



# **Micro Focus Security ArcSight Connectors**

## **SmartConnector for Windows Event Log – Native: Symantec Mail Security for Exchange Supplemental Configuration Guide**

### **Supplemental Configuration Guide**

Document Release Date: April 16, 2018

Software Release Date: April 16, 2018

## Legal Notices

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

<https://www.microfocus.com>

## Copyright Notice

© Copyright 2010 - 2020 Micro Focus or one of its affiliates

Confidential computer software. Valid license from Micro Focus required for possession, use or copying. The information contained herein is subject to change without notice.

The only warranties for Micro Focus 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. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein.

No portion of this product's documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's internal use, without the express written permission of Micro Focus.

Notwithstanding anything to the contrary in your license agreement for Micro Focus ArcSight software, you may reverse engineer and modify certain open source components of the software in accordance with the license terms for those particular components. See below for the applicable terms.

US Governmental Rights. For purposes of your license to Micro Focus ArcSight software, "commercial computer software" is defined at FAR 2.101. If acquired by or on behalf of a civilian agency, the US Government acquires this commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in 48 CFR. 12.212 (Computer Software) and 12.211 (Technical Data) of the Federal Acquisition Regulation ("FAR") and its successors. If acquired by or on behalf of any agency within the Department of Defense ("DOD"), the US Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 CFR. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This US Government Rights Section 18.11 is in lieu of, and supersedes, any other FAR, DFARS, or other clause or provision that addresses government rights in computer software or technical data.

## Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are US registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

## Documentation Updates

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

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

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

[ArcSight Product Documentation on the Micro Focus Security Community](#)

## Support

### Contact Information

<b>Phone</b>	A list of phone numbers is available on the Technical Support Page: <a href="https://softwaresupport.softwaregrp.com/support-contact-information">https://softwaresupport.softwaregrp.com/support-contact-information</a>
<b>Support Web Site</b>	<a href="https://softwaresupport.softwaregrp.com/">https://softwaresupport.softwaregrp.com/</a>
<b>ArcSight Product Documentation</b>	<a href="https://communitysoftwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs">https://communitysoftwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs</a>

## Revision History

Date	Description
08/30/2016	Updated versions supported.
08/14/2015	Updated Event Logging section.
02/16/2015	First edition of this configuration guide.

# Contents

- SmartConnector for Microsoft Windows EventLog – Native: Symantec Mail Security for Exchange .13
  - Product Overview .....13
    - Event Logging .....13
  - Connector Installation and Configuration .....13
    - Collect Events from the Event Log .....13
  - Symantec Mail Security Windows Event Log Mappings to ArcSight Fields .....14
    - General .....14
    - Managed Components .....14
      - Event 0 .....14
    - Management Service .....14
      - Event 1 .....14
      - Event 2 .....15
      - Event 3 .....15
      - Event 4 .....15
      - Event 5 .....15
      - Event 6 .....15
      - Event 7 .....15
      - Event 8 .....16
      - Event 9 .....16
      - Event 10 .....16
      - Event 11 .....16
      - Event 12 .....16
      - Event 50 .....16
      - Event 51 .....16
      - Event 102, 152, 212 .....17
      - Event 53 .....17
      - Event 54 .....17
      - Event 60 .....17
      - Event 63 .....17
      - Event 100 .....17
      - Event 101 .....18
      - Event 103 .....18
      - Event 104 .....18
      - Event 105 .....18
      - Event 150 .....18
      - Event 151 .....18
      - Event 153 .....19

Event 154 .....	19
Event 155 .....	19
Event 156 .....	19
Event 157 .....	19
Event 202 .....	19
Event 203 .....	20
Event 204 .....	20
Event 205 .....	20
Event 206 .....	20
Event 207 .....	20
Event 208 .....	20
Event 209 .....	21
Event 210 .....	21
Event 211 .....	21
Event 213 .....	21
Event 214 .....	21
Event 215 .....	21
Event 216 .....	22
Event 217 .....	22
Event 221 .....	22
Microsoft Exchange .....	22
Event 1 .....	22
Event 2 .....	22
Event 3 .....	23
Event 4 .....	23
Event 5 .....	23
Event 6 .....	23
Event 7 .....	23
Event 8 .....	24
Event 9 .....	24
Event 14 .....	24
Event 15 .....	24
Event 16 .....	24
Event 17 .....	25
Event 19 .....	25
Event 20 .....	25
Event 21 .....	25
Event 22 .....	25
Event 23 .....	26
Event 24 .....	26
Event 25 .....	26

