Security Event Mappings

SmartConnectors™ for Microsoft Windows Event Log – Unified

With Parser Version 1

June 30, 2012

ArcSight
An HP Company

HP ArcSight SmartConnectors for Microsoft Windows Event Log Security Event Mappings

June 30, 2012

Revision History

Date	Description
06/30/2012	Updates to security event mappings and introduction of parser versions. Updated mappings for Windows Security Events 528, 529, 530, 531, 532, 533, 535, 536, 537, 539, 540, 4624, 4625. Rebranded for HP ArcSight. Added Parser Version section.
11/15/2010	Added mappings for Security Event 5145.
05/26/2010	Added Device Custom String 4 mapping for Security Event 5136.
03/31/2010	Added mappings for Security Event 536.
02/11/2010	Added mappings for Microsoft Windows Server 2008/Vista security events. Updated mappings: Source Host Name is now mapped to Workstation Name and Source Network Address for Security Events 529, 530, 531, 532, 533, 534, 535, 537, and 539. Mapping for Source NT Domain has been added to Security Event 675.
08/21/2009	Added mappings for security events 516, 627, and 629. Revised mappings for security event 643.
03/27/2009	Updated mappings for Windows Security Events 537, 608, 642, and 680.
02/11/2009	Updated mappings for Windows Security Events 520, 529, 537, 592, 672, 675, 631, 620, 672
05/12/2008	Updated "Overview of Security Events Mapped to ArcSight ESM;" to add overall mapping for Windows field **Port number** mapped to ArcSight **Target Port** field. Added Target Port/Port Number to Security Event 861. Removed redundant Destination User Name mappings.
02/14/2008	Updated mappings for Windows Security Events 637 and 680. Added mappings for Windows Security Events 682 and 683.
12/18/2007	Added mappings for Windows Security Event 641.
11/12/2007	Updated mapping definition for User Right/Destination User Privilege for security event 608. Updated overview of fields mapped to ArcSight ESM.
08/15/2007	Updated "Overview of Security Events Mapped to ArcSight ESM;" for Device Custom String 6, Destination NT Domain, and Source NT Domain. Updated event 632 for Device Custom String 6; mapped to Member Name rather than Member ID.

Contents

About This Book

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

See the *SmartConnector for Microsoft Windows Event Log – Unified Configuration Guide* for the following information:

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

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

Default Windows Event Logs

There are three default Windows event logs:

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

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

System administrators use the Windows Event Log for troubleshooting errors. Each entry in the event log can have a severity of **Error**, **Warning**, **Information**. and **Success** or **Failure** audit.

SmartConnectors for Microsoft Windows Event Log

There are three SmartConnectors for Microsoft Windows Event Log:

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

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

- **SmartConnector for Microsoft Windows Event Log – Local**, which collects events from the Windows Event Log on your local machine. This connector supports event collection from Microsoft Windows XP/2000.
- **SmartConnector for Microsoft Windows Event Log – Domain**, which lets you collect Microsoft Windows Event Log events from multiple remote machines and forward them into the ArcSight system (such as multiple occurrences of the same application installed on different machines in one domain). This connector supports event collection from Microsoft Windows XP/2000/2003.

Parser Versions

A parser is a SmartConnector component that specifies how to parse the information contained in the device raw events, and how to map it to HP ArcSight security event schema fields. Parsers can be in the form of property files, map files, or CSV files. Each SmartConnector has its own parser or set of parsers.

Multiple parser versions lets each SmartConnector parse raw events in many different ways to generate ArcSight security events with appropriate mappings. For the SmartConnector for Microsoft Windows Event Log -- Unified, two parser versions are supported: Base Parser and Parser Version 1. In this document, variations between the two parser versions are highlighted in blue in the mappings tables. Values that are not used are indicated with a dash (—).

With multiple parser versions:

- One SmartConnector build supports multiple parser versions.
- Users can configure their connectors to use the available parser versions of their choice, depending on their event mapping requirements.
- Users can reconfigure connectors to use the appropriate parser version as needed.

Multiple parser versions currently are supported only for the SmartConnector for Microsoft Windows Event Log -- Unified. This functionality is not supported for user-developed HP ArcSight FlexConnectors.

Using Parser Versions

Each SmartConnector has its own internal `fcp.version` parameter setting to represent its current parser version. The default value for the `fcp.version` parameter is the base (or default) parser version, which is Parser Version 0. Each SmartConnector can support a total of 8 parser versions. The `fcp.version` parameter values range from 0 through 7. For the Microsoft Windows Unified SmartConnector, parser versions 0 and 1 are supported.

Be sure that when you have content with new mappings, you change the parser version to match that content.

To change parser versions:

1. From the `$ARCSIGHT_HOME\current\user\agent` directory, open the file `agent.properties` in an editor.
2. In the `agent.properties` file, locate the `fcp.version` parameter:

   ```
   agents[0].fcp.version=0
   ```

3. The default value for the `fcp.version` parameter is `0`, which designates the base parser. To use parser 1, change the `fcp.version` parameter value to `1`. For example:

   ```
   agents[0].fcp.version=1
   ```

4. Save and exit the `agent.properties` file.
5. Restart the connector.

Reconfiguring Parser Versions

After installing a connector, you can reconfigure it to use a different parser version as needed by changing the value of the `fcp.version` parameter for an installed connector.

Differentiating Event Output Between Parser Versions

The HP ArcSight security event output from the SmartConnector will differ from one parser version to another. The last digit of the Agent Version field of the ArcSight security event listed in the Console identifies the parser version with which a raw event was parsed, and you can use data in this field to verify the parser version used. The Agent Version field is the only field that identifies the parser version.

For example, for a raw event parsed by SmartConnector build 5.1.7.6076.0, the Agent Version field of the ArcSight security event will list this data in the Console:

- For Parser Version 0, the Agent Version will be 5.1.7.6076.0
- For Parser Version 1, the Agent Version will be 5.1.7.6076.1

Windows Vista and 2008 Event Descriptions

Event ID	Description
1100	The event logging service has shut down
1101	Audit events have been dropped by the transport.
1102	The audit log was cleared
1104	The security Log is now full
1105	Event log automatic backup
1108	The event logging service encountered an error
1866	The Intersite Messaging service received extended error string information from LDAP
4608	Windows is starting up
4609	Windows is shutting down
4610	An authentication package has been loaded by the Local Security Authority
4611	A trusted logon process has been registered with the Local Security Authority
4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
4614	A notification package has been loaded by the Security Account Manager.
4615	Invalid use of LPC port
4616	The system time was changed.
4618	A monitored security event pattern has occurred
4621	Administrator recovered system from CrashOnAuditFail
4622	A security package has been loaded by the Local Security Authority.
4624	An account was successfully logged on
4625	An account failed to log on
4634	An account was logged off
4646	1.00%
4647	User initiated logoff
4648	A logon was attempted using explicit credentials
4649	A replay attack was detected
4650	An IPsec Main Mode security association was established
4651	An IPsec Main Mode security association was established
4652	An IPsec Main Mode negotiation failed
4653	An IPsec Main Mode negotiation failed
4654	An IPsec Quick Mode negotiation failed
4655	An IPsec Main Mode security association ended
4656	A handle to an object was requested

Event ID	Description
4657	A registry value was modified
4658	The handle to an object was closed
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
4662	An operation was performed on an object
4663	An attempt was made to access an object
4664	An attempt was made to create a hard link
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
4670	Permissions on an object were changed
4671	An application attempted to access a blocked ordinal through the TBS
4672	Special privileges assigned to new logon
4673	A privileged service was called
4674	An operation was attempted on a privileged object
4675	SIDs were filtered
4685	The state of a transaction has changed
4688	A new process has been created
4689	A process has exited
4690	An attempt was made to duplicate a handle to an object
4691	Indirect access to an object was requested
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
4696	A primary token was assigned to process
4697	A service was installed in the system
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
4704	A user right was assigned

Event ID	Description
4705	A user right was removed
4706	A new trust was created to a domain
4707	A trust to a domain was removed
4709	IPsec Services was started
4710	IPsec Services was disabled
4711	PAStore Engine (1%)
4712	IPsec Services encountered a potentially serious failure
4713	Kerberos policy was changed
4714	Encrypted data recovery policy was changed
4715	The audit policy (SACL) on an object 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
4719	System audit policy was changed
4720	A user account was created
4722	A user account was enabled
4723	An attempt was made to change an account's password
4724	An attempt was made to reset an accounts password
4725	A user account was disabled
4726	A user account was deleted
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
4738	A user account was changed
4739	Domain Policy was changed
4740	A user account was locked out
4741	A computer account was created
4742	A computer account was changed

Event ID	Description
4743	A computer account was deleted
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
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
4758	A security-enabled universal 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
4764	A groups type was changed
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
4768	A Kerberos authentication ticket (TGT) was requested
4769	A Kerberos service ticket was requested
4770	A Kerberos service ticket was renewed
4771	Kerberos pre-authentication failed
4772	A Kerberos authentication ticket request failed
4773	A Kerberos service ticket request failed
4774	An account was mapped for logon
4775	An account could not be mapped for logon
4776	The domain controller attempted to validate the credentials for an account
4777	The domain controller failed to validate the credentials for an account

Event ID	Description
4778	A session was reconnected to a Window Station
4779	A session was disconnected from a Window Station
4780	The ACL was set on accounts which are members of administrators groups
4781	The name of an account was changed
4782	The password hash an account was accessed
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
4791	A basic application group was changed
4792	An LDAP query group was deleted
4793	The Password Policy Checking API was called
4794	An attempt was made to set the Directory Services Restore Mode administrator password
4800	The workstation was locked
4801	The workstation was unlocked
4802	The screen saver was invoked
4803	The screen saver was dismissed
4816	RPC detected an integrity violation while decrypting an incoming message
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
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
4875	Certificate Services received a request to shut down
4876	Certificate Services backup started
4877	Certificate Services backup completed

Event ID	Description
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
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
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
4899	A Certificate Services template was updated
4900	Certificate Services template security was updated
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
4909	The local policy settings for the TBS were changed
4910	The group policy settings for the TBS were changed
4912	Per User Audit Policy was changed
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

Event ID	Description
4931	An Active Directory replica destination naming context was modified
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
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
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
4953	A rule has been ignored by Windows Firewall because it could not parse the rule
4954	Windows Firewall Group Policy settings has 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
4960	IPsec dropped an inbound packet that failed an integrity check
4961	IPsec dropped an inbound packet that failed a replay check
4962	IPsec dropped an inbound packet that failed a replay check
4963	IPsec dropped an inbound clear text packet that should have been secured
4964	Special groups have been assigned to a new logon
4965	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI).
4976	During Main Mode negotiation, IPsec received an invalid negotiation packet.
4977	During Quick Mode negotiation, IPsec received an invalid negotiation packet.
4978	During Extended Mode negotiation, IPsec received an invalid negotiation packet.
4979	IPsec Main Mode and Extended Mode security associations were established.
4980	IPsec Main Mode and Extended Mode security associations were established
4981	IPsec Main Mode and Extended Mode security associations were established
4982	IPsec Main Mode and Extended Mode security associations were established

Event ID	Description
4983	An IPsec Extended Mode negotiation failed
4984	An IPsec Extended Mode negotiation failed
4985	The state of a transaction has changed
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
5028	The Windows Firewall Service was unable to parse the new security policy.
5029	The Windows Firewall Service failed to initialize the driver
5030	The Windows Firewall Service failed to start
5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
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
5038	Code integrity determined that the image hash of a file is not valid
5039	A registry key was virtualized.
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
5049	An IPsec Security Association was deleted
5050	An attempt to programmatically disable the Windows Firewall using a call to INetFwProfile.FirewallEnabled(FALSE
5051	A file was virtualized
5056	A cryptographic self test was performed
5057	A cryptographic primitive operation failed
5058	Key file operation
5059	Key migration operation
5060	Verification operation failed

