



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Microsoft IIS 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

Product Overview	4
Configuring the IIS Server	5
Configuring Remote Logging	7
Configuring IIS to Log Data on a Remote Share	7
Configuring Permissions for Remote Logging	8
Running the Connector as a Service Accessing Remote Files	9
Saving Log Files	9
Setting Up Remote Mount Point on UNIX	11
Installing the SmartConnector	12
Installing and Configuring the SmartConnector by Using the Wizard	12
Additional Configuration	15
Requesting URL Field too Long and Truncated	15
Changing Log File Name Prefix	15
Specifying File Name Suffix	15
Specifying the Locale Used for Determining the Current Date for File Names	16
Processing Threshold and Monitoring Interval	16
Device Event Mapping to ArcSight Fields	18
IIS Event Mappings	18
Troubleshooting	20
Send Documentation Feedback	21

Product Overview

Microsoft Information Internet Services (IIS) is a web server application and set of feature extension modules created by Microsoft for use with Microsoft Windows. IIS 8.5 supports HTTP, HTTPS, FTP, FTPS, SMTP, and NNTP. Microsoft IIS is not turned on by default when Windows is installed. The SmartConnector for Microsoft IIS Multiple Server File allows you to 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 Multiple Server File retrieves logs from multiple site folders in multiple servers. Enter parameters for each server independently.



In order to access the IIS logs when running the connector on Linux platforms, the log folder on the Windows host must first be made available through NFS (by installing the "UNIX Services for Windows" networking component). Alternatively, if **smbclient** software is installed on the UNIX machine, the IIS log folder should be shared out using the usual Windows method and mounted on the UNIX host first, using **smbclient** and suitable credentials.

If you are running the connector on Linux platform, to access IIS logs, do one of the following:

- Install the **UNIX Services for Windows** networking component to make the log folder on the Windows host available through NFS.
- Install the **smbclient** software on the UNIX machine. Mount the IIS log folder on the UNIX host using **smbclient** and suitable credentials, then share the folder using the usual Windows method.

Configuring the IIS Server

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. To configure logging at the site level, go to **Features View**, then double-click **Logging**.
 - To configure 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.
 - To configure 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)



If the following issue occurs while using IIS advanced logging: Incorrect format, expected [x] tokens, found [x], then refer to "[Troubleshooting](#)" on page 20 for the solution.

5. Under **Directory**, specify the path where the log file must 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 the time periods to determine when a new log file is to be created: **Hourly**, **Daily**, **Weekly**, or **Monthly**.
 - **Maximum file size (in bytes):** A log file is created when the file size reaches the specified maximum value. If this attribute is set to a value less than 1048576 bytes, the default value is implicitly 7 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.

Configuring 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 as the services run in a virtual network and cannot recognize mapped drives.



Note 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 website. For example, **W3SVCX**, where X is a random number generated by IIS to represent the specific website. IIS also creates the log file with exclusive write access, so that multiple machines cannot write to the same log file. Specify the folder in which these files can be found. For example, if you specify the following:

```
\IIS\logfiles\W3SVCx...
```

The connector looks 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.

Configuring IIS to Log Data on a Remote Share

To log website 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 that 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 "[Configuring Permissions for Remote Logging](#)" below.
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\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 websites 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.

Configuring 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**.

Running the Connector as a Service Accessing Remote Files

To run the SmartConnector as a service on Windows to access remote files, create a user with appropriate access.

1. From the Windows **Start** menu, select **Settings > Control Panel > Administrative Tools > Services**.
2. Select the SmartConnector service and right-click to select **Properties**.
3. Click the **Log On** tab.
4. Select to **Log on as: This account**, then enter the user account name with appropriate privilege to access the remote machine or machines, along with the **Password** and password confirmation.
5. Click **OK** for your changes to take effect and to close the **Properties** window.

Saving Log Files

By default, IIS creates a new log file for each website 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 must be saved. For information about saving log files on a remote share, see "["Configuring Remote Logging" on page 7](#)".
5. Click **Apply** and then click **OK** twice.

Setting Up Remote Mount Point on UNIX

From the Connector Appliance console:

1. Go to **Setup > System Admin > Remote File Systems**, create two remote mount points (created by default under /opt/mnt), with credentials to access those remote directories:
>> W3SVC1, CIFS, //xxx/y (remote share #1)
>> W3SVC2, CIFS, //xxx/z (remote share #2)
2. From **Manage**, select a container and select **Add a connector**. Select the Microsoft IIS Multiple Server File connector.
3. During the connector setup, click **Add Row** and enter /opt/mnt in the **Log Folder** field.
4. Set **Latest Log Only** to **true**.

With this configuration, the connector specifically looks for folders in /opt/mnt that are prefixed with W3SVC# (and then it uses the mount and related credentials set above to access those files).

Installing the SmartConnector

The following sections provide instructions for installing and configuring the Microsoft IIS Multiple Server 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, ensure that you have the following:

- Register an app in [Azure Active Directory](#) with Microsoft threat protection - **Incident.Read.All** permission.
- Application (Client) ID, Directory (Tenant) ID, and Client Secret.

Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the Microsoft IIS Multiple Server File Connector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the Microsoft IIS Multiple Server File 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 IIS Multiple Server File** as the type of connector, then click **Next**.
5. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.
6. Enter the device details for each IIS server you want to monitor:

Parameter	Description
Log Folder	<p>Enter the full path to the folder which contains the server log files. This directory must contain all sub-directories of the websites hosted on IIS (you can obtain this value from the Properties window of any these websites).</p> <p>To log 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 specify a full path statement in Log File Directory, then the default path will be used. For example, if you enter IISLogFile in Log File Directory, it indicates that the file is located at the following location: systemroot\System32\IISLogFile.</p> <p>You can modify this path if you want to change the log file directory for further configuration. This parameter is available in the agent.properties file at the following locations:</p> <ul style="list-style-type: none">• The remote server log file is at: \\MyLogServer\LogShare\W3SVC1, then enter it as agents[0].foldertable[0].folder=\\MyLogServer\\LogShare.• The local log file is at: C:\inetpub\logs\LogFiles\W3SVC1, then enter it as agents[0].foldertable[0].folder=C:\\inetpub\\logs\\LogFiles.
Wildcard	<p>Enter a wildcard that identifies the files to process. With IIS version 7, the default log file encoding scheme is UTF-8. For the earlier IIS versions, the default log file encoding scheme was ANSI, and the log file name would start with "ex". You must use:</p> <ul style="list-style-type: none">• u_ex*.log for UTF-8 file name scheme.• ex*.log for the ANSI log file name scheme.• httperr*.log to parse Microsoft Exchange IIS logs. <p>For more information about encoding, file name prefix, and file name suffix, see "Additional Configuration" on page 15.</p>
Encoding	Add encoding that identifies the files to process.
Latest Log Only	Select true or false . If you select true , only the log file with the latest times tamp in a site folder (such as W3VCX) are processed when connection is initiated. Otherwise, all log files are processed.



Note:

- Click **Export** to export the host name data that you have entered in the table to a CSV file.
- Click **Import** to import a CSV file data into the table instead of adding it manually.

For more information, see [SmartConnector Installation and User Guide](#).

7. Select a [destination and configure parameters](#).
8. Specify a name for the connector.
9. (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.

10. Select whether you want to install 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 [Installation and User Guide for SmartConnector](#).

Additional Configuration

Requesting URL Field too Long and Truncated

If the value Request Url is too long and truncated, you must manually add the following parameters to the agent.properties file:

```
size.validation.fields=requestUrl  
size.validation.sizes=10000
```

Changing 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 earlier 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 modify the connector's advanced parameters:

1. Open the agent.properties file located at \$ARCSIGHT_HOME\current\user\agent and edit the logfile.name.prefix:
 - For the **UTF-8** file name scheme, change the value to **u_ex**.
 - For the **ANSI** log file name scheme, change the value to **ex**.
2. Save the file and restart the connector for your changes to take effect.

Specifying 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

Specifying the Locale Used for Determining the Current Date for File Names

An internal 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 must be set to `en_US`.

To set advanced parameters for your SmartConnector, after connector installation:

1. Open the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`.
2. Locate the `localeforfilename` parameter and set its value to `en_US`.
3. Save the file and restart the connector for your changes to take effect.

Processing Threshold and Monitoring Interval

Parameters can be adjusted to control how long and how often the log file continues to be monitored for additions. The values are in milliseconds; `monitorinterval` is set to 1 minute by default and `processingthreshold` is set to 1 hour (3600000 milliseconds) by default. With a processing threshold of 24, the file will be marked as 'processed' only after 24 hours, which is a change from previous behavior.

When the `processingthreshold` parameter is set to a negative value (such as "-1"), the connector processes and deletes or persists the log file according to the mode set in the parameters for all files but the most recent. The most recent file is considered to be current and continues being watched. If you want to stop watching the most recent file in the

directory, set the **processingthreshold** to a positive value, such as 24 hours, to be sure the file is no longer updated.

The **monitorinterval** value determines how often the connector checks to determine whether the file was updated; the checking starts after all records in a file have been read and processed. The monitor interval should be less than the processing threshold. For example, the monitor interval could be 5 minutes and the processing threshold could be a few hours. Both values are specified in milliseconds.

There are a maximum of 256 reading threads per folder and the thread is assigned to the log file until the threshold time is passed. If there are a few files per folder, there is no problem. However, if there are 256 or more files in a folder, either the JVM memory and the parameter for the number of threads should be increased, or the **processingthreshold** parameter adjusted to a smaller value, or set to -1, which marks the files as 'processed' when read to the end.

To change the **processingthreshold parameter value, after connector installation:**

1. Open the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`.
2. Locate the **processingthreshold** parameter and set the value accordingly.
3. Save the file and restart the connector for your changes to take effect.

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	cs-host
Destination Host Name	cs-host
Destination Port	One of (s-port, cs-host)
Device Address	s-ip
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 HostName	s-computername
Device Process Name	s-sitename
Device Product	'Internet Information Server'
Device Receipt Time	date, time

Configuration Guide for Microsoft IIS Multiple Server 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	oneOf (c-ip, X-Forwarded-For)
Source Port	c-port
Source User Name	cs-username

Troubleshooting

Issue: Install the ArcSight SmartConnector in a separate machine to set up a share on an IIS machine so the ArcSight SmartConnector can read the logs from that share

Workaround: If your IIS version is 6.0 or later, 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 rather than the drive letter to point to the share.

If you want 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 rather than the drive letter to point to the share.
- Add the domain user to the Local Admin group so that the service can be started by the domain user.

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.

Issue while using IIS advanced logging

Issue: When you use the IIS advanced logging feature and encounter this issue: Incorrect format, expected [x] tokens, found [x]

Workaround: In the **Selected Fields** list, select the **URI Stem (cs-uri-stem)** logging field name, click **Move Down**, and then change its position to the end of the list.

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 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 IIS Multiple Site 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 Guidefor Microsoft IIS Multiple Site 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	15
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 Multiple Site File SmartConnector

This guide provides information for installing the SmartConnector for Microsoft IIS Multiple Site File and configuring the device for log file 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 SmartConnector for Microsoft IIS Single Server Multiple Site File lets you import activity and alarm events generated and stored in a log file by Microsoft IIS into the ArcSight ESM system.

There are three Microsoft IIS log file connectors:

- The SmartConnector for Microsoft IIS File retrieves logs from one web site per IIS server. File patterns are comma delimited and support different rotation patterns.
- The SmartConnector for Microsoft IIS Multiple Site File (this connector) retrieves logs from multiple web sites running on one physical IIS Server. All of those sites are under one folder that is checked recursively, drilling down to sites. Install one Microsoft IIS Multiple Site File connector per IIS server. The number of sites hosted per server is not important. Each site hosted by a single IIS server logs events to a distinct W3SVCx sub-folder on that server (or wherever it is configured to post logs.) The IIS Multiple Site connector is designed to process multiple W3SVCx log files in parallel.
- The SmartConnector for Microsoft IIS Multiple Server File can retrieve logs from multiple site folders in multiple servers. Enter parameters for each server independently.
- The SmartConnector for Microsoft IIS Multiple Server File only works on a Windows Platform.

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 `\servername\LogFiles` where *servername* 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 OpenText SSO.

- 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.

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 IIS Multiple Site File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Log Folder	Enter the full path to the folder containing the log files. This directory should be the directory that contains all the subdirectories for the web sites (you can obtain this value from any web site's Properties window). See step 9 in "Enabling Logging" for more information. To log 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:

Parameter	Description
	- If the remote server log file is at: \\MyLogServer\LogShare\W3SVC1, then set agents[0].logfilehome =\\MyLogServer\\LogShare
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.

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.

Install the SmartConnector

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 internal 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`. Save the file and 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
Device Severity	sc-status

Configuration Guide for Microsoft IIS Multiple Site File SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
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 SmartConnector in a separate machine; what are the steps for me to set up a share on an IIS machine so the ArcSight SmartConnector can read the logs from that share?

If your IIS version is 6.0 or later, 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 rather than the drive letter to point to the share.

If you want 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 rather than the drive letter to point to the share.
- Add the domain user to the Local Admin group so that 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 Multiple Site 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 IIS Syslog 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 Guidefor Microsoft IIS Syslog SmartConnector	4
Product Overview	5
Configuration	6
SyslogAgent Configuration	6
Configure the Syslog SmartConnectors	8
The Syslog Daemon SmartConnector	8
The Syslog Pipe and File SmartConnectors	9
Configure the Syslog Pipe or File SmartConnector	9
Install the SmartConnector	11
Syslog Installation	11
Prepare to Install Connector	11
Install Core Software	12
Set Global Parameters (optional)	12
Select Connector and Add Parameter Information	13
Select a Destination	15
Complete Installation and Configuration	15
Run the SmartConnector	17
Device Event Mapping to ArcSight Fields	18
IIS Event Mappings	18
Send Documentation Feedback	20

Configuration Guidefor Microsoft IIS Syslog SmartConnector

This guide provides information for installing the SmartConnector for Microsoft IIS Syslog and configuring the device for event collection. This SmartConnector is supported for installation on Windows platforms only. For more information, 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 Microsoft Internet Information Server (IIS) helps organizations increase Web site and application availability while lowering system administration costs. Microsoft IIS can send its application events to the Datagram SyslogAgent, which, in turn, sends event logs and application logs to a Datagram SyslogServer.

The Datagram SyslogAgent is installed as a service on Microsoft Windows clients and servers to provide syslog compatibility. It is based upon NTSyslog by SaberNet.net, which released it under the GNU license. The entries in the Event log (and, when specified, the Application logs) are sent to the Datagram SyslogServer.

Configuration

For the syslog connector, there is no log file to read to get the format when logged to the syslog server. Because the format is required for the connector to pull events, ArcSight recommends stopping the syslog service before running the SmartConnector, then restarting the syslog service for the connector to be able to get the format and begin processing events.

SyslogAgent Configuration

For complete installation and configuration information for Datagram SyslogAgent and SyslogServer, see <http://www.syslogserver.com/manuals.html>.

Datagram SyslogAgent supports forwarding of application logs to SyslogServer. By default, no application logging is configured.

Notes:

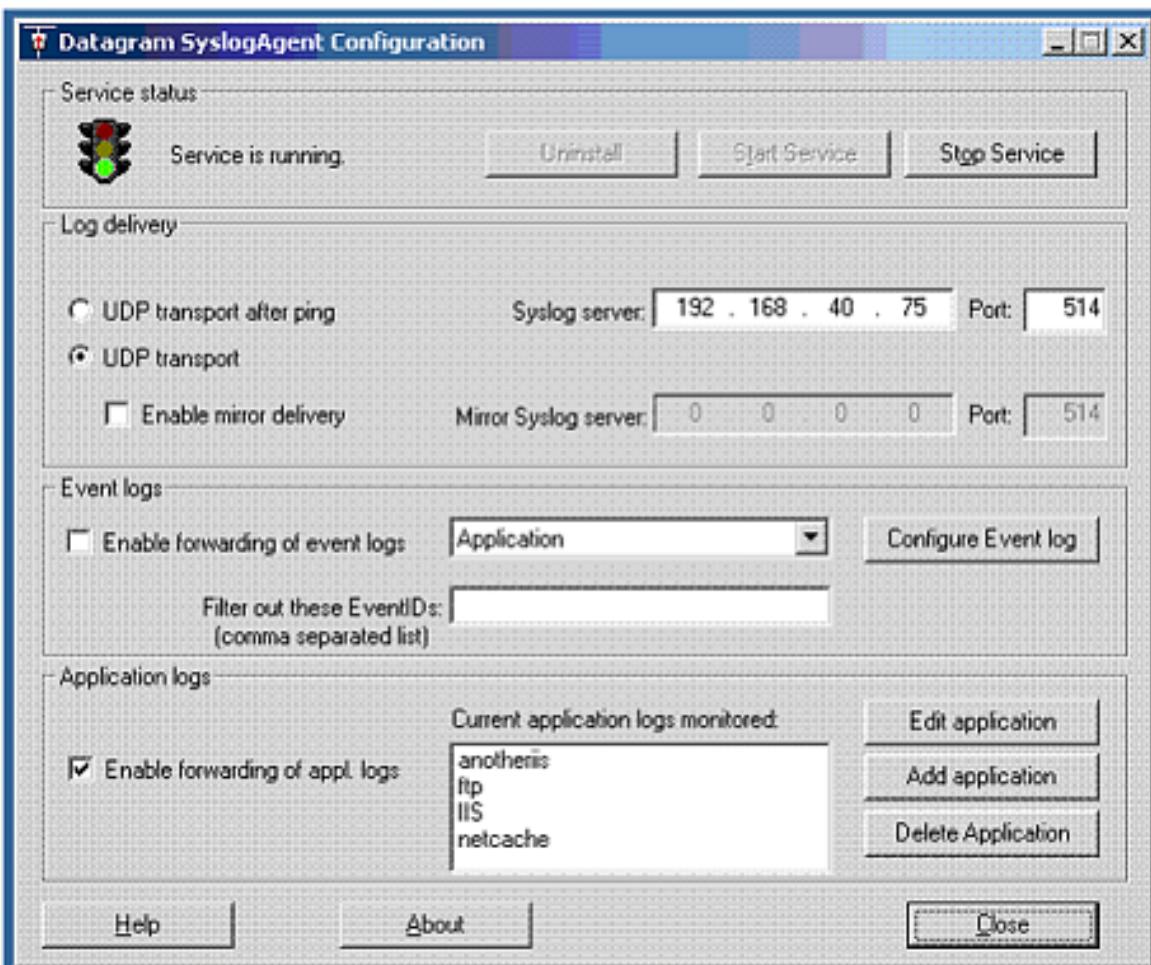
- The maximum number of configured application logs is ten; if more logs are configured, event loss can occur.
- If Application logs have the same number of tokens in the format line, incorrect mapping of event content can occur.

To enable application log forwarding for Microsoft IIS:

- 1 Open the Datagram SyslogAgent Configuration window.

Configuration Guide for Microsoft IIS Syslog SmartConnector

SyslogAgent Configuration



- 2 Under "Log delivery," be sure the IP address and port for the syslog server has been entered.
- 3 Under "Event logs," check the box for "Enable forwarding of event logs" and leave the default value of Application selected.
- 4 Under "Application logs," click on **Edit Application** or **Add Application** to open the **Configure application logging** window.
- 5 Configure the process name as `datagram_iis_syslog` ("Parse process name, or use").
- 6 For Severity, select **Information**.
- 7 Under "Syslog protocol conformity," make sure no boxes are checked.
- 8 Under "Ignore settings," make sure no boxes are checked.
- 9 After confirming your changes, a dialog box is displayed to ask whether to restart the service. Accept to restart for your changes to take effect.

Further syslog configuration can be accomplished from the Syslogserver Configuration Properties window once the syslog service has been installed and started.

Configure the Syslog SmartConnectors

The three ArcSight Syslog SmartConnectors are:

- Syslog Daemon
- Syslog Pipe
- Syslog File

The Syslog Daemon SmartConnector

The Syslog Daemon 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 (configurable) by default that can be used to receive syslog events. Use of the TCP protocol or a different port can be configured manually.

If you are using SmartConnector for Syslog Daemon, add the following statement in the `rsyslog.conf` file to forward Oracle Audit events so that Syslog Daemon will start receiving events: `*.* @@(remote/local-host-IP):514`

Sample example: `local1.warning @@10.0.0.1:514`



You can either use `*.*` to read all Syslog events or you can filter specific events by replacing regex with the specific event name. For example: `*.* @@(remote/local-host-IP):514` and `local1.warning @@10.0.0.1:514`



Use `@@` to send events over a TCP connection and use `@` to send events over an UDP connection.

If you are running SmartConnector for Syslog Daemon on the same machine as the Oracle 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 may be split into multiple messages on syslog daemon; no such restriction exists on syslog file or pipe.

The 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 (`/etc/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. Therefore, you must do 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.

Configure the Syslog Pipe or File SmartConnector

This section provides information about how 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. First, create a pipe or a file; then modify the **/etc/rsyslog.conf** file to send events to it.

For syslog pipe:

- 1 Create a pipe by executing the following command:

```
mkfifo /var/tmp/syspipe
```

- 2 Add the following line to your **/etc/rsyslog.conf** file:

```
*.debug /var/tmp/syspipe
```

or

```
*.debug |/var/tmp/syspipe
```

depending on your operating system.

- 3** After you have modified the file, restart the syslog daemon either by executing the scripts **/etc/init.d/syslogd stop** and **/etc/init.d/syslogd start**, or by sending a `configuration restart` signal.

On RedHat Linux, you would execute:

```
service syslog restart
```

On Solaris, you would execute:

```
kill -HUP `cat /var/run/syslog.pid`
```

This command forces the syslog daemon to reload the configuration and start writing to the pipe you just created.

For syslog file:

Create a file or use the default for the file into which log messages are to be written.

After editing the **/etc/rsyslog.conf** file, be sure to restart the syslog daemon as described above.

When you follow the SmartConnector Installation Wizard, you will be prompted for the absolute path to the syslog file or pipe you created.

Install the SmartConnector

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

Syslog Installation

Install this SmartConnector (on the syslog server or servers identified in the *Configuration* section) using the SmartConnector Installation Wizard appropriate for your operating system. The wizard will guide you through the installation process. When prompted, select one of the following **Syslog** connectors (see *Configure the Syslog SmartConnectors* in this guide for more information):

Syslog Daemon

Syslog Pipe

Syslog File

Because all syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, the name of the specific syslog SmartConnector you are installing is not required during installation.

The syslog daemon connector by default listens on port 514 (configurable) for UDP syslog events; you can configure the port number or use of the TCP protocol manually. The syslog pipe and syslog file connectors read events from a system pipe or file, respectively. Select the one that best fits your syslog infrastructure setup.

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.



When installing a syslog daemon SmartConnector in a UNIX environment, run the executable as 'root' user.

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'.

Install the SmartConnector

Parameter	Setting
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 **Syslog daemon, pipe, or file and click **Next**.****3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.**

Syslog Daemon Parameters	<i>Network port</i>	The SmartConnector for Syslog Daemon listens for syslog events from this port.
	<i>IP Address</i>	The SmartConnector for Syslog Daemon listens for syslog events only from this IP address (accept the default (ALL) to bind to all available IP addresses).
	<i>Protocol</i>	The SmartConnector for Syslog Daemon uses the selected protocol (UDP or Raw TCP) to receive incoming messages.
	<i>Forwarder</i>	Change this parameter to 'true' only if the events being processed are coming from another SmartConnector sending to a CEF Syslog destination, and that destination also has CEF forwarder mode enabled. That allows attributes of the original connector to be retained in the original agent fields.
Syslog Pipe Parameter	<i>Pipe Absolute Path Name</i>	Absolute path to the pipe, or accept the default: /var/tmp/syspipe
Syslog File Parameters	<i>File Absolute Path Name</i>	Enter the full path name for the file from which this connector will read events or accept the default: \var\adm\messages (Solaris) or \var\log\messages (Linux).
		A wildcard pattern can be used in the file name; however, in realtime mode, rotation can occur only if the file is over-written or removed from the folder. Realtime processing mode assumes following external rotation.
		For date format log rotation, the device writes to 'filename.timestamp.log' on a daily basis. At a specified time, the device creates a new daily log and begins to write to it. The connector detects the new log and terminates the reader thread to the previous log after 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, use a date format in the file name as shown in the following example: filename'yyyy-MM-dd'.log;
		For index log rotation, the device writes to indexed files - '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 it is allowed for the index to be skipped; for example, if 5 appears before 4, processing proceeds with 5 and will not read 4, even if 4 appears later. Use of 'true' is optional.
	<i>Reading Events Real Time or Batch</i>	Specify whether file is to be read in batch or realtime mode. For batch mode, all files are read from the beginning. The 'Action Upon Reaching EOF' and 'File Extension if Rename Action' parameters apply for batch mode only.
	<i>Action Upon Reaching EOF</i>	For batch mode, specify 'None', 'Rename', or 'Delete' as the action to be performed to the file when the connector has finished reading and reaches end of file (EOF). For realtime mode, leave the default value of 'None' for this parameter.
	<i>File Extension If Rename Action</i>	For batch mode, specify the extension to be added to the file name if the action upon EOF is 'Rename' or accept the default value of '.processed'.

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.

Install the SmartConnector

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.

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 Custom String 6	Datagram SyslogAgent
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 Syslog SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Severity	sc-status
Device Vendor	'Microsoft'
Message	message
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

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 Syslog 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 24.3

Configuration Guide for Microsoft Network Policy Server File SmartConnector

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

Configuration Guide for Microsoft Network Policy Server File SmartConnector	4
Product Overview	5
Configuring the SmartConnector	6
Configuring Microsoft NPS	6
Accounting Configuration Wizard	6
Configuring NPS Log File Properties	7
Configuring SQL Server Logging in NPS	9
Installing the SmartConnector	11
Preparing to Install the SmartConnector	11
Installing and Configuring the SmartConnector	11
Device Event Mapping to ArcSight Fields	13
Network Policy Server IAS Format Mappings to ArcSight Fields	13
Network Policy Server DTS Format Mappings to ArcSight Fields	14
Reason Codes	16
Microsoft Field Types and Descriptions	18
Microsoft DTS Reason Codes	23
Microsoft DTS Application Protocols	24
Specifying the Locale for Determining Current Date for File Names	25
Setting Advanced Parameters for the SmartConnector	25
Send Documentation Feedback	26

Configuration Guide for Microsoft Network Policy Server File SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Network Policy 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](#).

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

Network Policy Server (NPS) is the Microsoft implementation of a Remote Authentication Dial-in User Service (RADIUS) server and proxy in the Windows Server. As a RADIUS server, the NPS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless connection, authenticating switch, dial-up connection, virtual private network (VPN) remote access, and router-to-router connections.

Configuring the SmartConnector

Configuring Microsoft NPS

NPS logging is also known as RADIUS accounting.

To configure NPS logging, you must configure the events you want to log and view using the Event Viewer, and then determine the relevant information you want to log. It is necessary to determine whether you want to log user authentication and accounting information to text log files stored on the local computer or to an SQL Server database on either a local computer or a remote computer.

Following are the types of logging used for NPS:

- **Event logging:** This is used for auditing and troubleshooting connection attempts. You can configure NPS event logging by obtaining the NPS server properties in the NPS console.
- **User authentication and accounting requests to a local file logging:** This is used for connection analysis and billing purposes. This is also used as a security investigation tool because it provides a method for tracking the activity of a malicious user after an attack.
- **User authentication and accounting requests to a Microsoft SQL Server XML-compliant database logging:** This is used for multiple servers that are running on NPS and have one data source. This also provides the advantages of using a relational database.



Note: Accounting Configuration wizard can be used to configure SQL Server logging and local file logging.

For more information regarding the Microsoft Network Policy Server, see the Network Policy Server section in the [Microsoft documentation](#).

Accounting Configuration Wizard

The following accounting settings can be configured by using the Accounting Configuration wizard in the NPS console:

- **SQL logging only:** This setting is used to configure a data link to an SQL Server that connects NPS to send accounting data to the SQL server. You can also configure the

database on the SQL Server to ensure that the database is compatible with NPS SQL server logging.

- **Text logging only:** This setting is used to configure NPS to log accounting data to a text file.
- **Parallel logging:** This setting is used to configure the SQL Server data link and database. You can also configure text file logging so that NPS logs simultaneously to the text file and the SQL Server database.
- **SQL logging with backup:** This setting is used to configure the SQL Server data link and database. You can also configure text file logging that NPS uses if SQL Server logging fails.

Both SQL Server logging and text logging allows you to specify whether NPS will continue to process connection requests if logging fails. This can be specified while running the Accounting Configuration wizard in the **SQL Server logging properties > Local File Logging properties > Logging failure action** section.

Perform the following to run the Accounting Configuration Wizard:

1. Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.
2. Navigate to the console tree and click **Accounting > Configure Accounting**.

Configuring NPS Log File Properties

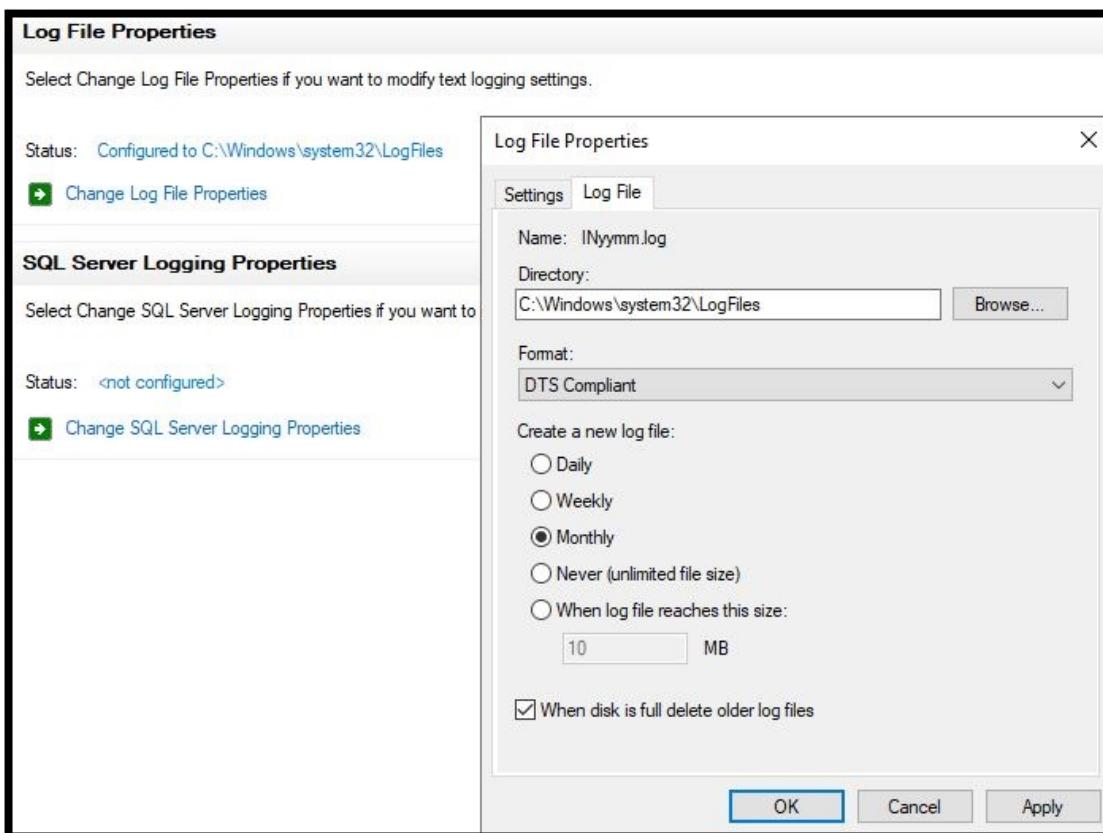


Note: Membership in the Domain Admins group is the minimum required permission to perform this procedure.

Perform the following to configure NPS log file properties:

1. Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.
2. Navigate to the console tree and click **Accounting**.
3. Navigate to **Log File Properties > Change Log File Properties** and then click **Settings**.
4. Under **Log the following information**, ensure to select the option that will ensure to collect enough log information to achieve your accounting goals. For example, select all check boxes if your logs need to accomplish session correlation.
5. Under **Logging failure action:**
 - Select the **If logging fails, discard connection requests** check box if you want NPS to stop processing Access-Request messages when log files are full or unavailable.

- Clear the **If logging fails, discard connection requests** check box if you want NPS to continue processing connection requests if logging fails.
6. Click **Log File** and perform the following:
- a. In the **Directory** field, enter the path for the directory where you want to store the NPS log files. The default location is the %systemroot%\System32\LogFiles folder if no further changes are made.
 - b. In the **Format** list, click **DTS Compliant or IAS (Legacy)**.
 - c. To configure NPS to start creating new log files at specified intervals under **Create a new log file**, select one of the following:
 - Click **Daily** for heavy transaction volume and logging activity.
 - Click **Weekly** or **Monthly** for lesser transaction volumes and logging activity.
 - Click **Never (unlimited file size)** to store all transactions in one log file.
 - Click **When log file reaches this size** to limit the size of each log file, and type a file size to create a new log. The default size is 10 megabytes.



7. Ensure to select the **When disk is full delete older log files** check box to create disk space for new log files when the hard disk is near capacity. However, this option remains unavailable if the value of the new log file is selected as **Never (unlimited file size)**.

size).

8. Click **Apply** to apply the changes and then click **OK**.

Configuring SQL Server Logging in NPS

Perform the following to configure SQL Server logging in NPS:



Note: Membership in Domain Admins, or equivalent, is the minimum required to complete this procedure.

1. Open the NPS console or the NPS Microsoft Management Console (MMC) snap-in.
2. Navigate to the console tree and click **Accounting**.
3. Navigate to the **SQL Server Logging Properties > Change SQL Server Logging Properties**.
4. Under **Log the following information**, select one of the following:
 - Click **Accounting requests** to log all accounting requests.
 - Click **Authentication requests** to log authentication requests.
 - Click **Periodic accounting status** to log periodic accounting status.
 - Click **Periodic status** to log periodic status, such as interim accounting requests.
5. Enter a desired number for the **Maximum number of concurrent sessions** to configure the number of concurrent sessions allowed between the server running NPS and SQL.
6. To configure the SQL Server data source:
Under **SQL Server Logging**, click **Configure**. Navigate to **Data Link Properties > Connection**, and specify the following:
 - Enter or select a name in the **Select or enter a server name** field to specify the name of the server on which the database is stored.
 - Select **Use Windows NT integrated security** to specify the authentication method with which to log on to the server. Or, select **Use a specific user name and password** and enter the **User name** and **Password**.
 - Select **Blank password** to allow a blank password.
 - Select **Allow saving password** to store the password.
 - Click **Select the database on the server** to specify the database for connecting to

the computer running the SQL Server, and select the desired database name from the list.

7. Click **Test Connection** to test the connection between NPS and SQL Server and then click **OK**.
8. Under **Logging failure action**, select the following:
 - If you want NPS to continue with text file logging if the SQL Server logging fails, select the **Enable text file logging for failover** check box.
 - If you want NPS to stop processing Access-Request messages when log files are full or unavailable, select the **If logging fails, discard connection requests** check box. Ensure to clear the check box, if you want NPS to continue processing connection requests if logging fails.



Note: The Microsoft Network Policy Server File connector supports only text-based logs, and not SQL logging.

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](#) section in the [ArcSight Management Center Administrator's Guide](#).

Preparing to Install the SmartConnector

Before you install any SmartConnectors, make sure that the OpenText ArcSight products such as ArcSight ESM or ArcSight Logger with which the connectors will communicate have already been installed correctly.

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

The installation steps described in this section are specific to the Microsoft Network Policy Server File SmartConnector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the Microsoft Network Policy Server 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 Network Policy Server File** as the type of connector, and then click **Next**.
5. Enter the following parameters to configure the SmartConnector, and then click **Next**.

Parameter	Description
Log File Home	Enter the value of Log file directory from Enter the path to the folder containing the Network Policy Server log files (for example, C:\WINDOWS\system32\LogFiles).
New Log Time Period	From the drop-down list, choose the time period that you selected in the Extended Logging Properties window. The options include Hourly , Daily , Weekly , Monthly , or Unlimited file size . The File size reaches limit selection is not supported.
Log File Type	Select IAS for IAS (Legacy) format; select DTS for DTS format.

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 mapping of ArcSight data fields to the device's specific event definitions.

Network Policy Server IAS Format Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Medium when Device Severity = Access-Reject; Low when Device Severity = Access-Accept, Accounting-Request
Application Protocol	protocol
Bytes In	Acct-Input-Octets
Bytes Out	Acct-Output-Octets
Destination Address	Login-IP-Host
Destination Port	Login-TCP-Port
Destination Process Name	Login-Service
Device Action	Acct-Status-Type ("1=Start","2=Stop")
Device Custom Number 2	Acct-Session-Time
Device Custom String 1	Class (see "Microsoft IAS Field Types and Descriptions")
Device Custom String 2	Service-Type
Device Custom String 3	ClientFriendlyName
Device Custom String 4	Acct-Input-Packets
Device Custom String 5	Acct-Output-Packets
Device Custom String 6	Called-Station-Id
Device Event Class Id	Packet-Type (1=Access-Request, 2=Access-Accept, 3=Access-Reject, 4=Accounting-Request)
Device Host Name	NAS-Identifier
Device Severity	Packet-Type (1=Access-Request, 2=Access-Accept, 3=Access-Reject, 4=Accounting-Request)
Device Version	MS-RAS-Version
External ID	Acct-Session-ID

Configuration Guide for Microsoft Network Policy Server File SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Message	Reason-Code
Name	Packet-Type (1=Access-Request, 2=Access-Accept, 3=Access-Reject, 4=Accounting-Request)
Source Host Name	Calling-Station-ID
Source Port	NAS-Port
Source Translated Address	Framed-IP-Address
Transport Protocol	protocol

Network Policy Server DTS Format Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Medium = Access-Reject; Low = Access-Request, Access-Accept, Accounting-Request, Access-Challenge
Application Protocol	Authentication-Type
Bytes In	Acct-Input-Octets
Bytes Out	Acct-Output-Octets
Destination Address	One of (NAS-IP-Address, Client-IP-Address)
Destination Host Name	One of (Client-Friendly-Name, NAS-Identifier)
Destination NT Domain	User-Name
Destination Port	NAS-Port
Destination Process Name	Login-Service
Destination User Name	User-Name
Device Action	Acct-Status-Type (1=Start, 2=Stop)
Device Address	Class
Device Custom Number 1	Session-Timeout
Device Custom Number 2	Acct-Session-Time
Device Custom Number 3	Acct-Interim-Interval
Device Custom String 1	Class
Device Custom String 2	Service-Type (2=Framed)
Device Custom String 3	Calling-Station-Id

Configuration Guide for Microsoft Network Policy Server File SmartConnector
 Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 4	Provider-Type (0 = No authentication occurred, 1 = Authentication occurs on the local NPS server, 2 = Connection request is forwarded to a remote RADIUS server for authentication)
Device Custom String 5	MS-CHAP-Domain
Device Custom String 6	Tunnel-Type (1=PPTP)
Device Event Class ID	One of (Packet-Type, Acct-Status-Type)
Device Host Name	Computer-Name
Device Process Name	Event-Source
Device Product	'NPS'
Device Receipt Time	Timestamp
Device Severity	Packet-Type
Device Vendor	'Microsoft'
Device Version	MS-RAS-Version
External ID	Acct-Session-Id
Message	Reason-Code
Name	One of (Packet-Type, Acct-Status-Type)
Source Translated Address	Framed-IP-Address
Transport Protocol	Framed-Protocol (1=PPP)

Reason Codes

Code	Meaning
0	Success
1	Internal error
2	Access denied
3	Malformed request
4	Global catalog unavailable
5	Domain unavailable
6	Server unavailable
7	No such domain
8	No such user
16	Authentication failure
17	Password change failure
18	Unsupported authentication type
19	No reversibly encrypted password is stored for the user account
32	Local users only
33	Password must be changed
34	Account disabled
35	Account expired
36	Account locked out
37	Invalid logon hours
38	Account restriction
48	Did not match remote access policy
49	Did not match connection request policy
64	Dial-in locked out
65	Dial-in disabled
66	Invalid authentication type
67	Invalid calling station
68	Invalid dial-in hours
69	Invalid called station

Configuration Guide for Microsoft Network Policy Server File SmartConnector

Reason Codes

70	Invalid port type
71	Invalid restriction
80	No record
96	Session timed out
97	Unexpected request

Microsoft Field Types and Descriptions

Field Type	Data Type	Description
User-Name	Text	The specified identity.
NAS-IP-Address	Text	The IP address of the NAS originating the request.
NAS-Port	Number	The physical port number of the NAS originating the request.
Service-Type	Number	The type of service.
Framed-Protocol	Number	The protocol to be used.
Framed-IP-Address	Text	The configured framed address.
Framed-IP-Netmask	Text	The configured IP netmask.
Framed-Routing:	Number	The routing method.
Filter-ID	Text	The name of the filter list for requesting authentication.
Framed-MTU	Number	The maximum configured transmission unit.
Framed-Compression	Number	The compression protocol used.
Login-IP-Host	Number	The IP address of the host.
Login-Service	Number	The service that will connect to the login host.
Login-TCP-Port	Number	The TCP port.
Reply-Message	Text	The displayed message when an authentication request is accepted.
Callback-Number	Text	The callback phone number.
Callback-ID	Text	The name of a location by the access server while performing callback.
Framed-Route	Text	The configured routing information on the access client.
Framed-IPX-Network	Number	The configured IPX network number on the NAS.

Field Type	Data Type	Description
Class	Text	<p>The attribute sent to the client in an Access-Accept packet. This is useful for correlating Accounting-Request packets with authentication sessions. The format is as follows:</p> <ul style="list-style-type: none"> • Type: Specifies the value 25 (1 octet). • Length: Specifies a value of 20 or greater (1 octet). • Checksum: Specifies an Adler-32 checksum that is computed over the remainder of the Class attribute (4 octets). • Vendor-ID: Specifies the ID of the access server vendor (4 octets). The high-order octet is 0 and the low-order 3 octets are the SMI Network Management Private Enterprise Code of the vendor in network byte order, as defined in RFC 1007 "Vendor SMI Network Management Private Enterprise Codes". • Version: Specifies the value of 1 (2 octets). • Server-Address: Specifies the IP address of the RADIUS server that issued the Access-Challenge. For multi-home servers, this is the address of the network interface that receives the original Access-Request (2 octets). • Service-Reboot-Time: Specifies the time at which the first serial number was returned (8 octets). • Unique-Serial-Number: Specifies a unique number to distinguish an individual connection attempt (8 octets). • String: Specifies information that is used to classify accounting records for additional analysis (0 or more octets). In IAS, the Class attribute from the profile is copied into the String field. • Class attribute: Specifies the combination of Serial-Number, Service-Reboot-Time, and Server-Address that must be a unique identification for each authentication that the server accepts. This is used to match the accounting and authentication records if the Class attribute is sent by the network access server in the accounting request packets.
Vendor-Specific	Text	The attribute used to support proprietary NAS features.
Session-Timeout	Number	The length of time (in seconds) before a session is terminated.
Idle-Timeout	Number	The length of idle time (in seconds) before a session is terminated.
Termination-Action	Number	The action that the NAS must take when service is completed.
Called-Station-ID	Text	The dialed phone number.

Configuration Guide for Microsoft Network Policy Server File SmartConnector

Microsoft Field Types and Descriptions

Field Type	Data Type	Description
Calling-Station-ID	Text	The origin phone number for the call.
NAS-Identifier	Text	The string that identifies the NAS originating the request.
Login-LAT-Service	Text	The host used for connection by Local Area Transport (LAT).
Login-LAT-Node	Text	The node used for connection by LAT.
Login-LAT-Group	Text	The authorized LAT group codes.
Framed-AppleTalk-Link	Number	The AppleTalk network number for the serial link (this is used only in case of a router).
Framed-AppleTalk-Network	Number	The AppleTalk network number that is required for the NAS query exists to allocate the AppleTalk node.
Framed-AppleTalk-Zone	Text	The AppleTalk default zone.
Acct-Status-Type	Number	The number that specifies whether an accounting packet starts or stops a bridging, routing, or terminal server session.
Acct-Delay-Time	Number	The length of time (in seconds) for which the NAS has been sending the same accounting packet.
Acct-Input-Octets	Number	The number of octets received during the session.
Acct-Output-Octets	Number	The number of octets sent during the session.
Acct-Session-ID	Text	The unique numeric string that identifies the server session.
Acct-Authentic	Number	The number that specifies which server has authenticated an incoming call.
Acct-Session-Time	Number	The length of time (in seconds) for which the session has been active.
Acct-Input-Packets	Number	The number of packets received during the session.
Acct-Output-Packets	Number	The number of packets sent during the session.
Acct-Terminate-Cause	Number	The reason that a connection was terminated.
Acct-Multi-SSN-ID	Text	The unique numeric string identifying the multilink session.
Acct-Link-Count	Number	The number of links in a multilink session.
Event-Timestamp	Time	The date and time for the event occurring on the NAS.
NAS-Port-Type	Number	The type of physical port used by the NAS for originating the request.
Port-Limit	Number	The maximum number of ports provided by the NAS.
Login-LAT-Port	Number	The connection port used by LAT.
Tunnel-Type	Number	The tunneling protocols to be used.

Configuration Guide for Microsoft Network Policy Server File SmartConnector

Microsoft Field Types and Descriptions

Field Type	Data Type	Description
Tunnel-Medium-Type	Number	The transport medium for creating a tunnel for protocols. For example, L2TP packets can be sent to multiple link layers.
Tunnel-Client-Endpt	Text	The IP address of the tunnel client.
Tunnel-server-Endpt	Text	The IP address of the tunnel server.
Acct-Tunnel-Connection	Text	An identifier assigned to the tunnel.
Password-Retry	Number	The number of times required for authentication before the NAS terminates the connection.
Prompt	Number	A number that indicates to the NAS whether it should (Prompt=1) or should not (Prompt=0) echo the response as it is typed.
Connect-Info	Text	Information that is used by the NAS to specify the type of connection made. Typical information includes connection speed and data encoding protocols.
Configuration-Token	Text	The type of profile used (sent from a RADIUS proxy server to a RADIUS proxy client) in an Access-Accept packet.
Tunnel-Pvt-Group-ID	Text	The group ID for a particular tunneled session.
Tunnel-Assignment-ID	Text	The tunnel assigned to a session.
Tunnel-Preference	Number	A number that indicates the preference of the tunnel type. This is indicated with the Tunnel- Type attribute when multiple tunnel types are supported by the access server.
Acct-Interim-Interval	Number	The length of interval (in seconds) between each interim update sent by the NAS.
Ascend-to-255	Text	The vendor-specific attributes for Ascend. For more information, see the Ascend documentation.
Client-IP-Address	Text	The IP address of the RADIUS client.
NAS-Manufacturer	Number	The manufacturer of the NAS.
MS-CHAP-Error	Number	The error data that describes an MS-CHAP transaction.
Authentication-Type	Number	The authentication scheme used for verification.
Client-Friendly-Name	Text	The name for the RADIUS client.
SAM-Account-Name	Text	The account name in the Security Accounts Manager (SAM) database.
Fully-Qualified-User-Name	Text	The user name in canonical format.

Configuration Guide for Microsoft Network Policy Server File SmartConnector
Microsoft Field Types and Descriptions

Field Type	Data Type	Description
EAP-Friendly-Name	Text	The name that is used with Extensible Authentication Protocol (EAP).
Packet-Type	Number	<p>The type of packet, which can be as follows:</p> <p>1=Access-Request</p> <p>2=Access-Accept</p> <p>3=Access-Reject</p> <p>4=Accounting-Request</p>
NP-Policy-Name	Text	The name of a remote access policy.

Microsoft DTS Reason Codes

Code	Meaning
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge

Microsoft DTS Application Protocols

Code	Meaning
1	PAP
2	CHAP
3	MS-CHAP
4	MS-CHAP v2
5	EAP
7	None
8	Custom
11	PEAP-MSCHAP

Specifying the Locale for Determining Current Date for File Names

The locale that is used to determine the current date for file names can be specified using the `localeforfilename` parameter. The default locale will be used if nothing is specified. This usually works unless Thailand is selected as the default locale, in which the numbers for the years are modified. The parameter needs to be set to `en_US` for Thailand.

Setting Advanced Parameters for the SmartConnector

After the SmartConnector has been installed, perform the following to set the advanced parameters:

1. Modify the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`.
2. Locate the `localeforfilename` parameter and set its value to `en_US`. Save the file and 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 Network Policy Server File SmartConnector
(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: 8.4.3

Configuration Guide for Microsoft Exchange PowerShell 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 Exchange PowerShell SmartConnector	5
Product Overview	6
Configuration	7
Mailbox Audit Logs	7
Enable Mailbox Audit Logging	8
Use the Shell to Enable Mailbox Audit Logging	9
Use the Shell to Specify Mailbox Audit Logging Settings	9
Administrator Audit Logs	10
Enable Administrator Audit Logging	10
Use the Shell to Enable Administrator Audit Logging	11
Use the Shell to Specify Administrator Logging Settings	11
Locate the Fully Qualified Domain Name	12
Install the SmartConnector	14
Prepare to Install Connector	14
Install Core Software	14
Set Global Parameters (optional)	15
Select Connector and Add Parameter Information	16
Select a Destination	17
Complete Installation and Configuration	17
Run the SmartConnector	18
Device Event Mapping to ArcSight Fields	19
Microsoft Exchange PowerShell Mappings	19
Microsoft Exchange PowerShell Mappings	20
Troubleshooting	21
Execute PowerShell Scripts	21

Turn on Execution Policy for PowerShell	21
Install Windows Management Framework 3.0 RC	23
Running the connector as Domain user account	24
Send Documentation Feedback	25

Configuration Guide for Microsoft Exchange PowerShell SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Exchange PowerShell 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 Exchange Management Shell is built on Windows PowerShell technology. It provides a powerful command-line interface for Microsoft Exchange Server 2010 and 2013 that enables automation of administrative tasks. With the Shell, you can manage every aspect of Exchange, including enabling new e-mail accounts, configuring SMTP connectors, storing database properties, storing transport agents, and more. The Shell can perform every task that can be performed by the Exchange Management Console and the Exchange Web interface, in addition to tasks that cannot be performed in those interfaces.

This connector is supported for installation on Windows platforms only. This connector remotely retrieves:

- Microsoft Exchange Server 2010 SP2 and 2013 Mailbox Audit and Admin Audit logs
- Microsoft Exchange Server 2016 Access Auditing logs

Configuration

You need to be assigned permissions before you can enable mailbox audit logging. You must log in as a domain user to install and run the connector. To see what permissions you need, see the "Mailbox audit logging" entry in the **Messaging Policy and Compliance Permissions** topic in the Microsoft Exchange TechNet Library.

For 2010, see "Understanding Mailbox Audit Logging" at [https://technet.microsoft.com/en-us/library/ff459237\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/ff459237(v=exchg.141).aspx).

For 2013, see "Mailbox audit logging" at [https://technet.microsoft.com/en-us/library/ff459237\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/ff459237(v=exchg.150).aspx).

For 2016, see "Mailbox auditing in Exchange 2016" at [https://technet.microsoft.com/en-us/library/ff459237\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/ff459237(v=exchg.160).aspx).

You can use administrator audit logging in Microsoft Exchange Server 2013 to log when a user or administrator makes a change in your organization. By keeping a log of the changes, you can trace changes to the person who made the change, augment your change logs with detailed records of the change as it was implemented, comply with regulatory requirements and requests for discovery, and more. For more information about audit logs, see the Administrator Audit Logging topic in the Microsoft Exchange TechNet Library.

For 2010, see "Administrator Audit Logging" at [https://technet.microsoft.com/en-us/library/dd335144\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/dd335144(v=exchg.141).aspx).

For 2013, see "Administrator audit logging" at [https://technet.microsoft.com/en-us/library/dd335144\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dd335144(v=exchg.150).aspx).

For 2016, see "Administrator audit logging in Exchange 2016" at [https://technet.microsoft.com/en-us/library/dd335144\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/dd335144(v=exchg.160).aspx).

Mailbox Audit Logs

Mailbox audit logs are generated for each mailbox that has mailbox audit logging enabled. Log entries are stored in the **Audits** subfolder of the audited mailbox **Recoverable Items** folder. This ensures that all audit logs are available from a single location, regardless of which client access method was used to access the mailbox or which server or workstation an administrator used to access the mailbox audit log.

By default, mailbox audit log entries are retained in the mailbox for 90 days. You can modify this retention period by using the `AuditLogAgeLimit` parameter together with the `Set-Mailbox` cmdlet.

Enable Mailbox Audit Logging

By using mailbox audit logging, you can track logons to a mailbox, and also track what actions are taken while the user is logged on. When you enable mailbox audit logging, some actions performed by administrators and delegates are logged by default. None of the actions performed by the mailbox owner are logged.

You can specify which user actions (for example, accessing, moving, or deleting a message) should be logged for a logon type (administrator, delegate user, or owner). See "Use the Shell to Specify Logging Settings." The following table lists the actions logged by mailbox audit logging, including the logon types for which the action is logged.

Action	Description	Administrator	Delegate	Owner
Copy	An item is copied to another folder.	Yes	Not applicable	Not applicable
Create	An item is created in the mailbox (for example, a message is sent or received). Note: Folder creation is not audited.	Yes*	Yes*	Yes
FolderBind	A mailbox folder is accessed.	Yes*	Yes**	Yes
HardDelete	An item is deleted permanently from the Recoverable Items folder.	Yes*	Yes*	Yes
MailboxLogin	The user signed in to their mailbox.	No	No	Yes***
MessageBind	An item is accessed in the reading pane or opened.	Yes	Not applicable	Not applicable
Move	An item is moved to another folder.	Yes*	Yes	Yes
MoveToDeleteItems	An item is moved to the Deleted Items folder.	Yes*	Yes	Yes
SendAs	A message is sent using Send As permissions.	Yes*	Yes*	Not applicable

Action	Description	Administrator	Delegate	Owner
SendOnBehalf	A message is sent using Send on Behalf permissions.	Yes*	Yes	Not applicable
SoftDelete	An item is deleted from the Deleted Items folder.	Yes*	Yes*	Yes
Update	An item's properties are updated.	Yes*	Yes*	Yes

Use the Shell to Enable Mailbox Audit Logging

This example enables mailbox audit logging for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditEnabled $true
```

For detailed syntax and parameter information, see Set-Mailbox in the Microsoft Exchange TechNet Library (<http://technet.microsoft.com/en-us/library/bb123981.aspx>).

Use the Shell to Specify Mailbox Audit Logging Settings

Use the shell to specify logging settings for Administrator, Delegate, and Owner access.

This example specifies that the **SendAs** or **SendOnBehalf** actions performed by delegate users will be logged for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditDelegate SendAs,SendOnBehalf -  
AuditEnabled $true
```

This example specifies that the **MessageBind** and **FolderBind** actions performed by administrators will be logged for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditAdmin MessageBind,FolderBind -  
AuditEnabled $true
```

This example specifies that the **HardDelete** action performed by the mailbox owner will be logged for Ben Smith's mailbox.

