



Hewlett Packard
Enterprise

HPE Security ArcSight Connectors

SmartConnector for Windows Event Log –
Unified: Symantec Mail Security for Exchange

Supplemental Configuration Guide

August 14, 2015

Supplemental Configuration Guide

SmartConnector for Microsoft Windows Event Log – Unified: Symantec Mail Security for Exchange

May 15, 2014

Copyright © 2010 – 2014 Hewlett Packard Enterprise Development LP

Warranty

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

Restricted Rights Legend

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

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

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

Revision History

Date	Description
08/14/2015	Updated Event Logging section.
05/15/2014	Added support for Microsoft Exchange Server 7.0 on Microsoft Windows 2008 R2 and Microsoft Windows 2012 R2.
09/30/2013	Updated "Collect Events from the Event Log" procedure.
09/28/2012	First edition of this configuration guide.

Contents

Product Overview.....	15
Event Logging.....	15
Connector Installation and Configuration	15
Collect Events from the Event Log.....	15
Symantec Mail Security Windows Event Log Mappings to ArcSight Fields	16
General	16
Managed Components.....	16
Event 0.....	16
Management Service	16
Event 1.....	16
Event 2.....	16
Event 3.....	16
Event 4.....	16
Event 5.....	16
Event 6.....	17
Event 7.....	17
Event 8.....	17
Event 9.....	17
Event 10, 11, 12.....	17
Event 50.....	17
Event 51.....	17
Event 52, 102, 152, 212.....	17
Event 53.....	17
Event 54.....	18
Event 55.....	18
Event 56.....	18
Event 57.....	18
Event 58.....	18
Event 59.....	18
Event 60.....	18
Event 61.....	18
Event 62.....	19
Event 63.....	19
Event 100.....	19
Event 101.....	19
Event 103.....	19
Event 104.....	19
Event 105.....	19

Event 106.....	19
Event 150.....	19
Event 151.....	20
Event 153.....	20
Event 154.....	20
Event 155.....	20
Event 156.....	20
Event 157.....	20
Event 158.....	20
Event 200.....	20
Event 201.....	20
Event 202.....	21
Event 203.....	21
Event 204.....	21
Event 205.....	21
Event 206.....	21
Event 207.....	21
Event 208.....	21
Event 209.....	21
Event 210.....	21
Event 211.....	22
Event 213.....	22
Event 214.....	22
Event 215.....	22
Event 216.....	22
Event 217.....	22
Event 218.....	22
Event 220.....	22
Event 221.....	22
Event 301.....	23
Microsoft Exchange	23
Event 1.....	23
Event 2.....	23
Event 3.....	23
Event 4.....	23
Event 5.....	23
Event 6.....	23
Event 7.....	23
Event 8.....	24
Event 9.....	24

Event 10.....	24
Event 11.....	24
Event 12.....	24
Event 13.....	24
Event 14.....	24
Event 15.....	25
Event 16.....	25
Event 17.....	25
Event 18.....	25
Event 19.....	25
Event 20.....	25
Event 21.....	25
Event 22.....	25
Event 23.....	25
Event 24.....	26
Event 25.....	26
Event 26.....	26
Event 27.....	26
Event 28.....	26
Event 29.....	26
Event 30.....	26
Event 31.....	26
Event 32.....	27
Event 33.....	27
Event 34.....	27
Event 35.....	27
Event 36.....	27
Event 37.....	27
Event 38.....	27
Event 39.....	28
Event 41.....	28
Event 42.....	28
Event 43.....	28
Event 44.....	28
Event 45.....	28
Event 46.....	28
Event 47.....	29
Event 48.....	29
Event 49.....	29
Event 51.....	29

Event 52.....	29
Event 53.....	29
Event 54.....	30
Event 55.....	30
Event 56.....	30
Event 57.....	30
Event 58.....	30
Event 59.....	30
Event 60.....	31
Event 61.....	31
Event 62.....	31
Event 63.....	31
Event 64.....	31
Event 65.....	31
Event 67.....	32
Event 68.....	32
Event 69.....	32
Event 70.....	32
Event 71.....	32
Event 72.....	32
Event 73.....	32
Event 74.....	33
Event 75.....	33
Event 76.....	33
Event 77.....	33
Event 78.....	33
Event 79.....	33
Event 80.....	33
Event 81.....	33
Event 82.....	34
Event 83.....	34
Event 84.....	34
Event 85.....	34
Event 86.....	34
Event 87.....	34
Event 88.....	34
Event 91.....	34
Event 92.....	35
Event 93.....	35
Event 94.....	35

Event 95.....	35
Event 98.....	35
Event 99.....	36
Event 100.....	36
Event 101.....	36
Event 102.....	36
Event 103.....	36
Event 104.....	37
Event 105.....	37
Event 106.....	37
Event 107.....	37
Event 108.....	37
Event 109.....	37
Event 110.....	38
Event 111.....	38
Event 112.....	38
Event 113.....	38
Event 114.....	38
Event 115.....	38
Event 116.....	38
Event 117.....	38
Event 118.....	39
Event 119.....	39
Event 120.....	39
Event 121.....	39
Event 122.....	39
Event 123.....	39
Event 124.....	39
Event 125.....	39
Event 126.....	40
Event 127.....	40
Event 128.....	40
Event 129.....	40
Event 130.....	40
Event 131.....	40
Event 132.....	40
Event 133.....	40
Event 134.....	40
Event 135.....	41
Event 136.....	41

Event 137	41
Event 138	41
Event 139	41
Event 140	41
Event 141	41
Event 142	41
Event 143	41
Event 144	42
Event 146	42
Event 147	42
Event 148	42
Event 149	42
Event 150	42
Event 151	42
Event 152	42
Event 153	43
Event 154	43
Event 155	43
Event 156	43
Event 157	43
Event 158	43
Event 159	43
Event 160	44
Event 161	44
Event 162	44
Event 163	44
Event 164	44
Event 165	44
Event 166	44
Event 167	44
Event 168	45
Event 169	45
Event 170	45
Event 171	45
Event 172	45
Event 173	45
Event 174	45
Event 175	46
Event 176	46
Event 177	46

Event 178.....	46
Event 179.....	46
Event 180.....	46
Event 181.....	46
Event 182.....	47
Event 183.....	47
Event 184.....	47
Event 185.....	47
Event 186.....	47
Event 187.....	47
Event 188.....	47
Event 189.....	47
Event 190.....	48
Event 191.....	48
Event 192.....	48
Event 193.....	48
Event 194.....	48
Event 195.....	48
Event 196.....	48
Event 197.....	49
Event 198.....	49
Event 199.....	49
Event 200.....	49
Event 201.....	49
Event 203.....	49
Event 204.....	49
Event 205.....	49
Event 206.....	50
Event 207.....	50
Event 208.....	50
Event 209.....	50
Event 210.....	50
Event 211.....	50
Event 212.....	50
Event 213.....	50
Event 214.....	51
Event 215.....	51
Event 218.....	51
Event 219.....	51
Event 220.....	51

Event 221	52
Event 222	52
Event 223	52
Event 224	52
Event 225	52
Event 226	52
Event 227	52
Event 228	52
Event 229	53
Event 230	53
Event 231	53
Event 232	53
Event 233	53
Event 234	53
Event 235	53
Event 236	53
Event 237	54
Event 238	54
Event 239	54
Event 240	54
Event 241	54
Event 242	54
Event 243	54
Event 246	54
Event 260	54
Event 261	55
Event 262	55
Event 263	55
Event 264	55
Event 265	55
Event 266	55
Event 267	55
Event 268	55
Event 269	56
Event 270	56
Event 271	56
Event 272	56
Event 273	56
Event 274	56
Event 275	56

Event 276.....	56
Event 277.....	57
Event 278.....	57
Event 279.....	57
Event 280.....	57
Event 281.....	57
Event 282.....	57
Event 283.....	57
Event 284.....	57
Event 285.....	58
Event 286.....	58
Event 288.....	58
Event 289.....	58
Event 290.....	58
Event 291.....	58
Event 292.....	59
Event 293.....	59
Event 294.....	59
Event 295.....	59
Event 296.....	59
Event 297.....	59
Event 298.....	59
Event 299.....	60
Event 300.....	60
Event 301.....	60
Event 302.....	60
Event 303.....	60
Event 304.....	60
Event 305.....	60
Event 306.....	61
Event 307.....	61
Event 308.....	61
Event 309.....	61
Event 310.....	61
Event 311.....	61
Event 312.....	61
Event 313.....	61
Event 314.....	62
Event 315.....	62
Event 316.....	62

Event 317	62
Event 318	62
Event 319	62
Event 320	62
Event 321	63
Event 322	63
Event 323	63
Event 324	63
Event 325	63
Event 326	63
Event 327	63
Event 328	64
Event 329	64
Event 330	64
Event 331	64
Event 332	64
Event 333	64
Event 334	65
Event 335	65
Event 336	65
Event 337	65
Event 338	65
Event 339	65
Event 340	65
Event 341	65
Event 342	66
Event 343	66
Event 344	66
Event 345	66
Event 346	66
Event 347	66
Event 348	66
Event 349	67
Event 350	67
Event 351	67
Event 352	67
Event 353	67
Event 354	67
Event 355	68
Event 356	68

Event 357	68
Event 358	68
Event 359	68
Event 360	68
Event 361	69
Event 362	69
Event 363	69
Event 364	69
Event 365	69
Event 366	69
Event 367	70
Event 368	70
Event 369	70
Event 370	70
Event 371	70
Event 372	70
Event 373	70
Event 374	70
Event 375	71
Event 376	71
Event 377	71
Event 378	71
Event 379	71
Event 380	71
Event 381	71
Event 382	72
Event 383	72
Event 384	72
Event 385	72
Event 386	72
Event 387	72
Event 388	72
Event 389	72
Event 390	73
Event 391	73
Event 392	73
Event 393	73
Event 394	73
Event 395	73
Event 396	73

Event 397	74
Event 398	74
Event 399	74
Event 400	74
Event 401	74
Event 402	74
Event 403	74
Event 404	75
Event 405	75
Event 406	75
Event 407	75
Event 408	75
Event 409	75
Event 410	75
Event 411	75
Event 412	76
Event 413	76

SmartConnector for Microsoft Windows Event Log – Unified: Symantec Mail Security for Exchange

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Unified: Symantec Mail Security for Exchange and its event mappings to ArcSight data fields. Symantec Mail Security 6.5 and 7.0 on Windows 2008 R2 and 2012 R2 are supported.

