Micro Focus Security ArcSight Connectors

SmartConnector for IBM SiteProtector DB

Configuration Guide

August 20, 2020

Configuration Guide

SmartConnector for IBM SiteProtector DB

August 20, 2020

Legal Notices

Micro Focus

The Lawn

22-30 Old Bath Road

Newbury, Berkshire RG14 1QN

UK

https://www.microfocus.com.

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:

https://community.microfocus.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
08/20/2020	Added the Old File Hash field mapping for IBM SiteProtector Mappings.
09/19/2019	Updated mapping for the deviceReceiveTime field in parser files.
05/17/2019	Added support to multiple timestamp starttime and endtime formats.
10/17/2017	Added encryption parameters to Global Parameters.
07/15/2017	Updated JDBC download information.
05/15/2017	End of support for versions 2.0, 2.9, and 3.0 due to end of support by vendor.
11/30/2016	Updated installation procedure for setting preferred IP address mode.
02/15/2016	Removed ODBC support due to Java 8 implementation.
09/30/2015	Updated list of tables requiring host access.
11/14/2014	Added support for SiteProtector v3.1.
06/30/2014	Updated mappings for Device Event Class ID and Device Action: added Source NT Domain mapping.
02/28/2014	Pre-release with updated parser.
02/14/2014	Added support for version 3.0 and troubleshooting information.
09/30/2013	Updated “Create an ODBC Data Source” section and added troubleshooting information regarding connection failure.

SmartConnector for IBM SiteProtector DB

This guide provides information for installing the SmartConnector for IBM SiteProtector DB for event collection. IBM SiteProtector version 3.1 is supported.

The SiteProtector system collects security events from the following protection devices and software:

- IBM Proventia Network Intrusion Detection System (IDS)
- IBM Proventia Network Mail Security System
- IBM Proventia G100 Server Intrusion Prevention System (IPS)
- IBM RealSecure 7.0 Server Sensor and Network Sensor
- IBM Proventia M10 Network Intrusion Prevention System (IPS)
- IBM Proventia Desktop Endpoint Security
- IBM Internet Scanner 7.0 SP2 software

Product Overview

IBM's SiteProtector simplifies and automates the enterprise protection process, reducing the costs and complexity of your security while analyzing and documenting the value of security within your organization. The centralized management system provides a framework for security process management to assist network, systems and security teams.

Configuration

Tables Requiring Host Access

For the SmartConnector to access log events, access should be granted for the following tables:

- AlertType
- AlertCategory
- VulnStatus
- Observances
- SensorData
- SensorDataAVP
- SecurityChecks
- CheckProducts
- Products
- Component
- Hosts

Download and Install a JDBC Driver

During the installation process, you will be directed to leave the wizard and copy the JDBC driver file you download to a SmartConnector folder. For information about and to download the MS SQL Server JDBC Driver, see:

http://msdn.microsoft.com/en-us/sqlserver/aa937724

> 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.

When you download the JDBC driver, the version of the jar file depends on the version of the JRE the connector uses:

- Version 7.2.1 and later use JRE 1.8 and require sqljdbc42.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- Version 7.1.2 and later use JRE 1.7 and require sqljdbc41.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
- Prior versions, which run JRE 1.6, require sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server)

Install the driver.

For software connectors, copy the jar file appropriate for your SQL Server version from the installation folder for the SQL Server JDBC driver to a temporary location; you will copy this file to `$ARCSIGHT_HOME/current/user/agent/lib`, (where `$ARCSIGHT_HOME` refers to the SmartConnector installation folder, such as `c:\ArcSight\SmartConnectors`) after the core SmartConnector software has been installed at step 3 of Install the SmartConnector. Copy only the jar file associated with the version of the driver to be installed to this location.

Add a 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 appropriate container or containers, as described in this section.

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 in step 3 of SmartConnector Installation.
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, enter 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.

14 Add the connector through the Connector Appliance/ArcSight Management Center interface; see the *Connector Appliance/ArcSight Management Center Online Help* for detailed information. Descriptions of parameters to be entered during connector configuration are provided in the "Install the SmartConnector" section of this guide.

Configure the JDBC Driver and Windows Authentication

This section provides guidance on how to use a JDBC driver with SmartConnectors that connect to Microsoft SQL Servers using Windows Authentication only. As previously described, download the SQL JDBC drivers from Microsoft and install the driver before beginning this procedure.

