micro Focus 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

Event Id 6144

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

Event Id 6145

Micro Focus ArcSight ESM Field	Device-Specific Field
Name	'One or more errors occurred while processing security policy I nthe group policy objects.'
Device Custom String 4	ErrorCode

Event Id 6272

Micro Focus 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

Micro Focus ArcSight ESM Field	Device-Specific Field
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

Event Id 6273

Micro Focus 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

Event Id 6274

Micro Focus 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.'

Event Id 6275

Micro Focus 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.'

Event Id 6276

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

Event Id 6277

Micro Focus 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.'

Event Id 6278

Micro Focus 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

Micro Focus ArcSight ESM Field	Device-Specific Field
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

Event Id 6279

Micro Focus 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

Event Id 6280

Micro Focus 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

Event Id 6281

Micro Focus 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.'

Event Id 6409

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

Event Id 6410

Micro Focus 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

Event Id 6416

Micro Focus 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

Micro Focus ArcSight ESM Field	Device-Specific Field
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.'

Event Id 8191

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

Mappings for Microsoft OAlerts

Event Id 300

ArcSight ESM Field	Device-Specific Field
Name	Microsoft Office Alerts
Device Product	OAlerts
File Type	%1
Message	%2
Device Version	%4

Mappings for DNS Client Operational

Event Id 1015

ArcSight Field	Vendor Field
Name	"Name resolution timed out after the DNS server did not respond"
Device Custom String 1	QueryName
Destination Address	Address
Destination Port	Address

Event Id 1016

ArcSight Field	Vendor Field
Name	"A name not found error was returned"
Device Custom String 1	QueryName
Destination Address	Address
Destination Port	Address

Event Id 1017

ArcSight Field	Vendor Field
Name	"The DNS server's response to a query"
Device Custom String 1	QueryName
Destination Address	Address
Destination Port	Address

Event Id 3006

ArcSight Field	Vendor Field
Name	"DNS query is called"
Device Custom String 1	QueryName
Device Custom String 5	ServerList
Device Custom Number 1	QueryType
Device Custom Number 2	QueryOptions
Device Custom Number 3	InterfaceIndex

Event Id 3008

ArcSight Field	Vendor Field
Name	"DNS query is completed"
Device Custom String 1	QueryName
Device Custom String 3	QueryResults
Device Custom Number 1	QueryType
Device Custom Number 2	QueryOptions
Device Custom Number 3	QueryStatus

Event Id 3009

ArcSight Field	Vendor Field
Name	"Network query initiated"
Device Custom String 1	QueryName
Device Custom String 4	AdapterName
Device Custom Number 1	InterfaceCount
Device Custom Number 2	NetworkIndex
Device Custom String 6	LocalAddress
Device Dns Domain	DNSServerAddress

Event Id 3010

ArcSight Field	Vendor Field
Name	"DNS Query sent to DNS Server"
Device Custom String 1	QueryName
Device Custom Number 1	QueryType
Device Dns Domain	DnsServerIpAddress

Event Id 3011

ArcSight Field	Vendor Field
Name	"Received response from DNS Server"
Device Custom String 1	QueryName
Device Custom Number 1	QueryType
Device Dns Domain	DnsServerIpAddress
Event Outcome	ResponseStatus

Event Id 3012

ArcSight Field	Vendor Field
Name	"NETBIOS query is initiated"
Device Custom String 1	QueryName
Device Custom String 4	AdapterName
Device Custom Number 1	InterfaceCount
Device Custom Number 2	NetworkIndex
Device Custom String 6	LocalAddress

Event Id 3013

ArcSight Field	Vendor Field
Name	"NETBIOS query is completed"
Device Custom String 1	QueryName
Device Custom String 3	QueryResults
Event Outcome	Status

Event Id 3014

ArcSight Field	Vendor Field
Name	"NETBIOS query is pending"
Device Custom String 1	QueryName

Event Id 3016

ArcSight Field	Vendor Field
Name	"Cache lookup called"
Device Custom String 1	QueryName
Device Custom Number 2	QueryType
Device Custom Number 3	InterfaceIndex