The *ArcSight SmartConnector Mappings to Windows Security Events* document provides the main mappings for the Windows Event Log SmartConnectors; the field mappings listed in this document are specifically for the *SmartConnector for Windows Event Log – Unified: Symantec Mail Security for Exchange*.

Product Overview

Symantec Mail Security for Microsoft Exchange provides high-performance, integrated mail protection against virus threats, spam, and security risks, and enforces company policies.

Event Logging

Symantec Mail Security for Exchange Server events and policy violations are reported in the Microsoft Windows Event Log. The event log displays information, warning, and error events. The SmartConnector for Microsoft Windows Event Log – Unified can be used to receive these events.

System Administrator privileges are required to configure or modify Symantec Mail Security settings.

Connector Installation and Configuration

Follow the installation and configuration procedures in the [SmartConnector Configuration Guide for Microsoft Windows Event Log – Unified](#), selecting **Microsoft Windows Event Log – Unified** as the connector to be configured.

Collect Events from the Event Log

To set up the connector to collect application events:

- 1 From \$ARCSIGHT_HOME\current\bin, double-click **runagentsetup.bat**.
- 2 Select **Modify Connector** on the window displayed and click **Next**.
- 3 Select **Modify connector parameters** and click **Next**.
- 4 Select **Navigate to the Modify table parameters** window.
- 5 To collect events from an application log, modify the **Application** field by selecting **true** for event collection in the Application field and enter **Symantec Mail Security** in the **Custom Log Names** field.

You can specify multiple Custom Log Names in a comma-separated format; for example:

`Symantec Mail Security, Exchange Auditing`
- 6 Click **Next** to update the parameters; when you receive the successful update message, click **Next**.

- 7 Select **Exit** and click **Next** to exit the configuration wizard.
- 8 Restart the connector for your changes to take effect.

For more information about application event support, see the *SmartConnector Configuration Guide for Microsoft Windows Event Log – Unified*.

Symantec Mail Security Windows Event Log Mappings to ArcSight Fields

General

ArcSight ESM Field	Device-Specific Field
Source Service Name	EventSource
Device Vendor	'Symantec'
Device Product	'Mail Security for Microsoft Exchange'

Managed Components

Event 0

ArcSight ESM Field	Device-Specific Field
Name	'Insufficient rights to access this application'

Management Service

Event 1

ArcSight ESM Field	Device-Specific Field
Name	'Service'
Message	

Event 2

ArcSight ESM Field	Device-Specific Field
Name	'Threat Event Feed'
Message	

Event 3

ArcSight ESM Field	Device-Specific Field
Name	'Computer State Feed'
Message	

Event 4

ArcSight ESM Field	Device-Specific Field
Device Action	'Stopped'

Event 5

ArcSight ESM Field	Device-Specific Field
Device Action	'Started'

Event 6

ArcSight ESM Field	Device-Specific Field
Name	'Settings'
Message	

Event 7

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get Product Computer Key'
Message	

Event 8

ArcSight ESM Field	Device-Specific Field
Name	'Server Feed'
Message	

Event 9

ArcSight ESM Field	Device-Specific Field
Destination Service Name	'Symantec Mail Security Management'

Event 10, 11, 12

ArcSight ESM Field	Device-Specific Field
Destination Service Name	'Symantec Mail Security Management'

Event 50

ArcSight ESM Field	Device-Specific Field
Name	'Threat Event Feed Enabled'
Device Action	'Enabled'

Event 51

ArcSight ESM Field	Device-Specific Field
Name	'Threat Event Feed Disabled'
Device Action	'Disabled'

Event 52, 102, 152, 212

ArcSight ESM Field	Device-Specific Field
Name	'Failed to read configuration from registry'
Message	'Registry=', 'Using default value ='

Event 53

ArcSight ESM Field	Device-Specific Field
Name	'Failed to update the registry'
Message	

Event 54

ArcSight ESM Field	Device-Specific Field
Name	'Unable to read database location from registry'
Message	

Event 55

ArcSight ESM Field	Device-Specific Field
Name	'Unable to open database connection'
Message	'DataBase Path =[file path]'
File Path	file path

Event 56

ArcSight ESM Field	Device-Specific Field
Name	'Unexpected COM exception occurred'
Message	'Unexpected COM exception occurred'

Event 57

ArcSight ESM Field	Device-Specific Field
Name	'Database query failed'
Message	'Database Query Failed. FunctionName ='

Event 58

ArcSight ESM Field	Device-Specific Field
Name	'Querying data'
Message	'Querying for Last days of data'

Event 59

ArcSight ESM Field	Device-Specific Field
Name	'Database is reset'
Message	'Last PageHandle was '

Event 60

ArcSight ESM Field	Device-Specific Field
Name	'No data available to send'
Message	

Event 61

ArcSight ESM Field	Device-Specific Field
Name	'Threat event feed sent.'
Message	'Threat Event Feed Sent.'

Event 62

ArcSight ESM Field	Device-Specific Field
Name	'Failed to open threat event feed registry key'
Reason	reason code

Event 63

ArcSight ESM Field	Device-Specific Field
Name	'Failed to Open Threat Event Feed Registry Key'
Message	'Created New Threat Event Feed Registry Key'

Event 100

ArcSight ESM Field	Device-Specific Field
Device Action	'Enabled'

Event 101

ArcSight ESM Field	Device-Specific Field
Device Action	'Disabled'

Event 103

ArcSight ESM Field	Device-Specific Field
Name	'Failed to update the registry'
Message	

Event 104

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get Virus Definition Version'
Message	

Event 105

ArcSight ESM Field	Device-Specific Field
Name	'Computer State Feed Sent'
Message	

Event 106

ArcSight ESM Field	Device-Specific Field
Name	'Failed to open computer state feed registry keys'
Reason	reason code

Event 150

ArcSight ESM Field	Device-Specific Field
Device Action	'Enabled'

Event 151

ArcSight ESM Field	Device-Specific Field
Device Action	'Disabled'

Event 153

ArcSight ESM Field	Device-Specific Field
Name	'Failed to update the registry'
Message	

Event 154

ArcSight ESM Field	Device-Specific Field
Name	' Unable to get OS Details'
Message	

Event 155

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get Adapter Details'
Message	

Event 156

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get Machine Details'
Message	

Event 157

ArcSight ESM Field	Device-Specific Field
Name	'Computer Data Feed Sent'
Message	

Event 158

ArcSight ESM Field	Device-Specific Field
Name	'Failed to open computer data feed registry keys'
Reason	reason code

Event 200

ArcSight ESM Field	Device-Specific Field
Name	'Process file'
File Name	file name
Message	'Process: ', 'File: [file name] ', 'Line: '

Event 201

ArcSight ESM Field	Device-Specific Field
Name	'Registry write failure'
Message	'This error occurred while attempting to write to registry key'

Event 202

ArcSight ESM Field	Device-Specific Field
Name	'NT Event Log full'
Message	'Unable to record events'

Event 203

ArcSight ESM Field	Device-Specific Field
Name	'Failed to initialize Server Feed'
Message	

Event 204

ArcSight ESM Field	Device-Specific Field
Name	'Unable to Initialize COM for Server Feed'
Message	

Event 205

ArcSight ESM Field	Device-Specific Field
Device Action	'Disabled'

Event 206

ArcSight ESM Field	Device-Specific Field
Device Action	'Enabled'

Event 207

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get SMSMSE Service Status Field'
Message	

Event 208

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get SMSMSE Service Scan Status Field'
Message	

Event 209

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get currently SMSMSE Virus Definition and Revision Field'
Message	

Event 210

ArcSight ESM Field	Device-Specific Field
Name	'Server Feed Sent'
Message	

Event 211

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get SMSMSE Virus Defintion Licence Information Field'
Message	

Event 213

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get SMSMSE Server Name Field'
Message	

Event 214

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get Exchange Server Installed Roles Field'
Message	

Event 215

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get Installed SMSMSE Version Field'
Message	

Event 216

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get Installed Exchange Version Field'
Message	

Event 217

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get Installed Exchange Domain Name Field'
Message	

Event 218

ArcSight ESM Field	Device-Specific Field
Name	'Failed to open server feed registry keys'
Reason	reason code

Event 220

ArcSight ESM Field	Device-Specific Field
Name	'Error in executing PowerShell command'
Message	message text

Event 221

ArcSight ESM Field	Device-Specific Field
Name	'Unable to get currently SMSMSE Virus Revision Field'
Message	

Event 301

ArcSight ESM Field	Device-Specific Field
Name	'Failed to push nse to spc server'
Reason	reason code

Microsoft Exchange**Event 1**

ArcSight ESM Field	Device-Specific Field
Name	'Auto-Protect'
Message	

Event 2

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate/Rapid Release'
Message	

Event 3

ArcSight ESM Field	Device-Specific Field
Name	'Manual and Scheduled Scanning'
Message	

Event 4

ArcSight ESM Field	Device-Specific Field
Device Action	'enabled'

Event 5

ArcSight ESM Field	Device-Specific Field
Device Action	'disabled'

Event 6

ArcSight ESM Field	Device-Specific Field
Name	'Auto-Protect options changed'
Message	