Event 26 .....	26
Event 28 .....	26
Event 29 .....	26
Event 30 .....	27
Event 31 .....	27
Event 33 .....	27
Event 37 .....	27
Event 41 .....	27
Event 43 .....	27
Event 45 .....	28
Event 68 .....	28
Event 70 .....	28
Event 71 .....	28
Event 74 .....	28
Event 75 .....	29
Event 76 .....	29
Event 77 .....	29
Event 78 .....	29
Event 79 .....	29
Event 80 .....	29
Event 81 .....	30
Event 82 .....	30
Event 83 .....	30
Event 84 .....	30
Event 85 .....	30
Event 86 .....	30
Event 87 .....	31
Event 92 .....	31
Event 95 .....	31
Event 98 .....	31
Event 99 .....	32
Event 107 .....	32
Event 110 .....	32
Event 111 .....	33
Event 112 .....	33
Event 113 .....	33
Event 114 .....	33
Event 115 .....	33
Event 116 .....	33
Event 117 .....	34
Event 118 .....	34

Event 119 .....	34
Event 120 .....	34
Event 121 .....	34
Event 122 .....	34
Event 123 .....	35
Event 124 .....	35
Event 125 .....	35
Event 126 .....	35
Event 127 .....	35
Event 128 .....	35
Event 129 .....	36
Event 130 .....	36
Event 131 .....	36
Event 132 .....	36
Event 133 .....	36
Event 134 .....	36
Event 135 .....	37
Event 136 .....	37
Event 137 .....	37
Event 138 .....	37
Event 139 .....	37
Event 140 .....	37
Event 141 .....	38
Event 142 .....	38
Event 143 .....	38
Event 144 .....	38
Event 160 .....	38
Event 161 .....	38
Event 162 .....	39
Event 163 .....	39
Event 164 .....	39
Event 167 .....	39
Event 168 .....	39
Event 177 .....	40
Event 178 .....	40
Event 179 .....	40
Event 180 .....	40
Event 181 .....	40
Event 182 .....	41
Event 183 .....	41
Event 184 .....	41



Event 185 .....	41
Event 186 .....	41
Event 187 .....	42
Event 188 .....	42
Event 189 .....	42
Event 190 .....	42
Event 196 .....	42
Event 198 .....	42
Event 200 .....	43
Event 201 .....	43
Event 205 .....	43
Event 206 .....	43
Event 207 .....	43
Event 208 .....	43
Event 209 .....	44
Event 210 .....	44
Event 211 .....	44
Event 212 .....	44
Event 213 .....	44
Event 215 .....	44
Event 219 .....	45
Event 220 .....	45
Event 221 .....	45
Event 222 .....	46
Event 223 .....	46
Event 229 .....	46
Event 230 .....	46
Event 231 .....	46
Event 232 .....	47
Event 234 .....	47
Event 240 .....	47
Event 242 .....	47
Event 243 .....	47
Event 246 .....	47
Event 260 .....	48
Event 261 .....	48
Event 262 .....	48
Event 264 .....	48
Event 266 .....	48
Event 267 .....	48
Event 268 .....	49

Event 269 .....	49
Event 270 .....	49
Event 271 .....	49
Event 272 .....	49
Event 273 .....	49
Event 274 .....	50
Event 275 .....	50
Event 279 .....	50
Event 280 .....	50
Event 281 .....	50
Event 283 .....	51
Event 284 .....	51
Event 291 .....	51
Event 292 .....	51
Event 293 .....	52
Event 295 .....	52
Event 296 .....	52
Event 297 .....	52
Event 298 .....	52
Event 301 .....	53
Event 304 .....	53
Event 307 .....	53
Event 308 .....	53
Event 309 .....	53
Event 310 .....	54
Event 311 .....	54
Event 312 .....	54
Event 313 .....	54
Event 314 .....	54
Event 315 .....	54
Event 316 .....	55
Event 317 .....	55
Event 318 .....	55
Event 319 .....	55
Event 320 .....	55
Event 321 .....	56
Event 322 .....	56
Event 323 .....	56
Event 326 .....	56
Event 330 .....	56
Event 331 .....	57