```
Set-Mailbox -Identity "Ben Smith" -AuditOwner HardDelete -AuditEnabled  
$true
```

Administrator Audit Logs

Administrator audit logs contain a record of all the cmdlets and parameters that have been run in the Exchange Management Shell and by the Exchange Administration Center (EAC). They are created on-demand when you run the Administrator audit log report in the EAC, or when you run the **New-AdminAuditLogSearch** cmdlet in the Shell.

By default, audit logging is configured to store audit log entries for 90 days. After 90 days, the audit log entry is deleted. You can change the audit log age limit using the AdminAuditLogAgeLimit parameter. You can specify the number of days, hours, minutes, and seconds that audit log entries should be kept. To specify a value, use the format dd.hh:mm:ss where the following applies:

- **dd** - The number of days to keep the audit log entry.
- **hh** - The number of hours to keep the audit log entry.
- **mm** - The number of minutes to keep the audit log entry.
- **ss** - The number of seconds to keep the audit log entry.

To specify multiple years, use the dd field. For example, 365 days equals one year; 730 days equals two years; 913 days equals two years and six months. For example, to set the audit log age limit to two years and six months, use the syntax 913.00:00:00.

Enable Administrator Audit Logging

Each audit log entry contains the information described in the following table. The audit log contains one or more audit log entries. The number of audit log entries is controlled by the audit log age limit specified using the Set-AdminAuditLogConfig cmdlet. Any audit log entry that exceeds the age limit is deleted. See "Use the Shell to Specify Administrator Logging Settings." The following table lists the actions logged by administrator audit log entry fields.

Field	Description
RunspaceId	This field is used internally by Exchange.
ObjectModified	This field contains the object that was modified by the cmdlet specified in the 'CmdletName' field.
CmdletName	This field contains the name of the cmdlet that was run by the user in the Caller field.

Field	Description
CmdletParameters	This field contains the parameters that were specified when the cmdlet in the CmdletName field was run. Also stored in this field, but not visible in the default output, is the value specified with the parameter, if any.
ModifiedProperties	This field contains the properties that were modified on the object in the ObjectModified field. Also stored in this field, but not visible in the default output, are the old value of the property and the new value that was stored. NOTE: This field is only populated if the LogLevel parameter on the "Set-AdminAuditLogConfig" cmdlet is set to 'Verbose'.
Caller	This field contains the user account of the user who ran the cmdlet in the CmdletName field.
Succeeded	This field specifies whether the cmdlet in the CmdletName field ran successfully. The value is either True or False.
Error	This field contains the error message generated if the cmdlet in the CmdletName field failed to complete successfully.
RunDate	This field contains the date and time when the cmdlet in the CmdletName field was run. The date and time are stored in Coordinated Universal Time (UTC) format.
OriginatingServer	This field indicates the server on which the cmdlet specified in the CmdletName field was run.
Identity	This field is used internally by Exchange.
IsValid	This field is used internally by Exchange.
ObjectState	This field is used internally by Exchange.

Use the Shell to Enable Administrator Audit Logging

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Administrator audit logging" entry in the "Exchange and Shell Infrastructure Permissions" topic ([https://technet.microsoft.com/en-us/library/dd638114\(v=exchg.141\).aspx](https://technet.microsoft.com/en-us/library/dd638114(v=exchg.141).aspx)).

To enable administrator audit logging, use the following command:

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $True
```

Use the Shell to Specify Administrator Logging Settings

Use the shell to specify logging settings for Administrator, Delegate, and Owner access.

This example enables administrator audit logging for every cmdlet and every parameter in the organization, with the exception of Get cmdlets.

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -  
AdminAuditLogCmdlets * -AdminAuditLogParameters *
```

This example enables administrator audit logging for specific cmdlets run in the organization. Any parameter used on the specified cmdlets is logged. Every time a specified cmdlet is run, a log entry is added to the audit log.

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -  
AdminAuditLogCmdlets *Mailbox, *Management*, *TransportRule* -  
AdminAuditLogParameters *
```

This example enables administrator audit logging only for specific parameters that are specified when running specific cmdlets. The parameter name and the cmdlet name must match the strings specified with the "AdminAuditLogCmdlets" and "AdminAuditLogParameters" parameters. For example, a log entry is generated only when a parameter with the string "Address" in the name is run on a cmdlet with the string "Mailbox" in its name.

```
Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -  
AdminAuditLogCmdlets *Mailbox* -AdminAuditLogParameters *Address*
```

Locate the Fully Qualified Domain Name

To fill in appropriate connector parameters to retrieve events from the correct source, you will need to know the Fully Qualified Domain Name (FQDN) of the Microsoft Exchange Server.

To find the FQDN, go to **Start -> Control Panel -> System**. Under **Computer name, domain, and workgroup settings**, find the **Full computer name**.

Configuration Guide for Microsoft Exchange PowerShell SmartConnector Configuration



Install the SmartConnector

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

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.

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 Exchange PowerShell** and click **Next**.
- 3 Enter the required SmartConnector parameters and device details to configure the SmartConnector, then click **Next**.

Parameter	Description
Server FQDN	Specify the fully qualified domain name to the Exchange Server.
PowerShell Path	Enter the path to the directory where the PowerShell application is located. The default location is 'C:\Windows\System32\WindowsPowerShell\V1.0'.
Frequency (seconds)	Enter the frequency at which each mailbox audit log is to be retrieved, in seconds. The default value is 600 seconds.
AliasName	Enter the alias name of the mailbox user.
DisplayName	Enter the display name of the mailbox user.
Info	Add any pertinent information.

You can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. The connector automatically runs a script to create a CSV file containing the mailboxes for the server whose FQDN you specify during configuration. This file is located at \$ARCSIGHT_HOME\user\agent\agentdata and has a file name of the format 'Mailboxes-yyyy_

mm_dd-HH_MM.csv'. You can click the 'Export' button to export the mailbox data you have entered into the table into a CSV file.

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 Exchange PowerShell Mappings

ArcSight ESM Field	Device-Specific Field
Destination User ID	One of (DestMailboxOwnerSid, MailboxOwnerSid)
Destination User Name	One of (DestMailboxOwnerUPN, MailboxOwnerUPN)
Device Action	One of (Operation, CmdletName)
Device Custom String 1	One of (LogonType, ObjectModified)
Device Custom String 2	One of (SourceItemSubjectsList, CmdletParameters)
Device Custom String 3	One of (ItemSubject, ModifiedProperties)
Device Custom String 4	One of (ClientInfoString, ObjectState)
Device Custom String 5	MailboxResolvedOwnerName
Device Custom String 6	ExternalAccess
Device Event Class ID	One of (Operation, CmdletName)
Device Host Name	OriginatingServer
Device Process Name	ClientProcessName
Device Product	'Exchange Server'
Device Receipt Time	One of (LastAccessed, RunDate)
Device Vendor	'Microsoft'
Event Outcome	One of (OperationResult and Status(Succeeded,"True","Succeeded","Failed"))
External ID	Identity
File Path	DestFolderPathName
Name	One of (Operation, CmdletName)
Old File Name	SourceItemAttachmentsList
Old File Path	FolderPathName
Old File Size	SourceItemAttachmentsList

Configuration Guide for Microsoft Exchange PowerShell SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Source Address	ClientIPAddress
Source Host Name	ClientMachineName
Source User ID	LogonUserSid
Source User Name	One of (DelegateUserDisplayName, LogonUserDisplayName, Caller)

Microsoft Exchange PowerShell Mappings

ArcSight ESM Field	Device-Specific Field
File Id	ItemId
File Name	ItemAttachments (the name part)
File Size	ItemAttachments (the number part)
Old File Permission	DirtyProperties

Troubleshooting

Execute PowerShell Scripts

This connector executes ArcSight Windows PowerShell scripts to retrieve information about mailboxes and events/logs from the Microsoft Exchange Server. Be sure you have turned on the execution policy for PowerShell through the Local Policy Editor to allow execution of these scripts. If other security measures block execution of these scripts, you can attempt to run the scripts directly.

When connection to the Exchange Server fails during configuration, search agent.log for information and execute a script directly from a PowerShell command line window.

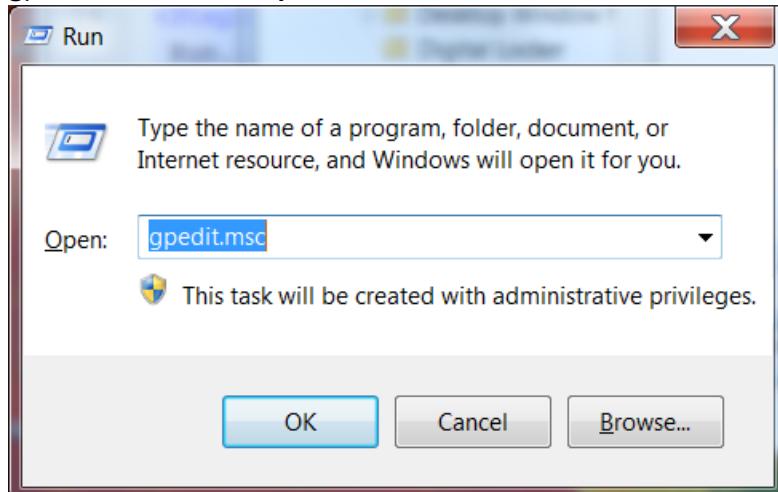
For example, from the box where the SmartConnector is installed, open a Windows command window and run the script collectMailboxes.ps1 against the Exchange Server to retrieve mailbox information.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell" -file  
"C:$ARCSIGHT_HOME\current\bin\agent\microsoft\exchange\collectMailboxes.ps1"  
"<Exchange Server FQDN Hostname>" "C:$ARCSIGHT_  
HOME\current\user\agent\agentdata" "" ""
```

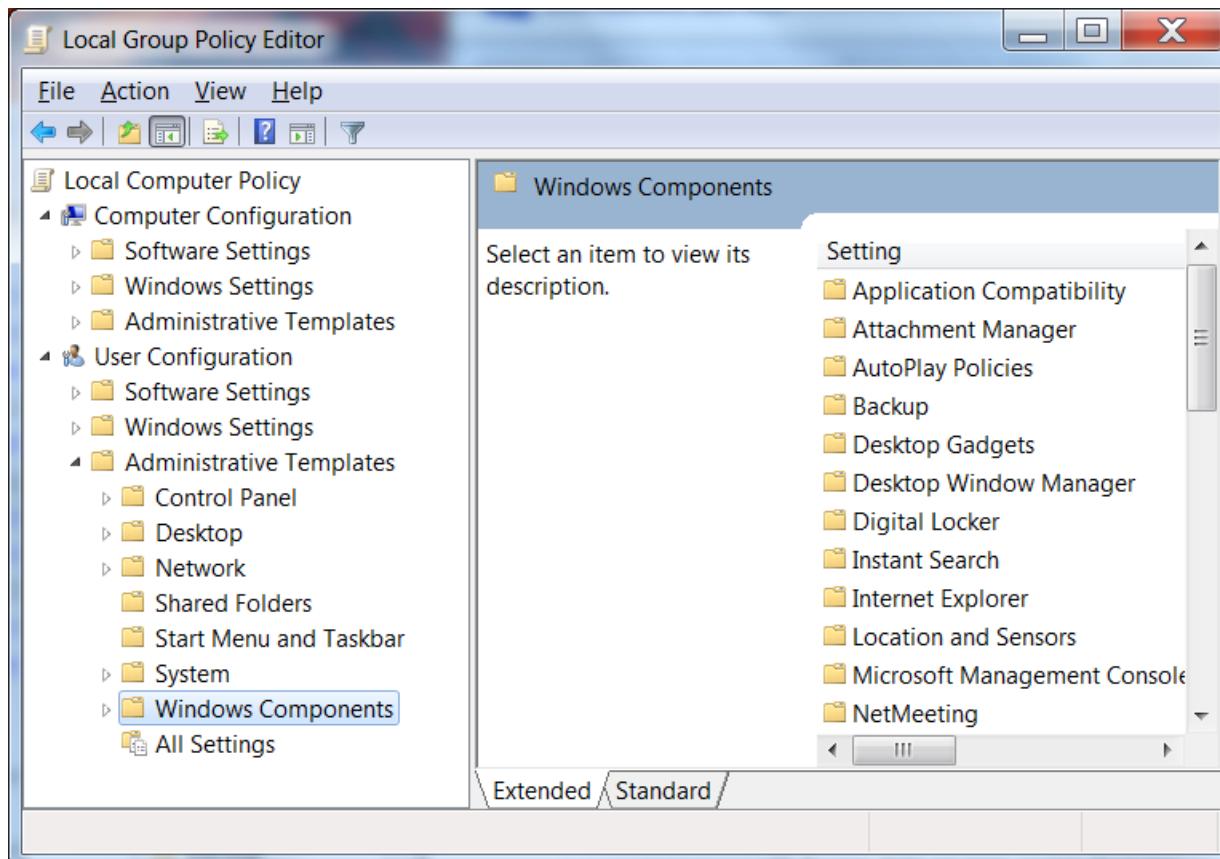
Turn on Execution Policy for PowerShell

Turn on the execution policy for PowerShell through the Local Policy Editor:

- 1 To open the Local Group Policy Editor from the command line, click **Start -> Run...**, enter gpedit.msc in the **Open:** box and click **OK**.



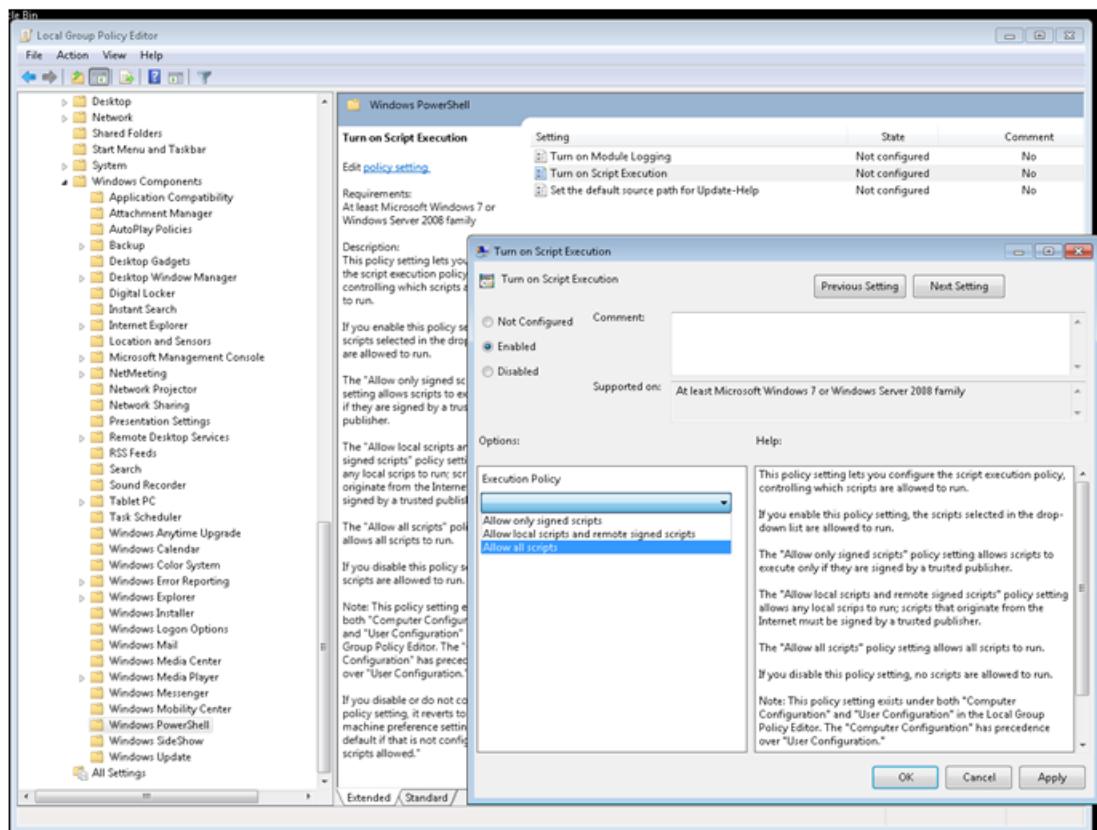
2 From the left pane, select **User Configuration -> Windows Components -> Microsoft PowerShell.**



If you do not see the PowerShell component, you will need to install Windows Management Framework. See "Install Windows Management Framework 3.0 RC."

3 With the Windows PowerShell component selected, check **Turn on Script Execution**.

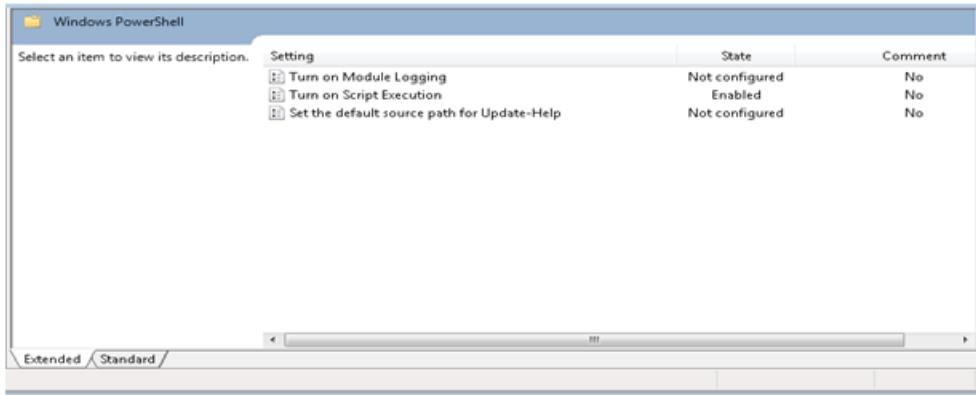
Configuration Guide for Microsoft Exchange PowerShell SmartConnector Troubleshooting



4 Under Options, Execution Policy, select Allow all scripts.

5 Click OK.

The Turn on Script Execution setting's state now shows Enabled.



Install Windows Management Framework 3.0 RC

1 Download the correct package for your operating system and architecture.

- Windows 7 Service Pack 1
- 64-bit versions: WINDOWS6.1-KB2506143-x64.MSU

- 2** Close all Windows PowerShell windows.
- 3** Uninstall any other versions of Windows Management Framework 3.0.
- 4** Run the MSU file you downloaded.

Running the connector as Domain user account

Stand-alone mode:

- 1** Open the command window as Domain user by holding shift and right click the command window icon.
- 2** Choose Run as different user.
- 3** Enter the credential for domain user account. Then, run the connector as usual: go to \$ARCSIGHT_HOME\current\bin and run: arcsight connectors

Service Mode:

- 1** Go to service (Run services.msc).
- 2** Right click on the connector service and choose Properties.
- 3** From the Log on tab, choose this account and enter the domain user account credentials.

For more information about scripting, see the [Group Policy Script Center](#).
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 PowerShell 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

Configuration Guide for Microsoft System Center Configuration Manager 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 System Center Configuration Manager DB SmartConnector	4
Product Overview	5
Supported Versions	5
Prerequisites	6
Downloading the JDBC Driver	6
Installing and Configuring the SmartConnector	7
Preparing to Install the SmartConnector	7
Installing and Configuring the SmartConnector	8
Adding JDBC Driver to the Connector Appliance/ArcSight Management Center	10
Device Event Mapping to ArcSight Fields	11
Configuration Manager 2012 Endpoint Protection Antimalware Event Mappings	11
Troubleshooting	13
Send Documentation Feedback	15

Configuration Guide for Microsoft System Center Configuration Manager DB SmartConnector

This guide provides information for installing the SmartConnector for Microsoft System Center Configuration Manager 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](#).

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 System Center 2012 Configuration Manager helps people use the devices and applications they need to be productive, while maintaining corporate compliance and control. It accomplishes this with a unified infrastructure that gives a single view to manage physical, virtual, and mobile clients, and provides tools and improvements that make it easier for IT administrators to do their jobs.

Supported Versions

Event collection from Linux platforms is not supported as Microsoft requires SQL Server be configured for Windows authentication for Microsoft System Center Configuration Manager.

Prerequisites

See your Microsoft Systems Center Configuration Manager product documentation for instructions for configuring the device to send events.

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, refer to this [Microsoft Documentation](#).

Installing and Configuring 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.



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
- 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.
 - a. 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`
 - b. For using 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.

7. Browse to `$ARCSIGHT_HOME/current/bin`, then double-click `runagentsetup` file to start the SmartConnector Configuration Wizard.
8. Specify the relevant Global Parameters, when prompted.

9. Select **Microsoft Systems Center Configuration Manager DB** from the Type drop-down, then click **Next**.
10. Select the following parameter details to configure the SmartConnector, then click **Next**.
11. Select the following device details to configure the SmartConnector, then click **Next**.

Parameter	Description
JDBC/ODB C Driver	Select the <code>com.microsoft.sqlserver.jdbc.SQLServerDriver</code> driver.
Database URL	<p>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>.</p> <p>To configure JDBC Driver and Windows Authentication, add <code>;integratedSecurity=true</code> 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, <code>jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integrate dSecurity=true</code></p>
Database User	Enter the user name of the MS SQL Server DB user with appropriate database privilege.
Database Password	Enter the password for the Microsoft SCCM database URL password.
Event Types	Select forefront as the default value of the event types.

12. Select a destination and configure parameters.
13. Specify a name for the connector.
14. 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.
15. Select whether you want to run the connector as a service or in the standalone mode.
16. Complete the installation.
17. Run the SmartConnector.
18. 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.

Configuration Manager 2012 Endpoint Protection Antimalware Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = 5, High = 4, Medium = 2, Low = 1 or 0
Destination Address	ComputerAddress
Destination Host Name	DestinationHostName
Destination NT Domain	Domain
Destination Process Name	Process
Destination User ID	UserID
Destination User Name	UserName
Device Action	Action
Device Custom Date 1	ActionTime
Device Custom Number 1	ExecutionStatus
Device Custom Number 2	LastMessageSerialNumber
Device Custom String 1	ThreatName
Device Custom String 3	DetectionID
Device Event Category	Category
Device Event Class ID	All of (CleaningAction, CategoryID, ActionSuccess)
Device External ID	MachineID
Device Host Name	_DB_HOST
Device Product	'SCCM_FEP'
Device Receipt Time	LastMessageTime
Device Severity	SeverityID

Configuration Guide for Microsoft System Center Configuration Manager DB SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Vendor	'Microsoft'
Device Version	ProductVersion
End Time	DetectionTime
Event Outcome	ActionSuccess (1=Success, 0=Failure)
File Name	Path
File Path	Path
File Type	Path
Name	(Action, Category, (ActionSuccess, "1=Successfully", "0=Unsuccessfully"))
Reason	ErrorCode

Troubleshooting

"What do I do when the driver could not establish a secure connection to SQL Server by using Secure Sockets Layer (SSL) encryption. The error is, Error: "Server chose TLSv1, but that protocol version is not enabled or not supported by the client?"

Go to folder ArcSightSmartConnectors/current/jre/lib/security.

In the file java.security, find option jdk.tls.disabledAlgorithms. Either disable or delete TLSv1.

"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.

"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 System Center Configuration Manager 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 System Center Operations Manager 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>

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 System Center Operations Manager 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 the JDBC Driver to the Connector Appliance/ArcSight Management Center	10
Device Event Mapping to ArcSight Fields	11
Operations Manager 2012 Event Mappings	11
Operations Manager 2007 Event Mappings	12
Additional Mappings for Microsoft Forefront Client Security Events	13
Operations Manager 2005 Event Mappings	13
Troubleshooting	15
Send Documentation Feedback	17

Configuration Guide for Microsoft System Center Operations Manager DB SmartConnector

This guide provides information for installing the SmartConnector for Microsoft System Center Operations Manager 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](#).

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 Systems Center Operations Manager is designed to simplify monitoring and management of large, heterogeneous IT infrastructures.

Microsoft Forefront Client Security provides unified, easily managed malware protection for business desktops, laptops, and server operating systems. Forefront Client Security with Microsoft Operations Manager 2005 is supported.



The preferred Operations Manager setup method is to use SQL Server Authentication. The ODBC source you create on the machine where you install the SmartConnector must match the configuration of the SCOM setup authentication type; otherwise, the SmartConnector cannot successfully authenticate.

Prerequisites

This section provides instructions to configure the Microsoft Systems Center Operations Manager Database to send events to the ArcSight SmartConnector.

If you are using the Audit Collection Services (ACS) agent with Operations Manager, use the SmartConnector for Microsoft Audit Collection System DB.

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 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 Systems Center Operations Manager DB** from the Type drop-down, then click **Next**.
10. Enter the required parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
JDBC/ODBC Driver	Select the com.microsoft.sqlserver.jdbc.SQLServerDriver driver.
Database 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 <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=mydatabase;integratedSecurity=true</p>
Database User	Enter the user name of the MS SQL Server DB user with appropriate database privilege.
Database Password	Microsoft SCOM database URL password.

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](#).

Adding the 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.

Due to limitations in event format in Operations Manager 2007, events cannot be further parsed by the Windows Event Log SmartConnector as is done with SCOM 2005.

Support for Microsoft Forefront Client Security events has been added; the mappings shown in the Forefront Client Security event mappings table are in addition to support for the same event mappings as for SCOM events.

Operations Manager 2012 Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 3; Medium = 2; Low = 1
Destination Host Name	LoggingComputer
Destination NT Domain	extracted from EventUser
Destination User Name	extracted from EventUser
Device Custom Date 2	TimeAdded
Device Custom Number 2	Number (Windows Event Number)
Device Custom String 1	RuleName
Device Custom String 2	PublisherName (Event Source)
Device Custom String 3	RuleCategory
Device Custom String 5	ObjectFullName
Device Event Category	Channel
Device Event Class ID	Both (Channel, Number)
Device Host Name	LoggingComputer
Device Product	'Operations Manager'
Device Receipt Time	TimeGenerated
Device Severity	RulePriority
Device Vendor	'Microsoft'

ArcSight ESM Field	Device-Specific Field
External ID	EventId
Message	EventParameters
Name	RuleName

Operations Manager 2007 Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 3; Medium = 2; Low = 1
Destination Host Name	LoggingComputer
Destination User ID	Destination User Name
Device Custom Date 2	TimeAdded
Device Custom Number 2	Number (Windows Event Number)
Device Custom String 1	RuleName
Device Custom String 2	PublisherName
Device Custom String 3	RuleCategory
Device Event Category	Channel
Device Event Class ID	Channel plus Number
Device Host Name	LoggingComputer
Device Product	'Microsoft Operations Manager 2007'
Device Receipt Time	TimeGenerated
Device Severity	RulePriority
Device Vendor	'Microsoft'
External ID	EventId
Message	EventParameters
Name	RuleName

Additional Mappings for Microsoft Forefront Client Security Events

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	Issue Name
Device Custom String 3	Risk
Device Product	'Microsoft Forefront'
Device Severity	Severity
Name	extracted from Message field

Operations Manager 2005 Event Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	Very High = Audit Failure; High = Error; Medium = Warning; Low = Success, Information, Audit Success
Destination Host Name	ComputerName
Destination User ID	UserName
Device Custom Date 2	TimeStored
Device Custom Number 3	isAlerted
Device Custom String 1	EventId
Device Custom String 4	idEvent
Device Custom String 5	oneof (SourceName,"Unknown")
Device Custom String 6	SourceCategory
Device Event Category	ProviderName
Device Event Class ID	SourceName plus EventId
Device Host Name	ComputerName
Device Product	Microsoft Operations Manager 2005
Device Receipt Time	TimeGenerated
Device Severity	EventType
Device Vendor	Microsoft

Configuration Guide for Microsoft System Center Operations Manager DB SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
File Name	MsgFileName
File Type	"Message File"
Message	Message
Name	Event name from Message field
Source Host Name	(Optional) SourceComputerName

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 System Center Operations Manager 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 SharePoint Server 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>

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 SharePoint Server DB SmartConnector	5
Product Overview	6
Prerequisites	7
Downloading the JDBC Driver	7
Installing the SmartConnector	9
Preparing to Install the SmartConnector	9
Installing and Configuring the SmartConnector	9
Adding the JDBC Driver to the Connector Appliance/ArcSight Management Center	12
Device Event Mapping to ArcSight Fields	13
SharePoint 2016/2013/2010/2019 Audit Data Mappings	13
SharePoint Query General Mappings	14
Mappings for Audit Event 1	14
Mappings for Audit Event 2	14
Mappings for Audit Event 3	14
Mappings for Audit Event 4	15
Mappings for Audit Event 5	15
Mappings for Audit Event 6	15
Mappings for Audit Event 7	15
Mappings for Audit Event 8	16
Mappings for Audit Event 10	16
Mappings for Audit Event 12	16
Mappings for Audit Event 13	16
Mappings for Audit Event 14	16
Mappings for Audit Event 15	17
Mappings for Audit Event 16	17
Mappings for Audit Event 30	17
Mappings for Audit Event 31	17
Mappings for Audit Event 32	18

Mappings for Audit Event 33	18
Mappings for Audit Event 34	18
Mappings for Audit Event 35	18
Mappings for Audit Event 36	19
Mappings for Audit Event 38	19
Mappings for Audit Events 39, 40	19
Mappings for Audit Event 50	19
Mappings for Audit Event 100	20
 Troubleshooting	21
 Send Documentation Feedback	23

Configuration Guide for Microsoft SharePoint Server DB SmartConnector

This guide provides information for installing the SmartConnector for Microsoft SharePoint Server 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](#).

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 SharePoint Server is a Web application platform associated with intranet content management and document management. SharePoint provides central management, governance, and security controls.

Microsoft SharePoint logs events that monitor usage and performance. It also logs events that monitor and audit resources. The SmartConnector for SharePoint parses audit logs.



The preferred SharePoint setup method is to use SQL Server Authentication.

Prerequisites

This section provides instructions for configuring the Microsoft SharePoint Server Database to send events to the ArcSight SmartConnector.

SharePoint can be implemented in two ways: as a stand-alone server or as part of a new or existing server farm. As a stand-alone server, the enterprise features will not be available and everything is done on the same box. This implementation is not supported because you cannot log to a SQL Database Server whether remote or local. (However, during the stand-alone installation, an SQL Server Express Edition is automatically installed locally.) Also, in a stand-alone configuration, you cannot create a server farm or join one.

As part of a new or existing server farm, SharePoint installs with all of its features. This is the implementation that the connector supports.



Supporting audit logs in a stand-alone implementation requires an API that communicates with the internal database.

If you are using the Audit Collection Services (ACS) agent with Microsoft SharePoint, use the SmartConnector for Microsoft Audit Collection System DB.

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](#) to [mssql-jdbc-9.4.0.jre8.jar](#).
- 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, which is 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
- 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 SharePoint Server DB** and click **Next**.
10. Enter the required parameters to configure the SmartConnector, then click **Next**.

Configuration Guide for Microsoft SharePoint Server DB SmartConnector

Installing the SmartConnector

Parameter	Description
JDBC/ODBC Driver	Select the <code>com.microsoft.sqlserver.jdbc.SQLServerDriver</code> driver.
URL	<p>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>.</p> <p>To configure JDBC Driver and Windows Authentication, add <code>;integratedSecurity=true</code> 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, <code>jdbc:sqlserver://mysqlserver:1433;DatabaseName=mydatabase;integratedSecurity=true</code></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 default event type is <code>audit_content</code> .

Make sure that the SmartConnector settings match the settings you entered in the data source configuration for the machine upon 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.
12. Click **Import** to select a CSV file to import into the table rather than add the data manually. See the SmartConnector Installation and User Guide for more information.
13. Select a [destination and configure parameters](#).
14. Specify a name for the connector.
15. (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.
---	--

16. Select whether you want to install the connector as a service or in the standalone mode.
17. Complete the installation.
18. [Run the SmartConnector](#).

19. 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 the 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.

SharePoint 2016/2013/2010/2019 Audit Data Mappings

ArcSight ESM Field	Device-Specific Field
Additional data	UserType
Additional data	webDescription
Additional data	webID
Device Custom String 2	Event ID
Device Custom String 3	Item Version
Device Custom String 4	Database Name
Device Custom String 6	Group Name
Device Event Category	One of("Custom Audit Event", "Internal Audit Event")
Device Event Class ID	Custom_Event_Name
Device Product	'SharePoint'
Device Receipt Time	Time_Occured
Device Vendor	'Microsoft'
External ID	Item_ID
File Id	Doc_Location
File ModificationTime	Doc_Time
File Name	Doc_Location
File Path	Doc_Location
File Type	Item_Type (1=Document, 3=Item, 4=List, 5=Folder, 6=Site, or 7=Site Collection)
Message	Event_Data
Name	Custom_Event_Name
Old FileId	Doc_ID
Old FileName	UI_Version

Configuration Guide for Microsoft SharePoint Server DB SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Old FileType	Doc_Type
Request Context	All of (EventData, Event_ID, Permission, EventMessage)
Source Address	Machine_IP
Source Host Name	Machine_Name
Source NT Domain	Extract NTDomain (User_Name)
Source Process Name	Event_Source
Source User Id	User_ID
Source User Name	Extract User Name(User_Name)
Source User Privileges	Permission

SharePoint Query General Mappings

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Permission Level ID
Device Custom Number 2	New Audit Mask
Device Custom String 2	Event ID
Device Custom String 3	Item Version

Mappings for Audit Event 1

ArcSight ESM Field	Device-Specific Field
Message	",VersionMajor,".",VersionMinor," was checked out."

Mappings for Audit Event 2

ArcSight ESM Field	Device-Specific Field
Message	All of (VersionMajor, '.', VersionMinor, 'is the new version of the document.')

Mappings for Audit Event 3

ArcSight ESM Field	Device-Specific Field
Message	'Viewed item'

Mappings for Audit Event 4

ArcSight ESM Field	Device-Specific Field
Message	One of ('All versions were deleted and moved to the Recycle Bin', 'All versions were deleted completely')

Mappings for Audit Event 5

ArcSight ESM Field	Device-Specific Field
Device Custom Number 3	Group ID
File Name	EventMessage
Message	'Updated Item'

Mappings for Audit Event 6

ArcSight ESM Field	Device-Specific Field
File Name	ProfileTargetName
File Type	FileID
Message	All of (ProfileDescription, 'The location is', ProfileTargetName)

Mappings for Audit Event 7

ArcSight ESM Field	Device-Specific Field
File ID	RelatedItemID
File Type	RelatedItemType (1=Document, 3=Item, 4=List, 5=Folder, 6=Site, 7=Site Collection)
FileName	RelatedItemLocation
Message	All of ('Deleted child at', RelatedItemLocation, 'GUID=', RelatedItemID)

Mappings for Audit Event 8

ArcSight ESM Field	Device-Specific Field
Message	All of ('Change in the schema of the object on those columns:', FieldRefColName, FieldColName)
Request URL	FieldSourceID

Mappings for Audit Event 10

ArcSight ESM Field	Device-Specific Field
Message	"Restoration of deleted items from the site collection recycle bin"

Mappings for Audit Event 12

ArcSight ESM Field	Device-Specific Field
Message	Both ('Copying object to', EventMessage)
Request URL	EventMessage

Mappings for Audit Event 13

ArcSight ESM Field	Device-Specific Field
File Name	NewRelativeURL
Message	All of ('Moving object to', NewRelativeURL)

Mappings for Audit Event 14

ArcSight ESM Field	Device-Specific Field
Device Custom Number 2	New Audit Mask
Message	Both ('The new audit mask is', NewAuditMask)

Mappings for Audit Event 15

ArcSight ESM Field	Device-Specific Field
Additional data	EventMessage
Message	'The search term and the object that is searched.'

Mappings for Audit Event 16

ArcSight ESM Field	Device-Specific Field
File ID	RelatedItemID
File Name	RelatedItemNewName
Message	All of ('Moved child to', RelatedItemNewName, 'GUID=', RelatedItemID)

Mappings for Audit Event 30

ArcSight ESM Field	Device-Specific Field
Destination User ID	UserID
Device Custom Number 3	Group ID
Device Custom String 6	Group Name
Message	All of ('New group', NewGroupName, '(Group ID=', NewGroupID, ') was created by user ID', UserID)

Mappings for Audit Event 31

ArcSight ESM Field	Device-Specific Field
Device Custom Number 3	Group ID
Message	All of ('Group ID', NewGroupID, 'was deleted')

Mappings for Audit Event 32

ArcSight ESM Field	Device-Specific Field
Destination NT Domain	UserName
Destination User ID	NewUserID
Destination User Name	UserName
Device Custom Number 3	Group ID
Message	All of ('Member ID', NewUserID, 'was added to group ID', NewGroupID)

Mappings for Audit Event 33

ArcSight ESM Field	Device-Specific Field
Destination User ID	UserID
Device Custom Number 3	Group ID
Message	'Member ID', UserID, 'was deleted from group ID', NewGroupID)

Mappings for Audit Event 34

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Permission Level ID
Message	All of ('New permission level:', PermissionLevelName, 'was created. The ID is', PermissionLevelID)
Source User Privileges	PermissionLevelName

Mappings for Audit Event 35

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Permission Level ID
Message	All of ('Permission level ID', PermissionLevelID, 'was deleted')

Mappings for Audit Event 36

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	Permission Level ID
Message	All of ('Updated permission:', PermissionLevelName, 'level ID', PermissionLevelID)
Source User Privileges	PermissionLevelName

Mappings for Audit Event 38

ArcSight ESM Field	Device-Specific Field
Additional data	SubsiteGUID
Destination User Privileges	Permission
Device Custom Number 3	Group ID
Message	All of ('Updated permission (Permission ID =', RoleID, 'for group or user ID', PrincipalID)

Mappings for Audit Events 39, 40

ArcSight ESM Field	Device-Specific Field
Additional data	URL
Additional data	SubsiteGUID
Message	All of ('The URL of the subsite is', URL, 'GUID of the subsite is', SubsiteGUID)

Mappings for Audit Event 50

ArcSight ESM Field	Device-Specific Field
End Time	DeleteEntriesEndDate
Message	All of ('Deleted', DeleteEntriesRows', entries at ', DeleteEntriesEndDate)

Mappings for Audit Event 100

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	Policy Name
Device Custom String 5	Policy ID
Message	Both (CustomPolicyDescription, CustomPolicyStatement)

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. 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 SharePoint Server 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 SQL Server Multiple Instance Audit 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 SQL Server Multiple Instance Audit DB SmartConnector	5
Product Overview	7
Prerequisites	7
Downloading the JDBC Driver	7
Mounting a Drive on Linux Platforms	8
Verifying if the TCP/IP Connection is Enabled with SQL Server 2008	9
Creating a Local SQL Server User	10
Creating a Domain User from the Domain Controller	11
Sharing Permissions for the Database Log Folder	14
Enabling Auditing	18
Enabling General Trace Auditing	19
Using a sample Procedure to Enable and Configure Auditing	19
C2 Auditing	21
Installing the SmartConnector	24
Preparing to Install Connector	24
Installing and Configuring the SmartConnector	24
Adding a JDBC Driver to the Connector Appliance/ArcSight Management Center ..	28
Running the Connector with a Standard Domain User Account	30
On the Domain Controller	30
On the Microsoft SQL Server 2005 Host	30
On the Connector Host	31
Creating the Trace File Access Share	32
Changing the Name of Processed Files	33
Device Event Mapping to ArcSight Fields	34

SQL Server Mappings to ArcSight ESM Events	34
Audit Events 104, 105, 106, 107	35
Audit Event 108	35
Audit Event 109	36
Audit Event 110	36
Audit Event 111	36
Audit Event 113	37
Audit Event 114	37
Audit Event 115, 118, 177	37
Audit Event 10, 12	38
Audit Event 13, 14, 15, 17	38
Troubleshooting	39
SQL Server Sample Audit Procedures	43
SQL Server 2008 and Later	43
SQL Server 2005	67
SQL Server 2000	81
Send Documentation Feedback	85

Configuration Guide for Microsoft SQL Server Multiple Instance Audit DB SmartConnector

This guide provides information for installing the SmartConnector for Microsoft SQL Server Multiple Instance Audit DB and configuring the device for audit log event collection via the SQL Trace mechanism. For supported devices and versions, see [Technical Requirements](#).

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

Microsoft SQL Server provides auditing as a way to trace and record activity that has happened on each instance of SQL Server (for example, successful and failed logins). SQL Server also provides an interface (SQL Query Analyzer) for managing audit records.

There are two possible authentication methods that can be used with the SmartConnector for Microsoft SQL Server Audit DB – *Microsoft Windows Authentication* and *Mixed Mode Authentication* (which uses both SQL Server and Windows authentication). Although Microsoft recommends Windows Authentication, this document describes installing and configuring the SmartConnector using both methods of authentication.

Prerequisites

Before installing the SmartConnector, perform the following configuration steps:

- [Download the SQL Server JDBC driver](#)
- [If installing the SmartConnector on Linux platforms, mount a drive on Linux platforms](#)
- [For SQL Server 2008, verify if TCP/IP connection is enabled](#)
- [Create a Local SQL Server User](#)
- [Create a Domain SQL Server User](#)
- [Share permissions for the database log folder](#)
- [Enable Auditing](#)

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](#).

Mounting a Drive on Linux Platforms

When installing the SmartConnector on Linux platforms, complete the following steps to allow connector access to the trace files on the SQL Server machine:

To mount the drive:

1. Open a terminal window.
2. Execute the following commands:

```
id <user>
sudo mkdir <mount point>
```

Replace:

<user> with the username of the user running the connector
<mount point> with the actual mount point on the Linux machine (for example, /mnt/mssql)

3. Execute the following command:

```
sudo mount //<ipaddressOfSQLServer>/<sqltrace> <mount point> -o
nosuid,uid=<uid>,gid=<guid>,username=<SQLServerusername>,password=<SQL
Serverpassword>,rw
```

Replace:

<sqltrace> with the name of the shared drive containing the trace files
<uid> and <guid> with information from execution of the commands in step 2
<SQLServerusername> and <SQLServerpassword> with the actual Windows share user and password required to access the SQL Server.

4. To verify the shared folder was successfully mounted, execute the following command:

```
ls <mount point>
```

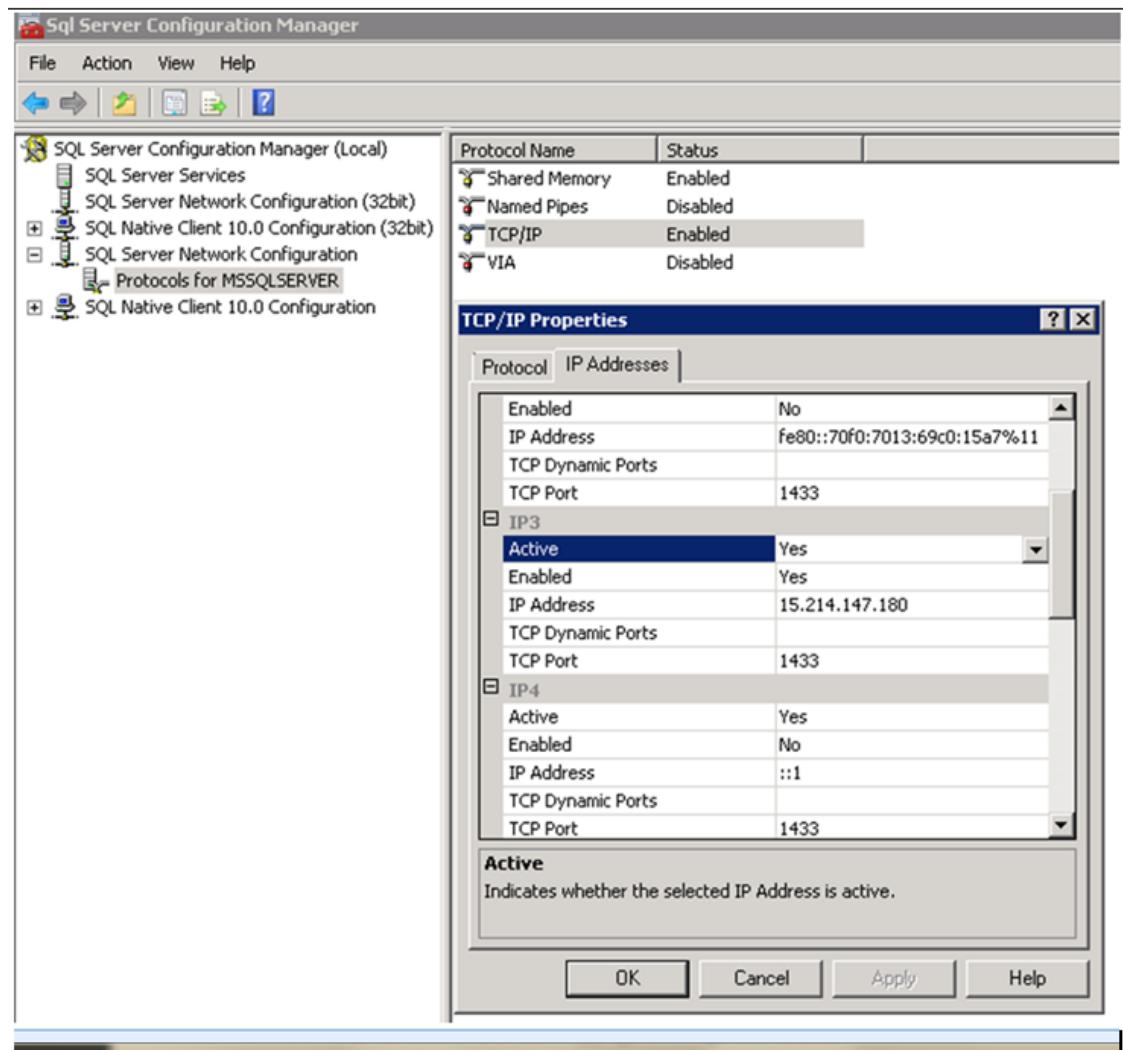
Verifying if the TCP/IP Connection is Enabled with SQL Server 2008

Connection to the SQL Server might be refused if the TCP/IP connection is not enabled.

To verify, complete the following steps:

1. Open **Start > All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > SQL Server Configuration Manager**.
2. In the left pane, expand **SQL Server Network Configuration** and select **Protocols for [your server]**.

3. Double-click **TCP/IP** and ensure that the IP address you are using to connect to your SQL Server is active and enabled.



Creating a Local SQL Server User

You must create a local SQL Server user when using SQL Server Authentication. Complete the following steps to create a local SQL Server user on SQL Server 2005 and later versions (2005, 2008, 2012, 2014, 2016) and to collect events using a non-administrative SQL Server 2005, 2008, 2012, 2014, 2016 database account:

1. Right-click **Security > Logins** and select **New Login...** to create a new database user account named `sqlaudit`.

2. On the **General** tab, select **SQL Server authentication** and provide a password for `sqlaudit`.
3. From the **User Mapping** tab, check the box in the **Map** column for the **master database** to set the default database of this user to master.
4. Grant this user (`sqlaudit`) **Connect**, **Execute**, and **Select** permissions.
5. Select **SQL Server > Properties > Security > Enable proxy account** to enable the proxy account to the `sqlaudit` user.
6. Go to **SQL Server > Properties > Permissions** and grant the user permission to **Alter trace**.

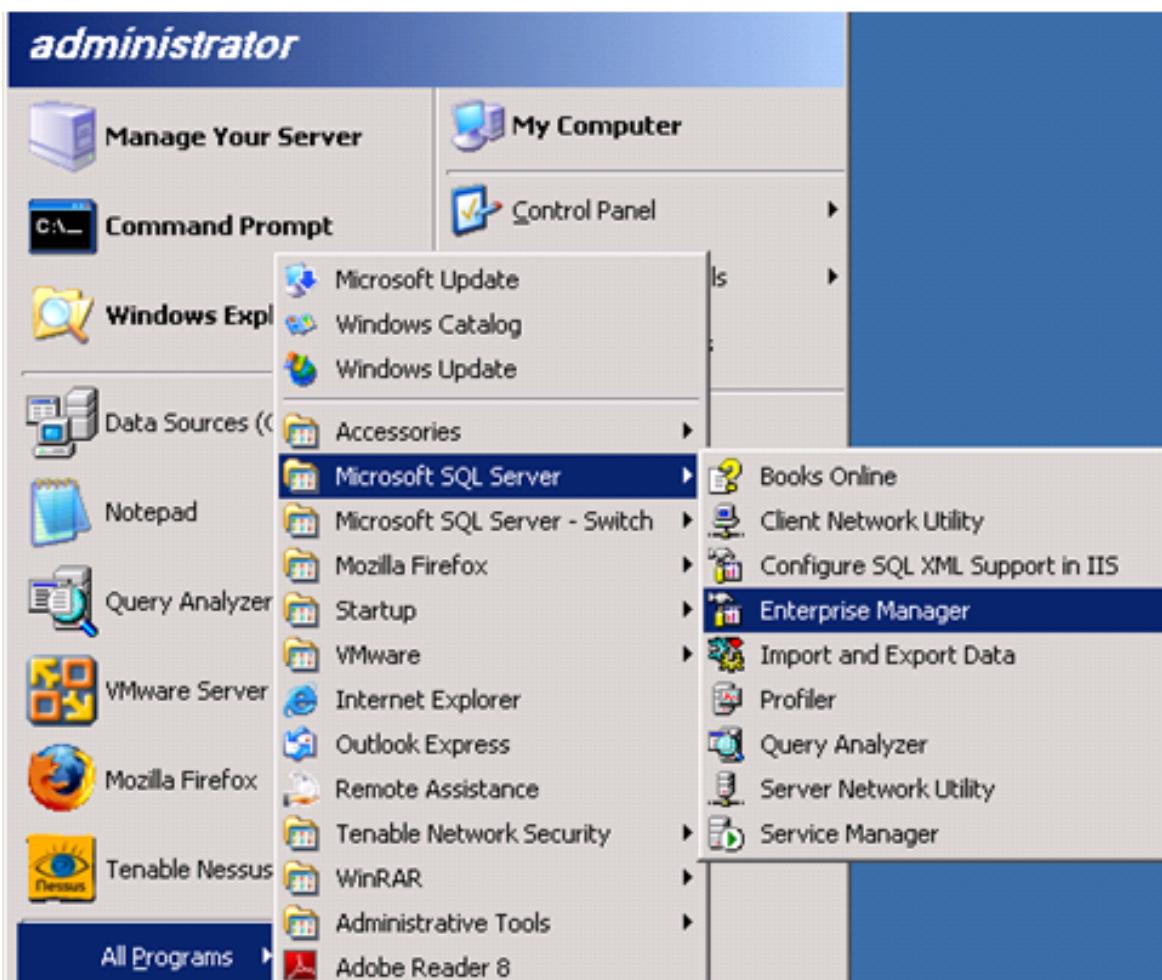
Creating a Domain User from the Domain Controller

This step is required for all authentication modes and operating system environments. System administrator privilege is required for SQL Server database access and for granting folder permissions.

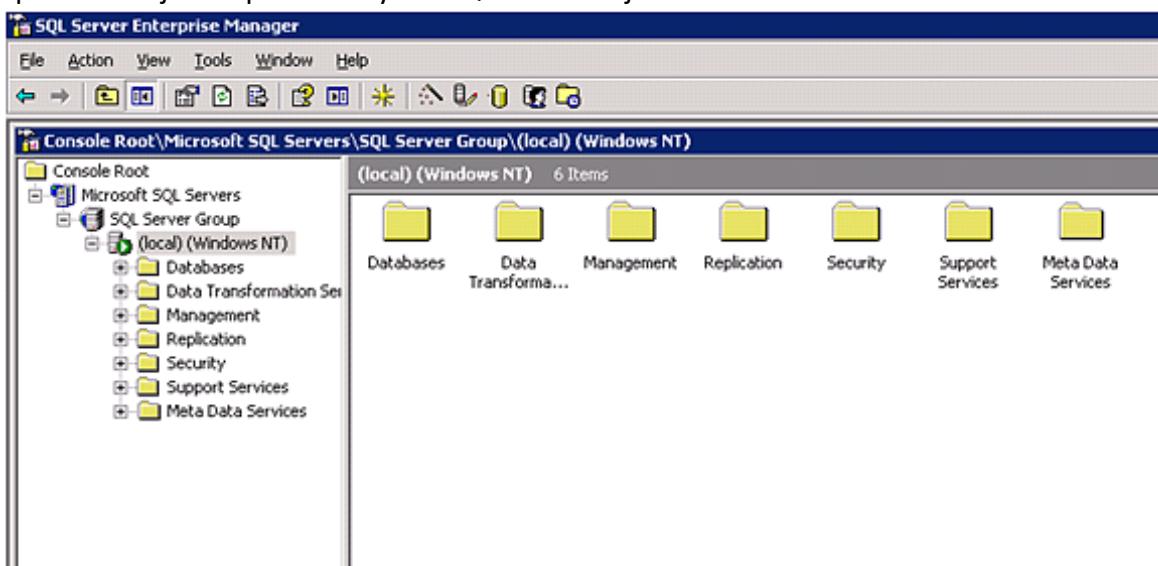
A valid SQL Logon ID (either SQL user account or a Domain/Windows user account) must be used and granted specific database permissions (see [Sharing Permissions for the Database Log Folder](#)).

The following procedure can be used to create a user in a Windows environment with Windows authentication.

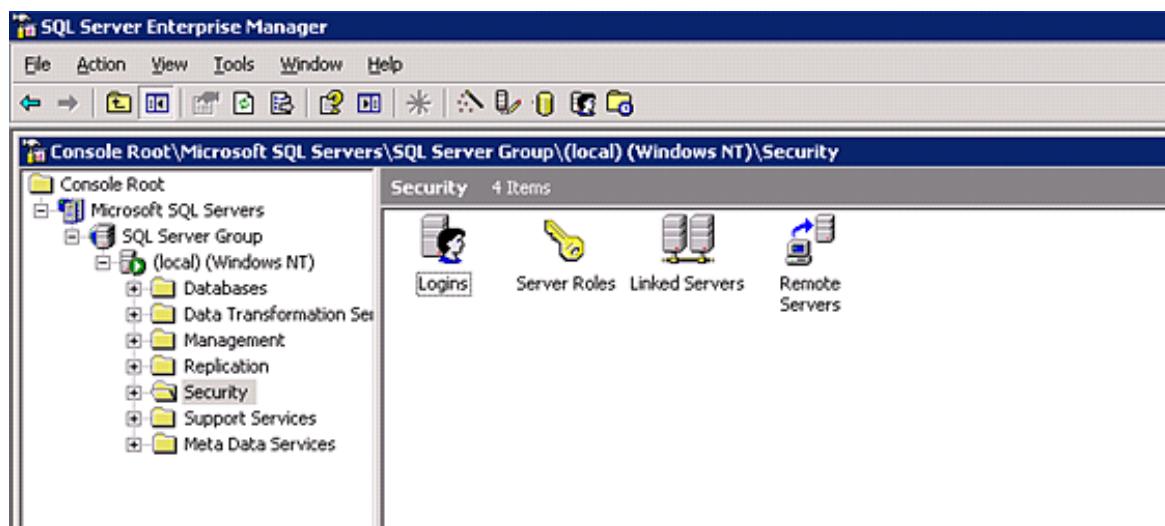
1. From the **Domain Controller**, access **Enterprise Manager** or **Server Management Studio** or from the **Start** menu, select **All Programs > Microsoft SQL Server > Enterprise Manager | Server Management Studio**.



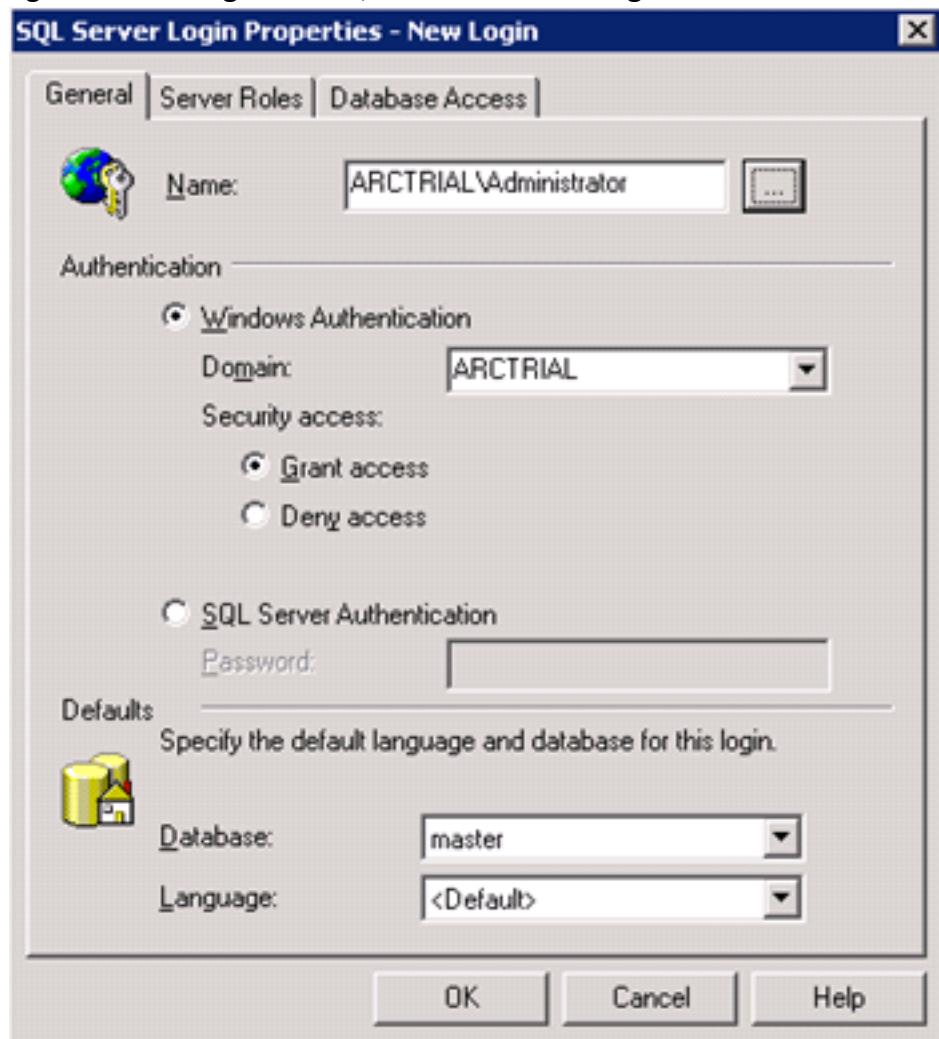
2. Open the Object Explorer for your SQL Server object.



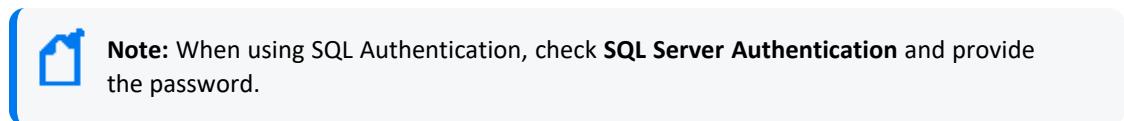
3. Expand the **Security** folder.



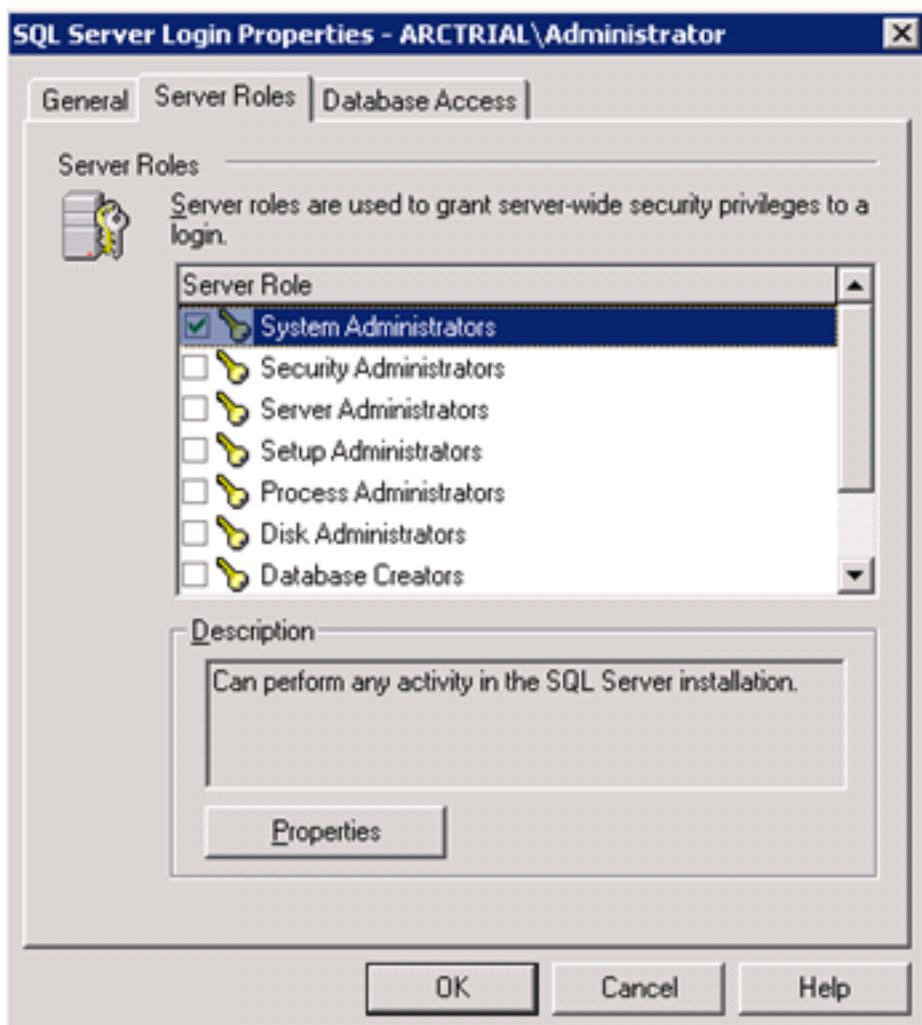
4. Right-click the **Logins** folder, then select **New Login**.



5. Select the Domain/Windows user account to be associated with the new SQL Server login.



6. Click the **Server Roles** tab; Check **System Administrators** and click **OK**.



Sharing Permissions for the Database Log Folder

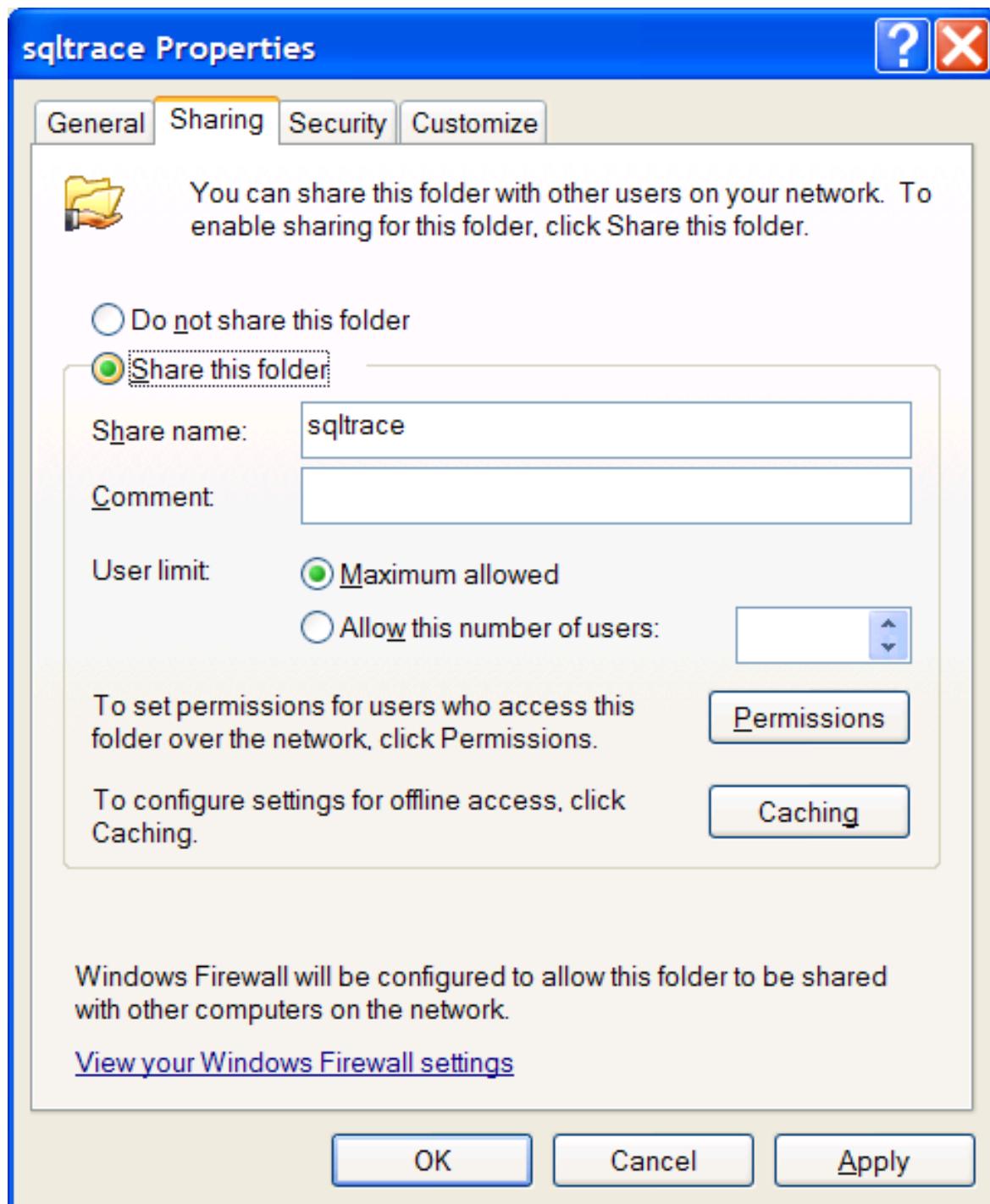
By default the Windows Service account is a local system account that will not have permission to access an SQL Server setup for Windows Authentication. So, for Windows

Authentication to work, the SQL Audit Connector Service must run as a valid Windows account that has been granted permissions in the SQL Server.

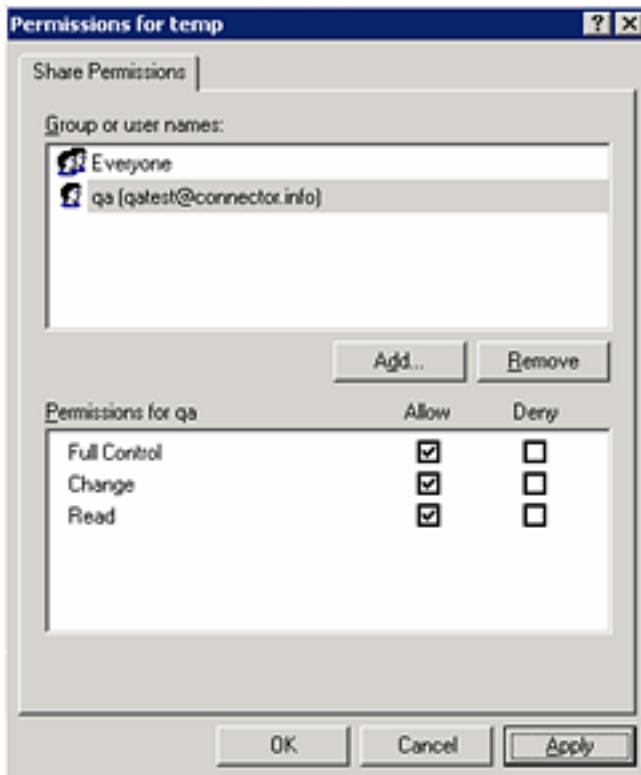
Use a valid SQL Logon ID,either SQL user account or a Domain/Windows user account and grant specific database permissions.

To share permissions for the database log folder:

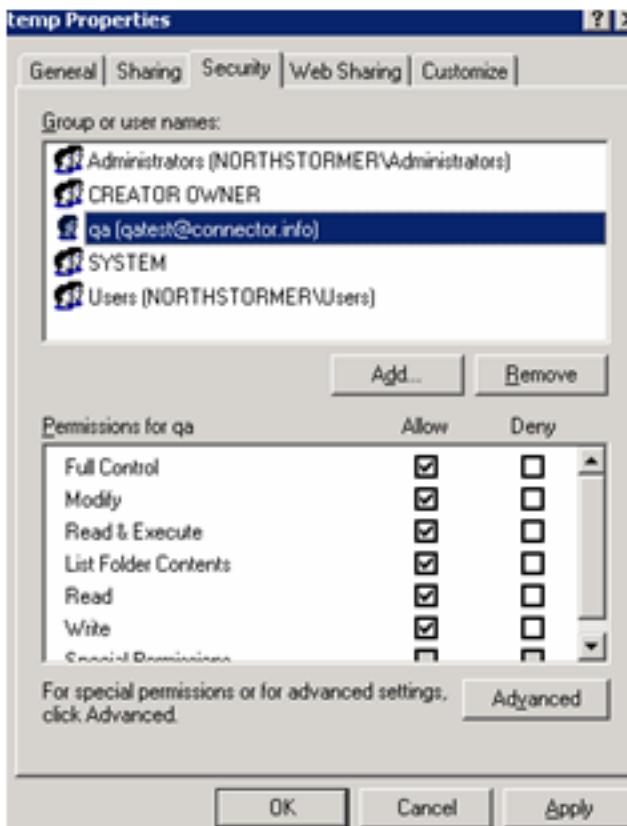
1. Log in to the SQL Server database machine.
2. Right-click the name of the log file folder (sqltrace in this example), then select **Properties**.
3. From the **Sharing** tab, select **Share this folder** and enter the name of the folder in the **Share name** field.



4. For **User limit**, keep the default value of **Maximum allowed** selected, or select **Allow this number of users** and select a value, then click **Apply**.
5. Click the **Permissions** button.



6. Click **Add** to add the user you created in [Create a Domain User from the Domain Controller](#).
7. Check **Allow** for **Full Control**, **Change**, and **Read** for this user, then click **Apply**.
8. Click **OK** to exit the **Permissions** window.
9. Click the **Security** tab and select the Domain Controller user you created.
10. Grant **Allow** permission for **Full Control** to this user.



11. Click **Apply** and then **OK** to exit the **Properties** window.

Enabling Auditing

SQL Server provides auditing as a way to trace and record activity on each instance of SQL Server (for example, successful and failed logins). SQL Server also provides an interface, SQL Query Analyzer, to manage audit records.

 **Note:** Auditing can only be enabled or modified by members of the 'sysadmin' fixed security role and every modification of an audit is an auditable event.

You can enable the following types of audit:

- **General trace auditing**, which provides some level of auditing but does not require the same number of policies as C2 auditing.
- **C2 auditing**, which requires that you follow very specific security policies. If you intend to enable C2 auditing, you should not audit to the Application log, since SQL Server will write audit information about user login activity to two places

simultaneously and unnecessarily degrade system performance. After you change audit settings, the database must be restarted.

Both these auditing can be done using SQL Query Analyzer, which provides a graphical user interface to monitor an instance of SQL Server.



Note: With Windows authentication mode, the user account that runs SQL Query Analyzer must be granted permission to connect to an instance of SQL Server. For C2 auditing, sysadmin privilege is required.

You can run SQL Query Analyzer directly from inside SQL Server Enterprise Manager.

During their installation process, many applications, including SQL Server, register with the event-log subsystem. Note that **SQL Server's ability to audit login activity (including failed login attempts) to the Windows Application Log is not enabled by default.**

Enabling General Trace Auditing

To configure auditing, launch **Enterprise Manager** or **Management Studio**, select a database server, right-click **Properties**, go to the **Security** tab, and set your desired level of auditing.

Even after enabling auditing to the Application log, details about user activity such as which tables users access, which queries users run, and which stored procedures users invoke are not provided.

Although SQL Server can audit user actions, your DBA must activate this feature. DBAs have unrestricted access to databases on the database server and are responsible for database management. In many environments, the systems administrator or network administrator is also the DBA.

Using a sample Procedure to Enable and Configure Auditing



If SQL Server auditing has already been enabled and configured on your sever, this procedure is not required.

To enable automatic auditing upon server startup, create a procedure to enable the auditing function. For more information see, [Sample SQL Audit Procedures](#).

- Within the sample procedure, replace the occurrences of the path to the trace folder with your actual path and file name (for example, c:\sqltrace\MyTrace.trc).
- Use a unique file name. If the file already exists, the SQL Server fails when you enable the trace.
- To understand the commands in sample procedures, see [What the Sample Procedures Collect](#).



If you are writing from a remote server to a local drive, use the UNC path and make sure the server has write access to your network share.

What the Sample Procedures Collect

Each trace statement in the procedure traces an Event ID and Column ID.

To see the current versions of column and event IDs, use the links below to see the events for SQL Server that can be added to or removed from a trace:

- For SQL Server 2005 and later (2008, 2012, 2014, 2016) Event IDs, see:
<http://msdn.microsoft.com/en-us/library/ms186265.aspx> and select the **Other Versions** drop-down list to select the appropriate version.

The `sp_trace_setevent` command is used in the sample procedure to add an event class or data column to a trace, or to remove one from it. The `AuditTrcProc` script provided determines the events, and the columns within the events, to be traced. You can add to or delete from the events specified to be traced in the sample procedure using the `sp_trace_setevent` command.

The `sp_trace_setevent` format is:

```
sp_trace_setevent @traceid, <event_id> <column_id> @on
```

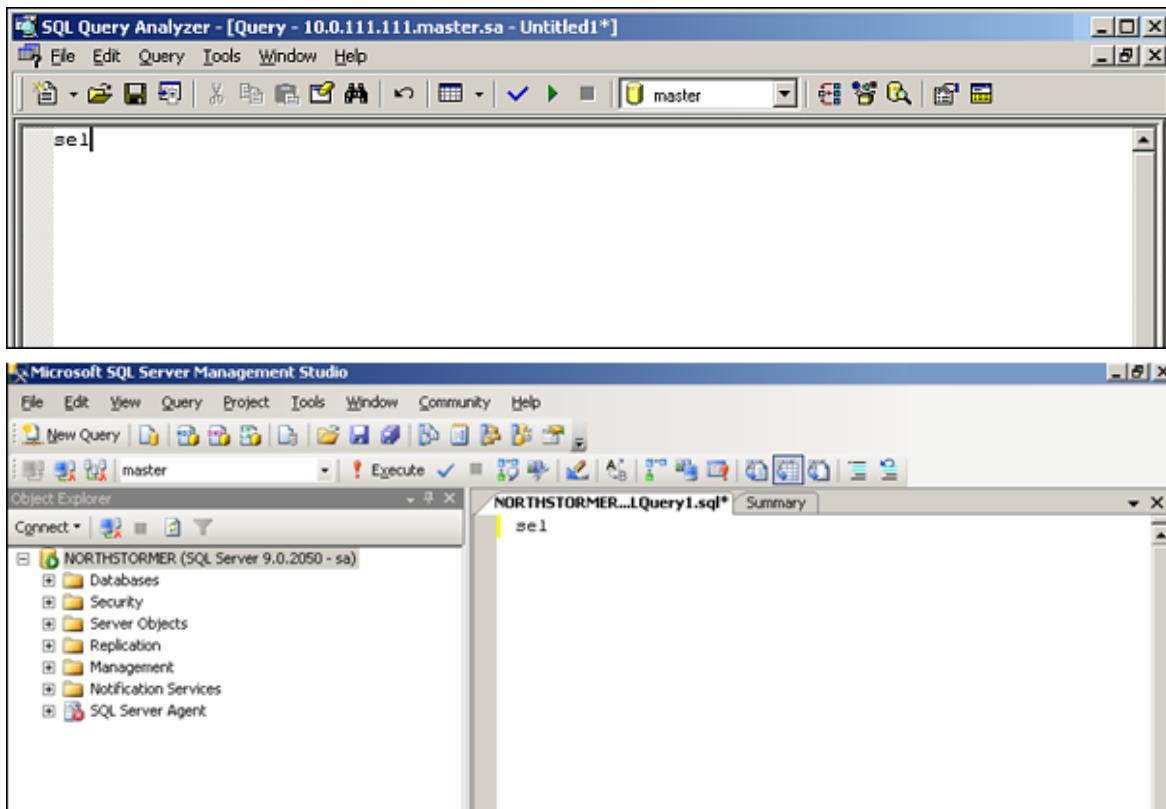
where the `<event ID>` and `<column ID>` to be traced have been specified. To fine-tune or modify the events to be traced, see the `sp_trace_setevent` Transact-SQL statement in *SQL Server 2005 Books Online* for all event IDs and column IDs supported.



For events to be parsed properly, be sure to select the same columns for each event type you trace.

Using the Sample Procedure

1. Perform the following steps from the SQL Query Analyzer. You can run SQL Query Analyzer directly from the **Start** menu, or you can run it from inside SQL Server Enterprise Manager.



2. Copy the content of the procedure to the SQL Query Analyzer new query pane, saving it as AuditTrcProc.sql.

3. Execute the procedure with the following SQL command:

```
EXEC AuditTrcProc
```

4. Make this procedure start automatically when the SQL Server restarts by executing the following command:

```
USE master
EXEC sp_procoption 'AuditTrcProc', 'startup', 'TRUE';
```

5. Verify whether the audit is being enabled as expected by running the following query:

```
SELECT * FROM :: fn_trace_getinfo(default)
```

6. Exit from the SQL Query Analyzer.

C2 Auditing

The **c2 audit mode** option is used to review both successful and unsuccessful attempts to access statements and objects. With this information, you can document system activity and look for security policy violations.

C2 auditing tracks C2 audit events and records them to a file in the \mssql\data directory for default instances of SQL Server, or the \mssql\$instanceName\data directory for named instances of SQL Server. If the file reaches a size limit of 200 MB, C2 auditing will start a new file, close the old file, and write all new audit records to the new file. This process continues until SQL Server is shut down or auditing is turned off.

Implications with C2 Auditing

Note the following implications with C2 auditing:

- As a best practice, store databases and their transaction logs on a dedicated disk device to avoid the following issues:
 - On a system that has limited disk space, you might find that our databases cannot grow because audit log files are consuming all the free space.
 - On a busy system, performance might suffer because both the databases and the audit logs use the same disk.
- SQL Server writes all auditable activity to a file with the format audittrace_YYYYMMDDHHMMSS.trc where YYYYMMDDHHMMSS is the log's creation time by year, month, day, hour, minute, and second. When a log reaches a maximum size of 200 MB, SQL Server automatically creates a new log and begins to record to the new log instead. This feature lets you safely move old log files out of the data folder or delete them.
- If SQL Server cannot write to a log file (for example, if the disk contains no more free space), it will halt all execution. SQL Server does not restart until it can resume logging. If you need to force SQL Server to run even though logging is not possible, you can use the -f flag to start a minimal SQL Server configuration from the command line. Using the -m flag with the -f flag starts the database in single-user mode, preventing clients from connecting to the database and performing transactions while auditing is disabled.

Enabling C2 Auditing from Command Line

1. Run the following query:

```
USE master
    EXEC sp_configure 'show advanced option','1'
    RECONFIGURE
    GO
    USE master
    EXEC sp_configure 'c2 audit mode','1'
    RECONFIGURE
```

2. Stop and start the server for C2 audit mode to take effect.

Enabling C2 Auditing with SQL Query Analyzer

Before enabling C2 auditing, note the following:

- You must be a member of the sysadmin role to enable or disable C2 auditing.
- You must have Sysadmin privilege to enable or disable this option.
- C2 audit mode is an advanced option. If you are using the sp_configure system stored procedure to change the setting, you can change C2 audit mode only when 'show advanced options' is set to '1.'

To enable C2 auditing with SQL Query Analyzer:

1. In the SQL Query Analyzer, enable the show advanced options configuration option using the following command:

```
USE master
EXEC sp_configure 'show advanced option', '1'
RECONFIGURE
```

2. To enable the feature, set c2 audit mode to 1 using the following command:

```
sp_configure 'c2 audit mode', 1
go
```

3. To disable the feature, set c2 audit mode to 0:

```
sp_configure 'c2 audit mode', 0
go
```

4. Stop and start the server for C2 audit mode to take effect.

After you enable C2 auditing for the default database or for an instance, the database server will log all activity to the data directory you specified during the installation process. (SQL Server does not let you log auditable events to an alternative location.) This directory holds the databases that SQL Server initially created. This directory is also the default location for all new databases and their transaction log files.

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 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 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 SQL Server Multiple Instance Audit DB** from the Type drop-down, then click **Next**.
10. Enter the following SmartConnector parameters to configure the SmartConnector, then click **Next**.

Configuration Guide for Microsoft SQL Server Multiple Instance Audit DB SmartConnector

Installing the SmartConnector

Parameters	Description
Windows Share Domain	Not shown for Windows platforms. Enter the name of the domain to be shared.
Windows Share User	Not shown for Windows platforms. Enter the name of the user for the Share Domain.
Windows Share Password	Not shown for Windows platforms. Enter the password for the Windows Share User.
JDBC Database Driver	Select the database driver com.microsoft.sqlserver.jdbc.SQLServerDriver.
Trace File Post Processing Mode	Values that can be set for this field are 'RenameFileInTheSameDirectory', 'DeleteFile', or 'PersistFile'. The connector performs some tests during configuration to make sure the folder on the SQL Server Instance containing the trace files has permissions to perform the post processing operation "DeleteFile" or 'RenameFileInTheSameDirectory'. If Post Processing Mode is set to one of these values and the trace file folder does not have permissions, the configuration setup warns you. It performs the same checks when the connector is run, and the connector will not process any trace files if the trace file folder does not have permissions for the post processing mode selected. This parameter has been implemented to prevent kernel panic on the Connector Appliance caused by read-only CIFS shares containing the trace files. The default value is 'RenameFileInTheSameDirectory'.

11. Click Add, then specify the following parameters:

Parameter	Description
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>. If you are configuring additional databases, click Add each time you want to enter a new row for each new database or instance. Change the URL for the database driver and the other values as appropriate.  NOTE: With Windows authentication, the local and remote machines must be on the same domain, and the user must have full control permissions to access the trace file folder on the remote machine.
User	Enter the login name of the user that you created on the DC machine in Create a Domain User from the Domain Controller .
Password	Enter the password assigned to the DC SQL Server user.

Configuration Guide for Microsoft SQL Server Multiple Instance Audit DB SmartConnector

Installing the SmartConnector

Parameter	Description
Audit Type	Select C2_AUDIT or GENERAL_AUDIT. If you want both types of audit on the same database instance, add one row to the parameter entry table selecting GENERAL_AUDIT and another row specifying the same database instance, but with C2_AUDIT selected.
Trace File Local Folder	Enter the path specifying the local folder on the SQL Server machine (for example, c:\sqltrace) to which the SQL Server Audit trace files are written. When typing back slashes in the file path, it is not necessary to escape them in the Installation Wizard. They are automatically escaped. If you enter the file path in the Agent Configuration Wizard later, the backslashes must be escaped.
Connector Data Folder	<p>Enter the path specifying the local folder on the SmartConnector machine to which the SQL Server Audit trace files are written.</p> <p>Scenario #1: When SQL Server and the SmartConnector are installed on the same machine, enter the same folder path specified for the "Trace Local Folder" parameter. (For example: c:\sqltrace.)</p> <p>Scenario #2: When the SmartConnector is installed on a Windows machine separate from the SQL Server, map a network drive on the SmartConnector machine to the shared folder on the SQL Server machine. (For example, map c:\sqltrace on SQL Server machine to z:\ on the SmartConnector machine.) Then, type the network share drive (z:\) as the value in the Connector Data Folder field.</p> <div style="border-left: 3px solid blue; padding-left: 10px;"><p>Note: When running the SmartConnector as a service, mapped drives do not work. For a service, use the remote network shared drives in the UNC Notation (For example \\servername.name.domain.com\foldername). When typing back slashes in the file path, it is not necessary to escape them in the Installation Wizard. They are automatically escaped. If you enter the file path in the Agent Configuration Wizard later, the backslashes must be escaped.</p></div> <p>Scenario #3: When installing the SmartConnector on Linux, use a mounted drive (e.g. /mnt/mssql) as the value in the "Connector Data Folder" field. Please see the "Mount a Drive on Linux Platforms" for more information.</p> <div style="border-left: 3px solid blue; padding-left: 10px;"><p>NOTE: If you use mapped drives, be aware of potential problems after a system reboot when SQL Server is started automatically. SQL Server will often start before the shares have been mapped and can cause a warning of a potential problem that occurs because the database engine could not open the database files. To solve this, restart SQL Server to reset the suspect flag or flags. If you use mapped files, it is a good idea to configure SQL Server to start manually after a system reboot.</p></div>

12. You can click the **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 add the data manually.

13. Select a [destination and configure parameters](#).
14. Specify a name for the connector.
15. (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.

16. Select whether you want to install the connector as a service or in the standalone mode.
17. Complete the installation.
18. [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*.

Running the Connector with a Standard Domain User Account

A Standard Domain User account can be used to run the connector only when the Microsoft SQL Server is set to Windows Authentication mode. Certain limitations apply related to the choice of the connector installation host, which are explained below. Configuration steps are required from the Domain Controller, the Microsoft SQL Server 2005 Host, and on the connector host, as described in the following sections.

On the Domain Controller

1. Create a new user account (for example, *arcsight*).
2. Add this new user to the **Remote Desktop Users** group.

On the Microsoft SQL Server 2005 Host

1. Open the MS SQL Server Management Studio to set the MS SQL Server to Windows Authentication mode.
2. From Object Explorer in the left pane, select the MS SQL Server host of interest, then right-click and select **Properties**.
3. Click the **Security** tab and set the **Server Authentication** to **Windows Authentication** mode. Click **OK**.
4. Restart the MS SQL Server service.
5. Return to the MS SQL Server Management Studio to set the appropriate permissions for the Standard Domain User *arcsight*.
6. From Object Explorer in the left pane, select the MS SQL Server host of interest and expand its tree.
7. Go to **Security > Logins**, then right-click and select **New Login**.
8. Click the **General** tab. Populate the **Login Name** box by using **Search** to select the new domain user *arcsight*. The option of Windows Authentication is automatically selected. The default database is automatically set to **master**.
9. Click the **User Mapping** tab. Select the **master** database.
10. Click the **Status** tab. **Permission to connect to database engine** is automatically set to **Grant** and **Login** is automatically set to **Enabled**. Click **OK**.

11. Go to **Databases > System Databases**, right-click **master** and select **Properties**.
12. Click the **Permissions** tab. From the **Users or roles** table, select the domain user **arcsight**.
13. From the **Explicit Permissions** table, select the **Grant** option for the **Connect, Execute, Select, and View** database state permissions. Click **OK**.
14. Select the MS SQL Server host of interest, right-click and select **Properties**.
15. Click the **Security** tab. In the **Server proxy account** section, select **Enable server proxy account**. Set the **Proxy account** and **Password** fields to the domain user **arcsight** and its password. Click **OK**.
16. Click the **Permissions** tab and select the domain user **arcsight** from the **Logins or roles** table.
17. From the **Explicit Permissions** table, select the **Grant** option for the **Alter trace, Connect SQL, and View server state** permissions. Click **OK**.
18. In Windows Explorer, go to the folder where the trace files are being logged (for example, `c:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\LOG`). Right-click and select **Sharing and Security**.
19. Click the **Sharing** tab and select **Share this folder**. Provide a share name if one is not present (for example, **LOG**). Click **Apply**.
20. Click the **Security** tab and go to the **Group or user names** table. Using **Add**, add the domain user **arcsight** and select that user.
21. For the selected **arcsight** user, go to the **Permissions for** table and select all the permissions available, including **Full Control**. Click **Apply**.
22. Now click **Advanced** and a new window entitled **Advanced Security Settings for** is displayed.
23. Go to the **Permission entries** table and select the user **arcsight**. Click **Edit** and ensure that all the permissions are **Allowed for This folder, subfolders and files**. Click **OK**.
24. For the selected **arcsight** user, select the option **Replace permission entries on all child objects with entries shown here that apply to child objects**. Click **Apply**. A new dialog box displays the message "This will remove explicitly defined permissions on all child objects and enable propagation of inheritable permissions to those child objects. Only inheritable permissions propagated from <share name> will take effect. Do you wish to continue?" Click **Yes**. Click **OK**.
25. Click **OK**.

On the Connector Host

When using Windows Authentication mode on the MS SQL Server, access to the SQL Server is possible only from Windows hosts belonging to the same domain as the domain of the MS SQL

Server host. Using Windows hosts whose domain has a trust relationship with the domain of the MS SQL Server host has not been verified.

Using a non-Windows host with the Windows authentication mode enabled is not supported, even when you are using a JDBC driver, because that non-Windows host is not part of a Windows domain, which is a requirement.

Make sure that you log in to the connector host with the same Standard Domain User account ***arcsight***, for which all the permissions to access the MS SQL Server trace files have been set.

Creating the Trace File Access Share

If you have already mapped a Network drive to access the trace files on the MS SQL Server, disconnect and remove that share. Create the network share again to access the Trace files on the MS SQL Server. Ensure that you can rename any old trace file and set it back to its original file name.

Changing the Name of Processed Files

To change the name of processed trace files:

1. From the \$ARCSIGHT_HOME\current\user\agent directory, open agent.properties to edit.
2. Locate the eventlogtypes parameter. Enter the appropriate event log names. The initial value is null.
3. Locate the mode and modeoptions parameters. Change the mode to **RenameFileInTheSameDirectory** to rename the file.
4. Enter a string for the modeoptions parameter. This string will be the suffix.

For example, if you enter processed, the file name is renamed to xxxx.processed.



Specifying **DeleteFile** will cause the file to be deleted. Specifying **RenameFileInTheSameDirectory** will cause the file to be renamed in the same directory. Using **PersistFile** will cause the file to be persisted.

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.

SQL Server Mappings to ArcSight ESM Events

ArcSight ESM Field	Device-Specific Field
Destination Host Name	ServerName
Destination NT Domain	NTDomainName
Destination Process Name	SPID
Destination User Name	LoginName
Destination User Privileges	Permissions
Device Action	EventClass
Device Custom Number 1	Duration
Device Custom Number 2	Reads
Device Custom Number 3	Writes
Device Custom String 1	ObjectName
Device Custom String 2	DatabaseName
Device Custom String 3	FileName
Device Custom String 4	OwnerName
Device Custom String 5	LoginSid
Device Custom String 6	_DB_NAME
Device Event Class ID	EventClass Success EventSubClass
Device External ID	DatabaseID
Device Host Name	_DB_HOST _DB_DSN
Device Product	'SQL Server'
Device Receipt Time	StartTime
Device Severity	EventClass Success EventSubClass
Device Vendor	'Microsoft'

Configuration Guide for Microsoft SQL Server Multiple Instance Audit DB SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Version	'Unknown'
Event Outcome	'Success' 'Failure'
Event Old File ID	Request ID:RequestID
Flex Number 1	CPU
Message	TextData
Reason	errorCode
Source Host Name	HostName
Source Process Name	ClientProcessID
Source Service Name	ApplicationName
Target Host Name	ServerName

Audit Events 104, 105, 106, 107

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetLoginName
File Hash	Line Number: LineNumber
File Type	Object Type:ObjectType
Source Host Name	ServerName
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	SessionLoginName LoginName

Audit Event 108

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetLoginName
Device Custom String 6	RoleName
File Type	Object Type:ObjectType
Source Host Name	ServerName

ArcSight ESM Field	Device-Specific Field
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	SessionLoginName LoginName

Audit Event 109

ArcSight ESM Field	Device-Specific Field
Destination User ID	TargetLoginName
Destination User Name	TargetUserName
Device Custom String 6	RoleName
Source Host Name	ServerName
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	SessionLoginName LoginName

Audit Event 110

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Device Custom String 6	RoleName
File Type	Object Type:ObjectType
Source Host Name	Servername
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	SessionLoginName LoginName

Audit Event 111

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	RoleName

Audit Event 113

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Device Custom String 3 Label	DBUserName
File Hash	Line Number: LineNumber
Source Host Name	ServerName
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	SessionLoginName LoginName

Audit Event 114

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Device Custom Number 3	ColumnPermissions
Device Custom String 3 Label	DBUserName
Device Custom String 6	ParentName
File Hash	Line Number: LineNumber
File Type	Object Type: ObjectType
Source Host Name	ServerName
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	SessionLoginName LoginName

Audit Event 115, 118, 177

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Device Custom String 3 Label	DBUserName
File Hash	Line Number: LineNumber

ArcSight ESM Field	Device-Specific Field
File Type	ObjectType: ObjectType
Source Host Name	ServerName
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	SessionLoginName LoginName

Audit Event 10, 12

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
File Hash	Row Counts:RowCounts
File ID	Group ID:GroupID
Source Host Name	ServerName
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	SessionLoginName LoginName

Audit Event 13, 14, 15, 17

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserName
Source Host Name	ServerName
Source NT Domain	NTDomainName
Source Process Name	SPID
Source User Name	LoginName

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. 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 receive events.

"If multiple SQL DB instances on the same host are depositing their Trace files into a common folder, will one MS SQL connector instance retrieve all audit events?"

Yes. But there must be a separate table entry for each instance and the trace files from each of the instances must be identified somehow uniquely; for example, by the instance name itself. Then the wildcard parameter could be specified separately for each of the entries. If the wildcard is not unique, there would be a problem because the connector launches multiple threads monitoring the same folder and processing the same files. The behavior would be somewhat unpredictable.

"I started the connector and there is no error in agent.log, but I did not get any events. Why is that?"

First check whether you did enable the audit by querying the database (as indicated in "Configuration"). If you did enable the audit, you may not have received any events because the SQL Server will hold the trace file until the file reaches the 1 MB size, then rotate. If you did not audit a number of high traffic events, chances are that you will wait for some time. Try to look at the folder on the machine the connector is monitoring.

"Why do I receive a 'the trace file is not ready for processing' message?"

This message is normal for the trace file to which SQL Server is currently writing because that file is not finished yet and hence not ready for processing. If it is occurring for all the trace files, there usually is a permission problem wherein the connector does not have the permission to rename the trace file. If you do not want the files renamed, you can change the **Trace File Post Processing Mode** parameter to PersistFile, in which case the connector just remembers the files it has processed. To do this:

- 1 From a DOS prompt, go to the \$ARCSIGHT_HOME\current\bin directory.

- 2** Double-click runagentsetup.bin.
- 3** Select **Modify Connector**; click **Next**.
- 4** Select **Modify connector parameters**; click **Next**.
- 5** Select **PersistFile** for the **Trace File Post Process Mode** parameter.
- 6** Click **Next** to continue. Click **Next** on the **Modify table parameters** window.
- 7** Click **Next** on the **Successfully updated parameters** window, and then check **Exit** and click **Next** to exit the wizard.



You can have the connector delete rather than rename the trace file by changing the mode value to 'DeleteFile'.

- 8** Restart the SmartConnector for your change to take effect.

"Why did I receive a message that the xp_cmdshell module has been turned off?"

With Microsoft SQL Server 2005, the xp_cmdshell module is turned OFF by default. To turn it on, there is a "Surface Area Configuration" tool in Microsoft SQL Server Programs group that will let you configure this, or you can enter the following commands in SQL Query Analyzer:

```
EXECUTE sp_configure 'show advanced options', 1
RECONFIGURE WITH OVERRIDE
GO
EXECUTE sp_configure 'xp_cmdshell', '1'
RECONFIGURE WITH OVERRIDE
GO
EXECUTE sp_configure 'show advanced options', 0
RECONFIGURE WITH OVERRIDE
GO
```

"What is the recommended configuration?"

It depends upon the case. For example, say we have an SQL Server machine (named S) and a connector machine (named A). If the database is busy, remotely install the connector; then, with the connector installed in A, monitor the folder remotely.

"What is the default size the SQL Server rotates for C2 Audit as well as for general auditing?"

C2 auditing rotation size is 200 M, which cannot be changed. General auditing rotation size is from 1 M to 5 M (the sample SQL above is configured to 1 M because we want the events loaded and sent to ArcSight Manager as quickly as possible).

"I run my connector as a service through the UNC path for access and DSN. The service failed to start, why is that?"

First, check the case we answered in the first question, then make sure to right-click on the Connector service name to make sure the Windows user can access the remote SQL Server Windows machine, and that this user can start the local Windows service. You can always right-click on the service name, select Properties, and change "Log on as" to "This account" to use a different user for test.

One use case is that if you configure the SQL Server to log trace to c:\trace (for example), you set up a scheduled job to move the trace files from time-to-time to c:\tmpdata (for example), and then you let the Connector in machine A monitor the \\S\tmpdata folder. In this case, when you configure the Connector, you would set the parameter as follows:

```
Folder of Trace Data File (Read by connector) \\S\tmpdata
Trace File Folder on Local SQL Server Machine C:\tmpdata
```

The cronjob can be as simple as (for example): Move c:\trace\sessiontrace*.trc
c:\tmpdata

Note that the latest file is always held by the SQL Server until it reaches a certain size, then is rotated.

Another use case is to monitor the c:\trace above directly, whether locally or remotely. For example, if the connector monitors the folder remotely, then the folder of trace data files (read by the connector) is \\S\trace. The trace file folder on the local SQL Server machine is **C:\trace**.

SQL Server Sample Audit Procedures

To enable automatic auditing upon server startup, create a procedure to enable the auditing function. Three sample procedures are provided to assist you in this task. These procedures enable auditing and specify the events to be audited.

SQL Server 2008 and Later

```
CREATE PROC AuditTrcProc AS
-- Create a Queue declare @rc int declare @TraceID int declare @maxfilesize
bigint set @maxfilesize = 1
-- Please replace the file name with an appropriate file name prefixed by a
path,
e.g., C:\sqltrace\sessionTrace.
-- The .trc extension will be appended to the filename automatically.
-- If you are writing from remote server to local drive, use UNC path and make
sure server has write access to your network share
declare @cmd sysname
set @cmd = 'copy c:\sqltrace\sessiontrace.trc c:\sqltrace\sessiontrace' + cast
(cast(rand() * 1000000 as int) as varchar) print @cmd
exec master..xp_cmdshell @cmd
set @cmd= 'del c:\sqltrace\sessiontrace.trc' print @cmd
exec master..xp_cmdshell @cmd
exec @rc = sp_trace_create @TraceID output, 2, N'c:\sqltrace\sessiontrace',
@maxfilesize, null if (@rc != 0) goto error
-- Client side File and Table cannot be scripted
-- Set the events and columns declare @on bit set @on = 1
exec sp_trace_setevent @TraceID, 10, 1, @on
exec sp_trace_setevent @TraceID, 10, 3, @on
```

```
exec sp_trace_setevent @TraceID, 10, 6, @on
exec sp_trace_setevent @TraceID, 10, 7, @on
exec sp_trace_setevent @TraceID, 10, 8, @on
exec sp_trace_setevent @TraceID, 10, 9, @on
exec sp_trace_setevent @TraceID, 10, 10, @on
exec sp_trace_setevent @TraceID, 10, 11, @on
exec sp_trace_setevent @TraceID, 10, 12, @on
exec sp_trace_setevent @TraceID, 10, 13, @on
exec sp_trace_setevent @TraceID, 10, 14, @on
exec sp_trace_setevent @TraceID, 10, 15, @on
exec sp_trace_setevent @TraceID, 10, 16, @on
exec sp_trace_setevent @TraceID, 10, 17, @on
exec sp_trace_setevent @TraceID, 10, 18, @on
exec sp_trace_setevent @TraceID, 10, 21, @on
exec sp_trace_setevent @TraceID, 10, 23, @on
exec sp_trace_setevent @TraceID, 10, 26, @on
exec sp_trace_setevent @TraceID, 10, 27, @on
exec sp_trace_setevent @TraceID, 10, 34, @on
exec sp_trace_setevent @TraceID, 10, 35, @on
exec sp_trace_setevent @TraceID, 10, 36, @on
exec sp_trace_setevent @TraceID, 10, 37, @on
exec sp_trace_setevent @TraceID, 10, 38, @on
exec sp_trace_setevent @TraceID, 10, 39, @on
exec sp_trace_setevent @TraceID, 10, 41, @on
exec sp_trace_setevent @TraceID, 10, 42, @on
exec sp_trace_setevent @TraceID, 10, 43, @on
exec sp_trace_setevent @TraceID, 10, 64, @on
```

```
exec sp_trace_setevent @TraceID, 12, 1, @on
exec sp_trace_setevent @TraceID, 12, 3, @on
exec sp_trace_setevent @TraceID, 12, 6, @on
exec sp_trace_setevent @TraceID, 12, 7, @on
exec sp_trace_setevent @TraceID, 12, 8, @on
exec sp_trace_setevent @TraceID, 12, 9, @on
exec sp_trace_setevent @TraceID, 12, 10, @on
exec sp_trace_setevent @TraceID, 12, 11, @on
exec sp_trace_setevent @TraceID, 12, 12, @on
exec sp_trace_setevent @TraceID, 12, 13, @on
exec sp_trace_setevent @TraceID, 12, 14, @on
exec sp_trace_setevent @TraceID, 12, 15, @on
exec sp_trace_setevent @TraceID, 12, 16, @on
exec sp_trace_setevent @TraceID, 12, 17, @on
exec sp_trace_setevent @TraceID, 12, 18, @on
exec sp_trace_setevent @TraceID, 12, 21, @on
exec sp_trace_setevent @TraceID, 12, 23, @on
exec sp_trace_setevent @TraceID, 12, 26, @on
exec sp_trace_setevent @TraceID, 12, 27, @on
exec sp_trace_setevent @TraceID, 12, 34, @on
exec sp_trace_setevent @TraceID, 12, 35, @on
exec sp_trace_setevent @TraceID, 12, 36, @on
exec sp_trace_setevent @TraceID, 12, 37, @on
exec sp_trace_setevent @TraceID, 12, 38, @on
exec sp_trace_setevent @TraceID, 12, 39, @on
exec sp_trace_setevent @TraceID, 12, 41, @on
exec sp_trace_setevent @TraceID, 12, 42, @on
exec sp_trace_setevent @TraceID, 12, 43, @on
```

```
exec sp_trace_setevent @TraceID, 12, 64, @on  
  
exec sp_trace_setevent @TraceID, 14, 1, @on  
exec sp_trace_setevent @TraceID, 14, 3, @on  
exec sp_trace_setevent @TraceID, 14, 6, @on  
exec sp_trace_setevent @TraceID, 14, 7, @on  
exec sp_trace_setevent @TraceID, 14, 8, @on  
exec sp_trace_setevent @TraceID, 14, 9, @on  
exec sp_trace_setevent @TraceID, 14, 10, @on  
exec sp_trace_setevent @TraceID, 14, 11, @on  
exec sp_trace_setevent @TraceID, 14, 12, @on  
exec sp_trace_setevent @TraceID, 14, 13, @on  
exec sp_trace_setevent @TraceID, 14, 14, @on  
exec sp_trace_setevent @TraceID, 14, 15, @on  
exec sp_trace_setevent @TraceID, 14, 16, @on  
exec sp_trace_setevent @TraceID, 14, 17, @on  
exec sp_trace_setevent @TraceID, 14, 18, @on  
exec sp_trace_setevent @TraceID, 14, 21, @on  
exec sp_trace_setevent @TraceID, 14, 23, @on  
exec sp_trace_setevent @TraceID, 14, 26, @on  
exec sp_trace_setevent @TraceID, 14, 27, @on  
exec sp_trace_setevent @TraceID, 14, 34, @on  
exec sp_trace_setevent @TraceID, 14, 35, @on  
exec sp_trace_setevent @TraceID, 14, 36, @on  
exec sp_trace_setevent @TraceID, 14, 37, @on  
exec sp_trace_setevent @TraceID, 14, 38, @on  
exec sp_trace_setevent @TraceID, 14, 39, @on  
exec sp_trace_setevent @TraceID, 14, 41, @on
```

```
exec sp_trace_setevent @TraceID, 14, 42, @on
exec sp_trace_setevent @TraceID, 14, 43, @on
exec sp_trace_setevent @TraceID, 14, 64, @on
exec sp_trace_setevent @TraceID, 15, 1, @on
exec sp_trace_setevent @TraceID, 15, 3, @on
exec sp_trace_setevent @TraceID, 15, 6, @on
exec sp_trace_setevent @TraceID, 15, 7, @on
exec sp_trace_setevent @TraceID, 15, 8, @on
exec sp_trace_setevent @TraceID, 15, 9, @on
exec sp_trace_setevent @TraceID, 15, 10, @on
exec sp_trace_setevent @TraceID, 15, 11, @on
exec sp_trace_setevent @TraceID, 15, 12, @on
exec sp_trace_setevent @TraceID, 15, 13, @on
exec sp_trace_setevent @TraceID, 15, 14, @on
exec sp_trace_setevent @TraceID, 15, 15, @on
exec sp_trace_setevent @TraceID, 15, 16, @on
exec sp_trace_setevent @TraceID, 15, 17, @on
exec sp_trace_setevent @TraceID, 15, 18, @on
exec sp_trace_setevent @TraceID, 15, 21, @on
exec sp_trace_setevent @TraceID, 15, 23, @on
exec sp_trace_setevent @TraceID, 15, 26, @on
exec sp_trace_setevent @TraceID, 15, 27, @on
exec sp_trace_setevent @TraceID, 15, 34, @on
exec sp_trace_setevent @TraceID, 15, 35, @on
exec sp_trace_setevent @TraceID, 15, 36, @on
exec sp_trace_setevent @TraceID, 15, 37, @on
exec sp_trace_setevent @TraceID, 15, 38, @on
```

Configuration Guide for Microsoft SQL Server Multiple Instance Audit DB SmartConnector
SQL Server Sample Audit Procedures

```
exec sp_trace_setevent @TraceID, 15, 39, @on
exec sp_trace_setevent @TraceID, 15, 41, @on
exec sp_trace_setevent @TraceID, 15, 42, @on
exec sp_trace_setevent @TraceID, 15, 43, @on
exec sp_trace_setevent @TraceID, 15, 64, @on
exec sp_trace_setevent @TraceID, 17, 1, @on
exec sp_trace_setevent @TraceID, 17, 3, @on
exec sp_trace_setevent @TraceID, 17, 6, @on
exec sp_trace_setevent @TraceID, 17, 7, @on
exec sp_trace_setevent @TraceID, 17, 8, @on
exec sp_trace_setevent @TraceID, 17, 9, @on
exec sp_trace_setevent @TraceID, 17, 10, @on
exec sp_trace_setevent @TraceID, 17, 11, @on
exec sp_trace_setevent @TraceID, 17, 12, @on
exec sp_trace_setevent @TraceID, 17, 13, @on
exec sp_trace_setevent @TraceID, 17, 14, @on
exec sp_trace_setevent @TraceID, 17, 15, @on
exec sp_trace_setevent @TraceID, 17, 16, @on
exec sp_trace_setevent @TraceID, 17, 17, @on
exec sp_trace_setevent @TraceID, 17, 18, @on
exec sp_trace_setevent @TraceID, 17, 21, @on
exec sp_trace_setevent @TraceID, 17, 23, @on
exec sp_trace_setevent @TraceID, 17, 26, @on
exec sp_trace_setevent @TraceID, 17, 27, @on
exec sp_trace_setevent @TraceID, 17, 34, @on
exec sp_trace_setevent @TraceID, 17, 35, @on
exec sp_trace_setevent @TraceID, 17, 36, @on
```

```
exec sp_trace_setevent @TraceID, 17, 37, @on
exec sp_trace_setevent @TraceID, 17, 38, @on
exec sp_trace_setevent @TraceID, 17, 39, @on
exec sp_trace_setevent @TraceID, 17, 41, @on
exec sp_trace_setevent @TraceID, 17, 42, @on
exec sp_trace_setevent @TraceID, 17, 43, @on
exec sp_trace_setevent @TraceID, 17, 64, @on

exec sp_trace_setevent @TraceID, 104, 1, @on
exec sp_trace_setevent @TraceID, 104, 3, @on
exec sp_trace_setevent @TraceID, 104, 6, @on
exec sp_trace_setevent @TraceID, 104, 7, @on
exec sp_trace_setevent @TraceID, 104, 8, @on
exec sp_trace_setevent @TraceID, 104, 9, @on
exec sp_trace_setevent @TraceID, 104, 10, @on
exec sp_trace_setevent @TraceID, 104, 11, @on
exec sp_trace_setevent @TraceID, 104, 12, @on
exec sp_trace_setevent @TraceID, 104, 13, @on
exec sp_trace_setevent @TraceID, 104, 14, @on
exec sp_trace_setevent @TraceID, 104, 15, @on
exec sp_trace_setevent @TraceID, 104, 16, @on
exec sp_trace_setevent @TraceID, 104, 17, @on
exec sp_trace_setevent @TraceID, 104, 18, @on
exec sp_trace_setevent @TraceID, 104, 21, @on
exec sp_trace_setevent @TraceID, 104, 23, @on
exec sp_trace_setevent @TraceID, 104, 26, @on
exec sp_trace_setevent @TraceID, 104, 27, @on
exec sp_trace_setevent @TraceID, 104, 34, @on
```

```
exec sp_trace_setevent @TraceID, 104, 35, @on
exec sp_trace_setevent @TraceID, 104, 36, @on
exec sp_trace_setevent @TraceID, 104, 37, @on
exec sp_trace_setevent @TraceID, 104, 38, @on
exec sp_trace_setevent @TraceID, 104, 39, @on
exec sp_trace_setevent @TraceID, 104, 41, @on
exec sp_trace_setevent @TraceID, 104, 42, @on
exec sp_trace_setevent @TraceID, 104, 43, @on
exec sp_trace_setevent @TraceID, 104, 64, @on

exec sp_trace_setevent @TraceID, 105, 1, @on
exec sp_trace_setevent @TraceID, 105, 3, @on
exec sp_trace_setevent @TraceID, 105, 6, @on
exec sp_trace_setevent @TraceID, 105, 7, @on
exec sp_trace_setevent @TraceID, 105, 8, @on
exec sp_trace_setevent @TraceID, 105, 9, @on
exec sp_trace_setevent @TraceID, 105, 10, @on
exec sp_trace_setevent @TraceID, 105, 11, @on
exec sp_trace_setevent @TraceID, 105, 12, @on
exec sp_trace_setevent @TraceID, 105, 13, @on
exec sp_trace_setevent @TraceID, 105, 14, @on
exec sp_trace_setevent @TraceID, 105, 15, @on
exec sp_trace_setevent @TraceID, 105, 16, @on
exec sp_trace_setevent @TraceID, 105, 17, @on
exec sp_trace_setevent @TraceID, 105, 18, @on
exec sp_trace_setevent @TraceID, 105, 21, @on
exec sp_trace_setevent @TraceID, 105, 23, @on
exec sp_trace_setevent @TraceID, 105, 26, @on
```

```
exec sp_trace_setevent @TraceID, 105, 27, @on
exec sp_trace_setevent @TraceID, 105, 34, @on
exec sp_trace_setevent @TraceID, 105, 35, @on
exec sp_trace_setevent @TraceID, 105, 36, @on
exec sp_trace_setevent @TraceID, 105, 37, @on
exec sp_trace_setevent @TraceID, 105, 38, @on
exec sp_trace_setevent @TraceID, 105, 39, @on
exec sp_trace_setevent @TraceID, 105, 41, @on
exec sp_trace_setevent @TraceID, 105, 42, @on
exec sp_trace_setevent @TraceID, 105, 43, @on
exec sp_trace_setevent @TraceID, 105, 64, @on

exec sp_trace_setevent @TraceID, 106, 1, @on
exec sp_trace_setevent @TraceID, 106, 3, @on
exec sp_trace_setevent @TraceID, 106, 6, @on
exec sp_trace_setevent @TraceID, 106, 7, @on
exec sp_trace_setevent @TraceID, 106, 8, @on
exec sp_trace_setevent @TraceID, 106, 9, @on
exec sp_trace_setevent @TraceID, 106, 10, @on
exec sp_trace_setevent @TraceID, 106, 11, @on
exec sp_trace_setevent @TraceID, 106, 12, @on
exec sp_trace_setevent @TraceID, 106, 13, @on
exec sp_trace_setevent @TraceID, 106, 14, @on
exec sp_trace_setevent @TraceID, 106, 15, @on
exec sp_trace_setevent @TraceID, 106, 16, @on
exec sp_trace_setevent @TraceID, 106, 17, @on
exec sp_trace_setevent @TraceID, 106, 18, @on
exec sp_trace_setevent @TraceID, 106, 21, @on
```

```
exec sp_trace_setevent @TraceID, 106, 23, @on
exec sp_trace_setevent @TraceID, 106, 26, @on
exec sp_trace_setevent @TraceID, 106, 27, @on
exec sp_trace_setevent @TraceID, 106, 34, @on
exec sp_trace_setevent @TraceID, 106, 35, @on
exec sp_trace_setevent @TraceID, 106, 36, @on
exec sp_trace_setevent @TraceID, 106, 37, @on
exec sp_trace_setevent @TraceID, 106, 38, @on
exec sp_trace_setevent @TraceID, 106, 39, @on
exec sp_trace_setevent @TraceID, 106, 41, @on
exec sp_trace_setevent @TraceID, 106, 42, @on
exec sp_trace_setevent @TraceID, 106, 43, @on
exec sp_trace_setevent @TraceID, 106, 64, @on

exec sp_trace_setevent @TraceID, 107, 1, @on
exec sp_trace_setevent @TraceID, 107, 3, @on
exec sp_trace_setevent @TraceID, 107, 6, @on
exec sp_trace_setevent @TraceID, 107, 7, @on
exec sp_trace_setevent @TraceID, 107, 8, @on
exec sp_trace_setevent @TraceID, 107, 9, @on
exec sp_trace_setevent @TraceID, 107, 10, @on
exec sp_trace_setevent @TraceID, 107, 11, @on
exec sp_trace_setevent @TraceID, 107, 12, @on
exec sp_trace_setevent @TraceID, 107, 13, @on
exec sp_trace_setevent @TraceID, 107, 14, @on
exec sp_trace_setevent @TraceID, 107, 15, @on
exec sp_trace_setevent @TraceID, 107, 16, @on
exec sp_trace_setevent @TraceID, 107, 17, @on
```

```
exec sp_trace_setevent @TraceID, 107, 18, @on
exec sp_trace_setevent @TraceID, 107, 21, @on
exec sp_trace_setevent @TraceID, 107, 23, @on
exec sp_trace_setevent @TraceID, 107, 26, @on
exec sp_trace_setevent @TraceID, 107, 27, @on
exec sp_trace_setevent @TraceID, 107, 34, @on
exec sp_trace_setevent @TraceID, 107, 35, @on
exec sp_trace_setevent @TraceID, 107, 36, @on
exec sp_trace_setevent @TraceID, 107, 37, @on
exec sp_trace_setevent @TraceID, 107, 38, @on
exec sp_trace_setevent @TraceID, 107, 39, @on
exec sp_trace_setevent @TraceID, 107, 41, @on
exec sp_trace_setevent @TraceID, 107, 42, @on
exec sp_trace_setevent @TraceID, 107, 43, @on
exec sp_trace_setevent @TraceID, 107, 64, @on
```