Event 7

ArcSight ESM Field	Device-Specific Field
Name	'Settings'
Message	

Event 8

ArcSight ESM Field	Device-Specific Field
Name	'VSAPI'
Message	

Event 9

ArcSight ESM Field	Device-Specific Field
Name	'Error'
Message	

Event 10

ArcSight ESM Field	Device-Specific Field
Name	'Added scan'
Message	'Added Scan: [Scan Type]'
Device Action	'Added'
Device Custom String 5	Scan Type

Event 11

ArcSight ESM Field	Device-Specific Field
Name	'Removed scan'
Message	'Removed Scan: [Scan Type]'
Device Action	'Removed'
Device Custom String 5	Scan Type

Event 12

ArcSight ESM Field	Device-Specific Field
Name	'Modified scan'
Message	'Modified Scan: [Scan Type]'
Device Action	'Modified'
Device Custom String 5	Scan Type

Event 13

ArcSight ESM Field	Device-Specific Field
Name	'Scan statistics'
Message	'Files Scanned: [file name]', 'Number Infected:', 'Number Repaired:'
File Name	file name

Event 14

ArcSight ESM Field	Device-Specific Field
Name	'Started Scan'
Message	'Started Scan: [Scan Type]'
Device Action	'Started'
Device Custom String 5	Scan Type

Event 15

ArcSight ESM Field	Device-Specific Field
Name	'Property Violation'
Message	

Event 16

ArcSight ESM Field	Device-Specific Field
Name	'Unscannable'
Message	

Event 17

ArcSight ESM Field	Device-Specific Field
Name	' Console Remote Install'
Message	

Event 18

ArcSight ESM Field	Device-Specific Field
Name	'Scanning mailbox'
Message	'Scanning mailbox'

Event 19

ArcSight ESM Field	Device-Specific Field
Name	'Console LiveUpdate'
Message	

Event 20

ArcSight ESM Field	Device-Specific Field
Name	'Heartbeat'
Message	

Event 21

ArcSight ESM Field	Device-Specific Field
Device Action	'stopped'

Event 22

ArcSight ESM Field	Device-Specific Field
Name	'Removed files from quarantine'
Message	'Removed file(s) from quarantine'
Device Action	'Removed'

Event 23

ArcSight ESM Field	Device-Specific Field
Name	'Global options changed'
Message	

Event 24

ArcSight ESM Field	Device-Specific Field
Name	'Reset scanning statistics'
Message	

Event 25

ArcSight ESM Field	Device-Specific Field
Device Action	'Updated'

Event 26

ArcSight ESM Field	Device-Specific Field
Name	'Background Scanning'
Message	

Event 27

ArcSight ESM Field	Device-Specific Field
Name	'Debug trace'
Message	'Debug Trace: File: [file name]', 'Line:'
File Name	file name

Event 28

ArcSight ESM Field	Device-Specific Field
Name	'Service failed to start'
Message	'Service failed to start. Check the log for other errors'

Event 29

ArcSight ESM Field	Device-Specific Field
Name	'Unable to record events'
Message	'NT Event Log full. Unable to record events'

Event 30

ArcSight ESM Field	Device-Specific Field
Name	'Virus Definitions Update was successful'
Message	'New virus definitions were retrieved'

Event 31

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate has determined that no update is necessary'
Message	'You already have the most recent virus definitions'

Event 32

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was unable to check for new virus definitions'
Message	'More information may be available in', 'HOSTBUSY'

Event 33

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was successful'
Message	'LiveUpdate was successful. New virus definitions were retrieved. A system restart is required to use them'

Event 34

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was unable to check for new virus definitions'
Message	'More information may be available in [file path]', 'NO CARRIER'
File Path	file path

Event 35

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was unable to complete successfully'
Message	'More information may be available in [file path]'
File Path	file path

Event 36

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was unable to complete successfully'
Message	'More information may be available in [file path]', 'CRITICAL ERROR'
File Path	file path

Event 37

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was canceled'
Message	

Event 38

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate exited with an unknown result'
Message	'More information may be available in [file path]'
File Path	file path

Event 39

ArcSight ESM Field	Device-Specific Field
Name	'Denied access to scan public folder'
Message	'Denied access to scan public folder'

Event 41

ArcSight ESM Field	Device-Specific Field
Name	'Out of Memory'
Message	

Event 42

ArcSight ESM Field	Device-Specific Field
Name	'Unable to Auto-Protect mailbox'
Message	'Unable to Auto-Protect mailbox'

Event 43

ArcSight ESM Field	Device-Specific Field
Name	'Auto-Protect process failed to start'
Message	

Event 44

ArcSight ESM Field	Device-Specific Field
Name	'Could not resolve Email address'
Message	'Could not resolve Email address'

Event 45

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine Failure'
Message	'This error occurred while scanning the attachment [file name] of message [subject] located in [file path]'
Reason	reason code
File Path	file path
File Name	file name
File Type	'attachment'
Additional data	subject

Event 46

ArcSight ESM Field	Device-Specific Field
Name	'Cannot scan a cab file within a cab file'
Message	'This error occurred while scanning the attachment of message located in', '(unused)'

Event 47

ArcSight ESM Field	Device-Specific Field
Name	'Do not have access privileges to folder'
Message	'Do not have access privileges to folder'

Event 48

ArcSight ESM Field	Device-Specific Field
Name	'The message with subject was changed'
Message	'The message with subject was changed before Symantec Mail Security for Microsoft Exchange could make desired changes. The action taken has been changed to Log Only.'

Event 49

ArcSight ESM Field	Device-Specific Field
Name	'Started scan
Message	message text
Device Action	'Started'

Event 51

ArcSight ESM Field	Device-Specific Field
Name	'The DLL for CAB files was not found'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 52

ArcSight ESM Field	Device-Specific Field
Name	'The DLL for LZ files was not found'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 53

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error in opening a compressed file'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 54

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error in accessing a compressed file'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 55

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error in updating a compressed file'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 56

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error in closing a compressed file'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 57

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error in extracting a file from a compressed file'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 58

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error in accessing a file from a compressed file'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 59

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error in decrypting a file in a compressed file'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 60

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error with a split file inside a compressed file'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment of message located in', '(unused)'

Event 61

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error disk full'
File Name	file name
File Path	file path
Message	'Scan Engine error disk full. This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 62

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error out of memory'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 63

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error'
File Name	file name
File Path	file path
Message	'There are too many levels in a compressed file. This error occurred while scanning the attachment [file name] of message located in [file path]'

Event 64

ArcSight ESM Field	Device-Specific Field
Name	'General Scan Engine error'
File Name	file name
File Path	file path
Message	'This error occurred while scanning the attachment [file name] of message located in [file path]. (unused)'

Event 65

ArcSight ESM Field	Device-Specific Field
Name	'Unable to backup message'
Message	'Unable to backup message from [file path] with subject before scan'
File Path	file path

Event 67

ArcSight ESM Field	Device-Specific Field
Name	'Unable to write file'
Message	'Unable to write file [file name]'
File Name	file name

Event 68

ArcSight ESM Field	Device-Specific Field
Name	'Unable to initialize Scan Engine'
Message	'The virus definitions may be missing or corrupt. Perform a LiveUpdate to retrieve the latest virus definitions'

Event 69

ArcSight ESM Field	Device-Specific Field
Name	'Mailbox or public folder could not be scanned due to a logon failure'
Message	'Mailbox or public folder could not be scanned to a logon failure. The mailbox or public folder may be invalid, corrupt, or missing.'

Event 70

ArcSight ESM Field	Device-Specific Field
Name	'The temporary directory specified in the registry value TempFileDir is invalid'
Message	

Event 71

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate retrieved new files but the virus definitions could not be updated'
Message	

Event 72

ArcSight ESM Field	Device-Specific Field
Name	'File is at line'
Message	'File: [file name]', 'Line:'
File Name	file name

Event 73

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan does not have configuration information'
Message	'Scheduled Scan does not have configuration information'

Event 74

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start since the service has already been started'
Message	

Event 75

ArcSight ESM Field	Device-Specific Field
Name	'A serious problem with event logging has occurred but the service still started'
Message	

Event 76

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start due to the program settings could not be obtained or is invalid'

Event 77

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start due to low memory conditions'

Event 78

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start due to problems with virus scanning statistics'

Event 79

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start since the NT account specified is not an Exchange Administrator. Check the account used in 'Services' Control Panel applet and verify that the account has Administrator rights'

Event 80

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start since due the inability to monitor mailboxes and/or public folders'

Event 81

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start due to the inability to logon to the Exchange Server'

Event 82

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start due to the inability to create some SMSMSE objects'

Event 83

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start due to problems with Microsoft Exchange's public folders'

Event 84

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start due to the inability to obtain a list of mailboxes'

Event 85

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start since the Auto-Protect process could not be started'

Event 86

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start due to the inability to logon to mailboxes'

Event 87

ArcSight ESM Field	Device-Specific Field
Name	'Service can not start'
Message	'Service can not start due to problems starting the SMSMSE engine'

Event 88

ArcSight ESM Field	Device-Specific Field
Name	'Items have been released from quarantine'
Message	'item(s) have been released from quarantine'

Event 91

ArcSight ESM Field	Device-Specific Field
Name	'Scanning folder'
Message	'Scanning folder [file path]'
File Path	file path

Event 92

ArcSight ESM Field	Device-Specific Field
Name	'The scan job was stopped'
Device Action	'Stopped'

Event 93

ArcSight ESM Field	Device-Specific Field
Name	'Error packaging the attachment for submission to Quarantine Server'
Message	'Error packaging the attachment [file name] for submission to Quarantine Server. Error [reason code]'
File Name	file name
Reason	reason code

