
Micro Focus

Arcsight Management Center

Software Version: 3.1.0

Administrator's Guide

Document Release Date: February 2022

Software Release Date: Feburary 2022



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2022 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.

U.S. 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 U.S. 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 C.F.R. 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 U.S. Government acquires this commercial computer software and/or commercial computer software documentation subject to the terms of the Agreement as specified in 48 C.F.R. 227.7202-3 of the DOD FAR Supplement ("DFARS") and its successors. This U.S. 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 U.S. 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

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

Contents

Chapter 1: Arcsight Management Center Overview	17
Chapter 2: Software Installation	18
Overview	18
Installing Arcsight Management Center	20
Prerequisites for Installation	21
Installation Steps	22
GUI Mode Installation	23
Console Mode Installation	24
Silent Mode Installation	25
About Licenses for Silent Mode Installations	25
Generating the Silent Install Properties File	25
Installing Using the Generated Properties File	27
Next Steps After Installation	28
Enabling/Disabling Arcsight Management Center as a System Service	28
Starting Services Automatically for a Non-Root Installation	28
Configuring Firewall Rules	30
Configuring the Firewall on Arcsight Management Center Appliance ..	30
Arcsight Management Center Operations	32
Connecting to the Arcsight Management Center User Interface	32
Arcsight Management Center Processes	32
The Arcsight Management Center Daemon (arcmcd)	33
Uninstalling Software Arcsight Management Center	33
Uninstalling in GUI Mode	34
Uninstalling in Console Mode	34
Uninstalling in Silent Mode	34
Installing the Arcsight Management Center Agent	35
Arcsight Management Center Agent Operations	37
Uninstalling the Arcsight Management Center Agent	37
Installing a vCHA (VMware Workstation - VMware Player - ESXi)	38
Chapter 3: The User Interface	40
The Menu Bar	40
Monitoring Summary	40
Node Management	40
Configuration Management	41

User Management	41
Administration	41
ArcMC Name	42
Stats (EPS In/Out)	42
Job Manager	43
Site Map	43
History Management	44
Dashboard	45
Overview	45
Monitoring Managed Nodes	45
The Monitoring Summary Dashboard	46
Device Configuration for Device Type	47
Device Health Metrics	47
Drilling Down	48
Details and Health History	48
Data Charts	49
ADP License Usage for the Last 30 Days	49
EPS License Reporting	50
Keystones:	50
EPS License Usage Calculation	51
Host Status Exceptions	51
Monitoring Rules	52
Preset Rules	52
Preset Rules Description	53
Managing Rules	56
Monitoring Rules Parameters	57
Rule Verification	61
Custom Rules Examples	61
Device Rule Management	62
Device Inactive Notification	62
Managing Devices	64
Managing Device Rules	65
Configuring Email Notifications	65
Example Email Notification	66
Configuring SNMP Notifications	66
Topology View	69
Deployment View	70
Prerequisites for Instant Connector Deployment	71

Additional Requirements For Windows Platforms	72
Instant Connector Deployment	73
Deployment on Linux Platform Using Non-root User	74
Troubleshooting	76
If the SSH certificate changes...	76
Deploying a Connector in Transformation Hub (CTH) (Standalone ArcMC)	76
Editing a CTH	79
Undeploying CTHs	79
Deploying Collectors	79
Non-TLS Collectors Deployment	79
TLS Collectors Deployment	80
FIPS Collectors Deployment	80
Post Deployment Collector Property Update	80
SecureData Encryption	81
Chapter 5: Managing Nodes	82
Node Management	82
The Navigation Tree	82
The Management Panel	83
Management Tabs	83
Tab Controls	84
The Locations Tab	85
The Hosts Tab	85
The Containers Tab	87
The Connectors Tab	89
The Connector Summary Tab	90
The ConApps Tab	92
The Loggers Tab	92
The ArcMCs Tab	93
The TH Nodes Tab	94
The Collectors Tab	94
Locations	95
Adding a Location	95
Editing a Location	95
Viewing All Locations	96
Deleting a Location	96
Hosts	96
About Adding a Host	97

Prerequisites for Adding a Host (for each Host Type)	97
Node Authentication Credentials	100
Managing SmartConnectors on ArcMC	101
Adding a Host	102
Adding a Host with Containers	102
Adding Transformation Hub as a Host to ArcMC	103
Preparing to Add Transformation Hub as a Host (Standalone ArcMC)	103
Adding Transformation Hub as a Host	104
Adding Transformation Hub Non-Containerized (THNC) as a Host	104
Importing Multiple Hosts	105
Prerequisites for Importing Multiple Hosts	105
CSV File Format	105
Host Field Values	106
Import Hosts Procedure	109
Import Hosts Job Logs	109
Exporting Hosts	110
Viewing All Hosts	111
Viewing Managed Nodes on a Host	111
Updating (or Installing) the ArcMC Agent	111
Regenerating your Marketplace Certificate	112
Chapter 6: Managing ArcSight Products	113
Managing Connector Appliances (ConApps)	113
Rebooting a ConApp	113
Shutting Down a ConApp	114
Editing or Removing a Configuration for a ConApp	114
Setting a Configuration on ConApps	115
Managing Other ArcSight Management Centers	115
Rebooting an ArcMC	116
Shutting Down an ArcMC	116
Editing or Removing a Configuration for ArcMC	116
Upgrading ArcMC	117
Remote Upgrade Using Node Management	118
Local Upgrade of ArcMC	119
Setting a Configuration on Managed ArcMCs	119
Managing SmartConnectors on ArcMC	120
Managing Loggers	121
Rebooting a Logger	121

Shutting Down a Logger	121
Editing or Removing a Configuration for a Logger	122
Upgrading a Logger	122
Setting a Configuration on Loggers	125
Managing Containers	125
Viewing All Containers	126
Viewing Connectors in a Container	126
Editing a Container	126
Deleting a Container	127
Changing Container Credentials	127
Sending a Command to a Container	128
Upgrading All Connectors in a Container	128
Modifying logger.properties	130
Uploading Files Larger Than 100 MB under Repository	130
Restarting a Container	131
Viewing Container Logs	132
Deleting a Container Log	132
Enabling FIPS on a Container	133
Enabling FIPS Suite B on a Container	134
Adding a Connector to a Container	134
Running Logfu on a Container	135
Managing Certificates on a Container	136
Adding CA Certificates to a Container	136
Removing CA Certificates from a Container	137
Adding a CA Certs File to a Container	137
Enabling or Disabling a Demo Certificate on a Container	138
Adding Multiple Destination Certificates to a Container	139
Viewing Certificates on a Container	139
Resolving Invalid Certificate Errors	140
Running Diagnostics on a Container	140
Managing Connectors	141
Viewing All Connectors	141
Adding a Connector	141
Prerequisites	141
Editing Connector Parameters	144
Updating Simple Parameters for a Connector	144
Updating Table Parameters for a Connector	145
Updating Simple and Table Parameters for Multiple Connectors	145

Managing Destinations	146
Adding a Primary Destination to a Connector	147
Adding a Failover Destination to a Connector	147
Adding a Primary or Failover Destination to Multiple Connectors	148
Removing Destinations	149
Re-Registering Destinations	150
Editing Destination Parameters	150
Editing Destination Runtime Parameters	151
Managing Alternate Configurations	152
Defining a New Alternate Configuration	152
Editing an Alternate Configuration	153
Editing Alternate Configurations in Bulk	153
Sending a Command to a Destination	153
Deleting a Connector	154
Sending a Command to a Connector	154
Running Logfu on a Connector	155
Changing the Network Interface Address for Events	155
Developing FlexConnectors	156
Editing FlexConnectors	158
Sharing Connectors in ArcExchange	158
Packaging and Uploading Connectors	159
Downloading Connectors	161
Configuration Suggestions for Connector/Collector Types	163
Included FlexConnectors	164
Configuring the Check Point OPSEC NG Connector	164
Adding the MS SQL Server JDBC Driver	167
Adding the MySQL JDBC Driver	168
Chapter 7: Managing Configurations	169
Generator ID Manager	170
Generator ID Management	170
Setting Up Generator ID Management	170
Getting Generator ID for Non-managed Nodes	170
Setting Generator IDs on Managed Nodes	171
Configuration Management	171
The Configurations Table	172
The Details Tab	172
General	172

Properties	173
The Subscribers Tab	173
Non-Compliance Reports	174
Creating a Subscriber Configuration	174
Editing a Subscriber Configuration	175
Deleting a Subscriber Configuration	176
Importing a Subscriber Configuration	176
Managing Subscribers	177
Viewing Subscribers	178
Adding a Subscriber	178
Unsubscribing a Subscriber	179
Pushing a Subscriber Configuration	179
Push Validation	180
Common Causes for Push Failure	180
Push Remediation	181
Checking Subscriber Compliance	181
Comparing Configurations	182
Configuration Management Best Practices	183
Subscriber Configuration Types	184
Connector Configuration Types	184
BlueCoat Connector Configuration	184
FIPS Configuration	185
Map File Configuration	185
Uploading Map Files Larger Than 1 MB	186
Parser Override Configuration	186
Syslog Connector Configuration	187
Windows Unified Connector (WUC) External Parameters Configuration	187
Limitations to WUC External Parameters Configurations	187
Windows Unified Connector (WUC) Internal Parameters Configuration	189
Limitations to WUC Internal Parameters Configurations	189
ArcMC/Connector Appliance Configuration Types	190
ArcMC/Connector Appliance Configuration Backup Configuration	190
Destination Configuration Types	191
Destination Configuration Parameters	191
Networks and Zones	191
Logger Configuration Types	192
Logger Configuration Backup Configuration	192
Logger Connector Forwarder Configuration	193

Logger ESM Forwarder Configuration	194
Logger Filter Configuration	195
Logger SmartMessage Receiver Configuration	196
Logger Storage Group Configuration	196
Logger TCP Forwarder Configuration	197
Logger Transport Receiver Configuration	198
Logger UDP Forwarder Configuration	199
SecureData Configuration	200
System Admin Configuration Types	201
Authentication External	201
Authentication Local Password	202
Authentication Session	203
DNS Configuration	203
FIPS Configuration	203
Network Configuration	204
NTP Configuration	204
SMTP Configuration	204
SNMP Poll Configuration	205
SNMP Trap Configuration	206
Logger Initial Configuration Management	207
Importing a Logger Initial Configuration	207
Pushing a Logger Initial Configuration	208
Deleting a Logger Initial Configuration	209
Event History	210
Managing Logger Event Archives	210
Managing Event Archives	211
Managing Logger Peers	212
Viewing Peers or Peer Groups	212
Adding or Removing Peers	213
Importing a Peer Group	213
Edit a Peer Group	214
Pushing a Peer Group	214
Deleting a Peer Group	215
Managing Transformation Hub	215
About Topics	215
Adding a Topic	216
About Routes	216
Creating a Route	217

Editing a Route	219
Deleting a Route	219
Deployment Templates	219
Managing Deployment Templates	219
Additional Files	220
Bulk Operations	222
Location	222
Host Tab	222
Container Tab	224
Collector Tab	224
Transformation Hub Tab	225
Updating Collector Properties	226
Retrieving Collector Logs	226
Updating Collectors Parameters	226
Updating Collector Destinations	227
Updating Collector Credentials	227
Restarting Collectors	227
Deleting Collectors	228
Enabling SecureData Encryption on Managed Connectors	228
Prerequisites for Addition of SecureData Client to Multiple Containers	228
Additional Requirements For Windows Platforms	229
Adding SecureData to Multiple Containers	230
Updating Transformation Hub Cluster Details in ArcMC	231
Updating Host Credentials	232
Downloading and Importing Host Certificates	232
Scanning a Host	233
The Scan Process	233
Moving a Host to a Different Location	235
Deleting a Host	235
Chapter 8: Managing Users on Managed Products	236
User Management Workflow	236
Users and User Lists	237
Permission Groups	239
Roles	241
Node Lists	242
Associations	243
Compliance Report	245

Exporting PDF Reports	246
Chapter 9: Snapshots	247
Creating a Snapshot	247
Chapter 10: Logger Consumption Report	248
Exporting PDF Reports	249
Chapter 11: Managing Repositories	250
Logs Repository	250
Uploading a File to the Logs Repository	250
CA Certs Repository	251
Uploading CA Certificates to the Repository	251
Removing CA Certificates from the Repository	252
Upgrade Files Repository	252
About the AUP Upgrade Process	252
Uploading an AUP Upgrade File to the Repository	253
Removing a Connector Upgrade from the Repository	253
Content AUP Repository	253
Applying a New Content AUP	254
Applying an Older Content AUP	255
User-Defined Repositories	255
Creating a User-Defined Repository	256
Retrieving Container Files	257
Uploading Files to a Repository	258
Deleting a User-Defined Repository	258
Updating Repository Settings	258
Managing Files in a Repository	259
Pre-Defined Repositories	259
Settings for Map Files	260
Settings for Parser Overrides	261
Settings for FlexConnector Files	261
Settings for Connector Properties	262
Settings for JDBC Drivers	263
Backup Files	263
Adding Parser Overrides	264
Chapter 12: System Administration	266
System	266
System Reboot	266
Network	266

System DNS	266
Hosts	267
NICs	267
Static Routes	269
Time/NTP	270
SMTP	271
License & Update	272
Updating the Appliance	272
Updating the License File	273
Process Status	273
System Settings	274
SNMP	274
SNMP Configuration	274
Viewing SNMP System Information	275
SSH Access to the Appliance	277
Enabling or Disabling SSH Access	278
Connecting to Your Appliance Using SSH	278
Diagnostic Tools	278
Display I/O Statistics	279
Display file	279
Display network connections	280
Display network interface details	281
Display network traffic	282
Display process summary	282
Display routing table	282
Edit text file	283
List directory	283
List open files	283
List processes	284
Ping host	284
Resolve hostname or IP Address	284
Scan network ports	285
Send signal to container	285
Tail file	285
Trace network route	286
Logs	286
Audit Logs	286
Configuring Audit Forwarding to a Specific Destination	287

Storage	287
RAID Controller/Hard Disk SMART Data	288
FTP	288
Models Supporting FTP	289
Enabling FTP	289
Adding a Subdirectory	290
Processing Log Data Received via FTP	291
Using FTPS (FTP over SSL)	291
Using FTPS with Blue Coat ProxySG	291
Security	292
SSL Server Certificate	292
Generating a Self-Signed Certificate	293
Generating a Certificate Signing Request (CSR)	294
Importing a Certificate	296
SSL Client Authentication	296
Uploading Trusted Certificates	297
Uploading a Certificate Revocation List	297
Enabling Client Certificate Authentication	298
FIPS 140-2	298
Users/Groups on ArcMC	299
Authentication	299
Sessions	299
Local Password	300
Users Exempted From Password Expiration	301
Forgot Password	302
External Authentication	302
Local Password	303
Client Certificate Authentication	303
Client Certificate and Local Password Authentication	304
LDAP/AD and LDAPS Authentication	304
RADIUS Authentication	306
Local Password Fallback	307
Login Banner	308
User Management	308
Users	309
Reset Password	311
Groups	312
System Admin Groups	312

ArcSight Management Center Rights Groups for Arcsight Management Center	313
Managing a User Group	313
Change Password	314
Appendix A: Audit Logs	316
Audit Event Types	316
Audit Event Information	316
Application Events	316
Platform Events	325
System Health Events	330
SNMP Related Properties	330
Appendix B: Destination Runtime Parameters	334
Appendix C: Special Connector Configurations	341
Microsoft Windows Event Log - Unified Connectors	341
Change Parser Version by Updating Container Properties	342
SSL Authentication	343
Database Connectors	343
Add a JDBC Driver	344
API Connectors	345
File Connectors	346
Syslog Connectors	346
Appendix D: Setting Up Your Arcsight Management Center Appliance	348
Appendix E: Restoring Factory Settings	351
Factory Restore Using System Restore	351
Factory Restore Using Acronis True Image	353
Appendix F: The Topology View and Unmanaged Devices	356
Send Documentation Feedback	359

Chapter 1: Arcsight Management Center Overview

The following topic is discussed here.

Arcsight Management Center (ArcMC) is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring in an efficient and cost-effective manner.

ArcMC offers these key capabilities:

- **Management and Monitoring:** deliver the single management interface to administrate and monitor ArcSight managed nodes, such as Connector Appliances, Loggers, Connectors, Collectors, other ArcMCs, and Transformation Hub.
- **SmartConnector Hosting:** for the hardware appliance, as a platform to host and execute SmartConnectors

ArcMC includes these benefits:

- Rapid implementation of new and updated security policies.
- Increased level of accuracy and reduction of errors in configuration of managed nodes.
- Reduction in operational expenses.



Caution: Customers may not alter any code related to the ArcMC product without direction from ArcSight support, and customization of the code is not supported by ArcSight.

Chapter 2: Software Installation

This chapter describes how to install Software Arcsight Management Center and the Arcsight Management Center Agent.

The following topics are discussed here.

Overview

The complete process of installing Software Arcsight Management Center includes these steps.

Select an Installation Mode

Select a mode in which to install Software Arcsight Management Center on your selected machine. You should plan to install as the root user. In addition, during the installation process, ArcMC will prompt you for a user name, under which the application will be started.

You can install Software Arcsight Management Center in these modes:

- **GUI:** In GUI mode, a wizard steps you through the installation and configuration process. For detailed instructions, see "["GUI Mode Installation" on page 23](#)".

Note: If you are using a Windows system to connect to the machine where Software ArcSight Management Center is to be installed, and prefer to install in GUI mode, you must connect using an X Window client, such as **Xming for Windows**.
- **Console:** In Console mode, a command-line process steps you through the installation and configuration process. See "["Console Mode Installation" on page 24](#)" for detailed instructions.
- **Silent:** In Silent mode, the installation process is scripted. There is no need to interact with the installer, as you provide the installation and configuration input through a file. See "["Silent Mode Installation" on page 25](#)" for detailed instructions.

Applying your License

A valid license is required for Software Arcsight Management Center. A license file is uniquely generated for each instance of a product; therefore, you cannot use the same license file to install multiple instances of the product.

To obtain your license, follow the instructions in the *Electronic Delivery Receipt* email received from ArcSight after placing your order.

You will be prompted to install a license during the installation of ArcMC. If no license is provided, an "Instant-On" license will be applied by default. The Instant-On license is valid for

30 days. During this time, you should obtain and apply the correct license from the [Software Entitlement portal](#).

Start as a Service

If installation was performed as a root user, Software Arcsight Management Center can be configured to start as a system service. For more information, see ["Enabling/Disabling Arcsight Management Center as a System Service" on page 28](#)

Make Host Resolvable

For the Apache web process to start, the Software Arcsight Management Center hostname must be resolvable. Add the hostname to either /etc/hosts or DNS.



Note: Values for these network settings cannot be changed through ArcSight Management Center: hostname, IP addresses for the network interfaces, static routes, /etc/hosts file, and time settings.

Secure Your Credentials

After initial setup is complete, connect to the application and change the default password to a secure password. To change the default password, follow the instructions in ["Users/Groups on ArcMC" on page 299](#).

Optionally, for additional security, rename the default admin username to a secure name. To change a username, follow the instructions in ["User Management" on page 308](#).

Install the ArcMC Agent (If Required)

Additionally, if you plan to manage one or more ArcMCs, Connector Appliances, or Loggers, you need to install the Arcsight Management Center Agent on each. For more information on manual Arcsight Management Center Agent installation, see ["Installing the Arcsight Management Center Agent" on page 35](#)

Open Firewall Ports

Open any required ports on your firewall for best functionality. For a list of required open ports, see ["Configuring Firewall Rules" on page 30](#)

Create an Account on the ArcSight Marketplace

The [ArcSight Marketplace](#) is an app store that enables rapid provisioning of your ArcSight SIEM deployment with content updates, trusted security content packages, and best practices.

ArcSight Management Center requires a global administrative account with the ArcSight Marketplace in order to download and perform some content updates. Browse the [ArcSight Marketplace](#) to set up your administrative account.

Installing Arcsight Management Center

The following section provides instructions to install Software Arcsight Management Center.

- ["Prerequisites for Installation" on the next page](#)
- ["Installation Steps" on page 22](#)
- ["Enabling/Disabling Arcsight Management Center as a System Service" on page 28](#)
- ["Configuring Firewall Rules" on page 30](#)

Prerequisites for Installation

Please note and verify the following prerequisites before beginning the process of installing software

Prerequisite	Description
File Verification	Micro Focus provides a digital public key to enable you to verify that signed software you download from the software entitlement site is indeed from Micro Focus and has not been manipulated in any way by a third party. Visit the following site for information and instructions: https://entitlement.mfgs.microfocus.com/ecommerce/eulfillment/digitalSignIn.do
File Descriptors Limit	The host on which ArcMC is installed must support a limit of 10240 file descriptors. Perform <code>ulimit -n</code> on the host to determine its current level. If the limit does not equal 10240, then do the following: - Option1: <ol style="list-style-type: none">1. Open (or create) <code>/etc/security/limits.conf</code>.2. Set these two parameters:<pre>* hard nofile 10240 * soft nofile 10240</pre>3. Save the file.4. Restart your session. - Option 2: Set the file descriptors limit by executing the following command: <code>ulimit -n 10240</code>
UTF-8 Support	Host must support UTF-8.
en_US.utf8	The en_US.utf8 locale needs to be present on the machine before installing or upgrading software ArcSight Management Center.
libnsl	The libnsl library needs to be present on the machine before installing or upgrading software ArcSight Management Center.
Unzip Package	The unzip command path needs to be set before installing Software ArcSight Management Center: For RHEL/CentOS 7.x: <code>yum install -y unzip</code> For RHEL/CentOS 8.x: <code>dnf install -y unzip</code>
Fontconfig	The fontconfig command path needs to be set before installing Software ArcSight Management Center: For RHEL/CentOS 7.x: <code>yum install -y fontconfig dejavu-sans-fonts</code> For RHEL/CentOS 8.x: <code>dnf install -y fontconfig dejavu-sans-fonts</code>

Prerequisite	Description
Perl	<p>The Perl package is required for the automatic installation of the ArcMC Agent.</p> <p>For RHEL/CentOS 7.x: <code>yum install -y perl</code></p> <p>For RHEL/CentOS 8.x: <code>dnf install -y perl</code></p>
Non-Root Account	<p>You can install Arcsight Management Center as a root or non-root user. However, when installing as a root user, a non-root user account is needed in order to run some required processes.</p> <ul style="list-style-type: none"> • To create a non-root user: <ol style="list-style-type: none"> a. Run the following command: <code>useradd {non-root user}</code> b. Configure the password for the non-root user: <code>passwd {non-root user} specify a password</code> c. Provide execute permissions for the <code>{ArcSight-ArcMC-3.1.0.Build Number.0.bin}</code> file: <code>chmod +x {ArcSight-ArcMC-3.1.0.Build Number.0.bin}</code> d. Switch to the non-root user: <code>su {non-root user}</code> e. Execute the .bin file: <code>./opt/{ArcSight-ArcMC-3.1.0.Build Number.0.bin}</code> <p>Follow the on-screen wizard to complete the process.</p> • When installing Arcsight Management Center as a root user, you can select the port on which it listens for secure web connections (HTTPS). When installing as a non-root user, the port must be configured to 9000. This value cannot be changed and must be externally accessible. • If Arcsight Management Center is installed as a non-root user, and the host is rebooted, ArcMC services will fail to start automatically. Start them manually with this command: <code><install_dir>/current/arcsight/arcmc/bin/arcmcd start</code> <p>Note: If installed with a non-root account, use an initialization script to launch services automatically. See "Starting Services Automatically for a Non-Root Installation" on page 28.</p>
Time Zone Database	tzdata-2021a-1.el8.noarch or later is required.
OS Upgrade	Upgrade to a supported operating system before performing the ArcMC installation. Refer to the Arcsight Management Center Release Notes, available from the ArcSight Software Marketplace , for the most current information on supported operating systems, supported browsers, and other technical requirements.

Installation Steps

To begin the installation, select a mode in which to install Software Arcsight Management Center on your selected machine. The three modes available are GUI Mode, Console Mode, and Silent Install.

GUI Mode Installation

In GUI Mode installation, you use the installer wizard to install the application.

To install Software Arcsight Management Center using the GUI mode:

1. Run these 2 commands from the directory where you copied the Software Arcsight Management Center installer:
 - chmod +x ArcSight-ArcMC-3.1.0.<installer_build_number>.0.bin
 - ./ArcSight-ArcMC-3.1.0.<installer_build_number>.0.binwhere <installer_build_number> is the build number of the latest installer.
The installation wizard starts. Review the dialog box, then click **Next**.
2. Review the License Agreement details, then scroll down to the end. Select **I accept the terms of the License Agreement**. Then, click **Next**.
3. Specify or browse to a folder where you want to install Arcsight Management Center, as shown below. The default installation directory is /opt. However, you should specify a new installation directory in /opt that will easily identify ArcSight Management Center files, such as /opt/arcmc, to distinguish them from files associated with other ArcSight products.
4. Review the summary of installation information on the **Pre-Installation Summary** dialog, then click **Install**.
The Arcsight Management Center installer begins the installation process.
5. When installation is complete, click **Next** to begin the configuration wizard.
6. If you run the Arcsight Management Center software installer as a root user, the next dialog enables you to specify an existing non-root user and to configure a port through which Arcsight Management Center users will connect through the UI.
For example, you can specify 443, the standard HTTPS port, or any other that suits your needs. If any port other than 443 is specified, users will need to specify the port number in the URL they use to access the Arcsight Management Center UI.
Specify the user name of the non-root user and the HTTPS port number, then click **Next**. (These values may not be changed later in the process.)
7. After the software is installed, click **Next** to begin Arcsight Management Center initialization.
8. After initialization is complete, click **Done** to launch the Arcsight Management Center Configuration wizard.



Note: The Configuration wizard should launch automatically. If it does not, use this command to launch the wizard:

```
<install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup
```

- If you have run the Arcsight Management Center software installer as a root user, the next dialog enables you to configure Arcsight Management Center to run as a system service. By default, Arcsight Management Center runs as a system service.

When you install Arcsight Management Center as a root user, a service called `arcsight_arcmc` can be configured, created, and enabled at runlevel 3 and 5.

Additionally, a few libraries are added using `ldconfig`. For a complete list of those libraries, see `/etc/ld.so.conf.d/arcsight_arcmc.conf` and `<install_dir>/current/arcsight/install/ldconfig.out`.

- You have installed Arcsight Management Center. Click **Start Arcsight Management Center Now**, or click **Start Arcsight Management Center later**, and then click **Finish**.

If you have selected to start Arcsight Management Center later, read the information in "[The Arcsight Management Center Daemon \(arcmcd\)](#)" on page 33 to understand how to start Arcsight Management Center at a later time.

- If you selected **Start Arcsight Management Center Now**, click **Finish** to exit the wizard.

Alternatively, wait for the next dialog which provides the URL to access the Arcsight Management Center interface.

Arcsight Management Center continues to start services and processes in the background. If you have selected to continue within the wizard, follow the instructions on the dialog or use the instructions in "[Connecting to the Arcsight Management Center User Interface](#)" on page 32 to connect to the Arcsight Management Center.

Console Mode Installation

In Console Mode installation, you use a command-line interface to install the application.



Note: After some initial steps in the CLI, the installation sequence is the same as the one described for the GUI mode install in "[GUI Mode Installation](#)" on the previous page. Follow the instructions provided for the GUI mode install to complete the installation.

To install Software Arcsight Management Center using the Console mode:

- Run these commands from the directory where you copied the Arcsight Management Center software:

```
chmod +x ArcSight-ArcMC-3.1.0.<installer_build_number>.0.bin
```

```
./ArcSight-ArcMC-3.1.0.<installer_build_number>.0.bin -i console
```

where <installer_build_number> is the build number of the latest installer.

The installation wizard starts in command-line mode.

2. Press **Enter** to continue. Then, follow the prompts to complete installation and configuration.



Note: If Arcsight Management Center is installed in Console mode, it will be uninstalled in Console mode as well. See "[Uninstalling in Console Mode](#)" on page 34 for more information.

Silent Mode Installation

Silent mode enables scripting of the installation process. Before you install Arcsight Management Center in silent mode, create two properties files required for the silent mode installation:

- A file to capture the installation properties
- A file to capture the configuration properties

After you have generated the two files, you need to merge them into one file and use the resulting file for silent mode installations.

About Licenses for Silent Mode Installations

As for any Software Arcsight Management Center installation, each silent mode installation requires a unique license file. Obtain licenses from Micro Focus Customer Support and install them on the machines on which you are installing in silent mode, or ensure that the location where the license is placed is accessible from those machines.

Generating the Silent Install Properties File

This procedure generates the two properties files and then instructs you to combine them into one file. The resulting file is used for future silent installations.

1. Log in to the machine on which you wish to generate the installation properties file.
If you want the silent mode installations to be done as root user, log in as root in this step.
Otherwise, log in as a non-root user.
2. Run this command:

```
./ArcSight-ArcMC-3.1.0.<installer_build_number>.0.bin -r <directory_location>
```

where <installer_build_number> is the build number of the installer file, and <directory_location> is the location of the directory where the generated properties file will be placed. This cannot be the same location where Arcsight Management Center is being installed.

The properties file *must* be called `installer.properties`.

3. Install Arcsight Management Center in GUI mode, as described in "[GUI Mode Installation on page 23](#)" Follow the steps until step 10, and proceed with the following:
 - a. Click **Previous** instead of **Done** to proceed further.
 - b. Click **Cancel** to stop the installation.
4. When the confirmation message appears, click **Cancel**. Click **Quit** to clear this message.
5. Navigate to the directory location you specified for the `installer.properties` file earlier.

The following is an example of the generated `installer.properties` file.

```
# Replay feature output
# -----
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.
#Choose Install Folder
#-----

USER_INSTALL_DIR=/opt/<arcmc_installation_folder>/<build
number>/installdir
#Install
#-----

-fileOverwrite_</opt/<arcmc_installation_folder>/<build
number>/installdir/UninstallerData/Uninstall_ArcSight_Management_Center_
3.1.0.lax=Yes
#Intervention Required
#-----
USER_AND_PORT_1=username
USER_AND_PORT_2=443
```

1. Start the configuration wizard with the option to record configuration properties:

```
<install_dir>/current/arcsight/arcmc/bin/arcsight arcmcsetup -i recorderui
```

When prompted to specify a file name to capture the configuration properties, specify a meaningful name. For example, `config.properties`, then browse to choose the same directory as the `installer.properties` file.

2. Step through the configuration wizard, as described starting at **Step 10** of "["GUI Mode Installation" on page 23](#)".
3. After the configuration properties file is generated, append the contents of this file to the `installer.properties` file generated in the previous procedure, "["Generating the Silent Install Properties File" on the previous page](#)", to create a combined file.

For example, you can use the `cat` command to concatenate both files:

```
cat installer.properties config.properties > <combinedproperties.properties>
```

4. Include the following property in the combined file:

```
ARCSIGHT_CONAPP_SETUP_PROPERTIES=<directory_location>/  
<combined_properties_file>
```

where <directory_location> is the path of the directory where the combined file is located, and <combined_properties_file> is the file name of the combined file you created earlier.

Use the combined file for future Arcsight Management Center silent mode installations, as described in "[Installing Using the Generated Properties File](#)" below.

Installing Using the Generated Properties File

Follow the steps below to install Arcsight Management Center using Silent mode:

1. Uninstall the previously installed version of ArcSight Management Center, as explained in "[Uninstalling Software Arcsight Management Center](#)" on page 33
2. Make sure the machine on which you install Arcsight Management Center complies with the requirements listed in the ArcSight Management Center Release Notes, and the prerequisites listed in "[Prerequisites for Installation](#)" on page 21.
3. Copy the combined properties file you generated previously to the location where you copied the Arcsight Management Center software.
4. Do one of the following:
 - Edit the licensePanel.path property in the silent mode properties file to include the location of the license file for this instance of the installation. (A unique license file is required for each instance of installation.), OR
 - Set the licensePanel.path property to point to a file, such as arcmc_license.zip. Then, for each instance of the silent mode installation, copy the relevant license file to the location and rename it to arcmc_license.zip. Doing so will avoid the need to update the combined properties file for each installation.
5. Run these 2 commands from the directory where you copied the Arcsight Management Center software:
 - chmod +x ArcSight-ArcMC-3.1.0.<installer_build_number>.0.bin
 - ./ArcSight-ArcMC-3.1.0.<installer_build_number>.0.bin -i silent -f <combined_properties_file>
 - where <installer_build_number> is the build number of the installer file. The rest of the installation and configuration proceeds silently without requiring further input.



Note: In some cases, a spurious error message may be displayed: "SLF4J: Failed to load class "org.slf4j.impl.StaticLoggerBinder". This is a harmless error and may be ignored.

Next Steps After Installation

To get started managing products with , you need to add hosts to manage. For more information on adding hosts, see ["About Adding a Host" on page 97](#).

Enabling/Disabling Arcsight Management Center as a System Service

If Arcsight Management Center is installed to run as a system service, you can use arcmcd to manage processes. For more information, see ["The Arcsight Management Center Daemon \(arcmcd\)" on page 33](#).

To enable or disable Arcsight Management Center as a system service:

1. On the menu bar, click **Administration > System Admin**.
2. In the navigation bar, click **Startup Settings**.
3. Under **Software Startup Options**, select **Start as a Service** to enable starting as a system service, or select **Do not start as a service** to disable.
4. Click **Save**.



Note: After enablement, you can reboot (which will automatically restart the service) or start the service manually without a reboot.

Starting Services Automatically for a Non-Root Installation

If Arcsight Management Center is installed as a non-root user, and the host is rebooted, ArcMC services will fail to start automatically. However, you can set them to start automatically by using an initialization script.



Note: Since the initialization script runs as su, it does not log to the console.

An example script is shown here. This is only an example. Your own script will need to be tailored for your environment.

```
#!/bin/sh  
  
# ArcMC          Wrapper script for the Arcsight Management Center  
# processname:    arcsight_arcmc  
# chkconfig:      2345 99 01
```

```
# description:          Arcsight Management Center
DAEMON=<install_dir>/current/arcsight/arcmc/bin/arcmcd
DAEMON_USER=<NonRootUser-with-which-arcmc-was-installed>
# Exit if the package is not installed
[ -x "$DAEMON" ] || exit 0
if [ $UID -ne 0 ] ; then
echo "You must run this as root."
exit 4
fi
su $DAEMON_USER -c "$DAEMON $1 $2"
exit $?
```

The DAEMON variable is used to specify the directory where arcmcd process is running.

The DAEMON_USER variable is used to specify which non-root user ArcMC will run as.

Finally, the su command simply wraps your existing script (defined in the variable DAEMON) and passes any parameters to the \$DAEMON script/

To configure an initialization script:

1. SSH to the VM using root user credentials.
2. Go to /etc/init.d
3. Specify the command vi arcsight_arcmc to create a service.
4. Specify the text of your script and save the file.
5. Give execute permission for the script using the command chmod +x arcsight_arcmc
6. Register the script using the command
chkconfig –add arcsight_arcmc
7. Specify the command chkconfig | grep arcsight_arcmc to determine what the chkconfig will report after you add the init script. Expected results:
arcsight_arcmc 0:off 1:off 2:on 3:on 4:on 5:on 6:off

Configuring Firewall Rules

Before Arcsight Management Center can receive data, some ports must be opened through the firewall.

- For Software Arcsight Management Center, you are responsible for setting up the firewall. ArcSight recommends that you configure your firewall so that only the required ports are open.
- For the Arcsight Management Center Appliance, ArcSight provides a script to configure your firewall. See "[Configuring the Firewall on Arcsight Management Center Appliance](#)" below for more information.

You can configure the firewall on your Arcsight Management Center as you would on any server, by editing `iptables-config` and white-listing the appropriate ports. For Arcsight Management Center Appliances only, you can use the provided script to close all but the appropriate ports in your firewall.



Tip: Be sure to update the firewall configuration when you add or remove any service or function that requires an open port, such as FTP, SNMP, or local connector.

After you first install or upgrade ArcMC, configure the firewall to be open only for the following ports, depending on your form factor and install:

Default Inbound Ports

Service	ArcMC Appliance	Software ArcMC root install	Software ArcMC non-root install
FTP	21	N/A	N/A
HTTPS	443	443	9000
NTP	123	N/A	N/A
Local Connectors	9001- 9008	N/A	N/A
SSH	22	22	22

Configuring the Firewall on Arcsight Management Center Appliance

Your Arcsight Management Center Appliance includes a script that you can use to configure the firewall. This script looks at your current Arcsight Management Center configuration and decides what ports to keep open. Alternatively, you can configure the firewall on your appliance as you would on any server, by editing `iptables-config` and white-listing the appropriate ports.

When called without arguments, the `/usr/sbin/arcfirewall` script previews and displays the ports that it will keep open, but takes no action to alter the firewall configuration. To alter firewall configuration, use the `-set` option.

To preview the list of ports the script will open:

1. Log into the appliance as root.
2. Run the following command:

```
/usr/sbin/arcfirewall
```

The script displays the ports that it would open, as shown in the following example.

```
[root@myserver ~]# /usr/sbin/arcfirewall
PREVIEW MODE - NO FIREWALL CHANGES...
List of ports that firewall would allow inbound from any IP address:
21/tcp
22/tcp
443/tcp
9001/tcp
9002/tcp
9003/tcp
9004/tcp
9005/tcp
9006/tcp
9007/tcp
9008/tcp
123/udp
```

To configure the firewall:

1. Log into the appliance as root.
2. Run the following command:

```
[root@myserver ~]# /usr/sbin/arcfirewall --set
```

The script configures the firewall leaving the previewed ports open.

If you configure an ArcMC appliance local container, assign it a network port, then run `arcfirewall`, the script will detect that the new port should be opened and list it in the preview of ports. You can then run `arcfirewall` with the `--set` option, as described above, to actually open the port.

If `arcfirewall` is not run, and the port not opened, the connector will not receive any events.

Arcsight Management Center Operations

This section details the operation of Arcsight Management Center: how to connect, which processes run while Arcsight Management Center is active, and commands for using the Arcsight Management Center command-line utility (arcmcd).

Connecting to the Arcsight Management Center User Interface

Use this URL to connect to Arcsight Management Center:

`https://<hostname or IP address >:<configured_port>`

where hostname or IP address is the system on which you installed Arcsight Management Center. If Arcsight Management Center was installed as root and the default port was used, then <configured_port> is optional.

To login for the first time, use the following default credentials:

Username: admin

Password: password

For security, change the default credentials immediately after you log in for the first time. For more information on changing credentials, see ["User Management" on page 308](#).

Arcsight Management Center Processes

The following processes run as part of Arcsight Management Center:

- apache
- aps
- postgresql
- web

Logging Into ArcMC If the Web Service is Down

If the web service stops, you can connect to ArcMC to restart it.

1. SSH to the host.
2. Specify `<arcmc_install_dir>/current/arcsight/arcmc/bin/arcmcd stop all`
3. Specify `<arcmc_install_dir>/current/arcsight/arcmc/bin/arcmcd status`. Wait for some time until all process status report "Not monitored".

4. Specify <arcmc install dir>/current/arcsight/arcmc/bin/arcmcd start all. Wait for some time until all the process status report "running".
5. Log into the ArcMC web UI as usual.

The Arcsight Management Center Daemon (arcmcd)



The arcmcd utility enables a number of management and control tasks for the Arcsight Management Center software process, including starting, stopping and restarting. The syntax to run arcmcd is as follows:

```
<install_dir>/current/arcsight/arcmc/bin/arcmcd <command>
```

Where <install_dir> is the installation directory of Arcsight Management Center, and <command> is a command listed below.

If Arcsight Management Center is installed to run as a system service, you can use arcmcd to manage a specific process.

arcmcd Commands

Command	Description
start	Starts aps, apache, postgresql, and web processes.
stop	Stops aps, apache, postgresql, and web processes.
restart	Restarts aps, apache, postgresql, and web processes.
status	Displays the current status of all processes.
quit	Stops aps, apache, postgresql, and web processes, as well as the Arcsight Management Center application.
start <process_name>	Starts the named process. For example, start apache.
stop <process_name>	Stops the named process. For example, stop apache.
restart <process_name>	Restarts the named process. For example, restart apache.

Uninstalling Software Arcsight Management Center

Uninstall Arcsight Management Center in the same user mode in which the installation was performed. For example, if you performed the installation as root, then you must perform the uninstallation as root

Uninstalling in GUI Mode

To uninstall Software Arcsight Management Center in GUI mode:

1. In the directory where you installed Arcsight Management Center, enter:

```
<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_3.1.0
```

2. The uninstall wizard starts. Click **Uninstall** to start uninstalling Arcsight Management Center and follow the prompts in the wizard.
3. After uninstalling, manually delete the /userdata directory.



Note: If using GUI mode and uninstalling Arcsight Management Center software over an SSH connection, make sure that you have enabled X window forwarding using the **-X** option, so that you can view the screens of the uninstall wizard.

If using PuTTY, you also need an X11 client on the host from which you are connecting.

Uninstalling in Console Mode

If you installed Arcsight Management Center in Console mode, then, by default, uninstallation occurs in Console mode.

To uninstall in Console mode:

1. At the command line, enter: `<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_3.1.0 -i console`
2. After uninstalling, manually delete the /userdata directory.

At the prompt, press **Enter** again to confirm uninstallation. The application will be uninstalled.

Uninstalling in Silent Mode

If you installed Arcsight Management Center in Silent mode, then, by default, uninstallation occurs in Silent mode.

To uninstall in Silent mode:

1. At the command line, enter: `<install_dir>/UninstallerData/Uninstall_ArcSight_Management_Center_3.1.0`.
The application will be uninstalled without further interaction.
2. After uninstalling, manually delete the /userdata directory.

Installing the Arcsight Management Center Agent

The Arcsight Management Center Agent runs on managed hosts and enables their management by Arcsight Management Center. Whether you need to install the Arcsight Management Center on a managed host depends on the host's form factor, which is summarized in the table and explained in detail below.

Host Type	ArcMC Agent Required?	Agent Installation
ArcMC, Logger, or Connector Appliance hardware form factor (all versions)	Yes	Automatically performed when adding host.
Software Connector Appliance (all versions)	Yes	Manual installation required; perform before adding host.
Software Logger (before version 6.0)	Yes	Manual installation required; perform before adding host.
Software Logger (version 6.0 or later)	Yes	Automatically performed when adding host.
Software ArcMC (before version 2.1)	Yes	Manual installation required; perform before adding host.
Software ArcMC (version 2.1 or later)	Yes	Automatically performed when adding host.
Connector (any)	No	None. ArcMC Agent is not required.
Collector (any)	No.	None. ArcMC Agent is not required.
Transformation Hub	No	None. ArcMC Agent is not required.

Automatic Installation

The ArcMC Agent is *automatically* installed when adding any of the following host types to ArcMC:

- Any hardware appliance (ArcSight Management Center Appliance, Connector Appliance, or Logger Appliance)
- Software Logger 6.0 or later
- Software ArcMC 2.1 or later

As part of the Add Host process, Arcsight Management Center automatically pushes the Arcsight Management Center Agent installer to the added host, installs the Agent, then starts the service. The host is then ready to manage in ArcSight Management Center. You will not

need to take any manual installation steps. For more information about the Add Host process, see ["About Adding a Host" on page 97](#).



Note: Perl is required for the automatic installation of the ArcMC Agent. Ensure that Perl is installed on the host prior to attempting to add the host to ArcMC.

Manual Installation

You must perform a *manual* installation of the ArcMC Agent on any of these host types *prior to* adding them to ArcMC for management:

- Software ArcSight Management Center (before version 2.1)
- Software Logger (before version 6.0)
- Software Connector Appliance (all versions)

An ArcMC used to manage products must have an Agent installed with the same version number as the ArcMC. For example, if your ArcMC 3.1.0 will be used to manage products, then the ArcMC Agent running on that ArcMC must also be version 3.1.0.

To manually install the Arcsight Management Center Agent:

1. In the directory to where you transferred the installer, run these 2 commands:
 - `chmod +x ArcSight-ArcMCAgent-.<agent_installer_build_number>.0.bin`
 - `./ArcSight-ArcMCAgent-.<agent_installer_build_number>.0.bin LAX_VM <install_dir>/current/local/jre/bin/java`
where `<agent_installer_build_number>` is the build number of the latest installer and `<install_dir>` is the installation directory of the software product.

The installation wizard starts.

2. Review the dialog box, then click **Next**. The required installation path is the install directory (that is, the same directory where Software Connector Appliance or Software Logger is installed).
3. Follow the prompts to complete the installation. The ArcMC Agent is automatically started upon completion of the installation process.



Note: If the ArcMC Agent fails to install on the localhost, localhost management will not be enabled. To verify correct installation of the Agent, check on the **Hosts** tab under **Issues**. Follow the instructions shown in the tooltip to install the Agent properly and resolve any issues shown.

Connectors and Transformation Hub

Connectors and Transformation Hub do not require the installation of the Arcsight Management Center Agent in order to be managed by ArcMC.

Arcsight Management Center Agent Operations

After installation, the *arcmcagent* process runs on the managed host. This process automatically starts after either automatic or manual installation. However, if the Agent stops for any reason, it can be manually started.

To manually start, stop, or restart the Agent on an appliance host:

1. On the managed host, click **Setup > System Admin > Process status**.
2. Select *arcmcagent* from the list of processes.
3. Click **Start, Stop, or Restart**, as necessary.

On Software ArcMC, Software Connector Appliance, or Software Logger

To manually start or stop the Agent on Software ArcMC, Software Connector Appliance, or Software Logger:

1. Run `<install_dir>/current/arcsight/<conapp|logger|arcmc>/bin/<conappd|loggerd|arcmc> <start|stop> arcmcagent`

Agent Verification

To verify that the Agent is running on a host, use one of the following procedures:

- In the managed host's GUI, click **Setup > System Admin > Process Status**. The Arcsight Management Center Agent (*arcmcagent*) will be shown as a process in the running state.
- (For Software ArcMC, Software Connector Appliance, or Software Logger Only) After you install the Agent, run this command at the command line:
`<install_dir>/current/arcsight/<conapp|logger>/bin/<conappd|loggerd> status`
The Agent is shown as a service in the running state.

Uninstalling the Arcsight Management Center Agent

To uninstall the Arcsight Management Center Agent, run the following command:

```
<install_dir>/arcmcagent/UninstallerData/Uninstall_ArcSight_Management_Center_Agent_<version number>
```

where <install_dir> is the name of the installation directory, and <version_number> is the version, of the ArcMC Agent.

The Uninstall Wizard will launch. Click **Uninstall** to begin the wizard. When the uninstallation completes, click **Done**.



- Always stop and then uninstall any previous version of the Arcsight Management Center Agent before installing a new version.
- If uninstalling either Software ArcMC, Software Logger, or Software Connector Appliance, make sure that the Arcsight Management Center Agent is uninstalled from the node before beginning the uninstall of the managed product.

Installing a vCHA (VMware Workstation - VMware Player - ESXi)

This section walks you through the steps for importing and configuring the VM to install a vCHA.

Import the virtual machine:

1. Open the VMware Workstation or VMware Player.
2. Select and download the <file-name>.ova file, and click **Open**.
3. Specify a name for the virtual machine, select a storage path and click **Import**.
4. After the VM has been imported, click **Power on this virtual machine** to start the VM and open a terminal.
5. Once the CLI interface is displayed, press ALT + F2 in order to access the ssh terminal.
6. Login to your VM as root and determine the VM's IP address: **ip addr**

Access the ArcMC Appliance:

1. Browse to the ArcMC using the previously determined IP address:
<https://<ip-address>/platform-ui/>
2. Accept the *License Agreement* and proceed to login using the default credentials (you are requested to change your password).
3. Navigate to **Administration > System Admin**.
4. From the left menu under **System**, select **Process Status** and verify that all the required processes are running.

Configure the DNS Settings and DNS Search Domains

1. Navigate to **Administration > System Admin**.
2. From the left menu under **System**, select **Network**.

For more information about DNS settings and DNS search domains, please see the "[Network](#)" on page 266 section.

Install vCHA on ESXi/Vcenter VMWare

Follow the steps below to deploy a vCHA (ova file) on ESXi/Vcenter 6.5

1. Log in to the VMware vSphere Web Client and go to the VMs tab.
2. Add the Deploy OVF Template action button via the Actions drop-down list.
3. Click **Deploy OVF Template**, a new window will open.
4. Click Browse, select the OVA file and click **Next**.
5. Select the location where you want to deploy the virtual appliance and click **Next**.
6. Select the resource you want to use to run the virtual appliance and click **Next**.
7. Review the package details advanced configuration options and click **Next**.
8. Select the desired storage location from the list of datastores and click **Next**.
 - a. Recommended virtual disk format: Thick provision lazy zeroed
9. From the drop-down list select a destination network for each source network and click **Next**.
10. Review the configuration data and click Finish when ready.
11. The system will now import and deploy the file, once completed click **Refresh** to update the system.
12. The Login PI 3 Appliance is now visible, select the VM and click Power On.
13. Once the VM is powered on, click the Open Console icon to open the VM console in a new window.

Chapter 3: The User Interface

This chapter provides a general overview of the Arcsight Management Center interface. Arcsight Management Center uses a browser-based user interface. Refer to the Arcsight Management Center Release Notes for the latest information on supported browsers.

The following topics are discussed here.

The Menu Bar

The menu bar provides access to the main functional components of Arcsight Management Center. It includes the **Dashboard**, **Node Management**, **Configuration Management**, **User Management** and **Administration** menus.

Monitoring Summary

The Monitoring Summary page displays information on all monitored products.

- The aggregated health status for products of each type is displayed in pie graph format, showing total number of nodes, as well as the number corresponding to each status. A summary table shows the same data in percentage format.
- The management panel displays the **Monitoring Summary** table, showing all products which are currently reporting issues.
- The navigation panel enables you to display a monitoring summary for individual product types in the management panel. Click the product type to display the product's monitoring summary.

For more information on viewing and configuring monitoring, see ["Dashboard" on page 45](#).

Node Management

Use **Node Management** to manage any of the following node types:

- Connectors or Collectors
- Hardware or Software Connector Appliances
- Hardware or Software Loggers
- Hardware or Software ArcSight Management Centers
- Transformation Hub

For more information on adding and managing nodes, see ["Managing Nodes" on page 82](#). From the same menu, you can also perform selected management tasks on managed ArcSight products. See ["Managing ArcSight Products" on page 113](#).

Configuration Management

Use **Configuration Management** to create and manage node configurations, synchronization (pushing) of configurations across multiple nodes, and expedite the initial configuration of Loggers. You can manage any of these configuration types:

- Subscriber configurations for:
 - Arcsight Management Center
 - Connectors
 - Connector Appliances
 - Destinations
 - Loggers
 - System administration
- Other configurations are also managed here:
 - Logger Initial configurations
 - Logger event archives
 - Management of Logger peers
 - Management of Transformation Hub
 - Bulk Operations
 - Generator ID Management
 - Management of Deployment Templates

For more information on subscriber configuration management, see "[Managing Configurations](#)" on page 169.

For more information on initial configurations, see "[Logger Initial Configuration Management](#)" on page 207.

User Management

User management enables you to manage users across all of your managed nodes. You can create and edit users, user lists, their associations, and roles. You can also check to see if each node complies with a list of authorized users on the managing .

For more information about user management, see "[Overview](#)" on page 1

Administration

The **Administration** menu contains these items:

- **Backup:** Enables you to back up your current ArcSight Management Center configuration. For more information, see [Managing Backups and Restores, on page 1](#).



This function isn't available when you deploy ArcMC in the containerized ArcSight Platform.

- **Repositories:** Enables you to manage repositories that store files, such as logs, certificates, and drivers. For more information, see ["Managing Repositories" on page 250](#).
- **Snapshot:** Enables you to take a snapshot image of ArcSight Management Center, to produce logs that are useful in troubleshooting. For more information, see ["Snapshots" on page 247](#).
- **Restore:** Enables you to restore your configuration from a saved backup. For more information, see [Managing Backups and Restores, on page 1](#).



This function isn't available when you deploy ArcMC in the containerized ArcSight Platform.

- **System Admin:** Describes the system administration tools that enable you to create and manage users and user groups, and to configure security settings for your system. For more information, see ["System Administration" on page 266](#).
- **Consumption Report:** Generates a report on Logger data consumption for selected managed nodes.

ArcMC Name

To assign ArcMC a name, add the property `arcmc.instance.name=<arcmc_instance_name>` to the `logger.properties` file.

You can set a name for your ArcMC during the CDF deployment for Fusion ArcMC.

A valid ArcMC name must meet the following criteria:

- Is a non-empty string
- Is equal to or less than 32 characters long
- It contains characters: A-Za-z0-9 _ -

For more information on how to edit the `logger.properties` file, please refer to the ["Modifying logger.properties" on page 130](#) section.

Stats (EPS In/Out)

The **Stats** menu item shows the total Events Per Second (EPS) in and out from all managed connectors (standalone SmartConnectors and connectors running on managed hosts).

Job Manager

The Job Manager shows all deployment jobs processed in a specified time frame. Using the Job Manager, you can identify issues that occurred during deployments.

The Job Manager shows the following for each job:

- **Name of the Job:** The job name (must be smaller than 255 characters).
- **Started By:** The user who ran the job.
- **Type:** Type of job.
- **Start/End Time:** The start and end time of the job.
- **Status:** Job status. If the job has a status of *Failed*, click **Retry** to re-run the job.
- **Details:** Job details.

Hover over any field to display details about the field in a tooltip. Click the Up/Down arrows at the top of any column to sort data by the selected parameter.

To view the Job Manager:

1. On the menu bar, click the Job Manager (notepad) icon . By default, the Job Manager displays all deployment jobs for the last 5 days. A red numeral on the Job Manager icon, if any, indicates the number of jobs currently in the In-Progress state.
- To change the time frame for job data displayed, specify the date criteria in the date boxes in the upper right corner, then click **Show Results**. You may specify any time frame in the last 180 days (6 months).
- To search for a specific job, specify the search criteria in the **Search** box.
- If a job is in progress, you can click **Refresh** on the menu bar to refresh the display.

Site Map

For ease of accessibility and convenience, the Site Map links to all pages in the Arcsight Management Center UI.

To access the site map: on the main toolbar, click **Site Map**. Select the desired link to navigate.

History Management

History management enables you to quickly and easily access previously-navigated pages. History management is available for Node Management, Configuration Management, User Management pages, and for some Administration pages.

In Node Management, the [navigation tree](#) shows the full path for any item selected on the tree. Click any node in the path to navigate directly to the corresponding page.

You also can return to any previously-browsed page by clicking the corresponding link in the breadcrumb trail.

In addition, you can use your browser's **Back** and **Forward** buttons to navigate to previously visited pages.

Dashboard

Using Arcsight Management Center, you can monitor the health status of all managed nodes. You can also configure warnings and alerts for issues of importance to you.



Note: In order for products to be monitored, they must be added as nodes to Arcsight Management Center. For more information on managing nodes, see "[Managing Nodes](#)" on page 82.

Monitoring is displayed on the **Dashboard > Monitoring Summary** page. Arcsight Management Center automatically monitors all managed nodes.

You can also configure notifications (email, SNMP, and through audit forwarding) about the status of managed nodes.

Overview

Using Arcsight Management Center, you can monitor the health status of all managed nodes. You can also configure warnings and alerts for issues of importance to you.



Note: In order for products to be monitored, they must be added as nodes to Arcsight Management Center. For more information on managing nodes, see "[Managing Nodes](#)" on page 82.

Monitoring is displayed on the **Dashboard > Monitoring Summary** page. Arcsight Management Center automatically monitors all managed nodes.

You can also configure notifications (email, SNMP, and through audit forwarding) about the status of managed nodes.

Monitoring Managed Nodes

Arcsight Management Center monitoring, on the **Dashboard > Monitoring Summary** page, displays the current health history of all managed nodes, both software and hardware.

- Monitored metrics for software nodes (such as Software Logger) include such software parameters as CPU usage, event flow, and disk usage statistics.
- Monitored metrics for hardware appliances (such as Logger Appliance) include both software as well as hardware-related attributes, such as remaining disk space and hardware status.
- Device health related information:
 - Devices have severity associated with them instead of status. Up is equivalent to "HEALTHY" and Down to "FATAL".
 - Sunburst Chart and corresponding breakdown table is enhanced to show the severity instead of status.

You can view a complete list of monitored parameters in "[Monitoring Rules Parameters](#)" on [page 57](#), and use them in creating your own custom rules. These rules breaches will also be displayed on the Health History and Hardware Status panels. Note that the layout and selection of the data panels in the Monitoring Summary is not customizable.

The Monitoring Summary Dashboard

The Monitoring Summary includes a variety of panels that display monitoring information on the health and status of your managed products.

To view the monitoring summary, click **Dashboard > Monitoring Summary**.

Total Number of Nodes

Each tile in the **Total Number of Nodes** panel displays the count of managed nodes of the specified type. These types are defined as follows.

Tile	Count
Devices	Devices which are forwarding events.
ArcMC/CHA	Includes managed ArcMCs and Connector Hosting Appliances, in both hardware and software form factors.
Connectors	Managed Connectors.
Collectors	Managed Collectors.
Loggers	Managed Loggers (hardware and software form factors).
Nodes	Nodes on the managed Transformation Hub. (Note that if Transformation Hub is upgraded, the Monitoring Summary will not reflect the correct Transformation Hub information until you import the new Transformation Hub certificate into ArcMC. See " Downloading and Importing Host Certificates " on page 232 for more information.)
	<p>Note: To display Transformation Hub Processing Data users need to turn on the C2AV pod on the Transformation Hub, for more information see the Transformation Hub Administrator's Guide. Event Parsing Error, Stream Processing EPS, and Stream Processing Lag are the metrics that will be available after the C2AV pod is turned on, otherwise only CPU Usage and Memory under Broker's Health will be displayed.</p> <p>Note: The stream processors metric name format has changed to SP_Name(SP_Type).</p>

To see the details of a node type, click the title corresponding to the node type. For example, to view the details of all Collectors, click **Collectors**.

Devices by Device Type

The **Devices by Device Type** display shows a color-coded sunburst of the various device types in use across your network. The table shows the total number of active and inactive devices by device product.

The inner ring of the sunburst shows the total devices.

The outer ring of the sunburst shows the total number of device types. For clarity of display, if the number of device types exceeds 1000, the outer ring is not shown.

The **Devices Information for All Device Types** table breaks down the information to display Device Type, Severity (Fatal, Critical, Warning, Healthy), and Total Devices.

To see the details of a device type, click the corresponding tile in the wheel, or its entry in the table.



Note: ArcMC 2.6 and 2.7 Device Monitoring function supports only Connectors 7.3 - 7.7. ArcMC 2.8 and later support Connectors 7.3 and later for Device Monitoring.

Device Configuration for Device Type

The Device Configuration for Device Type page allows you to modify the **Device Product time-out Interval**, **Device age-out Interval**, and **Disable Device Tracking**.

Device Product time-out Interval

The default value is set to 20 minutes, this can be modified. If the selected device type does not send events to the connector during the last 20 minutes, the device type will be marked as Inactive.

Device age-out Interval

The default value is set to 14 days, this can be modified. If the selected device type remains inactive for 14 days, the device type records will be purged from the system.

Disable Device Tracking.

This box can be checked to disable the selected device product family.



Note: If device product monitoring is re-enabled X days later while **Disable Device tracking** is enabled, the aged-out internal should be set to Y days, in which Y comes after X days. This will prevent the selected disable tracking product family device records from being removed of the ArcMC system.

Device Health Metrics

The dashboard displays device health information as severity. The Sunburst Chart shows the Severity as "HEALTHY", "FATAL", "WARNING", or "CRITICAL".



Note: The selection and layout of the panels on the Monitoring Summary is not customizable. You can, however, customize the issues reported for a given node type by creating custom breach rules, which can be viewed on the Severity Issue Summary. See "[Monitoring Rules](#)" on [page 52](#)

Drilling Down

You can view the details of problematic nodes, then take action to rectify any issues.

To view all details of a problematic node, select it in the upper table. The lower table shows issues associated with that node. Each issue is shown with these identifiers:

- **Metric Type:** Metric assigned to the issue.
- **Metric Name:** Name of the metric.
- **First Occurrence:** Local time of the issue's first occurrence.
- **Last Occurrence:** Local time of the issue's last occurrence.
- **Severity:** Issue severity.
- **Description:** Brief description of the issue.

To view details of nodes by severity:

1. On the menu bar, click **Dashboard > Monitoring Summary**.
2. Click the ring meter corresponding to any of the monitored product types, in the portion of the meter corresponding to the severity you wish to view. (For example, to view all nodes currently with Warning status, click the Warning, or yellow, part of the ring.) The corresponding **Severity Issue Summary** is displayed.
3. On the **Severity Issue Summary** page:

The upper table shows a list of all problematic nodes, with the following identifiers:

- **Name:** Node name.
- **Path:** Path to the node.
- **Type:** Type of node.
- **Lead/Breach:** Short summary of the most severe issue reported by the node. The node may be experiencing less severe issues as well.

Details and Health History

To view further health details of a problematic node, including history and status, click **Details**. The data tables show the detailed parameters of the selected node.

The Health History panel will show any rules breaches, including custom rules you have created yourself.



Note: The layout of the panels and selection of the displayed parameters is not customizable.

Data Charts

Each data chart represents values of the parameter over time. Use the drop-down list to change the interval shown from the last 4 hours, the last day, or the last week. Data charts can include any of the metrics shown under the [Valid Values for Metric Types](#) table.

Click the data legend to toggle display of the corresponding line from the chart. Hiding some lines may be helpful to clarify a chart with many lines.

ADP License Usage for the Last 30 Days

Your ADP license entitles you to a specified number of managed products and amount of managed traffic. The **ADP License Usage for the Last 30 Days** panel shows your ADP data usage for the previous month.

The graph shows all traffic in your ADP environment.

- Green (the default) indicates that data usage is within your licensed limit.
- Amber indicates periods when your data usage approached your licensed traffic limit.
- Red indicates periods when your data usage exceeded your licensed traffic limit.

The **Active Loggers** indicate the number of ADP Loggers the data from which contributes to the license monitoring report. For more details, you can export the license report to PDF format, which includes data on the last 365 days.

If your ArcMC is enabled as a License Server, the Daily Usage bar chart displays the overall ADP license consumption on a daily basis. The daily license usage is calculated from the managed connectors (version of 7.3.0 or later) and managed ADP loggers based on the following:

- If a Connector is managed by ArcMC, then ArcMC will include its event ingestion from all non-ADP or non-managed source devices in the ADP daily license usage calculation. If a source is also a managed ADP component, the event flow from this source to the managed Connector will not be tracked.
- If an ADP Logger is managed by ArcMC, then ArcMC will include its event ingestion from all non-ADP or non-managed source devices in the ADP daily license usage calculation. If a source is also a managed ADP component, the event flow from this source to the managed ADP Logger will not be tracked.

Each day, ArcMC collects the daily ingestion information from each Connector and ADP Logger. Connectors and Loggers give an accumulated ingestion total when not reachable by ArcMC at the time of ingestion collection (daily at 1:00:00 ArcMC local time by default). This scenario could be caused by any of the following:

- The ADP Logger or Connector was down.
- The ADP Logger or Connector's server certificate has changed.

- The ADP Logger or Connector was not managed by the ArcMC.

If any managed nodes (Connector, ADP logger) are not reachable during ingestion collection time, the daily consumption of these nodes will be counted and reflected in the consumption number on a daily report, when ArcMC license server has successfully pulled the consumption data from the affected nodes.

Note: Daily ingestion collection only applies to License Server ArcMCs and ArcMCs that are managed by the License Server.

The ingestion report on an individual ADP Logger includes its previous day's ingestion during the time window of [00:00:00 – 23:59:59] GMT. For license usage calculation, ArcMC collects the previous ADP Logger's ingestion during the time window of [01:00:00 – 24:59:59] ArcMC local time. The time window used for individual Logger ingestion tracking and ingestion calculation are different; hence, it is not recommended to compare these two reports because they will report different numbers.

To enable the display of ADP license usage:

1. Enable ArcMC as an ADP license server. In the ArcMC toolbar, click **ADP License Server**, then click **Yes**.
2. Upload a valid capacity license to the ArcMC on the **License and Upgrade** page.

To export the license report to PDF format:

1. Click **Export License Report**.
2. The PDF is downloaded to your local system.

EPS License Reporting

The customer is considered to be in compliance with the license agreement as long as the MMEPS value indicators remain at the limit or below the purchased license capacity. If 3 or more consecutive MMEPS value indicators exceed their capacity based on the purchased license, they are considered to be out of compliance.



Note: ArcMC will only report events from the managed EPS licensed Loggers.

You can download up to one year license reports in PDF format.

Keystones:

1. **Events per Day (EPD):** Is the total number of events generated in a 24 hour clock period. The clock is calculated based on UTC time starting at 00:00:00 and ending at 23:59:59, regardless of the local times used.

2. **Sustained EPS (SEPS):** Is the event “constant” per second supported by the system within the 24 hour clock period. It stabilizes peaks and valleys and gives a better indication of use
3. **Moving Median EPS (MMEPS):** Is the license usage. It uses the 45 day period SEPS data shifting the calculation window 1 day every 24 hours after the first 45 days. The clock is calculated based on UTC time starting at 00:00:00 and ending at 23:59:59, regardless of the local times used.
4. **License Limit:** Corresponds to the amount of EPS acquired in the license.
5. **Baselining:** The baselining period begins when an EPS licensed product is detected in ArcMC for the first time (day 1), and it continues for the next 45 days. Once ArcMC detects an EPS licensed product, the baseline is set, and it does not change even if the license is redeployed. During this period, the usage will be calculated as the median of the SEPS values available at that moment. MMEPS values are truncated to benefit the customer. For example:

MMEPS Calculation

Day 1: SEPS of day 1

Day 2: Truncated median of SEPS of days 1 and 2.

Day 3: Truncated median of SEPS of days 1, 2, and 3.

Day 45: Truncated median value of SEPS of days 1 through 45

EPS License Usage Calculation

The usage will be collected from each managed Loggers and ArcMCs once a day.

- **Moving Median Events Per Second (MMEPS):** The median value over the last 45 days.
- **Baselining:** The usage will be calculated as the median of the SEPS values available at that moment. MMEPS values are truncated to benefit the customer.

Host Status Exceptions

This feature lists all the managed nodes that are in either Fatal, Critical or Warning status. To access the monitoring metric details view of a managed node, click **Dashboard > Host Status Exceptions**.

The following fields are displayed in the host status exceptions page:

- Host name: Name of the host.
- Status: Status of the host (Fatal, Critical, Warning).
- Cause: Root cause for hosts to be unhealthy (usually due to being unreachable or triggering a specific rule).

- Type: Type of host.
- Logical Group Path: Host location within ArcMC.

Monitoring Rules

Monitoring rules are defined to generate monitoring warnings for each managed product type. ArcMC includes many [preset monitoring rules](#) for your use. You can use these rules as written, or customize them for your own use. In addition, you can [create your own custom monitoring rules](#).

A monitoring rule comprises a set of logical, performance, health, or other criteria. All criteria in the rule are evaluated together to determine the rule's total effect, which generates an alert from ArcMC.

Rules breaches will be displayed in the Warning Severity Issue Summary, which you can view by clicking one of the ring meters on the [Monitoring Dashboard](#).

For example, a rule could check for the number of *input events per second* (criterion #1) that reach a *certain type of device* (criterion #2). Should this number *exceed* (criterion #3) a specified *level* (criterion #4), then a *warning (alert)* should be returned.

Breach Function

The breach function checks the backend monitor metric data table. The metric data table is updated every 3 minutes, and the breach check function runs every four minutes at the 45th second. Reducing the rule's time range to a smaller number (e.g. 1 or 2) could result in an undetected breach.

Alerts can be delivered by [email](#) or by [SNMP](#), or can be recorded in [audit logs](#). Only when there is new breach detected (i.e. not found on the previous run), ArcMC sends the notification/alert if the notification option is enabled. If the breach keeps coming on the subsequent calls, the alert will only be sent the first time.

For more information on managing and creating rules, see "[Managing Rules](#)" on page 56.

Preset Rules

ArcSight Management Center includes preset rules to assist in monitoring. You can use these preset rules as written or customize them as needed for your own use. You can also [create custom rules](#) of your own.

By default, ArcMC preset rules are disabled. You must enable a preset rule in order for it to apply and trigger alerts.



Note: For customers with previous versions of ArcMC and who already have a list of existing rules, preset rules included in ArcMC are appended to your existing rules.

To review preset rules:

1. Click **Dashboard > Rules**. The Monitoring Rules summary is shown.
2. To view a rule's settings in detail, in the **Name** column, click the rule name.
3. To enable a disabled preset rule, under **Status**, select **Enable**.

Preset Rules Description

Name	Description	Products		
MM_DD_YYYY_RAID_BATTERY_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the Raid Battery has failed during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_POWER_SUPPLY_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the Power supply has failed during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_TEMPERATURE_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the temperature reaches a certain level during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_POWER_SUPPLY_Degraded_ArcMC_ConApp_Logger	Sends a warning when the power supply has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_VOLTAGE_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the voltage levels have been failing during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_FAN_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the fan has failed during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_HARD_DRIVE_Rebuilding_ArcMC_ConApp_Logger	Sends a warning when the hard drive has been rebuilding during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_RAID_CONTROLLER_Failed_ArcMC_ConApp_Logger	Displays a critical alert when the RAID controller has failed during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_CURRENT_Degraded_ArcMC_ConApp_Logger	Sends a warning when the current has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_RAID_CONTROLLER_Degraded_ArcMC_ConApp_Logger	Sends a warning when the raid controller has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger

Name	Description	Products		
MM_DD_YYYY_VOLTAGE_Degraded_ArcMC_ConApp_LOGGER	Sends a warning when the voltage has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_ALL_EPS_OUT_ArcMC_ConApp_LOGGER	Displays a critical alert when all outgoing events per second have failed during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_HARD_DRIVE_Failed_ArcMC_ConApp_LOGGER	Displays a critical alert when the hard drive has failed during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_Queue_Files_Accumulated	Displays a critical alert when files have accumulated in queue during the last 5 minutes.			Connector
MM_DD_YYYY_Full_GC	Sends a warning when the garbage collection count is higher than 7 during the last 60 minutes.			Connector
MM_DD_YYYY_Caching	Sends a warning when the connector caching is higher than 100 during the last 5 minutes.			Connector
MM_DD_YYYY_Receiver_Down	Sends a warning when the receiver has been down during the last 5 minutes.			Logger
MM_DD_YYYY_Events_Dropped_from_Cache	Displays a fatal alert when the connector events dropped from cache have been down during the last 5 minutes.			Connector
MM_DD_YYYY_Files_Dropped_From_Cache	Displays a critical alert when the connector files dropped from cache have been down during the last 5 minutes.			Connector
MM_DD_YYYY_LOGGER_Not_Receiving_Data	Displays a fatal alert when logger hasn't received data during the last 30 minutes.			Logger
MM_DD_YYYY_Storage_Disk_Usage_above_85%	Sends a warning when the storage limit goes over 85% during the last 5 minutes.			Logger
MM_DD_YYYY_JVM_MEMORY_ArcMC_ConApp_LOGGER	Sends a warning when the jvm memory reaches 800 GB during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_Connector_Restart	Sends a warning when the connector has restarted more than 5 times during the last 5 minutes.			Connector

Name	Description	Products		
MM_DD_YYYY_Memory Red Zone	Displays a critical alert when the Connector JVM memory has gone over 90% during the last 5 minutes.			Connector
MM_DD_YYYY_Memory Yellow Zone	Sends a warning when the Connector JVM memory has gone over 80% during the last 5 minutes.			Connector
MM_DD_YYYY_Events Dropped From Queue	Displays a fatal alert when more than 100 Connector queue events dropped during the last 5 minutes.			Connector
MM_DD_YYYY_Files Dropping From Queue	Displays a critical alert when Connector files dropped from queue during the last 5 minutes.			Connector
MM_DD_YYYY_RAID_ BATTERY_Degraded_ ArcMC_ConApp_Logger	Sends a warning when the raid battery has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_ TEMPERATURE_ Degraded_ArcMC_ ConApp_Logger	Sends a warning when the temperature has been degraded during the last 5 minutes in	ArcMC	ConApp	Logger
MM_DD_YYYY_EPS_OUT_ Connector	Displays a critical alert when the outgoing events per second have been degraded during the last 5 minutes.			Connector
MM_DD_YYYY_FAN_ Degraded_ArcMC_ ConApp_Logger	Sends a warning when the fan's RPMs have failed during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_HARD_ DRIVE_Degraded_ArcMC_ ConApp_Logger	Sends a warning when the hard drive has been degraded during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_ALL_EPS_ IN_ArcMC_ConApp_ Logger	Displays a critical alert when all incoming events per second have failed during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_CPU_ USAGE_ArcMC_ConApp_ Logger	Sends a warning when the cpu usage has exceeded 50% during the last 5 minutes.	ArcMC	ConApp	Logger
MM_DD_YYYY_QUEUE_ DROP_COUNT_Connector	Sends a warning when Objects dropped from file Queue during the last 5 minutes.			Connector
MM_DD_YYYY_CURRENT_ Failed_ArcMC_ConApp_ Logger	Displays a critical alert when the current has failed during the last 5 minutes.	ArcMC	ConApp	Logger

Managing Rules

To create a custom rule:

1. Click **Dashboard > Rules**.
2. In the toolbar, click **Add New Rule**.
3. Select values for the [rule parameters](#).
4. Click **Save**.

To edit an existing rule:

1. Click **Dashboard > Rules**.
2. Under **Monitoring Rules**, select the rule you wish to edit.
3. Click **Edit Rule**.
4. Select new values for the [rule parameters](#), as needed.
5. Click **Save**. Alternatively, click **Save As** to save the edited rule with a new name.

When creating or editing rules, the only characters that are allowed for naming them are the following:

- Letters (a-z and/or A-Z)
- Numbers and spaces
- Symbols (only restricted to): % _ and -

To export all rules to a text file:

1. Click **Dashboard > Rules**.
2. In the toolbar, click **Export**. Your rules are exported to a local text file called `monitor_breach_rules.properties` and downloaded locally.



Caution: Do not partially delete a rule from the exported breach rules file. The rules file to be uploaded should have all the properties for all the rules in the file. Before uploading a new breach rules file create a backup of the existing file.

To import a rule:

1. Click **Dashboard > Rules**.
2. In the toolbar, click **Import**. A new window will pop-up, click **Browse**, find the location of the file, select it, and click **Import**.

Global Settings

1. Click **Dashboard > Rules**.
2. In the toolbar, click **Global Settings**. The following settings are displayed: **SNMP Notifications**, **Email Notifications**, and **Audit Notifications**. These settings enable or disable notifications to be sent by ArcMC.

To enable (or disable) a rule:

1. Click **Dashboard > Rules**.
2. In the management panel, under **Monitoring Rules**, select the rule to enable or disable.
3. In the **Rule Name** column, click the rule name.
4. Under **Status**, toggle the status to **Enable** (or **Disable**).
5. Click **Save**.

To delete a rule:

1. Click **Dashboard > Rules**.
2. Under **Monitoring Rules**, select the rule you wish to delete.
3. Click **Delete**.
4. Click **OK** to confirm deletion.

Monitoring Rules Parameters

Monitoring rules are defined by rule parameters. The following table describes monitoring rules parameters and their valid values.

Monitoring Rules Parameters

Parameter	Description
Name	Name of the rule. (Max. length 50 characters)
Metric Type	Criterion being measured. For valid values of Metric Type, see the Valid Values for Metric Type table, below. Each metric type has a Value Type constraining the kind of value which may be assigned to it.
Product Type(s)	Managed product type (or types) to which the rule applies. These are automatically selected based on the Metric Type. For example, if you selected a metric type that applied only to hardware, such as Voltage, only products with hardware form factors would be available for selection. You can also deselect types to which to apply the rule, as applicable.

Monitoring Rules Parameters, continued

Parameter	Description
Specific Node Selector	Click View/Choose , then select one or more specific nodes to which the rule applies. If none are chosen, then the rule applies to all nodes of the selected Product Types.
Severity	Breach severity. Valid values are Healthy, Warning, Critical and Fatal. Thresholds for each of these values are defined by the administrator.
Aggregation	Aggregation function applied to Metric Type data points. Valid values: <ul style="list-style-type: none"> • ANY: any value • AVG: average value (numeric values only) • MIN: minimum value (numeric values only) • MAX: maximum value (numeric values only) • SUM: addition of values (numeric values only)
Measurement	A comparison between two criteria. Valid values: <ul style="list-style-type: none"> • GREATER: One field is greater than the other • LESS: One field is less than the other • EQUAL: One field is equal to the other • NOT_EQUAL: Two fields are unequal
Value	Threshold value for comparison. Valid values are dependent on Metric Type. <ul style="list-style-type: none"> • Percentage: Number from 1-100 (with no %-sign). • Numeric: Numeric string. • Boolean: true/false (case-insensitive) • Literal Status: Status of the appliance component, and can be one of the following values: <i>Ok, Degraded, Rebuilding, Failed, Unavailable</i>.
Notify Me	Select one or more notification mechanisms for alerts about the rule (Email , SNMP , or Audit Forwarding).
Status	If Enabled , the rule will apply and produce alerts, as specified in Notify Me . (ArcMC rule presets are Disabled by default.)
Time Range	Evaluation interval, in hours and minutes. The total of hours and minutes must not exceed 168 hours (7 days).



Note: Compound rules (AND/OR) are not supported.

Valid Values for Metric Type

Value	Description	Value Type
Description	Brief description of the rule. (Max. length 300 characters.)	What kind of value this is.
For Connector Appliances or Loggers only		
CPU Usage	CPU usage, as a percentage.	Percentage
JVM Memory	Memory of Java Virtual Machine.	Numeric
Disk Read	Number of reads of the disk.	Numeric
Disk Write	Number of writes to the disk.	Numeric
All EPS In	Total Events Per Second in.	Numeric
All EPS Out	Total Events Per Second out.	Numeric
For Connectors only		
Events/Sec (SLC)	Events Per Second (EPS) in (Since Last Checked)	Numeric
EPS In	Events Per Second (EPS) in.	Numeric
EPS Out	Events Per Second (EPS) out.	Numeric
Events Processed	Number of events processed.	Numeric
Events Processed (SLC)	Events processed (Since Last Checked).	Numeric
FIPS Enabled	1= FIPS enabled, 0=FIPS disabled.	Boolean
Command Responses Processed	Number of command responses processed.	Numeric
Queue Drop Count	Queue drop count.	Numeric
Queue Rate (SLC)	Queue rate (Since Last Checked).	Numeric
Active Thread Count	Active thread count.	Numeric
For hardware form factor products only		
Fan	Hardware fan status.	Literal Status
Disk Space	Hardware disk space status. Disk space will be reported as "degraded" if storage reaches 75% of its capacity. Other statuses are not used.	Literal Status
Voltage	Hardware voltage status.	Literal Status
Current	Hardware current status.	Literal Status
Temperature	Hardware temperature status.	Literal Status
Power Supply	Hardware power supply status.	Literal Status

Valid Values for Metric Type, continued

Value	Description	Value Type
RAID Controller	RAID controller status.	Literal Status
RAID Battery	RAID battery status.	Literal Status
Hard Drive	Hard drive status.	Literal Status
For Loggers Only		
Storage Group Usage	Current storage group usage, in bytes.	Numeric
Storage Group Capacity	Current storage group capacity, in bytes.	Numeric
For Transformation Hubs Only		
Transformation Hub All Bytes In	All bytes received by the Transformation Hub cluster.	Numeric
Transformation Hub All Bytes Out	All bytes transmitted by the Transformation Hub cluster. Note that due to the replication of each topic, Bytes Out will always exceed Bytes In.	Numeric
Transformation Hub Disk Usage	Disk usage of Transformation Hub's individual nodes.	Numeric
Transformation Hub Memory Usage	Memory usage of Transformation Hub's individual nodes.	Numeric
Transformation Hub SP EPS	Count of events per second received by Transformation Hub's Stream Processor.	Numeric
Transformation Hub SP Error	Count of events per second waiting to be processed received by Transformation Hub's Stream Processor which produced an error.	Numeric
Transformation Hub SP Lag	Count of events per second waiting to be received by Transformation Hub's Stream Processor.	Numeric
For Collectors Only		
Collector CPU Load Average	Average load of Collector CPU.	Numeric
GC Count	Count of Java garbage collection.	Numeric
Restart Count	Number of restarts.	Numeric
Total Memory	Total JVM memory.	Numeric
Used Memory	JVM memory in use.	Numeric

Rule Verification

It is possible to create syntactically valid rules that return confusing or meaningless alerts. For example, you could create a syntactically valid rule to trigger an alert if CPU usage is below 101%, but this rule would not return useful alerts (since it would alert you constantly).

Always verify your rules to ensure that they return meaningful values, to help you best detect problems and issues.



Note: Custom Polling Intervals: ArcSight Management Center uses three polling intervals (4 hours, 1 day, and 1 week) associated with metric data archive types across ArcSight products. These intervals can be adjusted for proper usage, if required.

It is strongly recommended that you adjust these intervals only if you fully understand the impact of the changes.

Polling intervals can be specified in the file `logger.properties` using a text editor.

- 4-hour data (minimum allowed interval 1 minute):

```
monitoring.data.poll.4hour.cron=10 0/3 * * *
```

This property indicates a poll at 3 minute intervals.

- 1-day data (minimum allowed interval 5 minutes):

```
monitoring.data.poll.1day.cron=15 0/10 * * *
```

This property indicates a poll at 10 minute intervals.

- 1-week data (minimum allowed interval 1 hour):

```
monitoring.data.poll.1week.cron=20 2 */2 * * *
```

This property indicates a poll at 2 hour intervals.

After making the changes and saving the edited file, a server restart is required for the changes to take effect.

Custom Rules Examples

Shown here are examples of custom monitoring rules.

Example 1: Warning Breach

This example specifies the following Warning condition:

"Generate a Warning breach if the average CPU usage of any ArcMC in the past 30 minutes is greater than 70%."

Name: ArcMC Warning

Metric Type: CPU Usage

Product Type: ArcMCs

Severity: Warning

Aggregation: AVG

Measurement: GREATER

Value: 70

Timespan: 30 minutes

Example 2: Critical Breach

Example 2 specifies the following Critical condition:

"Generate a Critical breach if the Power Supply fails on any Logger Appliance in the past hour."

Name: Logger Warning

Metric Type: Power Supply

Product Type: Loggers

Severity: Critical

Aggregation: ANY

Measurement: EQUAL

Value: Failed

Timespan: 60 minutes

Device Rule Management

Device Rule Management involves creating, editing and deleting rules specifically for devices. The operation of creating, editing and deleting rules is different than what is done for other entities. Rules are created on the Device List page. The contents of the rule are the same as those of the exiting rule.

The Device List page is where you manage rules. This page has two tabs: Devices and Manage Rules.

Device Inactive Notification

When ArcMC detects an inactive device, (time out value can be defined by the customer on the Device UI page, default value is set to 20 minutes), the internal defined device inactive rule is triggered, and an alert is sent out via snmp, email, and audit log.

There are two options for users who don't want to receive device inactive notifications:

1. Keep the device on “active” status: Review the connector’s device event status and configure a proper interval value for Device Product time-out interval on **Dashboard > Monitoring Summary> Devices UI** page.
2. Contact support to disable device inactive notifications.

Managing Devices

About

From the Devices page you can add one or more devices to a new rule or add one or more devices to an existing rule.

The Lead Breach column describes the Lead Breach for a device. The Severity column describes the severity of a device. Severity is defined when creating a rule. The # of Rules column describes the number of rules applied to the devices.

Procedure

Location: Dashboard > Monitoring summary > Devices count indicator > Devices page

To add one or more devices to a new rule

1. Select the desired device or devices.
2. Click **Add New Rule**.
3. From the Add New Rule dialog, specify the necessary information.

Device rules support "EPS out" and "Bytes out" measurements.

To add one or more devices to an existing rule

1. Select the desired device or devices.
2. Click **Add to Existing Rule**.
3. From the Add to Existing Rule dialog, specify the existing rule.

See also

- ["Device Rule Management" on page 62](#)
- ["Managing Device Rules" on the next page](#)

Managing Device Rules

About

The Manage Rules page lists of all the rules and options: Disable, Enable, Delete and Edit an existing rule. The multi-selection option is available for Disable, Enable and Deleting the Rules. You can Edit one rule at a time.

A device that has stopped sending events will be marked as "Fatal" and there is no rule to change that. The timeout value for each device product is configurable and documented.

Procedure

Location: Dashboard > Monitoring summary > Devices count indicator > Manage Rules tab

1. Click **Manage Rules**.
2. From the Rules Details page, specify the desired management option.

See also

- ["Device Rule Management" on page 62](#)
- ["Managing Devices" on the previous page](#)

Configuring Email Notifications

Email notifications will inform recipients about monitored nodes being down or out of communications.



Note: Email alerts do not include issues with connectors or Collectors. However, containers may be the subject of email alerts.

Before configuring email notifications, ensure that values are specified for your SMTP settings under **Administration > System Admin > System > SMTP**. For more information on SMTP settings, see ["SMTP" on page 271](#).

Once configured, email notifications must be configured for each of the notification rules you wish to trigger an alert.

To configure email notifications:

1. In a text editor, open the file .../userdata/arcmc/logger.properties. (If the file does not exist, you can create it in a text editor. When creating the file, ensure that it is owned by the non-root user.)

2. Add a new line with the new property named `monitoring.notification.emails` and a value equal to a comma-separated list of email addresses of all administrators you intend to receive notifications. For example, this value would send email alerts to `address1@example.com` and `address2@example.com`:

```
monitoring.notification.emails=address1@example.com,  
address2@example.com
```

3. Save the modified `logger.properties` file.
4. Restart the ArcMC web process.
5. In the rules editor, open the notification rule you wish to trigger an email alert, and under **Notify Me**, select *Email*.

Example Email Notification

An example of the email sent to recipients is shown here.

<URI> refers to the URI of a problematic node.

NodeN is the hostname of a problematic node.

This information is found on the **Hosts** tab under Node Management.

```
Subject: <Email title>  
The following nodes are either down or not reachable from ArcSight Management  
Center:
```

```
//Default/<URI>/<Node1>  
//Default/<URI>/<Node2>
```

Configuring SNMP Notifications

SNMP notifications will send SNMP traps about monitored nodes being down or out of communications.

To configure SNMP notifications on ArcMC appliance:

1. Under **Administration > System Admin > System > SNMP**, enable SNMP. Then, specify values for port, SNMP version, and other required settings for your SNMP environment.
2. In the rules editor, open the notification rule you wish to trigger an SNMP alert, and under **Notify Me**, select *SNMP*. Repeat for each rule you wish to trigger an SNMP alert.

Enabling SNMP on Software

Software ArcMC does not include UI controls for SNMP configuration. Instead, take these steps to configure Software ArcMC for SNMP notifications and monitoring.

To enable SNMP notifications on a software host:

1. Make sure following RPM packages are installed on the system: net-snmp, net-snmp-utils, net-snmp-libs, lm_sensors-libs.
2. Enable the SNMP service by entering: chkconfig snmpd on
3. Start the SNMP service by entering: service snmpd start
4. In a text editor, create a file /opt/arcsight/userdata/platform/snmp.properties with the following parameters, Items in angle brackets <> indicate you should substitute values appropriate for your own environment.

```
snmp.enabled=true  
snmp.version=V3  
snmp.port=161  
snmp.v3.authprotocol=SHA  
snmp.v3.authpassphrase=<password>  
snmp.v3.privacyprotocol=AES128  
snmp.v3.privacypassphrase=<password>  
snmp.user=<SNMP username>  
snmp.community=public  
snmp.system.location=<SNMP location>  
snmp.system.name=ArcMC Node 247  
snmp.system.contact=<your support email address>  
snmp.trap.enabled=true  
snmp.trap.version=V3  
snmp.trap.port=162  
snmp.trap.nms=<IP address of NNMI>  
snmp.trap.user=<SNMP trap user name>  
snmp.trap.community=public  
snmp.trap.v3.authprotocol=SHA  
snmp.trap.v3.authpassphrase=<password>  
snmp.trap.v3.privacyprotocol=AES128
```

```
snmp.trap.v3.privacypassphrase=<password>
```

-
5. Give the file permission: 644 and owner: arcsight.
 6. Copy the file ARCSIGHT-EVENT-MIB.txt file from \$ARCSIGHT_HOME/current/arcsight/aps/conf/ to location /usr/share/snmp/mibs. Give the file permission: 644 and owner: root:root.

7. Run the script arcsight_snmpconf script as a root user, as follows:

```
<ArcSight_Home>/current/arcsight/aps/bin/arcsight_snmpconf <ArcSight_Home>/userdata/platform/snmp.properties trap
```

8. Run the script a second time, as follows:

```
<ArcSight_Home>/current/arcsight/aps/bin/arcsight_snmpconf <ArcSight_Home>/userdata/platform/snmp.properties poll
```

This script will setup /etc/snmp/snmpd.conf file and restart the SNMP service.

9. Restart SNMP services: service snmpd restart



Note: To preserve the SNMP V3 Trap oldEngineID persistent in software ArcMC, set the \$ARCMC_HOME/userdata/platform/snmp_persist/snmpapp.conf file to be immutable:
#chattr +i \$file_path_of_snmpapp.conf
Follow the steps below to create the snmpapp.conf file if it does not exist in the snmp_persist folder:

- a) In a text editor, create a file <ARCSIGHT_HOME>/userdata/platform/snmp_persist/snmpapp.conf with the following entry: oldEngineID \$VALUE

\$VALUE: copy the value from the oldEngineID entry to /var/lib/net-snmp/snmpd.conf

For example: oldEngineID 0x80001f888011b5336c8d41895f00000000

- b) Give the file permission 600:

```
chmod 600 <ARCSIGHT HOME>/userdata/platform/snmp_persist/snmpapp.conf
```

- c) Set the owner:

If arcmc is installed as root user: # chown root:root <ARCSIGHT_HOME>/userdata/platform/snmp_persist/snmpapp.conf

If arcmc is installed as arcsight user: #chown arcsight:arcsight <ARCSIGHT_HOME>/userdata/platform/snmp_persist/snmpapp.conf

- d) Set immutable:

```
chattr +i <ARCSIGHT_HOME>/userdata/platform/snmp_persist/snmpapp.conf
```

10. In the rules editor, open the notification rule you wish to trigger an SNMP alert, and under **Notify Me**, select *SNMP*. Repeat for each rule you wish to trigger an SNMP alert.

Topology View

The Topology View displays your end-to-end data flow in browseable format. Shown are the logical relationships between network devices (event producers), connectors and Collectors, and their destinations in each of your ArcMC locations.

As your environment scales to thousands of source devices, you can use logical groupings (locations) to model subsystems, and datacenters can quickly trace issues and drill down on details.

To display the Topology View, click Dashboard > Topology View.

The left column highlights the current topology view. The available views are based on the [locations defined in ArcMC](#).

Each of monitor icons represents a Device Product type, and the bubbles on the left of each monitor icon indicate the number of devices for each Device Product type.

The severity status of each item in the topology view is indicated by its color. Item status may be Healthy (green), Fatal (red), Critical (amber), Warning (yellow), or Unknown (gray).

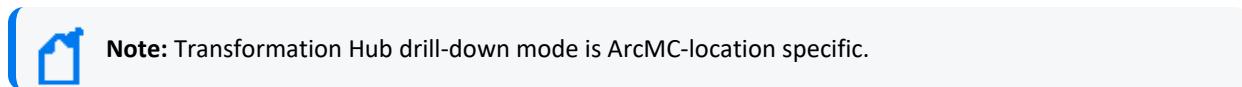
The status indicates the severity as reported by the managed product. Hovering over the device product show more details of the severity status. Clicking on any of the severity levels opens the device details filtered by that product type and severity combination.

The **Devices** area shows any devices which are forwarding events in your network.

- To view the EPS (events per second) traffic to and from a device, mouse over the device.

The **Connectors/Collectors** area shows connectors and Collectors in the current topology view, specific to the location.

- To view the EPS (events per second) traffic to and from a connector, and get an overview of the connector status, mouse over the connector. Also shown are name, Device Type, Status, Path, Rule Violation (if any), Version, and ArcMC Managed.
- To drill down and view the health of the connector in detail, including health history, click the connector.
- In some cases, such as immediately following adding a connector node, an unmanaged connector may be displayed. This will be replaced with the connector data within a few collection cycles as data from the new connector is collected.
- Connectors displayed with the  symbol are included in a different location from the one currently selected for viewing.



Note: Transformation Hub drill-down mode is ArcMC-location specific.

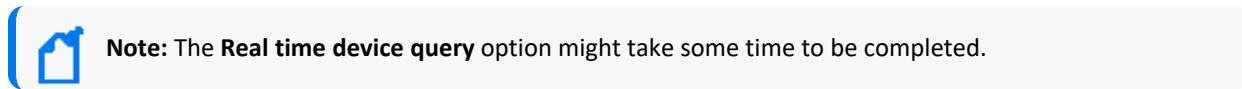
The **Destinations** area shows connector destinations.

- To drill down and view the health of an ArcMC-managed destination in detail, click the destination.

The Topology View refreshes automatically once per minute. (You can toggle automatic data refresh with the **Auto Refresh** control.) To refresh the view manually, click **Refresh** in the toolbar.

The **Export** button allows users to export the devices list, status, last reported, eps, event size, connector, and customer URI into a CSV file.

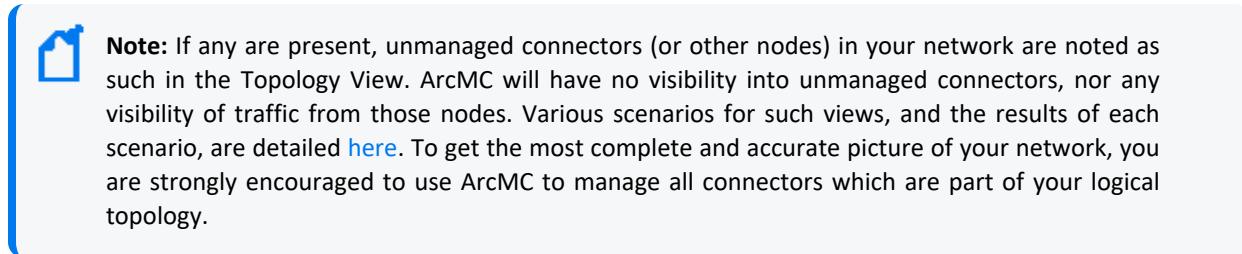
When exporting the devices list, users can choose between **Use stored data** and **Real time device query** information. These options are displayed from a drop-down after clicking the **Export** button.



Note: The **Real time device query** option might take some time to be completed.

You can also toggle the display of legends for the graphic with the **Legends** control.

Click **Deployment View** to show your environment's [Deployment View](#).



Note: If any are present, unmanaged connectors (or other nodes) in your network are noted as such in the Topology View. ArcMC will have no visibility into unmanaged connectors, nor any visibility of traffic from those nodes. Various scenarios for such views, and the results of each scenario, are detailed [here](#). To get the most complete and accurate picture of your network, you are strongly encouraged to use ArcMC to manage all connectors which are part of your logical topology.

Deployment View

The Deployment View shows the physical relationships between network devices (event producers), connectors, their hosts, and their destinations in each of your ArcMC locations.

To display the Deployment View, click **Dashboard > Deployment View**.

The left column highlights the current deployment view. The available views are based on the physical hosts.

Each of the monitor icons represents a Device Product type, and the bubbles on the left of each monitor icon indicate the number of devices for each Device Product type.

The severity status of each item in the topology view is indicated by its color. Item status may be Healthy (green), Fatal (red), Critical (amber), Warning (yellow), or Unknown (gray).

The status indicates the severity as reported by the managed product. Hovering over the device product shows more details of the severity status. Clicking on any of the severity levels opens the device details filtered by that product type and severity combination.

The **Devices** area shows any devices which are forwarding events in your network.

- To view the EPS (events per second) traffic to and from a device, mouse over the device.

The **Connectors/Collectors** area shows connectors and Collectors in the current topology view.

- To view the EPS (events per second) traffic to and from a connector, and get an overview of the connector status, mouse over the connector. Also shown are name, Device Type, Status, Path, Rule Violation (if any) and ArcMC Managed.
- To drill down and view the health of the connector in detail, including health history, click the connector.
- In some cases, such as immediately after adding a connector node, an unmanaged connector may be displayed. This will be replaced with the connector data within a few collection cycles as data from the new connector is collected.
- Connectors displayed with the  symbol are included in a different location from the one currently selected for viewing.

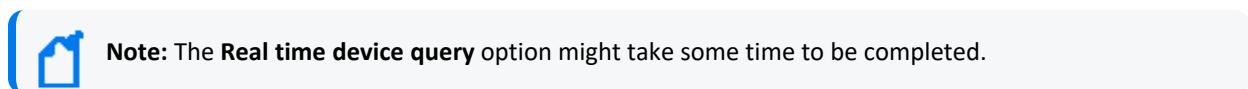
The **Destinations** area shows connector destinations.

- To drill down and view the health of an ArcMC-managed destination in detail, click the destination.

The Topology View refreshes automatically once per minute. (You can toggle automatic data refresh with the **Auto Refresh** control.) To refresh the view manually, click **Refresh** in the toolbar.

The **Export** button allows users to export the devices list, status, last reported, eps, event size, connector, and customer URI into a CSV file.

When exporting the devices list, users can choose between **Use stored data** and **Real time device query** information. These options are displayed from a drop-down after clicking the **Export** button.



You can also toggle the display of legends for the graphic with the **Legends** control.

Click **Topology View** to show the [topological](#) relationships in your environment.

Prerequisites for Instant Connector Deployment

The following are prerequisites for Instant Connector Deployment.

- You must set up one or more [deployment templates](#).
- Instant Connector Deployment is supported for accounts using SSH key authentication, but not supported for SSH with passphrase authentication. To enable SSH key authentication, the SSH key needs to be set up between a non-root user of ArcMC and a user of the remote host that will be used for deployment.
- In addition, it is strongly suggested you consult the Configuration Guide for the connector you plan to deploy before deployment, to understand any special considerations or features of the connector being installed.
- For more information regarding Connector destinations, please see the Smart Connectors User's Guide.
- The below prerequisites are not present by default on Linux 8.x, unlike in previous Linux versions (e.g. Linux 6.x and 7.x). Perform the following steps for RHEL/CentOS 8.1 on the machine where the ArcMC is or will be installed, and in the target Linux host (the VM where the Connector/Collector will be deployed):
 - a. Install python2:
For RHEL/CentOS 7.x:
`sudo yum install -y python2`
For RHEL/CentOS 8.x:
`sudo dnf install -y python2`
 - b. Create a symlink:
`sudo ln -s /usr/bin/python2 /usr/bin/python`
 - c. Install libselinux-python package:
For RHEL/CentOS 7.x:
`sudo yum install -y libselinux-python`
For RHEL/CentOS 8.x:
`sudo dnf install -y libselinux-python`



Note: If the yum/dnf command fails when installing libselinux- python on RHEL/CentOS, follow the steps below:
- Download `libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm`
- Install the package:
`rpm -i libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm`

Additional Requirements For Windows Platforms

The following additional items are required for Instant Connector Deployment on Windows platforms.

- Only the local admin account is supported for deployment.
- The following preparatory steps are required when deploying on a Windows VM.
 1. Enable PowerShell 4.0 or later.

<https://www.microsoft.com/en-us/download/details.aspx?id=40855>

2. Enable and configure PowerShell Remoting, with CredSSP authentication.

- Download the "ConfigureRemotingForAnsible.ps1" file:
 - <https://github.com/ansible/ansible/blob/devel/examples/scripts/ConfigureRemotingForAnsible.ps1>
 - Open Power Shell as Administrator and run the following command:
 - ConfigureRemotingForAnsible.ps1 -EnableCredSSP
3. Enable TLS 1.2.

Instant Connector Deployment

Instant Connector Deployment enables rapid installation of connectors or Collectors where you need them in your environment. You perform Instant Connector Deployment right from the Deployment View.

Before proceeding, ensure you have met all the [prerequisites](#) for performing Instant Connector Deployment.

To instantly deploy a connector or Collector:

1. Click **Dashboard > Deployment View**.
 2. In the **Connectors/Collectors** column label, click +, then select **Add Connector** or **Add Collector**.
 3. On the **Add Connector** (or **Add Collector**) dialog, specify values for the connector to be added. Any fields marked with an asterisk (*) are required. Note that your selected [deployment template](#) may populate some fields automatically, but you may overwrite the values in these fields, if needed, for a particular deployment. **Exception:** you may only use the latest version of the connector you have [uploaded to the repository when you set up deployment templates](#). You can add multiple destinations for each connector if needed.
 4. To add multiple hosts to the Host list, in the Host drop-down, click Add Host, then select or specify the name of each host.
- **Collector Hostname:** The Collector hostname must match the hostname of the remote machine. If the remote machine does not have proper DNS /hostname setup correctly, specify the IP address of the remote machine as the hostname.

- **Collector Destination:** A Collector's destination must be the th-syslog topic on your ArcMC-managed Transformation Hub.
 - **ArcSight SecureData Add-On Enablement:** To enable the ArcSight SecureData Add-on during deployment, under **Global Fields**, set **Format Preserving Encryption** to *Enabled*. For more information on enabling the SecureData Add-On, see "[SecureData Encryption](#)" on page 81.
4. To add multiple connectors (or Collectors) of the same type, click **Clone**. Then specify the information unique to the new connector (or Collector). When deploying multiple connectors, if any specified parameters (such as port number) are invalid, the deployment of all connectors in the job will fail.
 4. Click **Install**. The connector or Collector is deployed. Alternatively, click **Add** to add more connectors to the deployment job.



Note: Instant Connector Deployment (including Collectors) is not supported from RHEL/CentOS 6.9 to a remote Windows host.

You can track and manage deployment jobs and issues using the [Job Manager](#).



Note: If you later connect to a host where Connectors were installed through Instant Deployment, and run the Connector setup wizard from the command line, you should run agent setup from \$ARCSIGHT_HOME/current/bin by setting the mode with option, -i, such as: ./runagentsetup.sh -i console or ./runagentsetup.sh -i swing, where options are swing, console, silent, and so on. For more information on options, see the Smart Connectors User's Guide.

Deployment on Linux Platform Using Non-root User

Follow these steps to install a connector/collector using non-root user through instant deployment feature.

Step 1

Option 1: Provide blanket sudo rights to non-root users:

1. Edit the sudoers file on the remote machine where the connector/collector will be deployed:

- Open the sudoers file:

```
# visudo
```

- Locate the following lines in the file:

```
## Allow root to run any commands anywhere root ALL=(ALL) ALL
```

2. Provide blanket sudo rights to non-root user below the previously mentioned line.

```
<non-root-user> ALL= (ALL) NOPASSWD:ALL
```

3. Save the file.
4. Specify this non-root user and password in the instant deployment job.

Option 2: Provide rights to non-root user to execute specific set of commands as mentioned below:

1. Edit the sudoers file on the remote machine where the connector/collector will be deployed:

- Open the sudoers file:

```
# visudo
```

- Locate the following lines in the file:

```
## Allow root to run any commands anywhere root ALL=(ALL) ALL
```

2. Add special rights to the non-root user below the previously mentioned line:

```
<non-root-user> ALL=(ALL) NOPASSWD: /bin/chown root\:root <connector_install_dir>/current/config/agent/arc_<service_internal_name>, /bin/mv <connector_install_dir>/current/config/agent/arc_<service_internal_name> /etc/init.d/, /bin/chmod 755 /etc/init.d/arc_<service_internal_name>, /bin/rm -rf /etc/init.d/arc_<service_internal_name>
```



Note: <connector_install_dir> and <service_internal_name> should match exactly what the user will be entering in the instant deployment job. Provide these 4 commands in the sudoers for every connector/collector installation that will be done from ArcMC through this non-root user.

3. Save the file.
4. Specify this non-root user and password in the instant deployment job.

Step 2

Option 1: Use the Home user path.

The folder will be automatically created.

Option 2: Use an alternative path.

For non-root installation, users need to create the folder:

```
mkdir <path to folder>
```

Grant full permissions:

```
chmod 777 <path to folder>
```

Troubleshooting

This section describes possible scenarios in which users might encounter issues during the instant deployment of Connectors/Collectors.

Job does not start

Issue: Job does not start during a deployment(Connector/Collector) and no error message is displayed.

Possible solution: When the Job does not start and the status displayed is "Not Started", the possible reason is that the ArcMC has an 8.0 OS version or higher, and the python and associated library (libselinux) are not installed in the VM.

Job start but fails in the "Copy Installer" step

Issue: When a Job starts but fails in the "Copy Installer" step it will display the following message: "Aborting, the target uses SELinux but python bindings (libselinux-python) aren't installed!". This is related to a problem with the target host (where the Connector/Collector is going to be installed), the python or the SELinux are not installed there.

Possible solution: Go to the target host and install python and the SELinux library.

If the SSH certificate changes...

If the connector VM is redeployed, its SSH certificate will change and will no longer be able to use Instant Connector Deployment to deploy connectors to the VM. In this case, take the following steps to re-enable Instant Connector Deployment to the re-deployed VM.

1. Connect to the ArcMC's VM.
2. Change to the directory /home/<non root user>/.ssh
3. Open the file known_hosts.
4. Delete the line with the IP or hostname of the Connector's VM.
5. Save the file.

Deploying a Connector in Transformation Hub (CTH) (Standalone ArcMC)

A Connector in Transformation Hub (CTH) moves the security event normalization, categorization, and enrichment of connectors processing to the Docker containers environment of Transformation Hub, while reducing the work done by the Collector.

Ensure you have added a Transformation Hub host for a supported version (3.0 or later) before adding any CTHs. Transformation Hub 3.0 and later can have a maximum of 50 CTHs. Earlier versions can have up to 10 CTHs.

For a fresh installation, we provide 50 ports to support 50 of the CTHs.

If upgrading to Transformation Hub 3.1, you automatically get 50 ports for CTHs based on the new Transformation Hub images.



Note: CTHs cannot be configured with SecureData encryption. By default, CTH is set as TLS + CA.

To update the CTH port range:

1. Open logger.properties for editing.

Create the file if it does not exist.

```
/opt/arcmc/userdata/arcmc/logger.properties
```

```
chown <non-root user>:<non-root user> logger.properties
```

```
chmod 660 logger.properties
```

2. Add the following information to logger.properties.

```
# =====
```

```
# CTH port range
```

```
# =====
```

```
configuration.cth.end.port=39050
```

For Transformation Hub 3.3 and later use:

```
configuration.cth.end.port.post.th.32=32150
```

3. Restart the web process.

To deploy a CTH:



Note: To use the Global ID feature, Generator ID Manager has to be enabled in the ArcMC so that Generator ID can be set on the CTH.

1. Click **Dashboard > Deployment View**.
2. In the **Transformation Hub** column, click the managed Transformation Hub, then click the + icon.
3. On the **Deploy CTH** dialog, in **CTH Name**, specify a name for the CTH.

The name must be smaller than 256 characters.

- Under Acknowledgment mode, click the down arrow, then select the Acknowledgment mode for this CTH. (none/leader/all)

The mode you select affects the safety of stored events in case of immediate system failure.

Acknowledgment Mode	Description
none	<p>Acknowledgment off</p> <p>The producer will not wait for any acknowledgment from the server. The record will be immediately added to the socket buffer and considered sent.</p> <p>No guarantee can be made that the server has received the record in this case, and the retries configuration will not take effect (as the client won't generally know of any failures). The offset given back for each record will always be set to -1.</p>
leader	<p>Leader mode on</p> <p>The leader will write the record to its local log but will respond without awaiting full acknowledgment from all followers.</p> <p>In this case, if the leader fails immediately after acknowledging the record but before the followers have replicated it, the record will be lost.</p>
all	<p>All acknowledgments on</p> <p>The leader will wait for the full set of in-sync replicas to acknowledge the record; guaranteeing that the record will not be lost if at least one in-sync replica remains alive (strongest available guarantee). This is equivalent to the acks=-1 setting.</p>

- Under **Destination Topics**, click the down arrow, then select one or more destination topics (CEF, Avro, or binary) for the CTH.
- Select the corresponding ESM version. This is required for CTH to support Global ID when sending events to ESM 7.2
- Click **Deploy**.



Note: Please allow a few minutes after deploying or updating the CTH for the new values to be displayed.

The CTH deployment job status can be viewed in [Job Manager](#).

Once deployed, the CTH displays in Node Management on the Connectors tab, and in the Topology and Deployment View drill-down under the source topic.



Note: Destination topics must always be grouped the same for multiple CTHs. For example, if a CTH is sending events to both th-cef and th-esm topics, then any other CTH that sends events to one of these topics must also send events to the other topic, or events will be duplicated.

Editing a CTH

To edit a CTH:

1. Click **Dashboard > Deployment View**.
2. In the **Transformation Hub** column, click the managed Transformation Hub, then click the edit (pencil) icon.
3. On the **CTH Parameters** dialog, modify the name or destination topics, as needed.
4. Click **Redeploy**. The CTH is re-deployed. The job progress can be viewed in [Job Manager](#).

Undeploying CTHs

To undeploy one or more CTHs:

1. Click **Dashboard > Deployment View**.
2. Click on the Transformation Hub box to drill down.
3. Click the edit (pencil) icon.
4. On the **CTH Parameters** dialog, click **X** next to any CTHs to be undeployed.
5. Click **Redeploy**. The job progress can be viewed in [Job Manager](#).

Deploying Collectors

This section provides information about deploying Collectors, Non-TLS, TLS, and FIPS deployment.

1. Under **Dashboard > Deployment View**, click the  icon next to the **Connectors/Collectors** label and click **Add Collector**.
2. From the **Add Collector** window, under add collector details select the collector template.

Non-TLS Collectors Deployment

For Non-TLS Collector deployment:

1. Follow the steps in "[Deploying Collectors](#)" above section, and select the Syslog Daemon Collector template.
2. Scroll down to **Destination > Destination Template** and select the TH Collector Template.
3. Under **Kafka Broker Host(s):Port(s)**, confirm that port number is 9092, otherwise, change it accordingly.

4. Set the **Kafka Broker on SSL/TLS** flag to false.
5. Click **Install**.

TLS Collectors Deployment

For TLS Collector deployment:

1. Follow the steps in "[Deploying Collectors](#)" on the previous page section, and select the Syslog NG Daemon Collector template.
2. Scroll down to **Destination > Destination Template** and select the TH Collector Template.
3. Under **Kafka Broker Host(s):Port(s)** confirm that port number is 9093, otherwise, change it accordingly.
4. Set the **Kafka Broker on SSL/TLS** flag to true.
5. Click **Install**.

FIPS Collectors Deployment

FIPS can be enabled on Collectors either during the deployment of the Collector or while creating the Collector Configuration Template.

1. Follow the steps in "[Deploying Collectors](#)" on the previous page section.
2. From the **Add Collector** window, under add collector details select the collector template. Scroll down to the **Global Fields** section, and select **Enabled** from the **Enable FIPS mode** drop-down.
3. Replicate steps 2 through 4 in the "[TLS Collectors Deployment](#)" above section.
4. Click **Install**.

Post Deployment Collector Property Update

FIPS

1. Go to **Configuration Management > Bulk Operations**.
2. Click on the **Collector** tab, select one of the Collectors from the Manage Collectors table, and click **Properties**.
3. In the **Collector Property Update** window, click the  icon next to **Property List** and search for `fips.enable`.
4. Click **Edit** and set the Value to `true`.



Note: When setting the `fips.enable` property to `true`, you need to modify the property's `agents[0].destination[0].params.bootstraphosts` parameter port value to 9093, as well



as change the usessl parameter (SSL/TLS) value to true.

5. Click **Save**.

Non-TLS and TLS

For Non-TLS and TLS the process remains the same for steps 1 to 2 listed in "[Post Deployment Collector Property Update](#)" on the previous page In the **Collector Property Update** window, click the icon next to Property List and search for the agents[0].destination[0].params property. See the table below for the correct values.

Property	Parameter	Non-TLS	TLS
agents[0].destination[0].params	bootstraphosts	port value: 9092	port value: 9093
agents[0].destination[0].params	usessl	false	true

SecureData Encryption

To enable SecureData encryption, you must provide the SecureData server details in the [Deployment Template](#) for a connector.



Note: CTHs cannot be configured with SecureData encryption.

If any proxy settings are required, these must also be provided in the Deployment Template.

To explicitly specify that no proxy be used for the SecureData client, no parameters are needed in the Deployment Template. In addition, edit the file /etc/profile.d/proxy.sh (or its equivalent on Windows VM) and add/edit the line “export no_proxy and export NO_PROXY” with your SecureData server details.

If your SecureData client needs a certificate, then upload the valid certificate to ArcMC's cacerts repository when creating the deployment template.

After all settings are configured, and a connection is ensured from the connector host to the SecureData server, you can deploy the connector using the [Instant Connector Deployment](#) process.

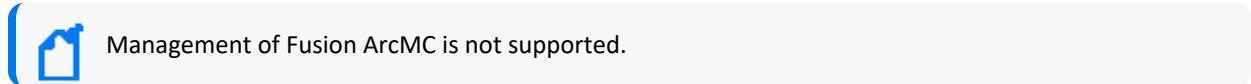


Warning: SecureData settings may only be updated once. Once encryption is turned on, it may not be turned off. Make sure you wish to use encryption before activating it.

Chapter 5: Managing Nodes

A *node* is a networked ArcSight product that can be centrally managed through ArcSight Management Center. Each node is associated with a single networked host which has been assigned a hostname, an IP address, or both.

Node types can include any of the following ArcSight products:



Management of Fusion ArcMC is not supported.

- Connector Appliances or Software Connector Appliances
- Logger Appliances or Software Loggers
- Containers, connectors, or Collectors
- Other ArcSight Management Centers, either software or Connector Hosting Appliances
- Transformation Hub

A single host, such as a single deployed Transformation Hub, can comprise multiple nodes for management purposes. In addition, a node can be in a parent or child relationship with other nodes.

You can perform any of the following node management tasks:

- View managed nodes by location, by host, or by node type.
- Add, view, edit, and delete locations for hosts.
- Add nodes from a host, import hosts from a CSV file, view and delete hosts, view all hosts in a location, update software on hosts, move hosts to different locations, and scan hosts for new connectors or containers.

For more information on adding hosts, see ["About Adding a Host" on page 97](#).

The following topics are discussed here.

Node Management

To manage nodes, on the menu bar, click **Node Management > View All Nodes**. The Node Management UI displays. The Node Management UI comprises two panels:

- The left side displays the navigation tree.
- The right side displays the management panel, enabling you to perform management operations on items selected in the navigation tree.

The Navigation Tree

The navigation tree organizes managed nodes into a hierarchy, and comprises the following:

- **System:** Displays the entire set of nodes managed by Arcsight Management Center.
- **Location:** Individual locations are displayed under **System**, listed in the order in which they were added. Locations are logical groupings you can use to organize a list of hosts. For more information, see "[Locations](#)" on page 95.
- **Host:** Each location branch shows all hosts assigned to that location, listed by hostname, in the order in which they were added. For more information, see "[Hosts](#)" on page 96.
- **Node Types:** Each host branch shows all managed nodes associated with that host. A node can be any of the following types:
 - **Connector Appliance or Software Connector Appliance:** Each Connector Appliance (hardware or software) is shown as a separate node.
 - **Logger Appliance or Software Logger:** Each Logger (hardware or software) is shown as a separate node.
 - **ArcSight Management Center:** Each ArcSight Management Center (hardware or software) is shown as a separate node.
 - **Container:** If the host includes any containers, each is shown as a node.
 - **Connector:** If a container node contains a connector, the connector is shown under the container node in which it is contained.
 - **Collector:** If a container node contains a Collector, the Collector is shown under the container node in which it is contained.
 - **Transformation Hub:** A managed Transformation Hub is shown as a node.

Since items in the tree are organized hierarchically, each item in the tree includes all branches displayed below it. For example, a **Location** branch includes all hosts assigned to that location. Click the wedge icon to toggle the view of any branch and any items included in the branch.

The Management Panel

Select an item in the navigation tree to display its details on one of the tabs in the central management panel. For example, to display the details of a host shown in the navigation tree, select the host in the tree. The management panel to the right of the tree will display details and controls pertaining to selected host.

Management Tabs

The tabs displayed in the management panel depend on the type of item selected in the navigation tree. The management tabs displayed will show detailed information associated with the selected item, depending on its position in the hierarchy.

Selected Item Type in Navigation Tree	Tabs Shown in Management Panel
System	Locations, Hosts, Containers, Connectors, Collectors, ConApps, Loggers, ArcMCs, TH Nodes
Location	Hosts, Containers, Connectors, Collectors, ConApps, Loggers, ArcMCs, TH Nodes
Host	Containers, Connectors, Collectors, ConApps, Loggers, ArcMCs, TH Nodes
Node	Connectors, Collectors, ConApps, Loggers, ArcMCs, TH Nodes

For example, if you selected a location item from the navigation tree, the **Hosts, Containers, Connectors, Collectors, ConApps, Loggers ArcMCs** and **TH Nodes** tabs would be shown. Each tab would display the items of the named type associated with the selected location, including details on those items.

Working with Items in the Management Panel

Selecting One or Multiple Items: To select an item from a list of items in the management panel, click the item. Use Shift+Click to select multiple adjacent list items, or Ctrl+Click to select multiple non-adjacent items.

Column Settings: Click the gear icon to change column settings:

- **Sorting:** To sort data by a column, select either **Sort Ascending** or **Sort Descending**.
- **Column Display:** To change the columns displayed in a table, select **Columns**. Then toggle one or more columns to display.
- **Filter:** To filter a list of items, select **Filters**. Then specify one or more filter criteria to display items matching those criteria.

Refreshing a List: To refresh the data in a list, click **Refresh** in the upper right corner.

Tab Controls

These controls are commonly displayed on all tabs in the management panel:

- **Toolbar Buttons:** Toolbar buttons enable operations related to the items on the tab.
- **Items Table:** Items corresponding to the tab header are displayed in a table. For example, locations are listed in tabular format on the Locations tab.
- **Bulk Operations Buttons:** On most tabs, bulk operations buttons enable you to perform operations on one or more items. Select one or multiple items in the list, then click the button to perform the indicated operation. For example, to delete multiple items such as hosts, select one or more hosts on the **Hosts** tab, then click **Delete**. The selected hosts would be deleted.

In addition, each tab may have controls individual to that item type. For example, the **Connectors** tab includes controls related to the management of connectors (see "[Managing Connectors](#)" on page 141).

The Locations Tab

The **Locations** tab displays all locations defined in Arcsight Management Center. The **Locations** tab includes these buttons:

Add Location	Adds a new location. For more information, see " Adding a Location " on page 95
Delete	Deletes one or more selected locations from ArcMC. For more information, see " Deleting a Location " on page 96

The **Locations** table displays these parameters for each location.

- **Name:** Location name.
- **Number of Hosts:** Number of hosts assigned to the location.
- **Action:** Drop-down includes a control for editing a location. For more information on editing a location, see "[Editing a Location](#)" on page 95.

For more information on managing locations, see "[Locations](#)" on page 95.

The Hosts Tab

The **Hosts** tab displays all hosts associated with the location selected in the navigation tree.

The **Hosts** tab includes these buttons:

Add Host	Adds a host. Available on the Hosts tab when a location is selected in the navigation tree. For more information on adding a host, see " About Adding a Host " on page 97.
Move	Moves selected hosts to a new location. For more information, see " Moving a Host to a Different Location " on page 235
Update Agent	Updates the ArcMC Agent on selected hosts. If the Agent is not currently installed, this button will install the Agent. For more information, see " Updating (or Installing) the ArcMC Agent " on page 111.
Delete	Deletes selected hosts from ArcMC. For more information, see " Deleting a Host " on page 235

The **Hosts** table displays these parameters for each host:

- **Hostname:** Fully qualified domain name (FQDN) or IP address of the host. The hostname must match the hostname in the host's SSL certificate. (If IP address was used to add the host, then the certificate will match the IP address used.)

- **Path:** Path to the host.
- **Agent Version:** Version number of the Arcsight Management Center Agent running on the host.
- **Issues:** Status of any issues associated with the host. Possible indicators include:
 - *None:* No issues are associated with the host.
 - *Internet connection Not Present:* The host is currently not reachable by internet connection. Displayed when ArcMC is not able to connect to the Marketplace for retrieving parser upgrade versions. If the user environment needs a proxy server for an internet connection, [configure the logger.properties file](#). If the user environment is an appliance, save the DNS settings on the **System Admin > Network** page.
 - *Valid Marketplace Certificate Not Found in ArcMC:* Displayed when the Marketplace certificate does not match the one found in ArcMC's trust store.
 - *Host Certificate Mismatch:* The hostname does not match the hostname in the SSL certificate. For instructions on downloading and importing certificates for the host, see ["Downloading and Importing Host Certificates" on page 232](#). If this issue is displayed for the localhost, and the certificate cannot be downloaded, please restart the web service on the localhost.
 - *ArcMC Agent Out of Date:* The host's Agent version cannot be upgraded from the managing ArcMC, or the Arcsight Management Center cannot communicate with the Arcsight Management Center Agent on the managed node. You may need to manually install the ArcMC Agent. For requirements and instructions, see ["Installing the Arcsight Management Center Agent" on page 35](#)
 - *ArcMC Agent Stopped:* The Agent process on the host has been stopped.
 - *ArcMC Agent Upgrade Recommended:* The host's Agent version is older than the one on the managing ArcMC. An Agent upgrade is recommended.
 - *ArcMC Agent Uninstalled:* The Agent on the host has been uninstalled.
 - *ArcMC Agent Down:* The Agent on the host is not running.
 - *Update the authentication credentials on the localhost, then install the ArcMC Agent:* For a localhost added for remote management, [authentication credentials need to be updated](#) to ensure authentication, then the [ArcMC Agent needs to be installed](#) to enable management. Take both of these steps to correct this issue.
 - *Error in REST Authentication:* The Transformation Hub node lacks the ArcMC certificate, ArcMC session ID, or ArcMC URL and port. To resolve this issue:
 - Make sure the user has the permission rights for the Transformation Hub operations.
 - Make sure the valid ArcMC certificate (with FQDN and .crt extension) is present in the Transformation Hub's location: /opt/arcsight/k8s-hostpath-volume/th/arcmccerts

- Make sure that the ArcMC URL is updated with correct FQDN and port in ArcSight Installer > Transformation Hub Configuration > ArcMC_Monitoring field.
- Note that each time the user replaces the ArcMC certificate to the TH's location, the TH's webservice pod has to be restarted for the new certificate to be read and updated in the trust store.
- **Model:** If the host is an appliance, this shows the ArcSight model number of the appliance. If the host is not an appliance, the label *Software* is shown.
- **Type:** Type of installation, either ArcMC Appliance or Software.
- **Version:** Version number of the software on the host.
- **Action:** Drop-down shows controls for executing host management tasks, which include:
 - [Scanning a host](#)
 - [Downloading certificate details](#)
 - [Updating host credentials](#)

For more information on host management, see ["Hosts" on page 96](#).

The Containers Tab

The **Containers** tab displays all containers associated with the item selected in the navigation tree. For example, if you selected a location in the tree, since locations include hosts, the **Containers** tab would display all containers associated with all hosts in the selected location. The **Containers** tab includes these buttons:

Properties	This operation previously performed on this tab, is now performed on the new Bulk Operations page.
Certificates	Manage certificates on selected containers. For more information, see "Managing Certificates on a Container" on page 136 .
FIPS	Enable or disable FIPS on selected containers. For more information, see "Enabling FIPS on a Container" on page 133 .
Upgrade	Upgrades all connectors in selected containers. For more information, see "Upgrading All Connectors in a Container" on page 128 .
Credentials	Manage credentials on selected containers. For more information, see "Changing Container Credentials" on page 127 .

Logs	Manage logs on selected containers. For more information, see " Viewing Container Logs " on page 132.
Restart	Restart all connectors in selected containers. For more information, see " Restarting a Container " on page 131.
Delete	Deletes the selected containers from Arcsight Management Center. For more information, see " Deleting a Container " on page 127.

The **Containers** table includes the following columns:

- **Name:** Name of the container.
- **Path:** Path to the container.
- **Issues:** Status of any issues associated with the container.
- **Port:** Port number through which the container is communicating.
- **Framework Ver:** Framework version number of the container.
- **Parser Ver:** Parser version number of the container.
- **Status:** Status of the container. Possible values for container status are:
 - *Improper configuration: Initial default state.*
 - *Initializing connection:* The connector has a resolvable URL, but Arcsight Management Center has not logged in to the connector yet.
 - *Down:* There was an exception trying to execute the login command.
 - *Unauthorized:* The login command was executed, but login has failed.
 - *Connecting:* The login is in progress.
 - *Connected:* The login was successful.
 - *Empty:* Login successful, but the container doesn't have connectors.
 - *Initialized:* Login successful and the container has connectors.
 - *Unknown:* No information on status. To resolve, manually SSH to the system and restart the container.
- **Last Check:** Date and time of last status check.
- **Action:** Drop-down shows a variety of controls for executing container management tasks, which include:
 - [Edit Container](#)
 - [Send Container Command](#)
 - [Add Connector](#)
 - [Run Logfu](#)

- [Download Certificate](#)
- [Display Certificates](#)
- [Deploy \(to ArcExchange\)](#)
- [Run FlexConnector Wizard](#)

For more information on container management, see ["Upgrading All Connectors in a Container" on page 128](#)

The Connectors Tab

The **Connectors** tab displays all connectors associated with the item selected in the navigation tree. For example, if you selected a container in the navigation tree, the **Connectors** tab would show all connectors in the selected container. For the details on managing connectors, see ["Managing Connectors" on page 141](#).



The Connectors tab will also show any deployed CTHs.

The **Connectors** tab includes these buttons, which perform operations on one or more selected connectors:

Add Connector	(Only shown when a container is selected in the navigation tree.) Adds a connector to the selected container.
Runtime Parameters	Edit the runtime parameters on selected connectors. For more information, see "Editing Connector Parameters" on page 144 .
Destinations	Sets the destinations of selected connectors. For more information, see "Managing Destinations" on page 146 .
Parameters	Sets parameters for selected connectors. For more information, see "Editing Connector Parameters" on page 144 .
Delete	Deletes connectors from ArcSight Management Center. For more information, see "Deleting a Connector" on page 154 .

The **Connectors** table displays the following parameters for each connector:

- **Name:** Name of the connector.
- **Path:** Path to the connector.
- **Group Name:** Name of the group for the connectors and CTHs. For connectors that have not been assigned to any group and older connector types no group name will be displayed.
- **Type:** Type of connector.
- **EPS In:** Events per second received by the connector.
- **EPS Out:** Events per second sent by the connector to its destination.

- **Cache:** Connector cache size. For more information on cache files, see the [Smart Connectors User Guide](#).
- **Last Check:** Date and time of the last status check.
- **Action:** Drop-down shows a variety of controls for executing connector management tasks. These include:
 - [Send Connector Command](#)
 - [Share a connector to ArcExchange](#)
 - [Edit a FlexConnector](#)

For more information on connector management, see "[Managing Connectors](#)" on page 141.

The Connector Summary Tab

To view a single connector in detail, click the connector in the navigation tree. The toolbar on the summary tab includes the following buttons for operations on the connector:

Connector Command	Sends a command to the connector. For more information, see " Sending a Command to a Connector " on page 154.
Remove Connector	Removes the connector. For more information, see " Deleting a Connector " on page 154.
Run Logfu	Run Logfu diagnostics on the connector. For more information, see " Running Logfu on a Connector " on page 155.
Share	Shares the connector through ArcExchange. For more information, see " Sharing Connectors in ArcExchange " on page 158.

Tables below the toolbar show connector specifics, including basic connector data, parameters, and connector destinations. These tables include the following columns:

Connector Data

- **Type:** Type of connector.
- **Status:** Connector status.
- **Input Events (SLC):** Total number of events received by the connector since it was last checked (generally once per minute).
- **Input EPS (SLC):** Events per second received by the connector since it was last checked (generally once per minute).
- In addition, the columns to the right include tools for [editing a connector](#), [editing runtime parameters](#), [adding a failover destination](#), and [sending a destination command](#).

Connector Parameters

Click **Connector Parameters** to toggle display of this table. The **Connector Parameters** table includes:

- Click  to edit parameters.
- **Parameters:** Parameters can include connector network port, IP address , protocol, and other information.
- **Value:** Parameter value.

Table Parameters (WUC Connectors Only)

WUC connectors (only) display these parameters.

- **Domain Name:** Connector domain name.
- **Host Name:** Connector host name.
- **User Name:** Connector user name.
- **Security Logs:** Indicates whether security events are collected.
- **System Logs:** Indicates whether system events are collected.
- **Application:** Indicates whether application events are collected from the Common Application Event Log.
- **Custom Log Names:** List of custom application log names, if any.
- **Microsoft OS Version:** Microsoft operating system for the connector.
- **Locale:** Connector locale.

Destinations

Click **Destinations** to toggle display of this table. The **Destinations** table includes:

- Click  to add additional destinations.
- **Name:** Destination name.
- **Output Events (SLC):** Total number of events output by the connector to the destination since it was last checked (generally once per minute).
- **Output EPS (SLC):** Events per second output by the connector to the destination since it was last checked (generally once per minute).
- **Cached:** Total number of events cached to be transmitted to the destination.
- **Type:** Destination type. Destination types are described in the SmartConnector User's Guide.
- **Location:** Location of the destination.
- **Device Location:** Location of the device on which the destination is located.
- **Comment:** Comments on the destination.

- **Parameters:** Destination-specific parameters, such as IP address , port, and protocol.
- **Action Buttons:** Action buttons enable destination management tasks, such as editing the destination, editing the runtime parameters, adding a new failover destination, sending destination commands and removing the destination.

For more information on managing connectors, see "[Managing Connectors](#)" on page 141.

The ConApps Tab

The **ConApps** tab displays all hardware and software Connector Appliances associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree, the **Connector Appliances** tab would display all Connector Appliances in Arcsight Management Center; if you selected a Location, the tab would display all Connector Appliances in the selected location.

The **Connector Appliances** tab includes the following button, which operates on one or more selected Connector Appliances:

Set Configuration	Sets the configuration for selected Connector Appliances. For more information, see " Setting a Configuration on ConApps " on page 115
--------------------------	--

The **Connector Appliances** table displays these parameters for each Connector Appliance:

- **Name:** Name of the Connector Appliance.
- **Path:** Path to the Connector Appliance.
- **Port:** Port number through which the Connector Appliance is communicating.
- **Version:** Software version of the Connector Appliance.
- **Status:** Status of the Connector Appliance.
- **Last Check:** Date and time of last status check.
- **Action:** Drop-down shows a variety of controls for executing Connector Appliance management tasks, including the following:
 - [Rebooting](#)
 - [Shutting down](#)
 - [Editing or removing a configuration](#)

For more information on Connector Appliance management, see "[Managing Connector Appliances \(ConApps\)](#)" on page 113.

The Loggers Tab

The **Loggers** tab displays all hardware and software Loggers associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree, the **Loggers**

tab would display all Loggers in Arcsight Management Center; while if you selected a Location, you would see all Loggers in that location.

The **Loggers** tab includes the following buttons, which perform operations on one or more selected Loggers:

Set Configuration	Sets the configuration for selected Loggers. For more information, see " Setting a Configuration on Loggers " on page 125.
Upgrade Logger	Upgrades selected Loggers. For more information, see " Upgrading a Logger " on page 122

The **Loggers** table displays these parameters for each Logger:

- **Name:** Name of the Logger.
- **Path:** Path to the Logger.
- **Port:** Port number through which the Logger is communicating.
- **Version:** Software version of the Logger.
- **Top Storage Use:** Displays the most used storage group and its percentage of storage.
- **Status:** Status of the Logger.
- **Last Check:** Date and time of last status check.
- **Action:** Shows controls for executing Logger management tasks, including the following:
 - [Rebooting](#)
 - [Shutting down](#)
 - [Editing or removing a configuration](#)

The ArcMCs Tab

The **ArcMCs** tab displays all Software ArcSight Management Centers and ArcSight Management Center Appliances associated with the item selected in the navigation tree. For example, if you selected **System** in the navigation tree, the **ArcMCs** tab would display all managed ArcSight Management Centers; while if you selected a Location, you would see all ArcMCs in that location.

The **ArcMCs** tab includes the following buttons, which perform operations on one or more selected ArcMCs:

Set Configuration	Sets the configuration for selected ArcMCs. For more information, see " Setting a Configuration on Managed ArcMCs " on page 119
Upgrade ArcMC	Upgrades selected ArcMCs. For more information, see " Upgrading ArcMC " on page 117

The **ArcMCs** table displays these parameters for each ArcMC:

- **Name:** Name of the Arcsight Management Center.
- **Path:** Path to the Arcsight Management Center.
- **Port:** Port number through which the Arcsight Management Center is communicating.
- **Version:** Software version of the Arcsight Management Center.
- **Status:** Status of the Arcsight Management Center.
- **Last Check:** Date and time of last status check.
- **Action:** Shows controls for executing ArcMC management tasks, including the following:
 - [Rebooting](#)
 - [Shutting Down](#)
 - [Editing a configuration](#)

For more information on managing other ArcSight Management Centers in Arcsight Management Center, see ["Managing Other ArcSight Management Centers" on page 115](#).

The TH Nodes Tab

ArcMC can only manage a single Transformation Hub. However, the single managed Transformation Hub may have any number of Transformation Hub nodes, each of which can be managed and monitored by ArcMC. When you add a Transformation Hub as a host to ArcMC, you add all of its nodes.

The **TH Nodes** tab displays all Transformation Hub nodes present in the managed Transformation Hub. For example, if you selected **System** in the navigation tree, the **TH Nodes** tab would display all managed Transformation Hub nodes; while if you selected a location, you would see all Transformation Hub nodes in that location.

The tab displays these parameters for each managed Transformation Hub node:

- **Name:** Name of the Transformation Hub node.
- **Port:** Port number through which the Transformation Hub node is communicating.
- **Type:** Type of Transformation Hub node.
- **Last Check:** Date and time of last status check.

For more information on managing Transformation Hub in Arcsight Management Center, see ["Managing Transformation Hub" on page 215](#).

The Collectors Tab

The **Collectors** tab displays all Collectors associated with the item selected in the navigation tree. For example, if you selected a container in the navigation tree, the **Collectors** tab would show all Collectors in the selected container.

The **Collectors** table displays the following parameters for each connector:

- **Name:** Name of the Collector.
- **Port:** Collector port.
- **Type:** Type of Collector.
- **Syslog Lines Received:** Events Received.
- **Custom Filtering:** Messages filtered out.
- **Status:** Collector status.
- **Last Check:** Date and time of the last status check.

For the details on managing Collectors, see ["Bulk Operations" on page 222](#).

Locations

A *location* is a logical grouping of hosts. The grouping can be based on any criteria you choose, such as geographical placement or organizational ownership. Locations are a useful way to organize a set of hosts.

For example, you could group all hosts in New York separately from hosts in San Francisco and assign them to locations named “New York” and “San Francisco”. Similarly, you could group hosts in a location named “Sales” and others in the location “Marketing”.

A location can contain **any number** of hosts. For information on adding hosts to locations, see ["About Adding a Host" on page 97](#).



Note: Arcsight Management Center includes one location by default (called *Default*) but you may add any number of locations. The name of the Default location may be edited, and the location itself may be deleted.

Adding a Location

You can add any number of locations.

To add a location:

1. Click **Configuration Management > Bulk Operations**.
2. In the navigation tree, click **System** and click the **Location** tab.
3. Click **Add**.
4. Specify the name of the new location, and click **Save**.

Editing a Location

You can edit the name of a location.

To edit a location:

1. Click **Configuration Management > Bulk Operations**.
2. In the navigation tree, click **System**, then click the **Location** tab.
3. On the **Locations** tab, choose a location to rename.
4. Click **Edit**.
5. Specify the new name of the location, and click **Save**. The location is renamed.

Viewing All Locations

You can see all the locations that exist in Arcsight Management Center.

To view all locations:

1. Click **Node Management**.
2. In the navigation tree, click **System**, then click the **Locations** tab to view all locations.

Deleting a Location

When you delete a location from Arcsight Management Center, any hosts in the location (and their associated nodes) are also deleted.



Tip: If you want to delete a location but still want to keep its hosts in Arcsight Management Center, relocate the hosts before deleting the location. See "["Moving a Host to a Different Location" on page 235](#).

To delete a location:

1. Click **Configuration Management > Bulk Operations**.
2. In the navigation tree, click **System**, then click the **Location** tab.
3. On the **Location** tab, choose one or more locations to delete.
4. Click **Delete**.
5. Click **Yes** to confirm deletion. The selected locations are deleted.

Hosts

A *host* is a networked system associated with a unique IP address or hostname. A host can be an ArcSight appliance, or a system running an ArcSight software product, such as Software Logger.

For information on adding hosts to manage, see "[About Adding a Host](#)" below.

About Adding a Host

After a host is added to Arcsight Management Center, ArcSight products on the host becomes *nodes*, and can be managed. For example, adding a host running Connector Appliance with 4 containers would add 5 nodes to Arcsight Management Center: the Connector Appliance itself, and each container.



Note: In ArcMC 2.2 and later, the ArcMC localhost is added automatically for remote management. You will be able to [manage the localhost as you would any other node](#).

Prerequisites for Adding a Host (for each Host Type)

Connection Information for Adding a Host

Host Type	Required Information
Appliance with Local Connectors (includes ArcSight Management Center Appliance, Connector Appliance, or Logger Appliance (L3XXX))	<ul style="list-style-type: none"> Hostname (FQDN) or IP address . Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. (If the FQDN fails to resolve, restart the web service.) Authentication credentials (username and password) for logging into the host. If the host is configured for external authentication, such as LDAP or RADIUS, use the external authentication credentials, if possible, or use the fall back credentials. <p>Note: See "Node Authentication Credentials" on page 100 for more information about authentication credentials.</p>
	<ul style="list-style-type: none"> Authentication credentials (username and password) for any local containers. If the appliance includes multiple containers, then the credentials for each container must be identical. For example, if the username and password for one container managed by a Connector Appliance is <i>myusername</i> and <i>mypassword</i>, then <i>myusername</i> and <i>mypassword</i> must be the credentials for all local containers managed by the same Connector Appliance.
Appliance without Local Connectors (includes Logger Appliance (non-L3XXX))	<ul style="list-style-type: none"> Hostname (FQDN) or IP address . Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. (If the FQDN fails to resolve, restart the web service.) Authentication credentials (username and password) for logging into the host. If the host is configured for external authentication, such as LDAP or RADIUS, use the external authentication credentials, if possible, or use the fall back credentials. <p>Note: See "Node Authentication Credentials" on page 100 for more information about authentication credentials.</p>

Connection Information for Adding a Host, continued

Host Type	Required Information
Software Form Factor (includes Software ArcSight Management Center, Software Connector Appliance, or Software Logger)	<ul style="list-style-type: none"> Hostname (FQDN) or IP address. Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. (If the FQDN fails to resolve, restart the web service.) Authentication credentials (username and password) for logging into the host. If the host is configured for external authentication, such as LDAP or RADIUS, use the external authentication credentials if possible, or use the fall back credentials. <p>Note: See "Node Authentication Credentials" on page 100 for more information about authentication credentials.</p> <ul style="list-style-type: none"> Port number assigned to the product.
Connector (includes SmartConnectors of all types)	<ul style="list-style-type: none"> Hostname (FQDN) or IP address. Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. (If the FQDN fails to resolve, restart the web service.) Authentication credentials (username and password) for the connector. <p>Note: See "Node Authentication Credentials" on page 100 for more information about authentication credentials.</p> <ul style="list-style-type: none"> Optionally, specify an inclusive port range separated by a hyphen (such as 9004-9008) to scan a port range for all connectors. <p>Note: If the port range includes multiple connectors, then the credentials for each connector in the range must be identical. For example, if the username and password for one connector in the range was <i>myusername</i> and <i>mypassword</i>, then <i>myusername</i> and <i>mypassword</i> must be the credentials for every connector in the port range.</p> <p>Note: Prior to adding a software-based SmartConnector as a host, you must prepare the Smart Connector as explained in SmartConnectors on ArcMC.</p>

Connection Information for Adding a Host, continued

Host Type	Required Information
Collector	<ul style="list-style-type: none"> Hostname (FQDN) or IP address . Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. (If the FQDN fails to resolve, restart the web service.) Authentication credentials (username and password) for the Collector. <p>Note: See "Node Authentication Credentials" on the next page for more information about authentication credentials.</p> <ul style="list-style-type: none"> Optionally, specify an inclusive port range separated by a hyphen (such as 48080-48088) to scan a port range for all Collectors. <p>Note: If the port range includes multiple Collectors, then the credentials for each Collector in the range must be identical. For example, if the username and password for one connector in the range was <i>myusername</i> and <i>mypassword</i>, then <i>myusername</i> and <i>mypassword</i> must be the credentials for every Collector in the port range.</p>
Transformation Hub - Non-Containerized Deployment	<ul style="list-style-type: none"> Hostname (FQDN) or IP address. Hostname or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. (If the FQDN fails to resolve, restart the web service.) Port number for the Transformation Hub (default 32080) In order to add Transformation Hub as a host, the active user must belong to an ArcMC permission group with rights to do so. By default, the admin user has such rights. <p>Note: Prior to performing the Add Host process, you need to generate the ArcMC certificate with complete FQDN and download the .crt file, then copy the certificate file to your Kubernetes master node. See Preparing to Add Transformation Hub as a Host for details on this process.</p>
Transformation Hub - Container Deployment Foundation (CDF)	<ul style="list-style-type: none"> Virtual FQDN or Virtual IP (VIP) address. VIP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for a VIP address. (If the FQDN fails to resolve, restart the web service.) Port number for the Transformation Hub (default 32080) The following Kubernetes cluster parameters: <ul style="list-style-type: none"> Cluster Port (default 443) Cluster Username and Password Contents of the certificate file. For more details, see here. In order to add Transformation Hub as a host, the active user must belong to an ArcMC permission group with rights to do so. By default, the admin user has such rights.

- An SSL Certificate:** An SSL certificate must be generated for any of the following host types to be managed:
 - Connector Appliance or Software Connector Appliance
 - Logger Appliance or Software Logger
 - Transformation Hub (any version)
 - ArcSight Management Center Appliance or Software ArcSight Management Center

The hostname in the certificate must match the hostname you are adding to Arcsight Management Center. For more information on generating certificates for these host types, consult the ArcSight Administrator's Guide for each product. (If a host to be added already has a certificate installed, you can use the existing certificate, as long as the hostname on the certificate matches the hostname of the host you are adding.)



Note: If the hostname does not match the hostname in the SSL certificate, you can regenerate a matching certificate by doing one of the following:

- For a hardware appliance, in **System Admin > Network**, click the **NICS** tab. Under **Host Settings**, note the entry in the Hostname field. (This is the value you should use to add the host to Arcsight Management Center.) Click **Restart Network Service**. Then, in the navigation menu, under **Security**, pick **SSL Server Certificate**. Click **Generate Certificate**. A new certificate will be generated that matches the hostname from the **NICS** tab.
- For software form factor, in **System Admin > SSL Server Certificate**, under **Enter Certificate Settings**, verify that the hostname from the NICS tab noted previously is entered in the **Hostname** field. Then, click **Generate Certificate**. A new certificate will be generated that matches the hostname from the **NICS** tab.

- **Check for Agent Installation:** Check the table under "[Installing the Arcsight Management Center Agent](#)" on page 35 to determine if the ArcMC Agent needs to be installed on a host prior to adding it to ArcMC. For some host types, the Agent will be installed automatically upon adding a host.



Note: Perl is required for the automatic installation of the ArcMC Agent. Ensure that Perl is installed on the host prior to attempting to add the host to ArcMC.

Node Authentication Credentials

ArcSight Management Center authenticates to each managed node each time it communicates with the node, using the node's authentication credentials—that is, username and password—you supply when first adding the host. If the host includes connectors or containers, then authentication credentials must also be supplied for these as well. (Exception: Transformation Hub does not require authentication credentials for individual nodes.) As a result, valid credentials for each node are required when adding a host.

Determining a Node's Credentials:

Consult the system administrator for each managed node to determine its current login credentials. Each ArcSight product ships with a default set of credentials. However, for optimal security, it is expected that the default credentials are changed as soon as possible by the administrator, so the default credentials may no longer be valid for authentication.

- For default credentials for ArcSight products, consult the relevant product administrator's guide. (For SmartConnector default credentials, consult the SmartConnector User's Guide, available from the [Micro Focus Community](#).)
- Some products can be configured by administrators to use external authentication, in which case the external authentication credentials or fallback credentials should be provided when adding the host to Arcsight Management Center. (SmartConnectors may not be configured for external authentication.)

Changed or Expired Credentials

If the username or password on a node are changed (or expire) any time after the node is added to ArcSight Management Center, then the node will no longer be managed. However, it will still appear in the list of managed nodes. For example, on some hosts, passwords are set to expire automatically after some time period, which would prevent successful authentication by Arcsight Management Center using the node's initial credentials. To avoid this issue, you may wish to use node credentials that do not expire. To continue management of node on which the credentials have changed or expired, use the [Update Host Credentials](#) feature.

Dynamic Credentials

If authentication credentials are configured to change dynamically (such as with RADIUS one-time passwords), then instead of providing external authentication credentials, you can provide the credentials of a local user on the managed node who is permitted to use fallback authentication. Arcsight Management Center will then try to authenticate to the managed node using the external authentication method first, and if this fails, it will try to authenticate to the managed node using the local user credentials.

Managing SmartConnectors on ArcMC

ArcMC can remotely manage previously-installed, software-based SmartConnectors; however, the remote management feature is disabled on software SmartConnectors by default.

You can install several SmartConnectors on a single host if supported by the hardware. ArcSight certifies a maximum of 4 SmartConnectors on Windows hosts and 8 on Linux hosts.

To manage software-based SmartConnectors with , you need to enable remote management on each connector, as follows:

1. In a text editor, in the installation directory for the SmartConnector, open the file /<install_dir>/user/agent/agent.properties .
2. Add the line: remote.management.enabled=true

3. If desired, customize the connector's listening port. The default is 9001. To change this value, add the line: `remote.management.listener.port=<port_number>`, where `<port_number>` is the new port number.
4. Save the file.
5. Restart the SmartConnector for changes to take effect.

Adding a Host

Before adding a host, ensure that you have the required information for the host on hand. For more information, see "[Prerequisites for Adding a Host \(for each Host Type\)" on page 97](#).

To add a host to ArcMC:

1. Click **Node Management**.
2. In the navigation tree, select a location to which you plan to add the host.
3. On the **Hosts** tab, click **Add Host**.
4. On the **Add a new Host** dialog, in **Hostname/IP**, specify either the hostname or IP address of the host.
5. In **Type**, select the type of node from the drop-down list.
6. Specify values for the required settings. (See [About Adding a Host](#) for the specific information required, based on the different type of nodes.)
 - In **Host Credentials** or **Connector Credentials**, specify the username and password required for authentication.
 - In **Port**, if required, specify the value of the port on which Arcsight Management Center will connect to the host.
7. Click **Add**. The host is added to Arcsight Management Center.



Note: You can quickly deploy a Connector or Collector directly to a host in the ArcMC Deployment View. For more information, see "[Instant Connector Deployment" on page 73](#).

Adding a Host with Containers

When you add a host that includes containers (such as Connector Appliance), Arcsight Management Center also attempts to retrieve the SSL certificates from any containers that reside on the host, and add each container as a separate node. Containers on the remote host can be managed only if Arcsight Management Center can authenticate using the certificates and supplied credentials. When the certificates are retrieved, you are prompted to import them into Arcsight Management Center.



Note: On Arcsight Management Center Appliance, all local containers are added automatically as hosts of type Software Connector.

Adding Transformation Hub as a Host to ArcMC

Before adding Transformation Hub as a host, ensure that you have the required information for the host on hand. For more information, see "[Preparing to Add Transformation Hub as a Host \(Standalone ArcMC\)](#)" below.

Preparing to Add Transformation Hub as a Host (Standalone ArcMC)

In order to add Transformation Hub as a managed host, you will need to generate the ArcMC certificate with complete FQDN and copy it to the ArcMC monitoring tab of the ArcSight installer.

To prepare for adding Transformation Hub as a host:

1. In ArcMC, click **Administration > System Admin**.
2. Under **Security > SSL Server Certificate**, under Hostname, specify the FQDN of the ArcMC.
3. Click **Generate Certificate**.
4. Once the certificate is generated, click **View Certificate** and copy the full content from -- BEGIN cert to END cert--
5. Access the ITOM Management Portal: <https://<TH-VIP>:5443>
6. From the left menu click **Suite > Management**.
7. Click the three dots on the right > **Reconfigure**.
8. Scroll down to **Management Center Configuration**.
9. Type the ArcMC username in the **Transformation Hub Administrator Username** field.
10. Type the ArcMC password in the **Transformation Hub Administrator Password** field.
11. Add the FQDN and port number in the **Management Center Host Names and Ports Managing This Cluster** field.
12. Paste the previously generated certificate from the ArcMC View Server Certificate page into the **Management Center Certificates** field and click **Save**.

In ArcMC, you can now follow the process outlined under [Adding Transformation Hub 3.1 as a Host](#).

Adding Transformation Hub as a Host

To add Transformation Hub as a managed host:

1. SSH to the Transformation Hub and navigate to: /opt/arcsight/kubernetes/scripts
 2. Generate the certificate by running the script: ./cdf-updateRE.sh
- Caution:** Review the Transformation Hub's Administrator's Guide to confirm if there are any changes in the script.
3. Copy the certificate (be sure to include from ----- BEGIN CERT to END CERT -----)
 4. Login to ArcMC
 5. Navigate to **Node Management > View All Nodes**.
 6. From the left navigation tree, select the location where you want to add the TH.
 7. Click **Add Host**.
 8. In the **Hostname/IP** field, type the IP address or hostname for the Virtual IP for an HA environment or master node for a single-master node environment.
 9. In the **Type** dropdown field, select **Transformation Hub - Containerized Deployment**.
 10. In the **Cluster Port** field, type the corresponding port (443 for TH 3.0 or later).
 11. In the **Cluster Username** field, type the Installer UI username.
 12. In the **Cluster Password** field, type the Installer UI password.
 13. Paste the Transformation Hub's certificate in the **Cluster Certificate** field.
 14. Click **Add**.

Adding Transformation Hub Non-Containerized (THNC) as a Host

To add THNC as a managed host:

In the THNC server:

1. During the THNC setup script, add the arcmc host when the option is prompted. For example: hostname:443.
2. Get a copy of the ArcMC server certificate, with the extension *.crt from the system where ArcMC is running.
3. Copy the ArcMC certificate file and paste it on /opt/arcsight/th/current/cert/webservice/ directory.
4. Restart the THNC services.

In ArcMC:

1. Go to **Node Management > View All nodes**
2. From the left navigation tree, select the location where you want to add the THNC.
3. Click **Add Host**.
4. In the **Hostname/IP** field, type the fully qualified name of the THNC.
5. In the **Type** field, select **Transformation Hub - Non-Containerized Deployment**.
6. In the **Port** field, type 8080 and click **Add**.

Importing Multiple Hosts

To quickly and easily add multiple hosts in bulk, you can import a comma-separated values (CSV) file that lists the names and required attributes of the hosts to be added.



Note: Arcsight Management Center 1.0 used a slightly different file format for importing connector hosts. That file format is not supported by Arcsight Management Center 2.1. Use the file format described here instead.

Prerequisites for Importing Multiple Hosts

The following prerequisites apply to importing hosts.

- **Add Host Prerequisites:** Any prerequisites for the Add Host process also apply to importing multiple hosts by a CSV file. See "["Prerequisites for Adding a Host \(for each Host Type\)" on page 97](#)".
- **Valid CSV File:** Ensure the values in your CSV file are valid and correct. An import hosts job will fail immediately upon receiving an invalid or incorrect value. The CSV file format is described under "["CSV File Format"](#) below.
- **Stop the Agent 1.0 Process:** In addition, if any of the hosts to be imported are running the Arcsight Management Center 1.0 Agent, stop the Agent process on each such host before the import. (This is not needed for later versions of the ArcMC Agent.)

CSV File Format

The CSV (comma-separated value) file requires the following header line to be its first line:

```
location,hostname,type,host username,host password,connector  
username,connector password,connector container name,port/port range,collector  
username,collector password, collector port/port range
```

Each subsequent line represents one host to be imported. Each line must include values for the following comma-separated fields for each host:

```
<Location>, <Hostname>, <Host Type>, <Host Username>, <Host Password>, <Connector Username>, <Connector Password>, <Connector Container Name>, <Port/Port Range>, <Collector Username>, <Collector Password>, <Collector Port/Port Range>
```



Note: The column connector container name (for instances in which users edit a container) has been added to the CSV file when importing or exporting hosts. If users don't want to import the values of this field, they can leave it blank. This applies for ArcMC versions 2.9.4 and later.

Collector port information will be exported as a single port. If more than one port is present, they will be exported individually. For example:

```
Default,example.com,Collector,,,,,collector,,48098
Default,example.com,Collector,,,,,collector,,48099
```

For importing hosts, users can import the Collector port information in a range or individually. For example:

```
Default,example.com,Collector,,,,,collector,,2001
Default,example.com,Collector,,,,,collector,,2002
```

```
Default,example.com,Collector,,,,,collector,,2001-2002
```

Some host types require values for all fields, and some are optional. An optional field with no value specified must still include a comma to represent the empty field.



Note: Only US ASCII characters are supported for import.

Host Field Values

Valid values for host fields are detailed in the following table. An asterisk (*) indicates a required field. An optional field with no value specified must still include a comma to represent the empty field.

Field	Description
Location*	Location to which the host will be assigned.
Hostname*	Hostname (FQDN) or IP address of the host. <ul style="list-style-type: none"> • FQDN or IP must be resolvable by ArcSight Management Center: either through DNS for a hostname, or directly for an IP address. • If hostname is used, the hostname entered must match the hostname from the host's SSL certificate. • For a hardware appliance, DNS must be configured on the managing appliance (System Admin > DNS).

Field	Description
Host Type*	<p>Host type. Valid (case-insensitive) values are:</p> <ul style="list-style-type: none"> • <code>appliance_with_local_connectors</code>: includes ArcSight Management Center Appliance, Connector Appliance and Logger Appliance (L3XXX) • <code>appliance_without_local_connectors</code>: includes Logger Appliance (non-L3XXX). • <code>software_form_factor</code>: includes Software ArcSight Management Center, Software Connector Appliance or Software Logger. • <code>software_connector</code>: includes all connectors and Collectors. • <code>Collector_software_connector</code>: indicates that connector and Collector reside on the same host. • <code>Collector</code>: includes all Collectors.
Host Username/Password*	<p>User name and password used to authenticate to the host.</p> <p>Note: See "Node Authentication Credentials" on page 100 for more information about authentication credentials.</p>
Connector Username/Password	<p>Username and password used to authenticate to the connector. Required for hosts of type Appliance with Local Connector and Software Connector; otherwise optional.</p> <p>Note: See "Node Authentication Credentials" on page 100 for more information about authentication credentials.</p>
Connector Container Name	<p>Name of the container.</p> <p>For example: Syslog Container or SmartConnector Container.</p>

Field	Description
Port/Port Range	<p>Starting port or port range for connector scan. Valid values:</p> <ul style="list-style-type: none"> • Port number • Port range • Comma-separated port numbers (for example, 9000,9004,9007) <p>Notes:</p> <ul style="list-style-type: none"> • <i>For software form factors</i>, port is required. • <i>For appliance form factors</i>, to add all local containers, leave the field blank. However, if any port numbers are entered, then certificates will be downloaded only for the specified port numbers, and only those containers will be imported. • <i>For connectors</i>, either a port or port range is required. If using port range, specify an inclusive port range, using a hyphen between starting and ending port. For example, a specified port range of 9001-9003 would scan ports 9001, 9002, and 9003. <p>Note: If the port range includes multiple connectors, then the credentials for each connector in the range must be identical. For example, if the username and password for one connector in the range was <i>myusername</i> and <i>mypassword</i>, then <i>myusername</i> and <i>mypassword</i> must be the credentials for every connector in the port range.</p>
Collector Username/Password	<p>Username and password used to authenticate to the Collector.</p> <p>Note: See "Node Authentication Credentials" on page 100 for more information about authentication credentials.</p>
Port/Port Range	<p>Port or port range for Collector scan. Valid values:</p> <ul style="list-style-type: none"> • Port number • Port range • Comma-separated port numbers (for example, 9000,9004,9007)

An example of a valid import file, importing two hosts, is shown here:

```
location,hostname,type,host_username,password1,connector_
username,password2,port/port range,username,password3,port/port range
```

```
CorpHQ,hostname.example.com,software_connector,username,password,connector_
username,connector_password,9001-9005,collector_username,collector_
password,9006
```

```
EMEA,hostname2.example.com,appliance_without_local_connectors,
logger_user,logger_pword,,,,,
```

In this example, the first line would represent the required header line, the second line a Software Connector, and the third line would represent a Logger Appliance.

Import Hosts Procedure

Only a single Import Hosts job may be executed at one time.



Note: Importing Transformation Hub host in ArcMC is not supported. Please add Transformation Hub host to ArcMC through the "[Adding a Host](#)" on page 102 process.

To import hosts from a CSV file:



Note: Before beginning the import, stop the Agent processes on any hosts running version 1.0 of the ArcMC Agent.

1. Create and save your CSV file in a text editor.
2. Log into Arcsight Management Center.
3. Select **Node Management > Import Hosts**. The Import Hosts wizard starts.
4. Click **Browse**, and browse to the location of your hosts CSV file.
5. Click **Import**. The hosts are imported as a background job.

If the CSV file is valid, connector certificates are retrieved automatically so that Arcsight Management Center can communicate with each connector in a container. The Upload CSV wizard lists the certificates. (To see certificate details, hover over the certificate.).

Automatic installation of the ArcMC Agent may increase the time required for the Import Hosts job.

- Select **Import the certificates...**, then click **Next** to import the certificates and continue.
- Select **Do not import the certificates...**, then click **Next** if you do not want to import the certificates. The Upload CSV wizard does not complete the upload CSV process.



Note: The Import Hosts wizard does not complete the upload if certificate upload failed for any of the connectors in a container, or if any of the certificates failed to import into the trust store.

1. The Import Hosts job executes.

Import Hosts Job Logs

Arcsight Management Center logs the results of all Import Hosts jobs. Each job produces a new log, named `import_hosts_<date>_<time>.txt`, where `<date>` and `<time>` are the date and time of the import hosts job.

- For Software ArcSight Management Center, logs are located in the directory <install_dir>/userdata/logs/arcmc/importhosts.
- For ArcSight Management Center Appliance, logs are located in the directory opt/arcsight/userdata/logs/arcmc/importhosts.

Log Format

Each entry in the log will show the success or failure of each host import attempt, in the following format:

```
<User initiating job>, <CSV filename>, <Time of import host job start>, <Hostname>, <Success/failure result>
```

For example:

```
admin, my_csv_file.csv, Tue Apr 08 14:16:58 PDT 2015, host.example.com, Host added successfully
```

If the import hosts job has failed due to one or more invalid entries in the CSV file, the result file will show the parsing error details with the line number and error.

For example:

```
Line [1] has [connector password] field empty. [connector password] field is required for this host type.
```

Exporting Hosts

Exporting hosts from an Arcsight Management Center will create a CSV list of hosts managed by that Arcsight Management Center. (Password information is not included in this file.)

After adding passwords for each host to the file, you can then import this list of hosts into another Arcsight Management Center, using the Import Hosts feature described under ["Importing Multiple Hosts" on page 105](#)

Exporting hosts is most useful when you are reassigning management of hosts from one ArcMC to another.

For example, consider two ArcSight Management Centers, called ArcMC East and ArcMC West. ArcMC East currently manages 50 hosts. However, you are consolidating management of all hosts to the new ArcMC West. To do this quickly and easily, you would export the hosts from ArcMC East into a CSV file. Then, you would add an additional entry for ArcMC East to the CSV file.

After adding in password data for each host, you would import the resulting CSV file into ArcMC West. At the end of the process, all of ArcMC East's hosts, and ArcMC East itself, would be managed by ArcMC West.

To export hosts in Arcsight Management Center:

1. Select **Node Management > Export Hosts**.
2. All hosts managed by the Arcsight Management Center are exported to the local CSV file (`exporthosts.csv`).
3. Optionally, open the file in a CSV editor. Add the password information for each host to the CSV file, then save the file.

Viewing All Hosts

You can see all the hosts managed by Arcsight Management Center, or view hosts by location.

To view all hosts:

1. Click **Node Management**.
2. In the navigation tree, click **System**. (To view by location, click the location you wish to view.)
3. Click the **Hosts** tab. All managed hosts are displayed.

Viewing Managed Nodes on a Host

You can view all the managed nodes on a host, by host type.

To view managed nodes on a host:

1. Click **Node Management**.
2. In the navigation tree, click the location to which the host is assigned. Then, click the host.
3. Click the appropriate tab to view the node types for the managed host: **Containers**, **Connectors**, **Connector Appliances**, **Loggers**, or **ArcMCs**.

Updating (or Installing) the ArcMC Agent

Hosts running an outdated version of the Arcsight Management Center Agent can be quickly upgraded to the latest version.

Agent installation or upgrade is supported on all versions of ArcMC Appliance, Connector Appliance (hardware) and Logger Appliance, Software Logger 6.0 or later, and software ArcMC 2.1 or later.



Tip: Check the version of the Agent on each host by clicking the **Hosts** tab and reviewing the **Agent Version** column.

To upgrade or install the Agent on one or more hosts:

1. Click **Node Management**.
2. In the navigation tree, click **System**, then click the **Hosts** tab.
3. Select one or more hosts to update.
4. Click **Update Agent**. The Agent Upgrade wizard launches. Follow the prompts to complete the Agent Upgrade wizard.

Regenerating your Marketplace Certificate

On rare occasions, you may need to regenerate ArcMC's certificate with the ArcSight Marketplace. This can sometimes be displayed as a "Host Certificate Mismatch" error.

To regenerate your Marketplace certificate in ArcMC:

1. Delete the existing marketplace certificate in ArcMC.

For software form factor:

```
rm -rf <install_dir>/current/arcsight/arcmc/config/certs/marketplace.microfocus.com
```

For ArcMC appliance:

```
rm -rf /opt/arcsight/arcmc/config/certs/marketplace.microfocus.com
```

2. Download the new Marketplace certificate in your browser. Browse to the Marketplace website (<https://marketplace.microfocus.com/arcsight>). A security exception will be noted.
3. Click **More Information**, then click **View Certificate**



Note: The exact procedure for downloading the certificate will depend on your browser. The procedure given here applies to Firefox. Consult your browser documentation for exact steps.

4. On the **Details** tab, click **Export**, and save the certificate as X.509 Certificate (PEM).
5. Save the downloaded certificate at the following location:

For software form factor:

```
<install_dir>/current/arcsight/arcmc/config/certs
```

For ArcMC appliance:

```
/opt/arcsight/arcmc/config/certs
```

6. Restart the ArcMC web service.

Chapter 6: Managing ArcSight Products

ArcSight Management Center enables management tasks on a variety of ArcSight products, including the following:

- Hardware and Software Connector Appliances
- Hardware and Software Arcsight Management Centers
- Hardware and Software Loggers
- Containers
- Software connectors
- Transformation Hub

This chapter discusses the remote management of these products.

Managing Connector Appliances (ConApps)

You can perform any of the following management tasks on managed Connector Appliances or Software Connector Appliances using Arcsight Management Center:

- [Reboot](#) or [shut down](#).
- [Edit or remove a configuration](#).
- [Set a configuration on one \(or multiple\) Connector Appliances](#).



Note: Not all Connector Appliance functionality is manageable through Arcsight Management Center. For a complete discussion of Connector Appliance features, see the Connector Appliance Administrator's Guide.

Rebooting a ConApp

To remotely reboot a managed Connector Appliance:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ConApps**.
4. In the list of Connector Appliances, locate the Connector Appliance to be rebooted.
5. In the **Action** drop-down of the Connector Appliance, select **Reboot ConApp**.
6. Click **Next** to confirm reboot.
7. The Connector Appliance is rebooted. Click **Done**.

Shutting Down a ConApp

To remotely reboot a managed Connector Appliance:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ConApps**.
4. In the list of Connector Appliances, locate the Connector Appliance to be shut down.
5. In the **Action** drop-down of the Connector Appliance, select **Shutdown ConApp**.
6. Click **Next** to confirm shutdown.
7. The Connector Appliance is shut down. Click **Done**.

Editing or Removing a Configuration for a ConApp

You can edit a configuration on, or remove property values of a list configuration from, a managed Connector Appliance.

Editing or removing a configuration will overwrite the node's current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on Connector Appliance:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ConApps**.
4. In the list of Connector Appliances, locate the desired Connector Appliance.
5. In the **Action** drop-down of the Connector Appliance, select **Edit/Remove Config**. The Update Configurations wizard is launched.
6. Review the dialog box, and click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.



Note: In order to edit a backup configuration on a Connector Appliance node, the node must have a scheduled backup to begin with.

Setting a Configuration on ConApps

You can set a configuration on one or multiple Connector Appliances using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple Connector Appliances. Only new values will be appended. For more information on list configurations, see "[List Configurations](#)" on page 173.
- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple Connector Appliances.



Caution: Setting a configuration on one or multiple Connector Appliances may make each Connector Appliance node non-compliant with its current subscriptions.

To set a configuration on one or more Connector Appliances:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Connector Appliances**.
4. In the list of Connector Appliances, select one or more Connector Appliances.
5. Click **Set Configuration**. The Set Configuration wizard is launched.
6. Review the dialog box, then click **Next**.
7. Follow the prompts to complete the wizard.
 - Click **Add Row** to add a new Property to a list configuration, then specify values as needed.
8. The configuration is set on the selected Connector Appliances. Click **Done**.

Managing Other ArcSight Management Centers

You can perform any of the following management tasks on managed Software ArcSight Management Centers or Arcsight Management Center Appliances:

- [Reboot](#) or [shut down](#).
- [Edit or remove a configuration](#).
- [Remotely upgrade an ArcSight Management Center](#).
- [Set a configuration on one \(or multiple\) ArcSight Management Centers](#).

Rebooting an ArcMC

To remotely reboot a managed ArcSight Management Center:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, locate the ArcSight Management Center to be rebooted.
5. In the **Action** drop-down of the ArcMC, select **Reboot ArcMC**
6. Click **Next** to confirm reboot.
7. The ArcSight Management Center is rebooted. Click **Done**.

Shutting Down an ArcMC

To remotely shut down a managed ArcSight Management Center:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, locate the ArcSight Management Center to be shut down.
5. In the **Action** drop-down of the ArcMC, select **Shutdown ArcMC**.
6. Click **Next** to confirm shutdown.
7. The ArcSight Management Center is shut down. Click **Done**.

Editing or Removing a Configuration for ArcMC

You can edit a configuration on, or remove property values of a list configuration from, a managed ArcSight Management Center.

Editing or removing a configuration will overwrite the node's current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on ArcSight Management Center:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcSight Management Centers, locate the desired ArcSight Management Center.
5. In the **Action** drop-down, select **Edit/Remove Config**. The Update Configurations wizard is launched.
6. Review the dialog box, then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.



Note: In order to edit a backup configuration on an ArcMC node, the node must have a scheduled backup to begin with.

Upgrading ArcMC



Note: Prior to upgrading a production (PROD) system, make sure to have a Backout Plan to minimize PROD down time. This plan will be how to restore an ArcMC to its working state prior to the Upgrade. See Appendix E: Restoring Factory Settings if using an Appliance. See Chapter 9: Managing Backups and Restores for restoring the working Configuration Backup. If there are any unexpected issues during or after the Upgrade, implement the Backout Plan. Restore the Configuration Backup of PROD in to a Staging Environment (STAGE). Test the upgrade in the STAGE environment to troubleshoot further.

Remote upgrades from ArcMC 2.9.2 to ArcMC 2.9.3 require a hot-fix to be applied, this hot-fix file that needs to be uploaded depends on the form factor, as follows:

Form Factor	Upgrade File Name	Comments
Appliance	arcmc-2190.enc	This file needs to be uploaded before remotely upgrading an ArcMC appliance from version 2.9.2 to 2.9.3
Software	arcmc-sw-2190-remote.enc	This file needs to be uploaded before remotely upgrading an ArcMC software from version 2.9.2 to 2.9.3



Note: The upgrade file name must not be changed.

To upload the file from the master ArcMC:

1. Download the hotfix file and store it in a secure network location. The file name should always be “arcmc-2190.enc” or “arcmc-sw-2190-remote.enc” depending on the form factor.
2. Click **Administration > Repositories**.
3. Select **Upgrade Files** from the navigation tree.
4. In the management panel, click **Upload**.
5. Click **Choose File** and browse to your hot fix file, then click **Submit**. The file is now uploaded.
6. Continue with the normal procedure outlined in the "[Remote Upgrade Using Node Management](#)" below

In ArcMC, you can remotely upgrade any of the following managed ArcMC types and versions.

Form Factor	Upgrade File Name	Can Upgrade From...	Can Upgrade To...	Comments
Appliance	arcmc-<build number>.enc	ArcMC version 2.0 or later	Any later ArcMC version.	
Software	arcmc-sw-<build number>-remote.enc	ArcMC version 2.1	Any later ArcMC version.	Remote operating system upgrade is not supported for software ArcMC, and, if required, must be performed manually.

Remote Upgrade Using Node Management

Remote upgrade first requires that you upload the appropriate file to your ArcMC repository first. You can then apply the upgrade file to managed ArcMCs.

To upload the upgrade file to your repository:

1. Download the ArcMC upgrade file for the upgrade version, as outlined in the table above, and store it in a secure network location.
2. Click **Administration > Repositories**.
3. In the navigation tree, pick **Upgrade Files**.
4. In the management panel, click **Upload**.
5. Click **Choose File** and browse to your upgrade file, then click **Submit**. The file is uploaded.

To remotely upgrade one or more managed ArcMCs:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **ArcMCs**.
4. In the list of ArcMCs, select one or more ArcMCs for upgrade. (You may select only the form factor appropriate for the upgrade file type, as outlined above.)
5. Click **Upgrade ArcMC**. The Upgrade wizard is launched.
6. Review the dialog box, then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.

Local Upgrade of ArcMC

A local upgrade uses the same file as remote upgrades, as described above.



Note: Although the filename for software ArcMC upgrade includes the word 'remote' (arcmc-sw-<build number>-remote.enc), this file should be used for local upgrades as well.

To perform a manual upgrade of an ArcMC local host:

1. Download the upgrade file for your form factor to a secure network location.
2. Click **Administration > System Admin**
3. In the navigation menu, under **System**, click **License & Update**.
4. In the management panel, under **Select File to Upload**, click **Browse**.
5. Browse to the upgrade file you downloaded in Step 1.
6. Click **OK**. The upgrade file is applied to the local host.



Note: In some cases, after the upgrade of a local host with an .enc file completes, an empty page is displayed. You may navigate away from this page as normal.

Setting a Configuration on Managed ArcMCs

You can set a configuration on one or multiple ArcSight Management Centers using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple ArcSight Management Centers. Only new values will be appended. (For more information on list configurations, see "[The Configurations Table](#)" on

[page 172](#)).

- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple ArcSight Management Centers.



Caution: Setting a configuration on one or more ArcSight Management Centers may make each ArcSight Management Center node non-compliant with its current subscriptions.

To set a configuration on one or more ArcSight Management Centers:

- Click **Node Management**.
- In the navigation tree, click **System**.
- In the management panel, click **ArcMCs**.
- In the list of ArcSight Management Centers, select one or more ArcSight Management Centers for which to set a configuration.
- Click **Set Configuration**. The Set Configuration wizard is launched.
- Review the dialog box, then click **Next**.
- Follow the prompts to complete the wizard.
 - Click **Add Row** to add a new Property to a list configuration, then specify values as needed.
- The configuration is set on the selected ArcSight Management Centers. Click **Done**.

Managing SmartConnectors on ArcMC

ArcMC can remotely manage previously-installed, software-based SmartConnectors; however, the remote management feature is disabled on software SmartConnectors by default.

You can install several SmartConnectors on a single host if supported by the hardware. ArcSight certifies a maximum of 4 SmartConnectors on Windows hosts and 8 on Linux hosts.

To manage software-based SmartConnectors with , you need to enable remote management on each connector, as follows:

- In a text editor, in the installation directory for the SmartConnector, open the file /<install_dir>/user/agent/agent.properties.
- Add the line: remote.management.enabled=true
- If desired, customize the connector's listening port. The default is 9001. To change this value, add the line: remote.management.listener.port=<port_number>, where <port_number> is the new port number.
- Save the file.
- Restart the SmartConnector for changes to take effect.

Managing Loggers

You can perform any of the following management tasks on managed Logger Appliances or Software Loggers using Arcsight Management Center.

- [Reboot](#) or [shut down](#).
- [Edit or remove a configuration](#).
- [Set a configuration on one \(or multiple\) Loggers](#).
- [Remotely upgrade a Logger](#).



Note: Not all Logger functionality is manageable through Arcsight Management Center. For a complete discussion of Logger features, see the Logger Administrator's Guide.

Rebooting a Logger

To remotely reboot a managed Logger:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, locate the Logger to be rebooted.
5. In the **Action** drop-down of the Logge, click **Reboot Logger**.
6. Click **Next** to confirm reboot.
7. The Logger is rebooted. Click **Done**.

Shutting Down a Logger

To remotely shut down a managed Logger:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, select the Logger to be shut down.
5. In the **Action** drop-down of the Logger, select **Shut Down Logger**.
6. Click **Next** to confirm shut down.
7. The Logger is shut down. Click **Done**.

Editing or Removing a Configuration for a Logger

You can edit a configuration on, or remove property values of a list configuration from a managed Logger.

Editing or removing a configuration will overwrite the node's current configuration. This may make the node non-compliant with its current subscriptions.

To edit or remove a configuration on a managed Logger:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, locate the desired Logger.
5. In the **Action** drop-down of the Logger, select **Edit/Remove Config**. The Update Configurations wizard is launched.
6. Review the dialog box, then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.



Note: In order to edit a backup configuration on a Logger node, the node must have a scheduled backup to begin with.

Upgrading a Logger

Remote upgrades to Logger 7 require a previous hot-fix to be applied if Logger's versions are any of the following:

- 6.7.0.8242
- 6.7.1.8253
- 6.7.1.8257
- 6.7.1.8262

The hot fix file to be uploaded is **preupgrade-logger-20190924.enc**. The name should be kept as is.

To upload the file from the master ArcMC:

1. Download the hotfix file and store it in a secure network location. The file name should always be preupgrade-logger-20190924.enc depending on the form factor.
2. Click **Administration > Repositories**.
3. Select **Upgrade Files** from the navigation tree.
4. In the management panel, click **Upload**.
5. Click **Choose File** and browse to your hot fix file, then click **Submit**. The file is now uploaded.
6. Continue with the normal procedure outlined in the "[To remotely upgrade one or more managed Loggers:](#)" on the next page

In ArcMC, you can remotely upgrade any of the following managed Logger types.

Form Factor	Upgrade File Name	Can Upgrade From Version...	Can Upgrade To Version...	Comments
Appliance	logger-<build number>.enc	6.0 or later	6.1 or later	The filename format for the remote upgrade file for Logger Appliance is logger-<build number>.enc
Software	logger-sw-<build number>-remote.enc	6.0 or later	6.1 or later	<ul style="list-style-type: none"> The filename format for the remote upgrade file for software Logger is logger-sw-<build number>-remote.enc Remote operating system upgrade is not supported for software Logger, and, if required, must be performed manually.



Note: Upgrading to Logger version 6.0 requires ArcMC Agent 1167.1 or later to be running on the managed Logger. Upgrade the Agent on the managed Logger before performing the upgrade to Logger 6.0.

To upload the upgrade file to your repository:

1. Download the Logger upgrade file for the upgrade version, as outlined in the table above, and store it in a secure network location.
2. Click **Administration > Repositories**.
3. In the navigation tree, pick **Upgrade Files**.
4. In the management panel, click **Upload**.
5. Click **Choose File** and browse to your upgrade file, then click **Submit**. The file is uploaded.

To remotely upgrade one or more managed Loggers:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, select one or more Loggers. (You may only select one form factor type to upgrade.)
5. Click **Upgrade Logger**. The Upgrade wizard is launched.
6. Review the dialog box, then click **Next**.
7. Follow the prompts to complete the wizard.
8. When the wizard is complete, click **Done**.



Note: In some cases, after the upgrade of a localhost with an .enc file completes, an empty page is displayed. You may navigate away from this page as normal.

Setting a Configuration on Loggers

You can set a configuration on one or multiple Loggers using the Set Configuration wizard.

- For list configurations, use the Set Configuration wizard to append property values to an existing configuration on multiple Loggers. Only new values will be appended. For example, if you had a common group of users on three Loggers, you could use the Set Configuration wizard to add the same new user to all three Loggers with a single action. (For more information on list configurations, see "[The Configurations Table](#)" on page 172.)
- For non-list configurations, use the Set Configuration wizard to overwrite the configuration on multiple Loggers.



Caution: Setting a configuration on one or multiple Loggers may make each Logger node non-compliant with its current subscriptions.

To set a configuration for one or more Loggers:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. In the management panel, click **Loggers**.
4. In the list of Loggers, select one or more Loggers for which to set a configuration.
5. Click **Set Configuration**. The Set Configuration wizard is launched.
6. Review the dialog box, and click **Next**.
7. Follow the prompts to complete the wizard.
 - Click **Add Row** to add a new Property to a list configuration, then specify values as needed.
8. The configuration is set on the selected Loggers. Click **Done**.

Managing Containers

A *container* is a single Java Virtual Machine (JVM) that can run up to four connectors. The exact number of connectors depends on your current service agreement and the type of connector.

Containers may run on ArcMIDs, on Connector Appliances, and on L3XXX model Loggers. The number of containers that can be run at one time is based on the product license. Check under **System Admin > License & Update** for this information.

Scanning a managed host will ensure all currently running containers on the host (and the connectors associated with them) are accurately inventoried. For more information, see ["Scanning a Host" on page 233](#).



Note: A connector of any of the following types must be the single connector running in its container:

- Trend Micro Control Manager (TMCM)
- Syslog
- Windows Unified Connector (WUC)



Note: For Microsoft Windows Event Log (WINC), only one connector can be created on an ArcMC appliance.

Viewing All Containers

You can view all containers managed in Arcsight Management Center.

To view all containers:

1. Click **Node Management**
2. In the navigation tree, click **System**. (Alternatively, to view containers on a specific host, select the host from the navigation tree.)
3. Click the **Containers** tab to display the containers.

Viewing Connectors in a Container

You can see all the connectors in a container.

To view connectors in a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the container whose connectors you wish to view.
3. Click the tree branch corresponding to the container.
4. Click the **Connectors** tab. The connectors in the container are displayed.

Editing a Container

The default name for a container is *Container N*, where N is a sequential number that indicates the order in which the container was added. However, you can edit a container's default name.

To edit a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host with container you wish to rename.
3. In the list of containers, locate the container you wish to edit.
4. In the **Action** drop-down of the container, click **Edit Container**.
5. In **Name**, specify the new container name, then click **Next**.
6. Click **Done**. The container is renamed.

Deleting a Container

When you delete a container, the connectors that it contains are also deleted.

To delete a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to delete.
5. Click **Delete**.
6. Click **OK** to confirm deletion. The selected containers are deleted.



Note: Containers on appliances can't be deleted.

Changing Container Credentials

You can change the user name and password associated with each container.



Caution: A container's default user name is `connector_user` and the default password is `change_me`. ArcSight strongly recommends that for optimal security, you should change each container's credentials to a non-default value before deploying it to production.

To change container credentials:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to change the credentials.

5. Click **Credentials**.
6. Follow the instructions in the wizard to update the credentials for the selected containers.

Sending a Command to a Container

You can run commands on a container to configure memory settings, pull an OPSEC certificate, generate a key, or restart the container.

To run a command on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. In the **Action** drop-down of the container, click **Send Container Command**. The Send Command wizard starts.
5. From the drop-down list, select the command you want to send, then click **Next**.
6. Specify appropriate values for the parameters and then click **Done**.

Upgrading All Connectors in a Container

You can upgrade all connectors in a container to a specific parser or framework version number.

Before Performing the Upgrade

Prior to performing a container upgrade, you will need to follow the steps below:

For connectors running 32-bit with version < 7.11, it is required to perform 32-bit to-64 bit migration before upgrading to a connector running >=7.11.

32-bit to 64-bit container migration.

1. Upgrade the appliance you currently have (a G8 migrated from conapp to ArcMC) to the latest ArcMC build.
2. Back up the container using the repositories page.
3. Emergency restore the container to the 64 bit connector AUP.
4. Restore the backup to the container using the repositories page.
 - **Case #1:** G8 appliances: model >= 6500 and restoreToVersion >= 7.9.0.8084 OR if connector is restored to any version less than 7.9.0, the connector will get restored to 32 bit, if connector is restored to any version greater than 7.9.0, the connector will get

restored to 64 bit.

- **Case #2:** G9 appliances: model >= 6600 and restoreToVersion >= 7.2.1.7714.0 if connector is restored to any version less than 7.2.1 - restore should not be allowed, if connector is restored to any version greater than 7.2.1, the connector will get restored to 64 bit.



Note: The above Emergency Restore to perform 32-bit to 64 bit connector migration does not support Appliances running on C5500 model.

To upload a version file to your repositories.

You can use a connector AUP file of the new parser or framework version in your ArcMC repository. If you opt to use this method, you will need to upload the version file to your repository as follows:

1. Click **Administration > Repositories**.
 2. In the navigation tree, pick **Upgrade Files**.
 3. In the management panel, click **Upload**.
 4. Click **Choose File** and browse to your connector AUP file, then click **Submit**. The file is uploaded.
- Alternatively, instead of using a parser AUP file from the repository, you can download and use parser files from the [ArcSight Marketplace](#). (Framework files are not available from the Marketplace.) Create your administrative account on the ArcSight Marketplace. If you have not created your Marketplace account, you are given an opportunity to sign up for an account during the parser upgrade process.

To perform the parser or framework upgrade on all connectors in a container:



Note: Parser Remote Upgrade on Connector in Transformation Hub (CTH) is not supported from ArcMC. Parsers on CTH are updated during the Transformation Hub releases.