Event ID	Description
5061	Cryptographic operation
5062	A kernel-mode cryptographic self test was performed
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 operation was attempted
5120	OCSP Responder Service Started
5121	OCSP Responder Service Stopped
5122	A Configuration entry changed in the OCSP Responder Service
5123	A configuration entry changed in the OCSP Responder Service
5124	A security setting was updated on OCSP Responder Service
5125	A request was submitted to OCSP Responder Service
5126	Signing Certificate was automatically updated by the OCSP Responder Service
5127	The OCSP Revocation Provider successfully updated the revocation information
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
5140	A network share object was accessed
5141	A directory service object was deleted
5145	A network share object was checked to see whether client can be granted desired access
5152	The Windows Filtering Platform blocked a packet
5153	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
5376	Credential Manager credentials were backed up

Event ID	Description
5377	Credential Manager credentials were restored from a backup
5378	The requested credentials delegation was disallowed by policy
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
5447	A Windows Filtering Platform filter has been changed
5448	A Windows Filtering Platform provider has been changed
5449	A Windows Filtering Platform provider context has been changed
5450	A Windows Filtering Platform sub-layer has been changed
5451	An IPsec Quick Mode security association was established
5452	An IPsec Quick Mode security association ended
5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started
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
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
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
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

Event ID	Description
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
5478	IPsec Services has started successfully
5479	IPsec Services has been shut down successfully
5480	IPsec Services failed to get the complete list of network interfaces on the computer
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
5485	IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces
5632	A request was made to authenticate to a wireless network
5633	A request was made to authenticate to a wired network
5712	A Remote Procedure Call (RPC) was attempted
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
6144	Security policy in the group policy objects has been applied successfully
6145	One or more errors occured while processing security policy in the group policy objects
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
8222	No fax devices were found

Windows Vista/2008/2008R2/7 Common Security Mappings

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Agent (Connector) Severity	High when Device Severity = Audit Failure Medium when Device Severity = Error or Warning; Low when Device Severity = Information or Audit Success:	High when Device Severity = Audit Failure 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)	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)	One of (Domain Name, Subject:Account Domain, New Token Information:Account Domain, Subject:Domain Name)
Destination Port	Network Information:Destination Port	Network Information:Destination Port
Destination Process Name	One of (Process Information:New Process Name, Process Information:Process Name)	One of (Process Information:New Process Name, Process Information:Process Name)
Destination Service Name	Service Information:Service Name	Service Information:Service Name
Destination User ID	One of (Subject:Logon ID, New Token Information:Logon 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)	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)	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)	One of (Account Action, Allowed)
Device Custom IPv6 Address 2	—.	One of (Network Information:Source Network Address, Local Network Address, Additional Information:Client Address, Network Information:Network Address, Network Information:Source Address, Client Machine:Calling Station Identifier, Network Information:Client Address)
Device Custom Number 1	Logon Type	Logon Type
Device Custom Number 3	Count	Count
Device Custom String 1	One of (Access Request Information:Access Mask, Operation: Accesses, Operation:Access Mask)	One of (Access Request Information:Access Mask, Operation: Accesses, Operation:Access Mask)
Device Custom String 2	Event Category	Event Category
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)	—

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 5	One of (Authentication Package Name, authentication Package, authentication, Detailed Authentication Information:authentication Package)	One of (Authentication Package Name, authentication Package, authentication, Detailed Authentication Information:authentication Package)
Device Event Category	Event log Type	Event log Type
Device Event Class ID	Event Source plus Event ID	Event Source plus Event ID
Device Host Name	One of (Additional Information: Caller Computer Name, Computer Name)	One of (Additional Information:Caller Computer Name, Computer Name)
Device NT Domain	One of (Domain Name, Subject:Account Domain)	One of (Domain Name, Subject:Account Domain)
Device Product	'Microsoft Windows'	'Microsoft Windows'
Device Receipt Time	Detect Time	Detect Time
Device Severity	Event Type	Event Type
Device Vendor	'Microsoft'	'Microsoft'
Event OutCome	—	One of (Event Type, Process Information:Exit Status)
External ID	Event ID	Event ID
File ID	One of (Object Handle ID, Object:Object Handle)	One of (Object Handle ID, Object:Object Handle)
File Name	Object:Object Name	Object:Object Name
File Type	One of (Object Type, Object:Object Type)	One of (Object Type, Object:Object Type)
Message	Message	Message
Name	Description	Description
Reason	—	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)
Source Address	One of (Network Information:Source Network Address, Local Network Address, Additional Information:Client 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)	One of (Source Workstation,Network Information:Workstation Name)
Source NT Domain	Subject:Client Domain	Subject:Client Domain
Source Port	One of (Network Information:Source Port, Network Information:Port, Network Information:Client Port)	One of (Network Information:Source Port, Network Information:Port, Network Information:Client Port)

Specific 2008 Windows Security Event Mappings

For descriptions of all Windows/Vista security events, see "Windows Vista and 2008 Event Descriptions" later in this document.

Account Logon

Credential Validation

Security events 4774, 4775, 4776, 4777

4774 An account was mapped for logon.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	Mapped Name	Mapped Name

4775 An account could not be mapped for logon.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	Account Name	Account Name

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	Logon Account	Logon Account

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	Logon Account	Logon Account
Reason	Error Code	Error Code

Kerberos Authentication Service

Security events 4768, 4771, 4772

4768 A Kerberos authentication ticket (TGT) was requested.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	One of (Network Information:Client Address, 'Client Address')	—
Reason	—	Additional Information:Result
Destination User Name	Account Information:Account Name	Account Information:Account Name
Destination NT Domain	Account Information:Supplied Realm Name	Account Information:Supplied Realm Name
Device Custom String 4	Additional Information:Result Code	—
Device Custom String 5	Additional Information:Pre-Authentication Type	Additional Information:Pre-Authentication Type
Source Address	Network Information:Client Address	Network Information:Client Address

4771 Kerberos pre-authentication failed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Network Information:Client Address	—
Destination User Name	Account Information:Account Name	Account Information:Account Name
Destination NT Domain	Account Information:Security ID	Account Information:Security ID
Destination Service Name	Service Information:Service Name	Service Information:Service Name
Reason	Additional Information:Failure Code	Additional Information:Failure Code

4772 A Kerberos Authentication ticket request failed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Network Information:Client Address	—

Kerberos Service Ticket Operations

Security events 4769, 4770, 4773

4769 A Kerberos service ticket was requested.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	One of (Network Information:Client Address, 'Client Address')	—
Destination User Name	Account Information:Account Name	Account Information:Account Name
Destination NT Domain	Account Information:Account Domain	Account Information:Account Domain
Destination Service Name	Service Information:Service Name	Service Information:Service Name
Device Custom String 6	Account Information:Logon GUID	Account Information:Logon GUID
Source Address	Network Information:Client Address	Network Information:Client Address

4770 A Kerberos service ticket was renewed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Network Information:Client Address	—
Destination User Name	Account Information:Account Name	Account Information:Account Name
Destination NT Domain	Account Information:Account Domain	Account Information:Account Domain
Destination Service Name	Service Information:Service Name	Service Information:Service Name

4773 A Kerberos service ticket request failed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Network Information:Client Address	—

Account Management

Application Group Management

Security events 4783, 4784, 4785, 4786, 4787, 4788, 4789, 4790, 4791, 4792

4785 A member was added to a basic application group.

4786 A member was removed from a basic application group.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	Subject:Account Name	Subject:Account Name
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	One of (Member:Security ID,Member:Account Name)	One of (Member:Security ID,Member:Account Name)
Device Custom String 6	Both (Group:Group Domain,Group:Group Name)	Both (Group:Group Domain,Group:Group Name)

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

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	Subject:Account Name	Subject:Account Name
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	One of (Member:Security ID,Member:Account Name)	One of (Member:Security ID,Member:Account Name)
Device Custom String 6	Both (Group:Account Domain, Group:Account Name)	Both (Group:Account Domain, Group:Account Name)

4783 A basic application group was created.

4784 A basic application group was changed.

4789 A basic application group was deleted.

4790 An LDAP query group was created.

4791 A basic application group was changed.

4792 An LDAP security group was deleted.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	Subject:Account Name	Subject:Account Name
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	One of (Group:Security ID, Group:Account Name)	One of (Group:Security ID, Group:Account Name)
Destination NT Domain	Group:Account Domain	Group:Account Domain

Computer Account Management

Security events 4741, 4742, 4743

4741 A computer account was created.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Device Custom String 6	Both (New Computer Account:Account Domain, New Computer Account:Account Name)	Both (New Computer Account:Account Domain, New Computer Account:Account Name)
Destination NT Domain	Subject:Account Domain	New Computer Account:Account Domain
Destination User Name	One of (Subject:Account Name, Subject:Security ID)	New Computer Account:Account Name

4742 A computer account was changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Device Custom String 6	Both (Computer Account That Was Changed:Account Domain, Computer Account That Was Changed:Account Name)	Both (Computer Account That Was Changed:Account Domain, Computer Account That Was Changed:Account Name)
Destination NT Domain	—	Computer Account That Was Changed: Account Domain
Destination User Name	One of (Subject:Account Name, Subject:Security ID)	Computer Account That Was Changed: Account Name

4743 A computer account was deleted.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Device Custom String 6	Both (Target Computer:Account Domain, Target Computer:Account Name)	Both (Target Computer:Account Domain, Target Computer:Account Name)
Destination NT Domain	Subject:Account Domain	Target Computer:Account Domain
Destination User Name	One of (Subject:Account Name, Subject:Security ID)	Target Computer:Account Name

Distribution Group Management

Security events 4744 – 4753, 4759 – 4762

4744 A security-disabled local group was created.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Device Custom String 6	Both (New Group:Group Domain, New Group:Group Name)	Both (New Group:Group Domain, New Group:Group Name)

4745 A security-disabled local group was changed.

4748 A security-disabled local group was deleted.

4749 A security-disabled global group was created.

4750 A security-disabled global group was changed.

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 deleted.

4760 A security-disabled universal group was changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)	Both (Group:Group Domain, Group:Group Name)

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

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

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID	extracted from Member:Security ID
Destination User ID	Member:Account Name	Member:Account Name
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)	Both (Group:Group Domain, Group:Group Name)

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Destination User Name	extracted from Member:Security ID	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID	extracted from Member:Security ID
Destination User ID	Member:Account Name	Member:Account Name
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)	Both (Group:Group Domain, Group:Group Name)

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	One of (Member:Security ID, Member:Account Name)	One of (Member:Security ID, Member:Account Name)
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)	Both (Group:Group Domain, Group:Group Name)

Other Account Management Events

Security events 4739, 4782, 4793

4739 Domain Policy was changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	—
Source NT Domain	Subject:Account Domain	Domain: Domain Name
Source User ID	Subject:Logon ID	—
Destination NT Domain	Domain: Domain Name	Subject:Account Domain
Message	Change Type	Change Type
Device Custom String 6	Both (Changed Attributes:Min. Password Age,Changed Attributes:Max. Password Age,Changed Attributes:Force Logoff,Changed Attributes:Lockout Threshold,Changed Attributes:Lockout Observation Window,Changed Attributes:Lockout Duration,Changed Attributes:Password Properties,Changed Attributes:Min. Password Length,Changed Attributes:Machine Account Quota,Changed Attributes:Mixed Domain Mode,Changed Attributes:Domain Behavior Version,Changed Attributes:OEM Information)	Both (Changed Attributes:Min. Password Age,Changed Attributes:Max. Password Age,Changed Attributes:Force Logoff,Changed Attributes:Lockout Threshold,Changed Attributes:Lockout Observation Window,Changed Attributes:Lockout Duration,Changed Attributes:Password Properties,Changed Attributes:Min. Password Length,Changed Attributes:Machine Account Quota,Changed Attributes:Mixed Domain Mode,Changed Attributes:Domain Behavior Version,Changed Attributes:OEM Information)

4782 The password hash account was accessed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	Subject:Account Name	Subject:Account Name
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	Target Account:Account Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain	Target Account:Account Domain

4793 The Password Policy Checking API was called.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source Host Name	Additional Information:Caller Workstation	Additional Information:Caller Workstation
Source User Name	Additional Information:Provided Account Name (unauthenticated)	Additional Information:Provided Account Name (unauthenticated)
Device Custom String 4	Additional Information:Status Code	—
Reason	—	Additional Information:Status Code

Security Group Management

Security events 4727 – 4735, 4737, 4754 – 4758, 4764

4730 A security-enabled global group was deleted.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Device Custom String 6	Both (Deleted Group:Group Domain, Deleted Group:Group Name)	Both (Deleted Group:Group Domain, Deleted Group:Group Name)

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.