Event 332 .....	57
Event 333 .....	57
Event 334 .....	57
Event 335 .....	57
Event 336 .....	58
Event 337 .....	58
Event 338 .....	58
Event 339 .....	58
Event 341 .....	58
Event 344 .....	58
Event 345 .....	59
Event 347 .....	59
Event 349 .....	59
Event 350 .....	59
Event 351 .....	60
Event 356 .....	60
Event 358 .....	60
Event 365 .....	60
Event 366 .....	60
Event 367 .....	61
Event 368 .....	61
Event 369 .....	61
Event 370 .....	61
Event 371 .....	61
Event 372 .....	61
Event 373 .....	62
Event 374 .....	62
Event 375 .....	62
Event 376 .....	62
Event 377 .....	62
Event 379 .....	62
Event 380 .....	63
Event 381 .....	63
Event 382 .....	63
Event 384 .....	63
Event 385 .....	63
Event 386 .....	64
Event 387 .....	64
Event 388 .....	64
Event 389 .....	64
Event 390 .....	64

Event 391 .....	65
Event 401 .....	65
Event 404 .....	65
Event 405 .....	65
Event 406 .....	66
Event 409 .....	66
Event 410 .....	66
Event 411 .....	66
Event 412 .....	66
Event 414 .....	67
Send Documentation Feedback .....	68

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

This guide provides information about the SmartConnector for Microsoft Windows Event Log – Native: Symantec Mail Security for Exchange and its event mappings to ArcSight data fields. Symantec Mail Security 6.5, 7.0, and 7.5 on Windows 2008 R2 and 2012 R2 are supported.

The *SmartConnector for Microsoft Windows Event Log – Native Windows Security Event Mappings* 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 – Native: 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 – Native 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 – Native*, selecting **Microsoft Windows Event Log – Native** 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 – Native*.

## Symantec Mail Security Windows Event Log Mappings to ArcSight Fields

### General

ArcSight ESM Field	Device-Specific Field
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'
Name	Service Stopped

## Event 5

ArcSight ESM Field	Device-Specific Field
Device Action	'Started'
Name	Service 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'
Name	'Waiting for synchronization'
Message	'Waiting for synchronization with Symantec Mail Security Management Service Plug-in'

## Event 10

ArcSight ESM Field	Device-Specific Field
Name	'Achieved synchronization with Symantec Mail Security Management Service Plug-in'

## Event 11

ArcSight ESM Field	Device-Specific Field
Name	'Monitoring Symantec Mail Security Management Service Plug-in'

## Event 12

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Mail Security Management Service Plug-in Unavailable'

## Event 50

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

## Event 51

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



## Event 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 60

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

## 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
Name	'Computer State Feed Enabled'

## Event 101

ArcSight ESM Field	Device-Specific Field
Name	'Computer State Feed 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 150

ArcSight ESM Field	Device-Specific Field
Name	'Computer Data Feed Enabled'

## Event 151

ArcSight ESM Field	Device-Specific Field
Name	'Computer Data Feed 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 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
Name	'Server Feed is Disabled'

## Event 206

ArcSight ESM Field	Device-Specific Field
Name	'Server Feed is 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 221

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

## 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'
Name	'Auto-Protect enabled'

## Event 5

ArcSight ESM Field	Device-Specific Field
Device Action	'disabled'
Name	'Auto-Protect 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 14

ArcSight ESM Field	Device-Specific Field
Name	'Started Scan'
Message	Both ('Started Scan: ',%1)
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 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	Both (Removed';%1,' 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 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 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 37

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

## Event 41

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

## Event 43

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

## Event 45

ArcSight ESM Field	Device-Specific Field
Name	'Scan Engine Failure'
Message	Both ('This error occurred while scanning the attachment '%4,' of message '%3,' located in '%2')
Reason	%1 (reason code)
File Path	%2 (file path)
File Name	%4 (file name)
File Type	'attachment'
Additional data	%3 (subject)

## 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 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 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 92

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

## 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	Both ('Completed Scan: '%1,' Violations: '%3,' Log Only: '%4,' Quarantine attachment/message body: '%7,' Delete attachment/message body: '%8,' Delete message: '%9,' Take no action: '%10)
Device Custom String 5	Scan Type
Additional data	numViolation
Additional data	logOnly
Additional data	numQuarantine
Additional data	numDeleteAttachmentAndMessageBody
Additional data	numDeleteMessage
Additional data	numRepairAttchmentAndMessageBody
Additional data	numTakeNoAction

## Event 99

ArcSight ESM Field	Device-Specific Field
Name	'Interrupted Scan'
Message	Both ('Interrupted Scan: '%1,' Violations: '%3,' Log Only: '%4,' Quarantine attachment/message body: '%7,' Delete attachment/message body: '%8,' Delete message: '%9,' Take no action: '%10')
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 107