```
exec sp_trace_setevent @TraceID, 108, 1, @on
exec sp_trace_setevent @TraceID, 108, 3, @on
exec sp_trace_setevent @TraceID, 108, 6, @on
exec sp_trace_setevent @TraceID, 108, 7, @on
exec sp_trace_setevent @TraceID, 108, 8, @on
exec sp_trace_setevent @TraceID, 108, 9, @on
exec sp_trace_setevent @TraceID, 108, 10, @on
exec sp_trace_setevent @TraceID, 108, 11, @on
exec sp_trace_setevent @TraceID, 108, 12, @on
exec sp_trace_setevent @TraceID, 108, 13, @on
exec sp_trace_setevent @TraceID, 108, 14, @on
exec sp_trace_setevent @TraceID, 108, 15, @on
```

```
exec sp_trace_setevent @TraceID, 108, 16, @on
exec sp_trace_setevent @TraceID, 108, 17, @on
exec sp_trace_setevent @TraceID, 108, 18, @on
exec sp_trace_setevent @TraceID, 108, 21, @on
exec sp_trace_setevent @TraceID, 108, 23, @on
exec sp_trace_setevent @TraceID, 108, 26, @on
exec sp_trace_setevent @TraceID, 108, 27, @on
exec sp_trace_setevent @TraceID, 108, 34, @on
exec sp_trace_setevent @TraceID, 108, 35, @on
exec sp_trace_setevent @TraceID, 108, 36, @on
exec sp_trace_setevent @TraceID, 108, 37, @on
exec sp_trace_setevent @TraceID, 108, 38, @on
exec sp_trace_setevent @TraceID, 108, 39, @on
exec sp_trace_setevent @TraceID, 108, 41, @on
exec sp_trace_setevent @TraceID, 108, 42, @on
exec sp_trace_setevent @TraceID, 108, 43, @on
exec sp_trace_setevent @TraceID, 108, 64, @on
exec sp_trace_setevent @TraceID, 109, 1, @on
exec sp_trace_setevent @TraceID, 109, 3, @on
exec sp_trace_setevent @TraceID, 109, 6, @on
exec sp_trace_setevent @TraceID, 109, 7, @on
exec sp_trace_setevent @TraceID, 109, 8, @on
exec sp_trace_setevent @TraceID, 109, 9, @on
exec sp_trace_setevent @TraceID, 109, 10, @on
exec sp_trace_setevent @TraceID, 109, 11, @on
exec sp_trace_setevent @TraceID, 109, 12, @on
exec sp_trace_setevent @TraceID, 109, 13, @on
```

```
exec sp_trace_setevent @TraceID, 109, 14, @on
exec sp_trace_setevent @TraceID, 109, 15, @on
exec sp_trace_setevent @TraceID, 109, 16, @on
exec sp_trace_setevent @TraceID, 109, 17, @on
exec sp_trace_setevent @TraceID, 109, 18, @on
exec sp_trace_setevent @TraceID, 109, 21, @on
exec sp_trace_setevent @TraceID, 109, 23, @on
exec sp_trace_setevent @TraceID, 109, 26, @on
exec sp_trace_setevent @TraceID, 109, 27, @on
exec sp_trace_setevent @TraceID, 109, 34, @on
exec sp_trace_setevent @TraceID, 109, 35, @on
exec sp_trace_setevent @TraceID, 109, 36, @on
exec sp_trace_setevent @TraceID, 109, 37, @on
exec sp_trace_setevent @TraceID, 109, 38, @on
exec sp_trace_setevent @TraceID, 109, 39, @on
exec sp_trace_setevent @TraceID, 109, 41, @on
exec sp_trace_setevent @TraceID, 109, 42, @on
exec sp_trace_setevent @TraceID, 109, 43, @on
exec sp_trace_setevent @TraceID, 109, 64, @on
exec sp_trace_setevent @TraceID, 110, 1, @on
exec sp_trace_setevent @TraceID, 110, 3, @on
exec sp_trace_setevent @TraceID, 110, 6, @on
exec sp_trace_setevent @TraceID, 110, 7, @on
exec sp_trace_setevent @TraceID, 110, 8, @on
exec sp_trace_setevent @TraceID, 110, 9, @on
exec sp_trace_setevent @TraceID, 110, 10, @on
exec sp_trace_setevent @TraceID, 110, 11, @on
```

```
exec sp_trace_setevent @TraceID, 110, 12, @on
exec sp_trace_setevent @TraceID, 110, 13, @on
exec sp_trace_setevent @TraceID, 110, 14, @on
exec sp_trace_setevent @TraceID, 110, 15, @on
exec sp_trace_setevent @TraceID, 110, 16, @on
exec sp_trace_setevent @TraceID, 110, 17, @on
exec sp_trace_setevent @TraceID, 110, 18, @on
exec sp_trace_setevent @TraceID, 110, 21, @on
exec sp_trace_setevent @TraceID, 110, 23, @on
exec sp_trace_setevent @TraceID, 110, 26, @on
exec sp_trace_setevent @TraceID, 110, 27, @on
exec sp_trace_setevent @TraceID, 110, 34, @on
exec sp_trace_setevent @TraceID, 110, 35, @on
exec sp_trace_setevent @TraceID, 110, 36, @on
exec sp_trace_setevent @TraceID, 110, 37, @on
exec sp_trace_setevent @TraceID, 110, 38, @on
exec sp_trace_setevent @TraceID, 110, 39, @on
exec sp_trace_setevent @TraceID, 110, 41, @on
exec sp_trace_setevent @TraceID, 110, 42, @on
exec sp_trace_setevent @TraceID, 110, 43, @on
exec sp_trace_setevent @TraceID, 110, 64, @on
exec sp_trace_setevent @TraceID, 111, 1, @on
exec sp_trace_setevent @TraceID, 111, 3, @on
exec sp_trace_setevent @TraceID, 111, 6, @on
exec sp_trace_setevent @TraceID, 111, 7, @on
exec sp_trace_setevent @TraceID, 111, 8, @on
exec sp_trace_setevent @TraceID, 111, 9, @on
```

```
exec sp_trace_setevent @TraceID, 111, 10, @on
exec sp_trace_setevent @TraceID, 111, 11, @on
exec sp_trace_setevent @TraceID, 111, 12, @on
exec sp_trace_setevent @TraceID, 111, 13, @on
exec sp_trace_setevent @TraceID, 111, 14, @on
exec sp_trace_setevent @TraceID, 111, 15, @on
exec sp_trace_setevent @TraceID, 111, 16, @on
exec sp_trace_setevent @TraceID, 111, 17, @on
exec sp_trace_setevent @TraceID, 111, 18, @on
exec sp_trace_setevent @TraceID, 111, 21, @on
exec sp_trace_setevent @TraceID, 111, 23, @on
exec sp_trace_setevent @TraceID, 111, 26, @on
exec sp_trace_setevent @TraceID, 111, 27, @on
exec sp_trace_setevent @TraceID, 111, 34, @on
exec sp_trace_setevent @TraceID, 111, 35, @on
exec sp_trace_setevent @TraceID, 111, 36, @on
exec sp_trace_setevent @TraceID, 111, 37, @on
exec sp_trace_setevent @TraceID, 111, 38, @on
exec sp_trace_setevent @TraceID, 111, 39, @on
exec sp_trace_setevent @TraceID, 111, 41, @on
exec sp_trace_setevent @TraceID, 111, 42, @on
exec sp_trace_setevent @TraceID, 111, 43, @on
exec sp_trace_setevent @TraceID, 111, 64, @on
exec sp_trace_setevent @TraceID, 212, 1, @on
exec sp_trace_setevent @TraceID, 212, 3, @on
exec sp_trace_setevent @TraceID, 212, 6, @on
exec sp_trace_setevent @TraceID, 212, 7, @on
```

```
exec sp_trace_setevent @TraceID, 212, 8, @on
exec sp_trace_setevent @TraceID, 212, 9, @on
exec sp_trace_setevent @TraceID, 212, 10, @on
exec sp_trace_setevent @TraceID, 212, 11, @on
exec sp_trace_setevent @TraceID, 212, 12, @on
exec sp_trace_setevent @TraceID, 212, 13, @on
exec sp_trace_setevent @TraceID, 212, 14, @on
exec sp_trace_setevent @TraceID, 212, 15, @on
exec sp_trace_setevent @TraceID, 212, 16, @on
exec sp_trace_setevent @TraceID, 212, 17, @on
exec sp_trace_setevent @TraceID, 212, 18, @on
exec sp_trace_setevent @TraceID, 212, 21, @on
exec sp_trace_setevent @TraceID, 212, 23, @on
exec sp_trace_setevent @TraceID, 212, 26, @on
exec sp_trace_setevent @TraceID, 212, 27, @on
exec sp_trace_setevent @TraceID, 212, 34, @on
exec sp_trace_setevent @TraceID, 212, 35, @on
exec sp_trace_setevent @TraceID, 212, 36, @on
exec sp_trace_setevent @TraceID, 212, 37, @on
exec sp_trace_setevent @TraceID, 212, 38, @on
exec sp_trace_setevent @TraceID, 212, 39, @on
exec sp_trace_setevent @TraceID, 212, 41, @on
exec sp_trace_setevent @TraceID, 212, 42, @on
exec sp_trace_setevent @TraceID, 212, 43, @on
exec sp_trace_setevent @TraceID, 212, 64, @on
exec sp_trace_setevent @TraceID, 213, 1, @on
exec sp_trace_setevent @TraceID, 213, 3, @on
```

```
exec sp_trace_setevent @TraceID, 213, 6, @on
exec sp_trace_setevent @TraceID, 213, 7, @on
exec sp_trace_setevent @TraceID, 213, 8, @on
exec sp_trace_setevent @TraceID, 213, 9, @on
exec sp_trace_setevent @TraceID, 213, 10, @on
exec sp_trace_setevent @TraceID, 213, 11, @on
exec sp_trace_setevent @TraceID, 213, 12, @on
exec sp_trace_setevent @TraceID, 213, 13, @on
exec sp_trace_setevent @TraceID, 213, 14, @on
exec sp_trace_setevent @TraceID, 213, 15, @on
exec sp_trace_setevent @TraceID, 213, 16, @on
exec sp_trace_setevent @TraceID, 213, 17, @on
exec sp_trace_setevent @TraceID, 213, 18, @on
exec sp_trace_setevent @TraceID, 213, 21, @on
exec sp_trace_setevent @TraceID, 213, 23, @on
exec sp_trace_setevent @TraceID, 213, 26, @on
exec sp_trace_setevent @TraceID, 213, 27, @on
exec sp_trace_setevent @TraceID, 213, 34, @on
exec sp_trace_setevent @TraceID, 213, 35, @on
exec sp_trace_setevent @TraceID, 213, 36, @on
exec sp_trace_setevent @TraceID, 213, 37, @on
exec sp_trace_setevent @TraceID, 213, 38, @on
exec sp_trace_setevent @TraceID, 213, 39, @on
exec sp_trace_setevent @TraceID, 213, 41, @on
exec sp_trace_setevent @TraceID, 213, 42, @on
exec sp_trace_setevent @TraceID, 213, 43, @on
exec sp_trace_setevent @TraceID, 213, 64, @on
```

```
exec sp_trace_setevent @TraceID, 214, 1, @on
exec sp_trace_setevent @TraceID, 214, 3, @on
exec sp_trace_setevent @TraceID, 214, 6, @on
exec sp_trace_setevent @TraceID, 214, 7, @on
exec sp_trace_setevent @TraceID, 214, 8, @on
exec sp_trace_setevent @TraceID, 214, 9, @on
exec sp_trace_setevent @TraceID, 214, 10, @on
exec sp_trace_setevent @TraceID, 214, 11, @on
exec sp_trace_setevent @TraceID, 214, 12, @on
exec sp_trace_setevent @TraceID, 214, 13, @on
exec sp_trace_setevent @TraceID, 214, 14, @on
exec sp_trace_setevent @TraceID, 214, 15, @on
exec sp_trace_setevent @TraceID, 214, 16, @on
exec sp_trace_setevent @TraceID, 214, 17, @on
exec sp_trace_setevent @TraceID, 214, 18, @on
exec sp_trace_setevent @TraceID, 214, 21, @on
exec sp_trace_setevent @TraceID, 214, 23, @on
exec sp_trace_setevent @TraceID, 214, 26, @on
exec sp_trace_setevent @TraceID, 214, 27, @on
exec sp_trace_setevent @TraceID, 214, 34, @on
exec sp_trace_setevent @TraceID, 214, 35, @on
exec sp_trace_setevent @TraceID, 214, 36, @on
exec sp_trace_setevent @TraceID, 214, 37, @on
exec sp_trace_setevent @TraceID, 214, 38, @on
exec sp_trace_setevent @TraceID, 214, 39, @on
exec sp_trace_setevent @TraceID, 214, 41, @on
exec sp_trace_setevent @TraceID, 214, 42, @on
exec sp_trace_setevent @TraceID, 214, 43, @on
```

```
exec sp_trace_setevent @TraceID, 214, 64, @on  
  
exec sp_trace_setevent @TraceID, 215, 1, @on  
exec sp_trace_setevent @TraceID, 215, 3, @on  
exec sp_trace_setevent @TraceID, 215, 6, @on  
exec sp_trace_setevent @TraceID, 215, 7, @on  
exec sp_trace_setevent @TraceID, 215, 8, @on  
exec sp_trace_setevent @TraceID, 215, 9, @on  
exec sp_trace_setevent @TraceID, 215, 10, @on  
exec sp_trace_setevent @TraceID, 215, 11, @on  
exec sp_trace_setevent @TraceID, 215, 12, @on  
exec sp_trace_setevent @TraceID, 215, 13, @on  
exec sp_trace_setevent @TraceID, 215, 14, @on  
exec sp_trace_setevent @TraceID, 215, 15, @on  
exec sp_trace_setevent @TraceID, 215, 16, @on  
exec sp_trace_setevent @TraceID, 215, 17, @on  
exec sp_trace_setevent @TraceID, 215, 18, @on  
exec sp_trace_setevent @TraceID, 215, 21, @on  
exec sp_trace_setevent @TraceID, 215, 23, @on  
exec sp_trace_setevent @TraceID, 215, 26, @on  
exec sp_trace_setevent @TraceID, 215, 27, @on  
exec sp_trace_setevent @TraceID, 215, 34, @on  
exec sp_trace_setevent @TraceID, 215, 35, @on  
exec sp_trace_setevent @TraceID, 215, 36, @on  
exec sp_trace_setevent @TraceID, 215, 37, @on  
exec sp_trace_setevent @TraceID, 215, 38, @on  
exec sp_trace_setevent @TraceID, 215, 39, @on  
exec sp_trace_setevent @TraceID, 215, 41, @on
```

```
exec sp_trace_setevent @TraceID, 215, 42, @on
exec sp_trace_setevent @TraceID, 215, 43, @on
exec sp_trace_setevent @TraceID, 215, 64, @on
exec sp_trace_setevent @TraceID, 216, 1, @on
exec sp_trace_setevent @TraceID, 216, 3, @on
exec sp_trace_setevent @TraceID, 216, 6, @on
exec sp_trace_setevent @TraceID, 216, 7, @on
exec sp_trace_setevent @TraceID, 216, 8, @on
exec sp_trace_setevent @TraceID, 216, 9, @on
exec sp_trace_setevent @TraceID, 216, 10, @on
exec sp_trace_setevent @TraceID, 216, 11, @on
exec sp_trace_setevent @TraceID, 216, 12, @on
exec sp_trace_setevent @TraceID, 216, 13, @on
exec sp_trace_setevent @TraceID, 216, 14, @on
exec sp_trace_setevent @TraceID, 216, 15, @on
exec sp_trace_setevent @TraceID, 216, 16, @on
exec sp_trace_setevent @TraceID, 216, 17, @on
exec sp_trace_setevent @TraceID, 216, 18, @on
exec sp_trace_setevent @TraceID, 216, 21, @on
exec sp_trace_setevent @TraceID, 216, 23, @on
exec sp_trace_setevent @TraceID, 216, 26, @on
exec sp_trace_setevent @TraceID, 216, 27, @on
exec sp_trace_setevent @TraceID, 216, 34, @on
exec sp_trace_setevent @TraceID, 216, 35, @on
exec sp_trace_setevent @TraceID, 216, 36, @on
exec sp_trace_setevent @TraceID, 216, 37, @on
exec sp_trace_setevent @TraceID, 216, 38, @on
```

```
exec sp_trace_setevent @TraceID, 216, 39, @on
exec sp_trace_setevent @TraceID, 216, 41, @on
exec sp_trace_setevent @TraceID, 216, 42, @on
exec sp_trace_setevent @TraceID, 216, 43, @on
exec sp_trace_setevent @TraceID, 216, 64, @on
exec sp_trace_setevent @TraceID, 217, 1, @on
exec sp_trace_setevent @TraceID, 217, 3, @on
exec sp_trace_setevent @TraceID, 217, 6, @on
exec sp_trace_setevent @TraceID, 217, 7, @on
exec sp_trace_setevent @TraceID, 217, 8, @on
exec sp_trace_setevent @TraceID, 217, 9, @on
exec sp_trace_setevent @TraceID, 217, 10, @on
exec sp_trace_setevent @TraceID, 217, 11, @on
exec sp_trace_setevent @TraceID, 217, 12, @on
exec sp_trace_setevent @TraceID, 217, 13, @on
exec sp_trace_setevent @TraceID, 217, 14, @on
exec sp_trace_setevent @TraceID, 217, 15, @on
exec sp_trace_setevent @TraceID, 217, 16, @on
exec sp_trace_setevent @TraceID, 217, 17, @on
exec sp_trace_setevent @TraceID, 217, 18, @on
exec sp_trace_setevent @TraceID, 217, 21, @on
exec sp_trace_setevent @TraceID, 217, 23, @on
exec sp_trace_setevent @TraceID, 217, 26, @on
exec sp_trace_setevent @TraceID, 217, 27, @on
exec sp_trace_setevent @TraceID, 217, 34, @on
exec sp_trace_setevent @TraceID, 217, 35, @on
exec sp_trace_setevent @TraceID, 217, 36, @on
```

```
exec sp_trace_setevent @TraceID, 217, 37, @on
exec sp_trace_setevent @TraceID, 217, 38, @on
exec sp_trace_setevent @TraceID, 217, 39, @on
exec sp_trace_setevent @TraceID, 217, 41, @on
exec sp_trace_setevent @TraceID, 217, 42, @on
exec sp_trace_setevent @TraceID, 217, 43, @on
exec sp_trace_setevent @TraceID, 217, 64, @on

exec sp_trace_setevent @TraceID, 218, 1, @on
exec sp_trace_setevent @TraceID, 218, 3, @on
exec sp_trace_setevent @TraceID, 218, 6, @on
exec sp_trace_setevent @TraceID, 218, 7, @on
exec sp_trace_setevent @TraceID, 218, 8, @on
exec sp_trace_setevent @TraceID, 218, 9, @on
exec sp_trace_setevent @TraceID, 218, 10, @on
exec sp_trace_setevent @TraceID, 218, 11, @on
exec sp_trace_setevent @TraceID, 218, 12, @on
exec sp_trace_setevent @TraceID, 218, 13, @on
exec sp_trace_setevent @TraceID, 218, 14, @on
exec sp_trace_setevent @TraceID, 218, 15, @on
exec sp_trace_setevent @TraceID, 218, 16, @on
exec sp_trace_setevent @TraceID, 218, 17, @on
exec sp_trace_setevent @TraceID, 218, 18, @on
exec sp_trace_setevent @TraceID, 218, 21, @on
exec sp_trace_setevent @TraceID, 218, 23, @on
exec sp_trace_setevent @TraceID, 218, 26, @on
exec sp_trace_setevent @TraceID, 218, 27, @on
exec sp_trace_setevent @TraceID, 218, 34, @on
```

```
exec sp_trace_setevent @TraceID, 218, 35, @on
exec sp_trace_setevent @TraceID, 218, 36, @on
exec sp_trace_setevent @TraceID, 218, 37, @on
exec sp_trace_setevent @TraceID, 218, 38, @on
exec sp_trace_setevent @TraceID, 218, 39, @on
exec sp_trace_setevent @TraceID, 218, 41, @on
exec sp_trace_setevent @TraceID, 218, 42, @on
exec sp_trace_setevent @TraceID, 218, 43, @on
exec sp_trace_setevent @TraceID, 218, 64, @on

exec sp_trace_setevent @TraceID, 235, 1, @on
exec sp_trace_setevent @TraceID, 235, 3, @on
exec sp_trace_setevent @TraceID, 235, 6, @on
exec sp_trace_setevent @TraceID, 235, 7, @on
exec sp_trace_setevent @TraceID, 235, 8, @on
exec sp_trace_setevent @TraceID, 235, 9, @on
exec sp_trace_setevent @TraceID, 235, 10, @on
exec sp_trace_setevent @TraceID, 235, 11, @on
exec sp_trace_setevent @TraceID, 235, 12, @on
exec sp_trace_setevent @TraceID, 235, 13, @on
exec sp_trace_setevent @TraceID, 235, 14, @on
exec sp_trace_setevent @TraceID, 235, 15, @on
exec sp_trace_setevent @TraceID, 235, 16, @on
exec sp_trace_setevent @TraceID, 235, 17, @on
exec sp_trace_setevent @TraceID, 235, 18, @on
exec sp_trace_setevent @TraceID, 235, 21, @on
exec sp_trace_setevent @TraceID, 235, 23, @on
exec sp_trace_setevent @TraceID, 235, 26, @on
```

```
exec sp_trace_setevent @TraceID, 235, 27, @on
exec sp_trace_setevent @TraceID, 235, 34, @on
exec sp_trace_setevent @TraceID, 235, 35, @on
exec sp_trace_setevent @TraceID, 235, 36, @on
exec sp_trace_setevent @TraceID, 235, 37, @on
exec sp_trace_setevent @TraceID, 235, 38, @on
exec sp_trace_setevent @TraceID, 235, 39, @on
exec sp_trace_setevent @TraceID, 235, 41, @on
exec sp_trace_setevent @TraceID, 235, 42, @on
exec sp_trace_setevent @TraceID, 235, 43, @on
exec sp_trace_setevent @TraceID, 235, 64, @on

-- Set the Filters
declare @intfilter int
declare @bigintfilter bigint

exec sp_trace_setfilter @TraceID, 10, 0, 7, N'SQL Profiler'

-- Set the trace status to start
exec sp_trace_setstatus @TraceID, 1

-- display trace id for future references
select TraceID=@TraceID
goto finish

error:
select ErrorCode=@rc return @rc
finish: return @TraceID
```

SQL Server 2005

```
CREATE PROC AuditTrcProc AS
-- Create a Queue declare @rc int declare @TraceID int declare @maxfilesize
bigint set @maxfilesize = 1
-- Please replace the file name with an appropriate file name prefixed by a
path,
e.g., C:\sqltrace\sessionTrace.
-- The .trc extension will be appended to the filename automatically.
-- If you are writing from remote server to local drive, use UNC path and make
sure server has write access to your network share
```

```
declare @cmd sysname
set @cmd = 'copy c:\sqltrace\sessiontrace.trc c:\sqltrace\sessiontrace' + cast
(cast(rand() * 1000000 as int) as varchar) print @cmd
exec master..xp_cmdshell @cmd
set @cmd= 'del c:\sqltrace\sessiontrace.trc' print @cmd
exec master..xp_cmdshell @cmd
exec @rc = sp_trace_create @TraceID output, 2, N'c:\sqltrace\sessiontrace',
@maxfilesize, null if (@rc != 0) goto error
-- Client side File and Table cannot be scripted
-- Set the events and columns declare @on bit set @on = 1
exec sp_trace_setevent @TraceID, 10, 1, @on
exec sp_trace_setevent @TraceID, 10, 3, @on
exec sp_trace_setevent @TraceID, 10, 6, @on
exec sp_trace_setevent @TraceID, 10, 7, @on
exec sp_trace_setevent @TraceID, 10, 8, @on
exec sp_trace_setevent @TraceID, 10, 9, @on
exec sp_trace_setevent @TraceID, 10, 10, @on
```

```
exec sp_trace_setevent @TraceID, 10, 11, @on
exec sp_trace_setevent @TraceID, 10, 12, @on
exec sp_trace_setevent @TraceID, 10, 13, @on
exec sp_trace_setevent @TraceID, 10, 14, @on
exec sp_trace_setevent @TraceID, 10, 15, @on
exec sp_trace_setevent @TraceID, 10, 16, @on
exec sp_trace_setevent @TraceID, 10, 17, @on
exec sp_trace_setevent @TraceID, 10, 18, @on
exec sp_trace_setevent @TraceID, 10, 21, @on
exec sp_trace_setevent @TraceID, 10, 23, @on
exec sp_trace_setevent @TraceID, 10, 26, @on
exec sp_trace_setevent @TraceID, 10, 27, @on
exec sp_trace_setevent @TraceID, 10, 34, @on
exec sp_trace_setevent @TraceID, 10, 35, @on
exec sp_trace_setevent @TraceID, 10, 36, @on
exec sp_trace_setevent @TraceID, 10, 37, @on
exec sp_trace_setevent @TraceID, 10, 38, @on
exec sp_trace_setevent @TraceID, 10, 39, @on
exec sp_trace_setevent @TraceID, 10, 41, @on
exec sp_trace_setevent @TraceID, 10, 42, @on
exec sp_trace_setevent @TraceID, 10, 43, @on
exec sp_trace_setevent @TraceID, 10, 64, @on
```

```
exec sp_trace_setevent @TraceID, 12, 1, @on
exec sp_trace_setevent @TraceID, 12, 3, @on
exec sp_trace_setevent @TraceID, 12, 6, @on
exec sp_trace_setevent @TraceID, 12, 7, @on
exec sp_trace_setevent @TraceID, 12, 8, @on
```

```
exec sp_trace_setevent @TraceID, 12, 9, @on
exec sp_trace_setevent @TraceID, 12, 10, @on
exec sp_trace_setevent @TraceID, 12, 11, @on
exec sp_trace_setevent @TraceID, 12, 12, @on
exec sp_trace_setevent @TraceID, 12, 13, @on
exec sp_trace_setevent @TraceID, 12, 14, @on
exec sp_trace_setevent @TraceID, 12, 15, @on
exec sp_trace_setevent @TraceID, 12, 16, @on
exec sp_trace_setevent @TraceID, 12, 17, @on
exec sp_trace_setevent @TraceID, 12, 18, @on
exec sp_trace_setevent @TraceID, 12, 21, @on
exec sp_trace_setevent @TraceID, 12, 23, @on
exec sp_trace_setevent @TraceID, 12, 26, @on
exec sp_trace_setevent @TraceID, 12, 27, @on
exec sp_trace_setevent @TraceID, 12, 34, @on
exec sp_trace_setevent @TraceID, 12, 35, @on
exec sp_trace_setevent @TraceID, 12, 36, @on
exec sp_trace_setevent @TraceID, 12, 37, @on
exec sp_trace_setevent @TraceID, 12, 38, @on
exec sp_trace_setevent @TraceID, 12, 39, @on
exec sp_trace_setevent @TraceID, 12, 41, @on
exec sp_trace_setevent @TraceID, 12, 42, @on
exec sp_trace_setevent @TraceID, 12, 43, @on
exec sp_trace_setevent @TraceID, 12, 64, @on
```

```
exec sp_trace_setevent @TraceID, 14, 1, @on
exec sp_trace_setevent @TraceID, 14, 3, @on
exec sp_trace_setevent @TraceID, 14, 6, @on
```

```
exec sp_trace_setevent @TraceID, 14, 7, @on
exec sp_trace_setevent @TraceID, 14, 8, @on
exec sp_trace_setevent @TraceID, 14, 9, @on
exec sp_trace_setevent @TraceID, 14, 10, @on
exec sp_trace_setevent @TraceID, 14, 11, @on
exec sp_trace_setevent @TraceID, 14, 12, @on
exec sp_trace_setevent @TraceID, 14, 13, @on
exec sp_trace_setevent @TraceID, 14, 14, @on
exec sp_trace_setevent @TraceID, 14, 15, @on
exec sp_trace_setevent @TraceID, 14, 16, @on
exec sp_trace_setevent @TraceID, 14, 17, @on
exec sp_trace_setevent @TraceID, 14, 18, @on
exec sp_trace_setevent @TraceID, 14, 21, @on
exec sp_trace_setevent @TraceID, 14, 23, @on
exec sp_trace_setevent @TraceID, 14, 26, @on
exec sp_trace_setevent @TraceID, 14, 27, @on
exec sp_trace_setevent @TraceID, 14, 34, @on
exec sp_trace_setevent @TraceID, 14, 35, @on
exec sp_trace_setevent @TraceID, 14, 36, @on
exec sp_trace_setevent @TraceID, 14, 37, @on
exec sp_trace_setevent @TraceID, 14, 38, @on
exec sp_trace_setevent @TraceID, 14, 39, @on
exec sp_trace_setevent @TraceID, 14, 41, @on
exec sp_trace_setevent @TraceID, 14, 42, @on
exec sp_trace_setevent @TraceID, 14, 43, @on
exec sp_trace_setevent @TraceID, 14, 64, @on
exec sp_trace_setevent @TraceID, 15, 1, @on
exec sp_trace_setevent @TraceID, 15, 3, @on
```

```
exec sp_trace_setevent @TraceID, 15, 6, @on
exec sp_trace_setevent @TraceID, 15, 7, @on
exec sp_trace_setevent @TraceID, 15, 8, @on
exec sp_trace_setevent @TraceID, 15, 9, @on
exec sp_trace_setevent @TraceID, 15, 10, @on
exec sp_trace_setevent @TraceID, 15, 11, @on
exec sp_trace_setevent @TraceID, 15, 12, @on
exec sp_trace_setevent @TraceID, 15, 13, @on
exec sp_trace_setevent @TraceID, 15, 14, @on
exec sp_trace_setevent @TraceID, 15, 15, @on
exec sp_trace_setevent @TraceID, 15, 16, @on
exec sp_trace_setevent @TraceID, 15, 17, @on
exec sp_trace_setevent @TraceID, 15, 18, @on
exec sp_trace_setevent @TraceID, 15, 21, @on
exec sp_trace_setevent @TraceID, 15, 23, @on
exec sp_trace_setevent @TraceID, 15, 26, @on
exec sp_trace_setevent @TraceID, 15, 27, @on
exec sp_trace_setevent @TraceID, 15, 34, @on
exec sp_trace_setevent @TraceID, 15, 35, @on
exec sp_trace_setevent @TraceID, 15, 36, @on
exec sp_trace_setevent @TraceID, 15, 37, @on
exec sp_trace_setevent @TraceID, 15, 38, @on
exec sp_trace_setevent @TraceID, 15, 39, @on
exec sp_trace_setevent @TraceID, 15, 41, @on
exec sp_trace_setevent @TraceID, 15, 42, @on
exec sp_trace_setevent @TraceID, 15, 43, @on
exec sp_trace_setevent @TraceID, 15, 64, @on
```

```
exec sp_trace_setevent @TraceID, 17, 1, @on
exec sp_trace_setevent @TraceID, 17, 3, @on
exec sp_trace_setevent @TraceID, 17, 6, @on
exec sp_trace_setevent @TraceID, 17, 7, @on
exec sp_trace_setevent @TraceID, 17, 8, @on
exec sp_trace_setevent @TraceID, 17, 9, @on
exec sp_trace_setevent @TraceID, 17, 10, @on
exec sp_trace_setevent @TraceID, 17, 11, @on
exec sp_trace_setevent @TraceID, 17, 12, @on
exec sp_trace_setevent @TraceID, 17, 13, @on
exec sp_trace_setevent @TraceID, 17, 14, @on
exec sp_trace_setevent @TraceID, 17, 15, @on
exec sp_trace_setevent @TraceID, 17, 16, @on
exec sp_trace_setevent @TraceID, 17, 17, @on
exec sp_trace_setevent @TraceID, 17, 18, @on
exec sp_trace_setevent @TraceID, 17, 21, @on
exec sp_trace_setevent @TraceID, 17, 23, @on
exec sp_trace_setevent @TraceID, 17, 26, @on
exec sp_trace_setevent @TraceID, 17, 27, @on
exec sp_trace_setevent @TraceID, 17, 34, @on
exec sp_trace_setevent @TraceID, 17, 35, @on
exec sp_trace_setevent @TraceID, 17, 36, @on
exec sp_trace_setevent @TraceID, 17, 37, @on
exec sp_trace_setevent @TraceID, 17, 38, @on
exec sp_trace_setevent @TraceID, 17, 39, @on
exec sp_trace_setevent @TraceID, 17, 41, @on
exec sp_trace_setevent @TraceID, 17, 42, @on
exec sp_trace_setevent @TraceID, 17, 43, @on
```

```
exec sp_trace_setevent @TraceID, 17, 64, @on
```

```
exec sp_trace_setevent @TraceID, 104, 1, @on
```

```
exec sp_trace_setevent @TraceID, 104, 3, @on
```

```
exec sp_trace_setevent @TraceID, 104, 6, @on
```

```
exec sp_trace_setevent @TraceID, 104, 7, @on
```

```
exec sp_trace_setevent @TraceID, 104, 8, @on
```

```
exec sp_trace_setevent @TraceID, 104, 9, @on
```

```
exec sp_trace_setevent @TraceID, 104, 10, @on
```

```
exec sp_trace_setevent @TraceID, 104, 11, @on
```

```
exec sp_trace_setevent @TraceID, 104, 12, @on
```

```
exec sp_trace_setevent @TraceID, 104, 13, @on
```

```
exec sp_trace_setevent @TraceID, 104, 14, @on
```

```
exec sp_trace_setevent @TraceID, 104, 15, @on
```

```
exec sp_trace_setevent @TraceID, 104, 16, @on
```

```
exec sp_trace_setevent @TraceID, 104, 17, @on
```

```
exec sp_trace_setevent @TraceID, 104, 18, @on
```

```
exec sp_trace_setevent @TraceID, 104, 21, @on
```

```
exec sp_trace_setevent @TraceID, 104, 23, @on
```

```
exec sp_trace_setevent @TraceID, 104, 26, @on
```

```
exec sp_trace_setevent @TraceID, 104, 27, @on
```

```
exec sp_trace_setevent @TraceID, 104, 34, @on
```

```
exec sp_trace_setevent @TraceID, 104, 35, @on
```

```
exec sp_trace_setevent @TraceID, 104, 36, @on
```

```
exec sp_trace_setevent @TraceID, 104, 37, @on
```

```
exec sp_trace_setevent @TraceID, 104, 38, @on
```

```
exec sp_trace_setevent @TraceID, 104, 39, @on
```

```
exec sp_trace_setevent @TraceID, 104, 41, @on
```

```
exec sp_trace_setevent @TraceID, 104, 42, @on
exec sp_trace_setevent @TraceID, 104, 43, @on
exec sp_trace_setevent @TraceID, 104, 64, @on
exec sp_trace_setevent @TraceID, 105, 1, @on
exec sp_trace_setevent @TraceID, 105, 3, @on
exec sp_trace_setevent @TraceID, 105, 6, @on
exec sp_trace_setevent @TraceID, 105, 7, @on
exec sp_trace_setevent @TraceID, 105, 8, @on
exec sp_trace_setevent @TraceID, 105, 9, @on
exec sp_trace_setevent @TraceID, 105, 10, @on
exec sp_trace_setevent @TraceID, 105, 11, @on
exec sp_trace_setevent @TraceID, 105, 12, @on
exec sp_trace_setevent @TraceID, 105, 13, @on
exec sp_trace_setevent @TraceID, 105, 14, @on
exec sp_trace_setevent @TraceID, 105, 15, @on
exec sp_trace_setevent @TraceID, 105, 16, @on
exec sp_trace_setevent @TraceID, 105, 17, @on
exec sp_trace_setevent @TraceID, 105, 18, @on
exec sp_trace_setevent @TraceID, 105, 21, @on
exec sp_trace_setevent @TraceID, 105, 23, @on
exec sp_trace_setevent @TraceID, 105, 26, @on
exec sp_trace_setevent @TraceID, 105, 27, @on
exec sp_trace_setevent @TraceID, 105, 34, @on
exec sp_trace_setevent @TraceID, 105, 35, @on
exec sp_trace_setevent @TraceID, 105, 36, @on
exec sp_trace_setevent @TraceID, 105, 37, @on
exec sp_trace_setevent @TraceID, 105, 38, @on
```

Configuration Guide for Microsoft SQL Server Multiple Instance Audit DB SmartConnector
SQL Server Sample Audit Procedures

```
exec sp_trace_setevent @TraceID, 105, 39, @on
exec sp_trace_setevent @TraceID, 105, 41, @on
exec sp_trace_setevent @TraceID, 105, 42, @on
exec sp_trace_setevent @TraceID, 105, 43, @on
exec sp_trace_setevent @TraceID, 105, 64, @on
exec sp_trace_setevent @TraceID, 106, 1, @on
exec sp_trace_setevent @TraceID, 106, 3, @on
exec sp_trace_setevent @TraceID, 106, 6, @on
exec sp_trace_setevent @TraceID, 106, 7, @on
exec sp_trace_setevent @TraceID, 106, 8, @on
exec sp_trace_setevent @TraceID, 106, 9, @on
exec sp_trace_setevent @TraceID, 106, 10, @on
exec sp_trace_setevent @TraceID, 106, 11, @on
exec sp_trace_setevent @TraceID, 106, 12, @on
exec sp_trace_setevent @TraceID, 106, 13, @on
exec sp_trace_setevent @TraceID, 106, 14, @on
exec sp_trace_setevent @TraceID, 106, 15, @on
exec sp_trace_setevent @TraceID, 106, 16, @on
exec sp_trace_setevent @TraceID, 106, 17, @on
exec sp_trace_setevent @TraceID, 106, 18, @on
exec sp_trace_setevent @TraceID, 106, 21, @on
exec sp_trace_setevent @TraceID, 106, 23, @on
exec sp_trace_setevent @TraceID, 106, 26, @on
exec sp_trace_setevent @TraceID, 106, 27, @on
exec sp_trace_setevent @TraceID, 106, 34, @on
exec sp_trace_setevent @TraceID, 106, 35, @on
exec sp_trace_setevent @TraceID, 106, 36, @on
```

```
exec sp_trace_setevent @TraceID, 106, 37, @on
exec sp_trace_setevent @TraceID, 106, 38, @on
exec sp_trace_setevent @TraceID, 106, 39, @on
exec sp_trace_setevent @TraceID, 106, 41, @on
exec sp_trace_setevent @TraceID, 106, 42, @on
exec sp_trace_setevent @TraceID, 106, 43, @on
exec sp_trace_setevent @TraceID, 106, 64, @on

exec sp_trace_setevent @TraceID, 107, 1, @on
exec sp_trace_setevent @TraceID, 107, 3, @on
exec sp_trace_setevent @TraceID, 107, 6, @on
exec sp_trace_setevent @TraceID, 107, 7, @on
exec sp_trace_setevent @TraceID, 107, 8, @on
exec sp_trace_setevent @TraceID, 107, 9, @on
exec sp_trace_setevent @TraceID, 107, 10, @on
exec sp_trace_setevent @TraceID, 107, 11, @on
exec sp_trace_setevent @TraceID, 107, 12, @on
exec sp_trace_setevent @TraceID, 107, 13, @on
exec sp_trace_setevent @TraceID, 107, 14, @on
exec sp_trace_setevent @TraceID, 107, 15, @on
exec sp_trace_setevent @TraceID, 107, 16, @on
exec sp_trace_setevent @TraceID, 107, 17, @on
exec sp_trace_setevent @TraceID, 107, 18, @on
exec sp_trace_setevent @TraceID, 107, 21, @on
exec sp_trace_setevent @TraceID, 107, 23, @on
exec sp_trace_setevent @TraceID, 107, 26, @on
exec sp_trace_setevent @TraceID, 107, 27, @on
exec sp_trace_setevent @TraceID, 107, 34, @on
```

```
exec sp_trace_setevent @TraceID, 107, 35, @on
exec sp_trace_setevent @TraceID, 107, 36, @on
exec sp_trace_setevent @TraceID, 107, 37, @on
exec sp_trace_setevent @TraceID, 107, 38, @on
exec sp_trace_setevent @TraceID, 107, 39, @on
exec sp_trace_setevent @TraceID, 107, 41, @on
exec sp_trace_setevent @TraceID, 107, 42, @on
exec sp_trace_setevent @TraceID, 107, 43, @on
exec sp_trace_setevent @TraceID, 107, 64, @on

exec sp_trace_setevent @TraceID, 108, 1, @on
exec sp_trace_setevent @TraceID, 108, 3, @on
exec sp_trace_setevent @TraceID, 108, 6, @on
exec sp_trace_setevent @TraceID, 108, 7, @on
exec sp_trace_setevent @TraceID, 108, 8, @on
exec sp_trace_setevent @TraceID, 108, 9, @on
exec sp_trace_setevent @TraceID, 108, 10, @on
exec sp_trace_setevent @TraceID, 108, 11, @on
exec sp_trace_setevent @TraceID, 108, 12, @on
exec sp_trace_setevent @TraceID, 108, 13, @on
exec sp_trace_setevent @TraceID, 108, 14, @on
exec sp_trace_setevent @TraceID, 108, 15, @on
exec sp_trace_setevent @TraceID, 108, 16, @on
exec sp_trace_setevent @TraceID, 108, 17, @on
exec sp_trace_setevent @TraceID, 108, 18, @on
exec sp_trace_setevent @TraceID, 108, 21, @on
exec sp_trace_setevent @TraceID, 108, 23, @on
exec sp_trace_setevent @TraceID, 108, 26, @on
```

```
exec sp_trace_setevent @TraceID, 108, 27, @on
exec sp_trace_setevent @TraceID, 108, 34, @on
exec sp_trace_setevent @TraceID, 108, 35, @on
exec sp_trace_setevent @TraceID, 108, 36, @on
exec sp_trace_setevent @TraceID, 108, 37, @on
exec sp_trace_setevent @TraceID, 108, 38, @on
exec sp_trace_setevent @TraceID, 108, 39, @on
exec sp_trace_setevent @TraceID, 108, 41, @on
exec sp_trace_setevent @TraceID, 108, 42, @on
exec sp_trace_setevent @TraceID, 108, 43, @on
exec sp_trace_setevent @TraceID, 108, 64, @on
```

```
exec sp_trace_setevent @TraceID, 109, 1, @on
exec sp_trace_setevent @TraceID, 109, 3, @on
exec sp_trace_setevent @TraceID, 109, 6, @on
exec sp_trace_setevent @TraceID, 109, 7, @on
exec sp_trace_setevent @TraceID, 109, 8, @on
exec sp_trace_setevent @TraceID, 109, 9, @on
exec sp_trace_setevent @TraceID, 109, 10, @on
exec sp_trace_setevent @TraceID, 109, 11, @on
exec sp_trace_setevent @TraceID, 109, 12, @on
exec sp_trace_setevent @TraceID, 109, 13, @on
exec sp_trace_setevent @TraceID, 109, 14, @on
exec sp_trace_setevent @TraceID, 109, 15, @on
exec sp_trace_setevent @TraceID, 109, 16, @on
exec sp_trace_setevent @TraceID, 109, 17, @on
exec sp_trace_setevent @TraceID, 109, 18, @on
exec sp_trace_setevent @TraceID, 109, 21, @on
```

```
exec sp_trace_setevent @TraceID, 109, 23, @on
exec sp_trace_setevent @TraceID, 109, 26, @on
exec sp_trace_setevent @TraceID, 109, 27, @on
exec sp_trace_setevent @TraceID, 109, 34, @on
exec sp_trace_setevent @TraceID, 109, 35, @on
exec sp_trace_setevent @TraceID, 109, 36, @on
exec sp_trace_setevent @TraceID, 109, 37, @on
exec sp_trace_setevent @TraceID, 109, 38, @on
exec sp_trace_setevent @TraceID, 109, 39, @on
exec sp_trace_setevent @TraceID, 109, 41, @on
exec sp_trace_setevent @TraceID, 109, 42, @on
exec sp_trace_setevent @TraceID, 109, 43, @on
exec sp_trace_setevent @TraceID, 109, 64, @on
```

```
exec sp_trace_setevent @TraceID, 110, 1, @on
exec sp_trace_setevent @TraceID, 110, 3, @on
exec sp_trace_setevent @TraceID, 110, 6, @on
exec sp_trace_setevent @TraceID, 110, 7, @on
exec sp_trace_setevent @TraceID, 110, 8, @on
exec sp_trace_setevent @TraceID, 110, 9, @on
exec sp_trace_setevent @TraceID, 110, 10, @on
exec sp_trace_setevent @TraceID, 110, 11, @on
exec sp_trace_setevent @TraceID, 110, 12, @on
exec sp_trace_setevent @TraceID, 110, 13, @on
exec sp_trace_setevent @TraceID, 110, 14, @on
exec sp_trace_setevent @TraceID, 110, 15, @on
exec sp_trace_setevent @TraceID, 110, 16, @on
exec sp_trace_setevent @TraceID, 110, 17, @on
```

```
exec sp_trace_setevent @TraceID, 110, 18, @on
exec sp_trace_setevent @TraceID, 110, 21, @on
exec sp_trace_setevent @TraceID, 110, 23, @on
exec sp_trace_setevent @TraceID, 110, 26, @on
exec sp_trace_setevent @TraceID, 110, 27, @on
exec sp_trace_setevent @TraceID, 110, 34, @on
exec sp_trace_setevent @TraceID, 110, 35, @on
exec sp_trace_setevent @TraceID, 110, 36, @on
exec sp_trace_setevent @TraceID, 110, 37, @on
exec sp_trace_setevent @TraceID, 110, 38, @on
exec sp_trace_setevent @TraceID, 110, 39, @on
exec sp_trace_setevent @TraceID, 110, 41, @on
exec sp_trace_setevent @TraceID, 110, 42, @on
exec sp_trace_setevent @TraceID, 110, 43, @on
exec sp_trace_setevent @TraceID, 110, 64, @on
```

```
exec sp_trace_setevent @TraceID, 111, 1, @on
exec sp_trace_setevent @TraceID, 111, 3, @on
exec sp_trace_setevent @TraceID, 111, 6, @on
exec sp_trace_setevent @TraceID, 111, 7, @on
exec sp_trace_setevent @TraceID, 111, 8, @on
exec sp_trace_setevent @TraceID, 111, 9, @on
exec sp_trace_setevent @TraceID, 111, 10, @on
exec sp_trace_setevent @TraceID, 111, 11, @on
exec sp_trace_setevent @TraceID, 111, 12, @on
exec sp_trace_setevent @TraceID, 111, 13, @on
exec sp_trace_setevent @TraceID, 111, 14, @on
exec sp_trace_setevent @TraceID, 111, 15, @on
```

```
exec sp_trace_setevent @TraceID, 111, 16, @on
exec sp_trace_setevent @TraceID, 111, 17, @on
exec sp_trace_setevent @TraceID, 111, 18, @on
exec sp_trace_setevent @TraceID, 111, 21, @on
exec sp_trace_setevent @TraceID, 111, 23, @on
exec sp_trace_setevent @TraceID, 111, 26, @on
exec sp_trace_setevent @TraceID, 111, 27, @on
exec sp_trace_setevent @TraceID, 111, 34, @on
exec sp_trace_setevent @TraceID, 111, 35, @on
exec sp_trace_setevent @TraceID, 111, 36, @on
exec sp_trace_setevent @TraceID, 111, 37, @on
exec sp_trace_setevent @TraceID, 111, 38, @on
exec sp_trace_setevent @TraceID, 111, 39, @on
exec sp_trace_setevent @TraceID, 111, 41, @on
exec sp_trace_setevent @TraceID, 111, 42, @on
exec sp_trace_setevent @TraceID, 111, 43, @on
exec sp_trace_setevent @TraceID, 111, 64, @on

-- Set the Filters declare @intfilter int declare @bigintfilter bigint
exec sp_trace_setfilter @TraceID, 10, 0, 7, N'SQL Profiler'
-- Set the trace status to start exec sp_trace_setstatus @TraceID, 1
-- display trace id for future references select TraceID=@TraceID goto finish
error:
select ErrorCode=@rc return @rc  finish:
return @TraceID
```

SQL Server 2000

```
CREATE PROC AuditTrcProc AS
```

```
-- Create a Queue declare @rc int declare @TraceID int declare @maxfilesize
bigint set @maxfilesize = 1

-- Please replace the text InsertFileNameHere, with an appropriate
-- filename prefixed by a path, e.g., c:\MyFolder\MyTrace. The .trc extension
-- will be appended to the filename automatically. If you are writing from
-- remote server to local drive, please use UNC path and make sure server has
-- write access to your network share

declare @cmd sysname

set @cmd = 'copy c:\temp\sessiontrace.trc c:\temp\session' + cast(cast(rand()
*
1000000 as int) as varchar) print @cmd

exec master..xp_cmdshell @cmd

set @cmd= 'del c:\temp\sessiontrace.trc' print @cmd

exec master..xp_cmdshell @cmd

exec @rc = sp_trace_create @TraceID output, 2, N'c:\temp\sessiontrace',
@maxfilesize, null if (@rc != 0) goto error
-- Client side File and Table cannot be scripted
-- Set the events declare @on bit set @on = 1

exec sp_trace_setevent @TraceID, 10, 1, @on
exec sp_trace_setevent @TraceID, 10, 6, @on
exec sp_trace_setevent @TraceID, 10, 9, @on
exec sp_trace_setevent @TraceID, 10, 10, @on
exec sp_trace_setevent @TraceID, 10, 11, @on
exec sp_trace_setevent @TraceID, 10, 12, @on
exec sp_trace_setevent @TraceID, 10, 13, @on
exec sp_trace_setevent @TraceID, 10, 14, @on
exec sp_trace_setevent @TraceID, 10, 16, @on
```

```
exec sp_trace_setevent @TraceID, 10, 17, @on
exec sp_trace_setevent @TraceID, 10, 18, @on
exec sp_trace_setevent @TraceID, 12, 1, @on
exec sp_trace_setevent @TraceID, 12, 6, @on
exec sp_trace_setevent @TraceID, 12, 9, @on
exec sp_trace_setevent @TraceID, 12, 10, @on
exec sp_trace_setevent @TraceID, 12, 11, @on
exec sp_trace_setevent @TraceID, 12, 12, @on
exec sp_trace_setevent @TraceID, 12, 13, @on
exec sp_trace_setevent @TraceID, 12, 14, @on
exec sp_trace_setevent @TraceID, 12, 16, @on
exec sp_trace_setevent @TraceID, 12, 17, @on
exec sp_trace_setevent @TraceID, 12, 18, @on
exec sp_trace_setevent @TraceID, 14, 1, @on
exec sp_trace_setevent @TraceID, 14, 6, @on
exec sp_trace_setevent @TraceID, 14, 9, @on
exec sp_trace_setevent @TraceID, 14, 10, @on
exec sp_trace_setevent @TraceID, 14, 11, @on
exec sp_trace_setevent @TraceID, 14, 12, @on
exec sp_trace_setevent @TraceID, 14, 13, @on
exec sp_trace_setevent @TraceID, 14, 14, @on
exec sp_trace_setevent @TraceID, 14, 16, @on
exec sp_trace_setevent @TraceID, 14, 17, @on
exec sp_trace_setevent @TraceID, 14, 18, @on
exec sp_trace_setevent @TraceID, 15, 1, @on
exec sp_trace_setevent @TraceID, 15, 6, @on
exec sp_trace_setevent @TraceID, 15, 9, @on
exec sp_trace_setevent @TraceID, 15, 10, @on
```

```
exec sp_trace_setevent @TraceID, 15, 11, @on
exec sp_trace_setevent @TraceID, 15, 12, @on
exec sp_trace_setevent @TraceID, 15, 13, @on
exec sp_trace_setevent @TraceID, 15, 14, @on
exec sp_trace_setevent @TraceID, 15, 16, @on
exec sp_trace_setevent @TraceID, 15, 17, @on
exec sp_trace_setevent @TraceID, 15, 18, @on
exec sp_trace_setevent @TraceID, 17, 1, @on
exec sp_trace_setevent @TraceID, 17, 6, @on
exec sp_trace_setevent @TraceID, 17, 9, @on
exec sp_trace_setevent @TraceID, 17, 10, @on
exec sp_trace_setevent @TraceID, 17, 11, @on
exec sp_trace_setevent @TraceID, 17, 12, @on
exec sp_trace_setevent @TraceID, 17, 13, @on
exec sp_trace_setevent @TraceID, 17, 14, @on
exec sp_trace_setevent @TraceID, 17, 16, @on
exec sp_trace_setevent @TraceID, 17, 17, @on
exec sp_trace_setevent @TraceID, 17, 18, @on