Event Id 3018

ArcSight Field	Vendor Field
Name	"Cache lookup for name"
Device Custom String 1	QueryName
Device Custom String 3	QueryResults
Device Custom Number 1	QueryType
Device Custom Number 2	QueryOptions

Event Id 3019

ArcSight Field	Vendor Field
Name	"Query wire called"
Device Custom String 1	QueryName
Device Custom Number 1	QueryType
Device Custom Number 2	NetworkIndex
Device Custom Number 3	InterfaceIndex

Event Id 3020

ArcSight Field	Vendor Field
Name	"Query response for name"
Device Custom String 1	QueryName
Device Custom String 3	QueryResults
Device Custom Number 1	QueryType
Device Custom Number 2	NetworkIndex
Device Custom Number 3	InterfaceIndex
Event Outcome	Status

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.

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.
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.

Category	Subcategory	ID	Message Summary
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.

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.
	Process Creation	4688	A new process has been created.
		4696	A primary token was assigned to process.
	Process Termination	4689	A process has exited.
	RPC Events	5712	A Remote Procedure Call (RPC) was attempted.

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	
		4983	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.

Category	Subcategory	ID	Message Summary
		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.

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.

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.

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.

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.

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.
	File Share	5140	A network share object was accessed.
		5142	A network share object was added.
		5143	A network share object was modified.
		5144	A network share object was deleted.
		5168	Spn check for SMB/SMB2 failed.
	File System	4664	An attempt was made to create a hard link.
		4985	The state of a transaction has changed.
		5051	A file was virtualized.
	Filtering Platform Connection	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
		5146	The Windows Filtering Platform has blocked a packet.
		5147	A more restrictive Windows Filtering Platform filter has blocked a packet.
		5150	The Windows Filtering Platform has blocked a packet.
		5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
		5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
		5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
		5156	The Windows Filtering Platform has allowed a connection.
		5157	The Windows Filtering Platform has blocked a connection.
		5158	The Windows Filtering Platform has permitted a bind to a local port.
		5159	The Windows Filtering Platform has blocked a bind to a local port.
Object Access	Filtering Platform Packet Drop	5152	The Windows Filtering Platform blocked a packet.
		5153	A more restrictive Windows Filtering Platform filter has blocked a packet.
Object Access	Handle Manipulation	4656	A handle to an object was requested.
		4658	The handle to an object was closed.
		4690	An attempt was made to duplicate a handle to an object.

Category	Subcategory	ID	Message Summary
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.

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 token 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.

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

Category	Subcategory	ID	Message Summary
Policy Change	Filtering Platform Policy Change	4712	IPsec Services encountered a potentially serious failure.
		5040	A change has been made to IPsec settings. An Authentication Set was added.
		5041	A change has been made to IPsec settings. An Authentication Set was modified.
		5042	A change has been made to IPsec settings. An Authentication Set was deleted.
		5043	A change has been made to IPsec settings. A Connection Security Rule was added.
		5044	A change has been made to IPsec settings. A Connection Security Rule was modified.
		5045	A change has been made to IPsec settings. A Connection Security Rule was deleted.
		5046	A change has been made to IPsec settings. A Crypto Set was added.
		5047	A change has been made to IPsec settings. A Crypto Set was modified.
		5048	A change has been made to IPsec settings. A Crypto Set was deleted.
Policy Change	Filtering Platform Policy Change	5440	The following callout was present when the Windows Filtering Platform Base Filtering Engine started.
		5441	The following filter was present when the Windows Filtering Platform Base Filtering Engine started.
		5442	The following provider was present when the Windows Filtering Platform Base Filtering Engine started.
		5443	The following provider context was present when the Windows Filtering Platform Base Filtering Engine started.
		5444	The following sub-layer was present when the Windows Filtering Platform Base Filtering Engine started.
		5446	A Windows Filtering Platform callout has been changed.
Policy Change	Filtering Platform Policy Change	5448	A Windows Filtering Platform provider has been changed.
		5449	A Windows Filtering Platform provider context has been changed.

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.

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.

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:

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.
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.

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

Category	Subcategory	ID	Message Summary
System	Other System Events	4823	NTLM authentication failed because access control restrictions are required.
		4824	Kerberos preauthenti9cation by using DES or RC4 failed bedause 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.

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.

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 Event Mappings (Connectors 8.2.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!