Event 94

ArcSight ESM Field	Device-Specific Field
Name	'Error sending the attachment to Quarantine Server'
Message	'Error sending the attachment [file name] to Quarantine Server [host name]'
File Name	file name
Reason	reason
Destination Host Name	host name

Event 95

ArcSight ESM Field	Device-Specific Field
Name	'Scan options changed'
Message	

Event 98

ArcSight ESM Field	Device-Specific Field
Device Action	'Completed'
Name	'Completed Scan'
Message	Completed Scan: [Scan Type] Violations: [numViolation] Log Only: [logOnly] Repair attachment/message body: [numRepairAttachmentAndMessageBody] Quarantine attachment/message body: [numQuarantine] Delete attachment/message body: [numDeleteAttachmentAndMessageBody] Delete message: [numDeleteMessage] Take no action: [numTakeNoAction]'
Device Custom String 5	Scan Type
Additional data	numViolation
Additional data	logOnly
Additional data	numQuarantine
Additional data	numDeleteAttachmentAndMessageBody
Additional data	numDeleteMessage
Additional data	numRepairAttachmentAndMessageBody
Additional data	numTakeNoAction

Event 99

ArcSight ESM Field	Device-Specific Field
Name	'Interrupted Scan'
Message	'Interrupted Scan: [Scan Type] Violations: [numViolation] Log Only: [logOnly] Repair attachment/message body: [numRepairAttachmentAndMessageBody] Quarantine attachment/message body: [numQuarantine] Delete attachment/message body: [numDeleteAttachmentAndMessageBody] Delete message: [numDeleteMessage] Take no action: [numTakeNoAction]'
Device Action	'Interrupted'
Device Custom String 5	Scan Type
Additional data	numViolation
Additional data	logOnly
Additional data	numQuarantine
Additional data	numDeleteAttachmentAndMessageBody
Additional data	numDeleteMessage
Additional data	numTakeNoAction

Event 100

ArcSight ESM Field	Device-Specific Field
Name	'Error sending alert to SMSMSE Alert server'
Message	'Error sending alert to SMSMSE Alert server [host name]'
Destination Host Name	host name

Event 101

ArcSight ESM Field	Device-Specific Field
Name	'Error opening message store'
Message	'Error opening message store with MAPI Error Code'
Reason	reason code

Event 102

ArcSight ESM Field	Device-Specific Field
Name	'Items have failed to be released from the quarantine'
Message	'item(s) have failed to be released from the quarantine.'

Event 103

ArcSight ESM Field	Device-Specific Field
Name	'Failed to quarantine attachment'
File Name	file name
File Path	file path
Message	'Failed to quarantine attachment named [file name] in message with subject in [file path]'

Event 104

ArcSight ESM Field	Device-Specific Field
Name	'Error occurred sending Windows Messenger service alert'
Message	'Error occurred sending Windows Messenger service alert to [host name]', 'Additional info:', '(unused)'
Destination Host Name	host name

Event 105

ArcSight ESM Field	Device-Specific Field
Name	'Failed to write quarantine report for attachment'
Message	'Failed to write quarantine report for attachment [file name] in message store in [file path] message with subject'
File Name	file name
File Path	file path

Event 106

ArcSight ESM Field	Device-Specific Field
Name	'Quarantine Server is full'
Destination Host Name	host name
File Name	file Name
Message	'Quarantine Server [host name] is full. Could not send the attachment [file name]'

Event 107

ArcSight ESM Field	Device-Specific Field
Name	'Service started'
Device Action	'started'
Device Version	version number

Event 108

ArcSight ESM Field	Device-Specific Field
Name	'Found a message that was not consistent with cached scan results'
Message	'The message was located in [file path]'
File Path	file path

Event 109

ArcSight ESM Field	Device-Specific Field
Name	'Failed to backup attachment'
File Name	file name
File Path	file path
Message	'Failed to backup attachment named [file name] in message with subject in [file path]'

Event 110

ArcSight ESM Field	Device-Specific Field
Name	'A process failed to start'
Message	'The process [service name] failed to start ([reason code])'
Destination Service Name	service name
Reason	reason code

Event 111

ArcSight ESM Field	Device-Specific Field
Name	'Update of information in header of file failed'
Message	'Update of information in header of file failed due to revision clash'

Event 112

ArcSight ESM Field	Device-Specific Field
Name	'Encrypted File Header was Invalid and could not be read'
Message	

Event 113

ArcSight ESM Field	Device-Specific Field
Name	'Deletion of Quarantined file failed'
Message	

Event 114

ArcSight ESM Field	Device-Specific Field
Name	'Could not restore quarantined file'
Message	

Event 115

ArcSight ESM Field	Device-Specific Field
Name	'Quarantined file contains header from older version of SMSMSE'
Message	

Event 116

ArcSight ESM Field	Device-Specific Field
Name	'File decryption failed'
Message	

Event 117

ArcSight ESM Field	Device-Specific Field
Name	'File encryption failed'
Message	

Event 118

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSELink packet size does not match declared size'
Message	

Event 119

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSELink packet is too large'
Message	

Event 120

ArcSight ESM Field	Device-Specific Field
Name	'The interface does not match'
Message	

Event 121

ArcSight ESM Field	Device-Specific Field
Name	'The function asked for is unknown or unsupported'
Message	

Event 122

ArcSight ESM Field	Device-Specific Field
Name	'The data size is not consistent with its intended use'
Message	

Event 123

ArcSight ESM Field	Device-Specific Field
Name	'The string data is not consistent with its intended use'
Message	

Event 124

ArcSight ESM Field	Device-Specific Field
Name	'The supplied buffer is too small for this operation'
Message	

Event 125

ArcSight ESM Field	Device-Specific Field
Name	'The operation succeeded but returned an unexpected response'
Message	

Event 126

ArcSight ESM Field	Device-Specific Field
Name	'The file could not be written'
Message	

Event 127

ArcSight ESM Field	Device-Specific Field
Name	'Internal logic error'
Message	

Event 128

ArcSight ESM Field	Device-Specific Field
Name	'An invalid configuration setting is in use'
Message	

Event 129

ArcSight ESM Field	Device-Specific Field
Name	'The named piped could not be opened'
Message	

Event 130

ArcSight ESM Field	Device-Specific Field
Name	'The error occurred receiving a connection to the named pipe'
Message	

Event 131

ArcSight ESM Field	Device-Specific Field
Name	'The error occurred flushing the contents of the pipe'
Message	

Event 132

ArcSight ESM Field	Device-Specific Field
Name	'The error occurred disconnecting from the pipe'
Message	

Event 133

ArcSight ESM Field	Device-Specific Field
Name	'The error occurred writing to the pipe'
Message	

Event 134

ArcSight ESM Field	Device-Specific Field
Name	'The error occurred reading from the pipe'
Message	

Event 135

ArcSight ESM Field	Device-Specific Field
Name	'A timeout occurred waiting for a response from the pipe'
Message	

Event 136

ArcSight ESM Field	Device-Specific Field
Name	'A thread could not be created'
Message	

Event 137

ArcSight ESM Field	Device-Specific Field
Name	'A thread did not end as expected'
Message	

Event 138

ArcSight ESM Field	Device-Specific Field
Name	'The process could not be started'
Message	

Event 139

ArcSight ESM Field	Device-Specific Field
Name	'The process was forcibly terminated'
Message	

Event 140

ArcSight ESM Field	Device-Specific Field
Name	'The process could not be stopped'
Message	

Event 141

ArcSight ESM Field	Device-Specific Field
Name	'The scan engine caused an exception'
Message	

Event 142

ArcSight ESM Field	Device-Specific Field
Name	'The scan engine did not return any results for the scan'
Message	

Event 143

ArcSight ESM Field	Device-Specific Field
Name	'The scan engine returned an error'
Message	

Event 144

ArcSight ESM Field	Device-Specific Field
Name	'The process has initiated a shutdown'
Message	

Event 146

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'Microsoft Exchange Store is asking for the wrong version'
Device Version	version number

Event 147

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'One or more parameters send to a VSAPI call are invalid'

Event 148

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'A Microsoft Exchange store memory allocation has failed.'

Event 149

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'GetTempFileName returned error'

Event 150

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'Scan function returned error on file [file name]'
File Name	file name

Event 151

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'VSAPI new stream function returned error'

Event 152

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'VSAPI read stream function returned error'

Event 153

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'VSAPI write stream function returned error'

Event 154

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'Create file failed with error while trying to open [file name]'
File Name	file name

Event 155

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'Open file failed with error while trying to open [file name]'
File Name	file name

Event 156

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'Write file failed with error while trying to write to [file name]'
File Name	file name

Event 157

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'Read file failed with error while trying to read from [file name]'
File Name	file name

Event 158

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'Close handle failed with error while closing file [file name]'
File Name	file name

Event 159

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSEVSAPI.DLL internal error'
Message	'Delete file failed with error while deleting file [file name]'
File Name	file name

Event 160

ArcSight ESM Field	Device-Specific Field
Name	'The scan completed but errors were returned'
Message	

Event 161

ArcSight ESM Field	Device-Specific Field
Name	'Internal Error'
Message	'SAVFMSEVSAPI.DLL Internal Error. An exception occurred calling JetGetTableColumnInfo'

Event 162

ArcSight ESM Field	Device-Specific Field
Name	'Internal Error'
Message	'SAVFMSEVSAPI.DLL Internal Error. An exception occurred calling JetRetrieveColumn\'

Event 163

ArcSight ESM Field	Device-Specific Field
Name	'Auto-Protect enabled'
Device Action	'enabled'

Event 164

ArcSight ESM Field	Device-Specific Field
Name	'Auto-Protect disabled'
Device Action	'disabled'

Event 165

ArcSight ESM Field	Device-Specific Field
Name	'Auto-Protect mode is changing'
Message	'Auto-Protect mode is changing from to (unused)'

Event 166

ArcSight ESM Field	Device-Specific Field
Name	'The process was forcibly terminated'
Message	'The process [service name] was forcibly terminated'
Destination Service Name	service name

Event 167

ArcSight ESM Field	Device-Specific Field
Name	'A process terminated unexpectedly'
Message	'The process [service name] terminated unexpectedly'
Destination Service Name	service name
Device Action	'terminated'

Event 168

ArcSight ESM Field	Device-Specific Field
Name	'A process was restarted'
Message	'The process [service name] was restarted'
Destination Service Name	service name
Device Action	'restarted'

Event 169

ArcSight ESM Field	Device-Specific Field
Name	'E-mail notifications could not be initialized using the MAPI profile'
Message	'E-mail notifications could not be initialized using the MAPI profile.' 'It failed with [reason code]', Notifications will not be sent.'
Reason	reason code

Event 170

ArcSight ESM Field	Device-Specific Field
Name	'A process in file at line'
Message	'Process:', 'File: [file name]', 'Line:'
File Name	file name

Event 171

ArcSight ESM Field	Device-Specific Field
Name	'Removed files from backup'
Message	'Removed file(s) from backup'
Device Action	'Removed'

Event 172

ArcSight ESM Field	Device-Specific Field
Name	'Items have been released from backup'
Message	'item(s) have been released from backup'

Event 173

ArcSight ESM Field	Device-Specific Field
Name	'Items have failed to be released from the backup'
Message	'item(s) have failed to be released from the backup.'