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to upgrade.
5. Click **Upgrade**.
6. On the upgrade page, under **Select Upgrade Type**, choose either **Parser upgrade** or **Framework upgrade**.

7. Under **Select Upgrade Version**, from the drop-down list, choose the version to which you want to upgrade the selected containers. (You can control the number of parser upgrade versions displayed in the drop-down, as described in [Modifying logger.properties](#).) (You can select the number of parser upgrade versions displayed in the drop-down as described in [Configuring ArcMC Parser Upgrades](#).)
 - a. For a parser upgrade, if the selected parser version is from the Marketplace and not the local repository, save your Marketplace credentials in ArcMC. This is a one-time task unless you wish to update these credentials.
8. Click **Upgrade**. The upgrade is performed on all containers.



Note: If you are performing parser upgrades through a proxy server, additional configuration is required. See [Modifying logger.properties](#) for more information.

Modifying logger.properties

To enable or modify some functionality, such as performing you may need to edit the file `<install_dir>/userdata/arcmc/logger.properties` with additional parameters in any text editor.

General Editing Procedure

If `<install_dir>/userdata/arcmc/logger.properties` does not exist, then create one in a text editor. This file must be owned by a non-root user. For an ArcMC appliance, use the 'arcsight' user, and for software ArcMC, use the non-root account used to install the ArcMC.

The `logger.properties` file may not be readable and writable by all users. Apply the following commands to the file.

```
chown <non-root user>:<non-root user> logger.properties
```

```
chmod 660 logger.properties
```

Finally, *restart the web process* after making any edits to `logger.properties`.

Uploading Files Larger Than 100 MB under Repository.

If `<install_dir>/userdata/arcmc/logger.properties` does not exist, then create one in a text editor. This file must be owned by a non-root user. For an ArcMC appliance, use the 'arcsight' user, and for software ArcMC, use the non-root account used to install the ArcMC.

Modify the `<install_dir>/userdata/arcmc/logger.properties` by adding:

```
connectorappliance.file.maxupload=400
```

After adding the previous line, owner and permissions need to be changed:

```
chown <non-root user>:<non-root user> logger.properties  
chmod 660 logger.properties
```

Finally, restart the web process after making any edits to logger.properties.

For Parser Upgrades Through a Proxy Server

If performing parser upgrades, and your environment connects to the Marketplace through a proxy server, you will need to modify the <install_dir>/userdata/arcmc/logger.properties file with the proxy details.

```
proxy.server=<server address>  
proxy.port=<server port>  
#Enter the proxy server credentials if the proxy server needs authentication  
proxy.username=<username>  
proxy.password=<password>
```

For the Number of Parser Upgrade Versions Displayed

You can control the number of parser upgrade versions displayed in the parser upgrade drop-down list. In logger.properties, set the parameter

```
marketplace.parser.update.latest.versions.count = <number of parser upgrade  
versions to be retrieved from Marketplace>
```

To Disable the Marketplace Connection

To disable ArcMC's Marketplace connection, in logger.properties, set the parameter

```
marketplace.enable=false
```

If set to false, you will not be able to see the available parser upgrade versions from the Marketplace. In addition, the containers under **Node Management > Containers** tab, will not display the *Parser Out of Date* status in the **Parser Version** column.

Restarting a Container

Restarting a container will restart all the connectors in the container. You can restart multiple containers in bulk.

To restart one or more containers:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which a container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to restart.
5. Click **Restart**.
6. Click **Yes** to confirm restart. The selected containers are restarted.

Viewing Container Logs

You can retrieve and view the log files for one or more containers. The log files are in .zip format.

Container logs must be uploaded to the Logs repository before they can be viewed. For instructions on how to upload logs, see "[Uploading a File to the Logs Repository](#)" on page 250.

To retrieve and view container logs:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to view logs.
5. Click **Logs**.
6. Click **Next** to begin the **Retrieve Container Logs** process. When complete, click **Done**.
7. Click **Administration > Repositories**.
8. In the left panel, click **Logs**.
9. In the management panel, click  to retrieve the log files (in .zip format) you want to view.

Deleting a Container Log

You can delete unneeded container logs as necessary.

To delete a container log file:

1. Click **Administration > Repositories**.
2. In the left panel, click **Logs**.
3. In the management panel, on the list of logs, click  next to the log file you want to delete.
4. Click **OK** to confirm deletion.

Enabling FIPS on a Container

FIPS mode is supported on local, and remote connectors and Collectors running version 4.7.5 or later, but certain connectors do not support FIPS mode. For information about which connectors do not support FIPS mode, see the [Installing FIPS-Compliant SmartConnectors](#) document. Before enabling FIPS on a container that contains connectors running as a service, review the caveats listed in that document.

FIPS is disabled by default on ArcSight Management Center, but can be enabled as described under ["FIPS 140-2" on page 298](#). After FIPS is enabled on the appliance, you can enable FIPS on a container. Any FIPS-compliant connector in that container (or one which is added later) will automatically communicate in FIPS mode.

- If the connector destination is ArcSight Manager, Connector Management automatically imports the ArcSight Manager certificate into its trust store and applies it to the container.
- However, if the connector destination is Logger, the Logger certificate must be uploaded manually and applied to the container.

A FIPS Suite B certificate must be uploaded manually, regardless of the connector destination, as described in under “Enabling FIPS Suite B on a Container”, below.

You enable or disable FIPS using the same procedure.

To enable or disable FIPS mode on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to enable FIPS.
5. Click **FIPS**.
6. Follow the instructions in the wizard to update FIPS status.

Check that the appropriate CA certificates are in the trust store so that the connectors in the container can validate their configured destinations successfully. If necessary, add the appropriate certificates to the container.



Note: A 32-bit FIPS connector enabled cannot be remotely managed if it is installed on a 64-bit Linux system.

Enabling FIPS Suite B on a Container

Managed connectors can communicate in FIPS Suite B mode with their destination. A FIPS Suite B certificate must be imported manually and applied to the container, regardless of the connector destination.

Before you perform the following procedure, make sure FIPS mode is enabled on ArcSight Management Center, as described in "["FIPS 140-2" on page 298](#).

To enable FIPS Suite B on a container:

1. Export the certificate for the connector destination (either ArcSight Manager or Logger) to a temporary directory. For example, on ArcSight Manager, from \$ARCSIGHT_HOME/current/bin, specify the following command: `./arcsoft runcertutil -L -n mykey -r -d /opt/arcsoft/manager/config/jetty/nssdb -o /tmp/managercert.cer`
2. Upload the certificate from the temporary directory to the CA Certs Repository, as described in "["CA Certs Repository" on page 251](#)".
3. Enable FIPS on the container as described above.
4. Add the certificate on the container, as described in "["Managing Certificates on a Container" on page 136](#)".
5. Click **Node Management**.
6. In the navigation tree, navigate to the host on which the container resides.
7. Click the **Containers** tab.
8. On the **Containers** tab, select one or more containers for which to enable FIPS Suite B.
9. Click **FIPS**.
10. Follow the instructions in the wizard to update FIPS Suite B status.

Adding a Connector to a Container

Each container may hold up to 4 connectors.

To add a connector to a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the container to which you wish to add a connector.
3. On the **Connectors** tab, click **Add Connector**. The **Connector Setup** wizard starts.
4. Click **Next**, then follow the prompts to set up the new connector.



Note: Always change the default credentials of any new connector to non-default values.

For more information, see "[Changing Container Credentials](#)" on page 127.

Running Logfu on a Container

The **Logfu** utility is a diagnostic tool that parses ArcSight logs to generate an interactive visual representation of the information contained within the logs. When event flow problems occur, it can be useful to have a visual representation of what happened over time.

To run Logfu on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, locate a container on which to run Logfu.
5. In the **Action** drop-down of the container, click **Run Logfu**.
6. The Logfu progress window is displayed as system data logs are retrieved and analyzed.
Data is then displayed by **Group**, **Field**, and **Chart**.
 - In the **Group** box, choose which type of data you would like to view. The **Group** box lists all connectors within the chosen container, plus many other types of data such as memory usage and transport rates.
 - Then, choose one of the Group box **data points**. Depending on which data point you chose, a list of fields appears in the Field box below.
 - Select a **field** to view. A graphic chart appears in the Chart box, providing rate and time information. The key at the bottom of the Chart box defines the data points mapped in the chart.
 - To choose a different data point for analysis, click **Reset Data**.
7. When complete, close the display window.

Managing Certificates on a Container

Connectors require a Certificate Authority (CA) issued or self-signed SSL certificate to communicate securely with a destination. The Certificate Management wizard, available from the **Containers** tab, helps you add and remove certificates on a container. Using the wizard, you can:

- Add a certificate to a container.
- Add certificates in bulk, enabling multiple containers at once.
- Enable or disable a demo certificate on a container that is in non-FIPS mode only.
- Add a CA Certs file on a container that is in non-FIPS mode only.
- Remove a certificate from a container.

From the **Containers** tab and the **Connectors** tab, you can view details about the certificates applied to a container. See "[Viewing Certificates on a Container](#)" on page 139.

For information about resolving invalid certificates, see "[Resolving Invalid Certificate Errors](#)" on page 140.

Adding CA Certificates to a Container

You can add a single CA certificate to a container that is in FIPS mode or non-FIPS mode.



Note: Whenever you enable or disable FIPS mode on a container, check that the required certificates are present in the trust store and add them if necessary.

Click the icon next to the container name to see the type of certificate applied to it. Click **Display Certificates** from the action drop down to see the list of available certificates on the container.

Before you perform the following procedure, make sure the certificate you want to add is loaded in the CA Certs repository.

To add a single CA certificate to a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to which you wish to add certificates.
5. Click **Certificates**. The Certificate Management wizard starts.
6. Review the dialog box, then click **Next**.

7. Under **Choose an Action**, select **Add Certificate**, then click **Next**.

8. Follow the instructions in the wizard to add the certificate.

If a container is down or a connector is running an older build, the wizard reports errors in the progress bar and on the Summary page.

Removing CA Certificates from a Container

You can remove CA certificates from a container when they are no longer needed. When you remove a CA certificate, the certificate is removed from the container's trust store; but it is **not** deleted from the repository.



Caution: Use caution when deleting certificates. When you delete a certificate on a container but the connector destination is still using that certificate, the connector can no longer communicate with the destination.

To remove CA certificates from a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers to which you wish to remove certificates.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, then click **Next**.
7. Under **Choose an Action**, select **Remove certificate**, then click **Next**.
8. Select one or more certificates from the certificate list, then click **Next**. The certificates are removed from the list of certificates and no longer used. When you remove a certificate from a container in FIPS mode, the container restarts automatically.
9. The Certificate Management wizard displays the certificates that are removed successfully in a comma-separated list. Certificates that cannot be removed are shown in a comma-separated list together with a reason why the certificate removal failed.

Adding a CA Certs File to a Container

You can add a CA Certs file to any container that is in non-FIPS mode.



Caution: When you apply a CA Certs file, the entire trust store on the container is overwritten. All previously-added certificates are overwritten.

Before you follow the procedure below, make sure that the CA Certs file you want to add is loaded in the CA Certs repository.

To add a CA Certs file to a non-FIPS mode container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, Select one or more non-FIPS mode containers to which you wish to add a CA Certs file.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, then click **Next**.
7. Under **Choose an Action**, select **CA Cert (Legacy)**.
8. Follow the instructions in the wizard.

After the CA Certs file has been added to a container, the container restarts automatically.

Enabling or Disabling a Demo Certificate on a Container

You can use the demo certificate on a container for testing purposes. By default, the demo certificate on a container is disabled. You can enable the demo certificate temporarily for testing purposes on a container that is non-FIPS mode.



Note: Enable a *demo* certificate on a container in non-FIPS mode for testing purposes only. Using a demo certificate in a production environment is a serious security issue because the demo certificate is not unique.

To enable or disable a demo certificate on a non-FIPS mode container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, Select one or more non-FIPS mode containers for which you wish to enable or disable a CA Certs file.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, then click **Next**.
7. Under **Choose an Action**, select **Demo CA (Legacy)**, then click **Next**.
8. Follow the instructions in the Certificate Management wizard.

After you add the demo certificate on a container, the container restarts automatically.

Adding Multiple Destination Certificates to a Container

You can add multiple destination certificates to a container, whether in FIPS mode or not.



Note: Whenever you enable or disable FIPS mode on a container, check that the required certificates are present in the trust store and add them if necessary.

Click the icon to display a list of the certificates available on the container.



Note: In the event that importing destination certificates for Transformation Hub fails due to changes in the certificate, please proceed to **remove** and then **add** the destination from the Connector as explained in "["Removing Destinations" on page 149](#)" and "["Adding a Primary Destination to a Connector" on page 147](#)".

To apply multiple destination certificates to a container:

1. Click **Node Management**.
2. In the navigation tree, click **System**.
3. Click the **Containers** tab.
4. On the **Containers** tab, containers for which you wish to add multiple destination certificates.
5. Click **Certificates**. The **Certificate Management** wizard starts.
6. Review the dialog box, then click **Next**.
7. Under **Choose an Action**, select **Import destination certificates** to add a certificate.
8. Follow the instructions in the wizard to complete the process.

Viewing Certificates on a Container

You can display a list of the CA certificates applied to a container and view the details for a particular certificate in the list. To view certificates on a container,

- On the **Containers** tab, in the **Action** drop-down for the container whose certificates you want to view, select **Display Certificates**.
- On the **Connectors** tab, click **Certificates** at the top of the page.

The Certificate List wizard displays the certificates applied to a container. To see details of a certificate, select the certificate, then click **Next** at the bottom of the page.

Resolving Invalid Certificate Errors

If no valid CA certificates exist for the connectors in the container, resolve the invalid certificate error as follows:

To resolve the invalid certificate error:

1. Select the container in the navigation tree.
2. Click the **Containers** tab. The error message is displayed.
3. In the **Action** drop-down of the container showing the issue, select **Download Certificates**.
4. Follow the instructions in the wizard to download and import the valid certificates.

Running Diagnostics on a Container

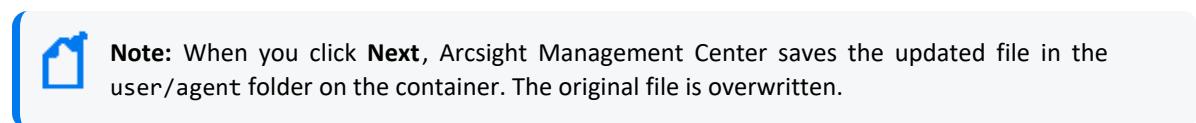
You can run diagnostics on a container.



Note: Diagnostic tools are also provided under **Administration > System Admin**.

To run diagnostics on a container:

1. Click **Node Management**.
2. In the navigation tree, navigate to the host on which the container resides.
3. Click the **Containers** tab.
4. On the **Containers** tab, select one or more containers for which to run diagnostics.
5. In the **Action** drop-down, click **Run Logfu**. The Diagnostics wizard starts.
6. Select the action you want to take on the selected container:
 - Select **Edit a configuration file** to edit a file in the user/agent folder on the container with the extension .properties, .csv, or .conf.
 - Select **Edit a user file** to edit any file (except binary files, such as .zip, .jar, or .exe) in the user/agent folder on the container.
7. From the list of available files, select the file you want to edit. The file displays in the Edit File panel. Make your edits, then click **Next** to save your edits and restart the container.



Note: When you click **Next**, Arcsight Management Center saves the updated file in the user/agent folder on the container. The original file is overwritten.

8. Click **Done** to close the Diagnostics wizard.

Managing Connectors

A *connector* (also known as a *SmartConnector*) is an ArcSight software component that collects events and logs from various sources on your network. A connector can be configured on Arcsight Management Center, on a Logger platform with an integrated Connector Appliance, or installed on a computer on your network, managed remotely. For a complete list of supported connectors, go to the ArcSight Customer Support site.



Note: The maximum number of selected entries when managing Connectors/Collectors is 50.

Procedures for managing connectors are described below.

Viewing All Connectors

You can see all currently managed connectors.

To view all connectors:

1. Click **Node Management**.
2. Click **System** in the navigation tree.
3. In the management panel, click the **Connectors** tab. All connectors display on the **Connectors** tab in the management panel.

Adding a Connector

Prerequisites

Before you add a connector, review the following important information.

- Make sure that the container, host, and location to which you want to add the connector exist in Arcsight Management Center. If any of these elements do not exist, create them.
- Follow the configuration best practices described in "[Configuration Suggestions for Connector/Collector Types](#)" on page 163.

If you are configuring the Check Point OPSEC NG Connector, see "[Configuring the Check Point OPSEC NG Connector](#)" on page 164 and refer to the SmartConnector Configuration Guide for Check Point OPSEC NG.

If you are configuring a database connector that requires the MS SQL Server Driver for JDBC, follow instructions in "[Adding the MS SQL Server JDBC Driver](#)" on page 167.



Caution: This connector type has special requirements concerning JDBC and authentication setup. Refer to the SmartConnector Configuration Guide for Microsoft SQL Server Multiple Instance Audit DB for this important information before installing the connector.

- If you are adding a software-based connector, make sure that the username and password for the connector match the username and password for the container to which you are adding the connector. If necessary, refer to "["Changing Container Credentials" on page 127](#).



Caution: Each connector's default user name is connector_user and the default password is change_me. A connector with these default values still in place should be considered non-secure. ArcSight strongly recommends that for optimal security, you should change each connector's credentials to non-default values before deploying the connector to production.

- File-based connectors use the Common Internet File System (CIFS) or Network File System (NFS). These stipulations apply when creating a local connector to run as part of ArcMC.
 - On a Windows system, a CIFS share needs to be configured before you add a file-based connector.
 - For all other connectors, an NFS mount needs to be established before a file-based connector can be added. In addition, when entering the connector parameters, specify the configuration file name without an extension in the **Configuration File** field. The extension .sdkrfilereader.properties is appended automatically.
- For detailed information about individual connector parameters, refer to the specific ArcSight SmartConnector Configuration Guide for the type of connector chosen. The configuration guide also describes how to set up the source device for use with the connector

To add a connector:



Tip: If you are adding a connector for the Check Point FW-1/VPN-1 system, see a more detailed procedure in "["Configuring the Check Point OPSEC NG Connector" on page 164](#).

1. Click **Node Management**.
2. In the navigation tree, browse to the host on which the connector will reside.
3. In the management panel, click the **Containers** tab.
4. On the **Containers** tab, locate the container where you will assign the connector.
5. In the **Action** drop-down, click **Add Connector**. The Connector Setup wizard starts.
6. Review the dialog box, then click **Next**.
7. Select a connector type from the pull-down list of available types, then click **Next**.

8. Specify basic parameters for the connector. Parameters vary based on the connector type. (Hover over a field for more information on a field.) When all fields have been entered, click **Next**.



Note: When entering parameters that include a file path, specify the path in POSIX format (for example, /folder/filename).

For file-based connectors on Windows systems, specify the name of the CIFS mount point you created for the connector. (You need to specify /opt/mnt/CIFS_share_name.)

Some connectors include table parameters. For example, the Microsoft Windows Event Log includes parameters for each host in the domain and one or more log types (security, application, system, directory service, DNS, file replication, and so on). You can import table parameters from a CSV file that was exported from another connector, as long as you export it and import it from the same containers. If the CSV file was exported from a different container, you need to change the secret parameters, such as the password, which appear in obfuscated format in the CSV file to plain text before you import the CSV file.



Note: For connectors that query Microsoft Active Directory to detect devices (for example, Microsoft Windows Event Log - Unified), if the “Network Security: LDAP Server Signing Requirements” policy is set to “Signing Required” on the Domain Controller, Arcsight Management Center will be unable to connect to the Active Directory or browse for devices. You see an error when selecting **Windows Host Browser** as the connector device browser type.

9. Select a primary destination for the connector and specify destination-specific parameters on the following page(s), then click **Next**. Destinations can be:

- ArcSight Logger SmartMessage (encrypted)
- ArcSight Manager (encrypted)
- CEF Syslog (plaintext, that is, unencrypted)



Note: FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from the destination**, then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination, and then click Next** if you do not want to import the certificate. The destination will not be added.

10. Specify connector details:

Parameter	Description
Name	A descriptive name for this connector.
Location	The location of the connector (such as the hostname).
Device Location	The location of the device that sends events to the connector.
Comment	Additional comments.

- When complete, click **Done**.

Editing Connector Parameters

ArcSight supports a large number of connector types to gather security events from a variety of sources, including syslog, log files, relational databases, and proprietary devices. Accordingly, configuration parameters vary widely depending on the type of connector being configured.

You can edit parameters (simple and table) for a specific connector, or for multiple connectors of the same type at the same time.



Note: The maximum number of selected entries when managing Connectors/Collectors is 50.

Updating Simple Parameters for a Connector

The following procedure describes how to update simple parameters for a specific connector.

To update parameters for a specific connector:

- Click **Node Management**.
- In the navigation tree, browse to the connector you wish to update.
- In the management panel, the **Connector** summary tab displays.
- On the **Connector** tab, next to **Connector Parameters**, click
- Modify parameters as necessary, then click **Next**.
-  **Note:** When editing parameters that include a file path, specify the path in POSIX format (for example, /folder/filename).
- When complete, click **Done**. The updated parameters display in the **Connector Parameters** table of the Connector summary tab.

Updating Table Parameters for a Connector

Certain connectors, such as the Microsoft Windows Event connector, have table parameters. You can update the table parameters for a specific connector when necessary.

To update table parameters for a specific connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector you wish to update. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, next to **Table Parameters**, click .
4. Modify parameters as necessary and then click **Next**.
 - To add more rows of parameter information, click the **Add Row** link.
 - You can use an Excel-compatible program to prepare a comma-separated values text file with the information and click the **Import File** button to load the entire table at once. The file needs to be in the same format as the rows shown on the Update Table Parameters page, and it needs to include a header row with parameter labels in the order shown on that page. For fields that require check box values, specify True or False as the value. An example is shown below.

	A	B	C	D	E	F
1	Domain Name	Host Name	User Name	Password	Security Logs	System Logs
2	test	1.1.1.1	admin	password	TRUE	FALSE
3	test2	1.1.1.1.1	admin	password	TRUE	FALSE

5. When complete, click **Done**. The updated table parameters display in the Table Parameters section of the Connector page.



Note: You can import a CSV file that was exported from another connector as long as you export and import the CSV file from the same container. If the CSV file was exported from a different container, you need to change the secret parameters, such as the password, which appear in obfuscated format in the CSV file to plain text before you import the CSV file.

Updating Simple and Table Parameters for Multiple Connectors

If you have multiple connectors of the same type, you can change the simple and table parameters for all the connectors at the same time.

To edit parameters for multiple connectors of the same type:

1. Click **Node Management**.
2. In the navigation tree, select the host where the connectors reside.
3. In the management panel, select the connectors whose parameters you want to update.
4. Click **Parameters**. The Update Connect Parameters wizard starts.
5. Review the dialog box, then click **Next**.
6. Follow the instructions in the wizard.
 - You can choose to modify the simple parameters for all the selected connectors at once or modify the simple parameters per connector.
 - If the connectors have table parameters, the table parameters are displayed so that you can modify them. If you have many table parameters to modify for multiple connectors, you can import the parameters from a CSV file. You can also export the table parameters to a CSV file for use as a backup or to import on another Connector Appliance.



Note: When you update parameters for connectors of different versions, the newer connectors might have additional parameters. In this case, only those parameters shared by all connectors are displayed for updating.

7. Click **Done** when complete.

Managing Destinations

Connectors can forward events to more than one destination, such as ArcSight Manager and ArcSight Logger. You can assign one or more destinations per connector. You can assign multiple destinations to a connector and specify a failover (alternate) destination in the event that the primary destination fails.

The following procedures describe how to perform these actions on a specific connector or for multiple connectors at the same time:

- Add a primary or failover destination
- Edit destination parameters and destination runtime parameters
- Remove destinations
- Re-register destinations
- Manage alternate configurations for a destination
- Send a command to a destination



Note: Compared to the standalone Connector destination list, ArcMC Appliance on-board Connector does not cover the following three options: CEF file, CSV file and Raw Syslog



Note: In the event that the Transformation Hub certificate changes, the Connectors that had that Transformation Hub as a destination will be lost. To re-enable them follow the steps under ----new section---

Adding a Primary Destination to a Connector

When you add a primary destination to a connector, you need to specify details for the destination, such as the destination hostname and port used.

To add a primary destination to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to add a destination. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, next to **Destinations**, click . The Add Destination wizard starts.
4. Follow the steps in the wizard. You can either select an existing destination or add a new destination. If you are adding a new destination, select the destination type and specify parameters for the destination. Destination types are described in the SmartConnector User's Guide.



Note: For containers running 5.1.2.5823 and later, Arcsight Management Center retrieves the certificate for the ArcSight Manager destination automatically and displays the certificate summary.

For containers running 5.1.2 and earlier, upload the certificate on the container and then add the destination.

FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from the destination**, then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.

5. Click **Done** when complete.

Adding a Failover Destination to a Connector

Each destination can have a failover destination in case the connection with the primary destination fails.



Tip: UDP connections cannot detect transmission failure. Use Raw TCP for CEF Syslog destinations.

To add a failover destination to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to add a destination. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click . The Add Destination wizard starts.
4. Follow the steps in the wizard to select from available destinations and specify the destination details.



Note: FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from the destination**, then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.

5. Click **Done** when complete.

Adding a Primary or Failover Destination to Multiple Connectors

You can add a primary or failover destination to several connectors at the same time.

To add a primary or failover destination to multiple connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors to which you wish to assign a destination.
5. Click **Destinations**. The Manage Destinations wizard launches.
6. Review the dialog, then click **Next**.
7. Under **Choose an Option**, select **Add a destination**, then click **Next**.
8. Select between creating a new destination or selecting an existing destination, then click **Next**.

- If you choose to **create a new destination**, select the destination type and then provide the destination parameters. Destination types are described in the SmartConnector User's Guide.
- If you choose to **select an existing destination**, select a destination from the list.



Note: Arcsight Management Center retrieves the ArcSight Manager certificate for the destination automatically and displays the certificate summary.

FIPS Suite B certificates are not retrieved automatically and must be uploaded manually.

To see certificate details, hover over the certificate.

- Select **Import the certificate to the connector from destination**, then click **Next** to import the certificate and continue.
- Select **Do not import the certificate to the connector from the destination** and click **Next** if you do not want to import the certificate. The destination will not be added.

9. Define the destination function by choosing between a primary or failover destination.
 - If you choose **Primary destination**, click **Next** to update the configuration.
 - If you choose **Failover destination**:
 - a. Select the primary destination that applies to your failover.
 - b. Check the box in the table header to modify all of the displayed connectors.
 - c. Click **Next** to update the configuration.
10. Click **Done** when complete.

Removing Destinations

You can remove a destination from a connector at any time. Each connector must have at least one destination; as a result, you may not remove all destinations from a connector.

To remove destinations from one or more connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors to which you wish to remove a destination.
5. Click  **Destinations**. The **Manage Destinations** wizard launches.
6. Review the dialog, then click **Next**.
7. Under **Choose an Option**, select **Remove a destination**, then click **Next**.
8. Follow the instructions in the wizard, and click **Done** when complete.

Re-Registering Destinations

At certain times, you might need to re-register the destinations for one or more connectors; for example, after you upgrade ESM, or if a Logger appliance or ESM appliance becomes unresponsive.

To re-register destinations for one or more connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors to which you wish to assign a destination.
5. Click **Destinations**. The **Manage Destinations** wizard launches.
6. Review the dialog, then click **Next**.
7. Under **Choose an Option**, select **Re-register destinations**, and then click **Next**.
8. Follow the instructions in the wizard and click **Done** when complete.

Editing Destination Parameters

The following procedures describe how to edit destination parameters for a specific connector and how to edit destination parameters for multiple connectors.



Note: When enabling the demo CA for one or more connectors, use the **Certificate** button, instead of editing the ESM destination.

To edit destination parameters for a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to edit destination parameters. In the management panel, the **Connector** summary tab displays.
3. In the **Destinations** table, click next to the destination you want to edit to display the **Edit Destination Parameters** page.
4. Make your changes, then click **Next**.
5. Click **Done** when complete.

To edit destination parameters for multiple connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors for which you wish to edit destination parameters.
5. Click **Destinations**. The **Manage Destinations wizard** opens.
6. Review the dialog, then click **Next**.
7. Under **Choose an Option**, select **Edit a destination**, then click **Next**.
8. Follow the instructions in the wizard and click **Done** when complete.

Editing Destination Runtime Parameters

The runtime parameters for a destination enable you to specify advanced processing options such as batching, time correction, and bandwidth control. The parameters you can configure are listed in ["Destination Runtime Parameters " on page 334](#). The user interface automatically displays the parameters valid for a destination.

The following procedures describe how to edit the runtime parameters for a specific connector and how to edit the runtime parameters for multiple connectors at the same time.

To edit destination runtime parameters for a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click next to the destination whose runtime parameters you want to edit.
4. Under **Add Alternate Configurations**, click  next to the alternate configuration that you want to edit.

If you have not set up alternate configurations, click  next to the **Default**. For more information about alternate configurations, see ["Managing Alternate Configurations " on the next page](#).

5. Specify or update values for the listed parameters, then click **Save**.

To edit destination runtime parameters for *multiple* connectors at the same time:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all connectors for which you wish to edit destination runtime parameters.
5. Click **Runtime Parameters** to open the wizard.
6. Follow these steps in the wizard to edit the runtime parameters:
 - a. Select the destinations whose runtime parameters you want to modify.
 - b. Select the configurations to be affected (default or alternate configurations).
 - c. Select the group of parameters you want to modify (for example, batching, cache, network, processing).
 - d. Modify the parameters.

Managing Alternate Configurations

An *alternate configuration* is a set of runtime parameters that is used instead of the default configuration during a specified portion of every day. For example, you might want to specify different batching schemes (by severity or size) for different times of a day. You can define more than one alternate configuration per destination, and apply them to the destination for different time ranges during the day. For example, you can define a configuration for 8 a.m. to 5 p.m. time range and another configuration for the 5 p.m. to 8 a.m. time range.

By default, a configuration labeled **Default** is applied to a destination. Any subsequent configurations you define are labeled **Alternate#1**, **Alternate#2**, and so on. The default configuration is used if the time ranges specified for other alternate configurations do not span 24 hours. For example, if you specify an alternate configuration, **Alternate#1** that is effective from 7 a.m. to 8 p.m., the **Default** configuration is used from 8 p.m. to 7 a.m.

If you need to apply the same alternate configuration for multiple destinations, you need to define an alternate configuration (with the same settings) for each of those destinations.

Defining a New Alternate Configuration

The process of defining a new alternate configuration includes first defining the configuration, then editing it to specify the time range for which that configuration is effective.

To define an alternate configuration:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click .
4. Under **Add Alternate Configurations**, click **Add**.
5. Specify or update values for the listed parameters.
6. Click **Save**. If this is the first alternate configuration you defined, it is saved as Alternate#1. Subsequent configurations are saved as Alternate#2, Alternate#3, and so on.

To specify the effective time range for which the configuration you just defined, edit the configuration you just defined using the following procedure, "[Editing an Alternate Configuration](#)" below.

Editing an Alternate Configuration

In addition to editing an alternate configuration to change parameter values, you can edit it to specify the time range for which it is effective.

To edit an alternate configuration:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to edit destination runtime parameters. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click .
4. From the list of alternate configurations, select the alternate configuration that you want to edit, then click .
5. Specify or update values for the listed parameters, including the time range in the From Hour/To Hour.
6. Scroll down to the end of the page and click **Save**.

Editing Alternate Configurations in Bulk

If you need to update the same parameters in multiple alternate configurations, follow the procedure described in "[Editing Destination Runtime Parameters](#)" on page 151.

Sending a Command to a Destination

You can send a command to a connector destination.

To send a command to a destination on a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to send a command. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, in the **Destinations** table, click .
4. Select the command you want to run, then click **Next**.
5. Specify values for the parameters that the user interface displays, then click **Finish**.

Deleting a Connector

To delete one or more connectors:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where the connectors reside.
3. In the management panel, click the **Connectors** tab.
4. From the list of connectors, select all the connectors you want to delete.
5. Click **Delete**.
6. Click **OK** to confirm deletion.
7. Reboot the Connector Appliance or Logger system that each connector was associated with.



Note: You can also delete a specific connector from its **Connector** summary tab. Click  at the top of the tab to delete the connector.

Sending a Command to a Connector

You can send a command to a connector.

To send a command to a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to send a command. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, click **Connector Command**.
4. From the **Command Type** drop-down list, select the command you want to send to the connector, then click **Next**.

Running Logfu on a Connector

Run Logfu on a connector to parse ArcSight logs and generate an interactive visual representation of the information contained within the logs.

To run Logfu on a connector:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector to which you wish to run Logfu. In the management panel, the **Connector** summary tab displays.
3. On the **Connector** summary tab, click **Run Logfu**.
4. The Logfu progress window is displayed as system data logs are retrieved and analyzed. Data is then displayed by **Group**, **Field**, and **Chart**.
 - In the **Group** box, choose a data type to view. The **Group** box lists all connectors within the chosen container, plus many other data types, such as memory usage and transport rates.
 - Next, choose one of the **Group** box **data points**. Depending on which data point you chose, a list of fields appears in the **Field** box below.
 - Select a **field** to view. A graphic chart appears in the **Chart** box, providing rate and time information. The key at the bottom of the **Chart** box defines the data points mapped in the chart.
 - To choose a different data point for analysis, click **Reset Data**.
5. When complete, close the Logfu display window.

Changing the Network Interface Address for Events

Arcsight Management Center has multiple network interfaces. By default, the connector determines which network interface address is used for events displayed in the ArcSight Console or Logger, but typically uses eth0.

To use a specific network interface address for events, add the parameter `connector.network.interface.name` to the Connector's `agent.properties` file. For example, to use the IP address for eth1, specify the following parameter:

```
connector.network.interface.name=eth1
```

Developing FlexConnectors

FlexConnectors are custom, user-designed *SmartConnectors* that can read and parse information from third-party devices and map that information to ArcSight's event schema.

Arcsight Management Center provides a FlexConnector Development wizard that enables you to quickly and easily develop a FlexConnector by creating a parser file, and enables you to test and package your new FlexConnector before deploying it. The wizard generates regular expressions and provides event field mapping suggestions automatically so you do not need to be an expert in regular expression authoring, parser syntax, or ArcSight event schema.

Use the FlexConnector Development wizard to develop FlexConnectors for simple log files. For complex log files, use the FlexConnector SDK (available from the ArcSight Customer Support site)

The FlexConnector Development wizard supports Regex Files, Folder Follower, and Syslog (Daemon, File, Pipe) FlexConnectors only.

The FlexConnector Development wizard does not support the extra processors property or multiple sub-messages. If you need these features, use the FlexConnector SDK to create your FlexConnector.



Caution: A FlexConnector that you develop with the FlexConnector Development wizard might perform more slowly than an ArcSight *SmartConnector*.

To develop a FlexConnector:

1. Click **Node Management**.
2. In the navigation tree, browse to the container where you wish to develop the connector.
3. In the management panel, click the **Connectors** tab.
4. On the **Connectors** tab, in the Action drop-down, click **Edit FlexConnector**. The FlexConnector Development wizard is launched.
5. Provide the vendor and product name of the device for which you are creating a FlexConnector, then click **Next**.
6. Select the data source type, then click **Next**:
 - Select **Syslog** to create a Syslog FlexConnector to read events from Syslog messages.
 - Select **File** to create a FlexConnector to parse variable-format log files using regular expressions (ArcSight FlexConnector Regex File) or to parse variable-format log files in batch mode (ArcSight FlexConnector Folder Follower).

7. Upload a sample log file for the data source type you selected in the previous step, then click **Next**.
8. The wizard finds the first unparsed line in the log file, generates a regular expression to match and extract tokens from that line, and displays the suggested field mappings for each extracted token in the **Mappings table**.

FlexConnector Development Wizard

Enter regular expression corresponding to text		Lines Skipped: 0%	Lines Parsed: 0%
Text 2005 Aug 24 13:57:54 EDT -04:00 %SPAN TREE-6-PORTFWD: Port 3/16 state in VLAN 203 changed to forwarding			
Regex	(\d+ \S+ \d+:\d+:\d+ \S+ (\S+) %SPAN TREE-6-PORTFWD: Port (\S+) state in VLAN (\d+) changed to forwarding)	<input type="button" value="Recalculate"/>	<input type="button" value="Reset"/>
Mappings table			
Extracted Value	Type	Format	Event Field
1 2005 Aug 24 13:57:54	TimeStamp	yyyy MMM dd HH:mm:ss	deviceReceiptTime
2 3/16	String	String	deviceInboundInterface
3 203	Integer	String	deviceInboundInterface
Extra Mappings table			
Event Field	Value		
name	_stringConstant(SPAN)	<input type="button" value="X"/>	
Add Row			
Cancel Skip Line Skip To End Previous Next			



Note: The mappings are displayed in descending order of probability (based on ArcSight training data). You can change the mappings by selecting from the list.

The percentage of parsed lines in the file is shown in the top right of the panel. You can use this percentage to estimate where you are in the log file. The percentage of unparsed lines skipped in the file is also shown in the top right of the panel.

- To change the regular expression in the **Regex** box and recalculate the mappings, edit the expression and then click the **Recalculate** button. You can set the regular expression back to the suggested value by clicking the **Reset** button.
- Field mappings that do not correspond directly to the extracted tokens in the unparsed line of the log file are displayed in the Extra Mappings table. You can change the Event Field and provide a token operation. To add a new Event Field, click **Add Row**.

You can use extra mappings to:

- Remap an extracted token to a different Event Field in addition to the existing mapping. For example, you can add an Event Field with the value \$3 where \$3 is the third token in the list of suggested mappings.
- Map a modified token or combination of tokens to an Event Field. For example, you can add an Event Field with the value _operation(\$1,\$3).
- Map an Event Field to a constant string or integer. For example, you can add an Event Field with the value _stringConstant(constant).

For a list of the token operations used when tokens are mapped to ArcSight event fields, refer to the FlexConnector Developer's Guide (available from the ArcSight Customer Support site).

9. Click **Next** to save the mapping to the parser file and display the next unparsed line in the log file.

After all unparsed lines in the log file have corresponding regular expressions and mappings, the wizard displays the parser file for review.

10. Review the parser file and make changes, if necessary, directly in the Review Parser File panel.

11. Click **Next** to save and package the parser file.

12. Select how you want to deploy the FlexConnector:

- Select **Deploy parser to existing connector in container**, then click **Next** to use the parser file with an existing connector. Click **Done** to close the FlexConnector wizard and re-display the **Container** tab.



Note: The **Deploy parser to existing connector in container** option displays only if the container already contains a connector of the same type.

- Select **Add new connector to container**, and then click **Next** to add the parser as a new connector. Follow the steps to add the connector to the container.

You can share FlexConnectors with other users. See "[Sharing Connectors in ArcExchange](#)" below.

Editing FlexConnectors

After you have developed a FlexConnector with the FlexConnector wizard and have deployed it in a container, you can edit the FlexConnector to make changes to the parser file when needed.

The FlexConnector Edit wizard is available on the **Connectors** tab in the **Action** drop-down.

Click **Edit Connector** in the **Action** drop-down for the FlexConnector to open the wizard, then edit the parser file.



Caution: Only edit a FlexConnector that is created with the FlexConnector wizard. Editing manually-created FlexConnectors might produce unpredictable results.

Sharing Connectors in ArcExchange

You can share FlexConnectors and parser overrides with other users.

A FlexConnector is a custom connector that you define to gather security events from log files, databases, and other software and devices. You can share the following FlexConnector types:

- Syslog FlexConnectors (to read events from syslog messages)
- Log File FlexConnectors (to read fixed-format log files)
- Regular Expression Log File FlexConnectors (to read variable-format log files)
- Regular Expression Folder Follower FlexConnectors (to read variable-format log files recursively in a folder)
- Regular Expression Multiple Folder Follower FlexConnectors (to read events in real time or batch mode from multiple folders)
- XML FlexConnectors (to read events recursively from XML-based files in a folder)

A parser override is a file provided by ArcSight used to resolve an issue with the parser for a specific connector, or to support a newer version of a supported device where the log file format changed slightly or new event types were added. You can share parser overrides for all connector types that use a parser.

To share a FlexConnector or parser override, you need to package and upload it to ArcExchange on the ArcSight online community (Protect 724) or to your local machine. You can also download a FlexConnector or parser override that you need from ArcExchange or from your local machine and add it to a container.



Note: ArcExchange will not be able to reach the ArcSight Protect724 Community if access is attempted through a proxy server.

Packaging and Uploading Connectors

Before uploading your FlexConnector or parser override to Protect 724 or to your local computer, you need to package it into a zip file (called an AUP package) using the upload wizard.

A FlexConnector AUP package contains the connector properties file, categorization file, connector parameters, and a manifest file with all the metadata on the package required for successful deployment. Metadata includes information about the AUP package, such as the package type, connector type, connector description, and so on. You can create only one AUP package per connector per device type. You can package a FlexConnector in Basic or Advanced mode. In **Basic** mode:

- The wizard packages the FlexConnector properties file automatically. If the wizard finds more than one properties file, you are prompted to select the file you want to package.
- The wizard packages the categorization file automatically *only* if it can be determined based on the device vendor and product information found in the properties file.
- The wizard does not package connector parameters. You are prompted to configure the connector when it is downloaded and deployed.

In **Advanced** mode:

- The wizard packages the FlexConnector properties file automatically. If the wizard finds more than one properties file, you are prompted to select the file you want to package. (Same as Basic mode.)
- The wizard packages the categorization file automatically if it can be determined based on the device vendor and product information found in the properties file. If the categorization file cannot be determined, you are prompted to select the categorization file you want to package from the list of files found in the container.
- The wizard displays connector parameters so you can configure the ones you want to display and set the default values you want to provide during connector deployment (download). The parameters you do not configure for display are pre-configured with the current values and will not be displayed during connector deployment.

A parser override package contains the parser override properties file and the manifest file only.

Follow the steps below to package and upload a FlexConnector or parser override.



- To upload to ArcExchange, you must have a valid username and password for Protect 724.
- Make sure that you have configured network settings under **Administration > System Admin > Network** and that Arcsight Management Center can communicate with the Protect 724 server.

To package and upload a FlexConnector or parser override:

1. Click **Node Management**.
2. In the navigation tree, browse to the connector for which you wish to upload a package. In the management panel, the **Connector** summary tab is displayed.
3. On the **Connector** details page, click . The upload wizard is launched.
4. Click **Next** and follow the steps in the wizard to:
 - a. Select the type of AUP package you want to create for the selected connector. Arcsight Management Center scans the container and displays the relevant files that can be packaged.
 - b. For a FlexConnector, select **Basic** to create a default package or select **Advanced** to customize the package to meet your needs.
 - c. If the connector contains several properties files, you are prompted to select the properties file you want to package. Certain connectors, such as syslog connectors, can have more than one parser override folder, in this case, you are prompted to select the folder you want to package.
 - d. If you previously selected Advanced mode for a FlexConnector, and the categorization file cannot be determined, you are prompted to select the categorization file you want

to package from a list of files found in the container.



Note: Categorization files are not packaged for parser overrides.

- e. If you previously selected Advanced mode for a FlexConnector, select the configuration parameters you want to display when the connector is deployed and then provide default values for these parameters. Parameters you do not select are pre-configured with the current values.

If any advanced connector parameters were previously modified from their defaults, the wizard displays these parameters so that you can select which ones you want to be configured automatically during deployment.



Note: Configuration parameters are not displayed for parser overrides. If the connector has table parameters, they are not displayed during packaging. However, when the connector is downloaded to a container, you are prompted to provide values for all the table parameters.

- f. Provide a description of the AUP package and instructions on how to configure the device used by the connector.

- g. Provide the vendor, product, and version of the device used by the connector.

If the wizard can determine the vendor, product, and version of the device, the information is displayed in the fields provided. You can change the information to meet your needs.

- h. Upload the created AUP package to ArcExchange or to your local machine. You will require a username and password for the Micro Focus Community.

Downloading Connectors

You can download a FlexConnector or parser override that is available from ArcExchange on the Micro Focus Community or from your local computer. You download a FlexConnector or parser override directly to a container.

You can download only one FlexConnector per container using the download wizard. However, there is no limit to the number of parser overrides you can download to a container.



- When downloading a parser override to a container, the download wizard overwrites any existing parser override with the same name in the container without prompting for confirmation. To avoid overwriting an existing parser override, send a **Get Status** command to the existing parser override to check the parser information before you download a new one. For information on sending a Get Status command, refer to "[Sending a Command to a Connector](#)" on page 154.
- Always back up the container to the Backup Files repository before downloading a connector or parser override so you can revert to the previous configuration if the download produces unexpected results.

Follow the steps below to download a FlexConnector or parser override to a container.

To download to ArcExchange, you must have a valid username and password for Protect 724. Also, make sure that you have configured network settings under **Administration > System Admin > Network** and that the appliance can communicate with the Protect 724 server.

To download a FlexConnector or parser override:

- Click **Node Management**.
- In the navigation tree, browse to the host on which the container resides.
- In the management panel, click the **Containers** tab.
- From the list of containers, locate the container into which you want to download the connector. In the **Action** drop-down, select **Run FlexConnector Wizard**.
- Click **Next** and follow the steps in the wizard to:
 - Select whether you want to download the connector from ArcExchange on Protect 724 or from your local computer.
 - Select the AUP package you want to download.

On the Micro Focus Community, you can search for a parser override or FlexConnector AUP package using a keyword or a combination of keywords.



Note: You can only download a parser override package to a container that has a connector of the same type as the package. You can download only one FlexConnector per container using the download wizard. If the container already contains a FlexConnector of the same type as the one you want to download, you can replace the existing FlexConnector with the one you are downloading, but you cannot create a new one.

- For a FlexConnector, provide connector configuration parameters, if needed. Pre-configured and advanced parameters are deployed automatically with the values that were packaged; you are not prompted to configure these parameters. The configurable parameters are displayed with suggested defaults, which you can modify if

necessary. The table parameters are displayed with no configured values, you have to provide the values manually, as needed.

- d. Add or select a destination for the connector.

If you are downloading the connector to a container that has an existing connector of the same type, you are *not* prompted for a destination.

The wizard copies the properties and categorization files to the appropriate locations and also installs the zip file for the AUP package in the user/agent/deployedaups folder on Arcsight Management Center to keep track of the deployment history.

After a successful download, the container is restarted automatically.

Configuration Suggestions for Connector/Collector Types

The following table provides configuration suggestions for different types of connectors or Collectors.

Connector/Collector Type	Effects of Limited Usage
Syslog	<p>Due to the nature of UDP (the transport protocol typically used by Syslog), these Connectors/Collectors can potentially lose events if the configurable event rate is exceeded. This is because the connector delays processing to match the event rate configured, and while in this state, the UDP cache might fill and the operating system drops UDP messages.</p> <p>Note: Do not use the Limit CPU Usage option with these connectors because of the possibility of event loss.</p>
SNMP	<p>Similar to Syslog connectors, when the event rate is limited on SNMP connectors, they can potentially lose events. SNMP is also typically UDP-based and has the same issues as Syslog.</p>
Database	<p>Because connectors follow the database tables, limiting the event rate for database connectors can slow the operation of other connectors. The result can be an event backlog sufficient to delay the reporting of alerts by as much as minutes or hours. However, no events will be lost, unless the database tables are truncated. After the event burst is over, the connector might eventually catch up with the database if the event rate does not exceed the configured limit.</p>

Connector/Collector Type	Effects of Limited Usage
File	Similar to database connectors, file-based connectors <i>follow</i> files and limiting their event rates causes an event backlog. This can eventually force the connector to fall behind by as much as minutes or hours, depending on the actual event rate. The connectors might catch up if the event rate does not exceed the configured rate.
Asset Scanner	<p>All connectors on ArcSight Management Center run as a service (not as an application). Therefore, asset scanner connectors running on Connector Appliance are <i>not</i> supported in Interactive mode.</p> <p>To run the asset scanner connector in Interactive mode, install the connector on a standalone system and manage it as a software-based connector.</p>
Proprietary API	The behavior of these connectors depends on the particular API, (for example, OPSEC behaves differently than PostOffice and RDEP). But in most cases, there will be no event loss unless the internal buffers and queues of the API implementation fill up. These connectors work much like database or file connectors.

Included FlexConnectors

ArcSight Arcsight Management Center Connector Appliance includes these prototype FlexConnectors:

- ArcSight FlexConnector File
- ArcSight FlexConnector ID-based Database
- ArcSight FlexConnector Multiple Database
- ArcSight FlexConnector Regular Expression File
- ArcSight FlexConnector Regular Expression Folder File
- ArcSight FlexConnector Simple Network Management Protocol (SNMP)
- ArcSight FlexConnector Time-based Database
- ArcSight FlexConnector XML File

You can use these prototypes to develop your own FlexConnectors, and these can be shared with other users. Refer to ["Sharing Connectors in ArcExchange" on page 158](#).

For more information, consult the FlexConnector Developer's Guide, available from ArcSight Customer Support.

Configuring the Check Point OPSEC NG Connector

The Check Point FW-1/VPN-1 OPSEC NG connector can operate in clear channel or sslca mode.



Note: The following stipulations apply to configuring the Check Point OPSEC NG Connector:

- This procedure is supported only for ArcSight connector release 4.6.2 or later.
- A hostname is called an Application Object Name on Check Point. A password is a Communication Activation Key on Check Point.

To configure a connector to operate in sslca mode:

On the Check Point SmartDashboard:

1. Create an OPSEC Application Object using the Check Point SmartDashboard. You need to provide these parameters when creating the application object.

Parameter	Description
Name	A meaningful name for the application object you are creating; for example, ArcSightLea-1. This name is used to pull the OPSEC certificate.
Host	The hostname of the ArcSight Management Center system managing the connector.
Client Entities	Select LEA.
Secure Internal Communication	If a DN string is not present, initialize the communication by providing an activation key. The activation key is used when the certificate is pulled. This is the SIC Name. Click Communication > Initialize .

After the object is created, note down the following information, which you will need to provide when continuing configuration.

- *SIC Name:* DN string that you obtain after initializing communication as described below.
 - *SIC Entity Name:* Double-click the Check Point Gateway name in the SmartDashboard to view its general properties. The SIC Entity Name is the SIC string configured in the general properties window.
 - Check Point IP address or hostname.
2. Pull the Check Point certificate.
- To do so, run the `Pull OPSEC Certificate` command on the container to which you are adding the connector. For detailed information about running a command on a container, see "["Sending a Command to a Container" on page 128](#)". You need to provide this information when running the command:

Parameter	Description
Server hostname or IP address	The name or IP address of the Check Point server.
Application object name	The OPSEC Application object name you specified in the previous step. This parameter is case sensitive.
Password	The activation key you entered when creating the OPSEC application object in the previous step.

If the certificate is pulled successfully, a message similar to this is displayed:

```
OPSEC SIC name (CN=ArcSightLea-1,0=cpfw1.5ad8cn) was retrieved and stored
in /opt/arcsight/connectors/<container
name>/current/user/agent/checkpoint/<name>. Certificate was created
successfully and written to "/opt/arcsight/connectors/<container
name>/current/user/agent/checkpoint/ArcSightLea-1.opsec.p12".
```

Note down the OPSEC SIC Name (CN=ArcSightLea-1,0=cpfw1.5ad8cn in the above example) and the file name (ArcSightLea-1.opsec.p12 in the above example).



Tip: If the certificate is not pulled successfully, check to ensure that the Application object name you specified is correct (including the case) and the container on which you are running the command is up and running.

3. Install Policy on the LEA client for the Check Point Gateway using the SmartDashboard.

On Connector Appliance:

1. Add a Check Point connector by following instructions described in "[Adding a Connector](#)" on page 141. You need to provide the following information.

Parameters	Values to input
Type	Check Point FW-1/VPN-1 OPSEC NG
Connection Type	SSLCA

Parameters	Values to input
Connector Table Parameters	<p>Server IP: The IP address of the Check Point server.</p> <p>Server Port: The port on the server that listens for SSLCA connections. Use the default value 18184.</p> <p>OPSEC SIC Name: The name you noted in "Create an OPSEC Application Object using the Check Point SmartDashboard. You need to provide these parameters when creating the application object." on page 165.</p> <p>OPSEC SSLCA File: The name you noted after pulling the certificate in "Pull the Check Point certificate." on page 165.</p> <p>OPSEC Entity SIC Name: The name you noted in "Create an OPSEC Application Object using the Check Point SmartDashboard. You need to provide these parameters when creating the application object." on page 165.</p>

2. An error similar to the following is displayed.

-1:[X] Unable to connect to the Lea Server[10.0.101.185] -1:1 connection test failed!

Select the **Ignore warnings** check box, then click **Next**.

3. Continue to configure the rest of the connector as described under ["Adding a Connector" on page 141](#).

Adding the MS SQL Server JDBC Driver

When you install and configure database connectors that use Microsoft SQL Server as the database, a JDBC driver is required. This driver does not ship pre-installed; you need to install it before configuring database connectors on the appliance.

To install a JDBC Driver:

1. From the Microsoft web site, download the MS SQL Server JDBC Driver to a computer that can access Arcsight Management Center.
2. Run the setup program to install the driver.
3. Follow the instructions in ["Uploading Files to a Repository" on page 258](#) to add the `sqljdbc.jar` file.



Tip: The name of the jar file may be different from that of some JDBC driver versions. Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database.

The new driver file is added to the repository, as shown in the following example.

After you have installed the JDBC driver, you need to upload the driver file to the containers that will hold the SQL Server database Connectors. Follow the instructions in ["Uploading Files to a Repository" on page 258](#).

After the driver file has been uploaded to a container, follow the instructions in "[Adding a Connector](#)" on page 141 to add a connector that requires a JDBC driver.

Adding the MySQL JDBC Driver

When you install and configure database connectors that use MySQL as the database, a JDBC driver is required. This driver does not ship pre-installed. Install it before configuring database connectors on the appliance.

To install a JDBC Driver:

1. From the MySQL web site, download the MySQL JDBC Driver to a computer that can access Arcsight Management Center.
<http://dev.mysql.com/downloads/connector/j/5.0.html>
2. Extract the driver.
3. Follow the instructions in "[Uploading Files to a Repository](#)" on page 258 to add the mysql-connector-java-x.x.x-bin.jar file. The new driver file is added to the repository.

After you have installed the JDBC driver, you need to upload the driver file to the containers that will hold the MySQL database Connectors. Follow the instructions in "[Uploading Files to a Repository](#)" on page 258.

After the driver file has been uploaded to a container, follow the instructions in "[Adding a Connector](#)" on page 141 to add a connector that requires a JDBC driver.



Note: For both **Adding the MS SQL Server JDBC Driver** and **Adding the MySQL JDBC Driver** cases, make sure to use the default path /lib when uploading the JDBC driver for on-board connector installation. For Instant Connector Deployment installation use user/agent/lib.

Chapter 7: Managing Configurations

A *configuration* is a group of related appliance or software settings and their associated values, which applies to one or more node types. A configuration created for a node can be pushed to nodes of the same type managed by Arcsight Management Center, assuring uniformity across a group of nodes.

Configurations come in these kinds:

- A *subscriber* configuration is for the routine management of multiple managed ArcSight products. You can easily assign values to, propagate, and maintain the same settings across multiple nodes of the same type, including connectors, Collectors, Connector Appliances, Loggers, or other ArcMCs.
- A *initial* configuration is for the rapid, uniform setup of multiple ArcSight Loggers (only). Use an initial configuration to expedite the initial deployment of ArcSight Loggers to a production environment.

Configuration management tasks include:

- *Configuration Creation*: A configuration for a node type can be created (as well as edited or deleted) in Arcsight Management Center.
- *Configuration Import*: A configuration can be created directly on a managed node, exported, then imported into Arcsight Management Center for sharing with nodes of the same type.
- *Configuration Push*: A configuration can be *pushed* from ArcMC to managed nodes. This copies the configuration from ArcMC and changes the settings on each destination node.
- *Subscriptions*: Managed nodes can be *subscribed* to a subscriber configuration, so they can receive a new or updated configuration pushed from Arcsight Management Center.
- *Compliance Checks*: Check whether the settings and their values on a managed node match the ones for a configuration type specified in Arcsight Management Center. If so, the node is said to be in *compliance* with the configuration.
- *Comparisons*: Compare two configurations of the same type quickly, with a field by field breakdown of each setting, its value, and any differences. You can compare the values of a configuration on a subscriber node to the values of the baseline or reference configuration on an ArcMC which manages it. You can also compare two configurations of the same type on a single ArcMC.

For example, a typical workflow for a subscriber configuration might work as follows: you can create a suitable DNS configuration for an appliance, specifying primary DNS server, secondary DNS server, and search domains for the appliance. (See "["Destination Configuration Types" on page 191](#).) You can then push your DNS configuration to subscribing appliances, and so ensure that DNS settings for all subscribed nodes are configured identically with a single action.

If you later updated the configuration to use a new primary DNS server, you could push the new configuration to all subscribers, and all of them would be updated for the new DNS server with one action.

At any time, you could verify any managed node's compliance with the configuration to determine if its settings were assigned the desired values.

The following topics are discussed here.

Generator ID Manager

Every event generated by an ArcSight component will have a unique Global Event ID. This will help in identifying the events in case the same event is seen in multiple ArcSight components like Logger, ESM, and Transformation Hub.

- "[Generator ID Management](#)" below
- "[Setting Up Generator ID Management](#)" below
- "[Getting Generator ID for Non-managed Nodes](#)" below
- "[Setting Generator IDs on Managed Nodes](#)" on the next page

Generator ID Management

This feature allows users to generate an ID to assign it to a non-managed product. Each assigned Generator ID should be unique for the ArcSight environment.

Setting Up Generator ID Management

1. On the top right side of the screen, click **Generator ID Manager**.
2. Select **Yes** to enable Generator ID Management in ArcMC.
3. Specify the numeric values between 1 and 16383 for the Generator ID range (**Start** and **End**) and click Save. ArcMC will set the generator ids for itself if not set already.
4. Restart all ArcMC processes to continue.

Getting Generator ID for Non-managed Nodes

1. Go to **Configuration Management** and select **Generator ID Management**.
2. Click **Assign a Generator ID**.
3. Select the **Event Producer Type**. Other fields are optional, click **Assign**.

4. Copy the ID by clicking the copy to clipboard icon and Click **OK**. A list of generated IDs will be displayed.

Setting Generator IDs on Managed Nodes

ArcMC will automatically set the generator IDs for each managed node when performing the following actions, if ArcMC is enabled as a Generator ID Manager:

Connectors

- Adding a Host version 7.11 or later.
- Scanning a Host
- Adding a Connector to a Container
- Connector upgrade to version 7.11 or later.
- Instant Deployment



Note: Multiple host deployment is disabled when the Generator ID Manager flag is enabled.

Logger

- Remote Upgrade: Upgrade from and to Logger version 6.7 or later.
- Adding a Host version 6.7 or later.

ArcMC

- Remote Upgrade: Upgrade from and to ArcMC version 2.9 or later.
- Adding a Host version 2.9 or later.
- Scanning a Host.
- Setting the Generator IDs on localhost by enabling the Generator ID Manager.

Transformation Hub

- Deploy CTH

Configuration Management

To create or manage configurations, on the menu bar, click **Configuration Management**. To manage a specific configuration type, select the configuration type from the sub-menu.

For example, to access subscriber configurations for Loggers, click **Configuration Management > Subscriber Configurations > Logger Configurations**.

The Configurations Table

The **Configurations** table lists all currently available subscriber configurations in ArcSight Management Center. Each listed configuration, whether it was created in ArcSight Management Center or imported from an existing node, is considered the baseline copy of that configuration, for pushing to managed nodes. The table includes the following columns.

- **Name:** The name of the configuration.
- **Type:** The type of configuration.
- **Last Edited By:** The most recent user to edit the configuration.
- **Compliance:** An aggregation of the status of the individual subscribers to that configuration.
 - *Compliant* indicates that all subscribers are in compliance.
 - *Non-Compliant* indicates that at least one subscriber is out of compliance.
 - *Unknown* indicates that the compliance status for one or more subscribers cannot be determined (for example, because connectivity to one or more subscribers is not available).



Tip: You can check the individual compliance of each subscriber on the **Subscribers** tab.

Click any column header to sort the **Configurations** table by that column.

To view the details of any configuration, click its name in the list. The **Details** and **Subscribers** tabs will display additional information.



Tip: To select multiple items from any list, Shift+Click or Ctrl+Click while selecting.

The Details Tab

The **Details** tab shows the specifics of the configuration, including any configured attributes and their values.

Configuration Name

Each configuration has a unique name. A configuration may be up to 255 characters in length.

General

General details describe the basics of the configuration, as follows:

- **Configuration Type:** The type of the configuration. For details of configuration types, see "[Subscriber Configuration Types](#)" on page 184.

- **Last Edited By:** The most recent user to edit the configuration.

Properties

A *property* is a group of one or more settings for the configuration. For example, for the NTP Server configuration, the property includes two settings: Enable as NTP Server (a Boolean value indicating whether to enable the product as an NTP server), and NTP Servers (a list of NTP servers).

The specific parameters included in each property are pre-defined for each configuration type. ArcSight Management Center prompts for values of each setting when the property is selected. Each parameter must be assigned a valid value corresponding to its data type. For instance, if the data type is integer, you must specify an integer value. A red asterisk (*) indicates a required parameter.

List Configurations

A configuration type that can include more than one property is known as a *list configuration*. A list configuration represents a configuration with multiple instances of data values of the same kind. Each instance is known as a *property*.

For example, the Connector Map File configuration could include information on multiple map files. Each Property would represent a different map file (with different values for file path and content).



Note: A pushed list configuration will override any existing configuration of the same type on the managed node. To *append* data to an existing configuration, use the bulk management tools (**Set Configuration**)

For a description of supported configuration types, the parameters associated with each type, and their data types, see "[The Configurations Table](#)" on the previous page.

The Subscribers Tab

The **Subscribers** list shows all managed nodes currently eligible to receive the configuration. (The list is empty if no hosts have been added yet.)

The tab includes these operations buttons:

Add Subscribers	Adds subscribers to the existing configuration.
Push	Pushes the configuration to one or more selected subscribers.
Check Compliance	Checks the compliance of all subscribers with the baseline configuration.
Unsubscribe	Removes one or more selected subscribers from the subscriber list.

The list includes the following columns:

- **Path:** The path of the subscribing node, consisting of location/hostname/node type.
- **Type:** The type of subscribing node.
- **Last Pushed At:** The time and date of the most recent push to the subscriber.
- **Last Push Status:** The status of the most recent push to the subscriber.
 - *Succeeded:* The configuration push was successful.
 - *Failed:* Hover over the link to determine the reason for the push failure. An error message is displayed to help in remediation of the issue. For more information, see "[Push Remediation](#)" on page 181.
 - *Unknown:* Initial status before the subscriber has received any pushes.
- **Last Compliance Check:** The date and time of the most recent compliance check.
- **Compliance:** Whether the node is in compliance with the configuration.
 - *Compliant* indicates the node is in compliance. The values for *all* settings associated with the configuration type match the values from the configuration.
 - *Non-Compliant* indicates the node is out of compliance. One or more values for the settings associated with the configuration type do not match the values from the configuration. Hover over *No* to show the cause of the node's non-compliance.
 - *Unknown* indicates either that the node's compliance could not be determined at the time of the most recent compliance check, or that the node has not yet undergone a compliance check.

Non-Compliance Reports

You can determine why a compliance status is Non-Compliant.

For a compliance status of *Non-Compliant*, click the status to display the **Configuration Comparison** dialog, which compares all setting values for the configuration on ArcMC and on the managed node.

Click **Push Configuration** to push the configuration to the managed node in order to make it Compliant.

Creating a Subscriber Configuration

You can create a subscriber configuration for pushing to any subscribed nodes.



Note: The following subscriber configuration types cannot be created in ArcMC, but can only be imported from managed nodes:

- Logger Storage Group
- Logger Filter
- Logger ESM Forwarder, Connector Forwarder, TCP Forwarder, UDP Forwarder
- Authentication External

For more information on importing a configuration from a managed node, see "[Importing a Subscriber Configuration](#)" on the next page.

To create a configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations**.



Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. Under **Configurations**, click **New**.
3. On the **Details** tab, select a configuration type from the **Configuration Type** drop-down list. (Only the appropriate configuration types are shown in the drop-down list.)
4. In **Configuration Name**, specify a name for the configuration. (Configuration names must be unique and may be up to 255 characters in length.)
5. Specify values for any required parameters, which are indicated with a red asterisk (*).



Note: For a description of valid parameters for each configuration type, and the data type associated with each, see "[Subscriber Configuration Types](#)" on page 184.

6. Optionally, add values for any optional parameters.
7. Optionally, to add an additional property for a list configuration: click **Add Property**, then specify values for the prompted parameters. Repeat adding properties as needed to completely define the configuration.
8. Click **Save**.

Editing a Subscriber Configuration

You can modify or delete values for a subscriber configuration. (You may not edit a configuration currently being pushed.)

To edit a configuration:

1. Click **Configuration Management > Subscriber Configurations > All Configurations**.
-  **Tip:** To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.
2. From the **Configurations** table, click the name of the configuration to be edited.
3. On the **Details** tab, click **Edit**.
 - Edit the general settings as needed.
 - Optionally, to add an additional property for a list property, click **Add Property**, then specify values for the prompted parameters. Repeat adding properties as needed to completely define the configuration.
 - Optionally, to delete a property from the configuration, click **Delete Property**.
4. When complete, click **Save**. After saving, if the configuration has any subscribers, you are prompted to push the updated configuration to the subscribers.

Deleting a Subscriber Configuration

A deleted subscriber configuration is no longer available for pushes to subscribers. You may not delete a configuration currently being pushed.

To delete a subscriber configuration:

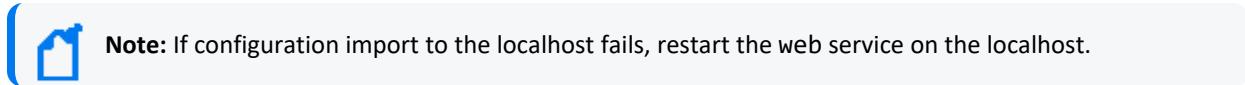
1. Click **Configuration Management > Subscriber Configurations > All Configurations**.
-  **Tip:** To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.
2. From the **Configurations** table, select one or more configurations to be deleted.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Importing a Subscriber Configuration

A subscriber configuration created on a managed node may be imported into ArcMC, for editing and pushing to other nodes of the same type.

For example, you can define a configuration on a managed Connector Appliance, then import the configuration into ArcMC. The imported configuration may then be edited and pushed to

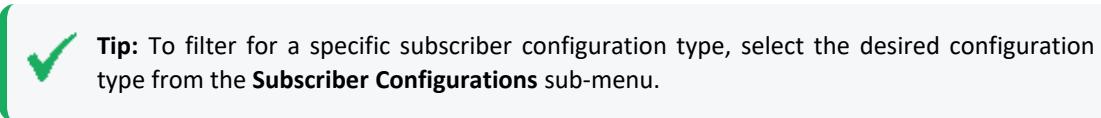
other managed Connector Appliances, just the same as you would with a configuration you originally created in ArcMC.



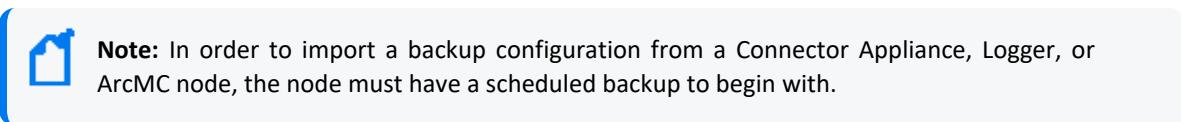
Note: If configuration import to the localhost fails, restart the web service on the localhost.

To import a subscriber configuration from a managed node:

1. Click **Configuration Management > Subscriber Configurations > All Configurations**.



- Tip:** To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.
2. Under **Configurations**, click **Import**.
 3. On the **Choose a Node** dialog, select the node from which you wish to import the configuration.
 4. Click **Continue**.
 5. On the **Import Configuration** dialog:
 - a. Select a configuration type for the imported configuration from the **Type** drop-down list. (The entries in the list depend on the configuration types which apply to the node chosen in Step 3.)
 - b. In **Name**, specify a name for the imported configuration.
 6. Click **Import**. The configuration is imported into ArcMC and is shown in the **Configurations** table.



Note: In order to import a backup configuration from a Connector Appliance, Logger, or ArcMC node, the node must have a scheduled backup to begin with.

Managing Subscribers

A *subscriber* is a managed node to which a configuration may be pushed. A subscriber to which a configuration is pushed will receive and process the pushed configuration and apply it to the managed node, so that the managed node's settings are the same as the settings specified in the configuration.

Each node can subscribe to *only one* configuration of each configuration type.

For example, a Logger appliance could subscribe to one Logger Storage Group configuration, but the same appliance could also subscribe to a Logger Filter configuration as well as a Logger Transport Receiver configuration.

Viewing Subscribers

To view subscribers for a configuration:

1. Click **Configuration Management > All Configurations**.
2. From the list of configurations, locate the configuration for which you wish to view subscribers.
3. Click the name of the configuration.
4. Click the **Subscribers** tab. The current subscribers are displayed.

Adding a Subscriber

A subscriber (that is, a subscribed node) can receive a pushed configuration.

To subscribe a node to a configuration:

1. Click **Configuration Management > All Subscriber Configurations**.



Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, click the name of the configuration to which you wish to add subscribers.
 3. Click the **Subscribers** tab.
 4. Click **Add Subscribers**.
 5. On the **Add Subscribers** dialog, select a node to add as a subscriber. The list of potential subscribers is determined by the selected configuration type. To select multiple nodes for subscription, Ctrl+Click each node.
-
- Note:** A node may only subscribe to one configuration of each type; for example, one DNS configuration.
- If you attempt to add a subscriber which is already subscribed to a configuration of the same type, the following message is displayed: *No available subscribers have been found for the selected configuration.*
6. Click **Add Subscribers**.
 7. Click **OK** to confirm completion. The subscriber is added to the recipients for the configuration.

Unsubscribing a Subscriber

After being unsubscribed, a node can no longer receive a pushed configuration.

To remove a subscriber from a configuration:

1. Click **Configuration Management > All Subscriber Configurations**.



Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, click the name of the configuration from which you wish to remove subscribers.
3. Click the **Subscribers** tab.
4. Select one or more subscriber from the list of subscribers.
5. Click **Unsubscribe**.
6. Click **OK** to confirm. The selected subscribers are unsubscribed.

Pushing a Subscriber Configuration

A pushed subscriber configuration synchronizes the configuration from ArcMC to all or a selection of the configuration's subscribers. Pushing must be performed manually.

When selecting subscribers, only valid potential subscribers for the configuration are shown. For example, if pushing a Logger configuration, which only applies to Loggers, only managed Loggers would be shown as potential subscribers, not Connector Appliances or ArcMCs.



Note: If a configuration push to the localhost fails, restart the web service on the localhost.

To push a subscriber configuration to all subscribers:

1. Select **Configuration Management > All Subscriber Configurations**.



Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, select a configuration to be pushed.
3. Click **Push**.

4. Click **Yes** to confirm the push. The configuration is pushed to all subscribers of the selected configuration. A compliance check is automatically performed on each subscriber.

To push a subscriber configuration to selected subscribers:

1. Select **Configuration Management > Subscriber Configurations > All Configurations**.



Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. From the **Configurations** table, select a configuration to be pushed, and click the name of the configuration.
3. On the **Configuration Details and Subscribers** page, click the **Subscribers** tab.
4. On the **Subscribers** tab, select one or more subscribers to which to push the configuration.
5. Click **Push**.
6. Click **Yes** to confirm the push. The configuration is pushed to the selected subscribers. A compliance check is automatically performed on each recipient.

Push Validation

During a push to subscribers, the configuration is automatically validated by ArcSight Management Center. Validation ensures that a pushed configuration contains appropriate, meaningful values for all settings. If any configuration values are found to be invalid, the push will fail, and an error message will be returned. Hover over the subscriber's entry on the **Subscribers** tab, in the **Push Status** column, to show the cause of the failed push. In addition, a compliance check is automatically performed after the push.

Common Causes for Push Failure

A push to a subscriber may fail for any number of reasons. These may include:

- **Validation Failure:** A push with invalid content will fail. Verify that your configuration includes valid setting values for the configuration type.
- **Lack of Connectivity:** Network or system issues can cause disrupt connectivity to a subscriber. Verify connectivity with the subscriber.
- **Agent Not Running on Host :** Verify that the ArcMC Agent process is active on the subscribing node. (This does not apply to connectors or Collectors, which do not require the Agent.)
- **Privileges on Subscribing Host:** In order to push a subscription, the ArcSight Management Center user (specified by the user credentials) must have privileges to view, edit, or delete

configuration settings on the subscriber nodes.

- **Expired License:** An expired host license will cause a push to the host to fail.

Push Remediation

If a push to a subscriber fails, you may be able to remedy the failure by following these steps:

1. Select the configuration from the **Configurations** table.
2. Click the **Subscribers** tab and choose the subscriber to which the push failed.
3. The **Last Push Status** will show *Failed*. Hover over this link to view the error message associated with the push failure.

After viewing the error message, you can take the appropriate steps on the managed node to address the issue. Resolution may require direct or remote access to the node outside of ArcSight Management Center.

After the issue is resolved, you can retry the failed configuration push.

Checking Subscriber Compliance

A subscribed node is in *compliance* with a configuration if the settings for the node match those assigned to the configuration in ArcSight Management Center.

The configuration listed in the managing ArcSight Management Center is considered the baseline copy of the configuration.

For example, you create an SMTP configuration in ArcSight Management Center named *Sample SMTP Configuration*, with these values assigned:

- Primary SMTP Server: *Mailserver1*
- Secondary SMTP Server: *Mailserver2*
- Outgoing Email Address: *admin@example.com*

A node would be in compliance with this configuration if the values for its primary and secondary SMTP servers, and outgoing email address, matched the values in *Sample SMTP Configuration*.

If any one of these values were different (for example, if a node had a primary SMTP Server of *CorporateMail1*) the node would be out of compliance.

You can manually check the compliance of all subscribers to a configuration.

To manually check subscriber compliance for a configuration:

1. Click Configuration Management > Subscriber Configurations > All Configurations.



Tip: To filter for a specific subscriber configuration type, select the desired configuration type from the **Subscriber Configurations** sub-menu.

2. In the **Configurations** table, select the configuration to be checked for compliance.
3. Click **Check Compliance**. All subscribers to the selected configuration are checked for compliance.
 - On the **Configurations** table, the **Compliance** column shows the aggregated compliance of all subscribers.
 - On the **Subscribers** tab for the configuration:
 - The **Last Compliance Check** column is updated to show the most recent check.



Automatic compliance checks will run every 12 hours. So this will be the date and time of the latest automatic check.

- The **Compliance** column indicates the individual compliance of each node.

Comparing Configurations

You can compare two configurations of the same type to verify whether they contain the same settings. The following two comparisons are possible:

- **Comparing two configurations on a single ArcMC.** You can compare two configurations of the same type on a single ArcMC. For example, you could compare the settings for two different SMTP configurations.
- **Comparing the configuration on a subscriber to the same configuration on its managing ArcMC.** You can quickly check to see how the settings for a configuration on a subscribing node differs from the same configuration on its managing ArcMC.

To compare two configurations of the same type on one ArcMC:

1. Click Configuration Management.
2. Select All Configurations.
3. In the list of configurations, select two configurations.
4. Click Compare.

The **Configuration Comparison** dialog shows each setting for the configuration and the current value for each compared item in the **Status** column.

To print the comparison as a PDF report, click **Export to PDF**.

To compare the configuration on a subscriber to the same configuration on its managing ArcMC:

1. Click **Configuration Management**.
2. Select **All Configurations**.
3. In the configurations list, select the configuration you wish to compare between ArcMC and the subscriber.
4. Under **Configuration Details & Subscribers**, click the **Subscribers** tab.
5. In the **Compliance** column, click the status link.

The **Configuration Comparison** dialog shows each setting for the configuration and the current value for each compared item.

Optionally, if the subscriber is Non-compliant with the configuration on its managing ArcMC, click **Push Configuration** to push the configuration to the subscriber (which will make it compliant).

To export the comparison as a PDF report, click **Export to PDF**.

Configuration Management Best Practices

Configuration management is a powerful tool for managing multiple ArcSight products. You can easily implement configurations across managed products with just a few actions.

- **Node management versus Configuration Management:** Use ArcSight Management Center's node management tools for the administration of individual nodes and their day-to-day operations. However, for consistent and wide-ranging changes to the data or settings of managed nodes, use configuration management if the appropriate configuration exists. For example, to change DNS settings across multiple managed nodes, it would be faster and easier to create the configuration in ArcMC and push it out to managed nodes, than to individually change the settings across multiple devices.
- **Implementing data settings across multiple appliances or products in bulk:** Use the Bulk Management (**Set Configuration**) tools to implement data settings across multiple appliances or products. For example, you can quickly configure all of your appliances to use the same hardware settings (such as SMTP server) with a single platform (in this case, SMTP configuration applied to managed nodes. (Pushing will overwrite any existing data.)
- **Compliance versus Non-Compliance:** If configuration compliance is not relevant to your configuration management, use the bulk management tools under Node Management to manage your node settings. A bulk push can also be performed under Configuration Management.

Subscriber Configuration Types

The following section lists the available subscriber configuration types, the parameters associated with each, their data types, and a brief description of what the parameter represents. When assigning values to parameters:

- Each parameter's value must be of the data type indicated (for example, the String data type indicates that you must specify a string for the value).
- *Required* parameters are marked with an asterisk (*) and must be assigned a value. A configuration missing a value for a required parameter cannot be saved or pushed.
- *Read-only* parameters cannot be edited in ArcSight Management Center.
- For security reasons, all password parameters are displayed with obfuscation.



Tip: For details of each entry field, in edit mode, hover over the field label and view its descriptive tooltip.

Connector Configuration Types

Connector configurations set values for settings on containers, connectors, or Collectors. The available connector configuration types are listed here.

BlueCoat Connector Configuration

A BlueCoat Connector configuration defines settings for one or more BlueCoat connectors. The configuration is only pushed to a target if a BlueCoat connector exists.

To push a BlueCoat Connector configuration from to a managed node that already has values defined for all fields listed here, then specify values for all fields in the pushed configuration. Default values may be used if necessary.

BlueCoat Connector Configuration Parameters

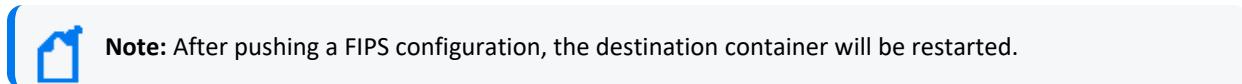
Parameter	Data Type	Description
Row Number*	Integer	Row number of the table parameter to which the configuration is pushed.
Log File Wildcard*	String	Log file wildcard.

BlueCoat Connector Configuration Parameters, continued

Parameter	Data Type	Description
Log File Type*	String	Log file type. Valid values are: <ul style="list-style-type: none">• main• im• ssl• streaming
Processing Mode	String	Processing mode. Valid values are Batch and Real time.
Post-Processing Mode	String	Post-processing mode. Valid values are: <ul style="list-style-type: none">• RenameFileInTheSame Directory• PersistFile• DeleteFile
Mode Options	String	Mode options. Required if Post-Processing Mode is chosen as RenameFileInTheSame Directory
Processing Threshold	Integer	Interval, in hours, after which the log file will be marked as processed.
Processing Limit	Integer	Number of files that can be read in the directory at the same time.

FIPS Configuration

A FIPS configuration enables or disables FIPS mode on a container.



FIPS Configuration Parameters

Parameter	Data Type	Description
Enabled*	Boolean	If Yes, FIPS is enabled on the container.

Map File Configuration

A map file configuration defines the path and content of one or more container map files. Each Path/Content pair represents a single map file. To include multiple files, add multiple Properties to the configuration.

- When pushed, the configuration deletes all *.properties files in the \map directory on the target, then adds the list of map files to the target, replacing any existing map files.
- If the configuration contains an empty list, all *.properties files are deleted.



Note: If importing and uploading a map configuration file, convert the downloaded CSV file into a .properties file before uploading.

Uploading Map Files Larger Than 1 MB

- a. Log in to the CDF Management Portal. See [Accessing the CDF Management Portal](#) for more information.
- b. From the left menu select **Deployment > Deployments**.
- c. Click ... (**Browse**) on the far right and choose **Reconfigure**. A new screen will open in a separate tab.
- d. Select the **Fusion** tab
- e. Scroll down to the **ArcMC Configuration** section, and specify the desired value for the **Maximum In-memory Buffer Size** parameter.
- f. Click **Save**. The ArcMC pod will be restarted.

If `<install_dir>/userdata/arcmc/logger.properties` does not exist, then create one in a text editor. This file must be owned by a non-root user. For an ArcMC appliance, use the 'arcsgit' user, and for software ArcMC, use the non-root account used to install the ArcMC.

Modify the `<install_dir>/userdata/arcmc/logger.properties` by adding:

```
configuration.max.inmemory.mb=2
```



Note: $2097152 = 2 * 1024 * 1024$

After adding the previous line, owner and permissions need to be changed:

```
chown <non-root user>:<non-root user> logger.properties
chmod 660 logger.properties
```

Finally, restart the web process after making any edits to `logger.properties`.

Map File Configuration Parameters

Parameter	Data Type	Description
Path*	String	Path to the map file.
Content*	String	Content of the map file.

Parser Override Configuration

A parser override configuration defines the path and content of one or more container parser override files.

Each Path/Content pair represents a single parser override file. To include multiple files, add multiple Properties to the configuration.

- When pushed, the configuration deletes all *.properties files in the \fcp directory on the target, then adds the list of parser override files to the target, replacing any existing parser override files.
- If the configuration contains an empty list, all *.properties files are deleted.

Parser Override Configuration Parameters

Parameter	Data Type	Description
Path*	String	Path to the parser override file.
Content*	String	Content of the parser file.

Syslog Connector Configuration

A Syslog connector configuration defines values for one or more Syslog connectors. The configuration is only pushed to the target node if a Syslog connector exists.

Syslog Connector Configuration Parameters

Parameter	Data Type	Description
Port*	Integer	Syslog connector port.
Protocol*	Enum	Protocol of the syslog connector (either UDP or Raw TCP).

Windows Unified Connector (WUC) External Parameters Configuration

A WUC External Parameters connector configuration defines the external parameters for one or more WUC connectors. The configuration is only pushed to the target node if a WUC connector exists.

Limitations to WUC External Parameters Configurations

A WUC external parameters configuration has the following limitations:

- Domain user password is not supported as a WUC configuration parameter. Instead, domain user password must be managed individually for each WUC host.
- WUC connectors are not FIPS-compliant.
- If you wish to push a WUC configuration from ArcMC to a managed node that already has values defined for all fields listed here, then you must specify values for all fields in the pushed configuration. Default values may be used if necessary.

WUC External Parameters Configuration Parameters

Parameter	Data Type	Description
Domain Name*	String	Windows domain name.
Domain User*	String	Windows domain user name.
Active Directory Host	String	Hostname for the Active Directory server, if one is used. <ul style="list-style-type: none"> ◦ If specified, values for User, User Password, Base DN, Protocol, and Port must be specified in subsequent entries.
Active Directory Use	String	Username for the AD server. <ul style="list-style-type: none"> ◦ Required if a value is provided for Active Directory Host.
Active Directory User Password	String	Password for AD server. <ul style="list-style-type: none"> ◦ Required if a value is provided for Active Directory Host.
Active Directory Base DN	String	Base DN of the Active Directory. <ul style="list-style-type: none"> ◦ Required if a value is provided for Active Directory Host.
Active Directory Protocol	String	Protocol for Active Directory. <ul style="list-style-type: none"> ◦ Required if a value is provided for Active Directory Host.
Active Directory Port	String	Port for Active Directory. <ul style="list-style-type: none"> ◦ Required if a value is provided for Active Directory Host.
Global Catalog Server	String	Hostname for the Global Catalog server, if one is used. <ul style="list-style-type: none"> ◦ If specified, values for User Name, User Password, and Base DN must be specified in subsequent entries.
Global Catalog User Name	String	Username for the GC server. <ul style="list-style-type: none"> ◦ Required if a value is provided for Global Catalog server.
Global Catalog User Password	String	Password for the GC server. <ul style="list-style-type: none"> ◦ Required if a value is provided for Global Catalog server.
Global Catalog Base DN	String	Base DN of the GC server. <ul style="list-style-type: none"> ◦ Required if a value is provided for Global Catalog server.
WEF Collection*	String	Indicates if Windows Event Format collection is enabled. Valid values are: <ul style="list-style-type: none"> ◦ Disabled ◦ Enabled (use Active Directory for sources) ◦ Enabled (do not use Active Directory for sources) <p>Note: WEF collection is only supported for Connector versions 6.0.6 or later. Otherwise, compliance checks for checks for WUC External Parameters configurations will always fail.</p>

Windows Unified Connector (WUC) Internal Parameters Configuration

A WUC Internal Parameters connector configuration defines the internal parameters for one or more WUC connectors. The configuration is only pushed to the target if a WUC connector exists.

Limitations to WUC Internal Parameters Configurations

A WUC internal parameters configuration has the following limitations:

- Domain user password is not supported as a WUC configuration parameter. Instead, domain user password must be managed individually for each WUC host.
- WUC connectors are not FIPS-compliant.
- If you wish to push a WUC configuration from ArcMC to a managed node that already has values defined for all fields listed here, then you must specify values for all fields in the pushed configuration. Default values may be used if necessary

WUC Internal Parameters Configuration Parameters

Parameter	Data Type	Description
Enable GUID Translation*	Boolean	If true, Globally Unique Identifier translation is enabled.
Enable SID Translation*	Boolean	If true, Security Identifier translation is enabled.
Enable SID Translation Always*	Boolean	If true, SID translation is used even for events Windows does not translate.
FCP Version	Integer	File Control Protocol version number.
Global Catalog Port	Integer	Port used by Global Catalog server.
Global Catalog Security Protocol	Enum	Security protocol used by Global Catalog server.
Host Browsing Threads Sleep Time	Integer	Time in milliseconds between host browsing queries.
Inactivity Sleep Time	Integer	Time in milliseconds to sleep if no events are retrieved from the configured hosts
Log Rotation Check Interval	Integer	Time in milliseconds to wait before checking for log rotation.
Reconnect Interval	Integer	Time in milliseconds after which the connection to a previously down host is to be retried.
Rotation Retry Count	Integer	Number of times to check that log has been rotated.

WUC Internal Parameters Configuration Parameters, continued

Parameter	Data Type	Description
Rotation Retry Interval	Integer	Interval in milliseconds for rotation retry.
Sleep Time	Integer	Time, in milliseconds, to sleep before collecting more events from hosts (-1 means disable sleep time).
Thread Count	Integer	Number of threads to use for the connector.

ArcMC/Connector Appliance Configuration Types

ArcMC/Connector Appliance configurations set values for settings on Software ArcSight Management Centers, ArcSight Management Center Appliances, and hardware or software Connector Appliances. The currently available ArcMC/Connector Appliance configuration type is listed here.

ArcMC/Connector Appliance Configuration Backup Configuration

An ArcMC/Connector Appliance Configuration Backup configuration sets values for scheduled configuration backups of ArcSight Management Center or Connector Appliance. Backup content includes all backup data.

After a push, the web process is automatically restarted on the subscriber.

For this configuration type, no automatic compliance checks will be performed. [You must check compliance manually](#). The following limitation applies:

- This Configuration is not supported if the Backup Server platform is CentOS 7.4.



Note: You can neither create nor import settings related to a one-time configuration backup.

ArcMC/Connector Appliance Configuration Backup Parameters

Parameters	Data Type	Description
Backup Server IP Address*	String	IP address of the remote system where the backup will be saved.
Port*	Integer	Port of the remote system. Default value is 22.
Base Remote Directory*	String	Destination directory on the remote system. Must be manually created on remote system prior to push. After a push, the destination host name is appended to this, to give it a unique value across all nodes.
User*	String	User name on destination.

ArcMC/Connector Appliance Configuration Backup Parameters, continued

Parameters	Data Type	Description
Password*	String	Password on the destination. (Obfuscated.)
Days of the Week*	List of comma-separated strings	Comma-delimited list of days of the week on which the backup will be performed. Valid values are <i>Su, M, T, W, Th, F, Sa</i> .
Hours of Day*	List of comma-separated integers	Comma-delimited list of hours of the day at which the backup will be performed. Valid values are integers from 0 to 23, where 0 is 12:00 midnight. For example, a value of 14 would correspond to 2 PM.

Destination Configuration Types

A destination configuration sets values for ESM destination settings on Connectors/Collectors. The available destination configuration types are listed here.

Destination Configuration Parameters

A Destination Configuration Parameters configuration defines values and behavior for destination configuration parameters.



Note: Destination Configuration Parameters configurations can only be imported from managed Collectors/Connectors, not created in ArcMC. See "[Importing a Subscriber Configuration](#)" on [page 176](#) for more information.

For a description of the parameters for this configuration type, see "[Destination Runtime Parameters](#) " on page 334.

Networks and Zones

A Networks and Zones configuration defines values and behavior for ArcSight ESM networks and zones. For more information on ESM networks and zones, consult the ArcSight Console documentation. For Connector Network and Zone Configuration information see the [Smart Connector's User Guide](#).



Note: So as not to interfere with ESM connector management, ArcMC will not push Network and Zones AUPs to a connector's ESM destination folder.

Networks and Zones Configuration Parameters

Parameter	Data Type	Description
Configuration Name*	String	Name of the configuration.
Networks CSV Content*	CSV	<p>Comma-separated Value (CSV) file. Click Upload to upload a valid CSV file, or click Download to download an existing file.</p> <p>Creating a CSV File</p> <p>The CSV must include the literal header line:</p> <pre>#Type,Name,Parent Group URI,Customer URI</pre> <p>Then, each line describes a Network. Each line must comprise values for the following fields, and end with a hard return (no white spaces). Begin the first of these network lines with the # character before Type.</p> <pre><Type>,<Name>,<Parent Group URI>,<Customer URI></pre>
Zones CSV Content*	CSV	<p>Comma-separated Value (CSV) file. Click Upload to upload a valid CSV file, or click Download to download an existing file.</p> <p>Creating a CSV File</p> <p>The CSV must include the literal header line:</p> <pre>#Name,Start Address,End Address,Parent Group URI,Network URI</pre> <p>Then, each line describes a Zone. Each line must comprise values for the following fields, and end with a hard return (no white spaces). Begin the first of these zone lines with the # character before Name.</p> <pre><Name>,<Start Address>,<End Address>,<Parent Group URI>,<Network URI></pre>

Logger Configuration Types

Logger configurations set values for settings on hardware and software Loggers. The available Logger configuration types are listed here.

Logger Configuration Backup Configuration

A Logger configuration backup configuration sets values for scheduled configuration backups of hardware and software Logger to a remote system. The following limitation applies:

- This Configuration is not supported if the Backup Server platform is CentOS 7.4.



Note: You can neither create nor import settings related to a one-time configuration backup.

Logger Configuration Backup Configuration Parameters

Parameter	Data Type	Description
SCP Port*	String	Port of the remote system. Default value is 22.
Backup Server IP Address*	String	IP address of the remote system where the backup will be saved.
Username*	String	User name on destination.
Password*	String	Password on destination. (Obfuscated.)
Base Remote Directory*	String	Destination directory on the remote system. After a push, the destination host name is appended to this, to give it a unique value across all nodes. When using a Logger appliance, some settings need to be configured in the /etc/hosts file. For more information, please refer to the <i>Configuring Hosts for the Appliance</i> chapter in the Logger Installation Guide.
Days of the Week*	List of comma-separated strings	Comma-delimited list of days of the week on which the backup will be performed. Valid values are <i>Su, M, T, W, Th, F, Sa</i> .
Hours of Day*	List of comma-separated integers	Comma-delimited list of hours of the day at which the backup will be performed. Valid values are integers from 0 to 23, where 0 is 12:00. For example, a value of 14 would correspond to 2 PM.
Backup Content*	String	Type of content to be included in the backup. Valid values are: <ul style="list-style-type: none">• <i>All</i>: includes all backup data.• <i>Report_Content_Only</i>: includes only report data.

Logger Connector Forwarder Configuration

A Logger Connector Forwarder configuration sets values for one or more connector forwarders on a Logger (version 6.1 or later). Each forwarder in the configuration is represented by a different Property.



Note: Logger Connector Forwarder configurations can only be imported from managed Loggers, not created in ArcMC. See "[Importing a Subscriber Configuration](#)" on page 176 for more information.

Logger Connector Forwarder Configuration Parameters

Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are <i>Unified</i> or <i>Regex</i> .
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Optional start of time range for selection.
End Time	DateTime	Optional end of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receive forwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable*	Boolean	If Yes , the forwarder is enabled.
Connection Retry Timeout*	Integer	Time, in seconds, to wait before retrying a connection.
Source Type*	Integer	Source Type. Valid values: <ul style="list-style-type: none"> • Apache HTTP Server Access • Apache HTTP Server Error • IBM DB2 Audit • Juniper Steel-Belted Radius • Microsoft DHCP Log • Other

Logger ESM Forwarder Configuration

A Logger ESM Forwarder configuration sets values for one or more ESM destinations on a Logger (version 6.1 or later). Each destination in the configuration is represented by a different Property.



Note: Logger ESM Forwarder configurations can only be imported from managed Loggers, not created in ArcMC. See "[Importing a Subscriber Configuration](#)" on page 176 for more information.

Logger ESM Forwarder Parameters

Parameter	Data Type	Description
Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are <i>Unified</i> or <i>Regex</i> .
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Start of time range for selection.
End Time	DateTime	End of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receive forwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable	Boolean	If Yes, the forwarder is enabled.

Logger Filter Configuration

A Logger Filter configuration sets values for one or more saved searches on a Logger.

Each filter in the configuration is represented by a different Property.



Note: Logger Filter configurations can only be imported from managed Loggers, not created in ArcMC. See "[Importing a Subscriber Configuration](#)" on page 176 for more information.

Logger Filter Configuration Parameters

Parameter	Data Type	Description
Filter Name*	String (Read-only)	Name of the filter.
Filter Category	String	Category of filter. Valid values are Shared , System and SearchGroup .

Logger Filter Configuration Parameters, continued

Parameter	Data Type	Description
Filter Type*	String	Type of filter. Valid values are RegexQuery or UnifiedQuery .
Query*	String	Query string.
Permission Group	String	<p>Permission group which with the Logger filter is associated. When the configuration is pushed:</p> <ul style="list-style-type: none"> If the permission group is not present on the target Logger, the permission group will be created during the push. If the permission group of the same name is already present on the target, but has different rights, the rights of the permission group on the target Logger will not be overwritten, and the association between the filter and the permission group will be removed.

Logger SmartMessage Receiver Configuration

A Logger SmartMessage Receiver sets values for one or more SmartMessage Receivers.

A SmartMessage Receiver configuration pushed to a target overwrites any existing SmartMessage receivers on the target; other types of receivers such as UDP and TCP are not affected.

Logger SmartMessage Receiver Configuration Parameters

Parameter	Data Type	Description
Receiver Name*	String	Name of the receiver.
Enabled*	Boolean	If Yes , SmartMessage reception is enabled.
Encoding*	String	<p>Encoding type. Valid values are:</p> <ul style="list-style-type: none"> UTF-8 US-ASCII

Logger Storage Group Configuration

A Logger Storage Group configuration sets values for one or more Logger storage groups.



Note: Logger Storage Group configurations can only be imported from managed Loggers, not created in ArcMC. See "[Importing a Subscriber Configuration](#)" on page 176 for more information.

Logger Storage Group Configuration Parameters

Parameter	Data Type	Description
Storage Group Name*	String (Read-only)	<p>Name of the storage group.</p> <ul style="list-style-type: none"> The pushed configuration must contain the same number of storage groups as configured on the Logger. The names of the storage groups in the pushed configuration must match the names of storage groups on the Logger.
Maximum Age (Days)*	Integer	Maximum age of events in storage, in days.
Maximum Size (GB)*	Integer	<p>Maximum size of the storage group, in gigabytes.</p> <ul style="list-style-type: none"> The cumulative size of all storage groups must not be greater than the storage volume size on the Logger.

Logger TCP Forwarder Configuration

A Logger Connector Forwarder configuration sets values for one or more TCP forwarders on a Logger (version 6.1 or later). Each forwarder in the configuration is represented by a different Property.



Note: Logger TCP Forwarder configurations can only be imported from managed Loggers, not created in ArcMC. See "[Importing a Subscriber Configuration](#)" on page 176 for more information.

Logger TCP Forwarder Configuration Parameters

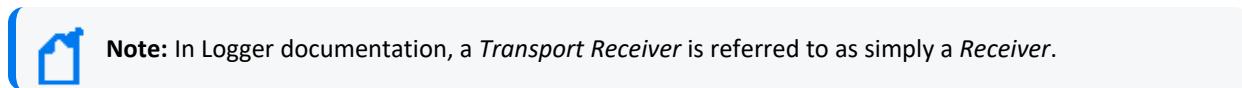
Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are <i>Unified</i> or <i>Regex</i> .
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Optional start of time range for selection.
End Time	DateTime	Optional end of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receive forwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable*	Boolean	If Yes , the forwarder is enabled.

Logger TCP Forwarder Configuration Parameters, continued

Parameter	Data Type	Description
Preserve System Timestamp*	Boolean	If Yes, the timestamp showing original event receipt time is preserved.
Preserve Original Syslog Sender*	Boolean	If Yes, event is sent as is, without inserting Logger's IP address in the hostname (or equivalent) field of the syslog event.
Connection Retry Timeout*	Integer	The time, in seconds, to wait before retrying a connection.

Logger Transport Receiver Configuration

A Logger Transport Receiver configuration sets values for one or more UDP, TCP, CEF UDP, or CEF TCP receivers.



A pushed Transport Receiver type configuration will overwrite any existing UDP, TCP, CEF UDP, or CEF TCP receiver. Any other type of receivers, such as SmartMessage receivers, are not affected.

Logger Transport Receiver Configuration Parameters

Parameter	Data Type	Description
Receiver Name*	String	Name of the receiver.
Receiver Type*	String	Receiver type. Valid values are: <ul style="list-style-type: none"> • UDP • TCP • CEF UDP • CEF TCP
Receiver Name*	String	Name of the receiver.

Logger Transport Receiver Configuration Parameters, continued

Parameter	Data Type	Description
Port*	Integer	Port number. Must be a non-zero positive number. Ensure this port is open on the destination.
Enabled*	Boolean	If Yes, transport reception is enabled.
Encoding*	String	<p>Encoding type. Valid values are:</p> <ul style="list-style-type: none"> • UTF-8 • Shift_JIS • EUC-JP • EUC-KR • US-ASCII • GB2312 • UTF-16BE • Big5 • GB18030 • ISO-8859-1 • Windows-1252 <p>For CEF UDP and CEF TCP receivers, only UTF-8 and US-ASCII apply.</p> <p>Caution: Selection of the wrong encoding for a CEF receiver will cause a push failure.</p>

Logger UDP Forwarder Configuration

A Logger Connector Forwarder configuration sets values for one or UDP forwarders on a Logger. Each forwarder in the configuration is represented by a different Property.



Note: Logger UDP Forwarder configurations can only be imported from managed Loggers, not created in ArcMC. See "[Importing a Subscriber Configuration](#)" on page 176 for more information.

Logger UDP Forwarder Configuration Parameters

Parameter	Data Type	Description
Forwarder Name*	String	Display name of the forwarder
Filter Type*	Enum	Filter type that was selected while creating a forwarder on logger. Valid types are <i>Unified</i> or <i>Regex</i> .
Query	String	Used to filter events that the forwarder will forward.
Unified Query Filters	String	Select from the default and user-defined Unified filters on the source Logger. Only visible if Filter Type is Unified.

Logger UDP Forwarder Configuration Parameters, continued

Parameter	Data Type	Description
Regular Expression Filters	String	Select from the default and user-defined Regex filters on the source Logger. Only visible if Filter Type is Regex.
Start Time	DateTime	Optional start of time range for selection.
End Time	DateTime	Optional end of time range for selection.
IP/Host*	String	IP address or host name of the destination that will receive forwarded events.
Port*	Integer	Port number on the destination that will receive forwarded events. Ensure this port is open on the destination.
Enable*	Boolean	If Yes, the forwarder is enabled.
Preserve System Timestamp*	Boolean	If Yes, the timestamp showing original event receipt time is preserved.
Preserve Original Syslog Sender*	Boolean	If Yes, event is sent as is, without inserting Logger's IP address in the hostname (or equivalent) field of the syslog event.

SecureData Configuration

A SecureData configuration sets values for the SecureData encryption client on a managed Logger.

SecureData Configuration Parameters

Parameter	Data Type	Description
Server*	String	SecureData server IP address.
Port*	String	SecureData server port.
Auth Identity*	String	SecureData authentication identity
Shared Secret*	String	SecureData shared secret
Event Fields*	String	Comma-separated list of event fields to be encrypted. Default data for event fields will be populated from the connector bin file uploaded in the repository. If there is no such file, then the default field will be defined by ArcMC.

System Admin Configuration Types

System Admin configurations set values for system administrative settings. The available System Admin configuration types are listed here.

Authentication External

An Authentication External configuration defines values and behavior for a hardware or software system requiring authentication to an external server, such as LDAP or RADIUS.

After changing the Authentication Method on a host, you must delete the host from ArcMC, then re-add it using Node Management.



Note: Authentication External configurations can only be imported from managed Loggers, not created in ArcMC. See "[Importing a Subscriber Configuration](#)" on page 176 for more information.

Authentication External Configuration Parameters

Parameter	Data Type	Description
Authentication Method*	String	System authentication method.
Allow Local Password Fallback for Default Admin Only*	Boolean	If Yes, the authentication server will fall back to local passwords for authentication for administrators.
Allow Local Password Fallback for All Users*	Boolean	If Yes, the authentication server will fall back to local passwords for authentication for all users.
LDAP Server Hostname[port]*	String	LDAP server hostname and port.
LDAP Backup Server Hostname [port]	String	LDAP backup server hostname and port.
LDAP Server Request Timeout (seconds)	Integer	LDAP server request timeout, in seconds.
RADIUS Server Hostname[port]	String	RADIUS server hostname and port.
RADIUS Backup Server Hostname [port]	String	RADIUS backup server hostname and port.
RADIUS Shared Authentication Secret	String	RADIUS authentication shared secret.
RADIUS Server NAS IP Address	String	RADIUS server Network Access Server IP address .

Authentication External Configuration Parameters, continued

Parameter	Data Type	Description
RADIUS Request Timeout (seconds)	Integer	RADIUS server request timeout, in seconds.
RADIUS Retry Request	Integer	Number of times to retry RADIUS server requests.
RADIUS Protocol	String	Type of RADIUS protocol.

Authentication Local Password

An Authentication Local Password configuration defines a hardware or software system's local password options and behavior.

Authentication Local Password Configuration Parameters

Parameter	Data Type	Description
Enable Account Lockout*	Boolean	If Yes , account lockouts are enabled after an incorrect password entry.
Lock Out Account after N Failed Attempts*	Integer	Number of failed attempts before lockout.
Remember Failed Attempts For (seconds)*	Integer	Time, in seconds, between failed attempts that will trigger a lockout.
Lockout Account for (minutes)*	Integer	Time, in minutes, that the account will be locked out.
Enable Password Expiration*	Boolean	If Yes , password expiration is enabled
Password Expires in (days)*	Integer	Interval, in days, after which a password expires.
Notify User (Days Before Expiration)*	Integer	Days before password expiration that the user is notified.
Users Exempted from Password Expiration Policy	List of comma-separated strings	Comma-separated list of users whose passwords will never expire.
Enforce Password Strength*	Boolean	If Yes , password strength is enforced.
Minimum Length (characters)*	Integer	Minimum number of password characters.
Maximum Length (characters)*	Integer	Maximum number of password characters.
Numeric [0-9]*	Integer	Minimum number of numeric password characters.
Upper Case [A-Z]*	Integer	Minimum number of uppercase password characters.
Lower Case [a-z]*	Integer	Minimum number of lowercase password characters

Authentication Local Password Configuration Parameters, continued

Parameter	Data Type	Description
Special [1\$^*...]*	Integer	Minimum number of special password characters.
Password Must Be At Least*	Integer	Minimum number of characters a new password must differ from the user's previous password.
Include "Forgot Password" link on Login Screen*	Boolean	If Yes, a link is provided where the user can recover a password.

Authentication Session

An Authentication Session configuration defines values for a hardware or software system's authentication sessions.

Authentication Session Configuration Parameters

Parameter	Data Type	Description
Max Simultaneous Logins Per User*	Integer	Maximum number of simultaneous logins per user. If Max Simultaneous Logins/User is set to 1, it is required to have at least another admin user, otherwise the admin user will not be able to log in.
Logout Inactive Session After (seconds)*	Integer	Inactivity session timeout, in seconds.
Disable Inactive Account After (days)*	Integer	Number of days of inactivity after which an account will be disabled.

DNS Configuration

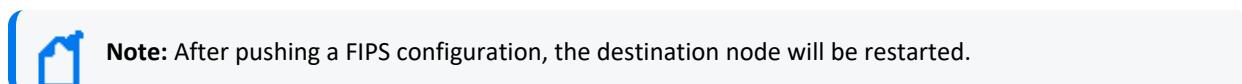
A DNS Configuration defines values for a hardware appliance's Domain Name Service.

DNS Configuration Parameters

Parameter	Data Type	Description
Primary DNS*	String	Primary DNS server.
Secondary DNS	String	Secondary DNS server.
DNS Search Domains	List of comma-separated strings	Comma-separated list of DNS search domains.

FIPS Configuration

A FIPS configuration enables or disables FIPS mode on a managed node.



FIPS Configuration Parameters

Parameter	Data Type	Description
Enabled*	Boolean	If Yes , FIPS is enabled on the node.

Network Configuration

A Network Configuration defines values for a hardware appliance's default gateway setting.



Note: Values for these network settings cannot be changed through ArcSight Management Center: hostname, IP addresses for the network interfaces, static routes, /etc/hosts file, and time settings.

Network Configuration Parameters

Parameter	Data Type	Description
Default Gateway*	String	Default network gateway.

NTP Configuration

An NTP Configuration defines values for a hardware appliance's Network Time Protocol.

NTP Configuration Parameters

Parameter	Data Type	Description
Enable as NTP Server*	Boolean	If Yes , the system is enabled as an NTP server.
NTP Servers*	List of comma-separated strings	Comma-separated list of NTP servers. Required even if Enable as NTP Server is false.

SMTP Configuration

An SMTP Configuration defines values for a hardware or software system's Simple Mail Transfer Protocol.

SMTP Configuration provides for authentication and security. This is implemented through the primary STMP server port, primary username, primary password, primary certificate, backup STMP server port, backup username, backup password, and backup certificate fields, along with the primary STMP server, backup STMP server, and outgoing email address fields.

SMTP Configuration Parameters

Parameter	Data Type	Description
Primary SMTP Server*	String	Primary SMTP server.
Secondary SMTP Server	String	Secondary SMTP server.
Outgoing Email Address*	String	Outgoing email address.
Enable Auth/TLS	Boolean	Enable/Disable secure authenticated mode of communication with SMTP server
Primary SMTP Server Port	Integer	Primary SMTP Server Port. Required if Auth/TLS is enabled.
Primary SMTP Server Username	String	Primary SMTP Server Username. Required if Auth/TLS is enabled.
Primary SMTP Server Password	String	Primary SMTP Server Password. Required if Auth/TLS is enabled.
Primary SMTP Server Certificate Content	String	Upload Primary SMTP Server Certificate. Required if Auth/TLS is enabled.
Secondary SMTP Server Port	Integer	Secondary SMTP Server Port. Required if Auth/TLS is enabled.
Secondary SMTP Server Username	String	Secondary SMTP Server Username. Required if Auth/TLS is enabled.
Secondary SMTP Server Password	String	Secondary SMTP Server Password. Required if Auth/TLS is enabled.
Secondary SMTP Server Certificate Content	String	Upload secondary SMTP Server Certificate. Required if Auth/TLS is enabled.

SNMP Poll Configuration

An SNMP Poll Configuration defines values for a hardware appliance's Simple Network Management Protocol monitoring. supports V2c and V3 of SNMP.

SNMP Poll Configuration Parameters

Parameter	Data Type	Description
Status	Boolean	If Yes, SNMP polling is enabled.
Port*	Integer	SNMP port.
SNMP Version*	String	Version of SNMP supported. Valid values are v2c and v3.
Community String	String	SNMP community string. Required for V2c only.
Username	String	Authentication username. Required for V3 only.
Authentication Protocol*	String	Authentication protocol. Valid values are MD5 and SHA. Required for V3 only.

SNMP Poll Configuration Parameters, continued

Parameter	Data Type	Description
Authentication Passphrase	String	Authentication passphrase. Required for V3 only.
Privacy Protocol	String	Privacy protocol. Valid values are DES and AES128. Required for V3 only.
Privacy Passphrase	String	Privacy passphrase. Required for V3 only.
System Name	String	Name of the SNMP system.
Point of Contact	String	Point of contact.
Location	String	System location.

SNMP Trap Configuration

An SNMP Trap Configuration defines values for a hardware appliance's Simple Network Management Protocol notifications. supports V2c and V3 of SNMP.



Note: In previous versions of , an SNMP Trap configuration was known as an SNMP Configuration.

SNMP Trap Configuration Parameters

Parameter	Data Type	Description
Status	Boolean	If Yes, SNMP polling is enabled.
NMS IP Address	String	IP address of network management server.
Port*	Integer	SNMP port.
SNMP Version*	String	Version of SNMP supported. Valid values are v2c and v3.
Community String	String	SNMP community string. Required for V2c only.
Username	String	Authentication username. Required for V3 only.
Authentication Protocol*	String	Authentication protocol. Valid values are MD5 and SHA. Required for V3 only.
Authentication Passphrase	String	Authentication passphrase. Required for V3 only.
Privacy Protocol	String	Privacy protocol. Valid values are DES and AES128. Required for V3 only.
Privacy Passphrase	String	Privacy passphrase. Required for V3 only.

Logger Initial Configuration Management

A *Logger initial configuration* is intended for the rapid, uniform setup of multiple ArcSight Loggers of the same model number and software version. Use a Logger initial configuration to expedite the initial deployment of Loggers to a production environment. Initial configuration management is supported on Logger version 6.1 or later.

A Logger initial configuration is not created in ArcMC. Instead, a suitable initial configuration is created on a managed Logger and imported into ArcMC. The configuration may then be pushed to other managed Loggers of the same model and software version number.

The following attributes are shown for each initial configuration:

Attribute	Description
Imported Init-Config Name	Name of the imported initial configuration.
Product Type	Type of Logger to which the configuration may be pushed: either Logger (appliance) or SWLogger (software)
Source Host	IP address of the host from which the configuration was imported.
Imported On	Date of import.
Imported By	User who imported the configuration.
SW Version	Software version of the configuration.
Source Model	For appliances, the model number of the source host Logger. (For software Logger, this is shown as Software.)

You can perform the following initial configuration management tasks:

- [Import an Initial Configuration](#)
- [Push an Initial Configuration](#)
- [View the Initial Configuration Event History](#)
- [Delete an Initial Configuration](#)

Importing a Logger Initial Configuration

An initial configuration created on a managed Logger (of version 6.1 or later) may be imported into ArcSight Management Center, for editing and pushing to other Loggers.

ArcMC can store up to 30 initial configurations.

To import an initial configuration from a Logger of version 6.1 or later:

1. Click **Configuration Management > Logger Initial Configurations**.
2. Under **Configurations**, click **Import**.
3. On the **Import Initial Configuration** dialog, in **Name**, specify a name for the configuration you wish to import.
4. Under **Source Host URI**, select the node from which you wish to import the configuration.
5. Click **Import**. The configuration is imported into ArcSight Management Center and is shown in the **Configurations** table.
6. Optionally, if you wish to push the imported configuration to managed nodes, when prompted to push, click **Yes**.



Note: An initial configuration is not created in ArcMC. Instead, create the initial configuration on a managed Logger, then import it into ArcMC for pushing to other managed Loggers.

Pushing a Logger Initial Configuration

You can push a Logger initial configuration to selected managed Loggers of version 6.1 or later. The destination Loggers must be of the same software version (and, for hardware appliances, model number) as the Logger on which the initial configuration was created.

The push process overwrites the settings on the destination Loggers.

Pushing a Logger initial configuration must be performed manually.



Note: Before performing a push, ensure that the destination Logger's storage volume is set up, and that it exceeds that of any source Logger.

To push an initial configuration to one or more managed Loggers of version 6.1 or later:

1. Click **Configuration Management > Logger Initial Configurations**.
2. From the **Configurations** table, select a configuration to be pushed.
3. Click **Push**.
4. On the **Make Selections for Push** dialog, under **Available Nodes**, the nodes eligible for receiving a push are displayed by location. Browse to the recipient node and click **Add**. The selected node is shown under **Selected Nodes**. (To select multiple nodes to receive a push, Ctrl+click each selected node.)
5. Click **Push**.

- Click **Yes** to confirm the push and change settings on the destinations. The configuration is pushed to the selected destination nodes.



Tip: In order to correctly view push status, click **Refresh**, even if the status is shown as In Progress.

Push Results on a Destination Logger

The results of a push of an initial configuration on a given setting of a destination Logger are dependent on the setting, as shown in the following table.

Setting on Destination	Result After Push
<ul style="list-style-type: none"> Archive storage settings Audit logs ESM destinations Event archives Finished tasks Forwarders Peer Loggers 	Blank: These settings will be blank on the destination, even if they are included in the pushed initial configuration. Also, all configurations on the destination Logger related to these settings will also be blanked.
<ul style="list-style-type: none"> Alerts User-created receivers (RFSFileReceiver, FileTransfer, FolderFollowerReceiver) 	Disabled: These settings are disabled on the destination Logger, but are editable through the destination Logger's UI.
<ul style="list-style-type: none"> Hosts file Groups Users 	<p>Copied From Source: These values are copied from the initial configuration and overwritten on the target.</p> <p>This may include user credentials that the Logger uses to authenticate to ArcMC, which could break the management link between ArcMC and the destination Logger (which requires these credentials). If an overwrite of these credentials occurs, to enable management, delete the host from ArcMC, then re-add the Logger as a host (with the new credentials).</p>
All other settings	Copied From Source: Values are copied from the initial configuration and overwritten on the target.

Deleting a Logger Initial Configuration

A deleted initial configuration is no longer available for pushes. You may not delete a configuration currently being pushed.

To delete an initial configuration:

1. Click **Configuration Management > Logger Initial Configurations**.
2. From the **Logger Initial Configurations** table, select one or more configurations to be deleted.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Event History

The **Event History** list records all imports, pushes, and deletes transactions related to initial configuration pushes. Each event in the history displays the following information:

Column	Description
Init-Config Name	Initial configuration's name.
Author	User who performed the action.
Event Type	Type of event recorded for the initial configuration. Event types include Push, Import, and Delete.
Event Occurrence	Local date and time of the event.
Source Host	URI of the host on which the initial configuration was created.
Destination URI for Push	If the event is of type Push, this is the URI of the destination node to which the initial configuration was pushed.
Event Status	Status of the event. Status types include: <ul style="list-style-type: none"> • In-progress: the transaction is still in progress. • Successful: the transaction succeeded. • Failed: the transaction failed. Click the failed status to view an indication of the failure reason.

To search for a specific event by any of these criteria, click the drop-down in the corresponding column header. Then, in **Filters**, select or specify the specific criterion for which you wish to show events. Only events matching the filter will be displayed in the **Event History** list.

For example, to see all pushes, in the **Event Type** column, click the header drop-down. Then, in **Filters**, select *Push*.

Managing Logger Event Archives

Logger Event Archives enable you to save the events for any day in the past (not including the current day). In , you can view Logger Event Archives on managed Loggers, and perform management tasks including loading, unloading, and indexing archives.

Logger Event Archive management is only available for managed Loggers of version 6.2 or later.

For complete information on managing Logger Event Archives, see the Logger Administrator's Guide.

The following parameters are shown on the Logger Event Archives list:

Parameter	Description
Peers	For Loggers, the number of peers of the Logger. To see the Logger's peers in detail, click the number shown.
Event Status	The status of a current archiving job, where status is one of the following values: <ul style="list-style-type: none"> <i>Loading</i>: The archive is being loaded on the managed Logger. <i>Loaded</i>: The archive is currently loaded on the managed Logger. <i>Unloading</i>: The archiving job is currently executing. <i>Archived</i>: The archiving job is complete. <i>Failed</i>: The archiving job was not successful.
Index Status	The status of a current indexing job, where status is one of the following values: <ul style="list-style-type: none"> <i>None</i>: No indexing status is available. <i>Pending</i>: The indexing job is about to begin. A pending job can be canceled by clicking in the Cancel column of the table. <i>Indexing</i>: The indexing job is in process. <i>Indexed</i>: The indexing job is complete. <i>Failed</i>: The indexing job was unsuccessful.
Cancel	Click the X to cancel a pending indexing job before it begins.

To view Logger event archives:

- Under **Configuration Management**, select **Logger Event Archive**.
- On the **Event Archive List** tab, select your criteria to search for Logger Event Archives on managed Loggers.
- Select a Start and End Date, then select one or more Loggers to search.
- Click **Search**. All Logger Event Archives matching the search criteria are listed in hierarchical format: by managed Logger, then by Storage Group, and finally by Event Archive.

To toggle the view open or closed, click **Expand** or **Collapse**.

Managing Event Archives

You can perform two management tasks on managed Loggers related to event archives: loading (or unloading) archives, and indexing them.

To load an event archive:

1. On the Event Archive List, select an archive to load.
2. Click **Load Archive**. The selected operation will be performed. The status of the job will be shown in the **Event Status** column.

To index an Event Archive:

1. On the Event Archive List, select an archive to index.
2. Click **Index Archive**. The selected archive will be indexed. The status of the indexing job will be shown in the **Index Status** column.

Viewing Load/Unload History

You can also view your Logger event archive load, unload, and indexing history. This displays the actions taken in ArcMC to view Logger Event Archives.

To view Logger event archive load/unload history:

1. Under **Configuration Management**, select **Initial Configurations > Logger Event Archive**.
2. Click the **Archive Load/Unload History** tab. The activity history is displayed.

Managing Logger Peers

Managed Loggers can be peered with any number of other Loggers. You can manage the peer relationship between Loggers in ArcMC. ArcSight recommends that, if possible, all peer Loggers be managed by ArcMC.

You can view peers; add or remove peers to a Logger; and import, edit, push, and delete peer groups. A *peer group* is a named set of Loggers you can use to organize and administer sets of Loggers more easily.



Note: For more information about Logger peering, please refer to the ArcSight Logger Administrator's Guide.

Viewing Peers or Peer Groups

You can view the peers of a Logger managed by ArcMC, as long as the Logger is version 6.1 or later.

To view peered Loggers in ArcMC:

1. Select Configuration Management > Logger Peers. The **Logger Peers** table is displayed with all managed Loggers of version 6.1 or later.
2. To view the Loggers peered to a specific Logger in the list , in the **Peer Loggers** column, click the link indicating the number of peers. The filterable **Peer Loggers** dialog lists all the Logger's peers.
3. To view peer groups in ArcMC, click **View Peer Groups**.

Adding or Removing Peers

You can add peers to, or remove peers from, a Logger managed by ArcMC, as long as the managed Logger is version 6.1 or later.



Note: If you remove a Logger not managed by ArcMC as a peer, you will not be able to add it back to the group unless you import the peer group including the Logger into ArcMC, or you add the removed Logger to ArcMC management.

To add peers to, or remove peers from, a Logger:

1. Select the Logger whose peers you wish to edit from the **Logger Peers** table.
2. Click **Edit Peers**.
3. All currently peered Loggers are shown.
 - a. To add one or more peers, click **Add Peers**. Then, in the **Add Peers** dialog, select the Loggers to be added as peers. Optionally, to create a new peer group in ArcMC, in **Peer Group Name**, specify a name for the peer group. Then, click **Add**.
 - b. To remove one or more Loggers as peers, select the Loggers to remove, and click **Remove Peers**. Click **Yes** to confirm removal as peers.



Note: For this release, Logger peering is supported using user name and password, not authorization code.

Importing a Peer Group

You can import Logger peer groups into ArcMC. Importing a peer group is only supported on Loggers version 6.1 or later.

To import a peer group from a Logger (of version 6.1 or later):

1. Select **Configuration Management > Logger Peers**.
2. Click **View Peer Groups**.
3. Click **Import Peers**.
4. On the **Select Peer** dialog, select a managed Logger. (The selected Logger will also be part of the imported peer group.) Then, click **Next**.
5. On the **Select Peer (of the Target)** dialog, select one or more peers to import into ArcMC.
6. In **Peer Group Name**, specify a name for the selected peer group.
7. Click **Import**. The selected peer group is imported into ArcMC.

Edit a Peer Group

You can edit a peer group, including the name, peered Logger hostname, and group members.

To edit a peer group:

1. Select **Configuration Management > Logger Peers**.
2. Click **View Peer Groups**.
3. Click the name of the peer group you wish to edit.
4. On the **Edit Peer Group** dialog, edit the peer group as needed. You can edit the peer group name, and add or remove peers from the group.
5. Click **Save**. Alternatively, click **Save As...** to save the peer group under a new name.

Pushing a Peer Group

You can push a peer group to one or multiple managed Loggers of version 6.1 or later. The Loggers in the group will become peered with the managed Loggers to which you pushed the group.

To push a peer group:

1. Click **Configuration Management > Logger Peers**.
2. Click **View Peer Groups**.
3. From the table, select a peer group to push.
4. Click **Push**.
5. On the **Destination Loggers** dialog, select one or more destination Loggers to which to

push the peer group.

6. Click **Push**. The peer group is pushed to the destination Loggers.

Deleting a Peer Group

You can delete a peer group from ArcMC.

To delete a peer group:

1. Click **Configuration Management > Logger Peers**.
2. Click **View Peer Group**.
3. From the list of peer groups, select a group to delete.
4. Click **OK** to confirm deletion.

Managing Transformation Hub

You can use ArcMC to perform management and monitoring of Transformation Hub. These functions include adding topics, managing routes, and status monitoring.

About Topics

A *topic* is a metadata tag that you can apply to events in order to categorize them.

Transformation Hub ships with several pre-set topics, and you can define any number of additional topics as needed.

A topic includes these components:

- **Name:** The name of the topic.



Note: ArcSight Avro is the displayed name for the type name event-avro for the ArcSight avro topic.

- **Topic Type:** The type of topic CEF (routable) Arcsight Avro (routable) BINARY (not routable) RAW (not routable) SYSLOG (not routable).
- **Partition Count:** A segment of a topic. There can be one or more partitions for each topic. The number of partitions limits the maximum number of consumers in a consumer group.
- **Replication Factor:** The number of copies of each partition in a topic. Each replica is created across one Transformation Hub node. For example, a topic with a replication factor of 3 would have 3 copies of each of its partitions, across 3 Transformation Hub nodes.

You can only use ArcMC to add topics (not delete them). The **Edit** option is only available for topics with a *null* topic type (topics not created by ArcMC. e.g. Kafka manager) and it allows the user to modify the **Topic Type** value.

To set the type for existing topics (only for topics not created by ArcMC. e.g. Kafka manager), users can access the **List of Topics** page located in **Configuration Management > Transformation Hub > Topics**.

This page will display detailed information for Topic Name, Topic Type, Routable Topic, Partitions Count, and Replication Factor. This option is only available for Transformation Hub 3.4+.

For more information on managing topic partitions and replication, please see [Managing Topics](#).

Adding a Topic

To add a topic:

1. Click **Configuration Management > Transformation Hub**.
2. On the Transformation Hub Configurations page, click **Topics > + Add**.
3. On the Add New Topic dialog, in **Topic Name**, specify a name for the new topic.
4. In **Topic Type**, select the type for the new topic.



Note: For Transformation Hub 3.4 users must select the topic type when adding the new topic. This option is disabled for Transformation Hub 3.3 or earlier.

5. In **# of Partitions**, specify the number of partitions the topic will have.
6. In **Replication Factor**, specify the number of copies that will be made for each partition.
7. Click **Save**.



Best Practice: When creating a topic, use a value for replication factor of at least 2. In addition, the number of partitions should be equal to the number of consumers which will be subscribed to the topic (now and in future). If ArcSight Database will be a consumer, the number of partitions should be a multiple of the number of Database nodes.

About Routes

A *route* is a method of retrieving events in a topic that meet certain criteria and then copying them into a new topic. Use routes to filter events into your topics for your own requirements, such as selecting a group of events for more detailed examination.

A route comprises these components:

- **Name:** Name of the route.
- **Routing Rule:** A logical filter that defines criteria by which events will be categorized into topics. The criteria are defined in terms of CEF and Avro fields for Transformation Hub 3.4 and later, and CEF only for Transformation Hub 3.3 and earlier.
- **Source Topic:** The topic being filtered for events which match the routing rule.
- **Destination Topic:** The topic to which a copy of an event matching the routing rule should be copied. (A copy of the event will remain in the source topic.)
- **Description:** A short description of the route.

You can add, edit, or delete routes in ArcMC. Routes only apply to CEF and Avro topics for Transformation Hub 3.4 and later, and CEF only for Transformation Hub 3.3 and earlier. Routes created to or from a binary topic (such as th-binary_esm) will not function.



Every Avro routing created in Transformation Hub 3.4 and earlier using th-arcsight-avro as source topic will be automatically overridden after upgrading to Transformation Hub 3.5. As a general guideline, th-arcsight-avro is no longer recommended as a source topic for Avro routing, since enrichment stream processors were added as intermediate layer between th-arcsight-avro and mf-event-avro-enriched in Transformation Hub 3.5. This makes the mf-event-avro-enriched topic the new primary source topic for Recon's database scheduler (replacing th-arcsight-avro). As a result, the routing starting point should start from the mf-event-avro-enriched topic to benefit from event enrichment.

Creating a Route

Before creating a route, ensure that your source and destination topics already exist. If not, [create them](#) before creating a route that uses them.

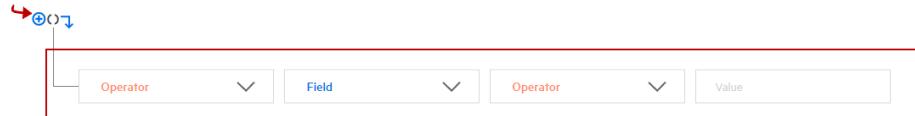
To create a route:

1. Click **Configuration Management > Transformation Hub**.
2. On the Transformation Hub Configurations page, click **Routes > +Add**.
3. In **Route Name**, specify a name for the route.
4. From the **Source Topic** drop-down list, select the topic from which events will be filtered.
5. From the **Destination Topic** drop-down list, select the destination to which events will be copied.
6. In **Description**, specify a short description of the route.
7. Under **Add Routing Rule**, use the Rule Editor to define the criteria for the routing rule.

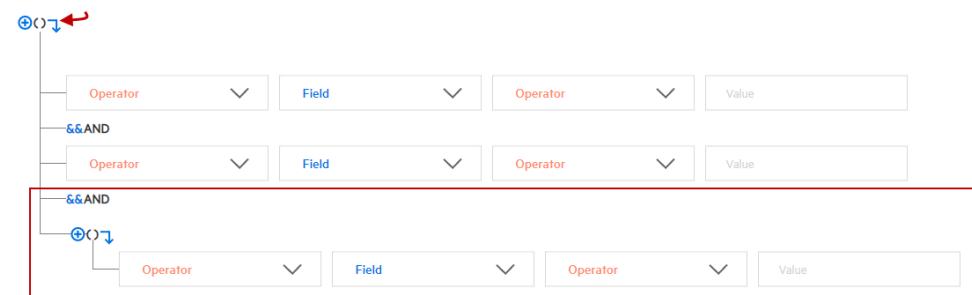


Note: Only routable topics are displayed in the drop-down list for both **Source Topic** and **Destination Topic** when adding a new route. This option is only available for Transformation Hub 3.4.

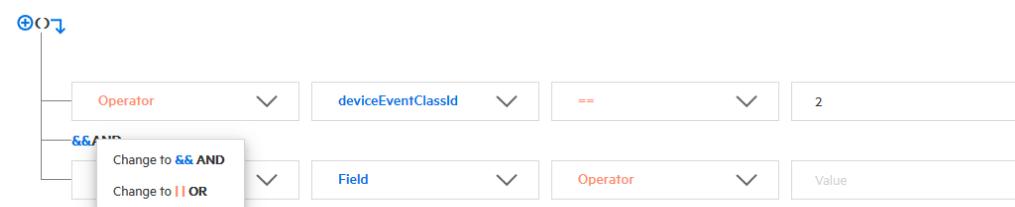
- Define a criterion by using the drop-downs to select a **Field**, **Operator**, and **Value** as a filter. **Fields** and **Operators** are based on the **Source Topic** type.
- Click + to add a new conjunction (& AND, || OR), or the right arrow to add a dependent conjunction. Then define any new required criteria as needed.



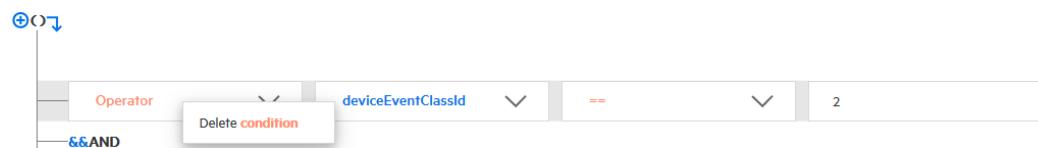
- You can create nested conjunctions by clicking the right arrow at the same level as the current conjunction.



- To change a conjunction, right-click the conjunction and select your choice from the drop-down menu.



- To delete a conjunction, right-click the conjunction and pick Delete. Note that deleting a conjunction will delete all the criteria associated with the deleted conjunction.



Note: If users have more than two source topics in routing, they need to increase service group through the CDF UI for the routing configuration. For more information please see the [Administrator's Guide for the ArcSight Platform](#).

The rule is shown in the rule field as you construct it. When the rule is complete, click **Save**.

Editing a Route

To edit a route:

1. Click **Configuration Management > Transformation Hub > Routes**.
2. On the Transformation Hub Configurations page, select the route to edit, then click **Edit**.
3. Edit the route as needed, then click **Save**.

Deleting a Route

To delete a route:

1. Click **Configuration Management > Transformation Hub > Routes**.
2. On the Transformation Hub Configurations page, select one or more routes to delete, then click **Delete**.
3. Click **Yes** to confirm deletion.

Deployment Templates

A *deployment template* is a pre-set collection of settings and parameters for a connector or Collector.

When you deploy that connector or Collector type using the Instant Connector Deployment process, and specify a deployment template, all of the settings you have predefined in the template are applied during the deployment.

You may specify any number of deployment templates for each connector type.



Note: During the deployment process, you are prompted to use the predefined template settings, but may choose to overwrite any of the predefined template settings to custom-fit a particular deployment.

Managing Deployment Templates



You should be familiar with the settings for connectors and Collectors before managing deployment templates. These settings are described in detail in the [Smart Connector User's Guide](#).

Prior to managing any deployment templates, first upload the appropriate 64-bit connector or Collector installer file to your ArcMC repository. Only the Linux and Windows 64-bit installers

are supported. The installer contains a list of currently supported connectors or Collectors and is used in the creation of the connector or Collector list in ArcMC. This upload only needs to be done in preparation to manage deployment templates.

To upload the installer file to ArcMC:

1. Download the connector or Collector installer file to a secure network location.
2. In ArcMC, click **Administration > Application > Repositories**.
3. In the navigation menu, click **Upgrade Files**.
4. Click **Upload**.
5. Under **Upload Upgrade Repository**, click **Choose File**. Then, browse to and select the installer file you previously downloaded.
6. Click **Submit**. The installer file is uploaded to ArcMC.

Additional Files

Note that some connector types may require additional, supplementary files to function correctly, such as Windows DLLs. Such files are not included in the connector installer file.

If additional files are required for a connector type, you must also upload these files to an ArcMC repository before attempting to deploy them using the Instant Connector Deployment process. After uploading the installer file as described, upload additional files (in ZIP format) to the following repositories:

File Type	Repository
SecureData server certificate (Certificate_FPE)	cacert. Note: The certificate must be Base 64 encoded. For Linux platforms (only), it must include the .pem extension.
Windows DLL, JavaLibrary	JDBC Drivers
FlexParsers	Flex Connectors

You will be able to specify the location of these additional files when you create the deployment template.

To create a deployment template:

Click **Configuration Management > Deployment Templates**.

1. In the navigation menu, from the list of supported connectors or Collectors, select the type of connector/Collector for which you wish to create a template.
2. In the management panel, click **New**.
3. To clone a template from an existing template of the same type, click **+ New/Clone**.

To clone a template, select one from the **Copy from** dropdown and the values are populated based on the selected template instance.

4. Specify values for any required settings (marked with an asterisk *), as well as any settings you wish to apply to all connectors or Collectors of that type when using Instant Connector Deployment. (**Note:** Spaces in file or path names are not supported.)
5. If additional files are needed for operation, such as a Voltage server certificate, under **File Table Fields**, specify values for file name, type, and any other required fields. If more than 1 additional file is needed, click **Add Row**, then specify the details of the additional file. Repeat for additional files as needed.
6. Click **Save**.



ArcSight SecureData Add-On Enablement: To enable the ArcSight SecureData Add-on during deployment, under **Global Fields**, set **Format Preserving Encryption** to *Enabled*. Note that only a single instance of the add-on is supported on Windows clients. If you wish to move the add-on to a new location, you must first uninstall the previously installed client before launching Instant Connector Deployment.

To delete a deployment template:

1. In the navigation menu, browse to the template you wish to delete. (Templates are sorted by connector/Collector type.)
2. In the management panel, select the template and click **Delete**. Click **Yes** to confirm deletion.

Bulk Operations

The following topics are discussed here.

Location

The **Location** tab displays all locations defined in Arcsight Management Center. The **Location** tab includes these buttons:

Add	Adds a new location. For more information, see " Adding a Location " on page 95
Edit	Edits the name of a location. For more information, see " Editing a Location " on page 95
Delete	Deletes one or more selected locations from ArcMC. For more information, see " Deleting a Location " on page 96

The **Manage Locations** table displays these parameters for each location.

- **Name:** Location name.
- **Number of Hosts:** Number of hosts assigned to the location.

Host Tab

The Host tab displays all hosts associated with the location selected in the navigation tree. The Hosts tab includes these buttons:

Update Credentials	Updates the host's credentials. For more information, see " Updating Host Credentials " on page 232
Download Certificate	Downloads the host's current certificates. For more information, see " Downloading and Importing Host Certificates " on page 232
Scan Host	Scans each port on non-appliance based hosts. For more information, see " Scanning a Host " on page 233
Move	Moves selected hosts to a new location. For more information, see " Moving a Host to a Different Location " on page 235
Delete	Deletes selected hosts from ArcMC. For more information, see " Deleting a Host " on page 235

The **Hosts** table displays these parameters for each host:

- **Hostname:** Fully qualified domain name (FQDN) or IP address of the host. The hostname must match the hostname in the host's SSL certificate. (If IP address was used to add the host, then the certificate will match the IP address used.)
- **Path:** Path to the host.
- **Agent Version:** Version number of the Arcsight Management Center Agent running on the host.

- **Issues:** Status of any issues associated with the host. Possible indicators include:
 - *None:* No issues are associated with the host.
 - *Internet connection Not Present:* The host is currently not reachable by internet connection. Displayed when ArcMC is not able to connect to the Marketplace for retrieving parser upgrade versions. If the user environment needs a proxy server for an internet connection, [configure the logger.properties file](#). If the user environment is an appliance, save the DNS settings on the **System Admin > Network** page.
 - *Valid Marketplace Certificate Not Found in ArcMC:* Displayed when the Marketplace certificate does not match the one found in ArcMC's trust store.
 - *Host Certificate Mismatch:* The hostname does not match the hostname in the SSL certificate. For instructions on downloading and importing certificates for the host, see ["Downloading and Importing Host Certificates" on page 232](#). If this issue is displayed for the localhost, and the certificate cannot be downloaded, please restart the web service on the localhost.
 - *ArcMC Agent Out of Date:* The host's Agent version cannot be upgraded from the managing ArcMC, or the Arcsight Management Center cannot communicate with the Arcsight Management Center Agent on the managed node. You may need to manually install the ArcMC Agent. For requirements and instructions, see ["Installing the Arcsight Management Center Agent" on page 35](#)
 - *ArcMC Agent Stopped:* The Agent process on the host has been stopped.
 - *ArcMC Agent Upgrade Recommended:* The host's Agent version is older than the one on the managing ArcMC. An Agent upgrade is recommended.
 - *ArcMC Agent Uninstalled:* The Agent on the host has been uninstalled.
 - *ArcMC Agent Down:* The Agent on the host is not running.
 - *Update the authentication credentials on the localhost, then install the ArcMC Agent:* For a localhost added for remote management, [authentication credentials need to be updated](#) to ensure authentication, then the [ArcMC Agent needs to be installed](#) to enable management. Take both of these steps to correct this issue.
 - *Error in REST Authentication:* The Transformation Hub node lacks the ArcMC certificate, ArcMC session ID, or ArcMC URL and port. To resolve this issue:
 - Make sure that the CDF Cluster has been configured correctly with the appropriate ArcMC details. For more information, please see [Configuring ArcMC to Manage a Transformation Hub](#).
 - Note that each time the user replaces the ArcMC certificate to the TH's location, the TH's webservice pod has to be restarted for the new certificate to be read and updated in the trust store.
- **Model:** If the host is an appliance, this shows the ArcSight model number of the appliance. If the host is not an appliance, the label *Software* is shown.

- **Type:** Type of installation, either ArcMC Appliance or Software.
- **Version:** Version number of the software on the host.

Container Tab

The Containers tab includes the **Properties** button, it allows you to modify the properties of Containers.

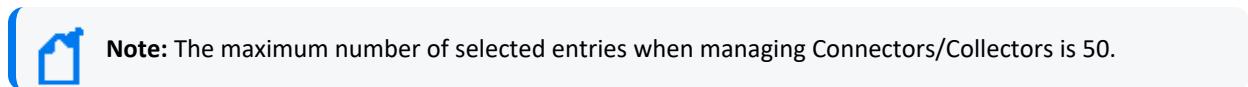
The **Containers** table includes the following columns:

- **Name:** Name of the container.
- **Path:** Path to the container.
- **Issues:** Status of any issues associated with the container.
- **Port:** Port number through which the container is communicating.
- **Framework Ver:** Framework version number of the container.
- **Parser Ver:** Parser version number of the container.
- **Status:** Status of the container. Possible values for container status are:
 - *Improper configuration: Initial default state.*
 - *Initializing connection:* The connector has a resolvable URL, but Arcsight Management Center has not logged in to the connector yet.
 - *Down:* There was an exception trying to execute the login command.
 - *Unauthorized:* The login command was executed, but login has failed.
 - *Connecting:* The login is in progress.
 - *Connected:* The login was successful.
 - *Empty:* Login successful, but the container doesn't have connectors.
 - *Initialized:* Login successful and the container has connectors.
 - *Unknown:* No information on status. To resolve, manually SSH to the system and restart the container.
- **Last Check:** Date and time of last status check.

Collector Tab

The **Collector** tab displays all Collectors associated with the item selected in the navigation tree. For example, if you selected a host in the navigation tree, the **Collectors** tab would show all Collectors associated with that host.

A Collector is a standalone System component in charge of processing efficiency improvements and the collection of raw data.



The **Collectors** tab includes the following buttons, which operates on one or more selected Collectors:

Properties	Update the properties of the selected Collectors. For more information, see " Updating Collector Properties " on the next page
Retrieve Logs	Retrieves Collector logs. For more information, see " Retrieving Collector Logs " on the next page
Update Parameters	Update the parameters of the selected Collectors. For more information, see " Updating Collectors Parameters " on the next page
Destinations	Manage Collector destinations. For more information, see " Updating Collector Destinations " on page 227
Credential	Manage Collector credentials. For more information on managing Collector credentials, see " Updating Collector Credentials " on page 227
Restart	Restart the selected Collectors. For more information on restarting Collectors, see " Restarting Collectors " on page 227.
Delete	Deletes the selected Collectors. For more information, see " Deleting Collectors " on page 228

The **Collectors** table displays the following parameters for each connector:

- **Name:** Name of the Collector.
- **Port:** Collector port.
- **Type:** Type of Collector.
- **Syslog Lines Received:** Number of events received.
- **Custom Filtering:** messages filtered out.
- **Status:** Collector status.
- **Version:** Collector version.
- **Last Check:** Date and time of the last status check.

Transformation Hub Tab

The **Transformation Hub** table includes the following columns:

- **Transformation Hub:** Name of the Transformation Hub.
- **Host:** Name of the host.
- **Port:** Port number through which the Transformation Hub is communicating.
- **Last Check:** Date and time of the last status check.

For more information on connector management, see "[Managing Connectors](#)" on page 141

Updating Collector Properties

To update Collector properties:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select the item you wish to manage.
3. Click **Properties**.
4. On the **Property Update** page, click **Edit**
5. Edit the Collector properties as needed.
6. To add a new property, specify the property, a value for the property, and click the check mark.
7. When complete, click **Save**.

Retrieving Collector Logs

To retrieve Collector logs:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Bulk Opeartions** page, select one or more items for which you wish to retrieve logs.
3. Click **Retrieve Logs**.
4. Follow the wizard prompts to zip the selected logs into a single file.
5. To view the logs, on the main menu bar, click **Admin > Repositories**. The log zip file is stored in the *Logs* respository.

Updating Collectors Parameters

To update Collector parameters:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select one or more items for which you wish to update parameters.
3. Click **Update Parameters**.
4. On the **Collector Parameter Update** page, specify values for the parameters, as needed.
5. Click **Save**. The parameters are updated for the selected items.

Updating Collector Destinations

To update Collector destinations:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select one or more items for which you wish to update destinations.
3. Click **Update Destinations**.
4. On the **Collector Destination Update** page, specify values for the destinations, as needed.
5. Click **Save**. The destinations are updated for the selected items.

Updating Collector Credentials

To update Collector credentials:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select one or more items for which you wish to update credentials.
3. Click **Credential**.
4. On the **Collector Credential Update** page, specify values for passwords, as needed. (The username is fixed as *collector*.)
5. Click **Save**. The passwords are updated for the selected Collectors.

Note: Updating Collector credentials from ArcMC does not update the actual credentials, just the credentials ArcMC uses to authenticate.

Restarting Collectors

To restart one or more Collectors:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select one or more items which you wish to restart.
3. Click **Restart**.
4. Click **Yes** to confirm restart. The Collectors are restarted.

Deleting Collectors

To delete Collectors:

1. Click **Configuration Management > Bulk Operations**.
2. On the **Manage Collectors** page, select one or more items which you wish to delete.
3. Click **Delete**.
4. Click **Yes** to confirm delete. The items are deleted.

Enabling SecureData Encryption on Managed Connectors

SecureData can be enabled as part of the [Instant Connector Deployment](#) process. However, you can also enable SecureData encryption on connectors or containers you [already manage in ArcMC](#).

To enable SecureData encryption on connectors or containers you already manage in ArcMC:

1. Ensure that the remote VM can communicate with the SecureData server. If not, edit the hosts file or configure DNS to enable communication.
2. If there is a certificate for the SecureData server, make sure it is successfully imported to the remote VM.
3. Ensure proxy settings allow the SecureData client to communicate with the SecureData server.
4. Install the SecureData client manually on the remote VM where the connectors reside.
5. Finally, in ArcMC, select the connectors or containers. Perform the Modify Property operation and provide the necessary SecureData and proxy details.

Prerequisites for Addition of SecureData Client to Multiple Containers

The following are prerequisites for the addition of the SecureData client to multiple containers.

- The process should be performed by an account with which the Connector was installed.



Note: If this user was a non-root user, that user must have access to the directory on the destination host with all permissions.

The process must have a dedicated port numbered higher than 1024.

Bulk SecureData client install is supported for accounts using SSH key authentication, but not supported for SSH with passphrase authentication. To enable SSH key authentication, the SSH key needs to be set up between a non-root user of ArcMC and a user of the remote host.

- You should consult and review the Format Preserving Encryption Environment Setup Guide for proxy settings.
- All the selected container host machines need to have same SSH credentials (username:password).
- The voltage client install path on all the selected containers hosts must be the same.
- You can only push voltage client in bulk to all the container hosts that are on the same platform e.g. all Linux, or all Windows.
- The below prerequisites are not present by default on RHEL/CentOS 8.x, unlike in previous RHEL/CentOS versions (e.g. RHEL/CentOS 6.x and 7.x). Perform the following steps for RHEL/CentOS 8.1 on the machine where the ArcMC is or will be installed, and in the target RHEL/CentOS host (the VM where the Connector/Collector will be deployed):

a. Install python2:

For RHEL/CentOS 7.x:

```
sudo yum install -y python2
```

For RHEL/CentOS 8.x:

```
sudo dnf install -y python2
```

b. Create a symlink:

```
sudo ln -s /usr/bin/python2 /usr/bin/python
```

c. Install libselinux-python package:

For RHEL/CentOS 7.x:

```
sudo yum install -y libselinux-python
```

For RHEL/CentOS 8.x:

```
sudo dnf install -y libselinux-python
```



Note: If the yum/dnf command fails when installing libselinux-python on RHEL/CentOS, follow the steps below:
 - Download libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm
 - Install the package:
 rpm -i libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm

Additional Requirements For Windows Platforms

For Windows platforms, only the local admin account is supported for the bulk-addition of the SecureData client.

In addition, the following preparatory steps are required when deploying on a Windows VM.

1. Enable PowerShell 4.0 or later.

<https://www.microsoft.com/en-us/download/details.aspx?id=40855>

2. Enable and configure PowerShell Remoting, with CredSSP authentication.

- Download the "ConfigureRemotingForAnsible.ps1" file:
 - <https://github.com/ansible/ansible/blob/devel/examples/scripts/ConfigureRemotingForAnsible.ps1>
- Open Power Shell as Administrator and run the following command:
 - ConfigureRemotingForAnsible.ps1 -EnableCredSSP

3. Enable TLS 1.2.

Adding SecureData to Multiple Containers

You can add the SecureData encryption client to multiple containers at once. The following limitations apply:

- The selected containers must meet all [prerequisites for adding SecureData](#).
- All selected container hosts must have the same user credentials (username and password), and must be the same platform (that is, all Windows or all Linux.)
- The SecureData client installation path on all container hosts will be the same.
- If a certificate is needed, upload the required certificate before proceeding to **Repositories > CA Certs**.



Note: CTHs cannot be configured with SecureData encryption.

To add SecureData encryption to multiple containers:

1. Click **Configuration Management > Bulk Operations**
2. On the **Container** tab, select the containers to which you wish to add SecureData encryption.
3. Click **Properties**.
4. On the Container Property Update dialog, click **Edit**.
5. in the **Property List** column, click the **Settings** icon, then search for any values with fpe in the name. Change or specify values for these properties as follows.

Property	Description
fencryption.enabled	If true, SecureData (Format Preserving) Encryption is enabled. Once enabled, encryption parameters cannot be modified. A fresh installation of the connector will be required to make any changes to encryption parameters.
fencryption.host.url	URL of the SecureData server

Property	Description
https.proxy.host	Proxy SecureData server (https)
https.proxy.port	Proxy port
fpencryption.user.identity	SecureData identity
fpencryption.shared.secret	SecureData shared secret
fpencryption.event.fields	Comma-separated list of fields to encrypt.
fpencryption.voltage.installdir	Absolute path where the SecureData client needs to be installed

6. Select Install SecureData Client.
7. To use SSH key-based authentication to Linux container hosts (only), select **SSH Key**.



Note: SSH key applies to Linux hosts only. If the SSH Key check box is selected for Windows hosts, the update will fail.

8. If needed, from the **SecureData Cert** drop-down, select a previously-uploaded certificate for SecureData.
9. In **Username** and **Password**, specify the common user credentials for all selected container hosts. (Password is not needed if SSH is enabled in Step 7.)
10. Click **Save**.

The SecureData client is pushed to the selected containers, and each one is restarted. To see if the encryption properties were updated successfully, wait on this page. The [Job Manager](#) shows the status of client installation on the containers.

Updating Transformation Hub Cluster Details in ArcMC

When you upgrade the Transformation Hub cluster to the latest version, and if you choose to manage the whole cluster with ArcMC, you need to update the cluster details in ArcMC. Doing this enables you to deploy CTHs on the latest version of the Transformation Hub cluster.



Note: Make sure that the **Cluster Username**, **Cluster Password**, and **Certificate** information, correspond to the upgraded version of the Transformation Hub.

To update Transformation Hub Cluster Details in ArcMC:

1. Click **Configuration Management > Bulk Operations**
2. Click the **Host** tab.
3. Select the Transformation Hub host.
4. Click **Update Cluster Details**.

5. In the **Hostname** field, type the fully qualified name of the TH.
6. In the **Cluster Port** field, type **443**.
7. In the **Cluster Username** field type the TH username.
8. In the **Cluster Password** field type the TH password.
9. SSH to the Transformation Hub and go to: /opt/arcsight/kubernetes/scripts/
10. Run the following script to generate the certificate: cdf-updateRE.sh
11. Copy the certificate name ca.crt (be sure to include from ----- BEGIN CERT to END CERT ---- -), navigate to the GUI, paste it on the **Cluster Certificate** field and click **Save**.

Updating Host Credentials

relies on a host's login credentials to connect and authenticate to the managed host. You specify these credentials when adding the host to for management. If these credentials ever change, the management link between and the host will be broken.

However, you can update the credentials uses to authenticate to a managed host, which will prevent the management link from being broken.

Updating host credentials on does not change the actual credentials on the managed host. You will need to change those on the host directly, either immediately before or immediately after performing this operation. Updating credentials will only update the credentials that uses to authenticate to the host.

To update host credentials:

1. Click **Configuration Management > Bulk Operations**.
2. Click the **Host** tab.
3. Select the host you want to update, click **Update Credentials**.
4. In **Username** and **Password**, specify the new credentials that will use to connect to the host.
5. Click **Save**.

Downloading and Importing Host Certificates

In case of a mismatch between the hostname and the hostname in the SSL certificate, you can download and import the host's current certificates.

To download and import host certificates:

1. Click **Configuration Management > Bulk Operations**.
2. Click the **Hosts** tab.
3. Select the desired host.
4. Click **Download Certificate**.
5. Click **Import** in the wizard and then Click **Done**.

Scanning a Host

Scanning a host will inventory all currently running containers on the host and the connectors associated with them.

To ensure accuracy and currency of container inventory, you will need to manually scan for new containers in any of the following circumstances:

- Additional containers or connectors are added to a remote host after it has been added to Arcsight Management Center.
- Containers and connectors are removed from a remote host managed in Arcsight Management Center.
- Any containers which were down when the initial, automatic scan was performed have since come back up.
- The license for a managed ArcSight Management Center (managed by another ArcSight Management Center) is upgraded to increase the number of licensed containers.

Any host that includes containers is scanned automatically when first added to ArcSight Management Center.

You can manually scan any host types that can run containers. These types include:

- Connector Appliances
- Loggers (L3XXX models only)
- ArcSight Management Center Appliances
- Connectors

The Scan Process

A host scan retrieves information on all CA certificates from any running containers on the host. The containers on the remote host can be managed only if Arcsight Management Center can authenticate using the certificates and the credentials. You are prompted to import any retrieved certificates into the Arcsight Management Center trust store.

A manual scan will be discontinued if any of the following are true:

- Any containers on a scanned Connector Appliance host are down.
- If you choose *not* to import any certificates that are retrieved.
- Authentication fails on any of the containers.

Note: When a Collector and connector are intended to run on the same host, add the Collector to ArcMC first, before the connector. Then perform a scan host to correctly detect the connector.

To manually scan a host:

1. Click **Configuration Management > Bulk Operations**.
2. In the navigation tree, select the location to which the host has been assigned.
3. Click the **Host** tab.
4. Select the host you want to scan, click **Scan Host**. The Host Scan wizard starts.
5. Specify values for the parameters in the following table, then click **Next**.

Parameter	Description
Starting Port	The port number on the host on which Arcsight Management Center starts scanning for containers.
Ending Port	The port number on the host on which Arcsight Management Center ends scanning for containers.
Connector Username	The Connector user name to authenticate with the host.
Connector Password	The password for the Connector you provided.
Collector Username	The Collector user name to authenticate with the host.
Collector Password	The password for the Collector you provided.

6. Connector certificates are retrieved automatically so that the Arcsight Management Center can communicate with each connector in a container. The Host Scan wizard lists the certificates. (To see certificate details, hover over the certificate.)
 - To continue the scan, select **Import the certificates**, then click **Next** to import the certificates and continue.
 - Otherwise, select **Do not import the certificates**, and then click **Next**. The Host Scan wizard discontinues the scan.

Moving a Host to a Different Location

You can assign one or more hosts to a new location. When you move a host, any nodes associated with it are also moved. For example, if you moved a Connector Appliance to a new location, all of its containers and managed connectors would also be moved to the new location.

To move one or more hosts:

1. Click **Configuration Management > Bulk Operations**.
2. Click the **Hosts** tab.
3. Select one or more hosts to move.
4. Click **Move**.
5. Follow the prompts in the **Host Move** wizard. The selected hosts are reassigned to their new locations.

Deleting a Host

When you delete a host, any nodes associated with the host are also deleted. Deleting a host removes its entry from ArcSight Management Center, but otherwise leaves the host machine unaffected.



Note: Use caution when deleting a host. Deleting a host will delete its associated nodes from any node list, association, peers listing, or subscribers listing that includes those nodes.

To delete one or more hosts:

1. Click **Configuration Management > Bulk Operations..**
2. Select one or more hosts to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion. The host (and any associated nodes) are deleted.

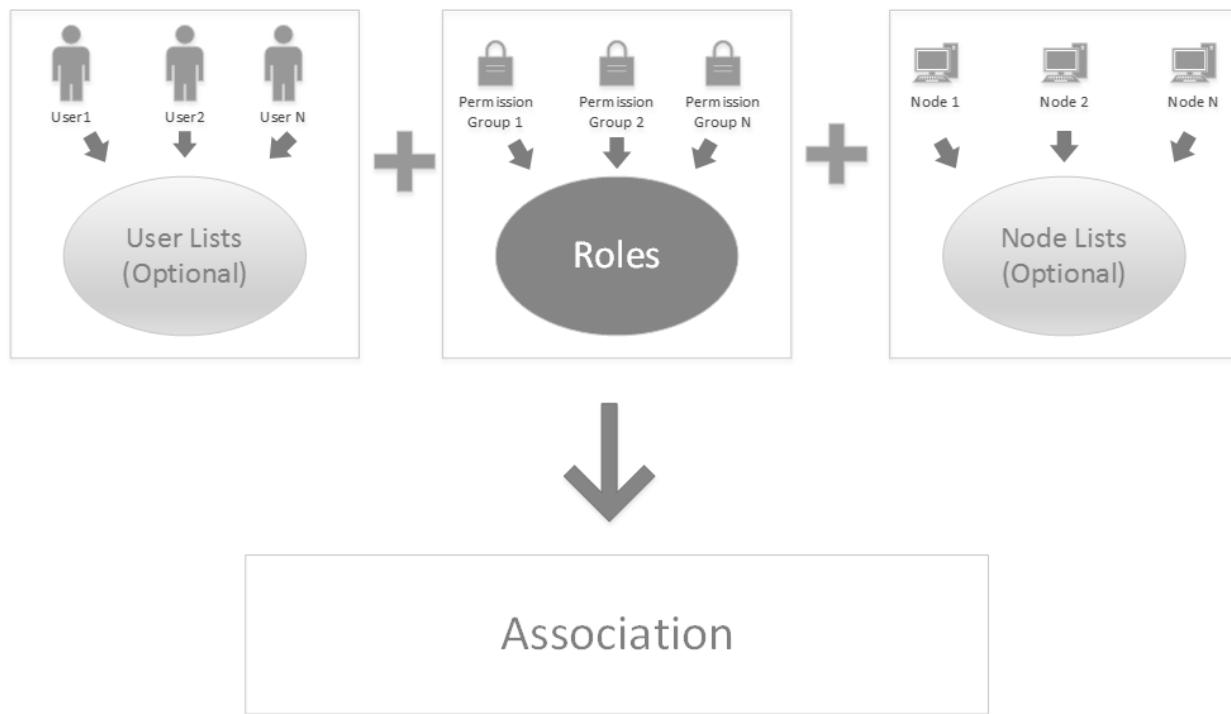
Chapter 8: Managing Users on Managed Products

Role-based access control (RBAC) user management enables you to manage product user access with custom roles across specified nodes.



Previous versions of ArcMC included user management across nodes as part of Configuration Management (where user information was defined in a Users configuration). In ArcMC 2.1, user management across nodes is now a separate, greatly improved RBAC (role-based access control) functionality.

User Management Workflow



User management in ArcSight Management Center follows this workflow:

1. Create users in ArcSight Management Center, or import them from managed nodes.
2. Optionally, group users into [user lists](#) for ease of organization and management.
3. Create (or import) [permission groups](#) to enable administrative privileges.
4. Create [roles](#) by assigning permission groups to grant functional access to products.
5. Optionally, create [node lists](#) to ease the organization of sets of nodes.
6. Create [associations](#) to associate users (or user lists), nodes (or node lists), and roles.

7. [Push associations to nodes](#) to enable access for users included in the association, with privileges appropriate for the role and access only to the desired nodes.
8. [Check compliance](#) of users on managed nodes with the managing ArcMC.

The following topics are discussed here.

Users and User Lists

A *user* is defined by a set of values for an individual's credentials and other identifiers, such as first and last name, email, and phone number. On nodes managed by ArcMC, users of those nodes and their permissions can be managed entirely by ArcMC.

Users can be grouped into named *user lists*, which can also be assigned access rights in the same way as individual users.

You can also import users from managed nodes.

Users are defined by these parameters:

Parameter	Description
User Name*	Name used for login credentials.
First Name*	User's first name.
Last Name*	User's last name.
Distinguished Name	User's distinguished directory name, if any.
Email*	User email address. Users pushed to nodes as part of an association will receive email confirmation of their new access to nodes at this address, along with a randomly generated password. (Please verify that this is the correct email address. Once pushed, the password will not be resent to a corrected email address.) Note: To ensure email alerts are sent, enable SMTP services and then restart the web services.
Title	User's job title.
Department	Department of employment.
Phone	Phone number for the user.
Notes	Relevant notes on the user.

To create a user:

1. Click **User Management > Users and User Lists**.
2. Click **New User**.
3. Specify values for the user details.
4. Click **Save**.

To import users from a managed node:



Note: Only US ASCII characters are supported for import.

1. Click **User Management > Users and User Lists**.
2. Click **Import User**.
3. On the node list, select the node from which you will import users.
4. On the **Import Users** page, use the arrow keys to move selected users from the **Available Users** list to the **Selected Users** list.
5. Click **Import**. The selected users are imported into .

To create a user list:

1. Click **User Management > Users and User Lists**.
2. Click **New User List**.
3. In **User List Name**, specify a name for the user list.
4. The **Selected Users** column shows all users currently selected for the users list. Use the directional arrows to add to, or remove from the **Available Users** list to the **Selected Users** list.
5. Click **Save**.

To edit a user or user list:

1. Click **User Management > Users and User Lists**.
2. On the **Users and User Lists** page, click the name of the user or user group you wish to edit.
3. Edit the user or user list as needed, then click **Save**. Click **Save As** to save an edited user list under a new name.

To delete users or user lists:

Use caution when deleting users. Deleting a user on ArcMC will delete the user from all nodes where the user was pushed as part of an association.

In order to delete a user, any nodes on which the user is present must be able to communicate with ArcMC.



You can only delete a user list if it is not part of any association. To delete a user list that is part of an association, delete the association first.

1. Click **User Management > Users and User Lists**.
2. On the **Users and User Lists** page, select the users or user lists you wish to delete.

3. On the toolbar, click **Delete**.
4. Click **Yes** to confirm deletion.

For information on how to assign users to roles, see "["Roles" on page 241](#)".

Permission Groups

A *permission group* is a set of access privileges. Access privileges are organized functionally, enabling you to assign different functions or different product access across users.

Permission groups are the building blocks of [roles](#). In themselves, permission groups do not enable access for any users. Permission groups can be bundled into [roles](#), and when users are assigned to those roles, they will gain the privileges which the individual permission groups grant them.

Permission groups can be created, imported from managed nodes, edited, and deleted in ArcMC.

You can create permission groups of the following types in ArcMC.

Group Type	Grants access to...
System Admin	System admin and platform settings.
Logger Rights	Logger general functionality. Does not include Logger Reports and Logger Search permissions.
Logger Reports	Logger report functionality.
Logger Search	Logger search functionality.
Conapp Rights	Connector Appliance general functionality.
ArcMC Rights	Arcsight Management Center general functionality. Note that ArcMC rights <i>View options</i> and <i>Edit, save and remove options</i> can only be granted to groups with either <i>View management</i> or <i>Edit, save, and remove management rights</i> .

You can create different permission groups to reflect different management access levels. For example, you could create two System Admin permissions groups, one with access to reboot and update privileges, and the other with access to global settings. However, a role can only be assigned one permission group per group type.

To create a permission group:

1. Select **User Management > Permission Groups**.
2. On the **Permission Groups** page, click **New**.
3. In **Group Name**, specify a name for the new group.
4. Select a type from the **Group Type** drop-down list.

5. In **Description**, specify a brief description of the permission group.
6. In the **Rights** list, select the rights to which the permission group controls. (Click **Select All** to select all rights in the list.)
7. Click **Save**.

To import one or more permission groups from a managed node:



Note: Only US ASCII characters are supported for import.

1. Select **User Management > Permission Groups**.
2. On the **Permission Groups** page, click **Import**.
3. From the list of managed nodes, select the node from which to import a group, then click **Next**.
4. The **Available Permission Group(s)** column shows available permission groups on the managed node. Select one or more groups, then use the **Add** button to move them to the **Selected Permission Group(s)** column. (Note that permission groups already present in ArcMC will be shown as disabled and unavailable for selection.)
5. Click **Import**. The groups are imported into ArcMC.

To edit a permission group:

1. Select **User Management > Permission Groups**.
2. From the list of groups, click the name of the group you wish to edit.
3. Specify values or select rights as needed.
4. Click **Save**. (Click **Save As** to save the group under a new name.)

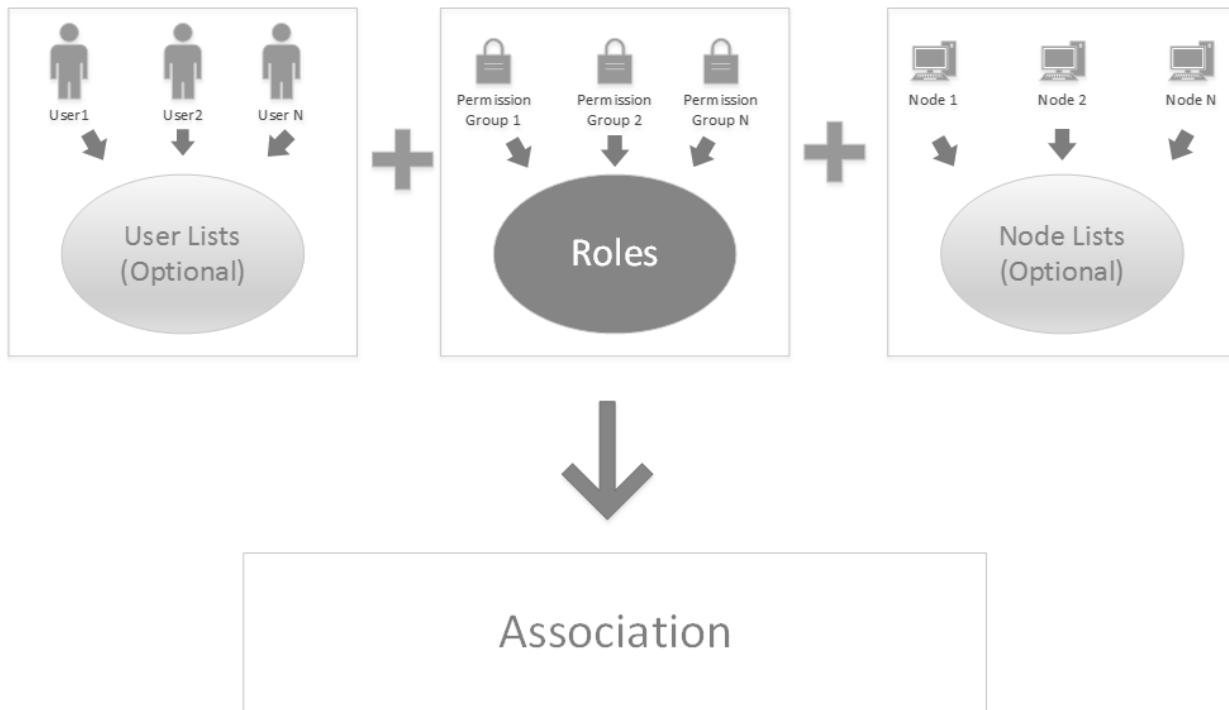
To delete a permission group:



You can only delete a permission group that is not currently assigned to any roles, nor is part of any **Filter** configuration.
To delete a permission group that is part of a role, delete the role first.
To delete a permission group that is part of a Filter configuration, remove it from the configuration.

1. Select **User Management > Permission Groups**.
2. From the list of groups, select the group you wish to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Roles



A *role* is a bundled set of [permission groups](#). By assigning a role to an association, you grant all privileges enabled by the role's component permission groups to all of the users or user lists in the association.

You can create and delete roles in ArcMC.

To create a role:

 **Note:** Prior to creating a role, create any [permission groups](#) it will include.

1. Select **User Management > Roles**.
2. Click **New**.
3. In **Role Name**, specify a name for the role.
4. In the **Available Permission Group(s)** column, select one or more permission groups. Use the **Add** button to move selected permission groups from the **Available Groups** column to the **Selected Permission Group(s)** column.
5. Click **Save**.

To delete one or more roles:

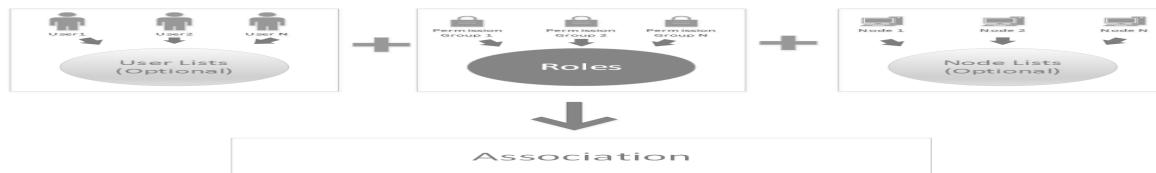


Before deleting a role, edit any associations of which it is a part to remove the role from each association.

1. Select **User Management > Roles**.
2. From the list of roles, select one or more roles to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

For information on assigning associations to roles, see "[Associations](#)" on the next page.

Node Lists



A *node list* is a named set of managed nodes. Using node lists allows you to organize nodes for the purpose of managing users of those nodes in a group.

All nodes in a node list included in an [association](#) will receive pushes of the association from .



An association is pushed only to nodes (or node lists) which it includes. To push an association to a particular node, make sure the node is included in the association, either directly or as part of a node list.

You can create, edit, and delete node lists.

To create a node list:

1. Click **User Management > Node Lists**.
2. Click **New**.
3. In the **Available Nodes** column, select multiple nodes or node lists to include. Use the **Add** button to move the selections to the **Selected Nodes** column.
4. Click **Save**.

To edit a node list:

1. Click **User Management > Node Lists**.
2. Select a node list to be edited.

3. Edit the node list as needed.
4. Click **Save**. (Click **Save As** to save the node list under a new name.)

To delete one or more node lists:



You can only delete a node list if it is not assigned to any associations. To delete a node list that is part of an association, first remove it from the association or delete the association.

1. Click **User Management > Node Lists**.
2. From the list of node lists, select one or more node lists to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Associations

An *association* is a bundled group of users (or user lists), along with any number of non-overlapping roles, and any number of nodes (or node lists). Associations are managed in and then pushed to managed nodes, in order to grant permissions to users of those nodes.

You can create associations, push them to included nodes, and delete associations.

To create an association:



Note: Prior to creating an association, create all users (or user lists), node lists, and roles to be included in the association.

1. Click **User Management > Associations**.
2. Click **New**.
3. In **Association Name**, specify a name for the new association.
4. In the **Available Users and User Lists** column, select multiple users or user lists to include. Use the **Add** button to move the selections to the **Selected Users and User Lists** column.
5. Click **Next**.
6. On the **Assign Roles** page, in the **Available Roles** column, select one or more roles to include. Use the **Add** button to move the selections to the **Selected Roles** column.
7. Roles in an association may not overlap in terms of product type.
8. Click **Next**.

9. In the **Available Nodes and Node Lists** column, select multiple nodes or node lists to include. Use the **Add** button to move the selections to the **Selected Nodes and Node Lists** column.
10. Click **Check Conflicts**. A conflict is returned if the permissions assigned in the association conflict with any other association that also assigned the same permission groups types. For example, if an existing association assigns read/write access to User A, and your newly-created new association assigns read-only rights to User A, then a conflict would be returned.
 - If a conflict was found in the association, edit the association to correct the conflict shown.
 - If no conflict was found, click **Yes** to push the new association to all nodes included in the association.

To push an association to its included nodes:

1. Click **User Management > Associations**.
2. Click the name of the association you wish to push.
3. Click **Push**. The association is pushed to its included nodes.



Note: An association is pushed only to nodes (or node lists) that it includes. To push an association to a particular node, make sure the node is included in the association, either directly or through a node list.

To edit an association:

1. Click **User Management > Associations**.
2. Click the name of the association you wish to edit.
3. Edit the components of the association as needed.
4. Click **Save**.

To delete one or more associations:

1. Select **User Management > Associations**.
2. From the list of associations, select one or more associations to delete.
3. Click **Delete**.
4. Click **Yes** to confirm deletion.

Compliance Report

The Compliance Report verifies and displays the compliance status of users on a managing ArcMC with the same users on managed nodes, to which associations including those nodes have been pushed. Compliance status includes permissions, names, and other user data.

To run the Compliance Report:

1. Click **User Management > Compliance Report**. The report displays compliance information.

The **User Info in Managing ArcMC** column displays users (or user groups) currently listed on each managing ArcMC in associations which have been pushed to nodes.

- Click the arrow to expand the column and view the permission groups for each user or user group in detail.
- Click the user name or user group name to view the current permission groups assigned to each user or user group.
- *User N/A* indicates that a user is present on the managed node but not on the managing ArcMC.
- *Permission Group N/A* indicates that user or user group currently has permissions on the Managed Node that are not assigned to the destination.
- Users not in associations which have been pushed to nodes are not shown.

The **User Info on Managed Node** column displays the users, user groups, or permission groups currently listed on the managed node being compared.

The **Compliance** column indicates the compliance of the user on the managed node to the user on the managing ArcMC. A status of *Compliant* indicates that all user values match; *Non-Compliant* means one or more values do not match or are missing.

Click the compliance status for a detailed view of each user value.

Matches	Indicates that the value on the managed node matches the value on the managing ArcMC.
Does Not Match	Indicates a discrepancy between the value on the managed node and the managing ArcMC.
Missing Value(s)	The value or values are missing and cannot be compared.



Note: Use the column headers to sort the tabular results across columns.

To export the compliance report results to PDF, click **Export to PDF**.

Exporting PDF Reports

You can export up to 100 KB of data (maximum) in PDF reports, this is the default amount.

To increase the limit of data to be exported add the following property to the `logger.properties` file (include the new increased value in bytes):

```
pdf.reports.size.limit.content=<new value in bytes>
```

Restart the web process after editing the `logger.properties` file.

For more information, please see "["Modifying logger.properties" on page 130](#).

Chapter 9: Snapshots

Arcsight Management Center records audit and debug information, including details of any issues that can occur during normal operations. These system logs form a *snapshot* of your Arcsight Management Center activity. System logs are helpful in troubleshooting issues.

ArcSight Customer Support may ask you to retrieve and submit system logs as part of an incident investigation.

The following topics are discussed here.

Creating a Snapshot

Creating a snapshot of Arcsight Management Center creates a set of zipped log files, which you can download locally.

Retrieve Snapshot Status		
Summary		
Name:	Thread-3277	
Request ID:	NstwAEEBABCq86y4HDEbw	
Processing Time:	37 sec 462 ms	
Status:	Complete	
Action		
Database content	9/8/13 9:18 PM	197 ms
Retrieving logs	9/8/13 9:18 PM	37 sec 264 ms
Download		

To create a snapshot:

1. Click **Administration > Application > Snapshot**.
2. The **Retrieve Snapshot Status** page displays. Depending on the size of the log files, the snapshot may take a few moments to generate.
3. When ready, click **Download** to download the ZIP file locally.

Submit the snapshot file as instructed by ArcSight Customer Support.



Note: An Arcsight Management Center snapshot does not include information on the activity of the Arcsight Management Center Agent on remotely-managed hosts.

To obtain logs for Arcsight Management Center Agent activity on a managed host, access the remote host. Under **Setup > Appliance Snapshot**, click the **Download** button.

Chapter 10: Logger Consumption Report

The Logger Consumption Report includes information on your Logger data consumption. You can choose which managed Logger 6.1 (or later) nodes to include in the report.

To generate a Logger Consumption report:

1. Click **Administration > Application > Consumption Report**.
2. Use the **Add** and **Remove** arrows to add or remove nodes from the **Available Nodes** column to the **Selected Nodes** column.
3. Click **Run Report**. The report is generated for the selected nodes.
4. Click **+** to expand the data on any node to view licensing specifics.
5. To export the license report to PDF, click **Export to PDF**.
6. Specify a time range for the report.
7. Click **OK** to exit the report.

Report Data

The report displays the licensed value and actual value for data consumption by managed Loggers.

Value	Description
Licensed Consumption	Shows the data consumption to which your license entitles you. For individual ADP Loggers, the license limit will be shown as <i>Not Applicable</i> , since ArcMC tracks the overall data limit, not those of individual Loggers. Note: If an ADP Logger is managed by a version of ArcMC earlier than 2.5, then the license limit will be incorrectly shown in the report as <i>Unlimited</i> .
Actual Consumption	Shows the current value of data consumption. Click the value to display the Consumption Chart, which shows data consumption in detail.
Status	Click any status hyperlink to view individual Logger data for the last 30 days. Status values are shown as follows: <i>OK</i> if the actual value is less than or equal to the license value. <i>In Violation</i> indicates that the actual value exceeds the license value, which constitutes a violation of the terms of your license. Your license permits you a number of violations for each 30-day period, which is shown on the <i>Violations Last 30 Days</i> line. Click any hyperlink to view individual Logger data for the last 30 days.

Exporting PDF Reports

You can export up to 5 MB of data in PDF reports, this is the default size.

To increase the limit of data to be exported add the following property to the `logger.properties` file (include the new increased value in bytes):

```
pdf.reports.size.limit.content=<new value in bytes>
```

Restart the web process after editing the `logger.properties` file.

For more information, please see "["Modifying logger.properties" on page 130](#).

Follow the steps below to increase the limit of data to be exported perform:

1. Log in to the CDF Management Portal. See [Accessing the CDF Management Portal](#) for more information.
2. From the left menu select **Deployment > Deployments**.
3. Click ... (**Browse**) on the far right and choose **Reconfigure**. A new screen will open in a separate tab.
4. Select the **Fusion** tab and scroll down to the **ArcMC Configuration** section to specify the desired value for the "**Maximum Exported PDF Report Size**" parameter.
5. Click **Save**. The ArcMC pod will be restarted

Chapter 11: Managing Repositories

Certain management operations require a specific upgrade or content update (.enc) file, or a certificate. Other operations, such as viewing logs, require you to load the logs to a Log repository. Arcsight Management Center can also maintain centralized repositories for files needed for host configuration and management.

By default, a number of pre-defined repositories are provided. However, you can create more repositories to suit your needs. Any repositories you create are referred to as *user-defined* repositories.

The following controls are used for repository functions:

- **Retrieve Container Files** copies a file from one or more managed hosts to the repository.
- **Upload to Repository** sends a file from your local computer (the computer running the browser) or a network host accessible from your local computer to the repository.
- **Retrieve** downloads a file from the repository.
- **Upload** copies a file from the repository to one or more managed nodes.

You can perform these operations using repositories:

- Manage logs in the Logs repository
- Manage CA certificates in the CA Certs repository
- Upgrade a connector using an upgrade file available in the Upgrade repository
- Apply a Content ArcSight Update Pack (AUP) on one or more connectors
- Maintain centralized repositories of files for connector configuration and management

The following topics are discussed here.

Logs Repository

To view logs, you need to first **Load** the logs of the container that contains the connector to the Logs repository, then **Retrieve** the logs to view them.



Note: If a container contains more than one connector, logs for all connectors are retrieved.

For information on loading, retrieving, and deleting container logs, see "[Viewing Container Logs](#)" on page 132.

Uploading a File to the Logs Repository

Uploading a file into the Log repository is useful for sharing annotated log or other files with other users. An uploaded file needs to be in .zip format.

To upload a ZIP file:

1. Click **Administration > Repositories**.
2. Click **Logs** from the left panel.
3. Click **Upload** from the management panel.
4. Specify the local file path or click **Browse** to select the ZIP file.
5. Click **Submit** to add the specified file to the repository or **Cancel** to quit.



Note: Due to a browser limitation in Internet Explorer 11, the progress of the file upload will not be shown.

CA Certs Repository

Connectors require a Certificate Authority (CA) issued or self-signed SSL certificate to communicate securely with a destination. The CA Certs repository (shown below) enables you to store CA Certs files (that contain one or multiple certificates) and single CA certificates. When certificates are stored in the CA Certs repository, you can add the certificates to a container so that the connectors in the container can validate their configured destinations.

You can add a single certificate to a container that is in FIPS or non-FIPS mode. You can only add a CA Certs file to a container that is in non-FIPS mode.

To associate a CA certificate to a connector, you need to:

- Upload the CA certificate or CA Certs file to the CA Certs repository, as described below.
- Add a CA certificate from the CA Certs repository to the container that contains the connector, as described in "[Managing Certificates on a Container](#)" on page 136.

Uploading CA Certificates to the Repository

You can upload a CA Certs file or a single certificate to the CA Certs repository.



Tip: Before you upload a single CA certificate, change the name of the certificate on the local computer to a name that you can recognize easily. This helps you distinguish the certificate when it is displayed in the Certificate Management wizard.

To upload certificates to the repository:

1. Click **Administration > Repositories**.
2. Click **CA Certs** in the left panel.
3. Click **Upload** in the management panel.

4. Specify the local path for the CA Certs file or the certificate, or click **Browse** to select it.
5. Click **Submit** to add the specified CA Certs file or the certificate to the repository, or **Cancel** to quit.

The CA Certs Repositories tab shows all the CA Certs files and single certificates that have been uploaded. The Type column shows CERTIFICATE for a single certificate and CACERT for a CA Certs file.

Removing CA Certificates from the Repository

When you delete a CA Certs file or a single certificate from the repository, it is deleted from Arcsight Management Center.



Note: When you delete a CA Certs file or a single certificate from the CA Certs repository, containers are not affected; the connectors continue to use the certificates, which are located in a trust store after being added to a container. For information about adding a CA certificate to a container, see "[Managing Certificates on a Container](#)" on page 136.

To remove a certificate from the repository:

1. Click **Administration > Repositories**.
2. Click **CA Certs** in the left panel.
3. Identify the certificate or the CA Certs file you want to remove and click the **Remove** button ().

Upgrade Files Repository

The Upgrade files repository enables you to maintain a number of connector upgrade files. You can apply any of these upgrade files to containers when you need to upgrade to a specific version. As a result, all connectors in a container are upgraded to the version you apply to the container.



Note: Logger ENC files are required for the remote upgrade of a Logger Appliance. For more information, see "[Upgrading a Logger](#)" on page 122.

About the AUP Upgrade Process



Note: The process discussed in this section only applies to upgrading connectors and to upgrading a remotely-managed Connector Appliance. If you are upgrading the local Arcsight Management Center (localhost), use an ENC file instead.

To upgrade a connector or to upgrade a remotely-managed Connector Appliance, you need to:

- Upload the appropriate .aup upgrade file to the Upgrade Files repository, as described below.
- Apply the .aup upgrade file from the Upgrade Files repository to the container (see "Upgrading All Connectors in a Container" on page 128).

Uploading an AUP Upgrade File to the Repository

To upload AUP upgrade files to the repository:

1. Download the upgrade files for the connector or the remote Connector Appliance from the ArcSight Customer Support site at <https://softwaresupport.softwaregrp.com/> to the computer that you use to connect to the browser-based interface.
2. Log in to the browser-based interface.
3. Click **SetupConfiguration > Administration > Repositories**.
4. Click **Upgrade AUP** from the left panel.
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier.
7. Click **Submit** to add the specified file to the repository or click **Cancel** to quit.
8. You can now use the AUP upgrade file to upgrade a container to a specific version. For instructions, see "Upgrading All Connectors in a Container" on page 128.

Removing a Connector Upgrade from the Repository

You can remove a connector upgrade file from the repository when you no longer need it. When you remove a connector upgrade file from the repository, it is deleted from Arcsight Management Center.

To remove a Connector upgrade from the repository:

1. Click **SetupConfiguration > Administration > Repositories**.
2. Click **Upgrade AUP** from the left panel.
3. Locate the upgrade file that you want to delete and click the associated  icon.

Content AUP Repository

ArcSight continuously develops new connector event categorization mappings, often called *content*. This content is packaged in ArcSight Update Packs (AUP) files. All existing content is

included with major product releases, but it is possible to stay completely current by receiving up-to-date, regular content updates through ArcSight announcements and the Customer Support site. The AUP files are located under Content Subscription Downloads.

The ArcSight Content AUP feature enables you to apply an AUP file to applicable connector destinations that you are managing. Only the event categorization information can be applied to the connectors using this feature.

You can maintain a number of Content AUP files in the Content AUP repository. When an AUP file with a version number higher than the ones already in the repository is loaded, it is automatically pushed out to the connector destinations being managed. However, these connectors or connector destinations are skipped:

- Connectors that are unavailable at the time of the AUP file push
- Connectors whose current version does not fall in the range of versions that the Content AUP supports
- The ESM destination on a connector
- All destinations of a connector that have an ESM destination with the AUP Master flag set to Yes

Also, when a new connector is added, the highest number Content AUP is pushed automatically to its destinations.