ArcSight ESM Field	Device-Specific Field
Name	'Service started'
Device Action	'started'
Device Custom String 2	Product Version

## Event 110

ArcSight ESM Field	Device-Specific Field
Name	'A process failed to start'
Message	Both ('The process '%1,' failed to start (%2,')')
Destination Service Name	%1 (service name)
Reason	%2 (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 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 167

ArcSight ESM Field	Device-Specific Field
Name	'A process terminated unexpectedly'
Message	Both ('The process '%1,' terminated unexpectedly')
Destination Service Name	%1 (service name)
Device Action	'terminated'

## Event 168

ArcSight ESM Field	Device-Specific Field
Name	'A process was restarted'
Message	Both ('The process '%12,' was restarted')
Destination Service Name	%1 (service name)
Device Action	'restarted'

## 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 196

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

## Event 198

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

## 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 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 215

ArcSight ESM Field	Device-Specific Field
Name	'An attachment has violated'
Message	%5 (message text)

ArcSight ESM Field	Device-Specific Field
File Name	%2 (name of attached file)
File Type	%1 (attachment file type)
File Path	%3 (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 219

ArcSight ESM Field	Device-Specific Field
Name	'An outbreak condition was detected'
Message	Both ('Outbreak Rule Information: '%1,' Threshold value for this rule is: '%2,' Current level for this rule is: '%3')
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	
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 234

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

## Event 240

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

## 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 264

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

## 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 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 283

ArcSight ESM Field	Device-Specific Field
Name	'An error has occurred trying to send an email notification'
Message	%1 (The error occurred while sending scan event notifications to administrators)
Reason	%2 (0x80004005)

## Event 284

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

## Event 291

ArcSight ESM Field	Device-Specific Field
Name	'A message has violated'
Message	%5 (The attachment 'Quarantined Attachment.txt' was Quarantined for the following reason(s): A Filtering Rule was violated.)
File Path	%3 (User1/Sent Items)
File Name	%2 (fwef)
File Type	%1 (message)
Device Custom String 6	Policy Settings
Device Custom String 5	Scan Type
Device Custom String 4	Rule Name
Device Action	Both (%5, '*was(*)for.*')

## 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	%1 (N15-195-H2140)

## 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 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 304

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

## 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	'Decompilers 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	'Decompilers 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 decompilers'

## 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	'Decomposers 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 decomposers'

## 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 decomposers'

## Event 317

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

## Event 318

ArcSight ESM Field	Device-Specific Field
Name	'LiveUpdate was successful'
Message	'New decomposers 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 decomposers'

## 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 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 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 341

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

## 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 '%1,' has expired, is damaged, or is not installed')

ArcSight ESM Field	Device-Specific Field
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 '%1,' will expire on '%2')
Device Host Name	%1 (host name)
Device Custom Date 1	%2 (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 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 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 358

ArcSight ESM Field	Device-Specific Field
Name	'Server was not able to receive Rapid Release Virus Definition update'
Message	'Server '%1(N15-H72),' was not able to receive Rapid Release Virus Definition update due to an FTP failure'
Destination Host Name	%1 (host name)
Application Protocol	'FTP'

## 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 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	%1 (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	%1 (message text)

## Event 382

ArcSight ESM Field	Device-Specific Field
Name	name

## 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 401

ArcSight ESM Field	Device-Specific Field
Name	'Failed to initialize AV scanner'
Message	'The virus definitions are either missing or corrupt'
Reason	%1 (reason code)

## Event 404

ArcSight ESM Field	Device-Specific Field
Name	'Virus definitions are old'
Message	'Virus definitions are '%1(2),' days old. To remain protected ensure that Liveupdate is working properly.'
Request URL	%2 (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 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'
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	%2 (Unable to communicate with Symantec to register. Please check your connection settings, and try again.)
Destination Host Name	host name

## Event 414

ArcSight ESM Field	Device-Specific Field
Name	'Symantec Premium AntiSpam registration failed on the server'
Message	%2 ('Unable to communicate with Symantec to register. Please check your connection settings, and try again.')
Destination Host Name	%1 (hostname)

# Send Documentation Feedback

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

## **Feedback on Supplemental Configuration Guide (Connectors )**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [arcsight\\_doc@microfocus.com](mailto:arcsight_doc@microfocus.com).

We appreciate your feedback!