Event 174

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine error'
Message	'The time allowed to scan this item was exceeded. This error occurred while scanning the attachment [file name] of message located in [file path]', '(unused)'
File Name	file name
File Path	file path

Event 175

ArcSight ESM Field	Device-Specific Field
Name	'AutoProtect mode switch failed'
Message	'AutoProtect mode switch failed while changing from to with error'

Event 176

ArcSight ESM Field	Device-Specific Field
Name	'Registry Write Failure'
Message	'HRESULT =', 'This error occurred while attempting to write to registry key'
Reason	reason code

Event 177

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security for Microsoft Exchange is running in an Auto-Protect mode that uses the Microsoft Virus Scanning API (VSAPI)'
Message	'The version of Microsoft's Exchange Information Store installed has a serious bug when using this API. You should use version 5.5.2651.76 or later. The Exchange information store will not release handles properly and SSS for Microsoft Exchange and Exchange Information Store will experience problems after several days of operation. (See SAVFMSE's ReadMe.TXT for more information and Microsoft Knowledge Base article Q248838 for the latest fixes to Service Pack 3.)'

Event 178

ArcSight ESM Field	Device-Specific Field
Name	'An error was returned from DAPI'
Message	

Event 179

ArcSight ESM Field	Device-Specific Field
Name	'The mailbox could not be created'
Message	'The mailbox could not be created because it already exists'

Event 180

ArcSight ESM Field	Device-Specific Field
Name	'The mailbox could not be created the server specified does not have a private store'
Message	

Event 181

ArcSight ESM Field	Device-Specific Field
Name	'The service will be shutdown'
Message	'The service will be shutdown due to an unexpected result from a system call'

Event 182

ArcSight ESM Field	Device-Specific Field
Name	'The service will be shutdown'
Message	'The service will be shutdown due to an unexpected failure waiting for Microsoft Exchange to start'

Event 183

ArcSight ESM Field	Device-Specific Field
Name	'The service will be shutdown'
Message	'The service will be shutdown due to an unexpected failure monitoring the MExchangeIS service'

Event 184

ArcSight ESM Field	Device-Specific Field
Name	'The service will be shutdown'
Message	The service will be shutdown due to an unexpected result from a system call

Event 185

ArcSight ESM Field	Device-Specific Field
Name	'The service will be shutdown'
Message	'The service will be shutdown due to an unexpected failure initializing virus protection'

Event 186

ArcSight ESM Field	Device-Specific Field
Name	'The service will be shutdown'
Message	'A timeout occurred while waiting for Microsoft Exchange to initialize the VSAPI interface'

Event 187

ArcSight ESM Field	Device-Specific Field
Name	'The service will be shutdown'
Message	'The service will be shutdown due to an unexpected shutdown of the SAVFMSECTRL process'

Event 188

ArcSight ESM Field	Device-Specific Field
Name	'MAPI support for the Exchange public folders could not be initialized'
Message	

Event 189

ArcSight ESM Field	Device-Specific Field
Name	'The public information store has not been mounted'
Message	

Event 190

ArcSight ESM Field	Device-Specific Field
Name	'The list of public information stores is empty'
Message	

Event 191

ArcSight ESM Field	Device-Specific Field
Name	'HTTP Request for server sent to Queue Manager'
Message	'HTTP Request for server [host name] (port [destination port]) sent to Queue Manager'
Destination Port	destination port
Destination Host Name	host name

Event 192

ArcSight ESM Field	Device-Specific Field
Name	'The policy already exists'
Message	'The policy [Policy Settings] already exists'
Device Custom String 6	Policy Settings

Event 193

ArcSight ESM Field	Device-Specific Field
Name	'The policy does not exist'
Message	'The policy [Policy Settings] does not exist'
Device Custom String 6	Policy Settings

Event 194

ArcSight ESM Field	Device-Specific Field
Name	'The rule does not exist'
Message	'The rule [Rule Name] does not exist'
Device Custom String 4	Rule Name

Event 195

ArcSight ESM Field	Device-Specific Field
Name	'Invalid rule does not match subpolicy'
Message	'Invalid rule [Rule Name] does not match subpolicy'
Device Custom String 4	Rule Name
Device Custom String 6	Policy Settings

Event 196

ArcSight ESM Field	Device-Specific Field
Name	'Cannot rename Standard policy'
Message	

Event 197

ArcSight ESM Field	Device-Specific Field
Name	'Invalid rule in policy'
Message	'Invalid rule [Rule Name] in policy [Policy Settings]'
Device Custom String 4	Rule Name
Device Custom String 6	Policy Settings

Event 198

ArcSight ESM Field	Device-Specific Field
Name	'The policy or subpolicy is disabled'
Device Action	'Disabled'

Event 199

ArcSight ESM Field	Device-Specific Field
Name	'Packet sent to server from thread'
Message	'Packet sent to server [host name] from thread. Status:'
Destination Host Name	host name

Event 200

ArcSight ESM Field	Device-Specific Field
Name	'Content filter engine started'
Device Action	'Started'

Event 201

ArcSight ESM Field	Device-Specific Field
Name	'Content filter engine stopped'
Device Action	'Stopped'

Event 203

ArcSight ESM Field	Device-Specific Field
Name	'General Content Filter Error'
Message	message text

Event 204

ArcSight ESM Field	Device-Specific Field
Name	'Content filter engine failed to start'
Message	

Event 205

ArcSight ESM Field	Device-Specific Field
Name	'Content filter engine failed to shutdown properly'
Message	

Event 206

ArcSight ESM Field	Device-Specific Field
Name	'A content filter error occurred while analyzing a message body'
Message	

Event 207

ArcSight ESM Field	Device-Specific Field
Name	'A content filter error occurred while attempting to get the categories'
Message	

Event 208

ArcSight ESM Field	Device-Specific Field
Name	'No categories were selected for content filtering'
Message	

Event 209

ArcSight ESM Field	Device-Specific Field
Name	'The Content Filter option is disabled'
Message	

Event 210

ArcSight ESM Field	Device-Specific Field
Name	'Content Filter policies are disabled'
Message	

Event 211

ArcSight ESM Field	Device-Specific Field
Name	'Content Filter Policy invalid'
Message	'Missing action'

Event 212

ArcSight ESM Field	Device-Specific Field
Name	'Property policy applied'
Message	

Event 213

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred in the MMC Browser'
Message	'Check the event log for further details'

Event 214

ArcSight ESM Field	Device-Specific Field
Name	'There was an error parsing the XML file'
File Name	file Name
Message	'Check the event log for further details'

Event 215

ArcSight ESM Field	Device-Specific Field
Name	'An attachment has violated'
Message	message text
File Name	name of attached file
File Type	attachment file type
File Path	path to attachment
Device Custom String 1	Virus name
Device Custom String 4	Rule Name
Device Custom String 5	Scan Type
Device Custom String 6	Policy Settings
Additional data	subject
Device Action	Action on attachment

Event 218

ArcSight ESM Field	Device-Specific Field
Name	'The policy setting has been violated'
Message	'The located in [file path] has violated the following policy settings [Policy Settings]. The following actions were taken on it. For more information, visit'
File Path	file path
Device Custom String 6	Policy Settings

Event 219

ArcSight ESM Field	Device-Specific Field
Name	'An outbreak condition was detected'
Message	'Outbreak Rule Information: [Outbreak Rule Information] Threshold value for this rule is: [thresholdValue] Current level for this rule is: [currentLevel]'
Device Custom String 6	Outbreak Rule Information
Device Custom String 4	Rule Name
Additional data	thresholdValue
Additional data	currentLevel

Event 220

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred while attempting to obtain the current virus definitions version on this machine'
Message	

Event 221

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred with LiveUpdate'
Message	'Check the event log for further details'

Event 222

ArcSight ESM Field	Device-Specific Field
Name	'The id does not match any current command requests'
Message	

Event 223

ArcSight ESM Field	Device-Specific Field
Name	'The command request is not yet complete'
Message	

Event 224

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred when transferring product file updates to server'
Destination Host Name	host name
Message	'Check the event log for further details'

Event 225

ArcSight ESM Field	Device-Specific Field
Name	'The Outbreak rule does not exist'
Device Custom String 4	Rule Name

Event 226

ArcSight ESM Field	Device-Specific Field
Name	'The Outbreak rule already exists'
Device Custom String 4	Rule Name

