
Micro Focus Security

ArcSight Micro Focus Security

Software Version: 8.2.0

SmartConnector for Trend Micro Apex Central Multiple DB

Document Release Date: May 2021

Software Release Date: May 2021



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2021 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:

<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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

About this PDF Version of Online Help

This document is a PDF version of the online help. This PDF file is provided so you can easily print multiple topics from the help information or read the online help in PDF format. Because this content was originally created to be viewed as online help in a web browser, some topics may not be formatted properly. Some interactive topics may not be present in this PDF version. Those topics can be successfully printed from within the online help.

Document Revision History

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.

To check for recent updates or to verify that you are using the most recent edition of a document, go to [ArcSight Product Documentation Community on the Micro Focus Security Community](#).

Document Changes

Date	Product Version	Description
05/14/2021	8.2.0	First edition of this guide for new multiple database connector.

Contents

SmartConnector for Trend Micro Apex Central Multiple DB	7
Product Overview	8
Prerequisites	9
Downloading JDBC Driver	9
Installation Prerequisites	9
Installing the SmartConnector	10
Preparing to Install Connector	10
Installing the Core Software	10
Installing JDBC Driver	12
Installing JDBC Driver for Software Connectors	12
Installing JDBC Driver for Connector Appliance	12
Adding a JDBC Driver to the Connector Appliance or ArcSight Management Center ..	12
Configuring the JDBC Driver and Windows Authentication	13
Configuring the SmartConnector by Using the Wizard	14
Device Event Mapping to ArcSight Fields	16
Apex Central 6.0, and 6.0 SP1 OfficeScan Log Mappings	16
Apex Central 6.0, and 6.0 SP1 Spyware Event Mappings	17
Apex Central 6.0, and 6.0 SP1 Web Security Event Mappings	18
Apex Central 6.0, and 6.0 SP1 Security Log Mappings	19
Web Security Log Blocking Types	21
Web Security Log Protocols	22
Security Event Reason Codes	23
Troubleshooting	24

Send Documentation Feedback	26
-----------------------------------	----

SmartConnector for Trend Micro Apex Central Multiple DB

This guide provides information to install the SmartConnector for Trend Micro Apex Central Multiple DB and configure the device for database event collection. The following products are supported with Trend Micro Apex Central versions 6.0 and 6.0 SP1:

- OfficeScan Client/Server Edition versions 10.6, 10.0, 8.0, 8.4
- InterScan Messaging Security Suite version 7.
- ScanMail for Lotus Domino 5.5

Product Overview

Trend Micro Apex Central Database is a software management solution that lets other Trend Micro products report security events to a central SQL Server database. The SmartConnector for Trend Micro Apex Central DB lets you import Virus Log, Security Log, Web Security Log, and Office Scan Antivirus Log activity and alarm events (generated and stored in the SQL Server database by Trend Micro Apex Central) into the ArcSight system.

The following Trend Micro Apex Central products are supported:

- **OfficeScan Client/Server Edition:**

It protects enterprise networks from viruses, Trojans, worms, hackers, and network viruses, plus spyware and mixed threat attacks.

- **InterScan Messaging Security Suite:**

It integrates high-performance antivirus and content filtering security plus the optional Trend Micro Spam Prevention Solution with anti-spam and anti-phishing, all in a single platform at the Internet messaging gateway.

- **ScanMail for Lotus Domino:**

It offers comprehensive virus protection and content security for the Lotus/Domino environments, providing real-time scanning for viruses, adware, and spyware hidden within email attachments and databases. It prevents viruses and other malicious code from entering your Domino environment.

Prerequisites

Downloading JDBC Driver

The connector requires JDBC driver to be present. To download the MS SQL Server JDBC Driver, see: <http://msdn.microsoft.com/en-us/sqlserver/aa937724>

During the SmartConnector installation process, you will be directed to leave the wizard and copy the JDBC driver file you download to a SmartConnector folder.



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.

Installation Prerequisites

Refer to the following table to download the JDBC driver and the jar files depending on the JRE version that the connector uses:

JAR File Version	JRE Version	JAR File Name
7.2.1 and later	1.8	sqljdbc42.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
7.1.2 and later	1.7	sqljdbc41.jar (available with Microsoft JDBC Driver 6.0 for SQL Server)
Earlier versions	1.6	sqljdbc4.jar (available with Microsoft JDBC Driver 4.0 for SQL Server)

Installing the SmartConnector

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

Micro Focus 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 Connector

Before you install any SmartConnectors, make sure that the Micro Focus 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* guide, available on [ArcSight Documentation](#).

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 from "[Specify the relevant Global Parameters, when prompted.](#)" on page 14.

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 the 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.
3. 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...