4758 A security-enabled universal group was deleted.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)	Both (Group:Group Domain, Group:Group Name)

4727 A security-enabled global group was created.

4731 A security-enabled local group was created.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Device Custom String 6	Both (New Group:Group Domain, New Group:Group Name)	Both (New Group:Group Domain, New Group:Group Name)

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

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

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

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

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID	extracted from Member:Security ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)	Both (Group:Group Domain, Group:Group Name)
Destination User ID	Member:Account Name	Member:Account Name

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	extracted from Member:Security ID	extracted from Member:Security ID
Destination NT Domain	extracted from Member:Security ID	extracted from Member:Security ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)	Both (Group:Group Domain, Group:Group Name)

4764 A group's type was changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Device Custom String 6	Both (Group:Group Domain, Group:Group Name)	Both (Group:Group Domain, Group:Group Name)
Device Custom String 5	Change Type	Change Type

User Account Management

Security events 4720, 4722 – 4726, 4738, 4740, 4765, 4766, 4767, 4780, 4781

4720 A user account was created.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	Subject:Account Name	Subject:Account Name
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	New Account:Account Name	New Account:Account Name
Destination NT Domain	New Account:Account	New Account:Account

4722 A user account was enabled.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Security ID, Subject:Account Name)	One of (Subject:Security ID, Subject:Account Name)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	One of (Target Account:Security ID, Target Account:Account Name)	One of (Target Account:Security ID, Target Account:Account Name)
Destination NT Domain	Target Account:Account Domain	Target Account:Account Domain

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

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

4738 A user account was changed.

4767 A user account was unlocked.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	Target Account:Account Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain	Target Account:Account Domain

4725 A user account was disabled.

4726 A user account was deleted.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	Target Account:Account Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain	Target Account:Account Domain

4740 A user account was locked out.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	Account That Was Locked Out:Account Name	Account That Was Locked Out:Account Name
Source Host Name	Additional Information:Caller Computer Name	Additional Information:Caller Computer Name
Destination NT Domain	Account that was locked out: Security ID	Account that was locked out: Security ID

4765 SID History was added to an account.

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	Target Account:Account Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain	Target Account:Account Domain
Device Custom String 6	Source Account:Account Name	Source Account:Account Name

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	Subject:Account Name	Subject:Account Name
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	Target Account:Account Name	Target Account:Account Name
Destination NT Domain	Target Account:Account Domain	Target Account:Account Domain

4781 The name of an account was changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	Subject:Account Name	Subject:Account Name
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	Target Account:Old Account Name	Target Account:Old Account Name
Destination NT Domain	Target Account:Account Domain	Target Account:Account Domain
Device Custom String 6	Target Account:New Account Name	Target Account:New Account Name

Process Creation

Security events 4688, 4696

4688 A new process has been created.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Process Information:New Process ID	—
Device Custom String 5	Process Information:Creator Process ID	—
Destination Process ID	—	Process Information:New Process ID
Source Process ID	—	Process Information:Creator Process ID

4696 A primary token was assigned to process.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Target Process: Target Process ID	—
Destination Process Name	Target Process: Target Process Name	Target Process: Target Process Name
Source Process Name	Process Information:Process Name	Process Information:Process Name
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	One of (New Token Information: Account Name, New Token Information: Security ID)	One of (New Token Information: Account Name, New Token Information: Security ID)
Destination NT Domain	New Token Information: Account Domain	New Token Information: Account Domain
Destination User ID	New Token Information: Logon ID	New Token Information: Logon ID
Device Custom String 5	Process Information:Process ID	—
Destination Process ID	—	Target Process:Target Process ID
Source Process ID	—	Process Information:Process ID

Process Termination

Security events 4689, 4789

4689 A process has exited.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Process Information:Process ID	—
Destination Process ID	—	Process Information:Process ID

4789 A basic application group was deleted.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Process Information:Process ID	—
Source User Name	Subject:Account Name	Subject:Account Name
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	One of (Group:Security ID, Group:Account Name)	One of (Group:Security ID, Group:Account Name)
Destination NT Domain	Group:Account Domain	Group:Account Domain

DS Access

Directory Service Access

Security event 4662

4662 An operation was performed on an object.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 5	Object:Object Type	Object:Object Type

Directory Service Changes

Security event 5136

5136 A directory service object was modified.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	Object: DN	Object: DN
Device Custom String 5	Object: Class	Object: Class
Device Custom String 4	Operation:Type	Operation:Type

Security events 5137, 5138, 5139, 5141

5137 A directory service object was created.

5141 A directory service object was deleted.

Event 5141 in the Directory Service Changes subcategory is available only in Windows Vista Service Pack 1 and in Windows Server 2008.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	Object: DN	Object: DN
Device Custom String 5	Object: Class	Object: Class

5138 A directory service object was undeleted.

5139 A directory service object was moved.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	Object: New DN	Object: New DN
Device Custom String 5	Object: Class	Object: Class

Logon/Logoff

Logon

Security events 4624, 4625, 4648

4624 An account was successfully logged on.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source Address	Network Information:Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Destination Process Name	Process Information:Process Name	Process Information:Process Name
Destination User Name	New Logon: Account Name	New Logon: Account Name (If no value use the value from the header user field without the domain.)
Destination NT Domain	New Logon: Account Domain	(Use the base domain.)
Destination User ID	New Logon: Logon ID	New Logon: Logon ID
Device Custom String 3	Process Information:Process ID	—
Device Process Name	Detailed Authentication Information:Logon Process	Detailed Authentication Information:Logon Process
Device Custom String 6	New Logon: Logon GUID	New Logon: Logon GUID
Device NT Domain	—	—
Destination Process ID	—	Process Information:Process ID
Reason	—	'Successful Logon'
Source Host Name	Subject: Client Name	**Logon Types 0,2,4,5,9,11:** Computer Name **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.
Source NT Domain	—	Subject: Account Domain

4625 An account failed to log on.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	Account For Which Logon Failed: Account Name	Account For Which Logon Failed: Account Name (If no value use the value from the header user field without the domain.)
Destination Process Name	Process Information:Caller Process Name	Process Information:Caller Process Name
Destination NT Domain	Account For Which Logon Failed: Account Domain	Account For Which Logon Failed: Account Domain (Use the base domain.)
Device Custom String 3	Process Information:Caller Process ID	—
Device Process Name	Detailed Authentication Information:Logon Process	Detailed Authentication Information:Logon Process
Device NT Domain	—	—
Source Address	Network Information:Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Host Name	Network Information:Workstation Name	**Logon Types 0,2,4,5,9,11:** Computer Name **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.
Source NT Domain	—	Subject: Account Domain
Source Process ID	—	Process Information:Caller Process ID
Reason	Failure Information:Failure Reason	Failure Information:Failure Reason

4648 A logon was attempted using explicit credentials.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device NT Domain	Subject:Account Domain	Subject:Account Domain
Source Address	Network Information:Network Address	Network Information:Network Address
Destination Process Name	Process Information:Process Name	Process Information:Process Name
Destination User Name	Account Whose Credentials Were Used: Account Name	Account Whose Credentials Were Used: Account Name
Destination NT Domain	Account Whose Credentials Were Used: Account Domain	Account Whose Credentials Were Used: Account Domain
Device Custom String 6	Account Whose Credentials Were Used: Logon GUID	Account Whose Credentials Were Used: Logon GUID
Device Custom String 3	Process Information: Process ID	—
Destination Process ID	—	Process Information:Process ID

Network Policy Server

Security events 6272 – 6280

All the events in the Network Policy Server subcategory are available only in Windows Vista Service Pack 1 and in Windows Server 2008.

6272 Network Policy Server granted access to a user.

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	User: Account Name	User: Account Name
Destination NT Domain	User: Account Domain	User: Account Domain
Destination User ID	User: Fully Qualified Account Name	User: Fully Qualified Account Name
Source User Name	Client Machine:Account Name	Client Machine:Account Name
Source User ID	Client Machine:Fully Qualified Account Name	Client Machine:Fully Qualified Account Name
Source Address	Client Machine:Calling Station Identifier	Client Machine:Calling Station Identifier
Device Custom String 1	Authentication Details: Proxy Policy Name	Authentication Details: Proxy Policy Name
Device Custom String 3	RADIUS Client: Client IP Address	RADIUS Client: Client IP Address
Destination Address	NAS: NAS IPv4 Address	NAS: NAS IPv4 Address
Destination Port	NAS: NAS Port	NAS: NAS Port
Device Custom String 5	Authentication Details: Authentication Type	Authentication Details: Authentication Type
Device Custom String 6	Authentication Details: Account Session Identifier	Authentication Details: Account Session Identifier
Destination User Privileges	Quarantine Information: Result	Quarantine Information: Result
Device Custom IPv6 Address 3	—	NAS:NAS IPv6 Address

6273 Network Policy Server denied access to a user.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	User: Account Name	User: Account Name
Destination NT Domain	User: Account Domain	User: Account Domain
Destination User ID	User: Fully Qualified Account Name	User: Fully Qualified Account Name
Source User Name	Client Machine:Account Name	Client Machine:Account Name
Source User ID	Client Machine:Fully Qualified Account Name	Client Machine:Fully Qualified Account Name
Source Address	Client Machine:Calling Station Identifier	Client Machine:Calling Station Identifier
Destination Address	NAS: NAS IPv4 Address	NAS: NAS IPv4 Address
Destination Port	NAS: NAS Port	NAS: NAS Port
Device Custom String 1	Authentication Details: Proxy Policy Name	Authentication Details: Proxy Policy Name
Device Custom String 3	RADIUS Client: Client IP Address	RADIUS Client: Client IP Address
Device Custom String 4	Authentication Details: Reason	—
Device Custom String 5	Authentication Details: Authentication Type	Authentication Details: Authentication Type
Device Custom String 6	Authentication Details: Account Session Identifier	Authentication Details: Account Session Identifier
Device Custom IPv6 Address 3	—	NAS:NAS IPv6 Address
Reason	—	Authentication Details: Reason Code
Message	Message	Authentication Details: Reason

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

6280 Network Policy Server unlocked the user account.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	User: Account Name	User: Account Name
Destination NT Domain	User: Account Domain	User: Account Domain
Destination User ID	User: Fully Qualified Account Name	User: Fully Qualified Account Name

Other Logon/Logoff Events

Security events 4778 – 4803

4778 A session was reconnected to a Window Station.

4779 A session was disconnected from a Window Station.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	Session: Session Name	Session: Session Name

4800 The workstation was locked.

4801 The workstation was unlocked.

4802 The screen saver was invoked.

4803 The screen saver was dismissed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	Subject:Session ID	Subject:Session ID

Special Logon

Security event 4672

4672 Special privileges assigned to new logon.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Privileges	Privileges	Privileges

Security event 4964

4964 Special groups have been assigned to a new logon.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	Subject:Account Name	Subject:Account Name
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	New Logon: Account Name	New Logon: Account Name
Destination NT Domain	New Logon: Account Domain	New Logon: Account Domain
Destination User ID	New Logon: Logon ID	New Logon: Logon ID
Device Custom String 3	New Logon: Logon GUID	New Logon: Logon GUID
Device Custom String 6	New Logon: Special Groups Assigned	New Logon: Special Groups Assigned