-- Set the Filters declare @intfilter int declare @bigintfilter bigint
exec sp_trace_setfilter @TraceID, 10, 0, 7, N'SQL Profiler'
-- Set the trace status to start exec sp_trace_setstatus @TraceID, 1
-- display trace id for future references select TraceID=@TraceID goto finish
error:  select ErrorCode=@rc return @rc  finish:
return @TraceID
```

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 SQL Server Multiple Instance Audit 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 Forefront Threat Management Gateway 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 Forefront Threat Management Gateway File	
SmartConnector	4
Product Overview	5
Configuring the Server	6
Threat Management Gateway 2010	6
Threat Management Gateway 2004/2006	9
Grant Access Privilege for Network Share	11
Install the SmartConnector	13
Prepare to Install Connector	13
Install Core Software	13
Set Global Parameters (optional)	14
Select Connector and Add Parameter Information	15
Select a Destination	15
Complete Installation and Configuration	16
Run the SmartConnector	17
Device Event Mapping to ArcSight Fields	18
Threat Management Gateway 2010 Web Proxy Service Log Mappings	18
Threat Management Gateway Firewall Service Log Mappings	19
Troubleshooting	21
Send Documentation Feedback	22

Configuration Guide for Microsoft Forefront Threat Management Gateway File SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Forefront Threat Management Gateway File (formerly Microsoft ISA 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

Microsoft Forefront Threat Management Gateway is a comprehensive, secure Web gateway for protecting against Web-based events, providing multiple layers of continuously updated, integrated protection. The Forefront Threat Management Gateway (TMG) server provides URL filtering, anti-malware inspection, intrusion prevention, firewall, and HTTP/HTTPS inspection in a single solution.

This SmartConnector can be used to collect events from one or more Threat Management Gateway servers.

Configuring the Server

Perform the following steps for each server from which the SmartConnector is to collect events.



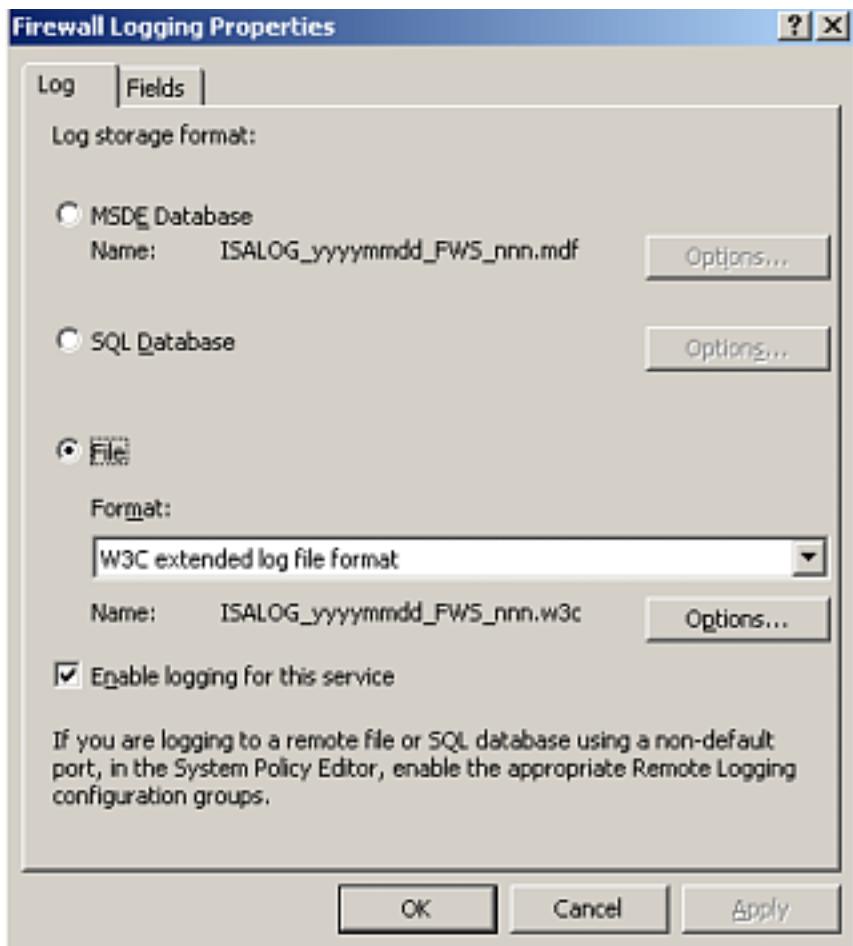
If you are planning to run the installed SmartConnector as a service, and the connector will be collecting events from multiple servers, the machine on which the connector is installed must have the same user credentials as the servers from which it is to collect events. Note that this connector cannot be run as a service when it is run remotely.

Threat Management Gateway 2010

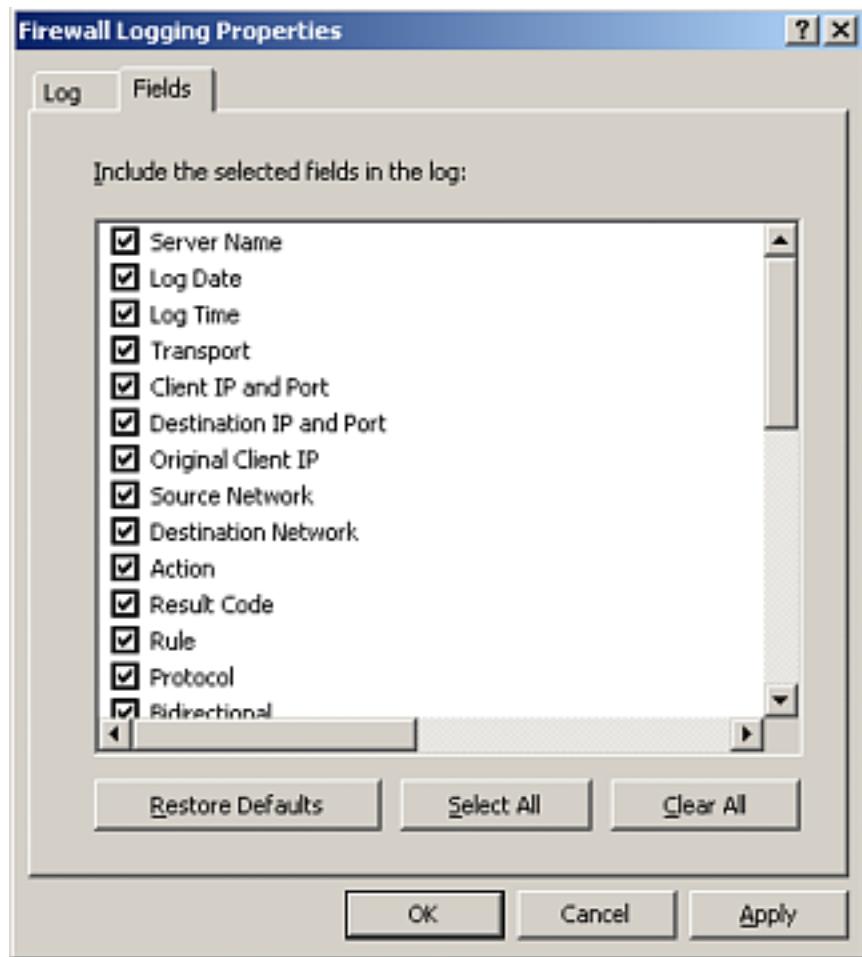
- 1 In the Management Console, expand the computer name in the left pane of the console and click the **Monitoring** node.
- 2 Click the **Logging** tab in the **Details** pane. Expose the **Task** pane if it is not already open. In the **Task** pane, click the **Tasks** tab and **Configure Firewall Logging**.



- 3 Select the **WC3 extended log file format** from the **Format** list. Confirm that a checkmark appears in the **Enable logging for this service** check box.

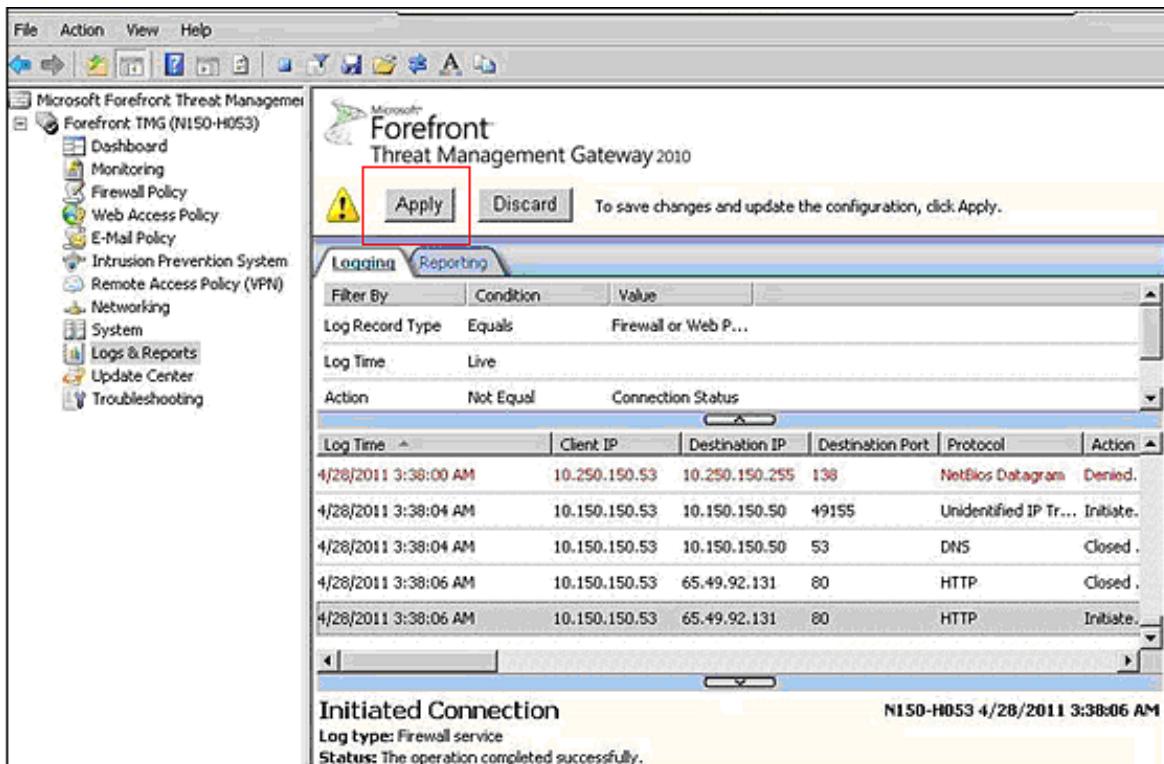


- 4 Click the **Fields** tab. Confirm that all fields are selected.



ArcSight recommends that you select all fields. Each field that appears in an event is mapped to an ArcSight field for correlation purposes; for example, Log Date and Log Time are mapped to Device Receipt Time, Transport is mapped to Transport Protocol, Protocol is mapped to Application Protocol, and so on. Any field that is not selected for logging cannot be processed.

- 5 Click **Apply** and then click **OK** in the Firewall Logging Properties dialog box.
- 6 Click **Apply** to save changes and update the firewall policy, as shown in the following image:

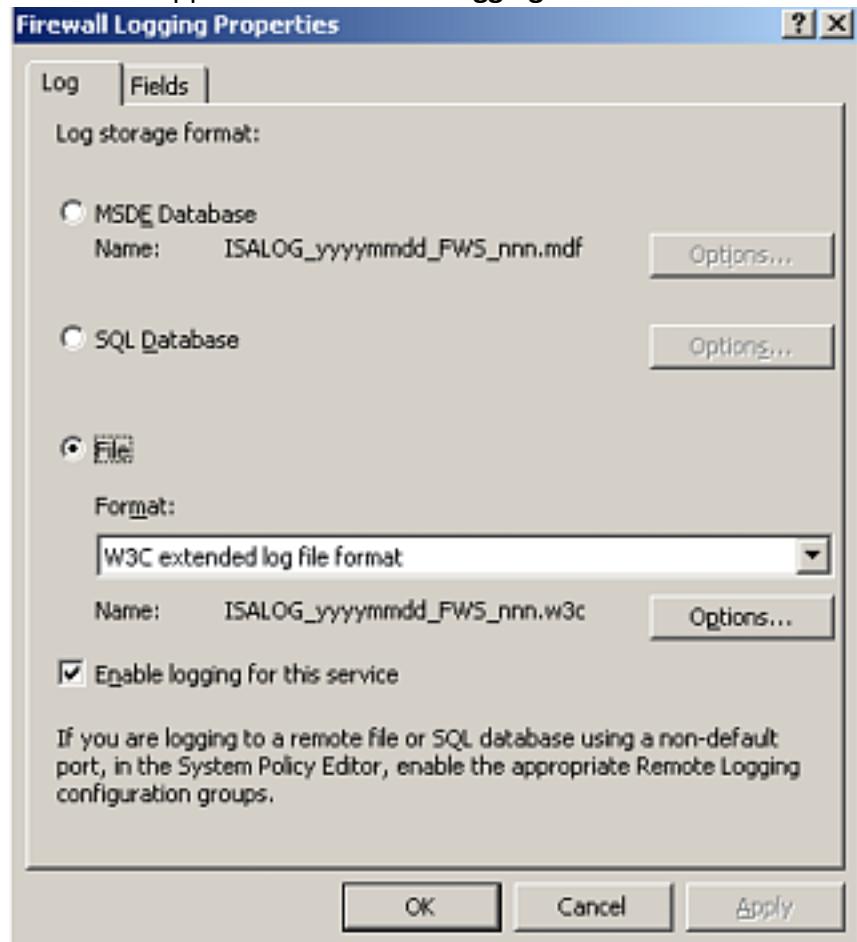


Threat Management Gateway 2004/2006

- 1 In the Management Console, expand the computer name in the left pane of the console and click the **Monitoring** node.
- 2 Click the **Logging** tab in the **Details** pane. Expose the **Task** pane if it is not already open. In the **Task** pane, click the **Tasks** tab and **Configure Firewall Logging**.

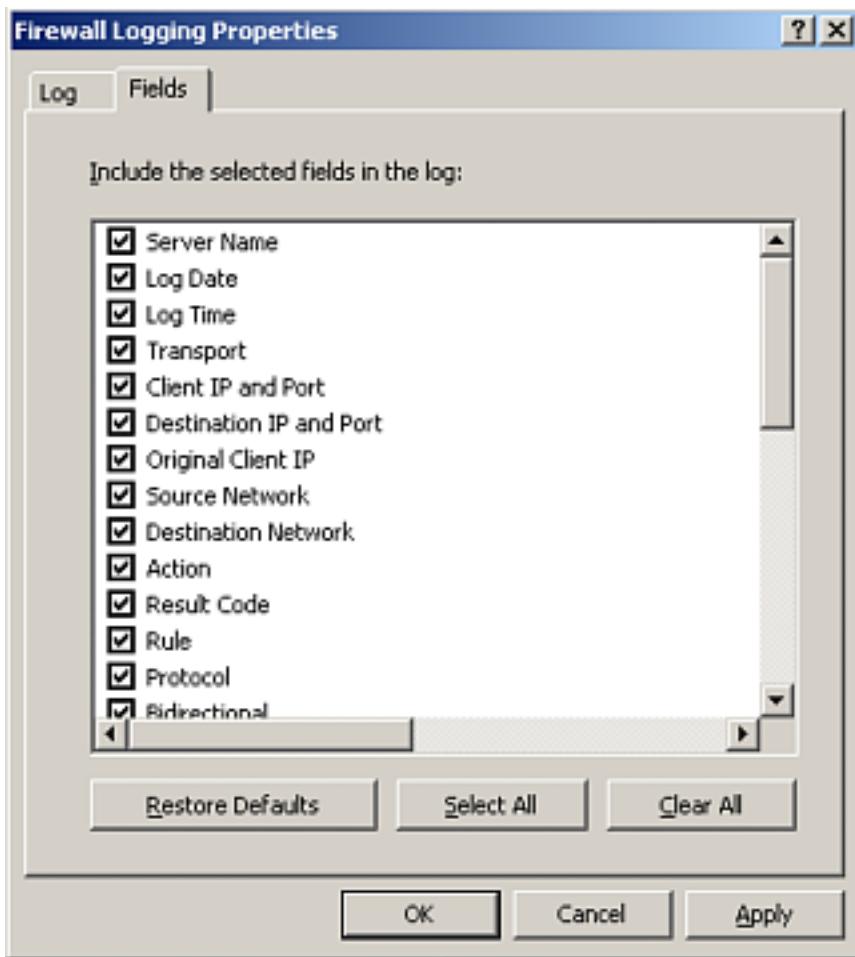


- 3 Select the **WC3 extended log file format** from the **Format** list. Confirm that a checkmark appears in the **Enable logging for this service** check box.



- 4 Click the **Fields** tab. Confirm that all fields are selected.

ArcSight recommends that you select all fields. Each field that appears in an event is mapped to an ArcSight field for correlation purposes; for example, Log Date and Log Time are mapped to Device Receipt Time, Transport is mapped to Transport Protocol, Protocol is mapped to Application Protocol, and so on. Any field that is not selected for logging cannot be processed.



5 Click **Apply** to save the changes and update the firewall policy.

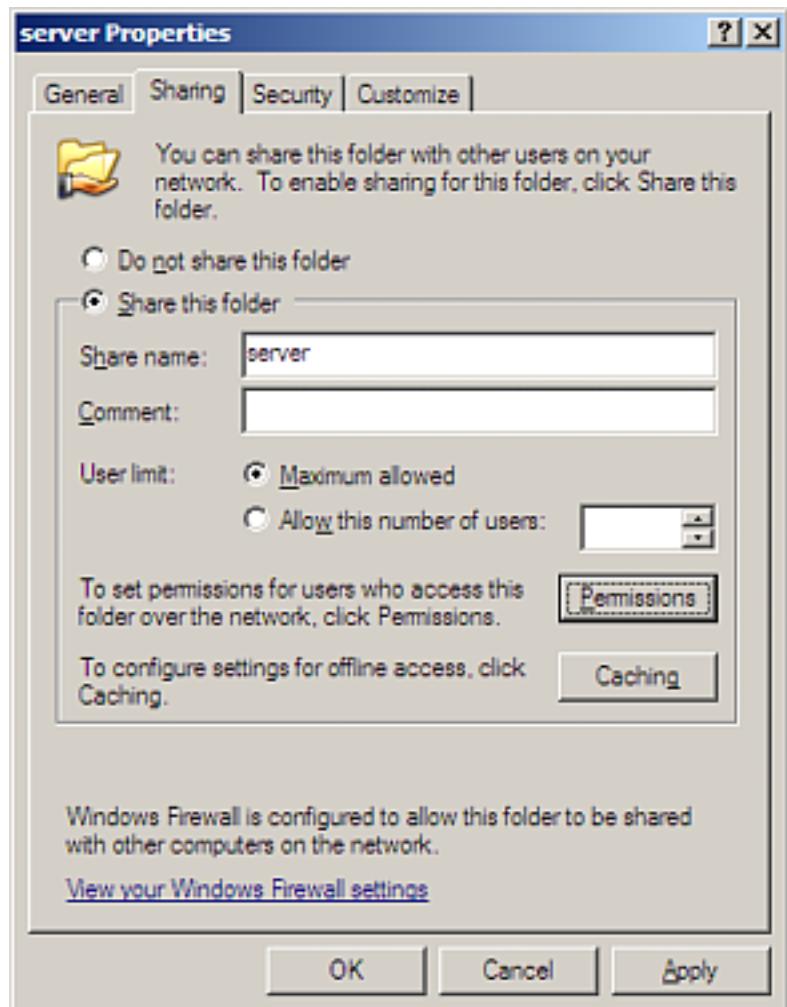
6 Click **OK** in the **Apply New Configuration** dialog box.

7 Click **OK** in the Firewall Logging Properties dialog box.

Grant Access Privilege for Network Share

To allow the SmartConnector to access the Server log folder, grant access as follows:

- 1 On each server, select the folder containing the logs. Right-click on the folder name and select **Properties**.
- 2 Click the **Sharing** tab.



3 Select **Share this folder**.

4 Click the **Permissions** tab to give the logon user of the SmartConnector machine the right to access the share you created.

5 Click **Add** and add the object type and location from the **Select Users, Computers, or Groups** dialog box. Click **OK** when you are finished adding the user; click **OK** to exit the **Permissions** window; click **OK** again to exit the **Properties** window.

If the SmartConnector is to read logs from a remote machine through a network share:

- 1** Use a UNC name for the folder to be shared (for example, \\computername\sharename) rather than a drive letter (such as F:).
- 2** Grant access privilege to the user who is to access this share.

 If you run the SmartConnector as a Windows service, use the **Log on** tab to enter the name and password for the user to whom access permission is to be granted.

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.

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 Forefront Threat Management Gateway File** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.

Parameter	Description
Server Log Folder	For each server, enter the log file home directory for your server log files.
Log Types	Enter the log file types to be collected (FWS, WEB, or both) from each server in the corresponding column.

You can click the 'Export' button to export the host name data you have entered into the table into a CSV file; you can click the 'Import' button to select a CSV file to import into the table rather than add the data manually. See the "SmartConnector User's Guide" for more information.

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.

Threat Management Gateway 2010 Web Proxy Service Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 400 – 599; Medium = 300 – 399; Low = 100 – 299
Application Protocol	cs-protocol
Bytes In	cs-bytes
Bytes Out	sc-bytes
Destination Address	r-ip
Destination Host Name	r-host
Destination Port	r-port
Destination Service Name	s-svcname
Device Action	action
Device Custom Number 3	time-taken
Device Custom String 1	c-agent
Device Custom String 2	FilterInfo
Device Custom String 3	sc-authenticated
Device Custom String 4	rule
Device Custom String 5	One of (cs-Network, cs-network)
Device Custom String 6	One of (sc-Network, sc-network)
Device Event Class ID	sc-status
Device Host Name	s-computername
Device Process Name	s-object-source
Device Product	'ISA Server'
Device Receipt Time	date, time

ArcSight ESM Field	Device-Specific Field
Device Severity	sc-status
Device Translated Address	NAT address
Device Vendor	'Microsoft'
Name	'Web Proxy Service Log'
Reason	UrlCategorizationReason
Request Client Application	c-agent
Request Method	s-operation
Request URL	cs-uri
Source Address	c-ip
Source Port	s-port
Source User Name	cs-username
Transport Protocol	cs-transport

Threat Management Gateway Firewall Service Log Mappings

ArcSight ESM Field	Device-Specific Field
Agent (Connector) Severity	High = 1 – 99, 400 – 999, 10000 – 11004, 13301, 20002; Medium = 300 – 399, 20001; Low = 0, 100 – 299, 20000
Application Protocol	application protocol
Bytes In	bytes received
Bytes Out	bytes sent
Destination Address	First part of destination
Destination Port	Second part of destination
Destination User Name	username
Device Action	action
Device Custom IPv6 Address 2	original client IP (Source IPv6 address)
Device Custom IPv6 Address 3	destination (destination IPv6 address)
Device Custom Number 1	bytes received intermediate
Device Custom Number 2	bytes sent intermediate
Device Custom Number 3	connection time

Configuration Guide for Microsoft Forefront Threat Management Gateway File SmartConnector Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 1	agent
Device Custom String 2	session ID
Device Custom String 3	connection ID
Device Custom String 4	rule
Device Custom String 5	source network
Device Custom String 6	destination network
Device Event Class ID	status
Device Host Name	computer
Device Payload ID	protocol payload
Device Product	'ISA Server'
Device Receipt Time	date, time
Device Severity	status
Device Translated Address	NAT Address
Device Vendor	'Microsoft'
Name	'Firewall Service Log'
Request Client Application	agent
Source Address	First part of source
Source Port	Second part of source
Transport Protocol	IP protocol

Troubleshooting

How do I specify the file rotation time zone when it is different from the connector host time zone?

The connector misses processing of events in realtime when the connector and file server are in different time zones. The `isalogfiletimezoneid` property has been added for specifying the log file rotation time zone.

To set this parameter, after connector installation, edit the `agent.properties` file located at `$ARCSIGHT_HOME\current\user\agent`. Locate the `isalogfiletimezoneid` parameter and set its value to the time zone for file rotation. Save the file and restart the connector for your changes to take effect.

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 Forefront Threat Management Gateway 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 MFT-Documentation-Feedback@opentext.com.

We appreciate your feedback!



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Microsoft Office 365 Management Activity 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 Office 365 Management Activity SmartConnector	5
Product Overview	6
Supported Audit Log Record Types	6
Microsoft Office 365 Event Retrieval Configuration	8
SmartConnector Application Registration in Azure AD	8
Generate Keys and Configure the Application Properties	13
Specify the Permissions the Connector Application Requires to Access the Office 365 Management Activity API	15
Limitations of the Microsoft Management Activity API	15
Specify Permissions in Microsoft Management Activity API	15
Install the SmartConnector	18
Prepare to Install Connector	18
Install Core Software	18
Set Global Parameters (optional)	19
Select Connector and Add Parameter Information	20
Select a Destination	22
Complete Installation and Configuration	22
Run the SmartConnector	23
Device Event Mapping to ArcSight Fields	23
Azure AD Common Mappings to ArcSight Fields	23
Azure AD Account Logon Mappings to ArcSight Fields	24
Azure AD Other Mappings to ArcSight Fields	24
Compliance Exchange Mappings to ArcSight Fields	24
CRM Mappings to ArcSight Fields	25
Data Insights REST API Mappings to ArcSight Fields	25
Discovery Mappings to ArcSight Fields	25
Exchange Online Admin Mappings to ArcSight Fields	26
Exchange Online DPL Mappings to ArcSight Fields	26
Exchange Online Mailbox Mappings to ArcSight Fields	27
Exchange Online Mailbox Item Mappings to ArcSight Fields	27
Exchange Online Mailbox Item Group Mappings to ArcSight Fields	28
Microsoft Teams Mappings to ArcSight Fields	29
(Office 365 Advanced Threat Protection) Threat Intelligence Mappings to ArcSight Fields	29
Microsoft Flow Mappings to ArcSight Fields	30
Advanced eDiscovery Mappings to ArcSight Fields	30

Project Mappings to ArcSight Fields	30
Security and Compliance Center to ArcSight Fields	31
Security and Compliance Center EOP Cmdlet Mappings to ArcSight Fields	31
Security and Compliance Alert Signals to ArcSight Fields	31
(Office 365 Advanced Threat Protection) Threat Intelligence Url to ArcSight Fields	32
Power Apps to ArcSight Fields	32
(Office 365 Advanced Threat Protection) Threat Intelligence Atp Content to ArcSight Fields	33
Microsoft Office 365 Common Mappings to ArcSight Fields	33
Power BI Audit Mappings to ArcSight Fields	34
SharePoint Online Common Mappings to ArcSight Fields	35
SharePoint Online and One Drive for Business List Mappings to ArcSight Fields	35
SharePoint Online and One Drive for Business File Mappings to ArcSight Fields	35
SharePoint Online Other Mappings to ArcSight Fields	36
SharePoint Online DLP Mappings to ArcSight Fields	36
SharePoint Online Sharing Mappings to ArcSight Fields	37
Sway Mappings to ArcSight Fields	38
Skype For Business Mappings to ArcSight Fields	38
Yammer Mappings to ArcSight Fields	38
Troubleshooting	39
Send Documentation Feedback	40

Configuration Guide for Microsoft Office 365 Management Activity SmartConnector

This guide provides information for installing the SmartConnector for Microsoft Office 365 and configuring the connector for event collection. Event collection is supported for Microsoft SharePoint Online, Exchange Online, Azure Active Directory (AD) and OneDrive.

This guide provides a high level overview of ArcSight SmartConnectors for the Cloud.

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

Microsoft Office 365 refers to subscription plans that include access to Office 365 applications that are enabled over the Internet (cloud services). Use the Microsoft Office 365 connector to retrieve information about user, admin, system, and policy actions and events from Microsoft Office 365 and Azure AD activity logs. You can use the actions and events from the Office 365 and Microsoft Azure Active Directory audit and activity logs to create solutions that provide monitoring, analysis, and data visualization. These solutions give organizations greater visibility into actions taken on their content.

For complete information about Microsoft Office 365, see the Microsoft website for Microsoft Office 365 documentation.

Supported Audit Log Record Types

The SmartConnector for Microsoft Office 365 supports the following Audit Log Record Types:

Value	Member Name	Description
1	ExchangeAdmin	Events from the Exchange Online admin audit log.
2	ExchangelItem	Events from an Exchange Online mailbox audit log for actions that are performed on a single item, such as creating or receiving an email message.
3	ExchangelItemGroup	Events from an Exchange Online mailbox audit log for actions that can be performed on multiple items, such as moving or deleted one or more email messages.
4	SharePoint	Sharepoint Online events.
6	SharePointFileOperation	Sharepoint Online file operation events.
8	AzureActiveDirectory	Azure Active Directory events.
9	AzureActiveDirectoryAccountLogon	Azure Active Directory OrgId logon events (deprecating).
10	DataCenterSecurityCmdlet	Data Center security cmdlet events.
11	ComplianceDLPSharePoint	Data loss protection (DLP) events in SharePoint and OneDrive for Business.
12	Sway	Events from the Sway service and clients.
13	ComplianceDLPExchange	Data loss protection (DLP) events in Exchange, when configured via Unified DLP Policy. DLP events based on Exchange Transport Rules are not supported.

Value	Member Name	Description
14	SharePoint Sharing Operation	SharePoint Online sharing events.
15	AzureActiveDirectoryStsLogon	Secure Token Service (STS) logon events in Azure Active Directory.
18	SecurityComplianceCenterEOPCmdlet	Admin actions from the Security and Compliance Center.
20	PowerBIAudit	Power BI events.
21	CRM	Microsoft CRM events.
22	Yammer	Yammer events.
23	Skype for Business CMDlets	Skype for Business events.
24	Discovery	Events for eDiscovery activities performed by running content searches and managing eDiscovery cases in the Security and Compliance Center.
25	Microsoft Teams	Events for Microsoft Teams.
28	ThreatIntelligence	Phishing and malware events from Exchange Online Protection and Office 365 Advanced Threat Protection.
30	MicrosoftFlow	Microsoft Power Automate (formerly called Microsoft Flow) events.
31	AeD	Advanced eDiscovery events.
33	Compliance DLP SharePoint Classification	Events related to DLP classification in SharePoint.
35	Project	Microsoft Project events.
36	SharePointListOperation	SharePoint List events.
38	DataGovernance	Events related to retention policies and retention labels in the Security and Compliance Center.
40	SecurityComplianceAlerts	Security and compliance alert signals.
41	ThreatIntelligenceUrl	Safe links time-of-block and block override events from Office 365 Advanced Threat Protection.
45	PowerAppsApp	Power Apps events
47	ThreatIntelligenceAtpContent	Phishing and malware events for files in SharePoint, OneDrive for Business, and Microsoft Teams from Office 365 Advanced Threat Protection.
52	DataInsightsRestApiAudit	Data Insights REST API events.
55	SharePointContentTypeOperation	SharePoint list content type events.

Value	Member Name	Description
56	SharePointFieldOperation	SharePoint list field events.
57	MicrosoftTeamsAdmin	Teams admin events.
68	ComplianceSupervisionExchange	Events tracked by the Communication compliance offensive language model.

See Microsoft documentation about Audit Log Record Types at:

<https://msdn.microsoft.com/en-us/library/office/mt607130.aspx#AuditLogRecordType>

Microsoft Office 365 Event Retrieval Configuration

The Office 365 connector uses the Office 365 Management Activity API which is a RESTful web service. The API relies on Azure AD and the OAuth2 protocol for authentication and authorization. To allow the connector to access the API, you must first register it in Azure AD and configure it with appropriate permissions.

SmartConnector Application Registration in Azure AD

The following configuration procedures allows you to establish an identity for the connector and specify the permission levels it needs in order to access the Management Activity API. Before registering the connector application with Azure AD, the following prerequisites must exist:

- An Office 365 subscription account must be enabled and configured.
- The Office 365 subscription must be associated with an Azure AD Tenant Domain account.

For more details see: [Associate your Office 365 account with Azure AD to create and manage apps](#).

To register your connector application in Azure AD:

Once you have a Microsoft tenant with the proper subscriptions, you can register your connector application in Azure AD.

1. Log in to the [Azure Management portal](#) using the credentials of your Microsoft tenant that has the subscription to Office 365 you wish to use.



2. In the left navigation panel, select **Azure Active Directory** (1). Select custom domain names (2) and add custom domain (3).

A screenshot of the Azure Active Directory portal. The left sidebar shows various services, with "Azure Active Directory" highlighted. The main area has a header with "Azure Active Directory" and buttons for "Overview", "Quick start", "Manage", and "Azure AD Connect". A "Custom domain names" link is circled with a blue oval. Below the header is a message: "Looking to move an on-premises application to the cloud and use Azure Active Directory Domain Services?". A table lists a single custom domain entry:

NAME	STATUS	FEDERATED	PRIMARY
connectorsqa.onmicrosoft.com	Available		

3. Add the custom domain name (1). Click on add domain (2) and verify (3).

The screenshot shows the Azure AD Custom Domains settings page. At the top, there is a form to add a custom domain:

- * Custom domain name: qacconn.onmicrosoft.com (with a green checkmark)
- Add Domain button

Below this, the custom domain qacconn.onmicrosoft.com is listed in the "Custom domain name" section:

- Delete link

A callout box provides instructions: "To use qacconn.onmicrosoft.com with your Azure AD, create a new TXT record with your domain name registrar using the info below."

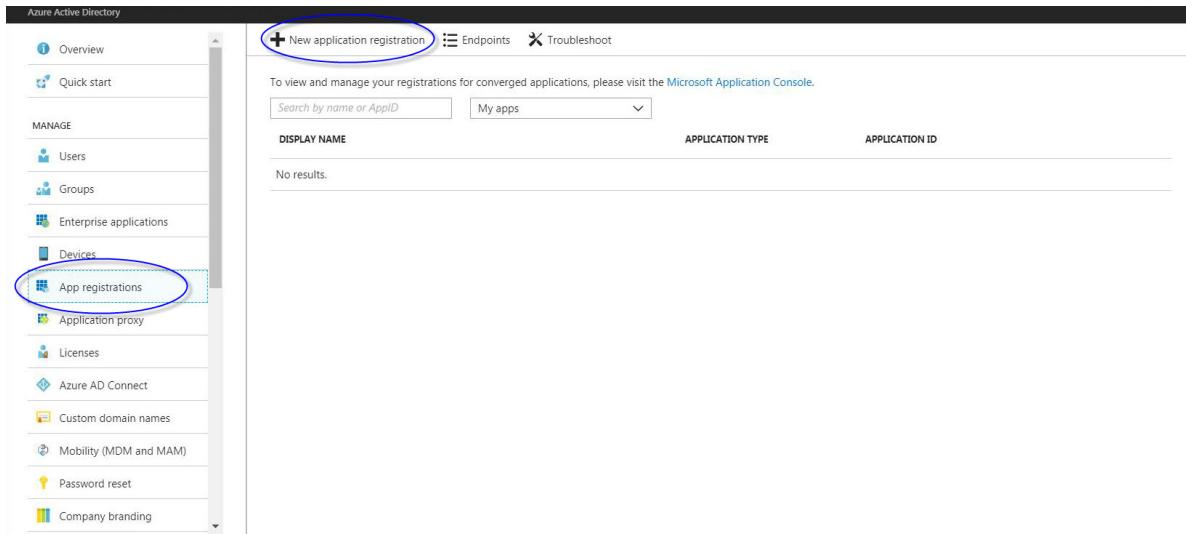
The "TXT" tab is selected under "RECORD TYPE". The configuration fields are:

- ALIAS OR HOST NAME: @
- DESTINATION OR POINTS TO ADDRESS: MS=ms89991300
- TTL: 3600

Below these fields are links for "Share these settings via email" and "Verify domain". The "Verify domain" section includes a note: "Verification will not succeed until you have configured your domain with your registrar as described above." and a "Verify" button.

APP ID URI: The URI is used as a unique logical identifier for your app. It must be a verified custom domain name used for external user to grant app access to their data in Windows Azure AD. This parameter is not required by the connector but it is required by Azure Active Directory to register the connector as a client application.

4. In the left navigation panel, select App registrations, then click on new application registration.



5. Enter a logical name, supported account types and redirect URI. Click register.

Home > Micro Focus - App registrations > Register an application

Register an application

* Name
The user-facing display name for this application (this can be changed later).
 

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Micro Focus only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.
 

By proceeding, you agree to the Microsoft Platform Policies [\[\]](#)

Register

SIGN-ON URL: This parameter is not required by the connector, but it is required by Azure Active Directory in order to register the connector as a client application. This value must be configured. You may want to configure this with any URL path that is not in use by any of your other applications. You can change this later as needed.

6. The "registered app" screen pops. Your connector app is now registered with Azure AD and has been assigned a client ID. However, there are several aspects of your connector app left to configure.

The screenshot shows the Azure portal's App registrations section. A new application named "SmartConnector" has been registered. Key details shown include:

- Display name:** SmartConnector
- Application (client) ID:** [REDACTED]
- Directory (tenant) ID:** [REDACTED]
- Object ID:** [REDACTED]
- Supported account types:** Multiple organizations
- Redirect URIs:** 1 web, 0 public client
- Application ID URI:** Add an Application ID URI
- Managed application in local directory:** SmartConnector

Generate Keys and Configure the Application Properties

Now that your connector application is registered, there are several important properties you must specify that determine how your connector application functions within Azure AD.

1. Click Certificates and secrets.

The screenshot shows the "Certificates & secrets" blade for the "SmartConnector" application. The left sidebar lists various management options, and the right pane shows the following details:

- Certificates:** No certificates have been added for this application. There is a button to "Upload certificate".
- Client secrets:** A secret string that the application uses to prove its identity when requesting a token. There is a button to "+ New client secret".

2. Click **New client secret**. Enter a description and select never expires. Click **Add**.

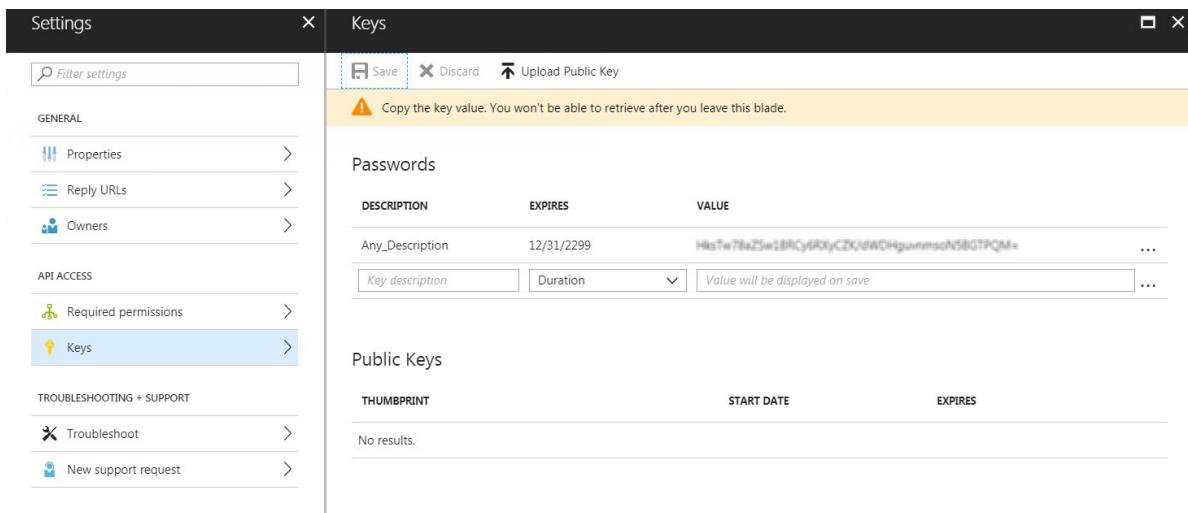
Add a client secret

Description
Description

Expires
 In 1 year
 In 2 years
 Never

Add **Cancel**

3. Scroll up to view the **Client ID** value. This value is automatically generated by Azure AD. Your connector application will use this value.
4. Use the highlighted Clipboard icon to copy the **Client ID** value and paste it somewhere it can be saved, such as a text document. This value will be used to configure the connector during the connector installation.



The screenshot shows the 'Keys' blade in the Azure portal. On the left, there's a navigation menu with 'Properties', 'Reply URLs', 'Owners', 'Required permissions', and 'Keys' (which is selected). The main area has tabs for 'Save', 'Discard', and 'Upload Public Key'. A warning message says 'Copy the key value. You won't be able to retrieve after you leave this blade.' Below this, there's a table for 'Passwords' with one row: 'Any_Description' (EXPIRES: 12/31/2299, VALUE: Hk5Tw7BaZSw1BRCy6R0jCZV/dWCHguunmsnN5BGTPQm=). There are also sections for 'Public Keys' and 'No results.'

5. Scroll down to view the **Reply URL**. This parameter is not required by the connector, but it is required by Azure Active Directory in order to register the connector as a client application. This value must be configured. You may want to configure this with any URL path that is not in use by any of your other applications. Sample value: [oauth2callback](#)
6. Click **Save** if you make any changes to these values. Example value:
7. Remain on the **Configuration** page for the next procedure.

Specify the Permissions the Connector Application Requires to Access the Office 365 Management Activity API

You need to specify exactly what permissions your connector application requires of the Office 365 Management Activity API. To do so, you add access to the Office 365 Management APIs to your connector application, and then you specify the permission(s) you need.

Limitations of the Microsoft Management Activity API

The maximum lifespan of events available from the Microsoft Management Activity API is seven days.

When the connector is first started, it can take up to 12 hours for the first events to become available from the Management Activity API. The events may also appear out of order. This is due to the limitation of the Management Activity API, as mentioned by Microsoft at:

<https://msdn.microsoft.com/library/office/mt227394.aspx>

Specify Permissions in Microsoft Management Activity API

To specify permission for the connector application to access the Microsoft Management Activity API

1. From the Azure Management Portal, click **App registrations**, select your connector application and click API permissions, click **Add a permission**.

Home > Micro Focus - App registrations > SmartConnector - API permissions

SmartConnector - API permissions

[Search \(Ctrl+ /\)](#)

[Overview](#)

[Quickstart](#)

Manage

- [Branding](#)
- [Authentication](#)
- [Certificates & secrets](#)
- [API permissions](#)
- [Expose an API](#)
- [Owners](#)
- [Roles and administrators \(Previous\)](#)
- [Manifest](#)

Support + Troubleshooting

- [Troubleshooting](#)
- [New support request](#)

API permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs.

[Add a permission](#)

API / PERMISSIONS NAME	TYPE	DESCRIPTION	ADMIN CONSENT...	STATUS
▼ Microsoft Graph (1)				
User.Read	Delegated	Sign in and read user profile	-	

These are the permissions that this application requests statically. You may also request user consenable permissions dynamically through code. [See best practices for requesting permissions](#)

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

[Grant admin consent for Micro Focus](#)

2. Select the Office 365 Management APIs.

Request API permissions

[Azure DevOps](#)
Integrate with Azure DevOps and Azure DevOps server

[Azure Rights Management Services](#)
Allow validated users to read and write protected content

[Azure Service Management](#)
Programmatic access to much of the functionality available through the Azure portal

[Data Export Service for Microsoft Dynamics 365](#)
Export data from Microsoft Dynamics CRM organization to an external destination

[Dynamics 365 Business Central](#)
Programmatic access to data and functionality in Dynamics 365 Business Central

[Dynamics CRM](#)
Access the capabilities of CRM business software and ERP systems

[Flow Service](#)
Embed flow templates and manage flows

[Intune](#)
Programmatic access to Intune data

[Office 365 Management APIs](#)
Retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity

[OneNote](#)
Create and manage notes, lists, pictures, files, and more in OneNote notebooks

[Power BI Service](#)
Programmatic access to Dashboard resources such as Datasets, Tables, and Rows in Power BI

[PowerApps Runtime Service](#)
Powerful data storage, modeling, security and integration capabilities

3. Click **Application permissions** and check the **ActivityFeed.Read**, **ActivityFeed.ReadDlp** and **ServiceHealth.Read**. Click **Add permissions**.

4. Click **Save** to save the configuration. Select API Office 365 and click done.

Request API permissions

[All APIs](#) [Office 365 Management APIs](#) <https://manage.office.com/> Docs

What type of permissions does your application require?

Delegated permissions Your application needs to access the API as the signed-in user.	Application permissions Your application runs as a background service or daemon without a signed-in user.
---	---

Select permissions [expand all](#)

Start typing a permission to filter these results

Permission	Admin consent required
ActivityFeed (2)	
<input checked="" type="checkbox"/> ActivityFeed.Read ⓘ Read activity data for your organization	Yes
<input checked="" type="checkbox"/> ActivityFeed.ReadDlp ⓘ Read DLP policy events including detected sensitive data	Yes
ServiceHealth (1)	
<input checked="" type="checkbox"/> ServiceHealth.Read ⓘ Read service health information for your organization	Yes

5. Click **Grant admin consent**.



This step must be performed by an admin account. Ask your administrator to go to the [Azure portal](#) > [App registrations](#) and click on the application that you registered. Then click [API permissions](#) > [Grant admin consent](#).

Grant consent

As an administrator, you can grant consent on behalf of all users in this directory. Granting admin consent for all users means that end users will not be shown a consent screen when using the application.

[Grant admin consent for Micro Focus](#)

Install the SmartConnector

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

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.

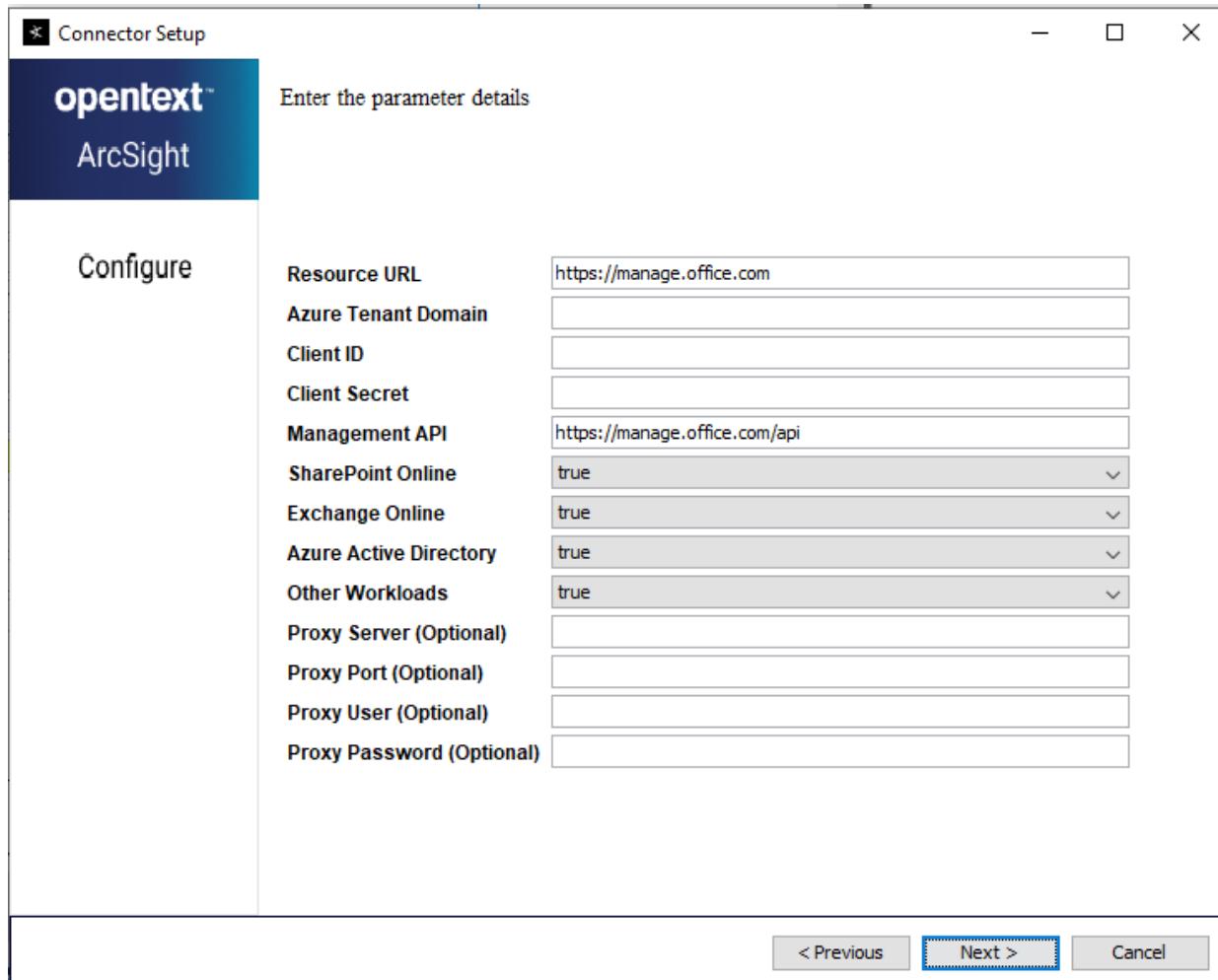
Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of 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.

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 Office 365** and click **Next**.
- 3 Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Description
Resource URL	The Office 365 Management URL. Default value: https://manage.office.com
Azure Tenant Domain	The domain name of the Office 365 Azure tenant. Sample value: mycompany.onmicrosoft.com
Client ID	The Client ID of the application registered in Azure Active Directory. See step 3 in the "Generate Keys and Configure the Application Properties" section.
Management API	The Office 365 Management API URL. Default value: https://manage.office.com/api
Client Secret	The Client Secret of the application registered in Azure Active Directory. See step 2 in the "Generate Keys and Configure the Application Properties" section.
SharePoint Online	To collect events from SharePoint Online, select 'true'.
Exchange Online	To collect events from Exchange Online, select 'true'.

Parameter	Description
Azure Active Directory	To collect events from Azure AD, select 'true'.
Proxy Server (Optional)	(Optional) The proxy server used to access the Internet.
Proxy Port (Optional)	(Optional) The proxy port used to access the Internet.
Proxy User (Optional)	(Optional) The proxy user used to access the Internet.
Proxy Password (Optional)	(Optional) The proxy password used to access the Internet.

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.

Azure AD Common Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
DestinationUserName	targetUPN
DestinationUserPrivileges	Role.DisplayName NewValue
Device Custom String 2	ModifiedProperties
Device Custom String 6	ExtendedProperties
File Type	AzureActiveDirectoryEventType, 0=AccountLogon, 1=AzureApplicationAuditEvent
Old File Hash	RequestType in ExtendedProperties (overloading field)

ArcSight ESM Field	Device-Specific Field
Old File Id	ResultStatusDetail in ExtendedProperties (overloading field)
Old File Name	UserAgent in ExtendedProperties (overloading field)
Old File Path	resultDescription in ExtendedProperties (overloading field)
Request Context	<code>__concatenate(targetContextId, targetName, targetObjectId, targetPUID, targetSPN)</code> in ExtendedProperties (overloading field)
Request Method	UserAuthenticationMethod in ExtendedProperties (overloading field)
SourceUserName	actorUPN
SourceUserPrivileges	Role.DisplayName OldValue

Azure AD Account Logon Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Number 1	LoginStatus
Device Custom String 5	Client (Client Details)
Old File Name	SupportTicketId (if its value is String)
Request Client Application	Application
Source NT Domain	UserDomain

Azure AD Other Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Source Username	Actor
Destination Username	Target
Device Custom Number 2	SupportTicketId (if its value is Long)
Device Custom String 3	Actor
Device Custom String 5	Target

Compliance Exchange Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	IsPolicyHit
Device Custom String 2 Label	Is Policy Hit
File Id	ObjectId

ArcSight ESM Field	Device-Specific Field
Old File Hash	SRPolicyMatchDetails/SRPolicyMatchDetails
Old File Id	SRPolicyMatchDetails/SRPolicyId
Old File Name	SRPolicyMatchDetails/SRPolicyName

CRM Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination Service Name	ServiceName
Destination User Id	SystemUserId
Destination User Name	UserUpn
Device Custom String 3	CrmOrganizationUniqueName
File Id	ObjectId
File Type	ItemType
Old File Hash	CorrelationId
Old File Id	EntityId
Old File Name	EntityName
Request Client Application	UserAgent
Request Context	__concatenate(ServiceContextId,ServiceContextIdType)
Request URL	__oneOf(InstanceUrl,ItemUrl)

Data Insights REST API Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
File Type	DataType

Discovery Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
File Hash	Cmdlet
File Id	CaseId
File Name	Case
File Path	SharepointLocations
File Permission	PublicFolderLocations

ArcSight ESM Field	Device-Specific Field
File Type	ObjectType
Old File Hash	CmdletOptions
Old File Path	ExchangeLocations

Exchange Online Admin Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	Parameters, Organization
Destination User Name	One of (StatusMailRecipients, User, Name, Identity)
DestinationUserPrivileges	Parameters, AccessRights
Device Custom Number 1	Public Folder Hierarchy Mailbox Count Quota
Device Custom String 5	Identity
Device Custom String 6	Organization Name
End Time	Parameters, EndDate, UTC, MM/dd/yyyy hh:mm:ss a z
File ID	ObjectId
File Name	ModifiedObjectResolvedName
File Type	Parameters, FileTypes
Request Method	ExternalAccess
Request Parameters	Parameters
Request URL	Parameters, PrivacyStatementURL
Source Host Name	OriginatingServer
Start Time	Parameters, StartDate, UTC, MM/dd/yyyy hh:mm:ss a z

Exchange Online DPL Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	ExchangeMetaData
Device Custom Date 1	Sent Time
Device Custom Number 1	Unique Count
Device Custom String 2	Subject
Device Custom String 3	Policy Name

ArcSight ESM Field	Device-Specific Field
Device Custom String 5	Actions
Device Custom String 6	Recipients
Device Severity	PolicyDetails
File Id	Incident Id
File Name	Message ID
Old File Id	Policy Id
Old File Name	PolicyDetails
Source User Name	ExchangeMetaData

Exchange Online Mailbox Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom IPv6 Address 2	Source IPv6 Address
Device Custom Number 1	LogonType
Device Custom String 2	ClientInfoString
Device Custom String 5	ExternalAccess
Device Custom String 6	OrganizationName
Device Version	ClientVersion
Source Address	ClientIPAddress
Source Host Name	OriginatingServer
Source Process Name	ClientProcessName
Source User Name	One of (LogonUserDisplayName, MailboxOwnerUPN)

Exchange Online Mailbox Item Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (SendAsUserSmtp,SendOnBehalfOfUserSmtp)
Destination User Privileges	MailboxOwnerSid
Device Custom Number 2 Label	Internal Logon Type
Device Custom Number2	InternalLogonType
Device Custom String 3	Subject

ArcSight ESM Field	Device-Specific Field
File Hash	MailboxGuid (overloading field)
File Id	InternetMessageId
File Name	Item.Attachments
File Path	Item.Path
File Permission	SessionId (overloading field)
File Size	Item.Attachments
Old File Name	Item (overloading field)
Old File Path	Item/ParentFolder
Source User Privileges	LogonUserSid

Exchange Online Mailbox Item Group Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User ID	DestMailboxOwnerSid
Destination User Name	DestMailboxOwnerUPN
Destination User Privileges	MailboxOwnerSid
Device Custom Number 2	InternalLogonType
Device Custom Number 2 Label	Internal Logon TypeA
Device Custom String 3	Subject
File Hash	MailboxGuid (overloading field)
File Id	DestFolder (Id)
File Path	DestFolder (Path)
File Permission	SessionId (overloading field)
File Type	Attachments in AffectedItems (overloading field)
Old File Hash	Path in AffectedItems (overloading field)
Old File Id	Folder (Id)
Old File Name	Item (overloading field)
Old File Path	Folder (Path)
Old File Type	Id in AffectedItems (overloading field)
Request Cookies	AffectedItems
Source User Privileges	LogonUserSid

Microsoft Teams Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	AdminActionDetail
Device Custom String 3	TeamName
File Hash	TeamGuid
File Id	ChannelGuid
File Name	<code>__oneOf(ChannelName, ItemName)</code>
File Permission	Members
File Type	ChannelType
Old File Id	<code>__oneOf(MessageId, ObjectId)</code>
Request Client Application	ClientApplication
Source User Name	UPN

(Office 365 Advanced Threat Protection) Threat Intelligence Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	Recipients
Device Custom Date 1	MessageTime
Device Custom Number 3	Subject
File Hash	SHA256
File Id	NetworkMessageId
File Name	FileName
File Permission	FileVerdict
Old File Hash	MalwareFamily
Old File Id	InternetMessageId
Old File Permission	Verdict
Old File Type	DetectionType
Request Context	AttachmentData
Request Method	DetectionMethod

ArcSight ESM Field	Device-Specific Field
Request URI	EventDeepLink
Source Address	SenderIp
Device Custom String 2	P2Sender
Source User Name	P1Sender

Microsoft Flow Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
File Name	FlowConnectorNames
File Permission	SharingPermission
File Type	UserTypeInitiated
Request Context	LicenseDisplayName
Request URI	FlowDetailsUrl
Source User Name	UserUPN

Advanced eDiscovery Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	StartTime
Device Custom Date 2	EndTime
File Name	CaseName
File Type	WorkingSetId
Old File Id	CasId

Project Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Action	Action
Device Custom String 5	EventSource
File Name	Entity
File Type	ItemType
Old File Hash	CorrelationId
Request Client Application	UserAgent

Security and Compliance Center to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	ModifiedBy
Device Action	RetentionAction
Device Custom Date 1	CreatedDateUTC
Device Custom Date 2	LastModifiedDateUTC
Device Custom String 3	PolicyName
Device Custom String 6	Workload
File Hash	Cmdlet
File Name	LabelName
File Type	ObjectType
Old File Hash	CmdletOptions
Old File Type	RetentionType
Source User Name	AlertEntityId

Security and Compliance Center EOP Cmdlet Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	ClientApplication
Device Custom String 2	CmdletVersion
Device Custom String 2 Label	CMD Let Version
File Hash	Parameters
File Type	SecurityComplianceCenterEventType
Old File Hash	NonPIIParameters
Old File Id	EffectiveOrganization

Security and Compliance Alert Signals to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Data
Device Custom String 3 Label	Data

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	Source
Device Custom String 6 Label	Source
Device Severity	Severity
Event Outcome	Status
File Id	AlertId
File Name	Name
File Permission	Category
File Type	AlertType
Old File Id	PolicyId
Old File Permission	Comments
Old File Type	EntityType
Source User Name	CreatedBy

(Office 365 Advanced Threat Protection) Threat Intelligence Url to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	TimeOfClick
Device Custom String 2	EventDeepLink
Device Custom String 5	UrlClickAction
Device Custom String 6	SourceWorkload
File Id	SourceId
Request Client Application	AppName
Request URI	Url
Source Address	UserIp

Power Apps to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	AdditionalInfo
Request Client Application	AppName

(Office 365 Advanced Threat Protection) Threat Intelligence Atp Content to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom Date 1	DetectionDate
Device Custom Date 2	LastModifiedDate
Device Custom String 2	EventDeepLink
Device Custom String 3	LastModifiedBy
Device Custom String 6	SourceWorkload
File Hash	FileData\SHA256
File Id	FileData\DocumentId
File Name	FileData\FileName
File Path	FileData\FilePath
File Permission	FileData\FileVerdict
File Size	FileData\FileSize
File Type	FileData\MalwareFamily
Request Method	DetectionMethod

Microsoft Office 365 Common Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Action	Operation
Device Custom IPv6 Address2	Source IPv6 Address
Device Custom Number 3	UserType
Device Custom String 1	OrganizationId
Device Custom String 4	UserKey

ArcSight ESM Field	Device-Specific Field
Device Event Category	(RecordType, 1=ExchangeAdmin, 2=ExchangeItem, 3=ExchangeItemGroup, 4=SharePoint, 6=SharePointFileOperation, 8=AzureActiveDirectory, 9=AzureActiveDirectoryAccountLogon, 10=DataCenterSecurityCmdlet, 11=ComplianceDLPSharePoint, 12=Sway, 13=ComplianceDLPExchange), 14=SharePointSharingOperation, 15=AzureActiveDirectoryStsLogon, 18=SecurityComplianceCenterEOPCmdlet, 20=PowerBI, 21=CRM, 22=Yammer, 23=SkypeForBusinessCmdlets, 24=Discovery, 25=MicrosoftTeams, 28=ThreatIntelligence, 30=MicrosoftFlow, 31=AeD, 33=ComplianceDLPSharePointClassification, 35=Project, 36=SharepointListOperation, 38=DataGovernance, 40=SecurityComplianceAlerts, 41=ThreatIntelligenceUrl, 45=PowerAppsApp, 47=ThreatIntelligenceAtpContent, 52=DataInsightRESTAPI, 55=SharePointContentTypeOperation, 57=MicrosoftTeamsAdmin, 68=ExchangeCommunicationCompliance
Device Event Class ID	Operation
Device Product	Workload, AzureActiveDirectory=Azure Active Directory, Exchange=Exchange Online, SharePoint=SharePoint Online, OneDrive=OneDrive
Device Receipt Time	CreationTime, UTC, yyyy-MM-dd'T'HH:mm:ss z
Device Vendor	"Microsoft"
Event Outcome	ResultStatus
External ID	Id
Message	Operation
Name	Operation
Source Address	ClientIP
Source Port	ClientIP
Source User ID	UserId

Power BI Audit Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	DeviceType
File Hash	ReportName
File Name	DashboardName
Old File Name	DatasetName
Request Context	Endpoint
Source User Privileges	WorkSpaceName

SharePoint Online Common Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 3	Site
Device Custom String 5	One of ((EventSource, 0=SharePoint, 1=ObjectModel) EventSource)
File Path	ObjectId
File Type	One of ((ItemType, 0=Invalid, 1=File, 5=Folder, 6=Web, 7=Site, 8=Tenant, 9=DocumentLibrary) ItemType)
Request Client Application	UserAgent
Source Process Name	SourceName

SharePoint Online and One Drive for Business List Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	ListBaseTemplateType
Device Custom String 6	ListTitle
File Id	ListId (overloading field)
File Name	FileName
File Path	FilePathUrl
Old File Hash	CorrelationId (overloading field)
Old File Id	ListItemUniqueId (overloading field)
Old File Type	ListBaseType
Request Context	ApplicationDisplayName
Request Cookies	WebId (overloading field)

SharePoint Online and One Drive for Business File Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Bytes In	FileSyncBytesCommitted
Destination User ID	EventData.<Shared by>

ArcSight ESM Field	Device-Specific Field
Destination User Name	One of (UserSharedWith, EventData.<Shared by>, TargetUserOrGroupName)
Destination User Privileges	SharingType
Device Custom String 6	PolicyDetails
Device CustomString 6 Label	PolicyDetails
File Name	DestinationFileName
File Path	DestinationRelativeUrl
File Type	DestinationFileExtension
Old File Hash	CorrelationId (overloading field)
Old File Id	ApplicationId (overloading field)
Old File Name	SourceFileName
Old File Path	SourceRelativeUrl
Old File Type	SourceFileExtension
Request Context	ApplicationDisplayName
Request URL	SiteUrl
Source User Name	EventData,<Invited account>

SharePoint Online Other Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 2	ModifiedProperties

SharePoint Online DLP Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	DocumentLastModifier
Device Custom String 6 Label	Document Last Modifier
File Id	UniqueId
File Name	FileName
File Path	FilePathUrl
File Size	FileSize
Old File Permission	FileOwner (overloading field)

ArcSight ESM Field	Device-Specific Field
Request Cookies	SiteCollectionGuid (overloading field)
Request Method	SharePointMetaData
Request Url	SiteCollectionUrl
Source Process Name	From

SharePoint Online Sharing Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Name	TargetUserOrGroupName
Destination User Privileges	TargetUserOrGroupType
Device Custom Number 1	Version
Device Custom Number 1 Label	Version
Device Custom String 2	ModifiedProperties\NewValue
Device Custom String 2 Label	Old Value
Device Custom String 6	ModifiedProperties\OldValue
Device Custom String 6 Label	New Value
File ID	UniqueSharingId
File Name	ModifiedProperties\Name
File Type	<code>__oneOf (__simpleMap(ItemType,"0=Invalid","1=File","5=Folder","6=Web","7=Site","8=Tenant","9=DocumentLibrary"),ItemType)</code>
Old File ID	ApplicationId
Old File Name	SourceFileName
Old File Path	SourceRelativeUrl
Old File Type	SourceFileExtension
Request Context	ApplicationDisplayName
Request Cookies	WebId
Request Method	EventData
Request Url	SiteUrl

Sway Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Custom String 6	DeviceType
File ID	SwayLookupId
File Type	ObjectType
Request Client Application	BrowserName
Request Context	Endpoint
Request Url	SiteUrl

Skype For Business Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination DNS Domain	DomainController
Destination User Name	Destination
Device Custom String 6	CmdletVersion
Event Outcome	Status
File Hash	EnableCustomTrunking
File Name	ObjectName
Source User Name	Organization

Yammer Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Destination User Id	TargetYammerUserId
Destination User Name	TargetUserId
Device Custom Number 1	VersionId
Device Custom Number 2	YammerNetworkId
File Id	FileId
File Name	FileName
Old File Id	MessageID
Source User Name	ActorUserId
Source User Privileges	ActorYammerUserId

Troubleshooting

What to do if the SmartConnector stops receiving new events after running for a few days?

By default, the connector sends a query to the Management API and gets new events every 30 seconds, this process can be interrupted by a proxy or a firewall.

Workaround: Increase the execution time between queries. Go to the `agent.properties` file and change the `content.uri.queue.producer.thread.sleeptime` value from 30000 to 300000.

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 Office 365 Management Activity
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 25.1

Configuration Guide for OpenText Network Detection & Response (Bricata) 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 OpenText Network Detection & Response (Bricata) SmartConnector	4
Product Overview	5
Configuration	6
Configuring for the Syslog SmartConnectors	6
Installing the SmartConnector	9
Preparing to Install the SmartConnector	9
Installing and Configuring the SmartConnector	10
Post-Installation Configuration	13
Device Event Mapping to ArcSight Fields	14
OpenText Network Detection & Response (Bricata) Event Mappings to ArcSight Fields	14
Send Documentation Feedback	16

Configuration Guide for OpenText Network Detection & Response (Bricata) SmartConnector

This guide provides information for installing the SmartConnector for OpenText Network Detection & Response (Bricata) and configuring the device for syslog 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

OpenText Network Detection & Response (NDR) is an advanced platform for network detection and response solutions for enterprises. OpenText NDR provides organizations with 360-degree protection, end-to-end visibility and context for direct answers, and powerful insight to take immediate action. The solution provides complete visibility of east-west traffic across network environments in real time and full-spectrum threat detection that extracts and stores high-fidelity metadata, including an indexed threat hunting repository. A multi-faceted suite of best-in-breed threat detection allows organizations to thoroughly inspect network traffic from every angle. Users can find unknown, hidden threats to conduct retrospective network traffic analysis and historical data testing to determine if threats have infiltrated the environment prior to known indicators being available. They can use meaningful visualizations and flexible network views to see everything in a single pane of glass or create custom views. With seamless response and extensive integrations, organizations can correlate alerts in real time, enrich existing workflows, automate responses and prevent threats. OpenText NDR is the only end-to-end network detection and response platform that allows both security teams and the entire enterprise to collaborate better, reduce security risk, and solve network problems faster than ever before.

Salient Features of OpenText NDR:

- Empowers high-performance enterprise security teams with total visibility into network traffic.
- Helps in fusing detection, forensic analysis, and proactive threat hunting.
- Empowers security teams to effectively defend against known threats and to identify those otherwise unseen using signature inspection, stateful anomaly detection, and machine learning-powered malware conviction.

Configuration

Configuring for the Syslog SmartConnectors

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 Daemon, Syslog Daemon NG, or Syslog File connector types depending on your requirement. The Syslog File type SmartConnectors also support Syslog Pipe.

Syslog Daemon SmartConnector

The Syslog Daemon 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 your selected SmartConnector.

Syslog Installation

Install this SmartConnector (on the syslog server or servers identified in the Configuration section) using the SmartConnector Installation Wizard appropriate for your operating system. The wizard will guide you through the installation process. When prompted, select one of the following Syslog connectors (see [Configure the Syslog SmartConnectors](#) in this guide for more information):

- Syslog Daemon
- Syslog Pipe
- Syslog File

Because all syslog SmartConnectors are sub-connectors of the main syslog SmartConnector, the name of the specific syslog SmartConnector you are installing is not required during installation.

The syslog daemon connector by default listens on port 514 (configurable) for UDP syslog events; you can configure the port number or use of the TCP protocol manually. The syslog pipe and syslog file connectors read events from a system pipe or file, respectively. Select the one that best fits your syslog infrastructure setup.

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. 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](#).

Post-Installation Configuration

OpenText NDR facilitates the export of three types of events which are alerts, metadata, and health events, from either the Central Management Console (CMC) or the sensor to various Security Information and Event Management (SIEM) destinations. To enable this functionality, the network configuration must permit the transmission of these events from the CMC or sensor to the designated SIEM ports. Currently, the Syslog Connector has been expanded to include support for Alerts. This section outlines the steps to configure the system for exporting events from the CMC to the Syslog Connector.

Perform the following steps to create a system export configuration:

1. Navigate to **System > Configuration > CMC Event Export(s)** in the main navigation menu.
2. Click **+EXPORT** on the action bar to generate a default export configuration.
3. Enter a name for the configuration in **Export Configuration Name**. Select **Default** export template from the Templates, and click **CREATE**. This will display the export configuration name and template values in the **Exports** view. The system will now populate the new configuration with the default settings.
4. Click **configuration** to view more details and make required modifications. The system permits the selection of one of event types for export.
5. The following are the event types: Alerts, Metadata, Health Alerts.
6. Select **ALERTS** as the event type and clear the Metadata and Health Alerts check boxes.
7. Navigate to **Export** and select **RAW** to stream raw JSON data to the connector. Select the same protocol that the connector was configured with.
8. Enter the IP address of the machine where the connector is installed and specify the port number over which the connector is configured to receive events.
9. Click **VERIFY** to validate the configuration and click **SAVE** on the action bar to save the export configuration.

Device Event Mapping to ArcSight Fields

The following table lists the mapping of ArcSight data fields to the device's specific event definitions. See *ArcSight 101* for more information about the ArcSight data fields.

OpenText Network Detection & Response (Bricata) Event Mappings to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Application Protocol	app_proto or app_proto_tc
Bytes In	bytes_toserver
Bytes Out	bytes_toclient
Destination Address	dest_ip
Destination Port	dest_port
Device Action	Action
Device Address	sensor_ipv4
Device Custom Number 3	linktype
Device Custom Number 3 Label	Linklayer protocol
Device Custom String 1	src_location_country or dest_location_country
Device Custom String 1 Label	Country
Device Event Category	category
Device Event Class ID	event_source:signature_id
Device External ID	event_source
Device Facility	Alert
Device Inbound Interface	interface
Device Payload ID	flow_id
Device Product	Network Detection and Response
Device Receipt Time	Start
Device Severity	Severity or event_type

Configuration Guide for OpenText Network Detection & Response (Bricata) SmartConnector
Device Event Mapping to ArcSight Fields

ArcSight ESM Field	Device-Specific Field
Device Vendor	OpenText
End Time	Last
External ID	signature_id
Message	signature
Name	signature
Old File ID	event_uuid
Source Address	src_ip
Source Host Name	sensor_hostname
Source Nt Domain	sensor_fqdn
Source Port	src_port
Start Time	Start
Transport Protocol	Proto

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 OpenText Network Detection & Response (Bricata 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: 8.4.3

Performance Tuning Guide for SmartConnectors

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

Performance Tuning Guide for SmartConnectors	4
Overview	4
Tuning SmartConnectors	5
How Much to Tune?	6
Reading SmartConnector Logs	6
Improving Memory Utilization	6
Improving Disk Space Utilization and Network Usage	7
Improving Disk Space Utilization or Caching	7
Improving CPU Usage	7
Improving Network Usage	8
Tuning Performance of Syslog SmartConnectors	8
Configuration Parameters	9
Architecture Overview	10
Tuning Transformation Hub Parameters	12
Performance Statistics for Syslog SmartConnectors	13
Performance Results Using Transformation Hub as a Destination	14
Tuning Performance of Windows Event Log - Native SmartConnectors	14
Windows Event Log - Native SmartConnector Parameters	15
Performance Statistics for Windows Event Log - Native SmartConnectors	15
Send Documentation Feedback	18

Performance Tuning Guide for SmartConnectors

This Performance Tuning document provides sizing and tuning recommendations to improve the performance and achieve optimal Events Per Second (EPS) results for ArcSight SmartConnector for Windows Event Log - Native and the Syslog 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](#).

Overview

Performance tuning requires an established performance baseline that can be used to compare if a performance issue arises. It is essential to collect data and analyze it effectively to identify and correct performance problems. Continuous monitoring of performance helps identify

possible symptoms and statistics, which can then be used to make configuration changes to correct performance issues.

This document addresses performance and stability issues that you have experienced with ArcSight SC 8.0.0.8322. A significant amount of code re-architecture was done for SmartConnector release 8.0.0.8322 to ensure that the connectors can achieve the maximum EPS.

The guidelines in this document are an attempt to simplify proactive monitoring and solve bottleneck scenarios.

The performance tuning guidance provided here is specific to Syslog and Windows Event Log - Native SmartConnectors. Most of the 200+ ArcSight SmartConnectors use the same connector framework, and any performance improvement changes might similarly impact other SmartConnectors.



Note: Performance tuning/monitoring needs careful study of possible scenarios, including input event size, input events per second, and connectors' hardware. Do not assume that updating parameters with higher numbers translates into better results.

Tuning SmartConnectors

The default configuration for each SmartConnector made in the agent.properties file might be sufficient for lower EPS. It might not utilize the full CPU capacity and might impede your hardware from achieving the best possible results. To reach higher EPS and optimal hardware utilization, you must tune parameters as per your requirement.

Ensure that the SmartConnector is tuned by an ArcSight administrator, who is aware of the types of events and the approximate EPS that the SmartConnector is expected to receive. The connector tuning also requires an understanding of SmartConnector logs. For more information, see "[Reading SmartConnector Logs](#)" on the next page.

You can tune the SmartConnector the first time after deployment, and any time after that if you see a drop in performance. You must monitor the input and the output EPS at regular intervals to see any drop in performance. The decrease in performance might be due to newer events coming to the connector or higher input EPS. Performance tuning is not required when input EPS for the connector is equal to output EPS..



Note: If you see a low input EPS while the number of events keep going up, the tuning exercise might not have been executed correctly. As a result, the event source throttles and makes it harder to debug. Hence, monitor the initial surge of EPS and wait to see a slow downward trend.

How Much to Tune?

Whenever you change the agent.properties file based on the tuning parameters, run multiple tests to ensure that you see sustained and desired EPS. While a small amount of data in cache is usually fine, ensure that you do not see any consistent build-up of data in cache or queue. Ensure that there are no errors in the logs.



Note: If you notice that the CPU utilization reaches 80% with a consistent cache or queue built-up, despite tuning parameters, then it might be an indicator that it is time to upgrade your hardware.

Reading SmartConnector Logs

When evaluating system performance, monitor the following parameter at peak event surges for approximately 20 to 30 minutes.

Parameter	Where to Find
Input EPS	Value of "Queue Rate(SLC)= " in agent.log
Queue Build-up	Browse to the <installation folder>/current/user/agent/agentdata/location, then count the number of files with suffix queue.syslogd
Cache	Value of "{C=" in agent.log
Output EPS	Value of "T=" in agent.log

For example, if the output EPS hovers around 21k (staying between 20k-22k) for 30 minutes, then the final output EPS can be considered as 21k.

Improving Memory Utilization

The minimum and maximum heap size in a connector are 1 GB, which allows more in-memory operations and faster execution. If there is more RAM available in the machine running the connector and you have high input EPS, OpenText recommends that you increase the heap size to 4 GB.

To increase the memory size in SmartConnectors running in stand-alone mode:

1. Open the following file:

Windows: ARCSIGHT_HOME\current\bin\scripts\connectors.bat

Linux: \$ARCSIGHT_HOME/current/bin/scripts/connectors.sh

2. Change the following parameter:

```
ARCSIGHT_MEMORY_OPTIONS=" -Xms1024m -Xmx1024m "
```

to

```
ARCSIGHT_MEMORY_OPTIONS=" -Xms4096m -Xmx4096m "
```

To increase the memory size SmartConnectors runing as a service:

1. Open the user/agent/agent.wrapper.conf file.

2. Change the following line:

```
wrapper.java.initmemory=1024 wrapper.java.maxmemory=1024
```

to

```
wrapper.java.initmemory=4096 wrapper.java.maxmemory=4096
```

Improving Disk Space Utilization and Network Usage

This section has the following information:

Improving Disk Space Utilization or Caching

Connectors use the disk to store cache and queue files. Disk space utilization is based on the number of cache and queue files and their respective sizes. The cache and queue files are created when the connector's various subsystems cannot process as fast as expected. For example, if the parsing is slow, queue files are saved in <installation folder>/current/user/agent/agentdata/.

If the destination cannot receive events at the rate the connector sends events, cache files build up. When the connector cannot send events to a destination, cache files are clustered in queue files. These queue files generate a cascading effect backwards.



Note: If the queue files or cache files reach their space limit, the newer events are dropped.

To avoid events getting dropped:

- If you see only cache files, increase the number of destination threads. If you see cache files and queue files, increase the number of destination threads and check if both clear up.
- If you see only queue files, increase the number of parser threads.
- If you have sudden surges and traffic peaks, consider creating more queue files so that events are not dropped and cached for later processing.

Improving CPU Usage

If the input EPS is high and there are enough free CPU cycles on the machine running the connector, you can increase the number of parsers and destination threads to improve the CPU

usage.

However, adding more threads than required is not recommended.

Improving Network Usage

Communication from the source to the connector and from the connector to the destination (along with all the hubs such as any routers or switches) must remain at the same network capacity.

- If the input EPS is higher than 50K, your network card must be 1 GB.
- If the input EPS is higher than 100K, your network card must be 10 GB.

Tuning Performance of Syslog SmartConnectors

You can improve the performance of SmartConnectors by implementing the following changes:

- Increasing the number of parser threads to improve parsing speed.
- Increasing heap memory to allow additional in-memory operations.
- Increasing destination write speed for CEF File, Transformation Hub and AWS s3 bucket to allow multiple parallel streams of write to the destination.

Syslog SmartConnectors can be configured with Logger, ESM, Transformation Hub, and files as single or multiple destinations.

Certain factors, such as configuring multiple destinations and the output EPS, might affect the performance of your SmartConnectors.

For example, with CEF files as a destination, the only limiting factor is disk speed. While with Logger as a destination, network latency and Logger hardware or performance affect the connector performance.

Enabling Transport Layer Security (TLS) decreases the throughput, though not significantly.

Configuration Parameters

Parameter	Description
Persistent Connection	<p>Set <code>transport.loggersecure.connection.persistent</code> to True when using Logger as destination.</p> <p>It allows reuse of the existing HTTPS connections and not tear them down for every batch of events.</p>
Custom SubAgent List	<p>If you are aware of the types of events received by the connector, you can set <code>agents[0].usecustomsubagentlist</code> to True, and specify in the <code>agents[0].customsubagentlist</code> parameter, comma-separated values.</p> <p>For example: example linux_audited_syslog, generic_syslog.</p>
Parser threads	Increase the number of parser threads for better performance if the input EPS is high.
Destination Threads	<p>If a queue is getting built up:</p> <ul style="list-style-type: none"> CEF - <code>transport.ceffile.threads</code> Logger - <code>transport.loggersecure.threads</code>
Number of Kafka Threads	<p>Set the <code>producerstransport.cefkafka.multiplekafka</code> parameter to True to use as many threads as possible as <code>transport.cefkafka.threads</code>.</p> <p>If the parameter is set to false, even if the number of destination threads is set to a higher number, the condition is not overruled.</p>
Time/size of buffers before events are sent to TH	<p><code>transport.cefkafka.buffer.bytes</code> and <code>transport.cefkafka.linger.ms</code>.</p> <p>The kafka threads wait for either the bytes to be full or the linger.ms to be completed before pushing events to the TH.</p>

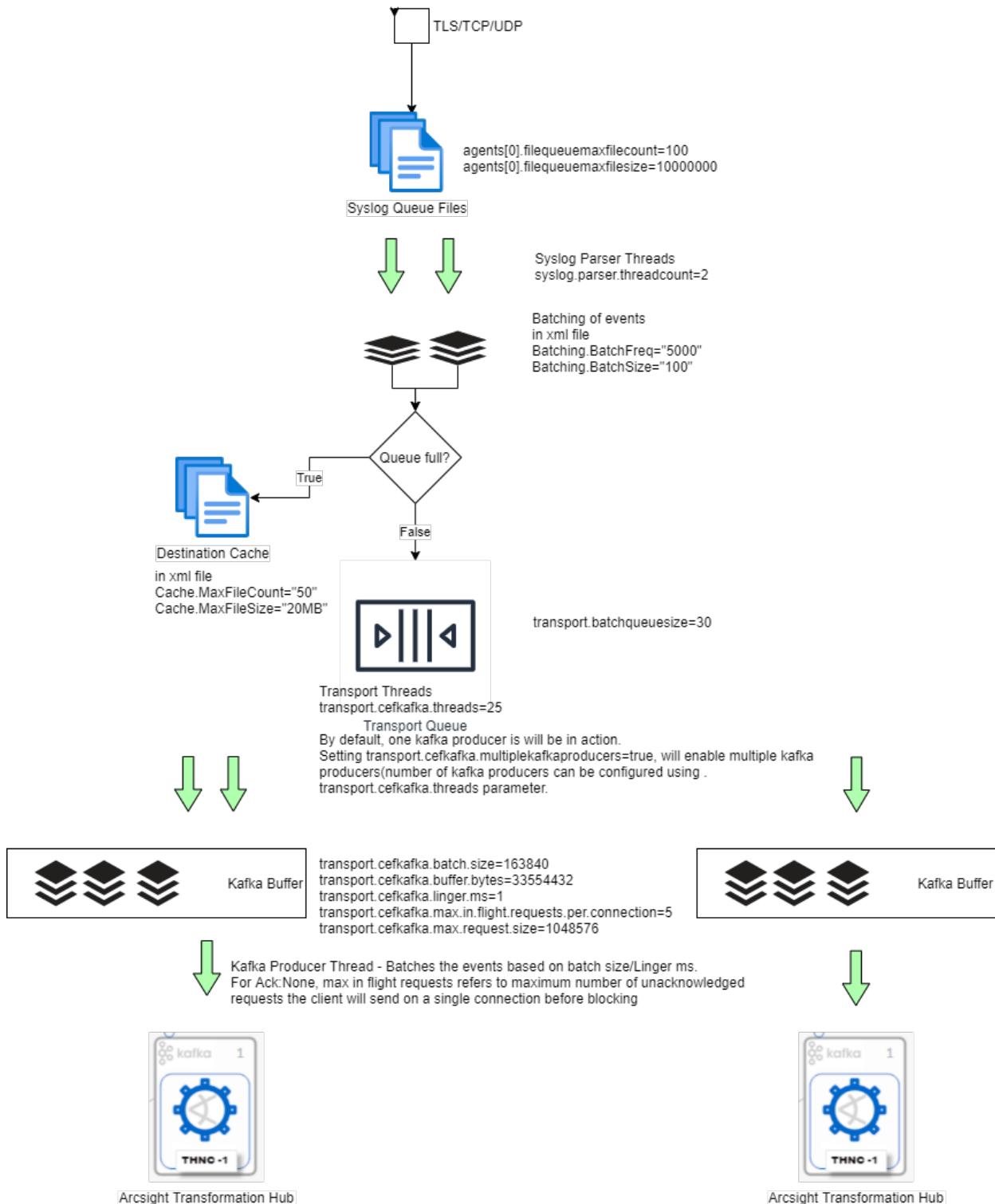
Syslog SmartConnector Parameters

Parameter	Description	Value
<code>agents[0].filequeueumaxfilecount</code>	<p>Sets the maximum number of queues.</p> <p>Incoming events received by the Syslog connector are saved in queue files.</p> <p>Ensure enough storage available in the disk. If Ad hoc EPS inputs are expected, increase this value to avoid event drops.</p>	100
<code>agents[0].filequeueumaxfilesize</code>	Maximum file size of a queue file (in bytes)	100
<code>Parsing: syslog.parser.threadcount</code>	Number of threads to process input raw events. (Syslog Parser Threads) Batching of Events in the XML File .	2

Parameter	Description	Value
Batching.BatchFreq	Batching frequency before sending events to a transport queue (in milliseconds)	5000
Batching.BatchSize	Number of events per batch before sending them to a transport queue	100
transport.batchqueuesize	Maximum queue size of batched events on hold. Syslog parser threads push processed events to this queue, and transport threads take the event batches to be sent to the destination.	30
Cache.MaxFileCount	Maximum number of cache files. If the destination is down or if there is event transfer latency, events are cached in the current/user/agent/agentdata folder.	50
Cache.MaxValueSize	Maximum size of a cache file	20 MB

Architecture Overview

The following diagram shows the architecture of Syslog SmartConnector that has Transformation Hub as a destination. The diagram also indicates parameters and values that can be set. However, you can tweak these values as per your requirements. For example, you can increase the thread count if you notice that the number of queue files increases. For more information about the parameters used in the diagram, see [Syslog SmartConnector Parameters](#).



Tuning Transformation Hub Parameters

Parameter	Description	Value
transport.cef kafka.threads	Maximum threads that can be processed by the transport.batchqueue and sent to the destination.	25
transport.cef kafka.batch.size	The Kafka producer attempts to batch records together into fewer requests whenever multiple records are sent to the same partition. Performance improves for both client and server.	163840
transport.cef kafka.buffer.bytes	Controls the default batch size in bytes	33554432
transport.cef kafka.linger.ms	The producer groups records that arrive in between request transmissions into a single batch request.	1
transport.cef kafka.max.in.flight.requests.per.connection	The maximum number of unacknowledged requests a client sends on a single connection before blocking the operation.	5
transport.cef kafka.max.request.size	The maximum size of a request in bytes. Limits the number of record batches the producer sends in a single request to avoid sending multiple and heavier requests.	1048576
transport.cef kafka.multiplekafkaproducers	The maximum number of cache files. Creates different kafka producer for each transport.cef kafka.threads, The multiplekafkaproducers must be set to true.	False

Performance Statistics for Syslog SmartConnectors

Performance tuning and measurement must be done based on the requirement of the user's environment.

The performance results in the following sections are achieved in the OpenText Lab settings. These numbers must be used as guidance. OpenText strongly recommends that you run the test in your setup.

Performance Results Using a CEF File as a Destination

Configurable Section	Description
Hardware Configuration	Connector: G 10 Appliance: ProLiant DL360 G10, RAM: 64 GB CPU: 32, 16 cores
Heap size	Initial Java Heap Size (in MB) = 1024 Maximum Java Heap Size (in MB) = 2048
Destination	CEF
Duration	10 Mins
Connector used	Syslog Deamon
Log file	Unix_OS_Events.txt
Agent.properties	transport.ceffile.connection.persistent=True agents[0].usecustomsubagentlist=True agents[0].customsubagentlist=generic_syslog

EPS	Parser Threads	Destination Threads
10k	5	5
20k	5	5
30k	10	10
40k	10	10
50k	10	10
60k	10	10
70	10	10
80k	10	10

EPS	Parser Threads	Destination Threads
90	15	15
100k	15	15
110k	151	15

Performance Results Using Transformation Hub as a Destination

Transformation Hub Leader ACK Performance Improvements:

Configurable Section	Description
Hardware Configuration	Connector:G10 Appliance (ProLiant DL360 G10) RAM (64 GB) CPU (32) ,16 cores
Heap size	Initial Java Heap Size = 4 GB Maximum Java Heap Size = 4 GB
Destination	Transformation Hub
Duration	10 mins
Connector used	Syslog Deamon
Log file	Cisco Merraki

Results

100.04k	None	99.95k
99.32k	Leader	99.36k
100.09k	All	99.99k

Tuning Performance of Windows Event Log - Native SmartConnectors

Windows Event Log - Native agent process has the following separate queues:

- **Processing queue:** It stores unprocessed events from Windows event logs.
- **Batching queue:** It stores the processed events that are ready to be batched.
- **Sending queue:** It stores event batches that are ready to be sent to the Windows Event Log - Native connector process.

A pool of threads monitors the processing queue for events, processes them, and puts them to the batching line.

Windows Event Log - Native SmartConnector Parameters

Parameter	Description
Queue parameters	<p>Parameters related to Queue.</p> <p><code>agents[0].filequeueumaxfilecount</code>: Maximum number of queue files to store the raw events. Default value is 100. If the queue is getting filled increase this value to have more number of queue files to avoid any event drop.</p> <p><code>agents[0].filequeueumaxfilesize</code>: Maximum size of each queue file. Default value is 10MB. If the queue is getting filled increase the size of queue file to store more events.</p>
Winc agent parameters	<p>Modify these parameters to send more events to the connector.</p> <p><code>winc.winc-agent.eventBatchSize</code>: The default number is 64.</p> <p><code>winc.winc-agent.processingThreadPoolSize</code>: The default size is 5.</p> <p><code>winc.winc-agent.senderThreadPoolSize</code>: The default size is 2.</p>
Eventprocessing threadcount	<p><code>syslog.parser.threadcount</code>:</p> <p>Event processing thread count for high input EPS. The default count is 2.</p> <p>If the queue file is built up in the <code>user\agent\agentdata</code> folder, then increase the thread count.</p>
Destination Threads	<p>High cache</p> <p>CEF - <code>transport.ceffile.threads</code></p> <p><code>transport.ceffile.connection.persistent=TRUE</code></p> <p><code>transport.ceffile.threads</code></p>

Performance Statistics for Windows Event Log - Native SmartConnectors

Performance tuning and measurement must be done based on the requirement of the user's environment.

The Performance results in the following sections are achieved in the OpenText Lab settings. These numbers must be used as guidance. OpenText strongly recommends that you must run the test in your setup.

Performance Results Using Windows Event Log - Native SmartConnector 8.4

Details	Details
Connector Machine	<ul style="list-style-type: none"> • Gen 10 • 16 core / 64 GB • Windows Server 2022
Destination (CEF File)	<ul style="list-style-type: none"> • Gen 10 • 16 core / 64 GB • Windows Server 2022
Build	8.4.0.8949
Maximum log size in event viewer	10 GB
Log size(Mixed Events)	7 KB

agent.default.properties Values

Default	Custom
winc.winc-agent.eventBatchSize=64	winc.winc-agent.eventBatchSize=59
winc.winc-agent.processingThreadPoolSize=5	winc.winc-agent.processingThreadPoolSize=30
winc.winc-agent.senderThreadPoolSize=2	winc.winc-agent.senderThreadPoolSize=7

Heap Size

Default	Custom
1GB-1GB	1GB-8GB

agent.properties

Default	Custom
agents[0].eventprocessorthreadcount=20	agents[0].eventprocessorthreadcount=40

Event IDs Used to Execute Performance Tests:

Event ID	Event Description
4634	An account was logged off
4624	An account was successfully logged on.
4672	Special privileges assigned to new logon.
4768	A Kerberos authentication ticket (TGT) was requested.
4769	A Kerberos service ticket was requested.

Default Values

Input EPS (Connector)	EPS Processed by Connector	EPS Sent to Destination	Thread	Cache	System CPU (%)	System RAM Usage (Mb)	Queue File Count
17k	17k	17k	2	0	32.9	7.5	1
21k	21k	21k	2	0	38.3	7.7	1
25k	25k	25k	2	0	44.6	7.8	1
32k	24k	24k	2	0	51.9	8.2	84

Queue File Count is the number of files containing windows events to be processed.

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 Performance Tuning Guide for SmartConnectors (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

Developer's Guide for ArcSight FlexConnector for REST

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.

Contents

Chapter 1: ArcSight FlexConnector for REST	5
REST FlexConnector Overview	6
Before You Begin	6
Basic Authentication	6
OAuth2 Authentication	7
REST API Endpoints	7
JSON Parsers	8
Prerequisites	8
Next Steps	8
Chapter 2: Developing the FlexConnector	9
Registering Your Connector Application	9
Salesforce OAuth2 Registration and Values	9
Google Apps OAuth2 Registration and Values	10
Creating OAuth2 Client Properties File	11
Configuring the Required Time Zone	13
Determining the Events URL to Use	13
General Information about REST API Endpoints	13
Salesforce REST APIs	15
Google Apps REST API	15
Run restutil to Obtain a Refresh Token for ArcSight Management Center	16
Create a JSON Parser File	17
Example JSON Structure	17
Example JSON Parser	18
trigger.node.location	19
Token Properties	19
Event Mappings	20
Viewing the Raw JSON Data	20
Next Steps	21
Chapter 3: Installing and Configuring the REST FlexConnector	22
Preparing to Install the FlexConnector	22
Installing Core Software	22
Adding JSON Parser	23

Setting Global Parameters (Optional)	23
Configuring Connector Parameters	24
Selecting a Destination and Completing Installation	28
Modifying Parameters to Optimize Connector Performance	29
Running the SmartConnector	31
Enabling SNI Manually	31
 Troubleshooting	32
Certificate Issue While Integrating the Flexconnector with Azure Sentinel Alerts.	32
Salesforce API is Unable to Receive Events	33
 Appendix A: About the REST FlexConnector Configuration Tool (restutil)	34
restutil Configuration Tool Syntax	34
Invoking the restutil Configuration Tool	35
Retrieving an Access Token	35
Retrieving Values from the Server	35
Retrieving Values Using an Authorized GET Command	36
 Send Documentation Feedback	38

Chapter 1: ArcSight FlexConnector for REST

The SmartConnectors provides a configurable method to collect security events from cloud-based applications such as Salesforce, Google Apps, and so on.

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](#).

REST FlexConnector Overview

The connector framework lets you develop FlexConnectors to collect events by configuring:

- OAuth2 for authentication with the vendor. See "[OAuth2 Authentication](#)" on the next page.
- Basic authentication. See "[Basic Authentication](#)" below.
- REST API endpoints exposed by the vendor for event collection. See "[REST API Endpoints](#)" on the next page.
- JSON parsers for parsing and mapping data (retrieved from the REST APIs). See "[JSON Parsers](#)" on page 8.

Before You Begin

Before beginning to develop your FlexConnector:

1. To fit the profile for the REST FlexConnector technology, make sure the vendor supports:
 - Basic or OAuth2 Authentication
 - REST API endpoints
 - JSON data format
2. Decide what kind of data you want to collect and determine the REST API endpoint for that data. Consult vendor documentation to determine data availability.

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.

Basic Authentication

You can configure your connector to use the Basic authentication method to obtain permission to collect events from the cloud application. In this case, the client provides an identifier and a shared secret (such as a user name and a password). Basic authentication is defined by [RFC 2617](#). If the vendor's website uses HTTPS as the protocol, then all communication will be secure and encrypted.

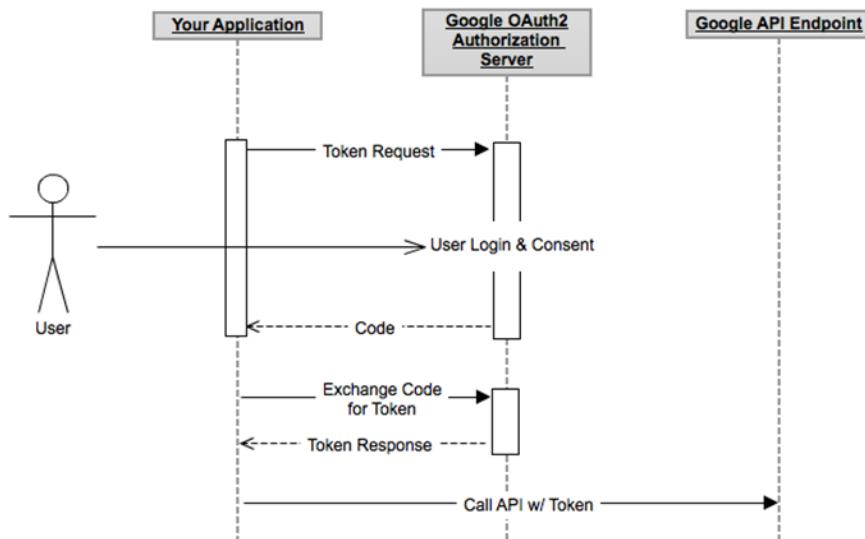
OAuth2 Authentication

You can configure your connector to use OAuth2 authentication to get permission for the connector to collect events from cloud applications. See "["Registering Your Connector Application"](#) on page 9 for details.

OAuth2 authentication ensures that the connector does not store a user's login credentials (user name and password) for a cloud vendor application.

The connector redirects the user to the vendor's login page. When the user logs in and gives the permission to the connector, the vendor provides tokens to the connector to use to make API calls.

The following figure is an example of this authentication:



REST API Endpoints

Security events can be retrieved from the vendor's predefined endpoints through HTTP requests. The REST FlexConnector supports data collection from cloud vendors where the retrieval of security events is exposed through REST-based APIs. Although events collected through REST APIs can be in XML or JSON formats, the REST FlexConnector supports only the JSON format. See "["Determining the Events URL to Use"](#) on page 13 for details.

For example, a REST API endpoint can look like this:

`https://abc.com/events?created_after=<>&maxEvents=<>...`

For the REST FlexConnector, the default query interval for the REST APIs is 30 seconds. This interval can be adjusted. See "[Modifying Parameters to Optimize Connector Performance](#)" on page 29.

JSON Parsers

The REST FlexConnector requires a JSON parser file. Most cloud vendors send data in JSON format. JSON supports these data types: arrays, objects, string, number, Boolean, or null. See "[Create a JSON Parser File](#)" on page 17 for details.

Prerequisites

- An Internet connection is required.
- Proxy information that might be required for the HTTP/HTTPS connection.
- Information required for OAuth2 authentication. See "[Creating OAuth2 Client Properties File](#)" on page 11 for details.
- The events URL, which is used as an endpoint for retrieving the events from the vendor. See "[Determining the Events URL to Use](#)" on page 13 for details.

Next Steps

Follow the steps in "[Developing the FlexConnector](#)" on page 9 to prepare for the install and configuration of the REST FlexConnector. After that, see "[Installing and Configuring the REST FlexConnector](#)" on page 22 to run the Configuration Wizard to install and configure the connector.

Chapter 2: Developing the FlexConnector

To develop a REST FlexConnector, perform the tasks described in this chapter, and then run the connector Configuration Wizard (described in ["Preparing to Install the FlexConnector" on page 22](#)). See ["Before You Begin" on page 6](#) before starting your configuration tasks.

Registering Your Connector Application

For OAuth2 authentication, contact the vendor and register the connector application. When you register, the vendor will supply values for creating a vendor-specific OAuth2 Client Properties file. The content and format of the OAuth2 Client Properties file are discussed in ["Creating OAuth2 Client Properties File" on page 11](#).



Note: You must also supply the vendor with a redirect_uri value. The redirect_uri must be registered with the vendor before you attempt to configure the connector or the authentication will fail.

For Basic authentication, contact the vendor to obtain a user name and password along with the events URL.

The following sections provide details on registering a connector application with the vendors using OAuth2 authentication. The instructions do not apply to vendors using Basic authentication. You can register with vendors other than Salesforce and Google Apps, but the auth_url, token_url, and scope values must be obtained from the vendor's documentation. The values for Salesforce and Google Apps are supplied in the following sections.

Salesforce OAuth2 Registration and Values

To register your Salesforce connector application:

1. Follow this link to register the application: <https://salesforce.com>.
2. Login to Salesforce and go to **App Setup > Create > Apps > New**.
3. Specify a name.
4. Set the **CallbackURL** (redirect_uri) as `https://localhost:<port>/<path>`
5. Select **Scope > Full Access**.
6. After the application is created, write down the **Consumer Key** (client_id) and **Consumer Secret** (client_secret) as these will be needed later during connector configuration.

For details, see the [Salesforce developer's documentation](#).

Salesforce OAuth2 values

After you register, create a Salesforce vendor-specific OAuth2 Client Properties file using these values (follow the steps for file creation described in "[Creating OAuth2 Client Properties File](#)" on the next page):

- client_id=<your client id>
- client_secret=<your client secret>
- auth_url=https://login.salesforce.com/services/oauth2/authorize
- token_url=https://login.salesforce.com/services/oauth2/token
- redirect_uri=https://localhost:<port>/<path>



Note: Verify with the vendor that the URLs provided above are correct. These may change, so be sure to have the most current URLs from the vendor.

Google Apps OAuth2 Registration and Values

To register your Google Apps connector application:

1. Register the application by using the following link: <https://code.google.com/apis/console/>
2. Click **Create A Project**.
3. Click **Services > Enable Audit API**.
4. Accept the license terms.
5. Click **API Access > Create an OAuth2 Client ID**.
6. Choose **Web Application**.
7. Enter the redirect_uri as https://localhost:<port>/<path>.
8. Write down the client_id and client_secret as these will be needed later during connector configuration.

For details, see the [Google Apps developer's documentation](#).

Google Apps OAuth2 values

After you register, create a Google Apps vendor-specific OAuth2 Client Properties file using these values (follow the steps for file creation described in "[Creating OAuth2 Client Properties File](#)" on the next page):

- client_id=<your client id>
- client_secret=<your client secret>
- auth_url=https://accounts.google.com/o/oauth2/auth
- token_url=https://accounts.google.com/o/oauth2/token
- redirect_uri=https://localhost:<port>/<path>

- scope=https://apps-apis.google.com/a/feeds/policies/
https://www.googleapis.com/auth/apps/reporting/audit.readonly



Note: Verify with the vendor that the URLs provided above are correct. These may change, so be sure to have the most current URLs from the vendor.

Creating OAuth2 Client Properties File

When using OAuth2 authentication, create an OAuth2 Client Properties file for each vendor from which you want to collect events. You can name the file to contain the vendor's name to help you keep track of your properties files. For example, an OAuth2 Client Properties file for the vendor Google could be named googleclient.properties. The file can reside on your local drive. You later browse for this file to add it to the "Enter parameter details" window in the connector Configuration Wizard.

This is the template for the OAuth2 Client Properties file:



Note:

- The OAuth2 Client Properties file must begin with a blank line or a comment statement.
- The order of the properties is important. For example, if you place auth_url before client id, then connector will respond with an error.

```
# comment statement
client_id=<your client id>
client_secret=<your client secret>
redirect_uri=https://localhost:<port-number>/<path>
auth_url=<available from cloud service provider>
token_url=<available from cloud service provider>
scope=<value, if any>
```

```
timestamp_format_of_api_vendor=<null or <default> or timestamp format vendor support
for API>
```



Note: If you want to retrieve events from Salesforce or Google Apps, see "[Salesforce OAuth2 values](#)" on page 9 or "[Google Apps OAuth2 values](#)" on the previous page for details on the values to use in vendor-specific OAuth2 Client Properties files.

The parameters and expected values in the OAuth2 Client Properties file are described in the following table:

Parameter	Description
client_id	This value is provided by the vendor when you register an application.
client_secret	This value is also provided by the vendor when you register an application. This value is obfuscated. The values client_id and client_secret helps the vendor identify an application.
redirect_uri	You configure this when you register an application. This is the URL to which the vendor sends the authorization code. For the REST Flex Connector, the redirect_uri must be on the local host. Both http and https schemes are supported. This URL should be of the form https://localhost:<port>/<path>. Examples: <code>http://localhost:8081/oauth2callback</code> <code>https://localhost:8081/oauth2callback</code> The <port> in this URL can be configured to any available port. Specify this URL when you register the application with the vendor. The connector allows either http or https, and the URL must be redirected to the unused port, <port> of local host <localhost> so that the authorization code can be captured automatically after vendor authentication. For an HTTPS connection, it shares the connector's default self-signed certificate, remote-management.p12 located in the user/agent directory.
auth_url	This is the URL of the vendor to which the initial request must be made to get an authorization code. Consult the vendor documentation to get this URL.
token_url	This is the URL of the vendor to which the request for an Access Token will be made. Consult the vendor documentation to get this URL.
scope	Required. Specifying a value for the scope parameter is optional, but the parameter itself is not and must appear in your configuration. The scope parameter allows applications to inform you and the vendor what type of information is to be retrieved from the vendor on behalf of the user. If there is more than one scope, you can specify these as a space-separated list of values. Note: Scope parameter field must be replaced with Resource For Windows ATP device (Microsoft 365 Defender connector). For Graph API, the resource value must be, Resource: https://graph.microsoft.com For Security API, the resource value must be, Resource: https://api.security.microsoft.com
timestamp_format_of_api_vendor	Required. Time format can be null or "default". The time is taken as millisecond. Ex: 1558502432847. It can also directly transmit the time format that the provider supports for the API. Example: <code>timestamp_format_of_api_vendor =yyyy-MM-dd'T'HH:mm:ss.SSS'Z'</code> <code>timestamp_format_of_api_vendor =</code> To see timestamp formats, see https://help.sumologic.com/03Send-Data/Sources/04Reference-Information-for-Sources/Timestamps%2C-Time-Zones%2C-Time-Ranges%2C-and-Date-Formats

**Note:**

- The access token is initially obtained during the connector configuration and will be used during event retrieval while the connector is running. Because OAuth2 gives an application temporary access permission, the access token will expire after a period of time and must be refreshed.
- After successful authentication, all the OAuth2 Client Properties, as well as access token and refresh token are persisted in the agent.properties file. Tokens and secrets are obfuscated.

Configuring the Required Time Zone

The user is required to configure the time zone in agent.properties. The default value for the **vendor_timezone** is **GMT**.

So, the Connector uses the **GMT** time zone by default to fetch the events from the vendor. If the user wants to change the time zone to the target location from which the events need to be fetched, then the required time zone needs to be configured.

Note: This property will be used when the server in which the connector is installed is in a one-time zone and the server from which events need to be fetched is in a different time zone.

Determining the Events URL to Use

For both Basic and OAuth2 authentication types, the events URL is the REST API endpoint used by the connector to get events from a vendor. A general discussion of REST endpoints, and details on using REST endpoints from Salesforce and Google Apps, follows.

Refer to the vendor documentation to determine which REST URL will provide the events you want. Also, be sure that the user who configures the connector has the privileges to access that URL. If you need a different events URL from those vendors, or from a vendor other than those mentioned, see "[About the REST FlexConnector Configuration Tool \(restutil\)](#)" on page 34.

General Information about REST API Endpoints

An events URL has query parameters in the path so that the user or the application can pass the value to retrieve the events that meet the specified condition.

- **Querying Based On TimeStamp:** Event retrieval can be limited by passing the start time. An example of an events URL:

`https://abc.com/events?start_time=<time>`

The connector relies on a timestamp query parameter for the start time (in the above example, it is `start_time`). To identify such a timestamp query parameter in the events URL, the connector expects to see a `$START_AT_TIME` after the `start_time` parameter. So, the full events URL in this example is:

```
https://abc.com/events?start_time=$START_AT_TIME
```

A tag and a start timestamp parameter are needed to collect the latest events and prevent duplicate events.

In addition to specifying the place holder `$START_AT_TIME`, you also must correctly map the `event.deviceReceiptTime` in the parser to the time at which the event happened (as reported by the device).

- **Rate Limiting:** REST API endpoints can also support querying for a maximum number of events. Google, for example, has the query parameter `limit` to use for this purpose. An example of a REST API is:

```
https://api.google.com/2.0/events?stream_type=admin_logs&created_after=$START_AT_TIME&limit=500
```

In the above example, a maximum of 500 events is requested from Google. If there are more than 500 events, then Google expects further API calls to retrieve the remaining events. Some vendors (such as Google Apps and Salesforce) provide **Next URLs** in the JSON response to let clients retrieve the remaining events. The connector supports this by making requests to the **Next URLs**. For further details, see ["Create a JSON Parser File" on page 17](#). Other vendors do not provide such URLs and the client will have to query more times to get the latest events.

There can be any number of other query parameters in a REST endpoint. All of them can be provided in the events URL. For example, an API could look like this:

```
https://abc.com/events?start_time=$START_AT_TIME&max=100&param1=PARAM1&param2=PARAM2&param3=PARAM3...
```

Some vendors may have dynamic content in their URLs. For example, Google Apps Events URL should have a `CustomerID` (that is dependent on the user who logged in) and, therefore, is not static. The connector expects the URL to be static. To obtain the dynamic content of a URL, refer to the vendor documentation and execute the REST Flex Configuration Tool to get the relevant content. Once you ensure that you have the entire URL that the connector can execute, you can run the connector.

The following subsections discuss three well-known vendors (Salesforce and Google Apps) and how to use their event URLs.



Note: If the APIs discussed in the following sections could be changed by the vendor, refer to the vendor's documentation for the correct APIs.

Salesforce REST APIs

Salesforce exposes many public APIs. All these APIs can support Salesforce Query Language (SOQL) queries. For example, an API to retrieve Login History data from Salesforce is:

```
https://<INSTANCE>.salesforce.com/services/data/v23.0/query/?q=SELECT  
LoginTime,LoginType,UserId,Status,SourceIp,LoginUrl From LoginHistory WHERE  
LoginTime>$START_AT_TIME
```

In the above URL, <INSTANCE> is the instance name, which differs for different users. You can find your <INSTANCE> by logging into Salesforce. After you log in successfully, you will see your Home Page on Salesforce. The URL of this page can appear like this:

```
https://na14.salesforce.com/<value>/<value>/...
```

In this case, the <INSTANCE> value is na14. Once you find your instance name, replace <INSTANCE> in the events URL so that the final URL for example, is:

```
https://na14.salesforce.com/services/data/v23.0/query/?q=SELECT  
LoginTime,LoginType,UserId,Status,SourceIp,LoginUrl From LoginHistory WHERE  
LoginTime>$START_AT_TIME
```

To use this URL, copy-and-paste it into the Events URL field in the **Enter the parameter details** window in the connector Configuration Wizard. After completion of the connector installation process, the agents.eventsurl= value can be modified in the \$ARCSIGHT_HOME\current\user\agent\agent.properties file.

The query part in the above example is:

```
SELECT LoginTime,LoginType,UserId,Status,SourceIp,LoginUrl From LoginHistory  
WHERE LoginTime>$START_AT_TIME
```

The \$START_AT_TIME is used by the connector to identify the timestamp parameter. In the example above, the timestamp parameter is LoginTime. You can specify any other valid SOQL query as part of the events URL. The following is a general SOQL example:

```
SELECT A, B, C FROM D WHERE B > $START_AT_TIME
```

In this second example, B should be the timestamp parameter.

For further details, see the [Salesforce REST API Developer's Guide](#).

Google Apps REST API

Google Apps exposes an Admin Audit API that can be used to monitor a Google Apps account. This API is:

```
https://www.googleapis.com/apps/reporting/audit/v1/<CustomerID>/207535951991?ma  
xResults=50&startTime=$START_AT_TIME
```

The <CustomerID> portion of this URL depends on the Google Apps account to be monitored. Before you start the connector Configuration Wizard, get the <CustomerID>, replace the <CustomerID> parameter in the events URL shown above with the actual value, and paste it into the **Events URL** field in the **Enter the parameter details** window during connector configuration. After completion of the connector installation process, the agents.eventsurl= value can be modified in the \$ARCSIGHT_HOME\current\user\agent\agent.properties file.

To get the <CustomerID> value, use the REST FlexConnector Configuration Tool. See "[About the REST FlexConnector Configuration Tool \(restutil\)](#)" on page 34 for details.

Also, ensure that the Provisioning API is enabled on the Google Apps account you are about to monitor. To do this, login to the Google Apps account, go to and select **Control Panel > Domain Settings > User Settings > Enable Provisioning API**.

For more details, see the [Google Developer's Guide](#).

Run restutil to Obtain a Refresh Token for ArcSight Management Center

Before configuring the connector on the Connector Appliance/ArcSight Management Center, obtain a refresh token, which the connector will use to access the vendor's log data.

Use the REST FlexConnector Configuration Tool (restutil) to obtain a refresh token. See "[About the REST FlexConnector Configuration Tool \(restutil\)](#)".

1. Ensure the connector software is installed on a host machine that has access to a web browser. See "[Installing Core Software](#)" for more information.
2. After installing the connector core software, navigate to \$ARCSIGHT_HOME\current\bin.
3. To retrieve a refresh token, invoke the tool with the token command:

```
arcsight restutil token [-proxy <proxy-info>] -config <OAuth2 Client Properties File>
```

For example:

```
arcsight restutil token -proxy proxy.atlanta.mf.com:8080 -config c:\temp\google.properties
```

4. A web browser opens and prompts you to log into the vendor application. Enter your user name and password and click through to access the vendor application.
5. The refresh token string is displayed in the command line window. Copy this string into the **Refresh Token** field during connector configuration.

Create a JSON Parser File

A JSON parser file must be created prior to configuring the connector. The parser file name will be required during connector configuration.

At this time, you will provide only the prefix of the parser file name. For example, if you provide the configuration file name as “google”, the connector expects the file `google.jsonparser.properties` file in `$ArcSight_Home/user/agent/flexagent` directory. If the connector cannot load this file, the connector configuration does not succeed, and the connector will not be able to parse the JSON data. For more details about JSON, see <http://www.json.org/> and <http://en.wikipedia.org/wiki/JSON>.

Example JSON Structure

The following is an example of JSON structure for the REST FlexConnector to help you create your own JSON parser:

```
{
    "kind": "audit#activities",
    "items": [
        {
            "kind": "audit#activity",
            "id": {
                "time": "2013-01-25T00:49:29.123Z",
                "uniqQualifier": "-6297847723024543031",
                "applicationId": "207535951991",
                "customerId": "ABCD1234"
            },
            "actor": {
                "callerType": "USER",
                "email": "john@abc.com"
            },
            "ownerDomain": "abc.com",
            "ipAddress": "1.1.1.1",
            "events": [
                {
                    "eventType": "USER_SETTINGS",
                    "name": "CREATE_USER",
                    "parameters": [
                        ...
                    ]
                }
            ]
        }
    ]
}
```

```
{  
    "name": "USER_EMAIL",  
    "value": "doe@abc.com"  
}  
  
"additional" : {  
    "additional1" : "add"  
}  
]  
}  
]  
],  
  
"next":  
"https://www.googleapis.com/apps/reporting/audit/v1/ABCD1234/207535951991?maxResults=10&alt=json&continuationToken=A:1357594673492000:-6925963958411121628:207535951991:C02deea2k"  
}
```

Example JSON Parser

An example JSON parser for such a structure would be:

```
trigger.node.location=/items/events  
  
token.count=10  
  
    token[0].name=kind  
    token[0].type=String  
    token[0].location=/kind  
  
    token[1].name=kindOfItem  
    token[1].type=String  
    token[1].location=../../kind  
  
    token[2].name=additional  
    token[2].type=String  
    token[2].location=additional/additional1  
  
    token[3].name=time  
    token[3].type=String  
    token[3].location=../../id/time  
  
    token[4].name=nextUrl  
    token[4].type=String
```

```
token[4].location=/next  
...  
...  
...  
  