Applying a New Content AUP

You can add a new content AUP file to the repository and push it automatically to all applicable managed nodes.

To apply a new Content AUP:

1. Download the new Content AUP version from the support site at <https://softwaresupport.softwaregrp.com/> to the computer that you use to connect to the browser-based interface.
2. Log in to the browser-based interface.
3. Click **Administration > Repositories**.
4. Click **Content AUP** from the left panel.
5. Click **Upload** from the management panel.
6. Click **Browse** and select the file you downloaded earlier.
7. Click **Submit** to add the specified file to the repository and push it automatically to all applicable connectors, or **Cancel** to quit.

You can verify the current Content AUP version on a connector by performing either of these steps:

- Run the `GetStatus` command on the node destination and check that the value for `aup [acp].version` is the same as the AUP version you applied. For information about running a command on a connector destination, see "["Sending a Command to a Connector" on page 154](#).
- Hover over a host name to see the AUP version applied to all destinations of that connector.

Applying an Older Content AUP

If you need to apply an older Content AUP from the Content AUP repository, delete all versions newer than the one you want to apply in the repository. The latest version (of the remaining AUP files) is pushed automatically to all applicable connectors.

To delete a Content AUP from the Content AUP repository:

1. Click **Administration > Repositories**.
2. Click **Content AUP** from the left panel.
3. Locate the AUP file that you want to delete and click the associated  icon. Repeat for multiple files.

User-Defined Repositories

A *user-defined repository* is a user-named collection of settings that control upload and download of particular files from connectors to the repository. Each repository uses a specified path, relative to `$ARCSIGHT_HOME/user/agent`, for files to be uploaded or downloaded. ArcSight connectors use a standard directory structure, so map files, for example, are always found in `$ARCSIGHT_HOME/user/agent`, (that is, the root directory, `$ARCSIGHT_HOME`, of the installation path) in a folder called `map/`.

After they are created, user-defined repositories are listed on the left-side menu, under the **New Repository** heading, and appear with the user-specified display name.

User-defined repositories should be grouped by file type and purpose, such as log files, certificate files, or map files. Each user-defined repository has a name, a display name, and an item display name, which are described under the repository **Settings** tab.

Files viewed in a user-defined repository can be bulk processed with specified hosts and can be exchanged with the user's browser host.

Creating a User-Defined Repository

You can create a new repository at any time.

The repository requires correct directory paths. Your file will be applied to the wrong directory if the entered path contains errors, such as extra spaces or incorrect spellings. You can verify your directory paths by accessing the Directory.txt file, which lists the directory structure for every entered path. View the Directory.txt file by accessing your container logs and finding the Directory.txt file.

To create a new user-defined repository:

1. Click **Administration > Repositories**.
2. Click **New Repository** under the **Repositories** section in the left panel.
3. For the new repository, specify the parameters listed in the following table.

Parameter	Description
Name	A unique name for the repository, typically based on the type of files it contains.
Display Name	The name that will be displayed on the left-side menu and for tabs: Process <i>names</i> , View <i>names</i> , Settings for <i>names</i> . Typically plural.
Item Display Name	The name used to describe a single item.
Recursive	Check to include sub-folders.
Sort Priority	-1 by default
Restart Connector Process	Check to restart the connector process after file operations.
Filename Prefix	An identifying word that is included in the names of retrieved files. For example, map files are identified by Map in the file name: localhost_Container_-1.Map-2009-04-06_12-22-25-607.zip
Relative path (Download)	The path for download, relative to \$ARCSIGHT_HOME, for example, user/agent/map or user/agent/flexagent. Leave this field blank to specify files in \$ARCSIGHT_HOME. Note: The relative path is used for download only.
Include Regular Expression	A description of filenames to include. Use .* to specify all files. The following example selects properties files that consist of map, followed by one or more digits, followed by .properties: map\.[0-9]+\.properties\$

Parameter	Description
Exclude Regular Expression	A description of filenames to exclude. The following example excludes all files with a certain prefix or in the agentdata folder. (agentdata/ cwsapi_fileset_).*\$
Delete Before Upload	Check to delete earlier copies before upload. CAUTION: If you check Delete Before Upload and do not specify a Relative path (Upload), all files and folders in current/user/agent will be deleted.
Delete Groups	Whether to delete folders recursively in \$ARCSIGHT_HOME/user/agent/map directory.
Relative path (Upload)	The path for upload, relative to \$ARCSIGHT_HOME/current/user/agent/flexagent/<connectornname>
Delete Relative Path	Whether the directory specified in Relative Path (Upload) and its contents should be removed when a file is uploaded from the repository.
Delete Include Regular Expression	Typically the same as the Include Regular Expression.
Delete Exclude Regular Expression	Typically the same as the Exclude Regular Expression.

- Click **Save** at the bottom of the page.

The new repository displays under the **New Repository** heading in the left-side window panel.

Retrieving Container Files

The **Retrieve Container Files** button copies a file from one or more containers to a repository. The specific files that are retrieved depend on the settings of the repository.

To retrieve a container file:

- Click **Administration > Repositories**.
- In the left panel, under **Repositories**, click the name of the repository to which you want to copy connector files.
- Click **Retrieve Container Files** in the management panel.
- Follow the instructions in the Retrieve Container Files wizard.

Uploading Files to a Repository

To upload files to a repository:

1. Click **Administration > Repositories**.
2. In the lower left panel (under **Repositories**), click the name of the repository to which you want to upload files.
3. Click **Upload To Repository** from the management panel.
4. Follow the instructions in the Repository File Creation wizard. Select **Individual files** to create a ZIP file with appropriate path information.



Caution: Be sure **not** to change the default sub-folder name **lib** in the **Enter the sub folder where the files will be uploaded** page of the Repository File Creation wizard.

Deleting a User-Defined Repository

To delete a user-defined repository:

1. Click **Administration > Repositories**.
2. From the left panel, click the name of the repository you want to delete.
3. Click **Remove Repository** from the management panel.

Updating Repository Settings.

To update the settings of a user-defined repository:

1. Click **Administration > Repositories**.
2. In the left panel, click the name of the repository whose settings you want to update.
3. Click the **Settings for Repository_Name** tab from the management panel.
4. Update the settings.
5. Click **Save** at the bottom of the page.

Managing Files in a Repository

Retrieving a File from the Repository

To retrieve a file from the repository:

1. Click **Administration > Repositories**.
2. From the left panel, click the name of the repository in which the file exists.
3. Click  from the management panel for the file that you want to retrieve.
4. Follow the file download instructions to copy the file to your local computer.

Uploading a File to the Repository

To upload a file to the repository:

1. Click **Administration > Repositories**.
2. In the left panel, click the name of the repository in which the file exists.
3. In the management panel, click **Upload to Repository** for the file that you want to upload.
4. Follow the Upload Container Files wizard instructions to upload the file to the containers of your choice.
5. Verify that the file was uploaded correctly:
 - If you have SSH access to the connectors, connect to them and check the file structure.
 - Obtain the connector logs and check the contents of the `Directory.txt` file for each connector.

Removing a File from the Repository

To remove a file from the repository:

1. Click **Administration > Repositories**.
2. In the left panel, click the name of the repository in which the file exists.
3. In the management panel, click  for the file that you want to delete.

Pre-Defined Repositories

You can define repositories for any connector-related files. The following repositories are pre-defined:

- **Backup Files:** connector cloning (see "[Backup Files](#)" on page 263).
- **Map Files:** enrich event data
- **Parser Overrides:** customize the parser (see "[Adding Parser Overrides](#)" on page 264)
- **FlexConnector Files:** user-designed connector deployment
- **Connector Properties:** agent.properties; subset of cloning
- **JDBC Drivers:** database connectors

To view the settings for a pre-defined repository, click the name of the repository and then click the **Settings** tab in the management panel. Settings for a pre-defined repository are read-only.

Settings for Map Files

This table lists the default settings for map files.

Map File Settings

Name	Default Setting
Name	map
Display Name	Map Files
Item Display Name	Map File
Recursive	Deselected (No)
Sort Priority	5
Restart Connector Process	Deselected (No)
Filename Prefix	Map
Download Relative Path	map
Download Include regular expression	map\.[0-9]+\.\.properties\$
Download Exclude regular expression	
Delete before upload	Selected (Yes)
Delete groups	Deselected (No)
Upload Relative Path	
Delete Relative Path	map
Delete Include regular expression	map\.[0-9]+\.\.properties\$
Delete Exclude regular expression	

Settings for Parser Overrides

This table lists the default settings for parser overrides.

Parser Override Settings

Name	Default Setting
Name	parseroverrides
Display Name	Parser Overrides
Item Display Name	Parser Override
Recursive	Selected (Yes)
Sort Priority	10
Restart Connector Process	Selected (Yes)
Filename Prefix	Parsers
Download Relative Path	fcp
Download Include regular expression	.*
Download Exclude regular expression	
Delete before upload	Selected (Yes)
Delete groups	Selected (Yes)
Upload Relative Path	
Delete Relative Path	fcp
Delete Include regular expression	.*
Delete Exclude regular expression	

Settings for FlexConnector Files

This table lists the default settings for FlexConnector files.

FlexConnector Settings

Name	Default Setting
Name	flexconnectors
Display Name	FlexConnector Files
Item Display Name	FlexConnector File
Recursive	Selected (Yes)
Sort Priority	15

FlexConnector Settings, continued

Name	Default Setting
Restart Connector Process	Selected (Yes)
Filename Prefix	FlexConnector
Download Relative Path	flexagent
Download Include regular expression	.*
Download Exclude regular expression	
Delete before upload	Selected (Yes)
Delete groups	Selected (Yes)
Upload Relative Path	
Delete Relative Path	flexagent
Delete Include regular expression	.*
Delete Exclude regular expression	

Settings for Connector Properties

Connector Default Property Settings

Name	Default Setting
Name	connectorproperties
Display Name	Connector Properties
Item Display Name	Connector Property File
Recursive	Deselected (No)
Sort Priority	20
Restart Connector Process	Selected (Yes)
Filename Prefix	ConnectorProperties
Download Relative Path	
Download Include regular expression	agent\.*
Download Exclude regular expression	
Delete before upload	Deselected (No)
Delete groups	Deselected (No)
Upload Relative Path	

Connector Default Property Settings, continued

Name	Default Setting
Delete Relative Path	
Delete Include regular expression	agent\.*
Delete Exclude regular expression	

Settings for JDBC Drivers

This table lists the default settings for JDBC Drivers.

JDBC Driver Settings

Name	Default Setting
Name	jdbcdrivers
Display Name	JDBC Drivers
Item Display Name	Connector JDBC Driver File
Recursive	Deselected (No)
Sort Priority	25
Restart Connector Process	Selected (Yes)
Filename Prefix	
Download Relative Path	lib
Download Include regular expression	
Download Exclude regular expression	
Delete before upload	Deselected (No)
Delete groups	Deselected (No)
Upload Relative Path	
Delete Relative Path	lib
Delete Include regular expression	
Delete Exclude regular expression	

Backup Files

Using the **Backup Files** repository, you can quickly copy a container to other containers. As a result, all connectors in the source container are copied to the destination container. This process is called *cloning* a container configuration. You can clone a container to several

containers at once. The contents of the source container replace the existing contents of the destination container.



Caution: Containers on Arcsight Management Center are pre-installed with the latest connector release. Do not clone older, software-based connectors (such as build 4.0.8.4964) to containers with newer connector builds (such as 4.0.8.4976 or later).

Cloning a connector using the Backup repository only works if the connector version numbers are the same.

To clone a container using the Backup Files repository:

1. Click **Node Management > View All Nodes**.
2. Click the **Containers** tab to list the containers and determine the source and destination for cloning.
3. Click **Administration > Repositories**.
4. Click **Backup Files** under the **Repositories** section in the management panel.
5. If the backup file that you need to use for cloning exists in the repository, go to the next step. Otherwise, follow the instructions in "[Retrieving a File from the Repository](#)" on page 259 to retrieve the container's backup file to the Backup repository.
The retrieved filename is in the format <connector name> ConnectorBackup <date>.
6. Follow the instructions in "[Uploading a File to the Repository](#)" on page 259 to upload the backup file to one or more containers.

The destination containers are unavailable while the backup file is applied and the connectors are restarted.



Note: The backup file does not include the container certificates. You have to re-apply the certificates to the container after you upload the backup file.

After applying the certificates, check the status of the destination container to make sure it is available.

Adding Parser Overrides

A parser override is a file provided by ArcSight used to resolve an issue with the parser for a specific connector, or to support a newer version of a supported device where the log file format changed slightly or new event types were added.

To use parser overrides, you need to:

- Upload a parser override file to the **Parser Overrides** repository.
- Download the parser override file to the container that contains the connector that will use the parser override.

Follow the steps below.

To upload a parser override file:

1. Click **Administration > Repositories**.
2. Click **Parser Overrides** under the **Repositories** section in the management panel.
3. On the **Parser Overrides** tab, click the **Upload To Repository** button.
4. Follow the wizard to upload the file. When prompted by the wizard, make sure you:
 - Select the **Individual Files** option from the **Select the type of file that you want to upload** field.
 - Add a slash (/) after fcp before adding the folder name in the **Enter the sub folder where the files will be uploaded** field. For example, fcp/multisqlserverauditdb.



Note: The folder name may only contain letters and numbers. Do not include special characters such as (,), <, or >.

When the upload is complete, the parser override file is listed in the table on the **Parser Overrides** tab.

To download the parser override file to a container:

1. Click **Administration > Repositories**.
2. Click **Parser Overrides** under the **Repositories** section in the management panel.
3. In the table on the **Parser Overrides** tab, locate the parser override file you want to download and click the up arrow next to the file.
4. Follow the wizard to select the container to which you want to add the parser overrides.

When the wizard completes, the parser overrides are deployed in the selected container.



Note: You can download a parser override file from ArcExchange. For more information, refer to "[Sharing Connectors in ArcExchange](#)" on page 158.

To verify that the parser override has been applied successfully, issue a Get Status command to the connector. See "[Sending a Command to a Connector](#)" on page 154. In the report that appears, check for the line starting with ContentInputStreamOverrides.

Chapter 12: System Administration

This chapter describes the System Administration tools that enable you to create and manage users and user groups, configure SMTP and other system settings, network, storage, and security settings for your system.

This chapter includes information on the following areas of system administration:

System

From the System tab, you can configure system specific settings such as network settings (if applicable) and SMTP.

System Reboot

To reboot or shutdown your system:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **System Reboot** in the **System** section.
3. Select from the following options:

Button	Description
Reboot	Your system reboots in about 60 seconds. The reboot process normally takes 5-10 minutes, during which time the system is unavailable.
Reboot in 5 Minutes	Your system reboots after a 5-minute delay. The reboot process normally takes 5-10 minutes, during which time the system is unavailable.
Shutdown	Automatically shuts down (powers off) the system.



Note: Each of the above actions can be cancelled. “Reboot” and “Shutdown” allow for cancellation within **60 seconds**. “Reboot in 5 Minutes” can be cancelled within **300 seconds**.

4. Click **Reboot**, **Reboot in 5 Minutes**, or **Shutdown** to execute the chosen action.

Network

System DNS

The **System DNS** tab allows you to edit the DNS settings and to add DNS search domains.

To change DNS settings:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **Network** in the **System** section.
3. In the **System DNS** tab, specify new values for the IP address of the primary and secondary DNS servers, or edit the list of search domains.
To add a new domain, click the  icon. To remove a domain, click the  icon. To change the search order of domains, select a domain name, and click the up or down arrow until the domain is in the desired position.
4. Click **Save**.
5. Click **Restart Network Service** to put the changes into effect.

Hosts

The **Hosts** tab allows direct editing of your system's `/etc/hosts` file. You can specify data in the System Hosts text box or import it from a local file.

To change the Hosts information:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Network** in the **System** section, then click the **Hosts** tab.
3. In the **System Hosts** text box, specify hosts information (one host per line) in this format:
`<IP Address> <hostname1> <hostname2> <hostname3>`



When editing your `etc/hosts` file, ensure that the IP address specified each host is unique and not duplicated across hosts. A single IP address can be associated with multiple hostnames, but the same IP address may not be used for multiple hosts.

To import information from a file, click **Import from Local File**, and locate the text file on the computer from which you are accessing your system.

4. Click **Save**.

NICs

The **NICs** tab enables you to set the IP addresses for the network interface cards (NICs) on your system. Additionally, you can configure the hostname and default gateway for your system.

To set or change the NICs settings:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Network** in the **System** section.
3. In the **NICs** tab, specify the following settings. To edit the IP address , subnet mask, or speed/duplex of an NIC, select the NIC and click **Edit** above the NIC Name list.

Setting	Description
Default Gateway	The IP address of the default gateway.
Hostname	<p>The network host name for this system. Make sure that your DNS can resolve the host name you specify to your system's IP address . Performance is significantly affected if DNS cannot resolve the host name.</p> <p>This name must be identical to the domain specified in the Certificate Signing Request, described in "Generating a Certificate Signing Request (CSR)" on page 294.</p> <p>Note: If you previously used a self-signed or CA-signed certificate on this system and are now changing its host name, you must regenerate a new self-signed certificate or CSR. Once obtained, the new certificate should be uploaded to ensure that the connectors which communicate with your system are able to validate the host name. For more information about generating a CSR, see "Generating a Certificate Signing Request (CSR)" on page 294.</p>
Automatically route outbound packets (interface homing)	<p>When this option is enabled (checked box), the response packets are sent back on the same system interface on which the request packets had arrived. Enabling this option can improve performance as the routing decisions do not need to be made (using the default gateway information and static routes) to send packets out from your system. If you have static routes configured, they are ignored when this feature is enabled.</p> <p>When this feature is disabled (unchecked box), the static routes (if configured) are used to determine the interface through which the response packets should leave your system.</p> <p>If you configure only one network interface, this setting does not provide any additional benefit.</p>

Setting	Description
IP Address	<p>The IP address for each network interface card (NICs) in your system.</p> <p>Add NIC Alias</p> <p>You can create an alias for any listed NIC. To do so:</p> <ol style="list-style-type: none"> Highlight the NIC for which you want to create an alias. Click Add. Create an alternative IP address for the alias. Click Save. <p>You can identify the alias from its original by an appended colon alongside a digit indicating the number of aliases you have created on a particular NIC.</p> <p>Notes:</p> <ul style="list-style-type: none"> You cannot alter the speed of an IP alias. You can create as many aliases as you choose.
Subnet Mask	The subnet mask associated with the IP address you entered for an NIC.
Speed/Duplex	<p>Select a speed and duplex mode, or let your system determine the network speed automatically:</p> <p>Auto (recommended)</p> <p>10 Mbps - Half Duplex</p> <p>10 Mbps - Full Duplex</p> <p>100 Mbps - Half Duplex</p> <p>100 Mbps - Full Duplex</p> <p>1 Gbps - Full Duplex</p>

4. Click **Save**.
5. Click **Restart Network Service** to put the changes into effect.

Static Routes

You can specify static routes for the NICs on your system.

To add, edit, or delete a static route:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Network** in the **System** section.
3. In the **Static Routes** tab:
 - To add a new static route, click **Add**.
 - To edit or delete an existing route, select the route first, then click **Edit** or **Delete**.

When adding or editing a static route, you need to configure these settings.

Setting	Description
Type	Whether the static route is to a Network or a Host
Destination	The IP address for the static route destination
Subnet Mask	The subnet mask if you specify a network as the destination
Gateway	The IP address of the gateway for the route

- Click **Save**.

Time/NTP

The **Time/NTP** tab enables you to configure system time, date, local timezone, and NTP servers. Micro Focus strongly recommends using an NTP server instead of manually configuring the time and date on your system.

To set or change the system time, date, or time zone manually:



Caution: If you manually set the date and time settings and are also using an NTP service, the date and time entered manually cannot be more than 16 minutes ahead of or behind the time that the NTP server is providing. If the manually entered time is more than 16 minutes different from the NTP server time, then the NTP service will fail to start.

- Click **Setup > System Admin** from the top-level menu bar.
- Click **Network** in the **System** section.
- In the **Time/NTP** tab, configure these settings.

Setting	Description
Current Time Zone	<p>The time zones appropriate to your system's location. To change this setting, click Change Time Zone...</p> <p>Local times zones follow the Daylight Saving Time (DST) rules for that area. Greenwich Mean Time (GMT) + and - time zones are DST agnostic.</p> <p>For example, the America/Los Angeles time zone varies by an hour compared with GMT when DST goes into and out of effect.</p> <ul style="list-style-type: none"> Pacific Standard Time (PST) = GMT-8 Pacific Daylight Time (PDT) = GMT-7
Current Time	The current date and time at the system's location. To change this setting, click Change Date/Time... and then specify the current date and time.

- The Time Zone change requires that you reboot the appliance. However, the Current Time change takes effect immediately.

To configure your system as an NTP server or for using an NTP server for your system:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Network** in the **System** section.
3. Click the **Time/NTP** tab.
4. Under **NTP Servers**, configure these settings.

To add a new NTP server, click the  icon. To remove a server, click the  icon. To change the order in which the NTP servers should be used, select a server and click the up or down arrow until the NTP server is in the desired position.

Setting	Description
Enable as an NTP server	Check this setting if this system should be used as an NTP server.
NTP Servers	<p>Specify the host name of an NTP server. For example, time.nist.gov. Micro Focus recommends using at least two NTP servers to ensure precise time on your system. To specify multiple NTP servers, type one server name per line.</p> <p>Notes:</p> <ul style="list-style-type: none"> • An ArcSight system can serve as an NTP server for any other ArcSight system. • If System A serves as an NTP server for System B, System B needs to list System A in its NTP Servers list. • Use the Test Servers button to verify the status of the servers entered into the NTP Servers box.

5. Click **Save**.



6. Click **Restart NTP Service** to put the changes into effect.

SMTP

Your system uses the Simple Mail Transfer Protocol (SMTP) setting to send email notifications such as alerts and password reset emails.

To add or change SMTP settings:

1. Click **Administration > Setup > System Admin**.
2. Click **SMTP** in the **System** section and specify these settings.

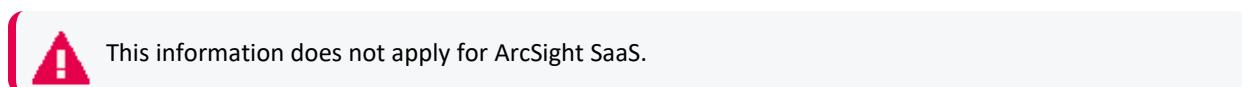
Setting	Description
Enable SMTP Auth Mode	Enable/Disable secure authenticated mode of communication with SMTP server.
Primary SMTP Server	Mandatory. The IP address or hostname of the SMTP server that will process outgoing email.
Primary SMTP Server Port	Primary SMTP Server Port. Required if SMTP Auth Mode is enabled.
Username	Primary SMTP Server Username. Required if SMTP Auth Mode is enabled.
Password	Primary SMTP Server Password. Required if SMTP Auth Mode is enabled.
Upload Cert File SMTP Primary	Upload Primary SMTP Server Certificate. Required if SMTP Auth Mode is enabled.
Backup SMTP Server	Mandatory. The IP address or hostname of the SMTP server that will process outgoing email in case the primary SMTP server is unavailable.
Ba ckup SMTP Server Port	Secondary SMTP Server Port. Required if SMTP Auth Mode is enabled.
Username	Secondary SMTP Server Username. Required if SMTP Auth Mode is enabled.
Password	Secondary SMTP Server Password. Required if SMTP Auth Mode is enabled.
Upload Cert File SMTP Backup	Upload secondary SMTP Server Certificate. Required if SMTP Auth Mode is enabled.
Outgoing Email Address	The email address that will appear in the From: field of outbound email.

3. Click **Save**.

For more information on SMTP Configuration, see [Connecting to Your SMTP Server](#).

License & Update

This page displays license information, the version of the components, and the elapsed time since Arcsight Management Center was last rebooted. From here, you can update Arcsight Management Center and apply a license.



Updating the Appliance

To update your Arcsight Management Center:

1. Download the update file from the Micro Focus Support site at <https://softwaresupport.softwaregrp.com/> to the computer from which you can connect

to Arcsight Management Center.

2. Click **Administration > Setup > System Admin** from the top-level menu bar.

3. Click **License & Update** in the **System** section.

4. Click **Browse** to locate the file.

5. Click **Upload Update**.

An “Update In Progress” page displays the update progress.

6. Once the update has completed, the Update Results page displays the update result (success/failure) and whether the update requires a reboot. If the update requires a reboot, the Arcsight Management Center reboots automatically.

Updating the License File

To update a license file:

1. Download the license update file from the Micro Focus Support site at <https://softwaresupport.softwaregrp.com/> to the computer from which you can connect to the Arcsight Management Center with your browser.

2. Log in to the Arcsight Management Center user interface using an account with administrator (upgrade) privileges.

3. Click **Administration > System Admin**.

4. Click **License & Update** in the **System** section.

5. Browse to the license file you downloaded earlier, and click **Upload Update**.

An “Update In Progress” page displays the update progress.

After the update has completed, the Update Results page displays the update result (success/failure). If you are installing or updating a license, a reboot is required.



Note: After updating the license file, refresh the browser to see the current list of enabled features.

Process Status

The **Process Status** page lists all processes related to your system and enables you to view the details of those processes and start, stop, or restart them.

To view the Process Status page:

1. Click **Administration > Setup > System Admin**.

2. In **System** section, click **Process Status**.

3. To view the details of a process, click the  icon to the left of the process name.
4. To start, stop, or restart a process, select the process and click **Start**, **Stop**, or **Restart** at the top of the **Processes** list.

System Settings

If you did not select Arcsight Management Center to start as a service during the installation process, you can do so using the **System Settings** page.

To configure Arcsight Management Center to start as a service:

1. Click **Administration > Setup > System Admin**.
2. Click **System Settings** in the left panel.
3. From under **Service Settings**, choose the appropriate option:
 - Start as a Service
 - Do not start as a Service
4. Click **Save**.

SNMP

SNMP (Simple Network Management Protocol) can be used to monitor the health of your appliance. supports versions 2c and 3 of SNMP.

SNMP Configuration

You can configure SNMP polling and notifications. If SNMP polling is configured, a manager station can query the SNMP agent residing on the . The information retrieved provides detailed information at the hardware and operating system level.

To configure SNMP polling:

1. In the main menu bar, click **Administration > Setup > System Admin**
2. In the navigation tree, under **System**, click **SNMP**.
3. On the **SNMP Poll Configuration** tab, ensure **Enabled** is selected.
 - For **Port**, the default is *161* but can be any available port. Ensure the specified port is open on your firewall.

- For **SNMP version**, select *V2c* or *V3*,
 - If *V2c* is selected, specify a community string of between 6 and 128 alphanumeric, underscore, and dash characters.
 - If *V3* is selected, specify the username (alphanumeric lower-case string of 4-16 characters, which must begin with an alphabetic characters and may include underscores), authentication protocol, authentication passphrase (4 to 256 characters), privacy protocol, and privacy passphrase (4 to 256 characters).

4. Click **Save**.

If an SNMP destination is configured, can send notifications for a limited set of events (see "[Viewing SNMP System Information](#)" below)

SNMP notifications differ from those sent by connectors, which are for a generic ArcSight event. The notifications listed here are specific to a single event, making them easier for understanding by a network management system.

To configure the destination for SNMP notifications:

1. In the main menu bar, click **Administration > System Admin**
2. In the navigation tree, under **System**, click **SNMP**.
3. On the **SNMP Destination** tab, ensure **Enabled** is selected. Then, specify values for the other parameters that match your existing NMS SNMP settings.
 - For Port, specify *162*. (Note: Specifying a non-default port may cause a brief delay. Give the process time to complete.)
 - For SNMP version, select *V2c* or *V3*, and then specify values for the prompted settings.
4. Click **Save**

Viewing SNMP System Information

SNMP notifications are viewable in any MIB browser. The following SNMP notifications are supported:

- **Application**
 - Login attempt failed
 - Password change attempt failed
 - User account locked
 - Reboot command launched
 - Manual backup failed
 - Enable FIPS mode successful

- Disable FIPS mode successful
- Enable FIPS mode failed
- Disable FIPS mode failed
- **Platform**
 - CPU Usage
 - Memory Usage
 - Disk Almost Full
 - Fan Failure
 - Power Supply Failure
 - Temperature Out of Range
 - Ethernet Link Down

To view system notifications in an MIB browser:

On your appliance:

You can download the ArcSight MIB file and other standard Net-SNMP MIB files using the following URLs:

- https://<system_name_or_ip>/platform-service/ARCSIGHT-EVENT-MIB.txt
- https://<system_name_or_ip>/platform-service/DISMAN-EVENT-MIB.txt
- https://<system_name_or_ip>/platform-service/HOST-RESOURCES-MIB.txt
- https://<system_name_or_ip>/platform-service/IF-MIB.txt
- https://<system_name_or_ip>/platform-service/UCD-SNMP-MIB.txt

In any standard MIB browser:

1. Load the MIB in the browser.
2. Specify the address and port number of the SNMP agent—your appliance, in this case.
3. Configure the community string that is set on your appliance.
4. Initiate the SNMP WALK operation of the OID from the browser.
5. Once the SNMP data is returned, interpret it based on the information described earlier in this section.

MIB Contents

Notifications are written to the following modules of the MIB file:

Module	Notification Types
HOST-RESOURCES-MIB	Standard hardware parameters.
IF-MIB	Objects for network interfaces.
IP-MIB	IP and ICMP implementations.
DISMAN-EVENT-MIB	Event triggers and actions for standard network management.

SSH Access to the Appliance

You can enable SSH access to the appliance. By default, SSH access to your appliance is disabled. For best security, it is strongly recommended that you enable SSH access only when necessary, such as for troubleshooting purposes.



Caution: By default, you are not prompted for a challenge/response when logging in using SSH. (This represents a change from the configuration of Connector Appliance.)

As a result, it is imperative that you change the default password for the “root” account on the ArcSight Management Center Appliance to a new, strong password as soon as possible. To obtain the default root password, contact ArcSight Customer Support.

Enablement options include:

- *Disabled*: No SSH access is enabled. This is the default value.
- *Enabled*: SSH access is always enabled.
- *Enabled, only for 8 hours*: SSH access is disabled automatically eight hours after it was enabled.
- *Enabled, only during startup/reboot*: SSH access is enabled during the time the appliance reboots and is starting up. It is disabled once all processes on the appliance are up and running. This option provides a minimal period of SSH access for situations such as when the appliance does not start successfully after a reboot.



Note: Even if SSH is disabled on your appliance, you can access its console if you have it set up for remote access using the Micro Focus ProLiant Integrated Lights-Out (iLO) Advanced remote management card.

Enabling or Disabling SSH Access

To enable or disable SSH access to your appliance:

1. Click **Administration > Setup >System Admin** from the top-level menu bar.
2. Click **SSH** in the **System** section.
3. Select an SSH enablement option.
4. Confirm the option. The change takes place immediately.

Connecting to Your Appliance Using SSH

Once you have enabled SSH access, follow these steps to connect to it using SSH:

1. Connect to the appliance as “root” using an SSH client.
2. When prompted to specify a password, specify a password and press **Enter**.



Note: On an upgraded G9 C6600 appliance, SSH connectivity will be blocked after upgrade. To unblock SSH, disable SSH and then re-enable it.

Diagnostic Tools

Arcsight Management Center provides several diagnostic tools that help you set up, manage, and troubleshoot your appliance. You can run these diagnostics on the local appliance only. To run a diagnostic tool on a remote container, refer to "[Running Diagnostics on a Container](#)" on [page 140](#).

To access the diagnostic tools:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **Diagnostic Tools** in the **System** section in the left panel to open the Diagnostic Tools page.
3. From the **Tool** drop-down box, select the tool you want to use.
4. Specify the required parameters for the tool you selected and click **Run** (click **Edit** for the Edit text file tool).

Each tool, the parameters, and buttons available are described below.

Display I/O Statistics

Use the Display I/O Statistics tool to monitor input/output statistics for devices, partitions, and network file systems on the appliance. This tool is equivalent to the Linux command `iostat`.

This tool uses the parameters described below:

Parameter	Description
Match Expression	Type an expression to display only lines in the file that match that expression. Linux regular expressions are supported. Note: The expression is case sensitive.
Exclude Expression	Type an expression to exclude lines that match that expression from the display. Linux regular expressions are supported. Note: The expression is case sensitive.

Display file

Use Display file to display the contents of a file. This tool is equivalent to the Linux command `cat`.

This tool uses the parameters described below:

Parameter/Button	Description
Category	Select the type of file you want to display.
File	Displays a list of files for the type selected in the Category field (described above). Select the file you want to display from the list. Note: Appliance models Cx400 do not have any boot log files; selecting Boot Log from the File list displays an empty pop-up window.
Match Expression	Type an expression to display only lines in the file that match that expression. Linux regular expressions are supported. Note: The expression is case sensitive.
Exclude Expression	Type an expression to exclude lines that match that expression from the display. Linux regular expressions are supported. Note: The expression is case sensitive.

Parameter/Button	Description
Display	<p>You can limit the number of lines you want to display.</p> <ul style="list-style-type: none"> Select Beginning of file to limit the display to the number of lines specified in the Number of Lines field (described below) starting from the top of the file. Select End of file to limit the display to the number of lines specified in the Number of Lines field (described below) starting from the bottom of the file. <p>Note: If you select Beginning of file or End of file, you also need to specify a value in the Number of Lines field, described below.</p> <p>To display all the lines in the file, leave both the Display and the Number of Lines field empty.</p>
Number of Lines	<p>Specify the number of lines you want to display from the beginning or end of the file.</p> <p>If you specify an expression to match or exclude, the display contains or omits the first (if you select Beginning of file) or last (if you select End of file) number of occurrences of that expression. For example, if you specify TCP in the Exclude Expression field, then select Beginning of file from the Display drop-down, and specify 10 in the Number of Lines field, the display contains the first 10 occurrences of the expression TCP found starting from the beginning of the file.</p> <p>Note: To display all the lines in the file, leave this field and the Display field (described above) empty.</p>
Run	Click this button to display the contents of the selected file. The file contents display in a pop-up window.

Display network connections

Use Display network connections to review your network connections and transport protocol statistics. The status information can indicate areas where a protocol is having a problem.

This tool is equivalent to the Linux command `netstat -pn [-t] [-u] [-w] [a] [-l] [-c]`.

This tool uses the parameters described below:

Parameter/Button	Description
Protocol	Leave this field empty to display statistics for all transport protocols or select from these options: <ul style="list-style-type: none"> RAW only displays raw IP protocol statistics. This option is equivalent to the netstat Linux command option -w. TCP only displays TCP protocol statistics. This option is equivalent to the netstat Linux command option -t. UDP only displays UDP protocol statistics. This option is equivalent to the netstat Linux command option -u.
Connection	Leave this field empty to display information for all non-listening connections or select from these options: <ul style="list-style-type: none"> All connections displays information for all current connections. This option is equivalent to the netstat Linux command option -a. Listening connections displays information for listening connections only. This option is equivalent to the netstat Linux command option -l.
Mode	Select Run Continuously to poll the network status continuously every five minutes. This option is equivalent to the netstat Linux command option -c. When Run Continuously is not selected, the network status is polled once.
Match Expression	Specify an expression to display only lines that match that expression in the output. Linux regular expressions are supported.
Exclude Expression	Specify an expression to exclude lines that match that expression from the output. Linux regular expressions are supported.
Run	Click this button to display the network connection information. The information displays in a pop-up window.

Display network interface details

Use Display network interface details to display the status of a currently active interface on the appliance. This tool is equivalent to the Linux command `ifconfig`.

This tool uses the parameters described below:

Parameter/Button	Description
Interface	Select the network interface on the appliance whose status you want to display. Note: If you leave this field empty, the status of all active network interfaces display.
Run	Click this button to display the status of the selected network interface. The status displays in a pop-up window.

Display network traffic

Use Display network traffic to monitor packets that are transmitted and received on the network. This tool is equivalent to the Linux command `tcpdump`.

This tool uses the parameters described below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host you want to monitor.
Match Expression	Specify an expression to show only network traffic that matches that expression in the display; For example, if you specify the expression echo, only network traffic from the specified host that includes the expression echo is displayed. Linux regular expressions are supported.
Exclude Expression	Specify an expression to exclude network traffic that matches that expression from the display; For example, if you specify the expression echo, all traffic except traffic that contains echo will be displayed. Linux regular expressions are supported.
Run	Click this button to display network traffic between the appliance and the specified host. The information displays in a pop-up window.

Display process summary

Use Display process summary to show a list of the currently running processes and see how long they have been running. This tool is equivalent to the Linux command `top -b -n 1`.

This tool uses the parameters described below:

Parameter/Button	Description
Match Expression	Specify an expression to display only processes that match that expression. Linux regular expressions are supported.
Exclude Expression	Specify an expression to exclude processes that match that expression from the display. Linux regular expressions are supported.
Run	Click this button to display the list of currently running processes. The list displays in a pop-up window.

Display routing table

Use Display routing table to see the routes through which traffic flows from the appliance. This tool is equivalent to the Linux command `ip route`.

This tool uses the parameters described below:

Parameter/Button	Description
Destination Host	<ul style="list-style-type: none"> Leave this field empty to see the entire IP routing table. Specify the IP address or hostname of a host to see IP routing information from the appliance to that host.
Run	Click this button to obtain the routing table. The routing table displays in a pop-up window.

Edit text file

Use Edit text file to edit files on the appliance. This tool uses the parameters described below:

Parameter/Button	Description
Category	Select the type of file you want to edit.
File	Displays a list of files for the type selected in the Category field (described above). Select the file you want to edit.
Edit	Click this button to display the file for editing. After editing the file, click Save or Revert .
Save	Click this button to save the edits you make to the file.
Revert	Click this button to cancel the edits you make to the file. After clicking Revert , click Save to save the reverted text.

List directory

Use List directory to display the contents of a directory on the appliance. This tool is equivalent to the Linux command `ls -alh`.

This tool uses the parameters described below:

Parameter/Button	Description
Directory	Specify the directory whose contents you want to display. For example: <code>/opt/arcsight/appliance</code>
Run	Click this button to display the directory list. The list displays in a pop-up window.

List open files

Use List open files to display a list of files in use. This tool uses the parameters described below:

Parameter/Button	Description
Match Expression	Specify an expression to display only the top processes that match that expression. Linux regular expressions are supported.
Exclude Expression	Specify an expression to exclude processes that match that expression from the display. Linux regular expressions are supported.
Run	Click this button to display the list of the top processes. The list displays in a pop-up window.

List processes

Use List processes to display the top CPU processes that are currently running together with memory and resource information. This tool is equivalent to the Linux command `ps -ef`.

This tool uses the parameters described below:

Parameter/Button	Description
Match Expression	Specify an expression to display only the top processes that match that expression. Linux regular expressions are supported.
Exclude Expression	Specify an expression to exclude processes that match that expression from the display. Linux regular expressions are supported.
Run	Click this button to display the list of the top processes. The list displays in a pop-up window.

Ping host

Use Ping host to test if a particular host is reachable across an IP network and to measure the round-trip time for packets sent from the appliance to the host. This tool is equivalent to the Linux command `ping`.

This tool uses the parameters described below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host you want to ping.
Run	Click this button to ping the specified host. The ping results display in a pop-up window.

Resolve hostname or IP Address

Use Resolve hostname to look up a hostname in the Domain Name Server and convert it to an IP address . This tool is equivalent to the Linux command `host`.

This tool uses the parameters described below:

Parameter/Button	Description
Hostname	Specify the hostname you want to resolve to an IP address .
Run	Click this button to look up the hostname in the Domain Name Server. The result displays in a pop-up window.

Scan network ports

Use Scan network ports to scan a specific host on the network for open ports. This tool is equivalent to the Linux command `nmap [-p]`.

This tool uses the parameters described below:

Parameter/Button	Description
Host	Specify the IP address or hostname of the host whose ports you want to scan.
Port Range	Optional. Specify a range of ports you want to scan. Separate port numbers in a range by a dash (-) and individual port numbers by a comma. For example, 80-90, 8080. If you do not provide a port range, all ports on the specified host are scanned. This option is equivalent to the netstat Linux command option -p.
Run	Click this button to start scanning ports on the specified host. The result displays in a pop-up window.

Send signal to container

Use Send signal to container to send a terminate command to a container. This tool is equivalent to the Linux command `kill -severity` (where `severity` is either -15 or -9).

This tool uses the parameters described below:

Parameter/Button	Description
Severity	Select the severity of the terminate command you want to send to the container. You can select KILL (Linux kill command option -9) or TERM (Linux kill command option -15).
Container	Select the container to which you want to send the signal.
Run	Click this button to send the signal. The result displays in a pop-up window.

Tail file

Use Tail file to display the last ten lines of a system, application, or log file. This tool is equivalent to the Linux command `tail -f`.

This tool uses the parameters described below:

Parameter/Button	Description
Category	Select the type of file you want to edit.
File	Displays a list of files for the category selected in the Category field (described above). Select the file from which you want to display the last ten lines.
Match Expression	Specify an expression to display only lines that match that expression. Linux regular expressions are supported.
Exclude Expression	Specify an expression to exclude lines from the display that match that expression. Linux regular expressions are supported.
Run	Click this button to display the last ten lines of the file you selected. The lines display in a pop-up window.

Trace network route

Use Trace network route to display the specific network route between the appliance and a specified host. This tool is equivalent to the Linux command traceroute.

This tool uses the parameters described below:

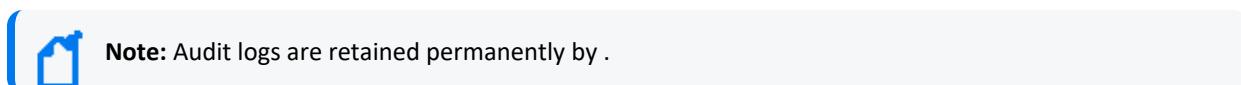
Parameter/Button	Description
Host	Specify the IP address or hostname of the host whose route you want to trace.
Run	Click this button to display the network route. The information displays in a pop-up window.

Logs

Your system can generate audit logs at the application and platform levels. Use the Logs sub-menu to search audit logs and to configure audit forwarding so that the system can send audit events to a destination, such as ESM.

Audit Logs

Your system's audit logs are available for viewing. Audit logs, as Common Event Format (CEF) audit events, can be sent to ArcSight ESM directly for analysis and correlation. For information about forwarding audit events, see "["Configuring Audit Forwarding to a Specific Destination" on the next page.](#)



To view audit logs:

1. Click **Administration > System Admin**.
2. Click **Audit Logs** in the **Logs** section.
3. Select the date and time range for which you want to obtain the log.
4. (Optional) To refine the audit log search, specify a string in the **Description** field and a user name in the **User** field. When a string is specified, only logs whose **Description** field contains the string are displayed. Similarly, when a user is specified, only logs whose **User** field contains the username are displayed.
5. Click **Search**.

Configuring Audit Forwarding to a Specific Destination

You can forward audit and system health events to an ArcSight ESM destination for correlation and analysis, and to Logger for event collection.

To forward audit events to specific destinations:

1. Click **Setup > System Admin** from the top-level menu bar.
2. Click **Audit Forwarding** in the **Logs** section.
3. Select destinations from the **Available Destinations** list and click the right arrow icon () to move the selected destination to the **Selected Destinations** list.
You can select multiple destinations at the same time and move them, or you can move all available destinations by clicking the () icon.
4. Click **Save Settings**.



Note: For software ArcMC, the following is required:

- The audit event forwarding connector needs to be installed under the /opt/arcsight/connector directory.
- During the installation, on the **Connector Detail** page, please input data for all fields, and continue with the installation process.

Storage

Use the Storage sub-menu to add an NFS mount or a CIFS mount, or SAN (if applicable) and to view the status of the hard disk array (RAID) controller and specific system processes.

RAID Controller/Hard Disk SMART Data

You can view information about the RAID controller or hard disk SMART data on the General Controller Information page. This information is not needed during normal system operations, but it can be helpful for diagnosing specific hardware issues. Due to the redundant nature of RAID storage, a single drive failure will not disable your system. Instead, performance degrades. Use this report to determine whether a performance issue is caused by a disk failure. Customer support can also use this information to diagnose problems.

To view the General Controller Information screen:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **RAID Controller** in the **Storage** section in the left panel.



Note: On some older models, the Hard Disk SMART Data menu item displays in the left pane instead of the RAID Controller menu item. Click **Hard Disk SMART Data** in the **Storage** section in the left pane to display diagnostic information from the hard drive.

3. The information displayed depends on the hardware model of your system. Click the arrows to open and close the sections.



Note: If the General Controller Information is not displayed, run `hpacucli controller slot=0 show config detail`.

FTP

Arcsight Management Center allows for the use of FTP and FTPS (FTP over SSL) as a method of delivering log files to the appliance. The default state for FTP and FTPS is *disabled*.

Blue Coat ProxySG appliances, in particular, support FTP and FTPS as a means of transferring files to Arcsight Management Center (For details on this and other methods, refer to the SmartConnector Configuration Guide for Blue Coat ProxySG).

FTPS

FTP can also be used over a secure channel, namely SSL. The use of FTPS requires that a certificate be generated on Arcsight Management Center. This certificate can be self-signed or signed by a certificate authority (CA). For detailed instructions on this option, see "[Using FTPS \(FTP over SSL\)](#)" on page 291.

Models Supporting FTP

The following table lists the Arcsight Management Center models that support the use of FTP. It can also assist in determining the maximum directory size allowed for storing files received over these protocols.



Note: If the maximum directory size is exceeded, FTP is disabled and audit event platform:453, `FTP service stopped` is sent. Until the directory size is lowered, all FTP connections are denied.

Model Name	Maximum Directory Size (GB)
C1400	275
C3400	275
C3500	475
C5400	235
C5500	475
C6500	500
C6600	500

Enabling FTP

In order to use the FTP protocol, you need to enable it on the appliance and set a maximum directory size for the accumulated files.

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **FTP** under the **Storage** section.
3. From within **FTP Settings**, check the **Enable FTP** check box.
4. If your FTP client is behind a firewall and you need to limit the ports used for passive mode data transfer, check the **Restrict port range...** check box.
 - **Port Range** allows you to set either an individual port (e.g., 12345) or a single port range (e.g., 20001-20010). Ensure any ports specified open on your firewall.



Note: When choosing a port or port range, choose a port that is unlikely to already be in use. If a chosen port is already in use, . For this reason, Micro Focus recommends using ports in the range of 10000 and above.

- The number of concurrent passive mode FTP clients is restricted to the number of ports specified. For example, if the specified range is 10 ports, then only 10 concurrent passive

FTP clients can be transferring at the same time.



Tip: Is FTP Running? verifies (Yes or No) that your FTP server is running successfully.

5. Specify a maximum directory size.

- The maximum directory size cannot be greater than the one allowed on your appliance model (see "[Models Supporting FTP](#)" on the previous page).
- If you change the maximum size, it must be greater than the value in the **Current Size** field.
- **Current Size** includes /opt/arcsight/incoming and all underlying subdirectories.
- If the maximum you have set is exceeded, FTP stops automatically.
- Once the file limitation is back within range, FTP automatically restarts.

6. Specify a password.



Caution: Anonymous FTP is not supported.

7. Click **Save**.



- Only file put operations are supported by the FTP server. There is no capability to retrieve data from the appliance.
- Data is processed faster and more efficiently when transferred in many small files instead of a few large files.

Adding a Subdirectory

Based on naming convention, incoming log files from different devices can potentially conflict within the same directory. To prevent this, you can create subdirectories to separate them. This window also shows the current size of the subdirectory.



Tip: Creating subdirectories is a good practice, as it allows you to verify how much space is being used and to easily delete subsets of file data.

To add files to the subdirectory:

1. From within the appliance, go to **Setup > System Admin > FTP**.
2. In the **Subdirectory** window, click **Add** to name the subdirectory.

The name appears in the window and displays its current size. Ensure that the directory

name matches the one configured on the FTP server.



Note: When naming subdirectories, the standard Linux directory naming conventions apply.

Processing Log Data Received via FTP

Receiving input from a connector via FTP requires that some steps be performed outside of the appliance. The following steps allow for the successful transfer of log data.

1. Enable FTP on the appliance. For detailed instructions, see "[Enabling FTP](#)" on page 289.
2. Configure the SmartConnector. For instructions on how to do this, see the SmartConnector Configuration Guide for Blue Coat ProxySG.



Tip: When configuring the Blue Coat SmartConnector for use with FTP, set up the SmartConnector to delete files after processing. This step helps to prevent an over accumulation of files on the FTP server.

To do so, in the `agent.properties`, change `agents[0].foldertable[0].mode=RenameInSameDirectory` to `agents[0].foldertable[0].mode=DeleteFile`.



Tip: When configuring the Blue Coat SmartConnector for use with FTP, point the connector to `/opt/arcsight/incoming/<or subdirectory>`.

3. Configure the device. For instructions on how to do this, see the documentation for your device.

Using FTPS (FTP over SSL)

FTPS is FTP used over a secure SSL channel. The use of FTPS requires that a certificate is generated on Arcsight Management Center.

Using FTPS with Blue Coat ProxySG

The use of FTPS requires several steps on both Arcsight Management Center and the Blue Coat ProxySG appliance. The first step is that a **self-signed certificate** or **CSR** is generated on Arcsight Management Center. If the certificate is self-signed, it must be imported into the Blue Coat ProxySG appliance. If signed by a CA, the certificate of the CA must be imported into the Blue Coat ProxySG appliance.

On Arcsight Management Center:

1. **Generate the certificate** (either a self-signed certificate or CSR) on Arcsight Management Center.

- For a self-signed certificate, see "[Generating a Self-Signed Certificate](#)" on the next page.
 - For a CA-signed certificate, see "[Generating a Certificate Signing Request \(CSR\)](#)" on [page 294](#) and "[Importing a Certificate](#)" on [page 296](#).
2. **Enable FTP** on Connector Appliance. For detailed steps, see "[Enabling FTP](#)" on [page 289](#).

On the Blue Coat ProxySG Appliance:

See your current Blue Coat ProxySG documentation for detailed instructions to complete the following necessary steps.

1. **Import the self-signed or the certificate of the CA** into the Blue Coat ProxySG appliance. If importing a self-signed certificate into the Blue Coat ProxySG appliance, click the **View Certificate** button on the **Generate Certificate** page to display the certificate to be used with FTPS. Copy its entire contents and paste them into the Import CA Certificate window on the BlueCoat ProxySG appliance.
2. **Add the imported certificate into the browser-trusted CA Certificates Lists** on the Blue Coat ProxySG.
3. **Configure the FTP upload client** on the Blue Coat ProxySG appliance, ensuring that you **select the option to use secure connections**.
4. **Run an upload test** on the Blue Coat ProxySG appliance to verify that it was able to successfully upload its log files to Connector Appliance over FTPS.

Security

Security settings enable you to configure SSL server certificates, enable and disable FIPS (Federal Information Processing Standards) mode on your system, and configure SSL client authentication for client certificate and Common Access Card (CAC) support.



Tip: For steps on how to create a user DN, see "[Users](#)" on [page 309](#), and refer to the section "Use Client DN" in the parameters table.

SSL Server Certificate

Your system uses Secure Sockets Layer (SSL) technology to communicate securely over an encrypted channel with its clients, such as SmartConnectors, when using the SmartMessaging technology and other ArcSight systems. Your system ships with a self-signed certificate so that an SSL session can be established the first time you use the appliance. For more information on this option, see "[Generating a Self-Signed Certificate](#)" on the next page.

Although a self-signed certificate is provided for your use, you should use a certificate authority (CA) signed certificate. To facilitate obtaining a CA-signed certificate, your system can generate a Certificate Signing Request. After a signed certificate file is available from the CA, it can be uploaded to your system for use in a subsequent authentication. For detailed instructions, see "[Generating a Certificate Signing Request \(CSR\)](#)" on the next page.

Your system generates an audit event when the installed SSL certificate is going to expire in less than 30 days or has already expired. The event with Device Event Class ID "platform:407" is generated periodically until you replace the certificate with one that is not due to expire within 30 days.

Generating a Self-Signed Certificate

Your system ships with a self-signed certificate so that an SSL session can be established the first time you connect. This type of certificate does not require signing from another entity and can be used immediately.

To generate a self-signed certificate:

1. Click **Administration > Setup > System Admin**.
2. Click **SSL Server Certificate** from the **Security** section in the left panel to display the **Generate Certificate/Certificate Signing Request** page.
3. Click the **Generate Certificate** tab.
4. From the **Generate Certificate For Protocol** field, use the **Network Protocol** drop-down menu to choose the appropriate protocol

Parameter	Description
HTTPS	Select this option to generate a CSR for use with the HTTPS protocol. This is the most commonly used option.
FTPS	Select this option only when generating a CSR for use with FTPS.

5. From the **Enter Certificate Settings** field, specify new values for the following fields:

Parameter	Description
Country	ISO 3166-1 two-letter country code, such as 'US' for the United States.
State/Province	State or province name, such as 'California.'
City/Locality	City name, such as 'Sunnyvale'.
Organization Name	Company name, governmental entity, or similar overall organization.
Organizational Unit	Division or department within the organization.

Parameter	Description
Hostname	<p>The host name or IP address of this system.</p> <p>When specifying the host name, make sure that this name matches the name registered in the Domain Name Service (DNS) server for the system. Additionally, this name must be identical to the host name specified in "NICs" on page 267.</p> <p>Note: If the host name or IP address of this system changes in the future, you must generate a new self-signed certificate or CSR. After a new certificate is obtained, you must upload it to ensure that the connectors which communicate with the system are able to validate the host name.</p>
Email Address	The email address of the administrator or contact person for this CSR.
Private Key Length	Private key length is 2048 bits.

6. Use the first two buttons to generate a CSR or a self-signed certificate. The **View Certificate** button is only used to view the resulting certificate.

Button	Description
Generate CSR	Click to generate a Certificate Signing Request (CSR).
Generate Certificate	Click to generate a self-signed certificate.
View Certificate	Click to view the generated certificate.

7. Click the **Generate Certificate** button to generate the self-signed certificate.
8. Click **Ok** after the confirmation message appears.
9. Click the **View Certificate** button to view the PEM encoded self-signed certificate.

Generating a Certificate Signing Request (CSR)

The first step in obtaining a CA-signed certificate is to generate a Certificate Signing Request (CSR). The CSR must be generated on the system for which you are requesting a certificate. That is, you cannot generate a CSR for System A on System B or use a third-party utility for generation.

The resulting CSR must be sent to a CA, such as VeriSign, which responds with a signed certificate file.

To generate a certificate signing request:

1. Click **Administration > System Admin**.
2. Click **SSL Server Certificate** from the **Security** section in the left panel to display the **Generate Certificate/Certificate Signing Request** page.
3. Click the **Generate Certificate** tab.

- From the **Generate Certificate For Protocol** field, use the **Network Protocol** drop-down menu to choose the appropriate protocol. From the **Generate Certificate For Protocol** field, use the **Network Protocol** drop-down menu to choose the appropriate protocol.

Parameter	Description
HTTPS	Select this option to generate a CSR for use with the HTTPS protocol. This is the most commonly used option.
FTPS	Select this option only when generating a CSR for use with FTPS.

- From the **Enter Certificate Settings** field, specify new values for the following fields:

Parameter	Description
Country	A two-letter country code, such as 'US' for the United States.
State / Province	State or province name, such as 'California.'
City / Locality	City name, such as 'Sunnyvale'.
Organization Name	Company name, governmental entity, or similar overall organization.
Organizational Unit	Division or department within the organization.
Hostname	The host name or IP address of this system. When specifying the host name, make sure that this name matches the name registered in the Domain Name Service (DNS) server for the system. Additionally, this name must be identical to the host name specified in " NICs " on page 267. Note: If the host name or IP address of this system changes in the future, you must generate a new self-signed certificate or CSR. After a new certificate is obtained, you must upload it to ensure that the connectors which communicate with the system are able to validate the host name.
Email Address	The email address of the administrator or contact person for this CSR.
Private Key Length	Select the length (in bits) of the private key: 1024 , 2048 , 4096 , or 8192 .

- Use the first two buttons to generate a CSR or a self-signed certificate. The **View Certificate** button is only used to view the resulting certificate.

Button	Description
Generate CSR	Click to generate a Certificate Signing Request (CSR).
Generate Certificate	Click to generate a self-signed certificate.
View Certificate	Click to view the generated certificate.

- Select **Generate CSR** to generate a certificate signing request.
- If the CSR was successfully generated, a pop-up window appears, allowing you to either download the CSR file or to cut-and-paste its content.

- To do so, copy all the lines from -----BEGIN CERTIFICATE REQUEST----- to -----END CERTIFICATE REQUEST-----.
9. Send the CSR file to your certificate authority to obtain the CA-signed certificate.
 10. After the CA-signed certificate file is obtained, continue on to "[Importing a Certificate below](#)".

Importing a Certificate

If you have obtained a certificate from your certificate authority (CA), follow the steps below to import it onto your system.

1. Click **Administration > System Admin**.
2. Click **SSL Server Certificate** under the **Security** section in the left panel.
3. Select the **Import Certificate** tab.
4. From the **Import Certificate For Protocol** field, use the **Network Protocol** drop-down menu to select the appropriate protocol type.

Parameter	Description
HTTPS	Select to import an HTTPS certificate. (This option may require a reboot).
FTPS	Select to import an FTPS certificate.

5. Click the **Browse** button to locate the signed certificate file on your local file system.



Note: The imported certificate must be in **Privacy Enhanced Mail (PEM)** format.

6. Click **Import and Install** to import the specified certificate.
7. If using **HTTPS** and depending on your browser, you may need to close and restart the browser for the new certificate to take effect. If you are unsure of your browser's requirements, close and restart it.

SSL Client Authentication

Your system supports client authentication using SSL certificates. SSL client authentication is a form of two-factor authentication that can be used as an alternate or in addition to local password authentication.



Note: CAC is a form of client certificate authentication. Information on client certificate authentication applies to CAC.

To configure to support CAC, you need to upload a trusted certificate, and enable client certificate authentication.

Uploading Trusted Certificates

A trusted certificate is used to authenticate users that log in to your system. Uploading a trusted certificate is required if you are using LDAPS authentication. The trusted certificate is used to authenticate the remote LDAPS server. The certificate needs to be in Privacy Enhanced Mail (PEM) format.

To upload a trusted certificate:

1. Click **Administration > Setup > System Admin**.
2. Click **SSL Client Authentication** in the **Security** section in the left panel.
3. On the **Trusted Certificates** tab, click **Browse** to find the trusted certificate on your local file system.
4. Click **Upload**.

The trusted certificate is uploaded and listed in the “Certificates in Repository” list on the same page where you uploaded it.

To view details about a trusted certificate, click the link displayed in the Certificate Name column.

To delete a trusted certificate, select the certificate and click **Delete**.

Uploading a Certificate Revocation List

A certificate revocation list (CRL) is a computer-generated record that identifies certificates that have been revoked or suspended before their expiration dates. To support CAC, you need to upload a CRL file to your ArcSight system. The CRL file needs to be in PEM format.

To upload a CRL file:

1. Click **Administration > System Admin**.
2. Click **SSL Client Authentication** in the **Security** section in the left panel.
3. In the **Certificate Revocation List** tab, click **Browse** to find the CRL file on your local file system.
4. Click **Upload**.

The CRL is uploaded and listed in the Certificate Revocation List.

To view details about a CRL, click the link displayed in the Issuer Name column.

To delete a CRL file, select it and click the **Delete** button.

Enabling Client Certificate Authentication

To enable client certificate authentication, see "[Client Certificate Authentication](#)" on page 303.

FIPS 140-2

Your system supports the Federal Information Processing Standard 140-2 (FIPS 140-2). FIPS 140-2 is a standard published by the National Institute of Standards and Technology (NIST) and is used to accredit cryptographic modules in software components. The US Federal government requires that all IT products dealing with Sensitive, but Unclassified (SBU) information meet these standards.

If your system needs to be FIPS 140-2 compliant, you can enable FIPS. Once you do so, the system uses the cryptographic algorithms defined by the NIST for FIPS 140-2 for all encrypted communication between its internal and external components.



Note: Do not perform any FIPS-related activity on the appliance while a FIPS mode change is in progress.

To be fully FIPS 140-2 compliant, all components that work together need to be in FIPS mode. For example, when you enable FIPS on ArcSight Management Center, the appliance becomes FIPS enabled and meets the standards for cryptographic algorithms defined by the NIST. However, containers must also have FIPS enabled.



Note: In ArcSight Management Center, enabling FIPS mode will disable the ability to regenerate a self-signed certificate.

To enable or disable FIPS mode:

1. Click **Administration > Setup > System Admin** from the top-level menu bar.
2. Click **FIPS 140-2** in the Security section in the left panel.
3. Click **Enable or Disable** for the Select FIPS Mode option.
4. Click **Save**.
5. When the **Application Reboot Required** message displays, restart your system. click the **System Reboot** link.
6. Check that the appropriate CA certificates are present in the trust store so that connectors can validate their destinations (ArcSight ESM or Arcsight Management Center) successfully. If the appropriate CA certificates are not in the trust store, you need to add them. For information on viewing and adding certificates, see "[Sending a Command to a Container](#)" on page 128.

Users/Groups on ArcMC

Use the **Users/Groups** sub-menu to configure users and user groups on ArcMC, and to set authentication options.



For managing users of managed products, see "[Managing Users on Managed Products](#)" on page 236.

Authentication

Authentication Settings enable you to specify the settings and policies for user login sessions, password rules and lockouts, and external authentication options.

Sessions

The **Session** tab enables you to specify the maximum number of simultaneous sessions for a single user account, and the length of time after which a user session is automatically logged out or a user account disabled. By default, a single user account can have up to 15 simultaneous active sessions, and a user account is logged out after 15 minutes of inactivity.

To change session settings:

1. Click **Administration > Setup > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. On the **Sessions** tab, update the parameters described in the following table.

Parameters	Description
Max Simultaneous Logins/User	The maximum number of simultaneous sessions allowed for a single user account. The default is 15 sessions . If Max Simultaneous Logins/User is set to 1, it is required to have at least another admin user, otherwise the admin user will not be able to log in.
Logout Inactive Session After	The length of time, in minutes, after which an inactive session is automatically ended. The default is 15 minutes . This value does not apply to the user interface pages accessed through the Monitor menu. If a user is on any of the Monitor menu pages and the session has been inactive for the specified number of minutes, the user's session remains active.
Disable Inactive Account After	The number of days after which an inactive user account is disabled. The default is 0 , meaning the account is never disabled.

4. Click **Save** to make the changes, or click another tab to cancel.

Local Password

The **Local Password** tab enables you to set password policies, such as the minimum and maximum number of characters and other password requirements.

To change the password settings:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Choose the **Local Password** tab.

Use the parameters described in the following table to customize your password settings.

Authentication Settings, Local Password tab

Parameter	Description
Lockout Account (policy)	
Enable Account Lockout	Select the check box to enable user accounts to be locked out as defined by the following settings. By default, the policy is disabled .
Lockout Account After	Number of failed login attempts after which a user account is locked out. The default is 3 .
Remember Failed Attempts For	The length of time, in minutes, for which a failed login attempt is remembered. The default is 1 .
Lockout Account For	The length of time, in minutes, for which a locked out account cannot be unlocked. The default is 15 .
Password Expiration (policy)	
Enable Password Expiration	Select the check box to enable user passwords to expire as defined by the following settings. By default, the policy is disabled .
Password Expires in	Number of days after which the password expires. The default is 90 .
Notify User	Number of days before expiration to notify the user. Select this option to allow users to update their password before expiration. The default is 5 .
Users Exempted From Password Expiration Policy	Click the link to set the number of users whose password should never expire. For information on how to use this feature, see " "Users Exempted From Password Expiration" on the next page ".
Password Strength Rules (policy)	
Enforce Password Strength	Select the check box to enforce password policy as defined by the following settings. By default, the policy is disabled .
Minimum Length	Minimum number of characters that a password must contain. The default is 10 .
Maximum Length	Maximum number of characters that a password can contain. The default is 20 .

Authentication Settings, Local Password tab, continued

Parameter	Description
Password Character Rules	
Password character rules define additional character requirements to ensure password strength.	
Numeric	Minimum number of numeric characters (0-9) in a password. The default is 2 .
Uppercase	Minimum number of uppercase characters (A-Z) in a password. The default is 0 .
Special	Minimum number of non-digit and non-letter characters that are required in a password. The default is 2 .
Lowercase	Minimum number of lowercase characters (a-z) in a password. The default is 0 .
Password Must be At Least N Characters Different From Old Password	Minimum number of characters by which the new password must differ from the previous one. The default is 2 .
Include "Forgot Password" link on Login Screen	<p>Select the check box to enable users to reset their local password using a "Forgot Password" link on the login page. By default, the option is disabled.</p> <p>An SMTP server must be configured on the system, and the username must have a correct email address for this feature to work successfully.</p> <p>If an SMTP server is not set, you cannot reset the password because the email containing the temporary password cannot be sent.</p> <p>You must specify an email address in the user settings for the user name. The temporary password is sent to that email address. If no email address is specified or if the email address is incorrect, the user will not receive the email.</p> <p>For information on how to use this feature, see "Forgot Password" on the next page.</p>

- Click **Save** to save the changes, or click another tab to cancel.

Users Exempted From Password Expiration

Even though you have set a password expiration policy for most users, you may want to have a user whose password does not expire automatically.

To exempt a user from the password expiration policy:

- Click **Administration > System Admin**.
- Click **Authentication** in the **Users/Groups** section.
- Select the **Local Password** tab, then click **Users Exempted From Password Expiration Policy**.
- The **Exempt Users From Password Expiration** page displays.

5. Select users from the **Non-exempted Users** list and click the right arrow icon  to move the selected users to the **Exempted Users** list. Do the reverse to remove users from the list of exempted users.

You can select multiple users at the same time and move them over. Or you can move all users by clicking the  icon.

6. Click **Save** to save the policy or **Cancel** to exit.

Forgot Password

This feature is available only if the **Include “Forgot Password” link on Login Screen** setting on the Authentication Settings page (**Setup > System Admin > Authentication > Local Password**) is set to **Yes**. By default, this setting is set to **No**. An SMTP server must be configured in order to use this feature. For more details on how to enable it, see "["Local Password" on page 300](#)".

If you forget your system password, use this feature to receive an email that provides a temporary password.

The temporary password is valid until the time specified in the email. If you do not log in within the specified time, only an administrator can reset the password to generate another temporary password.

To reset your password:

1. Click the **Forgot Password** link on the Login screen.
2. Specify a user name on the **Reset Password** dialog box.
3. Click **Reset Password**.

An automated email with a temporary password is sent to the email address specified for that user.

External Authentication

Besides providing a local password authentication method, your system supports Client Certificate/CAC, LDAP, and RADIUS authentication. It is not possible to enable all authentication methods simultaneously.



Note: CAC is a form of client certificate authentication. Information on client certificate authentication applies to CAC.

From the **External Authentication** tab, use the drop-down menu to choose one of the following authentication methods:

- "Local Password" below
- "Client Certificate Authentication" below
- "Client Certificate and Local Password Authentication" on the next page
- "LDAP/AD and LDAPS Authentication" on the next page
- "RADIUS Authentication" on page 306

Local Password

This option is the default method and implements the local password policies set in the **Local Password** tab. Leave this as the default, or click **Save** if changing from another option.

Client Certificate Authentication

This authentication method requires that users authenticate using a client certificate. For each client certificate, a user account with a Distinguished Name (DN) matching the one in the client certificate must exist on your system.



Caution: All SSL client certificates used for authentication must be FIPS compliant (hashed with FIPS-compliant algorithms) even if FIPS is not enabled on your system.

To configure client certificate authentication:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Click the **External Authentication** tab.
4. From the drop-down menu, choose **Client Certificate**.
5. **Allow Local Password Fallback** provides two options:
 - **Allow Local Password Fallback for Default Admin Only**
Select this option to allow the default admin user to log in using only a username and password if the client certificate is not available or invalid. This privilege is restricted to the default admin user only. Other users must have a valid client certificate to gain access to the system. This option is enabled by default.
 - **Allow Local Password Fallback for All Users**
Select this option to allow all users to log in using their local user name and password if their client certificate is invalid or unavailable.
For more information, see "[Local Password Fallback](#)" on page 307.
6. Click **Save**.

Client Certificate and Local Password Authentication

This authentication method requires that users authenticate using an SSL client certificate and a valid local password. *Local Password* refers to the password associated with the user credentials created in **User Management** in the **Users/Groups** section. See "["User Management" on page 308](#) for details.

A user account on your system must be defined with a Distinguished Name (DN) that matches the one in the client certificate.

For instructions on how to create a user DN, see "["Users" on page 309](#) and refer to the section called "Use Client DN" in the parameters table.



Caution: All SSL client certificates used for authentication must be FIPS compliant (hashed with FIPS-compliant algorithms) even if FIPS is not enabled on your system.

To configure client certificate and password authentication:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Click the **External Authentication** tab.
4. From the drop-down menu, choose **Client Certificate AND Local Password**.
5. **Allow Local Password Fallback** provides two options:
 - **Allow Local Password Fallback for Default Admin Only**
This option, always enabled, allows the default admin user to log in using only a username and password.
 - **Allow Local Password Fallback for All Users**
This option is always disabled. You cannot enable it when using the **Client Certificate AND Local Password** authentication method.
For more information, see "["Local Password Fallback" on page 307](#)".
6. Click **Save**.

LDAP/AD and LDAPS Authentication

This authentication method authenticates users against an LDAP server. Even when LDAP is enabled, each user account must exist locally on your system. Although the user name specified locally can be different from the one specified on the LDAP server, the Distinguished Name (DN) specified for each user account must match the one in the LDAP server.



Tip: For steps on how to create a user DN, see "[Users](#)" on page 309, and the parameter "[Use Client DN](#)" on page 310.

To set up LDAP authentication:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Click the **External Authentication** tab.
4. From the drop-down menu, choose **LDAP**.
5. **Allow Local Password Fallback** provides two options:

- **Allow Local Password Fallback for Default Admin Only**

Select this option to allow the default admin user to log in using only a username and password if LDAP authentication fails. This privilege is restricted to the default admin user only. All others must be authenticated by LDAP. This option is enabled by default.

- **Allow Local Password Fallback for All Users**

Select this option to allow all users to log in using their local user name and password if LDAP authentication fails.

For more information, see "[Local Password Fallback](#)" on page 307.

LDAP Server has the following parameters:

Parameter	Description
Server Hostname [:port] (optional)	(Optional) Specify the host name or IP address and port of the LDAP server in the following format: <code>ldap://<hostname or IP address >:<port></code> <code>ldaps://<hostname or IP address >:<port></code> Additional steps are required for the use of LDAPS. See " Using the LDAP over SSL (LDAPS) Protocol " below.
Backup Server Hostname [:Port] (optional)	(Optional) Specify the backup LDAP server to use if the primary server does not respond. If the server returns an authentication failure (bad password, unknown username, etc), then the backup server is not tried. The backup server is tried only when the primary server has a communication failure. Use the same format as the primary server to specify the host name and port.
Request Timeout	The length of time, in seconds, to wait for a response from the LDAP server. The default is 10 .

6. When finished, click **Save**.

Using the LDAP over SSL (LDAPS) Protocol

When choosing the LDAPS protocol to authenticate users, make sure the following conditions are true:

- The SSL certificate for the LDAPS server has been uploaded into the trusted store.
- The external authentication method is set to “LDAP”.
- The URL for the LDAPS server(s) starts with “ldaps://”.

After uploading the SSL certificate, restart the **aps** process (**Setup > System Admin > Process Status > aps Restart**).



RADIUS Authentication

This authentication method allows users to authenticate against a RADIUS server. Even when RADIUS authentication is enabled, each user account must exist locally on your system. The username must match the one in the RADIUS server, although the password can be different. A user must present a valid username and (RADIUS) password to be successfully authenticated.

To configure RADIUS authentication settings:

1. Click **Administration > System Admin**.
2. Click **Authentication** in the **Users/Groups** section.
3. Click the **External Authentication** tab.
4. From the drop-down menu, choose **RADIUS**.
5. **Allow Local Password Fallback** provides two options:
 - **Allow Local Password Fallback for Default Admin Only**
Select this option to allow the default admin user to log in using only a username and password if RADIUS authentication fails. This privilege is restricted to the admin user only. All others must be authenticated by RADIUS. This option is enabled by default.
 - **Allow Local Password Fallback for All Users**
Select this option to allow all users to log in using their local user name and password, if RADIUS authentication fails. For more information, see "[Local Password Fallback](#)" on the [next page](#).

6. Update the RADIUS Server parameters as necessary:

Parameter	Description
Server Hostname[:port]	Specify the host name and port of the RADIUS server.
Backup Server hostname[:port] (optional)	(Optional) Specify the backup RADIUS server to use if the primary server does not respond. If the server returns an authentication failure (bad password, unknown username, etc), then the backup server is not tried. The backup server is tried only when the primary server has a communication failure. Use the same format as the primary server to specify the host name and port.
Shared Authentication Secret	Specify a RADIUS passphrase.
NAS IP Address	The IP address of the Network Access Server (NAS).
Request Timeout	The length of time, in seconds, to wait for a response from the RADIUS server (in seconds). The default is 10 .
Retry Request	Number of times to retry a RADIUS request. The default is 1 .
RADIUS Protocol:	Use the drop-down menu to choose a protocol option. The default is None .

7. Click **Save.**

Local Password Fallback

You can use this feature to log in using your local user name and password if the external authentication (Certificate, LDAP, or RADIUS) fails, if you forgot your password to the authentication server, or if the authentication server is not available.

The Use Local Authentication allows the default admin to log in even when the remote authentication server is not available, by adding a **Use Local Authentication** check box to the login screen. Out-of-box, this option is enabled only for the default administrator. However, it is possible to allow local password fallback for all users. For example, you could configure the RADIUS authentication method to allow users to log in using local authentication instead of RADIUS should they fail to authenticate to the configured external RADIUS server(s).

For information on how to allow local password fallback for all users for all users, see "[Client Certificate Authentication](#)" on page 303, "[LDAP/AD and LDAPS Authentication](#)" on page 304, or "[RADIUS Authentication](#)" on the previous page.

To log in when authentication fails:

1. Select the **Use Local Authentication** check box.



Note: This option is only available to the default admin unless it has been enabled for other users.

2. Specify your login and password and click **Login**.

Login Banner

You can customize the message on the login screen to suit your needs. The text you specify in the **Content** field is displayed before the login screen. In addition, you can specify a confirmation message that the user must click to enable the **Username** and **Password** fields.

You must have the “Configure Login Settings” permission enabled for your user account to edit the login banner.

To customize the login banner:

1. Click **Administration > Setup > System Admin**.
2. Click **Login Banner** in the **Users/Groups** section.
3. Specify the text you want to display as the login banner in the **Content** field.

You can specify only unformatted text in this field; however, you can apply standard HTML tags to display formatted text. Loading images in this field is not allowed.

4. (Optional) Specify text in the **Confirmation** field. Any text entered will be displayed in the login banner. In order to log in, the user must click the text to continue to the **Username** and **Password** fields. For example, if you specify “Are you sure?”, then the user must click the text “Are you sure?” to display the login screen.



Note: If you leave the **Confirmation** field empty, the word "OK" will be displayed by default, and the user must click it to continue.

5. Click **Save**.

User Management



For a containerized environment only, Fusion user management replaces all user management functions. Use ArcMC user management standalone installations.

The **Users** and **Groups** tabs enable you to manage users and user groups on your system. User groups are a way to enforce access control to various sections of your system.

Users

Open the **Users** tab to manage the users that can log in to your system. You can add a new user, edit user information, or delete a user at any time. You must have the appropriate System Admin group rights to perform these functions.

To add a new user:

1. Click **Administration > Setup > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, click **Add** from the top left side of the page.

4. Specify the following parameters.

Parameter	Description
<i>Credentials</i>	
Login	The user's login name.
Password	The user's password.
Confirm Password	Reenter the user's password.
<i>Contact Information</i>	
Use Client DN	<p>If you enabled SSL client certificate or LDAP authentication, click this link to specify the user's Distinguished Name (Certificate Subject) information. The Distinguished Name should be similar to this format:</p> <p>CN=UserA,OU=Engg Team,O=ArcSight\, Inc.,L=Cupertino,C=US,ST=California</p> <p>To determine the DN, use this URL to display the certificate:</p> <p><a href="https://<hostname or IP address >/platform-service/">https://<hostname or IP address >/platform-service/</p> <p>DisplayCertificate</p> <p>OR</p> <p>Obtain the DN information from the browser that the user will open to connect to the system. For example, on Mozilla Firefox, click Tools > Options > Advanced > Encryption > View Certificates > Your Certificates > Select the certificate > View.</p>
First Name	The user's first name.
Last Name	The user's last name.
Email	The user's email address.
Phone Number	(Optional) The user's phone number.
Title	(Optional) The user's title.
Department	(Optional) The user's department.
Fax	(Optional) The user's fax number.
Alternate Number	(Optional) The user's alternate phone number.
Assign to Groups	Select the groups to which this user belongs. This setting controls the privileges a user has on this Arcsight Management Center.

Parameter	Description
System Admin	Select a rights level from the drop-down list: <ul style="list-style-type: none"> • Default <i>System Admin Group</i> gives the user rights to change the settings in the System Admin menu. Choosing this option displays all the tabs and menus. • <i>Read Only System Admin Group</i> allows the user read-only access. • <i>Unassigned</i> prevents user access to the System Admin menu.
ArcMC Rights	Select a rights level from the drop-down list: <ul style="list-style-type: none"> • Default <i>ArcMC Rights Group</i> gives the user rights to the Dashboard, Node Management, and Configuration Management menus, as well as the Backup/Restore and Repositories menus. Choosing this option displays all the tabs and menus. • <i>Read Only ArcMC Group</i> allows the user read-only access. • <i>Unassigned</i> prevents user access to all ArcMC components.
Notes	(Optional) Other information about the user.

5. Click **Save and Close**.

To edit a user:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, select the user (or users) you want to edit.
4. Click **Edit** from the top left side of the page.
5. Update the user information as necessary.
6. Click **Save User**.

To delete a user:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, select the user (or users) you want to delete.
4. Click **Delete** from the top left side of the page.

Reset Password

The Reset Password feature enables you to reset a user's password without knowing their password. If you are using an SMTP-configured server and have permissions to create and update users, you can reset a user's password by clicking the **Reset Password** button. An automated email including the new password string is sent to the user.

An SMTP server must be configured for the automated email containing the temporary password to be sent. If an SMTP server is not configured, the password will not be reset because an email cannot be sent.

To reset a user's password:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, select the user (or users) whose passwords you want to reset.
4. Click **Reset Password** from the top left side of the page.

The user must use the temporary string to log in within the time specified in the email. If the user does not log in within the specified time, the account becomes deactivated. If the account has been deactivated, the admin must re-activate it before resetting the password.

To activate a user:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. In the **Users** tab, select the user (or users) that you want to activate.
4. Select **Edit**.
5. Check the **Active** box.
6. **Save** the changes.

Groups

User groups define privileges to specific functions on your system and serve to enforce access control to these functions. For example, if you want User A to perform system admin related activities that are not Connector Appliance management specific, assign that user to the System Admin group, but not to the Connector Appliance group.

User groups are divided into the following types: System Admin and Connector Appliance Rights Groups. Each type has a pre-defined, default user group in which all privileges for the type are enabled. To authorize a subset of the privileges for a specific group type, create a new user group and enable only the privileges you want to provide for that group. Then, assign restricted users to the newly created group.

System Admin Groups

System Admin Group

The System Admin Group controls the system administration operations for your system, such as configuring network information, setting storage mounts, installing SSL certificates, and user management.

Read Only System Admin Group

In addition to the default System Admin Group that enables all rights (privileges), a Read Only System Admin Group is available on your system. Users assigned to this group can view System Admin settings, but cannot change them.

ArcSight Management Center Rights Groups for Arcsight Management Center

ArcSight Management Center Rights Group

The Connector Appliance Rights Group controls the Arcsight Management Center application operations for your system, such as viewing the Arcsight Management Center dashboards and backup operations.

Read Only ArcSight Management Center Group

In addition to the default Connector Appliance Rights Group that enables all rights (privileges), Connector Appliance provides more controlled authorizations and a “view only” default option. A read-only user can view the tabs and the operations displayed on the tabs, and can perform operations such as refresh, view certificate list, and Logfu.

Refer to your system’s user interface for a complete list of rights available to this group.



Caution: It is strongly recommended not to modify any rights for the default admin user, as this can cause access issues.

Managing a User Group

To create a new user group:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. Click the **Groups** tab.
4. Click **Add** from the top left side of the page.
5. Define the new group:
 - a. In the **Group Name** field, provide a name for the group.
 - b. In the **Description** field, provide a description for the group.

- c. From the Group Type drop-down box, select the group type.
- d. Click the down arrow icon next to the group type name to view and select privileges that you want to assign to the users in this group.
6. Click **Save and Close** to save the settings of the group, or click **Save and Edit Membership** to add users to this group.

To edit a user group:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. Click the **Groups** tab.
4. Select the group that you want to edit, and click **Edit** at the top left side of the page.
5. Update the user group information.
If you need to edit the group's membership:
 - a. Click **Save and Edit Membership** to display the Edit Group Membership page.
 - b. Click **Add** from the top left of the Edit Group Membership page.
 - c. Select users you want to add. By default, you can add only users who do not belong to other groups of the type that you are editing. To add such users, click **Show users that belong to other <group_type> groups**.
When you add a user who belongs to another group of the same type as the one you are updating, that user is automatically removed from the previous group.
- d. Click **OK**.
- e. Click **Back to Group List**.
6. Click **Save and Close**.

To delete a user group:

1. Click **Administration > System Admin**.
2. Click **User Management** in the **Users/Groups** section in the left panel.
3. Click the **Groups** tab.
4. Select the group (or groups) that you want to delete.
5. Click **Delete** at the top left side of the page.

Change Password

You can use the **Change Password** menu to change your application password. This feature is available to all users for changing their passwords, unlike the Reset Password feature that

enables a system administrator to reset the password of users without knowing the password. Passwords are subject to the secure password policy specified by the Admin user, as well as the following restrictions.

- Password reset attempts for the admin user will fail, to prevent an unauthenticated user from resetting the admin account.
- If the password reset attempt fails due to resetting an unknown or admin user, ArcMC will not report the failure.

To change your password:

1. Click **Administration > Setup > System Admin**.
2. Click **Change Password** in the **Users/Groups** section in the left panel to display the **Change Password for <User Name>** page.
3. Enter the old password, specify a new password, and specify the new password a second time to confirm.

Appendix A: Audit Logs

The following topics are discussed here.

Audit Event Types

You can forward Arcsight Management Center application audit events, which are in Common Event Format (CEF), to a destination of your choice.

Several types of audit events are generated by Arcsight Management Center:

- **Application events:** related to Arcsight Management Center functions and configuration changes
- **Platform events:** related to the Arcsight Management Center system
- **System health events:** related to Arcsight Management Center health.

Audit Event Information

An Arcsight Management Center audit event contains information about the following prefix fields.

- Device Event Class ID
- Device Severity
- Name
- Device Event Category (cat)

See "[Audit Logs](#)" on page 286 for details on how to generate audit logs.



Note: If no Syslog Daemon connector is installed or configured on your local machine, then no audit events will be visible.

Application Events

Application Events

Signature	Severity	Description	deviceEventCategory
Connector			
connector:101	1	Register connector successful	/Connector/Add/Success

Application Events, continued

Signature	Severity	Description	deviceEventCategory
connector:102	1	Connector removed successfully	/Connector/Delete
connector:103	1	Update connector parameters successful	/Connector/Parameter/Update/Success
connector:104	1	AUP Package create successful	/Connector/AUP Package/Create/Success
connector:105	1	AUP Package deploy successful	/Connector/AUP Package/Deploy/Success
connector:201	1	Connector add failed	/Connector/Add/Fail
connector:202	1	Connector delete failed	/Connector/Delete/Fail
connector:203	1	Connector parameters update failed	/Connector/Parameter/Update/Fail
Arcsight Management Center			
arcmc:101	1	ConfigurationBackupScheduler add success	/BackupScheduler/Add/Success
arcmc:102	1	ConfigurationBackupScheduler update successful	/BackupScheduler/Update/Success
arcmc:103	1	ConfigurationBackupScheduler delete success	/BackupScheduler/Delete/Success
arcmc:104	1	Scheduled Backup triggered	/Backup/Scheduled/Trigger
arcmc:105	1	Scheduled Backup completed	/Backup/Scheduled/Complete/Success
arcmc:106	1	Manual Backup completed	/Backup/Manual/Complete/Success
arcmc:107	1	Local Backup completed	/Backup/Local/Complete/Success
arcmc:108	1	You have exceeded the maximum number of managed connectors allowed by your license	/RemotelyManagedConnectors/Exceeded
arcmc:110	1	You have attempts to exceed the maximum number of managed products allowed by your license	/managedproducts/exceeded

Application Events, continued

Signature	Severity	Description	deviceEventCategory
arcmc:111	1	Reboot command launched successfully	Node/reboot/launched/Success
arcmc:112	1	New configuration created successfully	/Configuration/Add/Success
arcmc:113	1	Edit configuration successful	/Configuration/Edit/Success
arcmc:114	1	Delete configurations successful	/Configuration/Delete/Success
arcmc:115	1	Push configuration successful	/Configuration/Push/Success
arcmc:116	1	Import configuration successful	/Configuration/Import/Success
arcmc:117	1	Add subscriber to configuration successful	/Configuration/Subscribe/Success
arcmc:118	1	Unsubscribe node for configuration successful	/Configuration/Unsubscribe/Success
arcmc:119	1	Check compliance of configuration successful	/Configuration/Check Compliance/Success
arcmc:120	1	Configuration set successfully	/Node/Set/Configuration/Success
arcmc:121	1	Configuration appended successfully	/Node/Append/Configuration/Success
arcmc:122	1	Agent install success	/ArcMCAgent/Install/Success
arcmc:123	1	Upgrade agent successfully	/ArcMCAgent/Upgrade/Success
arcmc:124	1	Add/Push Logger Peers Successful	/Logger/AddPeers/Success
arcmc:125	1	Remove Logger Peers Successful	/Logger/RemovePeers/Success
arcmc:127	1	Create/Import Logger Peer Group Successful	/Logger/AddPeerGp/Success
arcmc:128	1	Delete Logger Peer Group Successful	/Logger/DeletePeerGp/Success
arcmc:129	1	Edit Logger Peer Group Successful	/Logger/EditPeerGp/Success

Application Events, continued

Signature	Severity	Description	deviceEventCategory
arcmc:130	1	Import Initial Configuration Successful	/Logger/ImportInitConfig/Success
arcmc:131	1	Pushed Initial Configuration	/Logger/PushInitConfig/Success
arcmc:132	1	Deleted Initial Configuration	/Logger/DelInitConfig/Success
arcmc:133	1	Host upgrade started.	/Node/Upgrade/Start
arcmc:134	1	Host upgrade successful.	/Node/Upgrade/Success
arcmc:138	1	Update rule/s	/ArcMC/UpdateRules/Success
arcmc:142	1	Rule add success	/ArcMC/AddRule" + SUCCESS
arcmc:143	1	Rule delete success	/ArcMC/DeleteRule" + SUCCESS
arcmc:201	1	ConfigurationBackupScheduler add failed	/BackupScheduler/Add/Fail
arcmc:202	1	ConfigurationBackupScheduler update failed	/BackupScheduler/Update/Fail
arcmc:203	1	ConfigurationBackupScheduler delete failed	/BackupScheduler/Delete/Fail
arcmc:205	1	Scheduled Backup failed	/Backup/Scheduled/Complete/Fail
arcmc:206	1	Manual Backup failed	/Backup/Manual/Complete/Fail
arcmc:212	1	New configuration creation failed	/Configuration/Add/Fail
arcmc:213	1	Edit configuration failed	/Configuration/Update/Fail
arcmc:214	1	Configuration deletion failed	/Configuration/Delete/Fail
arcmc:215	1	Push configuration failed	/Configuration/Import/Fail
arcmc:216	1	Import configuration failed	/Backup/Local/Push/Fail
arcmc:217	1	Add subscriber to configuration failed	/Configuration/Subscribe/Fail
arcmc:218	1	Unsubscribe node for configuration failed	/Configuration/Unsubscribe/Fail
arcmc:219	1	Check compliance of configuration failed	/Configuration/Check Compliance/Success

Application Events, continued

Signature	Severity	Description	deviceEventCategory
arcmc:220	1	Configuration set failed	/Node/Set/Configuration/Fail
arcmc:221	1	Configuration append failed	/Node/Append/Configuration/Fail
arcmc:222	1	Agent install failed	/ArcMCAgent/Install/Failure
arcmc:223	1	Upgrade agent failed	/ArcMCAgent/Upgrade/Fail
arcmc:224	1	Add/Push Logger Peers Failed	/Logger/AddPeers/Fail
arcmc:225	1	Remove Logger Peers Failed	/Logger/RemovePeers/Fail
arc mc:226	1	Alert message payload	/ArcMCMonitor/Breach
arcmc:230	1	Import Initial Configuration Failed	/Logger/ImportInitConfig/Fail
arcmc:234	1	Host upgrade failed.	/Node/Upgrade/Fail
arcmc:250	1	Push user assignment <assignment name>	/ArcMCUM/Push
arcmc:251	1	Decommission user <UserName>	/ArcMCUM/DeleteUser
arcmc:252	1	Add user <UserName>	/ArcMCUM/AddUser
Destination			
destination:102	1	Update destination successful	/Connector/Destination/Update/Success
destination:103	1	Remove destination successful	/Connector/Destination/Delete/Success
destination:104	1	Update destination configuration successful	/Connector/Destination/Configuration/Update/Success
destination:105	1	Register destination successful	/Connector/Destination/Registration/Success
destination:106	1	Create destination configuration successful	/Connector/Destination/Configuration/Add/Success
destination:107	1	Destination configuration delete successful	/Connector/Destination/Configuration/Delete/Success
destination:202	1	Destination update to a connector failed	/Connector/Destination/Update/Fail

Application Events, continued

Signature	Severity	Description	deviceEventCategory
destination:203	1	Destination delete from a connector failed	/Connector/Destination/Delete/Fail
destination:204	1	Destination configuration update failed	/Connector/Destination/Configuration/Update/Fail
destination:205	1	Register destination failed	/Connector/Destination/Registration/Fail
destination:206	1	Destination configuration add failed	/Connector/Destination/Configuration/Add/Fail
destination:207	1	Destination configuration delete failed	/Connector/Destination/Configuration/Delete/Fail
Container			
container:101	1	Container upgrade successful	/Container/Upgrade/Success
container:102	1	Push user file successful	/Container/UserFiles/Push/Success
container:103	1	User file delete from container	/Container/UserFiles/Delete
container:104	1	CA cert push to a container successful	/Container/CACert/Push/Success
container:105	1	Container demo CA enable successful	/Container/DemoCA/Enable/Success
container:106	1	Container demo CA disable successful	/Container/DemoCA/Disable/Success
container:109	1	Delete property from a container successful	/Container/Property/Delete/Success
container:110	1	Modify properties successful	/Container/Property/Update/Success
container:111	1	Container password update successful	/Container/Password/Update/Success
container:112	1	Container add successful	/Container/Add/Success
container:113	1	Container edit	/Container/Update
container:114	1	Remove container	/Container/Delete
container:115	1	Add certificate for a container successful	/Container/Certificate/Add/Success

Application Events, continued

Signature	Severity	Description	deviceEventCategory
container:116	1	Removing certificates successful [addtrust class 1ca]	/Container/Certificate/Delete/Success
container:117	1	Enabling FIPS mode successful	/Container/FIPS/Enable/Success
container:118	1	Disabling FIPS mode successful	/Container/FIPS/Disable/Success
container:119	1	Upgrade was triggered for container that resides on end of life appliance model	Container/FromEndOfLifeModel/Upgrade/Triggered
container:123	1	Emergency restore failed	/Container/EmergencyRestore/Fail
container:201	1	Container upgrade failed	/Container/Upgrade/Fail
container:202	1	User file push to a container failed	/Container/UserFiles/Push/Fail
container:204	1	CA cert push to a container failed	/Container/CACert/Push/Fail
container:205	1	Enable demo CA for a container failed	/Container/DemoCA/Enable/Fail
container:206	1	Disable demo CA for a container failed	/Container/DemoCA/Disable/Fail
container:209	1	Delete property from a container failed	/Container/Property/Delete/Fail
container:210	1	Update property to a container failed	/Container/Property/Update/Fail
container:211	1	Container password update failed	/Container/Password/Update/Fail
container:212	1	Container add failed	/Container/Add/Fail
container:215	1	Add certificate for a container failed	/Container/Certificate/Add/Fail
container:216	1	Delete certificate for a container failed	/Container/Certificate/Delete/Fail
container:217	1	Enable FIPS on a container failed	/Container/FIPS/Enable/Fail
container:218	1	Disable FIPS on a container failed	/Container/FIPS/Disable/Fail

Application Events, continued

Signature	Severity	Description	deviceEventCategory
container:219	1	SSL Certificate downloaded successfully	/Container/Certificate/Download/Success
container:220	1	SSL Certificate download failed	/Container/Certificate/Download/Fail
container:221	1	SSL Certificate imported successfully	/Container/Certificate/Import/Success
container:222	1	SSL Certificate import failed	/Container/Certificate/Import/Fail
container:226	1	Emergency restore successful	/Container/EmergencyRestore/Success
container:301	1	Container upgrade started	/Container/Upgrade/Start
Transformation Hub			
eventbroker:146	1	Transformation Hub Add Topic succesful	/EventBroker/Topic/Add/Success
eventbroker:147	1	Transformation Hub delete route/s successful	/EventBroker/Route/Add/Success
eventbroker:148	1	Transformation Hub Add Route/s successful	/EventBroker/Route/Add/Success
eventbroker:149	1	Transformation Hub Update Route successful	/EventBroker/Route/Update/Success
eventbroker:241	1	Transformation Hub Add Topic failed	/EventBroker/Topic/Add/Fail
eventbroker:242	1	Transformation Hub delete route/s failed	/EventBroker/Route/Add/Fail
eventbroker:243	1	Transformation Hub Add Route failed	/EventBroker/Route/Add/Fail
eventbroker:244	1	Transformation Hub Update Route failed	/EventBroker/Route/Update/Fail
Location			
location:101	1	Location add successful	/Location/Add/Success
location:102	1	Location edit	/Location/Update
location:103	1	Remove location	/Location/Delete
location:201	1	Location add failed	/Location/Add/Fail
Host			

Application Events, continued

Signature	Severity	Description	deviceEventCategory
host:101	1	Host add successful	/Host/Add/Success
host:103	1	Remove host	/Host/Delete
host:105	1	Host certificate download and import successful	/Host/Certificate/Download/Import/Success
host:201	1	Host add failed	/Host/Add/Fail
host:205	1	Host certificate download and import failed	/Host/Certificate/Download/Import/Fail
host:363	1	Move Host	/Host/Move/Success
host:364	1	Move Host	/Host/Move/Fail
Marketplace			
marketplace:150	1	Successfully saved Marketplace user in ArcMC	/Marketplace/User/Add/Success
marketplace:245	1	Failed to save Marketplace user in ArcMC	/Marketplace/User/Add/Fail
Deployment Templates			
deploymenttemplates:151	1	Successfully deleted template instance(s) in ArcMC	/DeploymentTemplates/TemplateInstance/Delete/Success
deploymenttemplates:246	1	Failed to delete template instance(s) in ArcMC	/DeploymentTemplates/TemplateInstance/Delete/Fail
deploymenttemplates:152	1	Successfully added template instance in ArcMC	/DeploymentTemplates/TemplateInstance/Add/Success
deploymenttemplates:247	1	Failed to add template instance in ArcMC	/DeploymentTemplates/TemplateInstance/Add/Fail
deploymenttemplates:153	1	Successfully updated template instance in ArcMC	/DeploymentTemplates/TemplateInstance/Update/Success
deploymenttemplates:248	1	Failed to update template instance in ArcMC	/DeploymentTemplates/TemplateInstance/Update/Fail
Generator ID			

Application Events, continued

Signature	Severity	Description	deviceEventCategory
generatorid:157	1	Generate ID create successful	/GeneratorID/Add/Success
generatorid:251	1	Generate ID create failed	/GeneratorID/Add/Fail
generatorid:158	1	Generate ID edit successful	/GeneratorID/Update/Success
generatorid:158	1	Generate ID edit failed	/GeneratorID/Update/Fail
generatorid:159	1	Generate ID delete successful	/GeneratorID/Delete/Success
generatorid:159	1	Generate ID delete failed	/GeneratorID/Delete/Fail

Platform Events

Platform Events

Signature	Severity	Definition	Category
platform:200	7	Failed password change	/Platform/Authentication/PasswordChange/Failure
platform:201	7	Failed login attempt	/Platform/Authentication/Failure/Login
platform:202	5	Password changed	/Platform/Authentication/Password
platform:203	7	Login attempt by inactive user	/Platform/Authentication/InactiveUser/Failure
platform:205	7	Automated password reset attempt made for admin account	/Platform/Authentication/PasswordChange/AdminFailure
platform:206	7	Failed automated password reset attempt for user	/Platform/Authentication/PasswordChange/Failure
platform:207	7	Automated password reset attempted for non-existent user	/Platform/Authentication/PasswordChange/UnknownUser
platform:213	7	Audit forwarding modified	/Platform/Configuration/Global/AuditEvents
platform:220	5	Installed certificate	/Platform/Certificate/Install

Platform Events, continued

Signature	Severity	Definition	Category
platform:221	7	Certificate mismatch failure	/Platform/Certificate/Mismatch
platform:222	1	Created certificate signing request	/Platform/Certificate/Request
platform:224	5	Re-generate self-signed certificate	/Platform/Certificate/Regenerate
platform:226	7	Uploaded update file damaged or corrupt	/Platform/Update/Failure/CorruptPackage
platform:227	5	Update installation success	/Platform/Update/Applied
platform:228	7	Update installation failure	/Platform/Update/Failure/Installation
platform:230	3	Successful login	/Platform/Authentication/Login
platform:234	7	Failed login attempt (LOCKED)	/Platform/Authentication/Failure/LOCKED
platform:239	1	User logout	/Platform/Authentication/Logout
platform:240	3	Added user group	/Platform/Groups/Add
platform:241	3	Updated user group	/Platform/Groups/Update
platform:242	5	Removed all members from group	/Platform/Authorization/Groups/Membership/Update/Clear
platform:244	3	Deleted user group	/Platform/Groups/Remove
platform:245	3	Added user	/Platform/Users/Add
platform:246	3	Updated user	/Platform/Users/Update
platform:247	3	Deleted user	/Platform/Users/Delete
platform:248	3	Session expired	/Platform/Authentication/Logout/SessionExpiration
platform:249	7	Account locked	/Platform/Authentication/AccountLocked
platform:250	3	Added remote mount point	/Platform/Storage/RFS/Add
platform:251	5	Edited remote mount point	/Platform/Storage/RFS/Edit
platform:252	7	Failed to create remote mount point	/Platform/Storage/RFS/Failure

Platform Events, continued

Signature	Severity	Definition	Category
platform:253	5	Removed remote mount point	/Platform/Storage/RFS/Remove
platform:260	5	Static route modified	/Platform/Configuration/Network/Route/Update
platform:261	5	Static route removed	/Platform/Configuration/Network/Route/Remove
platform:262	5	Appliance time modified	/Platform/Configuration/Time
platform:263		NIC settings modified	/Platform/Configuration/NIC
platform:264		NTP server settings modified	/Platform/Configuration/NTP
platform:265	5	DNS settings modified	/Platform/Configuration/Network/DNS
platform:266	5	Hosts file modified	/Platform/Configuration/Network/Hosts
platform:267	5	SMTP settings modified	/Platform/Configuration/SMTP
platform:268	5	Static route added	/Platform/Configuration/Network/Route/Add
platform:269	5	Updated Platform Settings	/Platform/Configuration
platform:280	7	Appliance reboot initiated	/Appliance/State/Reboot/Initiate
platform:281	3	Appliance reboot canceled	/Appliance/State/Reboot/Cancel
platform:282	9	Appliance poweroff initiated	/Appliance/State/Shutdown
platform:284	5	Enabled SAN Multipathing	/Platform/Storage/Multipathing/Enable
platform:285	5	Disabled SAN Multipathing	/Platform/Storage/Multipathing/Disable
platform:300	5	Installed trusted certificate	/Platform/Certificate/Install
platform:301	5	Installed certificate revocation list	/Platform/Certificate/Revocation/Install
platform:302	5	Deleted trusted certificate	/Platform/Certificate/Delete
platform:303	5	Deleted certificate revocation list	/Platform/Certificate/Revocation/Delete

Platform Events, continued

Signature	Severity	Definition	Category
platform:304	7	Failed installing trusted certificate	/Platform/Certificate/Install/Failure
platform:305	7	Failed installing certificate revocation list	/Platform/Certificate/Revocation/Install/Failure
platform:306	5	Start process	/Platform/Process/Start
platform:307	5	Stop process	/Platform/Process/Stop
platform:308	5	Restart process	/Platform/Process/Restart
platform:310	5	Enabled FIPS mode	/Platform/Configuration/FIPS/Enable
platform:311	7	Disabled FIPS mode	/Platform/Configuration/FIPS/Disable
platform:312	7	Web server cipher strength changed	/Platform/Configuration/WebServer/CipherStrength
platform:313	5	Enable SSH	/Platform/Configuration/SSH/Enable
platform:314	7	Disable SSH	/Platform/Configuration/SSH/Disable
platform:315	7	Enable SSH only during startup/reboot	/Platform/Configuration/SSH/StartupOnly
platform:316	7	Enable SSH only for 8 hours	/Platform/Configuration/SSH/Enable8Hours
platform:320	3	Appliance poweroff canceled	/Appliance/State/Shutdown/Cancel
platform:371	5	Restarted OS service	/Platform/Service/Restart
platform:400	1	Ran diagnostic command	/Platform/Diagnostics/Command
platform:407	7	SSL certificate expiration warning	/Platform/Certificate/SSL/Expiration
platform:408	5	Appliance startup completed	/Appliance/State/Startup
platform:409	3	Configure login warning banner	/Platform/Configuration/LoginBanner
platform:410	3	Network settings modified	
platform:411	5	Automated password reset	/Platform/Authentication/PasswordChange
platform:412	3	Set locale	/Platform/Configuration/Locale

Platform Events, continued

Signature	Severity	Definition	Category
platform:440	3	SNMP configuration modified	Platform/Configuration/SNMP
platform:450	3	FTP service enabled	
platform:451	3	FTP service disabled	
platform:454	3	FTP service configuration changed	
platform:455	3	Added sub directory	
platform:456	3	Removed sub directory	
platform:460	3	NIC alias added	/Platform/Network/Alias/Add
platform:462	3	NIC alias removed	/Platform/Network/Alias/Remove
platform:500	5	Remove member from group	/Platform/Authorization/Groups/Membership/Remove
platform:501	5	Group member added	/Platform/Authorization/Groups/Membership/Add
platform:502	5	User removed from group	/Platform/Authorization/Users/Groups/Remove
platform:503	5	User added to group	/Platform/Authorization/Users/Groups/Add
platform:530	5	Authentication Session settings successfully changed	/Platform/Configuration/Authentication/Sessions/Success
platform:540	5	Password Lockout settings successfully updated	/Platform/Configuration/Authentication/Password/Lockout/Success
platform:550	5	Password Expiration settings successfully updated	/Platform/Configuration/Authentication/Password/Expiration/Success
platform:560	5	Password Validation settings successfully updated	/Platform/Configuration/Authentication/Password/Validation/Success
platform:570	5	Allow Automated Password Reset settings successfully changed	/Platform/Configuration/Authentication/Password/AutomatedReset/Success

Platform Events, continued

Signature	Severity	Definition	Category
platform:590	5	RADIUS authentication settings successfully changed	/Platform/Configuration/Authentication/RADIUS/Success
platform:600	5	LDAP authentication settings successfully changed	/Platform/Configuration/Authentication/LDAP/Success
platform:610	5	Global authentication settings successfully changed	/Platform/Configuration/Authentication/Global/Success

System Health Events

System health events provide four status indicators:

- OK
- Degraded
- Rebuilding
- Failed

An **OK** event, indicating normal system behavior, is generated once every ten minutes (six events per hour, per sensor). For a status other than **OK** (**Degraded**, **Rebuilding**, or **Failed**), the event is sent every minute until the sensor returns an **OK** status.

SNMP Related Properties

The following list provides the event fields for system health events sent via SNMP traps. For detailed instructions on setting up SNMP traps, see ["SNMP" on page 274](#).

• event.deviceReceiptTime	• event.endTime
• event.deviceVendor	• event.deviceProduct
• event.deviceVersion	• event.deviceEventClassId
• event.name	• event.deviceSeverity
• event.deviceEventCategory	• event.deviceCustomNumber1
• event.deviceCustomNumber1Label	• event.deviceCustomString1
• event.deviceCustomString1Label	• event.deviceCustomString2
• event.deviceCustomString2Label	• event.deviceCustomString3

• event.deviceCustomString3Label	• event.deviceCustomString4
• event.deviceCustomString4Label	• event.deviceCustomString5
• event.deviceCustomString5Label	• event.deviceCustomString6
• event.deviceCustomString6Label	• event.destinationAddress
• event.deviceAddress	

The **snmp.mib.version** is set to 5.0.

System Health Events

Signature	Severity	Definition	Category
CPU			
cpu:100	1	CPU Usage	/Monitor/CPU/Usage
cpu:101	1	Health statistics per CPU	/Monitor/CPUn/Usage
Disk			
disk:101	1	Root Disk Space Remaining	/Monitor/Disk/Space/Remaining/Data
disk:102	1	Disk bytes read	/Monitor/Disk/drive/Read
disk:103	1	Disk bytes written	/Monitor/Disk/drive/Write
disk:104	1	Disk Space Remaining	/Monitor/Disk/Space/Remaining/Root
Hardware			
hardware:101	1	Electrical (Current) OK	/Monitor/Sensor/Current/Ok**
hardware:102	5	Electrical (Current) Degraded	/Monitor/Sensor/Current/Degraded**
hardware:103	8	Electrical (Current) Failed	/Monitor/Sensor/Current/Failed**
hardware:111	1	Electrical (Voltage) OK	/Monitor/Sensor/Voltage/Ok**
hardware:112	1	Electrical (Voltage) Degraded	/Monitor/Sensor/Voltage/Degraded**
hardware:113	1	Electrical (Voltage) Failed	/Monitor/Sensor/Voltage/Failed**
hardware:121	1	Battery OK	/Monitor/Sensor/Battery/Ok**
hardware:122	5	Battery Degraded	/Monitor/Sensor/Battery/Degraded **
hardware:123	8	Battery Failed	/Monitor/Sensor/Battery/Failed**
hardware:131	1	Fan OK	/Monitor/Sensor/Fan/Ok
hardware:132	5	Fan Degraded	/Monitor/Sensor/Fan/Degraded
hardware:133	8	Fan Failed	/Monitor/Sensor/Fan/Failed
hardware:141	1	Power Supply OK	/Monitor/Sensor/PowerSupply/Ok

System Health Events, continued

Signature	Severity	Definition	Category
hardware:142	5	Power Supply Degraded	/Monitor/Sensor/PowerSupply/Degraded
hardware:143	8	Power Supply Failed	/Monitor/Sensor/PowerSupply/Failed
hardware:151	1	Temperature OK	/Monitor/Sensor/Temperature/Ok
hardware:152	1	Temperature Degraded	/Monitor/Sensor/Temperature/Degraded
hardware:153	1	Temperature Failed	/Monitor/Sensor/Temperature/Failed
Memory			
memory:100	1	Platform memory usage	/Monitor/Memory/Usage/Platform
memory:101	1	Health statistics for JVM memory	/Monitor/Memory/Usage/Jvm
memory:102	1	Health statistics for platform buffers memory	/Monitor/Memory/Usage/Platform/Buffers
memory:103	1	Health statistics for platform cached memory	/Monitor/Memory/Usage/Platform/Cached
memory:104	1	Health statistics for platform free memory	/Monitor/Memory/Usage/Platform/Free
memory:105	1	Health statistics for JVM heap memory	/Monitor/Memory/Usage/Jvm/Heap
memory:106	1	Health statistics for JVM non-heap memory	/Monitor/Memory/Usage/Jvm/NonHeap
Network			
network:100	1	Network usage—Inbound	/Monitor/Network/Usage/iface/In
network:101	1	Network usage—Outbound	/Monitor/Network/Usage/iface/Out
network:200	1	Number of Apache connections	
NTP			
ntp:100	1	NTP synchronization	
RAID			
raid:101	1	RAID Controller OK	/Monitor/RAID/Controller/OK
raid:102	5	RAID Controller Degraded	/Monitor/RAID/Controller/Degraded
raid:103	8	RAID Controller Failed	/Monitor/RAID/Controller/Failed
raid:111	1	RAID BBU OK	/Monitor/RAID/BBU/Ok
raid:112	5	RAID BBU Degraded	/Monitor/RAID/BBU/Degraded
raid:113	8	RAID BBU Failed	/Monitor/RAID/BBU/Failed

System Health Events, continued

Signature	Severity	Definition	Category
raid:121	1	RAID Disk OK	/Monitor/RAID/DISK/Ok
raid:122	5	RAID Disk Rebuilding	/Monitor/RAID/DISK/Rebuilding
raid:123	8	RAID Disk Failed	/Monitor/RAID/DISK/Failed

Appendix B: Destination Runtime Parameters

The following table describes configurable destination parameters. The parameters listed in the table are not available for all destinations. The user interface automatically displays the parameters valid for a destination. For step-by-step instructions on updating the runtime parameters of a destination, see ["Editing Connector Parameters" on page 144](#).

Parameter	Description
Batching	Connectors can batch events to increase performance and optimize network bandwidth. When activated, connectors create blocks of events and send them when they either (1) reach a certain size or (2) the time window expires, whichever occurs first. You can also prioritize batches by severity, forcing the connector to send the highest-severity event batches first and the lowest-severity event batches later.
Enable Batching (per event)	Create batches of events of this specified size (5, 10, 20, 50, 100 , 200, 300 events).
Enable Batching (in seconds)	The connector sends the events if this time window expires (1, 5, 10, 15, 30, 60).
Batch By	This is Time Based if the connector should send batches as they arrive (the default) or Severity Based if the connector should send batches based on severity (batches of Highest Severity events sent first).
Time Correction	The values you set for these fields establish forward and backward time limits, that if exceeded, cause the connector to automatically correct the time reported by the device.
Use Connector Time as Device Time	Override the time the device reports and instead use the time at which the connector received the event. This option assumes that the connector will be more likely to report the correct time. (No Yes)
Enable Device Time Correction (in seconds)	The connector can adjust the time reported by the device Detect Time, using this setting. This is useful when a remote device's clock isn't synchronized with the ArcSight Manager. This should be a temporary setting. The recommended way to synchronize clocks between Manager and devices is the NTP protocol. The default is 0 .
Enable Connector Time Correction (in seconds)	The connector can also adjust the time reported by the connector itself, using this setting. This is for informational purposes only and allows you to modify the local time on the connector. This should be a temporary setting. The recommended way to synchronize clocks between Manager and connectors is the NTP protocol. The default is 0 .
Set Device Time Zone To	Ordinarily, it is presumed that the original device is reporting its time zone along with its time. And if not, it is then presumed that the connector is doing so. If this is not true, or the device isn't reporting correctly, you can switch this option from Disabled to GMT or to a particular world time zone. That zone is then applied to the time reported. Default: Disabled .
Device Time Auto-correction	

Parameter	Description
Future Threshold	The connector sends the internal alert if the detect time is greater than the connector time by Past Threshold seconds.
Past Threshold	The connector sends the internal alert if the detect time is earlier than the connector time by Past Threshold seconds.
Device List	A comma-separated list of the devices to which the thresholds apply. The default, (ALL), means all devices.
Time Checking	These are the time span and frequency factors for doing device-time auto-correction.
Future Threshold	The number of seconds by which to extend the connector's forward threshold for time checking. The default is 5 minutes (300 seconds).
Past Threshold	The number of seconds by which to extend the connector's rear threshold for time checking. Default is 1 hour (3,600 seconds).
Frequency	The connector checks its future and past thresholds at intervals specified by this number of seconds. Default is 1 minute (60 seconds).
Cache	Changing these settings will not affect the events cached, it will only affect new events sent to the cache.
Cache Size	Connectors use a compressed disk cache to hold large volumes of events when the ArcSight Manager is down or when the connector receives bursts of events. This parameter specifies the disk space to use. The default is 1 GB which, depending on the connector, can hold about 15 million events, but it also can go down to 5 MB . When this disk space is full, the connector drops the oldest events to free up disk cache space. (5 MB, 50 MB, 100 MB, 150 MB, 200 MB, 250 MB, 500 MB, 1 GB, 2.5 GB, 5 GB, 10 GB, 50 GB.)
Notification Threshold	The size of the cache's contents at which to trigger a notification. Default is 10,000 .
Notification Frequency	How often to send notifications after the Notification Threshold is reached. (1 minute, 5 minutes, 10 minutes , 30 minutes, 60 minutes.)
Network	
Heartbeat Frequency	This setting controls how often the connector sends a heartbeat message to the destination. The default is 10 seconds , but it can go from 5 seconds to 10 minutes . Note that the heartbeat is also used to communicate with the connector; therefore, if its frequency is set to 10 minutes , then it could take as much as 10 minutes to send any configuration information or commands back to the connector.
Enable Name Resolution	The connector tries to resolve IP addresses to hostnames, and hostnames to IP addresses , if required and if the event rate allows. This setting controls this functionality. The Source, Target and Device IP addresses , and Hostnames might also be affected by this setting. By default, name resolution is enabled (Yes).
Name Resolution Host Name Only	Default: Yes .

Parameter	Description
Name Resolution Domain From E-mail	Default: Yes .
Clear Host Names Same as IP Addresses	Default: Yes .
Limit Bandwidth To	A list of bandwidth options you can use to constrain the connector's output over the network. (Disabled , 1 kbit/sec to 100 Mbits/sec.)
Transport Mode	You can configure the connector to cache to disk all the processed events it receives. This is equivalent to pausing the connector. However, you can use this setting to delay event-sending during particular time periods. For example, you could use this setting to cache events during the day and send them at night. You can also set the connector to cache all events, except for those marked with a very-high severity, during business hours, and send the rest at night. (Normal Cache Cache (but send Very High severity events)).
Address-based Zone Population Defaults Enabled	This field applies to v3.0 ArcSight Managers. This field is not relevant in ESM v3.5 because the system has integral zone mapping. Default: Yes .
Address-based Zone Population	This field applies to v3.0 ArcSight Managers. This field is not relevant in ESM v3.5 because the system has integral zone mapping.
Customer URI	Applies the given customer URI to events emanating from the connector. Provided the customer resource exists, all customer fields are populated on the ArcSight Manager. If this particular connector is reporting data that might apply to more than one customer, you can use Velocity templates in this field to conditionally identify those customers.
Source Zone URI	Shows the URI of the zone associated with the connector's source address. (Required for ESM v3.0 compatibility.)
Source Translated Zone URI	Shows the URI of the zone associated with the connector's translated source address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)
Destination Zone URI	Shows the URI of the zone associated with the connector's destination address. (Required for ESM v3.0 compatibility.).
Destination Translated Zone URI	Shows the URI of the zone associated with the connector's translated destination address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)
Connector Zone URI	Shows the URI of the zone associated with the connector's address. (Required for ESM v3.0 compatibility.)
Connector Translated Zone URI	Shows the URI of the zone associated with the connector's translated address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)
Device Zone URI	Shows the URI of the zone associated with the device's address. (Required for ESM v3.0 compatibility.)
Device Translated Zone URI	Shows the URI of the zone associated with the device's translated address. The translation is presumed to be NAT. (Required for ESM v3.0 compatibility.)

Parameter	Description
Field Based Aggregation	<p>This feature is an extension of basic connector aggregation. Basic aggregation aggregates two events if, and only if, all the fields of the two events are the same (the only difference being the detect time). However, field-based aggregation implements a less strict aggregation mechanism; two events are aggregated if only the selected fields are the same for both alerts. It is important to note that field-based aggregation creates a new alert that contains only the fields that were specified, so the rest of the fields are ignored.</p> <p>Connector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers. For example, you could enable field-based aggregation to aggregate "accepts" and "rejects" in a firewall, but you should use it only if you are interested in the count of these events, instead of all the information provided by the firewall.</p>
Time Interval	Select a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. (Disabled , 1 sec, 5 sec, and so on, up to 1 hour.)
Event Threshold	Select a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (that is, contained the same selected fields) and you select an event threshold of 100, you then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (Disabled , 10 events, 50 events, and so on, up to 10,000 events.)
Field Names	Specify one or more fields, if applicable, to use as the basis for aggregating the events the connector collects. The result is a comma-separated list of fields to monitor. For example, "eventName,deviceHostName" would aggregate events if they have the same event- and device-hostnames. Names can contain no spaces and the first letter must not be capitalized.
Fields to Sum	Specify one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.
Preserve Common Fields	Choosing Yes adds fields to the aggregated event if they have the same values for each event. Choosing No , the default, ignores non-aggregated fields in aggregated events.
Filter Aggregation	<p>Filter Aggregation is a way of capturing aggregated event data from events that would otherwise be discarded due to an agent filter. Only events that would be filtered out are considered for filter aggregation (unlike Field-based aggregation, which looks at all events).</p> <p>Connector aggregation significantly reduces the amount of data received, and should be applied only when you use less than the total amount of information the event offers.</p>
Time Interval	Select a time interval, if applicable, to use as a basis for aggregating the events the connector collects. It is exclusive of Event Threshold. (Disabled , 1 sec, 5 sec, and so on, up to 1 hour.)
Event Threshold	Select a number of events, if applicable, to use as a basis for aggregating the events the connector collects. This is the maximum count of events that can be aggregated; for example, if 150 events were found to be the same within the time interval selected (that is, contained the same selected fields) and you select an event threshold of 100, you then receive two events, one of count 100 and another of count 50. This option is exclusive of Time Interval. (Disabled , 10 events, 50 events, and so on, up to 10,000 events.)
Fields to Sum	(Optional) Select one or more fields, if applicable, to use as the basis for aggregating the events the connector collects.

Parameter	Description
Processing	
Preserve Raw Event	<p>For some devices, a raw event can be captured as part of the generated alert. If that is not the case, most connectors can also produce a serialized version of the data stream that was parsed/processed to generate the ArcSight event. This feature allows the connector to preserve this serialized "raw event" as a field. This feature is disabled by default since using raw data increases the event size and therefore requires more database storage space. You can enable this by changing the Preserve Raw Event setting. The default is No. If you choose Yes, the serialized representation of the "Raw Event" is sent to the destination and preserved in the Raw Event field.</p>
Turbo Mode	<p>You can accelerate the transfer of a sensor's event information through connectors by choosing one of two "turbo" (narrower data bandwidth) modes. The default transfer mode is called Complete, which passes all the data arriving from the device, including any additional data (custom, or vendor-specific).</p> <p>Complete mode does indeed use all the database performance advances of ArcSight ESM v3.x. The first level of Turbo acceleration is called Faster and drops just additional data, while retaining all other information. The Fastest mode eliminates all but a core set of event attributes, in order to achieve the best throughput.</p> <p>The specific event attributes that apply to these modes in your enterprise are defined in the self-documented <code>\$ARCSIGHT_HOME/config/connector/agent.properties</code> file for the ArcSight Manager. Because these properties might have been adjusted for your needs, you should refer to this file for definitive lists. Only scanner connectors need to run in Complete mode, to capture the additional data.</p> <p>Note: Connector Turbo Modes are superseded by the Turbo Mode in use by the ArcSight Managers processing their events. For example, a Manager set to Faster will not pass all the data possible for a connector that is set for the default of Complete.</p>

Parameter	Description
Enable Aggregation (in seconds)	<p>When enabled, aggregates two or more events on the basis of the selected time value. (Disabled, 1, 2, 3, 4, 5, 10, 30, 60)</p> <p>The aggregation is performed on one or more matches for a fixed subset of fields:</p> <ul style="list-style-type: none"> • Agent ID • Name • Device event category • Agent severity • Destination address • Destination user ID • Destination port • Request URL • Source address • Source user ID • Source port • Destination process name • Transport protocol • Application protocol • Device inbound interface • Device outbound interface • Additional data (if any) • Base event IDs (if any) <p>The aggregated event shows the event count (how many events were aggregated into the displayed event) and event type. The rest of the fields in the aggregated event take the values of the first event in the set of aggregated events.</p>
Limit Event Processing Rate	<p>You can moderate the connector's burden on the CPU by reducing its processing rate. This can also be a means of dealing with the effects of event bursts.</p> <p>The choices range from Disabled (no limitation on CPU demand) to 1 eps (pass just one event per second, making the smallest demand on the CPU).</p> <p>Note: The effect of this option varies with the category of connector in use, as described in the connector Processing Categories table below.</p>
Fields to Obfuscate	
Store Original Time in	Disabled or Flex Date 1.
Enable Port-Service Mapping	Default: No .
Enable User Name Splitting	Default: No .

Parameter	Description
Split File Name into Path and Name	Default: No .
Generate Unparsed Events	Default: No .
Preserve System Health Events	Yes, No , or Disabled.
Enable Device Status Monitoring (in minutes)	Disabled or 1, 2, 3, 4, 5, 10, 30, 60, or 120 minutes.
Filters	
Filter Out	NA
“Very High Severity” Event Definition	NA
“High Severity” Event Definition	NA
“Medium Severity” Event Definition	NA
“Low Severity” Event Definition	NA
“Unknown Severity” Event Definition	NA
Payload Sampling	(When available.)
Max. Length	Discard, 128 bytes, 256 bytes , 512 bytes, 1 kbyte
Mask Non-Printable Characters	Default: False .

Appendix C: Special Connector Configurations

Certain connectors require additional configuration when used with Arcsight Management Center. This appendix describes the additional configuration. For general information about installing connectors, see ["Adding a Connector" on page 141](#).

The following topics are discussed here:

Microsoft Windows Event Log - Unified Connectors

The SmartConnector for Microsoft Windows Event Log - Unified is not part of a FIPS-compliant solution. When you add a Windows Event Log - Unified connector, be sure the container is not FIPS-enabled in order for the connector to collect events.

When adding a Windows Event Log - Unified connector, follow the specific instructions in the SmartConnector configuration guide for entering parameters, entering security certifications when using SSL, enabling audit policies, and setting up standard user accounts.

There are currently two parser versions for the Microsoft Windows Event Log - Unified SmartConnector.

- Parser Version 0 is generally available with each SmartConnector release
- Parser Version 1 is available with the Microsoft Windows Monitoring content

The Microsoft Windows Event Log - Unified SmartConnector configured for you during initial configuration uses Parser Version 1.

Detailed Security Event mappings for this parser version can be found in Security Event Mappings: SmartConnectors for Microsoft Windows Event Log - Unified with Parser Version 1 (MSWindowsEventLogUnifiedMappingsParserVersion1.pdf), available on ArcSight [Protect724](#).

When you install additional Microsoft Windows Event Log Unified connectors, they are installed with the generally available base parser version (Parser Version 0). Mappings for the base parser version are available with each SmartConnector release (Security Event Mappings: SmartConnectors for Microsoft Windows Event Log) and can be found on [Protect724](#), along with the SmartConnector configuration guide. You must use Parser Version 1 if you want the default Windows Monitoring content to work. For details see the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified, or SmartConnector Configuration Guide for Microsoft Windows Security Events - Mappings.



Note: The pre-bundled SmartConnector for Microsoft Windows Event Log - Unified installed using the First Boot Wizard is installed with Parser Version 1. Any Windows Event Log - Unified connectors you add using the connector configuration wizard are installed with Parser Version 0 (the base parser).

Change Parser Version by Updating Container Properties

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

Multiple parser versions enables each SmartConnector parse raw events in many different ways to generate ArcSight security events with appropriate mappings. The SmartConnector for Microsoft Windows Event Log -- Unified, supports two parser versions: Base Parser and Parser Version 1.

With multiple parser versions:

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

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

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

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

To update container properties (located in the `agent.properties` file) to change the parser version being used when mapping events:

1. Click **Manage** from the top-level menu bar.
2. Select a navigation path.
3. Select the container whose properties you want to update. You can select multiple containers.
4. Click **Properties**.
5. Follow the instructions in the wizard to update connector properties.

The `fcp.version` parameter value 0 designates the base parser. To use parser 1, change

the `fcp.version` parameter value to 1. For example:

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

SSL Authentication

If you choose to use SSL as the connection protocol, you must add security certificates for both the Windows Domain Controller Service and for the Active Directory Server. Installing a valid certificate on a domain controller permits the LDAP service to listen for, and automatically accept, SSL connections for both LDAP and global catalog traffic. With the First Boot Wizard installation of the connector, the certificates are already imported for you. If you add Windows Event Log - Unified connectors, see the SmartConnector Configuration Guide for Microsoft Windows Event Log - Unified for instructions.

Database Connectors

The following database connectors are available for installation with ArcSight Express:

- IBM SiteProtector DB*
- McAfee ePolicy Orchestrator DB*
- McAfee Vulnerability Manager DB*
- McAfee Network Security Manager DB*
- Microsoft SQL Server Audit Multiple Instance DB*
- Oracle Audit DB
- Symantec Endpoint Protection DB*
- Trend Micro Control Manager NG DB*
- Snort DB*

*These connectors extract events from an SQL Server or MySQL databases, which requires a JDBC driver. See "[Add a JDBC Driver](#)" on the next page for instructions.

All of these database connectors require the following information when being added to ArcSight Express; some connectors require additional parameters, such as event types or polling frequency.

Parameter	Description
Database JDBC Driver	If you are using an ODBC DRIVER, select 'sun.jdbc.odbc.JdbcOdbcDriver' driver. For JDBC drivers, select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver.
Database URL	If you are using an ODBC DRIVER, enter: 'jdbc:odbc:<ODBC Data Source Name>', where the <ODBC Data Source Name> is the name of the ODBC data source you just created. If you are using a JDBC DRIVER, enter: 'jdbc:sqlserver://<MS SQL Server Host Name or IP Address>:1433;DatabaseName=<MS SQL Server Database Name>,' substituting actual values for <MS SQL Server Host Name or IP Address> and <MS SQL Server Database Name>.
Database User	Specify the login name of the database user with appropriate privilege.
Database Password	Specify the password for the SiteProtector Database User.

Add a JDBC Driver

The IBM SiteProtector DB, McAfee ePolicy Orchestrator DB, McAfee Vulnerability Manager DB, McAfee Network Security Manager DB, Microsoft SQL Server Audit Multiple Instance DB, Symantec Endpoint Protection DB, and Trend Micro Control Manager NG DB connectors extract events from a SQL Server database. For information about and to download the MS SQL Server JDBC Driver, see the Microsoft web site.



Note: Different versions of the JDBC driver are required for different SQL Server database versions; be sure to use the correct driver for your database version. The name of the jar file may be different for some JDBC driver versions.

The SmartConnector for Snort DB extracts events from a MySQL database.

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the appropriate container or containers, as follows:

1. From ArcSight Express, select **Setup > Repositories**.
2. Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
3. Click **Upload to Repository**.
4. From the **Repository File Creation Wizard**, select **Individual Files**, then click **Next**.
5. Retain the default selection and click **Next**.
6. Click **Upload** and locate and select the *.jar* file you downloaded.
7. Click **Submit** to add the specified file to the repository and click **Next** to continue.
8. After adding all files you require, click **Next**.
9. In the **Name** field, specify a descriptive name for the zip file (JDBCdriver, for example). Click **Next**.

10. Click **Done** to complete the process; the newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
11. To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.
12. Select the container or containers into which the driver is to be uploaded; click **Next**.
13. Click **Done** to complete the process.

Configuration guides for the database connectors supported with ArcSight Express can be found on the microfocus.com website. The individual configuration guides that provide setup information and mappings for the applications listed below can be found on Micro Focus Community:

- IBM SiteProtector DB
- McAfee ePolicy Orchestrator DB
- McAfee Vulnerability Manager DB (formerly FoundScan)
- McAfee Network Security Manager DB
- Microsoft SQL Server Multiple Instance Audit DB
- Oracle Audit DB
- Symantec Endpoint Protection DB
- Trend Micro Control Manager DB
- Snort DB

API Connectors

The following API connectors are available for installation with ArcSight Express. They require a client and authentication credentials, as well as configuring the events types to be sent to the connector by the device.

- Cisco Secure IPS SDEE
- Sourcefire Defense Center eStreamer

For Cisco Secure IPS SDEE, if you want the SmartConnector to validate the Cisco IPS sensor's authentication certificate, obtain the authentication certificate from the IPS sensor and import it to the appliance.

For Sourcefire Defense Center eStreamer, add an eStreamer client, create an authentication certificate, and select event types to be sent to the connector.

See the individual configuration guides for these connectors for instructions.

Follow the instructions in "Uploading Certificates to the Repository" in the Connector Management for ArcSight Express 4.0 User's Guide to import the trusted certificates to ArcSight Express.

Configuration guides for the API connectors supported with ArcSight Express can be found on the microfocus.com website, as well as the individual configuration guides that provide setup information and mappings for the applications listed below.

- Cisco Secure IPS SDEE
- Sourcefire Defense Center eStreamer

File Connectors

File-based connectors use the Network File System (NFS) or the Common Internet File System (CIFS).

The following File connector is available for installation with ArcSight Express:

- Blue Coat Proxy SG Multiple Server File

See the configuration guide for device setup, parameter configuration, and mappings information for the SmartConnector for Blue Coat Proxy SG Multiple Server File.

File-based connectors use the Network File System (NFS) or the Common Internet File System (CIFS). For the file-based connectors on a Windows system, configure a CIFS share before you add the connectors.

For information on creating a CIFS Mount or an NFS Mount, see "Managing a Remote File System" in the Connector Management for ArcSight Express 4.0 User's Guide.

Syslog Connectors

If you selected Syslog Daemon during initial installation with the First Boot Wizard, the Syslog Daemon connector has already been installed.

You can add a Syslog File, Pipe, or Daemon connector in a new container. Syslog connectors for the following devices are available with ArcSight Express:

- Cisco PIX/ASA Syslog
- Cisco IOS Router Syslog
- Juniper Network and Security Manager Syslog
- Juniper JUNOS Syslog
- UNIX OS Syslog

Be sure your device is set up to send syslog events. See your device documentation or the SmartConnector Configuration Guide for device configuration information; the guide also includes specific device mappings to ArcSight event fields as well as further information needed for configuration if you are installing the Pipe or File connectors. Mappings in the SmartConnector for UNIX OS Syslog configuration guide apply to all syslog connectors. Specific mappings per device are documented in the configuration guide for the device.

Configuration guides for these syslog connectors supported with ArcSight Express can be found on the microfocus.com website:

- Cisco PIX/ASA Syslog
- Cisco IOS Syslog
- Juniper JUNOS Syslog
- Juniper Network and Security Manager Syslog
- UNIX OS Syslog

Appendix D: Setting Up Your Arcsight Management Center Appliance

This appendix gives instructions on setting up your Arcsight Management Center Appliance for first use.

Preparation

Prior to first use of your Arcsight Management Center appliance, do each of the following:

1. Unpack the appliance and its accompanying accessories.
2. Read carefully through the instructions, cautions, and warnings packaged with the appliance. Failure to do so can result in bodily injury or appliance malfunction.
3. Note and save the rack-mounting instructions included in the package.
4. Redeem your Management Appliance license key. You will need this key to access Management Appliance functionality.
5. Follow the rack installation instructions (included in your Appliance package) to securely mount the appliance in its rack and make the back panel connections.
6. Do one of the following to enable local access to the Appliance:
 - Connect a keyboard, monitor, and mouse to the ports on the Appliance.
 - Connect a terminal to the serial port on the Appliance using a null modem cable with DB-9 connector. The serial port requires a standard VT100-compatible terminal: 9600 bps, 8-bits, no parity, 1 stop bit (8N1), no flow control.
7. Power on the appliance.
8. Optionally, enable your appliance for out-of-band remote access. Download, review, and follow the instructions in the ProLiant Integrated Lights-Out User Guide, available on the product's website.

You are now ready to begin appliance set up.

Setup

During appliance setup, do the following:

1. Configure a new IP address for the appliance at the CLI.
2. Accept the End User License Agreement, then log in to the appliance.
3. Initialize the Arcsight Management Center appliance.

Each of these steps is described in detail below.

Configure a New IP Address

Use the appliance's Command Line Interface (CLI) to configure a new IP address . Arcsight Management Center Appliance ships with the default IP address 192.168.35.35 (subnet mask 255.255.255.0) on Eth0. You will also need to specify a default gateway, hostname, and DNS and NTP servers.

You will need the following information on hand before beginning:

- The new IP address , plus prefix or subnet mask.
- Your default gateway address.
- Your fully-qualified domain name.
- One or more name search domains and server addresses for DNS resolution.
- One or more NTP server addresses.

To configure a new IP address on the CLI:

1. On the CLI, connect to the appliance using these default credentials:

Login:admin

Password:password

2. Specify the new IP address with one of the following commands:

- `set ip eth0 <ip>/<prefix>`, where `<ip>` is the new IP address and `<prefix>` is your prefix, OR,
 - `set ip eth0 <ip> <subnetmask>`, where `<ip>` the new IP address and `<subnetmask>` is your subnet mask .
3. Specify `set defaultgw <address>`, replacing `<address>` with your default gateway IP address .
 4. Specify `set hostname <FQDN>`, replacing `<FQDN>` with the fully-qualified domain name of the host.
 5. Specify `set dns <search_domain_1>, <search_domain_2>...<search_domain_N> <nameserver1> <nameserver2>...<nameserver_N>`, replacing each `<search_domain_N>` with a search domain, and each `<nameserver_N>` with the IP address of a nameserver you wish to use for DNS.
 6. Specify `set <ntp_server_1> <ntp_server_2>...<ntp_server_N>`, replacing each `<ntp_server_N>` with the IP address of an NTP server you wish to set appliance time.
 7. Specify `show config` and review your settings. If any are incorrect, correct them as described in earlier steps.

You are now ready to accept the End User License Agreement.

Accept the End User License Agreement

Upon first connecting to the appliance through a browser, you are prompted to accept the End User License Agreement (EULA).

To accept the EULA:

1. In a browser, connect to the Arcsight Management Center appliance at <https://<IP>>, where <IP> is the new IP address you just configured.
2. Review the license.
3. Select the **I accept the terms of the License Agreement** check box, then click **Accept**.
4. Log in as an administrator using the default credentials.

Login:admin

Password:password

You may now initialize the appliance.

Initialize the Arcsight Management Center Appliance

You can now initialize the appliance by uploading the license file; optionally, setting date and time settings; and then changing the admin login credentials to non-default values.

To initialize the appliance:

1. On the **Arcsight Management Center Appliance Configuration** page, in the **License** field, browse for and upload your current license.
2. Click **Save**.
3. Set your date and time settings for the appliance.
4. Change the admin login credentials from their default values. For instructions, see "["Change Password" on page 314](#).

Your Arcsight Management Center appliance is now ready for use.

Appendix E: Restoring Factory Settings

You can restore an Arcsight Management Center to its factory settings using a built-in utility on the appliance. Restoration applies to new model Arcsight Management Centers as well as former Connector Appliances that have been migrated to Arcsight Management Center.

Restoring an ArcSight Management Center Appliance to factory settings irretrievably deletes all configuration settings. You should back up your configuration settings before performing a factory restore.

The utility used for the factory restore (and resulting appliance image) depends on the type of appliance being restored. Consult the table below to determine the utility to employ.

Appliance Model	System Restore Utility	Resulting Appliance Image
C6600 and C6700	System Restore	ArcSight Management Center
Any CX500 (including C6500)	System Restore	ArcSight Management Center
CX400 (running RHEL 5.x pre-Migration)	System Restore	ArcSight Management Center
CX400 (running RHEL 6.x pre-Migration)	Acronis True Image	Connector Appliance

Factory Restore Using System Restore

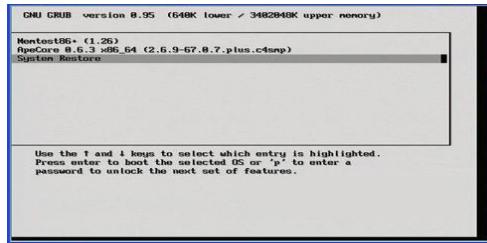
An appliance restored using System Restore will be restored to an ArcSight Management Center image.

To perform a factory restore using System Restore:

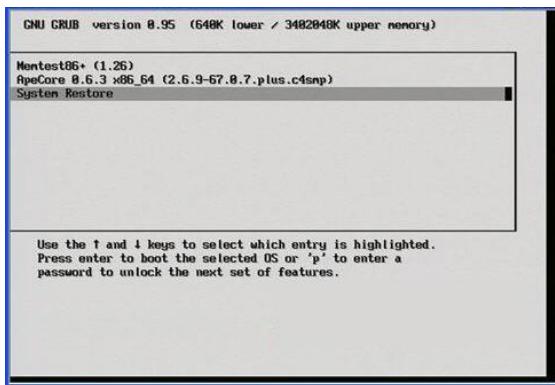
1. Note the IP address , default gateway, and netmask of the appliance.
2. Attach a keyboard, monitor, and mouse directly to the appliance.
3. Reboot Arcsight Management Center from the GUI. Click **Setup > System Admin > Reboot** and then click the **Start Reboot Now** button. You can also reboot using the command line interface.
4. When the following screen displays, press any key on your keyboard.



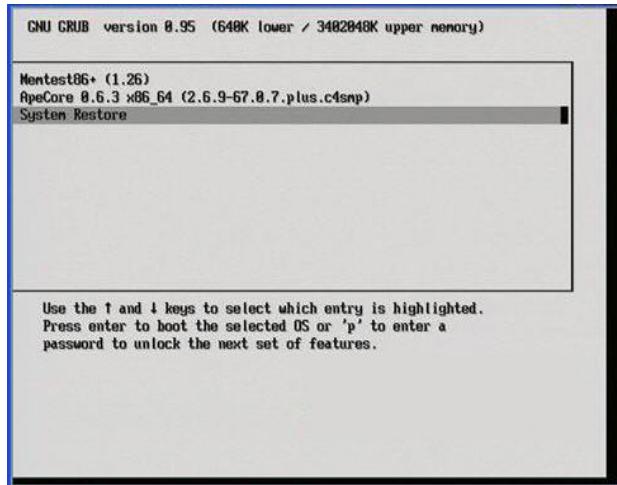
Note: This screen is displayed for a very short time. Make sure you press a key on your keyboard quickly; otherwise, the appliance continues to boot normally.



5. A screen similar to the one shown below appears on the attached monitor. Use the mouse or arrow keys to select **System Restore** and press **Enter**. The System Restore utility launches.



6. Press the **F1 (Auto-Select)** key.



7. Press the **F2** key to **Restore** the appliance.
8. When prompted **Proceed with restore?**, press **y**. The restore begins.
9. Allow the restore utility to complete the process.
10. When complete, press **Enter**.
11. Press the **F12** key to reboot the appliance.
12. When prompted **Reboot appliance?**, press **y**. The appliance will be rebooted.

The result of the restore process is a factory restored Arcsight Management Center.

For use, the appliance must now be configured with an IP address , default gateway, and netmask you noted previously.

Troubleshooting a G10 (C6700) ARI System Restore: IP Address

After performing a system restore using a G10 (C6700) appliance with an ARI image, and the IP address isn't automatically assigned, you need to access iLO in order to enable the network interface controller (NIC) and the SNMP service.

1. Identify the NIC with the flag UP: `ip a`
2. Run `ifdown <nic-name>` then `ifup <nic-name>` (eg: `eno1`, `ensf0`). Use the nic-name obtained in step 1.
3. To verify that the IP address has been assigned, check the NIC again: `ip a`
4. Access `/opt/local/monit/bin` and run `./monit summary` to confirm that the SNMP service is running.

Factory Restore Using Acronis True Image

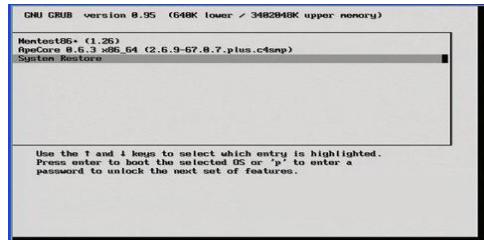
An appliance restored using Acronis True Image will be restored to a Connector Appliance image.

To perform a factory restore using Acronis True Image:

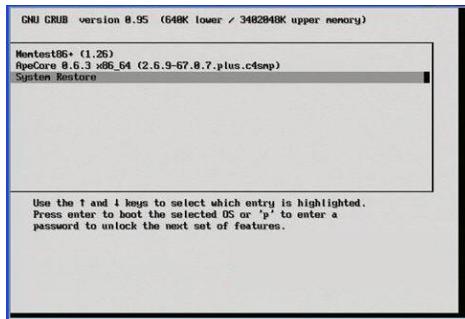
1. Note the IP address , default gateway, and netmask of the appliance.
2. Attach a keyboard, monitor, and mouse directly to the appliance.
3. Reboot Arcsight Management Center from the GUI. Click **Setup > System Admin > Reboot** and then click the **Start Reboot Now** button. You can also reboot using the command line interface.
4. When the following screen displays, press any key on your keyboard.



Note: This screen is displayed for a very short time. Make sure you press a key on your keyboard quickly; otherwise, the appliance continues to boot normally.



5. A screen similar to the one shown below appears on the attached monitor. Use the mouse or arrow keys to select **System Restore** and press **Enter**.



6. Click **Acronis True Image Server** to continue.
7. In the **Acronis True Image Echo Server** dialog box, select **Recovery** from the **Pick a Task** list and press **Enter**.
8. When the Restore Data Wizard starts, click **Next** to continue.
9. On the **Backup Archive Selection** page, select **Acronis Secure Zone** and click **Next**.
10. On the **Restoration Type Selection** page, select **Restore disks or partitions** and click **Next**.
11. On the **Partition or Disk to Restore** page, select the entire drive, labeled **cciss/c0d0** or **sda** (depending on the appliance model) and click **Next**.
12. On the **NT Signature selection for image restoration** page, select how you want the NT signature for the restored disk to be processed and click **Next**.
13. On the **Restored Hard disk Location** page, select the drive to restore (**cciss/c0d0** or **sda**) and click **Next**.
14. On the **Non-empty Destination Hard Disk Drive** page, select **Yes, I want to delete all partitions on the destination hard disk drive before restoring** and click **Next**.
15. On the **Next Selection** page, select **No, I do not** and click **Next** (there are no other partitions or disks to restore).
16. On the **Restoration Options** page, select **Validate backup archive for the data restoration process** if you want to validate the archive before resetting the appliance. Select **Reboot the computer automatically after the restoration is finished** if you want to reboot the appliance automatically. Click **Next**.
17. Review the checklist of operations to be performed and click **Proceed** to begin factory reset. Click **Back** to revisit previous pages.



Caution: Do not interrupt or power down the Arcsight Management Center during the reset process. Interrupting the reset process can force the system into a state from which it cannot recover.

Progress bars show the status of the current operation and the total progress.

18. When you see a message indicating that the data was restored successfully, click **OK**.
19. If you specified automatic reboot previously, the appliance reboots when the reset is complete. Otherwise, reboot manually.

The result of the restore process is a factory restored Connector Appliance.

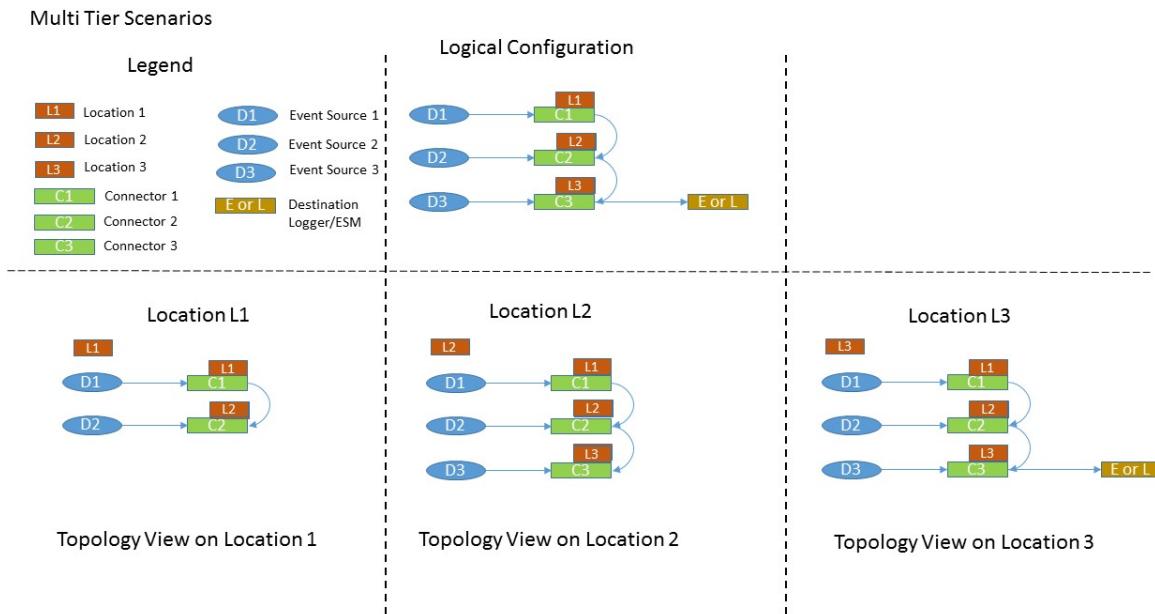
For use, the appliance must now be configured with an IP address , default gateway, and netmask you noted previously. For configuration instructions, see the document Getting Started with Connector Appliance, available from the Micro Focus Community.

Appendix F: The Topology View and Unmanaged Devices

This section details various scenarios for the inclusion of devices not managed by ArcMC in your network, and the effect of each scenario on the ArcMC Topology View. Particularly when connectors (or Collectors) are chained together in a multi-tier configuration, unmanaged products can block the view from their immediate downstream neighbor.

Scenario 1: No Unmanaged Devices

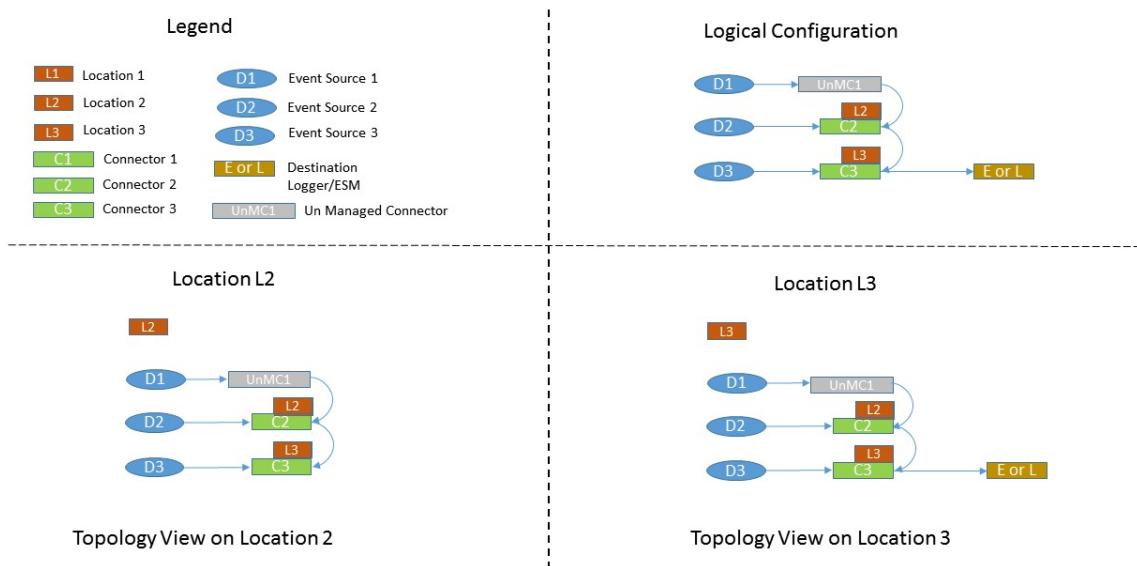
In this scenario, no unmanaged products are included in the network. As a result, the ArcMC Topology view is unimpeded and gives an accurate picture of the logical topology as viewed from any location.



Scenario 2: Unmanaged Connector in Location L1

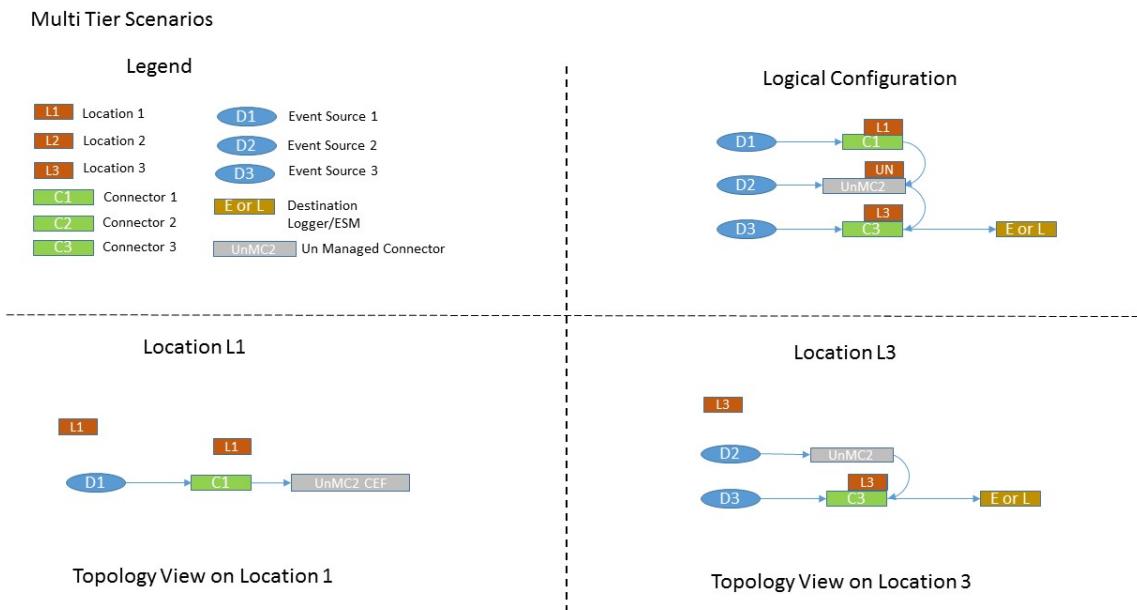
This scenario shows an unmanaged connector in location L1 and the results on the Topology View as seen from locations L2 and L3. No view is seen from L1, since it does not include any managed nodes. The view at the other downstream locations is as expected.

Multi Tier Scenarios



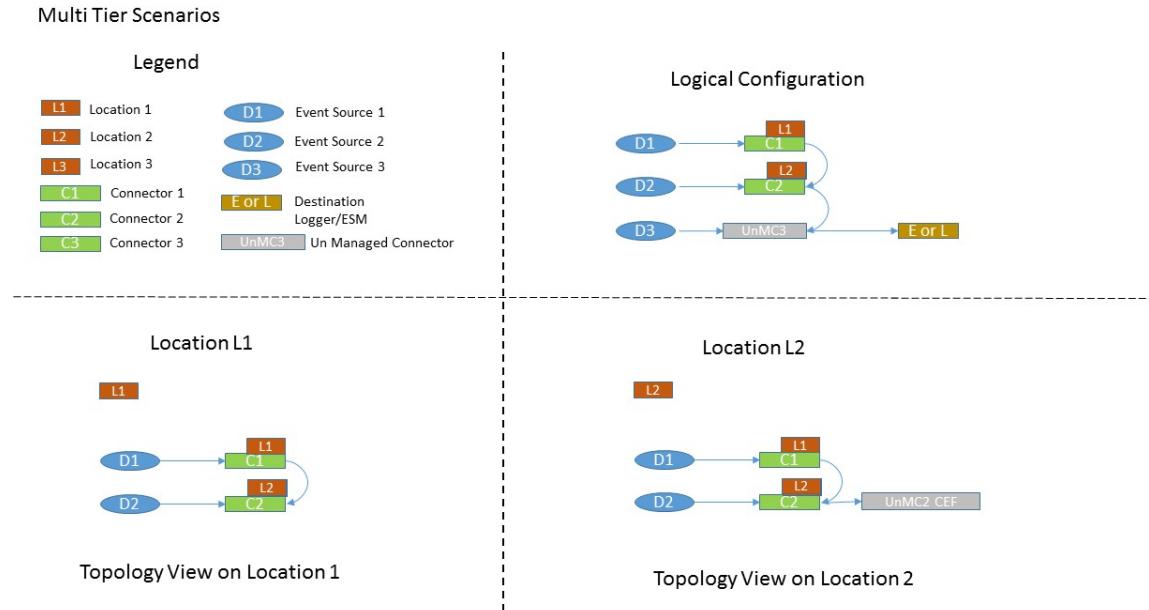
Scenario 3: Unmanaged Connector in Location L2

In this scenario, an unmanaged connector is located in Location L2 and chained to connectors in locations L1 and L2. This blocks the Topology view of L1 as seen from L3. In addition, the destination Logger or ESM shows no traffic from L1.



Scenario 4: Unmanaged Connector in Location L3

In this scenario, an unmanaged connector is in Location L3. This impedes an accurate Topology view of location 3. In fact, no traffic from locations L1 and L2 is shown for the destination Logger/ESM.



To get the most complete and accurate topological view, you are strongly encouraged to use ArcMC to manage all supported connectors (or Collectors) included in your logical topology.

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 ArcSight Management Center Administrator's Guide

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.

We appreciate your feedback!



OpenText

ArcSight ArcMC

Software Version: 24.2 (3.2.4)

Release Notes

Document Release Date: June 2024

Software Release Date: June 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2013-2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

About ArcSight Management Center	4
What's New in this Release	4
Technical Requirements	5
For ArcSight Management Center	5
For Managed ArcSight Products	6
Installer Files	6
Prerequisite for ArcMC Installation or Upgrade on RHEL 7.x	7
Upgrading ArcMC	8
Collectors and Connectors in Transformation Hub	9
Known Limitations	9
Closed Issues	9
Known Issues	10
Publication Status	11
Send Documentation Feedback	12

About ArcSight Management Center

ArcSight Management Center (ArcMC), part of the ArcSight Platform, is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring in an efficient and cost-effective way.

ArcMC offers these key capabilities:

- **Management and Monitoring:** A single management interface to administer and monitor ArcSight managed nodes, such as: Transformation Hub, Loggers, Collectors, Connectors, Connector Appliances, and other ArcMC instances.
- **Connector Deployment:** Remotely deploy and manage connectors across your network.
- **SmartConnector Hosting:** For the hardware appliance, ArcMC hosts SmartConnectors.

ArcMC includes these benefits:

- Rapid implementation of new and updated security policies.
- Increased level of accuracy and reduction of errors in configuration of managed nodes.
- Improves operational capabilities and lower total cost of ownership.

What's New in this Release

This release of ArcMC is a maintenance release and includes no new features. Supported third-party components have been updated, including: JRE 8u402, Apache Tomcat 9.0.86 and Postgres DB Server 15.6.

Product version number has been renumbered to CE 24.2, to reflect its inclusion in the ArcSight Platform CE 24.2 release. The technical version number of this release is 3.2.4.

More Information

For detailed information about ArcMC features and functionality, refer to the ArcMC Administrator's Guide, and other documentation, available from the [ArcSight Product Documentation Site](#).

Technical Requirements

For ArcSight Management Center

Server	For software form factor: <ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL) 9.2, 8.8, 7.9.• Rocky Linux 9.2. 8.8 (supported)• Additionally, for RHEL7.x installation of software ArcMC: See ""Prerequisite for ArcMC Installation or Upgrade on RHEL 7.x" on page 7.• CentOS 7.9. For appliance upgrade: Red Hat Enterprise Linux 7.9.
Client System	<ul style="list-style-type: none">• Windows 7, 8, 10• RHEL 7.8, 7.9, 8.1, 8.2, 8.3, 8.4.
CPU	1 or 2 Intel Xeon Quad Core (or equivalent)
Memory	<ul style="list-style-type: none">• 16 GB RAM• 80 GB Disk Space (for software form factor)
Supported Client Browsers	<ul style="list-style-type: none">• Microsoft Edge (latest version as of release date)• Firefox ESR (latest version as of release date)• Google Chrome (latest version as of release date)
Screen Resolution	Optimal screen resolution is 1920x1200
Hardware Models	For upgraded deployments, model C670X running RHEL 7.9.

For Managed ArcSight Products

Managed Node	Form Factor	Supported Product Versions	Certified Product Versions	Appliance Model
ArcMC	Software and Appliance	3.1.3	3.2.4	C6700
		3.1.2	3.2.3	
		3.1.1	3.2.2	
		3.1.0	3.2.1	
		3.2.0		
SmartConnector	Software	8.4.1	8.4.3	
		8.4.0		
		8.3.0		
Logger	Software and Appliance	7.2.2	7.3.0	L7700
		7.2.1		
Transformation Hub	Software	3.7.0	3.7.3	
		3.6.0		
ESM	Software	7.6.0	7.6.4	
		7.5.0		

Installer Files

Micro Focus provides a digital public key for you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party. Visit the following site for information and instructions:

<https://entitlement.mfgs.microfocus.com/ecommerce/eulfillment/digitalSignIn.do>

The installation package is available for download from the [OpenText entitlements portal](#). The installer files for ArcSight Management Center 24.2 (3.2.4) are named as follows:

- **For ArcMC:** ArcSight-ArcMC-3.2.4.Build Number.0.bin
- **Software installer for use remotely with ArcMC Node Management:** arcmc-sw-Build Number-remote.enc
- **For ArcMC Appliance (Upgrade Only):** arcmc-Build Number.enc
- **ArcMC Agent Installer:** The ArcMC Agent installer for all appliance nodes, and all types of software nodes, is bundled with the ArcMC installer file. You can remotely

install or upgrade the ArcMC Agent on a managed node directly from ArcMC, as follows:

- You can install the ArcMC Agent when you are adding the nodes through Node Management (**Add Host** section). For more information, see to **Chapter 2: Software Installation / Installing the ArcSight Management Center Agent** in the ArcMC Administrator's Guide. For information about upgrading the Agent on managed nodes check **Chapter 5: Managing Nodes / Updating (or Installing) the ArcMC Agent**.
- You can install or upgrade the ArcMC Agent remotely from a managing ArcMC server on all managed appliance nodes (Logger Appliance and ArcMC Appliance).
- You can install or upgrade the ArcMC Agent for remotely managed software nodes which are ArcMC v2.2 and Logger v7.0 or later.

Note: The ArcMC Agent cannot be upgraded or installed remotely on earlier versions of ArcMC and Logger, nor for any Connector Appliance-managed node. For these node types, you must use the manual installer named ArcSight - ArcMCAgent-3.2.0.Build Number.0.bin.

Prerequisite for ArcMC Installation or Upgrade on RHEL 7.x

Before installing or upgrading ArcMC on Red Hat Enterprise Linux (RHEL) 7.x, you must modify the inter-process communication (IPC) setting of the `logind.conf` file.

To modify the `logind.conf` file for RHEL 7.x:

1. Navigate to the `/etc/systemd` directory, and open the `logind.conf` file for editing.
2. Find the `RemoveIPC` line. `RemoveIPC` should be active and set to *no*. (Remove the `#` sign if it is there, and change the yes to no if necessary. The correct entry is: `RemoveIPC=no`).
3. Save the file.
4. From the `/etc/systemd` directory, enter the following command to restart the `systemd-logind` service and put the change into effect: `systemctl restart systemd-logind.service`

After you have modified this setting and met all installation requirements, you are ready to install ArcMC.

Upgrading ArcMC

Upgrade is supported from ArcSight Management Center all versions of 3.2.x to version 24.2 (3.2.4). You should also upgrade any managed ArcMC nodes to version 24.2 (3.2.4).

Before upgrading to ArcMC 3.2.4, ensure that you have upgraded the operating system on your appliance or host to a supported version. For more information about OS support, see "["Technical Requirements" on page 5](#)". For instructions on upgrading an appliance either remotely or locally, see Upgrading ArcMC in the ArcMC Administrator's Guide.

The following instructions are for upgrading software ArcMC using a wizard in GUI mode. You can also upgrade your ArcMC from the command line in console mode, and in silent mode. For more information, see the Installation chapter of the ArcMC Administrator's Guide.

If the target ArcMC node is managed by another ArcMC appliance, you can also perform an upgrade using the Node Management upgrade feature.

OpenText recommends that you perform a backup of your current ArcSight Management Center configuration before upgrading to ArcMC24.2 (3.2.4): For more information, see the **Managing Backups and Restores** section in the ArcMC Administrator's Guide.

To download and verify the signature of your downloaded files:

1. Log in to the host where you want to begin the installation process.
2. Change to the directory where you want to download the installer files.
3. Download all the necessary product installer files from the OpenText Downloads website along with their associated signature files (*.sig).

Evolving security needs imply the renewal of certificates for the signature verification procedure. To ensure a successful verification of your product signature, download the latest public keys file before proceeding with the verification process (step 1 of the Get the Public Keys procedure).

OpenText provides a digital public key that is used to verify that the software you downloaded from the OpenText software entitlement site is indeed from OpenText and has not been tampered with by a third party. For instructions on how to obtain the latest public keys file and how to verify the signature, see:

<https://support.microfocus.com/kb/doc.php?id=7025140>

If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please contact OpenText Customer Support.

4. Begin the installation.

Upgrading the ArcMC Agent

You should also upgrade the ArcMC Agent on all managed nodes that require the Agent for communication with ArcMC. For instructions on upgrading the ArcMC Agent on managed nodes, see the ArcMC Administrator's Guide.

Collectors and Connectors in Transformation Hub

As announced in the 23.1 release, the Collectors feature and the Connectors in Transformation Hub (CTH) feature have been deprecated, and from the ArcSight Platform 24.2 release on, only existing collectors and CTH deployments are supported. You can continue managing your collectors and CTHs in the platform, but you cannot create any new ones.

Known Limitations

ArcMC is known to have the following limitations.

Issue	Description
242313	The Host Status Exceptions page is not displaying the Transformation Hub rules. Workaround: None available at this time.
237161	If there are connectors installed in the path /opt/arcshift/connector*/ ArcMC upgrade fails.

Closed Issues

The following issues were resolved in this release.

Issue	Description

Known Issues

This release contains the following open issues. To address the issue, use the workaround, if any is indicated.

Key	Description
873115	<p>If the upgrade to RHEL 8.8 is interrupted or not completed, then the recovery process using the script opt/arcsight/current/arcsight/arcmc/bin/scripts/sw_restore.sh will fail.</p> <p>Workaround: Open the script sw_restore.sh in a text editor and change line 100 of the script as follows.</p> <pre>Replace /bin/tar -xzvf \$backupFile --preserve --same-owner -P >> \$backupLog2>&1 with /bin/tar -xzvf \$backupFile -p -s --same-owner -P >> \$backupLog2>&1</pre> <p>Save the script in the text editor, and then re-run it.</p>
698065	In some circumstances on Azure, there may be intermittent login and backend errors between Fusion, ArcMC and Kafka Manager.
648050	Historically, ArcMC users could create Transformation Hub routing rules that test a string field's value against text entered by a user. For example, "agent == abc". To prevent browser problems, ArcMC was changed in a previous release to reject some non-alphanumeric characters when defining field value tests in a routing rule. Existing rules that used those characters still work, but new field value tests cannot use those characters. New field tests can only use alphanumeric characters and the five following five characters: underscore (_), hyphen (-), colon (:), space (), and period (.).
590160	<p>When a new repository is created whose name ends with the suffix <code>_config</code> or is named <code>config_edit</code>, an HTTP 500 error will result.</p> <p>Workaround Do not create any repositories with the <code>_config</code> suffix or <code>config_edit</code> in the name.</p>
425040	When in Deployment/Topology view, the IP address of a Logger or ESM destination for Transformation Hub shows as an unknown IP.
387040	In some cases, after performing a search in the online help file, the file may become frozen and necessitate a restart of the browser.
363022	<p>For G10 Appliances with a 10G NIC, after a restore, the gateway is not correctly configured.</p> <p>Workaround: From the CLI, modify the IP address and gateway with the correct information. For reference, consult the ArcMC Admin Guide, section: "Configure a New IP Address".</p>

Key	Description
363017	<p>For G10 Appliances with a 10G NIC, after a restore, the IP address is not correctly configured.</p> <p>Workaround: From the CLI, modify the IP address with the correct information. For reference, consult the ArcMC Admin Guide, section: "Configure a New IP Address".</p>
359190	<p>On G10 appliances, ArcMC does not validate when the user enters invalid IP values when trying to modify the "IP Address" or the "Subnet Mask" field from a network interface (or also called NIC port).</p>
243608	<p>After a product type ages out (Device Age-Out) there is no way for the user to get that product type back. If Device Tracking is disabled for a device product and the device ages out, then there is no way to revert to enable tracking for that device product.</p>

Publication Status

Released: January 2024

Last Updated: Tuesday, June 4, 2024

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 Release Notes (ArcMC 24.2 (3.2.4))

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.

We appreciate your feedback!



OpenText

ArcSight ArcMC

Software Version: 24.3 CE (3.2.5)

Release Notes

Document Release Date: October 2024

Software Release Date: October 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2013-2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

About ArcSight Management Center	4
What's New in this Release	4
Technical Requirements	5
For ArcSight Management Center	5
For Managed ArcSight Products	6
Installer Files	6
Prerequisite for ArcMC Installation or Upgrade on RHEL 7.x	7
Upgrading ArcMC	8
Collectors and Connectors in Transformation Hub	9
Known Limitations	9
Closed Issues	9
Known Issues	10
Publication Status	11
Send Documentation Feedback	12

About ArcSight Management Center

ArcSight Management Center (ArcMC), part of the ArcSight Platform, is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring in an efficient and cost-effective way.

ArcMC offers these key capabilities:

- **Management and Monitoring:** A single management interface to administer and monitor ArcSight managed nodes, such as: Transformation Hub, Loggers, Collectors, Connectors, Connector Appliances, and other ArcMC instances.
- **Connector Deployment:** Remotely deploy and manage connectors across your network.
- **SmartConnector Hosting:** For the hardware appliance, ArcMC hosts SmartConnectors.

ArcMC includes these benefits:

- Rapid implementation of new and updated security policies.
- Increased level of accuracy and reduction of errors in configuration of managed nodes.
- Improves operational capabilities and lower total cost of ownership.

What's New in this Release

This release of ArcMC includes updates to the following third-party components: Spring Framework, JRE, Apache HTTP server, and Tomcat.

Product version number has been renumbered to CE 24.3. The technical version number of this release is 3.2.5.

More Information

For detailed information about ArcMC features and functionality, refer to the ArcMC Administrator's Guide, and other documentation, available from the [ArcSight Product Documentation Site](#).

Technical Requirements

For ArcSight Management Center

Server	For software form factor: <ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL) 9.2, 8.8, 7.9.• Rocky Linux 9.2. 8.8 (supported)• Additionally, for RHEL7.x installation of software ArcMC: See ""Prerequisite for ArcMC Installation or Upgrade on RHEL 7.x" on page 7.• CentOS 7.9. For appliance upgrade: Red Hat Enterprise Linux 7.9.
Client System	<ul style="list-style-type: none">• Windows 7, 8, 10• RHEL 7.8, 7.9, 8.1, 8.2, 8.3, 8.4.
CPU	1 or 2 Intel Xeon Quad Core (or equivalent)
Memory	<ul style="list-style-type: none">• 16 GB RAM• 80 GB Disk Space (for software form factor)
Supported Client Browsers	<ul style="list-style-type: none">• Microsoft Edge (latest version as of release date)• Firefox ESR (latest version as of release date)• Google Chrome (latest version as of release date)
Screen Resolution	Optimal screen resolution is 1920x1200
Hardware Models	For upgraded deployments, model C670X running RHEL 7.9.

For Managed ArcSight Products

Managed Node	Form Factor	Supported Product Versions	Certified Product Versions	Appliance Model
ArcMC	Software and Appliance	3.1.3	3.2.5	C6700
		3.1.2	3.2.4	
		3.1.1	3.2.3	
		3.1.0	3.2.2	
			3.2.1	
			3.2.0	
SmartConnector	Software	8.4.1	8.4.3	
		8.4.0		
		8.3.0		
Logger	Software and Appliance	7.2.2	7.3.0	L7700
		7.2.1		
Transformation Hub	Software	3.7.0	3.7.3	
		3.6.0		
ESM	Software	7.6.0	7.6.4	
		7.5.0		

Installer Files

Micro Focus provides a digital public key for you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party. Visit the following site for information and instructions:
<https://entitlement.mfgs.microfocus.com/ecommerce/eulfillment/digitalSignIn.do>

The installation package is available for download from the [OpenText entitlements portal](#). The installer files for ArcSight Management Center 24.3 CE (3.2.5) are named as follows:

- **For ArcMC:** ArcSight-ArcMC-3.2.5.<Build Number>.0.bin
- **Software installer for use remotely with ArcMC Node Management:** arcmc-sw-<Build Number>-remote.enc
- **For ArcMC Appliance (Upgrade Only):** arcmc-<Build Number>.enc

- **ArcMC Agent Installer:** The ArcMC Agent installer for all appliance nodes, and all types of software nodes, is bundled with the ArcMC installer file. You can remotely install or upgrade the ArcMC Agent on a managed node directly from ArcMC, as follows:
 - You can install the ArcMC Agent when you are adding the nodes through Node Management (**Add Host** section). For more information, see to **Chapter 2: Software Installation / Installing the ArcSight Management Center Agent** in the ArcMC Administrator's Guide. For information about upgrading the Agent on managed nodes check **Chapter 5: Managing Nodes / Updating (or Installing) the ArcMC Agent**.
 - You can install or upgrade the ArcMC Agent remotely from a managing ArcMC server on all managed appliance nodes (Logger Appliance and ArcMC Appliance).
 - You can install or upgrade the ArcMC Agent for remotely managed software nodes which are ArcMC v2.2 and Logger v7.0 or later.

Note: The ArcMC Agent cannot be upgraded or installed remotely on earlier versions of ArcMC and Logger, nor for any Connector Appliance-managed node. For these node types, you must use the manual installer named ArcSight - ArcMCAgent-3.2.0.<Build Number>.0.bin.

Prerequisite for ArcMC Installation or Upgrade on RHEL 7.x

Before installing or upgrading ArcMC on Red Hat Enterprise Linux (RHEL) 7.x, you must modify the inter-process communication (IPC) setting of the `logind.conf` file.

To modify the `logind.conf` file for RHEL 7.x:

1. Navigate to the `/etc/systemd` directory, and open the `logind.conf` file in a text editor.
2. Find the `RemoveIPC` line. Change the line to `RemoveIPC=no` (Remove the `#` sign if present.)
3. Save the file.
4. From the `/etc/systemd` directory, enter the following command to restart the `systemd-logind` service and put the change into effect:
`systemctl restart systemd-logind.service`

After you have modified this setting and met all installation requirements, you are ready to install ArcMC.

Upgrading ArcMC

Upgrade is supported from ArcSight Management Center all versions of 3.2.x to version 24.3 CE (3.2.5). You should also upgrade any managed ArcMC nodes to version 24.3 CE (3.2.5).

Before upgrading to ArcMC 3.2.5, ensure that you have upgraded the operating system on your appliance or host to a supported version. For more information about OS support, see "[Technical Requirements](#)" on page 5. For instructions on upgrading an appliance either remotely or locally, see Upgrading ArcMC in the ArcMC Administrator's Guide.

The following instructions are for upgrading software ArcMC using a wizard in GUI mode. You can also upgrade your ArcMC from the command line in console mode, and in silent mode. For more information, see the Installation chapter of the ArcMC Administrator's Guide.

If the target ArcMC node is managed by another ArcMC appliance, you can also perform an upgrade using the Node Management upgrade feature.

OpenText recommends that you perform a backup of your current ArcSight Management Center configuration before upgrading to ArcMC24.3 CE (3.2.5): For more information, see the **Managing Backups and Restores** section in the ArcMC Administrator's Guide.

To download and verify the signature of your downloaded files:

1. Log in to the host where you want to begin the installation process.
2. Change to the directory where you want to download the installer files.
3. Download all the necessary product installer files from the OpenText Downloads website along with their associated signature files (*.sig).

Evolving security needs imply the renewal of certificates for the signature verification procedure. To ensure a successful verification of your product signature, download the latest public keys file before proceeding with the verification process (step 1 of the Get the Public Keys procedure).

OpenText provides a digital public key that is used to verify that the software you downloaded from the OpenText software entitlement site is indeed from OpenText and has not been tampered with by a third party. For instructions on how to obtain the latest public keys file and how to verify the signature, see:

<https://support.microfocus.com/kb/doc.php?id=7025140>

If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please contact OpenText Customer Support.

4. Begin the installation.

Upgrading the ArcMC Agent

You should also upgrade the ArcMC Agent on all managed nodes that require the Agent for communication with ArcMC. For instructions on upgrading the ArcMC Agent on managed nodes, see the ArcMC Administrator's Guide.

Collectors and Connectors in Transformation Hub

As announced in the 23.1 release, the Collectors feature and the Connectors in Transformation Hub (CTH) feature have been deprecated, and from the ArcSight Platform 24.2 release on, only existing collectors and CTH deployments are supported. You can continue managing your collectors and CTHs in the platform, but you cannot create any new ones.

Known Limitations

ArcMC is known to have the following limitations.

Issue	Description
242313	The Host Status Exceptions page is not displaying the Transformation Hub rules. Workaround: None available at this time.
237161	If there are connectors installed in the path /opt/arcshift/connector*/ ArcMC upgrade fails.

Closed Issues

No previously tracked issues were resolved in this release.

Known Issues

This release contains the following open issues. To address the issue, use the workaround, if any is indicated.

Key	Description
873115	<p>If the upgrade to RHEL 8.8 is interrupted or not completed, then the recovery process using the script opt/arcsight/current/arcsight/arcmc/bin/scripts/sw_restore.sh will fail.</p> <p>Workaround: Open the script sw_restore.sh in a text editor and change line 100 of the script as follows.</p> <pre>Replace /bin/tar -xzvf \$backupFile --preserve --same-owner -P >> \$backupLog2>&1 with /bin/tar -xzvf \$backupFile -p -s --same-owner -P >> \$backupLog2>&1</pre> <p>Save the script in the text editor, and then re-run it.</p>
698065	In some circumstances on Azure, there may be intermittent login and backend errors between Fusion, ArcMC and Kafka Manager.
648050	Historically, ArcMC users could create Transformation Hub routing rules that test a string field's value against text entered by a user. For example, "agent == abc". To prevent browser problems, ArcMC was changed in a previous release to reject some non-alphanumeric characters when defining field value tests in a routing rule. Existing rules that used those characters still work, but new field value tests cannot use those characters. New field tests can only use alphanumeric characters and the five following five characters: underscore (_), hyphen (-), colon (:), space (), and period (.).
590160	<p>When a new repository is created whose name ends with the suffix <code>_config</code> or is named <code>config_edit</code>, an HTTP 500 error will result.</p> <p>Workaround Do not create any repositories with the <code>_config</code> suffix or <code>config_edit</code> in the name.</p>
425040	When in Deployment/Topology view, the IP address of a Logger or ESM destination for Transformation Hub shows as an unknown IP.
387040	In some cases, after performing a search in the online help file, the file may become frozen and necessitate a restart of the browser.
363022	<p>For G10 Appliances with a 10G NIC, after a restore, the gateway is not correctly configured.</p> <p>Workaround: From the CLI, modify the IP address and gateway with the correct information. For reference, consult the ArcMC Admin Guide, section: "Configure a New IP Address".</p>

Key	Description
363017	<p>For G10 Appliances with a 10G NIC, after a restore, the IP address is not correctly configured.</p> <p>Workaround: From the CLI, modify the IP address with the correct information. For reference, consult the ArcMC Admin Guide, section: "Configure a New IP Address".</p>
359190	<p>On G10 appliances, ArcMC does not validate when the user enters invalid IP values when trying to modify the "IP Address" or the "Subnet Mask" field from a network interface (or also called NIC port).</p>
243608	<p>After a product type ages out (Device Age-Out) there is no way for the user to get that product type back. If Device Tracking is disabled for a device product and the device ages out, then there is no way to revert to enable tracking for that device product.</p>

Publication Status

Released: October 2024

Last Updated: Friday, October 11, 2024

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 Release Notes (ArcMC 24.3 CE (3.2.5))

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.

We appreciate your feedback!



OpenText

ArcSight ArcMC

Software Version: 24.1 (3.2.3)

Release Notes

Document Release Date: January 2024

Software Release Date: January 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2013-2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

About ArcSight Management Center	4
What's New in this Release	4
Technical Requirements	5
For ArcSight Management Center	5
For Managed ArcSight Products	6
Installer Files	7
Prerequisite for ArcMC Installation or Upgrade on RHEL 7.x	8
Upgrading ArcMC	9
Known Limitations	10
Closed Issues	10
Known Issues	11
Publication Status	11
Send Documentation Feedback	12

About ArcSight Management Center

ArcSight Management Center (ArcMC), part of the ArcSight Platform, is a centralized management tool that simplifies security policy configuration, deployment maintenance, and monitoring in an efficient and cost-effective way.

ArcMC offers these key capabilities:

- **Management and Monitoring:** A single management interface to administer and monitor ArcSight managed nodes, such as: Transformation Hub, Loggers, Collectors, Connectors, Connector Appliances, and other ArcMC instances.
- **Connector Deployment:** Remotely deploy and manage connectors across your network.
- **SmartConnector Hosting:** For the hardware appliance, ArcMC hosts SmartConnectors.

ArcMC includes these benefits:

- Rapid implementation of new and updated security policies.
- Increased level of accuracy and reduction of errors in configuration of managed nodes.
- Improves operational capabilities and lower total cost of ownership.

What's New in this Release

This version of ArcMC includes the following improvement:

- ArcMC now has two methods for enabling email notifications: both through modification of the logger.properties file and through using a CSV file.
- Product version number has been renumbered to CE 24.1, to reflect its inclusion in the ArcSight Platform CE 24.1 release. The technical version number of this release is 3.2.3.

More Information

For detailed information about ArcMC features and functionality, refer to the ArcMC Administrator's Guide, and other documentation, available from the [ArcSight Product Documentation Site](#).

Technical Requirements

For ArcSight Management Center

Server	For software form factor: <ul style="list-style-type: none">• Red Hat Enterprise Linux (RHEL) 8.6, 8.4, 7.9.• Rocky Linux 8.6 (supported)• Additionally, for RHEL7.x installation of software ArcMC: See ""Prerequisite for ArcMC Installation or Upgrade on RHEL 7.x" on page 8.• CentOS 7.9. For appliance upgrade: Red Hat Enterprise Linux 7.9.
Client System	<ul style="list-style-type: none">• Windows 7, 8, 10• RHEL 7.8, 7.9, 8.1, 8.2, 8.3, 8.4.
CPU	1 or 2 Intel Xeon Quad Core (or equivalent)
Memory	<ul style="list-style-type: none">• 16 GB RAM• 80 GB Disk Space (for software form factor)
Supported Client Browsers	<ul style="list-style-type: none">• Microsoft Edge (latest version as of release date)• Firefox ESR (latest version as of release date)• Google Chrome (latest version as of release date)
Screen Resolution	Optimal screen resolution is 1920x1200
Hardware Models	For upgraded deployments, model C670X running RHEL 7.9.

For Managed ArcSight Products

Managed Node	Form Factor	Supported Product Versions	Certified Product Versions	Appliance Model
ArcMC	Software and Appliance	3.1.3	3.2.3, 3.2.2,	C6700
		3.1.2	3.2.1, 3.2.0	
		3.1.1		
		3.1.0		
		3.0.5		
		3.0.4		
		3.0.0 P3		
		3.0.0 P2		
		3.0.0		
		2.9.6		
		2.9.5		
SmartConnector	Software	8.3.0	8.4.0	
		8.2.0		
		8.1.0		
		8.0.0		
Collector	Software	8.2.0	8.4.0	
		8.1.0		
		8.0.0		
Logger	Software and Appliance	7.2.1	7.2.2	L7700
		7.2.0		
		7.1.1		
Transformation Hub	Software	3.6.0	3.7.0	
		3.5.0		
ESM	Software	7.5.0	7.6.0	
		7.4.0		

Installer Files

Micro Focus provides a digital public key for you to verify that the signed software you received is indeed from Micro Focus and has not been manipulated in any way by a third party. Visit the following site for information and instructions:
<https://entitlement.mfgs.microfocus.com/ecommerce/efulfillment/digitalSignIn.do>

The installation package is available for download from the [OpenText entitlements portal](#). The installer files for ArcSight Management Center 24.1 (3.2.3) are named as follows:

- **For ArcMC:** ArcSight-ArcMC-3.2.3.Build Number.0.bin
- **Software installer for use remotely with ArcMC Node Management as well as local upgrade:** arcmc-sw-Build Number-remote.enc
- **For ArcMC Appliance (Upgrade Only):** arcmc-Build Number.enc
- **ArcMC Agent Installer:** The ArcMC Agent installer for all appliance nodes, and all types of software nodes, is bundled with the ArcMC installer file. You can remotely install or upgrade the ArcMC Agent on a managed node directly from ArcMC, as follows:
 - You can install the ArcMC Agent when you are adding the nodes through Node Management (**Add Host** section). For more information, see to **Chapter 2: Software Installation / Installing the ArcSight Management Center Agent** in the ArcMC Administrator's Guide. For information about upgrading the Agent on managed nodes check **Chapter 5: Managing Nodes / Updating (or Installing) the ArcMC Agent**.
 - You can install or upgrade the ArcMC Agent remotely from a managing ArcMC server on all managed appliance nodes (Logger Appliance and ArcMC Appliance).
 - You can install or upgrade the ArcMC Agent for remotely managed software nodes which are ArcMC v2.2 and Logger v7.0 or later.

Note: The ArcMC Agent cannot be upgraded or installed remotely on earlier versions of ArcMC and Logger, nor for any Connector Appliance-managed node. For these node types, you must use the manual installer named ArcSight - ArcMCAgent-3.2.0.Build Number.0.bin.