> The JDBC driver 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.

Microsoft Type 4 JDBC drivers (versions 4.0 or later) support integrated authentication. Windows Authentication works only when using one of these drivers. You also will need to add `;integratedSecurity=true` to the JDBC URL entry for the connection to your database.

1 Copy the `sqljdbc_auth.dll` file from the JDBC driver download to the `$ARCSIGHT_HOME\jre\bin directory`. For example, the JDBC driver download path for SQL JDBC driver version 4.0 for 32-bit environment would be `sqljdbc_4.0\enu\auth\x86\sqljdbc_auth.dll` and, for 64-bit environment, `sqljdbc_4.0\enu\auth\x64\sqljdbc_auth.dll`.

> When upgrading a connector, the $ARCSIGHT_HOME\jre\bin directory is overwritten; therefore, you will need to copy the authentication file to this folder again after update.

2 Go to `$ARCSIGHT_HOME\current\bin` and double-click `runagentsetup` to continue the SmartConnector installation.

3 When entering the connector parameters, in the **JDBC Database URL** field, append `;integratedSecurity=true` to the end of the URL string.

The following is an example; note that the name or instance of the database configured at installation/audit time should be used.

```
jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true
```

4 Complete the remaining connector wizard configuration steps.

5 After completing the connector installation, if running on a Windows Server, change the service account to use the Windows account that should login 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.

Install the SmartConnector

The following sections provide instructions for installing and configuring your selected SmartConnector.

ArcSight recommends you do not install database connectors on the database server or any mission critical servers as this could cause performance issues.

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

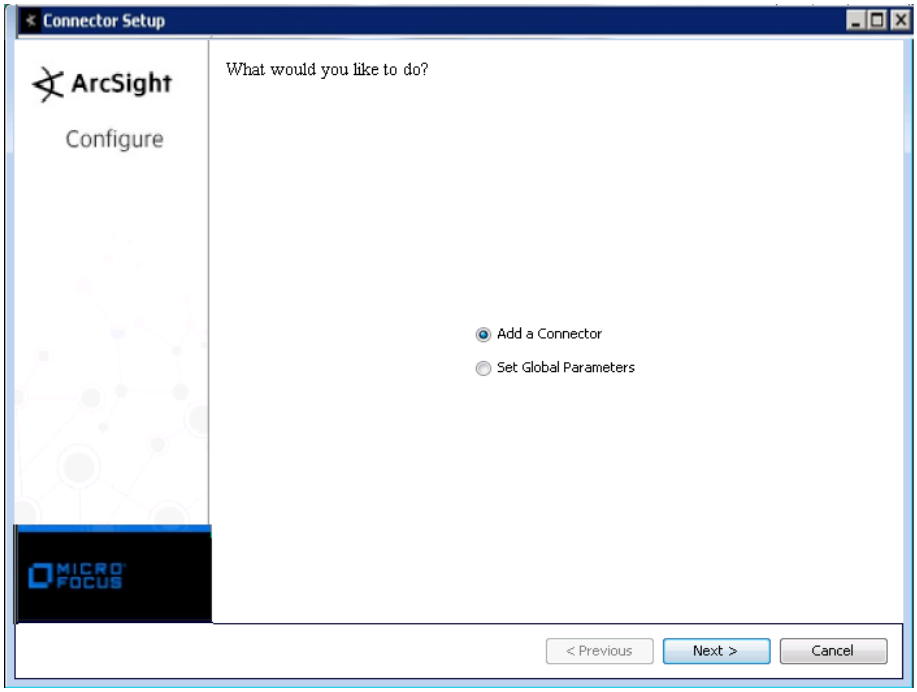
Install Core Software

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 Micro Focus SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the Micro Focus 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:



Download SQL Server JDBC Driver

To download a Microsoft SQL Server JDBC driver, click **Cancel** to leave the configuration wizard at this point and copy the jar file you downloaded earlier (see "Download and Install a JDBC Driver") to `$ARCSIGHT_HOME/current/user/agent/lib`.

From `$ARCSIGHT_HOME/current/bin`, double-click `runagentsetup` to return to the SmartConnector Configuration Wizard.

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 Micro Focus SecureData solutions to provide encryption. See the *Micro Focus 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 Micro Focus 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 Micro Focus 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 Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus 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.