Object Access

File Share

Security event 5140

5140 A network share object was accessed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source Address	Network Information:Source Address	Network Information:Source Address
File Path	Share Name	Share Name
Device Custom String 6	Share Name	Share Name

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

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

Other Object Access Events

Security events 4698, 4699, 4700, 4701, 4702

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.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	Task Information: Task Name	Task Information: Task Name
Additional Data	Task Information: Task Content	Task Information: Task Content

Handle Manipulation

Security events 4656, 4658, 4690

4656 A handle to an object was requested.

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

4658 The handle to an object was closed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Process Information:Process ID	—
Destination Process ID	—	Process Information:Process ID

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Old File ID	Source Handle Information: Source Handle ID	Source Handle Information: Source Handle ID
File ID	New Handle Information: Target Handle ID	New Handle Information: Target Handle ID
Device Custom String 3	New Handle Information: Target Process ID	—
Device Custom String 5	Source Handle Information: Source Process ID	—
Destination Process ID	—	New Handle Information:Target Process ID
Source Process ID	—	Source Handle Information: Source Process ID

Registry

Security event 4657

4657 A registry value was modified.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	Object:Object Value Name	Object:Object Value Name
Device Action	Object: Operation Type	Object: Operation Type
Old File Type	Change Information: Old Value Type	Change Information: Old Value Type
Device Custom String 4	Change Information: Old Value	Change Information: Old Value
File Type	Change Information: New Value Type	Change Information: New Value Type
Device Custom String 5	Change Information: New Value	Change Information: New Value
Device Custom String 3	Process Information:Process ID	—
Destination Process ID	—	Process Information:Process ID

Special

Security events 4659, 4660, 4661, 4663

Event 4659 may be generated by any resource manager when its subcategory is enabled. For Parser Version 1, the event may be generated by the Registry resource manager or by the File System Resource Manager. The "Object Access: Kernel Object" and "Object Access: SAM" subcategories are Parser Version 1s of subcategories that use these events exclusively.

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

4663 An attempt was made to access an object.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 1	Access Request Information: Accesses	Access Request Information: Accesses
Device Custom String 3	Process Information:Process ID	—
Destination Process ID	—	Process Information:Process ID

4660 An object was deleted.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Process Information:Process ID	—
Destination Process ID	—	Process Information:Process ID

4661 A handle to an object was requested.

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

Policy Change

Audit Policy Change

Security events 4715, 4719, 4902, 4904, 4905, 4906, 4907, 4908, 4912

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	Audit Policy Change:New Security Descriptor	Audit Policy Change:New Security Descriptor

4719 System audit policy was changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 5	Audit Policy Change: Subcategory	Audit Policy Change: Subcategory
Device Action	Audit Policy Change: Changes	Audit Policy Change: Changes
Device Custom String 6	Audit Policy Change: Category	Both (Audit Policy Change:Category, Audit Policy Change:Subcategory, Audit Policy Change:Subcategory GUID, Audit Policy Change:Changes)

4902 The Per-user audit policy table was created.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom Number 3	Number of Elements	Number of Elements
Device Custom String 6	Policy ID	Policy ID

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

4905 A user right was removed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Process: Process ID	—
Device Custom String 5	Event Source: Event Source ID	Event Source: Event Source ID
Device Custom String 6	Event Source: Source Name	Event Source: Source Name
Destination Process Name	Process: Process Name	Process: Process Name
Destination Process ID	—	Process:Process ID

4906 The CrashOnAuditFail value has changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom Number 2	New Value of CrashOnAuditFail	New Value of CrashOnAuditFail

4907 Auditing settings on object were changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 5	Object:Object Type	Object:Object Type
Device Custom String 3	Process Information:Process ID	—
Destination Process ID	—	Process Information:Process ID

4908 Special Groups Logon table modified.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	Special Groups	Special Groups

4912 Per User Audit Policy was changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	Policy for Account:Security ID	Policy for Account:Security ID
Device Custom String 5	Policy Change Details: Subcategory	Policy Change Details: Subcategory
Device Action	Policy Change Details: Changes	Policy Change Details: Changes
Device CustomString 3	—	(Policy Change Details:Category, Policy Change Details:Subcategory, Policy Change Details:Subcategory GUID, Policy Change Details:Changes)

Authentication Policy Change

Security events 4706, 4707, 4713, 4716, 4717, 4718, 4865, 4866, 4867

4706 A new trust was created to a domain.

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

4707 A trust to a domain was removed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 6	One of (Domain Information: Domain Name, Domain Information: Domain ID)	One of (Domain Information: Domain Name, Domain Information: Domain ID)

4713 Kerberos policy was changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Message	Both (Changes Made, Message)	'Changes Made'
Device Custom String 6	Both (Changes Made, Message)	Changes Made

4714 Encrypted data recovery policy was changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Message	Both (Changes Made, Message)	'Changed Made'
Device Custom String 6	Both (Changes Made, Message)	Changes Made

4716 Trusted domain information was modified.

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

4717 System security access was granted to an account.

4718 System security access was removed from an account.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Subject:Logon ID	Subject:Logon ID
Source User Name	One of (Subject:Account Name, Subject:Security ID)	One of (Subject:Account Name, Subject:Security ID)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Destination User Name	Account Modified: Account Name	Account Modified: Account Name

4865 A trusted forest information entry was added.

4866 A trusted forest information entry was removed.

4867 A trusted forest information entry was modified.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Trust Information: Operation ID	Trust Information: Operation ID
Device Custom String 5	Trust Information: Top Level Name	Trust Information: Top Level Name
Device Custom String 6	Trust Information: Forest Root	Trust Information: Forest Root

Authorization Policy Change

Security events 4704, 4705

4704 A user right was assigned.

4705 A user right was removed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	One of (Subject:Security ID, Subject:Account Name)	One of (Subject:Security ID, Subject:Account Name)
Source NT Domain	Subject:Account Domain	Subject:Account Domain
Source User ID	Subject:Logon ID	Subject:Logon ID
Destination User Name	Target: Account Name	Target: Account Name

MPSSVC Rule-Level Policy Change

Security event 4957

4957 Windows Firewall did not apply the following rule.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 4	Both (Error Information:Reason," resolved to an empty set.")	—
Device Custom String 6	Rule Information: Name	Rule Information: Name
Reason	—	Both (Error Information:Reason," resolved to an empty set.")

Subcategory (special)

Security event 4670

4670 Permissions on an object were changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 3	Process: Process ID	—
Device Custom String 4	Permissions Change: Original Security Descriptor	Permissions Change: Original Security Descriptor
Device Custom String 5	Permissions Change: New Security Descriptor	Permissions Change: New Security Descriptor
Destination Process ID	—	Process: Process ID

Privilege Use

Sensitive Privilege Use / Non Sensitive Privilege Use

Security event 4673

4673 A privileged service was called.

Fields in this event are completely supported by the connector. There are no specific mappings.

Security event 4674

4674 An operation was attempted on a privileged object.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Privileges	Requested Operation:Privileges	Requested Operation:Privileges
Device Custom String 3	Process Information:Process ID	—
Destination Process Name	Process Information:Process Name	Process Information:Process Name
Destination Process ID	—	Process Information:Process ID

System

Other System Events

Security events 5058, 5059

5058 Key file operation.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
File Name	Cryptographic Parameters: Key Name	Cryptographic Parameters: Key Name
File Type	Cryptographic Parameters: Key Type	Cryptographic Parameters: Key Type
File Path	Key File Operation Information: File Path	Key File Operation Information: File Path
Device Action	Key File Operation Information: Operation	Key File Operation Information: Operation
Device Custom String 4	Key File Operation Information: Return Code	—
Reason	—	Key File Operation Information: Return Code

5059 Key migration operation.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
File Name	Cryptographic Parameters: Key Name	—
File Type	Cryptographic Parameters: Key Type	—
Device Action	Additional Information:Operation	—
Device Custom String 4	Additional Information:Return Code	—
Reason	—	Additional Information:Return Code

Security State Change

Security events 4608, 4609

4608 Windows is starting up.

Fields in this event are completely supported by the connector. There are no specific mappings.

4609 Windows is shutting down.

Fields in this event are completely supported by the connector. There are no specific mappings.

Security events 4616, 4621

4616 The system time was changed.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom Date 1	Both (Previous Date, Previous Time)	Both (Previous Date, Previous Time)
Device Custom Date 2	Both (New Date, New Time)	Both (New Date, New Time)
Device Custom String 3	Process Information:Process ID	—
Destination Process Name	Process Information:Name	Process Information:Name
Destination Process ID	—	Process Information:Process ID

4621 Administrator recovered system from CrashOnAuditFail.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom Number 2	New Value of CrashOnAuditFail	New Value of CrashOnAuditFail

Security System Extension

Security events 4611, 4614, 4622, 4697

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination Process Name	Logon Process Name	Logon Process Name

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 5	Notification Package Name	Notification Package Name

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
File Path	Security Package Name	Security Package Name
Device Custom String 5	Security Package Name	Security Package Name

4697 A service was installed in the system.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
File Path	Service Information:Service File Name	Service Information:Service File Name
File Type	Service Information:Service Type	Service Information:Service Type
Device Custom String 5	Service Information:Service Start Type	Service Information:Service Start Type
Device Custom String 6	Service Information:Service Account	Service Information:Service Account

System Integrity

Security event 4612

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

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom Number 3	Number of audit messages discarded	Number of audit messages discarded

Other

Security event 521

521 Unable to log events to security log.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 4	Status code	—
Device Custom Number 2	Value of CrashOnAuditFail	Value of CrashOnAuditFail
Device Custom Number 3	Number of failed audits	Number of failed audits
Reason	—	Status code

Security event 525

525 The connection authorization policy could not be updated.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom Number 2	Value of CrashOnAuditFail	Value of CrashOnAuditFail

Security event 1100

1100 The event logging service has shut down.

Fields in this event are completely supported by the connector. There are no specific mappings.

Security event 1101

1101 Audit events have been dropped by the transport.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom Number 3	Audit Events Dropped:Reason	Audit Events Dropped:Reason

Security event 1102

1102 The audit log was cleared.

Fields in this event are completely supported by the connector. There are no specific mappings.

Security event 1104

1104 The security log is now full.

Fields in this event are completely supported by the connector. There are no specific mappings.

Security event 1105

1105 Event log automatic backup.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
File Type	Log	Log
File Name	File	File

Security event 1866

1866 The Intersite Messaging service received extended error string information from LDAP. Security event 8222

Fields in this event are completely supported by the connector. There are no specific mappings.

Security event 8222

8222 No fax devices were found

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	User Name	User Name
Device Custom String 3	Process ID	—
Destination Process ID	—	Process ID

Windows Server 2000/2003 Security Events

There are nine Windows audit policies that can be enabled or disabled (for Windows NT, there are only seven). These values are set to no auditing by default in the Default Domain Controller Group Policy object and the local workstation and server policies.

1 Audit Account Logon Events

This policy lets you determine whether to audit each occurrence of user logging on or logging off of another computer where this computer was used to validate the account. For domain controllers, this policy is defined in the Default Domain Controllers Group Policy object.

2 Audit Logon Events

This policy lets you determine whether an event should be logged each time a user logs on, logs off, or makes a network connection to this computer.

3 Audit Account Management

This policy lets you determine whether to audit each account management event, such as when a password is set or changed.

5 Audit Object Access

This policy lets you determine whether to audit a user accessing an object, such as a file or folder, that has its own system access control list specified.

4 Audit Directory Service Access

This policy lets you determine whether to audit a user accessing an Active Directory object, such as a file or folder, that has its own system access control list specified.

6 Audit Policy Change

This policy lets you determine whether to audit every time a change is made to user rights assignment policies, audit policies, or trust policies.

7 Audit Privilege Use

This policy lets you determine whether to audit each time a user exercises a user right.

8 Audit Process Tracking

This policy lets you determine whether to audit detailed tracking information for events such as activating or exiting a process.