Prerequisite for ArcMC Installation or Upgrade on RHEL 7.x

Before installing or upgrading ArcMC on Red Hat Enterprise Linux (RHEL) 7.x, you must modify the inter-process communication (IPC) setting of the `logind.conf` file.

To modify the `logind.conf` file for RHEL 7.x:

1. Navigate to the `/etc/systemd` directory, and open the `logind.conf` file for editing.
2. Find the `RemoveIPC` line. `RemoveIPC` should be active and set to `no`. (Remove the `#` sign if it is there, and change the yes to no if necessary. The correct entry is: `RemoveIPC=no`).
3. Save the file.
4. From the `/etc/systemd` directory, enter the following command to restart the `systemd-logind` service and put the change into effect: `sudo systemctl restart systemd-logind.service`

After you have modified this setting and met all installation requirements, you are ready to install ArcMC.

Upgrading ArcMC

Upgrade is supported from ArcSight Management Center version 3.1.0 to version 24.1 (3.2.3). You should also upgrade any managed ArcMC nodes to version 24.1 (3.2.3).

Before upgrading to ArcMC 3.2.3, ensure that you have upgraded the operating system on your appliance or host to a supported version. For more information about OS support, see ["Technical Requirements" on page 5](#). For instructions on upgrading an appliance either remotely or locally, see Upgrading ArcMC in the ArcMC Administrator's Guide.

The following instructions are for upgrading software ArcMC using a wizard in GUI mode. You can also upgrade your ArcMC from the command line in console mode, and in silent mode. For more information, see the Installation chapter of the ArcMC Administrator's Guide.

If the target ArcMC node is managed by another ArcMC appliance, you can also perform an upgrade using the Node Management upgrade feature.

Note: Micro Focus recommends that you perform a backup of your current ArcSight Management Center configuration before upgrading to ArcMC24.1 (3.2.3). For more information, see the **Managing Backups and Restores** section in the ArcMC Administrator's Guide.

To download and verify the signature of your downloaded files:

1. Log in to the host where you want to begin the installation process.
2. Change to the directory where you want to download the installer files.
3. Download all the necessary product installer files from the OpenText Downloads website along with their associated signature files (*.sig).

Evolving security needs imply the renewal of certificates for the signature verification procedure. To ensure a successful verification of your product signature, download the latest public keys file before proceeding with the verification process (step 1 of the Get the Public Keys procedure).

OpenText provides a digital public key that is used to verify that the software you downloaded from the OpenText software entitlement site is indeed from OpenText and has not been tampered with by a third party. For instructions on how to obtain the latest public keys file and how to verify the signature, see:

<https://support.microfocus.com/kb/doc.php?id=7025140>

If you discover a file does not match its corresponding signature (.sig), attempt the download again in case there was a file transfer error. If the problem persists, please contact OpenText Customer Support.

4. Begin the installation.

Upgrading the ArcMC Agent

You should also upgrade the ArcMC Agent on all managed nodes that require the Agent for communication with ArcMC. For instructions on upgrading the ArcMC Agent on managed nodes, see the ArcMC Administrator's Guide.

Known Limitations

ArcMC is known to have the following limitations.

Issue	Description
242313	The Host Status Exceptions page is not displaying the Transformation Hub rules. Workaround: None available at this time.
237161	If there are connectors installed in the path /opt/arcsoft/connector*/ ArcMC upgrade fails.

Closed Issues

The following issues were resolved in this release.

Issue	Description
751044	An issue has been fixed where after running for a long period, ArcMC could report a JDBC exception on Hibernate data access, SQL Exception for SQL max_stack_depth error.

Known Issues

This release contains the following open issues. To address the issue, use the workaround, if any is indicated.

Key	Description
698065	In some circumstances on Azure, there may be intermittent login and backend errors between Fusion, ArcMC and Kafka Manager.
425040	When in Deployment/Topology view, the IP address of a Logger or ESM destination for Transformation Hub shows as an unknown IP.
387040	In some cases, after performing a search in the online help file, the file may become frozen and necessitate a restart of the browser.
363022	For G10 Appliances with a 10G NIC, after a restore, the gateway is not correctly configured. Workaround: From the CLI, modify the IP address and gateway with the correct information. For reference, consult the ArcMC Admin Guide, section: "Configure a New IP Address".
363017	For G10 Appliances with a 10G NIC, after a restore, the IP address is not correctly configured. Workaround: From the CLI, modify the IP address with the correct information. For reference, consult the ArcMC Admin Guide, section: "Configure a New IP Address".
359190	On G10 appliances, ArcMC does not validate when the user enters invalid IP values when trying to modify the "IP Address" or the "Subnet Mask" field from a network interface (or also called NIC port).
243608	After a product type ages out (Device Age-Out) there is no way for the user to get that product type back. If Device Tracking is disabled for a device product and the device ages out, then there is no way to revert to enable tracking for that device product.

Publication Status

Released: January 2024

Last Updated: Monday, January 22, 2024

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 Release Notes (ArcMC 24.1 (3.2.3))

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.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 8.4.3

ArcSight CEF for Cloud Implementation Standard

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

ArcSight Common Event Format for Cloud Implementation Standard

The Common Event Format (CEF) Standard, developed by ArcSight, lets vendors and their customers quickly integrate their product information into ESM. CEF is an open log management standard that simplifies log management, letting third parties create their own device schemas that are compatible with a standard that is used industry-wide for normalizing security events. Technology companies and customers can use the standardized CEF format to facilitate data collection and aggregation, which can be analyzed later by an enterprise management system.

To know more about the CEF protocol, to see a list of CEF mappings as well as supported date formats, and to understand how to implement the standard, see [ArcSight Common Event Format Implementation Standard](#). It details the header and predefined extensions used within the standard as well as how to create user defined extensions.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Overview

The ArcSight CEF for Cloud Implementation Standard specifies the additional requirements needed for event retrieval, transport, and security of cloud-based logs, thereby providing a means by which cloud-based service providers can integrate with ArcSight's industry-leading log collection technology.

ArcSight SmartConnector technology addresses the core challenge of log collection by providing an effective and highly scalable infrastructure to simplify and optimize the aggregation and normalization of logs across thousands of devices and hundreds of locations.

Historically, ArcSight connectors were designed to run within an enterprise IT environment using a syslog-based standard, with all devices contained on the customer premises. Increasingly, enterprises around the world are adopting cloud-based services that have different characteristics and requirements than on premise devices and applications.

The ArcSight Cloud CEF Implementation Standard addresses these challenges by specifying the additional requirements needed for event retrieval, transport, and security of cloud-based logs, thereby providing a means by which cloud-based service providers can integrate with ArcSight's industry-leading log collection technology.

Challenges in Cloud Event Collection

Enabling log event collection between a cloud service provider and a customer running ArcSight security products differs significantly from traditional log collection processes. These differences include:

- **Network architecture:** The architecture of cloud technologies differs from the network architecture on which traditional ArcSight devices operate.
- **Event generation:** Security events generated by devices in the cloud differ from events generated by traditional security devices in content, format, and transport mechanism.
- **Security:** Log collection for cloud-based services involves securely importing events from outside to inside the customer's environment.
- **Scalability:** Each cloud application changes rapidly and the volume continues to grow, making it challenging to keep current with traditional log collection processes.

To address these differences, ArcSight has developed standards for:

- Event retrieval from cloud vendors that can be re-used across many different types of cloud service providers.
- Use of standard HTTPS for security and support of strong authentication and access control.
- The overall transport format for a retrieved batch of events using JSON.
- Common format for event content called ArcSight CEF.

Supported Industry Standards

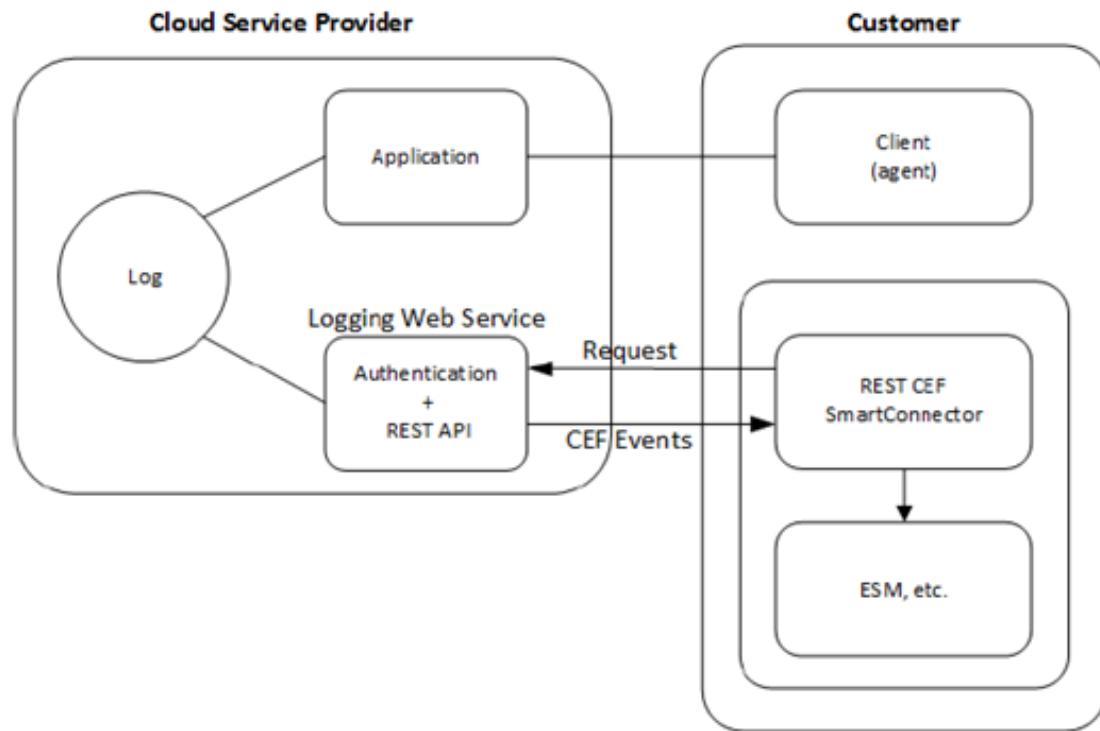
The Cloud CEF Implementation Standard supports the following industry standards:

- REST Web Service APIs
- OAuth 2.0 or Basic authentication
- JSON event transport format
- ArcSight Common Event Format

The ArcSight Cloud CEF Implementation Standard provides the development toolkit to integrate with the cloud service providers using these standards.

ArcSight CEF for the Cloud

The SmartConnector for ArcSight Common Event Format for REST is the device that customers of ArcSight and the cloud-based service provider will use to retrieve events. This is based on the following model:



Cloud service provider customers (“Client” in the diagram) interact with applications typically using a web browser or other user interface. The cloud-based application creates log entries as a by-product of these interactions. The particular log entries are application dependent.

The cloud service provider must provide a logging web service component. The logging web service retrieves the log entries and includes a REST API, support for authentication, and ArcSight Cloud CEF as the event format.

As an open log management standard, Cloud CEF improves the interoperability of security-related information by reducing various message syntaxes to one matching the ArcSight schema. This API must use ArcSight Cloud CEF as the event format.

There are three main elements to the Cloud CEF solution:

1. The REST CEF SmartConnector retrieves events through a REST API exposed by the cloud service provider.
2. Events are retrieved in ArcSight CEF format and transported over HTTPS (which may require an access token).
3. Retrieved events are sent to ArcSight products such as ArcSight Enterprise Security Manager (ESM).

SmartConnector for ArcSight Common Event Format REST

The [SmartConnector for ArcSight Common Event Format REST](#) lets customers configure an authentication method and the REST API URLs for event retrieval. The connector is typically located on customer premises, although it can be run on the service provider platform, where it attempts to retrieve the latest events as reported by the cloud service provider REST APIs.

The Cloud CEF Implementation Standard mandates that the cloud service provider adhere to the following conditions for authentication and event retrieval, by implementing an authentication mechanism and event retrieval APIs:

Authentication

Authentication is generally required to gain access to the cloud server containing the event data. Each cloud service provider defines the authentication method used for its servers. The REST CEF SmartConnector provides flexible authentication support. Initially the two authentication methods supported are OAuth 2.0 and Basic authentication. The REST CEF SmartConnector user chooses the authentication method at connector installation time based on the capabilities of the cloud service provider.

OAuth 2.0 Authentication: The OAuth 2.0 standard is defined by IETF RFC 649. With OAuth 2.0, a third party application (in this case, the REST CEF SmartConnector) can be allowed access to server resources without disclosing the credentials of the resource owner.

To achieve this, the cloud service provider implementation of OAuth 2.0 must support:

- Callback URLs for the local host, so that the connector can access the authentication code and complete the OAuth authentication.
- HTTPS for local host URLs

For example, <https://localhost:8080/oauth2callback> is an example of a supported callback URL, known as a `redirect_uri` in the OAuth 2.0 specification.

- Provisions for maintaining a valid refresh token without human intervention. If refresh tokens are used, there must be a mechanism for automatically extending the refresh token expiration date.

For example, if the refresh token is initially valid for 14 days and is used to acquire a new access token, the expiration date is extended for 14 more days.

Basic Authentication: In Basic authentication, the client provides an identifier (a username) and a shared secret (a password). Basic authentication is defined by RFC 2617. This authentication method uses TLS protocol, in which both the identifier and shared secret are encrypted. A client certificate might also be required by the vendor to verify the client's identity.

Event Retrieval APIs

The REST CEF SmartConnector retrieves events using REST API calls over secure transport (HTTPS). It expects CEF events in JSON format.

The API endpoint URL is comprised of several elements:

- The base URL
- The CEF events endpoint
- One or more event query arguments

Each of these elements are described in the following sections.

Base URL

The API endpoint base URL is specific to the cloud service provider, and includes the host name and path designation.

The base URL can be static or dynamic, although static URLs are recommended. If Dynamic URLs are used, the vendor must provide the means to get the dynamic portion of the URLs.

- Static URLs, such as `https://api.abc.com/1.0/auditEvents`, are the same for any user.
- Dynamic URLs, such as
`https://<SomeUserSpecificValue>.api.abc.com/1.0/auditEvents`, include a value (`<SomeUserSpecificValue>` in this example) derived from the authenticated user using OAuth.

CEF Events Endpoint

The CEF events component of the path denotes a service that conforms to the REST CEF SmartConnector standard.

For example, a base URL of `https://www.acmeapis.com/admin/reports` contains the hostname `www.acmeapis.com`, and the path specification `/admin/reports`.

When combined with the `cef-events` endpoint, the event retrieval URL becomes:

`https://www.acmeapis.com/admin/reports/cef-events`

Event Query Arguments

The following query parameters are defined:

- `startTime=<timestamp>`

where `<timestamp>` follows the form `yyyy-MM-dd'T'HH:mm:ss.SSSZ`.

Example: `2012-05-15T00:01:02.345-08:00`

The timestamp components after `yyyy-MM-dd'T'HH:mm:ss` are optional. The time zone designator is `Z` or `+hh:mm` or `-hh:mm`. If the `startTime` is not specified, events are retrieved beginning with the earliest available event.

- `maxResults=<number>`

where `<number>` is an integer. This specifies that no more than `<number>` events should be returned in the response. If `maxResults` is not specified, the number of events produced is determined by the cloud service provider.

- `eventType=<event type list>`

The `<event type list>` is a comma-separated list of the event types to retrieve. The individual event type names are specific to the cloud service provider. If `eventType` is not specified, events of all types are retrieved.

The REST CEF SmartConnector periodically requests new events from the server. The polling period has a default value of 30 seconds, which is user-configurable. If a request to the server for events produces some events, the connector immediately makes another request using the continuation capability. This process continues until a request for events produces no events, after which the connector reverts to the configured polling period.

Retrieved Response Format

The server returns the response in an HTML document. The content type is application/JSON, as defined by RFC 4627. Contained within the document is a collection of CEF-formatted event data. The document content is formatted as follows:

```
{  
  "format" : "cef",  
  "version" : "1.0",  
  "timestamp" : <timestamp in standard format>, "count" : <number>,  
  "events" : [  
    "CEF:Version|Device Vendor|Device Product|Device  
    Version|SignatureID|Name|Severity|[Extension]",  
    "CEF:Version|Device Vendor|Device Product|Device  
    Version|SignatureID|Name|Severity|[Extension]",  
    .  
    "CEF:Version|Device Vendor|Device Product|Device  
    Version|SignatureID|Name|Severity|[Extension]"  
  ],  
  "links" : [  
    {  
      "rel": "next",  
      "href": URL  
    }  
  ]}
```

Continuation

When the connector starts up, it makes a first request to the server using the Events URL provided in the setup configuration to get the first set of events, and uses the URL contained in the “links” array of the response for each subsequent request.

Whenever the server has more events than can be contained in a single response, the connector immediately makes additional requests to retrieve more events using the URL from links array contained in the response. If there are no events in the response, the connector waits for the configured polling period to retrieve more events using the URL from the links array contained in the response.

CEF Mappings

The ArcSight Common Event Format is defined in [ArcSight Common Event Format Implementation Standard](#). Cloud service providers must use this document to map native event fields to the appropriate CEF key value.

Summary

If a cloud service provider supports OAuth 2.0 or Basic authentication, and exposes REST APIs for event retrieval in ArcSight CEF (over JSON) format, ArcSight and cloud service providers customers can monitor their applications on the service provider's cloud platform.

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 ArcSight CEF for Cloud Implementation Standard (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnector

Software Version: CE 25.1

Configuration Guide for Microsoft Azure Event Hub SmartConnector

Document Release Date: February 2025

Software Release Date: February 2025

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2025 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft Azure Event Hub SmartConnector	7
Product Overview	8
Azure Event Logs	8
Related Azure Services	9
Azure Event Log Categories	9
Understanding Data Collection	14
Prerequisites	15
Supported Event Hub Tiers	15
Setting User Permissions in Azure	15
Permission Requirements	15
Configuration	16
Creating a Resource Group	16
Creating an Event Hub Namespace	17
Creating an Event Hub	18
Registering the Application in Azure AD	19
For registration of the App, the following steps must be implemented:	20
For authenticating the App, the following steps must be implemented:	20
Assigning IAM Role	21
Streaming Logs	22
Installing the SmartConnector	27
Preparing to Install the SmartConnector	27
Installing and Configuring the SmartConnector by Using the Wizard	28
Adding Support for New Log Sources	31
Supported Log Sources	31
Adding Support for New Log Sources	33
Configuring Advanced Parameters	35
Accessing Advanced Parameters	35
Additional Connector Configuration for Defender for Endpoint Data Source	37
Connector limits the character length of the rawEvent field	37
Migrating the SmartConnector	39
Prevention of Data Loss	40
Hardware Consideration	42
Device Event Mapping to ArcSight Fields	43
Event Mappings for Active Directory	43
Common Event Mapping	43

Sign-in Logs Event Mapping	43
Audit Logs Event Mapping	44
Event Mappings for Microsoft Defender for Cloud	45
Common Event Mapping	45
Security Alerts Event Mapping	45
Security Recommendations Event Mapping	46
Event Mappings for Activity	47
Common Event Mapping	47
Action Event Mapping	47
Administrative Event Mapping	48
Alert Event Mapping	49
Delete Event Mapping	49
Recommendation Event Mapping	50
Security Event Mapping	50
Service Health Event Mapping	51
Write Event Mapping	52
Event Mappings for Resource Log	52
Common Event Mapping	52
Activity Runs Event Mapping	54
Application Gateway Access Log Event Mapping	54
Archive Logs Event Mapping	55
Audit Event Mapping	55
Authoring Event Mapping	56
Automatic Tuning Event Mapping	56
Azure Firewall Application Rule Event Mapping	57
Azure Firewall Network Rule Event Mapping	57
Azure Site Recovery Jobs Event Mapping	57
Blocks Event Mapping	58
C2D Command , C2D Twin Operations, and D2C Twin Operations Event Mapping	58
Database Wait Statistics Event Mapping	59
Deadlocks Event Mapping	59
Engine Event Mapping	60
Errors Event Mapping	60
Gateway Logs Event Mapping	61
Job Logs Event Mapping	61
Jobs Operations Event Mapping	62
Load Balancer Alert Event Mapping	62
Network Security Group Event Mapping	62
Operational Logs Event Mapping	63

P2S Diagnostic Logs Event Mapping	63
Postgre SQL Logs Event Mapping	64
Query Store Wait Statistics Event Mapping	64
Requests Event Mapping	64
Routes Event Mapping	65
Service Log Event Mapping	65
Timeouts Event Mapping	66
Trigger Runs Event Mapping	66
Twin Queries Event Mapping	67
Workflow Runtime Event Mapping	67
Event Mappings for Windows AD	68
Event 4624	68
Event 4625	69
Event 4648	70
Event 4768	73
Event 4769	73
Event 4770	74
Event 4771	75
Event 4772	75
Event 4773	75
Event 4776	76
Event 4777	76
Event 5137	76
Event 5139	77
Event 5140	77
Event 5141	78
Event 5145	78
Event 6272	79
Event 6273	79
Event 6274	80
Event 6275	80
Event 6276	80
Event 6277	80
Event 6278	81
Event Mappings for Defender for Endpoint	81
AlertEvidence	81
AlertInfo	82
DeviceFileEvents	83
DeviceImageLoadEvents	84

DeviceInfo	85
DeviceLogonEvents	86
DeviceNetworkEvents	88
DeviceNetworkInfo	89
Troubleshooting	90
Reconfiguring the expired Client Secret or Client Certificate	90
Send Documentation Feedback	92

Configuration Guide for Microsoft Azure Event Hub SmartConnector

The Microsoft Azure Event Hub SmartConnector helps you monitor the activities on Microsoft Azure Cloud services.

This SmartConnector collects events and logs from the following Microsoft Azure log sources:

- Azure Active Directory
- Azure Monitor
- Microsoft Defender for Endpoint

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

Microsoft Azure is a set of cloud services to help organizations build, manage, and deploy applications on a massive, global network using their favorite tools and frameworks.

Azure Event Logs

The Microsoft Azure Event Hub connector collects the following event logs from Active Directory, Azure Monitor, and Microsoft Defender for Cloud in Azure:

- **Active Directory Logs**

- **Audit logs:** Provides records of system activities for compliance.
- **Sign-in logs:** Provides information related to user logins.



Note: To export Active Directory sign-in logs, you must have one of P1 or P2 premium editions of Azure Active Directory.

- **Activity Logs:** Provides data related to write operations, such as CREATE, UPDATE, and DELETE that were performed on resources in your subscription. For more information, see [Azure Activity log](#).

- **Resource Log (formerly known as Diagnostic Log):** Provides data related to operations performed within an Azure resource (the data plane).

Getting a secret from a key vault or making a request to a database. The content of resource log varies by the Azure service and resource type.

- **Microsoft Defender for Cloud**

- **Security alerts:** Provides data related to security actions performed on Microsoft Defender for Cloud in your subscription.
- **Recommendation logs:** Provides data related to prevention recommendations provided for the resources in your subscription.

- **Windows AD Logs:** Records details related to the system, security, and application stored on a Windows operating system. It contains information regarding hardware and software events occurring on a Windows operating system. It can be monitored to track system and application issues or forecast any potential issues.

- **Defender for Endpoint Logs:** Provides visibility into what is happening on a computer or other endpoint device. These logs include information about user activity, system activity, network connections, and more. These logs are also used to track suspicious activity, identify malware infections, and detect signs of data exfiltration or other malicious behavior. It can also be used to provide forensic evidence during the event of a security breach.

Related Azure Services

The following services are used when working with Microsoft Azure Event Hub SmartConnector:

- **Azure Resource Manager:** Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure subscription. You use management features, such as access control, locks, and tags, to secure and organize your resources after deployment. For more information, see [Azure Resource Manager](#).
- **Azure Event Hubs:** Azure Event Hubs is a big data streaming platform and event ingestion service. It can receive and process millions of events per second. Data sent to an event hub can be transformed and stored by using any real-time analytics provider or batching/storage adapters. For more information, see [Azure Event Hubs — A big data streaming platform and event ingestion service](#).

Azure Event Log Categories

Following tables list the categories for mappings supported by the Microsoft Azure Event Hub SmartConnector. The mappings are done using the schemas provided in the Azure documents.

Active Directory Log Categories

Categories	Certified
Signin	Yes
Audit	Yes

Activity Log Categories

Categories	Certified	Comments
Administrative	Yes	<p>These are the sub-categories:</p> <ol style="list-style-type: none"> 1. Action 2. Write 3. Delete <p>For more information, see Azure Activity Log event schema .</p>
Alert	Yes	Azure alerts.

Categories	Certified	Comments
Recommendation	Yes	Recommendation events from Azure Advisor.
Security	No	Same as Microsoft Defender for Cloud log events for Security Alert activity without remediation steps.
ServiceHealth	Yes	Service Health incidents occurred in Azure.

Resource Log Categories

Categories	Resource Type
AppServiceHTTPLogs	Microsoft.Web/sites
AppServiceIPSecAuditLogs	Microsoft.Web/sites
GatewayLogs	Microsoft.ApiManagement/service
JobLogs	Microsoft.Automation/automationAccounts JobStreams
JobStreams	Microsoft.Automation/automationAccount
CoreAnalytics	Microsoft.Cdn/profiles/endpoints
PipelineRuns	Microsoft.DataFactory/factories
TriggerRuns	Microsoft.DataFactory/factories
Audit	Microsoft.DataLakeAnalytics/accounts
Requests	Microsoft.DataLakeAnalytics/accounts
Audit	Microsoft.DataLakeStore/accounts
Requests	Microsoft.DataLakeStore/accounts
Connections	Microsoft.Devices/IotHubs
DeviceTelemetry	Microsoft.Devices/IotHubs
C2DCommands	Microsoft.Devices/IotHubs
DeviceIdentityOperations	Microsoft.Devices/IotHubs
FileUploadOperations	Microsoft.Devices/IotHubs
Routes	Microsoft.Devices/IotHubs
D2CTwinOperations	Microsoft.Devices/IotHubs
C2DTwinOperations	Microsoft.Devices/IotHubs
TwinQueries	Microsoft.Devices/IotHubs
JobsOperations	Microsoft.Devices/IotHubs
DirectMethods	Microsoft.Devices/IotHubs

Categories	Resource Type
DataPlaneRequests	Microsoft.DocumentDB/databaseAccounts
ArchiveLogs	Microsoft.EventHub/namespaces
OperationalLogs	Microsoft.EventHub/namespaces
AuditEvent	Microsoft.KeyVault/vaults
WorkflowRuntime	Microsoft.Logic/workflows
NetworkSecurityGroupEvent	Microsoft.Network/networksecuritygroups
NetworkSecurityGroupRuleCounter	Microsoft.Network/networksecuritygroups
LoadBalancerAlertEvent	Microsoft.Network/loadBalancers
LoadBalancerProbeHealthStatus	Microsoft.Network/loadBalancers
ApplicationGatewayAccessLog	Microsoft.Network/applicationGateways
ApplicationGatewayPerformanceLog	Microsoft.Network/applicationGateways
ApplicationGatewayFirewallLog	Microsoft.Network/applicationGateways
OperationalLogs	Microsoft.ServiceBus/namespaces
QueryStoreRuntimeStatistics	Microsoft.Sql/servers/databases
QueryStoreWaitStatistics	Microsoft.Sql/servers/databases
Errors	Microsoft.Sql/servers/databases
DatabaseWaitStatistics	Microsoft.Sql/servers/databases
Timeouts	Microsoft.Sql/servers/databases
Blocks	Microsoft.Sql/servers/databases
Audit	Microsoft.Sql/servers/databases
Execution	Microsoft.StreamAnalytics/streamingjobs
Authoring	Microsoft.StreamAnalytics/streamingjobs
AzureFirewallApplicationRule	Microsoft.Network/AzureFirewalls
AzureFirewallNetworkRule	Microsoft.Network/AzureFirewalls
ServiceLog	Microsoft.Batch/batchAccounts
SQLSecurityAuditEvents	Microsoft.Sql/servers/databases
SQLSecurityAuditEvents	Microsoft.Synapse/workspaces
AutomaticTuning	Microsoft.Sql/servers/databases
Deadlocks	Microsoft.Sql/servers/databases
ActivityRuns	Microsoft.DataFactory/factories
AzureBackupReport	Microsoft.RecoveryServices/Vaults

Categories	Resource Type
AzureSiteRecoveryEvents	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryJobs	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryProtectedDiskDataChurn	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryRecoveryPoints	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicatedItems	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicationDataUploadRate	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicationStats	Microsoft.RecoveryServices/Vaults
DscNodeStatus	Microsoft.Automation/automationAccounts
Engine	Microsoft.PowerBI
Engine	Microsoft.AnalysisServices/servers
GatewayDiagnosticLog	microsoft.network/p2svpngateways
GatewayDiagnosticLog	microsoft.network/virtualnetworkgateways
GatewayDiagnosticLog	microsoft.network/vpngateways
IkeDiagnosticLog	microsoft.network/p2svpngateways
IkeDiagnosticLog	microsoft.network/virtualnetworkgateways
IkeDiagnosticLog	microsoft.network/vpngateways
Operationlogs	microsoft.loadtestservice/loadtests
Operationlogs	Microsoft.Search/searchServices
P2Sdiagnosticlog	microsoft.network/virtualnetworkgateways
P2Sdiagnosticlog	microsoft.network/p2svpngateways
Routediagnosticlog	microsoft.network/virtualnetworkgateways
Routediagnosticlog	microsoft.network/vpngateways
OperationalLogs	Microsoft.NotificationHubs/namespaces
OperationalLogs	Microsoft.ServiceBus/Namespace
PostGreSQLLogs	Microsoft.DBforPostgreSQL

Microsoft Defender for Cloud Log Categories

Categories	Resource Type	Certified
Securityalerts	All resources	Yes
SecurityRecommendations	All resources	Yes

Windows AD Log Categories

Categories	Resource Type	Certified
Security	All resources	Yes

Defender for Endpoint Log Categories



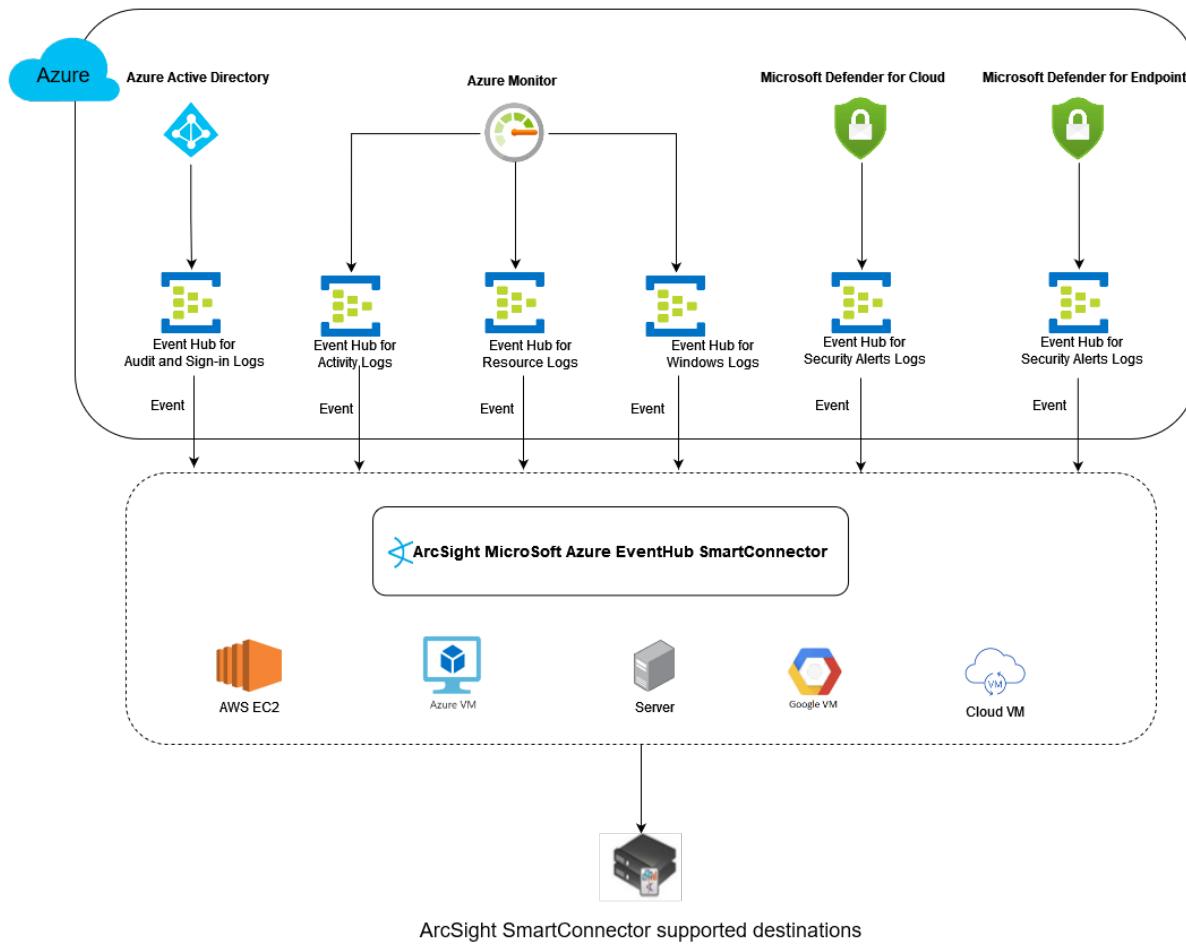
Important: The Defender for Endpoint Log Categories is supported only for **ArcSight Intelligence** deployments. In this case, the Microsoft Azure Event Hub SmartConnector acts as a carrier and sends events to the ArcSight supported destinations without normalizing the events. You can install the Microsoft 365 Defender SmartConnector to process the Microsoft 365 defender events. For more information, see [Configuration Guide for Microsoft 365 Defender SmartConnector](#).

Categories	Certified
Alert Evidence	Yes
Alert Info	Yes
Device Alert Events	Yes
Device Events	Yes
Device File Events	Yes
Device Image Load Events	Yes
Device Info	Yes
Device Logon Events	Yes
Device Network Events	Yes
Device Network Info	Yes
Device Network Info	Yes
Device Process Events	Yes
Device Registry Events	Yes
Dynamic Event Collection	Yes

The Microsoft Azure Event Hub SmartConnector currently includes mapping files for several log categories of activity, audit, sign-in, resource, and windows Active Directory log categories. If schemas are not available for any category in Azure documents, then, the mappings for these categories are not available in the connector. Such events are sent unparsed to the ArcSight destination.

Understanding Data Collection

The following diagram provides a high-level overview of how the Microsoft Azure Event Hub SmartConnector collects and sends data to ArcSight's destinations.



Understanding the process flow of data collection

1. Before installing the Microsoft Azure Event Hub SmartConnector, configure the required Event Hubs to stream the raw data. See [Streaming Logs](#).
2. After installing, ArcSight Microsoft Azure Event Hub SmartConnector collects logs in JSON format and then sends the events to the ArcSight SmartConnector supported destination.

Prerequisites

- [Supported Event Hub Tiers](#)
- [Setting User Permissions in Azure](#)

Supported Event Hub Tiers

Azure Event Hubs is a fully-managed, real-time data ingestion service that is simple, secure and scalable. Event Hubs lets you stream millions of events per second from any source so you can build dynamic data pipelines and respond to business challenges immediately. Keep data ingestion secure with geo-disaster recovery and geo-replication options.

With Azure Event Hubs for Apache Kafka, you can enable existing Kafka clients and applications to talk to Event Hubs without any code changes, giving you a managed Kafka experience without having to manage your own clusters.

The following tiers are supported: Standard, Premium, and Dedicated. For more information, refer to this [Microsoft Documentation](#).

Next Step: [Setting User Permissions in Azure](#)

Setting User Permissions in Azure

In Azure, users must be associated with a subscription to provide them with access to resources such as Resource group, Event Hub namespace, and Event hubs. Therefore, you must determine the subscription you want to use for Microsoft Azure Event Hub SmartConnector and add users to the required subscription. You must also assign users to a role to define their permission to perform tasks.

Permission Requirements

Scope	Description
Azure Subscription	The users must have the Security Administrator IAM role on the subscription.
Resource group	The users must create a resource group. The users must ensure that they are assigned the Application Administrator role and Owner role on the resource group before deploying the connector.

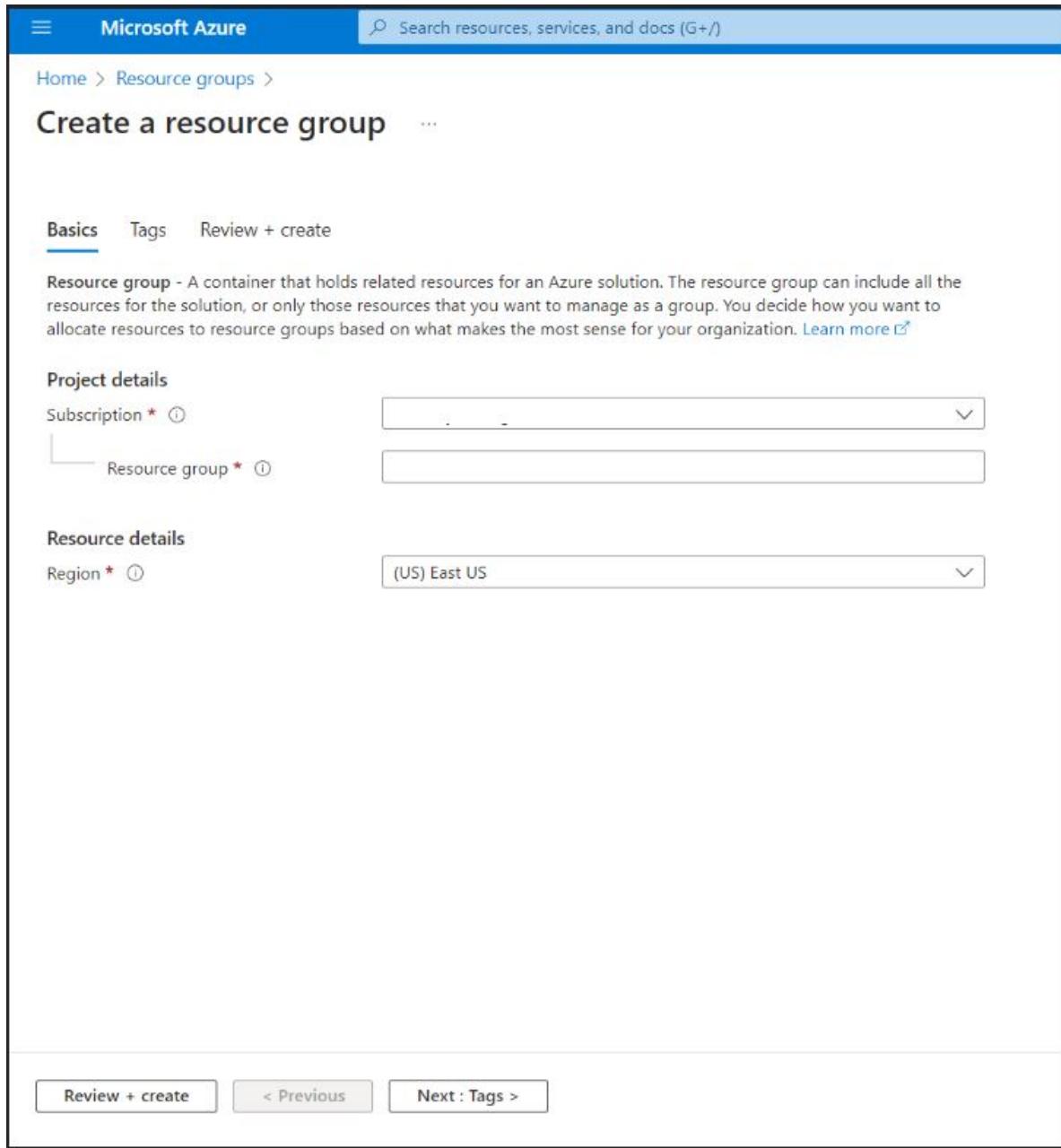
Configuration

The following configuration steps must be implemented before installing the connector:

Creating a Resource Group

1. Log in to the Azure portal and navigate to the **Resource Group** service.
2. Click **+Create**.
3. Select the **Subscription** and enter a name for the group in the **Resource group** field.
4. Navigate to **Resource details** and select the region.
5. (Optional) Click **Next:Tags** to create a tag for the group.

6. Click **Next:Review > +Create**.



Creating an Event Hub Namespace

1. Log in to the Azure portal and navigate to the **Event Hubs** service.
2. Click **+Create**.
3. Select the **Subscription** and the **Resource group** that is created above.
4. Navigate to **Instance Details** and enter a name in the **Namespace name** field.

5. Select the same **Location** that is selected while creating the **Resource Group**.
6. Select the pricing tier according your requirement. Ensure the selected pricing tier supports Apache Kafka. Refer to this [Microsoft documentation](#) for more plans.
7. Click **Review + Create**.

The screenshot shows the 'Create Namespace' wizard in the Microsoft Azure portal. The title bar says 'Microsoft Azure' and 'Event Hubs > Create Namespace'. The top navigation bar includes 'Search resources, services, and docs (G+/-)' and tabs for 'Basics', 'Advanced', 'Networking', 'Tags', and 'Review + create'. The 'Basics' tab is selected. The main area is titled 'Project Details' with a note about managing resources via subscription and resource groups. It shows fields for 'Subscription *' (dropdown), 'Resource group *' (dropdown with 'Create new' option), 'Namespace name *' (input field ending in '.servicebus.windows.net'), 'Location *' (dropdown set to 'East US') with an info message about availability zones, 'Pricing tier *' (dropdown with 'Browse the available plans and their features' link), and 'Throughput Units *' (slider set to 1). At the bottom are buttons for 'Review + create', '< Previous', and 'Next: Advanced >'.

Creating an Event Hub

1. Click the **Namespace** that is created above.
2. Navigate to **Event Hubs > +Event Hub**.

3. Enter a **Name** for the hub and select the **Partition count**. For more information regarding Partition count, refer to this [Microsoft Documentation](#).
4. Navigate to **Retention**. Select the **Cleanup policy** and choose the required **Retention time**.
5. Click **Review + create**.

The screenshot shows the 'Create Event Hub' wizard in the 'Event Hubs' section. The 'Basics' tab is selected. In the 'Event Hub Details' section, there is a text input field for 'Name' with a red asterisk indicating it is required, and a slider for 'Partition count' set to 2. In the 'Retention' section, there is a dropdown for 'Cleanup policy' showing 'Delete' and a text input for 'Retention time (hrs)' set to 1, with a note below stating 'min. 1 hour, max. 24 hours (1day)'. At the bottom are buttons for 'Review + create', '< Previous', and 'Next: Capture >'.



Note:

- Ensure to select the same **Subscription** and **Region** while creating the **Resource Group** and **Event Hub Namespace**.
- Creating a Resource Group and Event Hub Namespace is a one-time activity. For each data source, all the Event Hubs must be created under the same Event Hub Namespace.

Registering the Application in Azure AD

Azure Active Directory applications streamline secure access and authentication for Azure cloud resources, enabling centralized identity management and seamless integration with a

wide range of applications and services.

Azure AD applications provide robust security measures such as multi-factor authentication, conditional access policies, and role-based access control, ensuring authorized access and protecting against unauthorized entry.

For registration of the App, the following steps must be implemented:

1. Log in to Azure Portal.
2. Navigate to **Azure Active Directory** and select **App registrations**.
3. Click **+New registration** to create a new application registration.
4. Enter a name for the application, select the appropriate account type and click **Register**.

For authenticating the App, the following steps must be implemented:

The connector supports two methods of authentication: **Client Certificate** and **Client Secret**. You can choose either of them.



Note: From a security standpoint, **Client Certificates** are often considered to be more secure than **Client Secrets**.

1. If **Client Certificate** method is opted.

To generate the self-signed certificate implement the following steps:

- a. Open the command prompt and run the below command by replacing the certificate filename, password and validity days.

```
keytool -genkey -keystore <filename.pfx> -storetype PKCS12 -keyalg RSA  
-storepass <password> -validity <days> -keysize 2048
```

This will generate the .pfx certificate file. This certificate will be provided while installing the connector when **Client Certificate** mechanism is used for authentication.

- b. Run the below command to generate .cer certificate file by replacing the same filename and password as mentioned in the above step.

```
keytool -export -keystore <filename.pfx> -file <client.cer> -storetype  
PKCS12 -storepass <password>
```

This will generate the .cer certificate file. This must be uploaded in the Azure portal to authenticate the connector to access the Azure AD application. Implement the following steps to upload this certificate to the Azure portal:

- i. Navigate to the Application that is registered in step 3 and click **Certificates & secrets**.
 - ii. Under **Certificates > Upload Certificate**.
 - iii. Select the public key file of the certificate .cer file. Enter a meaningful description to it. Then click **Add**.
Certificate will be listed in **Certificates** section.
2. If **Client Secret** is opted then implement the following steps to configure the Client Secret in Azure:
- a. Navigate to the application that is registered in step 3 and click **Certificates & secrets**.
 - b. Under **Client Secret > +New Client Secret**.
 - c. Enter a **Description** to the secret. Set the value for expiry and click **Add**. This will generate the **Client Secret**.



Important: Note the generated Secret Key Value to provide the same while installing and configuring the connector. If you do not note down the Secret Value, you will not be able to retrieve it later.



Note: Ensure to note the expiry date of the **Client Secret** and **Client Certificate**. After the Client Secret/ Certificate expires, the connector will fail to authenticate the application and it will stop working. To reconfigure the new Client Secret or Client Certificate, see the [Troubleshooting](#) section.

Assigning IAM Role

IAM role must be assigned to this application in Event Hubs Namespace to allow the application to read data from Azure Event Hub.

To assign IAM role:

1. Navigate to **Event Hubs Namespace** created [here](#) and select **Access Control (IAM)**.
2. Click **Role Assignments > +Add** and select **Add role assignment**.
3. Assign **Azure Event Hubs Data Receiver** role and click **Next**.



Note: If you want to configure the SmartConnector to use **Microsoft Azure Event Hub** as a destination, an additional role as **Azure Event Hubs Data Sender** is required to send events to Microsoft Azure Event Hub.

4. Click **+Select members** and select the registered application.
5. Click **Next > Review + Assign**.

Streaming Logs

Azure Active Directory Logs

To send Azure Active Directory events to Event Hub, follow these steps:

1. Log in to the Azure portal.
2. Navigate to **Azure Active Directory** and select **Diagnostic settings**.
3. Click **+Add Diagnostic Setting** and enter a name for **Diagnostic setting name**.
4. Navigate to **Categories** and select **AuditLogs and SignInLogs**.
5. (Optional) For Intelligence, only **SignInLogs** must be enabled.
6. Navigate to **Destination details** and select **Stream to an event hub** as the destination.
7. Select the required **Subscription**, **Event Hub Namespace**, **Event Hub Name** and ensure to save the settings.

Activity Logs

To send Activity events to Event Hub, follow these steps:

1. Log in to the Azure portal.
2. Select the **Resource Group** from which you want to stream the **Activity Logs**.
3. Click **Activity Log > Export Activity Logs Settings**.
4. Click **+ Add Diagnostic Setting** and enter a name for **Diagnostic setting name**.
5. Navigate to **Categories**. Select the log categories that are required to be enabled.
6. Navigate to **Destination details** and select **Stream to an event hub** as the destination.
7. Select the required **Subscription**, **Event hub namespace**, **Event hub name** and ensure to save the settings.

Microsoft Defender for Cloud Event Logs

To send Microsoft Defender for Cloud events to Event Hub, follow these steps:

1. From the left sidebar, select **Microsoft Defender for Cloud**, and then click **Environment Setting**.
2. Select the specific subscription to be used when configuring data export.
3. On the **Subscription** settings, go to the sidebar and select **Continuous Export**.
4. Select the data type to be exported and choose from the filters on each type.
5. From **Export target**, choose the required **Subscription**, **Event Hub namespace**, **Event Hub name**, and **Event hub policy name**.

For the Event hub policy name:

- a. Navigate to the required Event Hub to which you want to stream the logs.
- b. Click **Shared access policy** tab > **+Add** to create a new policy and enter a name for it.
- c. Select the required permissions and click **Create**.
6. Save your changes.

Resource Logs

You must manually add diagnostic settings to configure streaming of these logs. The following procedure provides a brief overview of settings required for streaming Diagnostic Logs. For information, see [Azure documentation](#).

1. Select **Azure Home > Monitor > Diagnostic Settings**.
2. Select the required **Subscription**, **Resource group**, **Resource type**, and **Resource** from the drop-down.
3. Click **+Add diagnostic setting** and add a name for it.
4. Select the required log categories under **Logs** section.
5. Navigate to **Destination details** and select **Stream to an event hub** as the destination.
6. Select the required **Subscription**, **Event hub namespace**, **Event hub name** and ensure to save the settings.

Windows AD Logs

Azure Monitor Agent (AMA) collects the monitoring data from the guest operating system of Azure and hybrid virtual machines and delivers it to the Azure Monitor for use by features, insights, and other services.

Azure Monitor Agent uses data collection rules, where you define which data you want each agent to collect. Data collection rules let you manage data collection settings at scale and define unique, scoped configurations for subsets of machines. You can define a rule to send data from multiple machines to multiple destinations across regions and tenants. For more information refer to this [Microsoft Documentation](#).

Azure Monitor Agent must be installed on the resource to collect the Windows AD data. The resource can be either Azure or Non-Azure resource.

- Azure Resources: Azure Resources includes Azure VM.
- Non-Azure Resources: Non-Azure Resources includes the physical servers and virtual machines hosted outside of Azure (that is on-premises) or in other clouds.

To collect the Windows AD data from Non-Azure Resources, implement the following steps:

1. Establish connection between Non-Azure Resources and Azure.

Different methods can be used or connecting the machines in your hybrid environment directly with Azure. For connecting machines using a deployment script, implement the steps mentioned in the [Microsoft Documentation](#).

Generate the installation script from the Azure portal. This will download and install the **Microsoft Monitoring Agent** and establish the connection with Azure Arc.



Note: For authentication, log in using the pop-up browser while running the script.

Ensure the machine is registered in the Azure portal under **Servers-Azure Arc** after the successful execution of the script. This will confirm the connection establishment.

2. Register the Server extension for Azure Monitor Agent.

Azure Monitor Agent for Windows is an extension that can be installed on servers registered with Azure Arc to collect and send data to Azure Monitor.

- a. Navigate to **Servers-Azure Arc** and select the registered server.
- b. Navigate to **Settings** and click **Extension > +Add**.
- c. Select **Azure Monitor Agent for Windows** extension and click **Next**.
- d. Click **Review + Create**.

This will only install the agent. You must use Data Collection Rule to configure Azure Monitor Agent's data collection settings for it to start working.

3. Create a Log Analytics workspace in Azure.

- a. Log in to Azure portal.
- b. Navigate to **Log Analytics workspaces** and click **+ Create**.
- c. Specify the Resource group created [here](#).
- d. Enter a name for the workspace and select the same region that was selected while creating the Resource group.
- e. Click **Review+Create**.

4. Configure the **Azure Monitoring Agent** to send the logs to the Log Analytical workspace.

- a. Creating a Data Collection Rule in Azure Monitor (For more information regarding this, see this [Microsoft Documentation](#)):
 - i. Log in to Azure portal.
 - ii. Navigate to **Monitor** and select **Data Collection Rules**.
 - iii. Click **+Create** to create a new data collection rule and associations.

- On the Basics tab:
 - A. Enter a **Rule** name and specify the **Subscription**, **Resource Group**, **Region**, and **Platform Type**. Region specifies where the DCR will be created. The virtual machines and their associations can be in any subscription or resource group in the tenant.
 - B. Select the same region as your [Log Analytics workspace](#). Platform Type specifies the type of resources in which the rule can be applied. The Custom is for both Windows and Linux.
- On the Resources tab:
 - A. Click **+ Add resources** to add associated resources to the data collection rule. These resources can be Virtual Machines, Virtual Machine Scale Sets, and Azure Arc for servers. The Azure portal installs Azure Monitor Agent on those resources where it is not installed.
 - B. Select the resource group that is created [here](#) and specify the required resources. Click **Apply**.
- On the Collect and Deliver tab:
 - A. Click **+Add data source** to add a data source and select a destination.
 - B. Select the data source type and the data to collect for the resources. Select **Windows Event Logs**.
 - C. Select **Basic** to enable collection of event logs. Select **Custom** if you want control over the collected event logs.
 - D. Navigate to **Security** and enable both **Audit Success** and **Audit Failure** to configure the security event logs.
 - E. Click **Next:Destination>** to configure the destination to the data sources.
 - F. Click **+Add** to select destination and for sending Windows event data sources to Azure Monitor Logs only.
 - G. Select **Destination type** as **Azure Monitor Logs** and select the required Subscription.
 - H. Select the Log Analytics workspace that is created [here](#).
 - I. Click **Add data source > Review + Create** to review the details of the data collection rule associated with the set of virtual machines.
 - J. Select **+Create** to create the data collection rule.
- b. Creating a Data Export Rule in Azure Monitor:

- i. Log in to the Azure portal and Navigate to **Log Analytics workspace** created [here](#).
- ii. Navigate to **Settings** and select **Data Export > New export rule**.
 - On the Basics tab:
 - A. Enter a name For the Export rule.
 - B. Check the **Enable upon creation** check box and click **Next**.
 - On the Source tab:
 - A. Select the **Event table** and click **Next**.
 - On the Destination tab:
 - A. Select **EventHub as Destination**.
 - B. In **Destination details** and select the required **Subscription** and the **Event Hub Namespace** created [here](#).
 - C. Enter the **Event hub Name** for configuring the windows logs.
 - D. Click **Next** to create the Export rule.

Defender for Endpoint Logs

1. Log in to Microsoft Defender Security Center.
2. Click **Partners & APIs > Data export settings**.
3. Click **+Add data export settings** to add the export rule.
4. Provide a name to the export rule and select **Forward events to Azure Event Hub**.
5. Provide the **Event-hub Resource Id** of the Event Hub namespace that is created [here](#).
Navigate to Properties > Settings and copy the **Id** under **Essentials** Section.
6. Enter the Event Hub name to stream the Defender for Endpoint logs.
7. Select the types of events that the raw data streaming API senses and click **Save**.

Properties

Essentials	Encryption
Id: /subscriptions/...	Copy to clipboard
Name: jb-emitter-arcsgt	Key vault properties
Type: Microsoft.EventHub/Namespace	Key source
Location: East US	Require infrastructure enc...
Tags: View value as JSON	
SKU: View value as JSON	
Identity: ...	
System data: ...	

Properties

Provisioning state: Succeeded
Status: Active
Created at: 12/23/2022, 1:10:43 PM
Updated at: 3/9/2023, 10:06:26 AM
Service bus endpoint: https://...
Cluster arm id: ...
Metric id: ...
Is auto inflate enabled: false
Maximum throughput units: 0
Kafka enabled: true
Zone redundant: false
Private endpoint connecti...: ...
Disable local auth: false

Note: This data source is for ArcSight Intelligence only and is specific to the current release.

Installing the SmartConnector

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, ensure that you have the following:

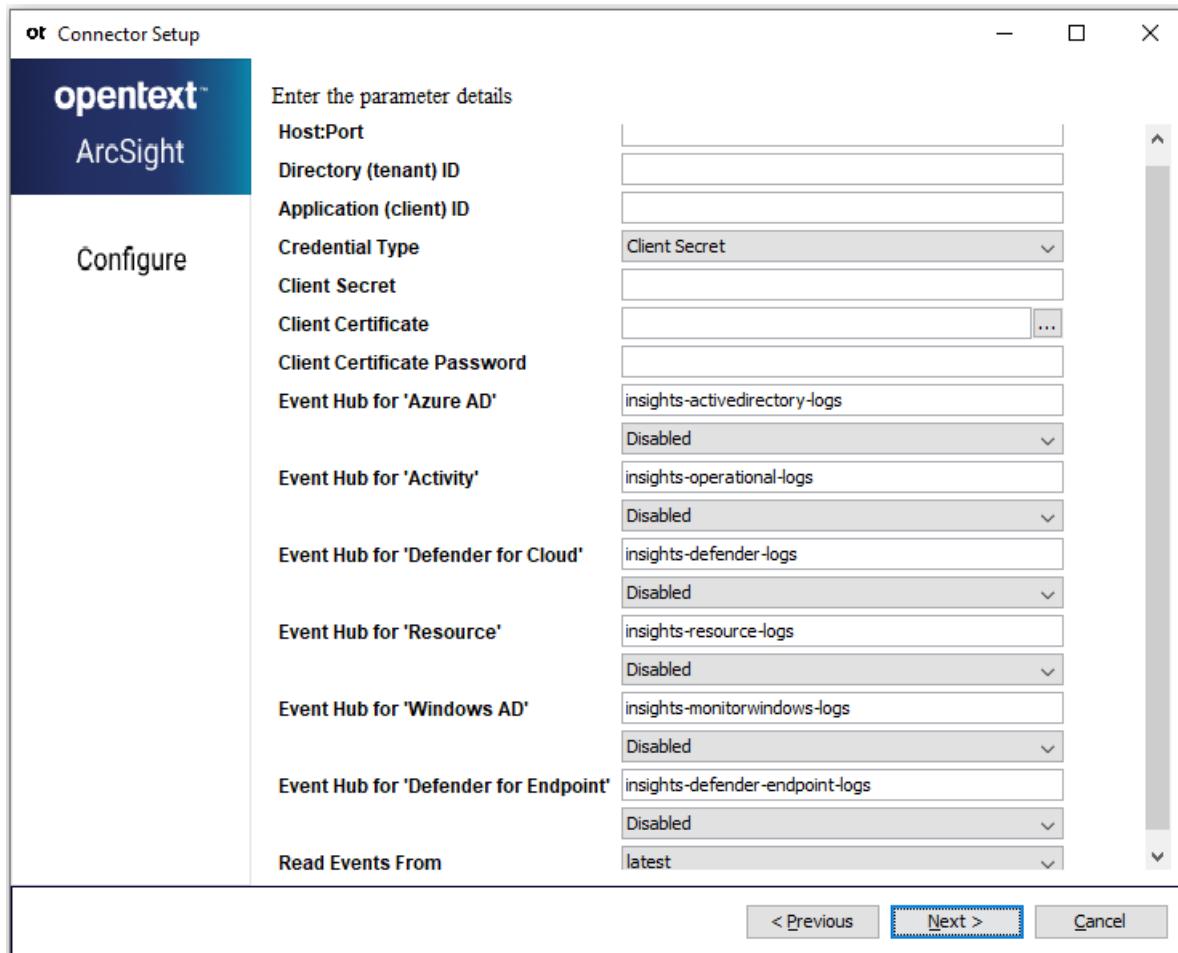
- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the Microsoft Azure Event Hub SmartConnector. For detailed installation steps or for manual installation steps, see [Installation and User Guide for SmartConnector](#).

To install and configure the Azure Event Hub connector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. From the **Type** drop-down list, select **Microsoft Azure Event Hub** as the type of connector, then click **Next**.
5. Enter the following SmartConnector parameter values, then click **Next**:



Parameters	Description
Host:Port	Enter the host and port of Event Hubs Namespace. Select the Event Hub from the Event Hub Namespace list and copy the host value from the Overview section. The recommended port value is 9093.
Directory (tenant) ID	Enter the Directory (tenant) ID of your registered application. For this value, refer to the Overview section of the application.
Application (Client) ID	Enter the Client ID generated for your registered application. For this value, refer to the Overview section of the application.
Credential Type	If Client secret is selected, then client secret will be used to authenticate the app. If Client certificate is selected, then client certificate will be used to authenticate the app

Parameters	Description
Client Secret	Enter the client secret value generated as mentioned in step 2 . This value is obfuscated. This field is mandatory if the Credential Type is Client secret. For detailed information, see Troubleshooting .
Client Certificate	Specify the client certificate path. This field is mandatory if the Credential Type is Client certificate. For detailed information, see Troubleshooting .
Client Certificate Password	Enter the password of client certificate.
Event Hub for 'Azure AD'	Enter the event hub name for Azure AD.
Event Hub for 'Activity'	Enter the event hub name for Activity.
Event Hub for 'Defender for Cloud'	Enter the event hub name for Defender for Cloud.
Event Hub for 'Resource'	Enter the event hub name for Resource.
Event Hub for 'Windows AD'	Enter the event hub name for Windows AD.
Event Hub for 'Defender for Endpoint'	Enter the event hub name for Defender for Endpoint.
Read Events From	Specify the value from where the connector will read the events.

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).
12. For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).



Note: For the Defender for Endpoint events, ensure to enable the **Preserve Raw Event** option while configuring the destination. Refer the steps mentioned here under [Configuring Processing in Configuring Destination Settings](#).

Adding Support for New Log Sources

The Microsoft Azure Event Hub SmartConnector supports new log sources because it is flexible in the parser loading technique without needing any code changes.. Most of the Azure activities go through the Microsoft Azure Monitor Event Hub by following the standard schema and reach Event Hub.

Supported Log Sources

The Microsoft Azure Event Hub SmartConnector supports logs with the following conditions without having any framework changes:

All events that are sent to Event Hub must be specified within the "records" key containing the "category" key. The events must be in the Json format.

```
{  
    "records": [  
        {  
            "key1": "Value1",  
            "key2": "Value2",  
            ...  
            "Key n": "Value n"  
        },  
        {  
            "key1": "Value1",  
            "key2": "Value2",  
            ...  
            "Key n": "Value n"  
        },  
        ...  
        ...  
        {  
            "key1": "Value1",  
            "key2": "Value2",  
            ...  
            "Key n": "Value n"  
        }  
    ]  
}
```

Event 1

Event 2

Event n

```
{  
    "records": [  
        {  
            "key1": "value1"  
            "category": "someCategoryValue"  
            ...  
            "key n": "value n"  
        },  
        .  
        .  
        .  
        {  
            "key1": "value1"  
            "category": "someCategoryValue"  
            ...  
            "key n": "value n"  
        }  
    ]  
}
```

The diagram illustrates the structure of a JSON object representing multiple events. The outermost curly brace groups the entire object. Inside, the key "records" points to an array of objects. Each object in the array represents an event. The first event is labeled "Event 1" and the second is labeled "Event n". Each event object contains several key-value pairs. A yellow box highlights the "category" field in both the first and second event objects, indicating its significance.

Adding Support for New Log Sources

Perform the following steps to add support for the new log sources:

1. Create a Json parser and then create the mappings. The value specified for the "**category**" field is considered as a name of the parser file.
For example, if the raw event appears as follows, then the parser file name will be `riskyusers.jsonparser.properties`.

```
{
    "key1": "value1",
    "category": "RiskyUsers",
    ...
    "key n": "value n"
}
```

Event 1



Note: Ensure that the parser file name is in lower case.

2. Perform the following steps to override a parser file:
 - a. Download ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-X.X.X.XXX.X.zip file.
 - b. Unzip the downloaded file to a temporary location.
 - c. Locate and copy the **azureeventhub** folder to <ARCSIGHT_HOME>/current/user/agent/fcp/.
 - d. Delete the unzipped directory from a temporary location.

The directory structure appears as follows:

Name	Date modified	Type	Size
activedirectory		File folder	
activity		File folder	
defendercloud		File folder	
defenderendpoint		File folder	
resource		File folder	
windowsad		File folder	

3. The Event Hubs are created at this step. Choose the Event Hub you want to send the data to and create your data collection rules as required.
4. Event Hubs and directories mentioned in [Step 1](#) are directly related. Copy the parser file in the directory that is related to the event hub to which you are sending the data.

The following table describes the relation between the parser folder and event hubs:

If data is sent to	Folder to copy a Parser file
Event Hub for 'Azure AD'	activedirectory
Event Hub for 'Resource'	resource
Event Hub for 'Activity'	activity
Event Hub for 'Defender for Cloud'	defendercloud



Note: Do not send the data to Event Hubs that are created for **Windows AD or Defender for Endpoint**.

5. Restart the connector.

The connector will start processing the events.

Configuring Advanced Parameters

Accessing Advanced Parameters

After installing the SmartConnector, you can edit the `agent.properties` file to modify the parameters. This file is located at `$ARCSIGHT_HOME\current\user\agent` directory.

1. Advanced Kafka Configuration Parameters

Parameter	Default	Specify
consumerthreadcount	1	Number of Kafka consumer threads that will be spawned to read data from Azure Event Hub.
offset.async.commit	true	Offset commit mechanism used by the Kafka Consumer.
groupid	kafkabusgroupid	Parameter that is used to identify the consumer group to which a consumer belongs.
polltimeout	50 ms	Maximum amount of time a Kafka consumer will wait for new messages to arrive from a Azure Event Hub before returning the control to the calling application.
maxpollrecords	500	Maximum number of records a consumer can fetch in a single poll request.
maxpartitionfetchbytes	1048576 Bytes	Maximum number of bytes that a consumer can fetch from a single partition in a single request.
reconnectbackoffms	50 ms	Amount of time that a Kafka client should wait before attempting to reconnect to a broker after a connection failure.
retrybackoffms	100 ms	Amount of time a Kafka client should wait before retrying a failed operation.
requesttimeoutms	40,000 ms	Maximum amount of time Kafka client will wait for a response from the Azure Event Hub before considering the request as failed.
heartbeatintervalms	3000 ms	Interval at which Kafka consumer will send heartbeats to the broker to indicate that it is still alive and processing messages.
connectionsmaxidlems	540,000 ms	Specifies the maximum amount of time a connection can remain idle before it is closed by the broker.

2. Advanced Performance Tuning Parameters

Parameter	Default	Specify
consumerthreadcount	1	The number of Kafka consumer threads that will be spawned to read data from Azure Event Hub. This number of threads must be kept equal to number of partitions you have in Event Hub for optimal performance.
offset.async.commit	true	Offset commit mechanism used by the Kafka Consumer. The default is Asynchronous commit which gives a better performance. If changed to Synchronous commit by setting the parameter value as false, the performance will decrease.

For more performance scaling options for Azure Event Hub, refer to this [Microsoft documentation](#).

Additional Connector Configuration for Defender for Endpoint Data Source

Connector limits the character length of the rawEvent field

The Microsoft Azure Event Hub connector currently limits the character length of the rawEvent field to 4000 for Microsoft Defender for Endpoint Data Source. The rawEvent field was getting truncated in the following scenarios:

- If the value exceeds 4000 characters from the connector side.
- If the value exceeds 16384 characters from the Avro output side with Amazon S3 as destination.

Workaround:

To increase the size of the raw event field:

1. Search for the following properties in agent.defaults.properties file under the \$ARCSIGHT_HOME\current\config\agent folder:
 - `size.validation.fields = field1, field2, field3...`
 - `size.validation.sizes = size1, size2, size3...`

In the agent.properties file, override the value of the rawEvent field to 1048576 in size.validation.sizes. Refer size.validation.fields to identify the value corresponding to rawEvent in size.validation.sizes. For more information, see [Overriding a default property](#).

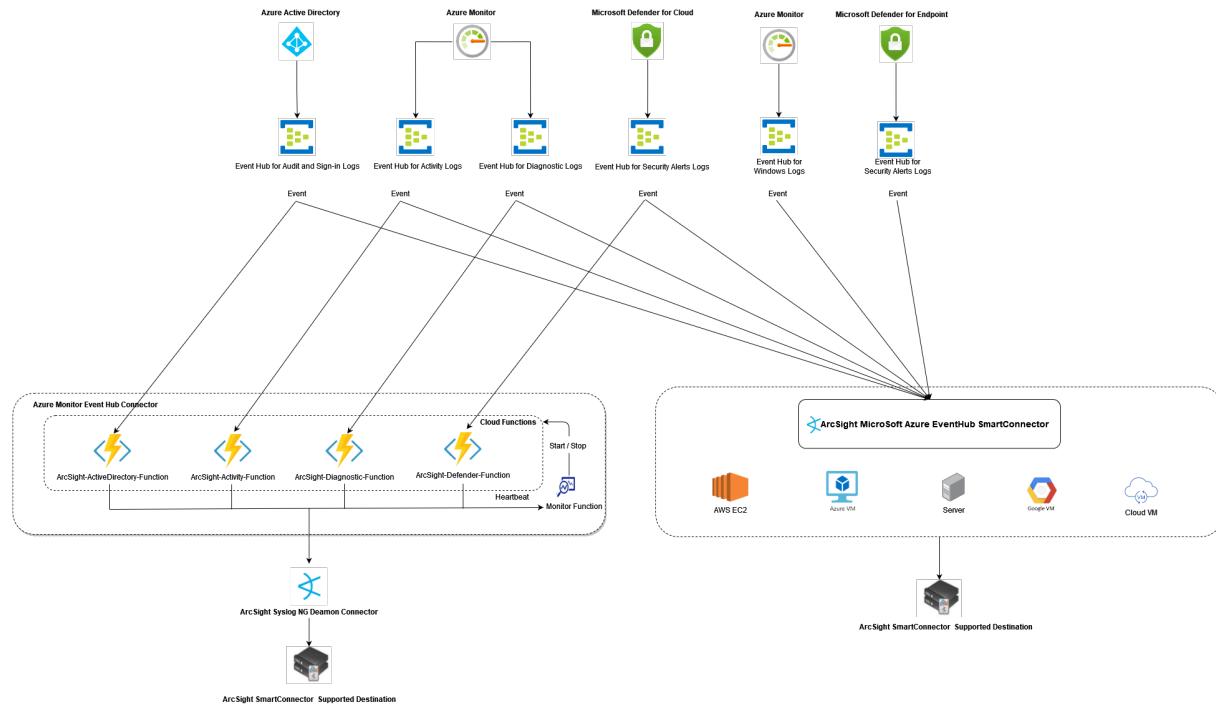
2. Browse the directory to find the \$ARCSIGHT_HOME\current\user\agent\avroschema\avro_schema_202111_1.2.0.avsc file and update the rawEvent maxLength to 1048576.
3. Restart the connector.



Note: \$ARCSIGHT_HOME in the file name is a placeholder and the value will depend on the standard reference for path.

Migrating the SmartConnector

The following diagram provides a high-level overview of the migration from the Azure Monitor Event Hub Connector to the Microsoft Azure Event Hub SmartConnector:



The following steps must be implemented for migrating from the Azure Monitor Event Hub Connector to Microsoft Azure Event Hub SmartConnector:

1. Stop the Azure Monitor Event Hub connector instance.
2. In the Azure portal, reuse the existing Resource group, Event Hub Namespace and Event hubs that were created for Azure AD logs, Activity logs, Resource logs and Defender for Cloud logs as part of the existing deployment. Delete all other resources that were created manually. Do not run the undeployment script as it will delete all the resources.
3. Windows AD logs and Defender for Endpoint logs are supported as part of the Microsoft Azure Event Hub SmartConnector.
Refer to this [section](#) for creating the Event Hubs. Also, see [here](#) for streaming the logs to the respective Event Hubs.
4. For creating Event Hubs and streaming logs refer to the following table for the Supported Logs:

Microsoft Azure Monitor Event Hub Connector		Microsoft Azure Event Hub Connector
Azure AD		Azure AD For more information, refer Product Overview .
Activity		Activity
Resource		Resource
Defender for Cloud		Defender for Cloud
		Windows AD For more information, refer Product Overview .
		Defender for Endpoint

5. In the Azure portal, register an application and assign IAM role to the application with these [steps](#).
6. Install the Microsoft Azure Event Hub SmartConnector and configure the Event Hubs based on the required Event Types as mentioned [here](#).



Note: The destination must be the same that was selected initially while configuring the Syslog NG SmartConnector with the same parameters for reusing the destination.

7. The Microsoft Azure Event Hub SmartConnector outputs the Avro files in S3 bucket and formats it in a similar way to the Microsoft Azure Monitor Event Hub Connector (This is done using a Syslog connector). When configuring the destination, select the same S3 bucket while collecting the data.
8. Start the SmartConnector. It will start processing the events and send it to the configured ArcSight destination.

Prevention of Data Loss

The ArcSight Microsoft Azure Event Hub SmartConnector reads the data from latest offset from event hubs. After the connector starts, all the events that reach the Event hub will be received.

By the time the installation of the Microsoft Azure Event Hub SmartConnector completes, the Microsoft Azure Monitor Event Hub Connector stops. Henceforth, to avoid the data loss, the following steps must be implemented:

1. Stop the streaming of data to existing Event Hubs.
2. All the events must be read which means you must wait till the Syslog NG connector's EPS becomes zero.
3. Run the Undeployment Script and remove the Syslog NG SmartConnector. Only the Resource Group will remain after running the Undeployment script, which can be reused in the next step.
4. Create new Event Hubs and Event Hubs Namespace.
Configure the data sources to stream to the new Event Hubs.
5. Install and configure the ArcSight Microsoft Azure Event Hub SmartConnector to use new Event Hubs created in step 3 based on the Event Types.
While Installing, ensure to set the offset to **Earliest** and to read all the events that reach the Event Hubs.
6. Start the SmartConnector.

Hardware Consideration

The following table provides insights on resources consumed during the testing environment that was done on 8 core 16 GB RHEL box:

Event Size	EPS Processed	Tested Hardware	CPU Utilization	Memory Utilization (approx.)
1 K	10 K	8 core 16 GB	8%	500 MB
1 K	25 K	8 core 16 GB	34%	700 MB
2.2 K	5 K	8 core 16 GB	8%	600 MB
2.2 K	10 K	8 core 16 GB	25%	700 MB

The hardware resources consumed by the connector are based on the size of event and the number of EPS being processed by the connector.

When the event size is increased for the same EPS, both CPU and memory consumption increase. If the EPS is increased with a constant event size, both CPU and memory consumption increase. The resource consumption increases for higher event size and higher EPS.



Note: During production you must ensure that the connector is not consuming more than 75% of host resources.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the ArcSight Console User's Guide for more information about the ArcSight data fields.

Event Mappings for Active Directory

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Class ID	operationName
Device Product	Azure Active Directory
Device Vendor	Microsoft
Name	operationName
Severity	Level

Sign-in Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Application Protocol	properties/clientAppUsed
Destination Process Name	properties/appDisplayName
Destination User ID	properties/userId
Destination User Name	properties/userDisplayName
Device Custom Date 1	properties/createdDateTime
Device Custom Floating Point 1	properties/location/geoCoordinates/latitude
Device Custom Floating Point 2	properties/location/geoCoordinates/longitude
Device Custom String 1	properties/deviceDetail/operatingSystem
Device Custom String 2	properties/isRisky
Device Custom String 3	properties/location
Device Custom String 4	location
Device Custom String 5	correlationId

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	properties/userPrincipalName
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
External ID	properties/id
Reason	resultDescription
Request Client Application	properties/deviceDetail/browser
Source Address	callerIpAddress

Audit Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	properties/targetResources/userPrincipalName
Device Event Category	properties/category
Device Custom String 1	properties/identityType
Device Custom String 2	properties/operationType
Device Custom String 3	properties/targetResources/modifiedProperties (Role.DisplayName)/displayName(Role.DisplayName)
Device Custom String 5	correlationId
Device Custom String 6	properties/targetResources
Device Receipt Time	time
Event Outcome	resultType
External ID	properties/id
File Hash	properties/targetResources/modifiedProperties (Role.DisplayName)/newValue(Role.DisplayName)
File Name	properties/targetResources/modifiedProperties (Group.DisplayName)/newValue(Group.DisplayName)
File Path	properties/targetResourceName
File Type	properties/targetResourceType
Old File Hash	properties/targetResources/modifiedProperties (Role.DisplayName)/oldValue(Role.DisplayName)
Old File Name	properties/targetResources/modifiedProperties (Group.DisplayName)/oldValue(Group.DisplayName),

ArcSight ESM Field	Device-Specific Field
Reason	resultDescription
Source Address	callerIpAddress
Source User ID	properties/initiatedBy/user/id,
Source User Name	properties/initiatedBy/user/userPrincipalName

Event Mappings for Microsoft Defender for Cloud

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Name	AlertDisplayName
Device Event Class ID	AlertType
Severity	Severity

Security Alerts Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	AlertType
Destination Host Name	CompromisedEntity, Entities/HostName
Device Custom Date 1	ProcessingEndTime
Device Custom Number 1	Entities/\$id
Device Custom String 1	ExtendedProperties
Device Custom String 2	IsIncident
Device Custom String 3	ResourceIdentifiers
Device Custom String 4	AlertUri
Device Custom String 5	Entities/Location/Asn & Entities/Location/CountryCode & Entities/Location/CountryName & Entities/Location/State & Entities/Location/City & Entities/Location/Longitude & Entities/Location/Latitude
Device Receipt Time	TimeGenerated
Device Severity	Severity
End Time	EndTimeUtc

ArcSight ESM Field	Device-Specific Field
Event Outcome	Status
External ID	SystemAlertId
File Path	AzureResourceId, Entities/AzureID, Entities/ResourceId
File Type	Entities/Type
Message	Description & RemediationSteps
Reason	Intent
Start Time	StartTimeUtc
Source Address	Entities/Address

Security Recommendations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	type
Device Action	assessmentEventDataEnrichment/action
Device Custom String 1	properties/metadata/policyDefinitionId
Device Custom String 2	properties/metadata/threats
Device Custom String 4	properties/links/azurePortal
Device Severity	properties/metadata/severity
File Name	file
File Path	ID
Message	properties/metadata/description & properties/metadata/remediationDescription
Name	properties/displayName
Event Outcome	properties/status/code
Reason	properties/status/cause

Event Mappings for Activity

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Name	operationName
Device Event Class ID	operationName
Severity	level

Action Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Port	properties/eventProperties/destinationPort
Destination Host Name	resourceId, properties/eventProperties/machineName
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Custom Date 1 Label	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/eventProperties, properties/policies
Device Custom String 3	properties/eventProperties/title
Device Custom String 4	location
Device Custom String 5	correlationId
Device Custom String 6	properties/isComplianceCheck
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
External ID	eventDataId
File Hash	properties/eventProperties/fileSha256
File Path	resourceId, properties/eventProperties/filePath
File Name	properties/eventProperties/fileName
File Type	resourceType, properties/eventProperties/type

ArcSight ESM Field	Device-Specific Field
Message	description
Old File Type	properties/eventProperties/resourceType
Reason	properties/eventProperties/cause
Request Client Application	properties/eventProperties/compromisedEntity
Source Address	callerIpAddress
Source Service Name	properties/eventProperties/attackedResourceType
Transport Protocol	properties/eventProperties/protocol

Administrative Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Action	identity/authorization/action
Device Custom Number 1	durationMs
Device Custom String 1	resultSignature
Device Custom String 4	location
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
File Path	resourceId
Message	identity/claims
Request Client Application	identity/claims/iss
Request URL	identity/claims/aud
Source Address	callerIpAddress

Alert Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom Number 1	properties/Threshold
Device Custom Number 2	properties/WindowSizeInMinutes
Device Custom String 1	properties/RuleUri, subStatus
Device Custom String 2	properties/RuleName
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
Event Outcome	status
External ID	eventDataId
File Path	resourceId
File Type	resourceType
Message	description

Delete Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Privileges	identity/authorization/evidence/role
Destination User Name	identity/claims/name
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	correlationId
Device Custom String 4	location
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
File Type	resourceType
Event Outcome	resultType

ArcSight ESM Field	Device-Specific Field
External ID	eventDataId
Message	description
Source Address	callerIpAddress

Recommendation Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/recommendationCategory
Device Custom String 3	properties/recommendationImpact
Device Custom String 4	properties/recommendationRisk
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
Event Outcome	status
External ID	eventDataId
File Path	resourceId
File Type	resourceType
Message	description

Security Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Process ID	properties/processId
Destination Process Name	properties/processName
Destination NT Domain	properties/domainName
Destination User ID	properties/accountLogonId
Destination User Name	caller, properties/username
Device Action	properties/ActionTaken

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/UserSID
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
External ID	eventDataId
Event Outcome	status
File Path	resourceId
File Type	resourceType
Message	description

Service Health Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Service Name	properties/impactedServices
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom String 1	properties/trackingId
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
External ID	eventDataId
Event Outcome	status
File Path	resourceId
File Type	resourceType
Message	description
Start Time	properties/impactStartTime
Reason	properties/communication

Write Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 4	location
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	time
External ID	eventDataId,
Event Outcome	properties/statusCode
File Path	resourceId
File Type	resourceType
Source Address	callerIpAddress

Event Mappings for Resource Log

Common Event Mapping

Device Event Mapping	ArcSight Fields
Name	operationName
Device Event Class ID	operationName
Severity	Level

App Service HTTP Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Additional Data Event Primary Stamp Name	EventPrimaryStampName
Additional Data Event Stamp Name	EventStampName
Additional Data Event Stamp Type	EventStampType

Bytes In	Properties/csbytes
Bytes Out	Properties/scbytes
Destination Address	Properties/CIP
Destination Hostname	Properties/cshost
Destination User Name	Properties/csusername
Device Custom Floating Point 1	Properties/timetaken
Device Custom Floating Point 1 Label	Time Taken
Device Custom Number 2	Properties/scstatus
Device Custom Number 2 Label	Status code
Device Event Category	Category
Device Event Class ID	Category
Device Hostname	Properties/computername
Device Product	Azure
Device Receipt Time	Time
Device Vendor	Microsoft
Event Outcome	Properties/result
File Path	Resourceid
Name	Category
Request Client Application	Properties/useragent
Request Method	Properties/Csmethod
Source Hostname	Host
Source Port	Properties/sport
Application Protocol	Properties/protocol

App Service IP Sec Audit Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Ad.serviceendpoint	Service endpoint
Destination Address	CIP
Destination Hostname	CsHost
Device Event Category	Category
Device Event Class ID	Operation Name

Device Product	Azure
Device Receipt Time	Time
Device Vendor	Microsoft
Event Outcome	Result
File Path	ResourceId
Message	Details
Name	OperationName
Source Address	XForwardedFor
Source Hostname	XForwardedHost

Activity Runs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 2	Error
Device Custom String 5	correlationId
Device Receipt Time	time
External ID	activityRunId
File ID	pipelineRunId
File Path	resourceId
File Name	pipelineName
Destination Process Name	activityName
Start Time	start
End Time	end
Message	Output

Application Gateway Access Log Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
Device External ID	instanceId

ArcSight ESM Field	Device-Specific Field
Source Address	properties/clientIP
Source Port	properties/clientPort
Request URL	properties/requestUri
Request Client Application	properties/userAgent
Event Outcome	properties/httpStatus
Bytes In	properties/receivedBytes
Bytes Out	properties/sentBytes
Device Custom Floating Point 1	properties/timeTaken
Device Custom String 1	properties/sslEnabled

Archive Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
External ID	ActivityId
Device Custom String 1	trackingId
Device Custom String 2	archiveStep
File Path	resourceId
File Name	eventHub
Start Time	startTime
Device Custom Number 1	failures
Device Custom Number 2	durationInSeconds
Message	message

Audit Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Event Outcome	resultType

ArcSight ESM Field	Device-Specific Field
Source Address	callerIpAddress
Destination User ID	identity
Device Custom String 1	properties/JobId
Device Custom String 2	properties/JobRunTime
Device Custom String 5	correlationId
Destination Process Name	properties/JobName
Start Time	properties/StartTime
End Time	properties/EndTime

Authoring Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Event Outcome	status
Device Receipt Time	time
Device Custom String 1	properties/Error
Device Custom String 5	properties/correlationId
Message	properties/Message
Reason	properties/Type

Automatic Tuning Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
File Path	ResourceId

Azure Firewall Application Rule Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceid
Message	properties/smrg

Azure Firewall Network Rule Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceid
Message	properties/smrg

Azure Site Recovery Jobs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Event Outcome	properties/resultType
Message	properties/resultDescription
Start Time	properties/startTime
End Time	properties/endTime
Device Custom String 2	properties/affectedResourceType
Device Custom String 3	properties/affectedResourceId
Device Custom String 5	properties/correlationId

Blocks Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	duration_d
File Path	ResourceId
Destination User Name	resource_owner_type_s

C2D Command , C2D Twin Operations, and D2C Twin Operations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Database Wait Statistics Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	delta_wait_time_ms_d
Device Custom Number 2	delta_waiting_tasks_count_d
File Path	ResourceId

Deadlocks Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	duration_d
File Path	ResourceId
Destination User Name	resource_owner_type_s

Engine Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
File Path	resourceId
Device Event Category	category
Start Time	properties/StartTime
Device Custom String 1	properties/ObjectID
Device Custom String 2	properties/ObjectType
Device Custom String 3	properties/ObjectName
Device Custom String 4	properties/ObjectPath
Device Custom String 5	properties/ObjectReference
End Time	properties/EndTime
Event Outcome	properties/Success
Device Custom Number 1	properties/ConnectionID
Device Custom Number 2	properties/SPID
Source NT Domain	properties/NTDomainName
Source Host Name	properties/ClientHostName
Source Process ID	properties/ClientProcessID
Device Custom String 6	properties/ApplicationName
Destination User Name	properties/User
Destination Service Name	properties/ServerName

Errors Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
File Path	ResourceId
Message	Message
Event Outcome	state_d
Reason	error_number_d

Gateway Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
Device Custom Number 1	durationMs
Device Custom String 2	location
Source Address	callerIpAddress
Request URL Method	properties/method
Request URL	properties/url
Event Outcome	properties/responseCode

Job Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	TimeGenerated
File Name	RunbookName_s
Destination User Name	Caller_s
Device Custom String 1	resourceId
Device Custom String 2	resourceGroup
Device Custom String 3	Tenant_g
Device Custom String 5	correlationId
File ID	JobId_g
Event Outcome	ResultType
Device Event Category	category

Jobs Operations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Load Balancer Alert Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Device Custom String 1	systemId
File Path	resourceId
Reason	properties/eventDescription
Destination Address	properties/eventProperties/public ip address

Network Security Group Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Destination MAC Address	properties/macAddress
Destination Address	properties/primaryIPv4Address
Device Custom String 1	properties/subnetPrefix

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	properties/ruleName
Device Custom String 3	properties/direction
Device Custom String 4	properties/priority
Device Custom String 5	properties/type
Message	properties/conditions
Transport Protocol	properties/conditions/protocols

Operational Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
File Path	resourceId
Device Custom String 1	subscriptionId
Device Custom String 4	Region
Device Receipt Time	EventTimeString
Message	EventProperties
Event Outcome	Status
Source Process Name	Caller
External ID	ActivityId

P2S Diagnostic Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Message	properties/message
Device External ID	properties/instance

Postgre SQL Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Device Custom String 3	ResourceGroup
Device Custom String 2	SubscriptionId
Source Service Name	LogicalServerName
Message	properties/message

Query Store Wait Statistics Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 1	TenantId
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	total_query_wait_time_ms_d
File Path	resourceId

Requests Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId

ArcSight ESM Field	Device-Specific Field
Event Outcome	resultType
Source Address	callerIpAddress
Destination Use ID	identity
Request Method	properties/HttpMethod
Request URL	properties/Path
Bytes In	properties/RequestContentLength
External ID	properties/ClientRequestId
Start Time	properties/StartTime
End Time	properties/EndTime

Routes Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Service Log Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Tenant
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
External ID	properties/id
File Type	properties/imageType

Timeouts Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Azure Logical Server Name_s	LogicalServerName_s
Azure Elastic Pool Name_s	ElasticPoolName_s
CS 4 Label	DatabaseName_s
File Path	ResourceId

Trigger Runs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 2	triggerEvent
Device Custom String 5	correlationId
Device Receipt Time	time
External ID	activityRunId
File Path	resourceId
File Name	pipelineName
Destination Process Name	activityName
Start Time	start
End Time	end
File ID	triggerId
File Type	triggerType

Twin Queries Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Device Custom Number 1	durationMs
Device Custom String 1	properties
Device Custom String 2	location
Event Outcome	resultType
File Path	resourceId
Message	resultDescription

Workflow Runtime Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Reason	code
Event Outcome	properties/status
Start Time	properties/startTime
End Time	properties/endTime
Device Custom String 1	properties/resource/subscriptionIdEndpoint
Device Custom String 2	properties/resource/resourceGroupName
Device Custom String 4	properties/resource/location
Device Action	properties/resource/actionName
File Name	properties/resource/workflowName

Event Mappings for Windows AD

Event 4624

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

Event 4625

OpenText ArcSight ESM Field	Device-Specific Field
Destination NT Domain	TargetDomainName
Destination Process Name	ProcessName
Destination User ID	“”
Destination UserName	TargetUserName
Device Custom Number 1	LogonType
Device Custom String 1	SubStatus
Device Custom String 3	ProcessId
Device Custom String 4	FailureReason
Device Custom String 5	AuthenticationPackageName
Device NT Domain	SubjectDomainName
Device Process Name	LogonProcessName
Message	<p>'This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request.</p> <ul style="list-style-type: none"> - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.'
Name	'An account failed to log on.'
Reason	FailureReason
Source Address	IpAddress
Source Host Name	WorkstationName
Source Port	IpPort
Source Process Name	ProcessId

Event 4648

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

Event 4656

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

OpenText ArcSight ESM Field	Device-Specific Field
File ID	HandleId
File Name	ObjectName
File Type	ObjectType

Event 4663

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

Event 4664

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

Event 4674

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

Event 4688

OpenText ArcSight ESM Field	Device-Specific Field
Name	'A new process has been created.'
Destination User Name	One of (SubjectUserName, SubjectUserSid, TargetUserName, TargetUserSid)
Destination NT Domain	One of (SubjectDomainName, desinationNtDomain)
Destination User ID	One of (SubjectLogonId, TargetLogonId)
Device Custom String 1	MandatoryLabel
Device Custom String 3	NewProcessId
Device Custom String 6	TokenElevationType
Device Custom String 5	ProcessId
Device Custom String 4	CommandLine
Destination Process Name	NewProcessName

OpenText ArcSight ESM Field	Device-Specific Field
Device NT Domain	SubjectDomainName
File Path	ParentProcessName
Message	'Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. Type 2 is an elevated token with no privileges removed or groups disabled. Type 3 is a limited token with administrative privileges removed and administrative groups disabled.'

Event 4768

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

Event 4769

OpenText ArcSight ESM Field	Device-Specific Field
Destination Nt Domain	TargetDomainName
Destination Service Name	ServiceName
Destination User Name	TargetUserName
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)

OpenText ArcSight ESM Field	Device-Specific Field
Device custom String 1	TicketOptions
Device custom String 1 Label	Ticket Options
Device custom String 3	IpAddress
Device Custom String 4	Status
Device Custom String 5	TicketEncryptionType
Device Custom String 6	LogonGuid
File Name	ServiceSid
Message	This event is generated every time access is requested to a resource such as a computer or a Windows service. The service name indicates the resource to which access was requested. This event can be correlated with Windows logon events by comparing the Logon GUID fields in each event. The logon event occurs on the machine that was accessed, which is often a different machine than the domain controller which issued the service ticket. Ticket options, encryption types, and failure codes are defined in RFC 4120.
Name	A Kerberos service ticket was requested.
Source Address	IpAddress
Source Port	IpPort

Event 4770

OpenText ArcSight ESM Field	Device-Specific Field
Destination Nt Domain	TargetDomainName
Destination Service Name	ServiceName
Destination User Name	TargetUserName
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device custom String 3	IpAddress
Message	Ticket options and encryption types are defined in RFC 4120.
Name	A Kerberos service ticket was renewed.
Source Address	IpAddress
Source Port	IpPort

Event 4771

OpenText ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device custom String 3	IpAddress
Source Address	IpAddress

Event 4772

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

Event 4773

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

Event 4776

OpenText ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Device Custom String 4	Status
Device Custom String 5	PackageName
Name	The domain controller attempted to validate the credentials for an account.
Reason	Status
Source Host Name	Workstation

Event 4777

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

Event 5137

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

Event 5139

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

Event 5140

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

Event 5141

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

Event 5145

OpenText ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom String 1	AccessList
Device Custom String 6	ShareName
Device NT Domain	SubjectDomainName
File Name	RelativeTargetName
File Path	ShareLocalPath
Name	'A network share object was checked to see whether client can be granted desired access.'
Source Address	IpAddress
Source NT Domain	SubjectDomainName
Source Port	IpPort
Source User ID	SubjectLogonId

Event 6272

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

Event 6273

OpenText ArcSight ESM Field	Device-Specific Field
Destination Address	NASIPv4Address
Destination NT Domain	SubjectDomainName
Destination Port	NASPort
Destination User ID	FullyQualifiedSubjectUserName
Destination User Name	SubjectUserName
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIPAddress
Device Custom String 4	Reason
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier

OpenText ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server denied access to a user. Contact the Network Policy Server administrator for more information.'
Source Address	CallingStationID
Source User ID	FullyQualifiedSubjectMachineName
Source User Name	SubjectMachineName

Event 6274

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

Event 6275

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

Event 6276

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

Event 6277

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

Event 6278

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

For information regarding the Common Event Mappings, refer to the [Windows Common Security Mappings](#) section of the *SmartConnector for Microsoft Windows Event Log - Native Configuration Guide*.

Event Mappings for Defender for Endpoint

AlertEvidence

ArcSight ESM Field	Device-Specific Value
Destination Address	Remoteip
Destination User ID	AccountSid
Destination User Name	AccountName
Device Address	LocalIP
Device Custom String 1	ThreatFamily

ArcSight ESM Field	Device-Specific Value
Device Custom String 1 Label	ThreatFamily
Device Custom String 2	AlertId
Device Custom String 2 Label	AlertId
Device Custom String 3	EvidenceRole
Device Custom String 3 Label	EvidenceRole
Device Custom String 4	AttackTechniques
Device Custom String 4 Label	AttackTechniques
Device Custom String 5	TenantId
Device Custom String 5 Label	Tenant Id
Device Event Category	Type
Device Event Class ID	Categories
Device External ID	DeviceId
Device Facility	ServiceSource
Device Host Name	DeviceName
Device Nt Domain	AccountDomain
Device Process Name	DetectionSource
File Hash	SHA1
File Type	entityType
Name	Title
Request Url	RemoteUrl
Start Time	Timestamp

AlertInfo

ArcSight ESM Field	Device-Specific Value
Device Custom String 4 label	AttackTechniques
Device Custom String 2	AlertId
Device Custom String 2 label	AlertId
Device Custom String 4	AttackTechniques
Device Custom String 5	TenantId
Device Custom String 5 label	Tenant Id

ArcSight ESM Field	Device-Specific Value
Device Event Category	Type
Device Event Class Id	Category
Device Facility	ServiceSource
Device Process Name	DetectionSource
Device Severity	Severity
Name	Title
Start Time	TimeStamp

DeviceFileEvents

ArcSight ESM Field	Device-Specific Value
Application Protocol	RequestProtocol
Device Custom Number 2	ReportId
Device Custom Number 2 Label	ReportId
Device Custom String 2	InitiatingProcessCommandLine
Device Custom String 2 Label	InitiatingProcessCommandLine
Device Custom String 3	ResquestAccountDomain
Device Custom String 3 Label	ResquestAccountDomain
Device Custom String 5	TenantId
Device Custom String 5 Label	TenantId
Device Event Category	Type
Device Event Class ID	ActionType
Device External ID	DeviceId
Device Host Name	DeviceName
Device Process Name	InitiatingProcessFileName
File Hash	SHA1
File Name	FileName
File Path	FolderPath
File Size	FileSize
Name	ActionType
Old File Hash	InitiatingProcessSHA1

ArcSight ESM Field	Device-Specific Value
Old File Name	InitiatingProcessFileName
Old File Path	InitiatingProcessFolderPath
Old File Size	InitiatingProcessFileSize
Source Nt Domain	InitiatingProcessAccountDomain
Source Process ID	InitiatingProcessId
Source User Name	InitiatingProcessAccountName
Start Time	Timestamp

DeviceImageLoadEvents

ArcSight ESM Field	Device-Specific Value
Device Custom String 2	InitiatingProcessCommandLine
Device Custom String 2 Label	InitiatingProcessCommandLine
Device Custom String 5	TenantId
Device Custom String 5 Label	TenantId
Device Event Category	type
Device Event Class ID	Action type
Device External ID	DeviceId
Device Host Name	DeviceName
File Hash	SHA1
File Name	FileName
File Path	FolderPath
File Size	FileSize
Name	Action type
Old File Hash	InitiatingProcessSHA1
Old File Name	InitiatingProcessFileName
Old File Path	InitiatingProcessFolderPath
Old File Size	InitiatingProcessFileSize
Source Nt Domain	InitiatingProcessAccountDomain
Source User ID	InitiatingProcessAccountSid

ArcSight ESM Field	Device-Specific Value
Source User Name	InitiatingProcessAccountName
Source Process ID	InitiatingProcessId
Start Time	TimeGenerated

DeviceInfo

ArcSight ESM Field	Device-Specific Value
Destination Address	PublicIP
Device Custom Date 1	InternetFacingLastSeen
Device Custom Date 1 Label	InternetFacingLastSeen
Device Custom Number 1	OSBuild
Device Custom Number 1 Label	OSBuild
Device Custom Number 2	ReportId
Device Custom Number 2 Label	ReportId
Device Custom String 1	TenantId
Device Custom String 1 Label	TenantId
Device Custom String 2	IsExcluded
Device Custom String 2 Label	IsExcluded
Device Custom String 3	IsAzureADJoined
Device Custom String 3 Label	IsAzureADJoined
Device Custom String 4	SensorHealthState
Device Custom String 4 Label	SensorHealthState
Device Custom String 5	ExposureLevel
Device Custom String 5 Label	ExposureLevel
Device Custom String 6	DeviceType
Device Custom String 6 Label	DeviceType
Device Event Category	Type
Device Event Class Id	One of(category,deviceCategory)
Device External Id	DeviceId
Device Host Name	DeviceName
Device Product	Microsoft Defender for Endpoint

ArcSight ESM Field	Device-Specific Value
Device Receipt Time	One of(TimeGenerated, Timestamp)
Device Vendor	Microsoft
Device Version	OSVersion
FileId	_ItemId
Name	Type
Raw Event	rawevent
Request Url	_Internal_WorkspaceResourceId
Transport Protocol	InternetFacingTransportProtocol
Additional Data OS Architecture	OSArchitecture
Additional Data Client Version	ClientVersion
Additional Data DeviceType	DeviceType
Additional Data Event Type	Type
Additional Data Internet Facing Local IP	InternetFacingLocalIp
Additional Data Internet Facing Reason	InternetFacingReason
Additional Data Is Internet Facing	IsInternetFacing
Additional Data Onboarding Status	OnboardingStatus
Additional Data OS Distribution	OSDistribution
Additional Data OS Version Info	OSVersionInfo
Additional Data Scanned IP	InternetFacingPublicScannedIp
Additional Data Time Received BySvc	TimeReceivedBySvc
Additional Data OS Platform	OSPlatform

DeviceLogonEvents

ArcSight ESM Field	Device-Specific Value
Reason	FailureReason
Application Protocol	Protocol
Destination Address	Remote IP
Destination Nt Domain	AccountDomain
Destination Port	RemotePort

ArcSight ESM Field	Device-Specific Value
Destination User Name	AccountName
Device Custom String 1	InitiatingProcessMD5
Device Custom String 2	InitiatingProcessCommandLine
Device Custom String 2 Label	InitiatingProcessCommandLine
Device Custom String 3	RemoteIPType
Device Custom String 4	LogonType
Device Custom String 5	TenantId
Device Custom String 5 Label	TenantId
Device Custom String 6	IsLocalAdmin
Device Event Category	Type
Device Event Class ID	ActionType
Device External ID	DeviceId
Device Host Name	DeviceName
Device Process Name	InitiatingProcessFileName
Name	ActionType
Old File Hash	InitiatingProcessSHA1
Old File Name	InitiatingProcessFileName
Old File Path	InitiatingProcessFolderPath
Old File Size	InitiatingProcessFileSize
Source Nt Domain	InitiatingProcessAccountDomain
Source Process ID	InitiatingProcessId
Source User ID	InitiatingProcessAccountId
Source User Name	InitiatingProcessAccountName
Start Time	TimeStamp

DeviceNetworkEvents

ArcSight ESM Field	Device-Specific Value
Application Protocol	Protocol
Destination Address	RemoteIP <div style="border: 1px solid #ccc; padding: 5px; margin-left: 20px;"> Note: If "ActionType" is "OutboundConnectionAccepted", then "destinationAddress" = RemoteIP. Otherwise, "destinationAddress" = LocalIP. </div>
Destination Port	RemotePort <div style="border: 1px solid #ccc; padding: 5px; margin-left: 20px;"> Note: If "ActionType" is "OutboundConnectionAccepted", then "destinationPort" = RemotePort. Otherwise, "destinationPort" = LocalPort. </div>
Device Custom Number 2	ReportId
Device Custom Number 2 Label	ReportId
Device Custom String 2	InitiatingProcessCommandLine
Device Custom String 2 Label	InitiatingProcessCommandLine
Device Custom String 3	RemoteIPType
Device Custom String 3 Label	RemoteIPType
Device Custom String 5	TenantId
Device Custom String 5 Label	Tenant Id
Device Event Category	Type
Device Event Class ID	Action type
Device External Id	DeviceId
Device Host Name	DeviceName
Name	Action type
Old File Hash	InitiatingProcessSHA1
Old File name	InitiatingProcessFileName
Old File Path	InitiatingProcessFolderPath
Old File Size	InitiatingProcessFileSize
Request Url	RemoteUrl

ArcSight ESM Field	Device-Specific Value
Source Address	LocalIP Note: If "ActionType" is "OutboundConnectionAccepted", "SourceAddress" = RemoteIP . Otherwise, "SourceAddress" = LocalIP .
Source Nt Domain	InitiatingProcessAccountDomain
Source Port	LocalPort Note: If "ActionType" is "OutboundConnectionAccepted", then "SourcePort" = RemotePort . Otherwise, "SourcePort" = LocalPort .
Source Process ID	InitiatingProcessId
Source User ID	InitiatingProcessAccountId
Source User Name	InitiatingProcessAccountName
Start time	Timestamp

DeviceNetworkInfo

ArcSight ESM Field	Device-Specific Value
Destination Mac Address	MacAddress
Device Address	IPv4Dhcp
Device Custom Number 2	ReportId
Device Custom Number 2 Label	ReportId
Device Custom String 2	NetworkAdapterName
Device Custom String 2 Label	NetworkAdapterName
Device Custom String 3	NetworkAdapterStatus
Device Custom String 3 Label	NetworkAdapterStatus
Device Custom String 4	NetworkAdapterType
Device Custom String 4 Label	NetworkAdapterType
Device Custom String 5	TenantId
Device Custom String 5 Label	TenantId
Device Event Class ID	Concat(Type+- Status "+ NetworkAdapterStatus)

ArcSight ESM Field	Device-Specific Value
Device External ID	DeviceId
Device Host Name	DeviceName
Name	Type
Start time	Time stamp

Troubleshooting

Reconfiguring the expired Client Secret or Client Certificate

The following warning will be displayed in the Azure Portal after the expiry of the **Client Secret** or **Client Certificate**:

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo and a search bar that says "Search resources, services, and docs (G+/)". Below the header, the URL "Home > Security ArcSight | App registrations >" is visible. The main content area has a title "Application" with a "Search" bar and navigation buttons for "Delete", "Endpoints", and "Preview features". On the left, there's a sidebar with "Overview", "Quickstart", "Integration assistant", and "Manage" sections. Under "Manage", there are links for "Branding & properties", "Authentication", and "Certificates & secrets". The "Certificates & secrets" link is underlined, indicating it's the active section. In the center, there's a large red rectangular callout box containing a red exclamation mark icon and the text "A certificate or secret has expired. Create a new one →". To the right of this callout, there's a "Essentials" section with fields for "Display name", "Application (client) ID", "Object ID", "Directory (tenant) ID", and "Supported account types : My organization only".

1. Create a new **Client Secret** or **Client Certificate** with the steps mentioned [here](#).
2. Stop the connector.
3. Start the connector setup again to reconfigure the new **Client Secret** or **Client Certificate**.
4. Restart the connector.

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 Configuration Guide for Microsoft Azure Event Hub SmartConnector
(SmartConnector CE 25.1)**

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: CE 24.3

Configuration Guide Microsoft Azure Monitor Event Hub Connector

Document Release Date: July 2024

Software Release Date: July 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2021 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft Azure Monitor Event Hub SmartConnector	6
Product Overview	8
Azure Event Logs	8
Related Azure Services	9
Azure Event Log Categories	10
Understanding Data Collection	14
Preparing to Deploy the Connector	15
Setting up VM or System for Deployment	15
Prerequisites	15
Preparing System for Deployment	16
Enabling Windows Powershell to Run the Script	16
Verifying Version of Az Module and Az.Resources	17
Setting up Azure Environment	17
Supported Azure Plans	18
Setting User Permissions in Azure	18
Permission Requirements	19
Installing the Syslog NG Daemon SmartConnector	19
Opening Ports	19
(Optional) Configuring Load Balancer	20
Deploying the Connector	21
Deploying the Connector in Azure Cloud	21
Updating the Keystore Certificate	23
Streaming Logs	25
Configuring Function Apps to Stay Connected	26
Verifying the Deployment in Azure	27
Additional Configurations	27
Customizing the Connector	28
Scaling Performance	29
Additional Security Configurations	29
Adding Role Assignments	29
Configuring Firewall Settings for Azure Resources	30
Disabling FTP/FTPS when using function apps	30
(Optional) Using a Private IP	31
Upgrading the Connector	33
Updating Parser Files	34
Undeploying the Connector	35

Device Event Mapping to ArcSight Fields	35
Event Mappings for Active Directory	36
Common Event Mapping	36
Sign-in Logs Event Mapping	36
Audit Logs Event Mapping	37
Event Mappings for Microsoft Defender for Cloud	38
Common Event Mapping	38
Security Alerts Event Mapping	38
Security Recommendations Event Mapping	39
Event Mappings for Activity	40
Common Event Mapping	40
Action Event Mapping	40
Administrative Event Mapping	41
Alert Event Mapping	42
Delete Event Mapping	42
Recommendation Event Mapping	43
Security Event Mapping	43
Service Health Event Mapping	44
Write Event Mapping	45
Event Mappings for Resource Log	45
Common Event Mapping	45
Activity Runs Event Mapping	45
Application Gateway Access Log Event Mapping	46
Archive Logs Event Mapping	47
Audit Event Mapping	47
Authoring Event Mapping	48
Automatic Tuning Event Mapping	48
Azure Firewall Application Rule Event Mapping	48
Azure Firewall Network Rule Event Mapping	49
Azure Site Recovery Jobs Event Mapping	49
Blocks Event Mapping	49
C2D Command , C2D Twin Operations, and D2C Twin Operations Event Mapping	50
Database Wait Statistics Event Mapping	50
Deadlocks Event Mapping	51
Engine Event Mapping	51
Errors Event Mapping	52
Gateway Logs Event Mapping	53
Job Logs Event Mapping	53
Jobs Operations Event Mapping	53

Load Balancer Alert Event Mapping	54
Network Security Group Event Mapping	54
Operational Logs Event Mapping	55
P2S Diagnostic Logs Event Mapping	55
PostgreSQL Logs Event Mapping	55
Query Store Wait Statistics Event Mapping	56
Requests Event Mapping	56
Routes Event Mapping	57
Service Log Event Mapping	57
Timeouts Event Mapping	57
Trigger Runs Event Mapping	58
Twin Queries Event Mapping	58
Workflow Runtime Event Mapping	59
 Troubleshooting	60
Error during Installation or Upgrade	60
Errors during Deployment	60
Connection Errors	61
Parsing Errors	61
Sharing Logs for Troubleshooting	61
AppService plan is not created in a stamp that supports VNet integration	62
 Send Documentation Feedback	63

Configuration Guide for Microsoft Azure Monitor Event Hub SmartConnector

The Microsoft Azure Monitor Event Hub SmartConnector is a Cloud-native connector that is deployed on the cloud environment.

Microsoft Azure Monitor Event Hub helps you monitor the activities on Microsoft Azure Cloud services.

This connector collects events and logs from Azure Active Directory and Azure Monitor, normalizes the events to Common Event Format (CEF), and then sends the them to either ArcSight Syslog NG Daemon SmartConnector or to ArcSight Load Balancer. The events that are sent to ArcSight Load Balancer, are consequently sent to the Syslog NG Daemon SmartConnector.



Important:

The Microsoft Azure Monitor Event Hub connector has been replaced by the [Microsoft Azure Event Hub](#) SmartConnector.

The Microsoft Azure Monitor Event Hub connector will not be shipped after April 2025.

Therefore, it is highly recommended to switch to the [Microsoft Azure Event Hub](#) SmartConnector before April 2025.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

Microsoft Azure is an ever-expanding set of cloud services to help your organization meet your business challenges. It is the freedom to build, manage, and deploy applications on a massive, global network using your favorite tools and frameworks.

Azure Event Logs

The Azure Monitor Event Hub connector collects the following event logs from Active Directory, Azure Monitor, and Microsoft Defender for Cloud in Azure:

- **Active Directory Logs**
 - **Audit logs:** Provides records of system activities for compliance.
 - **Sign-in logs:** Provides information related to user logins.
-  **Note:** To export Active Directory sign-in logs, you must have one of P1 or P2 premium editions of Azure Active Directory.
- **Activity Logs:** Provides data related to write operations, such as CREATE, UPDATE, and DELETE that were performed on resources in your subscription. For more information, see [Azure Activity log](#).
- **Resource Log (formerly known as Diagnostic Log):** Provides data related to operations performed within an Azure resource (the data plane). Example: Getting a secret from a key vault or making a request to a database. The content of resource log varies by the Azure service and resource type.
- **Microsoft Defender for Cloud**
 - **Security alerts:** Provides data related to security actions performed on Microsoft Defender for Cloud in your subscription.
 - **Recommendation logs:** Provides data related to prevention recommendations provided for the resources in your subscription.

Azure event logs such as activity log and resource log are emitted in JSON format. The Azure Monitor Event Hub connector collects these event logs, converts these to CEF using mapping files, and sends these to Syslog NG Daemon SmartConnector or Load Balancer. Every JSON field is mapped to the appropriate CEF key. Each event log type has various categories and each log category has its own schema. Azure logs have schema for various log categories. With the help of these logs schema, the source fields (in JSON) are mapped to appropriate CEF keys.

The Azure Monitor Event Hub connector currently includes mapping files for several log categories of activity, audit, sign-in, and resource log. The Azure documents do not have the schemas for a few categories. Therefore, the mappings for these categories are not available in

the connector. Such events are sent unparsed to the Syslog NG Daemon SmartConnector or to the Load Balancer, and then forwarded to the ArcSight destination.

Related Azure Services

The following services are used when working with Azure Monitor Event Hub connector:

- **Azure Resource Manager:** Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure subscription. You use management features, such as access control, locks, and tags, to secure and organize your resources after deployment. For more information, see [Azure Resource Manager](#).
- **Azure App Service plan:** In App Service, an app runs in an App Service plan. An App Service plan defines a set of compute resources for a web app to run. These compute resources are analogous to the server farm in conventional web hosting. One or more apps can be configured to run on the same computing resources (or in the same App Service plan). For more information, see [Azure App Service Plan Overview](#).
- **Azure Functions:** Azure Functions allows you to run small pieces of code (called "functions") without worrying about application infrastructure. With Azure Functions, the cloud infrastructure provides all the up-to-date servers you need to keep your application running at scale. For more information ,see [An introduction to Azure Functions](#).
- **Storage account:** An Azure storage account contains all of your Azure Storage data objects: blobs, files, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that is accessible from anywhere in the world over HTTP or HTTPS. Data in your Azure storage account is durable and highly available, secure, and massively scalable. For more information, see [Storage Account Overview](#).
- **Azure Event Hubs:** Azure Event Hubs is a big data streaming platform and event ingestion service. It can receive and process millions of events per second. Data sent to an event hub can be transformed and stored by using any real-time analytics provider or batching/storage adapters. For more information, see [Azure Event Hubs — A big data streaming platform and event ingestion service](#).

Azure Event Log Categories

Following tables list the categories for mappings supported by the Azure connector. The mappings are done using the schemas provided in the Azure documents.

Active Directory Log Categories

Categories	Certified
Signin	Yes
Audit	Yes

Activity Log Categories

Categories	Certified	Comments
Administrative	Yes	These are the sub-categories: <ol style="list-style-type: none">1. Action2. Write3. Delete For more information, see Azure Activity Log event schema .
Alert	Yes	Azure alerts.
Recommendation	Yes	Recommendation events from Azure Advisor.
Security	No	Same as Microsoft Defender for Cloud log events for Security Alert activity without remediation steps.
ServiceHealth	Yes	Service Health incidents occurred in Azure.

Resource Log Categories

Categories	Resource Type
GatewayLogs	Microsoft.ApiManagement/service
JobLogs	Microsoft.Automation/automationAccounts JobStreams
JobStreams	Microsoft.Automation/automationAccount
CoreAnalytics	Microsoft.Cdn/profiles/endpoints
PipelineRuns	Microsoft.DataFactory/factories
TriggerRuns	Microsoft.DataFactory/factories
Audit	Microsoft.DataLakeAnalytics/accounts
Requests	Microsoft.DataLakeAnalytics/accounts

Categories	Resource Type
Audit	Microsoft.DataLakeStore/accounts
Requests	Microsoft.DataLakeStore/accounts
Connections	Microsoft.Devices/IotHubs
DeviceTelemetry	Microsoft.Devices/IotHubs
C2DCommands	Microsoft.Devices/IotHubs
DeviceIdentityOperations	Microsoft.Devices/IotHubs
FileUploadOperations	Microsoft.Devices/IotHubs
Routes	Microsoft.Devices/IotHubs
D2CTwinOperations	Microsoft.Devices/IotHubs
C2DTwinOperations	Microsoft.Devices/IotHubs
TwinQueries	Microsoft.Devices/IotHubs
JobsOperations	Microsoft.Devices/IotHubs
DirectMethods	Microsoft.Devices/IotHubs
DataPlaneRequests	Microsoft.DocumentDB/databaseAccounts
ArchiveLogs	Microsoft.EventHub/namespaces
OperationalLogs	Microsoft.EventHub/namespaces
AuditEvent	Microsoft.KeyVault/vaults
WorkflowRuntime	Microsoft.Logic/workflows
NetworkSecurityGroupEvent	Microsoft.Network/networksecuritygroups
NetworkSecurityGroupRuleCounter	Microsoft.Network/networksecuritygroups
LoadBalancerAlertEvent	Microsoft.Network/loadBalancers
LoadBalancerProbeHealthStatus	Microsoft.Network/loadBalancers
ApplicationGatewayAccessLog	Microsoft.Network/applicationGateways
ApplicationGatewayPerformanceLog	Microsoft.Network/applicationGateways
ApplicationGatewayFirewallLog	Microsoft.Network/applicationGateways
OperationalLogs	Microsoft.ServiceBus/namespaces
QueryStoreRuntimeStatistics	Microsoft.Sql/servers/databases
QueryStoreWaitStatistics	Microsoft.Sql/servers/databases
Errors	Microsoft.Sql/servers/databases
DatabaseWaitStatistics	Microsoft.Sql/servers/databases
Timeouts	Microsoft.Sql/servers/databases

Categories	Resource Type
Blocks	Microsoft.Sql/servers/databases
Audit	Microsoft.Sql/servers/databases
Execution	Microsoft.StreamAnalytics/streamingjobs
Authoring	Microsoft.StreamAnalytics/streamingjobs
AzureFirewallApplicationRule	Microsoft.Network/AzureFirewalls
AzureFirewallNetworkRule	Microsoft.Network/AzureFirewalls
ServiceLog	Microsoft.Batch/batchAccounts
SQLSecurityAuditEvents	Microsoft.Sql/servers/databases
SQLSecurityAuditEvents	Microsoft.Synapse/workspaces
AutomaticTuning	Microsoft.Sql/servers/databases
Deadlocks	Microsoft.Sql/servers/databases
ActivityRuns	Microsoft.DataFactory/factories
AzureBackupReport	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryEvents	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryJobs	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryProtectedDiskDataChurn	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryRecoveryPoints	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicatedItems	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicationDataUploadRate	Microsoft.RecoveryServices/Vaults
AzureSiteRecoveryReplicationStats	Microsoft.RecoveryServices/Vaults
DscNodeStatus	Microsoft.Automation/automationAccounts
Engine	Microsoft.PowerBI
Engine	Microsoft.AnalysisServices/servers
GatewayDiagnosticLog	microsoft.network/p2svpngateways
GatewayDiagnosticLog	microsoft.network/virtualnetworkgateways
GatewayDiagnosticLog	microsoft.network/vpngateways
IkeDiagnosticLog	microsoft.network/p2svpngateways
IkeDiagnosticLog	microsoft.network/virtualnetworkgateways
IkeDiagnosticLog	microsoft.network/vpngateways
Operationlogs	microsoft.loadtestservice/loadtests
Operationlogs	Microsoft.Search/searchServices

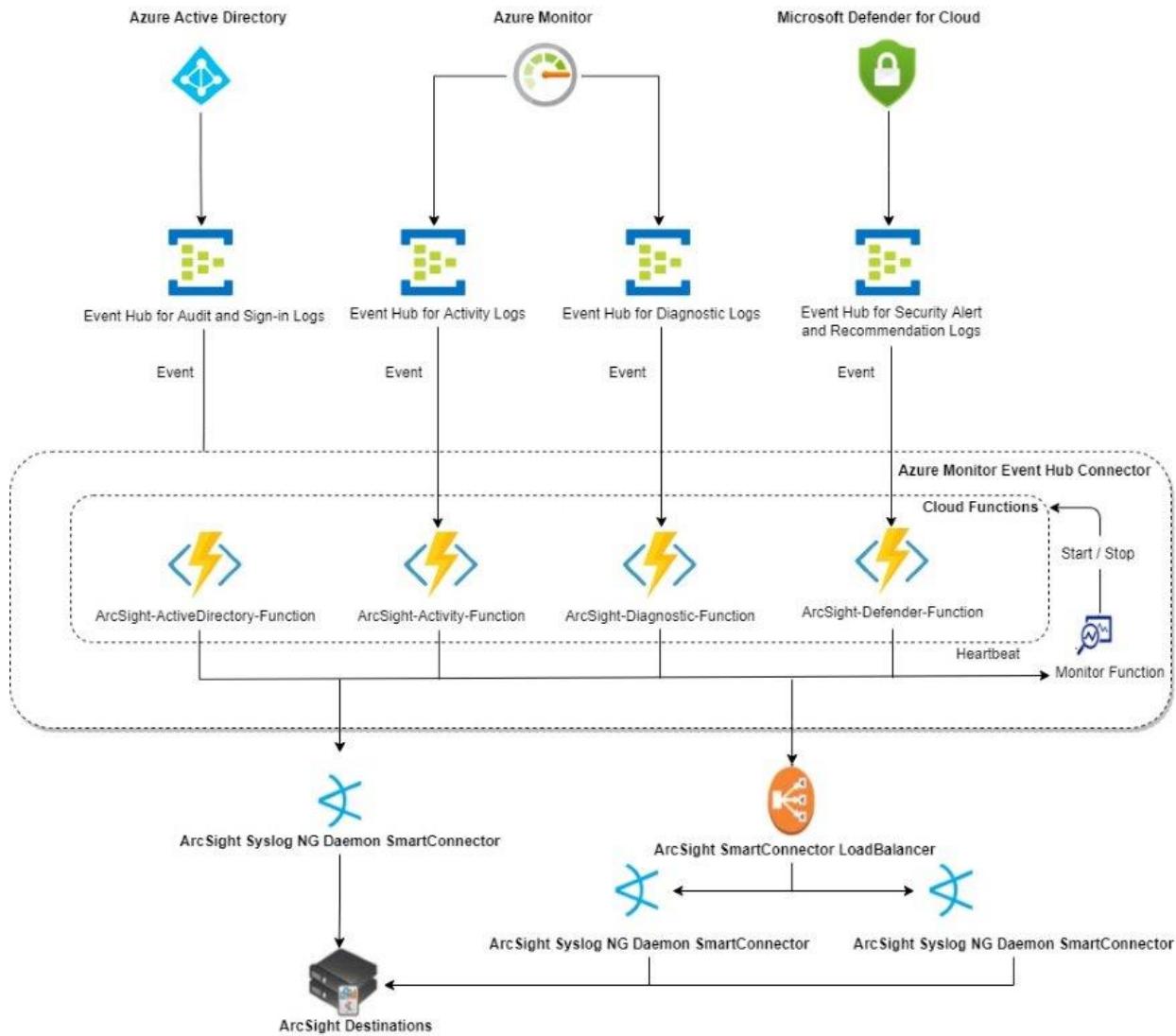
Categories	Resource Type
P2Sdiagnosticlog	microsoft.network/virtualnetworkgateways
P2Sdiagnosticlog	microsoft.network/p2svpngateways
Routediagnosticlog	microsoft.network/virtualnetworkgateways
Routediagnosticlog	microsoft.network/vpngateways
OperationalLogs	Microsoft.NotificationHubs/namespaces
OperationalLogs	Microsoft.ServiceBus/Namespace
PostGreSQLLogs	Microsoft.DBforPostgreSQL

Microsoft Defender for Cloud Log Categories

Categories	Resource Type	Certified
Securityalerts	All resources	Yes
SecurityRecommendations	All resources	Yes

Understanding Data Collection

The following diagram provides a high-level overview of how the Azure Monitor Event Hub connector collects and sends data to ArcSight's destinations.



Understanding the process flow of data collection

1. After installing, the Azure Monitor Event Hub connector creates event hubs for Active Directory, Azure Monitor, and Microsoft Defender for Cloud.
2. The Azure Monitor Event Hub connector then automatically configures the supported log types to be forwarded to the following event hubs: Active Directory, Activity, Resource, and Microsoft Defender for Cloud. To configure Microsoft Defender for Cloud, see [Streaming Logs](#).
3. The ArcSight Azure Event Processor collects logs in JSON format and then converts these to CEF format.

4. The ArcSight Azure Event Processor then forwards these CEF events to the Syslog NG Daemon SmartConnector or Load Balancer through a secured communication channel using TLS 1.2.
5. The Azure Monitor Event Hub connector establishes a TLS 1.2 connection by accepting a server certificate from the Syslog NG Daemon SmartConnector or ArcSight Load Balancer.
6. The Monitor App continuously monitors the heartbeat of the Syslog NG Daemon SmartConnector or Load Balancer to ensure that it is up and running to receive events. If the Syslog NG Daemon SmartConnector or Load Balancer is down due to an unexpected shutdown of the machine or network issues, this connector stops further processing of events from the event hub. The unprocessed events are sent back to the event hub to avoid data loss. After the Syslog NG Daemon SmartConnector or Load Balancer comes up, the Azure Monitor Event Hub connector continues to send the events to the Syslog NG Daemon SmartConnector. However, the Monitor App will not monitor Syslog NG Daemon SmartConnector connected to the Load Balancer.
7. The Syslog NG Daemon SmartConnector then sends the events to the ArcSight destination.

Preparing to Deploy the Connector

Before you begin deploying the Azure Monitor Event Hub connector, make sure that the following prerequisite tasks are completed:

Setting up VM or System for Deployment

To set up the VM or system for installation, make sure that you have the following prerequisites and prepare the system for deployment:

Prerequisites

Deploying or undeploying the Azure Monitor Event Hub connector can be performed from any on-prem or any cloud hosted virtual machine. Following are the supported environments:

- **Operating System:** Microsoft Windows Server 2012 , 2016, and 2019 (in the cloud with Azure)
- **Powershell:** 5.0 or higher. Ensure that Windows Powershell is enabled to run scripts on the machine where you want to deploy the connector. For more information see, "[Enabling Windows Powershell to Run the Script](#)" on the next page.
- **Az Module:** 6.5.0
- **Az.Resources:** 4.4.0



Note: If a higher version of AZ module is installed, you must downgrade it to 6.5.0 for the installation script to work. For more information see, "["Verifying Version of Az Module and Az.Resources" on the next page.](#)

Preparing System for Deployment

This section includes the following information:

Enabling Windows Powershell to Run the Script

PowerShell scripts are now signed in Azure Event Hub SmartConnectors. This allows users to run them in security-enabled environments with an execution policy set to either **RemoteSigned** or **AllSigned**. For more information, see [PowerShell Execution Policies](#). However, signed scripts can still run in unrestricted environments.

To deploy the Azure Monitor Event Hub connector, you must run a script in Windows PowerShell. You must enable the Windows Powershell to run scripts on the machine where you want to deploy the Azure Monitor Event Hub connector.



Note: This procedure needs to be done only once on the machine.

To enable Windows PowerShell to run scripts:

1. Upgrade the Windows PowerShell version to 5.0 or later.
2. Click Start and search for Windows PowerShell. Right-click Windows PowerShell and click **Run as administrator**.
3. Check the current script execution policy:
`Get-ExecutionPolicy`
4. If the current script execution policy is Restricted, change the script execution policy to one of the following options:
 - `Set-ExecutionPolicy AllSigned`
 - a. Enter Yes to All when prompted.
 - b. Run the `Get-ExecutionPolicy` command to ensure that PowerShell is now `AllSigned`.
 - c. Enter `Run Once` or `Always` Run when prompted to trust the publisher while running the script.
 - `Set-ExecutionPolicy RemoteSigned`

- a. Enter Yes to All when prompted.
- b. Run the Get-ExecutionPolicy command to ensure that PowerShell is now RemoteSigned.
- Set-ExecutionPolicy unrestricted
 - a. Enter Yes to All when prompted.
 - b. Run the Get-ExecutionPolicy command to ensure that PowerShell is now Unrestricted.

Verifying Version of Az Module and Az.Resources

1. Run the Get-InstalledModule command to ensure that "Az" version is 6.5.0 and "Az.Resources" version is 4.4.0.

If the Get-InstalledModule command does not show any results, skip to [step 1.b](#).

If you have the latest version of "Az" (such as 7.2.0), then perform the following steps to uninstall the current version and reinstall the required version:

- a. Run the following commands to uninstall the higher version of Az:

```
$Modules += (Get-Module -ListAvailable Az.*).Name
Foreach ($Module in ($Modules | Get-Unique))
{
    Write-Output ("Uninstalling: $Module")
    Uninstall-Module $Module -Force
}
Uninstall-Module Az -Force
```

- b. After the product is uninstalled, run the following command to install the supported version: Install-Module Az -RequiredVersion 6.5.0



Note: If you have a slow internet connection, the following might occur:

- The download progress might not be displayed while the libraries are downloading and installing the Az module. However, the download is in progress.
- The download and installation of the Az module might take up to 40 minutes.

2. Restart your machine.



Note: If you encounter any issue during the Az module uninstall, then close all the PowerShell windows and try again.

Setting up Azure Environment

Complete the following procedures to set up an Azure environment:

1. [Supported Azure Plans](#)
2. [Setting User Permissions in Azure](#)
3. [Installing the Syslog NG Daemon SmartConnector](#)
4. [Opening Ports](#)
5. [\(Optional\) Configuring Load Balancer](#)

Supported Azure Plans

- **Azure Datacentres with Stamps (Scale Units) with Premium V2 VMs:**

Only applications running on stamps that support Premium V2 scale units, possess the hardware required to use the VNet Integration (preview) feature.

- **AppService Plan with Basic Pricing Tier Created on a Stamp with Premium V2 VMs:**

Microsoft Azure Monitor Event Hub Connector requires an AppService plan with basic pricing tier. However, you must ensure that your AppService plan is created in a stamp that supports VNet Integration. VNET integration feature configuration requires a premium V2VM

It is possible that you have an existing AppService plan that was created in a stamp that does support Premium V2 even for a basic plan and it allows you to use the VNet Integration feature.

Workaround:

If you are on a basic plan and are unable to create VNet integration, try the following:

- You can temporarily upgrade the plan to complete the VNet configuration. After the VNet configuration completes, you scale back to the basic plan to use the VNet Feature.
- If your AppService plan does not show the feature to scale up to Premium V2, you might not be able to create a new AppService plan in the same Resource Group of the Premium V2 pricing Tier. This happens because the Resource Group sometimes, decides on a particular stamp and creates all resources in there. If you experience this issue, try creating the AppService plan in a different Resource Group.

Next Step: [Setting User Permissions in Azure](#)

Setting User Permissions in Azure

In Azure, users must be associated with a subscription to provide them with access to resources such as virtual machine, storage account, virtual network, and so on. Therefore, you must determine the subscription you want to use for the Azure Monitor Event Hub connector and add users to the required subscription. You must also assign users to a role to define their permission to perform tasks.

Permission Requirements

- **To deploy or upgrade:**

Scope	Description
Azure Active Directory	The users must have the Application Administrator and Security Administrator roles on the Azure Active Directory.
Resource Group	<p>The users must create a resource group.</p> <p>The users must ensure that they are assigned the Owner role on the resource group before deploying both Azure Monitor Function and Cloud Function applications.</p> <p>Note:</p> <ul style="list-style-type: none"> ◦ The users must have the Owner role assigned on the resource group so that they can assign the Contributor role for the Azure Monitor Function application over the resource group during deployment. ◦ The Azure Monitor Function application requires the Contributor role on the resource group to start or stop the Cloud Function application.

- **To run and monitor:** The users must have at least a **Contributor IAM** role on the subscription.



Note: The default value for **identifierUri** is ns1-test.xyz in app.properties. Ensure that you update with verified domain URI.

Next Step: [Installing the Syslog NG Daemon SmartConnector](#)

Installing the Syslog NG Daemon SmartConnector

Because Microsoft Azure Monitor Event Hub is a Cloud-native Connector, you must install the Syslog NG Daemon SmartConnector with TLS protocol to receive events from the Microsoft Azure Monitor Event Hub Connector. For more information, see [Installing the Syslog NG Daemon SmartConnector](#).

Next Step: [Opening Ports](#)

Opening Ports

You must ensure that the ports on the server on which you installed the Syslog NG Daemon SmartConnector is accessible from Azure.

Opening Ports on a Non-Virtual Machine

If you installed the Syslog NG Daemon SmartConnector on a physical, non-virtual machine, ensure that the ports on which you installed it are accessible to Azure.

Opening Ports on a Virtual Machine

If you have installed the Syslog NG Daemon SmartConnector on a virtual machine in Azure cloud, ensure that the ports on which you installed Syslog NG Daemon SmartConnector are open in both Azure and the virtual machine.

To open inbound ports on Azure:

1. Log in to Microsoft Azure as a user with administrator privileges.
2. Click **Virtual Machines > Virtual machine name > Networking > Add inbound port**.
3. Enter the same port or port range on which you installed the Syslog NG Daemon SmartConnector.
4. Update other fields and click **Add**.

To open ports in the virtual server:

1. Log in to the virtual Microsoft Windows Server machine.
2. Open Microsoft Windows Server Firewall.
3. Click **Inbound Rules > New Rule > Port > Next > TCP > Specific local ports**.
4. Enter the same port or port range on which you installed the Syslog NG Daemon SmartConnector.
5. Click **Next > Allow the connection > Next > Profile > Next**.
6. Name the rule and click **Finish**.

(Optional) Opening Port to Enable On-premises Connectivity

To connect from an on-premises network to an Azure Virtual Network (VNet), create an incoming port to allow the TCP port number (the default port is 1999) or a range of IP's between 0 and x.

From 00.000.0.000/00 (Azure cloud) to xx.xxx.xxx.xxx (on-premises Arcsight's Syslog SmartConnector).

Next Step: (Optional) Configuring Load Balancer

(Optional) Configuring Load Balancer

In environments where the event load is more than what can be handled by a single Syslog NG Daemon SmartConnector, you can configure Load Balancer to handle large event loads. For more information about configuring Load Balancer, see ArcSight SmartConnector [Load Balancer documentation](#).

Deploying the Connector

This section provides information about deploying the Azure Monitor Event Hub connector to collect and forward events from Azure Cloud Services to the Syslog NG Daemon SmartConnector or Load Balancer, and then the events can be sent to an ArcSight destination.

Complete the following procedures to deploy the Azure Monitor Event Hub connector:

1. ["Deploying the Connector in Azure Cloud" below](#)
2. ["Updating the Keystore Certificate" on page 23](#)
3. ["Streaming Logs" on page 25](#)
4. ["Configuring Function Apps to Stay Connected" on page 26](#)
5. ["Verifying the Deployment in Azure" on page 27](#)

Deploying the Connector in Azure Cloud

Deploying the Azure Monitor Event Hub connector will automatically deploy and configure the required components in your Azure Cloud.

When you deploy the Azure Monitor Event Hub connector against a subscription, you can monitor the events emitted from the services registered to the subscription. If you have multiple subscriptions and you want to monitor the services under all your subscriptions, you must deploy this connector against each of the subscriptions separately. The Azure Monitor Event Hub connector gets deployed directly into the Azure cloud and you do not need to set up a virtual machine in the cloud to deploy the connector.

To deploy the Azure Monitor Event Hub connector:

1. On the machine from where you want to deploy the connector, download the `arcsight-azure-monitor-eventhub-connector-x.x.x.zip`.
2. Extract the `arcsight-azure-monitor-eventhub-connector-x.x.x.zip` files to the desired location.
3. Edit the **app.properties** file.

- Configure the following application properties of this connector:

Properties	Description
resourceGroupName	Modify the name of the resourceGroupName property. The default value is arcsight-functions-group .
FunctionAppName1	Modify the name of the Function App. Function Apps must not contain the period symbol. The default value is arcsight-cloudfunctions
FunctionAppName2	Modify the name of the Function App. Function Apps must not contain the period symbol. The default value is arcsight-monitor-functions
connectorhostname	Specify the IP address of the Syslog NG Daemon SmartConnector or Load Balancer. The default value is 0.0.0.0 .
connectorport	Specify the port number of the Syslog NG Daemon SmartConnector or Load Balancer. The default value is 1999 .
keyStoreFileName	Specify the keystore file name of the Syslog NG Daemon SmartConnector or Load Balancer. The keyStoreFileName property is used by the event hub connector application running on Azure to establish a TLS connection over SSL with the client Syslog NG Daemon SmartConnector.
keyStorePassword	Specify the keystore password of the Syslog NG Daemon SmartConnector or Load Balancer The keyStorePassword property is used by the event hub connector application running on Azure to establish a TLS connection over SSL with the client Syslog NG Daemon SmartConnector.
storageaccountname	Specify a unique storageaccountname. Storage account names must be between 3 and 24 characters in length and might contain numbers and lowercase letters only.
Eventhubnamespace	Specify a unique Eventhubnamespace.
alwaysOn	Ensure to set the default value as true before starting a fresh deployment, or else change it to false if you would like it to be off.



Note: Copy the keystore file from the Syslog NG Daemon SmartConnector or Load Balancer to cloud. To access the keystore file, log in to Azure and click **Storage Accounts > <storage account name> > Files > Storage container > <function app name> > certs** folder.

- Specify the Service Plan. You can specify either **Consumptionplan** or **Appserviceplan**. The following table lists the service plans and their default values:

Service Plans	Default Values
servicePlanName	ArcSightPlan
servicePlanTier	Basic
servicePlanNumberOfWorkers	1
servicePlanWorkerSize	Small

- An App Service plan handles a fixed event load. You can modify the service plan values as required.
 - A Consumption plan is a serverless plan and allows you to scale automatically. It is not mandatory to specify any values for this plan.
- c. Specify the location based on the locale of the resources you want to monitor.
 - d. Save the file.



Note:

- The default identifierUri is **www.example.com** in **app.properties**. Ensure that you update with a verified domain URI.
- Back up the **app.properties** file because you would need to refer to these configurations during uninstallation.

4. The deployment script has an option to enable and disable event hubs for Active Directory, Azure Monitor and Microsoft Defender for Cloud.
5. Open Windows PowerShell as Administrator and run the following command:
`<extracted path>\DeployFunction.ps1`
6. When prompted, log in to Microsoft Azure as a user with required privileges for the subscription you want to use with Azure.
7. Select the appropriate subscription from the list displayed and click **Yes**.



Note: Ignore warnings displayed while deploying the Azure Monitor Event Hub connector.

Next Step: "[Updating the Keystore Certificate](#)" below

Updating the Keystore Certificate

The Syslog NG Daemon SmartConnector contains a default keystore certificate. Ensure that you associate this default keystore certificate with the new storage account to prevent errors.



Caution: : Do not use the existing resource groups in your Azure environment because this resource group will be deleted when you uninstall this connector.

To update the keystore certificate:

1. Go to the ArcSightSmartConnectors\current\user\agent\ folder and rename the required keystore certificate corresponding to the Syslog NG Daemon SmartConnector to `remote_management.p12`, which is the file name of the default keystore certificate so that the Azure connector identifies the custom keystore.
2. Log in to Microsoft Azure as a user with the required permissions for the subscription you want to use with Azure.
3. Click **All services > Storage accounts**.
4. In the Storage Accounts page, select the required storage account name.
5. In the Navigation pane, click **Data storage > File shares**.
6. Click to open the storage container name function.
7. Click to open the displayed folder and do one of the following:
 - If you are updating the keystore certificate for an existing Azure Monitor Event Hub connector and can view the certs folder, go to step 8.
 - If you have newly deployed an Azure Monitor Event Hub connector and cannot view the certs folder, do the following:
 - a. Go to the newly created storage account.
 - b. In the Navigation pane, click **Settings > Configuration**.
 - c. In the **Allow Blob anonymous access** option, click **Enabled** and then click **Save**.
 - d. Run the `DeployFunction.ps1` file again.
 - e. At the command prompt, "The deployment already exists. Do you want the installation to verify and update the resources? Y/N," enter **Y** and press **ENTER**.After the deployment process is completed, the certs folder will be created.
8. Click to open the certs folder and then delete the default certificate, `remote_management.p12`.
9. To upload the keystore certificate of the Syslog NG Daemon SmartConnector:
 - a. Click **Upload**.
 - b. In the URL field, browse to the required location and select `remote_management.p12`.
 - c. Click **Upload**.
10. Restart the function apps:
 - a. Click **Function Apps > <arcshift cloud function app name> > Restart**.
 - b. Click **Function Apps > <arcshift monitor app name> > Restart**.



Note: After restarting the function apps, if you do not see the updated certs folder inside Storage Accounts, then start the SyslogNG Connector and restart the `arcshift-monitor-functions` function.

Next Step: "Streaming Logs" below

Streaming Logs

After the installation completes, some logs stream automatically and some need to be configured.

Activity Logs

The install script automatically streams events from activity logs. There is no specific configuration required.

However, if you want to send activity logs from other account manually, complete the following steps:

1. Navigate to **Activity Logs > Monitoring > Diagnostic Settings**.
2. Add the setting by selecting the appropriate event hub and log categories to be monitored.

Active Directory Logs

The install script automatically streams events from Active Directory logs - audit logs, sign-in logs. There is no specific configuration required.

However, if you want to send Active Directory logs from other account manually, complete the following steps:

1. Navigate to **Activity Logs > Monitoring > Diagnostic Settings**.
2. Add the setting by selecting the appropriate event hub and log categories to be monitored.

Resource Logs

You must manually add diagnostic settings to configure streaming of these logs. The following procedure provides a brief overview of settings required for streaming Diagnostic Logs. For information, see [Azure documentation](#).

1. Select **Azure Home > Monitor > Diagnostic Settings**.
2. Select the event hub. The default event hub name is **eh-emitter-arcsgight**.
3. When the list of configured diagnostics is displayed, click **Edit** on the desired diagnostic to be updated. Click **Add**, to monitor a new resource.
4. From the Diagnostic settings window, select the **Stream to an event hub** check box or select the event hub.
5. On the Select event hub window:
 - a. From the **Select event hub namespace** drop-down list, specify a name of event hub namespace.

- b. From the **Select event hub name** drop-down list, select **insights-diagnostics-logs**.
 - c. From the **Select event hub policy name** drop-down list, select **ArcSightAccessKey**.
6. Click **OK**.
7. On the Diagnostic settings window, select the logs you want to stream.

Microsoft Defender for Cloud Event Logs

To send Microsoft Defender for Cloud events to Event Hub, follow these steps:

1. From the left sidebar, select **Microsoft Defender for Cloud**, and then click **Environment Setting**.
2. Select the specific subscription to be used when configuring data export.
3. On the **Subscription** settings, go to the sidebar and select **Continuous Export**.
4. Select the data type to be exported and choose from the filters on each type.
5. From **Export target**, choose the current subscription. Event hub namespace and name are defined in the **app.properties** file when deploying.
6. Go to the Event hub and create a new policy if needed.
7. Save your changes.

Next Step: "[Configuring Function Apps to Stay Connected](#)" below

Configuring Function Apps to Stay Connected

On the App Service Plan, function apps are designed to go to an idle state after a default timeout period. Therefore, you must manually configure the function apps to stay connected even if events are not streamed during the timeout period.



Note: For the **Always On** feature, ensure to set the default value as **True** in the **app.properties** before starting a fresh deployment, or else change it to **False** if you would like it to be off.

To configure the function apps to stay connected:

1. Click **Function Apps > Function Name > Application Settings > General Settings**.
2. For the **Always On** feature click **ON** if you want to keep it on or else click **OFF**.
Ensure that you do this for both <arcsight cloud function app name> and <arcsight monitor function app name>.

Next Step: "[Verifying the Deployment in Azure](#)" on the next page

Verifying the Deployment in Azure

To ensure that the Azure Monitor Event Hub connector installed successfully, verify the following:

1. The following Azure functions are installed in your Azure subscription: <**arcsight cloud function app name**> and <**arcsight monitor app name**>. These functions collect events from Azure event hubs and monitor the health of the connection downstream. To view the functions in Azure, click **Function Apps**.
2. The install script automatically streams events from the audit logs, sign-in logs, and activity logs. For Resource Log, you must manually add diagnostic settings to configure streaming of these logs. For more information, see [Step 7 in "Streaming Logs" on page 25](#).
3. Uploads the application settings listed in the **app.properties** file to Azure. This enables you to add or modify properties from Azure instead of modifying the **app.properties** file and redeploying the Azure Monitor Event Hub connector. To view the properties in Azure, click **Function Apps** > <**function app name**> > **Application Settings**. For more information about modifying these properties, see ["Customizing the Connector" on page 28](#).
4. The Azure Monitor Event Hub Connector converts JSON events to CEF format. To view the default certificates in Azure, click **Storage Accounts** > <**Storage account name**> > **File shares** > **Storage container** > <**function app name**> > **certs** folder. The default name of the storage account is **emitterarcsightstorage**.



Note: The Azure Monitor Event Hub connector supports custom mapping. If you want to modify the current mappings or support a new category, then create a map file. To upload the newly created map file to Azure, click **Storage Accounts** > <**Storage account name**> > **File shares** > **Storage container** > <**function app name**> > **maps** folder.

5. An Active Directory application called <**arcsight monitor app name**> is created and the Azure Website Contributor role is assigned to this application.
6. A resource group called <**arcsight functions group name**> is created. This resource group manages the resources of this connector. The default name of the resource group is **arcsightfunctions-group**.
7. An Azure storage account called <**storage account name**> is created. This storage account stores the Azure Monitor Event Hub connector certificate, function logs, and the parser files.

Additional Configurations

Customizing the Connector

You can customize the connector properties as required.

To customize the connector:

1. Log in to Microsoft Azure as a user with required privileges for the subscription you want to use with Azure.
2. Click **Function Apps > <arcsight cloud function app name> or <arcsight monitor function app name> > Platform Features > Application Settings.**



Important: Do not modify any of the settings other than those listed in this procedure as this may cause unpredictable performance or even outages.

3. (Conditional) To modify the connector port and connector name of the Syslog NG Daemon SmartConnector or Load Balancer:
 - a. Update the **Connector Port** field.
 - b. Update the **Connector Hostname** field with the IP address or hostname.



Note: Ensure that you do this for both <arcsight cloud function app name> and <arcsight monitor function app name>.

4. (Conditional) You can send the connector logs to a storage account. However, this consumes cloud storage

In the **logging.storage.enabled** field, enter **true**. The connector now sends logs from the function app to the storage account every 15 minutes.

To stop sending logs to the storage account, enter **false** in the **logging.storage.enabled** field.

5. Click **Save**.

Scaling Performance

You might need to modify your deployment or change certain configurations to improve the performance.

- Your Azure pricing plan also affects performance scaling.
A Consumption plan scales automatically and an App Service plan handles a fixed event load. A Consumption plan automatically creates Function App instances to scale up the load. For more information about the event load handled in a App Service plan, see the Azure Documentation.
- You can configure Load balancer in environments where the event load is more than what can be handled by a single Syslog NG Daemon SmartConnector.

Additional Security Configurations

This section has the following information:

Adding Role Assignments

Ensure that you have:

`Microsoft.Authorization/roleAssignments/write` and
`Microsoft.Authorization/roleAssignments/delete` permissions, such as User Access Administrator or Owner.

To add a role assignment:

1. Sign into the **Azure** portal.
2. From the search box, search for the **Resource Group** you want to assign roles to.
3. Click the **Resource Group** and navigate to the **Access Control (IAM)** page.
4. Click the **Role Assignments** tab to view the role assignments at this scope.
5. Click **Add > Add Role Assignment**.

The **Add Role Assignment** pane opens.



Note: If you do not have permissions to assign roles, the **Add Role Assignment** option is disabled.

6. From the role list, search or scroll to find the role that you want to assign and click to select it.
7. Go to the **Assign Access To** list and click to select the type of security principle to assign access to.

These principles generally are **User, Group or Service**.

8. If you selected a user-assigned managed identity or a system-assigned managed identity, select the subscription where the managed identity is located.
 9. From the **Select** section, search for the security principle by entering a string or scrolling through the list.
 10. To assign the role, click **Save**.
 11. From the **Role Assignments** tab, confirm that you see the role assignment in the list.
- To remove existing role assignments:
1. Open **Access control (IAM)** at a specific scope, such as management group, subscription, resource group, or resource, where you want to remove access.
 2. Click the **Role Assignments** tab to view all the role assignments at the scope.
 3. From **Role Assignments**, add a check mark next to the security principle with the role assignment you want to remove.
 4. Click **Remove**.
 5. A message is displayed, click **Yes** to confirm the changes.

Configuring Firewall Settings for Azure Resources

1. Sign into the **Azure** portal.
2. Navigate to the **Azure Resource** that needs to be monitored.
3. Go to **Networking**.
4. Select **Allow Access from Selected Networks**.
5. Add a new virtual network or select an existing network.
6. Under Firewall, enter the IP Address Range that needs to be allowed.
Additionally, you can select your client's IP address as well.
7. Select the **Resource Type** and the Instance name as **All in this Resource Group**.
8. Under **Exceptions**, check the option **Allow trusted Microsoft services to access this storage account**.
9. Verify if the Network Routing field shows **Microsoft Network Routing** as the default one.
10. Save the changes and refresh the resource modified.
11. Restart the function apps.

Disabling FTP/FTPS when using function apps

By default, FTP/FTPS is enabled when using Function App for TLS communication. You can disable FTP/FTPS if required.

To disable FTP/FTPS:

1. Go to the **Cloud Function App**.
2. Navigate to **Configuration > General Settings > Platform Settings**.
3. On the **FTP State** field, select **Disabled**.
4. Save the changes and restart the function app.
5. Perform the same steps on the Monitor function app and save changes.

(Optional) Using a Private IP

You can configure Event Hub and Function App to use a private IP. However, if you are on a basic subscription plan, then you must upgrade to a Standard or Premium plan.

To use a private IP:

1. Add a new or an existing VNet to Event Hubs, Storage Account, and Function Apps.

To add VNet to Event Hubs

- a. From your **Event Hub**, under **Settings**, click **Networking**
- b. Do one of the following:
 - Select **All Networks** to add all networks to access your resources.
 - Click **Selected Networks** to add selected networks to access your resource.
Add the **Existing virtual network** or **Create new virtual network**.

To add VNet to Storage Account

- a. From your **Storage Account**, click **Networking**, and then click the **Firewalls and Virtual Networks** tab.
- b. Select one of the followings:
 - **Enabled from all networks** - to add all networks to access your resources.
 - **Enabled from selected virtual networks and IP addresses** - to add selected networks to access your resource.
Add the **Existing virtual network** or **Add new virtual network**.

To add VNet to Function Apps

- a. Go to the **Function App > Settings > Networking > Outbound Traffic > VNet Integration**, add those to your VNet.
- b. Add or remove network interfaces from your virtual machines, for more information, see [Add network interfaces to or remove network interfaces from virtual machines](#).
2. Enable the Service endpoints of the previously used subnets.

- a. From **Virtual networks Service**, select your **VNet > Subnets**.
- b. Open all the subnets.
- c. Select **All Service Endpoints** and save your changes.
3. Check if the Function Apps communicate to the destination (ArcSight Syslog NG Daemon, ArcSight Load Balancer, etc.) through the Private IP.
4. From **Development Tools > Console Tool**, execute the tcpping command to your VM via private IP.

```
tcpping host:port
```

host: private IP

port: you may use port 3389 or the port used in your Function Apps.

5. After successfully executing the command above, from **Function Apps > Application Settings**, check if the setting already exists or add a new one:

APP SETTING NAME: JAVA_OPTS

VALUE: -Djava.net.preferIPv4Stack=true

6. In the field **connectorhostname**, enter your Private IP.

7. Next, in the field **Port**, enter the port of your Private IP.

8. Restart **Function Apps**.



Note: The VNet integration preview is a preview, if it does not work, you can disable and enable the VNet integration or create another subnet.

Upgrading the Connector

You can only do a binary upgrade of the Azure Monitor Event Hub connector. A binary upgrade upgrades the connector and also enables you to continue using the components and the custom settings created during deployment.

To upgrade the connector:

1. Stop all the connector specific Function App(s).
2. Stop the Syslog NG Daemon SmartConnector.
3. On the machine from where you want to upgrade the connector, download `arcsight-azure-monitor-eventhub-connector-x.x.x.zip`.
4. Extract the `arcsight-azure-monitor-eventhub-connector-x.x.x.zip` files to the desired location.
5. Configure the **app.properties** file. For more information, see Step 3 in **Deploying the Connector**. Ensure that you specify the same Function App names that you specified during deployment.
6. Open Windows PowerShell as Administrator and run the following command:

```
<extracted path>\DeployFunction.ps1
```

7. When prompted to enable or disable a specific event hub, press **0** to enable and **1** to disable.

The event hubs for Active Directory logs, Activity Logs, Resource Logs (formerly known as Diagnostic logs), and Microsoft Defender for Cloud logs are enabled by default. However, you can select to monitor only the specific event hubs.

8. Log in to Microsoft Azure as a user with required privileges for the subscription you want to use with Azure.
9. Select the required subscription.
10. When the script prompts you, select one of the following:
 - **Y:** to verify and update the resources.
The script first checks whether there is an existing installation of the Connector in the cloud, and then the installation will verify and update the resources.
 - **N:** to exit the script.
11. To configure the Function App(s) to stay connected, click **Function Apps > <function name> > Application Settings > General Settings** and update it to **Always on**.
12. Start all the connector specific Function App(s).
13. Start the Syslog NG Daemon SmartConnector.

Updating Parser Files

First, extract the new parser files from the AUP Extractor Tool:

To extract parser files:

1. Download the ArcSight-x.x.x.xxxxx.0-ConnectorParsers.aup package from the ArcSight Marketplace.
2. To apply monthly parser updates to Cloud Connectors:
 - a. Download the ArcSight-x.x.x.xxxxx.0-aup-extractor.jar utility from the location where you have downloaded the connector.



Note: Your system must have Java 1.8.x or later version installed and Java available in the operating system's path to use the aup-extractor.jar utility

- b. Run the following command to use the utility to extract parser files from the package:

```
java -jar aup-extractor.jar <AUP filename>
```

Examples:

- `java -jar aup-extractor.jar ArcSight-x.x.x.xxxxx.0-ConnectorParsers.aup` - When the .aup package is in the same directory where the JAR file is present.
- `java -jar aup-extractor.jar c:\MyFolder\ArcSight-CE 24.3xxxx.0-ConnectorParsers.aup` - When the .aup package is present in other directory.

You can either provide one or both the parameters. If you do not provide any parameters, the utility picks up any available. aup file and creates a new folder named **output** in the directory from where the utility is run and uploads the output files.

The following folders will be extracted:

- **aws_cloudwatch**: Contains security parser for AWS Cloudwatch.
 - **aws_securityhub**: Contains security parser for AWS Security Hub.
 - **azure_emitter**: Contains security parser for Azure emitter.
- c. Copy the parser files in the **output/azure_emitter** folder and upload them to the Azure environment.

To override parser files:

1. Stop the Cloud Function app and the Monitor Function app.
2. Go to **Cloud function app > App Service Editor (Preview)> Developer Tools**.
3. Click **Go**.
4. Right-click the **Maps** folder and click **Upload**.

5. Select the parser files to be overridden and click **OK**.
6. Restart the function apps.
7. Refresh the page by restarting the **App Service Editor (Preview)**.

To store and quick-view parser files:

Go to **Storage Accounts > Storage Account Name > File Shares > Storage Container > Function App Directory >Maps**.

Undeploying the Connector

Undeploying the Azure Monitor Event Hub connector deletes the Active Directory application (AzADApplication) and all the associated components such as storage account and event hubs created during deployment.

To undeploy the connector:

1. Open Windows PowerShell as Administrator and run the following command:

```
<deployed path>\UndeployFunction.ps1
```

2. Log in to Microsoft Azure as a user with the required privileges for the subscription you want to use with Azure.
3. Select the required subscription.
4. Enter **Yes** when prompted to confirm deletion of the installed resources, such as event hubs, storage account, function apps, and AzADApplication. This will undeploy the connector.



Note: The resource group will not be deleted when you undeploy the connector. However, post undeployment, you can delete the resource group if required.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the ArcSight Console User's Guide for more information about the ArcSight data fields.

Event Mappings for Active Directory

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Name	operationName
Device Event Class ID	operationName
Severity	Level

Sign-in Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Application Protocol	properties/clientAppUsed
Destination Process Name	properties/appDisplayName
Destination User ID	properties/userId
Destination User Name	properties/userDisplayName
Device Custom Date 1	properties/createdDateTime
Device Custom Floating Point 1	properties/location/geoCoordinates/latitude
Device Custom Floating Point 2	properties/location/geoCoordinates/longitude
Device Custom String 1	properties/deviceDetail/operatingSystem
Device Custom String 2	properties/isRisky
Device Custom String 3	properties/location
Device Custom String 4	location
Device Custom String 5	correlationId
Device Custom String 6	properties/userPrincipalName
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
External ID	properties/id
Reason	resultDescription
Request Client Application	properties/deviceDetail/browser
Source Address	callerIpAddress

Audit Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	properties/targetResources/userPrincipalName
Device Event Category	properties/category
Device Custom String 1	properties/identityType
Device Custom String 2	properties/operationType
Device Custom String 3	properties/targetResources/modifiedProperties(Role.DisplayName)/displayName (Role.DisplayName)
Device Custom String 5	correlationId
Device Custom String 6	properties/targetResources
Device Receipt Time	time
Event Outcome	resultType
External ID	properties/id
File Hash	properties/targetResources/modifiedProperties(Role.DisplayName)/newValue (Role.DisplayName)
File Name	properties/targetResources/modifiedProperties(Group.DisplayName)/newValue (Group.DisplayName)
File Path	properties/targetResourceName
File Type	properties/targetResourceType
Old File Hash	properties/targetResources/modifiedProperties(Role.DisplayName)/oldValue (Role.DisplayName)
Old File Name	properties/targetResources/modifiedProperties(Group.DisplayName)/oldValue (Group.DisplayName),
Reason	resultDescription
Source Address	callerIpAddress
Source User ID	properties/initiatedBy/user/id,
Source User Name	properties/initiatedBy/user/userPrincipalName

Event Mappings for Microsoft Defender for Cloud

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Name	AlertDisplayName
Device Event Class ID	AlertType
Severity	Severity

Security Alerts Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	AlertType
Destination Host Name	CompromisedEntity, Entities/HostName
Device Custom Date 1	ProcessingEndTime
Device Custom Number 1	Entities/\$id
Device Custom String 1	ExtendedProperties
Device Custom String 2	IsIncident
Device Custom String 3	ResourceIdentifiers
Device Custom String 4	AlertUri

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	Entities/Location/Asn & Entities/Location/CountryCode & Entities/Location/CountryName & Entities/Location/State & Entities/Location/City & Entities/Location/Longitude & Entities/Location/Latitude
Device Receipt Time	TimeGenerated
Device Severity	Severity
End Time	EndTimeUtc
Event Outcome	Status
External ID	SystemAlertId
File Path	AzureResourceId, Entities/AzureID, Entities/ResourceId
File Type	Entities/Type
Message	Description & RemediationSteps
Reason	Intent
Start Time	StartTimeUtc
Source Address	Entities/Address

Security Recommendations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	type
Device Action	assessmentEventDataEnrichment/action
Device Custom String 1	properties/metadata/policyDefinitionId
Device Custom String 2	properties/metadata/threats
Device Custom String 4	properties/links/azurePortal
Device Severity	properties/metadata/severity
File Name	file
File Path	ID
Message	properties/metadata/description & properties/metadata/remediationDescription

ArcSight ESM Field	Device-Specific Field
Name	properties/displayName
Event Outcome	properties/status/code
Reason	properties/status/cause

Event Mappings for Activity

Common Event Mapping

ArcSight ESM Field	Device-Specific Field
Name	operationName
Device Event Class ID	operationName
Severity	level

Action Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Port	properties/eventProperties/destinationPort
Destination Host Name	resourceId, properties/eventProperties/machineName
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Custom Date 1 Label	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/eventProperties, properties/policies
Device Custom String 3	properties/eventProperties/title
Device Custom String 4	location
Device Custom String 5	correlationId
Device Custom String 6	properties/isComplianceCheck
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
External ID	eventDataId

ArcSight ESM Field	Device-Specific Field
File Hash	properties/eventProperties/fileSha256
File Path	resourceId, properties/eventProperties/filePath
File Name	properties/eventProperties/fileName
File Type	resourceType, properties/eventProperties/type
Message	description
Old File Type	properties/eventProperties/resourceType
Reason	properties/eventProperties/cause
Request Client Application	properties/eventProperties/compromisedEntity
Source Address	callerIpAddress
Source Service Name	properties/eventProperties/attackedResourceType
Transport Protocol	properties/eventProperties/protocol

Administrative Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Action	identity/authorization/action
Device Custom Number 1	durationMs
Device Custom String 1	resultSignature
Device Custom String 4	location
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	time
Event Outcome	resultType
File Path	resourceId
Message	identity/claims
Request Client Application	identity/claims/iss
Request URL	identity/claims/aud
Source Address	callerIpAddress

Alert Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom Number 1	properties/Threshold
Device Custom Number 2	properties/WindowSizeInMinutes
Device Custom String 1	properties/RuleUri, subStatus
Device Custom String 2	properties/RuleName
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
Event Outcome	status
External ID	eventId
File Path	resourceId
File Type	resourceType
Message	description

Delete Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Privileges	identity/authorization/evidence/role
Destination User Name	identity/claims/name
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	correlationId
Device Custom String 4	location
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
File Type	resourceType
Event Outcome	resultType

ArcSight ESM Field	Device-Specific Field
External ID	eventDataId
Message	description
Source Address	callerIpAddress

Recommendation Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/recommendationCategory
Device Custom String 3	properties/recommendationImpact
Device Custom String 4	properties/recommendationRisk
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
Event Outcome	status
External ID	eventDataId
File Path	resourceId
File Type	resourceType
Message	description

Security Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Process ID	properties/processId
Destination Process Name	properties/processName
Destination NT Domain	properties/domainName
Destination User ID	properties/accountLogonId
Destination User Name	caller, properties/username
Device Action	properties/ActionTaken

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 2	properties/UserSID
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
External ID	eventDataId
Event Outcome	status
File Path	resourceId
File Type	resourceType
Message	description

Service Health Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination Service Name	properties/impactedServices
Destination User Name	caller
Device Custom Date 1	submissionTimestamp
Device Custom String 1	properties/trackingId
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	eventTimestamp
External ID	eventDataId
Event Outcome	status
File Path	resourceId
File Type	resourceType
Message	description
Start Time	properties/impactStartTime
Reason	properties/communication

Write Event Mapping

ArcSight ESM Field	Device-Specific Field
Destination User Name	identity/claims/name
Destination User Privileges	identity/authorization/evidence/role
Device Custom Date 1	submissionTimestamp
Device Custom String 1	subStatus
Device Custom String 4	location
Device Custom String 5	correlationId
Device Event Category	category
Device Receipt Time	time
External ID	eventDataId,
Event Outcome	properties/statusCode
File Path	resourceId
File Type	resourceType
Source Address	callerIpAddress

Event Mappings for Resource Log

Common Event Mapping

Device Event Mapping	ArcSight Fields
Name	operationName
Device Event Class ID	operationName
Severity	Level

Activity Runs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 2	Error

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	correlationId
Device Receipt Time	time
External ID	activityRunId
File ID	pipelineRunId
File Path	resourceId
File Name	pipelineName
Destination Process Name	activityName
Start Time	start
End Time	end
Message	Output

Application Gateway Access Log Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
Device External ID	instanceId
Source Address	properties/clientIP
Source Port	properties/clientPort
Request URL	properties/requestUri
Request Client Application	properties/userAgent
Event Outcome	properties/httpStatus
Bytes In	properties/receivedBytes
Bytes Out	properties/sentBytes
Device Custom Number 1	properties/timeTaken
Device Custom String 1	properties/sslEnabled

Archive Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
External ID	ActivityId
Device Custom String 1	trackingId
Device Custom String 2	archiveStep
File Path	resourceId
File Name	eventHub
Start Time	startTime
Device Custom Number 1	failures
Device Custom Number 2	durationInSeconds
Message	message

Audit Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Event Outcome	resultType
Source Address	callerIpAddress
Destination User ID	identity
Device Custom String 1	properties/JobId
Device Custom String 2	properties/JobRunTime
Device Custom String 5	correlationId
Destination Process Name	properties/JobName
Start Time	properties/StartTime
End Time	properties/EndTime

Authoring Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Event Outcome	status
Device Receipt Time	time
Device Custom String 1	properties/Error
Device Custom String 5	properties/correlationId
Message	properties/Message
Reason	properties/Type

Automatic Tuning Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
File Path	ResourceId

Azure Firewall Application Rule Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceid
Message	properties/smrg

Azure Firewall Network Rule Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceid
Message	properties/smrg

Azure Site Recovery Jobs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Event Outcome	properties/resultType
Message	properties/resultDescription
Start Time	properties/startTime
End Time	properties/endTime
Device Custom String 2	properties/affectedResourceType
Device Custom String 3	properties/affectedResourceId
Device Custom String 5	properties/correlationId

Blocks Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup

ArcSight ESM Field	Device-Specific Field
Device Custom String 4	DatabaseName_s
Device Custom Number 1	duration_d
File Path	ResourceId
Destination User Name	resource_owner_type_s

C2D Command , C2D Twin Operations, and D2C Twin Operations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Database Wait Statistics Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	delta_wait_time_ms_d
Device Custom Number 2	delta_waiting_tasks_count_d
File Path	ResourceId

Deadlocks Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	duration_d
File Path	ResourceId
Destination User Name	resource_owner_type_s

Engine Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
File Path	ResourceId
Device Event Category	category
Start Time	properties/StartTime
Device Custom String 1	properties/ObjectID
Device Custom String 2	properties/ObjectType
Device Custom String 3	properties/ObjectName
Device Custom String 4	properties/ObjectPath
Device Custom String 5	properties/ObjectReference

ArcSight ESM Field	Device-Specific Field
End Time	properties/EndTime
Event Outcome	properties/Success
Device Custom Number 1	properties/ConnectionID
Device Custom Number 2	properties/SPID
Source NT Domain	properties/NTDomainName
Source Host Name	properties/ClientHostName
Source Process ID	properties/ClientProcessID
Device Custom String 6	properties/ApplicationName
Destination User Name	properties/User
Destination Service Name	properties/ServerName

Errors Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
File Path	ResourceId
Message	Message
Event Outcome	state_d
Reason	error_number_d

Gateway Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
Device Custom Number 1	durationMs
Device Custom String 2	location
Source Address	callerIpAddress
Request URL Method	properties/method
Request URL	properties/url
Event Outcome	properties/responseCode

Job Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	TimeGenerated
File Name	RunbookName_s
Destination User Name	Caller_s
Device Custom String 1	resourceId
Device Custom String 2	resourceGroup
Device Custom String 3	Tenant_g
Device Custom String 5	correlationId
File ID	JobId_g
Event Outcome	ResultType
Device Event Category	category

Jobs Operations Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time

ArcSight ESM Field	Device-Specific Field
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Load Balancer Alert Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Device Custom String 1	systemId
File Path	resourceId
Reason	properties/eventDescription
Destination Address	properties/eventProperties/public ip address

Network Security Group Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Destination MAC Address	properties/macAddress
Destination Address	properties/primaryIPv4Address
Device Custom String 1	properties/subnetPrefix
Device Custom String 2	properties/ruleName
Device Custom String 3	properties/direction
Device Custom String 4	properties/priority
Device Custom String 5	properties/type
Message	properties/conditions
Transport Protocol	properties/conditions/protocols

Operational Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
File Path	resourceId
Device Custom String 1	subscriptionId
Device Custom String 4	Region
Device Receipt Time	EventTimeString
Message	EventProperties
Event Outcome	Status
Source Process Name	Caller
External ID	ActivityId

P2S Diagnostic Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Message	properties/message
Device External ID	properties/instance

PostgreSQL Logs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Device Custom String 3	ResourceGroup
Device Custom String 2	SubscriptionId
Source Service Name	LogicalServerName
Message	properties/message

Query Store Wait Statistics Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 1	TenantId
Device Receipt Time	TimeGenerated
File Name	Resource
File Type	ResourceType
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Custom String 4	DatabaseName_s
Device Custom Number 1	total_query_wait_time_ms_d
File Path	ResourceId

Requests Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Event Outcome	resultType
Source Address	callerIpAddress
Destination Use ID	identity
Request Method	properties/HttpMethod
Request URL	properties/Path
Bytes In	properties/RequestContentLength
External ID	properties/ClientRequestId
Start Time	properties/StartTime
End Time	properties/EndTime

Routes Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
File Path	resourceId
Device Custom String 1	properties
Device Custom String 2	location
Device Custom Number 1	durationMs
Event Outcome	resultType
Message	resultDescription

Service Log Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Tenant
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
External ID	properties/id
File Type	properties/imageType

Timeouts Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 1	TenantId
Device Custom String 2	SubscriptionId
Device Custom String 3	ResourceGroup
Device Receipt Time	TimeGenerated
File Name	Resource

ArcSight ESM Field	Device-Specific Field
File Type	ResourceType
Azure Logical Server Name_s	LogicalServerName_s
Azure Elastic Pool Name_s	ElasticPoolName_s
CS 4 Label	DatabaseName_s
File Path	ResourceId

Trigger Runs Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Custom String 2	triggerEvent
Device Custom String 5	correlationId
Device Receipt Time	time
External ID	activityRunId
File Path	resourceId
File Name	pipelineName
Destination Process Name	activityName
Start Time	start
End Time	end
File ID	triggerId
File Type	triggerType

Twin Queries Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Receipt Time	time
Device Custom Number 1	durationMs
Device Custom String 1	properties
Device Custom String 2	location

ArcSight ESM Field	Device-Specific Field
Event Outcome	resultType
File Path	resourceId
Message	resultDescription

Workflow Runtime Event Mapping

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	time
Device Event Category	category
File Path	resourceId
Reason	code
Event Outcome	properties/status
Start Time	properties/startTime
End Time	properties/endTime
Device Custom String 1	properties/resource/subscriptionId
Device Custom String 2	properties/resource/resourceGroupName
Device Custom String 4	properties/resource/location
Device Action	properties/resource/actionName
File Name	properties/resource/workflowName

Troubleshooting

This section includes:

- [Error during Installation or Upgrade](#)
- [Errors during Deployment](#)
- [Connection Errors](#)
- [Parsing Errors](#)
- [Sharing Logs for Troubleshooting](#)
- [AppService plan is not created in a stamp that supports VNet integration](#)

Error during Installation or Upgrade

The following connection error is displayed while installing or upgrading the connector:
“502 - Web server received an invalid response while acting as a gateway or proxy server.”

Workaround:

You can ignore this error message. Generally, the server tries to reconnect with the connector and the installation or upgrade process continues after the connection is established. However, if the server is unable to establish connection with the connector, the installation or upgrade process fails to proceed, and you are exited from the wizard.

Errors during Deployment

You might receive an error message prompting you to register the subscription <subscription id> with **Microsoft.Insights**.

Workaround:

In this case, you must register your subscription with the **microsoft.insights** provider.

To register:

1. Log in to Microsoft Azure as a user with administrator privileges.
2. Click **All Services > Subscriptions**.
3. Select the subscription you want for this connector.
4. Select **Resource Providers**.
5. Click **Register**.

Connection Errors

Connection errors are displayed when the Syslog NG Daemon SmartConnector hostname and port are not reachable from Azure cloud.

Workaround:

To ensure that the Syslog NG Daemon SmartConnector host and port are reachable from Azure cloud:

1. Open the relevant ports. The certificate file is overridden during the deployment of the Azure Monitor Event Hub connector.
2. Replace the remote connection management file in Azure with your remote connection management file.
3. Click **Storage Accounts > <*Storage account name*> > Files > Storage container > <*function app name*> > certs** folder.
4. Replace the **remote_management.p12** file with your **<*customname*>.p12** file.

Parsing Errors

Parsing errors are displayed if the event log categories are not supported by the Azure Monitor Event Hub connector. For a list of the supported categories, see Appendix A, “Azure Event Log Categories”.

Workaround:

You can contact technical support in the following scenarios:

- If you want to change the default mappings.
- If you want to add a new log type.
- See parsing errors.

Sharing Logs for Troubleshooting

You might want to share logs with technical support for troubleshooting.

Workaround:

To share logs:

1. Log in to Microsoft Azure as a user with security reader privileges or contributor privileges.
2. From the **Development Tools** menu, click **App Service Editor**.

3. Click **Go**.
4. On the new App Service Editor tab, select **Open Kudo Console** from the top drop-down menu.
5. On the new tab, go to: **site > wwwroot > logs**.
6. Download the function logs and send them to technical support.

AppService plan is not created in a stamp that supports VNet integration

Microsoft Azure Monitor Event Hub Connector requires an AppService plan with basic pricing tier. However, you must ensure that your AppService plan is created in a stamp that supports VNet Integration. the VNet integration feature configuration requires a premium V2VM.

It is possible that you have an existing AppService plan that was created in a stamp that does support Premium V2 even for a basic plan and it allows you to use the VNet integration feature.

Workaround:

If you are on a basic plan and are unable to create VNet integration, try the following:

You can temporarily upgrade the plan to complete the VNet configuration. After the VNet configuration completes, you scale back to the basic plan to use the VNet Feature.

If your AppService plan does not show the feature to scale up to Premium V2, you might not be able to create a new AppService plan in the same Resource Group of the Premium V2 pricing Tier. This happens because the Resource Group sometimes, decides on a particular stamp and creates all resources in there. If you experience this issue, try creating the AppService plan in a different Resource Group.

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 Configuration Guide Microsoft Azure Monitor Event Hub Connector
(SmartConnectors CE 24.3)**

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 MFI-Documentation-Feedback@opentext.com .

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 24.3

Implementing ArcSight Common Event Format (CEF) - Version 27

Document Release Date: July 2024

Software Release Date: July 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

What is CEF?	4
The Case for ArcSight CEF	4
CEF Implementation	4
Header Information	4
Header Field Definitions	5
Using CEF Without Syslog	8
The Extension Field	8
Character Encoding	9
ArcSight Extension Dictionary	10
CEF Key Names for Event Producers	10
CEF Key Names for Event Producers	10
CEF Key Names for Event Consumers	37
CEF Key Names For Event Consumers	38
Special Mappings	42
Firewall	42
Anti-Virus	42
Email	43
Wireless	43
IPv6 Format	43
User-Defined Extensions	43
Custom Extension Naming Guidelines	44
Format	44
Requirements	44
Limitations of Custom Extensions	44
Limitations Affecting ArcSight ESM	44
Limitations Affecting ArcSight Logger	45
Appendix A: Date Formats	45
Send Documentation Feedback	46

What is CEF?

Common Event Format (CEF) is an extensible, text-based format designed to support multiple device types by offering the most relevant information. Message syntaxes are reduced to work with ESM normalization. CEF specifically defines a syntax for log records containing a standard header and a variable extension, formatted as key-value pairs. The CEF format can be used with on-premise devices by implementing the ArcSight Syslog SmartConnector. CEF can also be used by cloud-based service providers by implementing the SmartConnector for ArcSight Common Event Format REST.



Note: This guide describes ArcSight CEF standard only. For information about descriptions of fields or schemas related to specific ArcSight products, such as the ArcSight Manager, ArcSight Logger, or ArcSight SmartConnector, contact Customer Support.

The Case for ArcSight CEF

The central problem of any security information and event management (SIEM) environment is integration. Device vendors each have their own format for reporting event information, and such diversity can make customer site integration time consuming and expensive. The CEF standard format, developed by ArcSight, enables vendors and their customers to quickly integrate their product information into ESM.

The CEF standard format is an open log management standard that simplifies log management. CEF allows third parties to create their own device schemas that are compatible with a standard that is used industry-wide for normalizing security events. Technology companies and customers can use the standardized CEF format to facilitate data collection and aggregation, for later analysis by an enterprise management system.

CEF Implementation

This document defines the CEF protocol and provides details about implementing the standard. It details the header and predefined extensions used within the standard, and explains the procedure to create user-defined extensions. It also includes a list of CEF supported date formats.

Header Information

CEF uses Syslog as a transport mechanism. It uses the following format that contains a Syslog prefix, a CEF header, and one or more extensions in this format:

<Syslog_prefix> <CEF_header>|[Extension]

The CEF header consists of seven fields separated by a pipe character (|). If the pipe character (|) is used in a “value” part of a CEF header field, it must be escaped. The pipe delimiter between the header fields must not be escaped.

The CEF header is -

CEF:Version|Vendor|Product|Version|Message ID|Name|Severity|

Header Field Definitions

Header Name	Field Name	Type	Size	Description
CEF Version	CEF Version	String	N/A	<p>CEF Version is an integer and identifies the version of the CEF format. Event consumers use this information to determine what the following fields represent.</p> <p>The current CEF format versions are:</p> <ul style="list-style-type: none"> • 0 (CEF:0) - for CEF Specification version 0.1 • 1 (CEF:1) - for CEF Specification version 1.x <p>For example, for CEF Specification version 1.2, the value of the CEF Version header field will be "1".</p>
Vendor	deviceVendor	String	63	<p>deviceProduct and deviceVendor are strings that uniquely identify the type of device that sent the message.</p> <p>No two products might use the same deviceVendor and deviceProduct pair. There is no central authority managing these pairs. Event producers must ensure that they assign unique name pairs.</p>
Product	deviceProduct	String	63	
Version	deviceVersion	String	31	The deviceVersion is the version of the product producing the logs.

Message ID	deviceEventClassId	String	1023	<p>deviceEventClassId is a unique identifier for each event-type. This can be a string or an integer. deviceEventClassId identifies the type of event reported.</p> <p>In the Intrusion Detection System (IDS) world, each signature or rule that detects certain activity has a unique Signature ID assigned. This is a requirement for other types of devices as well and helps correlation engines process the events. It is also known as Signature ID.</p> <p>Note: The ‘=’, ‘%’ , and '#' characters must be escaped in the vulnerability string that are mapped to deviceEventClassId , and if they are present in the description or name of the vulnerability. However, these characters must not be escaped when used as a delimiter.</p>
Name	name	String	512	<p>name is a string representing a human readable and understandable description of the event. The event name must not contain information that is specifically mentioned in other fields. For example: "Port scan from 10.0.0.1 targeting 20.1.1.1" is not a good event name. It must be: "Port scan". The other information is redundant and can be picked up from the rest of the fields.</p>

What is CEF?

Severity	agentSeverity	AgentSeverityEnumeration	N/A	agentSeverity is a string or integer and it reflects the importance of the event. <ul style="list-style-type: none"> The valid string values are: Unknown, Low, Medium, High, and Very-High. The valid integer values are: 0=Unknown, 1-3=Low, 4-6=Medium, 7-8=High, and 9-10=Very-High.
	deviceSeverity	String	63	deviceSeverity captures the language used by the data source to describe its interpretation of the danger posed by a particular event. For example, if a network IDS detects a DHCP packet that does not contain enough data to conform to the DHCP format, the device flags this as a high-priority exploit.

In which,

CEF:Version - is a mandatory header. The rest of the message is formatted using fields delimited by a pipe ("|") character. All of the following fields must be present and defined under ["What is CEF?" on page 4](#).

[Extension] - is a placeholder for additional fields, but is not mandatory. Any additional fields are logged as key-value pairs. For a table of definitions, see [ArcSight Extension Dictionary](#).

The following examples illustrate a CEF message using Syslog transport:

For CEF 0.x version

```
Sep 19 08:26:10 host CEF:0|Security|threatmanager|1.0|100|worm
successfully stopped|10|src=10.0.0.1 dst=2.1.2.2 spt=1232
```

For CEF 1.x version

```
Sep 29 08:26:10 host CEF:1|Security|threatmanager|1.0|100|worm
successfully stopped|10|src=10.0.0.1 dst=2.1.2.2 spt=1232
```

Using CEF Without Syslog

Syslog applies a syslog prefix to each message, no matter which device it arrives from, that contains the date and hostname in the following example:

```
Jan 18 11:07:53 host CEF:Version|...
```

Even if an event producer is unable to write Syslog messages, it is possible to write the events to a file by performing the following steps:

1. Discard the syslog prefix (Jan 18 11:07:53 host).
2. Begin the message with the following format:

```
CEF:Version|Device Vendor|Device Product|Device Version|Device Event  
Class ID|Name|Severity|[Extension]
```

The Extension Field

The **Extension** field contains a collection of key-value pairs. The keys are part of a predefined set. The standard allows to include additional keys as described in the [ArcSight Extension Dictionary](#) section. An event can contain any number of key-value pairs in any order, separated by spaces (" "). If a field contains a space, such as a file name, this is valid and can be logged in exactly that manner, as shown in the following example:

```
filePath=/user/username/dir/my file name.txt
```



Note:

- If there are multiple spaces before a key, all spaces but the last space are treated as trailing spaces in the prior value in the key. If you need trailing spaces, use multiple spaces, otherwise, use one space between the end of a value and the start of the following key.
- Trailing spaces are not preserved for the final key-value pair in the extension. It is highly recommended to not utilize leading or trailing spaces in CEF events unless absolutely necessary. If that is the case, ensure the ordering of key-value pairs in the extension is such that any value with trailing spaces is not the final value. For more information on best practices for creating CEF events, see the CEF Mapping Guidelines document.
- Extension values must follow the escape character guidelines defined for encoding symbols in CEF. See, "[Character Encoding](#)" on the next page.

Character Encoding

Because CEF uses the UTF-8 Unicode encoding method, certain symbols must use character encoding. Within this context, character encoding specifies how to represent characters that could be misinterpreted within the schema.

Ensure the following when encoding symbols in CEF:

- The entire message must be UTF-8 encoded.
- Spaces used in the header are valid. Do not encode a space character by using <space>.
- If a pipe (|) is used in the header, it must be escaped with a backslash (\). But note that the pipes in the extension do not need escaping. For example:

```
Sep 19 08:26:10 host CEF:0|security|threatmanager|1.0|100|detected a
\| in message|10|src=10.0.0.1 act=blocked a | dst=1.1.1.1
```
- If a backslash (\) is used in the header or the extension, it must be escaped with another backslash (\). For example:

```
Sep 19 08:26:10 host CEF:0|security|threatmanager|1.0|100|detected a
\\ in packet|10|src=10.0.0.1 act=blocked a \\ dst=1.1.1.1
```
- If an equal sign (=) is used in the extensions, it has to be escaped with a backslash (\). Equal signs in the header need no escaping. For example:

```
Sep 19 08:26:10 host CEF:0|security|threatmanager|1.0|100|detected a =
in message|10|src=10.0.0.1 act=blocked a \= dst=1.1.1.1
```
- Multi-line fields can be sent by CEF by encoding the newline character as \n or \r. Note that multiple lines are only allowed in the value part of the extensions. For example:

```
Sep 19 08:26:10 host CEF:0|security|threatmanager|1.0|100|Detected a
threat. No action needed.|10|src=10.0.0.1 msg=Detected a threat.\n No
action needed
```

ArcSight Extension Dictionary

The [CEF Key Names For Event Producers](#) and [CEF Key Names for Event Consumers](#) tables list the predefined names that establish usages for both event producers and event consumers. While the fields listed in both the tables are useful event consumers, the fields listed in the [CEF Key Names for Event Consumers](#) table must not be set by event producers.



Note:

- The **bytesIn** and **bytesOut** fields were containing only Integer values in CEF 0.1. However, from CEF 1.0 onwards, these fields also contain the Long values.
- All IP address fields in CEF 0.1 were containing IPv4 addresses only. However, from CEF 1.0 onwards, these fields also contain IPv6 addresses.

CEF Key Names for Event Producers

This table displays the CEF names along with the full names for each CEF key name. When sending events, the CEF key name is the proper form to use, because using the full name to send an event will fail.

CEF Key Names for Event Producers

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceAction	act	String	63	Action taken by the device.
0.1	applicationProtocol	app	String	31	Application level protocol, example: HTTP, HTTPS, SSHv2, Telnet, POP, IMPA, IMAPS, and so on.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomIPv6Address1	c6a1	IpAddress		<p>One of the four IPv6 address fields available to map fields that do not apply to any other in this dictionary.</p> <p>TIP: For tips on using these fields, see the guidelines defined under User-Defined Extensions.</p>
0.1	deviceCustomIPv6Address1Label	c6a1Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomIPv6Address3	c6a3	IpAddress		<p>One of the four IPv6 address fields available to map fields that do not apply to any other in this dictionary.</p> <p>TIP: For tips on using these fields, see the guidelines defined under User-Defined Extensions.</p>

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomIPv6AddressLabel	c6a3Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomIPv6Address4	c6a4	IPv6 Address		<p>One of the four IPv6 address fields available to map fields that do not apply to any other in this dictionary.</p> <p>TIP: For tips on using these fields, see the guidelines defined under User-Defined Extensions.</p>
0.1	deviceCustomIPv6Address4Label	c6a4Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceEventCategory	cat	String	1023	Represents the category assigned by the originating device. Devices often use their own categorization schema to classify event. Example: "/Monitor/Disk/Read"

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomFloatingPoint1	cfp1	Double		One of our floating point fields available to map fields that do not apply to any other in this dictionary.
0.1	deviceCustomFloatingPoint1Label	cfp1Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomFloatingPoint2	cfp2	Double		One of the four floating point fields available to map fields that do not apply to any other in this dictionary.
0.1	deviceCustomFloatingPoint2Label	cfp2Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomFloatingPoint3	cfp3	Double		One of the four floating point fields available to map fields that do not apply to any other in this dictionary.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomFloatingPoint3Label	cfp3Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomFloatingPoint4	cfp4	Double		One of the four floating point fields available to map fields that do not apply to any other in this dictionary.
0.1	deviceCustomFloatingPoint4Label	cfp4Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomNumber1	cn1	Long		One of the three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomNumber1Label	cn1Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomNumber2	cn2	Long		One of the three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
0.1	deviceCustomNumber2Label	cn2Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomNumber3	cn3	Long		One of the three number fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomNumber3Label	cn3Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	baseEventCount	cnt	Integer		A count associated with this event. How many times was this same event observed? Count can be omitted if it is 1.
0.1	deviceCustomString1	cs1	String	4000	One of the six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.