Event 227

ArcSight ESM Field	Device-Specific Field
Name	'Outbreak rule type is invalid'
Device Custom String 4	Rule Name

Event 228

ArcSight ESM Field	Device-Specific Field
Bytes Out	bytes out
Bytes In	bytes in
Reason	reason code
Name	'Response to packet received from server'
Message	'Response to packet = [bytes out] received from server [bytes in]. Result code = [reason code]. New Status: ', 'Id = '

Event 229

ArcSight ESM Field	Device-Specific Field
Name	'The Report Name already exists'
Message	

Event 230

ArcSight ESM Field	Device-Specific Field
Name	'The Report Name does not exist'
Message	

Event 231

ArcSight ESM Field	Device-Specific Field
Name	'Reporting Config Encountered an error with the Registry'
Message	

Event 232

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred when processing product file updates sent from console'
Message	

Event 233

ArcSight ESM Field	Device-Specific Field
Name	'Remote install error'
File Path	file path
Message	'No files were found in [file path]'

Event 234

ArcSight ESM Field	Device-Specific Field
Name	'Deletion of Backup file failed'
Message	

Event 235

ArcSight ESM Field	Device-Specific Field
Name	'The backup directory has exceeded a set limit'
Message	'Limit Information:'

Event 236

ArcSight ESM Field	Device-Specific Field
Name	'The quarantine directory has exceeded a set limit'
Message	'Limit Information:'

Event 237

ArcSight ESM Field	Device-Specific Field
Name	'Scan job already exists'
Message	'Scan job already exists'

Event 238

ArcSight ESM Field	Device-Specific Field
Name	'Scan job does not exist'
Message	'Scan job does not exist'

Event 239

ArcSight ESM Field	Device-Specific Field
Name	'Cannot delete scan job'
Message	'Cannot delete scan job'

Event 240

ArcSight ESM Field	Device-Specific Field
Name	'SESA initialization failed'
Message	'Events will not be logged to SESA'

Event 241

ArcSight ESM Field	Device-Specific Field
Name	'Attempt to log event to SESA failed'
Message	'Attempt to log event to SESA failed'

Event 242

ArcSight ESM Field	Device-Specific Field
Name	'XML data is missing or invalid or corrupt'
Message	

Event 243

ArcSight ESM Field	Device-Specific Field
Name	'XML cannot be loaded - data is corrupt or XML Parser not available'
Message	

Event 246

ArcSight ESM Field	Device-Specific Field
Name	'Dictionary files failed to load'
Message	

Event 260

ArcSight ESM Field	Device-Specific Field
Name	'The content filter engine is already initialized'
Message	

Event 261

ArcSight ESM Field	Device-Specific Field
Name	'The content filter attempted an undefined/illegal action'
Message	

Event 262

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred modifying some or all settings on server'
Message	

Event 263

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred while scanning folder'
Message	'An error occurred while scanning folder', 'Required item properties are missing.'

Event 264

ArcSight ESM Field	Device-Specific Field
Name	'The requested command is not implemented on the server'
Message	

Event 265

ArcSight ESM Field	Device-Specific Field
Name	'Could not perform scan command on scan job'
Message	'Could not perform scan command on scan job.' 'Microsoft Exchange Service is not running'

Event 266

ArcSight ESM Field	Device-Specific Field
Name	'Unable to obtain virus definition set version'
Message	'Run LiveUpdate to obtain or repair these files'

Event 267

ArcSight ESM Field	Device-Specific Field
Name	'Timeout reached waiting for a Heartbeat message to arrive'
Message	

Event 268

ArcSight ESM Field	Device-Specific Field
Name	'The SMTP service is not running or not responding'
Message	'This service is necessary for the Heartbeat, and for all e-mail notifications'

Event 269

ArcSight ESM Field	Device-Specific Field
Name	'Unexpected attachment contents were found in a Heartbeat message'
Message	

Event 270

ArcSight ESM Field	Device-Specific Field
Name	'Unable to validate the Heartbeat Mailbox'
Message	

Event 271

ArcSight ESM Field	Device-Specific Field
Name	'Auto Protect is not enabled'
Message	

Event 272

ArcSight ESM Field	Device-Specific Field
Name	'The VSAPI dll is not loaded or is in an invalid state'
Message	

Event 273

ArcSight ESM Field	Device-Specific Field
Name	'The Exchange Information Store is not running, or is not loaded'
Message	

Event 274

ArcSight ESM Field	Device-Specific Field
Name	'The internal Ctrl process is not running or is not available to take commands'
Message	

Event 275

ArcSight ESM Field	Device-Specific Field
Name	'An Unexpected error has occurred'
Message	

Event 276

ArcSight ESM Field	Device-Specific Field
Name	'An error has occurred while performing a system heartbeat'
Message	'The error"' 'This error occurred while', '(unused)'

Event 277

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSE install on remote server failed'
Destination Host Name	host name
Message	message text

Event 278

ArcSight ESM Field	Device-Specific Field
Name	'SAVFMSE install on remote server failed'
Destination Host Name	host name
Message	'Failed:', 'ExtResult='

Event 279

ArcSight ESM Field	Device-Specific Field
Name	'The server has not responded with status of last request'
Message	'The request may not have executed successfully'

Event 280

ArcSight ESM Field	Device-Specific Field
Name	'SMSMSE ' ' saved'
Source User Name	user name (from NTUser)
Source NT Domain	domain (from NTDomain)

Event 281

ArcSight ESM Field	Device-Specific Field
Name	'Unable to save SAVFMSE settings'
Message	

Event 282

ArcSight ESM Field	Device-Specific Field
Name	'Thread sent to Queue Manager'

Event 283

ArcSight ESM Field	Device-Specific Field
Name	'An error has occurred trying to send an email notification'
Message	message text
Reason	reason code

Event 284

ArcSight ESM Field	Device-Specific Field
Name	'A critical failure occurred while attempting to use Symantec Virus Definitions'
Message	

Event 285

ArcSight ESM Field	Device-Specific Field
Name	'The Content Filter scored the body of message'
Message	'The Content Filter scored the body of message with a value of ', 'The format of the message was:'

Event 286

ArcSight ESM Field	Device-Specific Field
Name	'The specified Heartbeat mailbox is not on the local server'
Message	'The specified Heartbeat mailbox is not on the local server.(unused)'

Event 288

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred uploading virus definitions to server'
Destination Host Name	host name
Message	'Check the server for problems and retry the action.'

Event 289

ArcSight ESM Field	Device-Specific Field
Name	'Http error sending packet to server'
Destination Host Name	host name
Message	'New Status:'

Event 290

ArcSight ESM Field	Device-Specific Field
Name	'Error on server'
Destination Host Name	host name
Reason	reason code
Message	'Result code =', ' New Status:'

Event 291

ArcSight ESM Field	Device-Specific Field
Name	'A message has violated'
Message	message text
File Path	file path
File Name	file name
File Type	'file type'
Device Custom String 6	Policy Settings
Device Custom String 5	Scan Type
Device Custom String 4	Rule Name
Device Action	Action on attachment

Event 292

ArcSight ESM Field	Device-Specific Field
Name	'Virus definition and content license are getting expire'
Message	'Virus definition and content license for Symantec Mail Security for Microsoft Exchange on server [host name] will expire on [Expiry Date]'
Destination Host Name	host name
Device Custom Date 1	Expiry Date

Event 293

ArcSight ESM Field	Device-Specific Field
Name	'Virus definition and content license has expired, is damaged or is not installed'
Message	'Virus definition and content license for Symantec Mail Security for Microsoft Exchange on server [host name] has expired, is damaged, or is not installed.'
Destination Host Name	host name

Event 294

ArcSight ESM Field	Device-Specific Field
Name	'Server unknown Symantec Enterprise Licensing error'
Destination Host Name	host name
Message	'Unknown Symantec Enterprise Licensing Error'

Event 295

ArcSight ESM Field	Device-Specific Field
Name	'Virus definitions can not be updated because your content license has expired, is damaged, or is not installed'
Message	

Event 296

ArcSight ESM Field	Device-Specific Field
Name	'Unable to apply virus definition updates sent from console because content license is expired, damaged or not installed'
Message	

Event 297

ArcSight ESM Field	Device-Specific Field
Name	'Unable to install license file because the file is damaged, invalid, or expired'
Message	

Event 298

ArcSight ESM Field	Device-Specific Field
Name	'Unable to install license file sent from console because the file is invalid'
Message	

Event 299

ArcSight ESM Field	Device-Specific Field
Name	'Successfully installed SMSMSE Virus Definition license file'
Device Custom Date 1	Expiry date
Message	'The license is valid until [expiry date]'

Event 300

ArcSight ESM Field	Device-Specific Field
Name	'Unscannable content was found in a message'
File Path	file path
File Name	file name
Message	'Unscannable content was found in [file path] a message located in with subject [file name] in the attachment'

Event 301

ArcSight ESM Field	Device-Specific Field
Name	'Unable to log events to SESA because no IP address is set for the SESA server'
Message	

Event 302

ArcSight ESM Field	Device-Specific Field
Name	'Error sending scan job to server'
Destination Host Name	host name
Message	'The custom policy does not exist on the server.'

Event 303

ArcSight ESM Field	Device-Specific Field
Name	'The policy settings has been violated'
Message	'The located in has violated the following policy settings: [Policy Settings] The following actions were taken on it.'
Device Custom String 6	Policy Settings

Event 304

ArcSight ESM Field	Device-Specific Field
Name	'Heartbeat succeeded'
Message	

Event 305

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was unable to check for new virus definitions or decomposers'
Message	'More information may be available in' ' HOSTBUSY.'

Event 306

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was unable to check for new virus definitions or decomposers'
Message	'More information may be available in' 'NO CARRIER.'