9 Audit System Events

This policy lets you determine whether to audit each time a user restarts or shuts down the computer, or when an event occurs that affects either the system security or the security log.

Windows 2000/XP/2003/2003R2 Common Security Mappings

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Agent (Connector) Severity	Very High = Audit_failure High = Error Medium = Warning Low = Information or Audit_success	Very High = Audit_failure High = Error Medium = Warning Low = Information or Audit_success
Destination Host Name	ComputerName Target Server Name	ComputerName Target Server Name
Destination NT Domain	Assigned To Domain Domain Name New Account Name New Domain Primary Domain Primary User Name Supplied Realm Name Target Account Name Target Domain User User Domain	Assigned To Domain Domain Name New Account Name New Domain Primary Domain Primary User Name Supplied Realm Name Target Account Name Target Domain User User Domain
Destination Process Id	—	Process ID Target Process ID Source Process ID New Process ID
Destination Process Name	Image File Name	Image File Name
Destination Service Name	Service Service Name	Service Service Name
Destination User ID	Logon ID New Account ID Primary Logon ID Target Account ID	Logon ID New Account ID Primary Logon ID Target Account ID
Destination User Name	Assigned to New Account Name Primary User Name Target Account Name Target User Name User	Assigned to New Account Name Primary User Name Target Account Name Target User Name User
Destination User Privileges	Privileges User Right	Privileges User Right
Device Action	One of (Account Action, Allowed)	One of (Account Action, Allowed)
Device Custom Number 1	Logon Type Pre-Authentication Type	Logon Type Pre-Authentication Type
Device Custom Number 2	New Process ID	New Process ID
Device Custom String 1	Accesses or Access Mask	Accesses or Access Mask
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 4	Error Code Failure Code Reason Result Code	—
Device Custom String 5	Authentication Authentication Package Authentication Package Name	Authentication Authentication Package Authentication Package Name
Device Custom String 6	Member ID Member Name Object Name Object Type	Member ID Member Name Object Name Object Type
Device Event Category	Eventlog Type	Eventlog Type
Device Event Class ID	EventSource plus EventID	EventSource plus EventID
Device Host Name	ComputerName	ComputerName
Device Product	'Microsoft Windows'	'Microsoft Windows'
Device Receipt Time	DetectTime	DetectTime
Device Severity	EventType	EventType
Device Vendor	'Microsoft'	'Microsoft'
External ID	EventID	EventID
File ID	Handle ID New Handle ID Object Handle	Handle ID New Handle ID Object Handle
File Name	Object Name Object Type File	Object Name Object Type File
File Type	Object Type (note that the content of this field is not necessarily related to a file)	Object Type (note that the content of this field is not necessarily related to a file)
Name	Description	Description
Reason	—	Error Code Failure Code Reason Result Code
Source Address	Client Address Source Network Address	Client Address Source Network Address
Source Host Name	Address Source Workstation Workstation Name Workstation	Address Source Workstation Workstation Name Workstation
Source NT Domain	Client Domain Logon account User Name User domain	Client Domain Logon account User Name User domain
Source Port	Port number Source Port	Port number Source Port

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source Process Name	Caller Process ID Logon Process Logon Process Name Path Session Name	Caller Process ID Logon Process Logon Process Name Path Session Name
Source User ID	Caller Logon ID Client Logon ID User ID	Caller Logon ID Client Logon ID User ID
Source User Name	Account Account Name Caller User Name Client User Name Logon account User account User Name	Account Account Name Caller User Name Client User Name Logon account User account User Name

Windows Server 2000/2003 Security Event Mappings

This section documents mappings for security events ArcSight has been able to successfully generate. Not all events are represented. For all other events, see the "Overview of Fields Mapped to ArcSight ESM" **Error! Bookmark not defined.**.

Security Event 512 — Windows is starting up

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Destination User Name	User	User
External ID	Event ID	Event ID

Security Event 514 — An authentication package has been loaded

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 5	Authentication Package Name	Authentication Package Name
External ID	Event ID	Event ID
Destination User Name	User	User

Security Event 515 — A trusted logon process has registered

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source Process Name	Logon Process Name	Logon Process Name
Destination User Name	User	User

Security Event 516 — Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom Number 3	Number of audit messages discarded	Number of audit messages discarded
External ID	Event ID	Event ID
Destination User Name	User	User

Security Event 517 — The audit log was cleared

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Client Logon ID	Client Logon ID
Source User Name	Client User Name	Client User Name
Source NT Domain	Client Domain Client User Name	Client Domain Client User Name
Destination User ID	Primary Logon ID	Primary Logon ID
Destination User Name	Primary User Name	Primary User Name
Destination NT Domain	Primary Domain Primary User Name	Primary Domain Primary User Name

Security Event 518 — Notification package loaded by the SAM

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Destination User Name	User	User

Security Event 520 — The system time was changed

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom Number 2	New Process ID	New Process ID
Device Custom Date 1	Both (Previous Date, Previous Time)	Both (Previous Date, Previous Time)
Device Custom Date 2	Both (New Date, New Time)	Both (New Date, New Time)
External ID	Event ID	Event ID
Source User ID	Client Logon ID	Client Logon ID
Source User Name	Client User Name	Client User Name
Source NT Domain	Client Domain Client User Name	Client Domain Client User Name
Destination User ID	Primary Logon ID	Primary Logon ID
Destination User Name	Primary User Name	Primary User Name
Destination NT Domain	Primary Domain Primary User Name	Primary Domain Primary User Name
Destination Process Name	Process ID	Process ID
Destination Service Name	Process Name	Process Name

Security Event 528 — Successful Logon

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
Device Host Name	—	Computer Name
Device NT Domain	—	—
External ID	Event ID	Event ID
Reason	—	Current Mapping
Source User Name	User Name	Caller User Name
Source Host Name	Workstation Name	**Logon Types 0,2,4,5,9:** Computer Name **Logon Types 3,6,7,8,11,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.
Source NT Domain	—	Caller Domain
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User Name If no value use the value from the header user field without the domain.
Destination NT Domain	Domain	Domain (Use the base domain.)
Destination Host Name	Computer Name	Computer Name
Destination Process Name	—	Logon Process

Windows XP and Windows Server 2003 add this field:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
N/A	Logon GUID	Logon GUID

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Process ID	Caller Process ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,11,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 529 — Logon Failure: Unknown user name or bad password

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	'Unknown user name or bad password'	—
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Device Host Name	Computer Name	Computer Name
Device NT Domain	—	—
Source User Name	User Name	Caller User Name
Source Host Name	Source Network Address	**Logon Types 0,2,4,5,9,11:** Computer Name **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
		value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.
Destination User Name	User	User Name (If no value use the value from the header user field without the domain.)
Destination Host Name	Computer Name	Computer Name
Destination NT Domain	Domain	Domain (Use the base domain.)
Reason	—	'Unknown user name or bad password'

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Process ID	Logon Process Caller Process ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 530 — Logon Failure: Account logon time restriction violation

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device NT Domain	—	—
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	'Account logon time restriction violation'	—
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Source User Name	Caller User Name User Name	Caller User Name
Source Host Name	Source Network Address	**Logon Types 0,2,4,5,9,11:** Computer Name **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.
Destination User Name	User	User Name (If no value use the value from the header user field without the domain.)
Destination Host Name	Computer Name	Computer Name
Destination NT Domain	Domain	Domain (Use the base domain.)
Reason	—	'Account logon time restriction violation'

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Logon ID	Logon Process Caller Logon ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9,11:**

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
		Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 531 — Logon Failure: Account currently disabled

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device NT Domain	—	—
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	'Account currently disabled'	—
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Source User Name	Caller User Name User Name	Caller User Name
Source Host Name	Source Network Address	**Logon Types 0,2,4,5,9,11:** Computer Name **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.
Destination User Name	User	User Name (If no value use the value from the header user field without the domain.)
Destination Host Name	Computer Name	Computer Name
Destination NT Domain	Domain	Domain (Use the base domain.)
Reason	—	'Account currently disabled'

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Process ID	Logon Process Caller Process ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 532 — Logon Failure: The specified user account has expired

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device NT Domain	—	—
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	'The specified user account has expired'	—
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Source User Name	Caller User Name User Name	Caller User Name
Source Host Name	Source Network Address	**Logon Types 0,2,4,5,9,11:** Computer Name **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	User	User Name (If no value use the value from the header user field without the domain.)
Destination Host Name	Computer Name	Computer Name
Destination NT Domain	Domain	Domain (Use the base domain.)
Reason	—	'The specified user account has expired'

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Process ID	Logon Process Caller Process ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 533 — Logon Failure: User not allowed to logon at this computer

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device NT Domain	—	—
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	'User not allowed to logon at this computer'	—
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Source User Name	Caller User Name User Name	Caller User Name
Source Host Name	Source Network Address	**Logon Types 0,2,4,5,9,11:** Computer Name **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.
Destination User Name	User	User Name (If no value use the value from the header user field without the domain.)
Destination Host Name	Computer Name	Computer Name
Destination NT Domain	Domain	Domain (Use the base domain.)
Reason	—	'User not allowed to logon at this computer'

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Process ID	Logon Process Caller Process ID

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 534 — Logon Failure: Requested logon type not granted

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	'The user has not been granted the requested logon type at this machine'	—
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Source User Name	User Name	Caller User Name
Source Host Name	Source Network Address	Source Network Address
Destination User Name	User	User Name
Destination Host Name	Computer Name	Computer Name
Destination NT Domain	Domain	Domain
Reason	—	'The user has not been granted the requested logon type at this machine'

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source Process Name	Logon Process Caller Process ID	Logon Process Caller Process ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 535 — Logon Failure – The specified account's password has expired

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device NT Domain	—	—
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	'The specified account's password has expired'	—
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Source User Name	Caller User Name User Name	Caller User Name
Source Host Name	Source Network Address	**Logon Types 0,2,4,5,9,11:** Computer Name **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination User Name	User	User Name (If no value use the value from the header user field without the domain.)
Destination Host Name	Computer Name	Computer Name
Destination NT Domain	Domain	Domain (Use the base domain.)
Reason	—	'The specified account's password has expired'

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Process ID	Logon Process Caller Process ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 536 — Logon failure – The NetLogon component is not active

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	'The NetLogon component is not active'	—
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Source User Name	Caller User Name User Name	Caller User Name
Source Host Name	Source Network Address	Source Network Address
Destination User Name	User	User Name
Destination Host Name	Computer Name	Computer Name
Destination NT Domain	Domain	Domain
Reason	—	'The NetLogon component is not active'

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Process ID	Logon Process Caller Process ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 537 — Logon failure - The logon attempt failed for other reasons

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	'An error occurred during logon'	—
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Source User Name	Target User Name User	Caller User Name
Source Host Name	Source Network Address	Source Network Address
Source NT Domain	Domain	Caller Domain
Destination User Name	Caller Target User Name Target User Name	User Name
Destination Host Name	Computer Name	Computer Name
Destination NT Domain	Caller Domain	Domain
Reason	—	'An error occurred during logon'

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Process ID	Logon Process Caller Process ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 538 — User Logoff

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain	Domain

Security Event 539 — Account Locked Out

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device NT Domain	—	—
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	'Account locked out'	—
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
External ID	Event ID	Event ID
Source User Name	Caller User Name User Name	Caller User Name
Source Host Name	Source Network Address	**Logon Types 0,2,4,5,9,11:** Computer Name **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.
Destination User Name	User	User Name (If no value use the value from the header user field without the domain.)
Destination Host Name	Computer Name	Computer Name
Destination NT Domain	Domain	Domain (Use the base domain.)
Reason	—	'Account locked out'

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Process ID	Logon Process Caller Process ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9,11:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 540 — Successful Network Logon