TIP: For tips on using these fields, see the guidelines defined under [User-Defined Extensions](#).

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomString1Label	cs1Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomString2	cs2	String	4000	One of the six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.
0.1	deviceCustomString2Label	cs2Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomString3	cs3	String	4000	<p>One of the six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.</p> <p>TIP: For tips on using these fields, see the guidelines defined under User-Defined Extensions.</p>
0.1	deviceCustomString3Label	cs3Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomString4	cs4	String	4000	<p>One of the six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.</p> <p>TIP: For tips on using these fields, see the guidelines defined under User-Defined Extensions.</p>
0.1	deviceCustomString4Label	cs4Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomString5	cs5	String	4000	<p>One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.</p> <p>TIP: For tips on using these fields, see the guidelines defined under User-Defined Extensions.</p>
0.1	deviceCustomString5Label	cs5Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceCustomString6	cs6	String	4000	<p>One of six strings available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.</p> <p>TIP: For tips on using these fields, see the guidelines defined under User-Defined Extensions.</p>

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomString6Label	cs6Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	destinationDnsDomain	destinationDnsDomain	String	255	The DNS domain part of the complete fully qualified domain name (FQDN).
0.1	destinationServiceName	destinationServiceName	String	1023	The service targeted by this event. Example: "sshd"
0.1	destinationTranslatedAddress	destinationTranslatedAddress	IpAddress		Identifies the translated destination that the event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1"
0.1	destinationTranslatedPort	destinationTranslatedPort	Integer		Port after it was translated; for example, a firewall. Valid port numbers are 0 to 65535.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomDate1	deviceCustomDate1	DateTime		<p>One of two timestamp fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.</p> <p>TIP: For tips on using these fields, see the guidelines defined under User-Defined Extensions.</p>
0.1	deviceCustomDate1Label	deviceCustomDate1Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceCustomDate2	deviceCustomDate2	DateTime		<p>One of the two timestamp fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible.</p> <p>TIP: For tips on using these fields, see the guidelines defined under User-Defined Extensions.</p>
0.1	deviceCustomDate2Label	deviceCustomDate2Label	String	1023	All custom fields have a corresponding label field. Each of these fields is a string and describes the purpose of the custom field.
0.1	deviceDirection	deviceDirection	DeviceDirectionEnumeration		Any information about what direction the observed communication has taken. The following values are supported: "0" for inbound or "1" for outbound
0.1	deviceDnsDomain	deviceDnsDomain	String	255	The DNS domain part of the complete fully qualified domain name (FQDN).

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceExternalId	deviceExternalId	String	255	A name that uniquely identifies the device generating this event.
0.1	deviceFacility	deviceFacility	String	1023	The facility generating this event. For example, Syslog has an explicit facility associated with every event.
0.1	deviceInboundInterface	deviceInboundInterface	String	128	Interface on which the packet or data entered the device.
0.1	deviceNtDomain	deviceNtDomain	String	255	The Windows domain name of the device address.
0.1	deviceOutboundInterface	deviceOutboundInterface	String	128	Interface on which the packet or data left the device.
0.1	devicePayloadId	DevicePayloadId	String	128	Unique identifier for the payload associated with the event.
0.1	deviceProcessName	deviceProcessName	String	1023	Process name associated with the event. An example might be the process generating the syslog entry in UNIX.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceTranslatedAddress	deviceTranslatedAddress	IpAddress		Identifies the translated device address that the event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1"
0.1	destinationHostName	dhost	String	1023	Identifies the destination that an event refers to in an IP network. The format must be a fully qualified domain name (FQDN) associated with the destination node, when a node is available. Examples: "host.domain.com" or "host".
0.1	destinationNtDomain	dntdom	String	255	The Windows domain name of the destination address.
0.1	destinationProcessId	dpid	Integer		Provides the ID of the destination process associated with the event. For example, if an event contains process ID 105, "105" is the process ID.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	destinationUserPrivileges	dpriv	String	1023	The typical values are “Administrator”, “User”, and “Guest”. This identifies the destination user’s privileges. In UNIX, for example, activity executed on the root user would be identified with destinationUser Privileges of “Administrator”.
0.1	destinationProcessName	dproc	String	1023	The name of the event’s destination process. Example: “telnetd” or “sshd”.
0.1	destinationPort	dpt	Integer		The valid port numbers are between 0 and 65535.
0.1	destinationAddress	dst	IpAddress		Identifies the destination address that the event refers to in an IP network. The format is an IPv4 address. Example: “192.168.10.1”
0.1	deviceTimeZone	dtz	String	255	The timezone for the device generating the event.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	destinationUserId	duid	String	1023	Identifies the destination user by ID. For example, in UNIX, the root user is generally associated with user ID 0.
0.1	destinationUserName	duser	String	1023	Identifies the destination user by name. This is the user associated with the event's destination. Email addresses are often mapped into the UserName fields. The recipient is a candidate to put into this field.
0.1	deviceAddress	dvc	IpAddress		Identifies the device address that an event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1".
0.1	deviceHostName	dvchost	String	63	The format should be a fully qualified domain name (FQDN) associated with the device node, when a node is available. Example: "host.domain.com" or "host".

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	destinationMacAddress	dmac	MacAddress		Six colon-separated hexadecimal numbers. Example: “00:0D:60:AF:1B:61”
0.1	deviceProcessId	dvcpid	Integer		Provides the ID of the process on the device generating the event.
0.1	endTime	end	DateTime		The time at which the activity related to the event ended. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1 st 1970). An example would be reporting the end of a session.
0.1	externalId	externalId	String	40	The ID used by an originating device. They are usually increasing numbers, associated with events.
0.1	fileCreateTime	fileCreateTime	DateTime		Time when the file was created.
0.1	fileHash	fileHash	String	255	Hash of a file.
0.1	fileId	fileId	String	1023	An ID associated with a file could be the inode.
0.1	fileModificationTime	fileModificationTime	DateTime		Time when the file was last modified.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	filePath	filePath	String	1023	Full path to the file, including file name itself. Example: C:\Program Files \WindowsNT\Accessories\wordpad.exe or /usr/bin/zip
0.1	filePermission	filePermission	String	1023	Permissions of the file.
0.1	fileType	fileType	String	1023	Type of file (pipe, socket, etc.)
0.1	flexDate1	flexDate1	DateTime		A timestamp field available to map a timestamp that does not apply to any other defined timestamp field in this dictionary. Use all flex fields sparingly and seek a more specific, dictionary supplied field when possible. These fields are typically reserved for customer use and should not be set by vendors unless necessary.
0.1	flexDate1Label	flexDate1Label	String	128	The label field is a string and describes the purpose of the flex field.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	flexString1	flexString1	String	1023	One of four floating point fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. These fields are typically reserved for customer use and should not be set by vendors unless necessary.
0.1	flexString1Label	flexString1Label	String	128	The label field is a string and describes the purpose of the flex field.
0.1	flexString2	flexString2	String	1023	One of four floating point fields available to map fields that do not apply to any other in this dictionary. Use sparingly and seek a more specific, dictionary supplied field when possible. These fields are typically reserved for customer use and should not be set by vendors unless necessary.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	flexString2Label	flexString2Label	String	128	The label field is a string and describes the purpose of the flex field.
0.1	fileName	fname	String	1023	Name of the file only (without its path).
0.1	fileSize	fsize	Long		Size of the file.
0.1	bytesIn	in	Integer		Number of bytes transferred inbound, relative to the source to destination relationship, meaning that data was flowing from source to destination.
0.1	message	msg	String	1023	An arbitrary message giving more details about the event. Multi-line entries can be produced by using \n as the new line separator.
0.1	oldFileCreateTime	oldFileCreateTime	DateTime		Time when old file was created.
0.1	oldFileHash	oldFileHash	String	255	Hash of the old file.
0.1	oldFileId	oldFileId	String	1023	An ID associated with the old file could be the inode.
0.1	oldFileModificationTime	oldFileModificationTime	DateTime		Time when old file was last modified.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	oldFileName	oldFileName	String	1023	Name of the old file.
0.1	oldFilePath	oldFilePath	String	1023	Full path to the old file, including the file name itself. Examples: c:\Program Files\WindowsNT\Accessories\wordpad.exe or /usr/bin/zip
0.1	oldFilePermission	oldFilePermission	String	1023	Permissions of the old file.
0.1	oldFileSize	oldFileSize	Long		Size of the old file.
0.1	oldFileType	oldFileType	String	1023	Type of the old file (pipe, socket, etc.)
0.1	bytesOut	out	Integer		Number of bytes transferred outbound relative to the source to destination relationship. For example, the byte number of data flowing from the destination to the source.
0.1	eventOutcome	outcome	String	63	Displays the outcome, usually as 'success' or 'failure'.
0.1	transportProtocol	proto	String	31	Identifies the Layer-4 protocol used. The possible values are protocols such as TCP or UDP.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	reason	reason	String	1023	The reason an audit event was generated. For example “badd password” or “unknown user”. This could also be an error or return code. Example: “0x1234”
0.1	requestUrl	request	String	1023	In the case of an HTTP request, this field contains the URL accessed. The URL should contain the protocol as well. Example: “http://www/secure.com”
0.1	requestClientApplication	requestClientApplication	String	1023	The User-Agent associated with the request.
0.1	requestContext	requestContext	String	2048	Description of the content from which the request originated (for example, HTTP Referrer)
0.1	requestCookies	requestCookies	String	1023	Cookies associated with the request.
0.1	requestMethod	requestMethod	String	1023	The method used to access a URL. Possible values: “POST”, “GET”, etc.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceReceiptTime	rt	DateTime		The time at which the event related to the activity was received. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1 st 1970)
0.1	sourceHostName	shost	String	1023	Identifies the source that an event refers to in an IP network. The format should be a fully qualified domain name (FQDN) associated with the source node, when a mode is available. Examples: "host" or "host.domain.com".
0.1	sourceMacAddress	smac	MacAddress		Six colon-separated hexadecimal numbers. Example: "00:0D:60:AF:1B:61"
0.1	sourceNtDomain	sntdom	String	255	The Windows domain name for the source address.
0.1	sourceDnsDomain	sourceDnsDomain	String	255	The DNS domain part of the complete fully qualified domain name (FQDN).

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	sourceServiceName	sourceServiceName	String	1023	The service that is responsible for generating this event.
0.1	sourceTranslatedAddress	sourceTranslatedAddress	IpAddress		Identifies the translated source that the event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1".
0.1	sourceTranslatedPort	sourceTranslatedPort	Integer		A port number after being translated by, for example, a firewall. Valid port numbers are 0 to 65535.
0.1	sourceProcessId	spid	Integer		The ID of the source process associated with the event.
0.1	sourceUserPrivileges	spriv	String	1023	The typical values are "Administrator", "User", and "Guest". It identifies the source user's privileges. In UNIX, for example, activity executed by the root user would be identified with "Administrator".
0.1	sourceProcessName	sproc	String	1023	The name of the event's source process.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	sourcePort	spt	Integer		The valid port numbers are 0 to 65535.
0.1	sourceAddress	src	IpAddress		Identifies the source that an event refers to in an IP network. The format is an IPv4 address. Example: "192.168.10.1".
0.1	startTime	start	DateTime		The time when the activity the event referred to started. The format is MMM dd yyyy HH:mm:ss or milliseconds since epoch (Jan 1 st 1970)

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	sourceUserId	suid	String	1023	Identifies the source user by ID. This is the user associated with the source of the event. For example, in UNIX, the root user is generally associated with user ID 0.
0.1	sourceUserName	suser	String	1023	Identifies the source user by name. Email addresses are also mapped into the UserName fields. The sender is a candidate to put into this field.
0.1	type	type	TypeEnumeration		0 means base event, 1 means aggregated, 2 means correlation, and 3 means action. This field can be omitted for base events (type 0).

CEF Key Names for Event Consumers

This table displays the CEF names along with the full names for each name. When sending events, the CEF key name is the proper form to use. If you use the full name to send an event, then it will fail.

CEF Key Names For Event Consumers

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	agentDnsDomain	agentDnsDomain	String	255	The DNS domain name of the ArcSight connector that processed the event.
0.1	agentNtDomain	agentNtDomain	String	255	
0.1	agentTranslatedAddress	agentTranslatedAddress	IpAddress		
0.1	agentTranslatedZoneExternalID	agentTranslatedZoneExternalID	String	200	
0.1	agentTranslatedZoneURI	agentTranslatedZoneURI	String	2048	
0.1	agentZoneExternalID	agentZoneExternalID	String	200	
0.1	agentZoneURI	agentZoneURI	String	2048	
0.1	agentAddress	agt	IpAddress		The IP address of the ArcSight connector that processed the event.
0.1	agentHostName	ahost	String	1023	The hostname of the ArcSight connector that processed the event.
0.1	agentId	aid	String	40	The agent ID of the ArcSight connector that processed the event.
0.1	agentMacAddress	amac	MacAddress		The MAC address of the ArcSight connector that processed the event.

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	agentReceiptTime	art	DateTim e		The time at which information about the event was received by the ArcSight connector.
0.1	agentType	at	String	63	The agent type of the ArcSight connector that processed the event
0.1	agentTimeZone	atz	String	255	The agent time zone of the ArcSight connector that processed the event.
0.1	agentVersion	av	String	31	The version of the ArcSight connector that processed the event.
0.1	customerExternalID	customerExternalID	String	200	
0.1	customerURI	customerURI	String	2048	
0.1	destinationTranslatedZoneExternalID	destinationTranslatedZoneExternalID	String	200	
0.1	destinationTranslatedZoneURI	destinationTranslatedZoneURI	String	2048	The URI for the Translated Zone that the destination asset has been assigned to in ArcSight.
0.1	destinationZoneExternalID	destinationZoneExternalID	String	200	
0.1	destinationZoneURI	destinationZoneURI	String	2048	The URI for the Zone that the destination asset has been assigned to in ArcSight.
0.1	deviceTranslatedZoneExternalID	deviceTranslatedZoneExternalID	String	200	

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	deviceTranslatedZoneURI	deviceTranslatedZoneURI	String	2048	The URI for the Translated Zone that the device asset has been assigned to in ArcSight.
0.1	deviceZoneExternalID	deviceZoneExternalID	String	200	
0.1	deviceZoneURI	deviceZoneURI	String	2048	Thee URI for the Zone that the device asset has been assigned to in ArcSight.
0.1	destinationGeoLatitude	dlat	Double		The latitudinal value from which the destination's IP address belongs.
0.1	destinationGeoLongitude	dlong	Double		The longitudinal value from which the destination's IP address belongs.
0.1	eventId	eventId	Id		This is a unique ID that ArcSight assigns to each event.
0.1	rawEvent	rawEvent	String	4000	
0.1	sourceGeoLatitude	slat	Double		
0.1	sourceGeoLongitude	slong	Double		
0.1	sourceTranslatedZoneExternalID	sourceTranslatedZoneExternalID	String	200	
0.1	sourceTranslatedZoneURI	sourceTranslatedZoneURI	String	2048	The URI for the Translated Zone that the destination asset has been assigned to in ArcSight.
0.1	sourceZoneExternalID	sourceZoneExternalID	String	200	

Implementing ArcSight Common Event Format (CEF) - Version 27
 ArcSight Extension Dictionary

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
0.1	sourceZoneURI	sourceZoneURI	String	2048	The URI for the Zone that the source asset has been assigned to in ArcSight.
1.2	agentTranslatedZoneKey	agentTranslatedZoneKey	Long	64-bit	ID of an agentTranslatedZone resource reference.
1.2	agentZoneKey	agentZoneKey	Long	64-bit	ID of an agentZone resource reference.
1.2	customerKey	customerKey	Long	64-bit	ID of a customer resource reference.
1.2	destinationTranslatedZoneKey	destinationTranslatedZoneKey	Long	64-bit	ID of a destinationTranslatedZone resource reference.
1.2	destinationZoneKey	dZoneKey	Long	64-bit	ID of a destinationZone resource reference.
1.2	deviceTranslatedZoneKey	deviceTranslatedZoneKey	Long	64-bit	ID of a deviceTranslatedZone resource reference.
1.2	deviceZoneKey	deviceZoneKey	Long	64-bit	ID of a deviceZone resource reference.
1.2	sourceTranslatedZoneKey	sTranslatedZoneKey	Long	64-bit	ID of a sourceTranslatedZone resource reference.

CEF Specification Version	CEF Field Name	CEF Key Name / Abbreviation	Data Type	Length / Size	Description
1.2	sourceZoneKey	sZoneKey	Long	64-bit	ID of a sourceZone resource reference.
1.2	parserVersion	parserVersion	String	8	The release timestamp (DD-MM-YY) of the parser file that processed the event.
1.2	parserIdentifier	parserIdentifier	String	36	The parser ID of the parser file that processed the event.

Special Mappings

In some cases, the mappings between fields of the original device and those of the ArcSight Extension Dictionary are not obvious. In that case, refer to the example in the following tables.

Firewall

Original Field	Mapped to CEF Name	Mapped to Full Name
Rule Number / ACL Number	cs1	deviceCustomString1

Anti-Virus

Original Field	Mapped to CEF Name	Mapped to Full Name
Virus name	cs1	deviceCustomString1
Signature / Engine Version	cs2	deviceCustomString2
Action (Quarantine, Cleaned, Deleted, ...)	act	deviceAction

Email

Original Field	Mapped to CEF Name	Mapped to Full Name
Recipient (for example, user@company.com)	duser	destinationUserName
Sender (for example, user@company.com)	suser	sourceUserName
Relay	cs1	deviceCustomString1

Wireless

Original Field	Mapped to CEF Name	Mapped to Full Name
SSID	cs2	deviceCustomString2
Channel	cn1	deviceCustomNumber1

IPv6 Format

The connector code automatically sets labels for the **IPv6 address** fields if the field is set. You can set the label to the following values: **Device IPv6 Address**, **Source IPv6 Address**, and **Destination IPv6 Address**.

If the custom extension name is in IPv6 format and used to map:

- device address, then use **c6a1**. Use **Device IPv6 Address** as the label, or let the connector code set the label for you.
- source address, then use **c6a2**. Use **SourceIPv6 Address** as the label, or let the connector code set the label for you.
- destination address, then use **c6a3**. Use **Destination IPv6 Address** as the label, or let the connector code set the label for you.

User-Defined Extensions

The Extension Dictionary provides a set of predefined extension names (CEF names such as "fname" and full names such as "filetype") that must cover most event log requirements. However, vendors' devices might generate more information that can be appropriately mapped into the predefined extensions or might generate information that

does not fit the orientation of the predefined extensions. In such cases, vendors can define their own custom extensions.

Custom Extension Naming Guidelines

Ensure the following when creating custom extensions:

Format

Custom extension names must take the form:
VendornameProductnameExplanatoryKeyName

Requirements

Custom extension names must meet the following requirements. Custom extension name(s) must be:

- a single word, with no spaces.
- alphanumeric.
- as clear and concise as possible.
- named different than any name listed in ArcSight Extension Dictionary.

Limitations of Custom Extensions

Custom extension names are recommended for use only when no reasonable mapping of the information can be established for a predefined CEF name. While the custom extension name mechanism can be used to safely send information to CEF consumers for storage, there are certain limitations as to when and how to access the data mapped into them.

Custom extension names also have significant limitations that implementers should be aware of. These limitations can fundamentally affect the experience of ArcSight product users.

Limitations Affecting ArcSight ESM

- Data submitted to ArcSight ESM using custom name extensions is retained, but is largely inaccessible except when directly viewing events. This data shows up in a section called "Additional Data".

- Data submitted to ArcSight ESM using custom name extensions cannot be used directly for reporting, as these "Additional Data" fields are not made available in the reporting schema. Thus, any data in the "Additional Data" section of events is not available in reports.
- Data submitted to ArcSight ESM using custom name extensions cannot be used directly for event correlation (as within Rules, Data Monitors, etc.). Therefore, any data in the "Additional Data" section is not available as output for correlation activities within the ESM system.

Limitations Affecting ArcSight Logger

- Data submitted to ArcSight Logger using custom name extensions is retained in the system, but is not available for use in the Logger reporting infrastructure.
- Data submitted to ArcSight Logger using custom name extensions is available for viewing by the customer using string-based search. Event export is also available for this purpose.

Appendix A: Date Formats

CEF supports several variations on time and date formats to accurately identify the time an event occurred. These formats are as follows:

- Milliseconds since January 1, 1970 (integer).

This time format supplies an integer with the count in milliseconds from January 1, 1970 to the time the event occurred.

- MMM dd HH:mm:ss.SSS zzz
- MMM dd HH:mm:ssss.SSS
- MMM dd HH:mm:ss zzz
- MMM dd HH:mm:ss
- MMM dd yyyy HH:mm:ss.SSS zzz
- MMM dd yyyy HH:mm:ss.SSS
- MMM dd yyyy HH:mm:ss zzz
- MMM dd yyyy HH:mm:ss

For a key to the date formats shown above, refer to the [SimpleDateFormat](#) page from the API specification for the Java™ Platform, Standard Edition document.

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 Implementing ArcSight Common Event Format (CEF) - Version 27
(SmartConnectors 24.3)**

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 MFI-Documentation-Feedback@opentext.com .

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector ..	41
Product Overview	42
Event Log Categories	42
WiNC Features	43
Custom Log Support	43
Event Filtering	44
Globally Unique Identifier (GUID)	44
Host Browsing	44
IPv6	44
Localization	44
Collect Forwarded Events	45
Supported Log Sources	45
Configuring Windows	47
Enabling Microsoft Windows Event Log Audit Policies	47
Enabling an Auditing Policy on a Local System	48
Setting Up an Audit Policy Within a Domain	49
Setting Up an Audit Policy for a Domain	49
Setting Up Standard User Accounts	50
Standard Domain User Account from Windows Server Domain Controllers ..	50
Standard Domain User Account from Domain Members	51
Standard Local User Account from Windows Workgroup Hosts	51
Add Security Certifications when Using SSL	52
Example: Windows Server 2012	52
Enabling FIPS at the OS Level	55
Configuring Log Sources	56
Microsoft Active Directory	56
Configuring an Audit Policy Setting for a Domain Controller	56
Configuring Auditing for Specific Active Directory Objects	57
Microsoft ADFS	59
Configuring Microsoft ADFS Logs	60
Microsoft Antimalware	60
Microsoft DNS Server Analytics	60
Configuring Microsoft DNS Server Analytic Logs	60
Microsoft Exchange Mailbox Access Auditing	61

Configuring Mailbox Access Auditing	61
Viewing Logged Events	65
Microsoft Exchange Mailbox Store	65
Configuring Mailbox Store Auditing	66
Enabling Mailbox Store	66
Accessing the Audited Information	67
Changing Default Log Storage location	68
Excluding Service Accounts	69
Microsoft Forefront Protection 2010	69
Configuring Forefront Protection	70
Microsoft Local Administrator Password Solution	70
Configuring Microsoft Local Administrator Password Solution	70
Microsoft Netlogon	71
Configuring Microsoft Netlogon Logs	71
Microsoft Network Policy Server	72
Configuring NPS Logging	72
Microsoft Remote Access	73
Configuring Remote Access	73
Microsoft Service Control Manager	73
Microsoft SQL Server Audit	73
Configuring SQL Server Audit	74
Customizing Event Source Mapping	74
Microsoft Sysmon	74
Configuring Microsoft Sysmon Logs	74
Microsoft Windows AppLocker	75
Configuring Microsoft Windows AppLocker	75
Microsoft Windows BITS Client Logs	75
Configuring Microsoft Windows BITS Client Event Logs	75
Microsoft Windows Defender Antivirus	75
Microsoft Windows Defender AntiVirus	75
Microsoft Windows ESENT	76
Microsoft Windows Event	76
Microsoft Windows Hyper V	76
Configuring Microsoft Windows Hyper V Logs	76
Microsoft Powershell	76
Auditing Powershell Objects in Windows	77
Configure an Audit Policy Setting for a Domain Controller	77
Configuring Auditing for Specific Powershell Objects	78

Microsoft Windows Update Client	80
Configuring Windows Update Client	80
Microsoft Windows WMI Activity Trace	81
Microsoft Windows WMI Analytic and Operation	81
Microsoft WINS Server	81
Configuring WINS Server for Event Collection	82
Oracle Audit	82
Configuring Auditing	82
Enabling Auditing	82
Auditing Administrative Users	83
Symantec Mail Security	83
Event Logging	83
Installing the SmartConnector	84
Installation Requirements	84
.NET Requirements	84
Preparing to Install the SmartConnector	84
SmartConnector Setup Scenarios	85
Installing and Configuring the SmartConnector	85
Using SSL for Connection (optional)	92
Post-Installation Permissions	92
Configuring Custom Logs and Filtering	93
Configuring Filter	94
Specifying Custom Log Names	95
Collecting Forwarded Events	96
Event Collector for Windows Event Forwarding	97
Source Hosts Windows OS Version	97
Additional Connector Configurations	98
Configuring Custom Logs and Filtering	98
Configuring Filter	100
Specifying Custom Log Names	101
Configuring the Host Browsing Thread Sleep Time	102
Creating a Source Hosts File	103
Collecting Events from the Event Log	103
Configuring Advanced Options	104
Accessing Advanced Parameters	104
Advanced Container Configuration Properties	105
Advanced Common Configuration Parameters	106

Advanced Configuration Parameters per Host	106
Advanced Configuration Parameters for SID and GUID Translation	107
Customizing Event Source Mapping	107
Creating an Override Map File	107
Customizing Event Parsing in a Clustered Environment	108
Creating Custom Parsers for System and Application Events	109
Before Creating a Parser	109
Creating and Deploying Your Own Parser	110
Customizing Localization Support	114
Configuring Log Sources	117
Event Mappings for Active Directory	117
General Mappings	117
NTDS Database Mappings	117
Event 1000	117
Event 1394	118
Event 1404	118
Event 1844	118
Event 2064	118
Event 2065	118
Event 2886	119
Windows 2022 NTDS Database Mappings	119
Event 1009	119
Event 1013	119
Event 1133	120
Event 1166	120
Event 1167	120
Event 1197	120
Event 1257	121
Event 1258	121
Event 1260	121
Event 1261	121
Event 1481	122
Event 1515	122
Event 1516	122
Event 1517	122
Event 1518	123
Event 1544	123

Event 1585	123
Event 1904	123
Windows 2008 NTDS Database Mappings	124
General	124
Event 1000	124
Event 1394	124
Event 1404	124
Event 1844	124
Event 2064	125
Event 2065	125
Event 2886	125
Windows 2008 General NTDS Mappings	126
Event 1000	126
Event 1004	126
Event 1104	126
Event 1126	126
Event 1308	127
Event 1394	127
Event 1463	127
Event 1844	127
Event 1863	128
Event 1864	128
Event 1869	129
Event 1898	129
Event 1925	129
Event 1926	129
Event 2013	130
Event 2014	130
Event 2041	130
Event 2064	131
Event 2087	131
Event 2088	132
Event 2092	132
Event 2886	133
General NTDS Mappings	133
Event 1000	133
Event 1004	133
Event 1104	134

Event 1126	134
Event 1308	134
Event 1394	135
Event 1463	135
Event 1844	135
Event 1863	135
Event 1864	136
Event 1869	136
Event 1898	136
Event 1925	137
Event 1926	137
Event 2013	137
Event 2014	138
Event 2041	138
Event 2064	138
Event 2087	138
Event 2088	139
Event 2092	139
Event 2886	140
NTDS ISAM Mappings	140
Event 102	140
Event 103	140
Event 300	141
Event 301	141
Event 302	141
Event 609	141
Event 611	142
Event 612	142
Event 614	142
Event 626	142
Event 700	143
Event 701	143
Event 702	143
Event 703	143
Event 704	143
Windows 2008 NTDS ISAM Mappings	144
Event 102	144
Event 103	144

Event 300	144
Event 301	144
Event 302	144
Event 609	145
Event 611	145
Event 612	145
Event 614	145
Event 626	146
Event 700	146
Event 701	146
Event 702	146
Event 703	147
Event 704	147
NTDS KCC Mappings	147
Event 1104	147
Event 1128	147
Event 1308	148
Event 1926	148
Windows 2008 NTDS KCC Mappings	149
Event 1104	149
Event 1128	149
Event 1308	149
Event 1926	150
Windows 2008 NTDS LDAP Mappings	150
Event 1000	150
Event 1004	150
Event 1126	151
Event 1220	151
Event 1308	151
Event 1394	151
Event 1869	152
Event 2087	152
Event 2088	153
Event 2886	154
Event 2887	155
NTDS Replication Mappings	155
Event 1188	155
Event 1232	156

Event 1863	156
Event 2087	157
Event 2092	157
Event 2887	158
Windows 2008 NTDS Replication Mappings	158
Event 1188	158
Event 1232	159
Event 1863	159
Event 2087	160
Event 2092	160
Event 2887	161
NTDS LDAP Mappings	161
Event 1000	161
Event 1004	161
Event 1126	162
Event 1138	162
Event 1139	162
Event 1213	162
Event 1215	162
Event 1216	163
Event 1220	163
Event 1308	163
Event 1317	163
Event 1394	164
Event 1535	164
Event 1655	164
Event 1869	164
Event 2041	165
Event 2087	165
Event 2088	166
Event 2089	166
Event 2886	167
Event 2887	167
Event 2889	168
Windows 2008 NTDS LDAP Mappings	168
Event 1000	168
Event 1004	168
Event 1126	168

Event 1220	169
Event 1308	169
Event 1394	169
Event 1869	169
Event 2087	170
Event 2088	170
Event 2886	171
Event 2887	172
Event Mappings for Microsoft ADFS	172
General - Windows Server 2022	172
Event 100	172
Event 102	173
Event 103	173
Event 105	173
Event 106	173
Event 111	174
Event 221	175
Event 227	175
Event 249	175
Event 298	176
Event 299	176
Event 300	176
Event 307	177
Event 309	177
Event 342	177
Event 352	178
Event 397	178
Event 403	178
Event 404	179
Event 405	180
Event 406 - Windows Server 2016	180
Event 406 - Windows Server 2019	181
Event 410	181
Event 411	182
Event 412	182
Event 413	183
Event 418	183
Event 420	183

Event 424	184
Event 431	184
Event 510	185
Event 512	185
Event 513	185
Event 515	186
Event 516	186
Event 575	187
Event 1000	187
Event 1102	188
Event 1200	188
Event 1201	188
Event 1202	188
Event 1203	188
Event 1204	189
Event 1205	189
Event 1206	189
Event 1210	189
Common Mappings for Events - 1200, 1201, 1202, 1203, 1204, 1205, 1206, and 1210	189
Event Mappings for Microsoft Antimalware	190
Windows 2012	191
Event 1000	191
Event 1001	191
Event 1002	192
Event 1005	192
Event 1011	192
Event 1013	193
Event 1116	193
Event 1117	195
Event 1150	196
Event 2000	196
Event 2001	197
Event 2002	197
Event 2010	198
Event 2011	198
Event 3002	199
Event 5000	199

Event 5001	199
Event 5004	199
Event 5007	200
Event 5010	200
Event 5012	200
Windows 2008 R2	200
General	200
Event 20088	200
Event 20106	201
Event 20184	201
Event 20249	201
Event 20252	201
Event 20255	202
Event 20258	202
Event 20266	202
Event 20271	203
Event 20272	203
Event 20274	204
Event 20275	204
Event Mappings for Microsoft DNS Server Analytics	205
Event Mappings	205
General	205
Event 256	205
Event 257	206
Event 258	207
Event 259	208
Event 260	208
Event 261	209
Event 262	210
Event 263	211
Event 264	212
Event 265	212
Event 266	213
Event 267	213
Event 268	214
Event 269	215
Event 270	215
Event 271	216

Event 272	217
Event 273	217
Event 274	218
Event 275	218
Event 276	218
Event 277	219
Event 278	219
Event 279	220
Event 280	220
Windows 2008 R2	221
General	221
Event 20088	221
Event 20106	222
Event 20184	222
Event 20249	222
Event 20252	222
Event 20255	223
Event 20258	223
Event 20266	223
Event 20271	224
Event 20272	224
Event 20274	225
Event 20275	225
Microsoft Exchange Mailbox Access Auditing	226
Events 10100, 10101	226
Event 10102	226
Events 10104,	227
Event Mappings for Microsoft Exchange Mailbox Store	228
General Exchange Events	228
Event 1016	228
Device Event Mapping to ArcSight Fields	228
Windows 2008	228
General	228
Event 7000	229
Event 7001	229
Event 7002	229
Event 7003	229
Event 7004	229

Event ID 7005	229
Event 7006	230
Event 7007	230
Event 7008	230
Event ID 7010	230
Event 7012	230
Event 7015	230
Event 7018	230
Event 7021	231
Event 7024	231
Event 7025	231
Event 7026	231
Event 7028	231
Event 7033	231
Event 7035	231
Event 7040	232
Event 7044	232
Event 7046	232
Event 7048	232
Event 7051	232
Event 7064	232
FSC Controller	233
Event 1000	233
Event 1001	233
Event 1020	233
Event 1021	233
Event 1022	233
Event 1023	234
Event 1024	234
Event 1025	234
Event 1026	234
Event 1028	234
Event 1037	235
Event 1041	235
Event 1043	235
Event 1044	235
Event 2102	235
Event 5167	235

Event 5183	236
Event 8046	236
Event 8055	236
FSC Eventing	236
Event 1075	236
Event 1076	236
FSC Manual Scanner	237
Event 1045	237
Event 1048	237
Event 1052	237
FSC Scheduled Scanner	237
Event 2080	237
Event 2081	237
Event 3009	238
FSC Realtime Scanner	238
Event 2000	238
Event 2001	238
FSC Transport Scanner	238
Event 2007	238
Event 2008	238
Event 3002	239
FSC Monitor	239
Event 1007	239
Event 1008	239
Event 1013	239
Event 1014	240
FSE On Demand Nav	240
Event 1049	240
Event 1050	240
FSE Mail Pickup	240
Event 1029	240
Event 1030	240
FSE IMC	241
Event 1002	241
Event 1003	241
FSE VS API	241
Event 5066	241
FSC VSS Writer	241

Event 1094	241
Event 1095	241
Get Engine Files	242
Event 2011	242
Event 2012	242
Event 2017	242
Event 2034	242
Event 2109	243
Event 6012	243
Event 6014	243
Event 6019	244
Event 6020	244
Microsoft Local Administrator Password Solution	244
Event 5	244
Event 10	245
Event 11	245
Event 12	245
Event 13	245
Event 14	245
Event 15	246
Event 16	246
Mappings for Microsoft Netlogon	246
General	246
Event 5827	246
Event 5828	247
Event 5829	247
Event 5830	248
Event 5831	248
Mappings for Network Policy Server	249
Mappings for Windows 2016, 2012, and 8	249
General	249
Event 13	249
Event 25	249
Event 4400	250
Event 4402	250
Event 4405	250
Mappings for Windows 2008 R2	250
General	250

Event 13	251
Event 4400	251
Event 4402	251
Event 4405	251
Mappings for Remote Access Events	252
Mappings for Windows 2022, 2016, 2012, and 2012 R2	252
General	252
Event 600	252
608	252
Event 635	252
Event 653	252
Event 654	252
Event 670	253
Event 671	253
Event 672	253
Event 700	253
Event 827	253
Event 848	253
Event 20019	253
Event 20084	254
Event 20085	254
Event 20088	254
Event 20106	254
Event 20169	255
Event 20184	255
Event 20249	255
Event 20252	255
Event 20255	256
Event 20258	256
Event 20266	256
20271	257
Event 20272	257
Event 20274	258
Event 20275	259
Windows 2008 R2	259
General	259
Event 20088	259
Event 20106	259

Event 20184	260
Event 20249	260
Event 20252	260
Event 20255	261
Event 20258	261
Event 20266	261
Event 20271	262
Event 20272	262
Event 20274	263
Event 20275	263
Windows 2016, 2012, 8, and 10	264
General	264
Event 7000	264
Event 7001	264
Event 7002	265
Event 7003	265
Event 7005	265
Event 7006	265
Event 7007	265
Event 7008	266
Event 7009	266
Event 7010	266
Event 7011	266
Event 7012	266
Event 7015	266
Event 7016	267
Event 7017	267
Event 7018	267
Event 7019	267
Event 7020	267
Event 7021	268
Event 7022	268
Event 7023	268
Event 7024	268
Event 7025	268
Event 7026	269
Event 7027	269
Event 7028	269

Event 7030	269
Event 7031	269
Event 7032	270
Event 7033	270
Event 7034	270
Event 7035	271
Event 7036	271
Event 7037	271
Event 7038	271
Event 7039	272
Event 7040	272
Event 7041	272
Event 7042	273
Event 7043	273
Event 7045	273
Microsoft SQL Server Audit Application Event Log Mappings	274
General	274
Event 615	274
Event 849	274
Event 852	274
Event 919	274
Event 958	275
Event 1486	275
Event 1814	275
Event 1945	275
Event 2007	276
Event 2812	276
Event 3014	276
Event 3402	276
Event 3406	277
Event 3407	277
Event 3408	277
Event 3412	278
Event 3421	278
Event 3454	278
Event 4356	279
Event 5084	279
Event 5579	279

Event 5701	279
Event 5703	280
Event 6253	280
Event 6527	280
Event 8128	280
Event 9013	281
Event 9666	281
Event 9688	281
Event 9689	281
Event 10981	281
Event 12288	282
Event 12291	282
Event 15268	282
Event 15457	282
Event 15477	283
Event 17069	283
Event 17101	283
Event 17103	283
Event 17104	283
Event 17107	284
Event 17108	284
Event 17110	284
Event 17111	284
Event 17115	284
Event 17125	285
Event 17126	285
Event 17136	285
Event 17137	285
Event 17147	286
Event 17148	286
Event 17152	286
Event 17162	286
Event 17164	287
Event 17176	287
Event 17177	287
Event 17199	288
Event 17201	288
Event 17311	288

Event 17144	289
Event 17106	289
Event 17150	289
Event 17142	289
Event 17167	290
Event 17836	290
Event 17806	290
Event 17550	291
Event 17551	291
Event 17561	291
Event 17656	291
Event 17658	292
Event 17663	292
Event 17573	292
Event 17811	292
Event 18264	293
Event 18265	293
Event 18267	294
Event 18452	294
Event 18453	294
Event 18454	295
Event 18456	295
Event 18461	295
Event 18470	296
Event 18488	296
Event 18496	296
Event 19030	296
Event 19031	297
Event 19032	297
Event 19033	297
Event 26018	297
Event 26022	297
Event 26037	298
Event 26048	298
Event 26067	298
Event 26076	299
Event 30090	299
Event 33090	299

Event 33204	299
Event 33205	300
Event 33217	301
Event 33218	301
Event 49903	301
Event 49904	301
Event 49910	302
Event 49916	302
Event 49917	302
Microsoft Sysmon	302
Windows 2012	302
General	302
Event 1	303
Event 2	304
Event 3	304
Event 4	305
Event 5	305
Event 6	305
Event 7	306
Event 8	306
Event 9	307
Event 10	307
Event 11	308
Event 12	308
Event 13	309
Event 14	309
Event 15	309
Event 16	310
Event 17	310
Event 18	311
Event 19	311
Event 20	311
Event 21	312
Event 22	312
Event 23	313
Event 255	313
Windows 2008 R2	314
General	314

Event 20088	314
Event 20106	314
Event 20184	314
Event 20249	315
Event 20252	315
Event 20255	315
Event 20258	316
Event 20266	316
Event 20271	316
Event 20272	317
Event 20274	317
Event 20275	318
Mappings for Microsoft Windows AppLocker	318
Event 8001	318
Event 8002	318
Event 8003	319
Event 8004	319
Event 8005	320
Event 8006	320
Event 8007	321
Microsoft Windows BITS Event	321
Microsoft Windows BITS Client	322
General	322
Event 3	322
Event 4	322
Event 59	323
Event 60	323
Event 61	324
Windows 2008 R2	325
General	325
Event 20088	325
Event 20106	326
Event 20184	326
Event 20249	326
Event 20252	326
Event 20255	327
Event 20258	327
Event 20266	327

Event 20271	328
Event 20272	328
Event 20274	329
Event 20275	329
Microsoft Windows Defender Antivirus	330
Mappings for Microsoft Windows Defender AntiVirus	330
Event 1000	330
Event 1001	330
Event 1002	331
Event 1009	332
Event 1010	333
Event 1011	334
Event 1013	335
Event 1015	335
Event 1116	336
Event 1117	338
Event 1150	339
Event 1151	340
Event 2000	341
Event 2001	341
Event 2002	342
Event 2003	343
Event 2010	343
Event 2011	344
Event 2030	345
Event 2031	345
Event 2041	345
Event 3002	346
Event 3007	346
Event 5000	346
Event 5001	347
Event 5004	347
Event 5007	347
Event 5009	347
Event 5010	348
Event 5011	348
Event 5012	348
Event 5013	348

Windows 2008 R2	349
General	349
Event 20088	349
Event 20106	349
Event 20184	349
Event 20249	350
Event 20252	350
Event 20255	350
Event 20258	351
Event 20266	351
Event 20271	351
Event 20272	352
Event 20274	352
Event 20275	353
Microsoft Windows ESENT	353
Microsoft Windows ESENT	353
General	353
Event 102	354
Event 103	354
Event 105	354
Event 224	354
Event 225	355
Event 300	355
Event 301	355
Event 302	355
Event 325	356
Event 326	356
Event 327	356
Event 330	356
Event 335	357
Event 455	357
Event 641	357
Windows 2008 R2	358
General	358
Event 20088	358
Event 20106	358
Event 20184	359
Event 20249	359

Event 20252	359
Event 20255	360
Event 20258	360
Event 20266	360
Event 20271	361
Event 20272	361
Event 20274	362
Event 20275	362
Specific Windows Security Event Mappings	363
General	363
104	363
1100	363
1101	363
1102	364
1104	364
1105	364
Event Mappings for Microsoft Windows Hyper V	364
Event 1	364
Event 2	364
Event 129	365
Event 155	365
Event 156	365
Event 3086	365
Event 3452	365
Event 12006	366
Event 12010	366
Event 12030	366
Event 12148	366
Event 12514	366
Event 12520	367
Event 12582	367
Event 12597	367
Event 13002	367
Event 13003	367
Event 14070	368
Event 14090	368
Event 14092	368
Event 14094	368

Event 14100	368
Event 14104	369
Event 14108	369
Event 15266	369
Event 15310	369
Event 18304	369
Event 18500	370
Event 18502	370
Event 18504	370
Event 18508	370
Event 18510	370
Event 18512	371
Event 18514	371
Event 18596	371
Event 18600	371
Event 18602	371
Event 18609	372
Event 19020	372
Event 19040	372
Event 20410	372
Event 20790	372
Event 22052	373
Event 26000	373
Event 26002	373
Event 26004	373
Event 26006	373
Event 26012	374
Event 26016	374
Event 26018	374
Event 26026	374
Event 26074	374
Event 26078	375
Event 27262	375
Event 33012	375
Event 33201	375
Event 33205	375
Event 33452	376
Event 33454	376

Event 33456	376
Event 33458	376
Event 33480	376
Event 33481	377
Event 33483	377
Event 33834	377
Event 36000	377
Windows PowerShell Mappings	377
Event 400, 403	377
Event 500, 501	378
Event 600	379
Event 800	379
Windows Microsoft-Windows-PowerShell/Operational Mappings	380
Event 4100	380
Event 4103	381
Event 4104	381
Event 4105	382
Event 8193	382
Event 8194	382
Event 8195	382
Event 8196, 12039	383
Event 8197	383
Event 24577	383
Event 24579	383
Event 24580	383
Event 24581	384
Event 24582	384
Event 24583	384
Event 24584	384
Event 24592	384
Event 24593	384
Event 24594	385
Event 24595	385
Event 24596	385
Event 24597	385
Event 24598	386
Event 24599	386
Event 40961	386

Event 40962	386
Event 53249	387
Event 53250	387
Event 53504	387
Microsoft Windows Update Client	387
Windows 2012	388
General	388
Event 16	388
Event 17	388
Event 18	388
Event 19	389
Event 20	389
Event 21	389
Event 22	390
Event 27	390
Event 28	390
Event 43	390
Event 44	390
Windows 2008 R2	391
General	391
Event 20088	391
Event 20106	391
Event 20184	392
Event 20249	392
Event 20252	392
Event 20255	393
Event 20258	393
Event 20266	393
Event 20271	394
Event 20272	394
Event 20274	395
Event 20275	395
Microsoft Windows WMI Activity Trace	396
Event 11	396
Microsoft Windows WinRM Analytic	396
Event 6	396
Event 11	397
Event 15	397

Event 142	397
Event 161	397
Event 162	398
Event 169	398
Event 81	398
Event 82	398
Windows 2012	399
Event 788	399
Event 789	399
Event 1050	399
Event 1295	399
Windows 2016, 2012, and 8	400
General	400
Event 4097	400
Event 4098	400
Event 4119	400
Event 4143	400
Event 4178	401
Event 4179	401
Event 4180	401
Event 4181	401
Event 4224	401
Event 4252	402
Event 4253	402
Event 4309	402
Event 4318	402
Event 4325	402
Event 4326	402
Event 4329	403
Event 4330	403
Event 4337	403
Event 5001	403
Event 5002	403
Oracle Audit	403
Oracle Windows Event	404
General	404
Event 4	404
Event 5	404

Event 8	404
Event 12	405
Oracle Audit SYSDBA	405
Event 34	405
Oracle Audit Trail	406
Event 34	406
Oracle Unified Audit Trail	407
Event 36	407
Symantec Mail Security Mappings	408
General	408
Managed Components	408
Management Service	408
Microsoft Exchange	415
Event Mappings	454
Windows Common Security Mappings	455
Specific Windows Security Event Mappings	456
Event 1100	456
Event 1101	457
Event 1102	457
Event 1104	457
Event 1105	457
Event 1074	457
Event 4608	458
Event 4609	458
Event 4610	458
Event 4611	458
Event 4612	459
Event 4614	459
Event 4615	459
Event 4616	460
Event 4618	460
Event 4621	461
Event 4622	461
Event 4624	461
Event 4625	462
Event 4626	463
Event 4627	464
Event 4634	465

Event 4646	465
Event 4647	466
Event 4648	466
Event 4867	495
Event 4868	495
Event 4869	496
Event 4870	496
Event 4871	496
Event 4872	496
Event 4873	497
Event 4874	497
Event 4875	497
Event 4876	497
Event 4877	498
Event 4878	498
Event 4879	498
Event 4880	498
Event 4881	498
Event 4882	499
Event 4883	499
Event 4884	499
Event 4885	499
Event 4886	500
Event 4887	500
Event 4888	500
Event 4889	500
Event 4890	500
Event 4891	501
Event 4892	501
Event 4893	501
Event 4894	501
Event 4895	501
Event 4896	502
Event 4897	502
Event 4898	502
Event 4899	502
Event 4900	502
Event 4902	502

Event 4904	503
Event 4905	503
Event 4906	503
Event 4907	504
Event 4908	504
Event 4909	504
Event 4910	504
Event 4911	505
Event 4912	505
Event 4913	505
Event 4928	506
Event 4929	506
Event 4930	506
Event 4931	506
Event 4932	507
Event 4933	507
Event 4934	507
Event 4935	507
Event 4936	507
Event 4937	507
Event 4944	507
Event 4945	508
Event 4946	508
Event 4947	508
Event 4948	508
Event 4949	508
Event 4950	508
Event 4951	509
Event 4952	509
Event 4953	509
Event 4954	509
Event 4956	509
Event 4957	509
Event 4958	510
Event 4960	510
Event 4961	510
Event 4962	510
Event 4963	510

Event 4964	511
Event 4965	511
Event 4976	511
Event 4977	512
Event 4978	512
Event 4979	512
Event 4980	512
Event 4981	512
Event 4982	513
Event 4983	513
Event 4984	513
Event 4985	514
Event 5024	514
Event 5025	514
Event 5027	514
Event 5028	515
Event 5029	515
Event 5030	515
Event 5031	515
Event 5032	515
Event 5033	516
Event 5034	516
Event 5035	516
Event 5037	516
Event 5038	516
Event 5039	517
Event 5040	517
Event 5041	517
Event 5042	517
Event 5043	517
Event 5044	518
Event 5045	518
Event 5046	518
Event 5047	518
Event 5048	518
Event 5049	518
Event 5050	519
Event 5051	519

Event 5056	519
Event 5057	519
Event 5058	520
Event 5059	520
Event 5060	521
Event 5061	521
Event 5062	521
Event 5063	521
Event 5064	522
Event 5065	522
Event 5066	522
Event 5067	523
Event 5068	523
Event 5069	523
Event 5070	523
Event 5071	524
Event 5120	524
Event 5121	524
Event 5122	524
Event 5123	525
Event 5124	525
Event 5125	525
Event 5126	525
Event 5127	525
Event 5136	526
Event 5137	526
Event 5138	526
Event 5139	527
Event 5140	527
Event 5141	527
Event 5142	528
Event 5143	528
Event 5144	529
Event 5145	529
Event 5146	530
Event 5147	530
Event 5152	530
Event 5153	531

Event 5154	531
Event 5155	531
Event 5156	532
Event 5157	532
Event 5158	533
Event 5159	533
Event 5168	534
Event 5376	534
Event 5377	535
Event 5378	535
Event 5379	535
Event 5380	536
Event 5381	536
Event 5382	537
Event 5440	537
Event 5441	537
Event 5442	537
Event 5443	538
Event 5444	538
Event 5446	538
Event 5447	538
Event 5448	538
Event 5449	538
Event 5450	539
Event 5451	539
Event 5452	539
Event 5453	539
Event 5456	540
Event 5457	540
Event 5458	540
Event 5459	540
Event 5460	540
Event 5461	540
Event 5462	541
Event 5463	541
Event 5464	541
Event 5465	541
Event 5466	541

Event 5467	542
Event 5468	542
Event 5471	542
Event 5472	542
Event 5473	542
Event 5474	543
Event 5477	543
Event 5478	543
Event 5479	543
Event 5480	543
Event 5483	544
Event 5484	544
Event 5632	544
Event 5633	544
Event 5712	545
Event 5888	545
Event 5889	545
Event 5890	546
Event 6144	546
Event 6145	546
Event 6272	546
Event 6273	547
Event 6274	547
Event 6275	548
Event 6276	548
Event 6277	548
Event 6278	548
Event 6279	549
Event 6280	549
Event 6281	549
Event 6409	550
Event 6410	550
Event 6416	550
Event 8191	550
Microsoft OAlerts	551
Event 300	551
Mappings for DNS Client Operational	551
Event 1015	551

Event 1016	551
Event 1017	552
Event 3006	552
Event 3008	552
Event 3009	552
Event 3010	553
Event 3011	553
Event 3012	553
Event 3013	554
Event 3014	554
Event 3016	554
Event 3018	554
Event 3019	555
Event 3020	555
Windows Event Log Event Descriptions by Category	556
 Troubleshooting	578
Unable to Receive Events from any Host if One or More Hosts were Down	578
Parameters Not Functioning as Expected	580
Log Message for Resource Adjustment	580
A Non-administrator User Is Unable to Run Windows Native Connector and the Log File Has Permission Error	580
Unable to extend buffer beyond 1048576	580
Connector is unable to receive events and displays error after upgrading to version 8.4.0	581
 Appendix: Internal Events	582
Specific Windows Security Event Mappings	582
General	582
104	582
1100	583
1101	583
1102	583
1104	583
1105	583
Collector Connected	584
Collector Disconnected	584
Collector Up	584
Collector Down	585

Collector Status Updated	585
Collector Status for “Collector Status Updated”	585
Host Status for “Collector Status Updated”	586
Event Log Status for “Collector Status Updated”	586
Collector Event Collection Started	587
Collector Status for “Collector Collection Started”	587
Host Status for “Collector Collection Started”	587
Event Log Status for “Collector Collection Started”	588
Collector Configuration Accepted	589
Collector Status for “Collector Configuration Accepted”	589
Host Status for “Collector Configuration Accepted”	589
Event Log Status for “Collector Configuration Accepted”	590
Send Documentation Feedback	591

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

ArcSight SmartConnectors intelligently collect a large amount of heterogeneous raw event data from security devices in an enterprise network, process the data into ArcSight security events, and transport data to destination devices.

To collect events from Microsoft Windows OS, use the ArcSight SmartConnector for Windows Event Log - Native (WiNC), which supports event collection from log sources such as Sysmon, Powershell etc.,

This guide provides a high level overview of WiNC. For supported installation platforms and log sources, see [Technical Requirements](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

Windows event logs record details related to the system, security, and application stored on a Windows operating system. They contain information about hardware and software events occurring on a Windows operating system and can be monitored to track system and some application issues or forecast any potential issues.

Windows event logs are stored in a standard format and consists of the following are the main elements:

- **Log name:** Name of the event log to which events from different logging components will be written such as system, security, and applications
- **Event date/time:** The date and time of the occurrence of event.
- **Task category:** The type of recorded event log.
- **Event ID:** A unique identifier for a specific logged event.
- **Source:** Name of the program or software , which generated the event log.
- **Level:** The severity level of the recorded event log, namely, Information, Error, Verbose, Warning, and Critical.
- **User:** Name of the user who logged onto the Windows computer when the event occurred.
- **Computer:** Name of the computer logging the event.

Event Log Categories

The Windows Event logs are classified into the following categories:

System Log: System logs contain events related to the system and its components such as failure to load the boot-start driver.

Application Log: Application logs contain events related to a software or an application hosted on a Windows computer such as failure to start Microsoft Word.

Security Log: Security logs contain events related to the safety of the system such as failed login attempts or file deletions that get recorded by using the Windows auditing process.

Setup Logs: Setup logs contain events that occur during the installation of the Windows operating system. On domain controllers, this logs also record events related to Active Directory.

Forwarded Event Logs: Forwarded event Logs contain event logs forwarded from other computers in the same network.

WiNC Features

The SmartConnector for Microsoft Windows Event Log – Native connects to local or remote machines inside a single domain or from multiple domains, to retrieve events from all types of event logs.

SmartConnectors collect real-time events, process, enrich data and improve efficiency. Data enrichment activities include normalization, categorization, Common Event Format (CEF), aggregation, and filtering. For information about SmartConnector capabilities in general, see [SmartConnector Features](#).

The infrastructure provided with the SmartConnector for Microsoft Windows Event Log – Native is capable of delivering critical features, such as Operational Windows Event Logs and event collection and event filtering from IPv6 hosts. It leverages the native technology on the Microsoft platform and provides the best support for Windows event features and capabilities (including collection for all log types).

The SmartConnector for Microsoft Windows Event Log – Native consists of the following major components:

- SmartConnector framework-based event processor.
- The Windows API application, which collects events from Microsoft Windows Event Logs.
- The Message Queue, which facilitates communication between the previous two components.

The Windows API event collection and the Message Queue components are started by the Connector at the time of Connector setup and at the start of the Connector process.

The security events are not audited by default. You must specify the type of security events to be audited.

Specific features of the Windows Event Log – Native connector are described in the following sections.

Custom Log Support

Supports event collection from non-administrative, operational, or custom logs.

Event Filtering

Supports filters that apply during event collection from the event source to the Connector. This enables you to filter unwanted events.

Globally Unique Identifier (GUID)

Supports translation and mapping of GUID (also known as UUID) within a forest (A forest is a complete instance of Active Directory). The Windows Event Log - Native SmartConnector can perform translation for GUIDs within a forest by querying the Global Catalog Server. The Global Catalog Server and Active Directory must be on the same machine. The Active Directory parameters are used for Global Catalog Server. The Connector is not configured to translate GUIDs by default. For more information about enabling GUID translation, see “[Advanced Configuration Parameters for SID and GUID Translation](#)”.

Host Browsing

Host browsing is used when hosts are added during installation by using Active Directory. Notification is sent to a destination when a new host is added to Active Directory.

IPv6

Supports event collection from IPv6 hosts and parsing of IPv6 events.

Localization

The Microsoft Windows Event Log - Native Connector supports security event localization for the following languages:

Language	Locale	Encoding
French	fr_CA	UTF-8
Japanese	ja_JP	Shift_JIS
Chinese Simplified	zh_CN	GB2312
Chinese Traditional	zh_TW	Big5

You can specify the locale and encoding for the event.name field during SmartConnector installation. See [Configuring Multiple Host Parameters](#). For localization of other languages, see [Customizing Localization Support for the Native Connector](#).

Collect Forwarded Events

The Connector reads events forwarded to a Windows Event Collector (WEC) host. WEC is a Microsoft capability that allows Windows host to collect events from multiple sources. Collecting forwarded events is different than traditional event collection, because the events are collected from multiple sources. For information about WEC functionality, refer to Microsoft Windows documentation.

To configure the Connector to collect forwarded events, see [Collecting Forwarded Events](#).

Supported Log Sources

Log Sources	Type of Logs	Event Mappings
Microsoft Active Directory	Application	Event Mappings for Microsoft Active Directory Logs
Microsoft ADFS	Security	Event Mappings for Microsoft ADFS Logs
Microsoft Antimalware	System	Event Mappings for Microsoft Antimalware Logs
Microsoft DNS Server Analytics	System	Event Mappings for Microsoft DNS Server Analytics Logs
Microsoft Exchange Mailbox Access Auditing	Application	Event Mappings for Microsoft Exchange Mailbox Access Auditing Logs
Microsoft Exchange Mailbox Store	Application	Event Mappings for Microsoft Exchange Mailbox Store Logs
Microsoft Forefront Protection	Applications	Event Mappings for Microsoft Forefront Protection Logs
Microsoft Local Admin Password Solution	System	Event Mappings for Microsoft Local Admin Password Solution Logs

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Product Overview

Log Sources	Type of Logs	Event Mappings
Microsoft Netlogon	System	Event Mappings for Microsoft Netlogon Logs
Microsoft Network Policy Server	System	Event Mappings for Microsoft Network Policy Server Logs
Microsoft Remote Access	System	Event Mappings for Microsoft Remote Access Logs
Microsoft Service Control Manager	System	Event Mappings for Microsoft Service Control Manager Logs
Microsoft SQL Server Audit Application	Application	Event Mappings for Microsoft SQL Server Audit Application Logs
Microsoft Sysmon	Custom	Event Mappings for Microsoft Sysmon Logs
Microsoft Windows AppLocker	System	Event Mappings for Microsoft Windows AppLocker Logs
Microsoft Windows BITS Client	Custom	Event Mappings for Microsoft Windows BITS Client Logs
Microsoft Windows Defender Antivirus	System	Event Mappings for Microsoft Windows Defender Antivirus Logs
Microsoft Windows ESENT	Application	Event Mappings for Microsoft Windows ESENT Logs
Microsoft Windows Event	System Security	Event Mappings for Microsoft Windows Event Logs
Microsoft Windows Hyper V	System Security	Event Mappings for Microsoft Windows Hyper V
Microsoft Windows Powershell	Application	Event Mappings for Microsoft Windows Powershell Logs

Log Sources	Type of Logs	Event Mappings
Microsoft Windows Update Client	System	Event Mappings for Microsoft Windows Update Client Logs
Microsoft Windows WINS Server	System	Event Mappings for Microsoft Windows WINS Server
Microsoft Windows WMI Activity Trace	Custom	Event Mappings for Microsoft Windows WMI Activity Trace Logs
Microsoft Windows WMI Analytic and Operational	System	Event Mappings for Microsoft Windows WMI Analytic and Operational Logs
Oracle Audit	Custom	Event Mappings for Oracle Audit
Symantec Mail Security for Exchange	Application	Symantec Mail Security for Exchange Server Logs

Configuring Windows

You must enable the appropriate auditing policies on Windows servers from which the connector collects information and also setup standard user accounts. This section has the following information:

Enabling Microsoft Windows Event Log Audit Policies

Because event information generated by Windows servers is based on the auditing policies that are enabled, make sure that appropriate auditing policies are enabled on Windows servers from which the connectors collect information.

Auditing events consumes system resources such as memory, processing power, and disk space. Auditing an excessive number of events can dramatically slow down your servers.



Note: You must be logged in as an administrator or a member of the Administrators group to set up audit policies. If your computer is connected to a network, network policy settings might also prevent you from setting up audit policies.

The method used to create an audit policy varies depending on whether the policy is being created on a member server, a domain controller, or a stand-alone server.

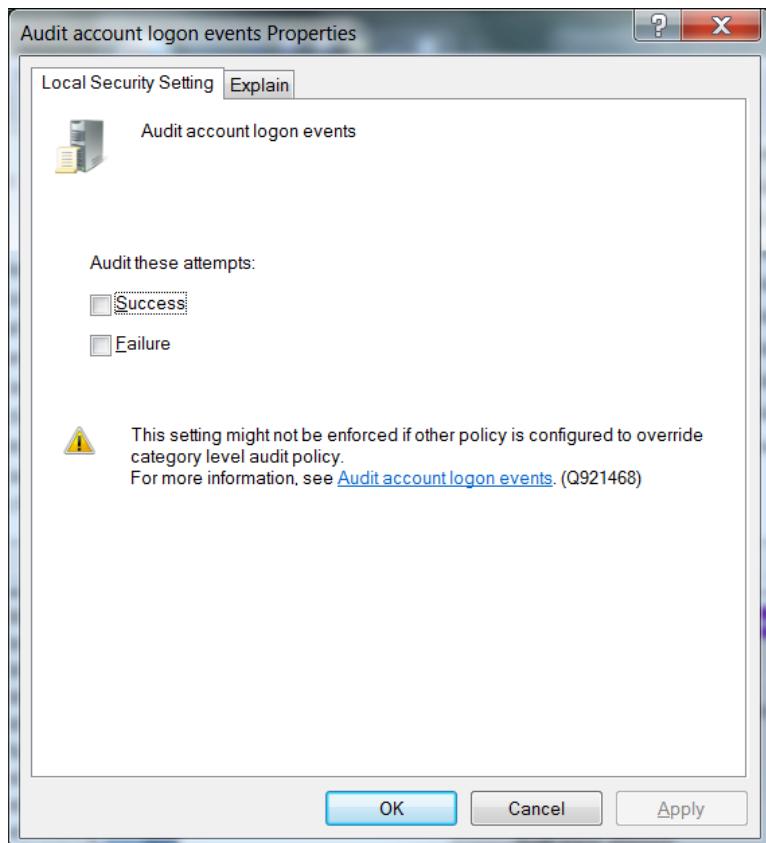
- To configure a domain controller, member server, or workstation, use **Active Directory Users and Computers**.
- To configure a system that does not participate in a domain, use **Local Security Settings**.

This section has the following information:

Enabling an Auditing Policy on a Local System

To establish an audit policy on a local system:

1. Select **Start > Control Panel > Administrative Tools > Local Security Policy**.
2. Double-click on **Local Policy** in the **Security Settings** tree to expand it.
3. Select **Audit Policy** from the tree. Doing so reveals the auditing information for that system.
4. To enable auditing for any of the areas, double-click on the type of audit. A dialog box similar to the following is displayed, letting you choose to perform a **Success** or a **Failure** audit (or both) on that type of event.





Note: To audit objects such as the Registry, printers, files, or folders, select the Object Access option. Otherwise, when you attempt to enable auditing for these objects, an error is displayed instructing you to make the necessary adjustments to the local audit policy (or, in the case of a domain environment, to the domain audit policy).

After you have enabled auditing, go through the system and fine-tune the type of events that will be audited in each category.

Setting Up an Audit Policy Within a Domain

To set up an audit policy for a domain controller:

1. Choose **Start > Programs > Administrative Tools > Active Directory Users and Computers.**
2. Navigate through the console tree to the domain you want to work with. Expand the domain.
3. Beneath the domain, you will see a **Computers** object and a **Domain Controllers** object. Select the appropriate object for your system and right-click on **Domain Controllers**. The Domain Controller's properties sheet is displayed.
4. Select the **Group Policy** tab. Select the group policy to which you want to apply the audit policy and click **Edit**.
5. Navigate through the tree to **Default Domain Controllers Policy > Computer Configuration > Windows Settings > Security Settings Local Policies > Audit Policy**.
6. When you select **Audit Policy**, a list of audit events is displayed in the right pane. To audit a group of events, double-click on the group; a dialog box is displayed that lets you enable **Success**, **Failure**, or both audits for that group of events.

After enabling auditing for a group of events, fine-tune the exact events you want to audit.

Setting Up an Audit Policy for a Domain

To set up auditing for all computers under a domain:

1. Click **Start > Administrative Tools > Domain Security Policy**.
2. Open **Default Domain Security Settings**.
3. Expand **Security Settings** if it is not already open.
4. Expand **Local Policy** and double-click on **Audit Policy**. A list of audit events is displayed in the right pane.

5. To audit a group of events, double-click on the group; a dialog box is displayed that lets you enable **Success**, **Failure**, or both audits for that group of events.

Setting Up Standard User Accounts

The connector does not require domain administrator privileges to collect Security events from Windows hosts. Event Log Reader privilege is required for system and custom application event collection including Forwarded Events Collection.

To configure the SmartConnector for Microsoft Windows Event Log – Native to use a Standard User account to collect Security events only from the target hosts, follow the steps provided in the following sections.

These steps describe how to configure and assign the privileges by creating a single user account such as **arcsight**. You can also create a group of users instead and follow the same steps provided for the configuration, assigning all the minimum privileges to the user group instead of the single user.



Note: Sometimes, although we have assigned appropriate privileges to the standard user, there could be other policies in your environment preventing the user account from accessing the security event logs. You can start identifying this problem by checking **Settings > Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security** options. There are many security policies defined that would require investigation; however, one policy to check right away is the **Network Access: Sharing and security model for local accounts**. Make sure this is set to **Classic – local users authenticate as themselves**.

Standard Domain User Account from Windows Server Domain Controllers

On the Windows Server Domain Controller:

1. Go to **Settings > Control Panel > Administrative Tools > Active Directory Users and Computers > <Domain of interest> > Users**.
2. Create a new **Domain User**, such as **arcsight**.
3. Go to **Settings > Control Panel > Administrative Tools > Active Directory Users and Computers > <Domain of interest> > Builtin**.
4. Open the properties of the security principal **Event Log Readers**.
5. From the **Members** tab, add the new Domain User **arcsight** to this security principal.

6. This Group Policy can take some time to take effect. To enable the policy immediately, run this command from the Windows Server Domain Controller and the Windows Domain Member command prompts:

```
GPUpdate /Force
```

This command will update any modifications you have made to any group policy, not just this one.

Standard Domain User Account from Domain Members

On the Windows Server Domain Controller:

1. Go to **Settings > Control Panel > Administrative Tools > Active Directory Users and Computers > <Domain of interest> > Users.**
2. Create a new Domain User, such as arcsight.
3. Go to **Settings > Control Panel > Administrative Tools > Group Policy Management > Default Domain Policy > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment.**
4. Open the **Manage auditing and security log** policy.
5. Enable **Define these Policy Settings** and add this new Domain User arcsight to this policy.
6. This Group Policy can take some time to take effect. To enable the policy immediately, run this command from the Windows Server Domain Controller and the Windows Domain Member command prompts:

```
GPUpdate /Force
```



Note: This command will update modifications to any group policy you have made, not just this one

Standard Local User Account from Windows Workgroup Hosts

On the Windows Workgroup host:

1. Go to **Settings > Control Panel > Administrative Tools > Computer Management > System Tools > Local Users and Groups > Users.**
2. Create a new **Local User**, such as arcsight.
3. Go to **Settings > Control Panel > Administrative Tools > Computer Management > System Tools > Local Users and Groups > Groups.**

4. Open the **Event Log Readers** group and add this new Local User arcsight to this group.
5. Go to **Settings > Control Panel > Administrative Tools > Local Security Policy > Security Settings > Local Policies > Security Options**.
6. Open the **Network access: Sharing and security model** for local accounts policy.
7. Set this policy to the option: **Classic – local users authenticate as themselves**.

Add Security Certifications when Using SSL

If you choose to use SSL as the connection protocol, security certificates for both the Windows Domain Controller Service and for the Active Directory Server are required. Installing a valid certificate on a domain controller permits the LDAP service to listen for, and automatically accept, SSL connections for both LDAP and global catalog traffic.

The certificates will be imported to the connector's certificate store during the connector installation process. See **step 3** of the installation procedure for instructions.

Procedures for Windows 2012 are shown; steps could vary with different Windows versions. For other Windows versions, see Microsoft's documentation for complete information.

Example: Windows Server 2012

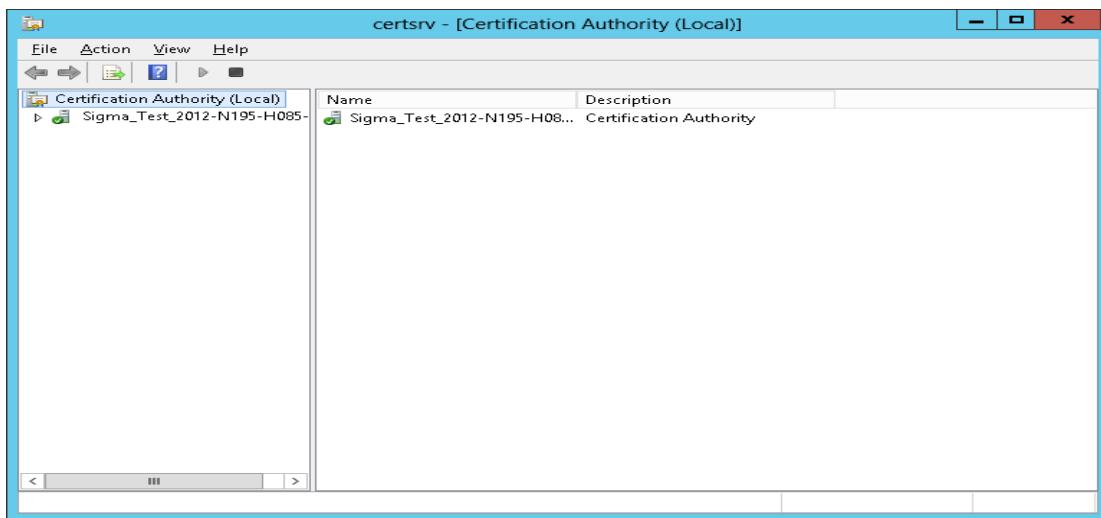
The following steps assume Windows Server 2012 as the operating system:

To export the certificates:

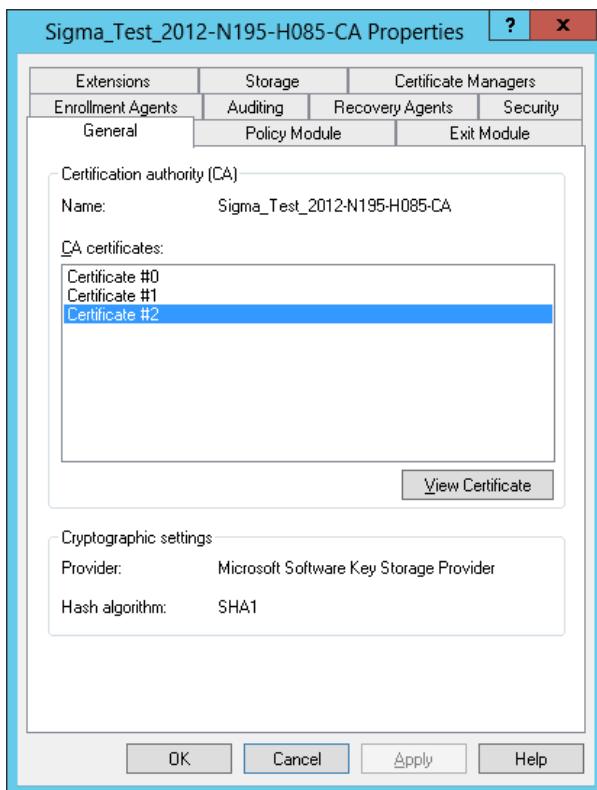
1. From the Windows **Start** menu, select **Administrative Tools**.
2. Select and double-click **Certification Authority**; one or more Domain Certificate Authority servers are shown.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Windows



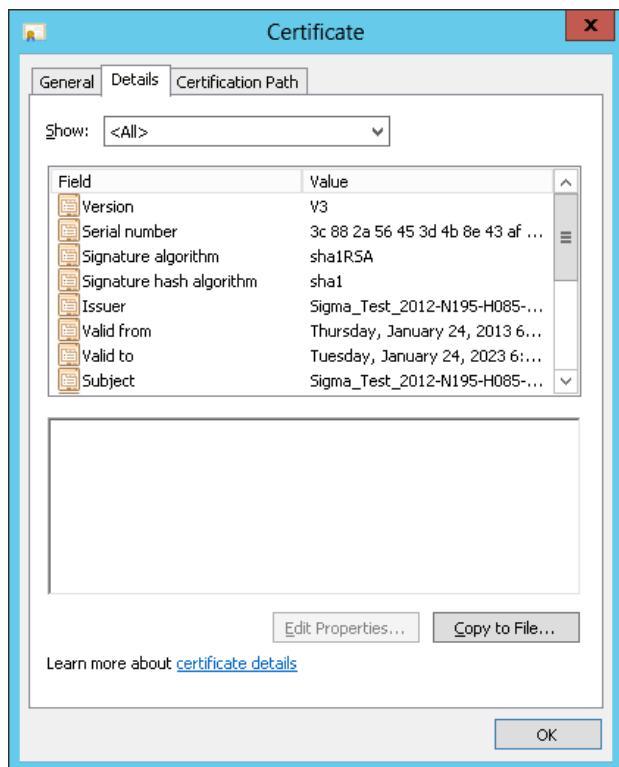
3. Select the Domain Certificate Authority server for the domain to which the Active Directory server belongs, right-click, and select **Properties** to open the **Properties** window.



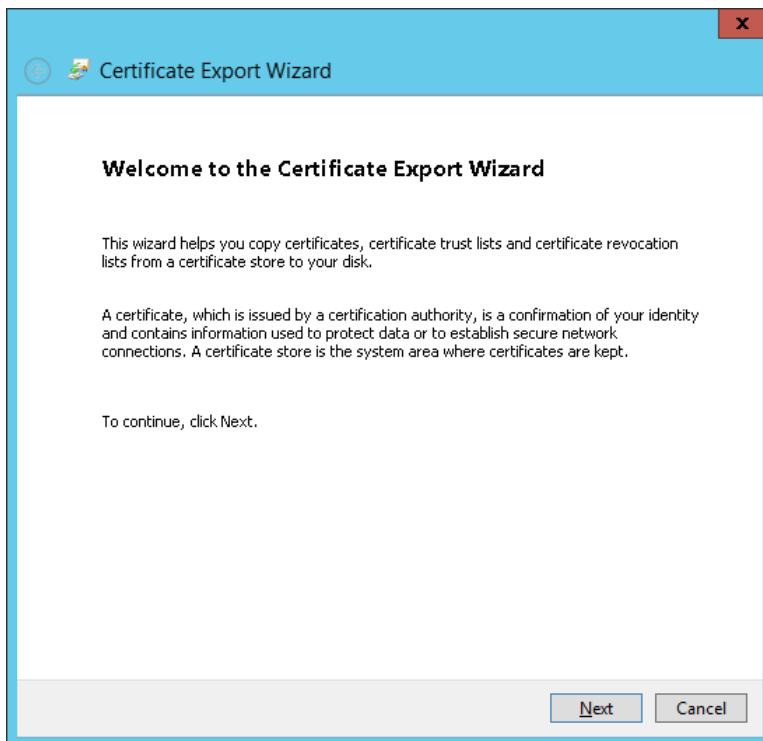
4. Click **View Certificate**.
5. Click the **Details** tab, and **Copy to File...**

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Windows



- Follow the steps in the **Certificate Export Wizard** to complete the export.



Enabling FIPS at the OS Level

1. From the Windows **Start** menu, select **Run**.
2. Enter `gpedit.msc`.
3. In the Group Policy Editor, navigate to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options**.
4. In the right pane, locate and click the “System cryptography: Use FIPS compliant5 algorithms for encryption, hashing, and signing” setting.
5. Set to **Enabled** and click **OK**.
6. Restart the computer.

Configuring Log Sources

This section provides information about configuring the following supported log sources:

Microsoft Active Directory

Microsoft Active Directory, an essential component of the Windows architecture, presents organizations with a directory service designed for distributed computing environments. Active Directory lets organizations centrally manage and share information on network resources and users while acting as the central authority for network security.

When you use Windows auditing, you can track both user activities and Windows activities. When you use auditing, you can specify which events are written to the Security log. For example, the Security log can maintain a record of both valid and invalid logon attempts and events that relate to creating, opening, or deleting files or other objects.

When you audit Active Directory events, Windows writes an event to the Security log on the domain controller. For example, if a user attempts to log on to the domain using a domain user account and the logon attempt is unsuccessful, the event is recorded on the domain controller and not on the computer on which the logon attempt was made. This is because it is the domain controller that made a failed attempt to authenticate. Auditing is turned off by default. An audit policy setting is configured for all domain controllers in the domain.

To enable auditing of Active Directory objects:

1. [Configure an audit policy setting for a domain controller.](#)
2. [Configure auditing for specific Active Directory Objects.](#)

Configuring an Audit Policy Setting for a Domain Controller

To audit events that occur on domain controllers, configure an audit policy setting that applies to all domain controllers in a non-Local Group Policy object (GPO) for the domain. You can access this policy setting through the Domain Controller's organizational unit. To audit user access to Active Directory objects, configure the Audit Directory Service Access event category in the audit policy setting. Configuration steps might vary depending on the version of Windows operating systems.

When you configure an audit policy setting, you can audit objects, but you cannot specify which object you want to audit.

The computer on which you want to configure an audit policy setting must be granted the Manage Auditing and Security Log user right. By default, Windows grants these rights to the Administrators group.



Note: The files and folders you want to audit must be on Microsoft Windows NT file system (NTFS) volumes.

To configure an audit policy setting for a domain controller:

1. Select **Start > Programs > Administrative Tools**, and then click **Active Directory Users and Computers**.
2. From the **View** menu, click **Advanced Features**.
3. Right-click **Domain Controllers**, then click **Properties**.
4. Click the **Group Policy** tab, click **Default Domain Controller Policy**, and then click **Edit**.
5. Click **Computer Configuration**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then double-click **Audit Policy**.
6. In the right pane, right-click **Audit Directory Services Access**, then click **Security**.
7. Click **Define These Policy Settings**, then select one or both the following check boxes:
Success: Click to audit successful attempts for the event category
Failure: Click to audit failed attempts for the event category
8. Right-click any other event category that you want to audit, then click **Security**.
9. Click **OK**.
10. To apply the changes you make to your computer's audit policy setting, you must propagate the policy settings to your computer. To initiate policy propagation, do one of the following:
 - Enter `secedit/refreshpolicy machine_policy` at the command prompt and then restart the computer.
 - Wait for automatic policy propagation, which occurs at regular intervals you can configure. By default policy propagation occurs every eight hours.

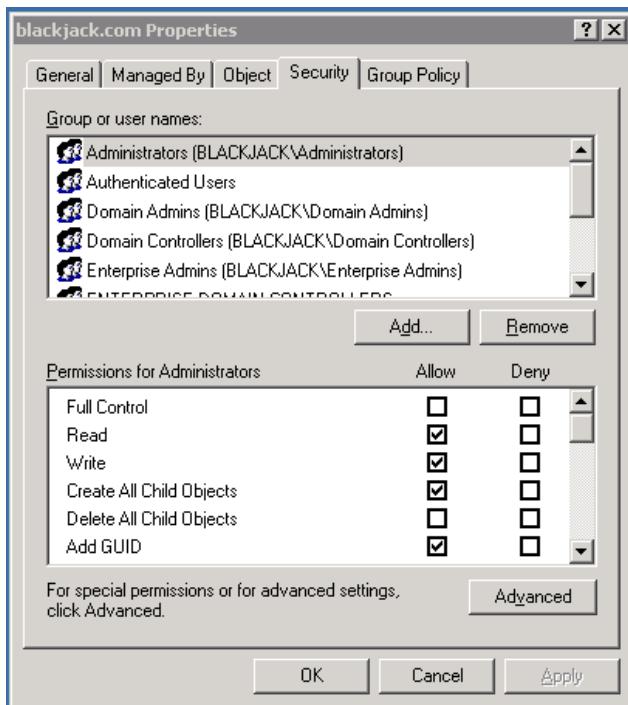
Configuring Auditing for Specific Active Directory Objects

After you configure an audit policy setting, you can configure auditing for specific objects, such as users, computers, organizational units, or groups, by specifying both the types of access and the users whose access you want to audit.

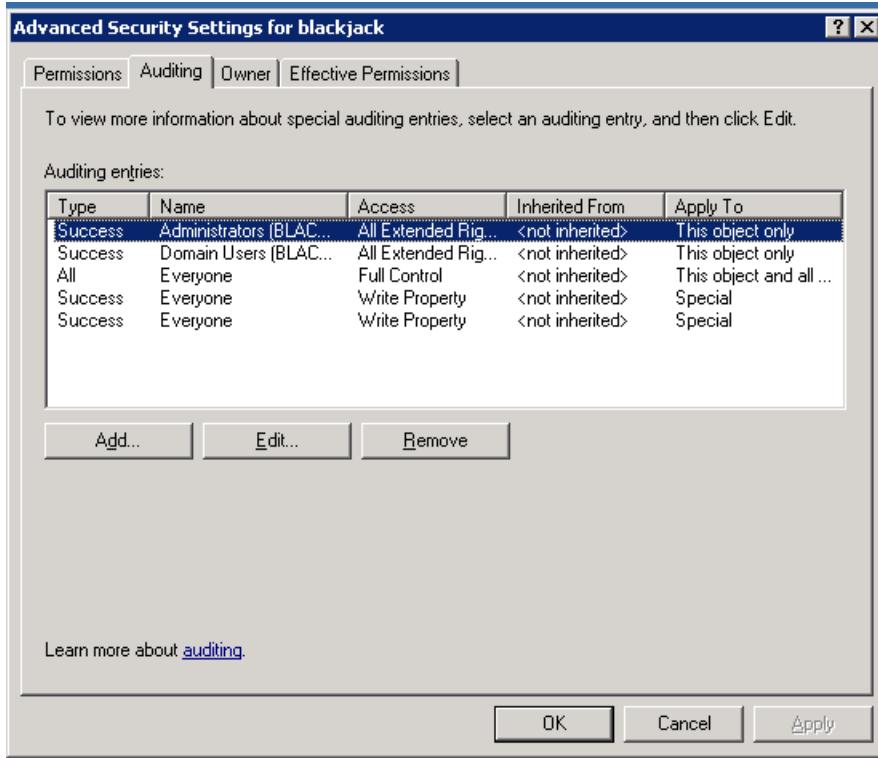
After you specify the events to audit for files, folders, printers, and Active Directory Objects, Windows tracks and logs these events. The configuration steps might depend on the version of Windows operating systems.

To configure auditing for specific Active Directory objects:

1. Click **Start > Programs > Administrative Tools**, then click **Active Directory Users and Computers**.
2. Verify that **Advanced Features** is selected on the **View** menu.
3. Right-click the Active Directory object you want to audit (blackjack.com in the example) and select **Properties**.



4. Click the **Security** tab, then click the **Advanced** button.
Advanced Security Settings for the object is displayed.
5. Click the **Auditing** tab.



6. To add an object, click **Add**.
7. Do one of the following:
 - Enter the name of the user or the group whose access you want to audit in the **Enter the object name to select** box, then click **OK**.
 - Browse the list of names and then double-click either the user or the group whose access you want to audit.
8. Click to select either the **Successful** checkbox or the **Failed** checkbox for the actions you want to audit, then click **OK**. Click **OK** on the next two windows to exit.

Microsoft ADFS

Microsoft ADFS is a software component in Windows Server that contains Active Directory, Federation Server, Federation Server Proxy, and ADFS Web Server. ADFS provides the following services:

- **Single Sign-On (SSO):** ADFS provides SSO authorization to users who want to access applications in different networks or organizations. It provides SSO access to internet-facing applications or services.

- **Identity Federation (Identity Management):** This provides the digital identity to the users and allows to centralize it. This helps to maintain security and rights across security and enterprise boundaries.

Configuring Microsoft ADFS Logs

For information about configuring Microsoft ADFS events logs, see <https://adfshelp.microsoft.com/AdfsEventViewer/GetAdfsEventList> in the Microsoft TechNet Library.

Microsoft Antimalware

Microsoft Antimalware is a network service. It provides real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your system.

The antimalware events are collected from the Windows Event system logs to your storage account. You can configure the storage account for your virtual machine to collect the antimalware events by selecting the appropriate storage account.

Microsoft DNS Server Analytics

Microsoft DNS Server Analytic Logs is a Windows system service and device driver that enables the Microsoft Windows Event Log – Native SmartConnector to monitor and collect the analytic events / logs from the DNS Server.

It provides information about operational events such as dynamic updates, zone transfers, and DNSSEC zone signing and unsigning.

This section provides information about the SmartConnector for Microsoft Windows Event Log – Native: Microsoft DNS Server Analytic Logs and its event mappings to ArcSight data fields.

Configuring Microsoft DNS Server Analytic Logs

For information about configuring Microsoft DNS Logging and Microsoft DNS analytic events logs, see Microsofts [DNS Logging and Diagnostics](#).

Microsoft Exchange Mailbox Access Auditing

Microsoft Exchange Server is the server side of a client-server, collaborative application product developed by Microsoft. It is part of Microsoft's line of server products, used by enterprises using Microsoft infrastructure solutions.

With Exchange Server 2010, Microsoft has added new native audit capabilities, such that the audit logs are maintained in the mailboxes themselves. Being able to get those audit logs is very difficult due to the potential number of mailboxes and the vast amount of data they might contain, and Windows Event Log integration for this will not work.

Therefore, for Microsoft Exchange 2010 and later versions, use the SmartConnector for Microsoft Exchange PowerShell, which retrieves Microsoft Exchange Server 2010 SP2 and 2013 Mailbox Audit logs remotely, and lets you specify the mailboxes to be audited.

Configuring Mailbox Access Auditing

You must complete the following tasks to enable mailbox access auditing:

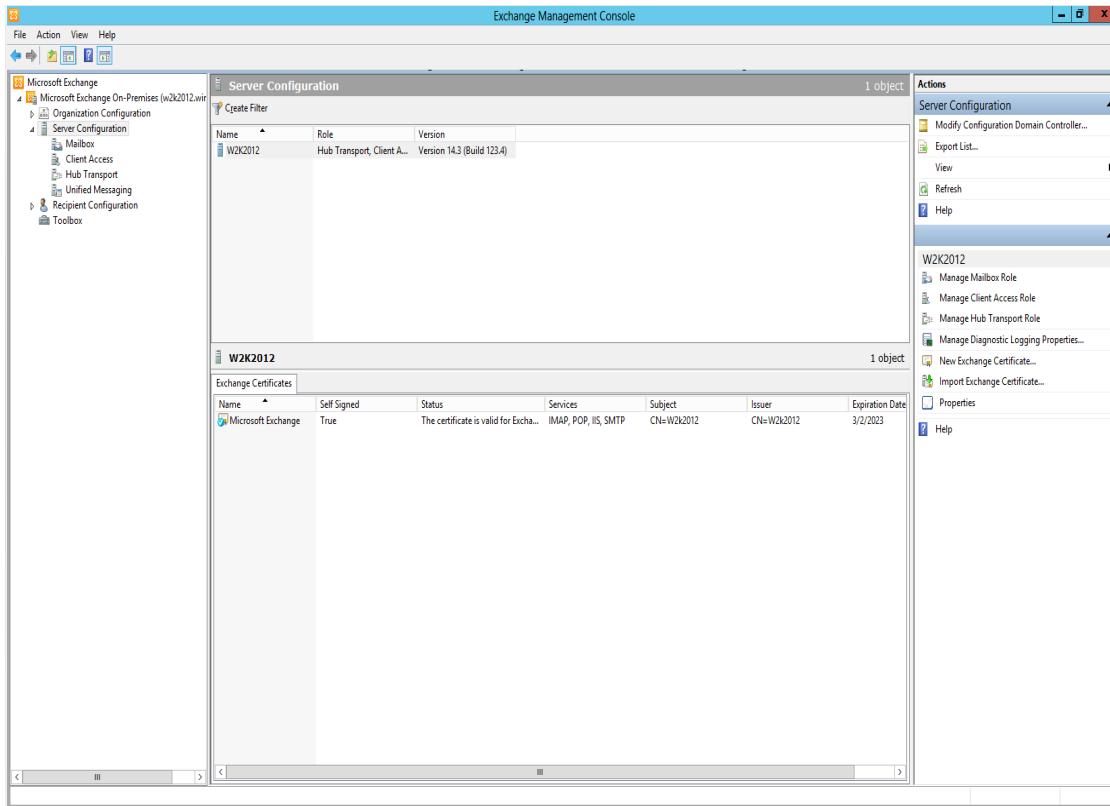
Enabling Auditing

To configure mailbox access auditing on a particular mailbox server:

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

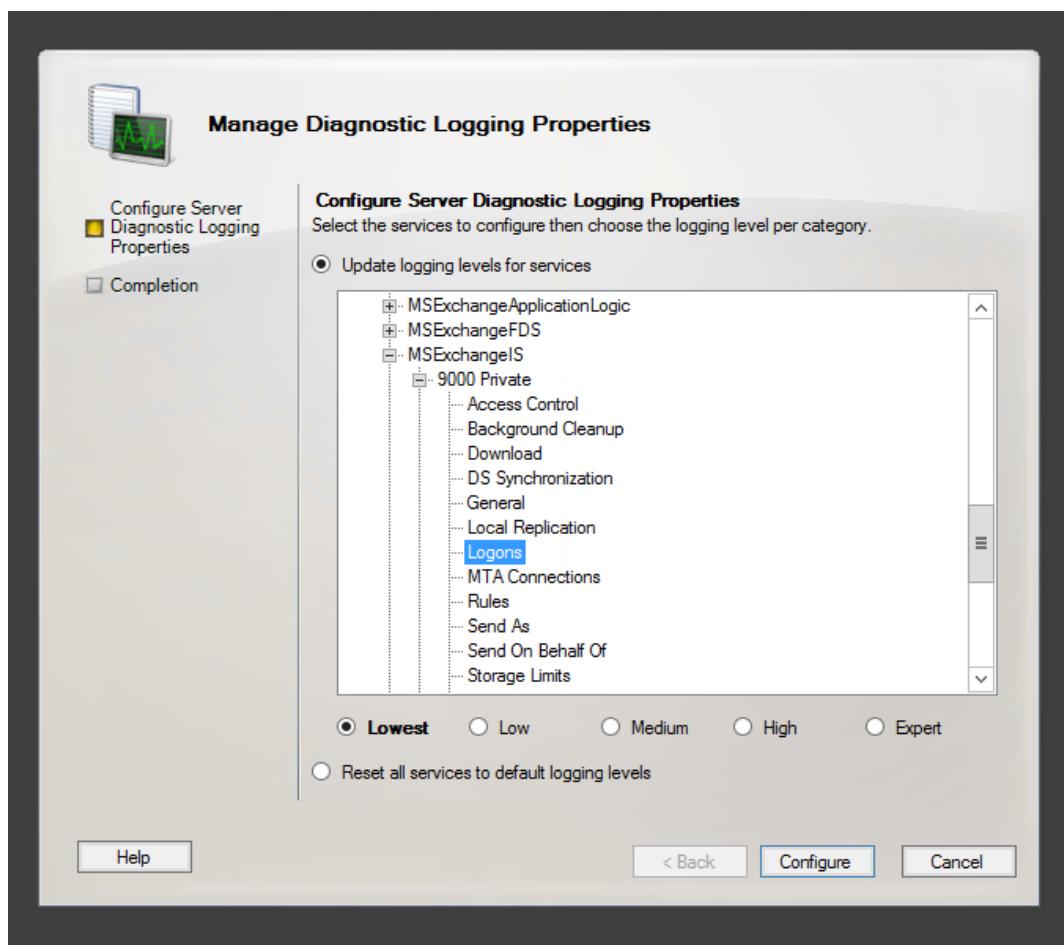
Configuring Log Sources

1. Select the server in the Exchange Management Console .



2. Select the **Manage Diagnostics Logging Properties** menu option from the action pane.

The **Manage Diagnostics Logging Properties** window is displayed.



3. Expand the **MSEExchangeIS** category and then expand the **9000 Private** category.
4. Under the **MSEExchangeIS\9000 Private** category, configure auditing for any or all of the possible actions:
 - Folder Access, to log events that correspond to opening folders, such as the Inbox, Outbox, or Sent Items folders
 - Message Access, to log events that correspond to explicitly opening messages
 - Extended Send As, to log events that correspond to sending a message as a mailbox-enabled user
 - Extended Send On Behalf Of, to log events that correspond to sending a message on behalf of a mailbox-enabled user

5. Click **Configure**.

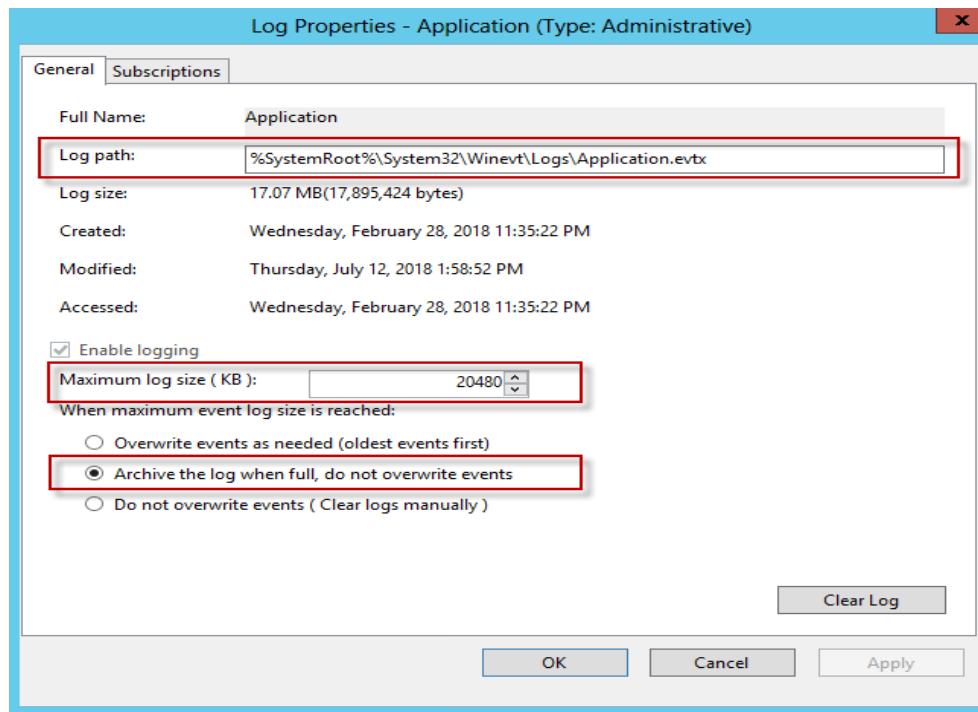
For more information about Exchange mailbox access auditing, see
http://www.msexchange.org/articles_tutorials/exchange-server-2007/compliance-policies-archiving/exchange-2007-mailbox-access-auditing-part1.html

For examples of configuring Exchange mailbox access auditing, see
<http://www.howexchangeworks.com/2009/09/mailbox-access-auditing-in-exchange.html>

Changing the Default Log Storage location

By default, the logs are stored in the Exchange Server installation directory (Drive\Program Files\Microsoft\Exchange Server\Logging\AuditLogs). The logs are archived by default when the location gets full. Therefore, make sure that the location of the logs is changed to a drive that has enough free space.

To modify the log storage location, select the properties for the Exchange Auditing log and change the options.



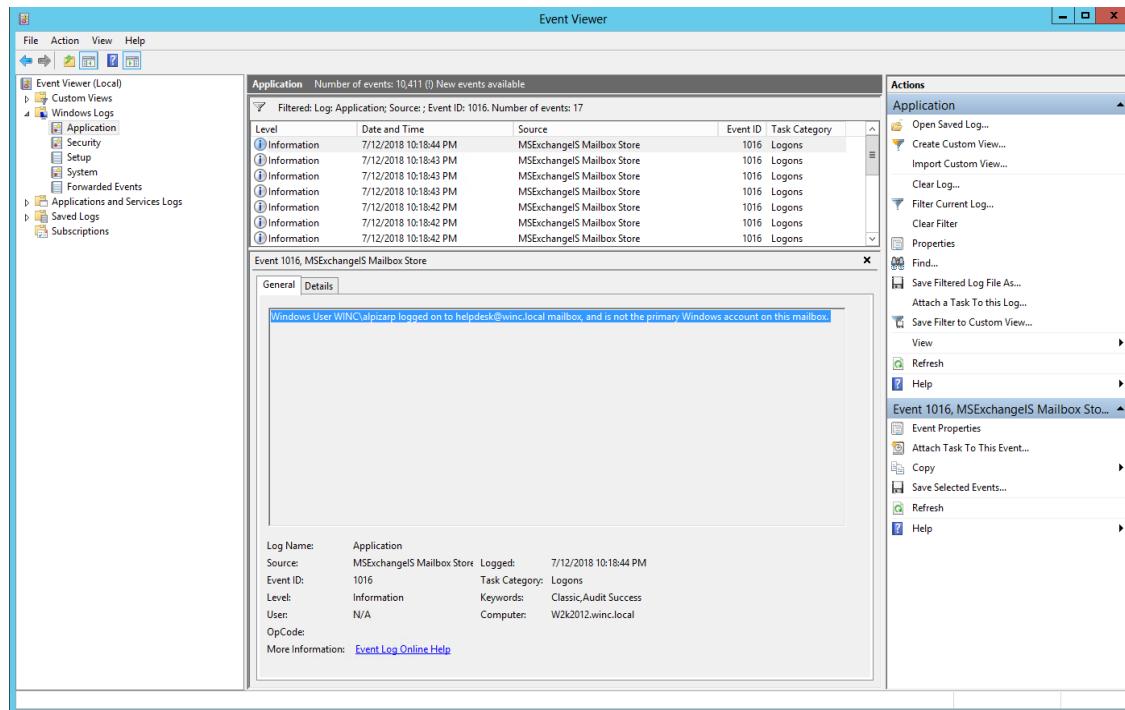
Excluding Service Accounts

Service accounts that have full access to the mailboxes might fill up your mailbox access log with events. To exclude service accounts from being audited, run the following command:

```
Get-MailboxDatabase -identity "server\sg\dbname" | Add-ADPermission -User "service account" -ExtendedRights ms-Exch-Store-Bypass-Access-Auditing -InheritanceType All
```

Viewing Logged Events

To view the information logged, navigate to **Event Viewer > Applications & Services Log > Exchange Auditing.**



Microsoft Exchange Mailbox Store

Microsoft Exchange Server is the server side of a client-server, collaborative application product developed by Microsoft. It is part of Microsoft's line of server products, used by enterprises using Microsoft infrastructure solutions.

This section provides information about configuring Microsoft Exchange Mailbox Store and understanding its event mappings to ArcSight data fields.

With Exchange Server 2010, Microsoft has added new native audit capabilities, such that the audit logs are maintained in the mailboxes themselves. Being able to get those audit logs is very difficult due to the potential number of mailboxes and the vast amount of data they may contain, and Windows Event Log integration for this will not work.

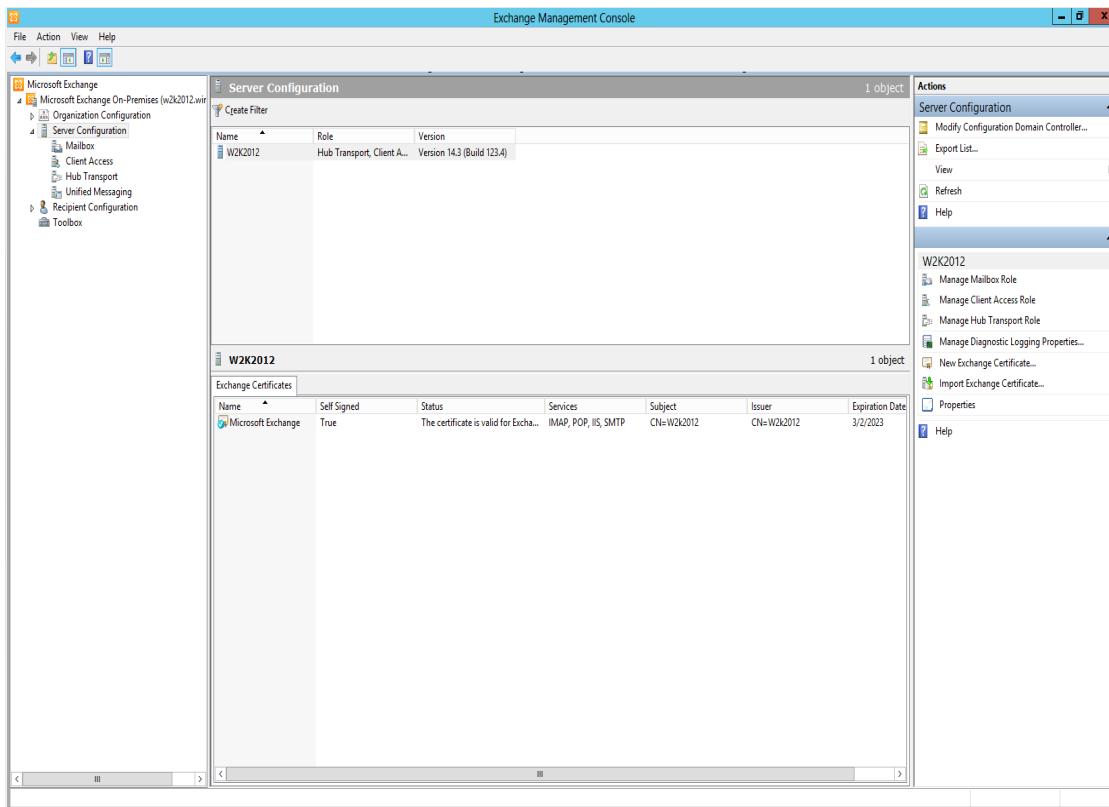
Therefore, for Microsoft Exchange 2010 and later versions, use the SmartConnector for Microsoft Exchange PowerShell, which retrieves Microsoft Exchange Server 2010 SP1 and 2013 Mailbox Audit logs remotely, and lets you specify the mailboxes to be audited.

Configuring Mailbox Store Auditing

Use the Exchange Management Console to access the configuration area for mailbox store auditing.

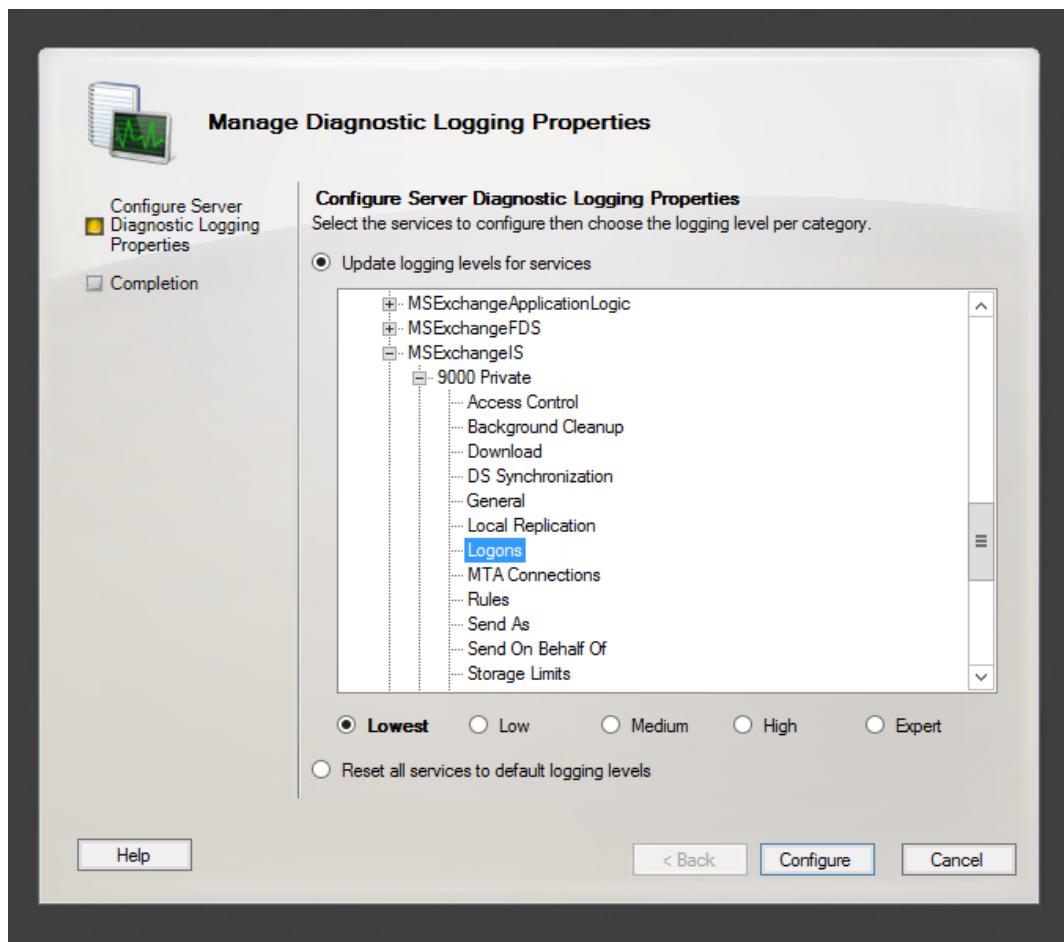
Enabling Mailbox Store

To access the configuration area for mailbox store auditing, use the Exchange Management Console. The following figure shows the new **Manage Diagnostic Logging Properties** menu option.



To configure mailbox store auditing on a particular mailbox server:

1. Select the server in the Exchange Management Console and then select the **Manage Diagnostic Logging Properties** menu option from the action pane.
The **Manage Diagnostic Logging Properties** window is displayed.



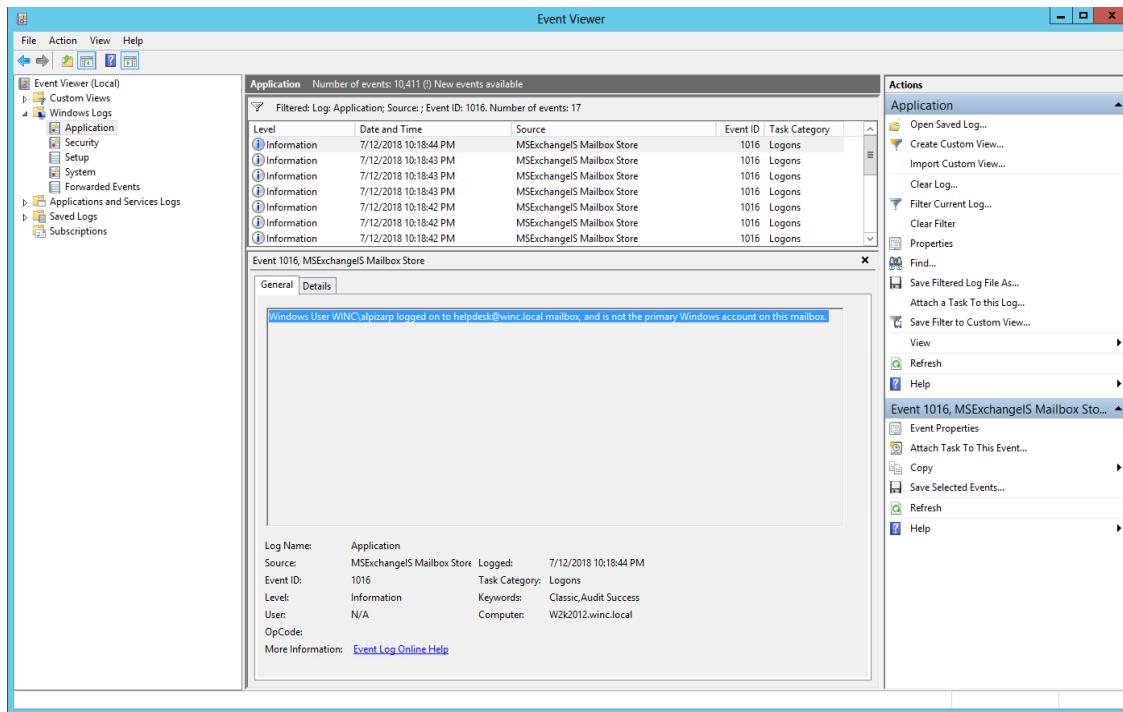
2. In this window, expand the **MSExchangeIS** category and then expand the **9000 Private** category.
3. Under the **MSExchangeIS\9000 Private** category, configure MailBox Store for Event 1016 by selecting **Logons**.
4. Click **Configure**.
5. To view events, go to Windows Event Viewer, 1016 events are saved in Application Windows Events.

Accessing the Audited Information

To view the information logged, navigate to **Event Viewer > Applications & Services Log > Exchange Auditing**.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

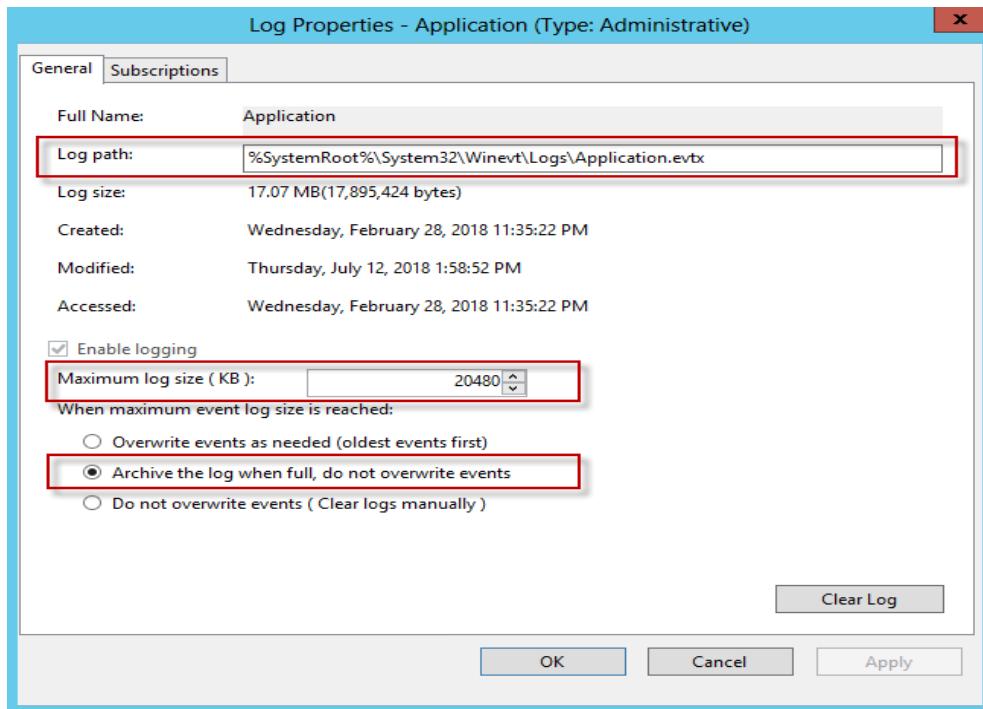
Configuring Log Sources



Changing Default Log Storage location

By default, the logs are stored in the Exchange Server installation directory (`Drive\Program Files\Microsoft\Exchange Server\Logging\AuditLogs`). The logs are archived by default when the location gets full. Therefore, make sure that the location of the logs is changed to a drive that has enough free space.

To modify the log storage location, select the properties for the Exchange Auditing log and change the options.



Excluding Service Accounts

Service accounts that have full access to the mailboxes might fill up your mailbox access log with events. To exclude service accounts from being audited, run the following command:

```
Get-MailboxDatabase -identity "server\sg\dbname" | Add-ADPermission -  
User "service account" -ExtendedRights ms-Exch-Store-Bypass-Access-  
Auditing -InheritanceType All
```

Microsoft Forefront Protection 2010

Microsoft Forefront Protection 2010 for Exchange Server (FPE) provides protection against malware and spam by including multiple scanning engines in a single solution. FPE provides customers with an administration console that includes customizable configuration settings, filtering options, monitoring features and reports, anti-spam protection, and integration with the Forefront Online Protection for Exchange (FOPE) product.

This section provides information about configuring Microsoft Forefront Protection and its event mappings to ArcSight data fields.

Configuring Forefront Protection

To enable writing events to the Windows Event Log from Forefront Protection:

1. In the Forefront Protection 2010 for Exchange Server Administrator Console, click **Policy Management**, and under **Global Settings**, click **Advanced Options**.
2. In the **Global Settings - Advanced Options** pane, under the **Logging Options** section, select the **Enable event logging** check box. When checked (the default), you can use the associated check boxes to individually enable or disable the following options (which are enabled by default):
 - **Incidents:** Enables or disables event logging for incidents.
 - **Engines:** Enables or disables event logging for engines.
 - **Operational:** Enables or disables logging for all other events, such as system information and health events.

When the **Enable event logging** check box is cleared, incidents logging is suspended for incidents, engines, and operational events.

3. Click **Save**.



Note: The relevant Microsoft Exchange and Microsoft Forefront Server protection services must be restarted in order for any changes to these settings to take effect. This typically includes the Microsoft Exchange Transport, Microsoft Exchange Information Store, and Microsoft Forefront Server Protection Controller services.

Microsoft Local Administrator Password Solution

Micorosoft Local Administrator Password Solution helps users in the management of local passwords of domain joined computers. The passwords are stored in Active Directory and protected by ACL. This ensures that only eligible users can access or reset passwords.

Configuring Microsoft Local Administrator Password Solution

For complete information about Microsoft Local Administrator Password Solution, see the TechNet Library for Windows Server: <http://technet.microsoft.com/en-us/library/hh831416>

Microsoft Netlogon

Netlogon is a Windows Server process that is responsible for communication between systems in response to a logon request. This handles authentication of users and other services within a domain.

Configuring Microsoft Netlogon Logs

For information about Microsoft's netlogon events logs configuration, see <https://support.microsoft.com/en-in/help/4557222/how-to-manage-the-changes-in-netlogon-secure-channel-connections-assoc> in the Microsoft TechNet Library.

Microsoft Network Policy Server

Internet Authentication Service (IAS) was renamed Network Policy Server (NPS) starting with Windows Server 2008. The content of this guide applies to both IAS and NPS.

Throughout the text, NPS is used to refer to all versions of the service, including the versions originally referred to as IAS.

Configuring NPS Logging

NPS logging is also called RADIUS accounting, and must be configured to your requirements whether NPS is used as a RADIUS server, proxy, NAP policy server, or any combination of the three configurations.

To configure NPS logging, you must configure the events logged and viewed with Event Viewer and determine other information you want to log. In addition, you must decide whether you want to log user authentication and accounting information to text log files stored on the local computer or to a SQL Server database on either the local computer or a remote computer.

Using the event logs in Event Viewer, you can monitor Network Policy Server (NPS) errors and other events that you configure NPS to record.

NPS records connection request failure events in the System and Security event logs by default. Connection request failure events consist of requests that are rejected or discarded by NPS. Other NPS authentication events are recorded in the Event Viewer system log on the basis of the settings that you specify in the NPS snap-in. Some events that might contain sensitive data are recorded in the Event Viewer security log.

The following information is from Microsoft Windows Server TechNet Library. For complete information, see RADIUS Accounting > NPS Events and Event Viewer > Configure NPS Event Logging ([http://technet.microsoft.com/en-us/library/cc731085\(v=ws.10\).](http://technet.microsoft.com/en-us/library/cc731085(v=ws.10).)

Use this procedure to configure Network Policy Server (NPS) to record connection request failure and success events in the Event Viewer system log.

Membership in Domain Admins, or equivalent, is the minimum required to complete this procedure.

To configure NPS event logging using the Windows interface:

1. Open the Network Policy Server (NPS) snap-in.
2. Right-click NPS (Local), and then click Properties.

3. On the General tab, select each required option, and then click OK.

Microsoft Remote Access

Routing and Remote Access is a network service in Windows that provides the following services:

- Dial-up remote access server
- Virtual private network (VPN) remote access server
- Internet Protocol (IP) router for connecting subnets of a private network
- Network address translator (NAT) for connecting a private network to the Internet
- Dial-up and VPN site-to-site demand-dial router

Configuring Remote Access

For complete information about Microsoft's Reporting and Remote Access Service, see Microsoft's TechNet Library for Windows Server, "Remote Access (DirectAccess, Routing and Remote Access)": <http://technet.microsoft.com/en-us/library/hh831416>

Microsoft Service Control Manager

Service Control Manager (SCM) is a special system process under Windows NT family of operating systems that starts, stops, and interacts with Windows service processes. It is located in %SystemRoot%\System32\services.exe executable. Service processes interact with SCM through a well-defined API, and the same API interface is used internally by the interactive Windows service management tools such as the MMC snap-in Services.msc and the command-line Service Control utility sc.exe.

For more information about Microsoft Service Control Manager, see [Microsoft Documentation](#).

Microsoft SQL Server Audit

With SQL Server 2008, Microsoft introduced an SQL Server Audit feature that provides a true auditing solution for enterprise customers. While SQL Trace can be used to satisfy many auditing needs, SQL Server Audit offers a number of advantages that can help DBAs more easily achieve their goals, such as meeting regulatory compliance requirements.

The SQL Server Audit feature is intended to replace SQL Trace as the preferred auditing solution. SQL Server Audit is meant to provide full auditing capabilities and only auditing capabilities, unlike SQL Trace, which is also used for performance debugging.

Configuring SQL Server Audit

For complete information about auditing in SQL Server, see [Microsoft's SQL Server documentation](#).

Using SQL Server Management Studio, create a server audit as follows:

1. In Object Explorer, expand the **Security** folder.
2. Right-click the **Audits** folder and select **New Audit** to open a **Create Audit** window.
3. Enter a name for your audit (for example, **LoginFailed**). For **Audit destination**, select **ApplicationLog** from the list.
4. Click **OK** to accept the default settings and save the new audit specification.
5. The new audit will appear in the **Audits** folder. To enable the audit, select the audit you created, right-click, and select **Enable Audit**.

Customizing Event Source Mapping

For information about customizing event source mapping, see [Customizing Event Source Mapping](#).

Microsoft Sysmon

Microsoft Sysmon Logs is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log.

It provides detailed information about process creations, network connections, and changes to file creation time. By collecting the events it generates using Windows Event Collection or SIEM agents and subsequently analyzing them, users can identify malicious or anomalous activity and understand how intruders and malware operate on your network.

This connector supports Microsoft Sysmon Operational version 11 events.

Configuring Microsoft Sysmon Logs

For complete information about Microsoft Sysmon Logs, see [Microsoft Documentation](#).

Microsoft Windows AppLocker

Microsoft AppLocker helps organizations control the apps and files including executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers, that can be run by users.

Configuring Microsoft Windows AppLocker

For complete information about Microsoft Windows AppLocker, see [Microsoft Documentation](#).

Microsoft Windows BITS Client Logs

Microsoft Windows Background Intelligent Transfer Service (BITS) helps programmers and system administrators to download files from or upload files to HTTP web servers and share files using Server Message Block (SMB) protocol. BITS will take the cost of the transfer into consideration, as well as the network usage so that the user's foreground work has as little impact as possible. It also handles network interruptions, pausing, and automatically resuming transfers, even after a reboot. BITS includes PowerShell cmdlets for creating and managing transfers as well as the BitsAdmin command-line utility.

Configuring Microsoft Windows BITS Client Event Logs

For information about Microsoft's BITS client events logs configuration, see [Microsoft documentation](#).

Microsoft Windows Defender Antivirus

Microsoft Defender Antivirus is built into Windows, and it works with Microsoft Defender for Endpoint to provide protection on your device and in the cloud.

Microsoft Windows Defender AntiVirus

For complete information about Microsoft Windows Defender Antivirus, see [Microsoft Documentation](#).

Microsoft Windows ESENT

Microsoft Windows ESENT is an embeddable and transactional database engine which is used for data storage. You can use ESENT for applications that need reliable, high-performance, and low-overhead storage of structured or semi-structured data. The ESENT engine can help with data needs ranging from something as simple as a hash table that is too large to store in memory to something more complex such as an application with tables, columns, and indexes. For more information, see [Microsoft Documentation](#).

Microsoft Windows Event

The Windows event log is a detailed record of system, security and application notifications stored by the Windows operating system that is used by administrators to diagnose system problems and predict future issues.

These event logs are used to record important hardware and software actions that the administrator can use to troubleshoot issues with the operating system. The Windows operating system tracks specific events in its log files, such as application installations, security management, system setup operations on initial startup, and problems or errors.

Microsoft Windows Hyper V

Microsoft Windows Hyper-V logs are a set of files that contain information about the Hyper-V hypervisor and virtual machines. For more information, see [Hyper-V Technology Overview](#) in the Microsoft documentation.

Configuring Microsoft Windows Hyper V Logs

For information about configuring Microsoft Windows Hyper V events logs, see [Configuring Custom Logs and Filtering](#).

Microsoft Powershell

PowerShell is a task-based command-line shell and scripting language built on .NET. PowerShell helps system administrators and power-users rapidly automate tasks that manage operating systems (Linux, macOS, and Windows) and processes.

PowerShell commands let you manage computers from the command line. PowerShell providers let you access data stores, such as the registry and certificate store, as easily as you access the file system. PowerShell includes a rich expression parser and a fully developed scripting language.

As it is widely used by the black hat community for initial access and further lateral movement within an enterprise, it is critical to properly collect and parse Windows Powershell logs. This would open the doors to writing correlation and hunt/search tools to find the APT's and other advanced threats.

Auditing Powershell Objects in Windows

When you audit Powershell events, Windows writes an event to the Security log on the domain controller. For example, if a user attempts to log on to the domain using a domain user account and the logon attempt is unsuccessful, the event is recorded on the domain controller and not on the computer on which the logon attempt was made. This is because it is the domain controller that made an unsuccessful attempt to authenticate.

To enable auditing of Powershell objects:

1. Configure an audit policy setting for a domain controller. (When you configure an audit policy setting, you can audit objects, but you cannot specify which object you want to audit.)
2. Configure auditing for specific Powershell Objects. After you specify the events to audit for files, folders, printers, and Powershell Objects, Windows tracks and logs these events.

Configure an Audit Policy Setting for a Domain Controller

Auditing is turned off by default. For domain controllers, an audit policy setting is configured for all domain controllers in the domain. To audit events that occur on domain controllers, configure an audit policy setting that applies to all domain controllers in a non-Local Group Policy object (GPO) for the domain. You can access this policy setting through the Domain Controller's organizational unit. To audit user access to Powershell objects, configure the Audit Directory Service Access event category in the audit policy setting.

The computer on which you want to configure an audit policy setting must be granted the Manage Auditing and Security Log user right. By default, Windows grants these rights to the Administrators group.



Note: The files and folders you want to audit must be on Microsoft Windows NT file system (NTFS) volumes.

To configure an audit policy setting for a domain controller (steps may vary for differing Windows operating systems):

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Powershell Users and Computers**.
2. From the **View** menu, click **Advanced Features**.
3. Right-click **Domain Controllers**; then click **Properties**.
4. Click the **Group Policy** tab, click **Default Domain Controller Policy**, and then click **Edit**.
5. Click **Computer Configuration**, double-click **Windows Settings**, double-click **Security Settings**, double-click **Local Policies**, and then double-click **Audit Policy**.
6. In the right pane, right-click **Audit Directory Services Access**, and then click **Security**.
7. Click **Define These Policy Settings**, then click to select one or both of the following check boxes:
 - Success: Click to audit successful attempts for the event category
 - Failure: Click to audit failed attempts for the event category
8. Right-click any other event category that you want to audit; then click **Security**.
9. Click **OK**.
10. Because the changes you make to your computer's audit policy setting takes affect only when the policy setting is propagated (or applied) to your computer, to initiate policy propagation, either enter `secedit/refreshpolicy machine_policy` at the command prompt and then restart the computer or wait for automatic policy propagation, which occurs at regular intervals you can configure. By default policy propagation occurs every eight hours.

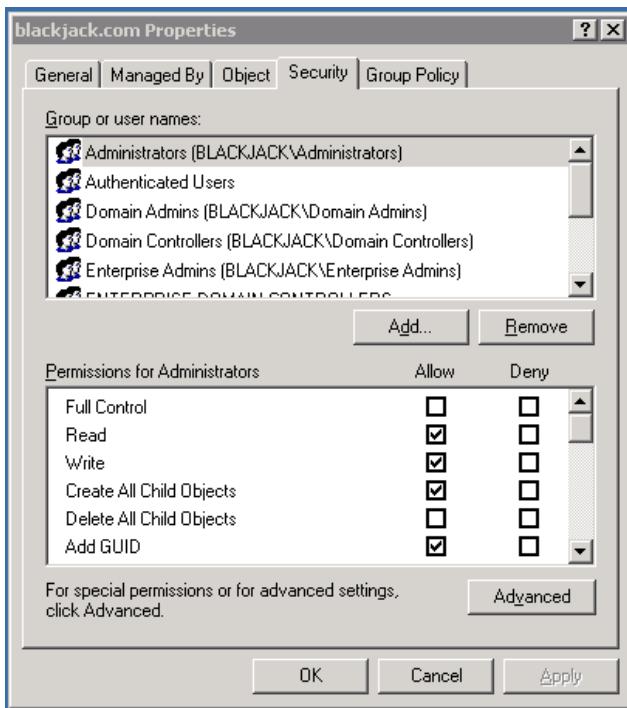
Configuring Auditing for Specific Powershell Objects

After you configure an audit policy setting, you can configure auditing for specific objects, such as users, computers, organizational units, or groups, by specifying both the types of access and the users whose access you want to audit.

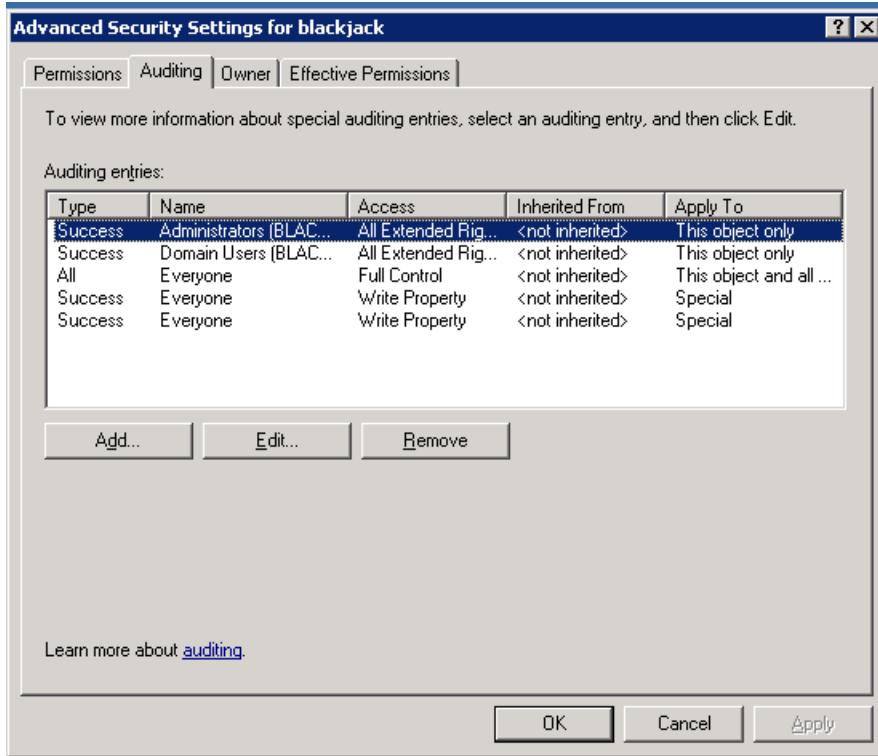
To configure auditing for specific Powershell objects (steps may vary for differing Windows operating systems):

1. Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Powershell Users and Computers**.

2. Verify that **Advanced Features** is selected on the **View** menu (the command has a checkmark beside it).
3. Right-click on the Powershell object you want to audit (`blackjack.com` in the example) and select **Properties**.



4. Click the **Security** tab, then click the **Advanced** button; **Advanced Security Settings** for the object is displayed. Click the **Auditing** tab.



5. To add an object, click **Add**.
6. Either enter the name of either the user or the group whose access you want to audit in the **Enter the object name to select** box, then click **OK**, or browse the list of names and then double-click either the user or the group whose access you want to audit.
7. Click to select either the **Successful** checkbox or the **Failed** checkbox for the actions you want to audit, then click **OK**. Click **OK** on the next two windows to exit.

Microsoft Windows Update Client

Microsoft Windows Update Client works in conjunction with Windows Server Update Services to support automated patch delivery and installation. It scans your computer and determines the version of Windows you are running and pushes new updates to your device.

Configuring Windows Update Client

For complete information about Windows Update Client, see Microsoft's TechNet Library for Windows Server, :<http://technet.microsoft.com/en-us/library/hh831416>

Microsoft Windows WMI Activity Trace

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. For more information see [Logging WMI Activity](#) and [Tracing WMI Activity](#).

Microsoft Windows WMI Analytic and Operation

Windows Management Instrumentation (WMI) is Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment.

WMI uses the Common Information Model (CIM) industry standard to represent systems, applications, networks, devices, and other managed components. For more information, see [WMI documentation](#).

Microsoft WINS Server

Microsoft WINS servers are designed to prevent the administrative difficulties that are inherent in the use of both IP broadcasts and static mapping files such as LMHOSTS files. Microsoft WINS is designed to eliminate the need for IP broadcasts (which use valuable network bandwidth and cannot be used in routed networks), while providing a dynamic, distributed database that maintains computer name-to-IP-address mappings.

WINS servers use a replicated database that contains NetBIOS computer names and IP address mappings (database records). When Windows-based computers log on to the network, their computer name and IP address mapping are added (registered) to the WINS server database, providing support for dynamic updates. The WINS server database is replicated among multiple WINS servers in a LAN or WAN. One of the benefits of this database design is that it prevents different users from registering duplicate NetBIOS computer names on the network.

WINS clients, referred to as WINS- enabled clients, are configured to use the services of a WINS server. Windows NT- based clients are configured with the IP address of one or

more WINS servers by using the WINS Address tab on the Microsoft TCP/IP Properties page in Control Panel > Network.

Configuring WINS Server for Event Collection

You can run the Registry Editor program at the command prompt to configure a WINS server by changing the values of the Registry parameters. Parameters for logging include:

Configuration Option	Description
Logging Enabled	Specifies whether logging of database changes to J50.log files should be turned on.
Log Detailed Events	Specifies whether logging events is verbose mode. (This requires considerable computer resources and should be turned off if you are tuning for performance.)

Oracle Audit

Auditing is a default feature of the Oracle server. The standard audit commands allow all system privileges to be audited along with access at the object level to any table or view on the database for select, delete, insert or update. Audit can be run for either successful or unsuccessful attempts or both. It can be for each individual user or for all users, and it can also be done at the session level or access level. At action level a single record is created per action and at session level one record is created for all audit actions per session.

The following sections provide information about the SmartConnector for Microsoft Windows Event Log – Native: Oracle Audit and its event mappings to ArcSight data fields.

Configuring Auditing

For complete information about Oracle database auditing, see "Configuring Auditing" in the *Oracle Database Security Guide* for your database version.

Enabling Auditing

Database auditing is enabled and disabled by the AUDIT_TRAIL initialization parameter in the database initialization parameter file, `init.ora`. Setting it to OS enables database auditing and directs all audit records to an operating system file:

`AUDIT_TRAIL=OS`

Auditing Administrative Users

Sessions for users who connect as SYS can be fully audited, including all users connecting as SYSDBA or SYSOPER. Use the AUDIT_SYS_OPERATIONS initialization parameter to specify whether such users are to be audited. For example, the following setting specifies that SYS is to be audited:

```
AUDIT_SYS_OPERATIONS = TRUE
```

The default value, FALSE, disables SYS auditing.

Symantec Mail Security

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.

Make sure that you have the System Administrator privileges to configure or modify Symantec Mail Security settings.

Installing the SmartConnector

This section has the following information:

Installation Requirements

.NET Requirements

- .NET 4.5.2, 4.6, 4.6.1 or 4.7.2.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the Administrator's Guide to ArcSight Platform, available on ArcSight Documentation.

If you are adding a connector to the ArcSight Management Center, see the ArcSight Management Center Administrator's Guide available on ArcSight Documentation for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

SmartConnector Setup Scenarios

The following examples describe some typical setup scenarios. For configuration details, see See “[Configure the Connector](#)”

- **Scenario 1 - Collect Application, Security, and System Logs for the Local Host:** You select local host logs on the first configuration window with no remote hosts, no custom logs or event filters, and no Windows Event Forwarding configuration. Locale and encoding of the local host are automatically detected and configured by the connector; therefore, configuration of these values for the local host is not necessary.
- **Scenario 2 - Collect Application, Security, and System Logs from Remote Hosts, from One Domain, and Enter the Hosts Manually:** In this scenario, you can collect logs from remote hosts and add the host entries manually. You can either add a table parameter in the entry window that is displayed or import a csv file containing host information. However, when importing, make sure your local host is in the csv file if you intend to collect events from the local host, as the content from the imported file replaces the existing host information.
- **Scenario 3 - Collect Application, Security, and System logs from Hosts Recorded in Active Directory:** Collect logs from a host recorded in Active Directory. The table parameter entry window is then displayed, where you can make configuration selections for each host.
- **Scenario 4 - Collect Forwarded Events or Other WEC Logs from Local Or Remote Hosts:** With any of the previous scenarios, to collect Forwarded Events or other WEC logs from the local host (or remote hosts); a window is displayed where you can specify the name of a csv file containing the source hosts names and Windows OS versions for the hosts after making configuration selections for your hosts on the table parameter entry window.

Installing and Configuring the SmartConnector

For additional information about installing the SmartConnectors, see the [ArcSight SmartConnector Installation and User Guide](#).

To install and configure the Windows Event Log - Native SmartConnector:

1. Start the installation process.
2. Follow the instructions to add the required details to complete the installation of core software.

3. After the installation completes, to configure the connector, you can either click **Next** or run the <ArcSightSmartConnectors_installDirectory>\current\bin\runagentsetup.bat file.
4. Select the relevant **Global Parameters**, the click **Next**.
5. From the **Type** drop-down, select **Microsoft Windows Event Log - Native** as the type of connector, then click **Next**.
6. In the **Configure Parameters** window, specify the following information:
 - a. Select logs for event collection:
 - The **Security log**, **System log**, and **Application log** options are selected by default. See “[Log Parser Support](#)” for a list of supported application and system events. For more information about the type of logs to select for different log sources, see [Selecting the Type of Logs for Event Collection](#).
 - **Custom Log:** Select this option to collect custom logs. For more information, see [Configuring Custom Logs and Filtering](#)
 - **ForwardedEvents Log:** If you select this option, you can collect events forwarded from a source host to any log type on the collector machine to which the connector has access.
Note: Security events cannot be forwarded to the Security event log on a collector machine, but can be forwarded to other log types.
 - b. If you selected the **ForwardedEvents Log** option, the Windows OS version of the event source host is not populated automatically in the normalized events. To populate this value, you must either provide the Windows OS version or configure the Active Directory. If both Active Directory and Windows OS version is available from the source host file , then value from Active Directory takes precedence. Select any of the following options to specify the Windows OS version for the hosts from which you want to collect events:
 - **Use file for OS version:** Select this option to supply the name of the source hosts in a file. If you select this option, you will be prompted to specify the file details.
 - **Use Active Directory for OS version:** Select this option, then the connector retrieves the host details from the configured Active Directory to identify the event source host Windows version information. Newly discovered hosts are [added to the lookup automatically](#) without having to reconfigure the connector itself.

For the connector to be able to browse the Active Directory to retrieve source host Windows version information, it must be placed within the same forest as the Active Directory.

If you select this option, you will be prompted to enter your domain credentials and Active Directory parameter information in the next screen.

- **Do not use any source for Windows OS version:** Select this option to not provide an Active Directory query or a CSV file to list all hosts involved in events forwarding along with their Windows OS version. If you select this option, no Windows OS version will be displayed in the event headers from the forwarding host.

c. Select one or many of the following parameters to add hosts for event collection:

- **Use Common Domain Credentials:** Select this option to specify common domain credentials.
- **Use Active Directory:** Select this option to use the host information (host name and version) from the configured Active Directory to identify the event source host Windows version information.
- **Enter Manually:** Select this option to manually specify all the host details.

7. Click **Next**.

8. One or more of the following screens will be displayed depending on your selections in the previous window:

- a. **WEF Source Hosts File Name:** If you selected **ForwardedEvents log** or **Use file for OS version** options in the previous window, then you are prompted to enter the name of the file that contains the source host information. This window is also displayed if you have selected **Is WEC** for any hosts in the table parameter window. For forwarded event collection, specify only the Event Collector hosts.
- b. **Device Details Collection:** The first row displays selections from the initial parameter entry window for the local host. Click **Add** to manually add a host, or click **Import** to select a .csv file to import host information. Make sure that there is a carriage return (only one CR) at the last entry in the .csv file. Else the import fails.

If you have added hosts for which you decide not to collect events, you can use the checkbox in the leftmost column to deselect rows in the table.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Installing the SmartConnector

Parameter	Description
Host Name	Host name or IP address of the target Windows host.
Domain Name	Name of the domain to which the host belongs. If you are using a Domain User account for a target host or using Active Directory, fill in the Domain Name field. This must be a name, not an IP address, for the OS version to be resolved.
User Name	Name of the user account with adequate privileges to collect Windows events from the target host. This will be the user name only, without the domain.
Password	Password for the user specified in User Name .
Windows Version	Select the Microsoft Operating System version this host is running.
Is WEC	If you selected Indicates that this is a WEC server on the initial configuration page, this selection is already checked for the local host.
Security	Select for security events to be collected from this host. This log is automatically selected for all hosts.
System	Select for system events to be collected from this host.
Application	Select for application events to be collected from the Common Application Event Log of this host.
ForwardedEvents	Select for events to be collected from the ForwardedEvents log of this host.
Custom Event Logs	Specify the custom application log names, separated by a comma (such as "Exchange Auditing, Directory Service"). For Windows Event Collector servers, use HardwareEvents . See " "Installing and Configuring the SmartConnector" on page 85 " for more information.

Parameter	Description
Filter	This is a filter you can get from the Microsoft event viewer when you want to collect particular events. You can copy the filter text to this field. For more information, see " Configure a Filter ."
Locale	Enter the value for your locale or accept the United States English default, en_US . Leave this field blank if you want the connector for the local host to automatically determine the correct Locale value. Values are: <ul style="list-style-type: none">■ French Canadian: fr_CA■ Japanese: ja_JP■ Simplified Chinese: zh_CN■ Traditional Chinese: zh_TW■ United States English (the default): en_US For localization of other languages, see " Customize Localization Support for the Native Connector " on page 39.
Encoding	Enter the encoding value for the language used to send localized log events, or accept the United States English default, en_US . This value cannot be determined automatically. Select from the following values: <ul style="list-style-type: none">■ French Canadian: fr_CA■ Japanese: Shift_JIS■ Simplified Chinese: GB2312■ Traditional Chinese: zh_TW■ United States English (the default): UTF-8 For localization of other languages, see " Customize Localization Support for the Native Connector " on page 39.

- c. **Domain Credentials:** If you selected **Use common domain credentials** option in the previous window, then you are prompted to specify the following details:



Note:

- A Domain User Name and Domain User Password is not required if you are performing local event collection.
- If the hosts Domain parameters are the same as Active Directory, then you do not have to enter both. The information will be taken from the Active Directory Domain and credentials.

Parameter	Description
Domain Name	Enter the name of the domain to which the host belongs. Work group hosts and stand-alone hosts can be added manually on the table parameters entry window.
Domain User Name	Enter the name of the user account with adequate privileges to collect Windows events from the target host. It is assumed that the AD server is located on the domain server and can be accessed with the domain user and password.
Domain User Password	Enter the password for the user specified in the Domain User Name field.

- d. **Active Directory Parameters:** If you selected **Use common domain credentials** option in the previous window, then you are prompted to specify the following details:



Note:

- A Domain User Name and Domain User Password is not required if you are performing local event collection.
- If the hosts Domain parameters are the same as Active Directory, then you do not have to enter both. The information will be taken from the Active Directory Domain and credentials.
- If GUID translation is enabled, then the Active Directory Domain and credentials are used. You must provide the complete domain name, including any qualifiers, such as .com.

Parameter	Description
Active Directory Domain	Enter the name of the Active Directory domain to which the host belongs.
Active Directory User Name	Enter the name of the user account with adequate privileges to collect Windows events from the target host. It is assumed that the AD server is located on the domain server and can be accessed with the domain user and password.
Active Directory User Password	Enter the password for the user specified in the Active Directory User Name field.
Active Directory Server	Enter the Active Directory Host Name or IP address required for authentication to the Microsoft Active Directory for the host browsing feature.

Parameter	Description
Active Directory Filter	<p>Enter the Active Directory Filter required for automatic host browsing to filter hosts by name, operating system, and creation time.</p> <p>The query can contain attributes for Common Names (cn), Operating System (operatingsystem) and Creation Time (whencreated) in 'YYMMDDHHmmSS' format, where YY=Last two digits of the year, MM=Month, DD=Date, HH=Hours, mm=Minutes, SS=Seconds in 24-hour format.</p> <p>The query can also contain wildcard characters (*) to match the attributes to different values.</p> <p>Active Directory Filter examples</p> <p>To create hosts after and inclusive of a particular time point, set filter to: <code>(&(cn=*)(operatingsystem=*)(whencreated>=YYMMDDHHmmSSZ))</code></p> <p>To create hosts between and inclusive of two time points, set filter to: <code>(&(cn=*)(operatingsystem=*)(whencreated>=YYMMDDHHmmSS)(whencreated<=YYMMDDHHmmSS))</code></p>
Active Directory Protocol	<p>Select whether the protocol to be used is non_ssl (the default value) or SSL. For SSL protocol, be sure to import the Active Directory security certificate to the connector before starting the connector.</p>
Use Active Directory host results for	<p>For WEF Only: If you selected “Use Active Directory for OSVersion” on the initial configuration window, the list of hosts retrieved from Active Directory is used to determine the Windows OS version for the WEF source hosts. When For WEF Only is selected, the result of the query will not populate the table of hosts on the table parameter entry window.</p> <p>For initial installation, Merge Hosts and Replace Hosts act the same because only the local host is present and preserved. If you selected Use Active Directory on the initial configuration screen under Parameters to add hosts for event collection, or you are modifying parameters to add hosts, the following applies.</p> <p>When Merge Hosts is selected, Active Directory is used to retrieve the hosts for collection (and can also be used for Windows Event Forwarding if WEC servers are present and Use file for OS is not selected on the initial configuration screen). The original host is not replaced and all other preconfigured hosts are preserved. Hosts are added from the list retrieved from Active Directory with Security events selected by default. If duplicates are found, the existing host entry is not overwritten.</p> <p>When Replace Hosts is chosen, Active Directory is used to retrieve the hosts for collection (and can also be used for Windows Event Forwarding when WEC servers are present and Use file for OS is not selected on the initial configuration screen). The local host is not replaced, but all other hosts preconfigured are replaced with those retrieved from Active Directory, with Security events selected by default.</p>

9. Select a destination, then configure the destination parameters.

10. Specify a name for the connector.

11. Select whether you want to run the connector as a service or in the standalone mode.
12. Complete the installation process.

Using SSL for Connection (optional)

If you are using SSL for connector connection, follow these steps.

To import the certificates to the connector's certificate store, click **Cancel** to exit the wizard:

1. From \$ARCSIGHT_HOME\current\bin, execute the **keytool** application to import the two certificates (see "[Add Security Certifications when Using SSL](#)" earlier in this guide).

```
arcsight agent keytoolgui
```

The graphical interface asks you to open a keystore

2. Select jre/lib/security/cacerts, then select **import cert** to import your certificate. Verify that the correct certificate has been imported.
3. When prompted **Trust this certificate?**, click **Yes**.
Repeat this process for the second certificate.
4. Save the keystore.
5. Verify the imported certificates by entering this command from \$ARCSIGHT_HOME\current\bin:

```
arcsight agent keytool -list -store clientcerts
```

The new certificates are listed.

6. Return to the configuration wizard by entering the following command from \$ARCSIGHT_HOME\current\bin:

```
runagentsetup
```

Post-Installation Permissions

The current/user/agent/agentdata folder stores raw events data and contains sensitive information which must be restricted using the following permission:

The user installing the connector and the system administrator must restrict permission for the current/user/agent/agentdata folder so that only they are authorized to access the folder and files present in it. For more information related to the folder permissions, check [Microsoft Documentation](#).

Configuring Custom Logs and Filtering

If you selected **Custom logs** in the **Select logs for event collection** section of the initial configuration window, and you want to add filtering for the local host, check **Custom Logs** in the **Select logs for event collection** section to ensure this window is displayed for you to enter filter parameters.

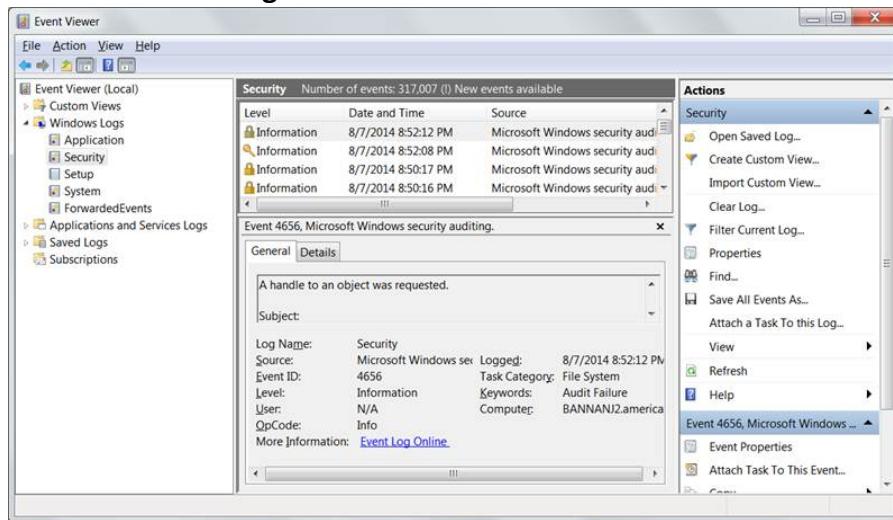
The parameters for each host are given in full along with descriptions in the following table. Selections from the initial parameter entry window for the local host are reflected in the first row of the table. Select options and provide custom log and filter information for each additional host manually.

After entering the parameter information, click **Next**.

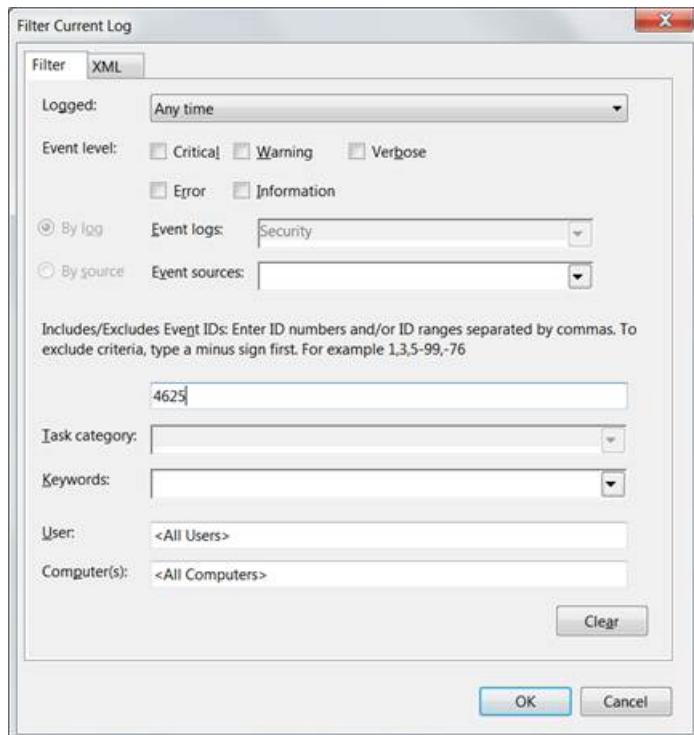
Configuring Filter

To configure a filter, first launch the event viewer and select the event log that needs the filter setting.

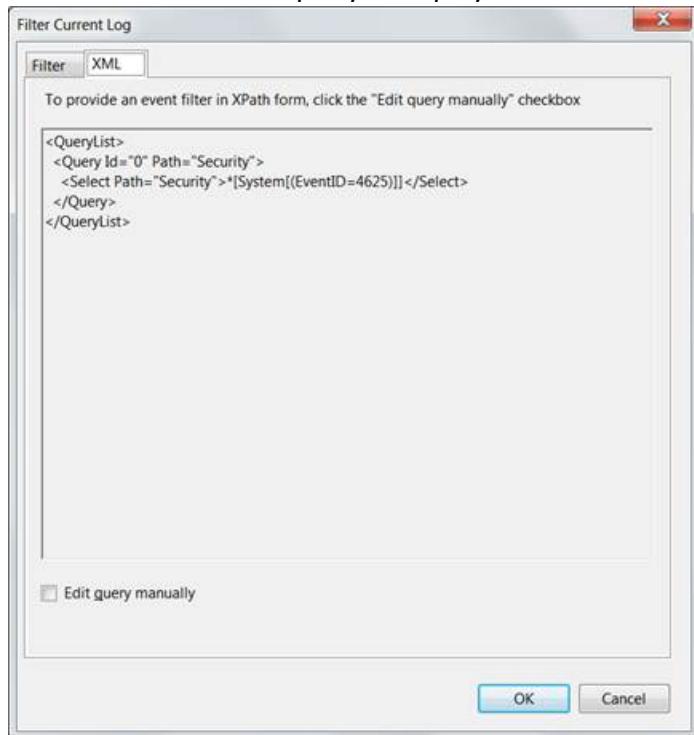
1. Click **Filter current log** to set the filter.



For example, to collect the logon failure events whose Event ID is 4625, enter the Event ID number as shown in the following figure.



2. Click the **XML** tab. The query is displayed in XML.



The expression that appears between `<Select>` and `</Select>` is the value that can be entered in the filter. Here it writes `*[System[(EventID=4625)]]`. This can be copied to the **Filter** column in the host table parameter for the desired event log.

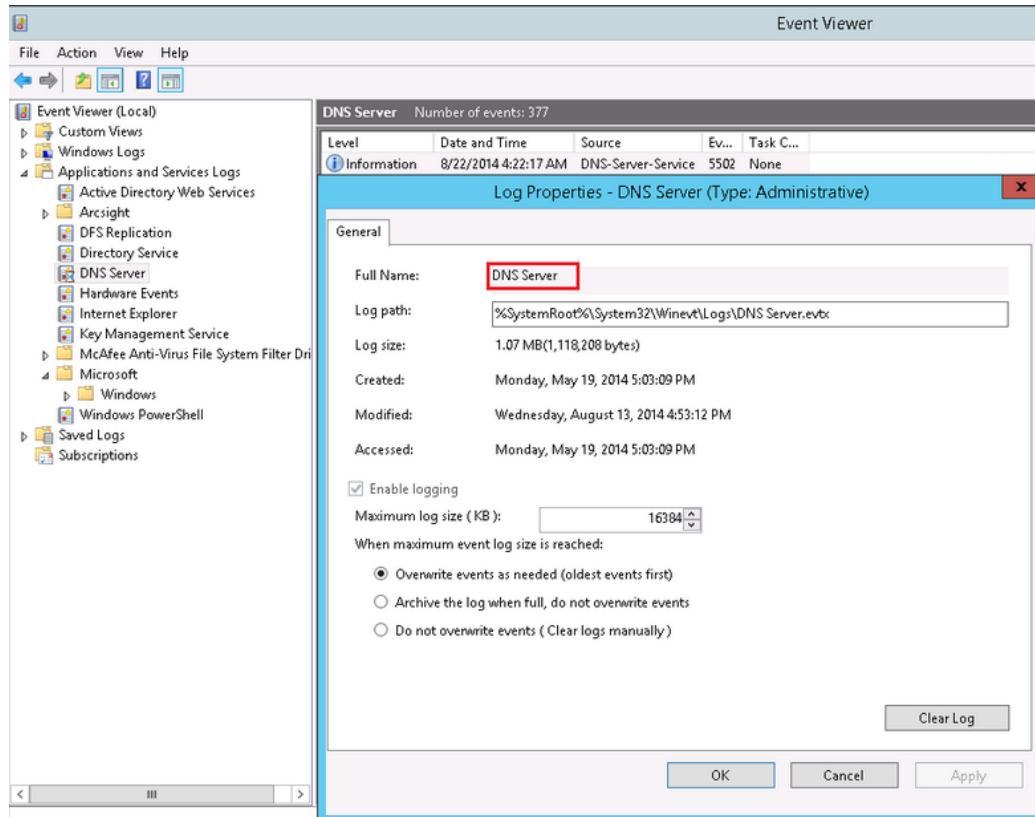
 **Note:** In certain cases, the text cannot be directly copied to the Filter column in the UI wizard. If the filter text contains “gt;”, “lt;”, “gt;=” or “lt;=”, you must replace it with “>”, “<”, “>=” or “<=” respectively.

Specifying Custom Log Names

In the Windows Host parameters window, a column for the **Custom Log Names** parameter lets you specify names of custom event logs. Applications also can generate events for a custom application event log, such as DNS Server, Directory Service, Exchange Auditing, and so on. (Parsing support for only the event header is supported for application events.)

For example, specify `Directory Service` for Active Directory and `Exchange Auditing` for Microsoft Exchange Audit. For Microsoft Windows Print Service Admin log, use `Microsoft-Windows-PrintService/Admin`.

To identify the Custom Event Log Name, select the **Custom Application Event Log** in the Microsoft Windows **Event Viewer**. The log name can be found from the properties of the event log in the **Full Name** field, as shown in the following figure.



For more information about setting this parameter, see “[Advanced Configuration Parameters per Host](#).”

Collecting Forwarded Events

The connector has the ability to read events forwarded to a Windows Event Collector host. Windows Event Collection is a Microsoft capability that lets a Windows host collect events from multiple sources. Collecting forwarded events is different than the traditional event collection because the events are collected from multiple sources.

With Microsoft Windows Event Collector (WEC), you can subscribe to receive and store events on a local computer (event collector) that are forwarded from any number of remote computers (event sources). Before using this feature, refer to Microsoft Windows documentation, to know more about Windows Event Collector functionality.



Note: When configuring Windows Event Collection (WEC), Microsoft by default adds to every forwarded event a **RenderingInfo** section that is a textual description of an event. This extra section introduces negative impacts on the resource usage of the WEC machine and the performance of the connector. Therefore, OpenText advises that you disable the **RenderingInfo** section. To do so, run the following command from the Windows command console: `wecutil ss <subscription-name> /cf:events`, where `subscription-name` is the WEC configuration created for event forwarding. This can be found in the **Event Viewer > Subscriptions** folder.

Event Collector for Windows Event Forwarding

You can forward events from a source host to any log type on the collector machine to which the connector would normally have access.



Note: Security events cannot be forwarded to the Security event log on a collector machine, but can be forwarded to other log types

Source Hosts Windows OS Version

When the connector is configured with the log that has forwarded events, the Windows OS version of the event source host is not populated automatically in the normalized events. To have this value populated, the Windows OS version should be provided as a source host file or the Active Directory should be configured. If the Windows OS version is available from the source host file as well as Active Directory, the value from Active Directory takes precedence. Active Directory as Source for OS Version. For more information, see [Microsoft Documentation](#).

When this selection is chosen during connector configuration, the connector pulls the host information (host name and version) from the configured Active Directory to identify the event source host Windows version information. Newly discovered hosts are added to the lookup automatically without reconfiguring the connector itself.

Active Directory information is checked upon connector startup and every 24 hours (86400000 milliseconds). To change the time setting, locate the `agent.properties` file in `$ARCSIGHT_HOME/current/agent` and set the `hostbrowsingthreadsleepetime` parameter to the number of milliseconds between host browsing queries.) This value should be greater than 0; if the value is set to 0, it will not perform periodic host browsing. For the connector to be able to browse the Active Directory to retrieve source host Windows version information, it should be placed within the same forest as the Active Directory.

File as Source for OS Version

When this selection is chosen during connector configuration, create a source host file in .csv format that contains the host name and Windows OS version and upload this file during the connector installation/configuration process (the WEF Source Hosts File Name in step 9).



Note: The host file, which is imported to or exported from the host table during installation, and the source host file specified in the WEF Source Hosts File Name field are two different entities. The source host file contains only the host name and version information to populate the version in the device version field.

When creating a source host file, make sure to specify the FQDN registered with Active Directory, as the connector finds the version information using the computer name in the event. An example of the source host file could be:

```
Hostsd.domain.com,Windows Server 2016
```

The valid versions descriptions (case sensitive) that can be used in source hosts files are:

```
Windows Server 2016
```



Note: OS version information is optional; events may still be parsed in a majority of cases.

Once configured, the OS version is loaded from the source host file when the connector is running on its first run, and is reloaded on the next startup of the connector when the source host file has a timestamp different from the one loaded from the last file processed.

The device version will not be populated in the normalized events.

Additional Connector Configurations

You can refer to the following sections for additional and optional connector configurations:

Configuring Custom Logs and Filtering

If you selected **Custom logs** in the **Select logs for event collection** section of the initial configuration window, and you want to add filtering for the local host, check **Custom Logs**

in the **Select logs for event collection** section to ensure this window is displayed for you to enter filter parameters.

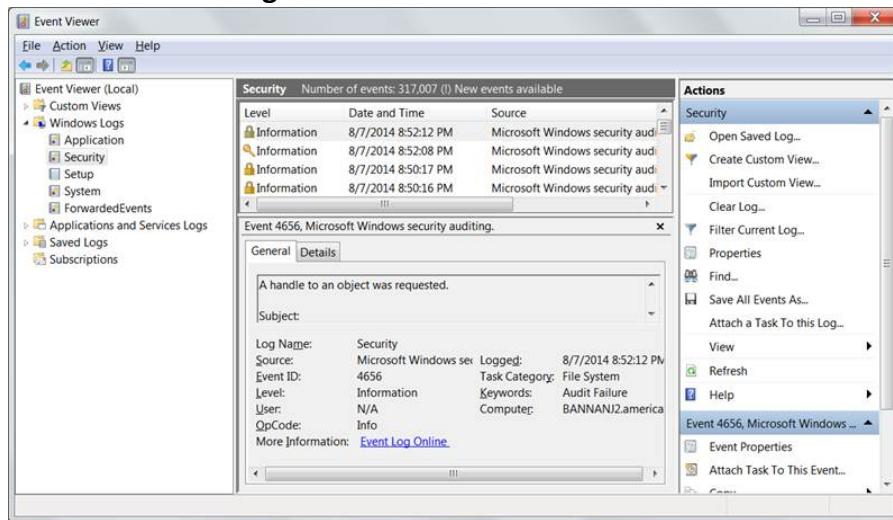
The parameters for each host are given in full along with descriptions in the following table. Selections from the initial parameter entry window for the local host are reflected in the first row of the table. Select options and provide custom log and filter information for each additional host manually.

After entering the parameter information, click **Next**.

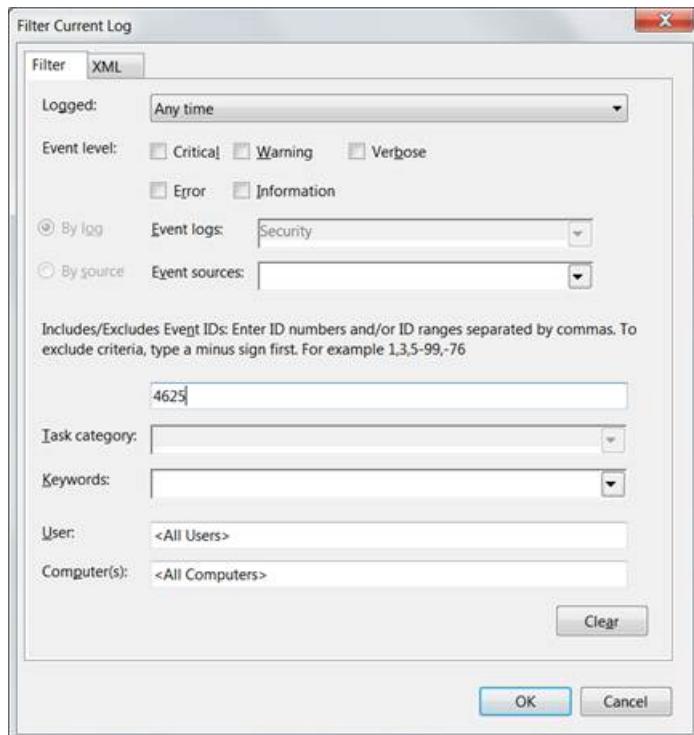
Configuring Filter

To configure a filter, first launch the event viewer and select the event log that needs the filter setting.

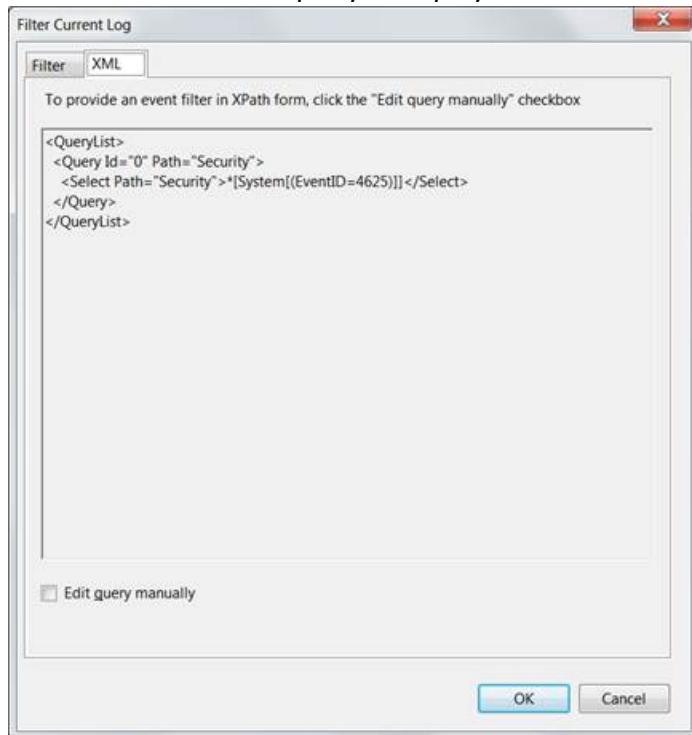
1. Click **Filter current log** to set the filter.



For example, to collect the logon failure events whose Event ID is 4625, enter the Event ID number as shown in the following figure.



2. Click the **XML** tab. The query is displayed in XML.



The expression that appears between `<Select>` and `</Select>` is the value that can be entered in the filter. Here it writes `*[System[(EventID=4625)]]`. This can be copied to the **Filter** column in the host table parameter for the desired event log.



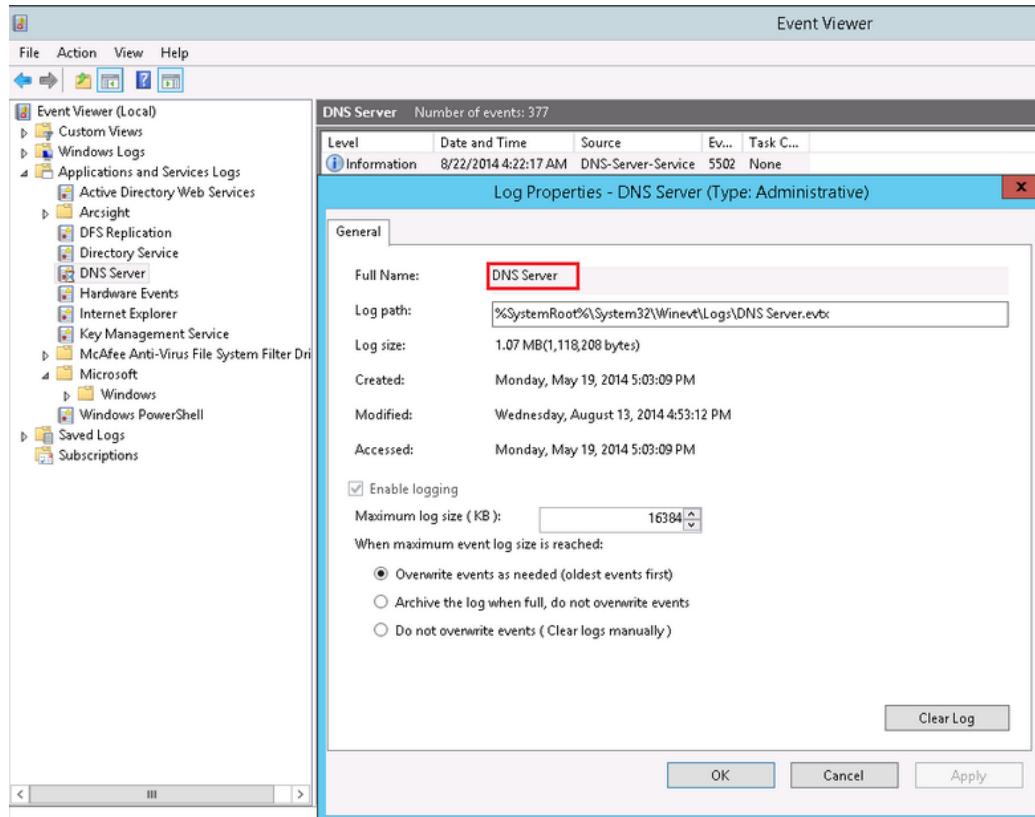
Note: In certain cases, the text cannot be directly copied to the Filter column in the UI wizard. If the filter text contains “gt;”, “lt;”, “gt;=” or “lt;=”, you must replace it with “>”, “<”, “>=” or “<=” respectively.

Specifying Custom Log Names

In the Windows Host parameters window, a column for the **Custom Log Names** parameter lets you specify names of custom event logs. Applications also can generate events for a custom application event log, such as DNS Server, Directory Service, Exchange Auditing, and so on. (Parsing support for only the event header is supported for application events.)

For example, specify `Directory Service` for Active Directory and `Exchange Auditing` for Microsoft Exchange Audit. For Microsoft Windows Print Service Admin log, use `Microsoft-Windows-PrintService/Admin`.

To identify the Custom Event Log Name, select the **Custom Application Event Log** in the Microsoft Windows **Event Viewer**. The log name can be found from the properties of the event log in the **Full Name** field, as shown in the following figure.



For more information about setting this parameter, see “[Advanced Configuration Parameters per Host](#).”

Configuring the Host Browsing Thread Sleep Time

If you selected **Use Active Directory for OS version** to specify the Windows OS version for the hosts from which you want to collect eventSelect this option, then the connector retrieves the host details from the configured Active Directory to identify the event source host Windows version information.

Newly discovered hosts are added to the lookup automatically without having to reconfigure the connector itself. Active Directory information is verified every time the connector starts and every 24 hours (86400000 milliseconds).

To change the time setting:

1. Open the agent.properties file in \$ARCSIGHT_HOME/current/agent
2. Set the **hostbrowsingthreadsleepetime** parameter to the number of milliseconds between host browsing queries. This value must be greater than 0. If the value is set to 0, then it does not perform periodic host browsing.

Creating a Source Hosts File

During connector configuration, if **File as Source for OS Version** is selected, then create a source host file in .csv format with the host name and Windows OS version, and upload the file during the connector configuration.



Note: The host file, which is imported to or exported from the host table during installation, and the source host file specified in the **WEF Source Hosts File Name** field are two different entities. The source host file contains only the host name and version information to populate the version in the device version field.

When creating a source host file, make sure to specify the FQDN registered with Active Directory, as the connector finds the version information using the computer name in the event. An example of the source host file could be:

Hostsd.domainind.com,Windows Server 2016

The valid versions descriptions (case sensitive) that can be used in source hosts files are:

Windows Server 2016



Note: OS version information is optional; events may still be parsed in a majority of cases.

After the configuration, the OS version is loaded from the source host file when the connector is running on its first run, and is reloaded on the next startup of the connector when the source host file has a timestamp different from the one loaded from the last file processed.

The device version will not be populated in the normalized events.

Collecting 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 **Directory Service** in the **Custom Log Names** field.

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

Directory Service, 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*.

Configuring Advanced Options

This section documents some of the advanced configuration parameters available with this connector. The table following the procedure for accessing advanced configuration parameters details the parameters you may choose to adjust, depending upon the needs of your enterprise.

Accessing Advanced Parameters

After SmartConnector installation, you can edit the `agent.properties` file to modify parameters. This file can be found at `$ARCSIGHT_HOME\current\user\agent`.

Advanced Container Configuration Properties

Specify	Parameter	Default
The protocol used between the connector and the collector. Currently supports TCP protocol.	mq.transport.protocol	tcp
The port used between the connector and the collector. The specified port will be bound during the connector installation. If more than one connector is to be installed on the same host, configure this with an unused port number.	mq.server.listener.port	61616
Whether the SID translation is required or not. The SID should be present in the remote host. Note: There may be a slight performance hit when being used.	winc.winc-agent.enableSidTranslation	True
The protocol used between the connector and the collector for event collection. Currently supports Raw TCP and TLS protocol. If you have installed the SmartConnector on the Win 2012 and Win 2012 R2 (with the latest security updates) and you want to use TLS, then perform the following steps: 1. Stop the connector. 2. Add the following cipher information in the agent.properties file: syslogng.ssl.cipher.suites=TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 3. Restart the connector.	agents[0].communicationprotocol	TLS
The port used between the connector and the collector for event collection. The default value is 30000, the port availability is checked sequentially and used if it's available.	agents[0].port	30000
Connector to use file queue to store the received raw events from the collector and process. Default value is true.	agents[0].usefilequeue	True
Maximum number of queue files to store the raw events. Default value is 100.	agents[0].filequeuemaxfilecount	100
Maximum size of each queue file. Default value is 10 MB.	agents[0].filequeuemaxfilesize	10000000
Number of event processing threads.	syslog.parser.threadcount	2

Advanced Common Configuration Parameters

Specify	Parameter	Default
Thread count for event processing threads dedicated for a single collector.	eventprocesssthreadcount	10
The queue size used to hold the ready to execute event processing task to improve performance. Larger queue length means bigger memory footprint and it does not necessarily help with performance improvement, as a limited number of threads are available for processing.	Executequeueuelength	100
By default the statistics are calculated every 10 minutes and dumped into both the agent.log and to the EventStats report file in user/agent/agentdata. This interval governs how often stats are calculated. Stats include average per last interval for events per second.	pdastatsinterval	600000ms
Whether to preserve the last ID processed before connector terminated or device went down.	preservestate	true
Event count before writing the preserve state.	preservedstatecount	100
Time interval in ms before writing the preserve state.	preservedstateinterval	10000

Advanced Configuration Parameters per Host

Specify	Parameter	Default
Whether to get the real-time events or read from the beginning of the event logs	startatend	true
To collect application events from custom application event logs, provide a comma separated list of the custom application event logs. Workgroup hosts have their separate shared SID cache.	eventlogtypes	null

Advanced Configuration Parameters for SID and GUID Translation

Specify	Parameter	Default
To enable GUID translation	enableguidtranslation	false
Size of the cache to store the GUIDs and their translated values	guidcachesize	50000
Time-to-live in ms for the GUID entries in the caches	guidcachetimetolive	600000
Interval in milliseconds (ms) at which the SID and GUID entries are to be expired from the caches	sidguidcacheexpirationthreadsleeptime	600000
Interval in ms at which the SID and GID caches are persisted to disk files. Each domain's SID cache is persisted to a separate disk file. The SID cache for workgroup hosts is persisted to a separate shared disk file.	sidguidcachepersistencethreadsleeptime	600000

Customizing Event Source Mapping

The Windows Event Log – Native application/system event parser loading mechanism relies on the event source for each event and attempts to load a parser with the following name convention:

`<Channel>\<ProviderName>.sdkkeyvaluefilereader.properties`

This convention works in the vast majority of cases but sometimes the parser needs more flexibility. In these cases, you can customize where to find these parsers by redirecting the variables `Channel` and `ProviderName`. For even more flexibility, the input `ProviderName` can be matched against a regular expression to avoid duplicate entries with minimal changes.

Creating an Override Map File

1. Navigate to `$ARCSIGHT_HOME/current/user/agent/fcp/winc/core_maps` and create an override map file with the name `customeventsources.map.csv` including the following columns:

```
SourceChannel
SourceProviderNamePattern
TargetProviderName
TargetChannel
```

The `SourceProviderNamePattern` value can be a string or a regular expression.

2. If there is no `winc/coremaps` subdirectory at `$ARCSIGHT_HOME/current/user/agent/fcp`, create one.
3. The last field `TargetChannel` is optional and, if empty, will be understood as the same as `SourceChannel`.

Customizing Event Parsing in a Clustered Environment

The default parser filename convention can cause problems in clustered environments, where the same event from different clusters can have different customized provider names. For example, SQL Server application events have the ProviderName `MSSQLSERVER`, resulting in a parser name of `application\mssqlserver.sdkkeyvaluefilereader.properties`.

In a clustered SQL Server environment, you can customize and configure the provider name for each cluster as `SQLSERVER01`, `SQLSERVER02`, and so forth. However, if the connector expects `MSSQLSERVER` as the provider name, the parsing fails for events with customized provider names, if the different providers have different names

To avoid this outcome, you can map all these different providers into one provider name value using the map file `$ARCSIGHT_HOME/user/agent/fcp/winc/core_maps/customeventsources.map.csv`.

The following are example entries based for a clustered environment:

```
Application, MSSQLSERVER01, MSSQLSERVER, Application
Application, MSSQLSERVER\d*, MSSQLSERVER, Application
Application, MSSQLSERVER.* , MSSQLSERVER, Application
```

The following are contents of a sample `customeventsources.map.csv` file with two entries:

```
#SourceChannel, SourceProviderNamePattern, TargetProviderName,
System, Service.* , service_control_manager,
Application, MSSQLSERVER.* , MSSQLSERVER,
```

Creating Custom Parsers for System and Application Events

The SmartConnector provides complete parsing of both the Windows event header and event description for all security events and some system events. For all system and application events, the connector provides complete parsing of the Windows event header. Also, the connector provides a framework to create and deploy your own parsers to parse the event description. Such a parser can parse events specific to a Channel and ProviderName.



Note: Custom Parsers or overrides you create are customizations. These are not certified for use through the ArcSight Quality Assurance Life Cycle of Testing. These are to be developed, tested, and maintained by the creator of the Custom Parser or override.

This section has the following topics:

Before Creating a Parser

Complete the following steps before creating a parser:

1. Generate the system or application events of interest.
2. Configure the connector to collect the system or application events and preserve the raw events.

When collecting events from system event logs (such as Service Control Manager, WINS), select **System** for **Windows Log type**.

When collecting events from application event logs (such as Microsoft Forefront Protection 2010 for Exchange, Microsoft SQL Server Audit), select **Application** for **Windows Log type**.

3. Run the connector to collect the system or application events and to generate the ArcSight raw events. The raw events will contain key-value pairs in JSON format. Using these generated raw events, see "[Create and Deploy Your Own Parser](#)" to map the values of these keys to the ArcSight event schema fields by creating a parser file.



Note: Not all raw events will have key-value pairs in the event body. Such events do not require that you create a parser to map anything to the ArcSight event schema fields. But you can still choose to create a parser to map the event name or description for such events.

Creating and Deploying Your Own Parser

To create and deploy your own parser:

1. Navigate to the directory location to deploy the parser file:

```
$ARCSIGHT_HOME\user\agent\fcp\winc
```

2. Identify the Channel for the events that need to be parsed (for example: System, Application, Directory Service, DNS Server, Key Management Service, and so on).
3. Identify the provider name of the events that need to be parsed, as events collected from a single channel can be generated by multiple provider names. For example, events collected from Channel: System can be generated by ProviderName: Service Control Manager, WINS, and so on.
4. Identify the SectionName of the event body that needs to be parsed, such as EventData, UserData, and so on.

- a. To parse the EventData section of the event body, create a key value parser file with the following naming convention, in the directory location identified in **Step 1**.

```
\{Normalized Channel}\  
\{Normalized ProviderName}.sdkkeyvaluefilereader.  
properties
```

For example, the key-value parser file name for:

- Channel: Security
- ProviderName: Microsoft Windows Event Log
- SectionName: EventData

will be:

```
\security\microsoft_windows_  
eventlog.sdkkeyvaluefilereader.properties
```

- b. To parse the other sections of the event body, such as UserData, create a JSON parser file with the following naming convention, in the directory location identified in **Step 1**.

```
\{Normalized Channel}\{Normalized ProviderName}.{Normalized  
SectionName}. jsonparser.properties
```

For example, the key-value parser file name for:

- Channel: Security
- ProviderName: Microsoft Windows Event Log
- SectionName: UserData

will be:

```
\security\microsoft_windows_eventlog.userdata.jsonparser.properties
```



Note: Normalize the Channel, ProviderName, and SectionName values by changing all letters to lower case, and then replacing each character that is not a letter or digit (including special characters and spaces) with an underscore character (_). Do not normalize the Locale and Encoding values.

5. Create mappings in these parsers as per your requirements by using conditional mappings based upon the ArcSight externalId field, which is already mapped to the Windows Event ID.

Because the connector already maps the Windows event header fields to ArcSight event fields as previously mentioned, those mappings need not be re-defined (unless you need to override the mapping values). The only mappings required are for mapping the specific event description.

- a. The following event header key-value parser can be used as a reference for:

- Channel: Security
- ProviderName: Microsoft Windows Event Log
- SectionName: EventData

to map the event name fields:

```
key.delimiter=&&
key.value.delimiter==
key.regexp=([^\&=]+)

event.deviceVendor=__getVendor("Microsoft")

conditionalmap.count=1
conditionalmap[0].field=event.externalId
conditionalmap[0].mappings.count=2

# The event logging service has shut down.
conditionalmap[0].mappings[0].values=1100
conditionalmap[0].mappings[0].event.flexString1=
conditionalmap[0].mappings[0].event.name=__stringConstant("The event
logging service has shut down.")
```

```
# The security log is now full.  
conditionalmap[0].mappings[1].values=1104  
conditionalmap[0].mappings[1].event.flexString1=  
conditionalmap[0].mappings[1].event.name=__stringConstant("The  
security log is now full.")
```

Make sure that no trailing spaces appear in your file after you copy and paste this example.

- b. The `UserData` section from following sample JSON parser can be used as a reference:

- Channel: Security
- ProviderName: Microsoft Windows Event Log
- SectionName: UserData

Sample `UserData` section:

```
{  
    "UserData": {  
        "LogFileCleared":  
  
            "@xmlns:auto-ns3":  
            "http://schemas.microsoft.com/win/2004/08/events",  
            "@_xmlns_":  
            "http://manifests.microsoft.com/win/2004/08/windows/eventlog",  
            "SubjectUserSid": "S-1-5-18",  
            "SubjectUserName": "SYSTEM",  
            "SubjectDomainName": "NT AUTHORITY",  
            "SubjectLogonId": "0x3e7"  
    }  
}
```

- c. The following `EventBody` JSON parser can be used as a reference:

- Channel: Security
- ProviderName: Microsoft Windows Event Log
- SectionName: UserData

Sample `EventBody` section:

```
trigger.node.location=/UserData  
event.deviceVendor=__getVendor("Microsoft")  
token.count=7  
token[0].name=SubjectUserSid
```

```
token[0].location=LogFileCleared/SubjectUserSid
token[0].type=String

token[1].name=SubjectUserName
token[1].location=LogFileCleared/SubjectUserName
token[1].type=String

token[2].name=SubjectDomainName
token[2].location=LogFileCleared/SubjectDomainName
token[2].type=String

token[3].name=SubjectLogonId
token[3].location=LogFileCleared/SubjectLogonId
token[3].type=String

token[4].name=Reason
token[4].location=AuditEventsDropped/Reason
token[4].type=String

token[5].name=Channel
token[5].location=AutoBackup/Channel
token[5].type=String

token[6].name=BackupPath
token[6].location=AutoBackup/BackupPath
token[6].type=String

conditionalmap.count=1
conditionalmap[0].field=event.externalId
conditionalmap[0].mappings.count=3

conditionalmap[0].mappings[0].values=1101
conditionalmap[0].mappings[0].event.name=__stringConstant("Audit
events have been dropped by the transport. The real time backup file
was corrupt due to improper shutdown.")
conditionalmap[0].mappings[0].event.deviceCustomNumber3=__safeToLong
(Reason)
conditionalmap[0].mappings[0].event.deviceCustomNumber3Label=__
stringConstant("Reason Code")

conditionalmap[0].mappings[1].values=1102
conditionalmap[0].mappings
[1].event.destinationNtDomain=SubjectDomainName
conditionalmap[0].mappings[1].event.destinationUserName=__
```

```
extractNTUser
(__oneOf(SubjectUserName,SubjectUserId))
conditionalmap[0].mappings[1].event.destinationUserId=SubjectLogonId
conditionalmap[0].mappings[1].event.name=__stringConstant("The audit
log was cleared.")

conditionalmap[0].mappings[2].values=1105
conditionalmap[0].mappings[2].event.fileType=Channel
conditionalmap[0].mappings[2].event.fileName=BackupPath
conditionalmap[0].mappings[2].event.name=__stringConstant("Event log
automatic backup")
```

Make sure that no trailing spaces appear in your file after you copy and paste this example.

6. Start the connector.

Verify categorization of new events to see if additional categorization are required. For information about categorization, see the Technical Note *ArcSight Categorization: A Technical Perspective* available from the OpenText [Software Support site](#). For more information about creating parsers, see the [Developer's Guide to FlexConnectors](#).

Customizing Localization Support

ArcSight SmartConnectors provide the event collection layer for ArcSight SIEM. Therefore, in the context of SmartConnectors, localization is related to the collection, parsing, and normalization of event messages that are generated by localized events and written in non-English languages. Localization (L10 N) is the process of converting a program to run in a particular locale or country, which includes displaying all text and translating the user interface into the native language.