Event 307

ArcSight ESM Field	Device-Specific Field
Name	'Virus definitions can not be updated because your content license has expired is damaged or is not installed'
Message	'Decomposers were successfully updated'

Event 308

ArcSight ESM Field	Device-Specific Field
Name	'Virus definitions can not be updated because your content license has expired is damaged or is not installed'
Message	'Decomposers were successfully updated. A system restart is required to use them'

Event 309

ArcSight ESM Field	Device-Specific Field
Name	'Virus definitions can not be updated because your content license has expired is damaged or is not installed'
Message	'You already have the most recent decomposers'

Event 310

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was successful'
Message	'New virus definitions and decomposers were retrieved'

Event 311

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was successful'
Message	'New virus definitions and decomposers were retrieved. A system restart is required to use them'

Event 312

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was successful'
Message	'New virus definitions were retrieved. You already have the most recent decomposers'

Event 313

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate retrieved new files but the virus definitions could not be updated'
Message	'Decomposers were successfully updated'

Event 314

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate retrieved new files but the virus definitions could not be updated'
Message	'Decompilers were successfully updated. A system restart is required to use them'

Event 315

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate retrieved new files but the virus definitions could not be updated'
Message	'You already have the most recent decompilers'

Event 316

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was successful'
Message	'New virus definitions were retrieved. A system restart is required to use them. You already have the most recent decompilers'

Event 317

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was successful'
Message	'New decompilers were retrieved. You already have the most recent virus definitions'

Event 318

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was successful'
Message	'New decompilers were retrieved. A system restart is required to use them. You already have the most recent virus definitions'

Event 319

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate has determined that no update is necessary'
Message	'You already have the most recent virus definitions and decompilers'

Event 320

ArcSight ESM Field	Device-Specific Field
Name	'The Symantec Mail Security for Microsoft Exchange Vulnerability Assessment scan was started'
Message	

Event 321

ArcSight ESM Field	Device-Specific Field
Name	'The Symantec Mail Security for Microsoft Exchange Vulnerability Assessment scan was completed'
Message	

Event 322

ArcSight ESM Field	Device-Specific Field
Name	'The Symantec Mail Security for Microsoft Exchange Vulnerability Assessment scan abnormally terminated'
Message	

Event 323

ArcSight ESM Field	Device-Specific Field
Name	'Attempt to log event to SESA failed because the SESA agent queue is full'
Message	'Once the queue is cleared events will start logging to SESA again'

Event 324

ArcSight ESM Field	Device-Specific Field
Name	'The message was rejected and the SMTP connection was terminated'
Message	'Spam detection, SCL=' 'Message Details:'

Event 325

ArcSight ESM Field	Device-Specific Field
Name	'The message was accepted, with the following additional action(s)'
Device Action	action
Message	'Spam detection, SCL=' 'Message Details:' 'The message was accepted, with the following additional action(s):'

Event 326

ArcSight ESM Field	Device-Specific Field
Name	'Failed to load heuristic anti-spam engine'
Message	'SPAM.DAT and/or SPAM.NET files may be missing or corrupt'

Event 327

ArcSight ESM Field	Device-Specific Field
Name	'The process was forcibly terminated'
Destination Process Name	process name
Message	message text
Device Action	'terminated'

Event 328

ArcSight ESM Field	Device-Specific Field
Name	'There are too many files within a compressed file'
File Path	file path
File Name	file name
Message	'Scan Engine error: This error occurred while scanning the attachment [file name] of message, located in [file path] '

Event 329

ArcSight ESM Field	Device-Specific Field
Name	'The maximum cumulative file size within a compressed file was exceeded'
File Path	file path
File Name	file name
Message	'Scan Engine error: This error occurred while scanning the attachment [file name] of message, located in [file path] '

Event 330

ArcSight ESM Field	Device-Specific Field
Name	'An outbreak condition is still being detected'
Device Custom String 4	Rule Name
Device Custom String 6	Outbreak Rule Information
Additional data	subject
Additional data	thresholdValue
Additional data	currentLevel

Event 331

ArcSight ESM Field	Device-Specific Field
Name	'A service started'
Destination Service Name	'Symantec Mail Security Utility Service'
Device Action	'Started'

Event 332

ArcSight ESM Field	Device-Specific Field
Name	'A service stopped'
Destination Service Name	'Symantec Mail Security Utility Service'
Device Action	'Stopped'

Event 333

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security Utility Service could not open service manager'
Message	

Event 334

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security Utility Service could not create service'
Message	

Event 335

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security Utility Service could not open service'
Message	

Event 336

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security Utility Service could not start'
Message	

Event 337

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security Utility Service bad service request'
Message	

Event 338

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security Utility Service could not be deleted'
Message	

Event 339

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security Utility Service handler not installed'
Message	

Event 340

ArcSight ESM Field	Device-Specific Field
Name	'The message was rejected and the SMTP connection was terminated'
Message	'Existing SCL', 'Symantec SCL=', ' Message Details:' ' The message was rejected and the SMTP connection was terminated.'

Event 341

ArcSight ESM Field	Device-Specific Field
Name	'Failed to load Symantec Premium AntiSpam engine'
Message	

Event 342

ArcSight ESM Field	Device-Specific Field
Name	'The message was rejected and the SMTP connection was terminated'
Message	'Message classified as:' ' Message Details:'

Event 343

ArcSight ESM Field	Device-Specific Field
Name	'The message was accepted'
Device Action	action
Message	'Message classified as:' ' Message Details:'

Event 344

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Premium AntiSpam license has expired, is damaged or is not installed'
Message	'Symantec Premium AntiSpam license for Symantec Mail Security for Microsoft Exchange on server has expired, is damaged, or is not installed'
Destination Host Name	host name

Event 345

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Premium AntiSpam license is getting expire'
Message	'Symantec Premium AntiSpam license for Symantec Mail Security for Microsoft Exchange on server will expire on'
Device Host Name	host name
Device Custom Date 1	Expiry date

Event 346

ArcSight ESM Field	Device-Specific Field
Name	'Successfully installed Symantec Premium AntiSpam license file'
Device Custom Date 1	Expiry date
Message	'The license is valid until [expiry date]'

Event 347

ArcSight ESM Field	Device-Specific Field
Name	'Invalid Symantec Premium AntiSpam license or Symantec Premium AntiSpam license has expired'
Message	

Event 348

ArcSight ESM Field	Device-Specific Field
Name	'SMTP scanning failed on the message'
Message	'SMTP scanning failed on the message with subject:' 'This message has been set as bad mail on the SMTP server.'

Event 349

ArcSight ESM Field	Device-Specific Field
Name	'Heuristic Antispam settings cannot be saved because Symantec Premium AntiSpam is currently installed'
Message	

Event 350

ArcSight ESM Field	Device-Specific Field
Name	'Unable to install license file sent from console because the file is expired'
Message	

Event 351

ArcSight ESM Field	Device-Specific Field
Name	'An external Anti-virus solution is scanning email traffic meant for Exchange'
Message	'If this continues your Exchange server could become corrupt. See help for how to exclude SMSMSE directories'

Event 352

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Premium AntiSpam license installed on the server'
Destination Host Name	host name
Message	'Enable and configure Premium AntiSpam to activate the service'

Event 353

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Premium AntiSpam registration failed on the server'
Destination Host Name	host name
Message	'The product will not receive spam definition updates until registration completes. If a valid license file has been provided, the console will display that the license is installed and will re-attempt registration when the feature is enabled via the console. To troubleshoot the registration issue, do the following: 1. Verify that your Exchange Server is running the Edge or Hub role. Premium AntiSpam is available only on Exchange Servers that run the Edge or Hub role. 2. Ensure that a valid, up-to-date Premium AntiSpam license is installed. 3. Confirm that the server has network and internet access. 4. Verify that DNS can resolve https://aztec.brightmail.com . 5. If using a proxy server, allow outbound secure https through firewall (port 443), for all users. 6. If using a proxy server, see the documentation for manually running Register.exe. For more information, check the event log.'

Event 354

ArcSight ESM Field	Device-Specific Field
Name	'There was an error on the server'
Destination Host Name	host name
Message	'Symantec Premium AntiSpam registration could not be completed. Install your license again.'

Event 355

ArcSight ESM Field	Device-Specific Field
Name	'There was an error on the server'
Destination Host Name	host name
Message	'There was an error on the server [host name] 'Virus scan messages during SMTP transport' option could not be enabled because on Exchange 2003 this requires a mailbox store or a public folder store to be mounted. Mount a store and try again.'

Event 356

ArcSight ESM Field	Device-Specific Field
Name	'Heartbeat message was already scanned and deleted by an external scan engine'
Message	'Exclude SMSMSE directories from future scans. See help for how to exclude SMSMSE directories.(unused),

Event 357

ArcSight ESM Field	Device-Specific Field
Destination Host Name	host name
Name	'Server was not able to receive Rapid Release Virus Definition update due to a failure to find a valid content license file'

Event 358

ArcSight ESM Field	Device-Specific Field
Name	'Server was not able to receive Rapid Release Virus Definition update'
Message	'Server [host name] was not able to receive Rapid Release Virus Definition update due to an FTP failure'
Destination Host Name	host name
Application Protocol	'FTP'

Event 359

ArcSight ESM Field	Device-Specific Field
Name	'Server was not able to receive Rapid Release Virus Definition update due to a failure'
Destination Host Name	host name
Reason	reason code

Event 360

ArcSight ESM Field	Device-Specific Field
Name	'Rapid Release virus definitions update could not be scheduled'
Destination Host Name	host name
Message	'The following Auto-Protect options are both enabled: Exchange background scanning, On virus definition update, force rescan before allowing access to information store. Disable at least one of these options to schedule Rapid Release updates'

Event 361

ArcSight ESM Field	Device-Specific Field
Name	'Rapid Release virus definitions update could not be scheduled'
Destination Host Name	host name
Message	"Run scan when virus definitions change' option is enabled for a scheduled scan. Disable this option for all scheduled scans to schedule Rapid Release updates'

Event 362

ArcSight ESM Field	Device-Specific Field
Name	'The following Auto-Protect options could not both be enabled'
Destination Host Name	host name
Message	'Rapid Release virus definitions update is enabled: 1. Exchange background scanning 2. On virus definition update, force rescan before allowing access to information store. Either disable at least one of these options or disable Rapid Release on LiveUpdate/Rapid Release Settings page, and try again.'