OS: Windows XP, Windows 2000, Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Destination Host Name	—	Computer Name
Destination NT Domain	—	Domain (Use the base domain.)
Destination User Name	—	User Name
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 5	Authentication Package	Authentication Package
Device Custom Number 1	Logon Type	Logon Type
Device NT Domain	—	—
External ID	Event ID	Event ID
Source Host Name	Workstation Name	**Logon Types 0,2,4,5,9,11:** Computer Name **Logon Types 3,6,7,8,10,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address. Use the host portion of the fully qualified domain name.
Source NT Domain	—	Caller Domain

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User Name	—	Caller User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain	Domain
Reason	—	Current mapping

Windows XP and Windows Server 2003 add: Logon GUID

Windows Server 2003 also adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Source User ID	Caller Logon ID	Caller Logon ID
Source NT Domain	Caller Domain Caller User Name User Name	Caller Domain
Source Process Name	Logon Process Caller Process ID	Logon Process Caller Process ID
N/A	Transited Services	Transited Services
Source Address	Source Network Address	**Logon Types 0,2,4,5,9:** Address (Resolve the IP address from the computer name) **Logon Types 3,6,7,8,10,11,12,13:** Source Network Address, if no value, Workstation Name, if no value, device address.
Source Port	Source Port	Source Port

Security Event 551 — User-initiated logoff

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain	Domain

Security Event 552 — Logon attempt using explicit credentials

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Source Process Name	Caller Process ID	Caller Process ID
Source Address	Source Network Address	Source Network Address
Source Port	Source Port	Source Port
Destination User ID	Logon ID	Logon ID
Destination User Name	Target User Name User	Target User Name User
Destination NT Domain	Target Domain Domain	Target Domain Domain
Destination Host Name	Target Server Name	Target Server Name

Security Event 560 — Object Open

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	**Parser Version 1**
Eventlog Type	Eventlog Type	Eventlog Type
Event Source	Event Source	Event Source
Event Category	Event Category	Event Category
Device Host Name	Computer Name	Computer Name
Device Custom String 6	Object Name	Object Name
Event ID	Event ID	Event ID
File Type (the content of this field is not necessarily related to a file)	Object Type	Object Type
File Name	Object Name	Object Name
File ID	Handle ID	Handle ID
Source User ID	Client Logon ID	Client Logon ID
Source User Name	Client User Name	Client User Name
Source NT Domain	Client Domain Client User Name	Client Domain Client User Name
Destination User ID	Primary Logon ID	Primary Logon ID
Destination User Name	Primary User Name User	Primary User Name User
Destination NT Domain	Primary Domain Primary User Name	Primary Domain Primary User Name
Destination Process Name	Image File Name Process ID	Image File Name Process ID
Destination Host Name	Computer Name	Computer Name
Destination User Privileges	Privileges	Privileges

Windows Server 2003 adds these fields:

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	**Parser Version 1**
N/A	Restricted Sid Count	Restricted Sid Count
Device Custom String 1	Accesses Access Mask	Accesses Access Mask

Security Event 562 — Handle Closed

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
File ID	Handle ID	Handle ID
Destination User Name	User	User
Destination Host Name	Computer Name	Computer Name
Destination Process Name	Image File Name Process ID	Image File Name
Destination Process ID	—	Process ID

Security Event 564 — Protected object was deleted

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
File ID	Handle ID	Handle ID
Destination User Name	User	User
Destination Host Name	Computer Name	Computer Name
Destination Process Name	Image File Name Process ID	Image File Name
Destination Process ID	—	Process ID

Security Event 565 — Object Open

OS: Windows 2000

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 1	Accesses Access Mask	Accesses Access Mask
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Object Name	Object Name
External ID	Event ID	Event ID
File ID	Handle ID	Handle ID
File Type (the content of this field is not necessarily related to a file)	Object Type	Object Type
File Name	Object Name	Object Name
Source User ID	Client Logon ID	Client Logon ID
Source User Name	Client User Name	Client User Name
Source NT Domain	Client Domain Client User Name	Client Domain Client User Name
Destination User ID	Primary Logon ID	Primary Logon ID
Destination User Name	Primary User Name User	Primary User Name User
Destination NT Domain	Primary Domain Primary User Name	Primary Domain Primary User Name
Destination Process Name	Process ID	—
Destination User Privileges	Privileges	Privileges
Destination Process ID	—	Process ID
Destination Host Name	Computer Name	Computer Name

Security Event 567 — Object Access Attempt

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Custom String 1	Accesses Access Mask	Accesses Access Mask
File ID	Handle ID	Handle ID
File Type (the content of this field is not necessarily related to a file)	Object Type	Object Type
Destination Process Name	Image File Name Process ID	Image File Name
Destination Process ID	—	Process ID
Destination Host name	Computer Name	Computer Name

Security Event 576 — Special Privileges Assigned to New Logon

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain	Domain
Destination User Privileges	Privileges	Privileges

Security Event 577 — User attempted privileged system service operation

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Client Logon ID	Client Logon ID
Source User Name	Client User Name	Client User Name
Source NT Domain	Client Domain Client User Name	Client Domain Client User Name
Destination User ID	Primary Logon ID	Primary Logon ID
Destination User Name	Primary User Name User	Primary User Name User
Destination NT Domain	Primary Domain Primary User Name	Primary Domain Primary User Name
Destination Service Name	Service	Service
Destination Host Name	Computer Name	Computer Name
Destination User Privileges	Privileges	Privileges

Security Event 578 — Privileged object operation

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	**Parser Version 1**
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
File ID	Object Handle	Object Handle
Source User ID	Client Logon ID	Client Logon ID
Source User Name	Client User Name	Client User Name
Source NT Domain	Client Domain Client User Name	Client Domain Client User Name
Destination User ID	Primary Logon ID	Primary Logon ID
Destination User Name	Primary User Name User	Primary User Name User
Destination NT Domain	Primary Domain Primary User Name	Primary Domain Primary User Name
Destination Process Name	Process ID	—
Destination Host Name	Computer Name	Computer Name
Destination User Privileges	Privileges	Privileges
Destination Process ID	—	Process ID

Security Event 592 — A New Process Has Been Created

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom Number 2	New Process ID	New Process ID
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain	Domain
Destination Process Name	Image File Name New Process ID	Image File Name
Destination Process ID	—	New Process ID

Security Event 593 — A Process Has Exited

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain	Domain
Destination Process Name	Image File Name Process ID	Image File Name
Destination Process ID	—	Process ID

Security Event 594 — Handle to an object was duplicated

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Destination User Name	User	User
Device Host Name	Computer Name	Computer Name
Destination Process Name	Target Process ID Source Process ID	Target Process ID Source Process ID

Security Event 595 — Indirect access to an object was obtained

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 1	Accesses Access Mask	Accesses Access Mask
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Object Name	Object Name
External ID	Event ID	Event ID
File Type (the content of this field is not necessarily related to a file)	Object Type	Object Type
File Name	Object Name	Object Name
Source User ID	Client Logon ID	Client Logon ID
Source NT Domain	Client Domain Client User Name	Client Domain Client User Name
Destination User ID	Primary Logon ID	Primary Logon ID
Destination User Name	Primary User Name User	Primary User Name User
Destination NT Domain	Primary Domain Primary User Name	Primary Domain Primary User Name
Destination Process Name	Process ID	—
Destination Process ID	—	Process ID

Security Event 600 — A Process was Assigned a Primary Token

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Destination User ID	Primary Logon ID	Primary Logon ID
Destination User Name	Primary User Name Target User Name User	Primary User Name Target User Name User
Destination NT Domain	Primary Domain Target Domain Primary User Name	Primary Domain Target Domain Primary User Name
Destination Process Name	Image File Name Process ID	Image File Name
Destination Process ID	—	Process ID

Security Event 601 — Attempt to install a service

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain	Domain
Destination Host Name	Computer Name	Computer Name
Destination Service Name	Service Name	Service Name

Security Event 602 — Scheduled Task created

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain User	Domain User

Security Event 608 — User Right Assigned

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	Assigned By	Assigned By
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain Assigned To User	Domain Assigned To User
Destination User Privilege (the user who granted the privilege)	User Right	User Right

Security Event 609 — User Right Removed

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain User	Domain User
Destination User Privilege	User Right	User Right

Security Event 610 — New Trusted Domain

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain Name Domain User	Domain Name Domain User

Security Event 611 — Removing Trusted Domain

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain Name Domain User	Domain Name Domain User

Security Event 612 — Audit Policy Change

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (New Policy:System:Success, New Policy:System:Failure, New Policy:Logon/Logoff:Success, New Policy:Logon/Logoff:Failure, New Policy:Object Access:Success, New Policy:Object Access:Failure, New Policy:Privilege Use:Success, New Policy:Privilege Use:Failure, New Policy:Detailed Tracking:Success, New Policy:Detailed Tracking:Failure, New Policy:Policy Change:Success, New Policy:Policy Change:Failure, New Policy:Account Management:Success, New Policy:Account Management:Failure, New Policy:Directory Service Access:Success, New Policy:Directory Service Access:Failure, New Policy:Account Logon:Success, New Policy:Account Logon:Failure)
External ID	Event ID	Event ID
Source User Name	User Name	—
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User Name
Destination NT Domain	Domain Name User	Domain Name User

Security Event 615 — IPSec Services has started successfully

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Destination User Name	User	User

Security Event 617 — Kerberos Policy Changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Changes made
External ID	Event ID	Event ID
Source User Name	User Name	—
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User Name
Destination NT Domain	Domain Name User	Domain Name User

Security Event 620 — Trusted Domain Information Modified

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User Name
Destination NT Domain	Domain Name Domain User	Domain Name Domain User

Security Event 621 — System Security Access Granted

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain User	Domain User

Security Event 624 — User Account Created

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	New Account ID	New Account ID
Destination User Name	New Account Name User	New Account Name User
Destination NT Domain	New Domain New Account Name User	New Domain New Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 626 — User Account Enabled

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User

Security Event 627 — Change password attempt

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	**Parser Version 1**
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 628 — User Account Password Set

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User

Security Event 629 — User Account Disabled

OS: Windows XP and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User

Security Event 630 — User Account Deleted

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	**Parser Version 1**
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 631 — Security Enabled Global Group Created

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (New Domain, New Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	New Account ID	New Account ID
Destination User Name	New Account Name User	New Account Name User
Destination NT Domain	New Domain New Account Name User	New Domain New Account Name User
Destination User Privileges	Privileges	New Account Name

Security Event 632 — Security Enabled Global Group Member Added

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 633 — Security Enabled Global Group Member Removed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 634 — Security Enabled Global Group Deleted

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 635 — Security Enabled Local Group Created

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (New Domain, New Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	New Account ID	New Account ID
Destination User Name	New Account Name User	New Account Name User
Destination NT Domain	New Domain New Account Name User	New Domain New Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 636 — Security Enabled Local Group Member Added

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name User	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 637 — Security Enabled Local Group Member Removed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name User	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 638 — Security Enabled Local Group Deleted

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 639 — Security enabled local group changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account name)
External ID	Event ID	Event ID
Source User ID	Caller User Name	Caller User Name
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Target Account Name

Security Event 641 — Group Changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Target Account Name
additionaldata.SamAccountName	Changed Attributes	Changed Attributes

Security Event 642 — User Account Changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Changed Attributes	Changed Attributes
Message	Dummy	Dummy

