opentext™

ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for IBM SiteProtector 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

Trademark Notices

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 IBM SiteProtector DB SmartConnector

Configuration Guide for IBM SiteProtector DB SmartConnector

This guide provides information for installing the SmartConnector for IBM SiteProtector DB 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

IBM 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.

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

Prerequisites

Access Requirements

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

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

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 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

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 SmartConnectorinstallation 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 **IBM SiteProtector DB** from the **Type** drop-down list and click **Next**.
10. Specify the following SmartConnector parameters, 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>. **Note:** If using Windows authentication append ;integratedSecurity=true to the end of the URL string. Note that you must use the name or instance of the database configured at installation/audit time. For example: jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true
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 either of the following optional parameters: **Payload Sampling:**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. **Sensor Response**. :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.

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 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 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*.

Configuring Advanced settings

To configure Payload Sampling to investigate the packet records data that triggered the security event, see Configuring Payload Sampling.

To know more about Turbo Mode, see Understanding Turbo Mode.

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. 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)

ArcSight ESM Field	Device-Specific Field
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
Device Payload ID	SensorDataID
Device Product	PRODUCT_NAME
Device Receipt Time	SensorDataAlertDateTime
Device Severity	AlertPriority

ArcSight ESM Field	Device-Specific Field
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

This section includes the following troubleshooting information:

The Connector is Unable to Reconnect to the MS SQL Server Database

In some cases, the connectors using MS SQL server databases are unable to reconnect to the database after losing and reacquiring network connection.

Workaround: Restart the connector.

Unable to Deploy SQL Server Native Client

In some cases, you might not be able to deploy an application that is dependent on SQL Server Native Client.

Workaround:

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.

Connection to SQL Server Fails or Hangs

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.

Workaround:

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.

Receive Error: Login failed for user 'sqluser'

If the user is not associated with a trusted SQL Server connection, the **Login failed for user 'sqluser'** error message is displayed.

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.

Workaround:

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.

The Connector becomes Clogged with Events after being Shut Down for a While

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.

Workaround:

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.

Receive Error: "Connector parameters did not pass the verification with error ..."

If you do not have the correct version of jar file, you might recieve this error message.

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.
- Earlier versions of the connector that run JRE 1.6 require sqljdbc4.jar.

Workaround:

If the connector faces issues in receiving events when MySQL JDBC Driver 5.1.38 is used, use MySQL JDBC driver 5.0.8 instead.

Unable to Determine whether the Device Event Class ID is Valid

Sometimes you might not be able to determine the Device Event Class ID such as 500123 is a valid signature ID or a bug.

Workaround:

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.

Connector is Running out of Memory with an Error Message: `Memory usage in red zone`

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).

Workaround:

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 256 MB. To resolve this issue, you need to increase the JVM heap size of the connector to a value greater than 256 MB.

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.

Unable to See the Latest Dynamic Event Categorization Information

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, contact IBM support or consult your product documentation.

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 IBM SiteProtector 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!