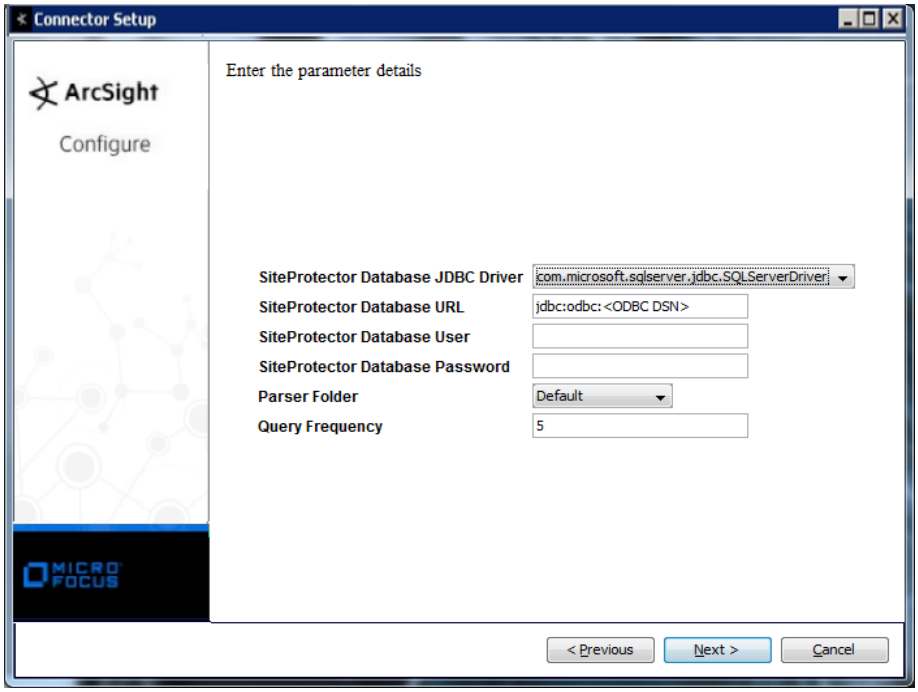
After making your selections, click **Next**. A summary screen is displayed. Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with "Add a Connector" window. Continue the installation procedure with "Select Connector and Add Parameter Information."

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 **IBM SiteProtector DB** and click **Next**.

3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Database JDBC Driver	Select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver.
Database URL	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	Enter the login name of the database user with appropriate privilege.
Database Password	Enter the password for the SiteProtector Database User.
Parser Folder	You can enable optional 'payload sampling' or 'sensor response.' When 'Payload Sampling' is selected during the installation process, the AttributeBlob field of the SensorDataAVP table is used in the main SQL query and retrieved payload is stored as part of event. When 'Sensor Response' is selected during the installation process, the SensorResponse table is used in the main SQL query and the content of the SensorResponse table will possibly be mapped to the deviceAction field. By default, these options are not enabled. Be aware that these options have a huge performance impact to your database. Enable either of these options only when absolutely necessary.
Query Frequency	Enter a value in seconds for how often you want the SmartConnector to query.

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*.

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.

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.

Payload Sampling

Many customers use ArcSight for security event analysis, including investigating the packet records data that triggered the security event. In ArcSight terms, these packet records are called *payload*. Payload refers to the information carried in the body of an event's network packet, as distinct from the packet's header data. While security event detection and analysis usually centers on header data, packet payload may also be forensically significant. ArcSight supports two ways to retrieve payload from Sourcefire eStreamer: Payload Sampling and On-Demand Payload.

- **Payload Sampling** allows up to 1023 bytes of the payload to be retrieved and displayed as ASCII characters in a custom string field for ***each*** event. An option is also provided to display up to 511 bytes in hexadecimal format. Be default, the payload sampling feature is not enabled due to its potentially large storage requirements. To enable payload sampling, select **true** for the Enable payload sampling parameter during connector installation.

- **On-Demand Payload Retrieval** lets you retrieve the entire payload if the payload is still held on the device.

You can retrieve, preserve, view, or discard payloads using the ArcSight Console. Because event payloads are relatively large, ArcSight does not store them by default. Instead, you can request payloads from devices for selected events through the Console. If the payload is still held on the device, the ArcSight SmartConnector retrieves it and sends it to the Console.