Security Event 643 — Domain Policy Changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	'Min. Password Age, Max. Password Age, Force Logoff, Lockout Threshold, Lockout Observation Window, Lockout Duration, Password Properties, Min. Password Length, Password History Length, Machine Account Quota, Mixed Domain Mode, Domain Behavior Version, OEM Information'
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	—
Source NT Domain	Caller Domain Caller User Name	—
Destination User ID	—	Caller Logon ID
Destination User Name	User	Caller User Name
Destination NT Domain	Domain Name User	Caller Domain
Destination User Privileges	Privileges	Privileges
additionaldata.MinPasswordAge	Min. Password Age	Min. Password Age
additionaldata.MaxPasswordAge	Max. Password Age	Max. Password Age
additionaldata.ForceLogoff	Force Logoff	Force Logoff
additionaldata.LockoutThreshold	Lockout threshold	Lockout threshold
additionaldata.LockoutObservationWindow	Lockout Observation Window	Lockout Observation Window
additionaldata.LockoutDuration	Lockout Duration	Lockout Duration
additionaldata.PasswordProperties	Password Properties	Password Properties
additionaldata.MinPasswordLength	Min. Password Length	Min. Password Length
additionaldata.PasswordHistoryLength	Password History Length	Password History Length
additionaldata.MachineAccountQuota	Machine Account Quota	Machine Account Quota
additionaldata.MixedDomainMode	Mixed Domain Mode	Mixed Domain Mode
additionaldata.DomainBehaviorVersion	Domain Behavior Version	Domain Behavior Version
additionaldata.OEMInformation	OEM Information	OEM Information

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Message	Description Domain Policy Changed	Description Domain Policy Changed
Name	'Domain Policy Changed'	'Domain Policy Changed'

Security Event 644 — User Account Locked Out

OS: All versions

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Source Host Name	—	Caller Machine Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Account Name User	Target Account ID

Security Event 645 — Computer Account Created

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	**Parser Version 1**
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	New Account ID	New Account ID
Destination User Name	New Account Name User	New Account Name User
Destination NT Domain	New Domain New Account Name User	New Domain New Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 646 — Computer Account Changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	**Parser Version 1**
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 647 — Computer Account Deleted

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	**Parser Version 1**
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 648 — Group Created

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 649 — Group changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 650 — Group member added or removed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name User	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 651 — Group member added or removed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name User	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 652 — Group deleted

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 653 — Group created

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (New Domain, New Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	New Account ID	New Account ID
Destination User Name	New Account Name User	New Account Name User
Destination NT Domain	New Domain New Account Name User	New Domain New Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 654 — Group changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 655 — Group member added or removed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name User	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 656 — Group member added or removed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name User	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 657 — Group deleted

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 658 — Group created

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (New Domain, New Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	New Account ID	New Account ID
Destination User Name	New Account Name User	New Account Name User
Destination NT Domain	New Domain New Account Name User	New Domain New Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 659 — Group changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 660 — Group member added or removed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name User	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 661 — Group member added or removed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name User	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 662 — Group deleted

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 663 — Group created

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (New Domain, New Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	New Account ID	New Account ID
Destination User Name	New Account Name User	New Account Name User
Destination NT Domain	New Domain New Account Name User	New Domain New Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 664 — Group changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 665 — Group member added or removed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name User	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 666 — Group member added or removed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	Member Name Member ID	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Member ID
Destination User Name	Target Account Name User	Member ID
Destination NT Domain	Target Domain Target Account Name User	Member ID
Destination User Privileges	Privileges	Privileges

Security Event 667 — Group deleted

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name User	Target Domain Target Account Name User
Destination User Privileges	Privileges	Privileges

Security Event 668 — Group type changed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	Both (Target Domain, Target Account Name)
External ID	Event ID	Event ID
Source User ID	Caller Logon ID	Caller Logon ID
Source User Name	Caller User Name	Caller User Name
Source NT Domain	Caller Domain Caller User Name	Caller Domain Caller User Name
Destination User ID	Target Account ID	Target Account ID
Destination User Name	Target Account Name User	Target Account Name User
Destination NT Domain	Target Domain Target Account Name	Target Domain Target Account Name
Destination User Privileges	Privileges	Privileges

Security Event 672 — Authentication Ticket Granted

OS: Windows 2000

This event is logged on domain controllers only.

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	Result Code	—
Device Custom Number 1	Pre-Authentication Type	Pre-Authentication Type
External ID	Event ID	Event ID
Source User ID	User ID	User ID
Source User Name	User Name	—
Source NT Domain	User Name	User Name
Source Address	Client Address	Client Address
Destination User ID	—	User ID
Destination User Name	User	User Name
Destination NT Domain	Supplied Realm Name User	Supplied Realm Name
Destination Service Name	Service Name	Service Name
Destination Host Name	Computer Name	Computer Name Client Address
Reason	—	Result Code

Security Event 673 — Service Ticket Granted

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	Failure Code	—
External ID	Event ID	Event ID
Source User Name	User Name	—
Source NT Domain	User Name	User Name
Source Address	Client Address	Client Address
Destination User Name	User	User Name
Destination NT Domain	User Domain User	User Domain
Destination Service Name	Service Name	Service Name
Destination Host Name	Computer Name	Computer Name Client Address
Reason	—	Failure Code

Security Event 674 — Ticket Granted Renewed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Source Address	Client Address	Client Address
Destination User Name	User	User
Destination NT Domain	User Domain User	User Domain User
Destination Service Name	Service Name	Service Name

Security Event 675 — Pre-Authentication Failed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	Failure Code	—
Device Custom Number 1	Pre-Authentication Type	Pre-Authentication Type
External ID	Event ID	Event ID
Source User ID	User ID	—
Source User Name	User Name	—
Source NT Domain	User ID	User Name
Source Address	Client Address	Client Address
Destination User ID	—	User ID
Destination User Name	User	User Name
Destination NT Domain	User	User ID
Destination Host Name	Computer Name	Computer Name Client Address
Destination Service Name	Service Name	Service Name
Reason	—	Failure Code

Security Event 676 — Authentication Ticket Request Failedx

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	Failure Code	—
External ID	Event ID	Event ID
Source User Name	User Name	—
Source NT Domain	User Name	User Name
Source Address	Client Address	Client Address
Destination User Name	User	User Name
Destination NT Domain	Supplied Realm Name User	Supplied Realm Name
Destination Host Name	Computer Name	Client Address Computer Name
Destination Service Name	Service Name	Service Name
Reason	—	Failure Code

Security Event 677 — Service Ticket Request Failed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	Failure Code	—
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Source Address	Client Address	Client Address
Destination User Name	User	User
Destination Service Name	Service Name	Service Name
Reason	—	Failure Code

Security Event 680 — Logon Attempt by:

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	Error Code	—
External ID	Event ID	Event ID
Source User Name	User (extracted from NTUser)	User (extracted from NTUser)
Source NT Domain	User (extracted from NTDomain)	User (extracted from NTDomain)
Source Host Name	—	Workstation
Destination User Name	Logon account (extracted from NTUser)	Logon account (extracted from NTUser)
Destination NT Domain	Logon account (extracted from NTDomain)	User (extracted from NTDomain)
Reason	—	Error Code

Security Event 681 — Logon Failed

OS: Windows 2000 and Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 4	Error Code	—
External ID	Event ID	Event ID
Source User Name	Account	Account
Source NT Domain	Account	Account
Source Host Name	—	Workstation
Destination User Name	User	Logon by (extracted from NTUser)
Destination NT Domain	User	Logon by (extracted from NTDomain)
Destination Host Name	Computer Name	Workstation
Reason	—	Error Code

Security Event 682 — Session reconnected to winstation

OS: Windows XP, Windows 2000, Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Source Host Name	Client Address	Client Name
Source Process Name	Session Name	Session Name
Source Address	Client Address	Client Address
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain User	Domain User

Security Event 683 — Session disconnected from winstation

OS: Windows XP, Windows 2000, Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Name	User Name
Source NT Domain	User Name	User Name
Source Host Name	Client Address	Client Name
Source Process Name	Session Name	Session Name
Source Address	Client Address	Client Address
Destination User ID	Logon ID	Logon ID
Destination User Name	User	User
Destination NT Domain	Domain User	Domain User

Security Event 806 — Per user audit policy was refreshed

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Destination User Name	User	User

Security Event 807 — Per user auditing policy set for user

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
Device Custom String 6	—	'System, Logon, Object Access, Privilege Use, Detailed Tracking, Policy Change, Account Management, DS Access, Account Logon'
External ID	Event ID	Event ID
Device Host Name	Computer Name	Computer Name

Security Event 848 — Policy was active when Windows firewall started

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Destination User Name	User	User

Security Event 850 — Port listed as exception when firewall started

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source Port	Port number	Port number
Target Port	Port number	Port number
Destination User Name	User	—

Security Event 861 — Firewall detected app listening for incoming traffic

OS: Windows 2003

HP ArcSight ESM Field	Device-Specific Field	
	Base Parser Version	Parser Version 1
Device Event Category	Eventlog Type	Eventlog Type
Device Host Name	Computer Name	Computer Name
Device Action	Allowed	Allowed
Device Custom String 2	Event Category	Event Category
Device Custom String 3	Event Source	Event Source
External ID	Event ID	Event ID
Source User Name	User Account	User Account
Source NT Domain	User Domain	User Domain
Source Port	Port number	Port number
Source Process Name	Path	Path
Destination User Name	User	User
Destination Service Name	Service	Service
Target Port	Port number	Port number

Logon Types

Logon Type	Description
2	Interactive (logon at keyboard and system screen)
3	Network (connection to shared folder on this computer from elsewhere on network)
4	Batch (scheduled task)
5	Service (service startup)
7	Unlock (unattended workstation with password-protected screen saver
8	NetworkCleartext (logon with credentials sent in the clear text. Usually indicates a logon to IIS with basic authentication.
9	NewCredentials
10	RemoteInteractive (Terminal Services, Remote Desktop, or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials)

Kerberos Failure Codes

Kerberos failure codes come directly from RFC 1510 - The Kerberos Network Authentication Service (V5) .

Dec Code	Hex Code	Kerberos RFC Description
1	0x1	Client's entry in database has expired
2	0x2	Server's entry in database has expired
3	0x3	Requested protocol version # not supported
4	0x4	Client's key encrypted in old master key
5	0x5	Server's key encrypted in old master key
6	0x6	Client not found in Kerberos database
7	0x7	Server not found in Kerberos database
8	0x8	Multiple principal entries in database
9	0x9	The client or server has a null key
10	0xA	Ticket not eligible for postdating
11	0xB	Requested start time is later than end time
12	0xC	KDC policy rejects request
13	0xD	KDC cannot accommodate requested option
14	0xE	KDC has no support for encryption type
15	0xF	KDC has no support for checksum type
16	0x10	KDC has no support for padata type
17	0x11	KDC has no support for transited type
18	0x12	Clients credentials have been revoked
19	0x13	Credentials for server have been revoked
20	0x14	TGT has been revoked
21	0x15	Client not yet valid - try again later
22	0x16	Server not yet valid - try again later
23	0x17	Password has expired
24	0x18	Pre-authentication information was invalid
25	0x19	Additional pre-authentication required*
31	0x1F	Integrity check on decrypted field failed
32	0x20	Ticket expired
33	0x21	Ticket not yet valid
33	0x21	Ticket not yet valid
34	0x22	Request is a replay

Dec Code	Hex Code	Kerberos RFC Description
35	0x23	The ticket isn't for us
36	0x24	Ticket and authenticator don't match
37	0x25	Clock skew too great
38	0x26	Incorrect net address
39	0x27	Protocol version mismatch
40	0x28	Invalid msg type
41	0x29	Message stream modified
42	0x2A	Message out of order
44	0x2C	Specified version of key is not available
45	0x2D	Service key not available
46	0x2E	Mutual authentication failed
47	0x2F	Incorrect message direction
48	0x30	Alternative authentication method required*
49	0x31	Incorrect sequence number in message
50	0x32	Inappropriate type of checksum in message
60	0x3C	Generic error (description in e-text)
61	0x3D	Field is too long for this implementation

Windows Server 2000/2003 Security Events by Event ID

Event ID	OS	Title
512	All Versions	Windows NT is starting up
513	Windows XP/2003	Windows NT is shutting down
514	All Versions	An authentication package has been loaded by the Local Security Authority
515	All Versions	A trusted logon process has registered with the Local Security Authority
516	All Versions	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits
517	All Versions	The audit log was cleared
518	All Versions	A notification package has been loaded by the Security Account Manager
519	Windows 2003	A process is using an invalid local procedure call port
520	Windows 2003	The system time was changed
528	All Versions	Successful Logon
529	All Versions	Logon Failure - Unknown user name or bad password