4. Exit from the installation wizard.
5. Depending on SmartConnector you can proceed with one of the following options:
 - [Installing JDBC Driver](#)
 - [Installing JDBC Driver for Software Connectors](#)
 - [Installing JDBC Driver for Connector Appliance](#)
 - [Configuring the SmartConnector by Using the Wizard](#)

Installing JDBC Driver

1. Copy the jar file you downloaded earlier (see ["Downloading JDBC Driver" on page 9](#)) to \$ARCSIGHT_HOME/current/user/agent/lib.
2. Go to \$ARCSIGHT_HOME/current/bin and double-click runagentsetup to return to the SmartConnector Configuration Wizard.

Installing JDBC Driver for Software Connectors

1. Copy the jar file that is 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.
2. Copy the only jar file that is associated with the version of the driver to be installed to this location.

Installing JDBC Driver for Connector Appliance

Adding a JDBC Driver to the Connector Appliance or 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 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*.



Note: Refer to the *Installing and Configuring the SmartConnector* section to know more about the descriptions of parameters to be entered during connector configuration.

Configuring 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.



Note: 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.



Note: 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:

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



Note: Use the name or instance of the database configured during installation or auditing.

4. Complete the remaining connector wizard configuration steps.
5. If running on a Windows Server, change the service account to use the Windows account that is configured to login to the database. The Connector will use the account to start the service, regardless of the account value setting entered in the connector setup process.

Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the Trend Micro Apex Central Multiple DB Connector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the Trend Micro Apex Central Multiple DB Connector:

1. Start the installation wizard.
2. Follow the instructions in the wizard to install the core software.
3. Download SQL Server JDBC Driver.
 - a. To download a Microsoft SQL Server JDBC driver, click **Cancel** to exit the configuration wizard and copy the jar file you downloaded earlier (see "[Downloading JDBC Driver](#)" on [page 9](#)) to \$ARCSIGHT_HOME/current/user/agent/lib.
 - b. Go to \$ARCSIGHT_HOME/current/bin and double-click runagentsetup to return to the SmartConnector Configuration Wizard.
4. Specify the relevant [Global Parameters](#), when prompted.
5. From the **Type** drop-down list, select **Trend Micro Apex Central Multiple DB** as the type of connector, then click **Next**.
6. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.
7. Enter the device details:

Parameter	Description
JDBC/ODBC Driver	Select the 'com.microsoft.sqlserver.jdbc.SQLServerDriver' driver.
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>. The default Trend Micro database name is 'db_ControlManager'.
User	Enter the login name of the database user with database privilege.
Password	Enter the password for the authorized database user.

8. Select a [destination and configure parameters](#).
9. Specify a name for the connector.
10. Select whether you want to [run the connector as a service or in the standalone mode](#).
11. Complete the installation.
12. [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.

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.

Apex Central 6.0, and 6.0 SP1 OfficeScan Log Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	AggregatedCount
Connector Severity	Very High = Critical; Medium = Error or Warning; Low = Unknown or Information
Destination Host Name	TrendMicroHostName (VLF_InfectionDestination)
Destination User Name	TrendMicroUser (One of (VLF_InfectionDestination, FVL_LoginUser))
Device Action	VLF_FirstAction (0 = Unknown, 1 = NA, 2 = Clean, 3 = Delete, 4 = Move, 5 = Rename, 6 = Pass, 7 = Strip, 8 = Drop, 9 = Quarantine, 10 = Replace, 11 = Archive, 12 = Stamp)
Device Custom Date 1	CLF_LogGenerationTime
Device Custom Number 1	VLF_PatternNumber
Device Custom Number 2	VLF_SecondAction
Device Custom String 1	VLF_Virus Name
Device Custom String 2	VLF_EngineVersion
Device Custom String 3	CLF_ProductVersion
Device Custom String 4	CLF_ReasonCode
Device Custom String 5	VLF_FirstActionResult
Device Custom String 6	VLF_SecondActionResult
Device Event Category	CLF_MsgLogType
Device Event Class ID	Both ("AV", VLF_FirstAction)
Device Host Name	CLF_ComputerName
Device Product	One of ("ScanMail for Lotus Domino","Apex Central")
Device Receipt Time	CLF_LogReceivedTime

ArcSight ESM Field	Device-Specific Field
Device Severity	CLF_Severity Code (0 = Unknown, 1 = Information, 2 = Warning, 3 = Error, 4 = Critical)
Device Vendor	'Trend Micro'
Device Version	One of (Product_Version,"5.0/5.5/6.0 SP1")
External ID	ID
File Name	VLF_FileName
File Path	VLF_FilePath
Message	VLF_FileNameInCompressedFile
Name	VLF_VirusName
Source Host Name	TrendMicroHostName (VLF_InfectionSource)
Source User Name	TrendMicroUser (VLF_InfectionSource)