(End Of Token Definitions)  
  
event.deviceReceiptTime=__createOptionalTimeStampFromString  
(time,"yyyy-MM-ddTHH:mm:ss.SSSZ")  
event.externalId=uniqQualifier  
event.deviceCustomString6=nextUrl  
  
...  
...
```

The syntax of a JSON parser is similar to that of XML parser. The parser consists of trigger.node.location, token properties, and event mappings:

trigger.node.location

This is mandatory. It is used to specify the node or nodes in a JSON parser for which events are to be built. It can be the root (trigger.node.location = /) or any other node specified relative to the root (trigger.node.location=/items/events) in the JSON. If the node specified as the trigger.node.location is an array, an event is built for every element in the array. If the node is not an array, one event is built corresponding to the object specified in the trigger.node.location. If the trigger.node.location has arrays in its path, then the number of events generated is the product of the number of elements in all arrays in the path.

In "[Example JSON Parser](#)" on the previous page, since the trigger.node.location is /items/events and both items and events are arrays, the number of events generated = (Number of elements in items) * (Number of elements in events). If the location were items, the number of events generated would only be the number of elements in items.

Token Properties

- token.name—A name you give to the token. Use this name later when you assign the token to a event schema field.
- token.type—The data type of the token.
- token.location—The location of the token in the JSON. Specify the location of the token in one of these ways:

- Relative to the root. For example, `token[0]` in the example has the location `/kind` which has been specified relative to the root `/`
- Relative to the trigger node. For example, `token[1]` in the JSON parser example has the location `.../.../kind`, which has been specified relative to the trigger node. (Which in this example is every element of the events array).
- You can specify the `token.location` by going up or down from a trigger node. For example, in `.../.../kind`, by specifying the first `...`, you are going to the array `events` of which the trigger is an element. By specifying the second `...`, you are going to the array `items` of which the `events` is an element.
- You can also specify the `token.location` to a particular element of an array. For example, a `token.location` in the JSON parser example can be `parameters[1]`, if we want the token location to be the second element of the `parameters` array.
- The total number of tokens should match the `token.count`.
- The token concept is the same as in XML, Regex, Syslog parsers, except for the `token.location` concept.

Event Mappings

Event mappings are the same as for any parser type.

If you are using the `$START_AT_TIME` in the REST API Events URL, you should map the timestamp at which the event happened to `event.deviceReceiptTime`. See "[Determining the Events URL to Use](#)" on page 13 for details. In the JSON parser example, the token `time` is mapped in that way. Most of the timestamps reported on the Web are in ISO-8601 format. To parse such timestamps, you can use the parser operation:

`_createOptionalTimeStampFromString`, and specify the timestamp format as:
`YYYY-MM-DDThh:mm:ss.SSSX`.

If the REST API supports sending next URLs (`nextURLs`) in the JSON to support rate limiting, then map the next URL to `event.deviceCustomString6`, as in the example in "[Example JSON Parser](#)" on page 18.

If you want to use the **next URL** feature to enable caching, then map a field that is unique for every event to `event.externalID`.

Viewing the Raw JSON Data

There are two methods to view raw JSON data:

- See the vendor's documentation, which will contain the information on the JSON structures sent by the REST APIs.

- Enable debug on the connector to see the JSON data retrieved by the connector:

- Add these properties to the \$ARCSIGHT_
HOME\current\user\agent\agent.properties file:

```
log.global.debug=true  
log.channel.file.property.package.com.arcsight=0
```

- Save the agent.properties file.
- Restart the connector.
- Raw JSON data is then available in \$ARCSIGHT_HOME\current\logs\agent.log.

Next Steps

When you have completed the configuration steps described in the previous sections of this chapter, you are ready to run the connector Configuration Wizard. The Wizard lets the user install the REST FlexConnector, enter the configuration parameters, and authenticate with the vendor. See "["Installing and Configuring the REST FlexConnector" on page 22](#).

Chapter 3: Installing and Configuring the REST FlexConnector

This chapter describes the steps to install and configure the REST FlexConnector.

Preparing to Install the FlexConnector

Before you install the FlexConnector, make sure that the ArcSight products with which the connector will communicate have already been installed correctly (such as ArcSight ESM or ArcSight Logger). This configuration guide takes you through the installation process with ArcSight Manager (encrypted) as the destination.

For complete product information, read the Administrator's Guide as well as the Installation and Configuration guide for your ArcSight product.

Before installing the FlexConnector, be sure the following are available:

- 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.

Unless specified otherwise at the beginning of this guide, this connector can be installed on all ArcSight supported platforms; for the complete list, see the *SmartConnector Platform Support* document, available from the OpenText SSO and Protect 724 sites.



Note: On the Linux platform, if you are logged in as root and use Firefox, some versions of the browser can cause the browser launched by the connector during configuration not to open. If you see this issue, try configuring the connector as a non-root user. If you configure the connector as a non-root user, however, you cannot run the connector as a service.

Installing Core Software

1. Download the SmartConnector executable for your operating system from the OpenText SSO site. (FlexConnectors are a type of SmartConnector.)
2. Start the SmartConnector Installer by running the executable.

Follow the installation 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 connector core component software has completed, the following window is displayed.

Adding JSON Parser

1. Before configuring the connector, you must exit the wizard to make your JSON parser available to the connector. Click **Cancel** to exit the wizard.
2. Copy your JSON parser file into the `$ARCSIGHT_HOME\current\user\agent\flexagent` directory. See "[Create a JSON Parser File](#)" for details on creating the JSON parser file.
3. Execute `runagentsetup` from `$ARCSIGHT_HOME\current\bin` to return to the wizard. Continue with "[Setting Global Parameters \(Optional\)](#)" if you want to set FIPS mode, remote management, or preferred IP version. Otherwise, continue with "[Configuring Connector Parameters](#)".

Setting Global Parameters (Optional)

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:

Global Parameter	Setting
FIPS mode	Set to Enabled to enable FIPS compliant mode. To enable FIPS Suite B Mode, see the <i>SmartConnector User Guide</i> under "Modifying Connector Parameters" for instructions. Initially, this value is set to Disabled .
Remote Management	Set to Enabled to enable remote management from [[[Undefined variable _ARST_Variables.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.

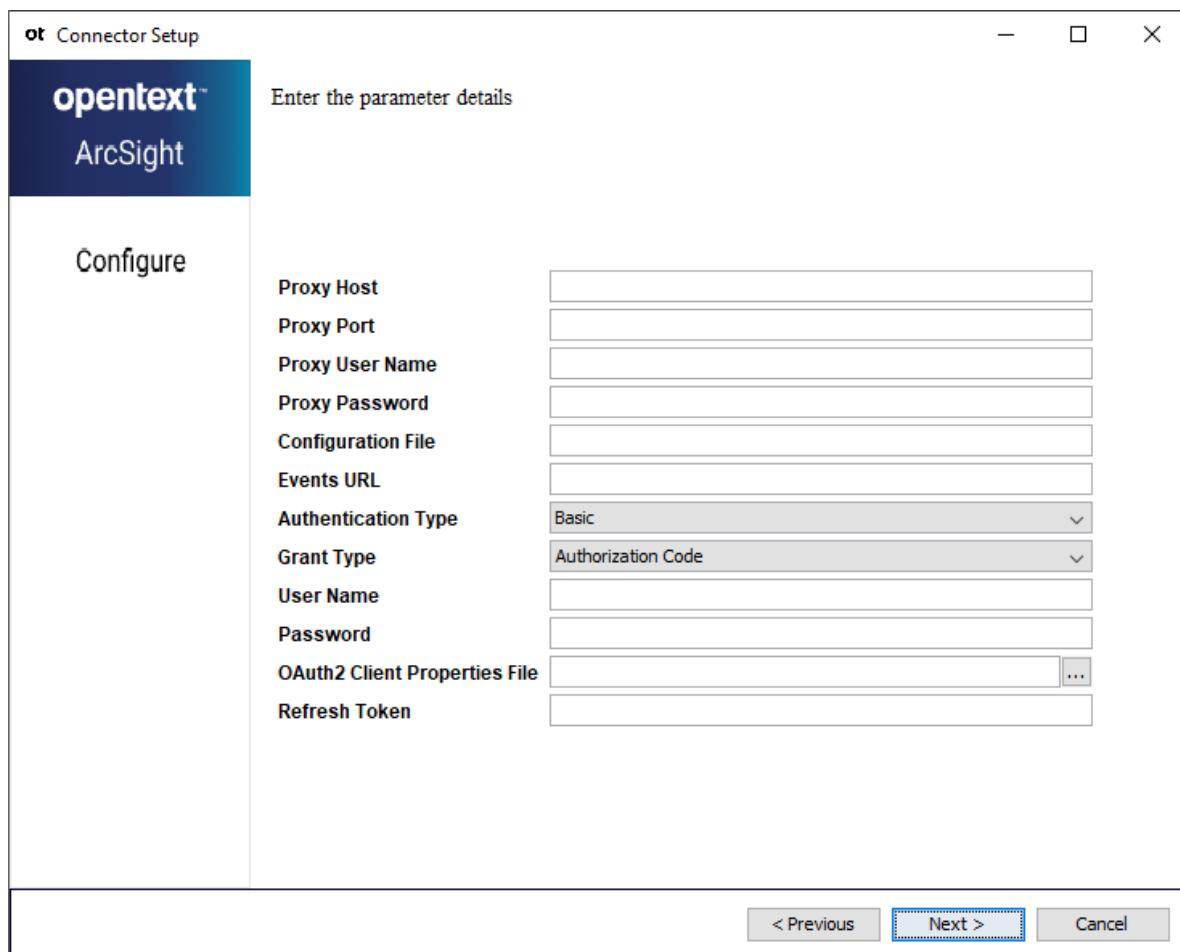
Global Parameter	Setting
Format Preserving Encryption	Data leaving the connector machine to a specified destination can be encrypted by selecting 'Enabled' to encrypt the fields identified in 'Event Fields to Encrypt' before forwarding events. If encryption is enabled, it cannot be disabled. Changing any of the encryption parameters again will require a fresh installation of the connector.
Format Preserving Host 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 authentication.
Event Fields to Encrypt	Recommended fields for encryption are listed; delete any fields you do not want encrypted from the list, and add any string or numeric fields you wish to be 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 the "Add a Connector" window. Continue the installation procedure with "Configure Connector Parameters".

Configuring Connector Parameters

To configure Connector Parameters

1. Select **Add a Connector** and click **Next**.
2. Select **ArcSight FlexConnector REST** and click **Next**.
3. Enter the required parameters to configure the connector, then click **Next**.



Note: If you do not use a proxy to access the Internet, leave the proxy fields blank and enter the other parameter values.

Parameter	Description
Proxy Host	Enter the proxy host IP address or name. This value is mandatory if you use a proxy to access the Internet.
Proxy Port	Enter the proxy port. This value is mandatory if you use a proxy to access the Internet.
Proxy User Name	Enter the proxy user name. This value is optional for additional proxy authentication. If you specify a proxy user name, you must also specify a proxy password.
Proxy Password	Enter the password for the proxy user specified in the Proxy User Name field. This value is optional for additional proxy authentication. This field is required only if you have specified a proxy user name.

Developer's Guide for ArcSight FlexConnector for REST
 Chapter 3: Installing and Configuring the REST FlexConnector

Parameter	Description												
Configuration File	<p>Enter the name of the parser file after the parser file is copied into the \$ARCSIGHT_HOME\current\user\agent\flexagent directory. For example, for \$ARCSIGHT_HOME\current\user\agent\flexagent\google.jsonparser.properties. You can enter the prefix google, and the connector assumes the file is named google.jsonparser.properties and resides in \$ARCSIGHT_HOME\current\user\agent\flexagent.</p> <p>For more information about creating parser, see "Create a JSON Parser File" on page 17.</p>												
Events URL	Enter the events URL. This is the REST API endpoint used by the connector to retrieve the events. See " Determining the Events URL to Use " on page 13 for general information about REST API endpoints, and specific information about the REST API endpoints for the vendors Salesforce and Google Apps.												
Authentication Type	Select Basic or OAuth2 as the type of authentication to be used.												
Grant Type	<p>Select one of the following grant types the connector must use to get Access Tokens:</p> <p>Authorization Code (default), Password, or Client Credentials</p> <p>Refer to the following table to specify the mandatory fields based on Authentication Type and Grant Type:</p> <table border="1"> <thead> <tr> <th>Authentication Type</th> <th>Grant Type</th> <th>Mandatory Fields</th> </tr> </thead> <tbody> <tr> <td>Basic</td> <td>The Grant Type field is not applicable for the Basic authentication type.</td> <td> <ul style="list-style-type: none"> • User Name • Password </td> </tr> <tr> <td>Oauth2</td> <td> Authorization code Password </td> <td> OAuth2 Client Properties File <ul style="list-style-type: none"> • User Name • Password • OAuth2 Client Properties File </td> </tr> <tr> <td></td> <td>Client Credentials</td> <td>OAuth2 Client Properties File</td> </tr> </tbody> </table>	Authentication Type	Grant Type	Mandatory Fields	Basic	The Grant Type field is not applicable for the Basic authentication type.	<ul style="list-style-type: none"> • User Name • Password 	Oauth2	Authorization code Password	OAuth2 Client Properties File <ul style="list-style-type: none"> • User Name • Password • OAuth2 Client Properties File 		Client Credentials	OAuth2 Client Properties File
Authentication Type	Grant Type	Mandatory Fields											
Basic	The Grant Type field is not applicable for the Basic authentication type.	<ul style="list-style-type: none"> • User Name • Password 											
Oauth2	Authorization code Password	OAuth2 Client Properties File <ul style="list-style-type: none"> • User Name • Password • OAuth2 Client Properties File 											
	Client Credentials	OAuth2 Client Properties File											
User Name	Enter the user name, if the authentication type is Basic or grant type is Password .												

Parameter	Description
Password	Enter the password for the user name, if the authentication type is Basic or grant type is Password .
OAuth2 Client Properties File	For OAuth2 authentication, browse and select the OAuth2 Client Properties File you created when you registered the connector, and acquired a redirect_uri. For information, see "Registering Your Connector Application" on page 9 and "Creating OAuth2 Client Properties File" on page 11 . Create a unique OAuth2 Client Properties File for each vendor from which you want to collect events.
Refresh Token	For OAuth2 only. Enter the refresh token. For information about how to produce the Refresh Token, see "Run restutil to Obtain a Refresh Token for ArcSight Management Center" on page 16 . (This applies only to users running the FlexConnector in the Connector Appliance or ArcSight Management Center environment. Other users, leave this field blank.)

4. This step is applicable when the authentication type is selected as **OAuth2** and the grant type is selected as **Authorization Code**. The connector launches a browser window to log in to the vendor application.

To log in to your vendor application, you must use only the browser window launched by the connector, and not any other browser window.

If there are multiple windows open for the vendor application in your browser, verify that you log in using the window that was opened by the connector wizard. Close other open browser windows that have been opened for the vendor application to ensure that you are logging in to the correct window.

To log in, enter your vendor application user name and password, and then click **Log In**. After logging in, another page could be displayed, asking you to give permission to your OAuth2 Client. This permission is required for the connector wizard to perform authentication. After you give the permission, if the redirect_uri is an https URL, you are redirected to a URL on the local host, and you view a page requesting that you trust the certificate provided by the connector running on the local host. You must trust this certificate. Note that this trust is not required if you specify a http URL for the redirect_uri.

When the connector launches a browser window, it attempts to use the default browser configured for your system. If the default browser does not launch, it will try to launch using other browsers (Firefox, Google Chrome, Internet Explorer, Konqueror, or Mozilla). Verify that you have one of these browsers configured on your system. Also, ensure that the proxy settings for your browsers are configured correctly so that you can access the Internet through your browser. The connector configuration wizard waits for 3 minutes for you to log in and grant permission.

If you do not log in after 3 minutes, a warning message is displayed indicating that the connector parameters did not pass a security verification. In such cases, you must:

a. **Refresh Token**

- i. Click **Yes** to continue with the installation without logging in. Note that when the connector starts retrieving events, the parameter **Refresh Token** must be modified and a login is required.
- ii. Or, you obtain the refresh token from the command line, and enter the Refresh Token. For more information, see "[Run restutil to Obtain a Refresh Token for ArcSight Management Center](#)" on page 16



Note: After obtaining the token refresh, the value can be changed from the agent.properties file. However, this is not recommended, as the refresh values are not encrypted.

b. **Modify the Refresh Token Parameter**

- i. Open command line %ARCSIGHT_HOME%/bin.
- ii. Run: `arcsight agentsetup -c`
 - A. Select **Modify Connector** and continue.
 - B. Choose **Modify connector parameters** and continue.
 - C. From the textbox, enter the Refresh Token obtained, for more information see "[Run restutil to Obtain a Refresh Token for ArcSight Management Center](#)" on page 16 .
 - D. Click **No** and continue.

A login request pops up to refresh token and the system automatically populates the textbox **Refresh Token**.

After you log into the vendor application, continue with the connector configuration. The next page is displayed automatically. To continue, to the ArcSight Connector Setup window that is available in the vendor application.

Selecting a Destination and Completing Installation

1. Make sure **ArcSight Manager (encrypted)** is selected and click **Next**. For information about this and other destinations listed, see the *ArcSight SmartConnector User Guide* and the Administrator's Guide for your ArcSight product.
2. Enter the **Manager Host Name**, **Manager Port**, and a valid ArcSight **User Name** and **Password**. This is the same user name and password you created during the ArcSight Manager installation. Click **Next**.
3. Enter a name for the connector and provide other information identifying the connector's use in your environment. Click **Next**; the connector starts the registration process.

4. The certificate import window for the ESM 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**, then the connector installation will end.
5. Review the Add Connector Summary and click **Next**. If the summary is incorrect, click **Previous** to make changes.
6. The wizard now prompts you to choose whether you want to run the connector as a stand-alone process or as a service. If you choose to run the connector as a stand-alone process, skip step 7. If you choose to run the connector as a service, the wizard prompts you to define service parameters.
7. 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**.
8. Click **Next**.

To complete the installation, choose **Exit** and click **Next**.



Note: Save any work on your computer or desktop and shut down any other running applications (including the ArcSight Console, if it is running), then shut down the system.

Complete any tasks needed in "[Modifying Parameters to Optimize Connector Performance](#)", then continue with the "[Running the SmartConnector](#)".

For connector upgrade or uninstall instructions, see the *SmartConnector User Guide*.

Modifying Parameters to Optimize Connector Performance

To optimize connector performance, you can modify parameter values to configure how frequently the connector retrieves events from the vendor. These parameters include `increasenexttimestampInMillis`, `maintaineventcache`, `queryfrequency`, `startattime`, `reauthenticate_onstartup`, `fetcheventsonstartup`, and `useexpirytimetorefreshtoken`, which are described in step 2.

After SmartConnector installation, access the connector's parameters as follows:

1. From the `$ARCSIGHT_HOME\current\user\agent` directory open the file `agent.properties` in a pure ASCII text editor (such as Notepad++).
2. In the `agent.properties` file, locate the parameters whose values you want to modify.

- The default value for the `increasenexttimestampinmillis` parameter is 1 millisecond. In most cases, you will not have to change this, since most providers support milliseconds in their timestamps. If your provider does not support milliseconds, you must change this parameter to a second (1000 milliseconds) to prevent duplicate events. When you make this change, the next time the connector makes an API call, it starts 1 second after the last timestamp.
- The default value for the `maintaineventcache` parameter is `false`. By default, no caching occurs. If you think you are getting duplicate events, you can enable caching by changing the value of `maintaineventcache` to `true`. Duplicates are suppressed based on the `event.externalId` (which is supposed to be unique) and `event.deviceReceiptTime`.
- The default value for the `queryfrequency` parameter is `30000 ms`; you can adjust this value to tune the connector performance. Note that `queryfrequency` influences the number of API calls the connector makes to the vendor. If vendor account has a limit for the number of API calls during a period of time, you can configure `queryfrequency` to reduce the number of API calls made by the connector. The greater the `queryfrequency` value, the fewer the number of API calls made by the connector over a period of time.
- Enter a value for the `startattime` parameter to specify an exact timestamp from which the connector is to start processing events.

The format of this timestamp should be `yyyy-MM-dd'T'HH:mm:ss.SSSZ` (Example: `2012-05-15T00:01:02.345-08:00`). If no time is specified, all events will be processed.

- The default value for `reauthenticate_onstartup` is `false`. When you change this value to `true`, the connector will attempt to reauthenticate the user each time the connector starts. It will launch the browser and expect the user to log in and give permission to the OAuth2 Client application.
- The default value for `fetcheventsonstartup` is `false`. When you change this value to `true`, the connector starts fetching events immediately after it starts, instead of waiting for the `queryfrequency` interval to fetch the events.
- The default value for `useexpirytimetorefreshtoken` is `true`. So, by default, the connector uses the expiry time of the access tokens (as sent by the vendor) to refresh the tokens, whenever needed. If the value is changed to `false`, the connector will ignore the expiry times sent by the vendor.

3. Save and exit the `agent.properties` file.

4. Restart the connector.

Running 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 *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.

Enabling SNI Manually

Server Name Indication (SNI) is a TLS extension, defined in RFC 4366. It enables TLS connections to virtual servers, in which multiple servers for different network names are hosted at a single underlying network address.

To enable SNI manually:

1. From

\$ARCSIGHT_HOME/current/bin/scripts/jvmcommonparams.bat (Windows)

or

\$ARCSIGHT_HOME/current/bin/scripts/jvmcommonparams.sh (Unix)

change the line

-Djsse.enableSNIExtension = false to -Djsse.enableSNIExtension = true.

2. If the connector is being run as a service, from

user/agent/agent.wrapper.conf change the line

-Djsse.enableSNIExtension=false to -Djsse.enableSNIExtension=true.

Troubleshooting

The following problems can affect connector authentication and connection to the vendor.

- Redirect to the vendor login page does not occur during connector configuration on Linux. Some browsers do not retain the proxy settings for certain users, which can prevent the redirect to the vendor login page. If this occurs, log in as a user other than **root** and start the connector.
- If the proxy is not configured properly, the connection between the connector and the vendor will fail. This will cause the authentication to fail during the connector configuration.
- If a network failure occurs during connector configuration, the authentication will fail. However, event retrieval attempts will be made if the network failure occurs while the connector is running.
- Any invalid values in the OAuth2 Client Properties file will cause the authentication to fail.
- On the expiration of the access token (typically in an hour), the connector will automatically refresh the token using the refresh token sent by the vendor and continue event retrieval. However, if the refresh token expires, the access token cannot be refreshed and the event retrieval will be interrupted. In this case, the connector must be restarted.

Certificate Issue While Integrating the Flexconnector with Azure Sentinel Alerts.

The following certificate exception error may be displayed while configuring up the Flex Rest Api connector.

```
Error[1]: [Unable to use the Events URL javax.net.ssl.SSLException:  
Certificate for <sent-frc-api.azure-api.net> doesn't match any of the subject  
alternative names: [* azurewebsites.net, *.scm.azurewebsites.net, *.azure-  
mobile.net, *.scm.azure-mobile.net, *.sso.azurewebsites.net]]
```

In the SmartConnector environment, the property to enable or disable Server Name Indication is disabled by default.

To enable the SNI:

- First, verify if the events URI is correct. If they are, based on your connector installation, choose one of the following steps:

- For stand alone installations, go to the current\bin\script folder and change to **True** the -Djsse.enableSNIExtension property in the following two files:
connectors.bat
jvmcommonparams.bat
- For service installations, go to the current\user\agent folder and change to **True** the -Djsse.enableSNIExtension property in the following file:
agent.wrapper.conf

Salesforce API is Unable to Receive Events

The Salesforce API may not be able to receive events, and instead, the following error is displayed:

```
[2021-03-06 10:36:22,507][FATAL][com.arcsight.agent.loadable.agent._FlexRestApiAgent] [refreshCredentials]There is no refresh token. Cannot refresh the access token. Please reconfigure the connector to have the user authenticated again.
```

The property scope=full refresh_token must be added.

To add the property scope=full refresh_token:

1. From the agent.properties file, go to agents[0].reauthenticate_onstartup=false.
2. Change the property to true.

Appendix A: About the REST FlexConnector Configuration Tool (restutil)

The restutil script lets you obtain the dynamic portion of an events URL. Some configuration values of the REST Flex Connector can include a dynamic portion that can be retrieved after running HTTP calls. For example, the Google Apps events URL has the customer id in the path and it can be retrieved via an authorized HTTP GET using the token obtained after the authentication is completed.

Use restutil to retrieve the dynamic portion of the events URL after installing core software and before beginning connector configuration. See "[Installing Core Software](#)" and "[Configuring Connector Parameters](#)".

restutil Configuration Tool Syntax

The following is the syntax of the restutil script:

```
arcsight restutil <command> <option-list>
<command> := [ authget | token | execute ]
<option-list> for authget := [ <proxy-option> ] <config-option> <url-option>
<option-list> for token := [ <proxy-option> ] <config-option>
<option-list> for execute := [ <proxy-option> ] <url-option> <execute-options-list>
<execute-options-list> := <execute-options> [ <execute-options-list> ]
<execute-options> := [ <token-option> | <method-option> | <header-option> |
<query-option> | <content-option> ]
<proxy-option> := -proxy <proxy-info>
<proxy-info> := <host>:<port>[:<user>:<password>]
<config-option> := -config <properties-file>
<url-option> := -url "<url>"
<token-option> := -token <token>
<method-option> := -method [GET|PUT|POST|DELETE|HEAD]
<header-option> := -header "<parameter-list>"
<query-option> := -query "<parameter-list>"
<content-option> := -content "<parameter-list>"
<parameter-list> := <parameter>;[ <parameter-list> ]
<parameter> := <name>=<value>
```

where <proxy-info> is <host>:<port> [:<user>:<password>], <properties-file> is the file imported during the setup, <method> is any HTTP command, such as GET, POST or DELETE, and <params> is a colon-separated list of parameter name and value which is expressed as <name>=<value>.

Invoking the restutil Configuration Tool

1. After installing core software (see "[Installing Core Software](#)"), create the configuration file and copy it to the \$ARCSIGHT_HOME directory.
The connector expects the properties file to be in the \$ARCSIGHT_HOME/user/agent/flexagent directory.
2. From the \$ARCSIGHT_HOME/bin directory, run the arcsight restutil script.

Retrieving an Access Token

To retrieve an access token, invoke the arcsight restutil script with the token command:

```
arcsight restutil token [ -proxy <proxy-info> ] -config <properties-file>
```

where <proxy-info> is <host>:<port> [:<user>:<password>] and <properties-file> is the file imported during configuration.

For example, the following command will print the token to the console:

```
# arcsight restutil token -proxy proxy.abc.com:8080\ -config google.properties  
...  
ya29.AHES6ZQp0jYZrsQYdGz2Nk0HAGfI3_AjTtxwOpeXywtZ-E_gpjQIDw  
◀ access token
```

Retrieving Values from the Server

To retrieve values from the server, invoke the arcsight restutil script with the execute command. A valid access token should be specified if the response is to be sent only to the authenticated user.

```
arcsight restutil execute [ -proxy <proxy-info> ] -url "<url>" [ -token  
<token> | -method <method> | -header "<params>" | -query "<params>" | -content  
"<params>" ]
```

This command can be used to run authorized and unauthorized commands. To run a command in an authorized way, obtain an access token with the arcsight restutil token command and pass the token using the -token option. In this case, the body of HTTP response will be displayed in the console. For example:

```
# arcsight restutil execute -token <token>\  
-proxy proxy.abc.com:8080\
```

```
-url "https://apps-apis.google.com/a/feeds/customer/2.0/customerId?alt=json"
. .
{
  "version": "1.0",
  "encoding": "UTF-8",
  "entry": [
    {
      "xmlns": "http://www.w3.org/2005/Atom",
      "xmlns$apps": "http://schemas.google.com/apps/2006",
      "id": "{$t": "https://apps-apis.google.com/a/feeds/customer/2.0/C03sabdb1"}, "updated": "{$t": "2013-02-22T20:23:34.364Z"}, "link": [{"rel": "self", "type": "application/atom+xml", "href": "https://apps-apis.google.com/a/feeds/customer/2.0/C03sabdb1"}, {"rel": "edit", "type": "application/atom+xml", "href": "https://apps-apis.google.com/a/feeds/customer/2.0/C03sabdb1"}], "apps$property": [{"name": "customerOrgUnitDescription", "value": "archp.mygbiz.com"}, {"name": "customerId", "value": "C03sabdb1"}, {"name": "customerOrgUnitName", "value": "archp.mygbiz.com"}, {"name": "description", "value": ""}], "name": "name", "value": "archp.mygbiz.com"}]
}
```

Retrieving Values Using an Authorized GET Command

Invoke the `arcsight restutil` script with the `authget` command to retrieve the result through an authorized GET command. This combines two commands. First, it obtains the access token and then executes the authorized GET command. The HTTP response will be displayed in the console. For example:

```
arcsight restutil authget [ -proxy <proxy-info> ] -config <properties-file> -url "<url>"
```

For example, the event URL for Google includes the customer id in the path. The following command returns the JSON formatted response that has the customer information. `customerID` should be part of the response.

```
# arcsight restutil authget -proxy proxy.abc.com:8080\ -config google.properties -url "https://apps-apis.google.com/a/feeds/customer/2.0/customerId?alt=json"
. .
{
  "version": "1.0",
  "encoding": "UTF-8",
  "entry": [
    {
      "xmlns": "http://www.w3.org/2005/Atom",
      "xmlns$apps": "http://schemas.google.com/apps/2006",
      "id": "{$t": "https://apps-apis.google.com/a/feeds/customer/2.0/C03sabdb1"}, "updated": "{$t": "2013-02-22T20:13:22.646Z"}, "link": [{"rel": "self", "type": "application/atom+xml", "href": "https://apps-apis.google.com/a/feeds/customer/2.0/C03sabdb1"}, {"rel": "edit", "type": "application/atom+xml", "href": "https://apps-apis.google.com/a/feeds/customer/2.0/C03sabdb1"}], "apps$property": }
```

```
[{"name":"customerOrgUnitDescription","value":"archp.mygbiz.com"},  
 {"name":"customerId","value":"C03sabdbl"},  
 {"name":"customerOrgUnitName","value":"archp.mygbiz.com"},  
 {"name":"description","value":""},  
 {"name":"name","value":"archp.mygbiz.com"}]}]
```

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 Developer's Guide for ArcSight FlexConnector for REST (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 25.1

Configuration Guide for Load Balancer

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

Overview	6
Why Use Load Balancer?	6
Load Balancer Features	7
How Load Balancer Works	9
Syslog-based Load Balancing	9
Support for Single-line Events	9
For TLS	9
For TCP	9
For UDP	9
File-based Load Balancing	9
Routing Policies	9
Routing policies supported in Load Balancer:	10
Load Balancer Modes	10
Installation and Configuration	12
Preparing to Install SmartConnectors	12
Configuring the Ethernet Connection	12
Installing the Load Balancer	13
Installing Load Balancer in Console Mode	14
Installing the Load Balancer in GUI Mode	17
Configuring Load Balancer	17
Configuration Scenarios	18
Configuring MemberHosts in Standalone Mode	18
Configuring MemberHosts as Peer	19
Configuring MemberHosts as Primary-Secondary	20
Syslog Load Balancing Routing Rule	22
File Load Balancing Routing Rule	26
Configuration Parameters	30
memberIdentity	31
memberHosts	31
notification	32
routing	33
statisticsLogging	40
webServer	40
globalParameters	41

clusterconfigurations	45
Configuring Load Balancer in Standalone Mode	46
Configuring Load Balancer in HA Mode	47
Configuring Syslog-based Load Balancing For TLS	50
Using CA Signed Certificates	50
Configuring TLS Certificates	52
Configuring the Syslog NG Server	52
Generating a Certificate Signing Request	52
Getting the CSR Signed by the CA	53
Importing the Digitally Signed Certificates into Load Balancer	53
Starting LoadBalancer	56
Running Load Balancer as a Service	56
Load Balancer Service Commands	58
Starting or Stopping the Load Balancer Service	58
Load Balancer Service-related Logs	59
Upgrading Load Balancer	59
Uninstalling Load Balancer	59
Load Balancer REST API	61
Configuration	61
Load Balancer API Reference	61
Retrieving a List of Routing Rules	61
Retrieving Details of a Routing Rule	62
Creating a Routing Rule	63
Deleting a Routing Rule	66
Enabling a Routing Rule	67
Disabling a Routing Rule	68
Retrieving a List of Sources	69
Retrieving Details of a Source	69
Creating a Source	70
Deleting a Source	71
Retrieving a List of Destinations	72
Retrieving Details of a Destination	74
Creating a Destination	75
Deleting a Destination	77
Retrieving a List of Destination Pools	78
Retrieving Details of a Destination Pool	79
Creating a Destination Pool	80

Deleting a Destination Pool	82
Adding a Destination to a Destination Pool	82
Deleting a Destination From a Destination Pool	84
REST API Common Errors	85
Load Balancer Troubleshooting	86
Interpreting Logs	86
Load Calculators Not Initialized or Destination Monitoring Not Working	86
Destination Configured with SCP Protocol but File Delivery Fails	87
Sources Relocated Away from [x] of [y] Destinations in Routing Rule	87
Warning Message in Passive or Secondary Node Logs	88
Calculating Loads for Routing	88
Appendix	89
Sample Configuration File	90
Standalone Mode Configuration File Template	93
HA Mode Configuration File Template	102
Publication Status	111
Send Documentation Feedback	112

Overview

ArcSight SmartConnector Load Balancer provides a “connector-smart” load balancing mechanism by monitoring the status and load of SmartConnectors. Currently it supports two types of event sources and SmartConnectors. One distributes the syslog input stream to syslog connectors using TLS, TCP, or UDP protocol and the other downloads files from a remote server and distributes them to the file-based connectors. Note that the TLS protocol is supported for the SmartConnector for Syslog NG Daemon only.

Load Balancer ensures efficiency by distributing the load to a pool of SmartConnectors. Load Balancer supports high availability configuration with active and standby nodes. It distributes the events received to one or more SmartConnectors predefined in the SmartConnector pool.

Load Balancer gathers the following information for SmartConnectors in the SmartConnector pool:

Availability: Load Balancer monitors SmartConnectors for availability. If a SmartConnector is down, then events are forwarded to the next available SmartConnector in the pool based on the defined load-balancing algorithm rules.

SmartConnector Load: CPU usage, memory usage, and queue drop rate for events.

Why Use Load Balancer?

Because the volume of events received from event sources vary, it makes it difficult to configure the SmartConnector and if the SmartConnector goes down, it leads to outage in continuous event collection. Load Balancer addresses these problems by distributing the events across SmartConnectors and by redistributing the events to available connectors if any connectors are down.

Load Balancer provides support to devices generating varying volumes of events, where:

- Overloaded connectors result in event loss and delayed collection
- Under-utilized connectors result in wasted resources
- Manual and tedious sizing and maintenance is necessary
- One connector becomes a single point of failure

Load Balancer is a solution for:

- Connector-smart load balancing
- Load balancing for TCP protocol without keeping the sessions sticky
- Load balancing for files
- An aggregation-preferred routing policy, which sends events from a single device to the same connector up to a certain threshold.

Load Balancer, together with the SmartConnector pool provides availability, reliability, and scalability as follows:

- Load Balancer supports High Availability (HA). If the active Load Balancer node is down, a passive Load Balancer node becomes an active node and continuously collects the events.
- If a SmartConnector is down, Load Balancer forwards the events to the next available connector in the SmartConnector pool per the load balancing rules.

Load Balancer Features

Load Balancer supports the following:

- High availability (HA) mode, which can be configured with two hosts.
- Syslog type of input stream or batch files on FTP server.
- Syslog-based and file-based SmartConnectors as destinations.
- TLS, TCP, and UDP protocol for syslog-type input or connectors.



Note: TLS is supported on the SmartConnector for Syslog NG Daemon only.

- Three routing policies — round robin, weighted round robin, and aggregation preferred.
- Event batching (TCP only) for better aggregation at the destination connector and better network throughput.
- Email notification for up or down status on member hosts and destination connectors.
- Load and health monitoring of connector destinations.
- Load Balancer runs either as a service or standalone application.

- TLS encryption is supported between devices and Load Balancer, Load Balancer and SmartConnectors, or both.
- Load Balancer accepts connections from both TCP and UDP on the same port.

How Load Balancer Works

This section provides information about Syslog-based load balancing, file-based load balancing, routing policies and Load Balancer modes.

Syslog-based Load Balancing

Support for Single-line Events

The load balancer parses the input stream into a line but not to an event. It supports single-line event stream but not multi-lined events.

For TLS

TLS is supported over TCP syslog connections. For TLS, you must use a SmartConnector for Syslog NG with TLS enabled. Using TLS, incoming events will be processed automatically, as long as a self-signed certificate is imported into any devices sending events to the Load Balancer.

For TCP

When the source is a syslog-based network process and configured to use TCP protocol, the input stream is parsed into event lines and bundled into a batch. Then the batch is distributed to one of the destinations in the destination pool.

For UDP

If a routing rule is configured to use UDP protocol, event batching does not happen. Instead, each incoming event is distributed into one of the destinations configured in the routing policy.

File-based Load Balancing

Load Balancer downloads files from an FTP server and distributes them to one of the locations associated with the file connectors. It supports batch files. File-based connectors that read and process files are good candidates for this feature.

Routing Policies

Routing policies are a set of rules that define the data distribution from a source to a set of destinations. Eligible sources are syslog servers or FTP servers. A destination pool consists of

one or more syslog or file connector destinations, all of the same type. Connector types cannot be mixed within a single destination pool. Routing policies define event or file distribution rules from a source to destination pool.

Routing policies supported in Load Balancer:

- **Round Robin:** Distributes events, batches, or files to each available destination in the destination pool in round robin fashion, beginning again at the start in a circular manner. File-based load balancing supports only the Round Robin policy.
- **Weighted Round Robin:** Distributes events in a round-robin fashion, but sends more events or batches to lightly loaded destinations.
- **Aggregation Preferred:** Events from the same source are sent to the same destination until a threshold is reached. Then, the load balancer will switch the routing to another destination. This routing policy is better suited if aggregation is enabled on connector destinations where events are sent to the same destination until certain load thresholds are met. For more information on the global properties for configuring this routing policy, see [global parameters](#) in the [configuration parameters](#) section.

Load Balancer Modes

The Load Balancer can be configured in the following modes:

- **Standalone mode:** Load Balancer runs as a single host without supporting the high availability feature. One host with a single static IP address is required to run Load Balancer in this mode.
- **HA mode as peer:** Load Balancer runs with two hosts. The host that starts first becomes active and another host runs as passive until the first host goes down. The second host becomes active and stays active, even if the first host comes back up again.
- **HA mode as primary-secondary:** Load Balancer runs with two hosts. One host can be designated as the preferred active host. In this mode, the host marked as primary runs as active node whenever it becomes available.

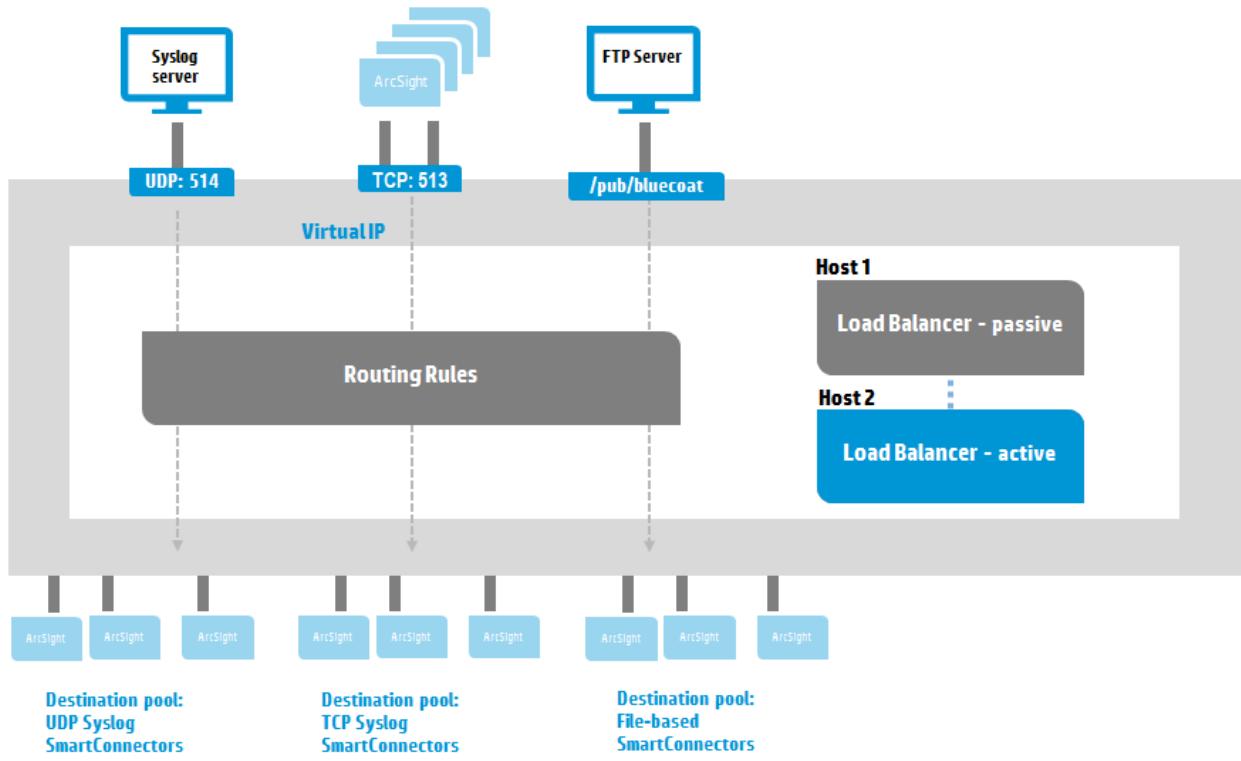
To use the high availability feature, Load Balancer must be installed on two separate hosts sharing a virtual IP address. For more information, see [Configuring Load Balancer in HA Mode](#).



Note: The High Availability feature, which is available using primary-secondary or peer mode, currently works only within the same subnet.

Load Balancer can be deployed between any syslog source, including SmartConnectors configured with CEF syslog or raw syslog destinations, or file source and SmartConnectors. The following diagram shows a Load Balancer deployment example running in HA mode. Both hosts

share the common virtual IP address to handle the connection fail-over when an active Load Balancer host goes down. As shown in the diagram, Load Balancer can be used for three different types of input sources and destination pool types.



When configuring the routing rule, source and destination types must match. If the source is TCP syslog, the connectors in the destination pool must be TCP syslog connectors. Likewise, if the source is a file type, the connectors on the destination must be file-based connectors that expect to handle files.

When the routing rule is configured with TCP protocol, events received from the same source IP and port number are bundled into event batches. Event batching happens when any of the following conditions are met: buffer size, number of events, or batching interval. The bundled event batch, which is optional, is persisted by default on the hard drive before it is sent to the destination connector in the `${ARCSIGHT_HOME} /user/loadbalancer/lbdata/persistence/{source}` directory of the currently active node. Note that persisted event batches are not shared across the member hosts and any unprocessed event batches awaiting bundling during the shutdown are sent when Load Balancer starts up again.

Installation and Configuration

This section describes the steps to install and configure Load Balancer.



Load Balancer is an independent component, not packaged with SmartConnectors.

Preparing to Install SmartConnectors

Before you proceed with the installation, make sure that you have done the following:

- Make sure that you meet the [system requirements](#)
- [Download the Load Balancer binary](#)

To run in HA mode, make sure that the following pre-requisites are met:

- Have two hosts with static IP addresses to install Load Balancer.
- Have a single, unused address for the VIP to run Load Balancer in HA mode.
- [Create an Ethernet configuration file to support failover migration.](#)

Configuring the Ethernet Connection

You must configure the Ethernet connection to support failover migration.

To configure the Ethernet connection:



Note: Step 3 and 4 can vary depending on the OS version and flavor. Use the instructions as a reference. Get help from the network administrator to execute the following steps.

1. To enable HA, identify two machines with one virtual IP address in the same subnet.
2. If Load Balancer is run by a non-root user, provide sudo capability to the user.
For example, if `arcsight` is the user that installs and runs Load Balancer, add the `arcsight` user and add sudoer capability with NOPASSWD.

```
# adduser arcsight // Creates arcsight group and adds the user to the group.  
# sudo visudo
```

```
// Add the following line, and exit.  
arcsight ALL=(ALL) NOPASSWD:ALL
```

3. (Conditional) If SmartConnectors is not deployed in Standalone mode, when using two machines for HA, create a network profile or Ethernet configuration file on each machine. In the supported distributions of Linux, this file is usually located in the /etc/sysconfig/network-scripts directory.
 - a. Go to the directory and verify that the file has the primary network interface (usually 'eth0') configuration. The IPADDR value of this file must display the IP address assigned to this machine. A similar configuration file must be created for the virtual IP address.
 - b. Log in as a privileged administrator and go to the directory where the Ethernet profiles are located.

```
# cd /etc/sysconfig/network-scripts
```

- c. Copy the default eth0 configuration to eth0:1.

```
# cp ifcfg-eth0 ifcfg-eth0:1
```

- d. Edit ifcfg-eth0:1 to modify DEVICE to eth0:1 and IPADDR to a virtual IP address and save the file.

```
DEVICE=eth0:1
IPADDR=<virtual-ip-address> # for example, 10.0.0.0
ONBOOT=no
NM_CONTROLLED=no
ARPCHECK=no
BOOTPROTO=static
```



Note: ONBOOT must be set to no in order to prevent the VIP address from being bound to the host automatically upon system reboot. Otherwise, the virtual IP address needs to be released manually when another host is running as the active node or it will lose the connection from the source devices

4. Verify the full path of the ifup command, usually /sbin/ifup. Make note of the full path of the ifup command and Ethernet profile.

Installing the Load Balancer

The installer runs both in console mode and GUI mode. Follow the instructions in one of the following sections for the appropriate mode:

- "[Installing Load Balancer in Console Mode](#)" on the next page
- "[Installing the Load Balancer in GUI Mode](#)" on page 17

Installing Load Balancer in Console Mode

To install the Load Balancer files in console mode:

- ### 1. Run the installer.



Note: The ‘-i console’ mode is automatically selected by default if you do not use graphical display or if the DISPLAY variable is not set. It can also be specifically invoked using the `-i console` switch as shown here.

ArcSight recommends that you quit all other programs before continuing with this installation.

Click the ‘Next’ button to proceed to the next window. If you want to change something on a previous window, click the ‘Previous’ button. To cancel this installation at any time, click the ‘Cancel’ button.

PRESS <ENTER> TO CONTINUE:

2. Type an absolute path or just press **Enter** to accept the default location.

Choose Install Folder

Select an installation folder. When upgrading from a previous version, select the folder that contains the currently installed ArcSight SmartConnector Load Balancer

Where to install:

Default Install Folder: /root/ArcSightSCLoadBalancer

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT

:

3. Type the option number that corresponds with the shortcut or link to be created for Load Balancer, if any. Press **Enter**.

Choose Link Location

Where would you like to create links?

->1- Default: /root

2- In your home folder

3- Choose another location...

4- Don't create links

ENTER THE NUMBER OF AN OPTION ABOVE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT

:

4. Check the pre-installation summary before proceeding to the installation, then press **Enter** to start the installation.

Pre-Installation Summary

Review the following information before continuing:

Product Name:

SmartConnector Load Balancer

Install Folder:

/root/ArcSightSCLoadBalancer

Link Folder:

/root

Install Set:

Typical

PRESS <ENTER> TO CONTINUE:

5. Upon completion, the screen displays the location where Load Balancer is installed.

Installing...

[===== | ===== | ===== | =====]

[----- | ----- | ----- | -----]

=====

Installation Complete

The core components of the ArcSight SmartConnector Load Balancer have been
successfully installed to:

/root/ArcSightSCLoadBalancer

PRESS <ENTER> TO EXIT THE INSTALLER:

6. Press **Enter** to exit.

Installing the Load Balancer in GUI Mode

To install the Load Balancer files in GUI mode:

1. Run the installer.

```
# sh ArcSightSCLoadBalancer-<build-number>.bin
```

The installer loads and the Introduction screen displays. Click **Next**.

2. Accept the default path or enter a new path in the “Where to install” field. Click **Next**.

 **Note:** If you are logged in as root , the install path is /root/ArcSightSCLoadBalancer.

3. Select your preferred option for creating a link to Load Balancer (the link folder). Click **Next**.
4. Review installation information in the Pre-Installation Summary. Click **Previous** to make changes or click **Install** to install Load Balancer.
5. Review the installation location and click **Done** to quit the installer.

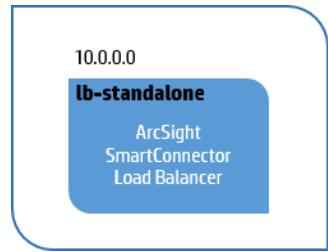
Configuring Load Balancer

This section has the following information related to configuring Load Balancer.

Configuration Scenarios

Configuring MemberHosts in Standalone Mode

Load Balancer can be configured to run in a standalone mode as shown in the following diagram:



```
<memberHosts vipAddress="10.0.0.0" vipPingPort="9090">  
    <memberHost name="lb-standalone" host="10.0.0.0" port="6702" isPrimary="false"  
        vipBindCommand="sudo /sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="sudo  
        /sbin/ifdown /etc/sysconfig/network-scripts/ifcfg-eth0:1"/>  
    </memberHosts>  
<memberIdentity>lb-standalone</memberIdentity>
```

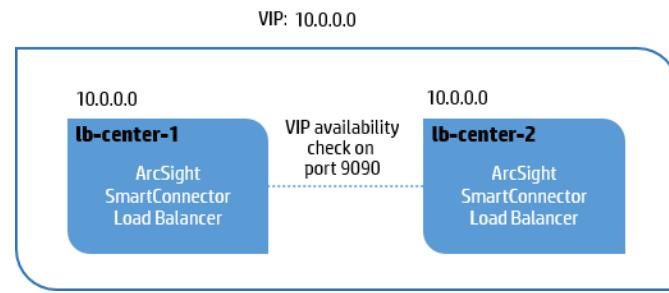


Note: `vipBindCommand` and `vipUnbindCommand` have `sudo` in the command because Load Balancer is not running as root.

Configuring MemberHosts as Peer

When Load Balancer is deployed to run as peer, Load Balancer is installed on two hosts sharing the same virtual IP address. In the diagram below

lb-center-1 and lb-center-2 are running as peer. The member host that starts first will run as the active member and pushes the configuration value to the other member host. Note that `isPrimary` is set to **false** in both configurations.



For **IbConfig.xml** on **lb-center-1**:

```
<memberHosts vipAddress="10.0.0.0" vipPingPort="9090">

    <memberHost name="lb-center-1" host="10.0.0.0" port="6702" isPrimary="false" vipBindCommand="sudo
/sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="sudo /sbin/ifdown
/etc/sysconfig/network-scripts/ifcfg-eth0:1"/>

</memberHosts>

    <memberHost name="lb-center-2" host="10.0.0.0" port="6702" isPrimary="false" \>
        vipBindCommand="sudo /sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" \
        vipUnbindCommand="sudo /sbin/ifdown /etc/sysconfig/network-scripts/ifcfg-eth0:1"/>

</memberHosts>

<memberIdentity>lb-center-1</memberIdentity>
```

For **IbConfig.xml** on **lb-center-2**:

```
<memberHosts vipAddress="10.0.0.0" vipPingPort="9090">  
    <memberHost name="lb-center-1" host="10.0.0.0" port="6702" isPrimary="false" vipBindCommand="sudo /sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="sudo /sbin/ifdown /etc/sysconfig/network-scripts/ifcfg-eth0:1"/>  
    </memberHosts>  
    <memberHost name="lb-center-2" host="10.0.0.0" port="6702" isPrimary="false" vipBindCommand="sudo /sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="sudo /sbin/ifdown /etc/sysconfig/network-scripts/ifcfg-eth0:1"/>  
    </memberHosts>  
<memberIdentity>lb-center-2</memberIdentity>
```



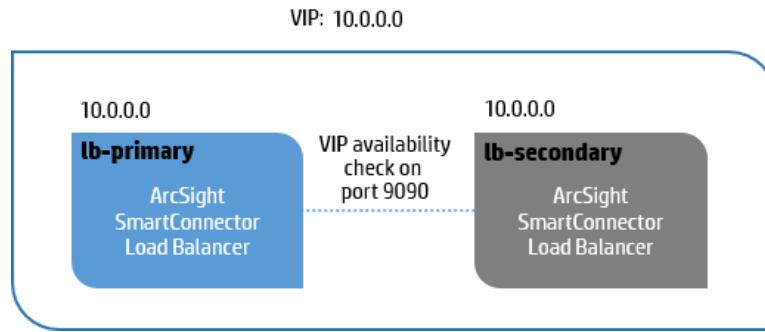
Note: `vipBindCommand` and `vipUnbindCommand` have `sudo` in the command because Load Balancer is not running as root.

Configuring MemberHosts as Primary-Secondary

When Load Balancer is going to be deployed as primary-secondary, Load Balancer is installed in two hosts sharing the same virtual IP address. In the diagram below lb-primary is designated as the primary load balancer and the value for `isPrimary` is set to `true` for `memberHost`, while it is set to `false` for lb-secondary. Always start lb-primary member host first to have configuration synchronized to lb-secondary member host.



Note: `vipBindCommand` and `vipUnbindCommand` do not have `sudo` in the command because Load Balancer is running as root.



For **lbConfig.xml** on **lb-primary**:

```

<memberHosts vipAddress="10.0.0.0" vipPingPort="9090">
    <memberHost name="lb-primary" host="10.0.0.0" port="6702" isPrimary="true"
    vipBindCommand="/sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="/sbin/ifdown
    /etc/sysconfig/network-scripts/ifcfg-eth0:1"/>
</memberHosts>
    <memberHost name="lb-center-2" host="10.0.0.0" port="6702" isPrimary="false"
    vipBindCommand="/sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="/sbin/ifdown
    /etc/sysconfig/network-scripts/ifcfg-eth0:1"/>
</memberHosts>
<memberIdentity>lb-primary</memberIdentity>
```

For **lbConfig.xml** on **lb-secondary**:

```

<memberHosts vipAddress="10.0.0.0" vipPingPort="9090">
    <memberHost name="lb-center-1" host="10.0.0.0" port="6702" isPrimary="true"
    vipBindCommand="/sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="/sbin/ifdown
    /etc/sysconfig/network-scripts/ifcfg-eth0:1"/>
```

```
</memberHosts>

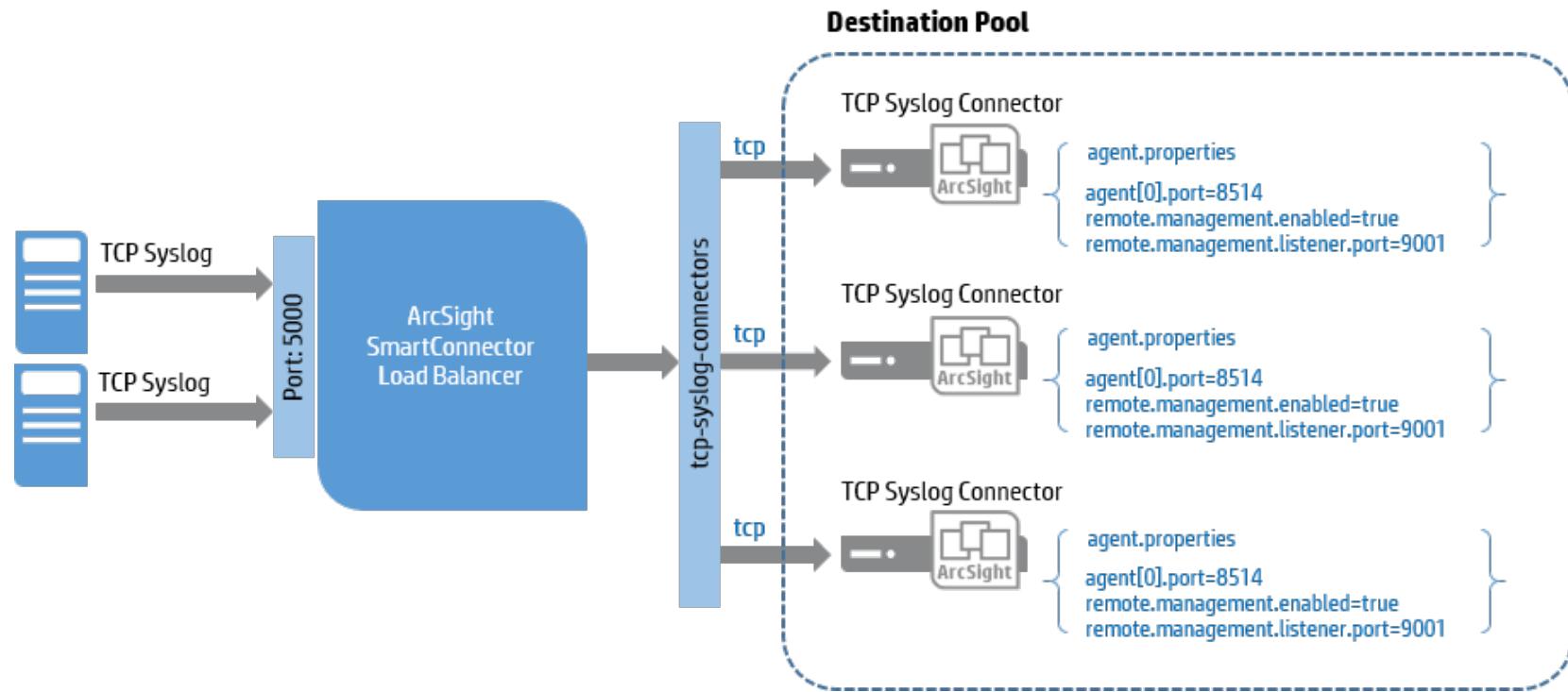
<memberHost name="lb-secondary" host="10.0.0.0" port="6702" isPrimary="false"
vipBindCommand="/sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="/sbin/ifdown
/etc/sysconfig/network-scripts/ifcfg-eth0:1"/>

</memberHosts>

<memberIdentity>lb-secondary</memberIdentity>
```

Syslog Load Balancing Routing Rule

The following diagram illustrates two syslog servers feeding an input stream into Load Balancer on port 5000 using a TCP connection. In this scenario, Load Balancer distributes the events to three TCP syslog connectors which are grouped as one destination pool called ‘tcp-syslog-connectors’. The following configuration file shows an example of how to configure the routing rule used in this scenario. Note that `remote.management.listener.port` is configured per destination. This information is used to detect the health and load of the connectors in destination pool and the connector is considered down if it is configured with an incorrect value.