Event ID	OS	Title
530	All Versions	Logon Failure - Account logon time restriction violation
531	All Versions	Logon Failure - Account currently disabled
532	All Versions	Logon Failure - The specified user account has expired
533	All Versions	Logon Failure - User not allowed to logon at this computer
534	All Versions	Logon Failure - The user has not been granted the requested logon type at this machine
535	All Versions	Logon Failure - The specified account's password has expired
536	All Versions	Logon Failure - The NetLogon component is not active
537	All Versions	Logon failure - The logon attempt failed for other reasons
538	All Versions	User Logoff
539	All Versions	Logon Failure - Account locked out
540	Windows XP/2000/2003	Successful Network Logon
552	Windows 2003	Logon attempt using explicit credentials
560	All Versions	Object Open
561	All Versions	Handle Allocated
562	All Versions	Handle Closed
563	All Versions	Object Open for Delete
564	All Versions	Object Deleted
565	Windows 2000	Object Open (Active Directory)
	Windows 2003	Object Open (W3 Active Directory)
566	Windows 2003	Object Operation (W3 Active Directory)
567	Windows 2003	Object Access Attempt
576	All Versions	Special privileges assigned to new logon
577	All Versions	Privileged Service Called
578	All Versions	Privileged object operation
592	All Versions	A new process has been created
593	All Versions	A process has exited
594	All Versions	A handle to an object has been duplicated
595	All Versions	Indirect access to an object has been obtained
600	All Versions	A process was assigned a primary token
601	Windows 2003	Attempt to install service
602	Windows 2003	Scheduled Task created
608	Windows 2003	User Right Assigned
609	All Versions	User Right Removed
610	Windows 2000	New Trusted Domain
	Windows 2003	New Trusted Domain
611	Windows 2000	Removing Trusted Domain

Event ID	OS	Title
	Windows 2003	Trusted Domain Removed
612	All Versions	Audit Policy Change
613	All Versions	IPSec policy agent started
614	All Versions	IPSec policy agent disabled
615	Windows 2000	IPSEC PolicyAgent Service
	Windows 2003	IPSec Services
616	Windows 2000	IPSec policy agent encountered a potentially serious failure
617	Windows 2000/2003,DC	Kerberos Policy Changed
618	Windows XP/2000/2003	Encrypted Data Recovery Policy Changed
619	All Versions	Quality of Service Policy Changed
620	Windows 2000	Trusted Domain Information Modified
	Windows 2003	Trusted Domain Information Modified
621	Windows 2003	System Security Access Granted
622	Windows 2003	System Security Access Removed
623	Windows 2003	Per User Audit Policy was refreshed
624	Windows 2000/2003	User Account Created
625	Windows 2003	Per user auditing policy set for user
	Windows 2000, DC	User Account Type Change
626	Windows 2000/2003	User Account Enabled
627	Windows 2000/2003	Change Password Attempt
628	Windows 2000/2003	User Account password set
629	Windows 2003	User Account Disabled
630	Windows 2000/ 2003	User Account Deleted
631	Windows 2000/2003, DC	Group created
632	Windows 2000/2003, DC	Group member added or removed
633	Windows 2000/2003, DC	Group member added or removed
634	Windows 2000/2003, DC	Group deleted
635	Windows 2000/2003	Group created
636	Windows 2000/2003	Group member added or removed
637	Windows 2000/2003	Group member added or removed
638	Windows 2000/2003	Group deleted
639	Windows 2000/2003	Group changed
640	All Versions	General Account Database Change
641	Windows 2000/2003, DC	Group changed
642	Windows 2000/2003	User Account Changed
643	Windows 2000	Domain Policy Changed

Event ID	OS	Title
	Windows 2003	Domain Policy Changed
644	All Versions	User Account Locked Out
645	Windows 2000/2003, DC	Computer Account Created
646	Windows 2000/2003, DC	Computer Account Changed
647	Windows 2000/2003, DC	Computer Account Deleted
648	Windows 2000/2003, DC	Group created
649	Windows 2000/2003, DC	Group changed
650	Windows 2000/2003, DC	Group member added or removed
651	Windows 2000/2003, DC	Group member added or removed
652	Windows 2000/2003, DC	Group deleted
653	Windows 2000/2003, DC	Group created
654	Windows 2000/2003, DC	Group changed
655	Windows 2000/2003, DC	Group member added or removed
656	Windows 2000/2003, DC	Group member added or removed
657	Windows 2000/2003, DC	Group deleted
658	Windows 2000/2003, DC	Group created
659	Windows 2000/2003, DC	Group changed
660	Windows 2000/2003, DC	Group member added or removed
661	Windows 2000/2003, DC	Group member added or removed
662	Windows 2000/2003, DC	Group deleted
663	Windows 2000/2003, DC	Group created
664	Windows 2000/2003, DC	Group changed
665	Windows 2000/2003, DC	Group member added or removed
666	Windows 2000/2003, DC	Group member added or removed
667	Windows 2000/2003, DC	Group deleted
668	Windows 2000/2003, DC	Group Type Changed
669	All Versions	Add SID History
670	All Versions	Add SID History
671	Windows 2003	User Account Unlocked
672	Windows 2000	Authentication Ticket Granted
	Windows 2003	Authentication Ticket Request
673	Windows 2000	Service Ticket Granted
	Windows 2003	Service Ticket Request
674	Windows 2000	Ticket Granted Renewed
	Windows 2003	Service Ticket Renewed
675	Windows 2000/2003, DC	Pre-authentication failed

Event ID	OS	Title
676	Windows 2000	Authentication Ticket Request Failed
	Windows 2003	Authentication Ticket Request Failed
677	Windows 2000	Service Ticket Request Failed
	Windows 2003	Service Ticket Request Failed
678	All Versions	Account Mapped for Logon by
679	Windows 2000	The name: %2 could not be mapped for logon by: %1
680	Windows 2000	Account Used for Logon by
	Windows 2003	Logon attempt
681	Windows 2000	The logon to Account:%2 by: %1 from workstation: %3 failed
	Windows 2003	The logon to Account:%2 by: %1 from workstation: %3 failed
682	Windows XP/2000/2003	Session reconnected to winstation
683	Windows XP/2000/2003	Session disconnected from winstation
684	Windows 2003	Set the security descriptor of members of administrative groups
685	Windows 2003	Account Name Changed
686	Windows 2003	Password of the following user accessed
687	All Versions	Application group operation
688	Windows 2003	Application group operation
689	Windows 2003	Application group operation
690	Windows 2003	Application group operation
691	Windows 2003	Application group operation
692	All Versions	Application group operation
693	Windows 2003	Application group operation
694	Windows 2003	Application group operation
695	Windows 2003	Application group operation
696	Windows 2003	Application group operation
806	Windows 2003	Per User Audit Policy was refreshed
807	Windows 2003	Per user auditing policy set for user

Windows Server 2003/2000Security Events by Category/Policy

Category: System Events — Policy: Audit system events

Event ID	Title
512	Windows NT is starting up
513	Windows NT is shutting down
514	An authentication package has been loaded by the Local Security Authority
515	A trusted logon process has registered with the Local Security Authority
516	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits
517	The audit log was cleared
518	An notification package has been loaded by the Security Account Manager
519	A process is using an invalid local procedure call (LPC) port
520	The system time was changed

Category: Logon/Logoff — Policy: Audit logon events

Event ID	Title
528	Successful Logon
529	Logon Failure - Unknown user name or bad password
530	Logon Failure - Account logon time restriction violation
531	Logon Failure - Account currently disabled
532	Logon Failure - The specified user account has expired
533	Logon Failure - User not allowed to logon at this computer
534	Logon Failure - The user has not been granted the requested logon type at this machine
535	Logon Failure - The specified account's password has expired
536	Logon Failure - The NetLogon component is not active
537	Logon failure - The logon attempt failed for other reasons
538	User Logoff
539	Logon Failure - Account locked out
540	Successful Network Logon
551	User-initiated Logoff
552	Logon attempt using explicit credentials
682	Session reconnected to winstation
683	Session disconnected from winstation

Category: Object Access — Policy: Audit object access

Event ID	Title
560	Object Open
561	Handle Allocated
562	Handle Closed
563	Object Open for Delete
564	Object Deleted
567	Object Access Attempt

Category: Directory Service — Policy: Audit directory service access

Event ID	Title
565	Object Open (Active Directory)
	Object Open (W3 Active Directory)
566	Object Operation (W3 Active Directory)

Category: Privilege Use — Policy: Audit privilege use

Event ID	Title
576	Special privileges assigned to new logon
577	Privileged Service Called
578	Privileged object operation

Category: Detailed Tracking — Policy: Audit process tracking

Event ID	Title
592	A new process has been created
593	A process has exited
594	A handle to an object has been duplicated
595	Indirect access to an object has been obtained
600	A process was assigned a primary token
601	Attempt to install service
602	Scheduled Task created
615	IPSEC PolicyAgent Service

Category: Policy Change — Policy: Audit policy change

Event ID	Title
608	User Right Assigned
609	User Right Removed
610	New Trusted Domain
	New Trusted Domain
611	Removing Trusted Domain
	Trusted Domain Removed
612	Audit Policy Change
613	IPSec policy agent started
614	IPSec policy agent disabled
616	IPSec policy agent encountered a potentially serious failure
617	Kerberos Policy Changed
618	Encrypted Data Recovery Policy Changed
619	Quality of Service Policy Changed
620	Trusted Domain Information Modified
	Trusted Domain Information Modified
621	System Security Access Granted
622	System Security Access Removed
623	Per User Audit Policy was refreshed
625	Per user auditing policy set for user
806	Per User Audit Policy was refreshed
807	Per user auditing policy set for user

Category: Account Logon — Policy: Audit account logon events

Event ID	Title
672	Authentication Ticket Granted
	Authentication Ticket Request
673	Service Ticket Granted
	Service Ticket Request
674	Ticket Granted Renewed
	Service Ticket Renewed
675	Pre-authentication failed
676	Authentication Ticket Request Failed
	Authentication Ticket Request Failed
677	Service Ticket Request Failed
	Service Ticket Request Failed

Event ID	Title
678	Account Mapped for Logon by
679	The name: %2 could not be mapped for logon by: %1
680	Account Used for Logon by
	Logon attempt
681	The logon to Account:%2 by: %1 from workstation: %3 failed
	The logon to Account:%2 by: %1 from workstation: %3 failed

Category: Account Management — Policy: Audit account management

Event ID	Title
624	User Account Created
625	User Account Type Change
626	User Account Enabled
627	Change Password Attempt
628	User Account password set
629	User Account Disabled
630	User Account Deleted
631	Group created
632	Group member added or removed
633	Group member added or removed
634	Group deleted
635	Group created
636	Group member added or removed
637	Group member added or removed
638	Group deleted
639	Group changed
640	General Account Database Change
641	Group changed
642	User Account Changed
643	Domain Policy Changed
	Domain Policy Changed
644	User Account Locked Out
645	Computer Account Created
646	Computer Account Changed
647	Computer Account Deleted
648	Group created
649	Group changed

Event ID	Title
650	Group member added or removed
651	Group member added or removed
652	Group deleted
653	Group created
654	Group changed
655	Group member added or removed
656	Group member added or removed
657	Group deleted
658	Group created
659	Group changed
660	Group member added or removed
661	Group member added or removed
662	Group deleted
663	Group created
664	Group changed
665	Group member added or removed
666	Group member added or removed
667	Group deleted
668	Group Type Changed
669	Add SID History
670	Add SID History
671	User Account Unlocked
684	Set the security descriptor of members of administrative groups
685	Account Name Changed
686	Password of the following user accessed
687	Application group operation
688	Application group operation
689	Application group operation
690	Application group operation
691	Application group operation
692	Application group operation
693	Application group operation
694	Application group operation
695	Application group operation
696	Application group operation