To add location support beyond that provided by ArcSight, complete the following these steps.

1. Identify the Channel, ProviderName, locale, and encoding of the event for which you want to localize the event data.
2. Configure the host table parameters with the appropriate locale and encoding parameter values identified in step 1.

```
agents[x].windowshoststable[y].locale=<Locale>
agents[x].windowshoststable[y].encoding=<Encoding>
```

where x is the index of the connector and y is the index of hosts in the connector configuration.

Example:

```
agents[0].windowshoststable[0].locale=de_DE  
agents[0].windowshoststable[0].encoding=UTF-8
```

3. To add support for locales and encodings not shown in the connector host table configuration selections, change the `Locale` and `Encoding` values of the following lines in the `agent.properties` file (which can be found at `$ARCSIGHT_HOME\current\user\agent`):
4. Enter the type of character set encoding of the events in the log file, for example `event.name`. Create your content relative to this location: `$ARCSIGHT_HOME\user\agent\fcp\winc\`.
5. Identify the parser from which you want to invoke the localization extra-processor map file.

```
$ARCSIGHT_HOME\user\agent\winc\<NormalizedChannel>\  
<NormalizedProviderName>.sdkkeyvaluefilereader.properties
```

Example:

```
$ARCSIGHT_HOME\user\agent\winc\security\  
microsoft_windows_security_  
auditing.sdkkeyvaluefilereader.properties
```



Note: Normalize the **Channel**, **ProviderName**, and **SectionName** values by changing all letters to lower case, and then replacing each character that is not a letter or digit (including special characters and spaces) with an underscore character (_). Do not normalize the **Locale** and **Encoding** values.

6. For each locale and encoding combination, declare an extra-processor map file within this parser.

```
extraprocessor[4].type=map  
extraprocessor  
[4].filename=winc/<NormalizedChannel>/<NormalizedProviderName>  
.<Locale>.<Encoding>.map.csv  
extraprocessor[4].conditionfield=event.oldFileHash  
extraprocessor[4].conditiontype>equals  
extraprocessor[4].conditionvalues=<Locale>|<Encoding>  
extraprocessor[4].charencoding=<Encoding>  
extraprocessor[4].allowoverwrite=true  
extraprocessor[4].overrideeventmappings=true  
extraprocessor[4].clearfieldafterparsing=false  
extraprocessor[4].flexagent=false
```

Example:

```
extraprocessor[4].type=map
extraprocessor[4].filename=winc/security/
    microsoft_windows_security_auditing.fr_CA.UTF-8.l10n.map.csv
extraprocessor[4].conditionfield=event.oldFileHash
extraprocessor[4].conditiontype>equals
extraprocessor[4].conditionvalues=fr_CA|UTF-8
extraprocessor[4].charencoding=UTF-8
extraprocessor[4].allowoverwrite=true
extraprocessor[4].overrideeventmappings=true
extraprocessor[4].clearfieldafterparsing=false
extraprocessor[4].flexagent=false
```

7. Create the L10N extra-processor map file:

```
$ARCSIGHT_HOME\user\agent\winc\<NormalizedChannel>\ 
    <NormalizedProviderName>.<Locale>.<Encoding>.l10n.map.csv
```



Note: When creating, editing, or saving the L10N extra-processor map file, don't use an application with a default of **ASCII**, **UTF-8**, or other generic encoding. Create the file on the localized device or in a localized editor, and be sure that the encoding isn't overwritten when you save it.

Example:

```
$ARCSIGHT_HOME\user\agent\winc\security\
    microsoft_windows_security_auditing.fr_CA.UTF-8.l10n.map.csv
```



Note: Normalize the **Channel**, **ProviderName**, and **SectionName** values by changing all letters to lower case, and then replacing each character that is not a letter or digit (including special characters and spaces) with an underscore character (_). Do not normalize the **Locale** and **Encoding** values.

8. Within this file, declare the getters and setters, and add all the localization content. Use the event.externalId field as the getter, and the field that you want to localize as the setter. A sample file is shown for French:

```
event.externalId, set.event.name
"4886","Les services de certificats ont reçu une demande de
certificat."
"4887","Les services de certificats ont approuvé une demande de
certificat et émis un certificat."
"4884","Les services de certificats ont importé un certificat dans sa
base de données."
"4885","Le filtre d'audit des services de certificats modifié."
"4882","Les autorisations de sécurité pour les services de certificats
```

```
ont été modifiées."  
"4883","Les services de certificats ont récupéré une clé archivée."  
"4880","Les services de certificats ont démarré."  
"4881","Les services de certificats se sont arrêtés."  
...  
...
```



Note: Additional mapping can be set from ESM. Go to your ESM Console and run **Get Additional Data**. The command can only collect additional data from supported sources. Unsupported sources collect additional data from the event header.

Configuring Log Sources

This section provides information about configuring the following supported log sources:

Event Mappings for Active Directory

This section has the following topics:

General Mappings

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

NTDS Database Mappings

Event 1000

ArcSight Field	Vendor Field
Device Version	%1 (Microsoft Active Directory Domain services version)
Name	'Microsoft Active Directory Domain Services startup complete'

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1404

ArcSight Field	Vendor Field
Name	'This directory service is now the intersite topology generator and has assumed responsibility for generating and maintaining intersite replication topologies for this site'

Event 1844

ArcSight Field	Vendor Field
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'

Event 2064

ArcSight Field	Vendor Field
Message	'Active Directory has detected that the quota-tracking table is either missing or not completely built. The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'
Name	'Active Directory has detected that the quota-tracking table is either missing or not completely built'

Event 2065

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has completed rebuilding the quota-tracking table. Quota enforcement is now in effect'

Event 2886

ArcSight Field	Vendor Field
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'

Windows 2022 NTDS Database Mappings

Event 1009

ArcSight Field	Vendor Field
Name	The Knowledge Consistency Checker (KCC) has started updating the replication topology for the directory service.

Event 1013

ArcSight Field	Vendor Field
Name	The replication topology update task terminated normally.

Event 1133

ArcSight Field	Vendor Field
Name	This directory service is the intersite topology generator for the following site.
Device Custom String 5 Label	Site
Device Custom String 5	%1

Event 1166

ArcSight Field	Vendor Field
Name	Active Directory Domain Services might use the following index to optimize a query. The approximate record count for using this index is as follows.
Old File Path	%1
Device Custom Number 1 Label	Record Count
Device Custom Number 1	%2

Event 1167

ArcSight Field	Vendor Field
Name	Active Directory Domain Services will use the following index as the optimal index for this query.
Old File Path	%1

Event 1197

ArcSight Field	Vendor Field
Name	The directory partition has the following number of full-replica sites and partial-replica sites.
Device Custom String 1 Label	Directory Partition
Device Custom String 1	%1
Device Custom Number 1 Label	Full-replica sites

ArcSight Field	Vendor Field
Device Custom Number 1	%2
Device Custom Number 2 Label	Partial-replica sites
Device Custom Number 2	%3

Event 1257

ArcSight Field	Vendor Field
Name	The security descriptor propagation task is processing a propagation event starting from the following container.
Device Custom String 6 Label	Container
Device Custom String 6	%1

Event 1258

ArcSight Field	Vendor Field
Name	The security descriptor propagation task has finished processing a propagation event starting from the following container.
Device Custom String 6 Label	Container
Device Custom String 6	%1
Device Custom Number 2 Label	Number of objects processed
Device Custom Number 2	%2

Event 1260

ArcSight Field	Vendor Field
Name	The security descriptor propagation task is waiting for a propagation event.

Event 1261

ArcSight Field	Vendor Field
Name	The security descriptor propagation task has been notified of waiting propagation events.

Event 1481

ArcSight Field	Vendor Field
Name	The operation on the object failed.
Reason	%1

Event 1515

ArcSight Field	Vendor Field
Name	Active Directory Domain Services received a request for directory service information for the following directory partition.
Device Custom String 1 Label	Directory partition
Device Custom String 1	%1
Device Custom Number 2 Label	Information level
Device Custom Number 2	%2

Event 1516

ArcSight Field	Vendor Field
Name	Active Directory Domain Services completed the request for directory service information.
Reason	%1

Event 1517

ArcSight Field	Vendor Field
Name	Active Directory Domain Services received a request for group memberships with the following parameters.
Old File Hash	%1
Old File Permission	%2
Old File Name	%4

Event 1518

ArcSight Field	Vendor Field
Name	Active Directory Domain Services completed the request for group memberships.
Reason	%1

Event 1544

ArcSight Field	Vendor Field
Name	The following directory service was chosen as a bridgehead server for this site.
Device Custom String 6 Label	Directory Service
Device Custom String 6	%1
Device Custom String 5 Label	Site
Device Custom String 5	%2
Device Custom String 1 Label	Directory partition
Device Custom String 1	%3

Event 1585

ArcSight Field	Vendor Field
Name	The Windows NT 4.0 or earlier replication checkpoint with the PDC emulator master was successful.

Event 1904

ArcSight Field	Vendor Field
Name	The Knowledge Consistency Checker (KCC) is using the Windows Server 2003 intersite replication topology generator algorithm.

Windows 2008 NTDS Database Mappings

General

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	Microsoft Active Directory Domain services version

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Microsoft Active Directory Domain services version)

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared. New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1404

ArcSight Field	Vendor Field
Name	'This directory service is now the intersite topology generator and has assumed responsibility for generating and maintaining intersite replication topologies for this site'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory has detected that the quota-tracking table is either missing or not completely built'
Message	'Active Directory has detected that the quota-tracking table is either missing or not completely built. The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2065

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has completed rebuilding the quota-tracking table. Quota enforcement is now in effect'

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Windows 2008 General NTDS Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory startup complete'
Device Version	%1 (Microsoft Active Directory Domain Services version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service
Source User Name	User

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory was unable to establish a connection with the global catalog'
Message	'Make sure a global catalog is available in the forest, and is reachable from this domain controller. You may use the nltest utility to diagnose this problem'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1463

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected and deleted some possibly corrupted indices as part of initialization'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition

ArcSight Field	Vendor Field
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID
Destination Host name	%5 (source directory service address)

Event 1863

ArcSight Field	Vendor Field
Name	'This directory server has not received replication information from a number of directory servers within the configured latency interval'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of directory servers in all sites
Device Custom Number 2	Number of directory servers in this site
Device Custom Number 3	Latency Interval (Hours)
File Type	Registry Key
File Name	%5 (Registry Key)

Event 1864

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'Directory servers that do not replicate in a timely manner may encounter errors. They may miss password changes and be unable to authenticate. A DC that has not replicated in a tombstone lifetime may have missed the deletion of some objects, and may be automatically blocked from future replication until it is reconciled'
Device Custom String 1	Directory partition
Device Custom Number 1	More than 24 hours
Device Custom Number 2	More than a week
Device Custom Number 3	More than one month

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory has located a global catalog'
Device Custom String 5	Site
Destination Host Name	%1 (Global catalog)

Event 1898

ArcSight Field	Vendor Field
Name	'Internal event: Schema object was modified'
Device Custom String 5	Schema object
File Name	%1 (Schema object name)
File Type	'Schema object'

Event 1925

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link for writable directory partition failed'
Message	'This directory service will be unable to replicate with the source directory service until this problem is corrected'
Destination Host Name	%2 (Source directory service address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source directory service
Source User Name	User

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)

ArcSight Field	Vendor Field
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
Source User Name	User

Event 2013

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services is rebuilding indices as part of the initialization process'
Device Custom Number 3	Indices

Event 2014

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services successfully completed rebuilding indice'
Device Custom Number 3	Indices

Event 2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom String 1	Event Code
Device Custom Number 3	Number of duplicate entries

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected that the quota-tracking table is either missing or not completely built'
Message	'The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Destination Host Name	%2 (Failing DNS host name)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Destination Host Name	%2 (Failing DNS host name)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	%4 (FSMO Role)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

General NTDS Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory startup complete'
Device Version	%1 (Microsoft Active Directory Domain Services version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service
Source User Name	User

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory was unable to establish a connection with the global catalog'
Message	'Make sure a global catalog is available in the forest, and is reachable from this domain controller. You may use the nltest utility to diagnose this problem'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)

ArcSight Field	Vendor Field
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1463

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected and deleted some possibly corrupted indices as part of initialization'

Event 1844

ArcSight Field	Vendor Field
Name	'The local domain controller could not connect with domain controller hosting directory partition to resolve distinguished names'
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID
Destination Host name	%5 (source directory service address)

Event 1863

ArcSight Field	Vendor Field
Name	'This directory server has not received replication information from a number of directory servers within the configured latency interval'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of directory servers in all sites

ArcSight Field	Vendor Field
Device Custom Number 2	Number of directory servers in this site
Device Custom Number 3	Latency Interval (Hours)
File Type	Registry Key
File Name	%5 (Registry Key)

Event 1864

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'Directory servers that do not replicate in a timely manner may encounter errors. They may miss password changes and be unable to authenticate. A DC that has not replicated in a tombstone lifetime may have missed the deletion of some objects, and may be automatically blocked from future replication until it is reconciled'
Device Custom String 1	Directory partition
Device Custom Number 1	More than 24 hours
Device Custom Number 2	More than a week
Device Custom Number 3	More than one month

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory has located a global catalog'
Device Custom String 5	Site
Destination Host Name	%1 (Global catalog)

Event 1898

ArcSight Field	Vendor Field
Name	'Internal event: Schema object was modified'
Device Custom String 5	Schema object
File Name	%1 (Schema object name)
File Type	'Schema object'

Event 1925

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link for writable directory partition failed'
Message	'This directory service will be unable to replicate with the source directory service until this problem is corrected'
Destination Host Name	%2 (Source directory service address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source directory service
Source User Name	User

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
Source User Name	User

Event 2013

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services is rebuilding indices as part of the initialization process'
Device Custom Number 3	Indices

Event 2014

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services successfully completed rebuilding indice'
Device Custom Number 3	Indices

Event 2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom String 1	Event Code
Device Custom Number 3	Number of duplicate entries

Event 2064

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has detected that the quota-tracking table is either missing or not completely built'
Message	'The table will be rebuilt in the background (resuming the progress of any previous rebuild, if possible). Until it has completed, quota enforcement will not be in effect'

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'

ArcSight Field	Vendor Field
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Destination Host Name	%2 (Failing DNS host name)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Destination Host Name	%2 (Failing DNS host name)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	%4 (FSMO Role)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

NTDS ISAM Mappings

Event 102

ArcSight Field	Vendor Field
Name	'The database engine started a new instance'
Device Version	All of (%5, %6, %7, %8)
Device Custom String 5	Instance ID

Event 103

ArcSight Field	Vendor Field
Name	'The database engine stopped the instance'
Device Custom String 5	Instance ID

Event 300

ArcSight Field	Vendor Field
Name	'The database engine is initiating recovery steps'

Event 301

ArcSight Field	Vendor Field
Name	'The database engine has begun replaying logfile'
File Name	%4 (logfile)
Device Custom Number 1	%7 (Time Seen)
Device Custom String 4	%5 (Processing Stats)
Device Custom String 5	%6 (Most Frequent Record Type)

Event 302

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed recovery steps'

Event 609

ArcSight Field	Vendor Field
Name	'The database engine is initiating index cleanup of database as a result of a Windows version upgrade'
Message	'This message is informational and does not indicate a problem in the database'
File Name	%4 (database)
Device Version	All of (%5,'.',%6,'.',%7,'.',%8)
Device Custom String 5	old device version

Event 611

ArcSight Field	Vendor Field
Name	'The secondary index of table will be rebuilt as a precautionary measure after the Windows version upgrade of this system'
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 612

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed index cleanup on database'
File Name	%4 (database)

Event 614

ArcSight Field	Vendor Field
Name	'The secondary index of table may be corrupt'
Message	'If there is no later event showing the index being rebuilt, then please defragment the database to rebuild the index'
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 626

ArcSight Field	Vendor Field
Name	'The database engine updated index entries in database because of a change in the NLS version'
Message	'This message is informational and does not indicate a problem in the database'
Device Custom Number 3	Index entries
File Name	%5 (database)

Event 700

ArcSight Field	Vendor Field
Name	'Online defragmentation is beginning a full pass on database'
File Name	%4 (database)

Event 701

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed a full pass on database'
File Name	%4 (database)

Event 702

ArcSight Field	Vendor Field
Name	'Online defragmentation is resuming its pass on database'
File Name	%4 (database)

Event 703

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed the resumed pass on database'
File Name	%4 (database)

Event 704

ArcSight Field	Vendor Field
Name	'Online defragmentation of database was interrupted and terminated'
Message	'The next time online defragmentation is started on this database, it will resume from the point of interruption'
File Name	%4 (database)

Windows 2008 NTDS ISAM Mappings

Event 102

ArcSight Field	Vendor Field
Name	'The database engine started a new instance'
Device Version	All of (%5,'.',%6,'.',%7,'.',%8)
Device Custom String 5	Instance ID

Event 103

ArcSight Field	Vendor Field
Name	'The database engine stopped the instance'
Device Custom String 5	Instance ID

Event 300

ArcSight Field	Vendor Field
Name	'The database engine is initiating recovery steps'

Event 301

ArcSight Field	Vendor Field
Name	'The database engine has begun replaying logfile'
File Name	%4 (logfile)
Device Custom Number 1	%7
Device Custom String 4	%5
Device Custom String 5	%6

Event 302

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed recovery steps'

Event 609

ArcSight Field	Vendor Field
Name	'The database engine is initiating index cleanup of database as a result of a Windows version upgrade'
Message	'This message is informational and does not indicate a problem in the database'
File Name	%4 (database)
Device Version	All of (%5,'.',%6,'.',%7,'.',%8)
Device Custom String 5	old device version

Event 611

ArcSight Field	Vendor Field
Name	'The secondary index of table will be rebuilt as a precautionary measure after the Windows version upgrade of this system'
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 612

ArcSight Field	Vendor Field
Name	'The database engine has successfully completed index cleanup on database'
File Name	%4 (database)

Event 614

ArcSight Field	Vendor Field
Name	'The secondary index of table may be corrupt'
Message	'If there is no later event showing the index being rebuilt, then please defragment the database to rebuild the index'

ArcSight Field	Vendor Field
File Name	%4 (database)
Device Custom String 5	'Database Index'
Device Custom String 6	'Database Table'

Event 626

ArcSight Field	Vendor Field
Name	'The database engine updated index entries in database because of a change in the NLS version'
Message	'This message is informational and does not indicate a problem in the database'
Device Custom Number 3	Index entries
File Name	%5 (database)

Event 700

ArcSight Field	Vendor Field
Name	'Online defragmentation is beginning a full pass on database'
File Name	%4 (database)

Event 701

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed a full pass on database'
File Name	%4 (database)

Event 702

ArcSight Field	Vendor Field
Name	'Online defragmentation is resuming its pass on database'
File Name	%4 (database)

Event 703

ArcSight Field	Vendor Field
Name	'Online defragmentation has completed the resumed pass on database'
File Name	%4 (database)

Event 704

ArcSight Field	Vendor Field
Name	'Online defragmentation of database was interrupted and terminated'
Message	'The next time online defragmentation is started on this database, it will resume from the point of interruption'
File Name	%4 (database)

NTDS KCC Mappings

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service

Event 1128

ArcSight Field	Vendor Field
Name	'A replication connection was created from source directory service to the local directory service'
Device Custom String 1	Creation Point Internal ID

ArcSight Field	Vendor Field
Device Custom String 4	Reason or Error Code
Device Custom String 5	Local directory service
Device Custom String 6	Source directory service

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Domain service

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller

Windows 2008 NTDS KCC Mappings

Event 1104

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) successfully terminated change notifications'
Message	'This event can occur if either this directory service or the destination directory service has been moved to another site'
Destination Host Name	%2 (Destination network address)
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 6	Destination directory service

Event 1128

ArcSight Field	Vendor Field
Name	'A replication connection was created from source directory service to the local directory service'
Device Custom String 1	Creation Point Internal ID
Device Custom String 4	Reason or Error Code
Device Custom String 5	Local directory service
Device Custom String 6	Source directory service

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)

ArcSight Field	Vendor Field
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Domain service

Event 1926

ArcSight Field	Vendor Field
Name	'The attempt to establish a replication link to a read-only directory partition failed'
Destination Host Name	%2 (Source domain controller address)
Destination User Name	User
Device Custom String 1	Directory partition
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller

Windows 2008 NTDS LDAP Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Device Custom String 5	Site
Destination Host Name	%1 (Global catalog)

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Source Host Name	%2 (Failing DNS host name)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Source Host Name	%2 (Failing DNS host name)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \'LDAP Interface Events\' event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

NTDS Replication Mappings

Event 1188

ArcSight Field	Vendor Field
Name	'A thread in Active Directory Domain Services is waiting for the completion of a RPC made to directory service'
Message	'Active Directory Domain Services has attempted to cancel the call and recover this thread. If this condition continues, restart the directory service'
Device Custom String 1	Thread ID
Device Custom String 5	Operation
Device Custom String 6	Directory service
Device Custom Number 2	Timeout period (minutes)

Event 1232

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to perform a remote procedure call (RPC) to server. The call timed out and was cancelled'
Destination Host Name	%2 (Destination Host Name)
Device Custom Number 2	Call Timeout (Mins)
Device Custom String 1	Thread ID
Device Custom String 5	Internal ID
Source User Name	User

Event 1863

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'This directory server has not received replication information from a number of directory servers within the configured latency interval. To identify the directory servers by name, use the dcdiag.exe tool. You can also use the support tool repadmin.exe to display the replication latencies of the directory servers. The command is \"repadmin /showvector /latency <partition-dn>\"'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of domain controllers in all sites
Device Custom Number 3	Number of domain controllers in this site
Device Custom Number 2	Latency Interval (Hours)
File Type	Registry Key
File Name	Both (%5,'\\Replicator latency error interval(hours)')

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address. This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Source Host Name	%2 (Failing DNS host name)
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	FSMO Role

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \"LDAP Interface Events\" event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

Windows 2008 NTDS Replication Mappings

Event 1188

ArcSight Field	Vendor Field
Name	'A thread in Active Directory Domain Services is waiting for the completion of a RPC made to directory service'
Message	'Active Directory Domain Services has attempted to cancel the call and recover this thread. If this condition continues, restart the directory service'
Device Custom String 1	Thread ID
Device Custom String 5	Operation
Device Custom String 6	Directory service
Device Custom Number 2	Timeout period (minutes)

Event 1232

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to perform a remote procedure call (RPC) to server. The call timed out and was cancelled'
Destination Host Name	%2 (Destination Host Name)
Device Custom Number 2	Call Timeout (Mins)
Device Custom String 1	Thread ID
Device Custom String 5	Internal ID
Source User Name	User

Event 1863

ArcSight Field	Vendor Field
Name	'This is the replication status for directory partition on this directory server'
Message	'This directory server has not received replication information from a number of directory servers within the configured latency interval. To identify the directory servers by name, use the dcdiag.exe tool. You can also use the support tool repadmin.exe to display the replication latencies of the directory servers. The command is \"repadmin /showvector /latency <partition-dn>\"'
Device Custom String 1	Directory partition
Device Custom Number 1	Number of domain controllers in all sites
Device Custom Number 3	Number of domain controllers in this site
Device Custom Number 2	Latency Interval (Hours)
File Type	Registry Key
File Name	Both (%5,'\\Replicator latency error interval(hours)')

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address. This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Source Host Name	%2 (Failing DNS host name)
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)

Event 2092

ArcSight Field	Vendor Field
Name	'This server is the owner of FSMO role, but does not consider it valid'
Message	'For the partition which contains the FSMO, this server has not replicated successfully with any of its partners since this server has been restarted. Replication errors are preventing validation of this role. Operations which require contacting a FSMO operation master will fail until this condition is corrected'
Device Custom String 1	FSMO Role

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \'LDAP Interface Events\' event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

NTDS LDAP Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 5	Internal ID
Device Custom String 4	Reason or Error Code
Reason	%3 (Reason or Error Code)

Event 1138

ArcSight Field	Vendor Field
Name	'Function entered'
Message	Both ('Internal event:Function', %1, 'entered')

Event 1139

ArcSight Field	Vendor Field
Name	'Function exited'
Message	Both ('Internal event:Function', %1, 'exited')

Event 1213

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because it was disconnected on the client side'
Device Custom String 5	Internal ID

Event 1215

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because the client closed the connection'
Device Custom String 5	Internal ID

Event 1216

ArcSight Field	Vendor Field
Name	'An LDAP client connection was closed because of an error'
Source Address	%1 (Source address)
Reason	%3 (Reason or Error Code)
Device Custom String 5	Internal ID

Event 1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed.'
Device Custom Number 3	Attempts
Device Custom String 6	Directory service
Device Custom Number 2	Period of time (minutes)
Device Custom String 4	Reason or Error Code

Event 1317

ArcSight Field	Vendor Field
Name	'The directory service has disconnected the LDAP connection'
Message	'The directory service has disconnected the LDAP connection from the following network address due to a time-out'

ArcSight Field	Vendor Field
Source Address	%1 (Source address)

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted.'

Event 1535

ArcSight Field	Vendor Field
Name	'The LDAP server returned an error'
Message	Both ('The LDAP server returned an error value:',%1)
Reason	%1 (Reason or Error Code)

Event 1655

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services attempted to communicate with the following global catalog and the attempts were unsuccessful'
Device Host Name	%1 (Host name)
Reason	%2 (Reason or Error Code)

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Destination Host Name	%1 (Host name)
Device Custom String 5	Site

Event 2041

ArcSight Field	Vendor Field
Name	'Duplicate event log entries were suppressed'
Message	'See the previous event log entry for details. An entry is considered a duplicate if the event code and all of its insertion parameters are identical. The time period for this run of duplicates is from the time of the previous event to the time of this event'
Device Custom Number 3	Number of duplicate entries

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions, and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources.'
Device Custom String 6	Source domain controller
Source Host Name	%2 (Host name)
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	All of (%5,'\\',%6)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers, or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 6	Alternate server name
Source Host Name	%2 (Host name)
Device Custom String 4	Reason or Error Code
File Type	'Registry Key'
File Name	All of (%5,'\\',%6)

Event 2089

ArcSight Field	Vendor Field
Name	'This directory partition has not been backed up'
Message	'This directory partition has not been backed up since at least the following number of days'
Device Custom String 1	Directory partition
Device Custom Number 2	Latency interval (hours)
File Type	'Registry Key'
File Name	All of (%3,'\\',%4)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a clear text (non-SSL/TLS-encrypted) connection.'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher.'

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "\\"LDAP Interface Events\\" event logging category to level 2 or higher.'

ArcSight Field	Vendor Field
Device Custom Number 1	number of simple binds performed without SSL/TLS
Device Custom Number 2	number of negotiate/Kerberos/NTLM/Digest binds performed without signing

Event 2889

ArcSight Field	Vendor Field
Name	'LDAP bind without requesting signing or performed a simple bind'
Message	'The following client performed a SASL (Negotiate/Kerberos/NTLM/Digest) LDAP bind without requesting signing (integrity verification), or performed a simple bind over a cleartext (non-SSL/TLS-encrypted) LDAP connection'
Source User Name	%2 (User name)
Source Address	%1 (Source address)

Windows 2008 NTDS LDAP Mappings

Event 1000

ArcSight Field	Vendor Field
Name	'Microsoft Active Directory Domain Services startup complete'
Device Version	%1 (Version)

Event 1004

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was shut down successfully'

Event 1126

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services was unable to establish a connection with the global catalog'
Device Custom String 4	Reason or Error Code
Device Custom String 5	Internal ID

Event 1220

ArcSight Field	Vendor Field
Name	'LDAP over Secure Sockets Layer (SSL) will be unavailable at this time because the server was unable to obtain a certificate'
Device Custom String 4	Reason or Error Code

Event 1308

ArcSight Field	Vendor Field
Name	'The Knowledge Consistency Checker (KCC) has detected that successive attempts to replicate with the following directory service has consistently failed'
Message	'The Connection object for this directory service will be ignored, and a new temporary connection will be established to ensure that replication continues. Once replication with this directory service resumes, the temporary connection will be removed'
Device Custom Number 2	Period of time (minutes)
Device Custom Number 3	Attempts
Device Custom String 4	Reason or Error Code
Device Custom String 6	Directory service

Event 1394

ArcSight Field	Vendor Field
Name	'All problems preventing updates to the Active Directory Domain Services database have been cleared'
Message	'New updates to the Active Directory Domain Services database are succeeding. The Net Logon service has restarted'

Event 1869

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services has located a global catalog'
Device Custom String 5	Site
Destination Host Name	%1 (Global catalog)

Event 2087

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not resolve DNS host name of the source domain controller to an IP address'
Message	'This error prevents additions, deletions and changes in Active Directory Domain Services from replicating between one or more domain controllers in the forest. Security groups, group policy, users and computers and their passwords will be inconsistent between domain controllers until this error is resolved, potentially affecting logon authentication and access to network resources'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Source Host Name	%2 (Failing DNS host name)

Event 2088

ArcSight Field	Vendor Field
Name	'Active Directory Domain Services could not use DNS to resolve the IP address of the source domain controller'
Message	'To maintain the consistency of Security groups, group policy, users and computers and their passwords, Active Directory Domain Services successfully replicated using the NetBIOS or fully qualified computer name of the source domain controller. Invalid DNS configuration may be affecting other essential operations on member computers, domain controllers or application servers in this Active Directory Domain Services forest, including logon authentication or access to network resources. You should immediately resolve this DNS configuration error so that this domain controller can resolve the IP address of the source domain controller using DNS'
Device Custom String 4	Reason or Error Code
Device Custom String 6	Source domain controller
File Type	'Registry key'
File Name	All of (%5,'\\',%6)
Source Host Name	%2 (Failing DNS host name)

Event 2886

ArcSight Field	Vendor Field
Name	'The security of this directory server can be significantly enhanced by configuring the server to reject SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP binds that do not request signing (integrity verification) and LDAP simple binds that are performed on a cleartext (non-SSL/TLS-encrypted) connection'
Message	'Even if no clients are using such binds, configuring the server to reject them will improve the security of this server. Some clients may currently be relying on unsigned SASL binds or LDAP simple binds over a non-SSL/TLS connection, and will stop working if this configuration change is made. To assist in identifying these clients, if such binds occur this directory server will log a summary event once every 24 hours indicating how many such binds occurred. You are encouraged to configure those clients to not use such binds. Once no such events are observed for an extended period, it is recommended that you configure the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the "LDAP Interface Events" event logging category to level 2 or higher'

Event 2887

ArcSight Field	Vendor Field
Name	'During the previous 24 hour period, some clients attempted to perform LDAP binds'
Message	'During the previous 24 hour period, some clients attempted to perform LDAP binds that were either: (1) A SASL (Negotiate, Kerberos, NTLM, or Digest) LDAP bind that did not request signing (integrity validation), or (2) A LDAP simple bind that was performed on a cleartext (non-SSL/TLS-encrypted) connection. This directory server is not currently configured to reject such binds. The security of this directory server can be significantly enhanced by configuring the server to reject such binds. For more details and information on how to make this configuration change to the server, please see http://go.microsoft.com/fwlink/?LinkId=87923 . Summary information on the number of these binds received within the past 24 hours is below. You can enable additional logging to log an event each time a client makes such a bind, including information on which client made the bind. To do so, please raise the setting for the \'LDAP Interface Events\' event logging category to level 2 or higher'
Device Custom Number 1	Number of simple binds performed without SSL/TLS
Device Custom Number 2	Number of Negotiate/Kerberos/NTLM/Digest binds performed without signing

Event Mappings for Microsoft ADFS

General - Windows Server 2022

ArcSight Field	Vendor Field
Device Product	'ADFS Auditing'
Device Vendor	'Microsoft'

Event 100

ArcSight Field	Vendor Field
Name	The federation service started successfully.

Event 102

ArcSight Field	Vendor Field
Name	There was an error in enabling endpoints of Federation Service.
Reason	Data

Event 103

ArcSight Field	Vendor Field
Name	The Federation Service stopped successfully.

Event 105

ArcSight Field	Vendor Field
Device Custom String 4	SacumenADFSAdapter
Device Custom String 4 Label	Identifier
Device Custom String 5	Proxy device TLS pipeline
Device Custom String 5 Label	Context
Device Custom String 6	The authentication method MFAadapter.ADFSAdapter, MFAAdapter, Version=1.0.0.0, Culture=neutral, PublicKeyToken=95c8f0 9183447d36 could not be loaded. Could not load file or assembly 'MFAAdapter, Version=1.0.0.0, Culture=neutral, PublicKeyToken=95c8f0__regexToken(Data,".*\\\"(.*)\\\"\") event.deviceCustomString6 event.deviceCustomString6Label= (Exception details) Represents errors that occur during the process of loading authentication provider. 9183447d36' or one of its dependencies. The system cannot find the file specified.
Device Custom String 6 Label	Exception details
Name	An error occurred loading an authentication provider.

Event 106

ArcSight Field	Vendor Field
Device Custom String 1	Data
Device Custom String 1 Label	Identifier

ArcSight Field	Vendor Field
Device Custom String 4	Data
Device Custom String 4 Label	Context
Name	An authentication provider was successfully loaded.

Event 111

ArcSight Field	Vendor Field
Device Custom String 5	http://schemas.microsoft.com/idfx/requesttype/issue
Device Custom String 5 Label	Request Type
Device Custom String 6	<pre>System.ArgumentOutOfRangeException: Not a valid Win32 FileTime.\nParameter name: fileTime\n at System.DateTime.FromFileTimeUtc(Int64 fileTime)\n at Microsoft.IdentityServer.Tokens.LsaLogonUserHelper.GetPasswordExpiryDetails(SafeLsaReturnBufferHandle profileHandle, DateTime& nextPasswordChange, DateTime& lastPasswordChange)\n at Microsoft.IdentityServer.Tokens.LsaLogonUserHelper.GetLsaLogonUserInfo(SafeHGlobalHandle pLogonInfo, Int32 logonInfoSize, DateTime& nextPasswordChange, DateTime& lastPasswordChange, String authenticationType, String issuerName)\n at Microsoft.IdentityServer.Tokens.LsaLogonUserHelper.GetLsaLogonUser(String domain, String username, String password, DateTime& nextPasswordChange, DateTime& lastPasswordChange, String issuerName)\n at Microsoft.IdentityServer.Service.LocalAccountStores.ActiveDirectory.ActiveDirectoryCpTrustStore.ValidateUser(IAuthenticationContext context)\n at Microsoft.IdentityServer.Service.Tokens.MsisLocalCpUing6Label=(Exception details) request on the services. serNameSecurityTokenHandler.ValidateTokenInternal(UsernameAuthenticationContext usernameAuthenticationContext, SecurityToken token)\n at Microsoft.IdentityServer.Service.Tokens.MsisLocalCpUserNameSecurityTokenHandler.ValidateToken(SecurityToken token)\n at Microsoft.IdentityServer.Web.WSTrust.SecurityTokenServiceManager.ValidateSecurityToken(SecurityToken userToken, SecurityToken deviceToken)</pre>
Device Custom String 6 Label	Exception details
Name	The Federation Service encountered an error while processing the WS-Trust request.

Event 221

ArcSight Field	Vendor Field
Device Custom String 1	ADMIN0012: OperationFault
Device Custom String 1 Label	Error
Name	A change to the token service configuration was detected, but there was an error reloading the changes to configuration.

Event 227

ArcSight Field	Vendor Field
Device Custom String 6	System.ObjectDisposedException: Cannot access a closed file. at System.IO._Error.FileNotOpen() at System.IO.FileStream.Flush(Boolean flushToDisk) at System.IO.StreamWriter.Flush(Boolean flushStream, Boolean flushEncoder) at System.IO.StreamWriter.Dispose(Boolean disposing) at System.IO.TextWriter.Dispose() [REDACTED]Data event.deviceCustomString6 event.deviceCustomString6Label= (Exception details) Represents error details that occur during the shutdown. at Serilog.Sinks.File.FileSink.Dispose() at Serilog.Sinks.File.RollingFileSink.CloseFile() at Serilog.Sinks.File.RollingFileSink.Dispose() at Serilog.LoggerConfiguration.<>c__DisplayClass32_0.<CreateLogger>g_Dispose() at MFAAdapter.ADFSAdapter.Finalize()
Device Custom String 6 Label	Exception details
Name	The Federation Service encountered an unexpected exception and has shut down.

Event 249

ArcSight Field	Vendor Field
File Hash	Data
Name	The certificate identified by thumbprint could not be found in the certificate store.

Event 298

ArcSight Field	Vendor Field
Device Custom String 1	ServiceState.IsDrsInitialized is false
Device Custom String 1 Label	Additional Information
Name	The Windows Hello for Business key receipt certificate background task will not run.

Event 299

ArcSight Field	Vendor Field
Destination DNS Domain	%3 (Relying Party)
Device Custom String 1	%2 (Activity ID)
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1 (Instance ID)
Device Custom String 4 Label	"Instance ID"
Message	<code>__concatenate("A token was successfully issued for the relying party ",%3)</code>
Name	"A token was successfully issued for relying party"

Event 300

ArcSight Field	Vendor Field
Device Custom String 1	%1 (Activity ID)
Device Custom String 1 Label	"Activity ID"
Device Custom String 5	%2 (Request type)
Device Custom String 5 Label	"Request Type"
Device Custom String 6	%3 (Exception details)
Device Custom String 6 Label	"Exception details"
Message	"The Federation Service failed to issue a token as a result of an error during processing of the WS-Trust request"
Name	"Federation Service failed to issue a token as a result of an error"
Source Nt Domain	<code>__extractNTDomain(%3)</code>
Source User Name	<code>__extractNTUser(%3)</code>

Event 307

ArcSight Field	Vendor Field
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Name	"Federation service configuration was changed"
Source Nt Domain	__extractNTDomain(%3)
Source User Name	__extractNTUser(%3)

Event 309

ArcSight Field	Vendor Field
Name	The Federation Service configuration was changed.
Device Custom String 1	%1
Device Custom String 1 Label	Security ID
Device Custom String 5	%4
Device Custom String 5 Label	New Value
Device Custom String 6	%3
Device Custom String 6 Label	Old Value
Source NT Domain	%2
Source User Name	%2

Event 342

ArcSight Field	Vendor Field
Name	Token validation failed
Device Custom String 4	Data
Device Custom String 4 Label	Token Type
Reason	Data
Device Custom String 6	Data
Device Custom String 6 Label	Exception

Event 352

ArcSight Field	Vendor Field
Device Custom String 5	Data Source=np:\\\\.\\\\pipe \\\\microsoft##wid\\\\ts q\\\\query;Initial Catalog=AdfsConfigurationV4;Integrated Security=True
Device Custom String 5 Label	Connection String
Device Custom String 6	A network-related or instance-specific error occurred while establishing a connection to SQL Server. The server was not found or was not accessible. Verify that the instance name is correct and that SQL Server is configured to allow remote connections. (provider: Named Pipes Provider, error: 40 - Could not open a connection to SQL Server)
Device Custom String 6 Label	Exception Details
Name	A SQL operation in the AD FS configuration database failed.

Event 397

ArcSight Field	Vendor Field
Device Custom String 1	N/A
Device Custom String 1 Label	HTTP Proxy
Device Custom String 4	N/A
Device Custom String 4 Label	HTTP Proxy
Device Custom String 5	N/A
Device Custom String 5 Label	Bypass proxy for local addresses
Device Custom String 6	N/A
Device Custom String 6 Label	Bypass proxy for addresses
Name	The federation server loaded the HTTP proxy configuration from WinHTTP settings.

Event 403

ArcSight Field	Vendor Field
Destination Address	%9 (Local IP)
Destination Dns Domain	%14
Destination Port	%8 (Local Port)

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

Device Custom Date 1	%3
Device Custom Date 1 Label	"Request Time"
Device Custom Number 1	%11
Device Custom Number 1 Label	"Content Length"
Device Custom String 1	%2
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Device Custom String 6	%16
Device Custom String 6 Label	"Proxy DNS name"
End Time	%3
Name	"An HTTP request was received"
Old File Hash	<u>_concatenate("Through Proxy:",%15)</u>
Old File Id	<u>_concatenate("Caller Identity:",%12)</u>
Old File Type	<u>_concatenate("Certificate Identity:",%13)</u>
Request Client Application	%10 (User Agent)
Request Method	%5 (HTTP Method)
Request Url File Name	%6 (Url Absolute Path)
Request Url Query	%7 (Query string)
Source Address	%4
Start Time	%3

Event 404

ArcSight Field	Vendor Field
Device Custom Date 1	%3
Device Custom Date 1 Label	"Response Time"
Device Custom String 1	%2
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"

ArcSight Field	Vendor Field
Device Custom String 5	%5
Device Custom String 5 Label	"Status Description"
End Time	%3
Event Outcome	%4
Name	"An HTTP response was dispatched"

Event 405

ArcSight Field	Vendor Field
Destination Host Name	%3
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Message	<code>__concatenate("Password change succeeded for following user:",%2)</code>
Name	"Password change succeeded"
Source Nt Domain	<code>__extractNTDomain(%2)</code>
Source User Name	<code>__extractNTUser(%2)</code>

Event 406 - Windows Server 2016

ArcSight Field	Vendor Field
Destination Host Name	%3
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Message	<code>__concatenate("Password change failed for following user:",%2)</code>
Name	"Password change failed"
Reason	%4
Source Nt Domain	<code>__extractNTDomain(%2)</code>
Source User Name	<code>__extractNTUser(%2)</code>

Event 406 - Windows Server 2019

ArcSight Field	Vendor Field
Destination Host Name	%4
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%3
Device Custom String 4 Label	"Device Certificate"
Message	<code>__concatenate("Password change failed for following user:",%2)</code>
Name	"Password change failed"
Reason	%5
Source Address	%6
Source Nt Domain	<code>__extractNTDomain(%2)</code>
Source User Name	<code>__extractNTUser(%2)</code>

Event 410

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%3
Device Custom String 4 Label	"Client Application"
Device Custom String 5	%13
Device Custom String 5 Label	"Proxy"
Device Custom String 6	%11
Device Custom String 6 Label	"Forwarded Client IP"
Name	"Following request context headers present"
Old File Id	<code>__concatenate(%6,":",%7)</code>
Request Client Application	%5
Request Url File Name	%9
Source Address	%15
Source Translated Address	<code>__regexToken(%11)</code>

Event 411

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 3	%5
Device Custom String 3 Label	"EventDataAddresses"
Device Custom String 4	%2
Device Custom String 4 Label	"Token Type"
Device Custom String 5	%3
Device Custom String 5 Label	"Error message"
Device Custom String 6	%4
Device Custom String 6 Label	"Exception details"
Name	"Token validation failed"
Reason	<code>__regexToken(%3)</code>
Request Url	%2
Source Address	<code>__regexTokenAsAddress(%5)</code>
Source User Name	<code>__regexToken(%3)</code>

Event 412

ArcSight Field	Vendor Field
Destination Dns Domain	%4
Device Custom String 1	%2
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%1
Device Custom String 4 Label	"Instance ID"
Device Custom String 6	%3
Device Custom String 6 Label	"Token type"
Message	<code>__concatenate("A token of type ",%3," for relying party ",%4," was successfully authenticated")</code>
Name	"A token for relying party was successfully authenticated"

Event 413

ArcSight Field	Vendor Field
Destination Dns Domain	%5
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Name	"An error occurred during processing of a token request"
Old File Hash	<code>__concatenate("Caller:",%2)</code>
Old File Id	<code>__concatenate("Device identity:",%6)</code>
Old File Name	<code>__concatenate("Act as User:",%4)</code>
Source Address	%7
Source User Name	<code>__extractNTUser(%3)</code>

Event 418

ArcSight Field	Vendor Field
File Hash	%4
File Name	%2
Name	"Trust between federation server proxy and service was successfully renewed"
Old File Hash	%3
Source Address	%1

Event 420

ArcSight Field	Vendor Field
File Hash	%4
File Name	%3
Name	"Trust between federation server proxy and service was successfully established"
Source Address	%2
Source User Name	<code>__extractNTUser(%1)</code>
Surce Nt Domain	<code>__extractNTDomain(%1)</code>

Event 424

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 6	%5
Device Custom String 6 Label	"Inner exception"
File Hash	%2
File Name	%3
Name	"The federation server proxy was not able to authenticate the client certificate presented in the request"
Source Address	%4

Event 431

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 4	%5
Device Custom String 4 Label	"Token Type"
Device Custom String 5	%4
Device Custom String 5 Label	"Request Type"
Device Custom String 6	%6
Device Custom String 6 Label	"Signature Algorithm"
File Size	%2
File Type	%3
Name	"An active request was received at STS with RST"

Event 510

ArcSight Field	Vendor Field
Name	More information for the event entry with Instance ID.
Device Custom String 4	%1
Device Custom String 4 Label	Instance ID

Event 512

ArcSight Field	Vendor Field
Device Custom Date 1	<code>__concatenate(%5, " ",%6)</code>
Device Custom Date 1 Label	"Last Bad Password Attempt"
Device Custom Number 1	%4
Device Custom Number 1 Label	"Bad Password Count"
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Message	<code>__concatenate("The account for the following user ",%2," is locked out. A login attempt is being allowed due to the system configuration")</code>
Name	"The account for the following user is locked out"
Source Address	%3
Source Nt Domain	<code>__extractNTDomain(%2)</code>
Source User Name	<code>__extractNTUser(%2)</code>

Event 513

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 6	%4
Device Custom String 6 Label	"Exception details"

ArcSight Field	Vendor Field
Name	"The Artifact REST service failed to return an artifact as a result of an error during processing"
Request Url	%3
Source Address	%2

Event 515

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Event Outcome	"This account may be compromised"
Message	<code>__concatenate("The following user ",%2," account was in a locked out state and the correct password was just provided. This account may be compromised")</code>
Name	"The following user account was in a locked out state and the correct password was just provided"
Source Address	%3
Source Nt Domain	<code>__extractNTDomain(%2)</code>
Source User Name	<code>__extractNTUser(%2)</code>

Event 516

ArcSight Field	Vendor Field
Device Custom Date 1	<code>__concatenate(%5, " ",%6)</code>
Device Custom Date 1 Label	"Last Bad Password Attempt"
Device Custom Number 1	%4
Device Custom Number 1 Label	"Bad Password Count"
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Name	"The following user account has been locked out due to too many bad password attempts"

ArcSight Field	Vendor Field
Source Address	%3
Source Nt Domain	__extractNTDomain(%2)
Source User Name	__extractNTUser(%2)

Event 575

ArcSight Field	Vendor Field
Device Custom String 4	Microsoft.IdentityServer.Service.AccountPolicy.SmartLockoutProvider, Microsoft.IdentityServer.Service, Version=10.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35
Device Custom String 4 Label	Type
Device Custom String 5	SmartLockoutProvider
Device Custom String 5 Label	Module Name
Device Custom String 6	N/A
Device Custom String 6 Label	Module Identifier
Name	The following threat detection module was successfully loaded.

Event 1000

ArcSight Field	Vendor Field
Device Custom String 1	N/A
Device Custom String 1 Label	Caller
Device Custom String 4	N/A
Device Custom String 4 Label	OnBehalfOf user
Device Custom String 5	N/A
Device Custom String 5 Label	ActAs user
Device Custom String 6	N/A
Device Custom String 6 Label	Device identity
Name	An error occurred during processing of a token request . The data in this event may have the identity of the caller (application) that made this request. The data includes an Activity ID that you can cross- reference to error or warning events to help diagnose the problem that caused this error.

Event 1102

ArcSight Field	Vendor Field
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 5	%4
Device Custom String 5 Label	"Additional details"
Name	"The Federation Service authorized a request to one of the REST endpoints"
Request Url	%3
Source Address	%2

Event 1200

ArcSight Field	Vendor Field
Name	"The Federation Service issued a valid token"

Event 1201

ArcSight Field	Vendor Field
Name	"The Federation Service failed to issue a valid token"

Event 1202

ArcSight Field	Vendor Field
Name	"The Federation Service validated a new credential"

Event 1203

ArcSight Field	Vendor Field
Name	"The Federation Service failed to validate a new credential"

Event 1204

ArcSight Field	Vendor Field
Name	"A password was changed"

Event 1205

ArcSight Field	Vendor Field
Name	"A password change was attempted, but failed"

Event 1206

ArcSight Field	Vendor Field
Name	"A Sign Out request was successfully processed"

Event 1210

ArcSight Field	Vendor Field
Name	"An extranet lockout event has occurred"

Common Mappings for Events - 1200, 1201, 1202, 1203, 1204, 1205, 1206, and 1210

ArcSight Field	Vendor Field
Application Protocol	AuthProtocol
Destination Dns Domain	RelyingParty
Destination Host Name	__regexToken(Server)
Destination Service Name	__regexToken(Server)
Device Custom Date 1	LastBadAttempt
Device Custom Date 1 Label	"Last Bad Attempt"
Device Custom Number 1	__oneOfLong(CurrentBadPasswordCount)
Device Custom Number 1 Label	"Current Bad Password Count"

ArcSight Field	Vendor Field
Device Custom Number 2	<code>__oneOfLong(ConfigBadPasswordCount)</code>
Device Custom Number 2 Label	"Config Bad Password Count"
Device Custom String 1	%1
Device Custom String 1 Label	"Activity ID"
Device Custom String 5	ForwardedIpAddress
Device Custom String 5 Label	"Forwarded Ip Address"
Device Custom String 6	AuditType
Device Custom String 6 Label	"Audit Type"
Device Domain	NetworkLocation
Device External Id	DeviceId
Device Process Name	ClaimsProvider
Event Outcome	AuditResult
Old File Hash	<code>__concatenate("SSO Binding Validation Level:",SSOBindingValidationLevel)</code>
Old File Name	<code>__concatenate("Device Auth:",DeviceAuth)</code>
Old File Path	<code>__concatenate("Primary Auth:",PrimaryAuth)</code>
Old File Type	<code>__concatenate("Failure Type:",FailureType)</code>
Reason	ErrorCode
Request Client Application	UserAgentString
Source Address	IpAddress
Source Nt Domain	<code>__extractNTDomain(UserId)</code>
Source Translated Address	<code>__regexToken(ForwardedIpAddress)</code>
Source User Name	<code>__extractNTUser(UserId)</code>

Event Mappings for Microsoft Antimalware

This section has the following topics:

Windows 2012

Event 1000

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Sid	SID
File Path	Scan resources

Event 1001

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Device Custom Number 1	Scan Time Hours
Device Custom Number 2	Scan Time Minutes
Device Custom Number 3	Scan Time Seconds

Event 1002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 1	Scan ID
Scan Type Index	Scan Type Index
Device Event Category	Scan Type
Scan Parameter Index	Scan Parameter Index
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Sid	SID

Event 1005

ArcSight Field	Vendor Field
Device Custom String 1 Label	Scan ID
Device Custom String 1	Scan ID
Device Custom String 5	Error Code
Device Custom String 5 Label	Error Code
Device Event Category	Scan Type
Device Action	Scan Parameters
Source Nt Domain	Domain
Source User Name	User
Reason	Error Code

Event 1011

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Sid	SID
Device Custom String 1	Threat Name
Device Custom Number 1	Threat ID
Device Custom Number 2	Severity ID
Device Custom Number 3	Category ID
FWLink	FWLink
File Path	Path
Device Severity	Severity Name
Device Custom String 4	Category Name
Device Custom String2	Signature Version
(Concatenating both the fields)	Engine Version

Event 1013

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom Date1	Timestamp
Source Nt Domain	Domain
Source User Name	User
Sid	SID

Event 1116

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 5	Detection ID
Device Custom Date 1	Detection Time
Device Custom Number 1	Threat ID
Device Custom String 1	Threat Name
Device Custom Number 2	Severity ID
Device Custom String 3	Severity Name

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Device Custom Number 3	Category ID
Device Custom String 4	Category Name
FWLink	FWLink
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
Source Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
File Path	Path
Origin ID	Origin ID
Origin Name	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action	Action Name
Error Code	Error Code
Reason	Error Description
Post Clean Status	Post Clean Status
Additional Action ID	Additional Action ID
Additional Action String	Additional Action String
Remediation User	Remediation User
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Engine Version

Event 1117

ArcSight Field	Vendor Field
Product Version	Device Version
Detection ID	Device Custom String 5
Detection Time	Device Custom Date 1
Threat ID	Device Custom Number 1
Threat Name	Device Custom String 1
Severity ID	Device Custom Number 2
Severity Name	Device Custom String 3
Category ID	Device Custom Number 3
Category Name	Device Custom String 4
FWLink	FWLink
Status Code	Status Code
Status Description	Status Description
State	State
Source ID	Source ID
Source Name	Source Name
Source Process Name	Process Name
Source User Name	Detection User
File Path	Path
Origin ID	Origin ID
Origin Name	Origin Name
Execution ID	Execution ID
Execution Name	Execution Name
Type ID	Type ID
Old File Type	Type Name
Pre Execution Status	Pre Execution Status
Action ID	Action ID
Device Action Name	Action Name

ArcSight Field	Vendor Field
Error Code	Error Code
Reason	Error Description
Post Clean Status	Post Clean Status
Additional Action ID	Additional Action ID
Additional Action String	Additional Action String
Remediation User	Remediation User
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Engine Version

Event 1150

ArcSight Field	Vendor Field
Device Version	Product Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Signature Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Engine Version

Event 2000

ArcSight Field	Vendor Field
Device Venison	Product Version
File Id	Current Signature Version
Old File Id	Previous Signature Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Signature Type Index	Signature Type Index

ArcSight Field	Vendor Field
Device Event Category	Signature Type
Update Type Index	Update Type Index
Device Custom String 6	Update Type
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Current Engine Version
(Concatenating both Engine Version and Signature Version in Device Custom String 2	Previous Engine Version

Event 2001

ArcSight Field	Vendor Field
Device Version	Product Version
Source Nt Domain	Domain
Source User Name	User
Sid	SID
Device Custom String 5	Error Code
Reason	Error Description
File Path	FWLink

Event 2002

ArcSight Field	Vendor Field
Product Verison	Device Version
(Concatenating both Previous Engine Version and Current Version in Device Custom String 2	Previous Engine Version
(Concatenating both Previous Engine Version and Current Version in Device Custom String 2	Current Engine Version
Source Nt Domain	Domain
Source User Name	User

ArcSight Field	Vendor Field
Sid	SID
Feature Index	Feature Index
Feature Name	Feature Index Name

Event 2010

ArcSight Field	Vendor Field
Device Version	Product Version
File Id	Current Signature Version
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String 2	Current Engine Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path
Dynamic Signature Version	Dynamic Signature Version
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value

Event 2011

ArcSight Field	Vendor Field
Device Version	Product Version
File Id	Current Signature Version
Signature Type Index	Signature Type Index
Device Event Category	Signature Type
Device Custom String 2	Current Engine Version
Dynamic Signature Type Index	Dynamic Signature Type Index
Dynamic Signature Type	Dynamic Signature Type
File Path	Persistence Path

ArcSight Field	Vendor Field
Dynamic Signature Version	Dynamic Signature Version
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Type	Persistence Limit Type
Persistence Limit Value	Persistence Limit Value
Removal Reason Index	Removal Reason Index
Reason	Removal Reason Value

Event 3002

ArcSight Field	Vendor Field
Device Version	Product Version
Device Custom String 5	Error Code
Reason	Error Description

Event 5000

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5001

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5004

ArcSight Field	Vendor Field
Device Version	Product Version
File Hash	Feature Name
File Id	Feature ID
Device Custom Number 1	Configuration
Device Custom Number 1 Label	Configuration

Event 5007

ArcSight Field	Vendor Field
Device Version	Product Version
Old File Name	Old Value
File Name	New Value

Event 5010

ArcSight Field	Vendor Field
Device Version	Product Version

Event 5012

ArcSight Field	Vendor Field
Device Version	Product Version

Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user ',%2,', has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port ',%2,' has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),' has connected and has been successfully authenticated on port ',One of (%3,%4),' . Data sent and received over this link is strongly encrypted.)'

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds

ArcSight Field	Vendor Field
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user ',%2,' connected on port ',%3,' on ',%4,' at ',%5,' and disconnected on ',%6,' at ',%7,'. The user was active for ',%8,' minutes, ',%9,' seconds, ',%10,' bytes were sent and ',%11,' bytes were received. The reason for disconnecting was ',%12,. The tunnel used was ',%13,. The quarantine state was ',%14,'.)

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user ',%2,' connected on port ',%3,' has been assigned address ',%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both ('The user with ip address ',%2,' has disconnected')

Event Mappings for Microsoft DNS Server Analytics

This section has the following topics:

Event Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'DNS Server Analytic'
Device Version	'Unknown'

Event 256

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"QUERY_RECEIVED"
Old File Id	RD

Event 257

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 2	DNSSEC
Device Custom Number 2 Label	"DNSSEC"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RESPONSE_SUCCESS"
Old File Id	AA,AD
Request Context	Zone
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event 258

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RESPONSE_FAILURE"
Reason	Reason
Request Context	Zone
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event 259

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Direction	Inbound/Outbound
File Hash	AdditionalInfo
Name	"IGNORED_QUERY"
Reason	Reason
Request Context	Zone
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event 260

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags

ArcSight Field	Vendor Field
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RECURSE_QUERY_OUT"
Old File Id	RD
Old File Hash	RecursionScope,CacheScope
Request Cookies	"Recursive query"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event 261

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"

ArcSight Field	Vendor Field
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
File Hash	AdditionalInfo
Name	"RECURSE_RESPONSE_IN"
Old File Id	AA,AD
Old File Hash	RecursionScope,CacheScope
Request Cookies	"Recursive query"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event 262

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Hash	AdditionalInfo
Name	"RECURSE_QUERY_TIMEOUT"
Old File Hash	RecursionScope,CacheScope

ArcSight Field	Vendor Field
Request Cookies	"Recursive query"
Request Url	QNAME
Source Port	Port
Source Address	InterfaceIP

Event 263

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 2	Secure
Device Custom Number 2 Label	"SECURE"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"DYN_UPDATE_RECV"
Request Cookies	"Dynamic update"
Request Url	QNAME
Source Port	Port
Source Address	Source

Event 264

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 5	PolicyName
Device Custom String 5 Label	"Policy Name"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"DYN_UPDATE_RESPONSE"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Dynamic update"
Request Url	QNAME
Source Address	InterfaceIP

Event 265

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound

ArcSight Field	Vendor Field
File Size	BufferSize
Name	"IXFR_REQ_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event 266

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_REQ_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event 267

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP

ArcSight Field	Vendor Field
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_RESP_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event 268

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"IXFR_RESP_RECV"
Old File Hash	ZoneScope
Request Context	Zone

ArcSight Field	Vendor Field
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event 269

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"AXFR_REQ_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event 270

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
File Size	BufferSize
Name	"AXFR_REQ_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event 271

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
Name	"AXFR_RESP_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event 272

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Custom String 6	RCODE
Device Custom String 6 Label	"Return Code"
Device Direction	Inbound/Outbound
Name	"AXFR_RESP_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	InterfaceIP

Event 273

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_RECV"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event 274

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_OUT"
Old File Hash	ZoneScope
Request Context	Zone
Request Cookies	"Zone XFR"
Request Url	QNAME
Source Address	Source

Event 275

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_ACK_IN"
Old File Hash	ZoneScope
Request Cookies	"Zone XFR"
Source Address	Source

Event 276

ArcSight Field	Vendor Field
Destination Address	Destination
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"XFR_NOTIFY_ACK_OUT"

ArcSight Field	Vendor Field
Request Context	Zone
Request Cookies	"Zone XFR"
Source Address	InterfaceIP

Event 277

ArcSight Field	Vendor Field
Destination Address	Destination
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
Name	"DYN_UPDATE_FORWARD"
Request Context	Zone
Request Cookies	"Dynamic update"
Source Address	ForwardInterfaceIP

Event 278

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
Name	"DYN_UPDATE_RESPONSE_IN"
Request Context	Zone
Request Cookies	"Dynamic update"
Request Url	QNAME
Source Address	Source

Event 279

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"INTERNAL_LOOKUP_CNAME"
Old File Id	RD
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	Source

Event 280

ArcSight Field	Vendor Field
Destination Address	InterfaceIP
Device Custom Number 1	TCP
Device Custom Number 1 Label	"TCP"
Device Custom Number 3	Flags
Device Custom Number 3 Label	"Flags"

ArcSight Field	Vendor Field
Device Custom String 1	QTYPE
Device Custom String 1 Label	"Query Type"
Device Custom String 4	XID
Device Custom String 4 Label	"XID"
Device Direction	Inbound/Outbound
File Size	BufferSize
Name	"INTERNAL_LOOKUP_ADDITIONAL"
Old File Id	RD
Request Cookies	"Lookup"
Request Url	QNAME
Source Port	Port
Source Address	Source

Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user ',%2,', has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port ',%2,' has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),' has connected and has been successfully authenticated on port ',One of (%3,%4),' . Data sent and received over this link is strongly encrypted.)'

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds

ArcSight Field	Vendor Field
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user ',%2,' connected on port ',%3,' on ',%4,' at ',%5,' and disconnected on ',%6,' at ',%7,'. The user was active for ',%8,' minutes, ',%9,' seconds, ',%10,' bytes were sent and ',%11,' bytes were received. The reason for disconnecting was ',%12,. The tunnel used was ',%13,. The quarantine state was ',%14,'.)

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user ',%2,' connected on port ',%3,' has been assigned address ',%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both ('The user with ip address ',%2,' has disconnected')

Microsoft Exchange Mailbox Access Auditing

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Events 10100, 10101

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom String 4	Mailbox Name
Device Custom String 5	Relatively Unique Identifier
File Name	%2 (Message ID or Folder name depending upon event)
File Path	%1 (Folder path)
Name	A folder in mailbox was opened by user.
Source Host Name	%9 (Account Name)
Source Process Name	%11 (Process Name)
Source Service Name	%13 (Application ID)
Target Address	Address
Destination User ID	%5 (Accessing User (full Exchange ID))
Destination User Name	%4 (Account Name)
Destination User Privileges	One of ('Administrative rights were used', '')

Event 10102

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom Number 3	Administrative Rights
Device Custom String 4	Mailbox Name
Device Custom String 5	Identifier

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Administrative Rights
File Name	Message ID or Folder name, depending upon event
File Path	Folder path (when relevant)
Name	A message in mailbox was opened by user.
Source Host Name	Machine Name
Source Process Name	Process Name
Source Service Name	Application ID
Source User ID	Accessing User (full Exchange ID)
Source User Name	Account Name
Target Address	Address

Events 10104,

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom Number 1	Source Process ID
Device Custom String 4	Mailbox Name
Device Custom String 5	Relatively Unique Identifier
Device Custom String 6	Sent as user
File Name	%3 (Message ID or Folder name, depending upon event)
Name	User sent a message on behalf of another user.
Source Host Name	10% (Machine Name)
Source Process Name	12% (Process Name)
Source Service Name	14% (Application ID)
Destination User ID	%6 (Accessing User (full Exchange ID))
Destination User Name	%5 (Account Name)
Destination User Privileges	One of ('Administrative rights were used', '')
Destination Host Name	%11 (Address)
Destination Address	%11 (Address)

Event Mappings for Microsoft Exchange Mailbox Store

The following section lists the mappings of ArcSight data fields to the device's specific event definitions:

General Exchange Events

ArcSight ESM Field	Device-Specific Field
Device Vendor	Microsoft
Device Product	Exchange Server

Event 1016

ArcSight ESM Field	Device-Specific Field
Device Customer String3	%2 (Mail Box)
Source Nt Domain	%1
Source User Name	%1

Device Event Mapping to ArcSight Fields

The following sections lists the mappings of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

Windows 2008

General

ArcSight ESM Field	Device-Specific Field
Device Product	'Forefront Protection'
Device Vendor	'Microsoft'

Event 7000

ArcSight ESM Field	Device-Specific Field
Message	'All the antimalware engines selected in the Forefront Administration Console for scanning have been enabled for updates.'
Name	'All the antimalware engines selected in the Forefront Administration Console'

Event 7001

ArcSight ESM Field	Device-Specific Field
Message	'Not all the antimalware engines selected in the Forefront Administration Console for scanning have been enabled for updates.'
Name	'Not all the antimalware engines selected in the Forefront Administration Console'

Event 7002

ArcSight ESM Field	Device-Specific Field
Name	'All the antimalware engines enabled for updates have been updated successfully at the last attempt'

Event 7003

ArcSight ESM Field	Device-Specific Field
Name	'Not all of the antimalware engines enabled for updates have successfully updated at the last attempt'

Event 7004

ArcSight ESM Field	Device-Specific Field
Name	'Less than half of the antimalware engines enabled for updates have updated successfully at the last attempt.'

Event ID 7005

ArcSight ESM Field	Device-Specific Field
Name	'All the antimalware engines enabled for updates have updated successfully in the last five days'

Event 7006

ArcSight ESM Field	Device-Specific Field
Name	'At least one of the antimalware engines enabled for updates has not been updated in the last five days.'

Event 7007

ArcSight ESM Field	Device-Specific Field
Name	'None of the antimalware engines enabled for updates have been updated in the last five days.'

Event 7008

ArcSight ESM Field	Device-Specific Field
Name	'The antimalware engines selected for transport scanning have been initialized.'

Event ID 7010

ArcSight ESM Field	Device-Specific Field
Name	The antimalware engines selected for realtime scanning have been initialized.'

Event 7012

ArcSight ESM Field	Device-Specific Field
Name	'The transport scan job is enabled'

Event 7015

ArcSight ESM Field	Device-Specific Field
Name	'The realtime scan job is enabled.'

Event 7018

ArcSight ESM Field	Device-Specific Field
Name	'The realtime scanning processes are running normally with no issues.'

Event 7021

ArcSight ESM Field	Device-Specific Field
Name	'The transport scanning processes are running normally with no issues.'

Event 7024

ArcSight ESM Field	Device-Specific Field
Name	'The MS Exchange Transport Service is running and the Forefront Agent is registered.'
Destination Service Name	'MS Exchange Transport Service'

Event 7025

ArcSight ESM Field	Device-Specific Field
Name	'The MS Exchange Transport Service is running but the Forefront Agent is not registered'
Destination Service Name	'MS Exchange Transport Service'

Event 7026

ArcSight ESM Field	Device-Specific Field
Name	'The MS Information Store is running and the Forefront VSAPI Library is registered.'

Event 7028

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Product is within the license period.'

Event 7033

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Product is within the license period'

Event 7035

ArcSight ESM Field	Device-Specific Field
Name	'There is at least amount of disk space available.'

Event 7040

ArcSight ESM Field	Device-Specific Field
Name	'The Eventing Service (FSCEventing) is functioning.'
Destination Service Name	'FSC Eventing'

Event 7044

ArcSight ESM Field	Device-Specific Field
Name	'The Mail Pickup Service (FSEMailPickup) is functioning.'
Destination Service Name	'FSEMailPickup'

Event 7046

ArcSight ESM Field	Device-Specific Field
Name	'Content Filter is enabled and definitions have been updated in the last one hour'

Event 7048

ArcSight ESM Field	Device-Specific Field
Name	'Content Filter is enabled and the last definition update was over 12 hours ago.'

Event 7051

ArcSight ESM Field	Device-Specific Field
Name	'The Monitor Service (FSCMonitor) is functioning.'
Destination Service Name	'FSCMonitor'

Event 7064

ArcSight ESM Field	Device-Specific Field
Name	'No archived undeliverable items exist'

FSC Controller

Event 1000

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is running.'
Destination Service Name	'Forefront Protection'

Event 1001

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service has stopped.'
Destination Service Name	'Forefront Protection'

Event 1020

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is starting.'
Destination Service Name	'Forefront Protection'

Event 1021

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection service is stopping.'
Destination Service Name	'Forefront Protection'

Event 1022

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Version'
Device Version	%1 (version)
Additional data	%2 (Virus Protection Feature)

Event 1023

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Service Pack'
Additional data	%1 (ServicePack)
Message	Both ('Forefront Protection Service Pack:',%1)

Event 1024

ArcSight ESM Field	Device-Specific Field
Name	'Product ID'
Additional data	%1 (ProductID)
Message	Both ('Product ID:', %1)

Event 1025

ArcSight ESM Field	Device-Specific Field
Name	'Licensed Components'
Message	All of (Licensed Components: Component, License Type, Expiration Date)

Event 1026

ArcSight ESM Field	Device-Specific Field
Name	'Licensed Engines'
Additional data	%1 (LicensedEngines)
Message	Both ('Licensed Engines:', %1)

Event 1028

ArcSight ESM Field	Device-Specific Field
Name	'System Information'
Additional data	%1 (System Information)
Message	Both ('System Information:', %1)

Event 1037

ArcSight ESM Field	Device-Specific Field
Name	'Event Tracing session has been started.'
Device Severity	'Information'

Event 1041

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has been started'

Event 1043

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has stopped'

Event 1044

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled Scan has completed'

Event 2102

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection application is still within the license period'

Event 5167

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection Monitor detected abnormal process shutdown'
Source Process Name	%1 (process name)
Message	Both ('Microsoft Forefront Protection Monitor detected abnormal' %1,' shutdown')

Event 5183

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan exceeded the allowed scan time limit'

Event 8046

ArcSight ESM Field	Device-Specific Field
Name	'AD Mark Created'

Event 8055

ArcSight ESM Field	Device-Specific Field
Name	'Ad Mark Removed'
Message	'Failed to Delete Reg Key'

FSC Eventing

Event 1075

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Eventing Service has started.'
Destination Service Name	'Forefront Protection Eventing'

Event 1076

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Eventing Service has stopped.'
Destination Service Name	'Forefront Protection Eventing'

FSC Manual Scanner

Event 1045

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan started.'
Request Client Operation	%1 (Request Client Operation)

Event 1048

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan stopped.'
Request Client Operation	%1 (Request Client Operation)

Event 1052

ArcSight ESM Field	Device-Specific Field
Name	'On-Demand Scan has been completed.'
Request Client Operation	%1 (Request Client Operation)

FSC Scheduled Scanner

Event 2080

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan enabled.'

Event 2081

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan disabled.'

Event 3009

ArcSight ESM Field	Device-Specific Field
Name	'Scheduled scan found virus.'
Device Custom String 4	mailbox name
Message	%2 (Message)
Device Custom String 1	virus name
Device Custom String 6	incident
Additional data	%4 (scan engine)
Device Action	%5 (Device Action)
File Name	%3 (File Name)

FSC Realtime Scanner

Event 2000

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan enabled.'

Event 2001

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan disabled.'

FSC Transport Scanner

Event 2007

ArcSight ESM Field	Device-Specific Field
Name	'Transport scan enabled.'

Event 2008

ArcSight ESM Field	Device-Specific Field
Name	'Transport scan disabled.'

Event 3002

ArcSight ESM Field	Device-Specific Field
Name	'Internet scan found virus'
File Path	%1 (folder)
Message	%2 (Message)
File Name	%4 (file name)
Device Custom String 6	Incident
Device Action	%6 (Device Action or State)
Device Custom String 1	virus name
Additional data	%3 (message ID)
Additional data	%5 (scan engine)

FSC Monitor

Event 1007

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor detected Information Store process started.'
Destination Process Name	'Information Store'

Event 1008

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor detected Information Store shutdown.'
Destination Process Name	'Information Store'

Event 1013

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor is active.'

Event 1014

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection Monitor is inactive.'

FSE On Demand Nav

Event 1049

ArcSight ESM Field	Device-Specific Field
Name	'The FseOnDemandNav service is running.'
Destination Process Name	'FseOnDemandNav'

Event 1050

ArcSight ESM Field	Device-Specific Field
Name	'The FseOnDemandNav service has stopped.'
Destination Process Name	'FseOnDemandNav'

FSE Mail Pickup

Event 1029

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Mail Pickup service is running.'
Destination Service Name	'Forefront Protection Mail Pickup'

Event 1030

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection Mail Pickup service has stopped.'
Destination Service Name	'Forefront Protection Mail Pickup'

FSE IMC

Event 1002

ArcSight ESM Field	Device-Specific Field
Name	'FSEIMC service started.'
Destination Service Name	'FSEIMC'

Event 1003

ArcSight ESM Field	Device-Specific Field
Name	'FSEIMC service stopped.'
Destination Service Name	'FSEIMC'

FSE VS API

Event 5066

ArcSight ESM Field	Device-Specific Field
Name	'Realtime scan exceeded the allowed scan time limit'

FSC VSS Writer

Event 1094

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection VSS Writer Service has started.'
Destination Service Name	'Forefront Protection VSS Writer Service'

Event 1095

ArcSight ESM Field	Device-Specific Field
Name	'The Forefront Protection VSS Writer Service has stopped.'
Destination Service Name	'Forefront Protection VSS Writer Service'

Get Engine Files

Event 2011

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection did not detect any new scan engine updates'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event 2012

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection performed a successful scan engine update'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event 2017

ArcSight ESM Field	Device-Specific Field
Name	'Forefront Protection has rolled back a scan engine'
Additional data	%1 (scan engine)

Event 2034

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection is attempting a scan engine update.'
Request URL	%2 (request url)
Additional data	%1 (scan engine)

Event 2109

ArcSight ESM Field	Device-Specific Field
Name	'The VBuster scan engine is no longer supported'
Message	'Updates are no longer available for this engine, and therefore the update check for this engine has been disabled. Please review the scan engine chosen for your scan jobs and make another selection to ensure up-to-date protection'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)

Event 6012

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)
Reason	%2 (Error Code)
Message	%3 (Error Detail)

Event 6014

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update.'
Additional data	%1 (scan engine)
Request URL	%2 (request url)
Additional data	%3 (proxy settings)
Reason	%4 (Error Code)
Message	%5 (Error Detail)

Event 6019

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)
Message	%2 (Error Detail)

Event 6020

ArcSight ESM Field	Device-Specific Field
Name	'Microsoft Forefront Protection encountered an error while performing a scan engine update'
Additional data	%1 (scan engine)
Request URL	%2 (request URL)
Message	%3 (Message)

Microsoft Local Administrator Password Solution

Event 5

ArcSight Field	Vendor Field
Name	<code>__ifThenElse(%1,"Validation passed for new local admin password","Validation failed for new local admin password against local password policy")</code>
Message	<code>__ifThenElse(%1,"Validation passed for new local admin password","Validation failed for new local admin password against local password policy")</code>
Reason	%1

Event 10

ArcSight Field	Vendor Field
Name	<code>__stringConstant("Password expiration too long for computer")</code>
Message	<code>__stringConstant("Password expiration too long for computer")</code>
Device Action	<code>__stringConstant("Resetting password now")</code>
Device Custom Number 1	<code>__safeToLong(%1)</code>
Device Custom String1 Label	Excessive Days
Device Custom String2 Label	Days to change password

Event 11

ArcSight Field	Vendor Field
Name	<code>__stringConstant("It is not necessary to change password yet")</code>
Message	<code>__stringConstant("It is not necessary to change password yet")</code>
Device Custom Number 2	<code>__safeToLong(%1)</code>

Event 12

ArcSight Field	Vendor Field
Name	<code>__stringConstant("Local Administrator password has been changed")</code>
Message	<code>__stringConstant("Local Administrator password has been changed")</code>

Event 13

ArcSight Field	Vendor Field
Name	<code>__stringConstant("Local Administrator password has been reported to AD")</code>
Message	<code>__stringConstant("Local Administrator password has been reported to AD")</code>

Event 14

ArcSight Field	Vendor Field
Name	<code>__stringConstant("Finished Successfully")</code>
Message	<code>__stringConstant("Finished Successfully")</code>

Event 15

ArcSight Field	Vendor Field
Name	<code>__stringConstant("Beginning Processing")</code>
Message	<code>__stringConstant("Beginning Processing")</code>

Event 16

ArcSight Field	Vendor Field
Name	<code>__stringConstant("Admin account management not enabled")</code>
Message	<code>__stringConstant("Admin account management not enabled")</code>
Device Action	<code>__stringConstant("Exiting")</code>

Mappings for Microsoft Netlogon

General

ArcSight Field	Vendor Field
Device Product	"NETLOGON"
Device Vendor	'Microsoft'

Event 5827

ArcSight Field	Vendor Field
Device Custom String 1	%3 (Account Type)
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4 (Machine Operating System)
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5 (Machine Operating System Build)
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6 (Machine Operating System Service Pack)
Device Custom String 6 Label	"Machine Operating System Service Pack"

ArcSight Field	Vendor Field
Event Outcome	"Denied"
Source Host Name	%1 (Machine SamAccountName)
Source Nt Domain	%2 (Domain)
Name	"Netlogon service denied vulnerable Netlogon secure channel connection from a machine account"

Event 5828

ArcSight Field	Vendor Field
Destination Nt Domain	%3 (Trust Target)
Device Custom String 1	%1 (Account Type)
Device Custom String 1 Label	"Account Type"
Event Outcome	"Denied"
Source Address	%4 (Client IP Address)
Source Nt Domain	%2 (Trust Name)
Name	"Netlogon service denied a vulnerable Netlogon secure channel connection using a trust account"

Event 5829

ArcSight Field	Vendor Field
Device Custom String 1	%3
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Allowed"

ArcSight Field	Vendor Field
Source Host Name	%1
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection"

Event 5830

Device Custom String 1	%3
Device Custom String 1 Label	"Account Type"
Device Custom String 4	%4
Device Custom String 4 Label	"Machine Operating System"
Device Custom String 5	%5
Device Custom String 5 Label	"Machine Operating System Build"
Device Custom String 6	%6
Device Custom String 6 Label	"Machine Operating System Service Pack"
Event Outcome	"Allowed"
Source Host Name	%1
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection because account is allowed in group policy"

Event 5831

ArcSight Field	Vendor Field
Destination Nt Domain	%3
Device Custom String 1	%1
Device Custom String 1 Label	"Account Type"
Event Outcome	"Allowed"
Source Address	%4
Source Nt Domain	%2
Name	"Netlogon service allowed a vulnerable Netlogon secure channel connection because trust account is allowed in group policy"

Mappings for Network Policy Server

This section has the following information:

Mappings for Windows 2016, 2012, and 8

General

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Product	'NPS'

Event 13

ArcSight ESM Field	Device-Specific Field
Name	'A RADIUS message was received'
Message	Both ('A RADIUS message was received from the invalid RADIUS client IP address',%1)
Source Address	%1 (client IP address)

Event 25

ArcSight ESM Field	Device-Specific Field
Name	'The address of remote RADIUS server in remote RADIUS server group resolves to local address will be ignored'
Message	Both ('The address of remote RADIUS server ',%1,' in remote RADIUS server group ',%2,', resolves to local address ',%3,'. The address will be ignored.')
Source Address	%3 (address)
Additional data	%2 (ServerGroup)
Destination Address	%1 (address)

Event 4400

ArcSight ESM Field	Device-Specific Field
Name	'A LDAP connection with domain controller for domain is established'
Message	Both ('A LDAP connection with domain controller ',%1,' for domain ',%2,' is established')
Destination Host Name	%1 (host name)
Destination NT Domain	%2 (domain name)

Event 4402

ArcSight ESM Field	Device-Specific Field
Name	'No Domain controller available for domain'
Message	Both ('There is no domain controller available for domain ',%1)
Destination NT Domain	%1 (domain name)

Event 4405

ArcSight ESM Field	Device-Specific Field
Name	'NPS cannot log accounting information in the primary data store'
Message	Both ('NPS cannot log accounting information in the primary data store (',%1,'). Due to this logging failure, NPS will discard all connection requests. Error information: ',%2)'
Destination NT Domain	%1 (domain name)
Reason	%2 (reason code)

Mappings for Windows 2008 R2

General

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Product	'NPS'

Event 13

ArcSight ESM Field	Device-Specific Field
Name	'A RADIUS message was received'
Source Address	%1 (client IP address)
Message	Both ('A RADIUS message was received from the invalid RADIUS client IP address ','%1')

Event 4400

ArcSight ESM Field	Device-Specific Field
Name	'A LDAP connection with domain controller for domain is established'
Destination Host Name	%1 (host name)
Destination NT Domain	%2 (domain name)
Message	Both (A LDAP connection with domain controller ',%1,' for domain ',%2,' is established)

Event 4402

ArcSight ESM Field	Device-Specific Field
Name	'No Domain controller available for domain'
Message	Both ('There is no domain controller available for domain' ',%1)
Destination NT Domain	%1 (domain name)

Event 4405

ArcSight ESM Field	Device-Specific Field
Name	'NPS cannot log accounting information in the primary data store'
Destination Host Name	%1 (host name)
Reason	%2 (reason code)
Message	Both ('NPS cannot log accounting information in the primary data store (',%1,'). Due to this logging failure, NPS will discard all connection requests. Error information: ',%2)')

Mappings for Remote Access Events

This section has the following sections:

Mappings for Windows 2022, 2016, 2012, and 2012 R2

General

ArcSight Field	Vendor Field
Device Product	'Microsoft Windows'
Device Vendor	'Microsoft'

Event 600

ArcSight Field	Vendor Field
Name	An operation is pending.

608

ArcSight Field	Vendor Field
Name	A device was specified that does not exist.

Event 635

ArcSight Field	Vendor Field
Name	There was an unknown error.

Event 653

ArcSight Field	Vendor Field
Name	A macro required by the modem was not found.

Event 654

ArcSight Field	Vendor Field
Name	A command or response refers to an undefined macro.

Event 670

ArcSight Field	Vendor Field
Name	The system was unable to read the section name.

Event 671

ArcSight Field	Vendor Field
Name	The system was unable to read the device type.

Event 672

ArcSight Field	Vendor Field
Name	The system was unable to read the device name.Event

Event 700

ArcSight Field	Vendor Field
Name	The expanded command is too long.

Event 827

ArcSight Field	Vendor Field
Name	The VPN connection cannot be completed because service is not running.

Event 848

ArcSight Field	Vendor Field
Name	VPN connection attempt failed due to internal error.

Event 20019

ArcSight Field	Vendor Field
Name	Remote Access Server Security Failure.

Event 20084

ArcSight Field	Vendor Field
Name	Remote Access Server will stop using IP Address.
Source Address	%1

Event 20085

ArcSight Field	Vendor Field
Name	Remote Access Server was unable to renew the lease for IP Address.
Source Address	%1

Event 20088

ArcSight Field	Vendor Field
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')
Name	'Remote Access Server acquired IP Address'

Event 20106

ArcSight Field	Vendor Field
Application Protocol	One of (%2, %3)
Device Custom String 5	Routing Domain ID
Device Outbound Interface	One of (%1, %2)
Message	One of ('Unable to add the interface ',%1,' with the Router Manager for the ',%2,' protocol. The following error occurred: ',%3), ('Unable to add the interface ',%2,' with the Router Mnager for the ',%3,' protocol. The following error occurred: ',%4))
Name	'Unable to add interface'

Event 20169

ArcSight Field	Vendor Field
Message	Both ('The Automatic Private IP Address ',%1,' will be assigned to dial-in clients. Clients may be unable to access resources on the network.')
Name	'Unable to contact a DHCP server'
Source Address	%2 (Address)

Event 20184

ArcSight Field	Vendor Field
Device Custom String 5	Routing Domain ID
Device Inbound Interface	One of (%1, %2)
Message	Both ("Interface ",One of(%1,%2)," is unreachable because it is not currently connected to the network.")
Name	'Interface is unreachable'

Event 20249

ArcSight Field	Vendor Field
Application Protocol	%3 (Protocol)
Device Custom String 4	Correlation-ID
Message	Both ('The user ',%2,' has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')
Name	'Failed to authenticate'
Source NT Domain	%2 (Domain of Connected User)
Source Port	%3 (Port)
Source User Name	%2 (Connected User)

Event 20252

ArcSight Field	Vendor Field
Application Protocol	%2 (Protocol)
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Message	Both ('The user connected to port ',%2,' has been disconnected because the authentication process did not complete within the required amount of time.')
Name	'Authentication process did not complete'
Source Port	%2 (Port)

Event 20255

ArcSight Field	Vendor Field
Application Protocol	%2 (Protocol)
Device Custom String 4	Correlation-ID
Message	%4 (Message Text)
Name	'Connection was prevented'
Source NT Domain	%3 (Domain of Connected User)
Source Port	%2 (Port)
Source User Name	%3 (Connected User)

Event 20258

ArcSight Field	Vendor Field
Application Protocol	%4 (Protocol)
Device Custom String 4	Correlation-ID
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')
Name	'Account does not have Remote Access privilege'
Source NT Domain	%3 (Domain of Connected User)
Source Port	%4 (Port)
Source User Name	%3 (Connected User)

Event 20266

ArcSight Field	Vendor Field
Application Protocol	One of (%3, %4)
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Device Custom String 5	Routing Domain ID
Message	Both ('The user ',One of (%2, %3),' has connected and has been successfully authenticated on port ',One of (%3, %4),'. Data sent and received over this link is strongly encrypted.)
Name	'Successfully authenticated'
Source NT Domain	One of (%2, %3)
Source Port	One of (%3, %4)
Source User Name	One of (%2, %3)

20271

ArcSight Field	Vendor Field
Device Custom String 4	Correlation-ID
Message	Both ('The user ',%2,' connected from ',%3,' but failed an authentication attempt due to the following reason: ',%4')
Name	'Failed an authentication attempt'
Reason	%5 (Reason)
Source Address	%3 (Address)
Source NT Domain	%2 (Domain of Connected User)
Source User Name	%2 (Connected User)

Event 20272

ArcSight Field	Vendor Field
Additional data	One of (%14, %15)
Additional data	One of (%12, %13)
Additional data	One of (%13, %14)
Application Protocol	One of (%3, %4)
Bytes In	One of (%11, %12)
Bytes Out	One of (%10, %11)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

ArcSight Field	Vendor Field
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
End Time	Both (One of(%6,%7)," ",One of(7,%8))
Message	Both (The user ',One of (%2, %3),' connected on port ',One of (%3, %4),' on ',One of (%4, %5),' at ',One of (%5, %6),' and disconnected on ',One of (%6, %7),' at ',One of (%7, %8,'. The user was active for ',One of (%8, %9),' minutes ', One of (%9, %10),' seconds. ', One of (%10, %11),' bytes were received. The reason for disconnecting was ', One of (%12, %13),'. The tunnel used was ', One of (%13, %14),'. The quarantine state was ', One of (%14, %15),'.')
Name	'User connected and disconnected'
Source NT Domain	One of (%2, %3)
Source Port	One of (%3, %4)
Source User Name	One of (%2, %3)
Start Time	Both (One of (%4, %5),' ',One of (%5, %6)))

Event 20274

ArcSight Field	Vendor Field
Application Protocol	One of (%3, %4)
Destination Address	One of (%4, %5)
Device Custom String 4	correlation-ID
Device Custom String 5	Routing Domain ID
Message	Both ('The user ',One of (%2, %3),' connected on port ',One of (%3, %4),' has been assigned address ',One of (%4, %5))
Name	'User connected and has been assigned address'
Source NT Domain	One of (%2, %3)
Source Port	One of %3, %4)
Source User Name	One of (%2, %3)

Event 20275

ArcSight Field	Vendor Field
Device Custom String 4	Correlation-ID
Device Custom String 5	Routing Domain ID
Message	Both ('The user with ip address ',One of (%2, %3),' has disconnected')
Name	'User disconnected'
Source Address	One of (%2, %3)

Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user ',%2,', has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port ',%2,', has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),', has connected and has been successfully authenticated on port ',One of (%3,%4),'. Data sent and received over this link is strongly encrypted.)'

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)

ArcSight Field	Vendor Field
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user ',%2,' connected on port ',%3,' on ',%4,' at ',%5,' and disconnected on ',%6,' at ',%7,'. The user was active for ',%8,' minutes, ',%9,' seconds, ',%10,' bytes were sent and ',%11,' bytes were received. The reason for disconnecting was ',%12,. The tunnel used was ',%13,. The quarantine state was ',%14,'.)

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user ',%2,' connected on port ',%3,' has been assigned address ',%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both ('The user with ip address ',%2,' has disconnected')

Windows 2016, 2012, 8, and 10

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'
Device Custom String 4	Reason or Error Code

Event 7000

ArcSight Field	Vendor Field
Name	'Service failed to start'
Message	'The 'param1' service failed to start due to error: 'param2''
Destination Service Name	param1
Device Custom String 4	param2 (Reason or Error Code)
Reason	param2

Event 7001

ArcSight Field	Vendor Field
Name	'A service depends on other service which failed to start'
Message	'The 'param1' service depends on the 'param2' service which failed to start because of error: 'param3''
Destination Service Name	param1
Source Service Name	param2
Device Custom String 4	param3 (Reason or Error Code)
Reason	param3

Event 7002

ArcSight Field	Vendor Field
Name	'The 'param1' service depends on the 'param2' group and no member of this group started'
Destination Service Name	param1

Event 7003

ArcSight Field	Vendor Field
Name	'A service depends on a nonexistent service'
Message	'The 'param1' service depends on a nonexistent service 'param2''
Destination Service Name	param1
Source Service Name	param2

Event 7005

ArcSight Field	Vendor Field
Name	'The 'param1' call failed with error 'param2'
Device Custom String 4	Param2 (Reason or Error Code)

Event 7006

ArcSight Field	Vendor Field
Name	'The 'param1' call failed for 'param2' with the following error 'param3''
Device Action	param2 (action)
Device Custom String 4	Param3 (Reason or Error Code)

Event 7007

ArcSight Field	Vendor Field
Name	'The system reverted to its last known good configuration'
Message	'The system is restarting'

Event 7008

ArcSight Field	Vendor Field
Name	'No backslash is in the account name'

Event 7009

ArcSight Field	Vendor Field
Name	'Timeout waiting for the service to connect'
Message	'Timeout 'param1' waiting for the 'param2' service to connect'
Destination Service Name	param2

Event 7010

ArcSight Field	Vendor Field
Name	'Timeout waiting for ReadFile'

Event 7011

ArcSight Field	Vendor Field
Name	'Timeout waiting for a transaction response from the 'param2' service'
Destination Service Name	param2

Event 7012

ArcSight Field	Vendor Field
Name	'Message returned in transaction has incorrect size'

Event 7015

ArcSight Field	Vendor Field
Name	'Boot-start or system-start driver 'param1' must not depend on a service'

Event 7016

ArcSight Field	Vendor Field
Name	'The 'param1' service has reported an invalid current state'
Destination Service Name	param1

Event 7017

ArcSight Field	Vendor Field
Name	'Detected circular dependencies demand starting 'param1''
Destination Service Name	param1

Event 7018

ArcSight Field	Vendor Field
Name	'Detected circular dependencies auto-starting services'

Event 7019

ArcSight Field	Vendor Field
Name	'Circular dependency: The 'param1' service depends on a service in a group which starts later.'
Destination Service Name	param1

Event 7020

ArcSight Field	Vendor Field
Name	'Circular dependency: The 'param1' service depends on a group which starts later'
Destination Service Name	param1

Event 7021

ArcSight Field	Vendor Field
Name	'About to revert to the last known good configuration because the 'param1' service failed to start'
Destination Service Name	param1

Event 7022

ArcSight Field	Vendor Field
Name	'The 'param1' service hung on starting'
Destination Service Name	param1

Event 7023

ArcSight Field	Vendor Field
Name	'A service terminated with error.'
Message	The 'param1' service terminated with the following error 'param2'
Destination Service Name	param1
Reason	param2
Device Custom String 4	param2 (Reason or Error Code)

Event 7024

ArcSight Field	Vendor Field
Name	'The 'param1' service terminated with the following service-specific error'
Destination Service Name	param1
Device Custom String 4	param2 (Reason or Error Code)

Event 7025

ArcSight Field	Vendor Field
Name	'At least one service or driver failed during system startup'
Message	'Use Event Viewer to examine the event log for details'

Event 7026

ArcSight Field	Vendor Field
Name	'The boot-start or system-start driver(s) did not load'
Message	'The following boot-start or system-start driver(s) did not load: 'param1''
Device Process Name	param1

Event 7027

ArcSight Field	Vendor Field
Name	'Windows could not be started as configured'
Message	'A previous working configuration was used instead'

Event 7028

ArcSight Field	Vendor Field
Name	'The 'param1' Registry key denied access to SYSTEM account programs'
Message	'The Service Control Manager took ownership of the Registry key'
File Name	param1

Event 7030

ArcSight Field	Vendor Field
Name	'The 'param1' service is marked as an interactive service'
Destination Service Name	param1
Message	'The system is configured to not allow interactive services. This service may not function properly.'

Event 7031

ArcSight Field	Vendor Field
Name	Both ('The ',param1,' service terminated unexpectedly')
Destination Service Name	param1 (service name)

ArcSight Field	Vendor Field
Message	Both ('The ',param1,' service terminated unexpectedly. It has done this ',param2,' time(s). The following corrective action will be taken in ',param3,' milliseconds: ',param5)
Device Action	param5 (action)

Event 7032

ArcSight Field	Vendor Field
Name	'The Service Control Manager tried to take a corrective action 'param1' after the unexpected termination of the 'param2' service'
Device Action	param1
Message	'This action failed with error'
Destination Service Name	param2
Device Custom String 4	param3 (Reason or Error Code)

Event 7033

ArcSight Field	Vendor Field
Name	'The Service Control Manager did not initialize successfully'
Message	'The security configuration server (scsdrv.dll) failed to initialize with error 'param1'. The system is restarting.'
Device Custom String 4	param1 (Reason or Error Code)

Event 7034

ArcSight Field	Vendor Field
Name	'A service terminated unexpectedly'
Message	'It has done this 'param2' times'
Destination Service Name	param1
Device Custom Number 3	param2 (Count)

Event 7035

ArcSight Field	Vendor Field
Name	'The 'param1' service was successfully sent a 'param2' control'
Destination Service Name	param2

Event 7036

ArcSight Field	Vendor Field
Name	'Service entered the 'param2" state'
Message	The 'param1' service entered the 'param2' state.'
Destination Service Name	param1
Device Action	param2

Event 7037

ArcSight Field	Vendor Field
Name	'The Service Control Manager encountered an error undoing a configuration change to the 'param1' service'
Message	'The service's 'param2' is currently in an unpredictable state. If you do not correct this configuration, you may not be able to restart the 'param1' service or may encounter other errors. To ensure that the service is configured properly, use the Services snap-in in Microsoft Management Console (MMC)'
Destination Service Name	param1

Event 7038

ArcSight Field	Vendor Field
Name	'A service was unable to log on with the currently configured password'
Message	'The 'param1' service was unable to log on as 'param2' with the currently configured password due to the following error: 'param3'. To ensure that the service is configured properly, use the Services snap-in in Microsoft Management Console (MMC)'
Destination Service Name	param1

ArcSight Field	Vendor Field
Destination User Name	param2
Device Custom String 4	param3 (Reason or Error Code)
Reason	param3

Event 7039

ArcSight Field	Vendor Field
Name	'A service process other than the one launched by the Service Control Manager connected when starting the 'param1' service'
Destination Service Name	param1
Message	'The Service Control Manager launched process 'param2' and process 'param3' connected instead. Note that if this service is configured to start under a debugger, this behavior is expected.'

Event 7040

ArcSight Field	Vendor Field
Name	'Start type of 'param1' service was changed from 'param2' to 'param3''
Message	'Start type of 'param1' service was changed from 'param2' to 'param3''
Destination Service Name	param1
Device Action	param3

Event 7041

ArcSight Field	Vendor Field
Name	'A service was unable to log on with the currently configured password.'
Destination Service Name	param1
Destination User Name	param2
Device Custom String 4	'Logon failure: the user has not been granted the requested logon type at this computer'
Message	'The 'param1' service was unable to log on as 'param2' with the currently configured password due to error. This service account does not have the necessary user right \Log on as a service'''
Reason	'Logon failure: the user has not been granted the requested logon type at this computer'

Event 7042

ArcSight Field	Vendor Field
Name	'A service was successfully sent a control'
Destination Service Name	param1 (service name)
Device Custom String 4	Reason or Error Code
Message	'The 'param1' service was successfully sent a 'param2' control. The reason specified was 'param3' ['param4'] Comment: 'param5'
Reason	Both ('param3,' 'param4')

Event 7043

ArcSight Field	Vendor Field
Name	'The 'param1' service did not shutdown properly after receiving a preshutdown control'
Destination Service Name	param1

Event 7045

ArcSight Field	Vendor Field
Name	'A service was installed in the system'
Destination Service Name	ServiceName
File Path	ImagePath
Device Custom String 5	StartType
Device Custom String 6	AccountName

Microsoft SQL Server Audit Application Event Log Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'SQL Server'
Destination User Name	""

Event 615

ArcSight Field	Vendor Field
Name	'Could not find database'
Message	'Could not find database ID ',%1,' , name ',%2,'

Event 849

ArcSight Field	Vendor Field
Name	'Using locked pages for buffer pool'
Message	'Using locked pages for buffer pool'

Event 852

ArcSight Field	Vendor Field
Name	'Using conventional memory in the memory manager'
Message	'Using conventional memory in the memory manager'

Event 919

ArcSight Field	Vendor Field
Name	'User is changing database script level'
Message	'User ',%1,' is changing database script level entry ',%2,' to a value of ',%3

ArcSight Field	Vendor Field
Source User Name	%1
Device Custom Number 1	%2 (Level entry)
Device Custom Number 2	%3 (Changed value)

Event 958

ArcSight Field	Vendor Field
Name	'The resource database build version'
Message	'The resource database build version is ',%1
Device Custom String 4	%1 (Database build version)

Event 1486

ArcSight Field	Vendor Field
Name	'Database Mirroring Transport is disabled in the endpoint configuration'
Message	'Database Mirroring Transport is disabled in the endpoint configuration'

Event 1814

ArcSight Field	Vendor Field
Name	'Could not create tempdb'
Message	'Could not create tempdb. You may not have enough disk space available.'

Event 1945

ArcSight Field	Vendor Field
Name	'Warning! The maximum key length'
Message	One of ('Warning! The maximum key length for a ",%1," index is ",%2," bytes. The index ",%3," has maximum length of ",%4," bytes. For some combination of large values, the insert/update operation will fail."), ('Warning! The maximum key length is ",%1," bytes. The index ",%2," has maximum length of ",%3," bytes. For some combination of large values, the insert/update operation will fail.')
Device Custom String 1	Both (One of (%2, %1), 'bytes') (Maximum key length)

ArcSight Field	Vendor Field
Device Custom String 2	One of (%3,%2) (Index)
Device Custom String 3	Both (One of (%4, %3), 'bytes') (Maximum index)
Device Custom String 4	%1 (Index Type)

Event 2007

ArcSight Field	Vendor Field
Name	'The module depends on the missing object'
Message	'The module ',%1,' depends on the missing object ',%2,'. The module will still be created; however, it cannot run successfully until the object exists.'
Device Custom String 1	%1 (Module)
Device Custom String 2	%2 (Missing object)

Event 2812

ArcSight Field	Vendor Field
Name	'Could not find stored procedure'
Message	'Could not find stored procedure ',%1
Device Custom String 2	%1 (Stored procedure)

Event 3014

ArcSight Field	Vendor Field
Name	%1 successfully processed
Message	%1 successfully processed %2 pages in %3.%4 seconds
Device Custom Number 1	%2 (Pages processed)
Device Custom String 6	%3.%4 (Processing Time)

Event 3402

ArcSight Field	Vendor Field
Name	%1 successfully processed
Message	%1 successfully processed %2 pages in %3.%4 seconds

ArcSight Field	Vendor Field
Device Custom Number 1	%2 (Pages processed)
Device Custom String 6	%3.%4 (Processing Time)

Event 3406

ArcSight Field	Vendor Field
Name	'Transactions rolled forward in database'
Message	%1' transactions rolled forward in database ',%2, (',%3,')
Device Custom Number 2	%1 (Transactions quantity)
Device Custom String 1	%2 (Database name)
Device Custom Number 1	%3 (Database ID)

Event 3407

ArcSight Field	Vendor Field
Name	'Transactions rolled back in database'
Message	%1,' transactions rolled back in database ',%2,' (',%3,')'
Device Custom Number 2	%1 (Transactions quantity)
Device Custom String 1	%2 (Database name)
Device Custom Number 1	%3 (Database ID)

Event 3408

ArcSight Field	Vendor Field
Name	'Recovery is complete'
Message	'Recovery is complete. This is an informational message only. No user action is required.'

Event 3412

ArcSight Field	Vendor Field
Name	The server instance was started using minimal configuration startup option (-f)
Message	Warning: The server instance was started using minimal configuration startup option (-f). Starting an instance of SQL Server with minimal configuration places the server in single-user mode automatically. After the server has been started with minimal configuration, you should change the appropriate server option value or values, stop, and then restart the server.

Event 3421

ArcSight Field	Vendor Field
Name	'Recovery completed for database'
Message	'Recovery completed for database ',%1,' (database ID ',%2,'), in ',%3,' second(s) (analysis ',%4,' ms, redo ',%5,' ms, undo ',%6,' ms.)'
Device Custom String 1	%1 (Database name)
Device Custom String 2	%4 ms (Analysis time)
Device Custom String 3	%5 ms (Redo time)
Device Custom String 4	%6 ms (Undo time)
Device Custom String 5	%3 s (Completed recovery time)
Device Custom String 6	%2 (Database ID)

Event 3454

ArcSight Field	Vendor Field
Name	'Recovery is writing a checkpoint in database.'
Message	'Recovery is writing a checkpoint in database ',%1,' (',%2,')'
Device Custom String 1	%1 (Database name)
Device Custom Number 1	%2 (Database ID)

Event 4356

ArcSight Field	Vendor Field
Name	Restore is complete on database
Message	Restore is complete on database '%1'. The database is now available.
Device Custom String 1	%1 (Database name)

Event 5084

ArcSight Field	Vendor Field
Name	'Setting database option'
Message	'Setting database option ',%1,' to ',%2,' for database ',%3,'
Device Custom String 1	%3 (Database name)
Device Custom String 2	%1 (Old option)
Device Custom String 3	%2 (New option)

Event 5579

ArcSight Field	Vendor Field
Name	'File system access'
Message	'#FILESTREAM: effective level =',%1,', configured level = ',%2,', file system access share name = ',%3,'

Event 5701

ArcSight Field	Vendor Field
Name	'Changed database context'
Message	'Changed database context to ',%1
Device Custom String 1	%1 (Database name)
Device Action	'Changed'

Event 5703

ArcSight Field	Vendor Field
Name	'Changed language setting'
Message	'Changed language setting to ',%1
Device Custom String 1	%1 (Language setting)
Device Action	'Changed'

Event 6253

ArcSight Field	Vendor Field
Name	'Common language runtime (CLR) functionality initialized using CLR'
Message	'Common language runtime (CLR) functionality initialized using CLR version ',%1,' from ',%2
File Path	%2
Device Custom String 4	%1 (File version)

Event 6527

ArcSight Field	Vendor Field
Name	'.NET Framework runtime has been stopped'
Message	'.NET Framework runtime has been stopped'

Event 8128

ArcSight Field	Vendor Field
Name	'Execute extended stored procedure.'
Message	'Using ',%1,' version ',%2,' to execute extended stored procedure ',%3,'. This is an informational message only; no user action is required.'
File Name	%1
Device Custom String 3	%2 (File version)
Device Custom String 4	%3 (Extended stored procedure)

Event 9013

ArcSight Field	Vendor Field
Name	'Tail of the log for database is being rewritten'
Message	'Tail of the log for database ',%1,' is being rewritten to match the new sector size of ',%2,' bytes. ',%3,' bytes at offset ',%4,' in file ',%5,' will be written'

Event 9666

ArcSight Field	Vendor Field
Name	'Service endpoint is in disabled or stopped state'
Message	'The ',%1,' endpoint is in disabled or stopped state'
Destination Service Name	%1

Event 9688

ArcSight Field	Vendor Field
Name	'Service Broker manager has started'
Message	'Service Broker manager has started'

Event 9689

ArcSight Field	Vendor Field
Name	'Service Broker manager has shut down'
Message	'Service Broker manager has shut down'

Event 10981

ArcSight Field	Vendor Field
Name	'Resource governor reconfiguration succeeded'
Message	'Resource governor reconfiguration succeeded'

Event 12288

ArcSight Field	Vendor Field
Name	'Package started'
File Name	%1

Event 12291

ArcSight Field	Vendor Field
Name	'Package failed'
File Name	%1

Event 15268

ArcSight Field	Vendor Field
Name	'Authentication mode'
Message	'Authentication mode is ',%1
Device Custom String 3	%1 (Authentication mode)

Event 15457

ArcSight Field	Vendor Field
Name	'Configuration option changed'
Message	'Configuration option ',%1,' changed from ',%2,' to ',%3,'. Run the RECONFIGURE statement to install'
Device Custom String 3	%1 (Configuration option)
Device Custom Number 1	%2 (Old value)
Device Custom Number 2	%3 (New value)

Event 15477

ArcSight Field	Vendor Field
Name	'Caution: Changing any part of an object name could break scripts and stored procedures'
Message	'Caution: Changing any part of an object name could break scripts and stored procedures'

Event 17069

ArcSight Field	Vendor Field
Name	'Microsoft SQL Server 2012 (SP1)'
Message	%1

Event 17101

ArcSight Field	Vendor Field
Name	'Microsoft Corporation'
Message	'Microsoft Corporation'

Event 17103

ArcSight Field	Vendor Field
Name	'All rights reserved'
Message	'All rights reserved'

Event 17104

ArcSight Field	Vendor Field
Name	'Server process ID"
Message	'Server process ID is ',%1
Destination Process ID	%1

Event 17107

ArcSight Field	Vendor Field
Name	'Perfmon counters for resource governor pools and groups failed to initialize and are disabled'
Message	'Perfmon counters for resource governor pools and groups failed to initialize and are disabled'

Event 17108

ArcSight Field	Vendor Field
Name	'Password policy update was successful'
Message	'Password policy update was successful'
Device Action	'Update'

Event 17110

ArcSight Field	Vendor Field
Name	'Registry startup parameters'
Message	'Registry startup parameters ',%1
Device Custom String 1	%1 (Parameters)

Event 17111

ArcSight Field	Vendor Field
Name	'Logging SQL Server messages'
Message	'Logging SQL Server messages in file ',%1
File Name	%1

Event 17115

ArcSight Field	Vendor Field
Name	'Command Line Startup'
Message	'Command Line Startup Parameters: ',%1

ArcSight Field	Vendor Field
Device Action	'Startup'
Device Custom String 1	%1 (Parameters)

Event 17125

ArcSight Field	Vendor Field
Name	'Using dynamic lock allocation'
Message	'Using dynamic lock allocation. Initial allocation of ',%1,' Lock blocks and ',%2,' Lock Owner blocks per node'
Device Custom Number 1	%1 (Lock blocks)
Device Custom Number 2	%2 (Lock owner blocks)

Event 17126

ArcSight Field	Vendor Field
Name	'SQL Server is now ready for client connections'
Message	'SQL Server is now ready for client connections'

Event 17136

ArcSight Field	Vendor Field
Name	'Clearing tempdb database'
Message	'Clearing tempdb database'

Event 17137

ArcSight Field	Vendor Field
Name	'Starting up database'
Message	'Starting up database ',%1
Device Custom String 1	%1 (Database name)

Event 17147

ArcSight Field	Vendor Field
Name	'SQL Server is terminating because of a system shutdown'
Message	'SQL Server is terminating because of a system shutdown. This is an informational message only. No user action is required.'

Event 17148

ArcSight Field	Vendor Field
Name	'SQL Server is terminating'
Message	'SQL Server is terminating in response to a 'stop' request from Service Control Manager'

Event 17152

ArcSight Field	Vendor Field
Name	'Node configuration'
Message	'Node configuration: node ',%1,' CPU mask: ',%2,' ',%3,' Active CPU mask: ',%4,' ',%5,'. This message provides a description of the NUMA configuration for this computer. This is an informational message only. No user action is required.'
Device Custom String 2	%1 (Node)
Device Custom String 3	%2 (CPU mask)
Device Custom String 4	%4 (Active CPU mask)
Device Custom String 5	%3 (Flag CPU mask)
Device Custom String 6	%5 (Flag Active CPU mask)

Event 17162

ArcSight Field	Vendor Field
Name	'SQL Server is starting'
Message	'SQL Server is starting at normal priority base (=7)'

Event 17164

ArcSight Field	Vendor Field
Name	'SQL Server detected sockets'
Message	'SQL Server detected ',%1,' sockets with ',%2,' cores per socket and ',%3,' logical processors per socket, ',%4,' total logical processors; using ',%5,' logical processors based on SQL Server licensing. This is an informational message; no user action is required.'
Device Custom Number 1	%1 (Detected sockets)
Device Custom Number 2	%2 (Cores per socket)
Device Custom Number 3	%3 (Processors per socket)
Device Custom String 3	%4 (Total processors)
Device Custom String 4	%5 (Using processors)

Event 17176

ArcSight Field	Vendor Field
Name	'This instance of SQL Server last reported using a process ID'
Message	'This instance of SQL Server last reported using a process ID of ',%1,' at ',%2,' (local) ',%3,' (UTC). This is an informational message only; no user action is required.'
Destination Process ID	%1
Device Custom Date 1	%2, 'MM/dd/yyyy hh:mm:ss aa' (Last Report Time (local))
Device Custom Date 2	%3 'MM/dd/yyyy hh:mm:ss aa' (Last Report Time (UTC))

Event 17177

ArcSight Field	Vendor Field
Name	'This instance of SQL Server has been using a process ID"
Message	'This instance of SQL Server has been using a process ID of ',%1,' since ',%2,' (local) ',%3,' (UTC). '

Event 17199

ArcSight Field	Vendor Field
Name	'Restart SQL Server using the trace flag'
Message	'Dedicated administrator connection support was not started because it is disabled on this edition of SQL Server. If you want to use a dedicated administrator connection, restart SQL Server using the trace flag ',%1,'. This is an informational message only. No user action is required.'
Device Custom Number 1	%1 (Trace flag)

Event 17201

ArcSight Field	Vendor Field
Name	'Dedicated admin connection support was established'
Message	'Dedicated admin connection support was established for listening locally on port ',%1
Destination Port	%1

Event 17311

ArcSight Field	Vendor Field
Name	SQL Server is terminating because of fatal exception
Message	SQL Server is terminating because of fatal exception %1. This error may be caused by an unhandled Win32 or C++ exception, or by an access violation encountered during exception handling. Check the SQL error log for any related stack dumps or messages. This exception forces SQL Server to shutdown. To recover from this error, restart the server (unless SQLAgent is configured to auto restart).
Device Custom String 6	%1 (Exception)
Reason	This error may be caused by an unhandled Win32 or C++ exception, or by an access violation encountered during exception handling.

Event 17144

ArcSight Field	Vendor Field
Name	SQL Server is not allowing new connections
Message	SQL Server is not allowing new connections because the Service Control Manager requested a pause. To resume the service, use SQL Computer Manager or the Services application in Control Panel.
Destination Port	The Service Control Manager requested a pause.

Event 17106

ArcSight Field	Vendor Field
Name	Common Criteria compliance mode is enabled
Message	Common Criteria compliance mode is enabled. This is an informational message only. no user action is required.

Event 17150

ArcSight Field	Vendor Field
Name	Lock partitioning is enabled
Message	Lock partitioning is enabled. This is an informational message only. No user action is required.

Event 17142

ArcSight Field	Vendor Field
Name	SQL Server service has been paused
Message	SQL Server service has been paused. No new connections will be allowed. To resume the service, use SQL Computer Manager or the Services application in Control Panel.

Event 17167

ArcSight Field	Vendor Field
Name	Support for distributed transactions was not enabled for this instance of the Database Engine
Message	Support for distributed transactions was not enabled for this instance of the Database Engine because it was started using the minimal configuration option. This is an informational message only. No user action is required.
Reason	It was started using the minimal configuration option.

Event 17836

ArcSight Field	Vendor Field
Name	Length specified in network packet payload did not match number of bytes read.
Message	Length specified in network packet payload did not match number of bytes read; the connection has been closed. Please contact the vendor of the client library. %1
Source Address	%1

Event 17806

ArcSight Field	Vendor Field
Name	SSPI handshake failed
Message	SSPI handshake failed with error code %1, state %2 while establishing a connection with integrated security; the connection has been closed. Reason: %3 %4 %5
Source Address	%5
Device Custom String 6	%1 (Error code)
Device Custom String 2	%2(State)
Reason	%3

Event 17550

ArcSight Field	Vendor Field
Name	'DBCC TRACEON, server process'
Message	'DBCC TRACEON ',%1,' server process ID (SPID) ',%2,'. This is an informational message only; no user action is required.'
Destination Process Name	'DBCC TRACEON' %1
Destination Process ID	%2

Event 17551

ArcSight Field	Vendor Field
Name	'DBCC TRACEOFF, server process'
Message	'DBCC TRACEOFF ',%1,' , server process ID (SPID) ',%2,'. This is an informational message only; no user action is required.'
Destination Process Name	'DBCC TRACEON' ,%1
Destination Process ID	%2

Event 17561

ArcSight Field	Vendor Field
Name	'index restored'
Message	'index restored for ',%2,'.',%3
Device Custom String 1	%2 (Report server database)
Device Custom String 3	%3 (Object name)

Event 17656

ArcSight Field	Vendor Field
Name	'Warning'
Message	'Warning *****'

Event 17658

ArcSight Field	Vendor Field
Name	'SQL Server started in single-user mode'
Message	'SQL Server started in single-user mode. This is an informational message only. No user action is required.'

Event 17663

ArcSight Field	Vendor Field
Name	'Server name'
Message	'Server name is ',%1
Destination Host Name	%1

Event 17573

ArcSight Field	Vendor Field
Name	DBCC CHECKDB Last Run time without errors
Message	CHECKDB for database '%1' finished without errors on %2 (local time). This is an informational message only; no user action is required.
Device Custom String 1	%1 (Database name)
Device Custom Date 1	%2 (DBCC CHECKDB Last Run time (local time))

Event 17811

ArcSight Field	Vendor Field
Name	'The maximum number of dedicated administrator connections for this instance'
Message	'The maximum number of dedicated administrator connections for this instance is "",%1,"'."
Device Custom Number 1	%1 (Maximum administrator connections)

Event 18264

ArcSight Field	Vendor Field
Name	Database backed up
Message	Database backed up. Database: %1, creation date(time): %2(%3), pages dumped: %4, first LSN: %5, last LSN: %6, number of dump devices: %7, device information: %8. This is an informational message only. No user action is required.
Device Custom String 1	%1 (Database name)
Device Custom Date 1	%2 (Creation Date)
Device Custom String 5	%5 (First LSN)
Device Custom String 6	%6 (Last LSN)
Device Custom Number 1	%4 (Pages Dumped)
Device Custom Number 2	%7 (Number of dump devices)
Device Custom String 4	%8 (Device Information)

Event 18265

ArcSight Field	Vendor Field
Name	Log was backed up
Message	Log was backed up. Database: %1, creation date(time): %2(%3), first LSN: %4, last LSN: %5, number of dump devices: %6, device information: %7. This is an informational message only. No user action is required.
Device Custom String 1	%1 (Database name)
Device Custom Date 1	%2 (Creation Date)
Device Custom String 5	%4 (First LSN)
Device Custom String 6	%5 (Last LSN)
Device Custom Number 1	%6 (Number of dump devices)
Device Custom String 4	%7 (Device Information)

Event 18267

ArcSight Field	Vendor Field
Name	Database was restored
Message	Database was restored: Database: %1 creation date(time): %2(%3), first LSN: %4, last LSN: %5, number of dump devices: %6, device information: %7. Informational message. No user action required
Device Custom String 1	%1 (Database name)
Device Custom Date 1	%2 (Creation Date)
Device Custom String 5	%4 (First LSN)
Device Custom String 6	%5 (Last LSN)
Device Custom Number 1	%6 (Number of dump devices)
Device Custom String 4	%7 (Device Information)

Event 18452

ArcSight Field	Vendor Field
Name	Login failed
Message	Login failed. The login is from an untrusted domain and cannot be used with Windows authentication. %1
Source Address	%1
Reason	The login is from an untrusted domain and cannot be used with Windows authentication.

Event 18453

ArcSight Field	Vendor Field
Name	'Login succeeded'
Message	'Login succeeded for user. Connection made using Windows authentication'
Destination User Name	%1
Destination NT Domain	%1
Device Custom String 1	%2 (Windows authentication)

Event 18454

ArcSight Field	Vendor Field
Name	'Login succeeded'
Message	'Login succeeded for user. Connection made using SQL Server authentication'
Source User Name	%1
Source Address	%2
Device Custom IPv6 Address 2	%2 (Source IPv6 Address)

Event 18456

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	'Login failed for user ',%1,'.',%2',%3
Device Custom String 3	%2 (Login failed)
Source User Name	%1
Source Address	%3

Event 18461

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	Login failed for user %1 Reason: Server is in single user mode. Only one administrator can connect at this time. %2
Destination NT Domain	Domain from %1 will be extracted
Destination User Name	User from %1 will be extracted
Reason	Server is in single user mode. Only one administrator can connect at this time.
Destination Address	%2

Event 18470

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	Login failed for user %1 Reason: The account is disabled. %2
Source User Name	%1
Reason	The account is disabled
Source Address	%2

Event 18488

ArcSight Field	Vendor Field
Name	'Login failed for user'
Message	'Login failed for user ',%1,'. Reason: The password of the account must be changed. ',%2
Source User Name	%1
Source Address	%2

Event 18496

ArcSight Field	Vendor Field
Name	'System Manufacturer and System Model Information'
Message	'System Manufacturer: ',%1,' System Model: ',%2,' '
Device Custom String 1	%1 (System Manufacturer)
Device Custom String 2	%2 (System Model)

Event 19030

ArcSight Field	Vendor Field
Name	'SQL Trace was started'
Message	'SQL Trace ID ',%1,' was started by login ',%2,' '
Device Custom String 1	%1 (Trace ID)
Source User Name	%2

Event 19031

ArcSight Field	Vendor Field
Name	'SQL Trace stopped'
Message	'SQL Trace stopped. Trace ID = ',%1,'. Login Name = ',%2
Source User Name	%2
Device Custom Number 1	%1 (Trace Id)

Event 19032

ArcSight Field	Vendor Field
Name	'SQL Trace was stopped due to server shutdown'
Message	'SQL Trace was stopped due to server shutdown. Trace ID = ',%1,'. This is an informational message only; no user action is required.'
Device Custom Number 1	%1 (Trace ID)

Event 19033

ArcSight Field	Vendor Field
Name	Server started with '-f' option
Message	Server started with '-f' option. Auditing will not be started. This is an informational message only; no user action is required.

Event 26018

ArcSight Field	Vendor Field
Name	'A self-generated certificate was successfully loaded for encryption'
Message	'A self-generated certificate was successfully loaded for encryption'

Event 26022

ArcSight Field	Vendor Field
Name	'Server is listening'
Message	'Server is listening on [,%1,' <,%2,'> ,,%3,']'

ArcSight Field	Vendor Field
Device Custom String 4	%1 (Listening Address)
Application Protocol	%2
Destination Port	%3

Event 26037

ArcSight Field	Vendor Field
Name	'SQL Server Network Interface library could not register the Server Principal Name'
Message	'Error: '%1,' state: '%2.'. Failure to register an SPN may cause integrated authentication to fall back to NTLM instead of Kerberos'

Event 26048

ArcSight Field	Vendor Field
Name	'Server local connection provider is ready to accept connection'
Message	'Server local connection provider is ready to accept connection on [%1]'
File Path	%1

Event 26067

ArcSight Field	Vendor Field
Name	'SQL Server Network Interface library could not register the Service Principal Name (SPN)'
Message	'The SQL Server Network Interface library could not register the Service Principal Name (SPN) '%1' for the SQL Server service. Windows return code: '%2,' state: '%3.'. Failure to register a SPN might cause integrated authentication to use NTLM instead of Kerberos. This is an informational message. Further action is only required if Kerberos authentication is required by authentication policies and if the SPN has not been manually registered.'
Source Service Name	%1
Reason	%2
Device Custom String 1	%3 (State)

Event 26076

ArcSight Field	Vendor Field
Name	'SQL Server is attempting to register a Service Principal Name (SPN)'
Message	'SQL Server is attempting to register a Service Principal Name (SPN) for the SQL Server service. Kerberos authentication will not be possible until a SPN is registered for the SQL Server service. This is an informational message. No user action is required.'

Event 30090

ArcSight Field	Vendor Field
Name	'New instance of full-text filter daemon host process has been successfully started.'
Message	'A new instance of the full-text filter daemon host process has been successfully started.'

Event 33090

ArcSight Field	Vendor Field
Name	'Attempting to load library into memory'
Message	'Attempting to load library ',%1,' into memory. This is an informational message only. No user action is required'
File Name	%1

Event 33204

ArcSight Field	Vendor Field
Name	'SQL Server Audit could not write to the security log'
Message	'SQL Server Audit could not write to the security log'

Event 33205

ArcSight Field	Vendor Field
Source Service Name	EventSource
Device Event Class ID	All of (class_type, ' ', action_id)
Device Action	action_id
Event Outcome	succeeded
File ID	object_id
File Type	class_type
File Name	object_name
File Size	sequence_number
File Hash	audit_schema_version
Old File ID	transaction_id
Message	statement
Source User ID	server_principal_id
Source User Name	server_principal_name
Source NT Domain	server_principal_name
Destination User ID	One of (server_principal_id, target_server_principal_id)
Destination NT Domain	One of (target_server_principal_name, server_principal_name)
Destination Host Name	server_instance_name
Device Custom Number 1	session_id
Device Custom Number 2	database_principal_id
Device Custom Number 3	target_database_principal_id
Device Custom String 1	object_name
Device Custom String 2	statement
Device Custom String 3	database_name
Device Custom String 4	Device Custom String 4 = database_principal_name
Device Custom String 5	One of (target_database_principal_name, database_principal_name)
Device Custom String 6	schema_name
Old File Name	All of('Additional Information : ',additional_information)

ArcSight Field	Vendor Field
Source Address	One of(additional_information, device address (In case the address is local machine))
Source Host Name	device host name (In case the address is local machine)
Destination User Name	One Of(target_server_principal_name,server_principal_name)
Device Custom IPv6 Address 2	additional_information

Event 33217

ArcSight Field	Vendor Field
Name	'SQL Server Audit is starting the audits'
Message	'SQL Server Audit is starting the audits. This is an informational message. No user action is required.'

Event 33218

ArcSight Field	Vendor Field
Name	'SQL Server Audit has started the audits'
Message	'SQL Server Audit has started the audits. This is an informational message. No user action is required.'

Event 49903

ArcSight Field	Vendor Field
Name	'Detected RAM'
Message	'Detected ',%1,' of RAM. This is an informational message; no user action is required.'
Device Custom Number 1	%1 (Detected RAM)

Event 49904

ArcSight Field	Vendor Field
Name	'Service account'
Message	'The service account is ',%1,'. This is an informational message; no user action is required.'
Source Service Name	%1

Event 49910

ArcSight Field	Vendor Field
Name	'Software Usage Metrics is disabled'
Message	'Software Usage Metrics is disabled'

Event 49916

ArcSight Field	Vendor Field
Name	'UTC adjustment'
Message	'UTC adjustment.'
Device Custom String 1	All of 1%, :, 2% (UTC Adjustment)

Event 49917

ArcSight Field	Vendor Field
Name	'Default collation'
Message	All of 'Default collation',%1,'(%2,',%3,').'
Device Custom String 1	%2 (Language)
Device Custom String 4	%1 (SQL collation)
Device Custom Number 2	%3 (Language ID)

Microsoft Sysmon

This section has the following sections:

Windows 2012

General

ArcSight Field	Vendor Field
Destination Process Id	ProcessId
Device Product	'Sysmon'

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Version	'Unknown'

Event 1

ArcSight Field	Vendor Field
Destination Process Name	Image
Destination Service Name	CommandLine
Device Action	'Process Create'
Device Custom String 1	IntegrityLevel
Device Custom String 4	CommandLine
Device Custom String 6	LogonGuid
Device Receipt Time	UtcTime
File Hash	Hashes
File Id	ProcessGuid
Message	Description
Name	'Process Created'
Old File Hash	MITRE ID
Old File Id	ParentProcessGuid
Old File Name	OriginalFileName
Old File Path	CurrentDirectory
Source Nt Domain	<code>__extractNTDomain(User)</code>
Source Process Id	ParentProcessId
Source Process Name	ParentImage
Source Service Name	ParentCommandLine
Source User Id	LogonId
Source User Name	<code>__extractNTUser(User)</code>

Event 2

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File creation time changed'
Device Receipt Time	UtcTime
File Create Time	CreationUtcTime
File Id	ProcessGuid
File Path	TargetFilename
Message	'File creation time changed'
Name	'File creation time changed'
Old File Create Time	PreviousCreationUtcTime
Old File Hash	MITRE ID

Event 3

ArcSight Field	Vendor Field
Destination Address	<code>__oneOfAddress(DestinationIp)</code> (for destination aware)
Device Custom IPv6 Address 2	<code>__stringToIPv6Address(SourceIp)</code> (for non-destination aware)
Device Custom IPv6 Address 3	<code>__stringToIPv6Address(DestinationIp)</code> (for non-destination aware)
Destination Host Name	DestinationHostname
Destination Port	<code>__safeToInteger(DestinationPort)</code>
Destination Process Name	Image
Device Action	<code>__concatenate("Initiated : ", Initiated)</code>
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Network connection detected'
Name	'Network connection detected'
Old File Hash	MITRE ID
Source Address	<code>__oneOfAddress(SourceIp)</code> (for destination aware)
Source Host Name	SourceHostname

ArcSight Field	Vendor Field
Source Nt Domain	<code>__extractNTDomain(User)</code>
Source Port	<code>__safeToInteger(SourcePort)</code>
Source Port Name	SourcePortName
Source User Name	<code>__extractNTUser(User)</code>
Transport Protocol	Protocol

Event 4

ArcSight Field	Vendor Field
Additional Data.Schema Version	SchemaVersion
Device Action	State
Device Receipt Time	UtcTime
Message	'Sysmon service state changed'
Name	'Sysmon service state changed'

Event 5

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Process Terminated'
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Process Terminated'
Name	'Process Terminated'
Old File Hash	MITRE ID

Event 6

ArcSight Field	Vendor Field
Device Action	'Driver Loaded'
Device Receipt Time	UtcTime

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
File Hash	Hashes
File Name	ImageLoaded
File Permission	SignatureStatus
File Type	Signed
Message	'Driver Loaded'
Name	'Driver Loaded'
Old File Hash	MITRE ID

Event 7

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Image Loaded'
Device Receipt Time	UtcTime
File Hash	Hashes
File Id	ProcessGuid
File Name	ImageLoaded
File Permission	SignatureStatus
File Type	Signed
Message	Description
Name	'Image Loaded'
Old File Hash	MITRE ID
Old File Name	OriginalFileName

Event 8

ArcSight Field	Vendor Field
Destination Process Name	TargetImage
Device Action	'CreateRemoteThread detected'
Device Process Id	SourceProcessId
Device Receipt Time	UtcTime

ArcSight Field	Vendor Field
File Id	TargetProcessGuid
Message	'CreateRemoteThread detected'
Name	'CreateRemoteThread detected'
Old File Hash	MITRE ID
Old File Id	SourceProcessGuid
Source Process Name	SourceImage

Event 9

ArcSight Field	Vendor Field
Device Action	'RawAccessRead detected'
Device Custom String 5	Device
Device Receipt Time	UtcTime
Destination Process Name	Image
File Id	ProcessGuid
Message	'RawAccessRead detected'
Name	'RawAccessRead detected'
Old File Hash	MITRE ID

Event 10

ArcSight Field	Vendor Field
Additional Data.Source Thread Id	SourceThreadId
Destination Process Name	TargetImage
Device Action	'Process accessed'
Device Custom String 1	GrantedAccess
Device Process Id	__safeToInteger(SourceProcessId)
Device Receipt Time	UtcTime
File Id	TargetProcessGUID
Message	'Process accessed'
Name	'Process accessed'

ArcSight Field	Vendor Field
Old File Id	SourceProcessGUID
Old File Hash	MITRE ID
Old File Path	CallTrace
Source Process Name	SourceImage

Event 11

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File Created'
Device Receipt Time	UtcTime
File Create Time	CreationUtcTime
File Id	ProcessGuid
File Path	TargetFilename
Message	'File created'
Name	'File created'
Old File Hash	MITRE ID

Event 12

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry object added or deleted'
Device Custom String 1	EventType
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	TargetObject
Message	'Registry object added or deleted'
Name	'Registry object added or deleted'
Old File Hash	MITRE ID

Event 13

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry value set'
Device Custom String 1	EventType
Device Custom String 4	Details
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	TargetObject
Message	'Registry value set'
Name	'Registry value set'
Old File Hash	MITRE ID

Event 14

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Registry key and value rename'
Device Custom String 1	EventType
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Path	NewName
Name	'Registry key and value rename'
Old File Hash	MITRE ID
Old File Path	TargetObject

Event 15

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'File stream created'

ArcSight Field	Vendor Field
Device Receipt Time	UtcTime
File Hash	Hash
File Id	ProcessGuid
File Create Time	CreationUtcTime
File Path	TargetFilename
Message	'File stream created'
Name	'File stream created'
Old File Hash	MITRE ID

Event 16

ArcSight Field	Vendor Field
Device Action	'Sysmon config state changed'
Device Receipt Time	UtcTime
File Hash	ConfigurationFileHash
Message	'Sysmon config state changed'
Name	'Sysmon config state changed'
Source Process Name	Configuration

Event 17

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Pipe Created'
Device Custom String 1	EventType
Device Custom String 6	PipeName
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Create Pipe'
Name	'Create Pipe'
Old File Hash	MITRE ID

Event 18

ArcSight Field	Vendor Field
Destination Process Name	Image
Device Action	'Pipe Connected'
Device Custom String 1	EventType
Device Custom String 6	PipeName
Device Receipt Time	UtcTime
File Id	ProcessGuid
Message	'Pipe Connected'
Name	'Pipe Connected'
Old File Hash	MITRE ID

Event 19

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Name
Device Receipt Time	UtcTime
Name	'WmiEventFilter activity detected'
Old File Hash	MITRE ID
Old File Path	EventNamespace
Source Nt Domain	__extractNTDomain(User)
Source User Name	__extractNTUser(User)

Event 20

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Name

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Device Receipt Time	UtcTime
File Path	Destination
File Type	Type
Name	'WmiEventConsumer activity detected'
Old File Hash	MITRE ID
Source Nt Domain	<code>__extractNTDomain(User)</code>
Source User Name	<code>__extractNTUser(User)</code>

Event 21

ArcSight Field	Vendor Field
Device Action	Operation
Device Custom String 1	EventType
Device Custom String 4	Filter
Device Custom String 5	Consumer
Device Receipt Time	UtcTime
Name	'WmiEventConsumerToFilter activity detected'
Old File Hash	MITRE ID
Source Nt Domain	<code>__extractNTDomain(User)</code>
Source User Name	<code>__extractNTUser(User)</code>

Event 22

ArcSight Field	Vendor Field
Destination Address	<code>__regexToken(QueryResults)</code>
Destination Process Name	Image
Device Action	'Dns query'
Device Custom IPv6 Address 3	Query result
Device Custom String 1	QueryName
Device Custom String 4	QueryResults
Device Receipt Time	UtcTime

ArcSight Field	Vendor Field
File ID	ProcessGuid
Message	'Dns query'
Name	'Dns query'
Old File Hash	MITRE ID

Event 23

ArcSight Field	Vendor Field
Device Custom String 1	IsExecutable
Device Custom String 4	Archived
Device Receipt Time	UtcTime
File Id	ProcessGuid
File Hash	Hashes
File Path	TargetFilename
Message	<code>__concatenate("File has been deleted from ", __extractNTDomain(TargetFilename))</code>
Name	'File Delete'
Old File Hash	MITRE ID
Source Nt Domain	<code>__extractNTDomain(User)</code>
Source Process Name	Image
Source User Name	<code>__extractNTUser(User)</code>

Event 255

ArcSight Field	Vendor Field
Device Receipt Time	UtcTime
Device Action	<code>__stringConstant("Level : Error")</code>
Message	Description
Name	'Error report'
Source Process Name	ID

Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user ',%2,' has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port ',%2,' has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user ',%3,' connected on port ',%4,', does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),' has connected and has been successfully authenticated on port ',One of (%3,%4),' . Data sent and received over this link is strongly encrypted.')

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user ',%2,' connected on port ',%3,', on ',%4,', at ',%5,', and disconnected on ',%6,', at ',%7,'. The user was active for ',%8,' minutes, ',%9,' seconds, ',%10,' bytes were sent and ',%11,' bytes were received. The reason for disconnecting was ',%12,. The tunnel used was ',%13,. The quarantine state was ',%14,'.)

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user ',%2,' connected on port ',%3,', has been assigned address ',%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both ('The user with ip address ',%2,', has disconnected')

Mappings for Microsoft Windows AppLocker

Event 8001

ArcSight Field	Vendor Field
Name	"The AppLocker policy was applied successfully to this computer."

Event 8002

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName

ArcSight Field	Vendor Field
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullPath or FilePath

Event 8003

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run but would have been prevented from running if the AppLocker policy were enforced."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullPath or FilePath

Event 8004

ArcSight Field	Vendor Field
Name	FilePath," was prevented from running."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl

ArcSight Field	Vendor Field
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullPath or FilePath

Event 8005

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullPath or FilePath

Event 8006

ArcSight Field	Vendor Field
Name	FilePath," was allowed to run but would have been prevented from running if the AppLocker policy were enforced."
Device Custom String 1	PolicyName

ArcSight Field	Vendor Field
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullPath or FilePath

Event 8007

ArcSight Field	Vendor Field
Name	FilePath," was prevented from running."
Device Custom String 1	PolicyName
Device Custom String 3	RuleId
Device Custom String 4	RuleSddl
Device Custom String 5	Fqbn
Device Custom String 6:	RuleName
Device Custom Number 1	FileHashLength
Destination User Name	TargetUser
Destination Process Id	TargetProcessId
File Hash	FileHash
Destination User Id	TargetLogonId
File Path	FullPath or FilePath

Microsoft Windows BITS Event

This section has the following sections:

Microsoft Windows BITS Client

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows BITS Client'

Event 3

ArcSight Field	Vendor Field
Destination Nt Domain	string2
Destination User Name	string2
Device Custom String 4	string
Device Custom String 4 Label	"Job Title"
Message	All of("The BITS service created a new job: ",string,", with owner ",string2)
Name	"The BITS service created a new job"

Event 4

ArcSight Field	Vendor Field
Device Custom Number 1	fileCount
Device Custom Number 1 Label	"File count"
Device Custom String 4	jobTitle
Device Custom String 4 Label	"Job Title"
Device Custom String 5	jobId
Device Custom String 5 Label	"Job ID"
Device Custom String 6	jobOwner
Device Custom String 6 Label	"Job Owner"
Message	All of("The transfer job is complete.User: ",User,", Transfer job: ",jobTitle,", Job ID: ",jobId,", Owner: ",jobOwner,", File count: ",fileCount)

ArcSight Field	Vendor Field
Name	"The transfer job is complete"
Source Nt Domain	User
Source User Name	User

Event 59

ArcSight Field	Vendor Field
Bytes In	bytesTransferredFromPeer
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS started the ",name," transfer job that is associated with the ",url," URL")
Name	"BITS started the transfer for job"

Event 60

ArcSight Field	Vendor Field
Bytes In	bytesTransferredFromPeer
Bytes Out	bytesTransferred
Destination Host Name	peer

ArcSight Field	Vendor Field
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS stopped the ",name," transfer job that is associated with the ",url," URL. The status code is 0x",hr)
Name	"BITS stopped transferring for job"
Old File Name	Both("Proxy :",proxy)
Old File Path	Both("Bandwidth Limit :",bandwidthLimit)
Reason	Both ("0x",hr)

Event 61

ArcSight Field	Vendor Field
Bytes In	bytesTransferredFromPeer
Bytes Out	bytesTransferred
Destination Host Name	peer
Device Custom Number 1	bytesTotal
Device Custom Number 1 Label	"Total Bytes"
Device Custom String 1	transferId
Device Custom String 1 Label	"Transfer ID"
Device Custom String 4	name

ArcSight Field	Vendor Field
Device Custom String 4 Label	"Job Title"
Device Custom String 5	Id
Device Custom String 5 Label	"Job ID"
File Create Time	fileTime
File Path	url
File Size	fileLength
Message	All of("BITS stopped the ",name," transfer job that is associated with the ",url," URL. The status code is 0x",hr)
Name	"BITS stopped transferring the job"
Old File Name	Both("Proxy :",proxy)
Old File Path	bandwidthLimit
Reason	Both("0x",hr)

Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user ',%2,', has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port ',%2,' has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),' has connected and has been successfully authenticated on port ',One of (%3,%4),' . Data sent and received over this link is strongly encrypted.)'

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds

ArcSight Field	Vendor Field
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user ',%2,' connected on port ',%3,' on ',%4,' at ',%5,' and disconnected on ',%6,' at ',%7,'. The user was active for ',%8,' minutes, ',%9,' seconds, ',%10,' bytes were sent and ',%11,' bytes were received. The reason for disconnecting was ',%12,. The tunnel used was ',%13,. The quarantine state was ',%14,'.)

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user ',%2,' connected on port ',%3,' has been assigned address ',%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both ('The user with ip address ',%2,' has disconnected')

Microsoft Windows Defender Antivirus

Mappings for Microsoft Windows Defender AntiVirus

Event 1000

ArcSight Field	Vendor Field
Device Action	Scan Parameter
Device Custom String 1	Scan ID
Device Custom String 1 Label	"Scan ID"
Device Event Category	Scan Type
Device Version	Product Version
File Path	Scan Resources
Message	An antimalware scan started
Name	MALWAREPROTECTION_SCAN_STARTED
Scan Parameter Index	Scan Parameter Index
Scan Type Index	Scan Type Index
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 1001

ArcSight Field	Vendor Field
Device Custom Number1	Scan Time Hours
Device Custom Number2 Label	"Minutes"
Device Action	Scan Parameter
Device Custom Number1 Label	"Hours"
Device Custom Number2	Scan Time Minutes
Device Custom Number3	Scan Time Seconds

ArcSight Field	Vendor Field
Device Custom Number3 Label	"Seconds"
Device Custom String1	Scan ID
Device Custom String1 Label	"Scan ID"
Device Event Category	Scan Type
Device Version	Product Version
Message	An anti-malware scan finished.
Name	MALWAREPROTECTION_SCAN_COMPLETED
Scan Parameter Index	Scan Parameter Index
Scan Type Index	Scan Type Index
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 1002

ArcSight Field	Vendor Field
Device Action	Scan Parameter
Device Custom String1	Scan ID
Device Custom String1 Label	"Scan ID"
Device Event Category	Scan Type
Device Version	Product Version
Message	An anti-malware scan was stopped before it finished.
Name	MALWAREPROTECTION_SCAN_CANCELLED
Scan Parameter Index	Scan Parameter Index
Scan Type Index	Scan Type Index
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 1009

ArcSight Field	Vendor Field
Device Custom Number1 Label	"Threat ID"
Device Custom Number2 Label	"Severity ID"
Device Custom Number1	Threat ID
Device Custom Number2	Severity ID
Device Custom Number3	Category ID
Device Custom Number3 Label	"Category ID"
Device Custom String1	Threat Name
Device Custom String1 Label	"Threat Name"
Device Custom String2	Signature Version,Engine Version
Device Custom String2Label	"Signature/Engine Version"
Device Custom String4	Category Name
Device Custom String4 Label	"Category Name"
Device Version	Product Version
File Path	Path
FWLink	FWLink
Message	The antimalware platform restored an item from quarantine.
Name	MALWAREPROTECTION_QUARANTINE_RESTORE
Old File ID	Severity Name
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 1010

ArcSight Field	Vendor Field
Device Custom Number 1	Threat ID
Device Custom Number 1 Label	“Threat ID”
Device Custom Number 2	Severity ID
Device Custom Number 2 Label	“Severity ID”
Device Custom Number 3	Category ID
Device Custom Number 3 Label	“Category ID”
Device Custom String 1	Threat Name
Device Custom String 1 Label	“Threat Name”
Device Custom String 2	Engine Version
Device Custom String 2 Label	“Engine Version”
Device Custom String 4	Category Name
Device Custom String 4 Label	“Category Name”
Device Custom String 5	Error Description
Device Custom String 5 Label	“Error Description”
Device Version	Product Version
File Path	Path
Message	The anti-malware platform could not restore an item from quarantine.
Name	MALWAREPROTECTION_QUARANTINE_RESTORE_FAILED
Old File ID	Severity Name
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 1011

ArcSight Field	Vendor Field
Device Custom Number 1 Label	"Threat ID"
Device Custom Number 2 Label	"Severity ID"
Device Custom Number 1	Threat ID
Device Custom Number 2	Severity ID
Device Custom Number 3	Category ID
Device Custom Number 3 Label	"Category ID"
Device Custom String 1	Threat Name
Device Custom String 1 Label	"Threat Name"
Device Custom String 2	Signature Version,Engine Version
Device Custom String 2 Label	"Signature/Engine Version"
Device Custom String 4	Category Name
Device Custom String 4 Label	"Category Name"
Device Version	Product Version
File Path	Path
FW Link	FWLink
Message	The anti-malware platform deleted an item from quarantine.
Name	MALWAREPROTECTION_QUARANTINE_DELETE
Old File ID	Severity Name
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 1013

ArcSight Field	Vendor Field
Device Custom Date 1	Timestamp
Device Custom Date 1 Label	"Action Time"
Device Version	Product Version
Message	The anti-malware platform deleted history of malware and other potentially unwanted software.
Name	MALWAREPROTECTION_MALWARE_HISTORY_DELETE
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 1015

ArcSight Field	Vendor Field
Device Custom Number1 Label	"Threat ID"
Device Custom Number2 Label	"Severity ID"
Device Custom Number1	Threat ID
Device Custom Number2	Severity ID
Device Custom Number3	Category ID
Device Custom Number3 Label	"Category ID"
Device Custom String1	Threat Name
Device Custom String1 Label	"Threat Name"
Device Custom String2	Signature Version,Engine Version
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String4	Category Name
Device Custom String4 Label	"Category Name"
Device Custom String6	Detection ID
Device Custom String6 Label	"Detection ID"

ArcSight Field	Vendor Field
Device Version	Product Version
File Path	Path Found
FWLink	FWLink
Message	The anti-malware platform detected suspicious behavior.
Name	MALWAREPROTECTION_BEHAVIOR_DETECTED
Old File ID	Severity Name
Old File Type	Detection Type
Request Context	Detection Origin
Source Nt Domain	Domain
Source Process Name	Process Name
Source Service Name	Detection Source
Source User ID	SID
Source User Name	User

Event 1116

ArcSight Field	Vendor Field
Device Custom Number1 Label	"Threat ID"
Device Custom Number2 Label	"Severity ID"
Action ID	Action ID
Additional Actions ID	Additional Actions ID
Device Action	Action Name
Device Custom Number1	Threat ID
Device Custom Number2	Severity ID
Device Custom Number3	Category ID
Device Custom Number3 Label	"Category ID"
Device Custom String1	Threat Name
Device Custom String1 Label	"Threat Name"
Device Custom String2	Signature Version,Engine Version

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

ArcSight Field	Vendor Field
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String4	Category Name
Device Custom String4 Label	"Category Name"
Device Custom String5	Error Description
Device Custom String5 Label	"Error Description"
Device Custom String6	Detection ID
Device Custom String6 Label	"Detection ID"
Device Version	Product Version
Execution ID	Execution ID
Execution Name	Execution Name
File Path	Path
FWLink	FWLink
Message	The anti-malware platform detected malware or other potentially unwanted software. Additional Actions String:
Name	MALWAREPROTECTION_STATE_MALWARE_DETECTED
Old File ID	Severity Name
Old File Type	Type Name
Origin ID	Origin ID
Post Clean Status	Post Clean Status
Pre Execution Status	Pre Execution Status
Reason	Error Code
Remediation User	Remediation User
Request Context	Origin Name
Request context	Detection Origin
Source ID	Source ID
Source Process Name	Process Name
Source Service Name	Source Name
Source User Name	Detection User
Start Time	Detection Time

ArcSight Field	Vendor Field
State	State
Status Code	Status Code
Status Description	Status Description
Type ID	Type ID

Event 1117

ArcSight Field	Vendor Field
Device Custom Number1 Label	"Threat ID"
Device Custom Number2 Label	"Severity ID"
Action ID	Action ID
Additional Actions ID	Additional Actions ID
Device Action	Action Name
Device Custom Number1	Threat ID
Device Custom Number2	Severity ID
Device Custom Number3	Category ID
Device Custom Number3 Label	"Category ID"
Device Custom String1	Threat Name
Device Custom String1 Label	"Threat Name"
Device Custom String2	Signature Version,Engine Version
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String4	Category Name
Device Custom String4 Label	"Category Name"
Device Custom String5	Error Description
Device Custom String5 Label	"Error Description"
Device Custom String6	Detection ID
Device Custom String6 Label	"Detection ID"
Device Version	Product Version
Execution ID	Execution ID

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

ArcSight Field	Vendor Field
Execution Name	Execution Name
File Path	Path
FWLink	FWLink
Message	The anti-malware platform performed an action to protect your system from malware or other potentially unwanted software. Additional Actions String:
Name	MALWAREPROTECTION_STATE_MALWARE_ACTION_TAKEN
Old File ID	Severity Name
Old File Type	Type Name
Origin ID	Origin ID
Post Clean Status	Post Clean Status
Pre Execution Status	Pre Execution Status
Reason	Error Code
Remediation User	Remediation User
Request context	Detection Origin
Request Context	Origin Name
Source ID	Source ID
Source Process Name	Process Name
Source Service Name	Source Name
Source User Name	Detection User
Start Time	Detection Time
State	State
Status Code	Status Code
Status Description	Status Description
Type ID	Type ID

Event 1150

ArcSight Field	Vendor Field
Device Custom String2	Signature Version,Engine Version
Device Custom String2 Label	"Signature/Engine Version"

ArcSight Field	Vendor Field
Device Version	Platform Version
Message	If your anti-malware platform reports status to a monitoring platform, this event indicates that the antimalware platform is running and in a healthy state.
Name	MALWAREPROTECTION_SERVICE_HEALTHY

Event 1151

ArcSight Field	Vendor Field
Device Custom Date1	Last full scan start time
Device Custom Date1 Label	"Last full scan start time"
Device Custom Date2	Last full scan end time
Device Custom Date2 Label	"Last full scan end time"
Device Custom Number1	safeToLong(updateRevisionNumber)
Device Custom Number1	AV signature age
Device Custom Number1 Label	"Last AV Signature Age"
Device Custom Number2	AS signature age
Device Custom Number2 Label	"Last AS Signature Age"
Device Custom Number3	Last quick scan age
Device Custom Number3 Label	"Last quick scan age"
Device Custom String 1	RTP State/ OA State/ IOAV State/ BM State
Device Custom String1 Label	"RTP State/ OA State/ IOAV State/ BM State"
Device Custom String2	Signature Version,Engine Version
Device Custom String2 Label	"Signature/Engine Version"
Device Custom String4	Last quick scan source
Device Custom String4 Label	"Last Quick Scan Source"
Device Custom String6	Last full scan source
Device Custom String6 Label	"Last full scan source"
Device Floating Point1	Last full scan age
Device Floating Point1 Label	"Last full scan age"
Device Version	Platform Version
End Time	Last quick scan end time

ArcSight Field	Vendor Field
File Create Time	AV signature creation time
Message	Endpoint Protection client health report (time in UTC).
Name	MALWAREPROTECTION_SERVICE_HEALTH_REPORT
Old File Create Time	AS signature creation time
Product status	Product status
Start Time	Last quick scan start time

Event 2000

ArcSight Field	Vendor Field
Device Custom String2	Current Engine Version,Previous Engine Version,Current Signature Version,Previous Signature Version
Device Custom String2 Label	"Current Engine Version/Previous Engine Version/Current Signature Version/Previous Signature Version"
Device Custom String6	Update Type
Device Custom String6 Label	"Update Type"
Device Event Category	Signature Type
Device Version	Product Version
Message	The anti-malware definitions updated successfully
Name	MALWAREPROTECTION_SIGNATURE_UPDATED
Signature Type Index	Signature Type Index
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User
Update Type Index	Update Type Index

Event 2001

ArcSight Field	Vendor Field
Device Custom String2	Current Engine Version,Previous Engine Version,Current Signature Version,Previous Signature Version
Device Custom String2 Label	"Current Engine Version/Previous Engine Version/Current Signature Version/Previous Signature Version"

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

ArcSight Field	Vendor Field
Device Custom String5	Error Description
Device Custom String5 Label	"Error Description"
Device Custom String6	Update Type
Device Custom String6 Label	"Update Type"
Device Event Category	Signature Type
Device Version	Product Version
File Path	Source Path
Message	The security intelligence update failed.
Name	MALWAREPROTECTION_SIGNATURE_UPDATE_FAILED
Reason	Error Code
Signature Type Index	Signature Type Index
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 2002

ArcSight Field	Vendor Field
Device Custom String2	Current Engine Version, Previous Engine Version
Device Custom String2 Label	"Current/ Previous Engine Version"
Device Event Category	Feature Name
Device Version	Product Version
Feature Index	Feature Index
Message	The anti-malware engine updated successfully.
Name	MALWAREPROTECTION_ENGINE_UPDATED
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 2003

ArcSight Field	Vendor Field
Device Custom String 2	Current Engine Version / Previous Engine Version
Device Custom String 2 Label	"Current/Previous Engine Version"
Device Custom String 5	Error Description
Device Custom String 5 Label	"Error Description"
Device Version	Product Version
Message	The anti-malware engine update failed.
Name	MALWAREPROTECTION_ENGINE_UPDATE_FAILED
Reason	Error Code
Source Nt Domain	Domain
Source User ID	SID
source User Name	User

Event 2010

ArcSight Field	Vendor Field
Device Custom Date1	Dynamic Signature Compilation Timestamp
Device Custom Date1 Label	"Dynamic Signature Compilation Timestamp"
Device Custom String1	Dynamic Signature Version
Device Custom String1 Label	"Dynamic Signature Version"
Device Custom String2	Current Engine Version,Current Signature Version
Device Custom String2 Label	"Current Engine Version/Current Signature Version"
Device Event Category	Signature Type
Device Version	Product Version
Dynamic Signature Type	Dynamic Signature Type
Dynamic Signature Type Index	Dynamic Signature Type Index
File Path	Persistence Path
Message	The anti-malware engine used the Dynamic Signature Service to get additional definitions.
Name	MALWAREPROTECTION_SIGNATURE_FASTPATH_UPDATED

ArcSight Field	Vendor Field
Persistence Limit Type	Persistence Limit Type
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Value	Persistence Limit Value
Signature Type Index	Signature Type Index
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 2011

ArcSight Field	Vendor Field
Device Custom Date1	Dynamic Signature Compilation Timestamp
Device Custom Date1 Label	"Dynamic Signature Compilation Timestamp"
Device Custom String1	Dynamic Signature Version
Device Custom String1 Label	"Dynamic Signature Version"
Device Custom String2	Current Engine Version,Current Signature Version
Device Custom String2 Label	"Current Engine Version/Current Signature Version"
Device Event Category	Signature Type
Device Version	Product Version
Dynamic Signature Type	Dynamic Signature Type
Dynamic Signature Type Index	Dynamic Signature Type Index
File Path	Persistence Path
Message	The Dynamic Signature Service deleted the out-of-date dynamic definitions.
Name	MALWAREPROTECTION_SIGNATURE_FASTPATH_DELETED
Persistence Limit Type	Persistence Limit Type
Persistence Limit Type Index	Persistence Limit Type Index
Persistence Limit Value	Persistence Limit Value
Reason	Removal Reason Value
Removal Reason Index	Removal Reason Index
Signature Type Index	Signature Type Index

ArcSight Field	Vendor Field
Source Nt Domain	Domain
Source User ID	SID
Source User Name	User

Event 2030

ArcSight Field	Vendor Field
Device Version	Product Version
Message	The anti-malware engine was downloaded and is configured to run offline on the next system restart.
Name	MALWAREPROTECTION_OFFLINE_SCAN_INSTALLED

Event 2031

ArcSight Field	Vendor Field
Name	MALWAREPROTECTION_OFFLINE_SCAN_INSTALL_FAILED
Message	The antimalware engine was unable to download and configure an offline scan.
Device Version	Product Version
Device Custom String 5 Label	“Error Description”
Device Custom String 5	Error Description
Reason	Error code

Event 2041

ArcSight Field	Vendor Field
Name	MALWAREPROTECTION_OS_EOL
Message	Antimalware support for this operating system has ended. You must upgrade the operating system for continued support.

Event 3002

ArcSight Field	Vendor Field
Device Custom String5	Error Description
Device Custom String5 Label	"Error Description"
Device Version	Product Version
File Hash	Feature Name
File ID	Feature ID
Message	Real-time protection encountered an error and failed.
Name	MALWAREPROTECTION_RTP_FEATURE_FAILURE
Reason	Error Code

Event 3007

ArcSight Field	Vendor Field
Name	MALWAREPROTECTION_RTP_FEATURE_RECOVERED
Message	Real-time protection recovered from a failure. We recommend running a full system scan when you see this error.
Device Version	Product Version
File ID	Feature ID
File Hash	Feature Name
Reason	reason

Event 5000

ArcSight Field	Vendor Field
Device Version	Product Version
Message	Real-time protection is enabled.
Name	MALWAREPROTECTION_RTP_ENABLED

Event 5001

ArcSight Field	Vendor Field
Device Version	Product Version
Message	Real-time protection is disabled.
Name	MALWAREPROTECTION_RTP_DISABLED

Event 5004

ArcSight Field	Vendor Field
Device Custom Number	"Configuration"
Device Custom Number1 Label	Configuration
Device Version	Product Version
File Hash	Feature Name
File ID	Feature ID
Message	The real-time protection configuration changed.
Name	MALWAREPROTECTION_RTP_FEATURE_CONFIGURED

Event 5007

ArcSight Field	Vendor Field
Device Version	Product Version
File Name	"New Value"
Message	The antimalware platform configuration changed.
Name	MALWAREPROTECTION_CONFIG_CHANGED
Old File Name	Old Value

Event 5009

ArcSight Field	Vendor Field
Name	MALWAREPROTECTION_ANTISPYWARE_ENABLED
Message	Scanning for malware and other potentially unwanted software is enabled.
Device Version	Product Version

Event 5010

ArcSight Field	Vendor Field
Device Version	Product Version
Message	Scanning for malware and other potentially unwanted software is disabled.
Name	MALWAREPROTECTION_ANTISPYWARE_DISABLED

Event 5011

ArcSight Field	Vendor Field
Name	MALWAREPROTECTION_ANTIVIRUS_ENABLED
Message	Scanning for viruses is enabled.
Device Custom String 1 Label	“Product Version”
Device Custom String 1	Product Version

Event 5012

ArcSight Field	Vendor Field
Device Version	Product Version
Message	Scanning for viruses is disabled.
Name	MALWAREPROTECTION_ANTIVIRUS_DISABLED

Event 5013

ArcSight Field	Vendor Field
Name	Tamper protection blocked a change to Microsoft Defender Antivirus.
Message	Tamper protection blocked a change to Microsoft Defender Antivirus.
Device Version	Product Version
File Name	Value

Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user ',%2,' has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port ',%2,' has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user ',%3,' connected on port ',%4,', does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),' has connected and has been successfully authenticated on port ',One of (%3,%4),' . Data sent and received over this link is strongly encrypted.')

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user ',%2,' connected on port ',%3,', on ',%4,', at ',%5,', and disconnected on ',%6,', at ',%7,'. The user was active for ',%8,' minutes, ',%9,' seconds, ',%10,' bytes were sent and ',%11,' bytes were received. The reason for disconnecting was ',%12,. The tunnel used was ',%13,'. The quarantine state was ',%14,'.)

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID

ArcSight Field	Vendor Field
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user ',%2,' connected on port ',%3,', has been assigned address ',%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both ('The user with ip address ',%2,', has disconnected')

Microsoft Windows ESENT

This section has the following event mapping information:

Microsoft Windows ESENT

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'ESENT'
Device Version	'Unknown'

Event 102

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine is starting a new instance

Event 103

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine stopped the instance

Event 105

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine started a new instance

Event 224

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4 to %5
Name	Deleting log files

Event 225

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	No log files can be truncated

Event 300

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
Name	The database engine is initiating recovery steps

Event 301

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
File Type	%6
Device Custom String 1	%7
Device Custom String 1 Label	Number of times log record seen
Name	The database engine has finished replaying log file

Event 302

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2

ArcSight Field	Vendor Field
Source Process Name	%3
Name	The database engine has successfully completed recovery steps

Event 325

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine created a new database"
Source Process Id	%2
Source Service Name	%1

Event 326

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine attached a database"
Source Process Id	%2
Source Service Name	%1
Source Process Name	%3

Event 327

ArcSight Field	Vendor Field
File Path	%5
Name	"The database engine detached a database"
Source Process Id	%2
Source Service Name	%1

Event 330

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2

ArcSight Field	Vendor Field
Source Process Name	%3
File Name	%4
Device Custom String 4	%7
Device Custom String 4 Label	Default engine version
Name	The database format version is being held back

Event 335

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%5
Reason	%7
Name	Replay of a create for database at log position was deferred

Event 455

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2
Source Process Name	%3
File Name	%4
Device Custom String 4	%5
Device Custom String 4 Label	Error
Name	Error occurred while opening log file

Event 641

ArcSight Field	Vendor Field
Source Service Name	%1
Source Process Id	%2

ArcSight Field	Vendor Field
Source Process Name	%3
Device Custom String 4	%5
Device Custom String 4 Label	Log format version
Device Custom String 5	%6
Device Custom String 5 Label	Current log format version
Name	The log format feature version could not be used

Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user ',%2,', has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port ',%2,', has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)

ArcSight Field	Vendor Field
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),', has connected and has been successfully authenticated on port ',One of (%3,%4),'. Data sent and received over this link is strongly encrypted.)'

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)

ArcSight Field	Vendor Field
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user ',%2,' connected on port ',%3,' on ',%4,' at ',%5,' and disconnected on ',%6,' at ',%7,'. The user was active for ',%8,' minutes, ',%9,' seconds, ',%10,' bytes were sent and ',%11,' bytes were received. The reason for disconnecting was ',%12,. The tunnel used was ',%13,. The quarantine state was ',%14,'.)

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user ',%2,' connected on port ',%3,' has been assigned address ',%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both ('The user with ip address ',%2,' has disconnected')

Specific Windows Security Event Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

104

ArcSight ESM Field	Device-Specific Field
Name	'The log file was cleared'
Message	concatenate('The ','Channel,' log file was cleared')
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName
File Type	Channel
File Path	BackupPath

1100

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

1101

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

1102

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

1104

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

1105

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

Event Mappings for Microsoft Windows Hyper V

Event 1

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Hypervisor
Name	The Hyper-V Hypervisor has started

Event 2

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Hypervisor
Name	The VM and host networking components failed to negotiate protocol version

Event 129

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Hypervisor
Name	Reset to device

Event 155

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Hypervisor
Name	The Diagnostic Policy service was stopped

Event 156

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Hypervisor
Name	Initial page allocation NUMA policy NUMA distribution disabled

Event 3086

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	The repository has logged performance summary

Event 3452

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Virtual machine failed to stop The device is not ready for use

Event 12006

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Unable to Connect: Windows is unable to connect to the automatic updates service

Event 12010

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Failed to power on with Error

Event 12030

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Failed to start

Event 12148

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-SynthStor
Name	Virtual machine started successfully

Event 12514

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Found a certificate for server authentication. Remote access to virtual machines is now possible.

Event 12520

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Auto-generating a self-signed certificate for server authentication

Event 12582

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-SynthNic
Name	Virtual machine started successfully

Event 12597

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Network adapter (%NIC_ID%) Connected to virtual network

Event 13002

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	A new virtual machine was created

Event 13003

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	The virtual machine was deleted

Event 14070

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Switch set up failed

Event 14090

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Virtual Machine Management service is shutting down while some virtual machines begin running

Event 14092

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Virtual Machine Management service is being shut down

Event 14094

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Hyper-V Virtual Machine Management service started successfully

Event 14100

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Shutting down physical computer. Stopping/saving all virtual machines

Event 14104

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	The Virtual Machine Management service is waiting for a servicing operation (servicing) to complete

Event 14108

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Unable to open handle to switch driver

Event 15266

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Failed to create virtual hard disk

Event 15310

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Created configuration store for '%1'

Event 18304

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	The virtual machine was realized

Event 18500

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Virtual machine started successfully

Event 18502

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Virtual machine was turned off

Event 18504

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Virtual machine was shut down by a user or process

Event 18508

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Virtual Machine Shut Down by Guest Operating System

Event 18510

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Virtual Machine Saved Successfully

Event 18512

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Virtual Machine Reset by Host

Event 18514

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Virtual Machine Reset by Guest Operating System

Event 18596

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	Virtual machine was restored successfully

Event 18600

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Chipset
Name	Virtual machine has encountered a watchdog timeout and was reset

Event 18602

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	VM has encountered a fatal error and a memory dump has been generated

Event 18609

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-Worker
Name	(VM Name) properties were successfully initialized

Event 19020

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	The WMI provider has started

Event 19040

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	The WMI provider has shut down

Event 20410

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Successfully started the Virtual Machine migration connection manager

Event 20790

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Failed to set security information for

Event 22052

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Live migrations can be enabled only on a domain joined computer

Event 26000

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Switch created, name

Event 26002

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Switch deleted, name

Event 26004

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Switch port created, switch name

Event 26006

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Switch port deleted, switch name

Event 26012

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Internal miniport created

Event 26016

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	External ethernet port

Event 26018

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	External ethernet port

Event 26026

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Internal miniport deleted

Event 26074

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Ethernet switch port connected

Event 26078

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Ethernet switch port disconnected

Event 27262

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	The system failed to create

Event 33012

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Could not find Ethernet switch

Event 33201

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Hyper-V Setup Remote management has been successfully enabled for members of the 'Hyper-V Administrators' group

Event 33205

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Hyper-V Setup Default Virtual Machine and Virtual Hard Disk paths have been successfully configured

Event 33452

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Replication health limits

Event 33454

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Replication health limits

Event 33456

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Replication

Event 33458

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Replication

Event 33480

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Change tracking has defined following limits for free disk space

Event 33481

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Change tracking has defined following limits for pending log file size

Event 33483

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Incremental Replication will timeout after 360 hours

Event 33834

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	Hyper-V would age out CDP reference points after 720 hours

Event 36000

ArcSight Field	Vendor Field
Device Product	Microsoft-Windows-Hyper-V-VMMS
Name	The repository has logged performance summary name

Windows PowerShell Mappings

Event 400, 403

ArcSight Field	Vendor Field
Name	'Engine state is changed'
Message	'Engine state is changed from',%2,'to',%1
File Hash	%1
Old FileHash	%2

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ', HostName,', Host Version: ',HostVersion,', Host ID: ',HostId)(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Path	CommandPath
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Event 500, 501

ArcSight Field	Vendor Field
Name	'Command State'
Message	'Command "','"%1,"' is ',%2
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ', HostName,', Host Version: ',HostVersion,', Host ID: ',HostId)(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Path	CommandPath
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Event 600

ArcSight Field	Vendor Field
Name	'Provider State'
Message	'Provider "%1," is "%2
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ', HostName, ' Host Version: ', HostVersion, ' Host ID: ', HostId)(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Path	CommandPath
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Event 800

ArcSight Field	Vendor Field
Name	'Pipeline execution details for command line'
Message	'Pipeline execution details for command line: ',%1
Device Custom String 1	%3(Details)
Device Custom Number 2	SequenceNumber(Sequence Number)
Device Custom String 4	All of ('Host Name: ', HostName, ' Host Version: ', HostVersion, ' Host ID: ', HostId)(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
Old File Name	ScriptName

ArcSight Field	Vendor Field
File Permission	CommandLine
Source NT Domain	UserId
Source User Name	UserId

Windows Microsoft-Windows-PowerShell/Operational Mappings

Event 4100

ArcSight Field	Vendor Field
Name	'Error Message'
Device Custom String 1	UserData(User Data)
Device Severity	Severity
Device Custom String 4	All of ('Host Name:', 'Host Name', 'Host Version:', 'Host Version', 'Host ID:', 'Host Id')(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	CommandName
File Type	CommandType
Old File Name	ScriptName
File Permission	CommandLine
Device Custom Number 2	SequenceNumber(Sequence Number)
Source NT Domain	User
Source User Name	User
Device Custom String 6	Connected User(Connected User)
Request Context	Shell ID
Message	Error Message, ' ', Recommended Action
Reason	Fully Qualified Error ID

Event 4103

ArcSight Field	Vendor Field
Name	'Command Invocation'
Message	Payload
Device Custom String 1	UserData(User Data)
Device Severity	Severity
Device Custom String 4	All of ('Host Name:', 'Host Name,' , Host Version: ', 'Host Version,' , Host ID: ', 'Host Id)(Host Information)
Request Client Application	HostApplication
Old File Id	RunspaceId
Device Custom Number 1	PipelineId(Pipeline ID)
File Name	Command Name
File Type	Command Type
Old File Name	Script Name
File Path	Command Path
File Permission	Command Line
Device Custom Number 2	SequenceNumber(Sequence Number)
Source NT Domain	User
Source User Name	User
Device Custom String 6	Connected User(Connected User)
Request Context	Shell ID

Event 4104

ArcSight Field	Vendor Field
Name	'Creating Scriptblock text'
Message	'Creating Scriptblock text(' , 'MessageNumber,' , ' of ' , 'MessageTotal,' , '\'):' , 'ScriptBlockText
Device Custom Number 1	MessageNumber(Message Number)
Device Custom Number 2	Message Total
File Name	ScriptBlockText
File Path	Path

Event 4105

ArcSight Field	Vendor Field
Name	'Started invocation of ScriptBlock'
Message	'Started invocation of ScriptBlock ID',ScriptBlockId
File ID	ScriptBlockId
Old File ID	RunspaceId

Event 8193

ArcSight Field	Vendor Field
Name	'Creating Runspace object'
Message	'Creating Runspace object Instance Id:',param1
Device Custom String 5	param1(Instance Id)

Event 8194

ArcSight Field	Vendor Field
Name	'Creating RunspacePool object'
Message	'Creating RunspacePool object Instance Id:',InstanceId
Device Custom String 5	param1(Instance Id)
Device Custom Number 1	MaxRunspaces(Max Runspaces)
Device Custom Number 2	MinRunspaces(Min Runspaces)

Event 8195

ArcSight Field	Vendor Field
Name	'Opening RunspacePool'
Message	'Opening RunspacePool'

Event 8196, 12039

ArcSight Field	Vendor Field
Name	'Modifying activity Id and correlating'
Message	'Modifying activity Id and correlating'

Event 8197

ArcSight Field	Vendor Field
Name	'Runspace state changed'
Message	'Runspace state changed to ',param1
Device Action	param1

Event 24577

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE has started to run script file'
Message	'Windows PowerShell ISE has started to run script file ',FileName
File Path	FileName

Event 24579

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stopping the current command'
Message	'Windows PowerShell ISE is stopping the current command'

Event 24580

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is resuming the debugger'
Message	'Windows PowerShell ISE is resuming the debugger'

Event 24581

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stopping the debugger'
Message	'Windows PowerShell ISE is stopping the debugger'

Event 24582

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stepping into debugging'
Message	'Windows PowerShell ISE is stepping into debugging'

Event 24583

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stepping over debugging'
Message	'Windows PowerShell ISE is stepping over debugging'

Event 24584

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is stepping out of debugging'
Message	'Windows PowerShell ISE is stepping out of debugging'

Event 24592

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is enabling all breakpoints'
Message	'Windows PowerShell ISE is enabling all breakpoints'

Event 24593

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is disabling all breakpoints'
Message	'Windows PowerShell ISE is disabling all breakpoints'

Event 24594

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is removing all breakpoints'
Message	'Windows PowerShell ISE is removing all breakpoints'

Event 24595

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is setting the breakpoint'
Message	'Windows PowerShell ISE is setting the breakpoint at line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24596

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is removing the breakpoint'
Message	'Windows PowerShell ISE is removing the breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24597

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is enabling the breakpoint'
Message	'Windows PowerShell ISE is enabling the breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24598

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE is disabling the breakpoint'
Message	'Windows PowerShell ISE is disabling the breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 24599

ArcSight Field	Vendor Field
Name	'Windows PowerShell ISE has hit a breakpoint'
Message	'Windows PowerShell ISE has hit a breakpoint on line #: ',CurrentLine,' of file ',FileName
Device Custom Number 3	CurrentLine(Current Line)
File Path	FileName

Event 40961

ArcSight Field	Vendor Field
Name	'PowerShell console is starting up'
Message	'PowerShell console is starting up'

Event 40962

ArcSight Field	Vendor Field
Name	'PowerShell console is ready for user input'
Message	'PowerShell console is ready for user input'

Event 53249

ArcSight Field	Vendor Field
Name	'Scheduled Job started'
Message	'Scheduled Job ',ScheduledJobDefName,' started at ',StartTime
Device Custom String 1	ScheduledJobDefName(Scheduled Job Name)
Start Time	Start Time

Event 53250

ArcSight Field	Vendor Field
Name	'Scheduled Job completed'
Message	'Scheduled Job ',ScheduledJobDefName,' completed at ',StopTime,' with state ',State
Device Custom String 1	ScheduledJobDefName(Scheduled Job Name)
End Time	StopTime
Device Action	State

Event 53504

ArcSight Field	Vendor Field
Name	'Windows PowerShell has started an IPC listening thread'
Message	'Windows PowerShell has started an IPC listening thread on process: ',param1,' in AppDomain: ',param2
Destination Process Id	param1
Device Custom String 1	param2(App Domain)

Microsoft Windows Update Client

This section has the following information

Windows 2012

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft-Windows-WindowsUpdateClient'

Event 16

ArcSight Field	Vendor Field
Name	'Unable to Connect: Windows is unable to connect to the automatic updates service'

Event 17

ArcSight Field	Vendor Field
Name	'Installation Ready: The following updates are downloaded and ready for installation'

Event 18

ArcSight Field	Vendor Field
Name	'Installation Ready : The updates are downloaded and scheduled for installation'
Device Custom String 4 Label	stringConstant("Scheduled Install Date")
Device Custom String 4	schedinstalldate
Device Custom String 5 Label	stringConstant("Scheduled Install Time")
Device Custom String 5	schedinstalltime
Device Custom String 6 Label	stringConstant("Update List")
Device Custom String 6	updatelist

Event 19

ArcSight Field	Vendor Field
Name	'Installation Successful: Window successfully installed the updates'
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant ("Update Revision Number")

Event 20

ArcSight Field	Vendor Field
Name	Installation Failure: Windows failed to install the Updates
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant ("Update Revision Number")

Event 21

ArcSight Field	Vendor Field
Name	Restart Required : The computer must be restarted
Device Custom String 6 Label	stringConstant("Update List")
Device Custom String 6	updatelist

Event 22

ArcSight Field	Vendor Field
Device Custom String 6	updatelist
Device Custom String 6 Label	__stringConstant (Update List)
Name	Restart Required : The computer will be restarted

Event 27

ArcSight Field	Vendor Field
Name	Automatic Updates is now paused

Event 28

ArcSight Field	Vendor Field
Name	Automatic Update is now resumed

Event 43

ArcSight Field	Vendor Field
Name	Installation Started: Windows has started installing the updates
Device Custom String 4 Label	stringConstant("Update Title")
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant ("Update Revision Number")

Event 44

ArcSight Field	Vendor Field
Name	Downloading Started: Windows Update started downloading an update
Device Custom String 4 Label	stringConstant("Update Title")

ArcSight Field	Vendor Field
Device Custom String 4	updateTitle
Device Custom String 5 Label	stringConstant("Update Guid")
Device Custom String 5	updateGuid
Device Custom Number3	safeToLong(updateRevisionNumber)
Device Custom Number3 Label	If updateRevisionNumber is blank set Label blank else stringConstant ("Update Revision Number")

Windows 2008 R2

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

Event 20088

ArcSight Field	Vendor Field
Name	Remote Access Server acquired IP Address
Destination Address	%1 (Assigned Address)
Message	Both ('The Remote Access Server acquired IP Address ',%1,' to be used on the Server Adapter.')

Event 20106

ArcSight Field	Vendor Field
Name	Unable to add interface
Device Outbound Interface	%1 (Interface)
Application Protocol	%2 (Protocol)
Message	%3 (Message Text)

Event 20184

ArcSight Field	Vendor Field
Name	Interface is unreachable
Device Inbound Interface	%1 (Interface)
Message	Both ('Interface ',%1,' is unreachable because it is not currently connected to the network.')

Event 20249

ArcSight Field	Vendor Field
Name	Failed to authenticate
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Message	Both ('The user ',%2,', has connected and failed to authenticate on port ',%3,'. The line has been disconnected.')

Event 20252

ArcSight Field	Vendor Field
Name	Authentication process did not complete
Device Custom String 4	Correlation-ID
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	Both ('The user connected to port ',%2,', has been disconnected because the authentication process did not complete within the required amount of time.')

Event 20255

ArcSight Field	Vendor Field
Name	Connection was prevented
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%2 (Protocol)
Source Port	%2 (Port)
Message	%4 (Message Text)

Event 20258

ArcSight Field	Vendor Field
Name	Account does not have Remote Access privilege
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The account for user ',%3,' connected on port ',%4,' does not have Remote Access privilege. The line has been disconnected.')

Event 20266

ArcSight Field	Vendor Field
Name	Successfully authenticated
Device Custom String 4	Correlation-ID
Source User Name	%3 (Connected User)
Source NT Domain	%3 (Domain of Connected User)

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Application Protocol	%4 (Protocol)
Source Port	%4 (Port)
Message	Both ('The user ',One of (%2,%3),', has connected and has been successfully authenticated on port ',One of (%3,%4),'. Data sent and received over this link is strongly encrypted.)'

Event 20271

ArcSight Field	Vendor Field
Name	Failed an authentication attempt
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Source Address	%3 (Address)
Reason	%5 (Reason)
Message	%4 (Message Text)

Event 20272

ArcSight Field	Vendor Field
Name	User connected and disconnected
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Start Time	Both (%4, %5)
End Time	Both (%5, %6)
Device Custom Number 1	User active minutes
Device Custom Number 2	User active seconds
Bytes Out	%10 (Bytes Out)
Bytes In	%10 (Bytes In)

ArcSight Field	Vendor Field
Additional data	%12
Additional data	%13
Additional data	%14
Message	Both ('The user ',%2,' connected on port ',%3,' on ',%4,' at ',%5,' and disconnected on ',%6,' at ',%7,'. The user was active for ',%8,' minutes, ',%9,' seconds, ',%10,' bytes were sent and ',%11,' bytes were received. The reason for disconnecting was ',%12,. The tunnel used was ',%13,. The quarantine state was ',%14,'.)

Event 20274

ArcSight Field	Vendor Field
Name	User connected and has been assigned address
Device Custom String 4	Correlation-ID
Source User Name	%2 (Connected User)
Source NT Domain	%2 (Domain of Connected User)
Application Protocol	%3 (Protocol)
Source Port	%3 (Port)
Destination Address	%4 (Assigned Address)
Message	Both ('The user ',%2,' connected on port ',%3,' has been assigned address ',%4')

Event 20275

ArcSight Field	Vendor Field
Name	User disconnected
Device Custom String 4	Correlation-ID
Source Address	%2 (Address)
Message	Both ('The user with ip address ',%2,' has disconnected')

Microsoft Windows WMI Activity Trace

Event 11

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	Microsoft Windows WMI Activity Trace
Name	WMI-Activity Query executed on Win23 BIOS
Device Custom String 1	ClientMachineFQDN
Device Custom String 3	CorrelationId
Device Custom String 4	IsLocal
Device Custom String 5	Operation
Device Custom Number 1	OperationId
Device Custom Number 2	GroupOperationId
Source Host Name	ClientMachine
Source User Name	User
Source Process Id	ClientProcessId
File Create Time	ClientProcessCreationTime
File Path	NamespaceName

Microsoft Windows WinRM Analytic

Event 6

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	Creating WSMAN Session
File Path	connection

Event 11

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	Creating WSMAN Shell
File Id	shellId

Event 15

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	WSMan Command

Event 142

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	WSMan Operation Identify Failed
Device Action	operationName
Device Custom Number 3	errorCode
Device Custom Number 3 Label	Error Code

Event 161

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	WinRM Cannot Process The Request
Message	authFailureMessage

Event 162

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	Authenticating The User Failed

Event 169

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	The Message Resource Is Present But The Message Was Not Found In The Message Table
Destination User Name	username
Request Method	authenticationMechanism

Event 81

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	The Message Resource Is Present But The Message Was Not Found In The Message Table
Device Action	operationName

Event 82

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	The Message Resource Is Present But The Message Was Not Found In The Message Table
Device Action	operation
Request Url	resourceURI

Windows 2012

Event 788

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	Processing Client Request For Operation
Device Action	operationName

Event 789

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	The Plugin For Operation
Device Action	resourceUrl.