Payloads are downloaded and stored only on demand; you must configure ESM to log these packets. By default, 256 bytes of payload will be retrieved.

Whether an event has a payload to store is visible in event grids. Unless you specifically request to do so, only the event's "payload ID" (information required to retrieve the payload from the event

source) is stored. Payload retention periods are controlled by the configuration of each source device.

Locate Payload-Bearing Events

The first step in handling event payloads is to be able to locate payload-bearing events among the general flow of events in a grid view. In an ArcSight Console Viewer panel grid view, right-click a column header and choose **Add Column -> Device -> Payload ID**. Look for events showing a Payload ID in that column.

Retrieve Payloads

In a Viewer panel grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab, then click **Retrieve Payload**.

Preserve Payloads

In a grid view, right-click an event with an associated payload, select **Payload**, then **Preserve**. Alternatively, in the Event Inspector, click the **Payload** tab, then **Preserve Payload**.

Discard Payloads

In a grid view, right-click an event with an associated payload and select **Payload**, then **Discard Preserved**. You also can use the Event Inspector: In a grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab. Click **Discard Preserved Payload**.

Save Payloads to Files

In a grid view, double-click an event with an associated payload. In the Event Inspector, click the **Payload** tab. Click **Save Payload**. In the **Save** dialog box, navigate to a directory and enter a name in the **File name** text field. Click **Save**.

Turbo Mode

Fields could be dropped depending upon the turbo mode for both ArcSight Manager and 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.

The ArcSight SourceIpV6Address and DestinationIpV6Address additional data fields represent the IPv6 source and destination addresses respectively. And the Source Address and Destination Address fields represent the IPv4 source and destination addresses, respectively.

When the IPv6 address fields contain a non-null value, the IPv4 address fields are still populated with the 24-bit portion of the IPv6 address and will start from 0. This is because not all modules within SiteProtector have been converted to accept an IPv6 address and still require an IPv4 address.

IBM SiteProtector Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	Device IpV6Address (SrcIPv6High, SrcIPv6Low)
Additional data	Source IpV6Address (SrcIPv6High, SrcIPv6Low)
Additional data	DestinationIpV6Address (DestIPv6High, DestIPv6Low)
Agent (Connector) Severity	High = 1, high, High; Medium = 2, medium, Medium; Low = 3, low, Low
Base Event Count	One of (:repeat-count, event_count, AlertCount)
Destination Address	DestAddressInt
Destination DNS Domain	DestinationDNSName
Destination Host Name	DestinationNetBiosName
Destination Mac Address	DestinationEthernetAddress
Destination NT Domain	One of (HostNBDomain, DestinationNetBiosName, Users Domain, UserName (from NTDomain))
Destination Port	One of (:port, port, dstport)
Destination Process Name	One of (:server, server)
Destination Service Name	One of (:DestPortName, :http-server, http-server)
Destination User Name	One of (:to, Target Account Name, User, :User, :user, UserName, :UserName, Target Account Name, to, AccountName)
Device Action	One of (AttackSuccessful, one of (VulnStatusDesc, :verdict, :action), all of (AttackSuccessful, "0=Attack Failed", "1=Attack Successful", "2=Attack Status Unknown"))
Device Action (Sensorresponse)	One of (ResponseTypeName, BLOCK, AttackSuccessful, one of (VulnStatusDesc, :verdict, :action), all of (AttackSuccessful, "0=Attack Failed", "1=Attack Successful", "2=Attack Status Unknown"))
Device Address	SensorAddressInt
Device Custom IPv6 Address 1	Device IPv6 Address (One of (IP_V6_HIGH, IP_V6_LOW, Sensor IPv6High, SensorIPv6Low))
Device Custom IPv6 Address 2	Source IPv6 Address (One of (SrcIPv6High, SrcIPv6Low))
Device Custom IPv6 Address 3	Destination IPv6 Address (One of (DestIPv6High, DestIPv6Low))
Device Custom Number 1	ProductID
Device Custom Number 2	IssueId
Device Custom Number 3	ObjectType
Device Custom String 1	One of (:port, port, dstport)
Device Custom String 2	One of (:victimip, victimip, :hosts)
Device Custom String 3	One of (:passwd, :password, PASSWORD)
Device Custom String 4	AlertTypeName
Device Custom String 5	VulnStatusDesc
Device Custom String 6	ObjectName
Device DNS Domain	SensorDNSName
Device Event Category	ObservanceTypeDesc
Device Event Class ID	AlertName
Device External ID	One of (SensorName, SensorGUID)
Device Host Name	One of (HOST_NB_NAME, SensorName)
Device Mac Address	SensorEthernetAddress