Apex Central 6.0, and 6.0 SP1 Spyware Event Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	AggregatedCount
Connector Severity	Very High = Critical; Medium = Error, Warning; Low = Unknown, Information
Destination Host Name	InfectionDestination
Device Custom Date 1	LogGenLocalDatetime
Device Custom Number 1	PatternType
Device Custom String 1	VirusName
Device Custom String 2	EngineVersion
Device Custom String 5	ActionResult
Device Custom String 6	PatternVersion
Device Event Category	MsgLogType
Device Event Class ID	'Spyware Detected'
Device Host Name	ComputerName
Device Product	'Apex Central'
Device Receipt Time	LogReceived Time
Device Vendor	'Trend Micro'

ArcSight ESM Field	Device-Specific Field
Device Version	'5.0'
External ID	ID
File Name	FileName
File Path	FileName
Name	'Spyware Detected'

Apex Central 6.0, and 6.0 SP1 Web Security Event Mappings

ArcSight ESM Field	Device-Specific Field
Application Protocol	SLF_Protocol
Base Event Count	AggregatedCount
Connector Severity	Very High = Critical; Medium = Error or Warning; Low = Unknown or Information
Destination Address	SLF_ServerIP
Destination Port	SLF_ServerPort
Device Action	SLF_Action (0=Unknown, 1=Pass, 2=Block)
Device Custom Date 1	CLF_LogGenerationTime
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom IPv6 Address 3	Destination IPv6 Address
Device Custom String 1	SLF_PolicyName
Device Custom String 4	CLF_ReasonCode
Device Custom String 5	CLF_ReasonCodeSource
Device Direction	SLF_Direction
Device Event Category	SLF_BlockingType
Device Event Class ID	Both("WB", SLF_BlockingType)
Device Host Name	CLF_ComputerName
Device Product	'Apex Central'
Device Receipt Time	CLF_LogReceivedTime

ArcSight ESM Field	Device-Specific Field
Device Severity	CLF_SeverityCode (0=Unknown, 1=Information, 2=Warning, 3=Error, 4=Critical)
Device Vendor	'Trend Micro'
Device Version	'5.0'
External ID	ID
File Name	SLF_FileName
Name	One of (SLF_BlockingRule, SLF_BlockingType)
Request URL	SLF_ObjectNameURL
Source Address	SLF_ClientIP

Apex Central 6.0, and 6.0 SP1 Security Log Mappings

ArcSight ESM Field	Device-Specific Field
Base Event Count	AggregatedCount
Connector Severity	Very High = Critical; Medium = Error or Warning; Low = Information
Destination Host Name	TrendMicroHostName (SL_Recipient)
Destination User Name	One of (Extracted from SL_Recipient , TrendMicroUser (SL_Recipient))
Device Action	SL_FilterAction (0=Unknown, 1=NA, 2=Deliver, 3=Delete, 4=Quarantine, 5=Postpone, 6=Forward, 7=Replace, 8=Archive, 100=Strip, 101=Pass)
Device Custom Date 1	CLF_LogGenerationTime
Device Custom String 1	SL_PolicyContent
Device Custom String 2	CLF_ProductVersion
Device Custom String 3	SL_FilterType (0=Unknown, 1=ContentFilter, 2=AttachmentFilter, 3=StandardFilter, 4=SizeFilter, 5=DisclaimerMgr, 6=SpamFilter, 7=OPP, 8=ImportFilter, 9=PhishingFilter, 10=UrlReputationFilter)
Device Custom String 4	CLF_ReasonCode
Device Custom String 5	CLF_ReasonCodeSource
Device Custom String 6	SL_MessageAction (0=Unknown, 1=NA, 2=Deliver, 3=Delete, 4=Quarantine, 5=Postpone, 6=Forward, 7=Replace, 8=Archive, 100=Strip, 101=Pass)
Device Event Category	CLF_MsgLogType
Device Event Class ID	Both("MS", SL_FilterAction)

SmartConnector for Trend Micro Apex Central Multiple DB

Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Host Name	CLF_ComputerName
Device Product	'Apex Central'
Device Receipt Time	CLF_LogReceivedTime
Device Severity	CLF_ServerityCode (0=Unknown, 1=Information, 2=Warning, 3=Error, 4=Critical)
Device Vendor	'Trend Micro'
Device Version	'5.0'
External ID	ID
File Name	SL_FileName
Message	One of (SL_ViolationDescription, SL_Subject)
Name	SL_PolicyName
Source Host Name	TrendMicroHostName (SL_Sender)
Source User Name	One of (Extracted from SL_Sender , TrendMicroUser (SL_Sender))