Event 1050

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	Response For Operation
Device Action	operationName

Event 1295

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Windows Remote Management'
Name	User Authenticated Successfully
Destination User Name	username

Windows 2016, 2012, and 8

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'
Device Custom String 4	Reason or Error Code

Event 4097

ArcSight Field	Vendor Field
Name	'WINS initialized properly and is now fully operational'

Event 4098

ArcSight Field	Vendor Field
Name	'WINS was terminated by the service controller'
Message	'WINS will gracefully terminate'

Event 4119

ArcSight Field	Vendor Field
Name	'WINS received a packet that has the wrong format'

Event 4143

ArcSight Field	Vendor Field
Name	'WINS scavenged its records in the WINS database'
Message	'The number of records scavenged is given in the data section'

Event 4178

ArcSight Field	Vendor Field
Name	'The WINS Pull configuration key could not be created or opened'
Message	'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

Event 4179

ArcSight Field	Vendor Field
Name	'The WINS Push configuration key could not be created or opened'
Message	'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

Event 4180

ArcSight Field	Vendor Field
Name	'The WINS\\Parameters key could not be created or opened'
Message	'Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

Event 4181

ArcSight Field	Vendor Field
Name	'# The subkey could not be created or opened'
Message	'This key should be there if you want WINS to do consistency checks on its database periodically. NOTE: Consistency checks have the potential of consuming large amounts of network bandwidth. Check to see if the permissions on the key are set properly, system resources are low, or the registry is having a problem'

Event 4224

ArcSight Field	Vendor Field
Name	'WINS encountered a database error'
Message	'This may or may not be a serious error. WINS will try to recover from it'

Event 4252

ArcSight Field	Vendor Field
Name	'WINS did not find any subkeys under the Pull key'

Event 4253

ArcSight Field	Vendor Field
Name	'WINS did not find any subkeys under the Push key'

Event 4309

ArcSight Field	Vendor Field
Name	'System Resource Information'
Device Custom Number 1	Processor Count
Device Custom Number 2	Physical Memory
Device Custom Number 3	Memory available for allocation

Event 4318

ArcSight Field	Vendor Field
Name	'WINS could not start due to a missing or corrupt database'
Message	'Restore the database using WINS Manager (or winscl.exe found in the Windows 2000 Resource Kit) and restart WINS'

Event 4325

ArcSight Field	Vendor Field
Name	'WINS could not read the Initial Challenge Retry Interval from the registry'

Event 4326

ArcSight Field	Vendor Field
Name	'WINS could not read the Challenge Maximum Number of Retries from the registry'

Event 4329

ArcSight Field	Vendor Field
Name	'The WINS server has started a scavenging operation'

Event 4330

ArcSight Field	Vendor Field
Name	'The WINS server has completed the scavenging operation'

Event 4337

ArcSight Field	Vendor Field
Name	'WINS Server could not initialize security to allow the read-only operations'

Event 5001

ArcSight Field	Vendor Field
Name	'WINS is scavenging the locally owned records from the database'
Message	'The version number range that is scavenged is given in the data section, in the second to fifth words, in the order: from_version_number (low word, high word) to_version_number (low word, high word)'

Event 5002

ArcSight Field	Vendor Field
Name	'WINS is scavenging a chuck on N records in the version number range from X to Y'
Message	'N, X and Y (low word, high word for version numbers) are given in the second to sixth words in the data section'

Oracle Audit

The following section lists the mappings of ArcSight data fields to the device's specific event definitions:

Oracle Windows Event

General

ArcSight ESM Field	Device-Specific Field
Source Service Name	EventSource
Device Vendor	'Oracle'

Event 4

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('Initializing SGA for instance ',%1)
Name	'Initializing SGA for instance'

Event 5

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	'Both ('Initializing SGA for process ',%1,' in instance ',%2)
Name	'Initializing SGA for process in instance'
Destination Process Name	%1 (Destination Process Name)

Event 8

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('Shutdown normal performed on instance ',%1)
Name	'Shutdown normal performed on instance'

Event 12

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Instance Name
Device Product	'Oracle'
Message	Both ('All process in instance ',%1,' stopped')
Name	'All process in instance stopped'

Oracle Audit SYSDBA

Event 34

ArcSight ESM Field	Device-Specific Field
Destination Process Name	ProcessId
Destination User Name	DATABASE USER
Destination User Privileges	PRIVILEGE
Device Action	first word from ACTION
Device Custom Number 1	STATUS
Device Custom String 6	CLIENT TERMINAL
Device Event Class Id	first word of ACTION
Device External ID	DBID
Device Product	'ORACLESYSDBA'
Device Vendor	'ORACLE'
Message	first word from ACTION
Name	first word from ACTION
Source Host Name	CLIENT TERMINAL
Source User Name	CLIENT USER

Oracle Audit Trail

Event 34

ArcSight ESM Field	Device-Specific Field
Additional data	LOGOFF_DEAD
Additional data	LOGOFF_LREAD
Additional data	LOGOFF_LWRITE
Additional data	LOGOFF_PREAD
Additional data	OBJ_CREATOR
Additional data	SESSIONCPU
Additional data	SES_TID
Additional data	STATEMENT
Destination Host Name	USERHOST
Destination NT Domain	USERHOST
Destination Process Name	ProcessId
Destination User Name	USERID
Destination User Privileges	PRIV_USED
Device Action	ACTION
Device Custom Number 1	RETURNCODE
Device Custom Number 2	SESSIONID
Device Custom Number 3	ENTRYID
Device Custom String 1	COMMENT_TEXT
Device Custom String 2	TERMINAL
Device Custom String 4	SES_LABEL
Device Custom String 5	SES_ACTIONS
Device Event Class Id	ACTION
Device External ID	DBID
Device Product	'Oracle'
Device Severity	RETURNCODE
Device Vendor	'ORACLE'

ArcSight ESM Field	Device-Specific Field
File Name	Object name
Name	ACTION
Source Address	extracted IP address from SES_LABEL (will auto map to Source Host Name)
Source NT Domain	OSSUSERID
Source User Name	OS_USERID
Reason	RETURNCODE
Transport Protocol	PROTOCOL
Device Custom IPv6 Address 2	Source IPv6 Address
File Name	Name
Source Port	Port

Oracle Unified Audit Trail

Event 36

ArcSight ESM Field	Device-Specific Field
Device External ID	DBID
Device Custom Number 2	SESID
Device Custom Number 3	ENTRYID
Destination User Name	DBUSER
Source User Name	CURUSER
Device Action	ACTION
Name	ACTION
Device Custom Number 1	RETCODE
Reason	RETCODE
Device Event Class Id	ACTION
File Name	OBJNAME
Device Product	'Oracle'
Device Custom String 3	SCHEMA
Old File ID	CLIENTID

Symantec Mail Security Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Symantec'
Device Product	'MailSecurity for Microsoft Exchange''

Managed Components

Event 0

ArcSight Field	Vendor Field
Name	'Insufficient rightstoaccessthisapplication'

Management Service

Event 1

ArcSight Field	Vendor Field
Name	'Service'
Message	

Event 2

ArcSight Field	Vendor Field
Name	'Threat Event Feed'
Message	

Event 3

ArcSight Field	Vendor Field
Name	'Computer State Feed'
Message	

Event 4

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Device Action	'Stopped'
Name	Service Stopped

Event 5

ArcSight Field	Vendor Field
Device Action	'Started'
Name	Service started

Event 6

ArcSight Field	Vendor Field
Name	'Settings'
Message	

Event 7

ArcSight Field	Vendor Field
Name	'Unable to get Product Computer Key'

Event 8

ArcSight Field	Vendor Field
Name	'Server Feed'
Message	

Event 9

ArcSight Field	Vendor Field
DestinationService Name	'SymantecMailSecurity Management'
Name	'Waiting for synchronization'
Message	'Waiting for synchronization with SymantecMailSecurity Management Service Plug-in'

Event 10

ArcSight Field	Vendor Field
Name	'Achieved synchronization with SymantecMailSecurity Management Service Plug-in'

Event 11

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'MonitoringSymantecMailSecurity Management Service Plug-in'

Event 12

ArcSight Field	Vendor Field
Name	'SymantecMailSecurity Management Service Plug-inUnavailable'

Event 50

ArcSight Field	Vendor Field
Name	'Threat Event FeedEnabled'

Event 51

ArcSight Field	Vendor Field
Name	'Threat Event FeedDisabled'

Event 102, 152, 212

ArcSight Field	Vendor Field
Name	'Failedtoreadconfigurationfromregistry'
Message	'Registry=', 'Usingdefault value ='

Event 53

ArcSight Field	Vendor Field
Name	'Failedtoupdate the registry'
Message	

Event 54

ArcSight Field	Vendor Field
Name	'Unable toreaddatabase locationfromregistry'
Message	

Event 60

ArcSight Field	Vendor Field
Name	'Nodata available tosend'
Message	

Event 63

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'FailedtoOpenThreat Event FeedRegistry Key'
Message	'CreatedNew Threat Event FeedRegistry Key'

Event 100

ArcSight Field	Vendor Field
Name	'Computer State FeedEnabled'

Event 101

ArcSight Field	Vendor Field
Name	'Computer State FeedDisabled'

Event 103

ArcSight Field	Vendor Field
Name	'Failedtoupdate the registry'

Event 104

ArcSight Field	Vendor Field
Name	'Unable toget VirusDefinitionVersion'
Message	

Event 105

ArcSight Field	Vendor Field
Name	'Computer State FeedSent'
Message	

Event 150

ArcSight Field	Vendor Field
Name	'Computer Data FeedEnabled'

Event 151

ArcSight Field	Vendor Field
Name	'Computer Data FeedDisabled'

Event 153

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'Failedtoupdate the registry'
Message	

Event 154

ArcSight Field	Vendor Field
Name	'Unable to get OSDetails'
Message	

Event 155

ArcSight Field	Vendor Field
Name	'Unable to get Adapter Details'
Message	

Event 156

ArcSight Field	Vendor Field
Name	'Unable to get Machine Details'
Message	

Event 157

ArcSight Field	Vendor Field
Name	'Computer Data FeedSent'
Message	

Event 202

ArcSight Field	Vendor Field
Name	'NTEvent Logfull'
Message	'Unable to record events'

Event 203

ArcSight Field	Vendor Field
Name	'Failedtoinitialize Server Feed'
Message	

Event 204

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'Unable toIntialize COM for Server Feed'
Message	

Event 205

ArcSight Field	Vendor Field
Name	'Server FeedisDisabled'

Event 206

ArcSight Field	Vendor Field
Name	'Server FeedisEnabled'
Message	

Event 207

ArcSight Field	Vendor Field
Name	'Unable toget SMSMSE Service StatusField'

Event 208

ArcSight Field	Vendor Field
Name	'Unable toget SMSMSE Service ScanStatusField'
Message	

Event 209

ArcSight Field	Vendor Field
Name	'Unable toget currently SMSMSE VirusDefinitionandRevisionField'
Message	

Event 210

ArcSight Field	Vendor Field
Name	'Server FeedSent'
Message	

Event 211

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Name	'Unable to get SMSMSE VirusDefinitionLicence InformationField'
Message	

Event 213

ArcSight Field	Vendor Field
Name	'Unable to get SMSMSE Server Name Field'
Message	

Event 214

ArcSight Field	Vendor Field
Name	'Unable to get Exchange Server InstalledRolesField'
Message	

Event 215

ArcSight Field	Vendor Field
Name	'Unable to get InstalledSMSMSE VersionField'
Message	

Event 216

ArcSight Field	Vendor Field
Name	'Unable to get InstalledExchange VersionField'
Message	

Event 217

ArcSight Field	Vendor Field
Name	'Unable to get InstalledExchange DomainName Field'
Message	

Event 221

ArcSight Field	Vendor Field
Name	'Unable to get currently SMSMSE VirusRevisionField'
Message	

Microsoft Exchange

Event 1

ArcSight Field	Vendor Field
Name	'Auto-Protect'
Message	

Event 2

ArcSight Field	Vendor Field
Name	'LiveUpdate/RapidRelease'
Message	

Event 3

ArcSight Field	Vendor Field
Name	'ManualandScheduledScanning'
Message	

Event 4

ArcSight Field	Vendor Field
Device Action	'enabled'
Name	'Auto-Protect enabled'

Event 5

ArcSight Field	Vendor Field
Device Action	'disabled'
Name	'Auto-Protect disabled'

Event 6

ArcSight Field	Vendor Field
Name	'Auto-Protect optionschanged'
Message	

Event 7

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Name	'Settings'
Message	

Event 8

ArcSight Field	Vendor Field
Name	'VSAPI'
Message	

Event 9

ArcSight Field	Vendor Field
Name	'Error'
Message	

Event 14

ArcSight Field	Vendor Field
Name	'StartedScan'
Message	Both('StartedScan: ',%1)
Device Action	'Started'
Device CustomString5	ScanType

Event 15

ArcSight Field	Vendor Field
Name	'Property Violation'
Message	

Event 16

ArcSight Field	Vendor Field
Name	'Unscannable'
Message	

Event 17

ArcSight Field	Vendor Field
Name	'Console Remote Install'
Message	

Event 19

ArcSight Field	Vendor Field
Name	'Console LiveUpdate'
Message	

Event 20

ArcSight Field	Vendor Field
Name	'Heartbeat'
Message	

Event 21

ArcSight Field	Vendor Field
Name	'stopped'
Message	

Event 22

ArcSight Field	Vendor Field
Name	'Removedfilesfromquarantine'
Message	Both('Removed','%1,' file(s)fromquarantine')
Device Action	'Removed'

Event 23

ArcSight Field	Vendor Field
Name	'Globaloptionschanged'
Message	

Event 24

ArcSight Field	Vendor Field
Name	'Reset scanningstatistics'
Message	

Event 25

ArcSight Field	Vendor Field
Device Action	'Updated'

Event 26

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'BackgroundScanning'
Message	

Event 28

ArcSight Field	Vendor Field
Name	'Service failedtostart'
Message	'Service failedtostart. Checkthe logfor other errors'

Event 29

ArcSight Field	Vendor Field
Name	'Unable torecordevents'
Message	'NTEvent Logfull.Unable torecordevents'

Event 30

ArcSight Field	Vendor Field
Name	'VirusDefinitionsUpdate wassuccessful'
Message	'New virusdefinitionswere retrieved'

Event 31

ArcSight Field	Vendor Field
Name	'LiveUpdate hasdeterminedthat noupdate isnecessary'
Message	'Youalready have the most recent virusdefinitions'

Event 33

ArcSight Field	Vendor Field
Name	'LiveUpdate wassuccessful'
Message	'LiveUpdate wassuccessful. New virusdefinitionswere retrieved. A systemrestart is requiredtouse them'

Event 37

ArcSight Field	Vendor Field
Name	'Globaloptionschanged'
Message	

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

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

Event 41

ArcSight Field	Vendor Field
Name	'Globaloptionschanged'
Message	

ArcSight ESM Field	Device-Specific Field
Name	'Out ofMemory'
Message	

Event 43

ArcSight Field	Vendor Field
Name	'Globaloptionschanged'
Message	

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

Event 45

ArcSight Field	Vendor Field
Name	'ScanEngine Failure'
Message	Both('Thiserror occurredwhile scanningthe attachment ',%4,' ofmessage ',%3,' locatedin ',%2)
Reason	%1 (reasoncode)
File Path	%2 (file path)
File Name	%4 (file name)
File Type	'attachment'
Additionaldata	%3 (subject)

Event 68

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'Unable to initialize ScanEngine'
Message	'The virusdefinitions may be missing or corrupt. Perform a LiveUpdate to retrieve the latest virusdefinitions'

Event 70

ArcSight Field	Vendor Field
Name	'The temporary directory specified in the registry value TempFileDir is invalid'
Message	

Event 71

ArcSight Field	Vendor Field
Name	'LiveUpdate retrieved new files but the virusdefinitions could not be updated'
Message	

Event 74

ArcSight Field	Vendor Field
Name	'Service cannot start since the service has already been started'
Message	

Event 75

ArcSight Field	Vendor Field
Name	'A serious problem with event logging has occurred but the service still started'
Message	

Event 76

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start due to the program settings could not be obtained or is invalid'

Event 77

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start due to low memory conditions'

Event 78

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start due to problems with virus scanning statistics'

Event 79

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot 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 Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start since due to the inability to monitor mailboxes and/or public folders'

Event 81

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start due to the inability to log onto the Exchange Server'

Event 82

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start due to the inability to create some SMS MSE objects'

Event 83

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start due to problems with Microsoft Exchange's public folders'

Event 84

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start due to the inability to obtain a list of mailboxes'

Event 85

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start since the Auto-Protect process could not be started'

Event 86

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start due to the inability to log on to mailboxes'

Event 87

ArcSight Field	Vendor Field
Name	'Service cannot start'
Message	'Service cannot start due to problems starting the SMSMSE engine'

Event 92

ArcSight Field	Vendor Field
Name	'The scan job was stopped'
Device Action	'Stopped'

Event 95

ArcSight Field	Vendor Field
Name	'Scan options changed'
Message	

Event 98

ArcSight Field	Vendor Field
Device Action	'Completed'
Name	'CompletedScan'

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

ArcSight Field	Vendor Field
Message	Both('CompletedScan: ',%1,' Violations: ',%3,' LogOnly: ',%4,' Quarantine attachment/message body: ',%7,' Delete attachment/message body: ',%8,' Delete message: ',%9,' Take noaction: ',%10)
Device CustomString5	ScanType
Additionaldata	numViolation
Additionaldata	logOnly
Additionaldata	numQuanrantine
Additionaldata	numDeleteAttachmentAndMessageBody
Additionaldata	numDeleteMessage
Additionaldata	numRepairAttachmentAndMessageBody
Additionaldata	numTakeNoAction

Event 99

ArcSight Field	Vendor Field
Name	'InterruptedScan'
Message	Both('InterruptedScan: ',%1,"Violations: ",%3,' LogOnly: ',%4,' Quarantine attachment/message body: ',%7,' Delete attachment/message body: ',%8,' Delete message: ',%9,' Take noaction: ',%10)
Device Action	'Interrupted'
Device CustomString5	ScanType
Additionaldata	numViolation
Additionaldata	logOnly
Additionaldata	numQuanrantine
Additionaldata	numDeleteAttachmentAndMessageBody
Additionaldata	numDeleteMessage
Additionaldata	numTakeNoAction

Event 107

ArcSight Field	Vendor Field
Name	'Service started'
Device Action	'started'

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Device CustomStirng2	Product Version

Event 110

ArcSight Field	Vendor Field
Name	'A processfailedtostart'
Message	Both('The process','%1,' failedtostart (',%2,')')
DestinationService Name	%1 (service name)
Reason	%2 (reasoncode)

Event 111

ArcSight Field	Vendor Field
Name	'Update ofinformationinheader offile failed'
Message	'Update ofinformationinheader offile faileddue torevisionclash'

Event 112

ArcSight Field	Vendor Field
Name	'EncryptedFile Header wasInvalidandcouldnot be read'
Message	

Event 113

ArcSight Field	Vendor Field
Name	'DeletionofQuarantinedfile failed'
Message	

Event 114

ArcSight Field	Vendor Field
Name	'Couldnot restore quarantinedfile'
Message	

Event 115

ArcSight Field	Vendor Field
Name	'Quarantinedfile containsheader fromolder versionofSMSMSE'
Message	

Event 116

ArcSight Field	Vendor Field
Name	'File decryptionfailed'
Message	

Event 117

ArcSight Field	Vendor Field
Name	'File encryptionfailed'
Message	

Event 118

ArcSight Field	Vendor Field
Name	'SAVFMSELinkpacket size doesnot matchdeclaredsize'
Message	

Event 119

ArcSight Field	Vendor Field
Name	'SAVFMSELinkpacket istoolarge'
Message	

Event 120

ArcSight Field	Vendor Field
Name	'The interface doesnot match'
Message	

Event 121

ArcSight Field	Vendor Field
Name	'The functionaskedfor isunknownor unsupported'
Message	

Event 122

ArcSight Field	Vendor Field
Name	'The data size isnot consistent withitsintendeduse'
Message	

Event 123

ArcSight Field	Vendor Field
Name	'The stringdata isnot consistent withitsintendeduse'
Message	

Event 124

ArcSight Field	Vendor Field
Name	'The suppliedbuffer istoosmallfor thisoperation'
Message	

Event 125

ArcSight Field	Vendor Field
Name	'The operationsucceededbut returnedanunexpectedresponse'
Message	

Event 126

ArcSight Field	Vendor Field
Name	'The file couldnot be written'
Message	

Event 127

ArcSight Field	Vendor Field
Name	'Internallogicerror'
Message	

Event 128

ArcSight Field	Vendor Field
Name	'Aninvalidconfigurationsettingisinuse'
Message	

Event 129

ArcSight Field	Vendor Field
Name	'The namedpipedcouldnot be opened'
Message	

Event 130

ArcSight Field	Vendor Field
Name	'The error occurred receiving a connection to the named pipe'
Message	

Event 131

ArcSight Field	Vendor Field
Name	'The error occurred flushing the contents of the pipe'
Message	

Event 132

ArcSight Field	Vendor Field
Name	'The error occurred disconnecting from the pipe'
Message	

Event 133

ArcSight Field	Vendor Field
Name	'The error occurred writing to the pipe'
Message	

Event 134

ArcSight Field	Vendor Field
Name	'The error occurred reading from the pipe'
Message	

Event 135

ArcSight Field	Vendor Field
Name	'A timeout occurred waiting for a response from the pipe'
Message	

Event 136

ArcSight Field	Vendor Field
Name	'A thread could not be created'
Message	

Event 137

ArcSight Field	Vendor Field
Name	'A thread did not end as expected'
Message	

Event 138

ArcSight Field	Vendor Field
Name	'The process could not be started'
Message	

Event 139

ArcSight Field	Vendor Field
Name	'The process was forcibly terminated'
Message	

Event 140

ArcSight Field	Vendor Field
Name	'The process could not be stopped'
Message	

Event 141

ArcSight Field	Vendor Field
Name	'The scan engine caused an exception'
Message	

Event 142

ArcSight Field	Vendor Field
Name	'The scan engine did not return any results for the scan'
Message	

Event 143

ArcSight Field	Vendor Field
Name	'The scan engine returned an error'
Message	

Event 144

ArcSight Field	Vendor Field
Name	'The process has initiated a shutdown'
Message	

Event 160

ArcSight Field	Vendor Field
Name	'The scan completed but errors were returned'
Message	

Event 161

ArcSight Field	Vendor Field
Name	'InternalError'
Message	'SAVFMSEVSAPI.DLL InternalError. An exception occurred calling JetGetTableColumnInfo'

Event 162

ArcSight Field	Vendor Field
Name	'InternalError'
Message	'SAVFMSEVSAPI.DLL InternalError. An exception occurred calling JetRetrieveColumn\'

Event 163

ArcSight Field	Vendor Field
Name	'Auto-Protect enabled'
Device Action	'enabled'

Event 164

ArcSight Field	Vendor Field
Name	'Auto-Protect disabled'
Device Action	'disabled'

Event 167

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'A processterminatedunexpectedly'
Message	Both('The process','%1,"terminatedunexpectedly')
DestinationService Name	%1 (service name)
Device Action	'terminated'

Event 168

ArcSight Field	Vendor Field
Name	'A processwasrestarted'
Message	Both('The process','%12,' wasrestarted')
DestinationService Name	%1 (service name)
Device Action	'restarted'

Event 177

ArcSight Field	Vendor Field
Name	'SymantecMailSecurity for Microsoft Exchange isrunninginanAuto-Protect mode that usesthe Microsoft VirusScanningAPI (VSAPI)'
Message	'The versionofMicrosoft'sExchange InformationStore installedhasa seriousbugwhen usingthisAPI.Youshoulduse version5.5.2651.76 or later.The Exchange information store willnot release handlesproperly andSSSfor Microsoft Exchange andExchange InformationStore willexperience problemsafter severaldaysofoperation. (See SAVFMSE'sReadMe.TXTfor more informationandMicrosoft Knowledge Base article Q248838 for the latest fixestoService Pack3.)'

Event 178

ArcSight Field	Vendor Field
Name	'Anerror wasreturnedfromDAPI'
Message	

Event 179

ArcSight Field	Vendor Field
Name	'The mailbox couldnot be created'
Message	'The mailbox couldnot be createdbecause it already exists'

Event 180

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'The mailbox couldnot be createdthe server specifieddoesnot have a private store'
Message	

Event 181

ArcSight Field	Vendor Field
Name	'The service willbe shutdown'
Message	'The service willbe shutdowndue toanunexpectedresult froma systemcall'

Event 182

ArcSight Field	Vendor Field
Name	'The service willbe shutdown'
Message	'The service willbe shutdowndue toanunexpectedfailure waitingfor Microsoft Exchange tostart'

Event 183

ArcSight Field	Vendor Field
Name	'The service willbe shutdown'
Message	'The service willbe shutdowndue toanunexpectedfailure monitoringthe MSExchangeS service'

Event 184

ArcSight Field	Vendor Field
Name	'The service willbe shutdown'
Message	The service willbe shutdowndue toanunexpectedresult froma systemcall

Event 185

ArcSight Field	Vendor Field
Name	'The service willbe shutdown'
Message	'The service willbe shutdowndue toanunexpectedfailure initializingvirusprotection'

Event 186

ArcSight Field	Vendor Field
Name	'The service willbe shutdown'
Message	'A timeout occurredwhile waitingfor Microsoft Exchange toinitialize the VSAPI interface'

Event 187

ArcSight Field	Vendor Field
Name	'The service willbe shutdown'
Message	'The service willbe shutdowndue toanunexpectedshutdownofthe SAVFMSECTRL process'

Event 188

ArcSight Field	Vendor Field
Name	'MAPI support for the Exchange publicfolderscouldnot be initialized'
Message	

Event 189

ArcSight Field	Vendor Field
Name	'The publicinformationstore hasnot beenmounted'
Message	

Event 190

ArcSight Field	Vendor Field
Name	'The list ofpublicinformationstoresisempty'
Message	

Event 196

ArcSight Field	Vendor Field
Name	'Cannot rename Standardpolicy'
Message	

Event 198

ArcSight Field	Vendor Field
Name	'The policy or subpolicy isdisabled'
Device Action	'Disabled'

Event 200

ArcSight Field	Vendor Field
Name	'Content filter engine started'
Device Action	'Started'

Event 201

ArcSight Field	Vendor Field
Name	'Content filter engine stopped'
Device Action	'Stopped'

Event 205

ArcSight Field	Vendor Field
Name	'Content filter engine failedtoshutdownproperly'
Message	

Event 206

ArcSight Field	Vendor Field
Name	'A content filter error occurredwhile analyzinga message body'
Message	

Event 207

ArcSight Field	Vendor Field
Name	'A content filter error occurredwhile attemptingtoget the categories'
Message	

Event 208

ArcSight Field	Vendor Field
Name	'Nocategorieswere selectedfor content filtering'
Message	

Event 209

ArcSight Field	Vendor Field
Name	'The Content Filter optionisdisabled'
Message	

Event 210

ArcSight Field	Vendor Field
Name	'Content Filter policiesare disabled'
Message	

Event 211

ArcSight Field	Vendor Field
Name	'Content Filter Policy invalid'
Message	'Missingaction'

Event 212

ArcSight Field	Vendor Field
Name	'Property policy applied'
Message	

Event 213

ArcSight Field	Vendor Field
Name	'Aerror occurredinthe MMCBrowser'
Message	'Checkthe event logfor further details'

Event 215

ArcSight Field	Vendor Field
Name	'Anattachment hasviolated'
Message	%5 (message text)

ArcSight Field	Vendor Field
File Name	%2 (name ofattachedfile)
File Type	%1 (attachment file type)
File Path	%3 (pathtoattachment)
Device CustomString1	Virusname
Device CustomString4	Rule Name
Device CustomString5	ScanType

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Device CustomString6	Policy Settings
Additionaldata	subject
Device Action	Actiononattachment

Event 219

ArcSight Field	Vendor Field
Name	'Anoutbreakconditionwasdetected'
Message	Both('OutbreakRule Information: ',%1,' Threesholdvalue for thisrule is: ',%2,' Current level for thisrule is: ',%3')
Device CustomString6	OutbreakRule Information
Device CustomString4	Rule Name
Additionaldata	thresholdValue
Additionaldata	currentLevel

Event 220

ArcSight Field	Vendor Field
Name	'Anerror occurredwhile attemptingtoobtainthe current virusdefinitionsversiononthis machine'
Message	

Event 221

ArcSight Field	Vendor Field
Name	'Anerror occurredwithLiveUpdate'
Message	'Checkthe event logfor further details'

Event 222

ArcSight Field	Vendor Field
Name	'The iddoesnot matchany current commandrequests'
Message	

Event 223

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'The commandrequest isnot yet complete'
Message	
Message	'Response topacket = [bytesout]receivedfromserver [bytesin]. Result code = [reason code].New Status: ', 'Id='

Event 229

ArcSight Field	Vendor Field
Name	'The Report Name already exists'
Message	

Event 230

ArcSight Field	Vendor Field
Name	'ReportingConfigEncounteredanerror withthe Registry'
Message	

Event 231

ArcSight Field	Vendor Field
Name	'ReportingConfigEncounteredanerror withthe Registry'
Message	

Event 232

ArcSight Field	Vendor Field
Name	'Anerror occurredwhenprocessingproduct file updateissent fromconsole'
Message	

Event 234

ArcSight Field	Vendor Field
Name	'DeletionofBackupfile failed'
Message	

Event 240

ArcSight Field	Vendor Field
Name	'SESA initializationfailed'
Message	'Events will not be logged to SESA'

Event 242

ArcSight Field	Vendor Field
Name	'XML data is missing or invalid or corrupt'
Message	

Event 243

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

Event 246

ArcSight Field	Vendor Field
Name	'Dictionary files failed to load'
Message	

Event 260

ArcSight Field	Vendor Field
Name	'The content filter engine is already initialized'
Message	

Event 261

ArcSight Field	Vendor Field
Name	'The content filter attempted an undefined/illegal action'
Message	

Event 262

ArcSight Field	Vendor Field
Name	'An error occurred modifying some or all settings on server'
Message	

Event 264

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'The requested command is not implemented on the server'
Message	

Event 266

ArcSight Field	Vendor Field
Name	'Unable to obtain virus definition set version'
Message	'Run LiveUpdate to obtain or repair these files'

Event 267

ArcSight Field	Vendor Field
Name	'Timeout reached waiting for a Heartbeat message to arrive'
Message	

Event 268

ArcSight Field	Vendor 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 Field	Vendor Field
Name	'Unexpected attachment contents were found in a Heartbeat message'
Message	

Event 270

ArcSight Field	Vendor Field
Name	'Unable to validate the Heartbeat Mailbox'
Message	

Event 271

ArcSight Field	Vendor Field
Name	'AutoProtect is not enabled'
Message	

Event 272

ArcSight Field	Vendor Field
Name	'The VSAPI dllisnot loadedor isinaninvalidstate'
Message	

Event 273

ArcSight Field	Vendor Field
Name	'The Exchange InformationStore isnot running, or isnot loaded'
Message	

Event 274

ArcSight Field	Vendor Field
Name	'The internalCtrlprocessisnot runningor isnot available totake commands'
Message	

Event 275

ArcSight Field	Vendor Field
Name	'AnUnexpectederror hasoccurred'
Message	

Event 279

ArcSight Field	Vendor Field
Name	'The server hasnot respondedwithstatusoflast request'
Message	'The request may not have executedsuccessfully'

Event 280

ArcSight Field	Vendor Field
Name	'SMSMSE ‘ ‘ saved’ ’
Source User Name	user name (fromNTUser)
Source NTDomain	domain(fromNTDomain)

Event 281

ArcSight Field	Vendor Field
Name	'Unable tosave SAVFMSE settings'
Message	

Event 283

ArcSight Field	Vendor 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 Field	Vendor Field
Name	'A critical failure occurred while attempting to use Symantec Virus Definitions'
Message	

Event 291

ArcSight Field	Vendor Field
Name	'A message has violated'
Message	%5 (The attachment 'QuarantinedAttachment.txt' was Quarantined for the following reason(s): A FilteringRule was violated.)
File Path	%3 (User1/Sent Items)
File Name	%2 (fwef)
File Type	%1 (message)
Device CustomString6	Policy Settings
Device CustomString5	ScanType
Device CustomString4	Rule Name
Device Action	Both(%5,*was(.*)for.*)

Event 292

ArcSight Field	Vendor 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]'

ArcSight Field	Vendor Field
DestinationHostName	host name
DeviceCustomDate 1	Expiry Date

Event 293

ArcSight Field	Vendor Field
Name	'Virusdefinitionandcontent license hasexpired, isdamagedor isnot installed'
Message	'Virusdefinitionandcontent license for SymantecMailSecurity for Microsoft Exchange on server [host name]hasexpired, isdamaged, or isnot installed.'
DestinationHostName	%1 (N15-195-H2140)

Event 295

ArcSight Field	Vendor Field
Name	'Virusdefinitionscannot be updatedbecause your content license hasexpired, is damaged, or isnot installed'
Message	

Event 296

ArcSight Field	Vendor Field
Name	'Unable toapply virusdefinitionupdateissent fromconsole because content license is expired, damagedor not installed'
Message	

Event 297

ArcSight Field	Vendor Field
Name	'Unable toinstalllicense file because the file isdamaged, invalid, or expired'
Message	

Event 298

ArcSight Field	Vendor Field
Name	'Unable toinstalllicense file sent fromconsole because the file isinvalid'
Message	

Event 301

ArcSight Field	Vendor Field
Name	'Unable to log events to SESA because no IP address is set for the SESA server'
Message	

Event 304

ArcSight Field	Vendor Field
Name	'Heartbeat succeeded'
Message	

Event 307

ArcSight Field	Vendor Field
Name	'Virus definitions cannot be updated because your content license has expired or is damaged or not installed'
Message	'Decomposers were successfully updated'

Event 308

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

Event 309

ArcSight Field	Vendor Field
Name	'Virus definitions cannot be updated because your content license has expired or is damaged or not installed'
Message	'You already have the most recent decomposers'

Event 310

ArcSight Field	Vendor Field
Name	'LiveUpdate was successful'
Message	'New virus definitions and decomposers were retrieved'

Event 311

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'LiveUpdate wassuccessful'
Message	'New virusdefinitionsanddecomposerswere retrieved. A systemrestart isrequiredtouse them'

Event 312

ArcSight Field	Vendor Field
Name	'LiveUpdate wassuccessful'
Message	'New virusdefinitionswere retrieved.Youalready have the most recent decomposers'

Event 313

ArcSight Field	Vendor Field
Name	'LiveUpdate retrievednew filesbut the virusdefinitionscouldnot be updated'
Message	'Decomposerswere successfully updated'

Event 314

ArcSight Field	Vendor Field
Name	'LiveUpdate retrievednew filesbut the virusdefinitionscouldnot be updated'
Message	'Decomposerswere successfully updated.A systemrestart isrequiredtouse them'

Event 315

ArcSight Field	Vendor Field
Name	'LiveUpdate retrievednew filesbut the virusdefinitionscouldnot be updated'
Message	'Youalready have the most recent decomposers'

Event 316

ArcSight Field	Vendor Field
Name	'LiveUpdate wassuccessful'
Message	'New virusdefinitionswere retrieved.A systemrestart isrequiredtouse them. You already have the most recent decomposers'

Event 317

ArcSight Field	Vendor Field
Name	'LiveUpdate wassuccessful'
Message	'New decomposerswere retrieved.Youalready have the most recent virusdefinitions'

Event 318

ArcSight Field	Vendor Field
Name	'LiveUpdate wassuccessful'
Message	'New decomposers were retrieved. A systemrestart is required to use them. You already have the most recent virusdefinitions'

Event 319

ArcSight Field	Vendor Field
Name	'LiveUpdate hasdeterminedthat noupdate isnecessary'
Message	'You already have the most recent virusdefinitionsanddecomposers'

Event 320

ArcSight Field	Vendor Field
Name	'The SymantecMailSecurity for Microsoft Exchange Vulnerability Assessment scan was started'
Message	

Event 321

ArcSight Field	Vendor Field
Name	'The SymantecMailSecurity for Microsoft Exchange Vulnerability Assessment scan was completed'
Message	

Event 322

ArcSight Field	Vendor Field
Name	'The SymantecMailSecurity for Microsoft Exchange Vulnerability Assessment scan abnormally terminated'
Message	

Event 323

ArcSight Field	Vendor 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 Field	Vendor Field
Name	'Failedtoloadheuristicanti-spamengine'
Message	'SPAM.DATand/or SPAM.NETfilesmay be missingor corrupt'

Event 330

ArcSight Field	Vendor Field
Name	'Anoutbreakconditionisstillbeingdetected'
Device CustomString4	Rule Name
Device CustomString6	OutbreakRule Information
Additionaldata	subject
Additionaldata	thresholdValue
Additionaldata	currentLevel

Event 331

ArcSight Field	Vendor Field
Name	'A service started'
DestinationService Name	'SymantecMailSecurity Utility Service'
Device Action	'Started'

Event 332

ArcSight Field	Vendor Field
Name	'A service stopped'
DestinationService Name	'SymantecMailSecurity Utility Service'
Device Action	'Stopped'

Event 333

ArcSight Field	Vendor Field
Name	'SymantecMailSecurity Utility Service couldnot openservice manager'
Message	

Event 334

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'SymantecMailSecurity Utility Service couldnot create service'
Message	

Event 335

ArcSight Field	Vendor Field
Name	'SymantecMailSecurity Utility Service couldnot openservice'
Message	

Event 336

ArcSight Field	Vendor Field
Name	'SymantecMailSecurity Utility Service couldnot start'
Message	

Event 337

ArcSight Field	Vendor Field
Name	'SymantecMailSecurity Utility Service badservice request'
Message	

Event 338

ArcSight Field	Vendor Field
Name	'SymantecMailSecurity Utility Service couldnot be deleted'
Message	

Event 339

ArcSight Field	Vendor Field
Name	'SymantecMailSecurity Utility Service handler not installed'
Message	

Event 341

ArcSight Field	Vendor Field
Name	'FailedtoloadSymantecPremiumAntiSpamengine'
Message	

Event 344

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'SymantecPremiumAntiSpamlicense hasexpired, isdamagedor isnot installed'
Message	('SymantecPremiumAntiSpamlicense for SymantecMailSecurity for Microsoft Exchange onserver ',%1,' hasexpired, isdamaged, or isnot installed')

ArcSight Field	Vendor Field
DestinationHost Name	host name

Event 345

ArcSight Field	Vendor Field
Name	'SymantecPremiumAntiSpamlicense isgettingexpire'
Message	('SymantecPremiumAntiSpamlicense for SymantecMailSecurity for Microsoft Exchange onserver ',%1,' wilexpire on',%2')
Device Host Name	%1 (host name)
Device CustomDate 1	%2 (Expiry date)

Event 347

ArcSight Field	Vendor Field
Name	'InvalidSymantecPremiumAntiSpamlicense or SymantecPremiumAntiSpamlicense has expired'
Message	

Event 349

ArcSight Field	Vendor Field
Name	'HeuristicAntispamsettingscannot be savedbecause SymantecPremiumAntiSpamis currently installed'
Message	

Event 350

ArcSight Field	Vendor Field
Name	'Unable toinstalllicense file sent fromconsole because the file isexpired'
Message	

Event 351

ArcSight Field	Vendor 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 Field	Vendor 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 Field	Vendor Field
Name	'Server was not able to receive RapidRelease VirusDefinitionupdate'
Message	'Server ',%1(N15-H72),' was not able to receive RapidRelease VirusDefinitionupdate due to an FTP failure'
DestinationHost Name	%1 (host name)
ApplicationProtocol	'FTP'

Event 365

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

Event 366

ArcSight Field	Vendor Field
Name	'Building Active Directory User Group Table Started'
Device Action	'Started'

Event 367

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Name	'BuildingActive Directory User GroupTable CompletedSuccessfully'
Message	

Event 368

ArcSight Field	Vendor Field
Name	'BuildingActive Directory User GroupTable Failed'
Message	

Event 369

ArcSight Field	Vendor Field
Name	'Scanprocessfailedtoreduce privileges'
Message	

Event 370

ArcSight Field	Vendor Field
Name	'Failedtoretrieve settingsfromthe sharedstorage location'
Message	

Event 371

ArcSight Field	Vendor Field
Name	'Failedtosave settingstothe sharedstorage location'
Message	

Event 372

ArcSight Field	Vendor Field
Name	'Anerror occurredwhenprocessingrecipientslist for releasingquarantine item(s)by mail'
Message	

Event 373

ArcSight Field	Vendor Field
Name	'Unable to validate Recipient Mailbox'
Message	

Event 374

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Name	'An error occurred when creating a folder specified for the Save to folder setting'
Message	

Event 375

ArcSight Field	Vendor Field
Name	'SMSMSE service is not started'
Message	

Event 376

ArcSight Field	Vendor Field
Name	'SMSMSE service is starting'
Message	'Please try again once it is started'

Event 377

ArcSight Field	Vendor Field
Name	'SMSMSE service is stopping'
Message	

Event 379

ArcSight Field	Vendor Field
Name	'VSAPI scheduled background scanning has been enabled'
Device Action	'enabled'
Device CustomString5	'VSAPI' (ScanType)

Event 380

ArcSight Field	Vendor Field
Name	'VSAPI scheduled background scanning has been disabled'
Device Action	'disabled'
Device CustomString5	'VSAPI' (ScanType))

Event 381

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Device Action	%1 (actiontaken)
Device CustomString4	Rule Name
Device CustomString5	ScanType
Name	'The message locatedinSMTPhasviolateda policy'
Message	%1 (message text)

Event 382

ArcSight Field	Vendor Field
Name	name

Event 384

ArcSight Field	Vendor Field
Name	'Releasedfilesfromquarantine tofile'
Device Action	'Released'
Additionaldata	numFile
Message	'Released[number offiles]file(s)fromquarantine tofile'

Event 385

ArcSight Field	Vendor Field
Name	'The WindowsTaskScheduler service isnot running'
Message	'Please start the WindowsTaskScheduler service andthen save your changes'

Event 386

ArcSight Field	Vendor Field
Name	'The WindowsTaskScheduler service isnot running'
Message	'Start the WindowsTaskScheduler service andthen apply the scheduledscansettings'

Event 387

ArcSight Field	Vendor Field
Name	'The WindowsTaskScheduler service isnot running'
Message	'Start the WindowsTaskScheduler service andthen apply the scheduledLiveUpdate settings'

Event 388

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Name	'The WindowsTaskScheduler service isnot running'
Message	'MailSecurity cannot generate scheduledreportsuntilthe service isstarted. Start the WindowsTaskScheduler service, andMailSecurity willgenerate scheduledreports'

Event 389

ArcSight Field	Vendor Field
Name	'Unable tocopythe license file'
Message	'Unable tocopy the SymantecPremiumAntiSpamlicense file tolicensesfolder'

Event 390

ArcSight Field	Vendor Field
Name	'SymantecMailSecurity hasfailedtore-initialize the PremiumAntiSpamengine'
Message	'Ifthere are any new spamdefinitions, they wouldnot be usedduringantispamprocessing'

Event 391

ArcSight Field	Vendor Field
Name	'The SymantecMailSecurity Utility service isnot running'
Message	'Thisservice isnecessary toprotect the Microsoft Exchange Server fromspam. Please restart the service tocontinue toprovide support for SymantecPremiumAntiSpam'
DestinationService Name	'The SymantecMailSecurity Utility'

Event 401

ArcSight Field	Vendor Field
Name	'Failedtoinitialize AV scanner'
Message	'The virusdefinitionsare either missingor corrupt'
Reason	%1 (reasoncode)

Event 404

ArcSight Field	Vendor Field
Name	'Virusdefinitionsare old'
Message	'Virusdefinitionsare ',%1(2),' daysold. Toremainprotectedensure that Liveupdate is workingproperly.'

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight Field	Vendor Field
Request URL	%2 (URL)

Event 405

ArcSight Field	Vendor Field
Name	'BackgroundScanofallStore databasescompleted'
Message	'BackgroundScanofallStore databasescompletedinhours(s)andminute(s). Totalitems were scannedfromthe start ofscanning'
Additionaldata	numScanned
Device CustomString5	'BackgroundScan' (ScanType)

Event 406

ArcSight Field	Vendor Field
Name	'BackgroundScanningispause'
Message	'Either scanwindow isover or scanisdisabled. Totalitemsare scannedfromthe start of scanning'
Device Action	'paused'

Event 409

ArcSight Field	Vendor Field
Name	'Failedtoinitialize AV Engine'
Reason	Error code

Event 410

ArcSight Field	Vendor Field
Name	'Failedtoinitialize AV Engine'
Message	'Failedtoinitialize AV Engine duringRequestImmediateUpdateEx'

Event 411

ArcSight Field	Vendor Field
Name	'Failedtosave Quarantine server settings'
Message	'Failedtosave Quarantine server settings, Server addressspecifiedby user isa Broadcast address'

Event 412

ArcSight Field	Vendor Field
Name	'SymantecPremiumAntiSpamregistrationfailedonthe server'
Message	%2 (Unable tocommunicate withSymantectoregister. Please checkyour connection settings, andtry agaiain.)
DestinationHostName	host name
ArcSight ESM Field	Device-Specific Field
Name	'SymantecPremiumAntiSpamregistrationfailedonthe server'
Message	%2 (Unable tocommunicate withSymantectoregister. Please checkyour connection settings, andtry agaiain.)
DestinationHostName	host name

Event 414

ArcSight Field	Vendor Field
Name	'SymantecPremiumAntiSpamregistrationfailedonthe server'
Message	%2 ('Unable tocommunicate withSymantectoregister. Please checkyour connection settings, andtry again.)
DestinationHostName	%1 (hostname)

Event Mappings

This section contains the following topics:

Windows Common Security Mappings

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

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Medium when Device Severity = Error or Warning; Low when Device Severity = Information or Audit_success
Destination Host Name	One of (Target Server Name, Computer Name, Target Server:Target Server Name)
Destination NT Domain	One of (Domain Name, Subject:Account Domain, New Token Information:Account Domain, Subject:Domain Name)
Destination Port	Network Information:Destination Port
Destination Process Name	One of (Process Information>New Process Name, Process Information:Process Name)
Destination Service Name	Service Information:Service Name
Destination User ID	One of (Subject:Logon ID, New Token Information:Logon ID)
Destination User Name	One of (Account Name, Subject:Account Name, Subject:Security ID, User, New Token Information:Account Name)
Destination User Privileges	One of (Additional Information:Privileges, New Right>User Right, Removed Right>User Right, Access Granted:Access Right, Access Removed:Access Right)
Device Action	One of (Account Action, Allowed, 'No', 'Blocked')
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom Number 1	Logon Type
Device Custom Number 2	Value of CrashOnAuditFail
Device Custom Number 3	Count
Device Custom String 1	One of (Access Request Information:Access Mask, Operation:Accesses, Operation:Access Mask)
Device Custom String 2	EventCategory
Device Custom String 4	One of (Error Code, Additional Information:Failure Code, Additional Information:Reason Code, Additional Information:Error Code, Failure Information:Failure Reason, Audit Events Dropped:Reason, Reason, Reason for Rejection, Error Information:Reason, Error Information>Error, Process Information:Exit Status)

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	One of (Authentication Package Name, Authentication Package, Authentication, Detailed Authentication Information:authentication Package)
Device Event Category	Event logType
Device Event Class ID	Both (Event Source , Event ID)
Device Host Name	Computer Name
Device NT Domain	One of (Domain Name, Subject:Account Domain)
Device Product	'Microsoft Windows'
Device Receipt Time	DetectTime
Device Severity	EventType
Device Vendor	'Microsoft'
External ID	Event ID
File ID	One of (Object Handle ID, Object:Object Handle)
File Name	Object:Object Name
File Type	One of (Object Type, Object:Object Type)
Message	Message
Name	Description
Source Address	One of (Network Information:Source Network Address, Local Network Address, Additional Information:Client Address)
Source Host Name	One of (Subject:Client Name, Network Information:Workstation Name, Source Workstation, Additional Information:Client Name)
Source NT Domain	Subject:Client Domain
Source Port	One of (Network Information:Source Port, Network Information:Port, Network Information:Client Port)
Source Process Name	One of (Logon Process Name, process Information:Caller Process ID)

Specific Windows Security Event Mappings

Event 1100

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

Event 1101

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

Event 1102

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

Event 1104

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

Event 1105

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

Event 1074

ArcSight ESM Field	Device-Specific Field
Name	The process has initiated the shutdown/restart of computer.
Message	concatenate(The process "%1," has initiated the "%5," of computer "%2," on behalf of user "%7," for the following reason: "%3")
Source Process Name	%1

ArcSight ESM Field	Device-Specific Field
Destination Host Name	%2
Reason	%3
Device Custom String4	Reason Code
Device Custom String5	Shutdown Type
Device Custom String6	Comment

Event 4608

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

Event 4609

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

Event 4610

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

Event 4611

ArcSight ESM Field	Device-Specific Field
Name	'A trusted logon process has been registered with the Local Security Authority. This logon process will be trusted to submit logon requests.'
Destination Process Name	LogonProcessName
Source Process Name	LogonProcessName
Destination User ID	SubjectLogonId

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

Event 4612

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

Event 4614

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

Event 4615

ArcSight ESM Field	Device-Specific Field
Name	'Invalid use of LPC port.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)

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

Event 4616

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

Event 4618

ArcSight ESM Field	Device-Specific Field
Name	'A monitored security event pattern has occurred.'
Destination User ID	TargetLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)

ArcSight ESM Field	Device-Specific Field
Destination NT Domain	TargetUserDomain
Device NT Domain	TargetUserDomain
Message	'This event is generated when Windows is configured to generate alerts in accordance with the Common Criteria Security Audit Analysis requirements (FAU_SAA) and an auditable event pattern occurs.'

Event 4621

ArcSight ESM Field	Device-Specific Field
Name	'Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.'
Device Custom Number 2	CrashOnAuditFail value.
Message	'This event is logged after a system reboots following CrashOnAuditFail.'

Event 4622

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

Event 4624

ArcSight ESM Field	Device-Specific Field
Name	'An account was successfully logged on.'
Additional data	TargetOutboundUserName
Additional data	TargetOutboundDomainName
Device NT Domain	SubjectDomainName
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Destination Process Name	ProcessName

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

Event 4625

ArcSight ESM Field	Device-Specific Field
Name	'An account failed to log on.'
Device NT Domain	SubjectDomainName
Source Address	IpAddress
Destination Process Name	ProcessName
Destination NT Domain	TargetDomainName
Device Custom String 1	SubStatus
Device Custom String 3	ProcessId
Reason	FailureReason
Device Process Name	LogonProcessName

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight ESM Field	Device-Specific Field
Destination User ID	''
Source Host Name	WorkstationName
Source Port	IpPort
Source Process Name	ProcessId
Device Custom String 4	FailureReason
Device Custom String 5	AuthenticationPackageName
Device Custom Number 1	LogonType
Destination UserName	TargetUserName
Message	<p>'This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request.</p> <ul style="list-style-type: none"> - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.'

Event 4626

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

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

Event 4627

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

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

Event 4634

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

Event 4646

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

Event 4647

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

Event 4648

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

Event 4649 - Event 4695

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

Event 4650

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

Event 4651

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

Event 4652

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

Event 4653

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

Event 4654

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

Event 4655

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

Event 4656

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

Event 4657

ArcSight ESM Field	Device-Specific Field
Name	'A registry value was modified.'
Device Custom String 6	ObjectName
Device Action	OperationType
Old File Type	OldValueType
Device Custom String 4	OldValue
File Type	NewValueType
File ID	HandleId

ArcSight ESM Field	Device-Specific Field
File Name	ObjectName
Device Custom String 5	NewValue
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event 4658

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

Event 4659

ArcSight ESM Field	Device-Specific Field
Name	'A handle to an object was requested with intent to delete.'
Device Custom String 1	AccessList
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
File Type	ObjectType
File ID	HandleId
File Name	ObjectName

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

Event 4660

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

Event 4661

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

Event 4662

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

Event 4663

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

Event 4664

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

Event 4665

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

Event 4666

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

Event 4667

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

Event 4668

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

ArcSight ESM Field	Device-Specific Field
Source NT Domain	ClientDomain

Event 4670

ArcSight ESM Field	Device-Specific Field
Name	'Permissions on an object were changed.'
Device Custom String 4	OldSd
Device Custom String 5	NewSd
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
File Type	ObjectType
File ID	HandleId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
File Name	ObjectName

Event 4671

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

Event 4672

ArcSight ESM Field	Device-Specific Field
Name	'Special privileges assigned to new logon.'
Destination User privileges	PrivilegeList

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

Event 4673

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

Event 4674

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

Event 4675

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

Event 4688

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

Event 4689

ArcSight ESM Field	Device-Specific Field
Name	'A process has exited.'
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId

ArcSight ESM Field	Device-Specific Field
Destination Process Name	ProcessName
Device Custom String 4	Status
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event 4690

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

Event 4691

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

Event 4692

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

Event 4693

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

Event 4694

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

Event 4695

ArcSight ESM Field	Device-Specific Field
Name	'Unprotection of auditable protected data was attempted.'
Destination User ID	SubjectLogonId

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

Event 4696 - Event 4697

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

Event 4697

ArcSight ESM Field	Device-Specific Field
Name	'A service was installed in the system.'
File Path	ServiceFileName
File Type	ServiceType
Device Custom String 5	ServiceStartType
Device Custom String 6	ServiceAccount
Destination User ID	SubjectLogonId
Destination Service Name	ServiceName

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

Event 4698 - Event 4700

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

Event 4699

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

Event 4700

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

Event 4701 - Event 4717

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

Event 4702

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

Event Id 4703

ArcSight ESM Field	Device-Specific Field
Name	'A token right was adjusted.'
Source User Name	One of (SubjectUserName, SubjectUserSid)
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Destination User Name	One of (TargetUserName, TargetUserSid)
Destination NT Domain	TargetDomainName
Destination User ID	TargetLogonId
Destination Process Name	ProcessName
Device Custom String 3	ProcessId

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	EnabledPrivilegeList
Device Custom String 4	DisabledPrivilegeList
Message	'A token right was adjusted.'

Event 4704

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

Event 4705

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

Event 4706

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

Event 4707

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

Event 4709

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

Event 4710

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

Event 4711

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

Event 4712

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

Event 4713

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

Event 4714

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

Event 4715

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

Event 4716

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

Event 4717

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

ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User Privileges	AccessGranted

Event 4718 - Event 4726

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

Event 4719

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

Event 4720

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

Event 4722

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

Event 4723

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

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

Event 4724

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

Event 4725

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

Event 4726

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

Event 4727 - Event 4728

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

Event 4728

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

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

Event 4729 - Event 4730

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

Event 4730

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

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

Event 4731

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

Event 4732

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

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

Event 4733

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

Event 4734

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

Event 4823

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

Event 4824

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

Event 4826

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

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

Event 4864

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

Event 4865

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

Event 4866

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

Event 4867

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

Event 4868

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

Event 4869

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

Event 4870

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

Event 4871

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

Event 4872

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

Event 4873

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

Event 4874

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

Event 4875

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

Event 4876

ArcSight ESM Field	Device-Specific Field
Name	'Certificate Services backup started.'
Destination User ID	SubjectLogonId

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

Event 4877

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

Event 4878

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

Event 4879

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

Event 4880

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

Event 4881

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

Event 4882

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

Event 4883

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

Event 4884

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

Event 4885

ArcSight ESM Field	Device-Specific Field
Name	'The audit filter for Certificate Services changed.'
Destination User ID	SubjectLogonId

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

Event 4886

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

Event 4887

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

Event 4888

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

Event 4889

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

Event 4890

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

Event 4891

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

Event 4892

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

Event 4893

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

Event 4894

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

Event 4895

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

Event 4896

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

Event 4897

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

Event 4898

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

Event 4899

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

Event 4900

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

Event 4902

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

Event 4904

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

Event 4905

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

Event 4906

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

Event 4907

ArcSight ESM Field	Device-Specific Field
Name	'Auditing settings on object were changed.'
Device Custom String 5	ObjectType
Device Custom String 3	ProcessId
Destination User ID	SubjectLogonId
Destination Process Name	ProcessName
File Type	ObjectType
File ID	HandleId
File Name	ObjectName
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName

Event 4908

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

Event 4909

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

Event 4910

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

Event 4911

ArcSight ESM Field	Device-Specific Field
Name	'Resource attributes of the object were changed.'
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File ID	HandleId
File Name	ObjectName
File Type	ObjectType
Destination Process ID	ProcessId
Destination Process Name	ProcessName

Event 4912

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

Event 4913

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

ArcSight ESM Field	Device-Specific Field
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
File ID	HandleId
File Name	ObjectName
File Type	ObjectType
Destination process ID	ProcessId
Destination process Name	ProcessName

Event 4928

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

Event 4929

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

Event 4930

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

Event 4931

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

Event 4932

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

Event 4933

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

Event 4934

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

Event 4935

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

Event 4936

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

Event 4937

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

Event 4944

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

Event 4945

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

Event 4946

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

Event 4947

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

Event 4948

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

Event 4949

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

Event 4950

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

Event 4951

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

Event 4952

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

Event 4953

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

Event 4954

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

Event 4956

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

Event 4957

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

Event 4958

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

Event 4960

ArcSight ESM Field	Device-Specific Field
Name	'IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.'

Event 4961

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

Event 4962

ArcSight ESM Field	Device-Specific Field
Name	'IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.'

Event 4963

ArcSight ESM Field	Device-Specific Field
Name	'IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.'

Event 4964

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

Event 4965

ArcSight ESM Field	Device-Specific Field
Name	'IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.'

Event 4976

ArcSight ESM Field	Device-Specific Field
Name	'During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.'
Source Address	LocalAddress

Event 4977

ArcSight ESM Field	Device-Specific Field
Name	'During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.'
Source Address	LocalAddress

Event 4978

ArcSight ESM Field	Device-Specific Field
Name	'During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.'
Source Address	LocalAddress

Event 4979

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

Event 4980

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

Event 4981

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

ArcSight ESM Field	Device-Specific Field
Source Port	LocalKeyModPort
Destination Address	RemoteAddress
Destination Port	RemoteKeyModPort

Event 4982

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

Event 4983

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

Event 4984

ArcSight ESM Field	Device-Specific Field
Name	'An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.'
Source Address	LocalAddress
Source Port	LocalKeyModPort
Destination Address	RemoteAddress

ArcSight ESM Field	Device-Specific Field
Destination Port	RemoteKeyModPort
Message	FailureReason
Device Custom String 4	Failure

Event 4985

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

Event 5024

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

Event 5025

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

Event 5027

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

Event 5028

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

Event 5029

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

Event 5030

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

Event 5031

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

Event 5032

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

Event 5033

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

Event 5034

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

Event 5035

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

Event 5037

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

Event 5038

ArcSight ESM Field	Device-Specific Field
Name	'Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.'

Event 5039

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

Event 5040

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

Event 5041

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

Event 5042

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

Event 5043

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

Event 5044

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

Event 5045

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

Event 5046

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

Event 5047

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

Event 5048

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

Event 5049

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

Event 5050

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

Event 5051

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

Event 5056

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

Event 5057

ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic primitive operation failed.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)

ArcSight ESM Field	Device-Specific Field
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Message	Reason
Reason	ReturnCode

Event 5058

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

Event 5059

ArcSight ESM Field	Device-Specific Field
Name	'Key migration operation.'
File Name	KeyName
File Type	KeyType
Device Action	Operation
Device Custom String 4	ReturnCode

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

Event 5060

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

Event 5061

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

Event 5062

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

Event 5063

ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic provider operation was attempted.'
Destination User ID	SubjectLogonId

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

Event 5064

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

Event 5065

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

Event 5066

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

Event 5067

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

Event 5068

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

Event 5069

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

Event 5070

ArcSight ESM Field	Device-Specific Field
Name	'A cryptographic function property modification was attempted.'
Destination User ID	SubjectLogonId

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

Event 5071

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

Event 5120

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

Event 5121

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

Event 5122

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

Event 5123

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

Event 5124

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

Event 5125

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

Event 5126

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

Event 5127

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

Event 5136

ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was modified.'
Device Custom String 6	ObjectDN
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Device Custom String 4	OperationType

Event 5137

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

Event 5138

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

Event 5139

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

Event 5140

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

Event 5141

ArcSight ESM Field	Device-Specific Field
Name	'A directory service object was deleted.'
Device Custom String 6	ObjectDN

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	ObjectClass
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjetDomainName
Device NT Domain	SubjectDomainName

Event 5142

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

Event 5143

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

Event 5144

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

Event 5145

ArcSight ESM Field	Device-Specific Field
Name	'A network share object was checked to see whether client can be granted desired access.'
Source NT Domain	SubjectDomainName
Source User ID	SubjectLogonId
Source Address	IpAddress
Device Custom IPv6 Address 2	IpAddress (Source IPv6 Address)
Device Custom String 1	AccessList
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
Destination User ID	SubjectLogonId
Source Port	IpPort
Device Custom String 6	ShareName
File Path	ShareLocalPath
File Name	RelativeTargetName

Event 5146

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

Event 5147

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

Event 5152

ArcSight ESM Field	Device-Specific Field
Name	'The Windows Filtering Platform blocked a packet.'
Source Address	SourceAddress
Source Port	SourcePort
Destination Address	DestAddress

ArcSight ESM Field	Device-Specific Field
Destination Port	DestPort
File Name	Application
File Path	Application
File Type	Application

Event 5153

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

Event 5154

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

Event 5155

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

ArcSight ESM Field	Device-Specific Field
File Name	Application
File Path	Application
File Type	Application

Event 5156

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

Event 5157

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

Event 5158

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

Event 5159

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

Event 5168

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

Event 5376

ArcSight ESM Field	Device-Specific Field
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device Custom Date 1	ProcessCreationTime
Device NT Domain	SubjectDomainName
File Path	BackupFileName
Message	'This event occurs when a user backs up their own Credential Manager credentials. A user (even an Administrator) cannot back up the credentials of an account other than his own.'
Name	'Credential Manager credentials were backed up.'
Source Process ID	ClientProcessId

Event 5377

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	ProcessCreationTime
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, SubjectUserSid)
Destination NT Domain	SubjectDomainName
Device NT Domain	SubjectDomainName
File Path	BackupFileName
Message	'This event occurs when a user restores his Credential Manager credentials from a backup. A user (even an Administrator) cannot restore the credentials of an account other than his own.'
Name	'Credential Manager credentials were restored from a backup.'
Source Process ID	ClientProcessId

Event 5378

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

Event 5379

ArcSight ESM Field	Device-Specific Field
Destination Process Name	TargetName
Device Custom Date 1	ProcessCreationTime
Device Custom Number 1	Type
Device Custom Number 2	CountOfCredentialsReturned
Device Custom String 3	ReadOperation

ArcSight ESM Field	Device-Specific Field
Reason	ReturnCode
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName or SubjectUserSid
Source User Id	SubjectLogonId
Source Process Id	ClientProcessId

Event 5380

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

Event 5381

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

Event 5382

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

Event 5440

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

Event 5441

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

Event 5442

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

Event 5443

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

Event 5444

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

Event 5446

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

Event 5447

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

Event 5448

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

Event 5449

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

Event 5450

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

Event 5451

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

Event 5452

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

Event 5453

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

Event 5456

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

Event 5457

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

Event 5458

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

Event 5459

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

Event 5460

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

Event 5461

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

Event 5462

ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.'
Device Custom String 4	Error

Event 5463

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

Event 5464

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

Event 5465

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

Event 5466

ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.'

Event 5467

ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.'

Event 5468

ArcSight ESM Field	Device-Specific Field
Name	'PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.'

Event 5471

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

Event 5472

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

Event 5473

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

Event 5474

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

Event 5477

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

Event 5478

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

Event 5479

ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.'

Event 5480

ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.'

Event 5483

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

Event 5484

ArcSight ESM Field	Device-Specific Field
Name	'IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.'
Device Custom String 4	Error

Event 5632

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

Event 5633

ArcSight ESM Field	Device-Specific Field
Name	'A request was made to authenticate to a wired network.'
Destination User ID	SubjectLogonId
Destination User Name	One of (SubjectUserName, Identity)
Destination NT Domain	SubjectDomainName

ArcSight ESM Field	Device-Specific Field
Device NT Domain	SubjectDomainName
Device Outbound Interface	InterfaceName
Device Custom String 4	One of (ReasonCode, ErrorCode)
Reason	One of (ErrorCode, both (ReasonText, ReasonCode))

Event 5712

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

Event 5888

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

Event 5889

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

Event 5890

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

Event 6144

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

Event 6145

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

Event 6272

ArcSight ESM Field	Device-Specific Field
Name	'Network Policy Server granted access to a user.'
Destination User Name	SubjectUserName
Destination NT Domain	SubjectDomainName
Destination User ID	FullyQualifiedSubjectUserName
Destination Address	NASIPv4Address
Destination Port	NASPort
Source User Name	SubjectMachineName
Source User ID	FullyQualifiedSubjectMachineName

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

ArcSight ESM Field	Device-Specific Field
Source Address	CallingStationID
Device Custom String 1	ProxyPolicyName
Device Custom String 3	ClientIPAddress
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier
Destination User Privileges	QuarantineState

Event 6273

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

Event 6274

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

Event 6275

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

Event 6276

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

Event 6277

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

Event 6278

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

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	AuthenticationType
Device Custom String 6	AccountSessionIdentifier
Destination User Privileges	QuarantineState

Event 6279

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

Event 6280

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

Event 6281

ArcSight ESM Field	Device-Specific Field
Name	'Code Integrity determined that the page hashes or an image file are not valid.'
File Path	Param1
Message	'The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error.'

Event 6409

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

Event 6410

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

Event 6416

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

Event 8191

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

Microsoft OAlerts

Event 300

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

Mappings for DNS Client Operational

Event 1015

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

Event 1016

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

Event 1017

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

Event 3006

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

Event 3008

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

Event 3009

ArcSight Field	Vendor Field
Name	"Network query initiated"
Device Custom String 1	QueryName

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

ArcSight Field	Vendor Field
Device Custom String 4	AdapterName
Device Custom Number 1	InterfaceCount
Device Custom Number 2	NetworkIndex
Device Custom String 6	LocalAddress
Device Dns Domain	DNSServerAddress

Event 3010

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

Event 3011

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

Event 3012

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

Event 3013

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

Event 3014

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

Event 3016

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

Event 3018

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

Event 3019

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

Event 3020

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

Windows Event Log Event Descriptions by Category

Category	Subcategory	ID	Message Summary
Account Logon	Credential Validation	4774	An account was mapped for logon.
	Credential Validation	4775	An account could not be mapped for logon.
	Credential Validation	4776	The domain controller attempted to validate the credentials for an account.
	Credential Validation	4777	The domain controller failed to validate the credentials for an account.
	Kerberos Authentication Service	4768	A Kerberos authentication ticket (TGT) was requested.
	Kerberos Authentication Service	4771	Kerberos pre-authentication failed.
	Kerberos Authentication Service	4772	A Kerberos authentication ticket request failed.
	Kerberos Service Ticket Operations	4769	A Kerberos service ticket was requested.
	Kerberos Service Ticket Operations	4770	A Kerberos service ticket was renewed.
Account Management	Application Group Management	4783	A basic application group was created.
		4784	A basic application group was changed.
		4785	A member was added to a basic application group.
		4786	A member was removed from a basic application group.
		4787	A non-member was added to a basic application group.
		4788	A non-member was removed from a basic application group.
		4789	A basic application group was deleted.
		4790	An LDAP query group was created.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

Category	Subcategory	ID	Message Summary
	Computer Account Management	4742	A computer account was changed.
		4743	A computer account was deleted.
Account Management	Distribution Group Management	4744	A security-disabled local group was created.
		4745	A security-disabled local group was changed.
		4746	A member was added to a security-disabled local group.
		4747	A member was removed from a security-disabled local group.
		4748	A security-disabled local group was deleted.
		4749	A security-disabled global group was created.
		4750	A security-disabled global group was changed.
		4751	A member was added to a security-disabled global group.
		4752	A member was removed from a security-disabled global group.
		4753	A security-disabled global group was deleted.
		4759	A security-disabled universal group was created.
		4760	A security-disabled universal group was changed.
		4761	A member was added to a security-disabled universal group.
		4762	A member was removed from a security-disabled universal group.
		4763	A security-disabled universal group was deleted.
Account Management	Other Account Management Events	4782	The password hash an account was accessed.
		4793	The Password Policy Checking API was called.
		4797	An attempt was made to query the existence of a blank password for an account.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

Category	Subcategory	ID	Message Summary
Account Management	Security Group Management	4727	A security-enabled global group was created.
		4728	A member was added to a security-enabled global group.
		4729	A member was removed from a security-enabled global group.
		4730	A security-enabled global group was deleted.
		4731	A security-enabled local group was created.
		4732	A member was added to a security-enabled local group.
		4733	A member was removed from a security-enabled local group.
		4734	A security-enabled local group was deleted.
		4735	A security-enabled local group was changed.
		4737	A security-enabled global group was changed.
		4754	A security-enabled universal group was created.
		4755	A security-enabled universal group was changed.
		4756	A member was added to a security-enabled universal group.
		4757	A member was removed from a security-enabled universal group.
		4799	A security-enabled local group membership was enumerated
Account Management	User Account Management	4758	A security-enabled universal group was deleted.
		4764	A group's type was changed.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

Category	Subcategory	ID	Message Summary
		4720	A user account was created.
		4722	A user account was enabled.
		4723	An attempt was made to change an account's password.
		4724	An attempt was made to reset an account's password.
		4725	A user account was disabled.
		4726	A user account was deleted.
		4738	A user account was changed.
		4740	A user account was locked out.
		4765	SID History was added to an account.
		4766	An attempt to add SID History to an account failed.
		4767	A user account was unlocked.
		4780	The ACL was set on accounts which are members of administrators groups.
		4781	The name of an account was changed:
		4794	An attempt was made to set the Directory Services Restore Mode.
		4798	A user's local group membership was enumerated.
		5376	Credential Manager credentials were backed up.
		5377	Credential Manager credentials were restored from a backup.
Detailed Tracking	DPAPI Activity	4692	Backup of data protection master key was attempted.
		4693	Recovery of data protection master key was attempted.
		4694	Protection of auditable protected data was attempted.
		4695	Unprotection of auditable protected data was attempted.
		4688	A new process has been created.
	Process Creation	4696	A primary token was assigned to process.
		4689	A process has exited.
	RPC Events	5712	A Remote Procedure Call (RPC) was attempted.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

Category	Subcategory	ID	Message Summary
DS Access	Detailed Directory Service Replication	4928	An Active Directory replica source naming context was established.
		4929	An Active Directory replica source naming context was removed.
		4930	An Active Directory replica source naming context was modified.
		4931	An Active Directory replica destination naming context was modified.
		4934	Attributes of an Active Directory object were replicated.
		4935	Replication failure begins.
		4936	Replication failure ends.
		4937	A lingering object was removed from a replica.
DS Access	Directory Service Access	4662	An operation was performed on an object.
		5136	A directory service object was modified.
	Directory Service Changes	5137	A directory service object was created.
		5138	A directory service object was undeleted.
		5139	A directory service object was moved.
		5141	A directory service object was deleted.
	Directory Service Replication	4932	Synchronization of a replica of an Active Directory naming context has begun.
		4933	Synchronization of a replica of an Active Directory naming context has ended.
Logon/Logoff	Account Lockout	4625	An account failed to logon
		4978	During Extended Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
		4979	IPsec Main Mode and Extended Mode security associations were established.
		4980	
		4981	
		4982	
		4983	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

Category	Subcategory	ID	Message Summary
		4984	An IPsec Extended Mode negotiation failed. The corresponding Main Mode security association has been deleted.
Logon/Logoff	IPsec Main Mode	4646	IKE DoS-prevention mode started.
		4650	An IPsec Main Mode security association was established. Extended Mode was not enabled. Certificate authentication was not used.
		4651	An IPsec Main Mode security association was established. Extended Mode was not enabled. A certificate was used for authentication.
	IPsec Main Mode	4652	An IPsec Main Mode negotiation failed.
		4653	An IPsec Main Mode negotiation failed.
		4655	An IPsec Main Mode security association ended.
		4976	During Main Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
		5049	An IPsec Security Association was deleted.
		5453	An IPsec negotiation with a remote computer failed because the IKE and AuthIP IPsec Keying Modules (IKEEXT) service is not started.
	IPsec Quick Mode	4654	An IPsec Quick Mode negotiation failed.
		4977	During Quick Mode negotiation, IPsec received an invalid negotiation packet. If this problem persists, it could indicate a network issue or an attempt to modify or replay this negotiation.
		5451	An IPsec Quick Mode security association was established.
		5452	An IPsec Quick Mode security association ended.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

Category	Subcategory	ID	Message Summary
Logon/Logoff	Logoff	4634	An account was logged off.
		4647	User initiated logoff.
	Logon	4624	An account was successfully logged on.
		4625	An account failed to log on.
		4626	User/Device claims information.
		4627	Group membership information.
		4648	A logon was attempted using explicit credentials.
		4675	SIDs were filtered.
	Network Policy Server	6272	Network Policy Server granted access to a user.
		6273	Network Policy Server denied access to a user.
		6274	Network Policy Server discarded the request for a user.
		6275	Network Policy Server discarded the accounting request for a user.
		6276	Network Policy Server quarantined a user.
		6277	Network Policy Server granted access to a user but put it on probation because the host did not meet the defined health policy.
		6278	Network Policy Server granted full access to a user because the host met the defined health policy.
		6279	Network Policy Server locked the user account due to repeated failed authentication attempts.
		6280	Network Policy Server unlocked the user account.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

Category	Subcategory	ID	Message Summary
Logon/Logoff	Other Logon/Logoff Events	4649	A replay attack was detected.
		4778	A session was reconnected to a Window Station.
		4779	A session was disconnected from a Window Station.
		4800	The workstation was locked.
		4801	The workstation was unlocked.
		4802	The screen saver was invoked.
		4803	The screen saver was dismissed.
	Other Logon/Logoff Events	5378	The requested credentials delegation was disallowed by policy.
		5632	A request was made to authenticate to a wireless network.
		5633	A request was made to authenticate to a wired network.
	Special Logon	4964	Special groups have been assigned to a new logon.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

Category	Subcategory	ID	Message Summary
Object Access	Application Generated	4665	An attempt was made to create an application client context.
		4666	An application attempted an operation:
		4667	An application client context was deleted.
		4668	An application was initialized.
	Central Policy Staging	4818	Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy
	Certification Services	4868	The certificate manager denied a pending certificate request.
		4869	Certificate Services received a resubmitted certificate request.
		4870	Certificate Services revoked a certificate.
		4871	Certificate Services received a request to publish the certificate revocation list (CRL).
		4872	Certificate Services published the certificate revocation list (CRL).
		4873	A certificate request extension changed.
		4874	One or more certificate request attributes changed.
		4875	Certificate Services received a request to shutdown.
		4876	Certificate Services backup started.
		4877	Certificate Services backup completed.
		4878	Certificate Services restore started.
		4879	Certificate Services restore completed.
		4880	Certificate Services started.
		4881	Certificate Services stopped.
		4882	The security permissions for Certificate Services changed.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

Category	Subcategory	ID	Message Summary
Object Access	Certification Services	4883	Certificate Services retrieved an archived key.
		4884	Certificate Services imported a certificate into its database.
		4885	The audit filter for Certificate Services changed.
		4886	Certificate Services received a certificate request.
		4887	Certificate Services approved a certificate request and issued a certificate.
		4888	Certificate Services denied a certificate request.
		4889	Certificate Services set the status of a certificate request to pending.
		4890	The certificate manager settings for Certificate Services changed.
		4891	A configuration entry changed in Certificate Services.
		4892	A property of Certificate Services changed.
		4893	Certificate Services archived a key.
		4894	Certificate Services imported and archived a key.
		4895	Certificate Services published the CA certificate to Active Directory Domain Services.
		4896	One or more rows have been deleted from the certificate database.
		4897	Role separation enabled.
		4898	Certificate Services loaded a template.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

Category	Subcategory	ID	Message Summary
Object Access	Detailed File Share	5145	A network share object was checked to see whether the client can be granted desired access.
		5140	A network share object was accessed.
		5142	A network share object was added.
		5143	A network share object was modified.
		5144	A network share object was deleted.
		5168	Spn check for SMB/SMB2 failed.
	File System	4664	An attempt was made to create a hard link.
		4985	The state of a transaction has changed.
		5051	A file was virtualized.
	Filtering Platform Connection	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network.
		5146	The Windows Filtering Platform has blocked a packet.
		5147	A more restrictive Windows Filtering Platform filter has blocked a packet.
		5150	The Windows Filtering Platform has blocked a packet.
		5151	A more restrictive Windows Filtering Platform filter has blocked a packet.
		5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections.
		5155	The Windows Filtering Platform has blocked an application or service from listening on a port for incoming connections.
		5156	The Windows Filtering Platform has allowed a connection.
		5157	The Windows Filtering Platform has blocked a connection.
		5158	The Windows Filtering Platform has permitted a bind to a local port.
		5159	The Windows Filtering Platform has blocked a bind to a local port.
Object Access	Filtering Platform Packet Drop	5152	The Windows Filtering Platform blocked a packet.
		5153	A more restrictive Windows Filtering Platform filter has blocked a packet.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

Category	Subcategory	ID	Message Summary
Object Access	Handle Manipulation	4656	A handle to an object was requested.
		4658	The handle to an object was closed.
		4690	An attempt was made to duplicate a handle to an object.
Object Access	Other Object Access Events	4671	An application attempted to access a blocked ordinal through the TBS.
		4691	Indirect access to an object was requested.
		4698	A scheduled task was created.
		4699	A scheduled task was deleted.
		4700	A scheduled task was enabled.
		4701	A scheduled task was disabled.
		4702	A scheduled task was updated.
Object Access	Other Object Access Events	5148	The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.
		5149	The DoS attack has subsided and normal processing is being resumed.
		5888	An object in the COM+ Catalog was modified.
		5889	An object was deleted from the COM+ Catalog.
		5890	An object was added to the COM+ Catalog.
Object Access	Registry	4657	A registry value was modified.
		5039	A registry key was virtualized.
Object Access	Special	4659	A handle to an object was requested with intent to delete.
		4660	An object was deleted.
		4661	A handle to an object was requested.
		4663	An attempt was made to access an object.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

Category	Subcategory	ID	Message Summary
Policy Change	Audit Policy Change	4715	The audit policy (SACL) on an object was changed.
		4719	System audit policy was changed.
		4817	Auditing settings on an object were changed.
		4902	The Per-user audit policy table was created.
		4904	An attempt was made to register a security event source.
		4905	An attempt was made to unregister a security event source.
		4906	The CrashOnAuditFail value has changed.
		4907	Auditing settings on object were changed.
		4908	Special Groups Logon table modified.
		4912	Per User Audit Policy was changed.
Policy Change	Authentication Policy Change	4713	Kerberos policy was changed.
		4716	Trusted domain information was modified.
		4717	System security access was granted to an account.
		4718	System security access was removed from an account.
		4739	Domain Policy was changed.
		4864	A namespace collision was detected.
		4865	A trusted forest information entry was added.
		4866	A trusted forest information entry was removed.
		4867	A trusted forest information entry was modified.
		4703	A token right was adjusted.
Policy Change	Authorization Policy Change	4704	A user right was assigned.
		4705	A user right was removed.
		4706	A new trust was created to a domain.
		4707	A trust to a domain was removed.
		4714	Encrypted data recovery policy was changed.
		4911	Resource attributes of the object were changed.
		4913	Central Access Policy on the object was changed.
		4709	IPsec Services was started.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

Category	Subcategory	ID	Message Summary
		4710	IPsec Services was disabled.
Policy Change	Filtering Platform Policy Change	4711	<p>May contain any one of the following:</p> <ul style="list-style-type: none">PAStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.PAStore Engine applied Active Directory storage IPsec policy on the computer.PAStore Engine applied local registry storage IPsec policy on the computer.PAStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.PAStore Engine failed to apply Active Directory storage IPsec policy on the computer.PAStore Engine failed to apply local registry storage IPsec policy on the computer.PAStore Engine failed to apply some rules of the active IPsec policy on the computer.PAStore Engine failed to load directory storage IPsec policy on the computer.PAStore Engine loaded directory storage IPsec policy on the computer.PAStore Engine failed to load local storage IPsec policy on the computer.PAStore Engine loaded local storage IPsec policy on the computer.PAStore Engine polled for changes to the active IPsec policy and detected no changes.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

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

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

Category	Subcategory	ID	Message Summary
		5449	A Windows Filtering Platform provider context has been changed.
		5450	A Windows Filtering Platform sub-layer has been changed.
		5456	PASStore Engine applied Active Directory storage IPsec policy on the computer.
		5457	PASStore Engine failed to apply Active Directory storage IPsec policy on the computer.
		5458	PASStore Engine applied locally cached copy of Active Directory storage IPsec policy on the computer.
		5459	PASStore Engine failed to apply locally cached copy of Active Directory storage IPsec policy on the computer.
		5460	PASStore Engine applied local registry storage IPsec policy on the computer.
		5461	PASStore Engine failed to apply local registry storage IPsec policy on the computer.
		5462	PASStore Engine failed to apply some rules of the active IPsec policy on the computer. Use the IP Security Monitor snap-in to diagnose the problem.
		5463	PASStore Engine polled for changes to the active IPsec policy and detected no changes.
		5464	PASStore Engine polled for changes to the active IPsec policy, detected changes, and applied them to IPsec Services.
		5465	PASStore Engine received a control for forced reloading of IPsec policy and processed the control successfully.
		5466	PASStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory cannot be reached, and will use the cached copy of the Active Directory IPsec policy instead. Any changes made to the Active Directory IPsec policy since the last poll could not be applied.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

Category	Subcategory	ID	Message Summary
Policy Change	Filtering Platform Policy Change	5467	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, and found no changes to the policy. The cached copy of the Active Directory IPsec policy is no longer being used.
		5468	PAStore Engine polled for changes to the Active Directory IPsec policy, determined that Active Directory can be reached, found changes to the policy, and applied those changes. The cached copy of the Active Directory IPsec policy is no longer being used.
		5471	PAStore Engine loaded local storage IPsec policy on the computer.
		5472	PAStore Engine failed to load local storage IPsec policy on the computer.
		5473	PAStore Engine loaded directory storage IPsec policy on the computer.
		5474	PAStore Engine failed to load directory storage IPsec policy on the computer.
		5477	PAStore Engine failed to add quick mode filter.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
Configuring Log Sources

Category	Subcategory	ID	Message Summary
Policy Change	MPSSVC Rule-Level Policy Change	4944	The following policy was active when the Windows Firewall started.
		4945	A rule was listed when the Windows Firewall started.
		4946	A change has been made to Windows Firewall exception list. A rule was added.
		4947	A change has been made to Windows Firewall exception list. A rule was modified.
		4948	A change has been made to Windows Firewall exception list. A rule was deleted.
		4949	Windows Firewall settings were restored to the default values.
		4950	A Windows Firewall setting has changed.
		4951	A rule has been ignored because its major version number was not recognized by Windows Firewall.
		4952	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.
		4953	A rule has been ignored by Windows Firewall because it could not parse the rule.
		4954	Windows Firewall Group Policy settings have changed. The new settings have been applied.
		4956	Windows Firewall has changed the active profile.
		4957	Windows Firewall did not apply the following rule:
		4958	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer:

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

Category	Subcategory	ID	Message Summary
Policy Change	Other Policy Change Events	4819	Central Access Policies on the machine have been changed.
		4909	The local policy settings for the TBS were changed.
		4910	The group policy settings for the TBS were changed.
		5063	A cryptographic provider operation was attempted.
		5064	A cryptographic context operation was attempted.
		5065	A cryptographic context modification was attempted.
		5066	A cryptographic function operation was attempted.
		5067	A cryptographic function modification was attempted.
		5068	A cryptographic function provider operation was attempted.
		5069	A cryptographic function property operation was attempted.
		5070	A cryptographic function property modification was attempted.
		5447	A Windows Filtering Platform filter has been changed.
		6144	Security policy in the group policy objects has been applied successfully.
		6145	One or more errors occurred while processing security policy in the group policy objects.
Policy Change	Subcategory (special)	4670	Permissions on an object were changed.
Privilege Use	Sensitive Privilege Use / Non Sensitive Privilege Use	4672	Special privileges assigned to new logon.
		4673	A privileged service was called.
		4674	An operation was attempted on a privileged object.
System	IPsec Driver	4960	IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations.
		4961	IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer.
		4962	IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

Category	Subcategory	ID	Message Summary
System	IPsec Driver	4963	IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt.
		4965	IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored.
		5478	IPsec Services has started successfully.
		5479	IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
		5480	IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
		5483	IPsec Services failed to initialize RPC server. IPsec Services could not be started.
		5484	IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks.
		5485	IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem.
System	Other System Events	4820	A Kerberos Ticket-granting-ticket (TGT) was denied because the device does not meet the access control restrictions.
		4821	A Kerberos service ticket was denied because the user, device, or both does not meet the access control restrictions.
		4822	NTLM authentication failed because the account was a member of the Protected User group.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector
 Configuring Log Sources

Category	Subcategory	ID	Message Summary
System	Other System Events	4823	NTLM authentication failed because access control restrictions are required.
		4824	Kerberos preauthentification by using DES or RC4 failed because the account was a member of the Protected User group
		4826	Boot Configuration Data Loaded.
		5024	The Windows Firewall Service has started successfully.
		5025	The Windows Firewall Service has been stopped.
		5027	The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.
		5028	The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.
		5029	The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.
		5030	The Windows Firewall Service failed to start.
		5032	Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network.
		5033	The Windows Firewall Driver has started successfully.
		5034	The Windows Firewall Driver has been stopped.
		5035	The Windows Firewall Driver failed to start.
		5037	The Windows Firewall Driver detected critical runtime error. Terminating.
		5058	Key file operation.
		5059	Key migration operation.
		6400	BranchCache: Received an incorrectly formatted response while discovering availability of content.
		6401	BranchCache: Received invalid data from a peer. Data discarded.
		6402	BranchCache: The message to the hosted cache offering it data is incorrectly formatted.

Configuration Guide for Microsoft Windows Event Log - Native SmartConnector

Configuring Log Sources

Category	Subcategory	ID	Message Summary
System	Other System Events	6403	BranchCache: The hosted cache sent an incorrectly formatted response to the client.
		6404	BranchCache: Hosted cache could not be authenticated using the provisioned SSL certificate.
		6405	BranchCache: %2 instance(s) of event id %1 occurred.
		6406	%1 registered to Windows Firewall to control filtering for the following: %2
		6407	1%
		6408	Registered product %1 failed and Windows Firewall is now controlling the filtering for %2
System	Security State Change	4608	Windows is starting up.
		4609	Windows is shutting down.
		4616	The system time was changed.
		4621	Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded.
System	Security System Extension	4610	An authentication package has been loaded by the Local Security Authority. Native Connector: An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts.
		4611	This logon process will be trusted to submit logon requests.
		4614	A notification package has been loaded by the Security Account Manager.
		4622	A security package has been loaded by the Local Security Authority.
		4697	A service was installed in the system.

Category	Subcategory	ID	Message Summary
System	System Integrity	4612	Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
		4615	Invalid use of LPC port.
		4618	A monitored security event pattern has occurred.
		4816	RPC detected an integrity violation while decrypting an incoming message.
		5038	Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.
		5056	A cryptographic self test was performed.
		5057	A cryptographic primitive operation failed.
		5060	Verification operation failed.
		5061	Cryptographic operation.
		5062	A kernel-mode cryptographic self test was performed.
		6281	Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error

Troubleshooting

This section has the following information:

Unable to Receive Events from any Host if One or More Hosts were Down

Issue: If the Windows Event Log - Native connector is running on Windows Server 2019 and one of the Windows events source machines is down, then the connector is unable to read events from the other event source machine. And, EPS drops to 0 in **wincagent.log**.

Workaround:

To fix this issue, the following properties have been added in the **agent.default.properties** file:

```
winc.winc-agent.checkHostStatusViaWmi=
winc.winc-agent.checkHostStatusViaPing=false
winc.winc-agent.endpointReconnectInterval=300000
winc.winc-agent.OStoCheckHostAlive=Windows Server 2019 Standard
```



Note: By default, the **winc.winc-agent.checkHostStatusViaWmi** parameter is blank, which means it uses the WMI (Windows Management Instrumentation) service to check if a machine is up or down.

If there is no issue with WMI in the event source host machine, then you do not need to change anything in the **agent.properties** file. If the WMI service is running in the host machine, the value of these properties will work by default for Windows Server 2019 Standard.

If the default properties do not work, then consider the following scenarios:

- If WMI is not running and ping is enabled in your environment, then you must add the following properties in **agent.properties**:

```
winc.winc-agent.checkHostStatusViaPing=true
winc.winc-agent.checkHostStatusViaWmi=false
```

- If both WMI and ping are not enabled in your environment, then you must add the following properties in **agent.properties**:

```
winc.winc-agent.checkHostStatusViaWmi=false
winc.winc-agent.checkHostStatusViaPing=false
winc.winc-agent.endpointReconnectInterval=300000
```

winc.winc-agent.endpointReconnectInterval value is specified in millisecond. You can increase or decrease this value as required so that the other connectors will get time to collect events from other hosts that are up.

- If you face any issues with other supported Operating Systems (OS), then you must modify the value of the following property in **agent.properties**:

```
winc.winc-agent.OStoCheckHostAlive=Windows Server 2019 Standard
```

Example:

```
winc.winc-agent.OStoCheckHostAlive=Windows Server 2019 Datacenter
```

Parameters Not Functioning as Expected

Issue: The **RenameFileInTheSameDirectory** and **DeleteFile** parameters are not functioning as expected.

Workaround: The **usenonlockingwindowsfilereader** parameter must be set to **true** in Windows environments for the **RenameFileInTheSameDirectory** and **DeleteFile** parameters to work as expected.

Log Message for Resource Adjustment

Issue: While the connector is starting, it logs that the temporary store will be downsized.

```
2015-01-26 15:11:17,668][ERROR]
[default.org.apache.activemq.broker.BrokerService]
[external] Temporary Store limit is 51200 mb, whilst the temporary data
directory: C:\arcsoft\SmartConnectors\current\activemq-
data\localhost\tmp_storage only has
47568 mb of usable space - resetting to maximum available 47568 mb.
```

Workaround: This message indicates that the system disk space is low. Although this may not cause an immediate impact, check for adequate disk storage to ensure it does not run out while running the connector. To avoid this log message, make sure the system has 50 GB of disk space available.

A Non-administrator User Is Unable to Run Windows Native Connector and the Log File Has Permission Error

For information about this issue, see the [A Non-administrator User Unable to Run Connectors on Windows and the Log File has Permission Error](#) section in ArcSight SmartConnector Installation Guide.

Unable to extend buffer beyond 1048576

Issue: By default, the maximum buffer size is set to 1048576. To increase the buffer size, `agents[0].tcpmaxbuffersize=10240` must be updated when the raw event size is large to avoid the events from getting truncated.

Workaround: The agents[0].tcpmaxbuffersize parameter must be added and set to a higher value in the agent.properties file to avoid the messages from getting truncated.

Connector is unable to receive events and displays error after upgrading to version 8.4.0

Issue: After upgrading to version 8.4.0, connector is unable to receive events and the following error is logged in the wincagent.log:

```
MQMessageSender - SSL Error: RemoteCertificateNameMismatch,  
RemoteCertificateChainErrors
```

```
MQMessageSender - Failed to create SSL_stream. Exception: The remote  
certificate is invalid according to the validation procedure
```

This issue occurs when there is a hostname mismatch in the connector-generated certificate after the first successful installation of the Microsoft Windows Event Log - Native connector.

Workaround: Complete the following procedure to generate a new set of certificates for internal communication:

1. Stop the Microsoft Windows Event Log – Native connector.
2. Add the following parameters in <install location>/current/user/agent/agent.properties. This will generate new set of certificates for the WiNC connector and will be consumed for internal component communication.

```
syslogng.tls.cert.file=user/agent/winc-  
ng.cert  
syslogng.tls.keystore.file=user/agent/winc_  
management.p12  
syslogng.tls.fips.keystore.file=user/agent/winc_  
management.fips.p12
```

3. Start the Microsoft Windows Event Log – Native connector.

Appendix: Internal Events

The Windows Event Log – Native connector documents the following types of internal events:

- [Specific Windows Security Event Mappings](#)
- [Collector Connected](#)
- [Collector Disconnected](#)
- [Collector Up](#)
- [Collector Down](#)
- [Collector Configuration Accepted](#)
- [Collector Status Updated](#)
- [Collector Event Collection Started](#)
- [Remote Agent Status](#)

Specific Windows Security Event Mappings

General

ArcSight Field	Vendor Field
Device Vendor	'Microsoft'
Device Product	'Microsoft Windows'

104

ArcSight ESM Field	Device-Specific Field
Name	'The log file was cleared'
Message	concatenate('The ',Channel,' log file was cleared')
Source Nt Domain	SubjectDomainName
Source User Name	SubjectUserName
File Type	Channel
File Path	BackupPath

1100

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

1101

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

1102

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

1104

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

1105

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

Collector Connected

Field	Description
Event Name	'Collector'
Device Event Category	'/Informational'
Agent Severity	'2'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Disconnected

Field	Description
Event Name	'Collector Disconnected'
Device Event Category	'/Informational/Warning'
Agent Severity	'3'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Up

Field	Description
Event Name	'Collector Up'
Device Event Category	'/Informational'

Field	Description
Agent Severity	'2'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Down

Field	Description
Event Name	'Collector Down'
Device Event Category	'/Informational/Warning'
Agent Severity	'3'
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Status Updated

Collector Status for “Collector Status Updated”

Field	Description
Event Name	'Collector Status Updated'
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason

Field	Description
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Host Status for “Collector Status Updated”

Field	Description
Event Name	'Collector Status Updated'
Device Host Name	<DeviceHostName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3, depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Event Log Status for “Collector Status Updated”

Field	Description
Event Name	'Collector Status Updated'
Device Host Name	<DeviceHostName>
Device Custom String 3 Label	'Event Log'
Device Custom String 3	<ConfiguredEventLogName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason

Field	Description
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Event Collection Started

Collector Status for “Collector Collection Started”

Field	Description
Event Name	'Collector Collection Started'
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Host Status for “Collector Collection Started”

Field	Description
Event Name	'Collector Collection Started'
Device Host Name	<DeviceHostName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason

Field	Description
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Event Log Status for “Collector Collection Started”

Field	Description
Event Name	'Collector Collection Started'
Device Host Name	<DeviceHostName>
Device Custom String 3 Label	'Event Log'
Device Custom String 3	<ConfiguredEventLogName>
Reason	<Event Collection SuccessStatus/FailureReason>
Device Event Category	'/Informational' or '/Informational/Warning' depending on the reason
Agent Severity	'2' or '3' depending on the reason
Device Custom String 1 Label	'Collector Host Name'
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	'Collector Domain Name'
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	'Collector Operating System Version'
Device Custom String 5	<Collector Operating System Version>

Collector Configuration Accepted

Collector Status for “Collector Configuration Accepted”

Field	Description
Event Name	‘Collector Configuration Accepted’
Reason	<SuccessStatus/FailureReason>
Device Event Category	‘/Informational’ or ‘/Informational/Warning’ depending on the reason
Agent Severity	‘2’ or ‘3’ depending on the reason
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<Collector Operating System Version>

Host Status for “Collector Configuration Accepted”

Field	Description
Event Name	‘Collector Configuration Accepted’
Device Host Name	<DeviceHostName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	‘/Informational’ or ‘/Informational/Warning’ depending on the reason
Agent Severity	‘2’ or ‘3’ depending on the reason
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<Collector Operating System Version>

Event Log Status for “Collector Configuration Accepted”

Field	Description
Event Name	‘Collector Configuration Accepted’
Device Host Name	<DeviceHostName>
Device Custom String 3 Label	‘Event Log’
Device Custom String 3	<ConfiguredEventLogName>
Reason	<SuccessStatus/FailureReason>
Device Event Category	‘/Informational’ or ‘/Informational/Warning’ depending on the reason
Agent Severity	‘2’ or ‘3’ depending on the reason
Device Custom String 1 Label	‘Collector Host Name’
Device Custom String 1	<Collector Host Name>
Device Custom String 2 Label	‘Collector Domain Name’
Device Custom String 2	<Collector Domain Name>
Device Custom String 5 Label	‘Collector Operating System Version’
Device Custom String 5	<Collector Operating System Version>

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 Configuration Guide for Microsoft Windows Event Log - Native SmartConnector (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnector

Software Version: CE 24.3

Configuration Guide for ArcSight Event Categorization Whitepaper

Document Release Date: July 2024

Software Release Date: July 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

ArcSight Event Categorization: A Technical Perspective	4
Technical Overview	4
Object	4
Behavior	4
Outcome	4
Technique	5
Device Group	5
Device Type	5
Significance	6
Motivation	6
Uniform Resource Identifiers (URI)	7
Tuple Descriptions	7
Examples of Categorizations and their Tuples	8
Firewall	8
Operating Systems and Applications	8
Host IDS, Operating Systems, and Applications	11
Host and Network IDS /IPS	12
Assessment Tool	18
Categorization Lifecycle	18
ArcSight Update Packs (AUPs)	19
Custom Categorization	19
How to Categorize Events	20
Individual Category Values	21
Object	21
Behavior	25
Outcome	28
Technique	29
Device Group	33
Device Type	35
Significance	38
Send Documentation Feedback	39

ArcSight Event Categorization: A Technical Perspective

This technical note describes ArcSight event categorization from a technical perspective. The document is meant for anyone who needs to understand ArcSight's categorization schema.

This document provides some basic information about the categorization schema, as well as how the categorization is exposed in the product.

It also explains how to install content updates (AUPs) and how to customize categorization.

Every possible value of the categorization fields are explained, so this document is meant to be used as a dictionary to get an understanding of all the categorization entries.

Technical Overview

The ArcSight Taxonomy uses seven dimensions (fields) to characterize an event. This means that we capture seven independent properties of an event. It helps to think about it in a way that events can be sliced and grouped in seven different independent ways. Following is a description of all of the dimensions:

Object

Events are always about a certain object. An object can, for example, be an application, the operating system, a database, a file, or the memory of a server. It is important to realize that we are referring to the targeted object or the focus of the event. It is not about who is doing something, but what is the object being accessed, altered, etc. or what is the focus of the event.

Behavior

Events not only refer to certain objects, but there is generally an action or a behavior associated with an event. What is being done to an object? Behaviors include access, execution, or modification, and so on.

Outcome

With the first two dimensions, we know what object is being referred to and what action targeted the object. However, we do not know whether the behavior was successful or not. Therefore, the outcome is a success, a failure, or an attempt. An attempt really indicates that

something was neither a success nor a failure and the outcome is not clear or there is no statement that could be made about the outcome.

Technique

Frequently, in a security context, we would like to get information about the type of events with respect to a security domain. Is an event talking about a denial of service, a brute force attack, IDS evasions, exploits of vulnerabilities, and so on.

Using all of this information we now can issue queries to the system that give us, for example, all of the successful DoS (denial of service) attacks that target databases. What would the conditions be?

Category Technique = /DoS

Category Object = /Host/Application/Database

Category Outcome = /Success

The URI notation used here is described below.

Device Group

Many devices serve a multitude of purposes in one product. Intrusion Prevention Systems, for example, generate events associated with their firewall capabilities, as well as their intrusion detection capabilities. Routers can generate events associated with user authentication, etc. To distinguish between these types of events, we introduced a dimension called Device Group. This dimension lets us query, for example, all the firewall-type events as opposed to all the events generated by a firewall. The distinction is that the former query also returns all the firewall messages in, for example, the operating system logs (such as iptables). Or, in the case of an intrusion prevention system, it has two types of events. One type about firewall-type events (for example, blocking and passing traffic) and the other type being intrusion detection style messages

(for example, detection of malicious behavior). The former type would contain the value 'Firewall' in the Device Group and the latter would be 'IDS.'

Device Type

This dimension lets us query for all types of events generated by a certain device type, no matter what device group the events belong to. For example, the events of the Device Type "firewall" are all the events generated by the Firewalls (Checkpoint, Cisco ASA, Juniper Firewall, etc.) no matter if those events are about blocking traffic or adding new users or restarting the device.

Sometimes security analysts might want to get logs from the same type of device regardless of the specific capability that had made the detection. Without this field, it is not possible to run a report to get events, for example, from all the firewalls or from all the routers in a company. The only way to accomplish that was to search for product names. And if the company used different products, the report would have to include all the names from all those products, which will eventually affect performance and will be a challenge to maintain.

The device type field was added to identify the device regardless of the type of event. For example, a Cisco router will have a device type of Router whether the event is about a communication being blocked, or someone authenticating through a secure tunnel across the internet.

Significance

We need the capability to separate normal events from hostile events. We also need to know whether certain activity reported by the device impacts the availability, confidentiality, or integrity of our systems. All this information is captured in the significance.

Significance expresses the broad characterization of events from a device's perspective. This determination is built into ArcSight's categorization efforts.

Motivation

All the content in ESM heavily relies on the categorization of events. ArcSight SmartConnectors not only parse events into syntactical tokens, but they also add semantic information in the form of categories such that the ArcSight Manager can later correlate these events. All content in ESM (rules, reports, data monitors, event graphs, pattern discovery, and so on) depends heavily on categories.

One of the biggest challenges that ArcSight ESM overcomes is that security devices (or devices in general) do not utilize a common naming schema to report events. For example, sensors A and B might refer to the same instance of an attack with completely different names. While one of them might use a number, the other might use a name. The solution to this problem is to map all the individual signatures to a common taxonomy, which can then be used to write sensor-independent content.

Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

The following is a list of benefits created by the ArcSight taxonomy:

- Vendor independence, mainly for content creation.
- Analysts do not need to remember specific nomenclatures for all the devices in the environment.
- ArcSight Taxonomy immediately captures event impact.
- Content generation is easier and more effective (Rules, Data Monitors, Forensic Analysis, Reports, Pattern Discovery).
- Content is generic (to support a new IDS, none of the rules have to be rewritten, because they utilize the categorized events).
- More powerful content can be written, for example, correlation rules can reason about “failures” and “successes” as opposed to relying upon the reporting devices.

Uniform Resource Identifiers (URI)

All the category fields in ArcSight use URIs (for example, /Host/Resource/Memory). URIs introduce a hierarchy/ relationship among values. On the content side, the following functions can be used to utilize this hierarchy:

`startsWith() endsWith() contains() matches()`

The above four functions help build flexible content. The `contains()` function checks whether a certain string is contained in the value. `startsWith()` looks for categories starting with a given expression. The `endsWith()` function, contrary to `startsWith()`, looks for categories ending with the given expression. The `matches()`function takes a regular expression to match a certain expression. For example, a report which lists all the events reporting resource errors, would use the following conditions:

`Category Object startsWith /Host/Resource`

`Category Significance = /Informational/Error`

This will then include all the children of /Host/Resource, such as /Host/Resource/Memory or /Host/Resource/CPU.

Tuple Descriptions

Our use of **tuple** is the collection of all the seven category fields. Along with the categorization of events, ArcSight introduced the concept of tuple descriptions. They are English text-descriptions of an event. These descriptions talk about an event from a very abstract level. We have provided a list of common tuples in this whitepaper. However, we will provide a complete list in the upcoming updates.

One value that this provides is that an analyst does not have to be an expert in all the different kinds of security devices and applications, but you may look at the tuple description to understand roughly what is going on.

Examples of Categorizations and their Tuples

The following list of tuples can be used to either categorize events or when building content (rules, reports, datamonitor, etc.). They are best used as a reference. Every category entry in every column can be combined with every category in the other column.



Note: The Device Type has no effect on the tuple, while the Device Group has.

Firewall

Network communication was allowed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application	Communicate		Firewall	Success	Informational
Host/Application/Service	Communicate/Query				

Network communication was blocked.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application	Communicate		Firewall	Failure	Informational/ Warning
Host/Application/Service	Communicate/Query				

Operating Systems and Applications

Component was found defective.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/Interface	Found/Defective		OS	Success	Informational/ Alert

Task execution was successful.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application	Execute		Application	Success	Informational
Host/Application/Service	Execute/Query		Operating System		
Host/Application/Database	Execute/Response				

Task execution failed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Execute		Application	Failure	Informational/Warning
Host/Application	Execute/Query		Operating System		Informational/Alert
Host Application/Service					Informational/Error
Host/Application/Database					

Configuration modification was successful.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Modify/Configuration		Application	Success	Informational
Host/Application			Operating System		Informational/Warning
Host/Application/Service					Informational/Alert
Host/Application/Database					

Configuration modification was attempted

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Modify/Configuration		Application	Attempt	Informational
Host/Application			Operating System		Informational/Warning
Host/Application/Service					
Host/Application/Database					

Configuration modification has failed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Modify/Configuration		Application	Failure	Informational/Warning
Host/Application			Operating System		Informational/Alert
Host/Application/Service					Informational/Error
Host/Application/Database					

System access was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application	Access		Application	Attempt	Informational
Host/Application/Service					
Process start was successful.					
Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/Process	Execute/Start		Application	Success	Informational

Exhausted resource was reported.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/Memory	Found/Exhausted		Application	Success	Informational/Warning Informational/Alert Informational/Error

File creation failed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/File	Create		Application	Failure	Informational/Warning Informational/Alert Informational/Error

Successful privilege modification was reported

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Operating System	Authorization/Modify		Application	Success	Informational
Host/Resource/File			Operating System		Informational/Warning
Host/Application/Service					Informational/Alert
Host/Resource/Registry					

Resource exhaustion was reported.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource	Found/Exhausted		Operating System	Success	Informational/Alert

Successful login

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application	Authorization/Verify		Application	Success	Informational
Host/Application/Service			Operating System		
Host/Application/Database					
Host/Operating System					

Failed login

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application	Authorization/Verify		Application	Failure	Informational/Warning
Host/Application/Service			Operating System		
Host/Application/Database					
Host/Operating System					

Database access was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Database	Access		Application	Attempt	Informational
	Access/Start				

Database shutdown was successful

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Database	Execute/Stop		Application	Success	Informational/Warning
					Informational/Warning

Connection to a database failed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Database	Communicate/Query		Application	Failure	Informational/Error

Host IDS, Operating Systems, and Applications

File access was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/File	Access		IDS/Host	Attempt	Informational
	Access/Start		Application		Informational/Warning
			Operating System		Informational/Alert

Service start was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Execute/Start		IDS /Host	Attempt	Informational
			Application		
			Operating System		

Service start failed.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Execute/Start		IDS/Host	Failure	Informational/Warning
			Application		Informational/Alert
			Operating System		Informational/Error

Service stop was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Execute/Stop		IDS/Host	Attempt	Informational
			Application		Informational/Warning
			Operating System		Informational/Error

Host and Network IDS /IPS

Access to resource was attempted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource	Access		IDS/Host	Attempt	Informational/Warning Informational/Alert
Modification of a res	ource was attempted.				
Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Resource/File	Modify		IDS/Host	Attempt	Informational

Brute Force attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Authorization/Verify	Brute	IDS/Network	Attempt	Compromise
Host/Application		Force/Login	IDS/Host		
Host/Operating System					

Denial of Service attack was detected

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Communicate	DoS	IDS/Host	Attempt	Compromise
Host/Application/Database	Communicate/Query		IDS/Network		
Host/Operating System					
Host/Application					
Host/Resource/Interface					
Network					

Anomalous traffic was detected

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Communicate	Traffic	IDS/Network	Attempt	Suspicious
Host/Application	Communicate/Query	Anomaly/...	IDS/Host		
Host/Operating System					
Host/Resource/Interface					
Network					

Vulnerability exploit was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Communicate	Exploit/Vulnerability	IDS/Network	Attempt	Compromise
Host/Application	Communicate/Query				
Host/Application/Service					

Injection attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Communicate	Code/Application	IDS/Network	Attempt	Compromise
Host/Application	Communicate/Query	Command			
Host/Application/DB					
Host/Application/Service					
Host/Operating System					

Directory traversal attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Communicate	Exploit//DirectoryTraversal	IDS/Network	Attempt	Compromise
Host/Application	Communicate/Query				
Host/Application/DB					
Host/Application/Service					
Host/Operating System					

Privilege escalation attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Communicate	Exploit/Privilege Escalation	IDS/Network	Attempt	Compromise
Host/Application	Communicate/Query				
Host/Application/DB					
Host/Application/Service					
Host/Operating System					

Policy breach was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Communicate	Policy/Breach	IDS/Network	Attempt	Info/Warning
Host/Application	Communicate/Query				
Host/Application/DB					
Host/Application/Service					
Host/Operating System					
Network					

Potentially harmful traffic was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Communicate	Policy/Malevolence	IDS/Network	Attempt	Suspicious
Host/Application	Communicate/Query				
Host/Application/DB					
Host/Application/Service					
Host/Operating System					

Redirection attack was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Communicate	Redirection	IDS/Network	Attempt	Compromise
Host/Application	Communicate/Query	Redirection/Application			
Host/Application/DB		Redirection/DNS			
Host/Application/Service		Redirection/ICMP			
Host/Operating System					

Infected system was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Malware/Adware	Found	N/A	IDS/Network	Success	Compromise
/Backdoor				Failure	Informational/Warning
/Spyware				Attempt	Compromise
/Virus					
/Worm					
Note: These categorizations can have the source as the target and not the destination.					

Scanning activity was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Communicate	Scan	IDS/Network	Attempt	Recon
Host/Application	Communicate/Query	Scan/Service		Success	
Host/Application/Service		Scan/Port			
Host/Application/System		Scan/Vulnerability			
Host/Operating System					
Host/Application/Malware/Backdoor					
Host/Application/Malware/DoS Client					

Malware was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Malware	Found		IDS/Network	Attempt	Compromise
Malware activity was detected.					
Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Malware	Communicate Communicate/Query		IDS/Network	Attempt	Compromise

Anti-virus Malware infection was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Malware/Adware /Backdoor /Spyware /Virus /Worm	Found	N/A	IDS/Host/AntiVirus	Success Failure Attempt	Compromise
Note: It is possible for these categorizations to have the source as the target and not the destination.					

Malware installation was detected.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host /Application /Malware	Create	N/A	IDS/Host/AntiVirus	Success	Compromise
/Adware				Failure	Informational/Warning
/Backdoor				Attempt	Compromise
/Spyware					
/Virus					
/Worm					

Malware deletion was reported.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host /Application /Malware	Delete	N/A	IDS/Host/AntiVirus	Success	Informational/Warning
/Adware				Failure	Compromise
/Backdoor				Attempt	Compromise
/Spyware					
/Virus					
/Worm					

Scan for malware in progress.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Execute/Query	Scan	IDS/Host/AntiVirus	Attempt	Informational
Host/Application					
Host/Application/DB					
Host/Application/Service					
Host/Operating System					
Network					

Scan for malware has started.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Execute/Start	Scan	IDS/Host/AntiVirus	Success	Informational
Host/Application					
Host/Application/DB					
Host/Application/Service					
Host/Operating System					
Network					

Scan for malware is aborted.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application/Service	Execute/Stop	Scan	IDS/Host/AntiVirus	Success	Informational/Warning
				Failure	Informational/Error
				Attempt	Informational/Warning

Task execution was blocked.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Execute/Stop	N/A	IDS/Host/AntiVirus	Success	Informational/Warning
				Failure	Informational/Error
				Attempt	Compromise
Host/Application					
Host/Application/DB					
Host/Application/Service					
Host/Operating System					

Malware quarantine was reported.

Object	Behavior	Technique	Device Group	Outcome	Significance
Host	Modify/Attribute	N/A	IDS/Host/AntiVirus	Success	Informational/Warning
				Failure	Compromise
				Attempt	
Host/Application					
Host/Resource/File					

Assessment Tool

Object	Behavior	Technique	Device Group	Outcome	Significance
Host/Application	Found/Vulnerable		Assessment Tool	Failure	Informational/Alert

Categorization Lifecycle

Out of the box, ArcSight SmartConnectors contain content dating from the last major ArcSight release. This means that all the content updates which happened between the last release and the current date will not be included in the connector release. When the next Connector Framework version is released, the connector content is synchronized again. In the meantime, if you have a content subscription, you can download the latest Content AUP from ArcSight's software site. These updates are commonly referred to as ArcSight Updates (AUPs).

If there is a need to categorize events before ArcSight releases categorization or there is a need to overwrite certain ArcSight provided categories, custom categorizations can be deployed. This is the only way categorization can be changed (by overwriting the ArcSight provided categories). An even more important case for categorization is one in which custom signatures are deployed on, for example, intrusion detection systems. ArcSight has no way of knowing those signatures. Therefore, you are responsible for categorizing those events. AUPs and custom categorization are explained in the following sections.

ArcSight Update Packs (AUPs)

ArcSight delivers categorization updates on a regular basis. These updates are called AUP (ArcSight Update Pack) and are delivered to you with a content subscription on a regular basis. These updates contain the very latest categorization files for all the ArcSight connectors.

To apply one of these updates, replace the existing .aup file in your ArcSight ESM Manager's /updates directory. The Manager automatically finds the new content and pushes it to your SmartConnectors. The affected SmartConnectors each trigger an event with a Device Event Class ID of agent:025 when the update occurs. The event will show up on your Console for you to verify that the update has successfully taken place. The

name field of the event will have the current version of the AUP, and the SmartConnector ID that was updated.

To verify which AUP a certain connector is running, use the navigator in the Console to go to the connector in question. Right-click on it and select: Send Command -> Status > Get Status. The first line indicates the version of the AUP this connector is using:

Agent Content Version 2020-03-30-19-56-19_8288

If you run into problems while deploying the AUP on the Manager, make sure that the file you downloaded does not have a ".zip" extension, but has an ".aup" extension.

Custom Categorization

Why would you need custom categorization? AUPs (ArcSight Update Pack) are delivered to you with a content subscription on a regular basis. However, if custom signatures are added to a device, ArcSight has no way of supporting them. Also, if a custom connector is built, categorization has to be done manually.

Categorization happens on the ArcSight SmartConnector. The connector contains a mapping table (a categorization file) for each of the devices. A categorization file contains a header-line and is followed by all the categorization entries. The header line looks as follows:

event.deviceEventClassId,set.event.categoryObject,set.event.categoryBehavior,

set.event.categoryTechnique, set.event.categoryDeviceGroup, set.event.categorySignificance, set.event.categoryOutcome, set.event.categoryDeviceType

This tells the connector to look out for Device Event Class (DEC) IDs and, whenever a match is found, it is to set the following seven category fields.

To build a categorization file it is therefore necessary to know about as many possible DEC IDs as possible. The values of those DEC IDs then have to be added to the categorization file along with the correct category entries. A sample entry looks as follows:

```
[1:1919],/Host/Application/Service,/Communicate/Query,/Exploit/Vulnerability,  
/IDS/Network,/Compromise,/Attempt
```

Once the file is generated, it has to be placed under:

```
$AGENT_HOME/user/agent/acp/categorizer/current/<deviceVendor>/<deviceProduct>.csv
```

The values for deviceVendor and deviceProduct can be obtained from an event of this device. The two values need to be sanitized, such that all characters are lowercase and all special characters, including spaces, are to be replaced with an underscore "_". For example, if the vendor is "CheckPoint" and the product is "Firewall/1", the file is:

```
$AGENT_HOME/user/agent/acp/categorizer/current/checkpoint/firewall_1.csv
```

For the changes to take effect, restart the connector. Also, note that the user categorization files will overwrite the ArcSight assigned categories. This means that if the default ArcSight categorization covers a certain event and the connector finds a user entry for it, the user entry gets the precedence. This remains after upgrading the connector version.

Should you deploy an ArcSight AUP file or an ArcSight Connector framework upgrade, be aware that the custom categorization also overwrites all the categorizations in the AUP file and connector framework package. To use the official ArcSight categorization, remove the deviceEventClassIds in question from your custom categorization file.

How to Categorize Events

This section is meant for users that need to categorize events for the ArcSight ESM. It outlines some of the approaches that make categorization easier.

- When categorizing events, it is important to keep in mind that the categories should say what the event is about. No interpretations! If a network-based intrusion detection system (NIDS) reports a denial of service attack, it is probably only an attempt, we cannot know whether it was successful or not. The ArcSight correlation system will handle this decision, utilizing information from other devices.
- Make sure all the fields are defined. Only the technique is an optional field
- If an event does not clearly indicate whether it's a success or not, mark it as an attempt.

- Remember: /Host/Delete means that a host was deleted
- It helps to sometimes think about categorization from a content perspective. How would you write content that utilizes this specific message?
- Always be as specific as possible. An event talking about an interface on a host would not be /Host, but /Host/Resource/Interface
- Always focus on the event only. Don't think about the context of an event and do not attempt to come up with a conclusion. For example, if a system reports multiple unsuccessful logins with a short period of time, we cannot say that it is brute force attack unless the detecting device says that it is a brute force attack.

Individual Category Values

Object

/Actor

Prime movers for events.

/Actor/Agent

An automated system including automated DoS clients, viri, and worms.

/Actor/Cluster

Several affiliated Agents such as a cluster of DDoS clients.

/Actor/Group

Several affiliated Users such as a hacker group, a university, or a nation state.

/Actor/Resource

A resource or object related to a user

/Actor/Role

A user role, used for defining/granting permissions

/Actor/User

A human being.

/Host

Boxen - PDAs, devices connected via Bluetooth, Windows boxes, Linux boxes, etc.

/Host/Application

A software program that is not an obvious part of the operating system itself.

/Host/Application/Database

Should this be separate?

/Host/Application/Database/Data

Operations executed on the data in a database, such as deleting a tuple, updating a tuple, ...

/Host/Application/Instant Messenger

ICQ, Yahoo Messenger, AOL Messenger, ...

/Host/Application/License

An OS license

/Host/Application/Malware

A malware application.

/Host/Application/Malware/Spyware

/Host/Application/Malware/Virus

A self-replicating, persistent infection that also executes other behaviors on the infected host.

/Host/Application/Malware/Worm

A self-replicating, transient infection that primarily exists to infect other hosts.

/Host/Application/Malware/Adware

/Host/Application/Malware/Backdoor

An application that listens for network connections that is meant to give a remote user some measure of control over the host.

/Host/Application/Workflow

A workflow process in an application.

/Host/Application/Malware/DoS Client

An application that will participate in a (possibly distributed) denial of service attack.

/Host/Application/Malware/Spyware/Keylogger

Keylogger Application

/Host/Application/Module

A module of an application. This may be a virus engine or a version update for an application.

/Host/Application/Peer to Peer

An application that listens for and establishes network connections to other installations of the same application.

/Host/Application/Service

An application that is executed at OS startup. Frequently accepts network connections.

/Host/Application/Service/Email

Email communication.

/Host/Application/Service/MMS

Multimedia Message Service

/Host/Application/Service/Phone Call

/Host/Application/Service/Remote Control

Things like gotomypc.com or remote desktop

/Host/Application/Service/SMS

Simple Message Service

/Host/Application/Signature

A signature or rule. Could be a vendor update like a virus DAT file or IDS update.

/Host/Operating System

The core system software that controls access to resources on a host.

/Host/Operating System/License

An OS license

/Host/Operating System/Module

A module of an OS. This may be used for a kernel or patch update, etc

/Host/Resource

An operating system service with an aspect of limited supply. This property is also sometimes described as the price of the resource.

/Host/Resource/Backup

backup related activities

/Host/Resource/CPU

Events directed at this object relate to the consumption or use of the overall processing power of the host.

/Host/Resource/File

In general, the long term storage mechanism: files, directories, hard disks, etc.

/Host/Resource/Interface

Interface to network.

/Host/Resource/Interface/Tunnel

Packaging of a lower network protocol layer within a higher layer. VPNs, HTTP tunneling, etc

/Host/Resource/Memory

Events directed at this object relate to the consumption or use of the overall memory of the host.

/Host/Resource/Process

A single executable module that runs concurrently with other executable modules generally characterized by a shared address space. May support multiple execution threads.

/Host/Resource/Registry

Central configuration repository for OS and applications.

/Host/Resource/Storage Device

Used for adding a hard drive or a usb device to a system

/Phone

POTS

/Vector

The replicant for a bit of malicious code.

/Location

A physical location.

/Network

Events directed at these objects involve transport, supporting hardware (such as routers), or many hosts on the same subnet

/Network/Routing

Routing related events

/Network/Switching

Switching related events (VLANs, ...)

/Vector/Backdoor

An application that listens for network connections that is meant to give a remote user some measure of control over the host.

/Vector/DoS Client

An application that will participate in a (possibly distributed) denial of service attack.

/Vector/Virus

A self-replicating, persistant infection that also executes other behaviors on the infected host.

/Vector/Worm

A self-replicating, transient infection that primarily exists to infect other hosts.

Behavior

/Access

The object or services of the object were accessed connection to network, logging into service (shell, web, phone calls).

/Access/Start

Start of an ongoing access, like a login.

/Access/Stop

End of an ongoing access.

/Authentication

/Authentication/Add

/Authentication/Delete

/Authentication/Modify

Changes to passwords and other authentication mechanisms.

/Authentication/Verify

/Authorization

Authorization in general

/Authorization/Add

/Authorization/Delete

/Authorization/Modify

Changes to permission flags or other authorization mechanisms.

/Authorization/Verify

/Authorization/Review

This permission is reviewed for identity management.

/Authorization/Add/Request/Approval

An approval for a request for authorization for a resource, user, or role

/Authorization/Add/Request/Create

The creation of an authorization request for a resource, user, or role

/Authorization/Add/Request/Start

The start of an authorization request for a resource, user, or role

/Authorization/Add/Request/Cancel

The cancelling of an authorization request for a resource, user, or role

/Authorization/Delete/Request/Approval

The approval of a request to remove an authorization for a resource, user, or role

/Authorization/Delete/Request/Create

The creation of a request to remove an authorization for a resource, user, or role

/Authorization/Delete/Request/Start

The start of a request to remove an authorization for a resource, user, or role

/Authorization/Delete/Request/Cancel

The cancelling of a request to remove an authorization for a resource, user, or role

/Found/Compliant

A system was found compliant.

/Check

Just a check

/Check/Configuration

A configuration state. (e.g., a failure would indicate a weak configuration, etc)

/Check/Operational

Check whether a component is operational (e.g., a failure would indicate a defective component)

/Check/Resource

The object targeted was found to be a certain stage (e.g., a failure on a /resource/memory would indicate exhausted memory)

/Check/Security

An check of the security posture (e.g., a failure would indicate the presence of a vulnerability or insecurity in the object.

/Communicate

Transactions on the wire

/Communicate/Query

Communication of a request to a service.

/Communicate/Response

Communication of a response to a request from a service.

/Create

Resource creation, installation of applications or services, etc.

/Delete

Reversal of all the creation events - uninstalling an application or service, etc.

/Execute

Relates to the loading and executing of code, booting/shutdown of hardware, etc.

/Execute/Cancel

Cancelling the execution of an application, process, or workflow.

/Execute/Timeout

The timing out of the execution of an application, process, or workflow.

/ Execute/Query/Approval

Granting an approval for the object in question

/Execute/Query

/Execute/Response

The answer coming back from an Execute/Query: A report delivered back from an application, status messages from applications, ...

/Execute/Start

Starting an application or service, executing a command in a shell, host boot up, etc.

/Execute/Stop

Stopping an application or service, completing a command in a shell, host shutdown, etc.

/Execute/Response

The answer coming back from an Execute/Query: A report delivered back from an application, status messages from applications, ...

/Modify

Changing some aspect of an object.

/Modify/Attribute

Some attribute of an object changed - file name, modification date, create date, hash(?), etc.

/Modify/Configuration

The configuration of an object changed - application, OS, or registry changes.

/Modify/Content

The content of the object changed - writing to or deleting from a file, database, etc.

/Print

Printing of a document.

/Substitute

Replacement of files, upgrades of software, or failover of services and hosts.

Outcome

/Attempt

We know this was tried but cannot confirm or deny success.

/Success

We are pretty darned sure this really happened as described.

/Failure

We are pretty darned sure this did not work out as planned.

Technique

/Brute Force

Brute Force Attacks

/Brute Force/Login

Continued trial for logins

/Brute Force/URL Guessing

Continued trial for URLs to access information or scripts

/Code

Execution of malicious code

/Code/Application Command

Execution of an application-command

/Code/Shell Command

Shell command is executed

/Code/Trojan

Execution of a trojan

/Code/URL

Malicious links in emails/IM's/web pages

/Code/Virus

Code of a virus is seen on the wire. This could be because the virus is transmitted or executed.

/Code/Worm

Code of a worm is seen on the wire. This could be because the worm is transmitted or executed.

/Concern/Company

Something of concern to the company, this is not an information leak, but for example a disgruntled employee, a resume sent outside of the company, etc.

/Concern/Nation State

Something of concern to the nation state. Examples are communication with prohibited countries, such as the OFAC list, etc. Also terrorist activity or threats (in terms of threatening someone in an email)

/Covert Channel

Covert Channel detected, .e.g., Loki

/DoS

A DoS Attack is going on!

/DDoS

A denial of service technique that uses numerous hosts to perform the attack.

/Email/Abuse

/Email/Hoax

/Email/Phishing

/Email/Spam

/Exploit/Directory Traversal

/Exploit/Privilege Escalation

/Exploit/Vulnerability

Exploiting a vulnerability, Bufferoverflows, Information Access (Directory Traversal), Code Injection, Format String

/Exploit/Weak Configuration

Exploiting of a week root/root login, insecure software version,SMTP relay

/Information Leak

Information leaking out of the trusted network

/Information Leak/Company Information

Any kind of company confidential information, such as financial records, board meeting minutes, etc

/Information Leak/Encrypted Communication

If encrypted traffic is identified, without any further qualification, this could be an information leak

/Information Leak/Personal Information

Any kind of personal information seen on the wire, such as SSN, credit card numbers, PHI data, etc

/Information Leak/Unauthorized Access

Unauthorized access of an object (e.g., a file). Not directory listings, ... they would be plain information leaks.

/Policy

Policy related things, e.g., Internet-PORN access,...

/Policy/Breach

A breach of policy happened

/Policy/Compliant

Policy was complied to.

/Policy/Malevolence

Malicious activity seen, such as browsing hacker web sites, downloading keyloggers, downloading hacker documentation, exploit code, etc

/Redirection

Redirection of an entity.

/Redirection/Application

Redirection attacks on the application layer: e.g., Cross site scripting, mail routing, Javascript spoofing

/Redirection/DNS

Changes to the DNS which are not authoritative

/Redirection/ICMP

ICMP redirects

/Redirection/IP

Redirection via the IP protocol: e.g. Source routing.

/Redirection/Routing Protocols

Attacks aimed at routing protocols, e.g., BGP, RIP, OSPF,...

/Scan

Any type of scanning. Via the object a network/host/application/OS scan can be identified.

/Scan/IP Protocol

The IP header contains the transport protocol. TCP and UDP are not the only ones. This is a search for other responding protocols

/Scan/Port

A range of ports is scanned

/Scan/Service

A service is scanned, e.g., DDoS client discovery, Backdoors, RPC services, Scan for a specific application (e.g., NMB)

/Scan/Vulnerability

The search for vulnerabilities

/Traffic Anomaly

Something in the network traffic is wrong, strange, ...

/Traffic Anomaly/Application Layer

Application layer issues like syntax errors, overflows, wrong commands.

/Traffic Anomaly/Application Layer/Encoding

Encoding used on the application layer. E.g., Unicode, otherwise encoded URLs, etc. /Traffic Anomaly/Application Layer/Flow

Peer does not follow the order of the commands.

/Traffic Anomaly/Application Layer/Man in the Middle

Man in the Middle attack.

/Traffic Anomaly/Application Layer/Syntax Error

Syntax error in one of the application-layer commands.

/Traffic Anomaly/Application Layer/Unsupported Command

A command which does not exist or is not supported.

/Traffic Anomaly/IDS Evasion

/Traffic Anomaly/Network Layer

Everything with IP, ICMP, ...

/Traffic Anomaly/Network Layer/Flow

Problems in the communication of the network layer. e.g. IP fragment ID out of order, ...

/Traffic Anomaly/Network Layer/IP Fragments

Fragmented IP packets

/Traffic Anomaly/Network Layer/Man in the Middle

Man in the Middle attack

/Traffic Anomaly/Network Layer/Source Routing

The IP packet contains routing information

/Traffic Anomaly/Network Layer/Spoof

Source or destination IP is spoofed

/Traffic Anomaly/Transport Layer

Everything related to TCP, UDP, SSL, ...

/Traffic Anomaly/Transport Layer/Flow

TCP connection problems: SYNACK without SYN, Sequence number mismatches, out of limit seqnumbers, time exceeded

/Traffic Anomaly/Transport Layer/Hijack

Hijacking of a connection

/Traffic Anomaly/Transport Layer/Port

Anomalies with regards to the port number, such as services running on non-standard ports.

/Traffic Anomaly/Transport Layer/Spoof

Source or destination IP is spoofed

Device Group

/Application

/Assessment Tools

Vulnerability Scanners, Configuration Scanners, Port Scanners, ...

/Data Loss Prevention

This category is used for devices that detects and prevents potential data breaches/data exfiltration transmissions.

/Firewall

This category is for any device that blocks or authorizes traffic based on sets of rules.

/Honey Pot

/IDS

/IDS/Host

/IDS/Host/Antivirus

/IDS/Host/File Integrity

/IDS/Network

This category is for devices that monitor traffic traveling on the wire. This group is also used for IPS detection. But if the IPS reports traffic being blocked, then the device will change to Firewall. The outcome for this device group is almost always “Attempt” since the success or failure of an attack cannot be confirmed just based on what is detected on the wire.

/IDS/Network/Traffic Analysis

Devices like Arbor which do anomaly detection

/Identity Management

/Identity Management/AAA

/Network Equipment

/Network Equipment/NAC

Network Access Control device - determines policy compliance state of hosts and enforces network security policies with regards to allowing access onto a network.

/Network Equipment/Router

/Network Equipment/Switches

/Node Manager

This is mainly for devices that monitor systems? (hardware or software) configuration and health. It is not for devices that monitor security related incidents.

/Operating System

/Physical Access System

Badge Readers, etc.

/Proxy

/Security Information Manager

Correlated events

/VPN

Device Type

/Access and Identity Management

These are devices that administer resource authentication and access controls.

/Anti-Virus

Anti-Viruses are devices that prevent, detect, and remove malwares such as computer viruses, worms, trojans, spywares, etc.

/Applications

Applications are programs that are distinct from the operating system. They are usually not a part of the initial installation of the operating system.

/Content Security

Content filtering devices are used to filter out potentially threatening and offensive online content. This includes incoming emails, constant spam, and even websites. As the name suggests, such devices scans the content of online content and verifies its safety by passing it through its own blacklist of words. Some CFDs can also store well-known spam sites and email domains and warn you ahead of time before you interact with them. These devices throw an “Access Denied” error when anyone tries to access unverified, possibly malicious content. The basic configuration of this network security device blocks pornographic or hateful content. But besides, your organization can also block out product-selling spam and unwanted newsletters.

/Data Loss Prevention Threat Intelligence

Data loss prevention (DLP), per Gartner, can be defined as technologies which perform both content inspection and contextual analysis of data sent via messaging applications such as email and instant messaging, in motion over the network, in use on a managed endpoint device, and at rest in on-premises file servers or in cloud applications and cloud storage. These solutions execute responses based on policy and rules defined to address the risk of inadvertent or accidental leaks or exposure of sensitive data outside authorized channels.

/Data Security

These devices monitor the integrity and access control of devices.

/Database

These applications manage sets of data structurally stored in the local computer.

/Firewall

/HoneyPot

A honeypot is a network-attached system set up as a decoy to lure cyber attackers and detect, deflect and study hacking attempts to gain unauthorized access to information systems. The function of a honeypot is to represent itself on the internet as a potential target for attackers -- usually, a server or other high-value asset -- and to gather information and notify defenders of any attempts to access the honeypot by unauthorized users.

/Host-based IDS/IPS

These devices monitor and analyze the internals of a system up to its network interfaces.

/Integrated Security

An integrated security system can include some or all the following: Video surveillance, Video monitoring, Video review and analysis, Access Control, Audio warning speaker, License plate recognition. Integrated systems communicate and work together. For example, when you combine access control with video surveillance, you can match the time stamp from the access control with the video.

/Log Consolidator

These devices are used to store logs generated on different devices. They do not perform any type of correlation or pattern matching on those logs.

/Mail

These devices are mail servers used to transfer electronic mail.

/Mainframe

This is used for mainframe systems.

/Network Access Control

These devices provide a combination of security solutions. Such a device can be an IDS, an Anti-Virus, and a Vulnerability Scanner all included.

/Network-based IDS/IPS

These devices monitor and analyze traffic on the network.

/Network Monitoring

A device where all networking components like routers, switches, firewalls, servers, and VMs are monitored for fault and performance and evaluated continuously to maintain and optimize their availability. One important aspect of network monitoring is that it should be proactive. Finding performance issues and bottlenecks proactively helps in identifying issues at the initial stage. Efficient proactive monitoring can prevent network downtime or failures.

/Node Manager

These devices are used to monitor individual systems. They are used to audit systems in the enterprise and to monitor their operational status.

/Operating System

The Operating System is the software that facilitates applications to communicate with the hardware on which it is residing.

/Physical Security

These devices manage physical access to resources. Some examples are badge readers, retina scanners, fingerprint scanners, etc.

/Policy Management

These devices are used to manage policies in the enterprise.

/Printer

An external hardware output device that takes the electronic data stored on a computer or other device and generates a hard copy.

/Router

These devices are used to route network traffic.

/Security Management

These devices are used for log and security event aggregation, correlation, and storage. ArcSight ESM is an example of that.

/Switch

A network switch (also called switching hub, bridging hub, and, by the IEEE, MAC bridge[1]) is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.

/VPN

These devices provide secure remote access to a destination through a public or private network.

/Vulnerability Assessment

These devices determine whether systems in the enterprise are vulnerable and whether the proper steps to make them less vulnerable are taken.

/Web Cache

A Web cache (or HTTP cache) is a system for optimizing the World Wide Web. It is implemented both client-side and server-side. The caching of multimedias and other files can result in less overall delay when browsing the Web.

/Web Filtering

These devices are used to monitor web traffic. Web Proxies belong to this category.

/Web Server

These devices are web servers such as Apache.

/Wireless Security

These devices are used to monitor wireless network communications.

Significance

/Compromise

A host, network, application (see Object) is compromised

/Hostile

An overt assault

/Suspicious

Looks fishy but might be innocent

/Recon

Scans and their ilk

/Normal

Day to day activity

/Informational

Produced by polling, such as the output from top, etc

/Informational/Warning

Possible problem

/Informational/Error

Execution problem

/Informational/Alert

Situational problem

/Compromise/Integrity

/Compromise/Availability

/Compromise/Confidentiality

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 Configuration Guide for ArcSight Event Categorization Whitepaper
(SmartConnector CE 24.3)**

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 8.4.3

Format Preserving Encryption Environment Setup Guide

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Format Preserving Encryption Environment Setup Guide

This guide describes about setting up SmartConnectors with Format Preserving Encryption.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Setting Up SmartConnectors with Format Preserving Encryption

Running a SmartConnector with Format Preserving Encryption enabled requires correct environment setup for the machine hosting the SmartConnector.

The setup primarily involves addressing the following areas:

- Ensuring proper connectivity between the connector machine and the SecureData appliance server
- Ensuring the availability of an appliance certificate in all locations needed by the SmartConnector

In addition, if you are not using Instant Connector Deployment with ArcSight Management Center, or if you are upgrading a connector 7.6.0 or older to 7.7.0 or higher either through the ArcSight Management Center or standalone, you must manually install the client for each connector host. Consult your SecureData Appliance documentation for instructions for your platform. Follow the instructions to verify that the connectivity is established from the SecureData Client to the SecureData Server and the test program runs as expected before proceeding with SmartConnector configuration for data encryption. Data encryption parameters are described in the SmartConnector Installation and User Guide.

Network Connectivity

During connector configuration, during connector initialization at runtime, and also occasionally (even though not frequently) during events processing, the SmartConnector must connect to the SecureData appliance through the HTTPS protocol. Therefore, the HTTPS connectivity between the connector machine and the appliance server must be good.

Installing Voltage Simple API Java

1. Download the Voltage Simple API java client installer for Windows or Linux platform from the [Voltage SecureData](#) site.
2. Copy the installer into the following path of the machine that will host the client:
 - **For Windows:** C:\voltage
 - **For Linux:** /opt/voltage



Note: The connector will not be able to use the client if you use a different path to install the client, and the encryption cannot be performed. Note that if the installer prompts you to create a subfolder in the specified path, decline the option.

3. Run the installer.
 - **For Windows:** Double click the **.msi** file.
 - **For Linux:**
 - a. Use the **gzip -dk** command to unzip the **.sh.gz** file.
 - b. Execute the **chmod +x** command to make the **.sh** installer executable.
 - c. Run the **.sh** installer file. A license agreement is displayed.
 - d. Enter **Y** to accept the license agreement.
4. After the client is installed, go to the installation path and ensure that the following files and folders are present:
 - lib/
 - trustStore/ (Only present on Linux OS)
 - sample/
 - doc/
 - ReadMe.txt
 - License.txt

Ensuring Network Connectivity

The following sections describe steps to be followed to ensure connectivity for Linux and Windows operating systems.

Linux

- Edit the /etc/hosts file of the connector machine to include a line for the IP address and the hostname for the SecureData appliance. This step is required only if the DNS does not recognize the SecureData appliance FQDN.
- If your connector machine does not require a proxy to make an HTTPS connection to the SecureData appliance server, you do not need to set up a proxy. Verify that no global proxy is set for your machine. For a given user, you can open a fresh terminal, log in as the user, and enter `env | grep -i proxy` to determine whether a proxy has been inadvertently set by someone else.

- If your connector machine requires a proxy to make an HTTPS connection to the SecureData appliance server, set up a proper proxy. There is more than one way to set up a proxy. The System Administrator can choose the proper way to do it for the case in hand. However, keep in mind the following three important items:
 - If there are machines that do not require a proxy to be reached from the connector machine (such as ESM or Logger, for example), then the no_proxy/NO_PROXY environment variables must be set to bypass proxies for those hosts.
 - Make sure that the proxy-related variables are set globally, that is, for all users.
 - Verify that whatever proxy-related variables you have set are not transient (valid for one shell/terminal), and also verify they are actually in effect. You might require to reboot your machine to verify.

On a fresh terminal, enter **env | grep -i proxy** to see all proxy-related environment variables. For a machine that has a number of hosts that require a proxy and a number of hosts that do not require a proxy, you should see something like:

```
no_proxy=localhost,.xxx.com,.aaa.bbb.com
NO_PROXY=localhost,.xxx.com,.aaa.bbb.com
https_proxy=dddd.cccc.hh.com:8080
HTTPS_PROXY=dddd.cccc.hh.com:8080
```

Windows

- Edit the C:\Windows\System32\Drivers\etc\hosts file of the connector machine to include a line for the IP address and the hostname for the SecureData appliance. This step is required only if the DNS does not recognize the SecureData appliance FQDN.
- If your connector machine does not require a proxy to make an https connection to the SecureData appliance server, do not set up a proxy. Verify that no global proxy is set for your machine.

For a given user, you can open a fresh terminal, log in as the user, and enter **env | grep -i proxy** to determine whether a proxy has been inadvertently set by someone else.

- If your connector machine requires a proxy to reach certain hosts and does not require a proxy to reach some hosts, you can set these parameters from your browser's **Internet Options > Connections > LAN Settings > Advanced** tab.

After setting the correct proxies and bypass list properly, open a command prompt as Administrator and enter the following command to import the Internet Options into

the HTTP protocol connection:

```
netsh winhttp import proxy source=ie
```

Secure Data Appliance Certificates

To be able to make a successful connection and encrypt data, the server certificate must be present in all needed locations. These locations are highlighted in the following sections.

Windows

For SmartConnectors running in Windows, the server certificate must be in the following three locations. Perform these steps after installing the connector core software, but prior to selecting connector and adding parameter information.

- Connector certificate store - `../current/jre/lib/security/cacerts`. When using FIPS for the connector, the certificate must be placed into `..\current\user\agent\fips\bcfips_ks`

You can import any certificate to this store by using the `../current/jre/bin/keytool` utility. For example, from the `$ARCSIGHT_HOME/current/bin` directory, execute the following command to import the certificate:

```
arcsight keytoolgui
```

Open the keystore in `$ARCSIGHT_HOME/jre/lib/security/cacerts` (the password will be changeit).

From the Menu bar, select Tools and Import Certificate. Upload the certificate file.

Trust the certificate.

- Trusted Root Certification Authority for the local computer. Use the Windows certificate import wizard to import the certificate.
- Trusted Root Certification Authority for the current user. Use the Windows certificate import wizard to import the certificate.

Finally, it is always advisable to have unchained server certificates. Windows certificates in trusted authority are subject to CRL verification and it may involve verifying the entire chain. The process, controlled by Windows, may require connecting outside the hosts to verify the chain of trust, resulting somewhat troublesome. If a component cannot be verified, Windows does not trust it and the connection to the SecureData appliance fails.

Linux

For SmartConnectors running on Linux, the server certificate must be in the following two locations. Perform these steps after installing the connector core software, but prior to selecting connector and adding parameter information.

- Connector certificate store - `../current/jre/lib/security/cacerts`. When using FIPS for the connector, the certificate must be placed into `..\current\user\agent\fips\bcfips_ks`

You can import any certificate to this store using the `../current/jre/bin/keytool` utility. For example, from the `$ARCSIGHT_HOME/current/bin` directory, execute the following command to import the certificate:

`arcsight keytoolgui`

Open the keystore in `$ARCSIGHT_HOME/jre/lib/security/cacerts` (the password is `changeit`).

From the Menu bar, select Tools and Import Certificate. Upload the certificate file.

Trust the certificate.

- The store used by the SecureData client. Assuming the client directory is `/opt/voltage`, the store would be `/opt/voltage/trustStore`. The certificate must be Base64 encoded, not DER; otherwise, the `./c_rehash` command will fail. Copy the server certificate (in `*.pem` format) in the directory `/opt/voltage/trustStore`, and run the following command:

`/opt/voltage/trustStore/c_rehash .`



Note: Do not forget to type `'.'`.

Upgrading from the Voltage Simple API Java 5.10 client to 5.20

The following steps describe the process to upgrade from Voltage Simple API Java 5.10 client to 5.20.

1. Stop the connectors which are using the client you are going to upgrade.
2. For Linux machines: Delete the content of the current Voltage Client Installation Directory (default: `/opt/voltage`).

3. For Windows machines: Find the installer for the version that you want to uninstall and run it. Follow the wizard and select Remove, after the process is complete go to the installation folder and delete any remaining files or folders from the installation directory (default: C:\voltage).
4. Run the installer for the new version, choose exactly the same installation folder as the one from the previous client, if the installation folder is changed the connector will fail since it won't be able to find the components from the Voltage client.
5. On Linux, after installing the new version of the client, make sure you reimport the SecureData Server certificate in the client.
 - a. Go to /opt/voltage/trustStore (assuming the installation directory for the Voltage Client is /opt/voltage) and copy the certificate with a *.pem extension.
 - b. In the same folder, run the command: ./c_rehash .

Note: Don't forget to type '.'. Keep in mind that the certificate must be Base64 encoded.
6. After the client is installed, and the connection to the Voltage server is available, the connector can be started. It should encrypt the data in the same way it did with the older version of the client.



Note: The standalone installed connectors will expect the Voltage Client's install path to be /opt/voltage (Linux) or C:\voltage (Windows). If the connector was installed using the one-click functionality, users must be careful not to change the path where the connector will look for the Voltage Client.

For more information about the Voltage Simple API Java Client, refer to the official Voltage Guides.

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 Format Preserving Encryption Environment Setup Guide (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: CE 24.4

Configuration Guide for FlexConnector for Kafka

Document Release Date: October 2024

Software Release Date: October 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for ArcSight Kafka FlexConnector	4
Product Overview	5
Managing Parsers	6
Creating Parsers	6
Example Parser Files	6
Parser File Location	7
Serializing and Deserializing Data	7
Overriding Parser Files	7
Streaming Logs	8
Collecting Events From Apache Kafka	8
Prerequisite	9
Installing the FlexConnector	9
Copying the Parser File	9
Enabling SSL Encryption and Authentication (Optional)	9
Enabling SSL for Inter Broker Communication (Optional)	10
Configuring the FlexConnector	11
Collecting Events From Azure Event Hub Kafka	13
Prerequisite	14
Installing the FlexConnector	14
Copying the Parser File	14
Enabling SASL_SSL Authentication	15
Enabling Shared Access Signatures(Optional)	15
Configuring the FlexConnector	15
Configuration	18
Creating a Resource Group	18
Creating an Event Hub Namespace	19
Creating an Event Hub	20
Registering the App	21
For registration of the App, the following steps must be implemented:	22
For authenticating the App, the following steps must be implemented:	22
Assigning IAM Role	23
Configuring Advanced Parameters	23
Running the Connector	24
Publication Status	25
Send Documentation Feedback	26

Configuration Guide for ArcSight Kafka FlexConnector

This guide provides information about installing the ArcSight Kafka FlexConnector and configuring the device for event collection.

The Arcsight Kafka FlexConnector helps you subscribe and collect events from a topic of a Kafka server or Azure Event Hubs.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

Kafka is a distributed event streaming technology that stores messages in a Kafka Topic and provides them to Subscribers. Events and other security relevant data are then typically streamed to ArcSight or to 3rd-party subscribers. The Arcsight Kafka FlexConnector enables you to subscribe to and read this data from a Topic or from an Azure Event Hub. The connector requires a parser to isolate relevant fields within the message data. The parser analyzes the message data and places it into field names. You must define and build parsers before configuring and installing the connector.

In a publish-subscribe system, publishers send messages to more than one consumers by using a single destination, called as topics. Topics only contain a specific event type. Consumers subscribe to messages published to topics, by using an instantaneous pull-based mechanism, which allows for handling of high volume of data in real-time. A topic can have more than one subscribers or consumers. For more information about Apache Kafka, refer to the [Kafka documentation](#).

The Kafka FlexConnector provides the customers the ability to collect data from Kafka and write custom parsers to map, normalize, and categorize that data. Flex connectors are have all features and capabilities that SmartConnectors provide. But, the FlexConnectors do not come with out-of-the-box parsers and therefore, you must develop parsers based on your log format.

The Kafka FlexConnector can read and parse events from the following sources:

- **Apache Kafka:** Apache Kafka is a publish-subscribe based messaging queue system and a robust queue that handles a high volume of data. It enables you to pass messages from one end-point to another.
- **Microsoft Azure Event Hub:** Microsoft Azure Event Hubs provides a Kafka endpoint that can be used by your Kafka based applications as an alternative to run Kafka clusters.
Kafka FlexConnector supports Apache Kafka protocol 1.0 and later to communicate with Azure Event Hubs. However, Microsoft Azure Event Hub Kafka endpoint does not support the Advanced Message Queuing Protocol (AMQP) and HTTPS protocols.

The Kafka FlexConnector supports events in the following formats:

- JSON
- CEF
- REGEX
- SYSLOG
- KEY-VALUE
- AVRO

Managing Parsers

Before you install and configure the FlexConnector, you must create parsers based on the log format. This section has the following information:

Creating Parsers

The Kafka FlexConnector cannot directly parse messages from Kafka, because there is no generic Kafka parser that can parse every message received from different devices that can send data to a given Kafka topic. You must create your individual parsers before setting up the connector.

To understand the parser file structure, see [Parser File Structure](#) in the [ArcSight FlexConnector Developer's Guide](#).

To develop your connector, you should be familiar with FlexConnector development. See the [FlexConnector Developer's Guide](#) for details.



Note: Consult the vendor documentation to verify the supported browsers and browser versions. If a supported browser is not used, the vendor login page might not display properly, preventing login, and you will be unable to configure the connector.

Example Parser Files

You can use the example configuration files for specific type of log format to create the parser files:

Log Format	Example Configuration files
JSON	Example Configuration File for JSON Log Format .
CEF	Configuration file is not required for CEF Log Format.
REGEX	Example Configuration File for Regex Log Format .
SYSLOG	Example Configuration File for Syslog Log Format .
KEY-VALUE	Example Configuration File for Key-Value Log Format.
AVRO	Example Configuration File for JSON Log Format . If the content type is AVRO , then you must create a JSON parser.

Parser File Location

The following table describes the location and filename of the configuration file used for each type of FlexConnector. The vendor or database is usually named for the device vendor (such as “superSecure”).

Type	Location	Filename
JSON	ARCSIGHT_HOME\user\agent\flexagent	vendor.jsonparser.properties
CEF	ARCSIGHT_HOME\user\agent\flexagent	
Regex	ARCSIGHT_HOME\user\agent\ flexagent	vendor.sdkfilereader.properties
Syslog	ARCSIGHT_HOME\user\agent\flexagent\syslog	vendor.subagent.sdkfilereader.properties
Key-Value	ARCSIGHT_HOME\user\agent\flexagent	
Avro	ARCSIGHT_HOME\user\agent\flexagent	

Serializing and Deserializing Data

The connector consumes only data that is serialized using the correct serializers, because the corresponding deserializers are not configurable. The Serializers are responsible for converting objects into data types and also deserializing parsed data to be converted back into complex types, after first validating the incoming data.

- **To serialize data, use the following serializers:**
 - Key serializer: org.apache.kafka.common.serialization.StringSerializer
 - Value serializer: org.apache.kafka.common.serialization.BytesSerializer
- **To deserialize data, the Kafka FlexConnector uses the following deserializers:**
 - Key deserializer: org.apache.kafka.common.serialization.StringDeserializer
 - Value deserializer: org.apache.kafka.common.serialization.BytesDeserializer

Next Step:

- [Stream Logs](#)

Overriding Parser Files

To override parser files:

1. Stop the connector and navigate to the path
`<connector_home>/current/users/agent/fcp/connectorname_log`,
for example

```
<connector_home>/current/users/agent/fcp/cisco_syslog>
```

The following files should be found under the location:

`cisco_syslog.subagent.sdkrfilereader.properties`

`cisco_sdsyslog.subagent.sdkrfilereader.properties`

As well as an "extra processor" parser required for main-level REGEX type agents:

`cisco_sdsyslog.sdkkeyvaluefilereader.properties`

2. In order to override these files, create the sub-folder structure and the required file(s) under

```
<connector_home>/current/users/agent/fcp/cisco_syslog
```

3. Make sure the override only includes the changes or additions to the base /shipped parser.
4. Start the connector.
5. To confirm the override was successful, go to the `agent.out.wrapper.log` file look for the **"An over-ride file was found and loaded"** note.



Note: The Override file should be created with the same file name and under the same folder location and replaced without affecting or making changes in the `agent.properties` file.

Streaming Logs

You can configure the flex connectors to stream logs from Apache Kafka and Azure Event Hubs. Select one of the following topics based on your event source.

Collecting Events From Apache Kafka

To enable the FlexConnector to read data from Kafka topics, you must configure the connector to read data from Kafka topics, after you have installed it. You can also configure advanced authentication and enable inter broker SSL communication.

When using Apache Kafka protocol with your clients, set the configuration for authentication and encryption using the SASL mechanisms.

To install and configure the FlexConnectors to collect event data from Apache Kafka, complete the following steps:

1. [Prerequisites](#)
2. [Installing the FlexConnector](#)
3. [Copy the Parser file](#)
4. [Enable SSL Encryption and Authentication \(Optional\)](#)

5. [Enable SSL for Inter Broker Communication \(Optional\)](#)
6. [Configure the FlexConnector](#)

Prerequisite

Before installing the FlexConnector, make sure that the following are available:

- Create the parser file based on the log format.
- Local access to the machine where the FlexConnector is to be installed.
- Vendor login credentials (user name and password). During the configuration, you are redirected to the vendor's login page, where you will log into the vendor's application using your vendor credentials. After you log into the vendor application, the connector can access and collect vendor log data.

Installing the FlexConnector

1. Download the latest executable for your operating system.
2. Start the FlexConnector Installer by running the executable.
3. Follow the installation wizard to install the core software
4. Exit the Installation wizard.

Copying the Parser File

You must copy the parser configuration file to the ARCSIGHT_HOME\user\agent\flexagent folder. For more information about the specific parser file locations, see the [Parser File Locations and Names](#) section in [Developer's Guide to FlexConnectors](#).

Enabling SSL Encryption and Authentication (Optional)

If you want to enable advanced authentication, then you must configure the truststore, keystore, and password in the `server.properties` file of every broker.



Note: `ssl.truststore.password` is optional but highly recommended. If a password is not set, access to the truststore is still available, but integrity checking is disabled.

As Passwords are directly stored in the broker configuration file, restrict access to these by using file system permissions.

To configure trust store, keystore, and passwords, add the following lines in the `server.properties` file of every broker:

```
ssl.truststore.location=/var/private/ssl/kafka.server.truststore.jks
```

```
ssl.truststore.password=test1234
ssl.keystore.location=/var/private/ssl/kafka.server.keystore.jks
ssl.keystore.password=test1234
ssl.key.password=test1234
```

Enabling SSL for Inter Broker Communication (Optional)

You can add a configuration to the `config/server.properties` file to set up a secure communication between brokers, so that the Kafka brokers are available only through SSL. You must restart brokers after making changes to configuration.

- To enable SSL for inter broker communication, add the following line:
`security.inter.broker.protocol=SSL`
- Configure the Apache Kafka broker ports which listen to client and inter-broker SSL connections. Configure the `listeners` and the `advertised.listeners`, in case the value is different.

```
listeners=SSL://kafka1:9093
advertised.listeners=SSL://0.0.0.0:9093
```

- Configure the PLAINTEXT ports if:
 - SSL is not enabled for inter-broker communication.
 - Some clients connecting to the cluster do not use SSL.

```
listeners=PLAINTEXT://kafka1:9092,SSL://kafka1:9093
advertised.listeners=PLAINTEXT://0.0.0.0:9092,SSL://0.0.0.0:9093
```



Note: `advertised.host.name` and `advertised.port` configure a single PLAINTEXT port are incompatible with secure protocols. Use `advertised.listeners` instead.

- To enable the broker to authenticate clients (2-way authentication), configure all the brokers for client authentication. It is recommended to set this value to required.

```
ssl.client.auth=required
```



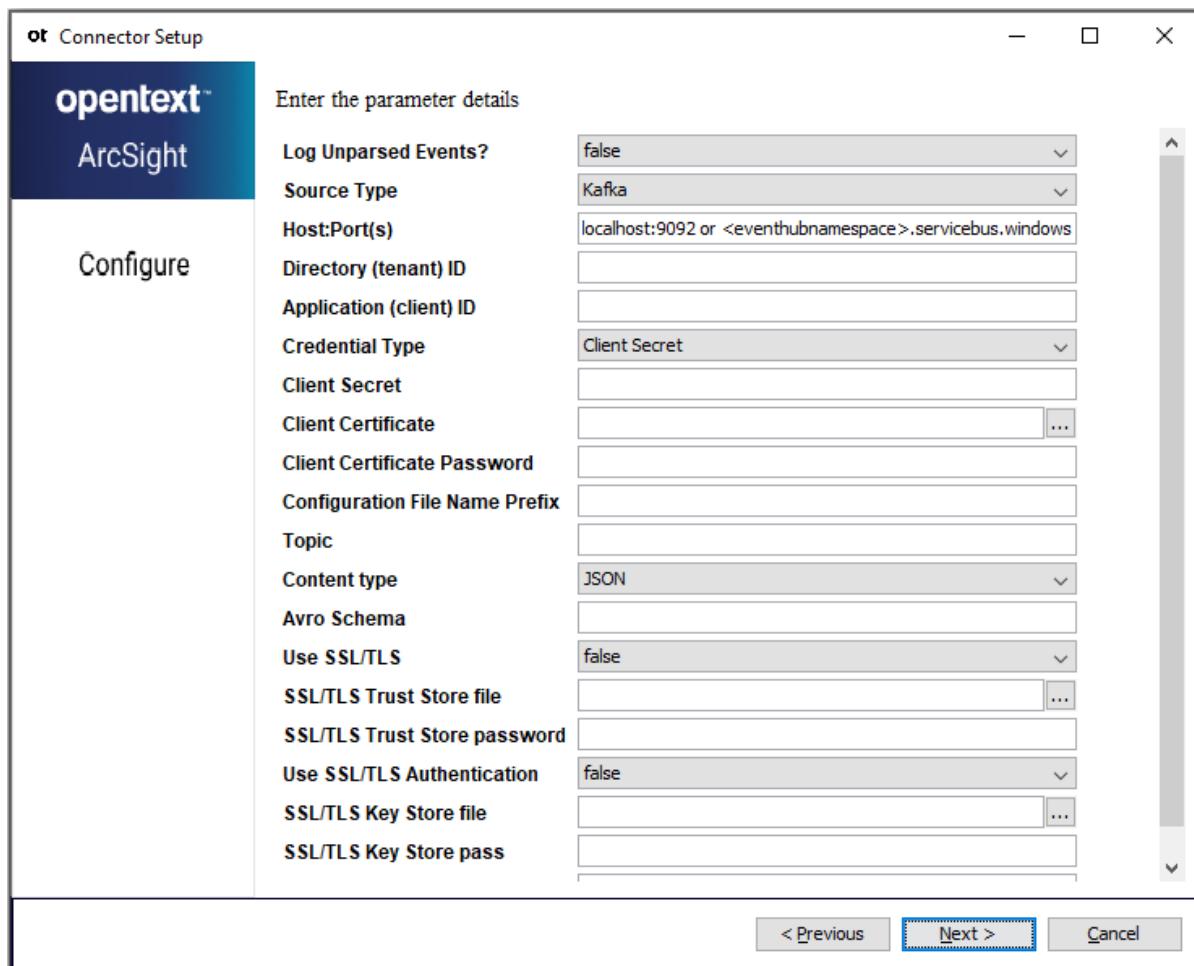
Note: Do not use `requested` as it creates a false sense of security.



Important: If any of the SASL authentication mechanisms are enabled on a given listener, the SSL client authentication is disabled, even if `ssl.client.auth=required` is previously configured. The broker will only authenticate clients via SASL on that listener.

Configuring the FlexConnector

1. Browse to \$ARCSIGHT_HOME/current/bin, then double-click **runagentsetup.bat** file to start the SmartConnector Configuration Wizard.
2. Specify the relevant Global Parameters, when prompted.
3. From the **Type** drop-down menu, select **ArcSight FlexConnector Kafka** and click **Next**.



4. Enter the parameter details and click **Next**.

Parameter	Setting
Log Unparsed Events?	Log unparsed events on the log folder and only use it for regex and syslog content types.
Source Type	Select the required source type as either Azure Event Hub or Kafka to read the data from.

Parameter	Setting
Host:Port(s)	Enter the host and port of the Kafka server or the Event Hubs Namespace. For the host value, refer to the Overview section of the Event Hub Namespace. The recommended port value is 9093.
Directory (tenant) ID	Enter the Directory (tenant) ID of your registered application. For this value, refer to the Overview section of the registered application.
Application (Client) ID	Enter the Client ID generated for your registered application. For this value, refer to the Overview section of the registered application.
Credential Type	Enter the credential type as either Client Secret or Client Certificate .
Client Secret	Enter the client secret value generated while registering the application. This value is obfuscated. This field is mandatory if the Credential Type is Client secret.
Client Certificate	Specify the client certificate path. This field is mandatory if the Credential Type is Client Certificate.
Client Certificate Password	Enter the password of client certificate.
Configuration File Name Prefix	Enter prefix for the name of the parser file. For example: for \$ARCSIGHT_HOME\current\user\agent\flexagent\google.jsonparser.properties. You can enter the prefix google, and the connector assumes the file name is google.jsonparser.properties and resides in \$ARCSIGHT_HOME\current\user\agent\flexagent. For more information, see Developer's Guide to FlexConnectors .
Topic	Enter Event Hub(s) namespace name.
Content type	Select content type from the drop-down list. The supported content types are: JSON , CEF , SYSLOG , REGEX , KEY-VALUE , and AVRO .
Avro Schema	(Applicable only if the content type is Avro) Enter a schema file name with full path and file extension (For example: /opt/TestSchema.avsc). Note that this must be the same schema that was used while writing the security events to Kafka topic.
Use SSL/TLS	Select true , if you have configured advanced authentication or if Kafka server requires it for encrypted data.
SSL/TLS Trust Store file	(Applicable only if you have selected true for the previous option) Enter file path of the SSL/TLS Trust Store file. To enable SASL plain authentication, do not specify any value here.
SSL/TLS Trust Store password	(Applicable only if you have selected true for the previous option) Enter the SSL/TLS Trust Store password of the store file above. To enable SASL plain authentication, do not specify any value here.

Parameter	Setting
Use SSL/TLS Authentication	(Applicable only if you have selected true for the previous option) Select true from the drop-down list if the Kafka server requires it for authentication. You also need to enable the Use SSL/TLS parameter. To enable SASL plain authentication, select false from the drop-down list.
SSL/TLS Key Store file	(Applicable only if you have selected true for the previous option) Enter the file path of the SSL/TLS Key Store file. To enable SASL plain authentication, do not specify any value here.
SSL/TLS Key Store pass	(Applicable only if you have selected true for the previous option) Enter the SSL/TLS Key Store password. To enable SASL plain authentication, do not specify any value here.
SSL/TLS Key password	(Applicable only if you have selected true for the previous option) Enter the SSL/TLS Key password. To enable SASL plain authentication, do not specify any value here.

5. Select a [destination and configure parameters](#).
6. Specify a name for the connector.
7. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**.
The certificate is imported and the Add connector Summary window is displayed.
(If you select **Do not import the certificate to connector from destination**, the connector installation will end.)
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.

Next Step:

- [Configure Advanced Parameters \(Optional\)](#)
- [Run the Connector](#)

Collecting Events From Azure Event Hub Kafka

The Azure Event Hub Kafka endpoint can be used from applications with just a minimal configuration change:

- Update the connection string in the configurations to point to the Kafka endpoint exposed by your event hub instead of pointing to a Kafka cluster and start streaming events from the applications that use the Kafka protocol into Event Hubs.
- This integration also supports frameworks like Kafka Connect, which is currently in preview.

The Arcsight Kafka FlexConnector uses Shared Access Signature (SAS) to authorize access to secure resources.

For more information, see the [Azure Documentation](#).

To install and configure the FlexConnectors to collect event data from Apache Kafka, complete the following steps:

1. [Configuration](#)
2. [Prerequisites](#)
3. [Installing the FlexConnector](#)
4. [Copy the Parser file](#)
5. [Enable SASL_SSL Authentication](#)
6. [Enable Shared Access Signature \(Optional\)](#)
7. [Configure the FlexConnector](#)

Prerequisite

Before installing the FlexConnector, make sure that the following are available:

- Create the parser file based on the log format.
- Local access to the machine where the FlexConnector is to be installed.
- Vendor login credentials (user name and password). During the configuration, you are redirected to the vendor's login page, where you will log into the vendor's application using your vendor credentials. After you log into the vendor application, the connector can access and collect vendor log data.

Installing the FlexConnector

1. Download the latest executable for your operating system.
2. Start the FlexConnector Installer by running the executable.
3. Follow the installation wizard to install the core software
4. Exit the Installation wizard.

Copying the Parser File

You must copy the parser configuration file to the ARCSIGHT_HOME\user\agent\flexagent folder. For more information about the specific parser file locations, see the [Parser File Locations and Names](#) section in [Developer's Guide to FlexConnectors](#).

Enabling SASL_SSL Authentication

Every time events are published or consumed from Event Hubs for Kafka, your clients are trying to access the Event Hubs resources. Ensure that the resources are accessed with an authorized entity. Event Hubs for Kafka require the TLS-encryption (as all data in transit with Event Hubs is TLS encrypted). This can be done by specifying the SASL_SSL option in the configuration file.

Enabling Shared Access Signatures(Optional)

Azure Event Hubs also provide the Shared Access Signatures (SAS) for delegated access to Event Hubs for Kafka resources. Authorizing access with an OAuth 2.0 token-based mechanism provides superior security and ease of use over SAS. The built-in roles can also eliminate the need for ACL-based authorization, which has to be maintained and managed by the user.

This feature can be used with your Kafka clients by specifying the SASL_SSL for the protocol and PLAIN for the mechanism, as shown in the following example:

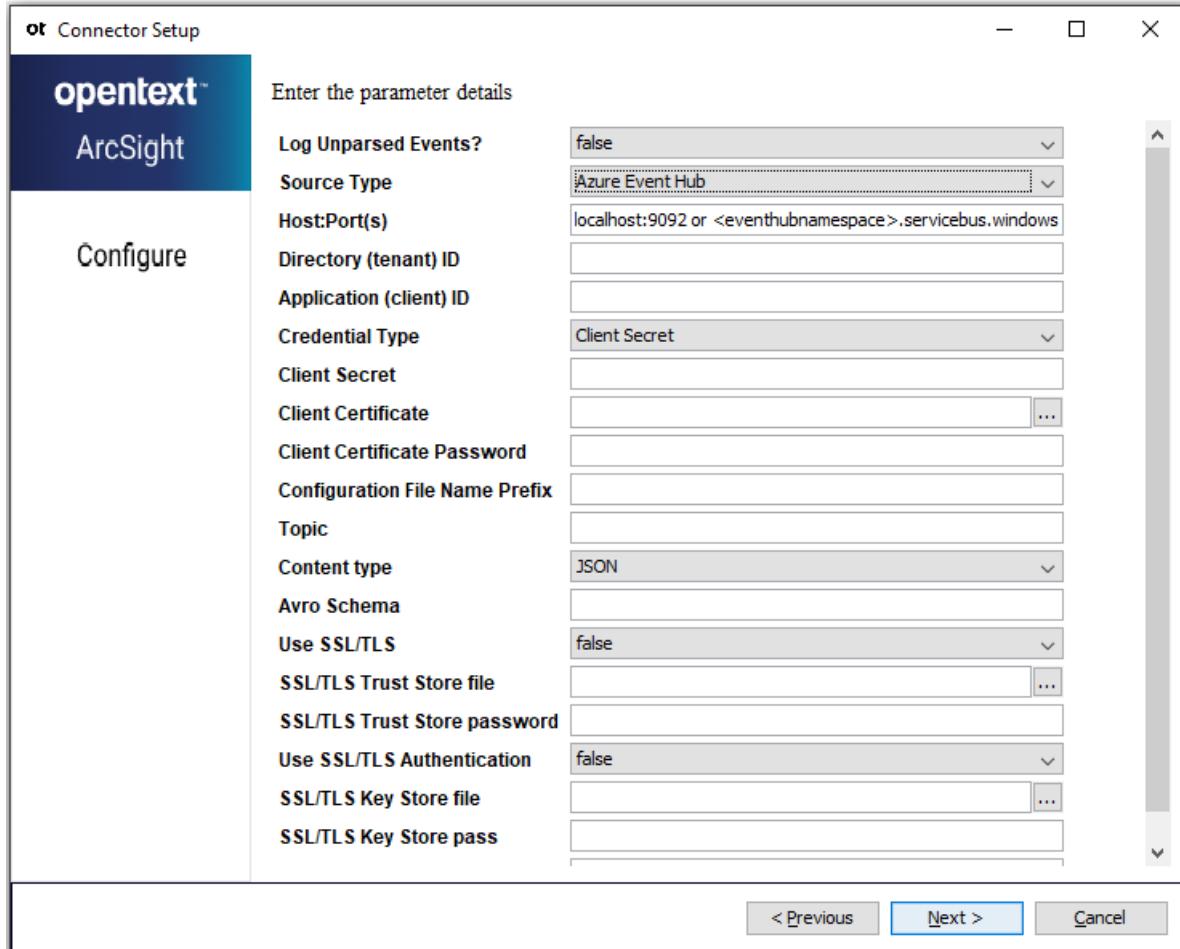
```
bootstrap.servers=NAMESPACENAME.servicebus.windows.net:9093  
security.protocol=SASL_SSL  
sasl.mechanism=PLAIN  
  
sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule  
required username="$ConnectionString" password="  
{YOUR.EVENTHUBS.CONNECTION.STRING}";
```



Note: When using SAS authentication with Kafka clients, established connections are not disconnected after the SAS key is regenerated.

Configuring the FlexConnector

1. Browse to \$ARCSIGHT_HOME/current/bin, then double-click **runagentsetup.bat** file to start the SmartConnector Configuration Wizard.
2. Specify the relevant Global Parameters, when prompted.
3. From the **Type** drop-down menu, select **ArcSight FlexConnector Kafka** and click **Next**.



4. Enter the parameter details and click **Next**.

Parameter	Setting
Log Unparsed Events?	Log unparsed events on the log folder and only use it for regex and syslog content types.
Source Type	Select the required source type as either Azure Event Hub or Kafka to read the data from.
Host:Port(s)	Enter the host and port of the Kafka server or the Event Hubs Namespace. For the host value, refer to the Overview section of the Event Hub Namespace. The recommended port value is 9093.
Directory (tenant) ID	Enter the Directory (tenant) ID of your registered application. For this value, refer to the Overview section of the registered application.
Application (Client) ID	Enter the Client ID generated for your registered application. For this value, refer to the Overview section of the registered application.
Credential Type	Enter the credential type as either Client Secret or Client Certificate .

Parameter	Setting
Client Secret	<p>Enter the client secret value generated while registering the application. This value is obfuscated.</p> <p>This field is mandatory if the Credential Type is Client secret.</p> <p>For detailed information, see Registering the Application in Azure AD section of the Configuration Guide of Microsoft Azure Event Hub Connector.</p>
Client Certificate	<p>Specify the client certificate path.</p> <p>This field is mandatory if the Credential Type is Client Certificate.</p> <p>For detailed information, see Registering the Application in Azure AD section of the Configuration Guide of Microsoft Azure Event Hub Connector.</p>
Client Certificate Password	Enter the password of client certificate.
Configuration File Name Prefix	<p>Enter prefix for the name of the parser file.</p> <p>For example: for \$ARCSIGHT_HOME\current\user\agent\flexagent\google.jsonparser.properties. You can enter the prefix google, and the connector assumes the file name is google.jsonparser.properties and resides in \$ARCSIGHT_HOME\current\user\agent\flexagent.</p> <p>For more information, see Developer's Guide to FlexConnectors.</p>
Topic	Enter Event Hub(s) namespace name.
Content type	Select content type from the drop-down list. The supported content types are: JSON , CEF , SYSLOG , REGEX , KEY-VALUE , and AVRO .
Avro Schema	<p>(Applicable only if the content type is Avro)</p> <p>Enter a schema file name with full path and file extension (For example: /opt/TestSchema.avsc).</p> <p>Note that this must be the same schema that was used while writing the security events to Kafka topic.</p>
Use SSL/TLS	Select true , if you have configured advanced authentication or if Kafka server requires it for encrypted data.
SSL/TLS Trust Store file	<p>(Applicable only if you have selected true for the previous option) Enter file path of the SSL/TLS Trust Store file.</p> <p>To enable SASL plain authentication, do not specify any value here.</p>
SSL/TLS Trust Store password	<p>(Applicable only if you have selected true for the previous option) Enter the SSL/TLS Trust Store password of the store file above.</p> <p>To enable SASL plain authentication, do not specify any value here.</p>
Use SSL/TLS Authentication	<p>(Applicable only if you have selected true for the previous option) Select true from the drop-down list if the Kafka server requires it for authentication. You also need to enable the Use SSL/TLS parameter.</p> <p>To enable SASL plain authentication, select false from the drop-down list.</p>

Parameter	Setting
SSL/TLS Key Store file	(Applicable only if you have selected true for the previous option) Enter the file path of the SSL/TLS Key Store file. To enable SASL plain authentication, do not specify any value here.
SSL/TLS Key Store pass	(Applicable only if you have selected true for the previous option) Enter the SSL/TLS Key Store password. To enable SASL plain authentication, do not specify any value here.
SSL/TLS Key password	(Applicable only if you have selected true for the previous option) Enter the SSL/TLS Key password. To enable SASL plain authentication, do not specify any value here.

5. Select a [destination and configure parameters](#).
6. Specify a name for the connector.
7. (Optional) If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**.
The certificate is imported and the Add connector Summary window is displayed.
(If you select **Do not import the certificate to connector from destination**, the connector installation will end.)
8. Select whether you want to run the connector as a service or in the standalone mode.
9. Complete the installation.

Next Step:

- [Configure Advanced Parameters \(Optional\)](#)
- [Run the Connector](#)

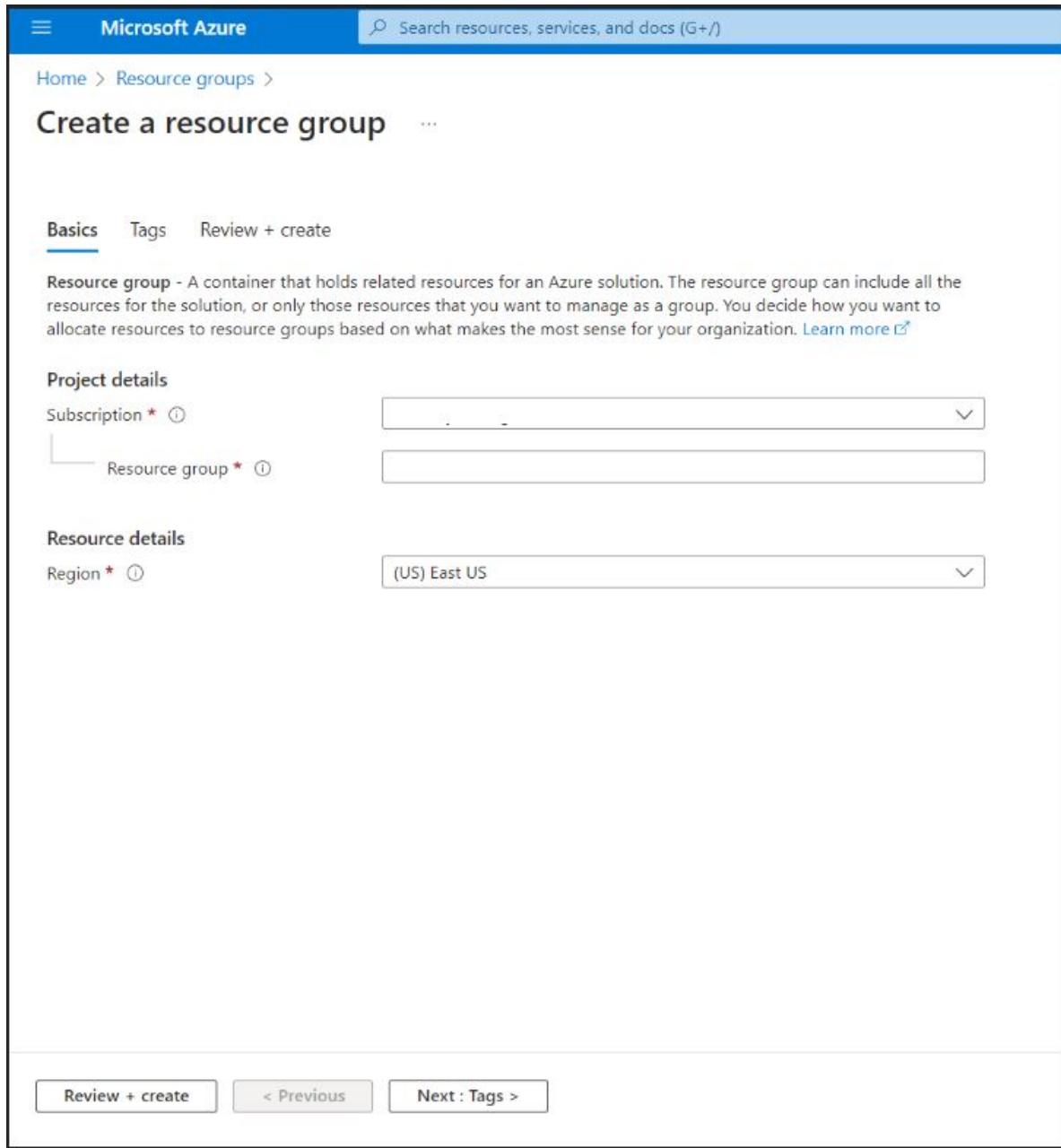
Configuration

The following configuration steps must be implemented before installing the connector:

Creating a Resource Group

1. Log in to the Azure portal and navigate to the **Resource Group** service.
2. Click **+Create**.
3. Select the **Subscription** and enter a name for the group in the **Resource group** field.
4. Navigate to **Resource details** and select the region.
5. (Optional) Click **Next:Tags** to create a tag for the group.

6. Click **Next:Review > +Create**.



Creating an Event Hub Namespace

1. Log in to the Azure portal and navigate to the **Event Hubs** service.
2. Click **+Create**.
3. Select the **Subscription** and the **Resource group** that is created above.
4. Navigate to **Instance Details** and enter a name in the **Namespace name** field.
5. Select the same **Location** that is selected while creating the **Resource Group**.

6. Select the **Pricing tier** as **Standard**. Refer to this [Microsoft documentation](#) for more plans.
7. Click **Review + Create**.

The screenshot shows the 'Create Namespace' wizard in the Microsoft Azure portal. The 'Basics' tab is selected. In the 'Project Details' section, 'Subscription' and 'Resource group' dropdowns are shown. Under 'Instance Details', 'Namespace name' is set to 'mynamespace.servicebus.windows.net', 'Location' is 'East US', and 'Pricing tier' is 'Standard'. A note indicates that the region supports Availability zones. 'Throughput Units' is set to 1. Navigation buttons at the bottom include 'Review + create', '< Previous', and 'Next: Advanced >'.

Creating an Event Hub

1. Click the **Namespace** that is created above.
2. Navigate to **Event Hubs > +Event Hub**.
3. Enter a **Name** for the hub and select the **Partition count**. For more information regarding Partition count, refer to this [Microsoft Documentation](#).
4. Navigate to **Retention**. Select the **Cleanup policy** and choose the required **Retention time**.

5. Click **Review + create**.

The screenshot shows the 'Create Event Hub' wizard in the Azure portal. The 'Basics' tab is active. In the 'Event Hub Details' section, the 'Name' field is empty. The 'Partition count' is set to 2. Under 'Retention', the 'Cleanup policy' is set to 'Delete' and the 'Retention time (hrs)' is set to 1. At the bottom, there are buttons for 'Review + create', '< Previous', and 'Next: Capture >'.



Note: Ensure to select the same **Subscription** and **Region** while creating the **Resource Group** and **Event Hub Namespace**.

Registering the App

Registering an application in Azure portal is necessary when you want to use Azure services like Azure Active Directory, Azure Monitor, and more. By registering an application, you can create a unique identity for it, and then configure the necessary permissions and settings so that it can interact with the Azure services. To authenticate an application, you can use Azure Active Directory, which provides a secure and scalable way to manage user identities and access to resources.

For registration of the App, the following steps must be implemented:

1. Log in to Azure Portal.
2. Navigate to **Azure Active Directory** and select **App registrations**.
3. Click **+New registration** to create a new application registration.
4. Enter a name for the application, select the appropriate account type and click **Register**.

For authenticating the App, the following steps must be implemented:

To authenticate the application, you can either choose **Client Certificate** or **Client Secret**.



Note: From a security standpoint, **Client Certificates** are often considered to be more secure than **Client Secrets**.

1. If **Client Certificate** is opted to Client Certificate in Azure.

To generate the self-signed certificate implement the following steps:

- a. Open the command prompt and run the below command by replace the certificate filename and password.

```
keytool -genkey -keystore <filename.pfx> -storetype PKCS12 -keyalg RSA  
-storepass <password> -validity 730 -keysize 2048
```

This will generate the **.pfx** certificate file. This certificate will be uploaded while installing the connector when **Client Certificate** is used to authenticate the Azure AD Application.

- b. Run the below command to generate **.cer** certificate file by replacing the same filename and password as mentioned in the above step.

```
keytool -export -keystore <filename.pfx> -file <client.cer> -storetype  
PKCS12 -storepass <password>
```

This will generate the **.cer** certificate file. This must be uploaded in the Azure portal to authenticate the connector to access the Azure AD application. Implement the following steps to upload this certificate to the Azure portal:

- i. Navigate to the Application that is registered in step 3 and click **Certificates & secrets**.

- ii. Under **Certificates > Upload Certificate**.

- iii. Select the Public Client Certificate from the drop down and enter a **Description** to it. Then click **Add**.

Certificate will be listed in **Certificates** section.

2. If **Client Secret** is opted then implement the following steps to configure the Client Secret in Azure:

- a. Navigate to the application that is registered in step 3 and click **Certificates & secrets**.
- b. Under **Client Secret > +New Client Secret**.
- c. Enter a **Description** to the secret. Set the value for expiry and click **Add**. This will generate the **Client Secret**.



Important: Note the generated Secret Key Value to provide the same while installing and configuring the connector. If you do not note down the Secret Value, you will not be able to retrieve it later.



Note: Ensure to note the expiry date of the **Client Secret** and **Client Certificate**. After the Client Secret/ Certificate expires, the connector will fail to authenticate the application and it will stop working. To reconfigure the new Client Secret or Client Certificate, see the [Troubleshooting](#) section.

Assigning IAM Role

IAM role must be assigned to this application in Event Hubs Namespace to allow the application to read data from Azure Event Hub.

To assign IAM role:

1. Navigate to **Event Hubs Namespace** created [here](#) and select **Access Control (IAM)**.
2. Click **Role Assignments > +Add** and select **Add role assignment**.
3. Assign **Azure Event Hubs Data Receiver** role and click **Next**.
4. Click **+Select members** and select the registered application.
5. Click **Next > Review + Assign**.

Configuring Advanced Parameters

If you choose to perform any of the operations shown in the following table, do so before adding your connector. After installing core software, you can set the following parameters in the **agent.properties** file, as required:

Parameter	Setting
bootstrap.servers	Host-IP.
group.id	Use for multiple connectors in a Kafka topic.

Parameter	Setting
max.poll.records	The maximum number of records returned in a single call to a poll(). Default value is 500 (maximum).
auto.commit.interval.ms	The frequency in milliseconds in which the consumer offsets are auto-committed to Kafka if the enable.auto.commit value is set to True : 5000 milliseconds.
reconnect.backoff.ms	The base waiting time, before attempting to reconnect to a given host. It avoids repeatedly connecting to a host in a tight loop. This backoff applies to all client connection attempts to a broker: 50 times
retry.backoff.ms	The amount of waiting time before attempting to retry a failed request to a given topic partition. It avoids repeatedly sending requests in a tight loop under some failure scenarios: 100 times.
request.timeout.ms	It controls the maximum amount of waiting time for a request response. If the response is not received before the timeout elapses, the client resends or fails the request (if the connection attempts have reached the limit: 30000 milliseconds).
client.id	An id string to pass to the server when making requests. It tracks the request source beyond just ip/port, by allowing a logical application name to be included on the server-side login request. For tracking: arcsight
heartbeat.interval.ms	The expected time between heartbeats to the consumer coordinator when using Kafka's group management facilities. Heartbeats are used to ensure that the consumer's session stays active and facilitates rebalancing when new consumers join or leave the group. The value must be set lower than session.timeout.ms and higher than 1/3 of that value. It can be adjusted even lower to control the expected time for normal rebalances.
connections.max.idle.ms (Idle connections timeout)	The server socket processor threads close the connections that appear idle for more than 600000 ms.
auto.offset.reset	It can be executed when there is not an initial offset in Kafka or if the current offset does not exist in the server anymore.
disable.activemq	The values can be: True: Disable ActiveMQ False: Enable ActiveMQ

Running the Connector

Connectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On

Windows platforms, Connectors also can be run using shortcuts and optional **Start** menu entries.

For more information, see [Running SmartConnectors](#).

Publication Status

Released: October 2024

Updated: October 2024

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 Configuration Guide for FlexConnector for Kafka (SmartConnectors CE 24.4)

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 MFI-Documentation-Feedback@opentext.com .

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: CE 25.1

Configuration Guide for Linux Audit File SmartConnector

Document Release Date: February 2025

Software Release Date: February 2025

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2025 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Linux Audit File SmartConnector	4
Product Overview	4
Configuration	6
Preparing to Install the SmartConnector	6
Installing and Configuring the SmartConnector by Using the Wizard	8
Configuring Event Merging	8
Device Event Mapping to ArcSight Fields	9
Send Documentation Feedback	12

Configuration Guide for Linux Audit File SmartConnector

This guide provides information for installing the SmartConnector for Linux Audit File and configuring the device for event collection. Linux auditd is the userspace component to the Linux Auditing System that is responsible for writing audit records to the disk.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 25.1](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

The Linux auditd daemon is similar to network-based intrusion detection systems and host-based intrusion detection systems and can help you detect violations of your security policies. It however, does not enforce security policies. Because the audit daemon is part of the Linux kernel, it is included in most major Linux distributions by default.

Configuration

For complete information about the Linux auditd daemon, see the man pages for `auditd`, `auditd.conf`, and `auditctl`. You can access these man pages by running the `man auditd` or `man auditctl` commands, from the command line of your Linux system.

- `auditctl` is responsible for controlling the status and some basic system parameters of `auditd`. Using audit rules, `auditctl` controls which components of your system are subjected to the audit and to what extent they are audited. Audit rules can be passed to `auditd` on the `auditctl` command line as well as by composing a rule set and instructing `auditd` to process this file.
 - `auditd` has built-in functions to watch access attempts to files without needing to monitor the applicable system calls. Administrators can add rules by amending the provided configuration files or at run time using the command line. The default location for the audit daemon rules is `/etc/audit/audit.rules`.
- `auditd` adds events to the audit log file as they occur. By default, the system stores audit logs in `/var/log/audit/`.

Before you can start generating audit logs and processing them, configure how the daemon is started in the `/etc/sysconfig/auditd` configuration file and configure how the audit system functions once the daemon has been started in `/etc/audit/auditd.conf`.

Preparing to Install the SmartConnector

The following sections provide instructions for installing and configuring the Linux Audit File SmartConnector.



Connector Appliance or ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector by Using the Wizard

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant Global Parameters, when prompted.
4. From the **Type** drop-down list, select **Linux Audit File** as the type of connector, then click **Next**.
5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Log File Name	Enter the path to and name of the log file. The default value is /var/log/audit/audit.log.

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. Select whether you want to [run the connector as a service or in the standalone mode](#).
9. Complete the installation.
10. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [SmartConnector Installation and User Guide](#).



When using Windows authentication, after completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should log in to the database. The connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

Configuring Event Merging

The Linux Audit system provides a way to track security-relevant information on the system. Based on pre-configured rules, Linux Audit generates log entries to record as much information as possible about the events happening on your system. These events often contain multiple sub-events that can span multiple lines. The event merging feature aggregates the related sub-events into one large event with a concatenated long

message.

To enable event merging:

1. Set up Linux Audit connector. See [Installing the SmartConnector](#).
2. Edit the fcp.version parameter in the agent.properties file (located in the \$ARCSIGHT_HOME/current/user/agent folder) as follows: agents [0].fcp.version=1
3. [Run the SmartConnector](#).