ArcSight ESM Field	Device-Specific Field
Device Payload ID	SensorDataID
Device Product	PRODUCT_NAME
Device Receipt Time	SensorDataAlertDateTime
Device Severity	AlertPriority
Device Vendor	'ISS'
End Time	One of (end-time,:end-time)
External ID	RowID
File Hash	One of (:CRC, CRC)
File ID	algorithm-id
File Name	One of (LogFile, :file, :filename, :FILENAME, FILENAME)
File Path	HostOSName
File Size	One of (Servername_Length, :C-SIZE, SIZE, C-SIZE)
Message	One of (Message, :msg, :reason, reason, ChkBriefDesc)
Name	AlertName
Old File Hash	oneOf(Message,:msg,:reason,reason,ChkBriefDesc
Old File Name	:contentFound
Request Context	:arg
Request Cookies	:cookie
Request URL	One of (URL, :URL, :URI, :channel)
Source Address	SrcAddressInt
Source DNS Domain	SourceDNSName
Source Host Name	One of (:host, :CLIENT, CLIENT, Caller Machine Name)
Source Mac Address	SourceEthernetAddress
Source NT Domain	SourceNetBiosName
Source Port	SourcePort
Source User Name	One of (:user, :login, login, :loginname, :name, name, :from, :nick, :nickname, from)
Start Time	One of (Start-time,:start-time)
Transport Protocol	One of (ProtocolID, Service protocol, protocol)

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.

"Device event class ID is something like 500123. Is this a valid signature ID or a bug?"

Issue the following SQL query against the SiteProtector database to determine whether the device event class ID is valid:

```
SELECT a.secchkid AS oldsecchkid, a.chkname, b.secchkid AS
newsecchkid
From securitychecks a, checkproducts b WHERE
a.chkname=b.productcheckname ORDER BY a.secchkid;
```

If OldSecChkID contains '500123' and its NewSecChkID field contains a value that is less than 500000, it is possibly a bug. On the other hand, if there is no entry for '500123' or the NewSecChkID field is same as OldSecChkID field, then this is not a bug in ArcSight code.

"The connector is doing Full GC repeatedly, and is running out of memory with an error message similar to: `Memory usage in red zone. (nextWait: 250, currentUsage: 99%, redZoneStartTime: 1275943555839, elapsed: 0ms)`**. After running out of memory, it automatically shuts down (software connector), or it keeps restarting (ConApp). What can I do to resolve this issue?"**

The number of database rows fetched by the connector is taking more memory than that assigned to the connector. The default JVM heap size is set to 256MB. To resolve this issue, you need to increase the JVM heap size of the connector to a value greater than 256MB.

For Windows:

- Create a file in the /user/agent directory, called `setmem.bat`.
- Add the following line to the file and save it: `set ARCSIGHT_MEM_OPTIONS= -Xms256m -Xmx1024m`
- Restart the connector

For other platforms:

- Create a file in the /user/agent directory, called `setmem.sh`.
- Add the following line to the file and save it: `ARCSIGHT_MEMORY_OPTIONS="  -Xms256m -Xmx1024m "`
- Restart the connector.

In both the cases, the -Xmx option has to be set to a value greater than 256m, for example -Xmx512m, -Xmx1024m.

"I cannot see the latest the dynamic event categorization information. What should I do?"

To see the latest information about categorization for dynamic events (all >500k SecChkIDs), IBM recommends running an update script once a month.

Use the following query to update dynamic event categorization:

```
UPDATE u
SET SecChkID = i.SecChkID
FROM UDSecurityChecks u
```

```
INNER JOIN (SELECT DISTINCT cp.SecChkID,
cp.ProductCheckName
FROM CheckProducts cp
INNER JOIN Algorithm a ON cp.AlgorithmID = a.AlgorithmID
AND a.NameSpace = 'PAM') i ON u.TagName =
i.ProductCheckName
WHERE u.SecChkID IS NULL
```

This script is provided as a convenience. Procedures can change at any time. If you have issues with this procedure, please contact IBM support or consult your product documentation.