Event 363

ArcSight ESM Field	Device-Specific Field
Name	'The following Auto-Protect options could not both be enabled'
Destination Host Name	host name
Message	'Rapid Release virus definitions update is enabled: 1. Exchange background scanning 2. On virus definition update, force rescan before allowing access to information store. Either disable at least one of these options or disable Rapid Release on LiveUpdate/Rapid Release Settings page, and try again. 'Virus scan messages during SMTP transport' option could not be enabled since on Exchange 2003, this requires a mailbox store or a public folder store to be mounted. Mount a store and try again.'

Event 364

ArcSight ESM Field	Device-Specific Field
Name	"Run scan when virus definitions change' option could not be enabled'
Destination Host Name	host name
Message	'Rapid Release virus definitions update is enabled. Either disable this option or disable Rapid Release on LiveUpdate/Rapid Release Settings page, and try again'

Event 365

ArcSight ESM Field	Device-Specific Field
Name	'Internal error: Failed to retrieve message properties'
Message	'Content filtering, scanning statistics and message violation logging may be affected'

Event 366

ArcSight ESM Field	Device-Specific Field
Name	'Building Active Directory User Group Table Started'
Device Action	'Started'

Event 367

ArcSight ESM Field	Device-Specific Field
Name	'Building Active Directory User Group Table Completed Successfully'
Message	

Event 368

ArcSight ESM Field	Device-Specific Field
Name	'Building Active Directory User Group Table Failed'
Message	

Event 369

ArcSight ESM Field	Device-Specific Field
Name	'Scan process failed to reduce privileges'
Message	

Event 370

ArcSight ESM Field	Device-Specific Field
Name	'Failed to retrieve settings from the shared storage location'
Message	

Event 371

ArcSight ESM Field	Device-Specific Field
Name	'Failed to save setting to the shared storage location'
Message	

Event 372

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred when processing recipients list for releasing quarantine item(s) by mail'
Message	

Event 373

ArcSight ESM Field	Device-Specific Field
Name	'Unable to validate Recipient Mailbox'
Message	

Event 374

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred when creating a folder specified for the Save to folder setting'
Message	

Event 375

ArcSight ESM Field	Device-Specific Field
Name	'SMSMSE service is not started'
Message	

Event 376

ArcSight ESM Field	Device-Specific Field
Name	'SMSMSE service is starting'
Message	'Please try again once it is started'

Event 377

ArcSight ESM Field	Device-Specific Field
Name	'SMSMSE service is stopping'
Message	

Event 378

ArcSight ESM Field	Device-Specific Field
Name	name

Event 379

ArcSight ESM Field	Device-Specific Field
Name	'VSAPI scheduled background scanning has been enabled'
Device Action	'enabled'
Device Custom String 5	'VSAPI' (Scan Type)

Event 380

ArcSight ESM Field	Device-Specific Field
Name	'VSAPI scheduled background scanning has been disabled'
Device Action	'disabled'
Device Custom String 5	'VSAPI' (Scan Type))

Event 381

ArcSight ESM Field	Device-Specific Field
Device Action	action taken
Device Custom String 4	Rule Name
Device Custom String 5	Scan Type
Name	'The message located in SMTP has violated a policy'
Message	message text

Event 382

ArcSight ESM Field	Device-Specific Field
Name	name

Event 383

ArcSight ESM Field	Device-Specific Field
Name	'Released files from quarantine to email'
Device Action	'released'

Event 384

ArcSight ESM Field	Device-Specific Field
Name	'Released files from quarantine to file'
Device Action	'Released'
Additional data	numFile
Message	'Released [number of files] file(s) from quarantine to file'

Event 385

ArcSight ESM Field	Device-Specific Field
Name	'The Windows Task Scheduler service is not running'
Message	'Please start the Windows Task Scheduler service and then save your changes'

Event 386

ArcSight ESM Field	Device-Specific Field
Name	'The Windows Task Scheduler service is not running'
Message	'Start the Windows Task Scheduler service and then apply the scheduled scan settings'

Event 387

ArcSight ESM Field	Device-Specific Field
Name	'The Windows Task Scheduler service is not running'
Message	'Start the Windows Task Scheduler service and then apply the scheduled LiveUpdate settings'

Event 388

ArcSight ESM Field	Device-Specific Field
Name	'The Windows Task Scheduler service is not running'
Message	'Mail Security cannot generate scheduled reports until the service is started. Start the Windows Task Scheduler service, and Mail Security will generate scheduled reports'

Event 389

ArcSight ESM Field	Device-Specific Field
Name	'Unable to copy the license file'
Message	'Unable to copy the Symantec Premium AntiSpam license file to licenses folder'

Event 390

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security has failed to re-initialize the Premium AntiSpam engine'
Message	'If there are any new spam definitions, they would not be used during antispam processing'

Event 391

ArcSight ESM Field	Device-Specific Field
Name	'The Symantec Mail Security Utility service is not running'
Message	'This service is necessary to protect the Microsoft Exchange Server from spam. Please restart the service to continue to provide support for Symantec Premium AntiSpam'
Destination Service Name	'The Symantec Mail Security Utility'

Event 392

ArcSight ESM Field	Device-Specific Field
Name	'Failed to quarantine item'
File Path	file path
Message	'Please check the quarantine directory specified in the registry value 'QuarantineDirectoryStr' or contact your administrator if the problem persists. Failed to quarantine attachment'

Event 393

ArcSight ESM Field	Device-Specific Field
Name	'An error occurred in SMSMSE EWS Client component'
Message	'The following is the description of the error:'

Event 394

ArcSight ESM Field	Device-Specific Field
Name	'Scan Failed'
Message	'Scan Failed'

Event 395

ArcSight ESM Field	Device-Specific Field
Name	'The scan encountered an error'
Reason	reason code
Message	'The scan type encountered an error'

Event 396

ArcSight ESM Field	Device-Specific Field
Name	'The scan type could not be completed'
Reason	reason code
Message	'The scan could not be completed as Microsoft Exchange's Client Access Server is not reachable.'

Event 397

ArcSight ESM Field	Device-Specific Field
Name	'The Symantec Mail Security quarantine directory has exceeded a set threshold percentage limit'
Message	'Limit Information:'

Event 398

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security for Microsoft Exchange cannot verify the SMTP address for this display name'
Message	'Content filtering rules if enabled, will be skipped until this display name is resolved in Active Directory. LDAP Query:, Domain Names:'

Event 399

ArcSight ESM Field	Device-Specific Field
Name	'Virus definitions authenticity check failed'
Reason	reason code
Message	'Server will try to use previous virus definitions'

Event 400

ArcSight ESM Field	Device-Specific Field
Name	'No valid virus definitions are available'
Reason	reason code
Message	'Server will attempt to download new virus definitions. Error code: [reason code]. For more information, visit'

Event 401

ArcSight ESM Field	Device-Specific Field
Name	'Failed to initialize AV scanner'
Message	'The virus definitions are either missing or corrupt'
Reason	reason code

Event 402

ArcSight ESM Field	Device-Specific Field
Name	'Failed to get LegacyExchangeDN to build user address cache for the following SMTP addresses'
Destination Address	address

Event 403

ArcSight ESM Field	Device-Specific Field
Name	'Failed to get LegacyExchangeDN to build user address cache for the following SMTP addresses'
Destination Address	address
Message	'SMSMSE will retry building this cache after minutes'

Event 404

ArcSight ESM Field	Device-Specific Field
Name	'Virus definitions are old'
Message	'Virus definitions are days old. To remain protected ensure that Liveupdate is working properly'
Request URL	URL

Event 405

ArcSight ESM Field	Device-Specific Field
Name	'Background Scan of all Store databases completed'
Message	'Background Scan of all Store databases completed in hours(s) and minute(s). Total items were scanned from the start of scanning'
Additional data	numScanned
Device Custom String 5	'Background Scan' (Scan Type)

Event 406

ArcSight ESM Field	Device-Specific Field
Name	'Background Scanning is paused'
Message	'Either scan window is over or scan is disabled. Total items are scanned from the start of scanning'
Device Action	'paused'

Event 407

ArcSight ESM Field	Device-Specific Field
Name	'The spam configuration file update encountered errors'
Message	message text

Event 408

ArcSight ESM Field	Device-Specific Field
Name	'SMTP scanning failed on the message'
Message	'This message will be rescanned upon reaching the mailbox only if you have configured rescanning on Mail Security for the mailbox role.'

Event 409

ArcSight ESM Field	Device-Specific Field
Name	'Failed to initialize AV Engine'
Reason	Error code

Event 410

ArcSight ESM Field	Device-Specific Field
Name	'Failed to initialize AV Engine'
Message	'Failed to initialize AV Engine during RequestImmediateUpdateEx'

Event 411

ArcSight ESM Field	Device-Specific Field
Name	'Failed to save Quarantine server settings'

ArcSight ESM Field	Device-Specific Field
Message	'Failed to save Quarantine server settings, Server address specified by user is a Broadcast address'

Event 412

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Premium AntiSpam registration failed on the server'
Message	message text
Destination Host Name	host name

Event 413

ArcSight ESM Field	Device-Specific Field
Name	'Registry open in write mode failure'
Reason	reason code
Message	'Cannot open registry. Error code: [reason code] Please follow below URL for further details.'