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Linux Audit Mappings to ArcSight Fields for log type PROCTITLE

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Proctitle
Device Custom String 1 Label	Proctitle

Linux Audit Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	proto
Destination Address	One of (daddr,laddr,dst)
Destination Mac Address	dmac
Destination Port	One of (dest, dport, lport)
Destination Process ID	One of (egid, opid)
Destination Process Name	One of (exe, comm, cmd ,ocomm)
Destination Service Name	One of (com, ocomm, grantors)
Destination User ID	One of (auid, new auid, old auid, old-auid, ouid)
Destination User Name	One of (new-seuder, acct, OUID)
Destination User Privilege	new-role
Device Action	op
Device Custom Number 1	calipso_doi

Configuration Guide for Linux Audit File SmartConnector
 Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	One of (oses,ses,new ses, oldses,old-ses)
Device Custom Number 3	uid
Device Custom String 1	One of (dev, old, nsec)
Device Custom String 2	One of (key, calipso_type, new, sec)
Device Custom String 3	One of (success, res)
Device Custom String 4	One of(syscall,SYSCALL,op)
Device Custom String 5	subj
Device Custom String 6	One of (terminal, tty)
Device Event Category	All (type, res, SYSCALL)
Device Event Class ID	One of (res, type, both (type, res))
Device Host Name	node
Device Inbound Interface	inif
Device Outbound Interface	outif
Device Process Name	'auditd'
Device Product	'auditd'
Device Receipt Time	timestamp
Device Vendor	'Unix'
Device Version	One of (ver,kernel)
Event Outcome	One of (result, res, __simpleMap(success,"yes=Successful","no=Failed"))
Event Reason	One of (reason,cause)
External ID	callid
File Hash	One of (proctitle,data,cmd,fp)
File ID	One of (watch_inode,cap_fver,sw)
File Name	One of (path, name, watch, obj)
File Path	cwd One of (cwd,root_dir)
File Permission	One of (mode, perm)
File Size	ksize
Flex String 2	One of (ppid,direction)
Message	msg
Name	One of (res, SYSCALL,type, both (res, type),'Linux Audit Message')

Configuration Guide for Linux Audit File SmartConnector

Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Old File Hash	mac
Old File ID	All of (a0,a1,a2,...), argc
Old File Name	cipher
Old File Path	cmdline
Request URL	pfs
Source Address	One of (addr,saddr,src)
Source Host Name	hostname
Source Mac Address	smac
Source Port	One of (sport, rport)
Source Process ID	One of (pid, Spid, spid)
Source User ID	One of (sauid, uid, oauid,AUID)
Source User Name	One of (user, old-seuser, EUID,OAUID)
Source User Privileges	One of (old-role, EGID)



Note: The connector will not receive events if MySQL JDBC driver 5.1.38 was used when you configured it. To fix this issue, apply MySQL JDBC driver 5.0.8.

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 Configuration Guide for Linux Audit File SmartConnector (SmartConnectors CE 25.1)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: CE 25.1

Configuration Guide for Linux Audit Syslog SmartConnector

Document Release Date: February 2025

Software Release Date: February 2025

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2025 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

SmartConnector for Linux Audit Syslog	4
Product Overview	5
Configuration	6
Configuring Event Merging	6
Configuring to Recieve Syslog Events	7
Installing the SmartConnector	10
Preparing to Install the SmartConnector	10
Installing and Configuring the SmartConnector by Using the Wizard	10
Device Event Mapping to ArcSight Fields	14
Send Documentation Feedback	17

SmartConnector for Linux Audit Syslog

This guide provides information for installing the SmartConnector for Linux Audit Syslog and configuring the device for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 25.1](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

The Linux auditd daemon can help you detect violations of your security policies. It detects violations of security policy but does not enforce it. Rather, it is similar to network-based intrusion detection systems and host-based intrusion detection systems. Because the audit daemon is part of the Linux kernel, it is included in most major Linux distributions by default.

Configuration

For complete information about the Linux auditd daemon, see the man pages for `auditd`, `auditd.conf`, and `auditctl`. You can access these man pages by running the `man auditd` or `man auditctl` commands, from the command line of your Linux system.

Linux auditd does not log to syslog by default. To enable syslog logging, edit `# /etc/audisp/plugins.d/syslog.conf` and change the line `active = no` to `active = yes`.

- `auditctl` is responsible for controlling the status and some basic system parameters of `auditd`. Using audit rules, `auditctl` controls which components of your system are subjected to the audit and to what extent they are audited. Audit rules can be passed to `auditd` on the `auditctl` command line as well as by composing a rule set and instructing `auditd` to process this file.
- `auditd` has built-in functions to watch access attempts to files without needing to monitor the applicable system calls. Administrators can add rules by amending the provided configuration files or at run time using the command line. The default location for the audit daemon rules is `/etc/auditd/audit.rules`.

Before you can start generating audit logs and processing them, configure the audit daemon itself. Configure how it is started in the `/etc/sysconfig/auditd` configuration file and configure how the audit system functions once the daemon has been started in `/etc/auditd.conf`.

Configuring Event Merging

The Linux Audit system provides a way to track security-relevant information on the system. Based on pre-configured rules, Linux Audit generates log entries to record as much information as possible about the events happening on your system. These events often contains multiple sub-events that can span multiple lines. The event merging feature aggregates the related sub-events into one large event with a concatenated long message.

To enable event merging:

1. Set up Linux Audit connector. See [Installing the SmartConnector](#).
2. Edit the `syslog.subagent.parsers` parameter in the `agent.properties` file (located in the `$ARCSIGHT_HOME/current/user/agent` folder) as follows:

```
agents[0].syslog.subagent.parsers=linux_auditd_syslog\::merge
```

3. [Run the SmartConnector](#).

Configuring to Recieve Syslog Events

The syslog SmartConnectors use a sub-connector architecture that lets them receive and process syslog events from multiple devices. There is a unique regular expression that identifies the device. For example, the same SmartConnector can process events from a Cisco Router and a NetScreen Firewall simultaneously. The SmartConnector inspects all incoming messages and automatically detects the type of device that originated the message.

You can install the syslog SmartConnector as a syslog daemon, pipe, or file connector. You can use the Syslog Deamon, Syslog Deamon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Syslog Daemon SmartConnector

The Syslog Deamon SmartConnector is a syslogd-compatible daemon designed to work in operating systems that have no syslog daemon in their default configuration, such as Microsoft Windows. The SmartConnector for Syslog Daemon implements a UDP receiver on port 514 by default, or can be configured on another port to receive syslog events. You can also configure to use the TCP protocol.

To use the SmartConnector for Syslog Daemon, add the following statement in the *rsyslog.conf* file:

```
*.* @@(remote/local-host-IP):514
```

Example: local1.warning @@10.0.0.1:514

- To read all Syslog events, use `*.*`
- To filter specific events, replace regex with the specific event name.
- For example: `*.* @@(remote/local-host-IP):514` and `local1.warning @@10.0.0.1:514`.
- To send events over a TCP connection, use `@@` and to send events over an UDP connection, use `@`.

If you are running SmartConnector for Syslog Daemon on the same machine as the server, you must provide the IP address of the local host. If you want to forward events to other machines, you must provide the IP address of the same.

Messages longer than 1024 bytes might be split into multiple messages on syslog daemon. No such restriction exists on syslog file or pipe.

Syslog Pipe and File SmartConnectors

When a syslog daemon is already in place and configured to receive syslog messages, an extra line in the syslog configuration file *rsyslog.conf* can be added to write the events to either a file or a system pipe and the ArcSight SmartConnector can be configured to read the events from it. In this scenario, the ArcSight SmartConnector runs on the same machine as the syslog daemon. The additional configurations for the ArcSight syslog file or syslog pipe SmartConnectors in the system where all Syslog Daemon SmartConnector configurations are done.

The Syslog Pipe SmartConnector is designed to work with an existing syslog daemon. This SmartConnector is especially useful when storage is a factor. In this case, *syslogd* is configured to write to a named pipe, and the Syslog Pipe SmartConnector reads from it to receive events.

The Syslog File SmartConnector is similar to the Pipe SmartConnector. However, this SmartConnector monitors events written to a syslog file such as *messages.log* rather than to a system pipe.

Using the SmartConnector for Syslog Pipe or File

This section provides information to set up your existing syslog infrastructure to send events to the ArcSight Syslog Pipe or File SmartConnector.

The standard UNIX implementation of a syslog daemon reads the configuration parameters from the */etc/rsyslog.conf* file, which contains specific details about which events to write to files, write to pipes, or send to another host.

For Syslog Pipe:

1. Execute the following command to create a pipe:

```
mkfifo /var/tmp/syspipe
```

2. Add one of the following lines depending on your OS to the */etc/rsyslog.conf* file:

```
*.debug /var/tmp/syspipe
```

or

```
*.debug |/var/tmp/syspipe
```

3. Restart the syslog daemon in one of the following methods:

Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

```
kill -HUP `cat /var/run/syslog.pid`
```

For Syslog File:

1. Create a file or use the default file into which log messages must be written.
2. Modify the /etc/rsyslog.conf file

The syslog daemon is forced to reload the configuration and start writing to the pipe.

3. Restart the syslog daemon in one of the following methods:

- a. Restart the syslog daemon in one of the following methods:
Enter the following commands:

```
/etc/init.d/syslogd stop  
/etc/init.d/syslogd start
```

or

Execute the following command to send a configuration restart signal:

On RedHat Linux:

```
service syslog restart
```

On Solaris:

```
kill -HUP `cat /var/run/syslog.pid`
```

Installing the SmartConnector

The following sections provide instructions for installing and configuring the Linux Audit Syslog SmartConnector.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the Linux Audit Syslog Connector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the Linux Audit Syslog Connector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. Do one of the following depending on your requirement:

- Select **Syslog Daemon** from the **Type** drop-down:
 - a. Click **Next** and specify the following parameters:

Parameter	Description
Network port	The SmartConnector for Syslog Daemon listens for syslog events from this port.
IP Address	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address, apart from the default (ALL) to bind to all available IP addresses.
Protocol	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Forwarder	This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None .

- b. Click **Next**.
- Select **Syslog File** from the **Type** drop-down:

a. Click **Next**, and specify the following parameters:

Parameter	Description
Pipe Absolute Path Name	Specify an absolute path to the pipe, or accept the default value: /var/tmp/syspipe.
File Absolute Path Name	<p>Specify the full path name for the file from which this connector will read events. The following are default values:</p> <ul style="list-style-type: none">Solaris:\var\adm\messagesLinux:\var\log\messages <p>You can use a wildcard pattern in the file name.</p> <p>In the real-time mode, rotation can occur only if the file is over-written or removed from the folder. The real-time processing mode assumes the following external rotation:</p> <ul style="list-style-type: none">Date format log rotation: The device creates a new log at a specified time in the with the naming convention filename.timestamp.log. The connector detects the new log and terminates the reader thread to the previous log after the processing is complete. The connector then creates a new reader thread to the new filename.timestamp.log and begins processing that file. To enable this log rotation, specify timestamp in yyyy-MM-dd date format. For example, filename.yyyy-MM-dd.logIndex log rotation: The device writes to indexed files in the following format: filename.log.001, filename.log.002, filename.log.003, and so on. At startup, the connector processes the log with highest index. When the device creates a log with a greater index, the connector terminates the reader thread to the previous log after processing completes, creates a thread to the new log, and begins processing that log. To enable this log rotation, use an index format, as shown in the following example:filename'%d,1,99,true'.log; Specifying true indicates that the index can be skipped. For example, if 5 appears before 4, processing proceeds with 5 and will not read 4. Use of true is optional.

Parameter	Description
Reading Events Real Time or Batch	Specify whether to read files in batch mode or real-time mode. In batch mode, all files are read from the beginning.
Action Upon Reaching EOF	This option applies to Batch Mode only. Specify None , Rename , or Delete as the action to be performed to the file when the connector finishes reading and reaches end of file . For the real-time mode, retain the default value None .
File Extension If Rename Action	This option applies to Batch Mode only. Specify the extension to be added to the file name if the action on reaching the end of file is specified as Rename . The default value is Processed , which adds a .processed extension.

- b. Click **Next**.
5. Select a [destination and configure parameters](#).
 6. Specify a name for the connector.
 7. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

8. Select whether you want to install the connector as a service or in the standalone mode.
9. Complete the installation.
10. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Linux Audit Mappings to ArcSight Fields for log type PROCTITLE

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Proctitle
Device Custom String 1 Label	Proctitle

Device Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	proto
Destination Address	One of (daddr,laddr,dst)
Destination Mac Address	dmac
Destination NT Domain	One of (new-seuser,acct)
Destination NT Domain	One of (new-seuser,acct)
Destination Port	One of (dest, dport, lport)
Destination Process ID	One of (egid,opid)
Destination Process Name	One of (exe, comm, cmd ,ocomm)
Destination Service Name	One of (com, ocomm, grantors)
Destination User ID	One of (auid, new auid, old auid, old-auid, ouid)
Destination User Name	One of (new-seuder, acct, OUID)
Destination User Privilege	new-role
Device Action	op
Device Custom IPv6 Address 2	src
Device Custom IPv6 Address 3	dst
Device Custom Number 1	calipso_doi
Device Custom Number 2	One of (oses,ses,new ses, oldses,old-ses)
Device Custom Number 3	uid

Configuration Guide for Linux Audit Syslog SmartConnector
 Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	One of (dev, old, nsec)
Device Custom String 2	One of (key, calipso_type, new, sec)
Device Custom String 3	One of (success, res)
Device Custom String 4	One of(syscall,SYSCALL,op)
Device Custom String 5	subj
Device Custom String 6	One of (terminal, tty)
Device Event Class ID	One of (res, type, both (type, res))
Device Event Category	All (res,SYSCALL,type)
Device Host Name	node
Device Inbound Interface	inif
Device Outbound Interface	outif
Device Process Name	auditd, audisp-syslog, augenrules, dbus-daemon, firewalld, kernel, setroubleshoot, systemd, system-logind
Device Product	auditd
Device Receipt Time	timestamp
Device Vendor	'Unix'
Device Version	One of (ver,kernel)
Event Outcome	One of (result, res, __simpleMap(success,"yes=Successful","no=Failed"))
Event Reason	One of (reason,cause)
External ID	callid
File Hash	One of (proctitle,data,cmd,fp)
File ID	One of (watch_inode,cap_fver,sw)
File Name	One of (path, name, watch, obj)
File Path	One of (cwd,root_dir)
File Permission	One of (mode, perm)
File Size	ksize
Flex String2	One of (ppid,direction)
Message	msg
Name	One of (res, SYSCALL,type, both (res, type),'Linux Audit Message')
Old File Hash	mac

Configuration Guide for Linux Audit Syslog SmartConnector

Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Old File ID	All of (a0,a1,a2,...), argc
Old File Name	cipher
Old File Path	cmdline
Request URL	pfs
Source Address	One of (addr,saddr,src)
Source Host Name	hostname
Source Mac Address	smac
Source Port	One of (sport, rport)
Source Process ID	One of (pid, Spid, spid)
Source User ID	One of (sauid, uid, oauid,AUID)
Source User Name	One of (user, old-seuser, EUID,OAUID)
Source User Privileges	One of (old-role, EGID)



Note: The connector will not receive events if MySQL JDBC driver 5.1.38 was used when you configured it. To fix this issue, apply MySQL JDBC driver 5.0.8.

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 Configuration Guide for Linux Audit Syslog SmartConnector (SmartConnectors CE 25.1)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 8.4.3

Tech Notes - SmartConnectors Locales and Encodings

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Chapter 1: ArcSight Locales and Encodings	4
Chapter 2: Localized ArcSight ESM	5
Before you Install a Localized Version of ArcSight ESM	5
ArcSight Database	5
Selecting an Encoding	5
ArcSight Manager	6
ArcSight Console	6
ArcSight SmartConnectors	7
Setting the Encoding for Selected SmartConnectors	7
Localization of Date Formats in Tokens and Operations	7
Key-Value Parsers for Localized Devices	8
Chapter 3: Examples	9
Scenario 1 - Events received in a single language only	9
Database	9
ArcSight Manager, Console, and Web	9
Scenario 2 - Events received in multiple languages	9
Database	9
ArcSight Manager, Console, and Web	10
Chapter 4: Preparing to Install the Language Update	11
Verifying the Character Set used on your Database	11
Chapter 5: Installing the Language Update	13
List of possible values for the agent.parser.locale.name property	13
Send Documentation Feedback	18

Chapter 1: ArcSight Locales and Encodings

The information in this technical note applies to ArcSightESM v4.0 SP1 and later and ArcSightLogger v2.0 and later.

ArcSight products are translated into various languages, for instance Japanese, traditional Chinese, simplified Chinese, and Korean. Setting the Locale for any of these languages ensures that you get the appropriate environment in terms of language settings, number format, date/time format, timezone settings, and Daylight Saving Time setting for that country or language. This document describes the updates to be taken into consideration when configuring ArcSightESM for a supported language.

ArcSightLogger can log events in some non-English and some non-Western languages, but has not yet been localized to a non-English language. Logger should support every encoding, but has only been certified with a representative sample.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Chapter 2: Localized ArcSight ESM

Before you Install a Localized Version of ArcSight ESM

The ArcSight Manager, Database, and Console components should all be configured with the same locale.

By default, all communication between ArcSight components is done using UTF-8 character encoding. Even though ArcSight ESM supports only UTF-8 internally, if your connector receives events in UTF-16, for example, the events are still stored correctly since these events get converted to UTF-8 by the connector before they are passed on to the Manager. The Manager then passes these events to the database where they are converted to the language-specific encoding you selected while installing the database before being persisted.

If you are currently on ESM v4.0 GA and would like to switch to a localized version of the product, you must complete the following tasks:

1. Upgrade to v4.0 SP1. See the *Upgrading ArcSight™ ESM v4.0 GA to v4.0 SP1* document for instructions.
2. Install the language update. See "[Installing the Language Update](#)" in this document.

ArcSight Database

Before you install ArcSight Database, choose the encoding scheme.



Note: You cannot make changes to the encoding after you have installed the database. Any change will require reinstallation.

Selecting an Encoding

You can choose between UTF-8 and pre-defined language-specific encodings during database installation. The advantage of using UTF-8 is that it supports all major languages in the world, so no data is lost when it is saved in the database. On the other hand, UTF-8 requires more space to store certain characters than the character's language-specific encoding. For example, if a certain Japanese character can be stored in two bytes using JA16SJIS encoding, the same character might take 3 bytes if stored in UTF-8.

Select an encoding in the **Allowed TNS Clients** drop-down list in the Oracle Installation Wizard. The following table lists the available languages.

Language	Encoding
English	WE8MSWIN1252
French	WE8ISO8859P1
Japanese	JA16SJIS
Chinese_Simplified	ZHS16CGB231280
Chinese_Traditional	ZHT16BIG5
Korean	K016KSC5601
Unified_UTF8	UTF8

In the table, "English" represents all western European languages. If you need to use a character set not shown in the table, see the *ArcSight Installation and Configuration Guide* for instructions on how to set it correctly.

If you anticipate that you will be storing events in multiple languages, choose a character set (encoding) that is compatible with ALL languages you intend to use.

For more than one non-English language, you should choose Unified_UTF8.

If you select Unified_UTF8, you must select the language in which you want the standard content to be installed on the database.

If you already have the database installed with an encoding other than Unified_UTF8, but would like to change the encoding to Unified_UTF8, you must re-install the database and select Unified_UTF8 Database Character Set when prompted during the installation.

ArcSight Manager

Install the ArcSight Manager on an operating system that is of the same language as the language you selected while installing the database. During startup, ArcSight Manager automatically detects and uses the locale from the operating system.

ArcSight Console

Install the ArcSight Console on an operating system that is of the same language as the language you selected while installing the database. During startup, ArcSight Console automatically detects and uses the locale from the operating system.

ArcSight SmartConnectors

If a device is configured to use a language-specific encoding (not Unicode), the connector receiving events from this device should be configured to use the same encoding as the device.

Setting the Encoding for Selected SmartConnectors

You can set the encoding to a character set corresponding to your Locale for the following SmartConnectors only:

- SAP Real-Time Security Audit Multi-Folder Connector.

See the *SmartConnector for SAP Real-time Security Audit Multi-Folder Configuration Guide* for instructions on how to configure the encoding for this connector.

- IBM DB2 Audit File Connector.

See the *SmartConnector for IBM DB2 Audit File Configuration Guide* for instructions on how to configure the encoding for this connector.

- Oracle SYSDBA Audit Multi-Folder Connectors

See the *SmartConnector for Oracle SYSDBA Audit Multi-Folder Configuration Guide* for instructions on how to configure the encoding for this connector.

These SmartConnectors support all character sets supported by Java. For a list of the character sets supported by Java see <http://java.sun.com/j2se/1.5.0/docs/guide/intl/encoding.doc.html>.



You must change the encoding to match the log files' encoding only if the log files use an encoding other than the default one.

Connectors not mentioned above use the default encoding of the operating system on which they reside. Each operating system comes with default encodings for various languages of the world. So, the encoding used in a connector is either based on the character set that you selected when installing the ArcSight Database or the operating system you are using.

Localization of Date Formats in Tokens and Operations

If your connector receives logs that contain timestamps in a non-English language or a date format that is customarily used by a non-English locale (for example, "mai 24, 2006 12:56:07.615" where "mai" is German for May) that your connector is set to, configure the `agent.parser.locale.name` property in the `agent.properties` file. This file is located in `ARCSIGHT_HOME/current/user/agent` directory.

Set the `agent.parser.locale.name` property to the value that corresponds to the connector's locale. By default, this property is set to `en_US`. Refer to "[List of possible values for the agent.parser.locale.name property](#)" on page 13 for possible values for this property.

Key-Value Parsers for Localized Devices

Some localized devices not only send localized values but also localized keys in event messages. In such a case, additional processing may be needed to translate the keys to English for the event messages to be properly parsed. For example, assume that the content of a key-value parser is:

`event.destinationUserName=User`

And the received event message is:

`User=김` where 김 is Korean for KIM.

In this case, the parser works fine as-is, since double-byte is already supported.

If the received event message is: `우새르 = 김` where 우새르 is Korean for User, then additional mapping is needed to translate 우새르 to User.

If you encounter a need for a localized device, contact ArcSight Support.

Windows Event Log Connector supports the following locales to parse the non-English language Keys in the Windows Event Log description:

- ja (Japanese)
- de (German)
- zh_CN (Simplified Chinese)
- zh_TW (Traditional Chinese)

Contact ArcSight Support for assistance with other non-supported languages.

Chapter 3: Examples

The following examples cover two different scenarios.

Scenario 1 - Events received in a single language only

This scenario describes what to do when your connector(s) receive data in a single language only, such as Japanese. In ESM , the default encoding for Japanese is JA16SJIS.

Database

While installing the database, in the ArcSight Oracle Installation Wizard, select one of the following from the **Database Character Set** drop down menu:

- Japanese
- Unified_UTF8

If you select **Japanese**, the database uses JA16SJIS encoding when saving the data into the database.

If you select **Unified_UTF8**, you must also select **Japanese** in the ArcSight Database Schema Initialization screen to ensure that the default system resources get installed in Japanese.

Keep in mind, some characters might take 3 bytes when stored in UTF-8 but might take only 2 bytes when stored in JA16SJIS.

ArcSight Manager, Console, and Web

You must install the ArcSight Manager, Console, and Web on a Japanese operating system. On startup, these components automatically pick up and use the locale from the operating system.

Scenario 2 - Events received in multiple languages

This scenario is an example of what to do when you are dealing with multiple connectors that receive data in different languages.

Database

When you install the database, in the ArcSight Oracle Installation Wizard:

1. Select **Unified_UTF8** from the **Database Character Set** dropdown menu. This ensures that no data is lost in translation when persisted in the database.
2. In the ArcSight Database Schema Initialization screen, select the language in which you want the standard content resources to be installed.

ArcSight Manager, Console, and Web

When you installed the ArcSight Database you selected a language in which to install the system resources. You should install the ArcSight Manager, Console, and Web on an operating system of that same language. On startup, these components automatically pick up the locale from the operating system.

Chapter 4: Preparing to Install the Language Update

If you are currently running ESM v4.0 GA and would like to switch to a localized version, you must upgrade your ESM installation (ArcSight Database, Manager, Console, and Web server) to v4.0 SP1.



Note: While upgrading your database to v4.0 SP1, make sure that the character set you select during the upgrade is compatible with the one that you selected when installing your existing database.

Once your system is running ESM v4.0 SP1, you need to install the language update.

Verifying the Character Set used on your Database

If you currently use ESM v4.0 SP1, your database already has a character set specified. Follow this procedure to validate the character set that was selected when the v4.0 SP1 database was installed:

1. Run the following command from the ARCSIGHT_HOME/bin directory:

```
arcdbutil sql
```

2. When prompted for user-name, enter:

```
/ as sysdba
```

3. Run the following SQL statement:

```
SQL>select "PARAMETER", "VALUE" from SYS.GV$_NLS_PARAMETERS where  
PARAMETER='NLS_CHARACTERSET';
```



Note: You can set the encoding only during database installation. To change the encoding after installation, you must reinstall ArcSight Database.

The following character sets (encodings) are supported for ArcSight Database:

Language	Character Set
English	WE8MSWIN1252
French	WE8ISO8859P1
Japanese	JA16SJIS
Chinese Simplified	ZHS16CGB231280

Tech Notes - SmartConnectors Locales and Encodings
Chapter 4: Preparing to Install the Language Update

Language	Character Set
Chinese Traditional	ZHT16BIG5
Korean	KO16KSC5601
Unified UTF8	UTF-8

Chapter 5: Installing the Language Update

By now, your database should be set to the encoding of your choice. If you have not already done so, follow the instructions in "[Verifying the Character Set used on your Database](#)" to verify the database encoding, before you proceed.

You must install the language update on ArcSight Manager, Console and Web. Refer to the Release Notes for the Language Update for installation instructions.

List of possible values for the agent.parser.locale.name property

The table below lists the possible values for this property.

Values	Language	Country	Variant
ar	Arabic		
ar_AE	Arabic	United Arab Emirates	
ar_BH	Arabic	Bahrain	
ar_DZ	Arabic	Algeria	
ar_EG	Arabic	Egypt	
ar_IQ	Arabic	Iraq	
ar_JO	Arabic	Jordan	
ar_KW	Arabic	Kuwait	
ar_LB	Arabic	Lebanon	
ar LY	Arabic	Libya	
ar_MA	Arabic	Morocco	
ar_OM	Arabic	Oman	
ar_QA	Arabic	Qatar	
ar_SA	Arabic	Saudi Arabia	
ar_SD	Arabic	Sudan	
ar_SY	Arabic	Syria	
ar_TN	Arabic	Tunisia	
ar_YE	Arabic	Yemen	
be	Belarusian		

Values	Language	Country	Variant
be_BY	Belarusian	Belarus	
bg	Bulgarian		
bg_BG	Bulgarian	Bulgaria	
ca	Catalan		
ca_ES	Catalan	Spain	
cs	Czech		
cs_CZ	Czech	Czech Republic	
da	Danish		
da_DK	Danish	Denmark	
de	German		
de_AT	German	Austria	
de_CH	German	Switzerland	
de_DE	German	Germany	
de_LU	German	Luxembourg	
el	Greek		
el_GR	Greek	Greece	
en	English		
en_AU	English	Australia	
en_CA	English	Canada	
en_GB	English	United Kingdom	
en_IE	English	Ireland	
en_IN	English	India	
en_NZ	English	New Zealand	
en_US	English	United States	
en_ZA	English	South Africa	
es	Spanish		
es_AR	Spanish	Argentina	
es_BO	Spanish	Bolivia	
es_CL	Spanish	Chile	
es_CO	Spanish	Columbia	
es_CR	Spanish	Costa Rica	

Values	Language	Country	Variant
es_DO	Spanish	Dominican Republic	
es_EC	Spanish	Ecuador	
es_ES	Spanish	Spain	
es_GT	Spanish	Guatemala	
es_HN	Spanish	Honduras	
es_MX	Spanish	Mexico	
es_NI	Spanish	Nicaragua	
es_PA	Spanish	Panama	
es_PE	Spanish	Peru	
es_PR	Spanish	Puerto Rico	
es_PY	Spanish	Paraguay	
es_SV	Spanish	El Salvador	
es_UY	Spanish	Uruguay	
es_VE	Spanish	Venezuela	
et	Estonian		
et_EE	Estonian	Estonia	
fi	Finnish		
fi_FI	Finnish	Finland	
fr	French		
fr_BE	French	Belgium	
fr_CA	French	Canada	
fr_CH	French	Switzerland	
fr_FR	French	France	
fr_LU	French	Luxembourg	
hi_IN	Hindi	India	
hr	Croatian		
hr_HR	Croatian	Croatia	
hu	Hungarian		
hu_HU	Hungarian	Hungary	
is	Icelandic		
is_IS	Icelandic	Iceland	

Values	Language	Country	Variant
it	Italian		
it_CH	Italian	Switzerland	
it_IT	Italian	Italy	
iw	Hebrew		
iw_IL	Hebrew	Israel	
ja	Japanese		
ja_JP	Japanese	Japan	
ko	Korean		
ko_KR	Korean	Korea	
lt	Lithuanian		
lt_LT	Lithuanian	Lithuania	
lv	Latvian		
lv_LV	Latvian	Latvia	
mk	Macedonian		
mk_MK	Macedonian	Macedonia	
nl	Dutch		
nl_BE	Dutch	Belgium	
nl_NL	Dutch	Netherlands	
no	Norwegian		
no_NO	Norwegian	Norway	
no_NO_NY	Norwegian	Norway	Nynorsk
pl	Polish		
pl_PL	Polish	Poland	
pt	Portuguese		
pt_BR	Portuguese	Brazil	
pt_PT	Portuguese	Portugal	
ro	Romanian		
ro_RO	Romanian	Romania	
ru	Russian		
ru_RU	Russian	Russia	
sk	Slovak		

Values	Language	Country	Variant
sk_SK	Slovak	Slovakia	
sl	Slovenian		
sl_SI	Slovenian	Slovenia	
sq	Albanian		
sq_AL	Albanian	Albania	
sv	Swedish		
sv_SE	Swedish	Sweden	
th	Thai		
th_TH	Thai	Thailand	
th_TH_TH	Thai	Thailand	TH
tr	Turkish		
tr_TR	Turkish	Turkey	
uk	Ukrainian		
uk_UA	Ukrainian	Ukraine	
vi	Vietnamese		
vi_VN	Vietnamese	Vietnam	
zh	Chinese		
zh_CN	Chinese	China	
zh_HK	Chinese	Hong Kong	
zh_TW	Chinese	Taiwan	

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 Tech Notes - SmartConnectors Locales and Encodings (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Message Trace Rest API SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Configuration Guide for Message Trace Rest API SmartConnector 8.4.3

This guide provides information to install the SmartConnector for Message Trace Rest API and configure the end point for event collection. For supported devices and versions, see [Technical Requirements for SmartConnector](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

Message tracking or message tracing, as it is called in Office 365, is one of the most basic tools used by administrators to monitor the email flow. As emails travel through Office 365, some information about them gets stored in logs and is available for administrative purposes. Even if users delete or purge messages, the administrator is able to view basic information about sent and received emails.

Message tracing does not allow you to view a message's content. However, it can provide a lot of important data about the message, such as the following:

- Sender and recipient
- Sent and received dates
- Subject and size
- Delivery status and details of events, which include:
 - Delivered
 - Failed
 - Pending
 - Expanded
 - Quarantined
 - Filtered as spam
 - Unknown
- IP address used to send the message
- Message ID, a unique number identifying a message. If a message has more than one recipient, the message tracing tool logs an entry for every recipient of the message. Each of these entries has the same Message-ID but a different Message Trace ID in the message trace search.

Installing the Connector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Preparing to Install the Connector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the Connector, do the followings:

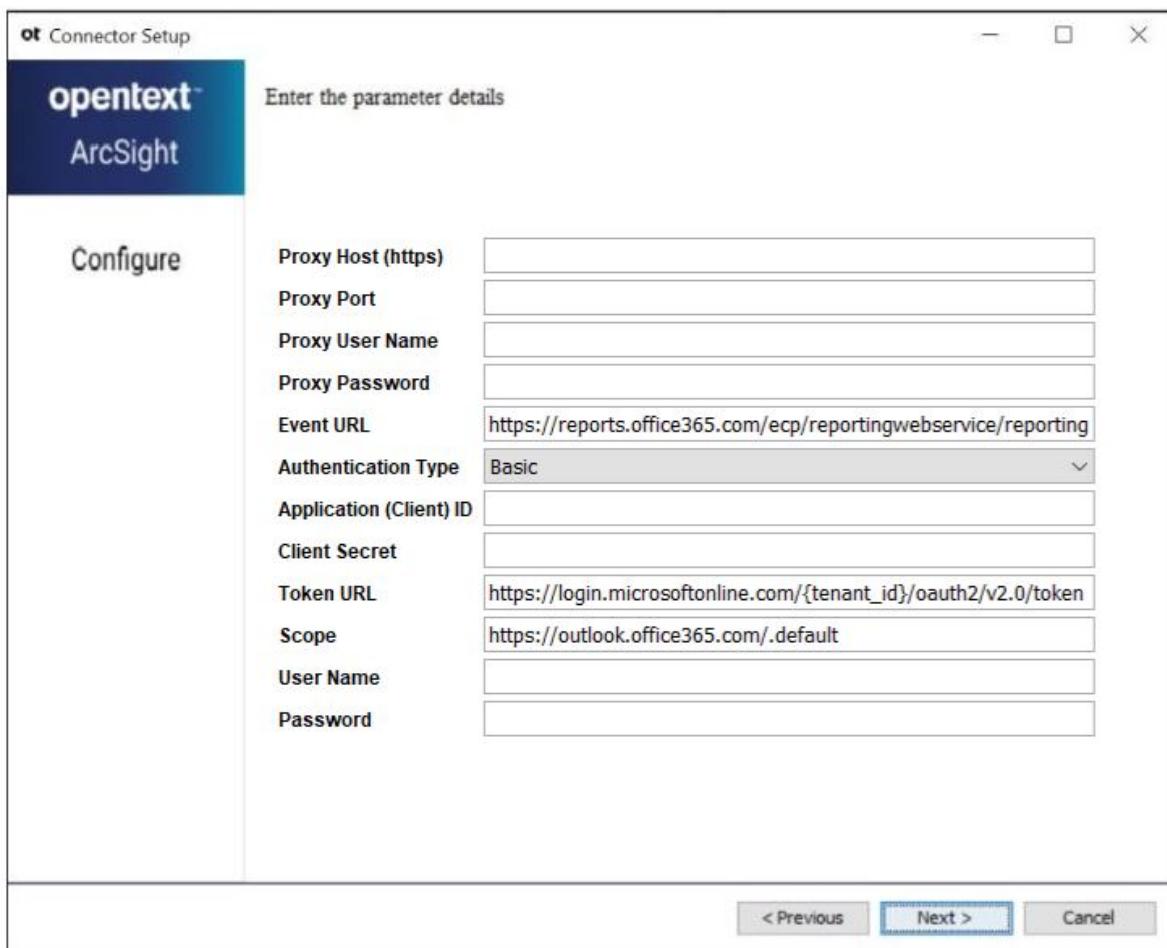
- In the [Azure portal](#), create an Azure AD App Registration to receive the events from Office 365 message trace REST API.
- Assign your application the **Global Reader** role to enable an access to the Reporting Web Service.
- Add the **ReportingWebService.Read.All** permission to the application.
- Generate **Client ID** and **Client Secrets**.

Installing and Configuring the Connector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. From the **Type** drop-down menu, select **Message Trace REST API** as the type of connector, and then click **Next**.
5. Enter the following parameters to configure the connector, and then click **Next**:

Configuration Guide for Message Trace Rest API SmartConnector

Installing the Connector



Parameter	Description
Proxy Host (https)	(Optional) If proxy is enabled for your machine, the IP address or host name of the proxy server required for proxy configuration to access the internet.
Proxy Port	(Optional) If proxy is enabled for your machine, the port number of the proxy server required for proxy configuration.
Proxy User Name	(Optional) If proxy is enabled for your machine, the user name for the proxy server. Specify this value only if proxy needs access to the Internet. If you enter the proxy user name, you must provide the proxy password.
Proxy Password	(Optional) If proxy is enabled for your machine, the password for the proxy server user. Specify this value only if proxy needs access to internet and you have specified a user name for the proxy server.
Event URL	This is a mandatory field. The URL from where you need to fetch events. The default value is: https://reports.office365.com/ecp/reportingwebservice/reporting.svc/MessageTrace

Authentication Type	<p>This is a mandatory field.</p> <p>An authentication method to secure REST APIs. You can select either Basic or OAuth2-Client Credentials for the authentication in message trace REST API.</p> <p>The default value is: Basic</p>
Application (Client) ID	<p>The client application ID assigned to your app.</p> <p>This is a mandatory field when you select the Authentication Type parameter value as OAuth2-Client Credentials.</p>
Client Secret	<p>The client secret key generated for your app in the registration portal.</p> <p>This is a mandatory field when you select the Authentication Type parameter value as OAuth2-Client Credentials.</p>
Token URL	<p>The URL to get access token.</p> <p>This is a mandatory field when you select the Authentication Type parameter value as OAuth2-Client Credentials.</p> <p>The default value is: <a href="https://login.microsoftonline.com/<tenant_id>/oauth2/v2.0/token">https://login.microsoftonline.com/<tenant_id>/oauth2/v2.0/token In this URL, <tenant_id> is the directory tenant ID in the GUID or domain-name format, against which the application will operate.</p>
Scope	<p>This is a mandatory field when you select the Authentication Type parameter value as OAuth2-Client Credentials.</p> <p>The URL to identify scope. API users will be asked to consent to all of the configured permissions present on the Azure AD App Registration for the respective resource (for example: https://reports.office365.com).</p> <p>The default value is: https://outlook.office365.com/.default</p>
User Name	<p>The user name for the Office 365 server with administrative permissions.</p> <p>This is a mandatory field when you select the Authentication Type parameter value as Basic.</p>
Password	<p>The password for the Office 365 user.</p> <p>This is a mandatory field when you select the Authentication Type parameter value as Basic.</p>

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select **Do not import the certificate to connector from destination**, the connector installation will end.

9. Select whether you need to run the connector as a service or in the standalone mode.
10. Complete the installation.

11. [Run the SmartConnector.](#)
12. For instructions about upgrading the connector or modifying its parameters, see [Installation and User Guide for SmartConnector](#).

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device-specific event definitions. For more information about the ArcSight data fields, refer to the [ArcSight Console User's Guide for ESM](#).

ArcSight ESM Field	Device-Specific Field
Destination Address	ToIP
Device Product	'Exchange Online'
External Id	MessageTraceId
Name	Both('Message ',Status)
Source Address	FromIP
Source User Name	SenderAddress
Destination User Name	RecipientAddress
Device Custom String 3	Subject
Device Custom String 6	Organization
Device Event Class Id	Both('Message ',Status)
Device Receipt Time	Received
Device Vendor	'Microsoft'
File Id	MessageId
File Size	Size

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 Configuration Guide for Message Trace Rest API SmartConnector
(SmartConnectors 8.4.3)**

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 24.4.1

Configuration Guide for Microsoft 365 Defender SmartConnector

Document Release Date: December 2024

Software Release Date: December 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft 365 Defender SmartConnector	4
Product Overview	5
Understanding Event Collection	5
Preparing to Install the SmartConnector	6
Microsoft 365 Defender API in Microsoft Threat Protection (Security API)	6
Registering an Azure Active Directory Application with appropriate Permissions for Microsoft 365 Defender	6
Adding Permissions for Microsoft 365 Defender Incidents	7
Generating Client Secret for the Application	7
Microsoft 365 Defender API in Microsoft Graph	7
Registering an Azure Active Directory Application with appropriate Permissions for Microsoft 365 Defender	7
Adding Permissions for Microsoft 365 Defender Incidents	8
Generating Client Secret for the Application	8
Microsoft 365 Defender API in Certificate-based Authentication	8
Creating Self-Signed Certificate	9
Installing and Configuring the SmartConnector	10
Device Event Mapping to ArcSight Fields	13
Event Mapping for Alerts via Security API	15
Incident	15
Alerts	15
Devices	16
Entities	17
Event Mapping for Alert V2 via Graph API - alert V2	18
Alerts	18
Device Evidence	18
Process Evidence	19
File Evidence	20
IP Evidence	20
Url Evidence	20
Registry Value Evidence	21
Cloud Application Evidence	21
Oauth Application Evidence	21
Analyzed Message Evidence	22
Send Documentation Feedback	23

Configuration Guide for Microsoft 365 Defender SmartConnector

The ArcSight Microsoft 365 Defender configuration guide provides information to install the SmartConnector for Microsoft 365 Defender and configure the connector for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

The SmartConnector for Microsoft 365 Defender retrieves incidents from Microsoft 365 Defender, normalizes and sends these incidents to the configured destinations.

For more information about Microsoft 365 Defender and its services, see the [Microsoft 365 Defender documentation](#).

Understanding Event Collection

The SmartConnector for Microsoft 365 Defender uses access tokens to authenticate and allow an application to access an API. The access token will be retrieved by using the client credentials - client ID and client secret.

The following call details are used to access the retrieved tokens:

Request type: Post

Token URL: `https://login.windows.net/<tenant_id provided in setup>/oauth2/token`

Parameters:

```
grant_type = client_credentials  
client_id=<client_id provided in setup>  
client_secret = <client_secret provided in setup>  
resource=https://api.security.microsoft.com
```

The retrieved access token will be valid for one hour by default. A new access token will be retrieved after the old access token expires.

Microsoft 365 Defender incidents are retrieved by using the following Event URL:

`https://api.security.microsoft.com/api/incidents?$filter=lastUpdateTime+ge+<START_AT_TIME>`

<START_AT_TIME> is replaced with the current time in the following format:

`yyyy-MM-dd'T'HH:mm:ss.SSSSSSS'Z'`

Limitations

- Maximum page size is 100 incidents
- Maximum rate of requests is 50 calls per minute and 1500 calls per hour

The SmartConnector for Microsoft 365 Defender uses certificate-based authentication method to authenticate applications and services that need to access the Graph API. To authenticate

using certificate, an Application must be registered with Azure AD and certificate needs to be uploaded in the Azure AD portal to obtain the Application ID and Client Secret.

The following call details are used to access the retrieved tokens:

Request type: Post

Token URL: `https://login.windows.net/<tenant_id provided in setup>/oauth2/token`

Parameters:

```
grant_type = client_credentials
```

```
client_id=<client_id provided in setup>
```

```
client_assertion_type = The value must be set to urn:ietf:params:oauth:client-assertion-type:jwt-bearer
```

```
client_assertion= An assertion (a JSON web token) is created. Log in with the certificate that you registered as credentials for your application.
```

```
resource=https://api.security.microsoft.com
```

The retrieved access token will be valid for one hour by default. A new access token will be retrieved after the old access token expires.

Preparing to Install the SmartConnector

Before Installing the SmartConnector, complete the following procedures:

1. [Microsoft 365 Defender API in Microsoft Threat Protection \(Security API\)](#)
2. [Microsoft 365 Defender API in Microsoft Graph](#)
3. [Microsoft 365 Defender API in Certificate-based Authentication](#)

Microsoft 365 Defender API in Microsoft Threat Protection (Security API)

Registering an Azure Active Directory Application with appropriate Permissions for Microsoft 365 Defender

1. Log in to Azure as a **Global Administrator User**.
2. Navigate to **Azure Active Directory > App Registrations > New Registration**.

3. In the registration form, select your application.
4. Click **Register**.

Adding Permissions for Microsoft 365 Defender Incidents

1. On the **Application Page**, select **API Permissions > Add a Permission > APIs my Organization uses**.
2. Type **Microsoft Threat Protection** on the search panel, and select **Microsoft Threat Protection**. Your application can now access **Microsoft 365 Defender**.
3. Choose **Application Permissions > Incident.Read.All** and select **Add Permissions**.

For more information regarding Azure Active Directory application with the appropriate permissions for Microsoft 365 Defender Incidents, see <https://docs.microsoft.com/en-us/microsoft-365/security/defender/api-hello-world?view=o365-worldwide>

Generating Client Secret for the Application

1. Click **Certificates and Secrets**.
2. Click **New Client Secret**.
3. Add **Description** to the secret and click **Add**.
4. Note the generated **Secret Value**.



Important: If you do not note down the **Secret Value**, you will not be able to retrieve it later.

5. On the application page, go to **Overview** and **Copy** the following:
 - Application (Client) ID
 - Directory (Tenant) ID

Microsoft 365 Defender API in Microsoft Graph

Registering an Azure Active Directory Application with appropriate Permissions for Microsoft 365 Defender

1. Log in to **Azure** as a **Global Administrator User**.
2. Navigate to **Azure Active Directory > App Registrations > New Registration**.

3. In the registration form, select your application.
4. Click **Register**.

Adding Permissions for Microsoft 365 Defender Incidents

1. Navigate to the application page and select **API Permissions > Microsoft Graph**.
2. Select **Delegated permissions**, and type **security** in the search bar. Then select **SecurityAlert.Read.All** and click **Add permission**.
3. Click **admin consent** for your tenant. Multiple permissions can be selected. You can then grant admin consent for all.

For more information regarding Azure Active Directory application with the appropriate permissions for Microsoft 365 Defender Incidents,
see<https://techcommunity.microsoft.com/t5/microsoft-365-defender-blog/the-new-microsoft-365-defender-apis-in-microsoft-graph-are-now/ba-p/3603099>

Generating Client Secret for the Application

1. Click **Certificates and Secrets**.
2. Click **New Client Secret**.
3. Add **Description** to the secret and click **Add**.
4. Note the generated **Secret Value**.



Important: If you do not note down the **Secret Value**, you will not be able to retrieve it later.

5. On the application page, go to **Overview** and **Copy** the following:
 - Application (Client) ID
 - Directory (Tenant) ID

Microsoft 365 Defender API in Certificate-based Authentication

Certificate-based authentication is used to authenticate applications and services that need to access the Graph API. To authenticate using certificate, an Application must be registered with Azure AD to obtain the Application ID and Client Secret. The Application must also generate a self-signed certificate or obtain a certificate from a Trusted Certificate Authority (CA). The

Certificate is then uploaded to the Azure AD Application Registration and is used to authenticate the application when it requests access to the Graph API.

When an Application requests access to the Graph API using certificate-based authentication, Azure AD verifies the Certificate to ensure that it is valid and issued by a trusted CA. If the certificate is valid, Azure AD grants the Application an Access Token, which the Application can use to access the Graph API.

Creating Self-Signed Certificate

1. Create the self-signed certificate. Refer to the [Microsoft documentation](#) for more information regarding the self-signed certificate and authenticating the Application.
2. Register an Azure Active Directory Application with appropriate permissions for Microsoft 365 Defender as per the following steps:
 - a. Log in to **Azure** as a **Global Administrator User**.
 - b. Navigate to **Azure Active Directory > App Registrations > New Registration**.
 - c. In the registration form, select your application.
 - d. Click **Register**.
3. Add the required permissions for Microsoft 365 Defender Incidents as per the following steps:
 - a. On the **Application Page**, select **API Permissions > Add a Permission > APIs my Organization uses**.
 - b. Type **Microsoft Threat Protection** on the search panel, and select **Microsoft Threat Protection**. Your application can now access **Microsoft 365 Defender**.
 - c. Choose **Application Permissions > Incident.Read.All** and select **Add Permissions**.
 - d. For more information regarding Azure Active Directory application with the appropriate permissions for Microsoft 365 Defender Incidents, see <https://docs.microsoft.com/en-us/microsoft-365/security/defender/api-hello-world?view=o365-worldwide>
4. Generate the Client Secret for the Application as per the following steps:
 - a. Click **Certificates and Secrets**.
 - b. Click **New Client Secret**.
 - c. Add **Description** to the secret and click **Add**.
 - d. Note the generated **Secret Value**.



Important: If you do not note down the **Secret Value**, you will not be able to retrieve it later.

- e. On the application page, go to **Overview** and **Copy** the following:
 - Application (Client) ID
 - Directory (Tenant) ID
5. Select **Certificates & Secrets > Certificates**.
6. Click **Upload Certificate** and select the required certificate file to be uploaded.
7. Click **Add**.
After the certificate is uploaded, the **Thumbprint**, **Start Date**, and **Expiration Values** are displayed.

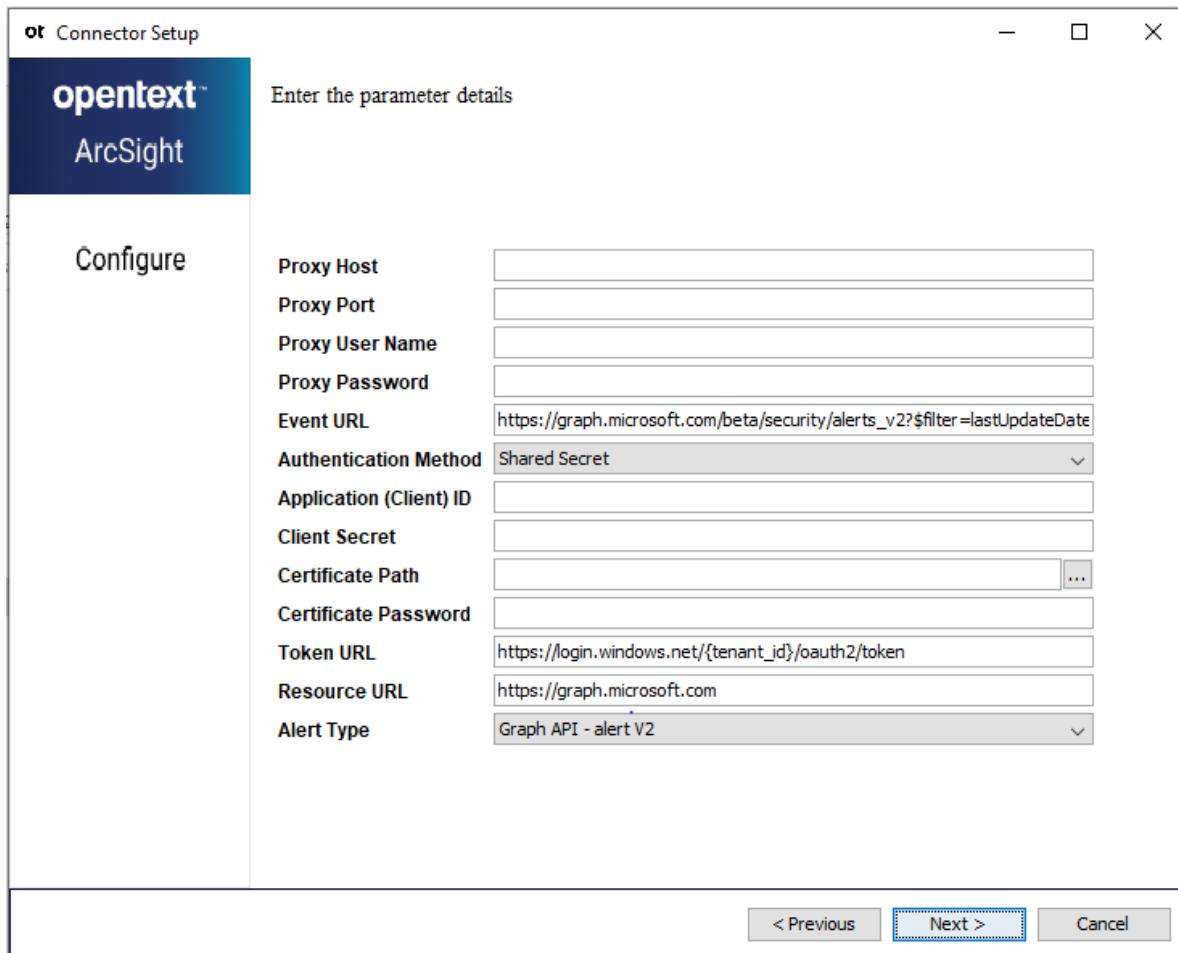
Installing and Configuring the SmartConnector

The installation steps described in this section are specific to the Microsoft 365 Defender Connector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the Microsoft 365 Defender Connector:

Start the installation wizard.

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. From the **Type** drop-down list, select **Microsoft 365 Defender** as the type of connector, then click **Next**.
5. Enter the following parameters to configure the SmartConnector and then click **Next**.



Parameter	Description
Proxy Host (https)	(Optional) If proxy is enabled for your machine, the IP address or host name of the proxy server required for proxy configuration to access the internet.
Proxy Port	(Optional) If proxy is enabled for your machine, the port number of the proxy server required for proxy configuration.
Proxy User Name	(Optional) If proxy is enabled for your machine, the user name for the proxy server. Specify this value only if proxy needs access to the Internet. If you enter the proxy user name, you must provide the proxy password.
Proxy Password	(Optional) If proxy is enabled for your machine, the password for the proxy server user. Specify this value only if proxy needs access to internet and you have specified a user name for the proxy server.

Parameter	Description
Event URL	<p>This is a mandatory field.</p> <p>The URL from where you need to fetch events.</p> <p>The default value is: <code>https://graph.microsoft.com/beta/security/alerts_v2?\$filter=lastUpdateDateTime+ge+\$START_AT_TIME</code></p> <p>Sample URL for Graph API - alert V2 -</p> <pre><code>https://graph.microsoft.com/beta/security/alerts_v2?\$filter=lastUpdateDateTime+ge+\$START_AT_TIME</code></pre> <p>Sample URL for Security API -</p> <pre><code>https://api.security.microsoft.com/api/incidents?\$filter=lastUpdateTime+gt+\$START_AT_TIME</code></pre> <div style="background-color: #e0f2e0; padding: 10px;">  Note: If you want to fetch events of a specific period, use the startattime parameter in <code>agent.properties</code>. Do not remove "<code>\$START_AT_TIME</code>" in the URL. </div> <p>Event URL will depend on the selected Alert Type.</p>
Authentication Method	<p>This is a mandatory field.</p> <p>An authentication method for authenticating using Certificate. You can select either Shared Secret or Certificate for the authentication method in Microsoft 365 defender.</p> <p>The default value is: Shared Secret</p>
Application (Client) ID	<p>The client application ID assigned to your application.</p> <p>This is a mandatory field when you select the Authentication Method parameter value as Shared Secret or Certificate both.</p>
Client Secret	<p>The client secret key generated for your application in the registration portal.</p> <p>This is a mandatory field when you select the Authentication Method parameter value as Shared Secret.</p>
Certificate Path	<p>The certificate file path(.pfx) that you will provide.</p> <p>This is a mandatory field when you select the Authentication Method parameter value as Certificate.</p>
Certificate Password	<p>The certificate password that you will provide.</p> <p>This is a mandatory field when you select the Authentication Method parameter value as Certificate.</p>

Parameter	Description
Token URL	<p>The URL to get the access token.</p> <p>The default value is: https://login.windows.net/{tenant_id}/oauth2/token. It is mandatory that you must replace the {tenant_id} in the URL with <your Tenant ID>.</p>
Resource URL	<p>The URL to locate the resources.</p> <p>The default value is: https://graph.microsoft.com</p> <p>Sample URL for Security API - https://api.security.microsoft.com</p> <p>Sample URL for Graph API - alert V2 - https://graph.microsoft.com</p> <p>Resource URL will depend on the selected Alert Type.</p>
Alert Type	<p>The type of alert through which you want to fetch events. You can select any of the following alert types:</p> <ul style="list-style-type: none"> • Security API (For further information, visit this website). • Graph API - alert V2 (For further information, visit this website).

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select **Do not import the certificate to connector from destination**, the connector installation will end.

9. Select whether you want to run the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).
12. For instructions about upgrading the connector or modifying parameters, see [SmartConnector Installation and User Guide](#).

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device-specific event definitions. For more information about the ArcSight data fields, refer to the [ArcSight Console User's Guide for ESM](#).

Security API

Each incident retrieved from Microsoft 365 Defender is processed, split, and sent to the configured destinations in the following structure:

- **Incidents**

One top-level incident event is sent per incident.

- **Alerts**

- One alert event is sent for each device present in the alert.

- One alert event is sent for each entity present in the alert.

Alert events can be correlated using the **alertId (Device Custom String 2)** and the **incidentId (External ID)** fields.

Graph API - alert V2

Each alert retrieved from Microsoft 365 Defender is processed, split, and sent to the configured destinations in the following structure:

Alerts

- One alert event is sent for each evidence present in the alert.
- One top-level alert event is sent per alert.

Sample alert:

```
Alert1
{
  Evidence1
  Evidence2
}
```

ArcSight security event format expected by the connector:

1. Alert1 + Evidence1 (+ device evidence if applicable)
2. Alert1 + Evidence2 (+ device evidence if applicable)
3. Alert1 (top level alert event)

Event Mapping for Alerts via Security API

Incident

ArcSight ESM Field	Device-Specific Field
Additional Data	redirectIncidentId
Additional Data	assignedTo
Additional Data	determination
Device Custom String 4	tags
Device Event Class ID	"365DefenderIncident"
Device Product	"365 Defender"
Device Receipt Time	lastUpdateTime
Device Severity	severity
Device Vendor	"Microsoft"
Event Outcome	status
External ID	incidentId
Name	incidentName
Reason	classification
Start Time	createdTime

Alerts

ArcSight ESM Field	Device-Specific Field
Additional Data	actorName
Additional Data	assignedTo
Additional Data	detectorId
Additional Data	investigationId
Additional Data	serviceSource
Additional Data	determination
Additional Data	classification
Device Action	investigationState
Device Custom Date 1	firstActivity

ArcSight ESM Field	Device-Specific Field
Device Custom Date 2	lastActivity
Device Custom String 1	threatFamilyName
Device Custom String 2	alertId
Device Custom String 6	mitreTechniques
Device Event Category	category
Device Event Class ID	category
Device Process Name	detectionSource
Device Receipt Time	lastUpdatedTime
Device Severity	severity
End Time	resolvedTime
Event Outcome	status
External ID	incidentId
Message	description
Name	title
Start Time	creationTime

Devices

ArcSight ESM Field	Device-Specific Field
Additional Data	firstSeen
Additional Data	rbacGroupName
Additional Data	aadDeviceId
Additional Data	healthStatus
Destination Host Name	deviceDnsName
Device Custom String 3	riskScore
Device Custom String 4	tags
Device Custom String 5	<code>__concatenate (osPlatform, ,version, ,osProcessor, ,osBuild)</code>
Device External ID	mdatpDeviceId

Entities

ArcSight ESM Field	Device-Specific Field
Additional Data	registryValueType
Additional Data	evidenceCreationTime
Additional Data	sha1
Additional Data	deliveryAction
Additional Data	mailboxDisplayName
Destination Address	ipAddress
Destination Nt Domain	domainName
Destination Process ID	processId
Destination User ID	userSid
Destination User Name	__oneOf(accountName,recipient)
Device Custom String 3	__oneOf (registryKey,mailboxAddress)
Device Custom String 4	__oneOf (processCommandLine,subject)
Device Custom String 5	__oneOf (registryValue,userPrincipalName)
Device External ID	deviceId
File Create Time	processCreationTime
File Hash	sha256
File Name	fileName
File Path	filePath
File Type	entityType
Old File Create Time	parentProcessCreationTime
Old File ID	parentProcessId
Old File Name	parentProcessFileName
Request Url	url
Source User Name	sender

Event Mapping for Alert V2 via Graph API - alert V2

Alerts

ArcSight ESM Field	Device-Specific Field
Device Event Category	category
Device Event Class ID	category
Device Process Name	detectionSource
Device Receipt Time	lastUpdateDateTime
Device Severity	category
End Time	resolvedDateTime
Event Outcome	status
External ID	incidentid
flex Number1	evidenceCount
flex Number1Label	evidenceCount
flex String2	parentEvent
flex String2Label	parentEvent
Message	description
Name	title
Request URL	alertWebUrl
Start Time	createdDateTime

Device Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole
File Modification Time	firstSeenDateTime
Device External Id	mdeDeviceId
Destination Host Name	deviceDnsName
Device Custom String 3	osPlatform version osBuild
Additional Data	healthStatus

ArcSight ESM Field	Device-Specific Field
Old File Permission	riskScore
Source Translated Address	lastExternalIpAddress
Source Address	lastIpAddress
Device Inbound Interface	ipInterfaces
Source User Name	loggedOnUsers (accountName)
Source NT Domain	loggedOnUsers (domainName)

Process Evidence

ArcSight ESM Field	Device-Specific Field
Destination Process Id	processId
Old File Id	parentProcessId
Device Custom Date 1	processCreationDateTime
Device Custom Date 2	parentProcessCreationDateTime
Device Custom String 4	processCommandLine
Device Custom String 5	remediationStatus & remediationStatusDetails
Additional Data.Sha1	sha1
File Hash	sha256
File Name	fileName
File Path	filePath
File Size	fileSize
Old File Hash	parentProcessImageFile/sha256
Old File Name	parentProcessImageFile/fileName
Old File Path	parentProcessImageFile/filePath
Old File Size	parentProcessImageFile/fileSize
Destination User Name	__oneOf (userAccount/accountName,userAccount/userPrincipalName)
Destination NT Domain	userAccount/domainName
Destination User ID	userAccount/userSid

File Evidence

ArcSight ESM Field	Device-Specific Field
Additional Data	fileDetails/sha1
File Hash	fileDetails/sha256
File Name	fileDetails/fileName
File Path	fileDetails/filePath
File Size	fileDetails/fileSize
Device Custom String 5	remediationStatus & remediationStatusDetails
User Evidence	
File Create Time	createdDateTime
Old File Type	evidenceRole
Destination User Name	__oneOf(userAccount_accountName,userAccount_userPrincipalName)
Destination NT Domain	userAccount/domainName
Destination User ID	userAccount/userSid

IP Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole
Device Custom String 5	remediationStatus & remediationStatusDetails
Source Address	ipAddress

Url Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	remediationStatus & remediationStatusDetails
Source DNS Domain	url

Registry Value Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole
Device Custom String 3	registryKey
Device Custom String 5	remediationStatus & remediationStatusDetails
Old File Permission	registryHive
Old File Path	registryValue
Old File Name	registryValueName
Additional Data	registryValueType

Cloud Application Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole
Device Custom String 5	remediationStatus & remediationStatusDetails
Old File ID	appId
Additional Data	displayName
File ID	instanceId
Old File Name	instanceName

Oauth Application Evidence

ArcSight ESM Field	Device-Specific Field
File Create Time	createdDateTime
Old File Type	evidenceRole

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	remediationStatus & remediationStatusDetails
Old File ID	appId
Additional Data	displayName
Old File Permission	objectId
Destination NT Domain	publisher

Analyzed Message Evidence

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	threats
Device Custom String 3 Label	Threats
Device Custom String 4	networkmessageid
Device Custom String 4 Label	Networkmessageid
Source Address	senderIp
Old File Type	evidenceRole
Device Custom String 5	remediationStatus & remediationStatusDetails
Device Custom String 5 Label	Remediation Status
Destination User Name	recipientEmailAddress
Source User Name	p1Sender/emailAddress
Source NT Domain	p1Sender/domain
Additional Data p2 Sender Domain	p2Sender/domain
Device Custom Number 1	urlCount
Device Custom Number 1 Label	urlCount
Device Custom Number 2	attachmentsCount
Device Custom Number 2 Label	attachmentsCount
Additional Data p2 Sender Email	p2Sender/emailAddress
Additional Data URLs	urls
Additional Data Delivery Action	deliveryAction
Destination Geo Location Info	deliveryLocation

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 Configuration Guide for Microsoft 365 Defender SmartConnector
(SmartConnectors 24.4.1)**

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 MFI-Documentation-Feedback@opentext.com .

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Microsoft Audit Collection System DB SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

Configuration Guide for Microsoft Audit Collection System DB SmartConnector	4
Product Overview	5
Prerequisites	7
Installing and Configuring Microsoft Audit Collection Services	7
Deploying Audit Collection Services	7
Downloading the JDBC Driver	8
Installing the SmartConnector	9
Preparing to Install the SmartConnector	9
Installing and Configuring the SmartConnector	9
Adding JDBC Driver to the Connector Appliance/ArcSight Management Center	12
Device Event Mapping to ArcSight Fields	13
Microsoft ACS with Operations Manager 2007-2012 Mappings	13
Microsoft Auditing Collection System Mappings	14
Troubleshooting	16
Send Documentation Feedback	18

Configuration Guide for Microsoft Audit Collection System DB SmartConnector

This guide provides information to install the SmartConnector for Microsoft Audit Collection System DB and configuring the device for event collection.

This guide provides a high level overview of ArcSight SmartConnectors.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

The Microsoft Audit Collection System (ACS) offers a solution to the problem of security log management. With ACS, audit events are securely sent to a central repository in real time and are stored in an SQL database.

In Operations Manager, you can use Audit Collection Services (ACS) to collect records generated by an audit policy and store them in a centralized database. By default, when an audit policy is implemented on a Microsoft Windows computer, that computer automatically saves all events generated by the audit policy to its local Security log. This is so for Windows workstations as well as servers.



With ACS, only a user who has specifically been given the right to access the ACS database can run queries and create reports on the collected data.

In Operations Manager 2007, the deployment of ACS involves the following:

ACS Forwarders

The service that runs on ACS forwarders is included in the Operations Manager agent. By default, this service is installed but not enabled when the Operations Manager agent is installed. You can enable this service for multiple agent computers at once using the Enable Audit Collection task. After you enable this service, all security events are sent to the ACS collector in addition to the local Security log.

ACS Collector

The ACS collector receives and processes events from ACS forwarders and then sends this data to the ACS database. This processing includes disassembling the data so that it can be spread across several tables within the ACS database, minimizing data redundancy, and applying filters so that unnecessary events are not added to the ACS database.

ACS Database

The ACS database is the central repository for events that are generated by an audit policy within an ACS deployment. The ACS database can be located on the same computer as the ACS collector, but for best performance, each should be installed on a dedicated server.

The server that hosts the ACS database must have Microsoft SQL Server 2005 or Microsoft SQL Server 2008. You can choose an existing or new installation of SQL Server. The Enterprise edition is recommended by Microsoft because of the stress of daily ACS database maintenance.



This connector does not retrieve the fields 'String07 - String22' fields in the dtEvent tables in the interest of high performance SQL Query. These fields often are not populated by the ACS collector and do not contain any significant pieces of information when they are populated. However, String01 through String06 are mapped to the Device Custom String fields. See the Event Mappings section for more detail. All the remaining important fields in the dtEvent tables are retrieved into the ArcSight fields.



In high throughput environments, if the connector is shut down for extended periods of time, a large number of events can collect which can clog the connector on restart. This condition can be avoided by setting preservestate to false. See the Troubleshooting section for instructions on setting preservestate.

Prerequisites

Installing and Configuring Microsoft Audit Collection Services

For complete information about installation and configuration requirements for Microsoft ACS, see <http://technet.microsoft.com/en-us/library/bb381258.aspx>

Deploying Audit Collection Services

To deploy ACS:

1. Plan an audit policy for your organization.
2. Plan your ACS server deployment. Identify the server that will act as the ACS database and the Operations Manager 2007 Management Server that will act as the ACS collector.
3. Identify the Operations Manager agents that will be ACS forwarders. All computers from which you want to collect security events must be ACS forwarders.
4. Install and configure prerequisites for ACS components.
5. (Optional) Do the following to separate administrator and auditor roles:
 - a. [Create a local group](#) for users who access and run reports on the data in the ACS database.
 - b. Grant the newly created local group access to the SQL database by creating a [new SQL Login](#) for the group and assigning that login the db_datareader permission.
 - c. Add accounts of users who will act as auditors to the local group.
6. Deploy the ACS Database and ACS Collector or Collectors. See "How to Install an ACS Collector and Database" at <http://technet.microsoft.com/en-us/library/bb381258.aspx> for complete information.
7. Run the **Enable Audit Collection** task to start the ACS Forwarder service on the ACS forwarders. For more information, see <http://technet.microsoft.com/en-us/library/bb381258.aspx>.
8. Implement your audit policy within your organization.

Downloading the JDBC Driver

The SmartConnector installation requires JDBC driver to be present. During the installation process, you will be directed to leave the wizard and copy the JDBC driver file you downloaded to a SmartConnector folder.



Note: Different versions of the JDBC driver are required for different SQL Server database versions. The name of the jar file may be different for some JDBC driver versions. Make sure that you use the correct driver for your database version

Refer to the following information to download the correct jar file depending on the JRE version used by the SmartConnector:

- SmartConnector Version 8.3.0 uses JRE 1.8.0_312 and supports jar files from version mssql-jdbc-6.4.0.jre8.jar ([Download Microsoft JDBC Driver 6.4 for SQL Server](#)) to mssql-jdbc-9.4.0.jre8.jar ([Download Microsoft JDBC Driver 9.4.0 for SQL Server](#)).
- SmartConnector Version 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar ([Download Microsoft JDBC Driver 6.0 for SQL Server](#)).
- SmartConnector Version 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar ([Download Microsoft JDBC Driver 6.0 for SQL Server](#)).
- Earlier versions of SmartConnector run JRE 1.6 and require sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server).

For more information related to the Microsoft JDBC driver, see [Microsoft Documentation](#).

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

ArcSight recommends that you do not install the database connectors on the database server or any mission critical servers as this might cause performance issues.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and Configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Exit the installation wizard.
4. Copy the jar file associated with the version of the driver that you downloaded earlier to \$ARCSIGHT_HOME/current/user/agent/lib
5. To use JDBC driver with SmartConnectors to connect to Microsoft SQL Servers by using Windows authentication, copy the sqljdbc_auth.dll file from the JDBC driver download to the \$ARCSIGHT_HOME\jre\bin directory.

An example of The JDBC driver download path for SQL JDBC driver is:

- For version 4.0 for 32-bit environment is `sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll`
- For 64-bit environment, `sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll`

To use the latest version of SQL JDBC Driver such as 9.4:

- Copy the `mssql-jdbc-9.4.0.jre8.jar` file associated with the version of the driver that you downloaded earlier to `$ARCSIGHT_HOME/current/user/agent/lib`
- Copy the `mssql-jdbc_auth-9.4.0.x64.dll` file from the JDBC driver download to the `$ARCSIGHT_HOME\jre\bin` directory.



Note: If you are upgrading the SmartConnector, you must copy the authentication file to `$ARCSIGHT_HOME\jre\bin` again after update, as the upgrade process overwrites the `$ARCSIGHT_HOME\jre\bin` directory.

6. Copy certificate and JDBC files to SmartConnector folders as follows:

- Copy the `jssecacerts` certificate that you installed during the device configuration to the SmartConnector installation folder `$ARCSIGHT_HOME/current/jre/lib/security`.



Note: You must copy this file again to the installation folder after upgrading the SmartConnector as this file gets overwritten during the upgrade process.

- Copy the `vjdbc.jar` and `commons-logging-1.1.jar` files to the SmartConnector installation folder `$ARCSIGHT_HOME/current/user/agent/lib`. These files are located in the `lib` directory that was created when you downloaded the JDBC driver and unzipped the package.

7. Browse to `$ARCSIGHT_HOME/current/bin`, then double-click `runagentsetup.bat` file to start the SmartConnector Configuration Wizard.

8. Specify the relevant Global Parameters, when prompted.

9. From the **Type** drop-down list, select **Microsoft Audit Collection System DB** as the type of connector, then click **Next**.

10. Enter the following parameters to configure the SmartConnector, then click **Next**.

Configuration Guide for Microsoft Audit Collection System DB SmartConnector

Installing the SmartConnector

Parameter	Description
JDBC Driver	Select the <code>com.microsoft.sqlserver.jdbc.SQLServerDriver</code> driver.
JDBC URL	Enter <code>jdbc:sqlserver://<MS SQL Server Host Name or IP Address>:1433;DatabaseName=<MS SQL Server Database Name></code> . Replace with the actual values for <MS SQL Server Host Name or IP Address> and <MS SQL Server Database Name>. To configure JDBC Driver and Windows Authentication, add <code>;integratedSecurity=true</code> to the JDBC URL entry for the connection to your database.  Note: The name or instance of the database configured at installation or audit time must be used. For example, <code>jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true</code>
Database User	Enter the login name of the database user with database audit privilege.
Database Password	Enter the password for the database user.

11. Select a [destination and configure parameters](#).
12. Specify a name for the connector.
13. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

14. Select whether you want to install the connector as a service or in the standalone mode.
15. Complete the installation.
16. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).



Note: When using Windows authentication, after completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should log in to the database. The connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

Adding JDBC Driver to the Connector Appliance/ArcSight Management Center

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the required containers, as follows:

1. From the Connector Appliance/ArcSight Management Center, select **Setup > Repositories**.
2. Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
3. Click **Upload to Repository**.
4. From the **Repository File Creation Wizard**, select **Individual Files**, then click **Next**.
5. Retain the default selection and click **Next**.
6. Click **Upload** and locate and select the .jar file you downloaded.
7. Click **Submit** to add the specified file to the repository and click **Next** to continue.
8. After adding all the files you require, click **Next**.
9. In the **Name** field, enter a descriptive name for the zip file (for example, JDBCdriver). Click **Next**.
10. Click **Done** to complete the process. The newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
11. To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.
12. Select one or more containers into which you want to upload the driver, then click **Next**.
13. Click **Done** to complete the process.
14. Add the connector through the Connector Appliance/ArcSight Management Center interface. For more information, see the *Connector Appliance/ArcSight Management Center Online Help*.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Microsoft ACS with Operations Manager 2007-2012 Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Audit_failure; High = Error; Medium = Warning, Unknown; Low = Audit_success, Information
Destination Host Name	One of (EventMachine, DB_HOST)
Destination NT Domain	One of (PrimaryDomain, TargetDomain)
Destination Process Name	One of (PrimarySid, TargetSid)
Destination User ID	PrimaryLogonId
Destination User Name	One of (PrimaryUser, TargetUser)
Device Custom Date 1	CollectionTime
Device Custom Number 2	Id
Device Custom String 1	StringValue01
Device Custom String 2	StringValue02
Device Custom String 3	StringValue03
Device Custom String 4	StringValue04
Device Custom String 5	StringValue05
Device Custom String 6	StringValue06
Device Event Category	Source
Device Event Class ID	Both (Source, EventId)
Device External ID	_DB_CURRENT_TABLE_ID
Device Host Name	AgentMachine
Device NT Domain	HeaderDomain
Device Process Name	HeaderSid
Device Product	'Microsoft Auditing Collection System'
Device Receipt Time	CreationTime

Configuration Guide for Microsoft Audit Collection System DB SmartConnector
 Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Severity	Type (0=Unknown, 1=Error, 2=Warning, 4=Information, 8=Audit_success, 16=Audit_failure)
Device Vendor	'Microsoft'
Device Version	SCOM 2007/2012
External ID	SequenceNo
Name	One of (Category, 'ACS Event')
Source NT Domain	One of (ClientDomain, PrimaryDomain)
Source Process Name	ClientSid
Source User ID	ClientLogonId
Source User Name	One of (ClientUser, HeaderUser, PrimaryUser)

Microsoft Auditing Collection System Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Audit_failure; High = Error; Medium = Warning, Unknown; Low = Audit_success, Information)
Destination Host Name	AuditMachine
Destination NT Domain	One of (PrimaryDomain, TargetDomain)
Destination Process Name	One of (TargetSid, PrimaryUser)
Destination User ID	PrimaryLogonId
Destination User Name	One of (PrimaryUser, TargetUser)
Device Custom Date 1	CollectionTime
Device Custom Number 2	Id
Device Event Category	Source
Device Event Class ID	Both (Source, EventId)
Device Host Name	AgentMachine
Device NT Domain	HeaderDomain
Device Process Name	HeaderSid
Device Product	'Microsoft Auditing Collection System'
Device Receipt Time	CreationTime
Device Severity	Type (0=Unknown, 1=Error, 2=Warning, 4=Information, 8=Audit_success, 16=Audit_failure)

Configuration Guide for Microsoft Audit Collection System DB SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Version	ACS
External ID	SequenceNo
Name	One of (Category, 'ACS Internal Event')
Source NT Domain	ClientDomain
Source Process Name	ClientSid
Source User ID	ClientLogonId
Source User Name	One of (ClientUser, HeaderUser)

Troubleshooting

"What do I do when the connector can't reconnect to the MS SQL Server database?"

In some cases, connectors using MS SQL Server databases are unable to reconnect to the database after losing and reacquiring network connection. Restarting the connector will resolve this problem.

"How do I deploy SQL Server Native Client?"

When deploying an application that is dependent on SQL Server Native Client, you will need to redistribute SQL Server Native Client with your application. Unlike Microsoft Data Access Components (MDAC), which is now a component of the operating system, SQL Server Native Client is a component of SQL Server. Therefore, it is important to install SQL Server Native Client in your development environment and redistribute SQL Server Native Client with your application.

The SQL Server Native Client redistributable installation program, named sqlncli.msi, is available on the SQL Server installation media and is available as one of the SQL Server Feature Pack components on the Microsoft Download site. For more information about deploying SQL Server Native Client with your application, see "Deploying Applications with SQL Server Native Client" available from Microsoft.

"Why does my connection to SQL Server fail/hang?"

Oracle has released Java 6 update 30 (6u30) that behaves differently from JRE 6u29, causing possible database connection problems for SQL Server database connectors using JDBC connection. These connection problems can occur with JRE 1.6.0_29 (6u29) and later versions.

Microsoft recommends using JRE 6u30 (and above) instead of JRE 6u29. Apply the "SQL Server 2008 R2 Service Pack 1 Cumulative Update 6" patch to the SQL server if you are experiencing connection failures or hangs.

"Why am I receiving the message 'Login failed for user 'sqluser'. The user is not associated with a trusted SQL Server connection."

Only Microsoft JDBC driver v4 or later support integrated authentication. The driver also does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

"How can I keep the connector from becoming clogged with events after being shut down for awhile?"

If the connector is shut down for some time on an active database, a lot of events can accumulate that can clog the connector on restart. The preservestate parameter can be used to avoid this situation. This parameter is enabled (true) by default. Setting preservestate to disabled (false) in the agent.properties file allows the connector to skip the old events and start from real time. The agent.properties file is located in the \$ARCSIGHT_HOME\current\user\agent folder. Restart the connector for your change to take effect.

"What do I do when I receive "Connector parameters did not pass the verification with error ..." message?"

You may not have the correct version of jar file. When you download the JDBC driver, the version of the jar file depends on the version of JRE the connector uses. Versions 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar. Versions 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar. Prior versions of the connector that run JRE 1.6 require sqljdbc4.jar.

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 Configuration Guide for Microsoft Audit Collection System DB SmartConnector (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 24.1

Configuration Guide for Microsoft DHCP File SmartConnector

Document Release Date: January 2024

Software Release Date: January 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft DHCP File SmartConnector	4
Product Overview	5
Configuring DHCP	6
Rotating Log Format	6
Auditing Logging	7
Naming of Audit Log Files	7
Enabling Audit Logging for Windows 2012 R2	8
Enabling Audit Logging for Windows 2016	9
Installing the SmartConnector	12
Preparing to Install the SmartConnector	12
Installing the SmartConnector	12
Device Event Mapping to ArcSight Fields	14
Microsoft DHCP IPv4 Event Mappings to ArcSight ESM Fields	14
Microsoft DHCP IPv6 Event Mappings to ArcSight ESM Fields	15
Event IDs for IPv4	15
Event IDs for IPv6	17
Troubleshooting	19
Send Documentation Feedback	20

Configuration Guide for Microsoft DHCP File SmartConnector

This guide provides information for installing and configuring the SmartConnector for Microsoft DHCP File for log file event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

The Dynamic Host Configuration Protocol (DHCP) is an Internet Engineering Task Force (IETF) standard designed to reduce the administration burden and complexity of configuring hosts on a TCP/IP-based network. When you deploy DHCP servers on your network, you can provide client computers and other TCP/IP-based network devices with valid IP addresses automatically. You also can provide the additional configuration parameters these clients and devices need (DHCP options) that let them connect to other network resources, such as DNS servers, WINS servers, and routers.

Configuring DHCP

You must have read/write access to the DHCP folder to read the DHCP files. If the connector is running as a service, then the SYSTEM user must have read/write access to the DHCP folder.



Note: You must restart the connector after you have completed the configuration, so that the connector can start processing events.

Rotating Log Format

The rotating log format used by the new multiple-instance is different from the previous single-instance connector. The new time-based format is based upon that of the Java 1.6 `SimpleDateFormat`. For more information, see <http://java.sun.com/javase/6/docs/api/java/text/SimpleDateFormat.html>. Some examples:

Log Format	Rotating Logs
/var/log/'MMddyyyy'.log	/var/log/07082009.log
	/var/log/07092009
	/var/log/07102009
/var/log/'yyyy/MMdd'/access.log	/var/log/2009/0708/access.log
	/var/log/2009/0709/access.log
	/var/log/2009/0710/access.log
/var/log/'yyyy/MMdd'/access-'HHmm'.log	/var/log/2009/0708/access-0900.log
	/var/log/2009/0708/access-1000.log
	/var/log/2009/0708/access-1100.log

The log format can also be specified for index-based rotating logs. Here are some examples:

Log Format	Rotating Logs
/var/log/access.'%02d.01,99'.log	/var/log/access.01.log
	/var/log/access.02.log

Log Format	Rotating Logs
	/var/log/access.03.log

Auditing Logging

The following can be specified for DHCP servers running Windows Server 2012 R2, 2016 and 2019:

- The directory path in which the DHCP server stores audit log files. DHCP audit logs are located by default at %windir%\System32\dhcp.
- A maximum size restriction (in megabytes) for the total amount of disk space available for all audit log files created and stored by the DHCP service.
- An interval for disk checking that is used to determine how many times the DHCP server writes audit log events to the log file before checking for available disk space on the server.
- A minimum size requirement (in megabytes) for server disk space used during disk checking to determine whether sufficient space exists for the server to continue audit logging.



Notes:

- The user the connector is running as requires read/write access to the DHCP folder to read the DHCP files. If the connector is running as a service, the SYSTEM user requires read/write access to the DHCP folder.
- You can selectively enable or disable the audit logging feature at each DHCP server. For more information, see "Enabling Audit Logging."
- Only the directory path in which the DHCP server stores audit log files can be modified using the DHCP console. To do so, first select the applicable DHCP server in the console tree. On the **Action** menu, click **Properties**. Next, click the **Advanced** tab and edit **Audit log file path** as necessary. Other audit logging parameters are adjusted through registry-based configuration changes.

Naming of Audit Log Files

The audit logging behavior discussed in this section applies only to Windows Server 2012 R2, 2016 and 2019 DHCP. In Windows NT and Windows 2000, the file name format differed.

The DHCP server bases the name of the audit log file on the current day of the week, as determined by checking the current date and time at the server. For example, when the DHCP server starts, if the current date and time are the following:

Monday, April 7, 2003, 04:56:42 P.M.

The server audit log file is named:

DhcpSrvLog-Mon.Log

When a DHCP server starts or a new day begins (when the local time on the computer is 12:00 A.M.), the server writes a header message in the audit log file, indicating that logging has started. Then, depending upon whether the audit log file is a new or existing file, the following actions occur:

- If the file already existed without modification for more than a day, it is overwritten.
- If the file already existed but was modified within the previous 24 hours, the file is not overwritten. Instead, new logging activity is appended to the end of the existing file.

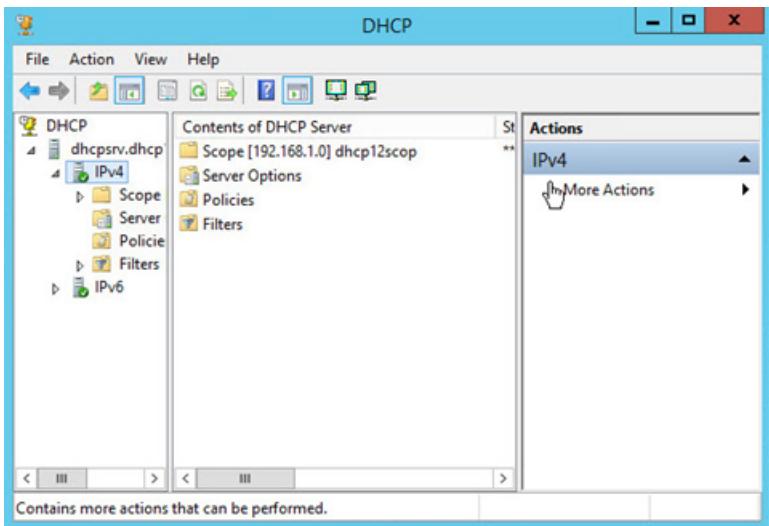
After audit logging starts, the DHCP server performs disk checks at regular intervals, to ensure both the ongoing availability of server disk space and that the current audit log file does not become too large or grow too quickly.

At 12:00 A.M. local time on the server computer, the DHCP server closes the existing log and moves to the log file for the next day of the week. For example, if the day of the week changes at 12:00 A.M. from Wednesday to Thursday, the log file named DhcpSrvLog-Wed.Log is closed and the file named DhcpSrvLog-Thu.Log is opened and used for logging events.

Enabling Audit Logging for Windows 2012 R2

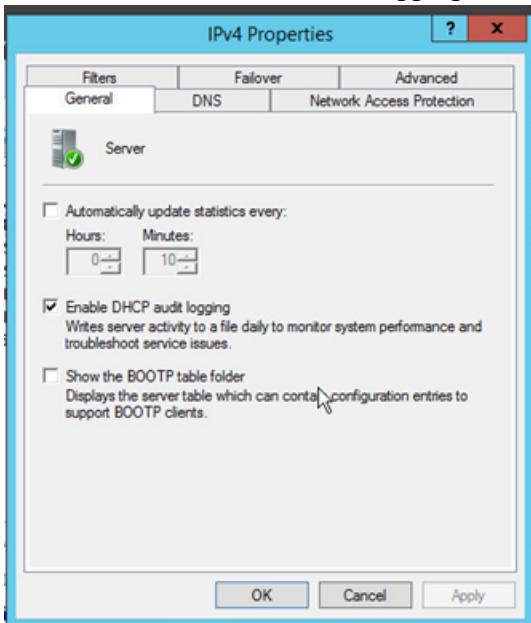
To configure DHCP for event collection:

- 1 Go to **Start > Administrative Tools > DHCP**.
- 2 Expand the applicable DHCP server tree, and then expand **IPv4** or **IPv6**.



3 Right-click on **IPv4** or **IPv6** and select **Properties**.

4 Check **Enable DHCP audit logging** on the **General** tab.



5 Click **OK**.

Enabling Audit Logging for Windows 2016

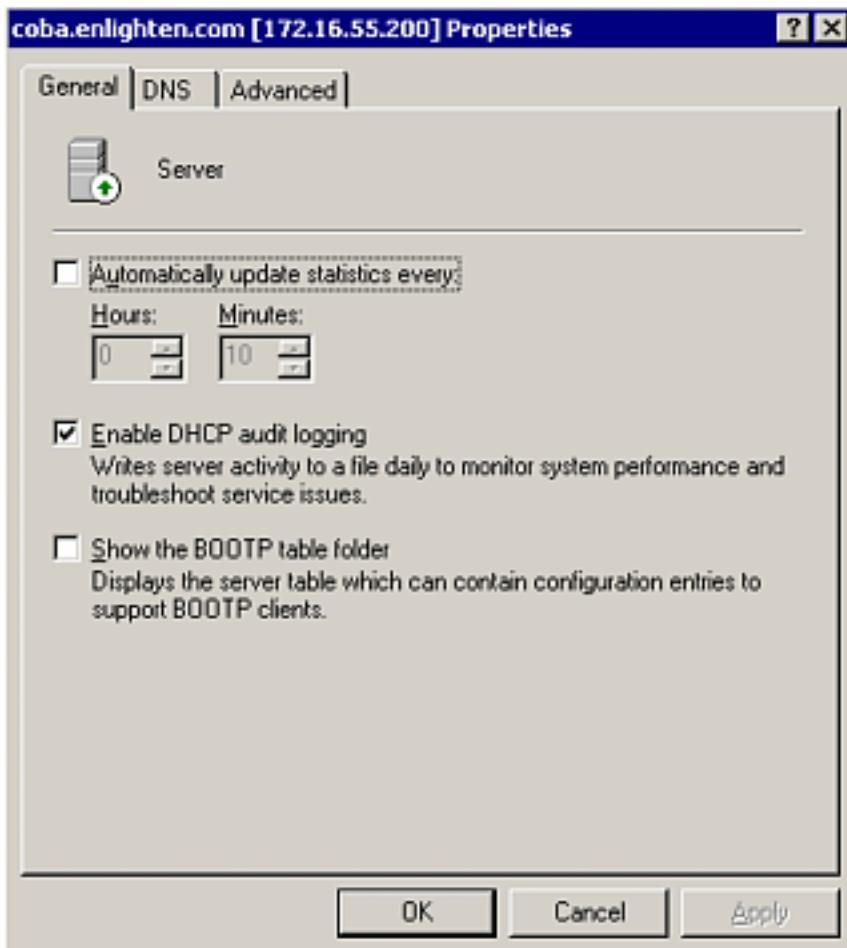
To configure DHCP for event collection:

1 Launch DHCP configuration.

2 Right click on the domain name; select **Properties**.

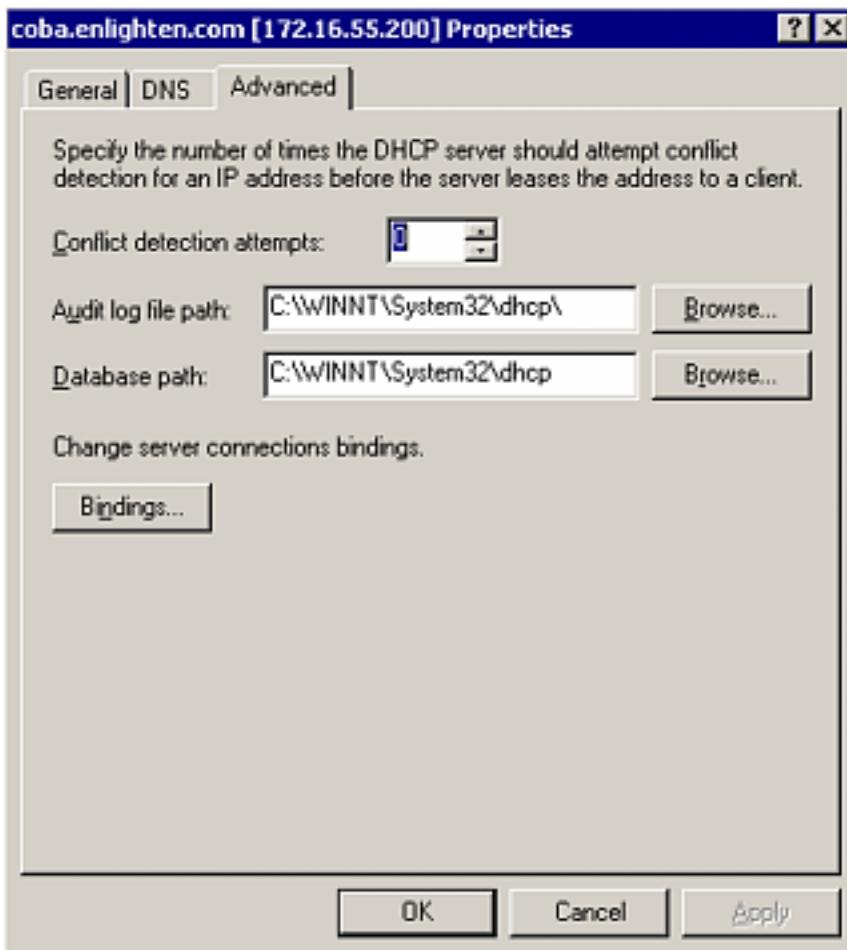
3 From the Properties window, General tab, select **Enable DHCP audit logging**.

Configuring DHCP



4 Click the **Advanced** tab.

Configuring DHCP

**5** Change or accept the default audit log path.

You will find a rotating scheme of files following each day of the week; for example:

DhcpSrvLog.Mon.Log
DhcpSrvLog.Tue.Log
DhcpSrvLog.Wed.Log
DhcpSrvLog.Thu.Log
DhcpSrvLog.Fri.Log
DhcpSrvLog.Sat.Log
DhcpSrvLog.Sun.Log

For IPv6, the file names contain V6; for example: DhcpV6SrvLog.Mon.Log

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.



Note: Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing the SmartConnector

The installation steps described in this section are specific to the Microsoft DHCP File SmartConnector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the Microsoft DHCP File SmartConnector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. From the **Type** drop-down list, select **Microsoft DHCP File** as the type of connector, then click **Next**.
5. Enter the following parameters to configure the SmartConnector and then click **Next**.

Parameter	Description
Log File	<p>Enter the parameters for each DHCP server log file to be read by the connector.</p> <p>When you click Add, the default value populated for each of the DHCP server log files is 'C:\WINNT\System32\DHCP\dhcpSrvLog-'EEE'.log'.</p> <p>Edit the default value for each of the log files.</p> <p> Note: When you edit the default value, ensure that 'EEE' is present in the file name because it is a variable and configures connector to read newly generated files.</p> <p>If IPv6 is used, add v6 to the log file name. For example, 'C:\WINDOWS\System32\DHCP\dhcpV6SrvLog-'EEE'.log'. V6 is case-insensitive.</p>

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.

	Note: If you select Do not import the certificate to connector from destination, the connector installation will end.
---	--

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Microsoft DHCP IPv4 Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	high = 50..99; medium = 14, 18, 31, 33, 34, 35, 36; low = 00, 01, 02, 10, 11, 12, 13, 15, 16, 17, 20, 21, 22, 23, 24, 25, 30, 32
Device Custom Number 1	leases expired
Device Custom Number 2	leases deleted
Device Custom Number 3	QResult (Windows 2008)
Device Custom String 1	Probation Time (Windows 2008)
Device Custom String 2	Correlation ID (Windows 2008)
Device Custom String 3	DHCID (Windows 2008)
Device Custom String 4	MAC Vendor Prefix
Device Custom String 5	Ethernet Vendor
Device Custom String 6	Relay Agent Information
Device Event Class Id	ID
Device Product	'DHCP Server'
Device Receipt Time	Date, Time
Device Severity	ID
Device Vendor	'Microsoft'
Device Version	2012/2016 depend on format of log
External ID	Transaction ID (Windows 2008)
Name	Description
Source Address	IP_Address
Source Host Name	Host_Name
Source Mac Address	MAC_Address
Source User Name	UserName (Windows 2008)

Microsoft DHCP IPv6 Event Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	high = 11023, 11025, 11028, 11029; medium = 11005, 11006, 11007, 11014, 11016; low = 11000, 11001, 11002, 11003, 11004, 11008, 11009, 11010, 11011, 11012, 11013, 11015, 11017, 11018, 11019, 11020, 11021, 11024, 11022, 11030, 11031, 11032
Device Custom IPv6 Address 1	Subnet_Prefix
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom Number 1	leases expired
Device Custom Number 2	leases deleted
Device Custom Number 3	Duid Length
Device Custom String 1	Error Code
Device Custom String 2	Duid Bytes(Hex)
Device Custom String 3	Dhcid
Device Event Class ID	ID
Device Product	'DHCP Server'
Device Receipt Time	Create Time Stamp (Date, Time)
Device Severity	ID
Device Vendor	'Microsoft'
Device Version	2012/2016 depend on format of log
Name	Description
Source Host Name	Host_Name
Source User Name	User_Name

Event IDs for IPv4

ArcSight ESM Field	Device-Specific Field
00	The log was started.
01	The log was stopped.
02	The log was temporarily paused due to low disk space.

Configuration Guide for Microsoft DHCP File SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
10	A new IP address was leased to a client.
11	A lease was renewed by a client.
12	A lease was released by a client.
13	An IP address was found to be in use on the network.
14	A lease request could not be satisfied because the scope's address pool was exhausted.
15	A lease was denied.
16	A lease was deleted.
17	A lease was expired.
18	A lease was expired and DNS records were deleted (Windows 2008).
20	A BOOTP address was leased to a client.
21	A dynamic BOOTP address was leased to a client.
22	A BOOTP request could not be satisfied because the scope's address pool for BOOTP was exhausted.
23	A BOOTP IP address was deleted after checking to see it was not in use.
24	IP address cleanup operation has begun.
25	IP address cleanup statistics.
30	DNS update request to the named DNS server.
31	DNS update failed.
32	DNS update successful.
33	Packet dropped due to NAP policy (Windows 2008).
34	DNS update request failed as the DNS update request queue limit exceeded. (Windows 2012 R2)
35	DNS update request failed. (Windows 2012 R2)
36	Packet dropped because the server is in failover standby role or the hash of the client ID does not match. (Windows 2012 R2)
50	Unreachable domain.
51	Authorization succeeded.
52	Upgraded to a Windows Server 2008 operating system.
53	Cached authorization.
54	Authorization failed. When this event occurs it is likely followed by the server being stopped.

Configuration Guide for Microsoft DHCP File SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
55	Authorization (servicing).
56	Authorization failure. Stopped servicing. You must first authorize the server in the directory before starting it again.
57	Server found in domain. Another DHCP server exists and is authorized for service in the same domain.
58	Server could not find domain.
59	Network failure. A network-related failure prevented the server from determining if it is authorized.
60	No DC is DS Enabled.
61	Another DHCP server was found on the network that belongs to the Active Directory domain.
62	Another DHCP server was found on the network.
63	Restarting rogue detection.
64	No DHCP enabled interfaces.
Event ID	Meaning

Event IDs for IPv6

ArcSight ESM Field	Device-Specific Field
11000	Solicit.
11001	Advertise.
11002	Request.
11003	Confirm.
11004	Renew.
11005	Rebind.
11006	Decline.
11007	Release.
11008	Information Request.
11009	Scope Full.
11010	Started.
11011	Stopped.
11012	Audit Log Paused.

Configuration Guide for Microsoft DHCP File SmartConnector
 Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
11013	DHCP Log File.
11014	Bad address.
11015	Address is already in use.
11016	Client deleted.
11017	DNS record not deleted.
11018	Expired.
11019	Expired and deleted count.
11020	Database cleanup begin.
11021	Database cleanup end.
11022	DNS IPv6 Update Request.
11023	Service not authorized in AD.
11024	Service authorized in AD.
11025	Service has not determined if it authorized in AD.
11028	DNS IPv6 update request failed as the DNS update request queue limit exceeded. (Windows 2012 R2)
11029	DNS IPv6 update request failed. (Windows 2012 R2)
11030	DHCPv6 stateless client records purged. (Windows 2012 R2)
11031	DHCPv6 stateless client record is purged as the purge interval has expired for this client record. (Windows 2012 R2)
11032	DHCPv6 Information Request from IPv6 Stateless Client. (Windows 2012 R2)
Event ID	Meaning

Troubleshooting

What do I do if I receive a 'File Not Found' Exception?

When the connector is collecting events from a Microsoft Windows 2008, or 2012 R2 64-bit machine, an exception such as the following may occur:

```
java.io.FileNotFoundException: C:\Windows\System32\dhcp\dhcpSrvLog-XXX.log
```

Windows 64-bit systems redirect file access from System32 to SysWOW64 for 32-bit applications. DHCP Server is a 64-bit application that still writes the log to the System32/dhcp folder; therefore, the SmartConnector cannot locate the log file. To work around this problem, redirection must occur on the connector side by configuring the log folder on the DHCP connector as:

```
C:\Windows\Sysnative\dhcp\dhcpSrvLog-XXX.log  
please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receivee events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.
```

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 Configuration Guide for Microsoft DHCP File SmartConnector (SmartConnectors 24.1)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector	4
Product Overview	5
Supported Version	5
Configuration	6
Using Server Debug Logging Options	6
Installing the SmartConnector	9
Preparing to Install the SmartConnector	9
Installing the SmartConnector	9
Map Files	10
Device Event Mapping to ArcSight Fields	12
Microsoft DNS DGA Trace Log Multiple Server File Mappings to ArcSight ESM Fields	12
Send Documentation Feedback	14

Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector

This guide provides information for installing the SmartConnector for Microsoft DNS DGA Trace Log Multiple Server File and configuring the device for event collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

The Domain Name System (DNS) is a hierarchical distributed database and an associated set of protocols that define a:

- Mechanism for querying and updating the database
- Mechanism for replicating the information in the database among servers
- Schema of the database

With DNS, the host names reside in a database that can be distributed among multiple servers, decreasing the load on any one server and providing the ability to administer this naming system on a per-partition basis. DNS supports hierarchical names and allows registration of various data types in addition to host name to IP address mapping used in HOSTS files.

This ArcSight SmartConnector lets you import events generated by the Microsoft DNS Trace Log Multiple Server File device into the ArcSight System . See the section "Device Event Mapping to ArcSight Data Fields" later in this document for the specific events mapped to fields in the ArcSight database.

The new feature enables users to apply a Domain Generation Algorithm (DGA) and:

- Whitelist filters on real time
- Filter and drop events prior a license check
- Use the Connector immediately after installation. Required files are pre-configured.
- Populate a dga_whitelist.txt locally or remotely (via ArcMC) to avoid getting events from trusted domains
- Add Map files to /user/agent/map/ to extend connector functionalities

See the section "Map Files" later in this document for more information.

Supported Version

Microsoft's Domain Name Service (DNS) included with Microsoft Windows 2008, Microsoft Windows 2012, Microsoft Windows 2016 and Microsoft Windows 2012 R2 are supported.

Configuration

For information about DNS Monitoring, see [http://technet.microsoft.com/en-us/library/cc783975\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc783975(WS.10).aspx).

The primary tool used to manage DNS servers is the DNS console, which can be found in the **Administrative Tools** folder in the **Start** menu's **Programs** folder.

DNS server event messages are separated and kept in their own system event log, the DNS server log. The DNS server log contains events logged by the DNS server service. Most critical DNS server service events are logged here, such as when the server starts but cannot locate initializing data.

You can change the event types logged by DNS servers using the DNS console. You can also use the DNS console to selectively enable additional debug logging options for temporary trace logging to a text-based file of DNS server activity.

Using Server Debug Logging Options

By default, all debug logging options are disabled. When selectively enabled, the DNS Server service can perform additional trace-level logging of selected types of events or messages for general troubleshooting and debugging of the server. `Dns.log` contains debug logging activity. By default, it is located in the `windir\System32\DNS` folder.

The following DNS debug logging options are available:

Packet Direction

- *Outgoing*
Packets sent by the DNS server are logged in the DNS server log file.
- *Incoming*
Packets received by the DNS server are logged in the log file.

Packet Content

- *Queries/Transfers*
Specifies that packets containing standard queries (per RFC 1034) are logged in the DNS server log file.
- *Updates*
Specifies that packets containing dynamic updates (per RFC 2136) are logged in the DNS server log file.

- *Notifications*

Specifies that packets containing notifications (per RFC 1996) are logged in the DNS server log file.

Transport Protocol

- *UDP*

Specifies that packets sent and received over UDP are logged in the DNS server log file.

- *TCP*

Specifies that packets sent and received over TCP are logged in the DNS server log file.

Packet Type

- *Request*

Specifies that request packets are logged in the DNS server log file (a request packet is characterized by a QR bit set to 0 in the DNS message header).

- *Response*

Specifies that response packets are logged in the DNS server log file (a response packet is characterized by a QR bit set to 1 in the DNS message header).

Other Options

- *Filter packets by IP address*

Provides additional filtering of packets logged in the DNS server log file.

- *Details*

Specifies that all event details be logged in the DNS server log file.

Log File

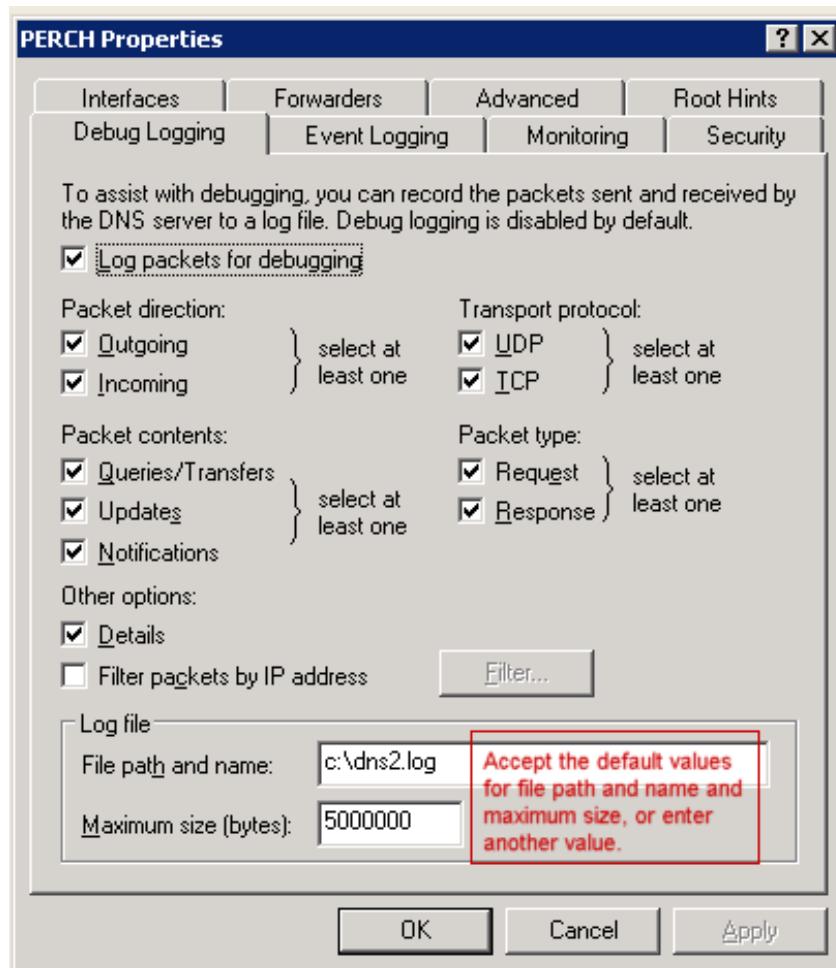
File path and name

Allows you to specify the name and location of the DNS server log file. *Log file maximum size limit* enables you to set the maximum file size for the DNS server log file.

To select and enable debug logging options on the DNS server:

1. To open DNS, go to **Control Panel > System and Security > Administrative Tools**, then double-click **DNS**.
2. In the console tree, right-click the applicable DNS server, then click **Properties**.
3. Click the **Debug Logging** tab.
4. To set the debug logging options, first select **Log packets for debugging**. To ensure collecting the appropriate information for processing by ArcSight, select the options

shown in the following figure:



5. In addition to selecting events for the DNS debug log file, select the default values or specify the file name, location, and maximum file size for the file.

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.



Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing the SmartConnector

The installation steps described in this section are specific to the Microsoft DNS DGA Trace Log Multiple Server File SmartConnector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the SmartConnector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. From the **Type** drop-down list, select **Microsoft DNS DGA Trace Log Multiple Server File** as the type of connector, then click **Next**.

5. Enter the following device details to configure the SmartConnector and then click **Next**.

Parameter	Description
Folder	The absolute path to the location of the log files. - For Windows platform, use: 'c:\Program Files\DNS_Multi_File\logs\' - For Linux platform, use: '/var/log/dnsmultifile/' For multiple servers, click Add and enter information about the additional server. - For Windows platform, use: '\\<servername>\folder\folder.'
Wildcard	The log file name ('*.log') has two parts: - Part 1: ('*') is the file name - Part 2: ('.log') is the file type For example: 'dnsmulti.log'
Log File Type	Accept the default "tracelog".

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

Map Files

By adding map files, users can increment the functionalities of the Connector.

Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector

Installing the SmartConnector

File	Description	Sample Content
dga_whitelist.txt	White list file. Includes all domains that are not scanned by the DGA detection.	google.com youtube.com facebook.com baidu.com wikipedia.org yahoo.com reddit.com google.co.in qq.com taobao.com amazon.com twitter.com
map.2.properties	Numbered connector map file. It calls the _domainWhitelist operation. This operation is a lookup for whitelisted domains in each event and marks them as WHITELISTED, so they can be dropped by the filter later.	!Flags,Overwrite+set.expr (destinationHostName).event.deviceCustomFloatingPoint2Label __domainWhitelist(destinationHostName)
map.3.properties	Numbered connector map file. It calls the dgaForbiddenTrigrams operation. This operation applies the forbiddenTrigrams DGA classifier in every event and returns 1 or 0 for each.	!Flags,Overwrite+set.expr (destinationHostName).event.deviceCustomNumber1_dgaForbiddenTrigrams(destinationHostName)
map.4.properties	Numbered connector map file. It calls the ForbiddenTrigramsHelper operation. This is a helper function that adds a label to the dga field in CEF.	!Flags,Overwrite+set.expr (deviceCustomNumber1).event.deviceCustomNumber1Label__dgaForbiddenTrigramsHelper (deviceCustomNumber1)
map.5.properties	Numbered connector map file. It sets the event.dropEventFlag based on the value of event.deviceCustomFloatingPoint2Label. It is set to "true" when the value of event.deviceCustomFloatingPoint2Label is WHITELISTED.	event.deviceCustomFloatingPoint2Label,set.event.dropEventFlag, WHITELISTED,true



Note:

- Adjust the sequence numbers of your new map files based on any existing map files. For example, if the last map file in the connector is number 3, the new DGA map file must be set to 4 and so on.
- The domains are whitelisted based on the top-level domain. The domains that do not follow the Internet Assigned Numbers Authority (IANA) standard will not be processed.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Microsoft DNS DGA Trace Log Multiple Server File Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 2, 3, 5, 16, SERVFAIL, NXDOMAIN, REFUSED, BADVERS, BADSIG; Medium = 1, 4, 6-10, 17-22, Error, Warning, FORMERR, NOTIMP, YXDOMAIN, YXRRSET, NXRRSET, NOTAUTH, NOTZONE, BADKEY, BADTIME, BADMODE, BADNAME, BADALG, BADTRUNC; Low = 0, 11-15, 23-65535, Information, Success, NOERROR (based on Rcode values at: http://www.networksorcery.com/enp/protocol/dns.htm#Rcode , Return code)
Application Protocol	application protocol
Bytes In	Size, incoming bytes
Destination Address	destination address
Destination DNS Domain	destination DNS domain
Destination Host Name	destination host name
Destination NT Domain	destination NT domain
Device Action	Action taken by the device
Device Custom Floating Point 2 Label	WHITELISTED
Device Custom IPv6 Address 2	Source IPv6 address
Device Custom Number 1	0 or 1
Device Custom Number 1 Label	DNS-Analytics
Device Custom String 1	Thread Id
Device Custom String 2	OpCode
Device Custom String 3	Flags (character codes)
Device Custom String 4	Reason or error code
Device Direction	Snd=Outbound, Rcv=Inbound

Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Event Category	Context
Device Event Class ID	Event Name
Device Product	'DNS Trace Log'
Device Receipt Time	DateTime
Device Severity	One of (Information, Warning, Error, Success, NOERROR)
Device Vendor	'Microsoft'
File Name	file name
File Path	file path
Message	Rcode description (based on Rcode descriptions at: http://www.networksorcery.com/enp/protocol/dns.htm#Rcode , Return code)
Name	Rcode name (based on Rcode name at: http://www.networksorcery.com/enp/protocol/dns.htm#Rcode , Return code)
Request URL	Question Name
Source Address	Source network address
Source DNS Domain	sourceDNSDomain
Source Host Name	Source host name
Source Port	Source port
Source Service Name	sourceServiceName
Start Time	startTime
Transport Protocol	transport protocol (UDP)

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

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 Configuration Guide for Microsoft DNS DGA Trace Log Multiple Server File SmartConnector (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Microsoft DNS Trace Log Multiple Server File SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft DNS Trace Log Multiple Server File SmartConnector	4
Product Overview	5
Configuration	6
Using Server Debug Logging Options	6
Install the SmartConnector	9
Prepare to Install Connector	9
Install Core Software	9
Set Global Parameters (optional)	10
Select Connector and Add Parameter Information	11
Select a Destination	12
Complete Installation and Configuration	12
Run the SmartConnector	13
Device Event Mapping to ArcSight Fields	14
Microsoft DNS Trace Log Multiple Server File Mappings to ArcSight ESM Fields	14
Send Documentation Feedback	16

Configuration Guide for Microsoft DNS Trace Log Multiple Server File SmartConnector

This guide provides information for installing the SmartConnector for Microsoft DNS Trace Log Multiple Server File and configuring the device for event collection. For supported devices and versions, see [Technical Requirements](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

The Domain Name System (DNS) is a hierarchical distributed database and an associated set of protocols that define a:

- Mechanism for querying and updating the database
- Mechanism for replicating the information in the database among servers
- Schema of the database

With DNS, the host names reside in a database that can be distributed among multiple servers, decreasing the load on any one server and providing the ability to administer this naming system on a per-partition basis. DNS supports hierarchical names and allows registration of various data types in addition to host name to IP address mapping used in HOSTS files.

This ArcSight SmartConnector lets you import events generated by the Microsoft DNS Trace Log Multiple Server File device into the ArcSight System. See the section "Device Event Mapping to ArcSight Data Fields" later in this document for the specific events mapped to fields in the ArcSight database.

Configuration

Detailed information regarding DNS Monitoring can be found at:
[http://technet.microsoft.com/en-us/library/cc783975\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc783975(WS.10).aspx).

The primary tool used to manage DNS servers is the DNS console, which can be found in the **Administrative Tools** folder in the **Start** menu's **Programs** folder.

DNS server event messages are separated and kept in their own system event log, the DNS server log. The DNS server log contains events logged by the DNS server service. Most critical DNS server service events are logged here, such as when the server starts but cannot locate initializing data.

You can change the event types logged by DNS servers using the DNS console. You also can use the DNS console to selectively enable additional debug logging options for temporary trace logging to a text-based file of DNS server activity.

Using Server Debug Logging Options

By default, all debug logging options are disabled. When selectively enabled, the DNS Server service can perform additional trace-level logging of selected types of events or messages for general troubleshooting and debugging of the server. Dns.log contains debug logging activity. By default, it is located in the `windir\System32\DNS` folder.

The following DNS debug logging options are available:

Packet Direction

Outgoing

Packets sent by the DNS server are logged in the DNS server log file.

Incoming

Packets received by the DNS server are logged in the log file.

Packet Content

Queries/Transfers

Specifies that packets containing standard queries (per RFC 1034) are logged in the DNS server log file.

Updates

Specifies that packets containing dynamic updates (per RFC 2136) are logged in the DNS server log file.

Notifications

Specifies that packets containing notifications (per RFC 1996) are logged in the DNS server log file.

Transport Protocol

UDP

Specifies that packets sent and received over UDP are logged in the DNS server log file.

TCP

Specifies that packets sent and received over TCP are logged in the DNS server log file.

Packet Type

Request

Specifies that request packets are logged in the DNS server log file (a request packet is characterized by a QR bit set to 0 in the DNS message header).

Response

Specifies that response packets are logged in the DNS server log file (a response packet is characterized by a QR bit set to 1 in the DNS message header).

Other Options

Filter packets by IP address

Provides additional filtering of packets logged in the DNS server log file.

Details

Specifies that all event details be logged in the DNS server log file.

Log File

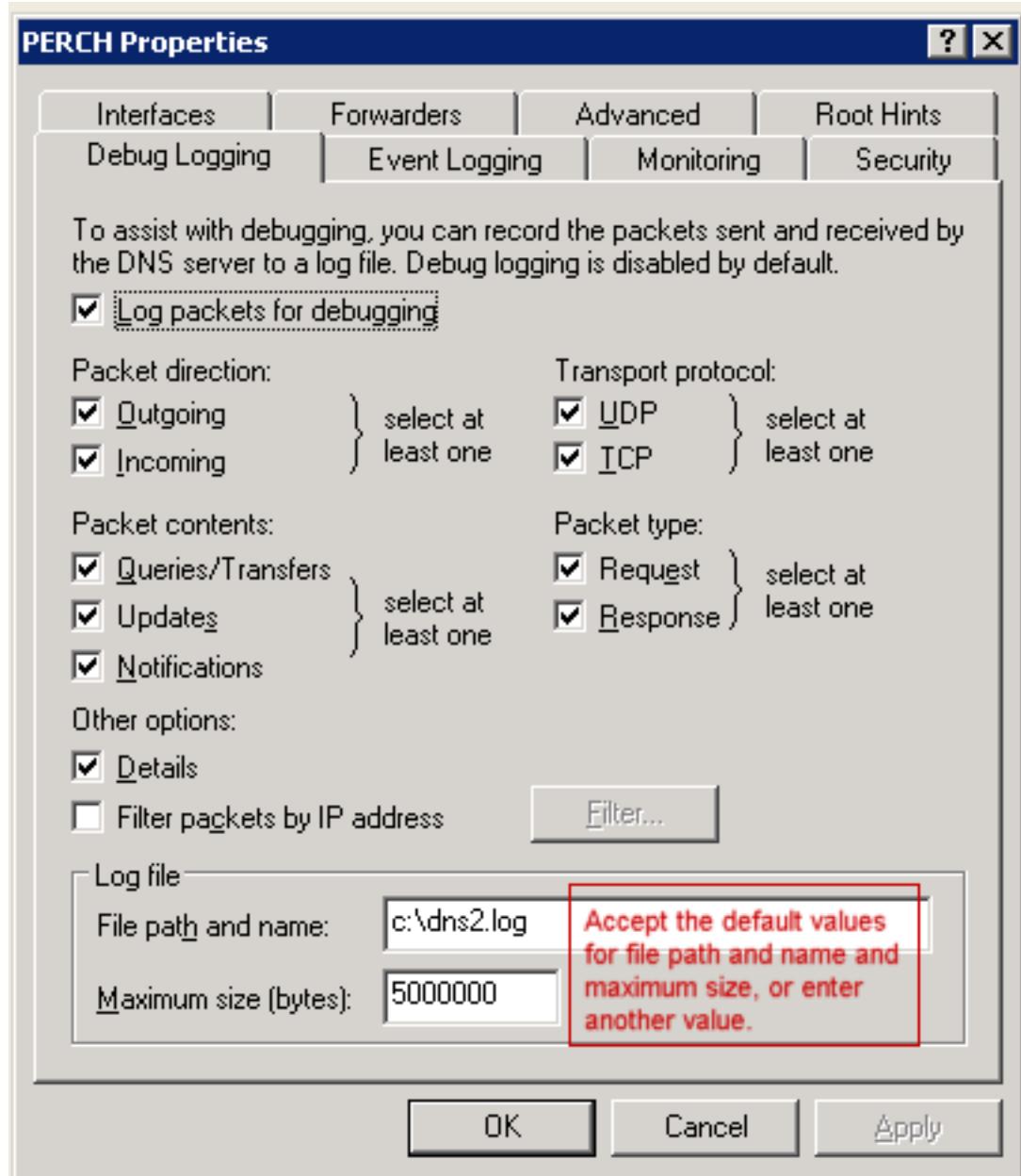
File path and name lets you specify the name and location of the DNS server log file.

Log file maximum size limit lets you set the maximum file size for the DNS server log file.

To select and enable debug logging options on the DNS server:

- 1 Open DNS. (Click **Start** -> **Control Panel** -> **Administrative Tools**. Double-click **DNS**.)
- 2 In the console tree, right-click the applicable DNS server, then click **Properties**.
- 3 Click the **Debug Logging** tab.

- 4 To set the debug logging options, first select **Log packets for debugging**. To ensure collecting the appropriate information for processing by ArcSight, select the options shown in the following figure.



In addition to selecting events for the DNS debug log file, select the default values or specify the file name, location, and maximum file size for the file.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.



Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the OpenText SSO site.

- 1 Download the SmartConnector executable for your operating system from the OpenText SSO site.
- 2 Start the SmartConnector installation and configuration wizard by running the executable.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

Introduction

Choose Install Folder

Choose Shortcut Folder

Pre-Installation Summary

Installing...

3 When the installation of SmartConnector core component software is finished, the following window is displayed:

Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using OpenText SecureData solutions to provide encryption. See the *OpenText SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the OpenText SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.

Configuration Guide for Microsoft DNS Trace Log Multiple Server File SmartConnector

Install the SmartConnector

Parameter	Setting
Format Preserving Identity	The OpenText SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for OpenText SecureData.
Format Preserving Secret	Enter the secret configured for OpenText SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

- 1 Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
- 2 Select **Microsoft DNS Trace Log Multiple Server File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Folder	<p>The absolute path to the location of the log files.</p> <p>- For Windows platform, use: 'c:\Program Files\DNS_Multi_File\logs\'</p> <p>- For Linux platform, use: '/var/log/dnsmultifile/'</p> <p>For multiple servers, click Add and enter information about the additional server.</p> <p>- For Windows platform, use: '\\<servername>\folder\folder.'</p>
Wildcard	<p>The log file name ('*.log') has two parts:</p> <p>- Part 1: ('*') is the file name</p> <p>- Part 2: ('.log') is the file type</p> <p>- For example: 'dnsmulti.log'</p>
Log File Type	Accept the default "tracelog".

Select a Destination

- 1** The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.
- 2** Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.
- 3** Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
- 4** If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

- 1** Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.
- 2** The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.
- 3** If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.
- 4** Click **Next** on the summary window.
- 5** To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to \$ARCSIGHT_HOME\current\bin and run: `arcsight connectors`

To view the SmartConnector log, read the file \$ARCSIGHT_HOME\current\logs\agent.log; to stop all SmartConnectors, enter `Ctrl+C` in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Microsoft DNS Trace Log Multiple Server File Mappings to ArcSight ESM Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 2, 3, 5, 16, SERVFAIL, NXDOMAIN, REFUSED, BADVERS, BADSIG; Medium = 1, 4, 6-10, 17-22, Error, Warning, FORMERR, NOTIMP, YXDOMAIN, YXRRSET, NXRRSET, NOTAUTH, NOTZONE, BADKEY, BADTIME, BADMODE, BADNAME, BADALG, BADTRUNC; Low = 0, 11-15, 23-65535, Information, Success, NOERROR (based on Rcode values at: http://www.networksorcery.com/enp/protocol/dns.htm#Rcode , Return code)
Application Protocol	application protocol
Bytes In	Size, incoming bytes
Destination Address	destination address
Destination DNS Domain	destination DNS domain
Destination Host Name	destination host name
Destination NT Domain	destination NT domain
Device Action	Action taken by the device
Device Custom IPv6 Address 2	Source IPv6 address
Device Custom Number 2	TTL
Device Custom String 1	Thread Id
Device Custom String 2	OpCode
Device Custom String 3	Flags (character codes)
Device Custom String 4	Reason or error code
Device Direction	Snd=Outbound, Rcv=Inbound
Device Event Category	Context
Device Event Class ID	Event Name (For events which have Device Event Category as "PACKET" the DECID has been appended OPCODE with Rcode value.)

Configuration Guide for Microsoft DNS Trace Log Multiple Server File SmartConnector
 Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Product	'DNS Trace Log'
Device Receipt Time	DateTime
Device Severity	One of (Information, Warning, Error, Success, NOERROR)
Device Vendor	'Microsoft'
File Name	file name
File Path	file path
Message	Rcode description (based on Rcode descriptions at: http://www.networksorcery.com/enp/protocol/dns.htm#Rcode , Return code)
Name	Rcode name (based on Rcode name at: http://www.networksorcery.com/enp/protocol/dns.htm#Rcode , Return code)
Request URL	Question Name
Source Address	Source network address
Source DNS Domain	sourceDNSDomain
Source Host Name	Source host name
Source Port	Source port
Source Service Name	sourceServiceName
Start Time	startTime
Transport Protocol	transport protocol (UDP)

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

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 Configuration Guide for Microsoft DNS Trace Log Multiple Server File
SmartConnector (SmartConnectors 8.4.3)**

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: CE 24.4.1

Configuration Guide for Microsoft Exchange Message Tracking Log Multiple Server File SmartConnector

Document Release Date: December 2024

Software Release Date: December 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft Exchange Message Tracking Log Multiple Server File SmartConnector	4
Product overview	5
Configuration	6
Enable message tracking for Exchange 2016	6
Enable message tracking for Exchange 2013 SP1 and earlier	6
Configure for internal to external email traffic	7
Creating shared folder to read logs	8
Installing and configuring the SmartConnector	9
Preparing to install the SmartConnector	9
Installing and configuring the SmartConnector	9
Configuring advanced log processing parameters	11
Device event mapping to ArcSight fields	13
Microsoft Exchange message tracking log 2013, 2013 SP1, and 2016 mappings	13
Microsoft Exchange message tracking log 2007 and 2010 mappings	14
Troubleshooting	16
Send Documentation Feedback	18

Configuration Guide for Microsoft Exchange Message Tracking Log Multiple Server File SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Exchange Message Tracking Log Multiple Server File and configuring the device for event collection. For supported devices and versions, see [Technical Requirements](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product overview

Microsoft Exchange Server helps you manage a reliable messaging system with built-in protection against spam and viruses, while providing people throughout your organization with anywhere access to e-mail, voicemail, calendars, and contacts from a wide variety of devices.

Configuration

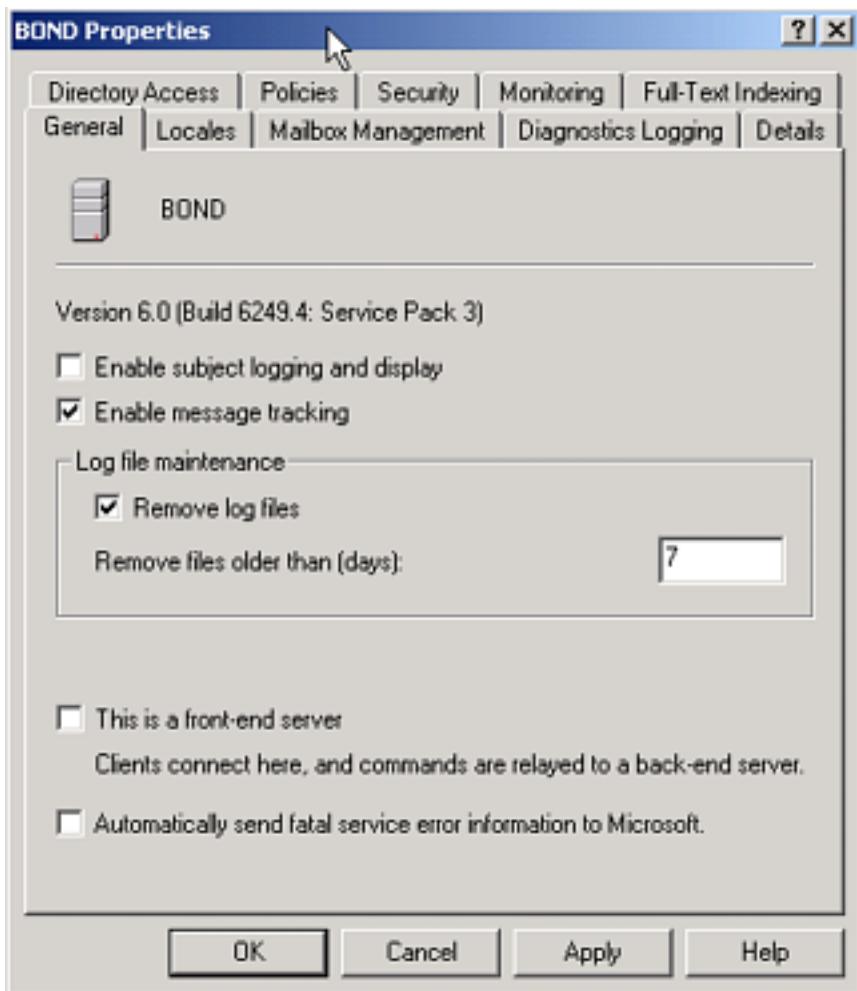
Enable message tracking for Exchange 2016

For information on enabling message tracking in Microsoft Exchange 2016, see:
[https://technet.microsoft.com/en-us/library/aa997984\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/aa997984(v=exchg.160).aspx)

Enable message tracking for Exchange 2013 SP1 and earlier

To enable message tracking:

1. In the **Exchange System Manager**, right-click an Exchange server, then select **Properties**.



2. On the **General** tab, select the **Enable message tracking** check box.



If the **Enable message tracking** check box is unavailable or appears dimmed, there is a server policy object applied to this server. You must either enable message tracking on the policy or remove the server from this policy.

3. In the **Remove files older than (days)** text box, enter the number of days that you want the files to remain on the server before being deleted.

Configure for internal to external email traffic

When the Microsoft Exchange server sends an email, the action initiates numerous internal events that include all the queuing stages between when the message is sent and when it is received. Each of these internal events generates an event class ID, and all these events are sent to the ArcSight Manager by the Exchange Message Tracking Log

SmartConnector. Unless you need to troubleshoot the internal workings of the Exchange server, the only two events that are relevant to security monitoring are the send (outgoing) and receive (incoming) events.

The EventId parameter of the Get-MessageTrackingLog cmdlet can be used to filter the message tracking log entries by the value of the EventId field, which classifies each message event. Include only Send and Receive eventIds.

For more information, see Get-MessageTrackingLog at the following location:
[https://technet.microsoft.com/en-us/library/aa997573\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/aa997573(v=exchg.160).aspx)

Creating shared folder to read logs

Many customers do not prefer to install SmartConnectors on their servers in a production environment.

As a best practice, OpenText recommends that you create a shared folder to periodically dump logs. You can configure SmartConnector with a service/user account that has the required privileges to read the log files from this shared folder.

Installing and configuring the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

Preparing to install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Installing and configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Specify the relevant [Global Parameters](#), when prompted.
4. In the **Type** list, select **Microsoft Exchange Message Tracking Log Multiple Server File**, then click **Next**.
5. In the **Enter the parameter details** page, select the required value for the following parameters, and then click **Next**:

Parameter	Description
Log Folder	<p>Replace the default file path with the path for each of your Exchange servers.</p> <p>For example:</p> <p><SmartConnector_installdir>\Logs</p>  <p>If you have created shared folders, then make sure that this path points to them.</p>
Log File Format	<p>The default value of MSGTRK*LOG lets the connector locate all message logs starting with MSGTRK and ending with .LOG, regardless of the date format used for individual log files. The format uses a wildcard and not a regular expression. This connector does not support regular expressions for file format. Accept this default value, or enter a specific alternative value.</p>

6. Select a [destination and configure parameters](#).
7. Specify a name for the connector.
8. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.

	If you select Do not import the certificate to connector from destination , the connector installation will end.
---	---

9. Select whether you want to install the connector as a service or in the standalone mode.
10. Complete the installation.
11. Optionally, configure advanced parameters in the agent.properties file to make any changes in the default behavior of the connector.
12. [Run the SmartConnector](#).

For more information about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).

Configuring advanced log processing parameters

By default, when you run the Exchange Message Tracking Log Multiple Server File SmartConnector for the first time after installation, it reads and processes all the old and present log files in the shared folder and sends the files to the configured destination. The `preservestate` and `startatend` parameters in the `agent.properties` file are set to false by default and the connector does not bookmark the old logs. As a result, whenever you restart the connector, it will read, process, and send all the old logs to the configured destination again, leading to duplicate log entries.

To bookmark old logs to avoid duplicate log entries:

1. Configure the following advanced parameters with the specified values in the `agent.properties` file, after installing but before running the connector:
 - `agents[0].foldertable[0].mode=RenameFileInTheSameDirectory`
 - `agents[0].foldertable[0].modeoptions=processed`
 - `agents[0].foldertable[0].preservestate=true`
 - `agents[0].foldertable[0].startatend=true`
 - `agents[0].foldertable[0].usenonlockingwindowsfilereader=true`

2. Run the connector.

The connector will start reading the old log files and bookmark them in the `agentdata` folder located at the following path:

`<connector_HOME>\current\user\agent\agentdata`



The time required to bookmark log files depends on the number of files in each exchange server and the `processinglimit` parameter in the `agent.properties` file. You can increase `processinglimit` if you have a large number of files. The default limit is 256.

3. Stop the connector after it bookmarks all the old log files.



If the `startatend` parameter is set to true, then the connector will not read real-time logs.

4. Set the `startatend` parameter to false in the `agent.properties` file:

`agents[0].foldertable[0].startatend=false`

5. Restart the connector.

Now, the connector will ignore the old logs as they have been bookmarked and process only the real-time logs, which will be sent to the configured destination.

Device event mapping to ArcSight fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Microsoft Exchange message tracking log 2013, 2013 SP1, and 2016 mappings

ArcSight ESM Field	Device-Specific Field
Additional data	custom-data
Additional data	message-info
Additional data	network-message-id
Additional data	recipient-status
Additional data	related-recipient-address
Additional data	tenant-id
Additional data	transport-traffic-type
Bytes In	total-bytes (RECEIVE)
Bytes Out	total-bytes (except for RECEIVE)
Destination Address	client-ip
Destination Host Name	client-hostname
Destination User Name	recipient-address
Device Address	server-ip
Device Custom IPv6 Address 1	server-ip (Device IPv6 Address)
Device Custom IPv6 Address 3	client-ip (Destination IPv6 Address)
Device Custom Number 1	recipient-count
Device Custom String 1	internal-message-id
Device Custom String 2	message-id
Device Custom String 3	reference
Device Custom String 4	connector-id

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	source-context
Device Custom String 6	return-path
Device Event Category	source
Device Event Class ID	event-id
Device Host Name	server-hostname
Device Product	"Exchange Server"
Device Receipt Time	date-time, 'GMT'
Device Vendor	'Microsoft'
Flex String 1	directionality
Message	message-subject
Name	event-id
Source Address	original-client-ip
Source Service Name	source
Source User Name	sender-address

Microsoft Exchange message tracking log 2007 and 2010 mappings

ArcSight ESM Field	Device-Specific Field
Additional data	custom-data
Additional data	message-info
Additional data	original-client-ip
Additional data	original-server-ip
Additional data	recipient-status
Additional data	related-recipient-address
Additional data	tenant-id
Bytes In	total-bytes (RECEIVE)
Bytes Out	total-bytes (except for RECEIVE)
Destination User Name	recipient-address

ArcSight ESM Field	Device-Specific Field
Device Address	server-ip
Device Custom IPv6 Address 1	server-ip
Device Custom IPv6 Address 2	client-ip
Device Custom Number 1	recipient-count
Device Custom String 1	internal-message-id
Device Custom String 2	message-id
Device Custom String 3	reference
Device Custom String 4	connector-id
Device Custom String 5	source-context
Device Custom String 6	return-path
Device Event Category	source
Device Event Class ID	event-id
Device Host Name	server-hostname
Device Product	'Exchange Server'
Device Receipt Time	date-time, 'GMT'
Device Vendor	'Microsoft'
Flex String 1	directionality
Message	message-subject
Name	event-id
Source Address	client-ip
Source Host Name	client-hostname
Source Service Name	source
Source User Name	sender-address

Troubleshooting

What do we need to do if the connector is to read logs from a remote machine through network share

You should have a good knowledge of UNC/network share and understand their limitations to make it possible for the Exchange SmartConnector to work from a remote machine.

There are three things to consider:

- 1** Use UNC name for such a share (for example, \computername\sharename) instead of the driver name (such as F:).
- 2** Giving access privilege to the user you use to access such share. (If you run the connector as a Winodws service, use the 'Log on' tab to enter user name and password for the user to which the file share gives access permission.)
- 3** If you have to use a drive letter, call the following code piece in your connector initialization method:

```
Process_process=Runtime.getRuntime().exec("net use I:  
10.0.80.233\ShareTest/user:XXXXX-T40\ShareTest ShareTestPassword");
```

I configured the connector, but it never receives events. What is the problem?

Verify that the user configured to start the connector service has the necessary permissions to view and open the log files you want the connector to read, particularly if the files will be read from a shared folder on another host. Write access is not required.

One or more of the following errors may appear in agent.log.

```
[2007-11-06 15:06:03,486][FATAL]  
[default.com.arcsight.agent.loadable.agent._  
ExchangeTrackingLogFileAgent]  
[mainLoop] com.arcsight.common.InitializationException: Exception  
initializing 'com.arcsight.agent.db.a.o': Log filename pattern must  
be  
[prefix,],
```

When this error is observed, the problem usually lies in the syntax of the rotationschemeparams setting. This parameter is a list of the various parameters used in the naming of the log files. The default for Exchange is yyyyMMdd,.log, based upon the current day and rotated daily. The way to specify these parameters is with a comma:

```
agents[0].rotationschemeparams=yyyyMMdd,.log  
[2007-11-07 13:13:39,111][WARN][default.com.arcsight.agent.db.a.v]  
[startNewThread] Agent Started, but the file[C:\Testing\exch1.log\]  
did not appear yet...will retry after [5] seconds.
```

The second parameter, which is commonly misconfigured, is the `logfilefilename` parameter, which should be populated with the local or full UNC path to the log file folder, but not the filename format:

```
agents[0].logfilefilename=C:\\Testing\\
```

The last key parameters are `rotationscheme` and `followexternalrotation`, which together define the rotation method used by the application to move to the next file. Neither of these are configurable through the standard installation wizard, and these values are not the default values.

```
agents[0].rotationscheme=Daily  
agents[0].followexternalrotation=false
```

To adjust these settings, open `agent.properties` (located under the connector's `/current/user/agent` directory) in a text editor and edit the values. Save the file and restart the connector.

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

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 Configuration Guide for Microsoft Exchange Message Tracking Log Multiple Server File SmartConnector (SmartConnectors CE 24.4.1)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: CE 24.4

Configuration Guide for Microsoft Forefront DB SmartConnector

Document Release Date: October 2024

Software Release Date: October 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft Forefront DB SmartConnector	4
Product overview	5
Prerequisites	6
Configuring logging to a SQL Server database	6
Enabling SQL Server logging in Forefront UAG	6
Downloading the JDBC driver	6
Installing the SmartConnector	8
Preparing to install the SmartConnector	8
Installing and configuring the SmartConnector	9
Adding JDBC Driver to the Connector Appliance/ArcSight Management Center	11
Device event mapping to ArcSight fields	13
Forefront UAG Mappings	13
Troubleshooting	15
Send Documentation Feedback	17

Configuration Guide for Microsoft Forefront DB SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Forefront DB and configuring the device for event collection.

This guide provides a high level overview of ArcSight SmartConnectors. For supported devices and versions, see [Technical Requirements](#).

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product overview

Microsoft Forefront Unified Access Gateway (UAG), is a computer software solution that provides secure remote access to corporate networks for remote employees and business partners. It incorporates remote access technologies such as reverse proxy, virtual private network (VPN), DirectAccess and Remote Desktop Services.

Prerequisites

This section provides instructions for configuring Microsoft Forefront Unified Access Gateway to send events to the ArcSight SmartConnector.

Configuring logging to a SQL Server database

For complete information about configuring logging to both a local and a remote SQL Server database, see "Logging to a SQL Server in the Microsoft Forefront Unified Access Gateway" in the Microsoft TechNet Library:

<http://technet.microsoft.com/en-us/library/dd897065.aspx>

Enabling SQL Server logging in Forefront UAG

To enable SQL Server logging, do the following:

1. Open a command line prompt and navigate to the MonitorMgr folder of the Forefront UAG installation directory. If Forefront UAG is installed in Program Files, the folder is located in the following location: Program Files\Microsoft Forefront Unified Access Gateway\utils\MonitorMgr\.
2. At the command line:
Enter MonitorMgrUtil -setsqllogging 1, to enable SQL Server logging.
Enter MonitorMgrUtil -setsqllogging 0 to disable SQL Server logging.
3. On the toolbar of the Forefront UAG Management console, click the **Activate configuration** icon and then click **Activate**.
4. Restart the Forefront UAG Monitor Manager service.

Downloading the JDBC driver

This section provides information about creating an ODBC data source. The data source configuration is performed on the machine on which you are installing the SmartConnector, and there can be only one data source per SmartConnector. This data source must match the existing configuration of the Microsoft Forefront Unified Access Gateway.

The SmartConnector installation requires JDBC driver to be present. During the installation process, you will be directed to leave the wizard and copy the JDBC driver file you downloaded to a SmartConnector folder.



Note: Different versions of the JDBC driver are required for different SQL Server database versions. The name of the jar file may be different for some JDBC driver versions. Make sure that you use the correct driver for your database version

Refer to the following information to download the correct jar file depending on the JRE version used by the SmartConnector:

- SmartConnector Version 8.3.0 uses JRE 1.8.0_312 and supports jar files from version mssql-jdbc-6.4.0.jre8.jar ([Download Microsoft JDBC Driver 6.4 for SQL Server](#)) to mssql-jdbc-9.4.0.jre8.jar ([Download Microsoft JDBC Driver 9.4.0 for SQL Server](#)).
- SmartConnector Version 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar ([Download Microsoft JDBC Driver 6.0 for SQL Server](#)).
- SmartConnector Version 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar ([Download Microsoft JDBC Driver 6.0 for SQL Server](#)).
- Earlier versions of SmartConnector run JRE 1.6 and require sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server).

For more information related to the Microsoft JDBC driver, see [Microsoft Documentation](#).

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

ArcSight recommends that you do not install database connectors on the database server or any mission critical servers as this might cause performance issues.

Preparing to install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords
- Minimum DB privileges - OpenText recommends the following minimum permissions to access the database:
 - Explicit CONNECT permission
 - Explicit SELECT permission
 - Public role
 - db_datareader_role

For more information about any specific permission, see the documentation of the specific database.

Installing and configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Exit the installation wizard.
4. Copy the jar file associated with the version of the driver that you downloaded earlier to \$ARCSIGHT_HOME/current/user/agent/lib
5. To use JDBC driver with SmartConnectors to connect to Microsoft SQL Servers by using Windows authentication, copy the sqljdbc_auth.dll file from the JDBC driver download to the \$ARCSIGHT_HOME\jre\bin directory.

An example of The JDBC driver download path for SQL JDBC driver is:

- For version 4.0 for 32-bit environment is sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll
- For 64-bit environment, sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll

To use the latest version of SQL JDBC Driver such as 9.4:

- Copy the mssql-jdbc-9.4.0.jre8.jar file associated with the version of the driver that you downloaded earlier to \$ARCSIGHT_HOME/current/user/agent/lib
- Copy the mssql-jdbc_auth-9.4.0.x64.dll file from the JDBC driver download to the \$ARCSIGHT_HOME\jre\bin directory.



Note: If you are upgrading the SmartConnector, you must copy the authentication file to \$ARCSIGHT_HOME\jre\bin again after update, as the upgrade process overwrites the \$ARCSIGHT_HOME\jre\bin directory.

6. Copy certificate and JDBC files to SmartConnector folders as follows:

- Copy the jssecacerts certificate that you installed during the device configuration to the SmartConnector installation folder \$ARCSIGHT_HOME/current/jre/lib/security.



Note: You must copy this file again to the installation folder after upgrading the SmartConnector as this file gets overwritten during the upgrade process.

- Copy the vjdbc.jar and commons-logging-1.1.jar files to the SmartConnector installation folder \$ARCSIGHT_HOME/current/user/agent/lib. These files are located in the lib

directory that was created when you downloaded the JDBC driver and unzipped the package.

7. Browse to \$ARCSIGHT_HOME/current/bin, then double-click runagentsetup.bat file to start the SmartConnector Configuration Wizard.
8. Specify the relevant Global Parameters, when prompted.
9. Select **Microsoft Forefront DB** from the Type drop-down, then click **Next**.
10. Enter the following SmartConnector Parameters:

Parameter	Description
JDBC/ODBC Driver	Select the com.microsoft.sqlserver.jdbc.SQLServerDriver driver.
URL	<p>Enter jdbc:sqlserver://<MS SQL Server Host Name or IP Address>:1433;DatabaseName=<MS SQL Server Database Name>. Replace the actual values for <MS SQL Server Host Name or IP Address> and <MS SQL Server Database Name>.</p> <p>To configure JDBC Driver and Windows Authentication, add ;integratedSecurity=true to the JDBC URL entry for the connection to your database.</p> <p> Note: The name or instance of the database configured at installation or audit time must be used. For example, jdbc:sqlserver://mysqlserver:1433;DatabaseName=my database;integratedSecurity=true</p>
User	Enter the user name of the MS SQL Server DB user with appropriate database privilege.
Password	Enter the password for the database user.
Event Types	Specify the appropriate event types. The currently supported event type is 'uag' (Unified Access Gateway).

 **Note:** Make Sure that the SmartConnector settings match the settings you entered in the data source configuration for the machine on which you are installing the SmartConnector.

11. Click **Export** to export the host name data you have entered into the table into a CSV file or click **Import** to select a CSV file to import into the table rather than adding the data manually.
12. Select a [destination and configure parameters](#).
13. Specify a name for the connector.

14. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

15. Select whether you want to install the connector as a service or in the standalone mode.
16. Complete the installation.
17. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).



Note: When using Windows authentication, after completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should log in to the database. The connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

Adding JDBC Driver to the Connector Appliance/ArcSight Management Center

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the required containers, as follows:

1. From the Connector Appliance/ArcSight Management Center, select **Setup > Repositories**.
2. Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
3. Click **Upload to Repository**.
4. From the **Repository File Creation Wizard**, select **Individual Files**, then click **Next**.
5. Retain the default selection and click **Next**.
6. Click **Upload** and locate and select the .jar file you downloaded.
7. Click **Submit** to add the specified file to the repository and click **Next** to continue.
8. After adding all the files you require, click **Next**.

9. In the **Name** field, enter a descriptive name for the zip file (for example, JDBCdriver). Click **Next**.
10. Click **Done** to complete the process. The newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
11. To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.
12. Select one or more containers into which you want to upload the driver, then click **Next**.
13. Click **Done** to complete the process.
14. Add the connector through the Connector Appliance/ArcSight Management Center interface. For more information, see the *Connector Appliance/ArcSight Management Center Online Help*.

Device event mapping to ArcSight fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

Forefront UAG Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = Error, 3, 4; Medium = Warning, 2; Low = Information, 0, 1
Application Protocol	One of (protocol, ipsApplicationProtocol)
Bytes In	bytesrecv
Bytes Out	bytessent
Destination Host Name	DestHost
Destination Port	DestHostPort
Destination Service Name	UagServiceName
Device Action	Action (0=Not Logged, 1=Bind, 2=Listen, 3=Get host by name, 4=Get host by address, 5=Redirect Bind, 6=Establish, 7=Terminate, 8=Denied, 9=Allowed, 10=Failed, 11=Intermediate, 12=Successful Connection, 13=Unsuccessful Connection, 14=Disconnection, 15=User Cleared Quarantine, 16=Quarantine Timeout) if UagErrorCode is '0'
Device Custom Number 1	MalwareInspectionResult
Device Custom Number 2	ClientAuthenticate
Device Custom Number 3	processingtime
Device Custom String 1	UAG_RULE
Device Custom String 2	Context Id
Device Custom String 3	Malware Inspection Result
Device Custom String 4	ClientAuthenticate (0=Not Logged, 1=YES, 2=NO)
Device Custom String 5	ipsScanResult (0=Unknown, 1=Inspected, 2=Blocked, 3=Detected)
Device Custom String 6	MalwareInspectionAction (0>No action, 1=Allowed, 2=Cleaned, 3=Blocked)
Device Event Category	UagType
Device Event Class ID	UagErrorCode
Device Host Name	servername
Device Product	'Forefront UAG'

Configuration Guide for Microsoft Forefront DB SmartConnector
Device event mapping to ArcSight fields

ArcSight ESM Field	Device-Specific Field
Device Receipt Time	logTime
Device Severity	One of (UagSeverity, MalwareInspectionThreatLevel)
Device Vendor	'Microsoft'
File Type	mimetype
Message	Both (UagModuleId, FilterInfo)
Name	'Microsoft Firewall Service event'
Reason	resultcode
Request Client Application	ClientAgent
Request Method	operation
Request Protocol	One of (protocol, 'https')
Request URL	uri
Source Port	SrcPort
Source User Name	ClientUserName
Transport Protocol	transport

Troubleshooting

"What do I do when the connector can't reconnect to the MS SQL Server database?"

In some cases, connectors using MS SQL Server databases are unable to reconnect to the database after losing and reacquiring network connection. Restarting the connector will resolve this problem.

"How do I deploy SQL Server Native Client?"

When deploying an application that is dependent on SQL Server Native Client, you will need to redistribute SQL Server Native Client with your application. Unlike Microsoft Data Access Components (MDAC), which is now a component of the operating system, SQL Server Native Client is a component of SQL Server. Therefore, it is important to install SQL Server Native Client in your development environment and redistribute SQL Server Native Client with your application.

The SQL Server Native Client redistributable installation program, named sqlncli.msi, is available on the SQL Server installation media and is available as one of the SQL Server Feature Pack components on the Microsoft Download site. For more information about deploying SQL Server Native Client with your application, see "Deploying Applications with SQL Server Native Client" available from Microsoft.

"Why does my connection to SQL Server fail/hang?"

Oracle has released Java 6 update 30 (6u30) that behaves differently from JRE 6u29, causing possible database connection problems for SQL Server database connectors using JDBC connection. These connection problems can occur with JRE 1.6.0_29 (6u29) and later versions.

Microsoft recommends using JRE 6u30 (and above) instead of JRE 6u29. Apply the "SQL Server 2008 R2 Service Pack 1 Cumulative Update 6" patch to the SQL server if you are experiencing connection failures or hangs.

"Why am I receiving the message 'Login failed for user 'sqluser'. The user is not associated with a trusted SQL Server connection."

Only Microsoft JDBC driver v4 or later support integrated authentication. The driver also does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

"How can I keep the connector from becoming clogged with events after being shut down for awhile?"

If the connector is shut down for some time on an active database, a lot of events can accumulate that can clog the connector on restart. The preservestate parameter can be used to avoid this situation. This parameter is enabled (true) by default. Setting preservestate to disabled (false) in the agent.properties file allows the connector to skip the old events and start from real time. The agent.properties file is located in the \$ARCSIGHT_HOME\current\user\agent folder. Restart the connector for your change to take effect.

"What do I do when I receive "Connector parameters did not pass the verification with error ..." message?"

You may not have the correct version of jar file. When you download the JDBC driver, the version of the jar file depends on the version of JRE the connector uses. Versions 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar. Versions 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar. Prior versions of the connector that run JRE 1.6 require sqljdbc4.jar.

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 Configuration Guide for Microsoft Forefront DB SmartConnector
(SmartConnectors CE 24.4)**

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: CE 24.4

Configuration Guide for Microsoft Forefront Protection Server Management Console DB SmartConnector

Document Release Date: October 2024

Software Release Date: October 2024

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2024 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft Forefront Protection Server Management Console DB SmartConnector	4
Product overview	5
Prerequisites	6
Downloading the JDBC driver	6
Installing the SmartConnector	7
Preparing to install the SmartConnector	7
Installing and configuring the SmartConnector	8
Adding JDBC Driver to the Connector Appliance/ArcSight ManagementCenter	10
Device event mapping to ArcSight fields	12
MS FPSMC Notification event mappings	12
MS FPSMC Quarantine event mappings	13
Troubleshooting	14
Send Documentation Feedback	16

Configuration Guide for Microsoft Forefront Protection Server Management Console DB SmartConnector

This guide provides information to install the SmartConnector for Microsoft Forefront Protection Server Management Console DB and to configure the device for event collection.

This guide provides a high level overview of ArcSight SmartConnectors.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product overview

The Microsoft Forefront Protection Server Management Console (FPSMC) is a management tool that provides information technology administrators with a way to centrally manage Forefront Protection 2010 for Exchange Server and Forefront Protection 2010 for SharePoint deployments within your enterprise. Using a browser-based user interface, the management console provides centralized management.

Prerequisites

Downloading the JDBC driver

The SmartConnector installation requires JDBC driver to be present. During the installation process, you will be directed to leave the wizard and copy the JDBC driver file you downloaded to a SmartConnector folder.



Note: Different versions of the JDBC driver are required for different SQL Server database versions. The name of the jar file may be different for some JDBC driver versions. Make sure that you use the correct driver for your database version

Refer to the following information to download the correct jar file depending on the JRE version used by the SmartConnector:

- SmartConnector Version 8.3.0 uses JRE 1.8.0_312 and supports jar files from version mssql-jdbc-6.4.0.jre8.jar ([Download Microsoft JDBC Driver 6.4 for SQL Server](#)) to mssql-jdbc-9.4.0.jre8.jar ([Download Microsoft JDBC Driver 9.4.0 for SQL Server](#)).
- SmartConnector Version 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar ([Download Microsoft JDBC Driver 6.0 for SQL Server](#)).
- SmartConnector Version 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar ([Download Microsoft JDBC Driver 6.0 for SQL Server](#)).
- Earlier versions of SmartConnector run JRE 1.6 and require sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server).

For more information related to the Microsoft JDBC driver, see [Microsoft Documentation](#).

Installing the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

ArcSight recommends that you do not install database connectors on the database server or any mission critical servers as this could cause performance issues.

Preparing to install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, refer to the *Administrator's Guide to ArcSight Platform*, available on [ArcSight Documentation](#).

If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* available on [ArcSight Documentation](#) for instructions.

Before installing the SmartConnector, make sure that the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords
- Minimum DB privileges - OpenText recommends the following minimum permissions to access the database:
 - Explicit CONNECT permission
 - Explicit SELECT permission
 - Public role
 - db_datareader_role

For more information about any specific permission, see the documentation of the specific database.

Installing and configuring the SmartConnector

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Exit the installation wizard.
4. Copy the jar file associated with the version of the driver that you downloaded earlier to \$ARCSIGHT_HOME/current/user/agent/lib
5. To use JDBC driver with SmartConnectors to connect to Microsoft SQL Servers by using Windows authentication, copy the sqljdbc_auth.dll file from the JDBC driver download to the \$ARCSIGHT_HOME\jre\bin directory.

An example of The JDBC driver download path for SQL JDBC driver is:

- For version 4.0 for 32-bit environment is sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll
- For 64-bit environment, sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll

To use the latest version of SQL JDBC Driver such as 9.4:

- Copy the mssql-jdbc-9.4.0.jre8.jar file associated with the version of the driver that you downloaded earlier to \$ARCSIGHT_HOME/current/user/agent/lib
- Copy the mssql-jdbc_auth-9.4.0.x64.dll file from the JDBC driver download to the \$ARCSIGHT_HOME\jre\bin directory.



Note: If you are upgrading the SmartConnector, you must copy the authentication file to \$ARCSIGHT_HOME\jre\bin again after update, as the upgrade process overwrites the \$ARCSIGHT_HOME\jre\bin directory.

6. Copy certificate and JDBC files to SmartConnector folders as follows:

- Copy the jssecacerts certificate that you installed during the device configuration to the SmartConnector installation folder \$ARCSIGHT_HOME/current/jre/lib/security.



Note: You must copy this file again to the installation folder after upgrading the SmartConnector as this file gets overwritten during the upgrade process.

- Copy the vjdbc.jar and commons-logging-1.1.jar files to the SmartConnector installation folder \$ARCSIGHT_HOME/current/user/agent/lib. These files are located in the lib

directory that was created when you downloaded the JDBC driver and unzipped the package.

7. Browse to \$ARCSIGHT_HOME/current/bin, then double-click runagentsetup.bat file to start the SmartConnector Configuration Wizard.
8. Specify the relevant Global Parameters, when prompted.
9. Select **Microsoft Forefront Protection Server Management Console DB** from the Type drop-down list, then click **Next**.
10. Specify the following parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
JDBC/ODBC Driver	Select the com.microsoft.sqlserver.jdbc.SQLServerDriver driver.
URL	<p>Enter jdbc:sqlserver://<MS SQL Server Host Name or IP Address>:1433;DatabaseName=<MS SQL Server Database Name>. Replace with the actual values for the host name or IP address and database name.</p> <p>To configure JDBC Driver and Windows Authentication, add ;integratedSecurity=true to the JDBC URL entry for the connection to your database.</p> <p>Note: The name or instance of the database configured at installation or audit time must be used. For example, jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true</p>
User	Enter the login name of the database user with appropriate privilege.
Password	Enter the database password for the database user.
Event Types	<p>Enter the log event types the connector is to process. The default values are the following event types:</p> <ul style="list-style-type: none"> • notification • quarantine

11. Select a **destination and configure parameters**.
12. Specify a name for the connector.
13. (Conditional) If you have selected **ArcSight Manager** as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination**, and then click **Next**. The certificate is imported and the **Add connector Summary** window is displayed.



Note: If you select Do not import the certificate to connector from destination, the connector installation will end.

14. Select whether you want to install the connector as a service or in the standalone mode.
15. Complete the installation.
16. [Run the SmartConnector](#).

For instructions about upgrading the connector or modifying parameters, see [Installation and User Guide for SmartConnector](#).



Note: When using Windows authentication, after completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should log in to the database. The connector will use the account used to start the service, regardless of the account value setting entered in the connector setup process.

Adding JDBC Driver to the Connector Appliance/ArcSight ManagementCenter

After downloading and extracting the JDBC driver, upload the driver into the repository and apply it to the required containers, as follows:

1. From the Connector Appliance/ArcSight Management Center, select **Setup > Repositories**.
2. Select **JDBC Drivers** from the left pane and click the **JDBC Drivers** tab.
3. Click **Upload to Repository**.
4. From the **Repository File Creation Wizard**, select **Individual Files**, then click **Next**.
5. Retain the default selection and click **Next**.
6. Click **Upload** and locate and select the .jar file you downloaded.
7. Click **Submit** to add the specified file to the repository and click **Next** to continue.
8. After adding all the files you require, click **Next**.
9. In the **Name** field, enter a descriptive name for the zip file (for example, JDBCdriver). Click **Next**.
10. Click **Done** to complete the process. The newly added file is displayed in the **Name** field under **Add Connector JDBC Driver File**.
11. To apply the driver file, select the driver .zip file and click the up arrow to invoke the **Upload Container Files** wizard. Click **Next**.

12. Select one or more containers into which you want to upload the driver, then click **Next**.
13. Click **Done** to complete the process.
14. Add the connector through the Connector Appliance/ArcSight Management Center interface. For more information, see the *Connector Appliance/ArcSight Management Center Online Help*.

Device event mapping to ArcSight fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

MS FPSMC Notification event mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	JobType
Device Custom Number 2	JobId
Device Custom String 1	ProductVersion
Device Custom String 2	EngineName
Device Custom String 3	Platform
Device Custom String 4	EngineVersion
Device Custom String 5	SignatureVersion
Device Custom String 6	UpdateVersion
Device Event Category	TypeName
Device Event Class ID	TypeName
Device Product	'Forefront Protection Server Management Console'
Device Receipt Time	DateStamp_UTC
Device Vendor	'Microsoft'
Event Outcome	One of (Success, 'true', 'Success', 'Failure')
File Name	FileName
File Path	EnginePath
Message	MessageText
Name	TypeName
Reason	MessageCode
Request URL	Source
Source FQDN	Machine

MS FPSMC Quarantine event mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = High, Low = Medium
Destination FQDN	HostName
Destination Host Name	ServerName
Destination NT Domain	One of (RecipientNames, DomainFQDN)
Destination User Name	RecipientNames
Device Custom Number 1	UserRole
Device Custom String 1	Subject
Device Custom String 2	ObjectSID
Device Custom String 3	UserDescription
Device Event Category	IncidentCategory
Device Event Class ID	One of (IncidentCategory, 'Virus', both (IncidentCategory, Detected), both (IncidentCategory, IncidentName))
Device Product	'Forefront Protection Server Management Console'
Device Receipt Time	DetectionTime
Device Severity	Incident Category (Virus=High, Incident=Medium)
Device Vendor	'Microsoft'
File Name	QuarantinedFile
File Path	FilePath
Name	IncidentName
Source User ID	One of (RecipientNames, UserId)
Source User Name	One of (RecipientNames, UserName, SenderName)

Troubleshooting

"What do I do when the connector can't reconnect to the MS SQL Server database?"

In some cases, connectors using MS SQL Server databases are unable to reconnect to the database after losing and reacquiring network connection. Restarting the connector will resolve this problem.

"How do I deploy SQL Server Native Client?"

When deploying an application that is dependent on SQL Server Native Client, you will need to redistribute SQL Server Native Client with your application. Unlike Microsoft Data Access Components (MDAC), which is now a component of the operating system, SQL Server Native Client is a component of SQL Server. Therefore, it is important to install SQL Server Native Client in your development environment and redistribute SQL Server Native Client with your application.

The SQL Server Native Client redistributable installation program, named sqlncli.msi, is available on the SQL Server installation media and is available as one of the SQL Server Feature Pack components on the Microsoft Download site. For more information about deploying SQL Server Native Client with your application, see "Deploying Applications with SQL Server Native Client" available from Microsoft.

"Why does my connection to SQL Server fail/hang?"

Oracle has released Java 6 update 30 (6u30) that behaves differently from JRE 6u29, causing possible database connection problems for SQL Server database connectors using JDBC connection. These connection problems can occur with JRE 1.6.0_29 (6u29) and later versions.

Microsoft recommends using JRE 6u30 (and above) instead of JRE 6u29. Apply the "SQL Server 2008 R2 Service Pack 1 Cumulative Update 6" patch to the SQL server if you are experiencing connection failures or hangs.

"Why am I receiving the message 'Login failed for user 'sqluser'. The user is not associated with a trusted SQL Server connection."

Only Microsoft JDBC driver v4 or later support integrated authentication. The driver also does not provide function to supply Windows authentication credentials such as user name and password. In such cases, the applications must use SQL Server Authentication. When installing the connector on a non-Windows platform, configure the Microsoft SQL Server for Mixed Mode Authentication or SQL Server Authentication.

"How can I keep the connector from becoming clogged with events after being shut down for awhile?"

If the connector is shut down for some time on an active database, a lot of events can accumulate that can clog the connector on restart. The preservestate parameter can be used to avoid this situation. This parameter is enabled (true) by default. Setting preservestate to disabled (false) in the agent.properties file allows the connector to skip the old events and start from real time. The agent.properties file is located in the \$ARCSIGHT_HOME\current\user\agent folder. Restart the connector for your change to take effect.

"What do I do when I receive "Connector parameters did not pass the verification with error ..." message?"

You may not have the correct version of jar file. When you download the JDBC driver, the version of the jar file depends on the version of JRE the connector uses. Versions 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar. Versions 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar. Prior versions of the connector that run JRE 1.6 require sqljdbc4.jar.

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 Configuration Guide for Microsoft Forefront Protection Server Management Console DB SmartConnector (SmartConnectors CE 24.4)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Microsoft IIS File SmartConnector

Document Release Date: October 2023

Software Release Date: October 2023

Legal Notices

Open Text Corporation
275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Copyright 2023 Open Text.

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

Trademark Notices

"OpenText" and other Open Text trademarks and service marks are the property of Open Text or its affiliates. All other trademarks or service marks are the property of their respective owners.

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:

<https://www.microfocus.com/support-and-services/documentation>

Contents

Configuration Guide for Microsoft IIS File SmartConnector	5
Product Overview	6
Configuration	7
Configure Logging	7
Remote Logging	9
Configure IIS to Log Data on a Remote Share	9
Configure Permissions for Remote Logging	10
Save Log Files	11
Install the SmartConnector	12
Prepare to Install Connector	12
Install Core Software	12
Set Global Parameters (optional)	13
Select Connector and Add Parameter Information	14
Select a Destination	15
Complete Installation and Configuration	16
Additional Configuration	17
Change Log File Name Prefix	17
Specify File Name Suffix	17
Specify the Locale Used for Determining the Current Date for File Names	18
Run the SmartConnector	19
Device Event Mapping to ArcSight Fields	20
IIS Event Mappings	20

Troubleshooting 22

Send Documentation Feedback 23

Configuration Guide for Microsoft IIS File SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Internet Information Server (IIS) File and configuring the device for log file collection.

Intended Audience

This guide provides information for IT administrators who are responsible for managing the ArcSight software and its environment.

Additional Documentation

The ArcSight SmartConnector documentation library includes the following resources:

- [Technical Requirements Guide for SmartConnector](#), which provides information about operating system, appliance, browser, and other support details for SmartConnector.
- [Installation and User Guide for SmartConnectors](#), which provides detailed information about installing SmartConnectors.
- [Configuration Guides for ArcSight SmartConnectors](#), which provides information about configuring SmartConnectors to collect events from different sources.
- [Configuration Guide for SmartConnector Load Balancer](#), which provides detailed information about installing Load Balancer.

For the most recent version of this guide and other ArcSight SmartConnector documentation resources, visit the [documentation site for ArcSight SmartConnectors 8.4](#).

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to MFI-Documentation-Feedback@opentext.com.

For specific product issues, [contact Open Text Support for Micro Focus products](#).

Product Overview

The SmartConnector for Microsoft IIS File lets you import activity and alarm events generated and stored in a log file by Microsoft IIS into the ArcSight ESM system.

The SmartConnector for Microsoft IIS File (this connector) retrieves logs from one web site per IIS server. File patterns are comma delimited and support different rotation patterns. For supported devices and versions, see [Technical Requirements](#).

Configuration

Configure Logging

For complete configuration information, see the *Windows Server IIS 7 Operations Guide* under **Monitor Activity on a Web Server**, the “Configuring Logging in IIS 7” section, from which the information in this section has been derived.

To configuration logging in IIS:

1 Open IIS Manager.

For Windows Server 2012, on the **Start** page click the **Server Manager** tile and then click **OK** in **Server Manager**. Click the **Tools** menu, and then click **Internet Information Services (IIS) Manager**.

For Windows 8, on the **Start** page type **Control Panel** and then click the **Control Panel** icon in the search results. On the **Control Panel** screen, click **System and Security**, click **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**.

2 In the **Connections** tree view, select your website.

3 When configuring logging at the site level, in **Features View**, double-click **Logging**.

When configuring per site logging at the server level, on the **Logging** page under **One log file per site**, select **Site** from the drop-down list. By default, **Site** is selected.

When configuring per server logging at the server level, on the **Logging** page, under **One log file per site**, select **Server** from the drop-down list. By default, **Site** is selected.

4 On the **Logging** page, in the **Log file** section under **Format**, select the **W3C** log file format to use the centralized W3C log file format to log information about all sites on the server. Specify at least the following fields in the **W3C Logging Fields** dialog box by clicking **Select Fields** on the **Logging page**. Fields are separated by spaces and time is recorded in Coordinated Universal Time (UTC).

Date (date)

Time (time)

Client IP Address (c-ip)

User Name (cs-username)

Server Name (s-computername)

Server IP Address (s-ip)

Server Port (s-port)

- Method (cs-method)
- URI Stem (cs-uri-stem)
- Protocol Status (sc-status)
- Protocol Version (cs-version)
- Host (cs-host)

5 Under **Directory**, specify the path where the log file should be stored. The default is <SystemDrive>\inetpub\logs\LogFiles. As a best practice, store log files, such as failed request trace logs, in a directory other than systemroot.

6 In the **Log File Rollover** section, select one of the following options:

Schedule: Select one of these values to determine when a new log file is to be created: **Hourly, Daily, Weekly, or Monthly.**

Maximum file size (in bytes): Select this to create a log file when the file reaches a certain size, in bytes. The minimum file size is 1048576 bytes. If this attribute is set to a value less than 1048576 bytes, the default value is implicitly assumed as 1048576 bytes.

Do not create a new log file: Select this for a single log file that continues to grow as information is logged.

7 Select **Use local time for file naming and rollover** to specify that log file naming and time for log file rollover uses the local server time. When this option is not selected, Coordinated Universal Time (UTC) is used. (Regardless of this setting, timestamps in the actual log file will use the time format for the log format that you select from the Format list. For example, W3C log file format uses UTC time format for timestamps.)

8 Click **Apply** in the **Actions** pane.

Remote Logging

You can write log data to a remote share over a network using a full Universal Naming Convention (UNC) path for centralized log file storage and backup.



Mapped drives cannot be used for remote logging; services run in a virtual network and cannot recognize mapped drives.

Be aware that remote logging can negatively affect performance because IIS writes the log file data over the network. In addition, if the network goes down and IIS cannot send events to the remote machine, IIS, not the SmartConnector, determines whether these events are recovered or lost.

In the remote share, IIS creates a unique directory for each Web site; for example **W3SVCX**, where *X* is a random number generated by IIS to represent the specific Web site. IIS also creates the log file with exclusive write access, so that multiple machines cannot write to the same log file. Be sure to specify the folder in which these files can be found; for example:

`\IIS\logfiles\W3SVCx...`

The connector will look only for the following subdirectories:

`W3SVx...`
`FTPSVCx...`
`SMTPSVCx...`
`NNTPSVCx...`



Microsoft highly recommends that you enable Internet Protocol security (IPSec) between your Web server running IIS and the remote server before configuring remote logging. If IPSec is not enabled between the server and remote server, data packets containing log data are potentially at risk of being intercepted by malicious individuals and wire-sniffing applications while the data packet travels through the network.

Configure IIS to Log Data on a Remote Share

To log Web site data on a remote share:

- 1 Create a log file directory on a remote server in the same domain as your Web server running IIS.

- 2** Change the directory properties so the directory is a share and assign the **Everyone** group **Full Control** permissions.
- 3** Ensure that your server running IIS has **Full Control** access permission on the remote share and read and write permissions on the remote log file directory. For more information, see "Configure Permissions for Remote Logging."
- 4** In IIS Manager, expand the local computer, right-click the **Web Sites** folder, and click **Properties**.
- 5** On the **Web Site** tab, ensure that the **Enable logging** check box is selected.
- 6** In the **Active log format** list box, select a log file format.
- 7** Click **Properties**.
- 8** Click the **General** tab, and in the **Log file directory** box, enter the full UNC path. For example, enter `\server\share\LogFiles` where `server` represents the name of the remote server and `LogFiles` represents the name of the share where the log files are stored.
- 9** Click **Apply** and then click **OK**. All Web sites within the directory begin logging data to the remote share.



Logging to a UNC share is not supported by IIS FTP. You must configure the FTP log files location to a path on the local machine.

Configure Permissions for Remote Logging

IIS can store log files on a remote share as long as the remote computer allows IIS to create log files and write the data to the remote share.

To configure permissions for remote logging:

- 1** On the remote computer, navigate to `systemroot\System32`, right-click the **LogFiles** folder, and click **Sharing and Security**.
- 2** On the **Sharing** tab, click **Share this folder** and then click **Permissions**.
- 3** Click **Add**.
- 4** Click **Object Types**.
- 5** Select the **Computers** check box and click **OK**. You can deselect all other options.

- 6** In the **Enter the object name to select** box, enter the object name in the form *Domain\WebServer* object and click **OK**.
- 7** In the **Group or user names** list, select the *Domain\WebServer* object and, in the **Permissions** section, select the **Allow** check box next to **Full Control**.
- 8** In the **Group or user names** list, select **Everyone**.
- 9** In the **Permissions** section, clear all permissions and click **OK**. The remote computer now has the appropriate access permissions.
- 10** To set the appropriate file permissions, click the **Security** tab.
- 11** Select the *Domain\WebServer* object and, in the **Permissions** section, select the **Allow** check box next to **Full Control**.
- 12** Click **Apply**. Then click **OK**.

Save Log Files

By default, IIS creates a new log file for each Web site in the *systemroot\System32\LogFiles* directory. However, you can specify the directory into which log files are saved and you can determine when new log files are started. To protect logged data, set appropriate Access Control with IIS on the log file directory.

To set options for saving log files:

- 1** In IIS Manager, expand the local computer, expand the Web or FTP Sites directory, right-click the Web or FTP site, and click **Properties**.
- 2** On the **Web Site** or **FTP SITE** tab, click **Properties** next to the **Active log format** list box.
- 3** Select the log schedule to use when starting a new log file.



"Midnight" is midnight local time for all log file formats except the W3C Extended format. For W3C Extended log file format, "midnight" is midnight Greenwich Mean Time (GMT) by default, but can be changed to midnight local time. To open new W3C Extended logs using local time, select the **Use local time for file naming and rollover** check box. The new log starts at midnight local time, but the time recorded in the log files is still GMT.

- 4** Under **Log file directory**, enter the directory where log files should be saved. For information about saving log files on a remote share, see "Remote Logging."
- 5** Click **Apply** and then click **OK** twice.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.



Connector Appliance/ArcSight Management Center supports mounting for Network File System (NFS) and CIFS (Windows) shares. When you install this connector on one of these devices, establish a CIFS mount on the device before adding the connector. Provide this share name during connector configuration. For more information, see **Remote File Systems** in the Connector Appliance or ArcSight Management Center Administrator's Guide.

Prepare to Install Connector

Before you install any SmartConnectors, make sure that the ArcSight products with which the connectors will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger).

For complete product information, read the *Administrator's Guide* as well as the *Installation and Configuration* guide for your ArcSight product before installing a new SmartConnector. If you are adding a connector to the ArcSight Management Center, see the *ArcSight Management Center Administrator's Guide* for instructions, and start the installation procedure at "Set Global Parameters (optional)" or "Select Connector and Add Parameter Information."

Before installing the SmartConnector, be sure the following are available:

- Local access to the machine where the SmartConnector is to be installed
- Administrator passwords

Install Core Software

Unless specified otherwise at the beginning of this guide, this SmartConnector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Product and Platform Support* document, available from the OpenText SSO site.

- 1 Download the SmartConnector executable for your operating system from the OpenText SSO site.

2 Start the SmartConnector installation and configuration wizard by running the executable.

Follow the wizard through the following folder selection tasks and installation of the core connector software:

- Introduction
- Choose Install Folder
- Choose Shortcut Folder
- Pre-Installation Summary
- Installing...

3 When the installation of SmartConnector core component software is finished, the Add a Connector window is displayed.

Set Global Parameters (optional)

If you choose to perform any of the operations shown in the following table, do so before adding your connector. You can set the following parameters:

Parameter	Setting
FIPS mode	Select 'Enabled' to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the SmartConnector User Guide under "Modifying Connector Parameters" for instructions. Initially, this value is set to 'Disabled'.
Remote Management	Select 'Enabled' to enable remote management from ArcSight Management Center. When queried by the remote management device, the values you specify here for enabling remote management and the port number will be used. Initially, this value is set to 'Disabled'.
Remote Management Listener Port	The remote management device will listen to the port specified in this field. The default port number is 9001.
Preferred IP Version	When both IPv4 and IPv6 IP addresses are available for the local host (the machine on which the connector is installed), you can choose which version is preferred. Otherwise, you will see only one selection. The initial setting is IPv4.

The following parameters should be configured only if you are using OpenText SecureData solutions to provide encryption. See the *OpenText SecureData Architecture Guide* for more information.

Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Policy URL	Enter the URL where the OpenText SecureData Server is installed.
Proxy Server (https)	Enter the proxy host for https connection if any proxy is enabled for this machine.
Proxy Port	Enter the proxy port for https connection if any proxy is enabled for this machine.
Format Preserving Identity	The OpenText SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for OpenText SecureData.
Format Preserving Secret	Enter the secret configured for OpenText SecureData to use for encryption.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted and add any string or numeric fields you want encrypted. Encrypting more fields can affect performance, with 20 fields being the maximum recommended. Also, because encryption changes the value, rules or categorization could also be affected. Once encryption is enabled, the list of event fields cannot be edited.

After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

Select Connector and Add Parameter Information

- 1 Select **Add a Connector** and click **Next**. If applicable, you can enable FIPS mode and enable remote management later in the wizard after SmartConnector configuration.
- 2 Select **Microsoft IIS File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Log Folder	Enter the value of 'Log file directory' from the General Properties page of the IIS Extended Logging Properties window. To log accounting information to a remote server, specify the log file name by entering a Universal Naming Convention (UNC) name, such as '\\MyLogServer\LogShare'. If you do not supply a full path statement in 'Log File Directory,' the default path is used. For example, if you enter 'IISLogFile' in 'Log File Directory,' the file is located at 'systemroot\System32\IISLogFile.'
	Users can modify it if they would like to change the log file directory for further configuration. This parameter is located in the agent.properties file at:
	- If the remote server log file is at: \\MyLogServer\LogShare\W3SVC1, then set agents [0].logfilehome=\\\\\\MyLogServer\\\\LogShare\\\\W3SVC1
	- If the local log file is at: C:\\inetpub\\logs\\LogFiles\\W3SVC1, then set agents [0].logfilehome =C:\\\\inetpub\\\\logs\\\\LogFiles\\\\W3SVC1
New Log Time Period	From the drop-down menu, choose the time period you selected in the Extended Logging Properties window. Selections supported by the connector include 'Hourly', 'Daily', 'Weekly', 'Monthly', or 'Unlimited file size'. The 'When file size reaches:' selection is not supported. See "Specify File Name Suffix" for more information.

Choose the SmartConnector for Microsoft IIS Multiple Site File if your Web Server hosts multiple sites.

Select a Destination

- The next window asks for the destination type; select a destination and click **Next**. For information about the destinations listed, see the *ArcSight SmartConnector User Guide*.
- Enter values for the destination. For the ArcSight Manager destination, the values you enter for **User** and **Password** should be the same ArcSight user name and password you created during the ArcSight Manager installation. Click **Next**.
- Enter a name for the SmartConnector and provide other information identifying the connector's use in your environment. Click **Next**. The connector starts the registration process.
- If you have selected ArcSight Manager as the destination, the certificate import window for the ArcSight Manager is displayed. Select **Import the certificate to the connector from destination** and click **Next**. (If you select **Do not import the certificate to connector from destination**, the connector installation will end.) The certificate is imported and the **Add connector Summary** window is displayed.

Complete Installation and Configuration

1 Review the **Add Connector Summary** and click **Next**. If the summary is incorrect, click **Previous** to make changes.

2 The wizard now prompts you to choose whether you want to run the SmartConnector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, select **Leave as a standalone application**, click **Next**, and continue with step 5.

3 If you chose to run the connector as a service, with **Install as a service** selected, click **Next**. The wizard prompts you to define service parameters. Enter values for **Service Internal Name** and **Service Display Name** and select **Yes** or **No** for **Start the service automatically**. The **Install Service Summary** window is displayed when you click **Next**.

4 Click **Next** on the summary window.

5 To complete the installation, choose **Exit** and Click **Next**.

For instructions about upgrading the connector or modifying parameters, see the *SmartConnector User Guide*.

Additional Configuration

Change Log File Name Prefix

With IIS version 7, the default log file encoding scheme is switched to UTF-8. Therefore, the log file name has been changed accordingly to start with u_ex. For prior IIS versions, the default log file encoding scheme was ANSI, and the log file name started with ex. To address this issue, in support of IIS 7 events, a new advanced parameter has been added that lets you set the log file name prefix.

After SmartConnector installation, you can change the connector's advanced parameters by editing the agent.properties file located at \$ARCSIGHT_HOME\current\user\agent. For logfile.name.prefix change the value to u_ex for UTF-8 file name scheme; change the value to ex for the ANSI log file name scheme. Save the file and restart the connector for your changes to take effect.

Specify File Name Suffix

For the connector to detect the log file, the log file name suffix must be consistent with the current day and type of log. The format of the name suffix must be as shown in the following table.

Time Period	Suffix Format	Example
Hourly	Prefix + Year + Month + Day + Hour	If current date is 08/07/2015 at 12:00, name is u_ex15080712 or ex15080712
Daily	Prefix + Year + Month + Day	If current date is 08/07/2015, name is u_ex150807 or ex150807
Weekly	Prefix + Year + Month + Week (Week is the week of the month)	If current date is 08/07/2015, name is u_ex150802 or ex150802
Monthly	Prefix + Year + Month	If current date is 08/07/2015, name is u_ex1508 or ex1508
Unlimited	Prefix + 'tend1'	Name is u_extend1 or extend1

Specify the Locale Used for Determining the Current Date for File Names

An advanced parameter named `localeforfilename` has been added to specify the locale used for determining the current date for file names. If not specified, the default locale will be used, which normally works unless the default locale is Thailand, which numbers years differently. For Thailand, the parameter should be set to `en_US`.

To set advanced parameters for your SmartConnector, after connector installation, edit the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`. Locate the `localeforfilename` parameter and set its value to `en_US`. Restart the connector for your changes to take effect.

Run the SmartConnector

SmartConnectors can be installed and run in stand-alone mode, on Windows platforms as a Windows service, or on UNIX platforms as a UNIX daemon, depending upon the platform supported. On Windows platforms, SmartConnectors also can be run using shortcuts and optional Start menu entries.

If the connector is installed in stand-alone mode, it must be started manually and is not automatically active when a host is restarted. If installed as a service or daemon, the connector runs automatically when the host is restarted. For information about connectors running as services or daemons, see the *ArcSight SmartConnector User Guide*.

To run all SmartConnectors installed in stand-alone mode on a particular host, open a command window, go to \$ARCSIGHT_HOME\current\bin and run: arcsight connectors

To view the SmartConnector log, read the file \$ARCSIGHT_HOME\current\logs\agent.log; to stop all SmartConnectors, enter Ctrl+C in the command window.

Device Event Mapping to ArcSight Fields

The following section lists the mappings of ArcSight data fields to the device's specific event definitions. See the *ArcSight Console User's Guide* for more information about the ArcSight data fields.

IIS Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	400..599 = High; 300..399 = Medium; 0, 100..299 = Low
Bytes In	sc-bytes
Bytes Out	cs-bytes
Destination Address	s-ip
Destination Host Name	s-computername
Destination Port	One of (s-port, cs-host)
Device Custom IPv6 Address 1	cs-host (Device IPv6 Address)
Device Custom IPv6 Address 2	c-ip (Source IPv6 Address)
Device Custom IPv6 Address 3	s-ip (Destination IPv6 Address)
Device Custom Number 1	s-siteid
Device Custom String 1	cs(Referer)
Device Custom String 2	time-taken
Device Custom String 3	sc-win32-status
Device Custom String 4	s-queuename
Device Event Class ID	One of (cs-version, '(HTTP http).*'), 'HTTP', one of (sc-status, '-', cs-method, sc-status), one of (cs-version, one of (cs-method, ' (GET PUT HEAD TRACK TRACE POST SEARCH PROPFIND OPTIONS)'), sc-status, all of (cs-method, ':', sc-status)), (sc-status, '-', s-reason, all of (cs-version, ':', sc-status)))
Device Host Name	cs-host
Device Process Name	s-sitename
Device Product	'Internet Information Server'
Device Receipt Time	date, time

Configuration Guide for Microsoft IIS File SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Severity	sc-status
Device Vendor	'Microsoft'
Name	'IIS action'
Protocol	cs-version
Reason	s-reason
Request Client Application	cs(User-Agent)
Request Cookies	cs(Cookie)
Request Method	cs-method
Request URL	cs-uri
Request URL File Name	cs-uri-stem
Request URL Query	cs-uri-query
Source Address	c-ip
Source Port	c-port
Source User Name	cs-username

Troubleshooting

I want to install the ArcSight connector in a separate machine. What are the steps for me to set up a share on the IIS machine so the ArcSight connector can read the logs from that share?

This works only for IIS 6.0 or later. If your IIS version is 6.0 or later, you can run the ArcSight connector service with a domain admin user:

- Use the domain admin user as the Logon User in the ArcSight connector service.
- Create a share on the log file directory on the remote machine (where IIS is located).
- During connector setup, use the UNC name rather than the drive letter to point to the share.

To run the ArcSight connector service with a user other than domain admin:

- Use the domain user as the Logon User in the ArcSight connector service.
- Create a share on the log file directory on the remote machine (where IIS is located).
- Grant privileges to the domain user on the share on the IIS machine.
- During connector setup, use the UNC name rather than the drive letter to point to the share.
- Add the domain user to the Local Admin group so the service can be started by the domain user.

please confirm that when customer used MySQL JDBC driver 5.1.38, they had issue to receive events. And the workaround is to apply older driver 5.0.8, after that connector is able to received events.

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 Configuration Guide for Microsoft IIS File SmartConnector (SmartConnectors 8.4.3)

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 MFI-Documentation-Feedback@opentext.com.

We appreciate your feedback!