Web Security Log Blocking Types

0	Unknown	1	Filename	2	WebMailSite
3	WebServer	4	UrlPattern	5	JavaVbScript
6	TrueFiletype	7	UserDefine	8	ServerDefine
9	WebPolicy	11	PhishPhish	12	PhishSpyware
13	PhishVirusAccomplice	14	PhishForgedSignature	15	PhishDiseaseVector
16	PhishMalApplet	17	PhishReputation	20	PolicyIpTranslate
21	PolicyJavaScan	22	PolicyMmc	31	Pharming
32	UrlBlocking	33	UrlFiltering	34	ClientIpBlocking
35	DestinationPortBlocking	36	WebReputation	41	UnsupportedFileType
42	ExceedFileCountLimit	43	ExceedFileSizeLimit	44	ExceedDecompressLayerLimit
45	ExceedDecompressTimeLimit	46	ExceedCompressionRatioLimit	47	PasswordProtectedFile
48	RestrictedSpywareType	60	StringPattern	-1	VirusMalware
-2	SpywareGrayware	-3	NetworkVirus	-4	Intellitrapp
-5	SuspiciousVirusMalware	-6	SuspiciousSpywareGrayware	-7	Fraud
-8	SuspiciousBehavior				

Web Security Log Protocols

0	UNKNOWN	1	SMTP	2	POP3
3	IRC	4	DNS	5	HTTP
6	FTP	7	TFTP	8	SMB
9	MSN	10	AIM	11	YMSG
12	GMAIL	13	YAHOO_MAIL	14	HOTMAIL
15	RDP	16	DHCP	17	TELNET
18	LDAP	19	FILE_TRANSFER	20	SSH
21	DAMEWARE	22	VNC	23	CISCO_TELNET
24	KERBEROS	25	DCE_RPC	26	SQL
27	PCANYWHERE	28	ICMP	29	SNMP
30	VIRUS_PATTERN_TCP	31	VIRUS_PATTERN_UDP	32	HTTPS
256	BITTORRENT	257	KAZAA	258	LIMEWARE
259	BEARSHARE	260	BLUBSTER	261	EDONKEY_EMULE
262	EDONKEY2000	263	FILEZILLA	264	GNUCLEUS
265	GNUTELLA	266	WINNYLLA	268	MORPHEUS
269	NAPTER	270	SHAREAZA	271	WINMX
272	MLDONKEY	273	DIRECT_CONNECT	274	SOULSEEK
275	OPENNAP	276	KURO	277	IMESH
278	SKYPE	279	GOOGLE_TALK	10001	IP
10002	ARP	10003	TCP	10004	UDP
10005	IGMP				

Security Event Reason Codes

-1	EMPTY	0	UNKNOWN
1	VSAPI_SCAN_ENGINE	2	VSAPI_SCAN_ENGINE_SECOND
3	VSAPI_SCAN_PATTERN	4	VSAPI_SCAN_PATTERN_SECOND
5	MTA	6	SMTP_SERVER
7	HTTP_SERVER	8	FTP_SERVER
9	SCAN_MODULE	10	TVCS_AGENT
11	FIREWALL_MODULE	12	FIREWALL_PATTERN
13	ANTISPAM_FILTER	14	CONTENT_FILTER
15	ATTACHMENT_FILTER	16	DISCLAIMER_FILTER
17	ACTIVEUPDATE	18	HOOK_MODULE
19	NOTIFICATION_MODULE	20	LOG_MODULE
21	POLICY_MODULE	22	VSAPI2_SCAN_ENGINE
23	VSAPI2_SCAN_ENGINE_SECOND	24	VSAPI2_SCAN_PATTERN
25	VSAPI2_SCAN_PATTERN_SECOND	26	CAV_LITE_SCAN_PATTERN
27	CAV_LITE_SCAN_PATTERN_SECOND	28	TSC_SCAN_ENGINE
29	TSC_SCAN_PATTERN	30	PRODUCT_REGISTRY_MODULE
31	DAMAGE_CLEANUP_ENGINE	32	DAMAGE_CLEANUP_TEMPLATE
33	VA_PATTERN	34	VA_ENGINE
35	ASPY_PATTERN	36	ASPY_ENGINE
37	SSAPI_ENGINE	38	SSAPI_PATTERN
39	UFE_ENGINE	40	UFEF_PATTERN
41	UFEP_PATTERN	42	FPGA_ENGINE
43	NCIT_ENGINE	44	VSAPI_PLUS_ENGINE

Troubleshooting

Issue: Unable to 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.

Workaround: Restart the connector to resolve this issue.

Issue: 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.

Issue: Connection to SQL Server fails/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.

Issue: The user is not associated with a trusted SQL Server connection. Receives error message: Login failed for user 'sqluser'

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.

Issue: The connector gets clogged with events after shut down

Workaround: 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`. 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 SmartConnector for Trend Micro Apex Central Multiple DB (Micro Focus Security ArcSight Connectors 8.2.0)

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 Documentation-Feedback@microfocus.com.

We appreciate your feedback!