```
<routing>
  <destinationPools>
    <destinationPool name="tcp-syslog-connectors">
      destinations="tcp-syslog-1,tcp-syslog-2,tcp-syslog-3"/>
    </destinationPools>
  <destinations>
    <destination name="tcp-syslog-1" type="syslog" host="10.0.0.0">
```

```
port="8514" protocol="tcp">
<additionalParameters type="connector">
<properties>
<property key="remote.management.listener.port" value="9001"/>
</properties>
</additionalParameters>
</destination>
<destination name="tcp-syslog-2" type="syslog" host="10.0.0.0"
port="8514" protocol="tcp">
<additionalParameters type="connector">
<properties>
<property key="remote.management.listener.port" value="9001"/>
</properties>
</additionalParameters>
</destination>
<destination name="tcp-syslog-3" type="syslog" host="10.0.0.0"
port="8514" protocol="tcp">
<additionalParameters type="connector">
<properties>
```

```
        <property key="remote.management.listener.port" value="9001"/>

    </properties>

</additionalParameters>

</destination>

</destinations>

<routingRules>

    <routingRule name="firewall-syslog" sourceName="syslog-receiver"
        destinationPoolName="tcp-syslog-connectors"
        routingPolicy="WeightedRoundRobin" enabled="true">

        <additionalParameters type="listener">

            <properties>

                <property key="syslog.address.prepend.mode" value="scan"/>

            </properties>

        </additionalParameters>

    </routingRule>

</routingRules>

<sources>

    <source name="syslog-receiver" type="syslog" port="5000"
        protocol="tcp"/>

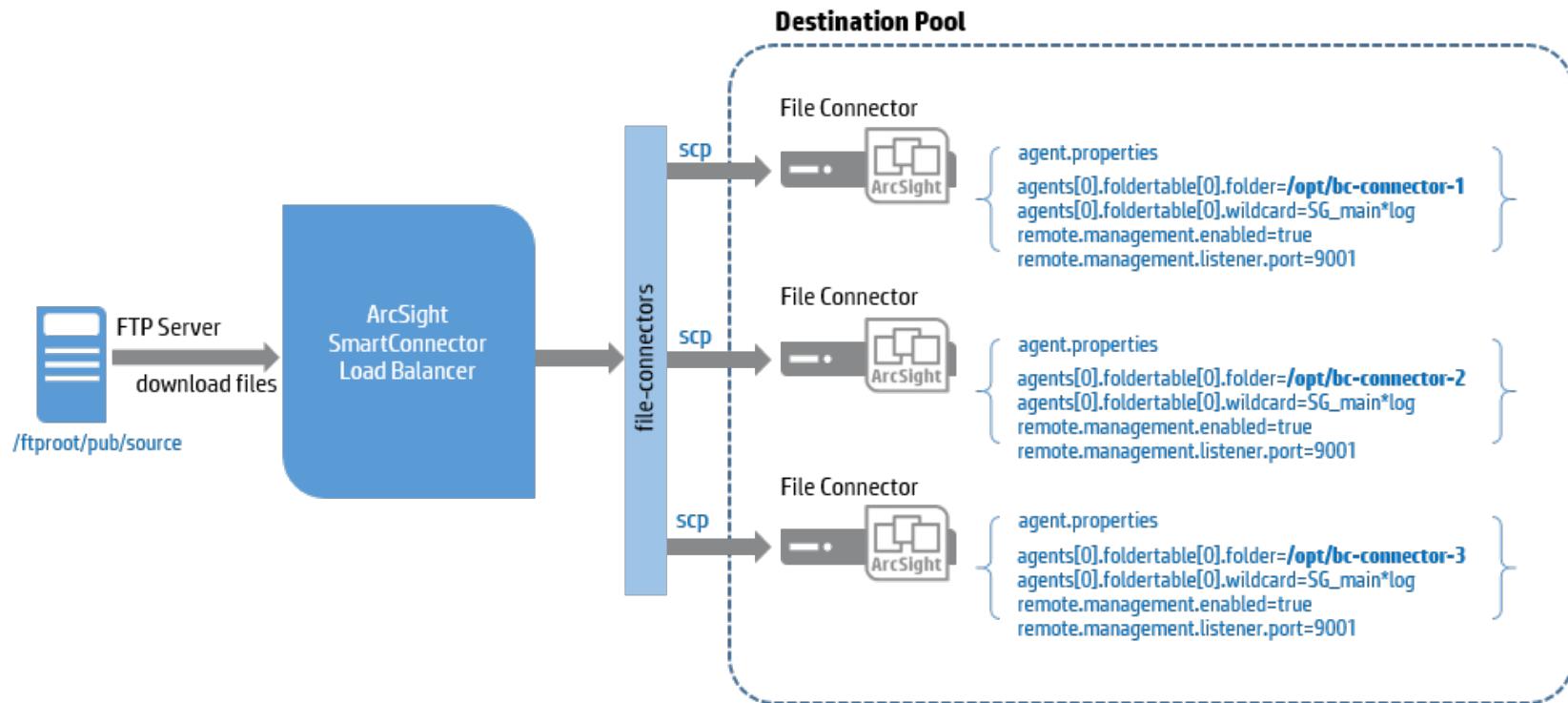

```

```
</sources>  
</routing>
```

File Load Balancing Routing Rule

The following diagram shows a configuration example of a routing rule for file load balancing. To define the source, an FTP host address, the credentials, and the path need to be defined. Here, the FTP root directory is /ftproot/pub, so the actual location to FTP client should be the `source` directory. The rest of the routing rule configuration is similar to syslog routing rule configuration.

-  **Note:** When uploading files to the source FTP server, be sure to use a temporary file name and specify the filter in the `fileFilter` parameter to filter out temporary files. After file upload is complete, rename the file to an original name.
-  **Note:** The agent name for file connectors is specified in this configuration.



```
<routing>
  <destinationPools>
    <destinationPool name="file-connectors"
      destinations="file-connector-1,file-connector-2,file-connector-3"/>
  </destinationPools>
  <destinations>
    <destination name="file-connector-1" type="file">
```

```
path="/opt/bc-connector-1" host="10.0.0.0" protocol="scp"
username="admin" password="password"
knownHostsFile="/home/arcsight/.ssh/known_hosts">
<additionalParameters type="connector">
<properties>
<property key="remote.management.listener.port" value="9001"/>
<property key="agent.name" value="bc-connector-1"/>
</properties>
</additionalParameters>
</destination>
<destination name="file-connector-2" type="file">
path="/opt/bc-connector-2" host="10.0.0.0" protocol="scp"
username="admin" password="password"
knownHostsFile="/home/arcsight/.ssh/known_hosts">
<additionalParameters type="connector">
<properties>
<property key="remote.management.listener.port" value="9001"/>
<property key="agent.name" value="bc-connector-2"/>
</properties>
```

```
</additionalParameters>

</destination>

<destination name="file-connector-3" type="file"
    path="/opt/bc-connector-3" host="10.0.0.0" protocol="scp"
    username="admin" password="password"
    knownHostsFile="/home/arcsight/.ssh/known_hosts">

    <additionalParameters type="connector">
        <properties>
            <property key="remote.management.listener.port" value="9001"/>
            <property key="agent.name" value="bc-connector-3"/>
        </properties>
    </additionalParameters>
</destination>

</destinations>

<routingRules>

    <routingRule name="file-rule" sourceName="file-watcher"
        destinationPoolName="file-connectors" routingPolicy="RoundRobin"
        enabled="true"/>

</routingRules>
```

```
<sources>
  <source name="file-watcher" type="file" path="/source"
    host="10.0.0.0" protocol="ftp" username="admin"
    password="OBFUSCATE.1:B8R3Ts5XXui0aBjFn1Js7Q=="
    moveToDirectory=".done" fileFilter="SG_main.*log"
    localWorkDirectory="/tmp" recursive="true" passive="false" />
</sources>
</routing>
```

Configuration Parameters

Configure Load Balancer with the following parameters:

- "memberIdentity" on the next page
- "memberHosts" on the next page
- "notification" on page 32
- "routing" on page 33
- "statisticsLogging" on page 40
- "webServer" on page 40
- "globalParameters" on page 41
- "clusterconfigurations" on page 45

memberIdentity

memberHost in the memberHosts section defines the list of hosts that run Load Balancer, where each member host must have a unique name. The value of memberIdentity must be configured with the member host name that identifies the current host.

Ensure that:

- The valid name consists of alphanumeric characters without spaces.
- The matching names are found in memberHosts/memberHost/name.
- The host configuration is the configuration for the current node.

memberHosts

Configure the list of member hosts that participate in load balancing in this section. The mode is determined by this configuration. Up to two member hosts are allowed.

- vipAddress : Specifies the virtual IP address when running Load Balancer with two hosts to enable HA mode.
- vipPingPort : Specifies the port used internally to detect the virtual IP binding status. Change the value if this port is being used by another application. (Default port is 9090.)
- memberHost : Configures the participating host where Load Balancer will be installed and running.
 - name: Specifies a unique name that identifies the host.
 - address: Specifies the IP address of the participating host. Load Balancer must be installed on this host.
 - port: Specifies the port number used by the underlying library for HA support.
 - isPrimary: Specifies the running mode for Load Balancer.
 - Set this value to true to designate a primary host when Load Balancer is running in primary-secondary mode.
 - Only one host can be configured as the designated primary host.

- To run Load Balancers in peer mode, set this value to `false` for both member hosts.
 - `vipBindCommand`: Specifies the full command used to bind the virtual IP address to this host. Prior to configuring this, the Ethernet connection virtual IP address should have been configured. See "[Configuring the Ethernet Connection](#)" on page 12 for details.
 - In Linux, `/sbin/ifup` shows the Ethernet configuration.
 - Be sure to use the absolute path when specifying the command. For example, if the virtual IP address profile is located in:
`/etc/sysconfig/network-scripts/ifcfg-eth0:1`
specify:
`sudo /sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1.`
-  **Note:** If Load Balancer is running as the root user, remove '`sudo`'.
- `vipUnbindCommand`: Specifies the full command used to unbind the virtual IP address from this host. It defines the counter command for binding. Refer to the details in the previous `vipBindCommand`.

notification

The configuration information provided in this section sets up notifications when certain events occur, such as when a member host goes up or down, or when a destination host goes down or up.

- `enable`: Specifies whether the sending of notification is enabled or disabled. Set this value to `true` to enable notifications.
- `enabledNotification`: Specifies the events for which notifications are sent. Notifications are supported for the following types of events:
 - `MemberHostUp`
 - `MemberHostDown`
 - `DestinationUp`

- DestinationDown

Notifications are sent only for specified supported events. For example, if only the MemberHostDown event is listed, the notification will be sent only when one of the configured hosts is down.

- event: Specifies the events for which a notification will be sent.
 - name : Specifies the event name.
 - message : Specifies the custom message. If undefined, a default message is used.
- email: Configures the email sender, receiver, prefix, and SMTP server.
 - prefix: Configures the value used to tag the notification message in the subject line. When not configured, the subject will not have a prefix tag.
 - recipients: Specifies a list of one or more valid email addresses of the recipients. Separate each email address by a space.
 - sender: Specifies the sender's email address.
 - smtpServer: Specifies the SMTP server configuration. If this value is not configured, the email will not be sent.

routing

Use this section to define the routing rules. Data will be received from the source machine and distributed to the destinations in the destination pool. In routing configuration, every name should be unique whether the name is used for source or destination. The source cannot be referenced in more than one routing rule. The destination can be referenced in more than one destination pool.

When configuring a routing rule, the incoming and outgoing protocol used for one routing rule must be the same. For example, if routing rule A has source configured with TCP, destinations in the destination pool in routing rule A must be configured with the same TCP. TLS and TCP destinations can be mixed. If the source is configured with UDP, destinations in the same routing rule must be configured with UDP. Note that TLS cannot be mixed with UDP.

- **sources:** A list of sources
 - **source:** Specifies the data ingress.
 - **name:** Specifies the unique name that identifies the source.
 - **type:** Specifies the source type. Valid source types are `file` and `syslog`.
 - Specify `syslog` if the events are fed from a syslog server or syslog connector.
 - Specify `file` if files are to be distributed to a destination.
 - Specify `netflow` if the events are of type IP Flow (NetFlow/J-Flow) and IP Flow Information Export (IPFIX) versions supported by SmartConnector.
 - **protocol:** Specifies the protocol that Load Balancer will use to listen:
 - For `syslog` type, `tls`, `tcp` and `udp` are supported.
 - For `file` type, `ftp` is supported.
 - **host:** If the source is configured as a `file` type, specify the host IP address, host name, or FQDN from which Load Balancer will download the files.
 - **port:** Specifies the port used:
 - For the `syslog` type, specify the port where Load Balancer will be listening. All port numbers must be unique or there will be a binding error.
 - For the `file` type, this specifies the FTP server port to which Load Balancer connects to download files. Skip the configuration of this value if FTP server is configured with the default port. (The default FTP port is 21.)

The following configuration values apply only to the `file` type source.

- **path:** Specifies the path where the files are located in the FTP server. This path should be based off the FTP root directory. For example, if the FTP root directory is configured as `/ftp/pub` and the files are located under `/ftp/pub/source`, specify `/source` to this value.
- **username:** Specifies the user name used to log into the FTP server.

- `password`: Specifies the password configured for the user. The plaintext password is encrypted and persisted during the Load Balancer startup.
- `fileFilter`: Specifies the Java-style regular expression used to filter the files to download from the specified path. For example, `.*log` will filter the files with names ending with 'log'. To download the files with names starting with 'Simple' and ending with 'log', use `Simple.*log`.



Note: When uploading files to the source FTP server, be sure to use a temporary file name and specify the filter in the `fileFilter` parameter to filter out temporary files, otherwise Load Balancer may download an incomplete file. After file upload is complete, rename the file to an original name.

- `recursive`: Specifies that Load Balancer downloads the file recursively from subdirectories when set to `true`. By default, it is set to `true`.



Note: Load Balancer cannot handle a file larger than 1 GB – 1 byte (approximately 1 GB). When Load Balancer detects a file that exceeds the maximum size, it logs an error message and continues to the next file.

- `localWorkDirectory`: Specifies the existing path to the directory where Load Balancer will place the downloaded files temporarily before they are actually sent out to the destination. Configuring this field is required when FTP is configured with the `file` source type.
- `moveToDirectory`: Specifies the directory on the source to which the files should be moved after the files are successfully delivered to the destination. This directory can be created as a sub-directory under the source directory that is specified in `path` or can be located in another location. In the case of moving the files to a sub-directory of the source files, be sure to provide a name that starts with dot so that it is treated as a hidden directory such as `.done`. Otherwise it will recursively download the files from sub-directories and move them to another nested sub-directory unless `recursive` is set to `false`. See the option to turn off recursive search. If this is set to `blank` or omitted, files are deleted instead.
- `passive`: FTP server can be configured to run in passive or active mode. Set this value to `true` if FTP server is running in passive mode. Otherwise set to `false`.

- **destinations:** A list of destinations.
 - **destination:** Specifies a destination where events or file will be sent.
 - Only connectors are supported as destinations. Identify the connectors to be used as destinations and configure the following values:
 - **name:** Specifies a unique name that identifies the destination.
 - **type:** Specifies the destination type. Valid destination types are `file` and `syslog`. The type must match the connector type. If a syslog connector is used as a destination, configure `type` as `syslog`. If the connector is reading files from certain directory such as a Bluecoat connector, configure `type` as `file`. If the IP Flow (NetFlow/J-Flow) or IP Flow Information Export (IPFIX) connector is used as a destination, configure `type` as `netflow`.
 - **host:** Specifies the destination address where the connector is installed. Applicable whether the `type` is set to `syslog` or `file`.
 - **protocol:** Specify the protocol used to send data to the destination connector.
 - For `syslog` type, `tls`, `tcp` and `udp` are supported.
 - For `file` type, `ftp` and `scp` are supported. When `ftp` is used, the connector installation host should be running an FTP server to receive the file from Load Balancer.
 - **port:** For `syslog` destinations, this value specifies the configured port where the connector listens for events. This port number should match the port number found in the `agent.properties` file of the destination connector. For `file` type, this can be skipped if the default ports are being used. The default FTP port is 21 and SCP is 22.

The following configuration values are applicable only to `file` type source.

- **username:** Specifies the user name used to log into the FTP server or to run an `scp` command.
- **password:** Specifies the password set for the user. This password will also be encrypted when the Load Balancer starts up.
- **path:** Specifies the path to where the files will be moved. If protocol is configured as `ftp`, this path should be relative to the FTP root directory. For `scp`, it should be a full path.

- `knownHostsFile`: Specifies the file path of known hosts file if the destination protocol is `scp`. This file should contain the host key used for SSH connections, which is usually added to `$HOME/.ssh/known_hosts` on an initial SSH connection to a specified host. Specify the path of default known hosts file or the one created for Load Balancer testing, if it exists. Note that `$ARCSIGHT_HOME/user/loadbalancer` is assumed to be the base directory if the path does not start with `/`. Currently `ssh-rsa` or `ssh-dsa` are accepted as valid algorithms.

Specify the destination connector information using in the following section to enable Load Balancer to communicate with the connector and to check the health and load. Before configuring the following values, first go to the connector installation directory on the machine where the connector is installed and ensure that remote management is enabled and get the port number configured for remote management. Corresponding property names for these two values in `agent.properties` are `remote.management.enabled` and `remote.management.listener.port`. If the destination is a file connector, the agent name—which is specified near the end of the installation wizard process during the connector configuration step and persisted into destination descriptor—will be needed. Note that agent name within the container should be unique when more than one connector is configured within the container.

- `additionalParameters/properties`
 - `username`: Specifies the user name used to log into the connectors. You can optionally change the default remote management user name value whenever the remote management user name of connectors is changed. To change the user name, update the `lbConfig.xml` configuration file by adding the following property under each destination:
`<property key="username" value="newusername"/>`
 - `password`: Specifies the password set for the user. You can optionally change the default remote management password value whenever the remote management password of connectors is changed. The plaintext password is encrypted and persisted during the Load Balancer startup. Note: The new password must contain XML acceptable format.
To change the password, update the `lbConfig.xml` configuration file by adding the following property under each destination:
`<property key="password" value="newpassword"/>`

- `remote.management.listener.port`: Specifies the value of `remote.management.listener.port` of the destination connector.
- `load.expression`: Specifies custom load-level calculation expressions as per-destination overrides. Expressions can be used to favor certain destinations over others. Weaker destinations can be pre-favored to be less utilized by having a large constant value added or multiplied to their load.



Note: For information on configuring an expression to calculate the load per destination, see "[Calculating Loads for Routing](#)" on page 88.

- `agent.name`: Provide this value only if the destination is a file connector.

When you install the connector, the default port is specified under the connector installation in `config/agent/agent.defaults.properties` as `remote.management.listener.port`. If you change the `remote.management.listener.port` property value to anything other than the default, then this property is present in `agent.properties` under `user/agent`. In that case, you must update the change in the value to the correct value in the `agent.properties` file.

For management of certificates from destinations, Load Balancer creates a directory on the Load Balancer machine such as `<ARCSIGHT_HOME>/certs` and populates downloaded certificates from the destinations under this folder. The automatic download and import of certificates is done in the background.



IMPORTANT:

On remote connector installations (destination connectors), turn on the remote management enabled flag. In the `user/agent/agents.properties` file, add `remote.management.enabled=true`. Do this before starting the connectors.



Start the destination connectors before starting Load Balancer. Doing so ensures Load Balancer is able to query destinations for usage, load, and health statistics. More importantly, this also lets Load Balancer contact the connector host on the provided port and download the certificates for the connectors, which then enables the destination monitoring. If the connector is not up when Load Balancer starts, Load Balancer will check periodically to see if the connector comes up and then includes it for destination monitoring.

- `destinationPools`: A list of destination pools.
 - `destinationPool`: Specifies the destination group that can handle the same type of events. All destinations in one destination pool must be of the same type.
 - `name`: Specifies a unique name that identifies the destination pool.
 - `destinations`: Specifies comma-separated destination names. Valid destination names are the ones already configured.



Note: Only destination names configured under the `destination` section can be used here.

- `routingRules`: A list of routing rules.
 - `routingRule`: Specifies the routing rule that defines the data flow. Data received on the source will be distributed to the destinations in the destination pool.
 - `name`: Specifies a unique name that identifies the routing rule.
 - `sourceName`: Specifies the source name that is configured in `sources`.
 - `destinationPoolName`: Specifies the name of the destination pool that is configured in `destinationPools`.
 - `routingPolicy`: Specifies the routing policy algorithm. Valid routing policies are `RoundRobin`, `WeightedRoundRobin`, and `AggregationPreferred` for `syslog` type. For `file` type, only `RoundRobin` is supported.
 - `enabled`: Specifies activation of the routing rule if set to `true`. Otherwise, the routing rule will not be applied.

- additionalParameters/properties
 - listener: Specifies the type of listener, which currently includes the `syslog.address.prepend.mode` property. This property allows Load Balancer to detect IPv4 addresses, IPv6 addresses, Solaris-style addresses, and hostnames. It will add the Load Balancer's current time and the remote socket address which sent the event, if needed. The available values are: `disabled` (the default—no information is added), `scan` (only adds information if Load Balancer does not detect an address), and `always` (always adds information).
Load Balancer supports the IETF Standard (RFC 5424) syslog header. If the input log is not in this format, Load Balancer might not detect addresses properly. For details, see "["syslog.header.timestamp.ip: " on page 45](#).



Note: Using the `scan` value will have a negative performance impact. Enable the `scan` mode only if it is necessary. It is recommended to use the routing rules with the `disabled` or `always` option if it is known that the sources will always have or not have addresses included.

statisticsLogging

- `logInterval`: Specifies the statistics logging interval in milliseconds. By default, the statistics are logged every minute (60,000 ms).

webServer



Note: This configuration is required per Load Balancer installation now and will be enabled in a future release

- `httpsPort` : Specify the HTTPS port. By default, it uses 8443 as the listening port.

globalParameters

- `read.timeout`: Specifies how long the socket's `read()` or `recv()` operations while waiting for the incoming data before throwing a `SocketTimeoutException` error. Setting a timeout prevents the application from getting stuck indefinitely if no data is received or the connection is lost. The default is `300000` (5 minutes).
- `retry.count`: Specifies the maximum number of delivery retries for an undelivered message. The default is 5. When a delivery attempt fails, the message is forwarded to another connector within the same destination pool. This process repeats until the message is successfully delivered or until the specified `retry.count` limit is reached.
- `retry.delay`: Specifies the time in milliseconds before the delivery retry of an undelivered message. The default is 0.
- `batch.buffersize`: Specifies the maximum buffer size in bytes that can be used for the batch criteria. Load Balancer creates an event batch right before the total event size limit is reached.
- `batch.eventcount`: Specifies the total number of events that can be used as the batch cut-off criteria.
- `batch.timeout`: Specifies the timeout in milliseconds. A new batch will be created if the time reaches this value after the last batching and at least one event is waiting in the buffer.



Note: Load Balancer applies these three batch parameters together using whichever condition is met first.

- `trust.store.relative.location`: Specifies the location of the trust store as a relative path in relation to the Load Balancer installation. The default value is `jre/lib/security/`, which translates to, for example:
 `$ARCSIGHT_HOME/jre/lib/security`
- `trust.store.name`: Specifies the name of the trust store specified under `trust.store.relative.location`. The default location is `cacerts`, which internally translates to, for example:
 `$ARCSIGHT_HOME/jre/lib/security/cacerts` (using the trust store relative location.)
- `trust.store.password`: Specifies the password for the trust store.
- `destination.monitoring.interval.ms`: Specifies the time interval in milliseconds for the destinations being monitored. This applies to all destinations across all destination pools. The status and health information of the

destination is queried once every time interval. The default value is 60,000ms = 1 minute. It is not recommended to reduce this time period as excessive destination querying impairs Load Balancer's performance and SmartConnectors refresh this information once a minute.

- `weighted.interval.max`: Specifies the maximum time interval before re-calculating the load distribution for Weighted Round Robin mode. This should be at least a few times the target interval.
- `weighted.interval.target`: Specifies the ideal time interval before re-calculating the load distribution for Weighted Round Robin mode. As event rates through Load Balancer always vary slightly, this will not be an exact number.
- `aggregation.connector.event.ratio`: Specifies the ratio of EPS-to-queue rate below which sources will be reallocated away from a connector in Aggregation Preferred mode. This is specified as a ratio, for example, 0.9 to indicate 90%.
- `aggregation.connector.fail.periods`: Specifies the number of consecutive monitoring intervals in which a connector must fail the above check before action is taken in Aggregation Preferred mode to prevent transient issues from causing unneeded reallocations. Note that this is based on the statistics logger configuration, not `destination.monitoring.interval.ms`.
- `aggregation.reallocated.warn.ratio`: Specifies the ratio of the number of connectors that must be reallocated in Aggregation Preferred mode before a warning message is sent to the log file that says there is insufficient capacity. This is specified as a ratio, for example, 0.9 to indicate 90%.
- `aggregation.reallocation.max.ratio`: Specifies the maximum ratio of events from the previous monitoring interval to reallocate away from a connector in a single monitoring interval in Aggregation Preferred mode. This is specified as a ratio, for example, 0.9 to indicate 90%. Reallocation of sources continues until either this or the `aggregation.reallocation.max.sources` limit is reached, depending on which occurs first.
- `aggregation.reallocation.max.sources`: Specifies the maximum number of sources to reallocate away from a connector in a single monitoring interval in Aggregation Preferred mode. Reallocation of sources continues until either this or the `aggregation.reallocation.max.ratio` limit is reached, whichever occurs first.
- `queue.max.consumer`: (TCP only) Specifies the maximum queue size for the per event source buffer, before batches are created, as a number of events. If there are a number of sources each sending a small amount of events, this should be

somewhat low. If there are a few sources each sending a large amount of events, this should be somewhat high. Tune this to be roughly 1-2 seconds' worth of events, given the batching parameters and expected event rate. Note that these queues are usually nearly empty and are just to absorb load. Events that are in this queue are not persisted anywhere and will be lost if Load Balancer terminates unexpectedly. When this queue is full, no further events are read off of the socket, so event sources will experience TCP backpressure.

- `queue.max.producer`: Specifies the maximum queue size for the per destination asynchronous buffer as a number of batches (TCP) or events (UDP). While this buffer is full, TCP will buffer batches on disk up to `persistent.queue.disk.limit` bytes, and UDP will buffer events in memory up to the `udp.events.queue.capacity` value before starting to drop events. Events in this queue are still persisted on disk for TCP.
- `udp.consumer.threads`: Specifies the number of threads used to read UDP packets from the network.
- `tcp.consumer.threads`: Specifies the number of threads to use to dispatch TCP event batches. If files are appearing in the `$ARCSIGHT_HOME/user/loadbalancer/lbdata/persistence/RULE-NAME` directory faster than they are disappearing, consider increasing this value, up to the number of destinations in a single destination pool.
- `persistent.queue.disk.limit`: The maximum size, in bytes, of the persisted event batches for each TCP routing rule. This includes internal overhead, but not file system overhead. For example, if you have two TCP routing rules, you need at least two times this much disk space available, plus a margin for file system metadata and to account for block sizes. This should be at least 1073741824 (1 GiB), and must be at least twice the expected throughput per second.
- `persist`: Persist event batch on disk for TCP mode. Defaults to `true`. Disable to remove the disk as a bottleneck, but all events in-flight in Load Balancer will be lost if it is shut down.
- `load.expression.default`: Specifies custom load-level calculation expressions as a global default override for all destinations (excluding those which do not have their own per-destination expression.) For more information, see ["Calculating Loads for Routing" on page 88](#).
- `ssl.enabled.protocols`: Enabled TLS protocols. The default protocol is TLSv1.2.
- `ssl.cipher.suites`: Enabled cipher suites for TLS connections. The default value is: `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`.

- `ssl.keystore.password`: Password for the `ssl.keystore.file`. Note: The plaintext password is encrypted and persisted during the Load Balancer startup. The default is `changeit`.
- `ssl.key.password`: Password for the key in the `ssl.keystore.file`. Note: The plaintext password is encrypted and persisted during the Load Balancer startup. The default is `changeit`.
- `ssl.keystore.file`: Keystore file for remote management and TLS syslog listeners. If this file does not exist, it will be automatically created with the parameters described below, and also overwrite the `ssl.cert.file` with the newly generated certificate. This path is relative to `ARCSIGHT_HOME/user/loadbalancer`. The default is `loadbalancer.p12`.
- `ssl.cert.file`: Certificate file for remote management and TLS syslog listeners. If this file does not exist, it will be automatically created by exporting the certificate from `ssl.keystore.file`. This path is relative to `ARCSIGHT_HOME/user/loadbalancer`. The default is `loadbalancer.cer`.
- `ssl.cert.validity`: How long, in days, an automatically generated certificate should be valid. The default is 3650.
- `ssl.cert.key.size`: SSL key size, in bits. The default is: 2048.
- `ssl.cert.organization`: "O" (organization) field in the distinguished name ("DN") of an automatically generated certificate. The default is ArcSight.
- `ssl.cert.organizational.unit`: "OU" (organizational unit) field in the DN of an automatically generated certificate. The default is `loadbalancer`.
- `ssl.cert.locality`: "L" (locality/city) field in the DN of an automatically generated certificate. The default is NA.
- `ssl.cert.state`: "ST" (state) field in the DN of an automatically generated certificate. The default is NA.
- `ssl.cert.country`: "C" (state) field in the DN of an automatically generated certificate. The default is US.
- `reload.configuration`: Specifies whether the configuration can be reloaded from primary node in primary-secondary mode. You must set this value in the configuration file of the primary node. Do not modify this value in the secondary node.

To change the configuration in primary-secondary mode without downtime:

- a. Shut down the primary node.
- b. Set the value of `reload.configuration` to true.

- c. Modify the value of configuration.



Note: You can not modify the value of memberhosts.

- d. Start the primary node.
- **syslog.header.timestamp.ip:**
Specifies the regular expression to detect IP addresses in the event header. You can use this property only when the **syslog.address.prepend.mode** property is set to **scan**.
Load Balancer supports the IETF Standard (RFC 5424) syslog header. If the input log is not in this format, Load Balancer might not detect addresses properly. To workaround this issue, specify a regular expression with any of the following capturing groups that applies to your format:
 - 1st group: Captures time stamp
 - 2nd group: Captures Solaris style IP address ([1.1.1.1.1])
 - 3rd group: Captures non-Solaris style IP address
 - 4th group: Captures IPv6 address
 - 5th group: Captures the rest of the message

clusterconfigurations

hazelcast.max.no.heartbeat.seconds: Specifies the timeout interval in seconds, for a node to assume that it is not reachable. The default value is: 300 seconds. If any event loss is observed during the fail-over, you can reduce this timeout interval for a faster fail-over.

Example:

```
<hazelCastParameters>
<properties>
```

```
<property key="hazelcast.max.no.heartbeat.seconds" value="60"/>
</properties>
</hazelCastParameters>
```

Configuring Load Balancer in Standalone Mode

When Load Balancer runs in standalone mode, only one host is required.

To configure Load Balancer in standalone mode:

1. Log on to the host.
2. Go to \$ARCSIGHT_HOME/config/loadbalancer.
3. Copy the lbConfig.xml.template.standalone file to the \$ARCSIGHT_HOME/user/loadbalancer/ directory to configure Load Balancer to run in standalone mode.
4. Go to \$ARCSIGHT_HOME/user/loadbalancer directory and rename the file lbConfig.xml .
5. In the lbConfig.xml file, configure the host under the memberHost parameter.
 - a. List the host for Load Balancer.
 - b. Match "memberIdentity" on page 31 and the memberHosts/memberHost name so that Load Balancer can identify itself. See "Configuring MemberHosts in Standalone Mode" on page 18 for more information.
 - c. Set isPrimary=true.
6. Configure the routing and other parameters. Routing rules must be defined to have the events distributed from a source to a set of destinations (SmartConnectors). See "Syslog Load Balancing Routing Rule" on page 22 or "File Load Balancing Routing Rule" on page 26 for more information.
 - a. Configure destinations and destination pools.
 - b. Configure sources.

- c. Configure routing rules.
7. Configure the web server.



Note: The web server configuration settings must be configured. The function will be enabled in a future release for remote management. The value can be changed in the future, but a value must be entered to proceed.

8. Finish configuration. Refer to the [Configuration Parameters](#) and the [Sample Configuration File](#) for more information. Other optional configuration settings include:
 - Notification
 - Statistics Logging
9. Start the destination connectors before you start Load Balancer to ensure that Load Balancer can query the destinations for connector health and load.
10. Go to the `$ARCSIGHT_HOME` directory on the host and start Load Balancer.

```
# bin/arcsight loadbalancer
```



Note: If there are any configuration errors, Load Balancer will not start. Instead, it logs the configuration error messages at `logs/loadbalancer.log`. If this happens, fix the issue associated with the error message and start Load Balancer again.

Configuring Load Balancer in HA Mode

To configure Load Balancer to run in High Availability (HA) mode, first decide the type (peer or primary-secondary HA) and configure Ethernet file accordingly. (See "[Preparing to Install SmartConnectors](#)" on page 12.) Configure either the HA primary member host or the one that will be started first in peer mode with the full configuration in the XML configuration file. The secondary host (for primary-secondary configuration) or the passive host (for peer configuration) that starts second must be configured with the settings for member hosts and web service only. Other configuration settings will be synchronized when the second member host is started after the first member host.



Note: The host that starts first will overwrite the configuration file of the host that is started second. If the Load Balancer host with an incomplete configuration file is started first, the configuration can be lost. It is recommended to make a backup of the completed configuration file before starting Load Balancer.

To configure Load Balancer in HA mode:

1. Log on to the primary member host or the one where the Load Balancer will start first (for peer configuration).
2. Go to `$ARCSIGHT_HOME/config/loadbalancer`. Copy the `lbConfig.xml.template` file to the `$ARCSIGHT_HOME/user/loadbalancer/` directory if Load Balancer will be running in HA mode.
3. Go to `$ARCSIGHT_HOME/user/loadbalancer` directory and rename the file `lbConfig.xml`.
4. In the `lbConfig.xml` file, configure both participating member hosts and the routing rules.
 - a. List both participating member hosts for Load Balancer. (For security reasons, Load Balancer only communicates with known hosts using configured ports.)
 - b. Match up `memberIdentity` with one of `memberHosts/memberHost/name` so that Load Balancer can identify itself. See "["Configuring MemberHosts as Peer" on page 19](#)" and "["Configuring MemberHosts as Primary-Secondary" on page 20](#)" for more information.
 - c. For primary-secondary configuration, set `isPrimary=true` on the primary host. On the secondary host, set `isPrimary=false`.
 - d. For peer mode, set both hosts to `isPrimary=false`.
 - e. Refer to "["Configuration Parameters" on page 30](#)" to configure a secondary host and finish the host configuration.
5. Configure the routing and other parameters. Routing rules must be defined to have the events from a source be distributed to a set of destinations (SmartConnectors). See "["Syslog Load Balancing Routing Rule " on page 22](#)" or "["File Load Balancing Routing Rule " on page 26](#)" for more information.
 - a. Configure destinations and destination pools.
 - b. Configure sources.

- c. Configure routing rules.
6. Configure the web server.



Note: The web server configuration settings must be configured. The function will be enabled in a future release for remote management. The value can be changed in the future, but a value must be entered to proceed.

7. Finish optional configuration. Refer to the [Configuration Parameters](#) and the [Sample Configuration File](#) for more information. Other optional configuration settings include:
 - Notification
 - Statistics Logging
8. Log on to the second host and do the following:
 - a. Go to `$ARCSIGHT_HOME/config/loadbalancer` and copy the `lbConfig.xml.template` file to the `$ARCSIGHT_HOME/user/loadbalancer/` directory. Go to `$ARCSIGHT_HOME/user/loadbalancer` directory and rename the file `lbConfig.xml`.
 - b. Edit member hosts in the `lbConfig.xml` file. Make sure that `memberIdentity` is different from the one configured following step 4b.
 - c. The routing rule can be copied from the configuration file created in step 5 if preferred, but it is not required because the configuration values will be synchronized and persist after startup.



Note: If a firewall is enabled, Load Balancer member hosts may not be able to discover each other. The configured port in `memberHost` must be open. Also, the webserver needs to be configured to start Load Balancer.

9. Configure the firewall to open the ports on both hosts as needed to allow the two participating hosts to detect each other. Configure the firewall rule as needed. The configured ports include: `memberHosts/vipPingPort`, `memberHost/port` and all listening ports configured in `source` and `outbound` ports configured for destinations.
10. Start the destination connectors before you start Load Balancer to ensure that Load Balancer can query the destination for connector health and load.

11. Go to the \$ARCSIGHT_HOME directory on the primary or active host and start Load Balancer.

```
# bin/arcsight loadbalancer
```



Note: The virtual IP address is obtained by the host where Load Balancer is first started when Load Balancer is configured as peer. If Load Balancer is configured as primary-secondary, the virtual IP address will be used by the primary host.



Note: If there are any configuration errors, Load Balancer will not start. Instead, it logs the configuration error messages at logs/loadbalancer.log. If this happens, fix the issue associated with the error message and start Load Balancer again.

12. Log on to the secondary or passive host and start Load Balancer.

Configuring Syslog-based Load Balancing For TLS

In the destination definition of the lbConfig.xml file, change the protocol from tcp to tls. These are configurable per destination (listener).

Incoming events will be processed automatically, if a self-signed certificate is imported into any device sending events to the Load Balancer. Also, you must set up CA-signed certificates if you want to use HA Otherwise, you will have to import the certificate for both Load Balancers into all of the devices.

Using CA Signed Certificates

Load Balancer uses several digital, public-key certificates as part of establishing secure TLS communications. During the initial configuration of Load Balancer, these certificates are self-signed. In some circumstances, it might be necessary to obtain certificates digitally signed by a certificate authority (CA).

You can replace the self-signed certificate with a certificate signed by a well-known CA, such as VeriSign, Thawte, or Entrust. You can also replace the self-signed certificate with a certificate digitally signed by a less common CA, such as a CA within your company or organization.



Note: There are many well-known CAs and identifying the commonly used CAs varies with country.

Configuring TLS Certificates

This section provides instructions about configuring TLS certificates to get them digitally signed by a CA.

Before configuring the TLS Certificates, add the following global parameters in the **IbConfig.xml** file to select the certificate and keystore.

```
<globalParameters>
<properties>
<property key="ssl.cert.file" value="LBTLS.cer"/>
<property key="ssl.keystore.file" value="LB"/>
</properties>
</globalParameters>
```

Configuring the TLS certificates involves the following steps:

- "[Generating a Certificate Signing Request](#)" below
- "[Getting the CSR Signed by the CA](#)" on the next page
- "[Importing the Digitally Signed Certificates into Load Balancer](#)" on the next page

Configuring the Syslog NG Server

If the input source is Syslog NG server and you want to configure TLS with the CA-signed certificate enabled, you must add TLS function to the Syslog NG setup. For more information, refer to the *Add TLS Function to the Syslog NG Setup* section in the [SmartConnector for Syslog NG Daemon Configuration Guide](#).

Generating a Certificate Signing Request

To obtain a digitally signed certificate, you must first generate a certificate signing request (CSR) that is presented to the CA.

To generate one or more CSRs, perform the following steps on the Load Balancer server:

1. Log in to the Load Balancer server as the *root* user.
2. Create JKS Keystore and Keypair using the following command:

```
/root/ArcSightSCLoadBalancer/current/jre/bin/#./keytool -keystore  
/root/ArcSightSCLoadBalancer/current/user/loadbalancer/lbcert.jks -storepass changeit -genkeypair -  
alias mykeyX -keysize 2048 -keyalg RSA
```

The above command creates the **lbcert.jks** file. Enter the certificate subject information and then press **Enter** to use the same password used for the keystore password.

3. Generate the CSR by using the following command:

```
/root/ArcSightSCLoadBalancer/current/jre/bin/#./keytool -keystore  
/root/ArcSightSCLoadBalancer/current/user/loadbalancer/lbcert.jks -storepass changeit -certreq -alias  
mykeyX -file /root/ArcSightSCLoadBalancer/current/user/loadbalancer/lbreq.csr
```

Getting the CSR Signed by the CA

You should get the CSR signed by the CA.

To get the CSR signed by the CA:

1. Submit the CSRs to the CA for signature.
2. Obtain the signed certificate files from the CA.

The details of how this is done depend on the CA. For more information, consult your CA.

Importing the Digitally Signed Certificates into Load Balancer

This section provides instructions about importing the digitally signed certificates into Load Balancer. Copy the files that contain the digital certificates signed by the CA to the Load Balancer server. If the files are signed by an enterprise or organizational CA rather than a well-known CA, you must copy the CA's self-signed root certificate to the Load Balancer server.

You must import the intermediate, root, and signed certificates. You can specify the desired alias names for the intermediate and root certificates. However, the signed certificate must be imported with the same alias that was used while creating a certificate pair, which is webserver.

To import the certificate files to the Load Balancer server:

1. Log in to the Load Balancer server as the *root* user.
2. Back up the **loadbalancer.cer** file present at the following location:
`/root/ArcSightSCLoadBalancer/current/user/loadbalancer`
3. Import the trusted CA certificate:

```
/root/ArcSightSCLoadBalancer/current/jre/bin/#!/keytool -importcert -file  
/root/ArcSightSCLoadBalancer/current/user/loadbalancer/certnew.cer -storepass changeit -keystore  
/root/ArcSightSCLoadBalancer/current/user/loadbalancer/lbcert.jks
```

The CA certificate can be downloaded from the in-house CA server.

4. Import the signed certificate:
`/root/ArcSightSCLoadBalancer/current/jre/bin/#!/keytool -keystore
/root/ArcSightSCLoadBalancer/current/user/loadbalancer/lbcert.jks -storepass changeit -importcert -
alias mykeyX -file /root/ArcSightSCLoadBalancer/current/user/loadbalancer/certsign.cer`
5. Convert Keystore to P12 certificate:
`/root/ArcSightSCLoadBalancer/current/jre/bin/#!/keytool -importkeystore -srckeystore
/root/ArcSightSCLoadBalancer/current/user/loadbalancer/lbcert.jks -srcstorepass changeit -
deststorepass changeit -srcstoretype JKS -deststoretype PKCS12 -destkeystore
/root/ArcSightSCLoadBalancer/current/user/loadbalancer/LB.p12`
6. Copy the converted P12 certificate to the `.../current/user/agent` folder, where the destination connector is located.



Note: The default name of the P12 certificate is `remote_management.p12`.

- Import the certificate files to the Syslog Daemon connector using the following command:

```
/ArcSightSmartConnectors/current/jre/bin/#./keytool -importcert -file /tmp/certnew.cer -storepass  
changeit -alias mykey -keystore /root/ArcSightSmartConnectors/current/jre/lib/security/cacerts
```



Note: The Syslog Daemon connector can now send TLS events to Load Balancer.

- Restart Load Balancer.

The most common issues while using CA-signed certificate

- No trace of connection (even though the internal logs show connection attempts), network or firewall issues, an incorrectly configured destination, or unable to listen on IP address.
- When using new certificates, an incorrectly configured clock can cause problems. Ensure that the time or time zone in all the systems match.
- Ensure that the **Common Name** field is set to the correct FQDN or IP address. If you use FQDN, ensure that your DNS server works correctly.
- If the P12 certificates at Load Balancer and SmartConnector do not match, then the following exception occurs at SmartConnector:
`java.io.IOException: An existing connection was forcibly closed by the remote host`

Starting LoadBalancer

Start the LoadBalancer from the host that has been fully configured first (primary or active) to allow the configuration to correctly sync to the passive or secondary node. Otherwise, the configuration information will not be passed properly if the passive or secondary host is started first.

To start the LoadBalancer:

1. Go to the \$ARCSIGHT_HOME directory and start LoadBalancer with the following command:

```
# bin/arcsight loadbalancer
```
2. If you have a secondary machine, log in to the machine, then start LoadBalancer.



Note: In primary-secondary HA mode, if the secondary node starts before the primary node, the configuration will not be copied properly.

Running Load Balancer as a Service

To run Load Balancer as a service, the initial installation must be completed and there must be a working configuration file. Validate the working configuration file by running Load Balancer as a standalone application, as shown in "[Starting LoadBalancer](#)" above.

To install the files needed to run Load Balancer as a service:

1. Go to the \$ARCSIGHT_HOME directory and run the following command as root:

```
# bin/arcsight loadbalancer_service -i
```

This command installs the files necessary to run Load Balancer as a service.
2. Run the command without any switches to see the usage:

```
# bin/arcsight loadbalancer_service
ServiceTool - ArcSight SmartAgent Service Tool
Version : 1.0
Confidential commercial computer software. Valid license required.
Usage: ServiceTool <parameters>
Optional Parameters:
-sd <description> Service/Script description (Install only) (Load Balancer for Arcsight
SmartConnectors)
```

```
-sn <name> Service/Script name (Install only) (connlb)
```

Options:

```
-h help - Get help for this command
```

```
-i install - Installs the SmartConnectors LoadBalancer as a service
```

```
-r remove - Removes the SmartConnectors LoadBalancer Service
```



Note: If you are not the root user, an error message displays when invoking service tool:

```
# bin/arcsight loadbalancer_service
Assuming ARCSIGHT_HOME: /home/arcsight/beta1/current
Assuming JAVA_HOME: /home/arcsight-1/beta1/current/jre

ArcSight Load Balancer Service Tool starting...
*****
ERROR: This program should be run as [root]. Exiting...
*****
```

3. After the service `arc_connlb` is created, it can be accessed with service commands. For example:

```
# service arc_connlb status
```

```
Running as root
```

```
Output will be logged to $ARCSIGHT_HOME/current/logs/lb.out.wrapper.log
```

```
Getting status of ArcSight Load Balancer for Arcsight SmartConnectors...
```

```
ArcSight Load Balancer for Arcsight SmartConnectors is not running.
```

4. (Optional) To give the service a different name, use the `-sn` switch during service installation. The line below shows the service name changed to `arc_loadbalancer`. (The `arc_` is added before all services names.) If no other name is suggested, the default service name is '`connlb`' .

```
# bin/arcsight loadbalancer_service -sn loadbalancer -i
```

5. Use the `-sd` switch to give a different service description. For example, change the service description to 'LBService':

```
# bin/arcsight loadbalancer_service -i -sd LBService
```

6. Using the service description change shown step 5, the status command displays as follows:

```
# service arc_connlb status
```

Running as root

Output will be logged to \$ARCSIGHT_HOME/current/logs/lb.out.wrapper.log

Getting status of ArcSight LBService...

ArcSight LBService is not running.

7. To remove the service files, use the following command:

```
# bin/arcsight loadbalancer_service -r
```

Load Balancer Service Commands

Other commands available when running Load Balancer as a service include:

- start — Starts Load Balancer as a service.
- stop — Stops Load Balancer as a service.
- restart — Stops the service, if it's running, then restarts it.
- dump — Captures the current JVM state including all the running threads and their states. The output will be present in `lb.out.wrapper.log`. The Load Balancer service continues to run normally after the dump. This command needs Load Balancer to be running or the command will have no effect.
- console — Runs the Load Balancer service as an application from the current window, which can be stopped with a `Ctrl + c` or with the `stop service` command from another window. The log will be displayed on the console.

Usage is displayed if no command is given. For example:

```
# service arc_connlb
```

Running as root

Output will be logged to \$ARCSIGHT_HOME/current/logs/lb.out.wrapper.log

Usage: \$ARCSIGHT_HOME/current/bin/lb.wrapper.sh { start | stop | restart | dump | status | console }

Starting or Stopping the Load Balancer Service

After you have installed Load Balancer as a service, you can start or stop the service at any time. You are expected to be a `root` user to run Load Balancer as a service.

To start or stop the Load Balancer service:



Note: Only root users can run Load Balancer as a service.

1. To start the Load Balancer service, use the following command:

```
# /etc/init.d/arc_connlb start
```

or

```
service arc_connlb start
```



Note: If you changed the default service name (connlb), use that name in place of ‘connlb’.

2. To stop the Load Balancer service, use the following command:

```
# /etc/init.d/arc_connlb stop
```

or

```
service arc_connlb stop
```

Load Balancer Service-related Logs

The log will be redirected to `lb.out.wrapper.log` under the `logs` directory.

Upgrading Load Balancer

Perform the following steps to upgrade to Load Balancer CE 25.1:

1. Download Load Balancer CE 25.1 from the [Support website](#).
 2. Stop Load Balancer. If running in High Availability (HA) mode, stop Load Balancer on both hosts.
-
- Note:** OpenText does not support running mismatched versions of Load Balancer during the upgrade.
3. Install Load Balancer CE 25.1 in the same directory where you had the previous version installed. It will create a new directory for the current version.
 4. If Load Balancer is running in HA mode, repeat the installation steps on the other host.
 5. Start Load Balancer. If running in HA mode, start the primary instance first.
- ## Uninstalling Load Balancer
- Load Balancer can be uninstalled using the GUI or console mode.
- Load Balancer Service-related Logs
- Page 59 of 112

To uninstall Load Balancer in GUI mode:

1. Run the `./Uninstall_ArcSightSmartConnectorLBscript` in the `$ARCSIGHT_HOME/current/UninstallerData` folder to launch the GUI uninstaller. For example:

```
./Uninstall_ArcSightSmartConnectorLB -i swing
```

2. Follow the screen prompts.

To uninstall Load Balancer in console mode:

1. Run the `./Uninstall_ArcSightSmartConnectorLB -console` command to uninstall Load Balancer in console mode. For example:

```
./Uninstall_ArcSightSmartConnectorLB -i console
```

2. Add '`-i silent`' to launch the silent mode installation.

Load Balancer REST API

Load Balancer provides an Application Programming Interface (API) for programmatic access to Load Balancer resources. You can use Standard APIs to configure Load Balancer.

Configuration

This section describes how to configure Load Balancer using Rest API.

The following configurations must be done in the same sequence:

1. Source
2. Destination
3. Destination pools
4. Routing rules

When Load Balancer is configured to run in HA mode, you can execute REST APIs either using the virtual IP or the actual IP address of the primary/active node. Requests to the secondary/standby node will not be successful.

The following element is unique to each node. You must add it to both primary and secondary nodes.

```
<webServer httpsPort="8443" certificatePath="config/loadbalancer.cer"
keystorePath="config/loadbalancer.p12"/>
```

The following values used in this element are relative to ARCSIGHT_HOME:

- **certificatePath:** Location of the certificate file.
- **keystorePath:** Location of the keystore file.

Load Balancer API Reference

Retrieving a List of Routing Rules

This method displays all the routing rules.

API Reference	GET /config/routingRules
Sample Request	URI: GET https://127.0.0.1:8443/config/routingRules

Sample Response	<p>Success Code: 200 (OK)</p> <p>Body:</p> <pre>[{ "name": "syslog-tcp-rule", "sourceName": "syslog-tcp", "destinationPoolName": "tcp-syslog-connectors", "routingPolicy": "RoundRobin", "enabled": true, "additionalParameters": { "type": "listener", "properties": { "property": [{ "key": "syslog.address.prepend.mode", "value": "scan" }] } } }, { "name": "syslog-udp-rule", "sourceName": "syslog-udp", "destinationPoolName": "udp-syslog-connectors", "routingPolicy": "WeightedRoundRobin", "enabled": true }]</pre>
------------------------	--

Retrieving Details of a Routing Rule

This method displays details of the selected routing rule.

API Reference	GET /config/routingrules/routingrule/<name of the routing rule>
Sample Request	URI: GET https://127.0.0.1:8443/config/routingrules/routingrule/syslog-tcp-rule

Sample Response	<p>Status: 200 (OK)</p> <p>Body:</p> <pre>{ "name": "syslog-tcp-rule", "sourceName": "syslog-tcp", "destinationPoolName": "tcp-syslog-connectors", "routingPolicy": "RoundRobin", "enabled": true, "additionalParameters": { "type": "listener", "properties": { "property": [{ "key": "syslog.address.prepend.mode", "value": "scan" }] } } }</pre>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Routing rule not found, routing rule=[syslog-tcp-rule-non-existent]" }]</pre> <p>Reason: This error occurs when you try to retrieve a routing rule that is not present.</p>

Creating a Routing Rule

This method adds a new routing rule.

API Reference	POST /config/routingrules/routingrule
Content-Type	application/json

Sample Request	<p>URI: POST <code>https://127.0.0.1:8443/config/routingrules/routingrule</code></p> <p>Body:</p> <pre>{ "name": "syslog-udp-rule", "sourceName": "syslog-udp", "destinationPoolName": "udp-syslog-connectors", "routingPolicy": "WeightedRoundRobin", "enabled": false }</pre>
Sample Response	<p>Status: 201 (Created)</p> <p>Body:</p> <pre>{ "name": "syslog-udp-rule", "sourceName": "syslog-udp", "destinationPoolName": "udp-syslog-connectors", "routingPolicy": "WeightedRoundRobin", "enabled": false }</pre>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Routing rule not found, routing rule=[syslog-tcp-rule-non-existent]" }]</pre> <p>Reason: This error occurs when the routing rule in the request contains a source name that is already referred by some other routing rule.</p>

Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "description": "Duplicate name found for Routing Rule=[syslog-tcp-rule]", "errorSource": "Configuration" }]</pre> <p>Reason: This error occurs when the routing rule in the request contains a name that is already present in some other routing rule.</p>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "description": "Destination pool undefined: routing rule=[syslog-udp-rule], destination pool=[udp-syslog-connectors]", "errorSource": "Configuration" }]</pre> <p>Reason: This error occurs when the destination pool mentioned in the request is not present in lbConfig.xml.</p>

Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration" "description": "UDP Sources or destinations may only be used with other UDP sources and destinations: Routing Rule=[syslog-tcp-rule2]" }]</pre> <p>Reason: This error occurs when the protocol of the source is not similar to the protocol of the destination used in the destination pool of the request.</p>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ Can not construct instance of com.arcsight.lb.bean.RoutingPolicy from String value 'WeightedRoundRobin-NoExist': value not one of declared Enum instance names: [RoundRobin, AggregationPreferred, WeightedRoundRobin] at [Source: org.glassfish.jersey.message.internal.ReaderInterceptorExecutor\$UnCloseableInputStream @66ee8a07; line: 7, column: 47] (through reference chain: com.arcsight.lb.bean.RoutingRule["routingPolicy"]) }]</pre> <p>Reason: This error occurs when the routing policy mentioned in the request is not one these: RoundRobin, AggregationPreferred, and WeightedRoundRobin.</p>

Deleting a Routing Rule

This method deletes the selected routing rule.

API Reference	DELETE /config/routingrules/routingrule/<name of the routing rule to be deleted>
Sample Request	<p>URI: DELETE https://127.0.0.1:8443/config/routingrules/routingrule/syslog-udp-rule1</p>

Sample Response	<p>Status: 200 (OK)</p> <p>Body:</p> <pre>{ "name": "syslog-udp-rule", "sourceName": "syslog-udp", "destinationPoolName": "udp-syslog-connectors", "routingPolicy": "WeightedRoundRobin", "enabled": false }</pre>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Routing rule not found, routing rule=[syslog-udp-rule1]" }]</pre> <p>Reason: This error occurs when you try to delete a routing rule that is not present.</p>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Routing rule cannot be deleted while it is enabled, routing rule=[syslog-tcp-rule]" }]</pre> <p>Reason: This error occurs when you try to delete a routing rule that is in the enabled state.</p>

Enabling a Routing Rule

This method enables the selected routing rule.

API Reference	PUT /config/routingrules/routingrule/<name of the rule to be enabled>/enable
Sample Request	URI: PUT https://127.0.0.1:8443/config/routingrules/routingrule/syslog-udp-rule/enable

Sample Response	<p>Status: 200 (OK)</p> <p>Body:</p> <pre>{ "name": "syslog-udp-rule", "sourceName": "syslog-udp", "destinationPoolName": "udp-syslog-connectors", "routingPolicy": "WeightedRoundRobin", "enabled": false }</pre>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Routing rule is already Enabled: routing rule=[syslog-udp-rule]" }]</pre> <p>Reason: This error occurs when you try to enable a routing rule that is in the enabled state.</p>

Disabling a Routing Rule

This method disable the selected routing rule.

API Reference	PUT /config/routingrules/routingrule/<name of the rule to be disabled>/disable
Sample Request	URI: PUT https://127.0.0.1:8443/config/routingrules/routingrule/syslog-udp-rule/disable
Sample Response	<p>Status: 200 (OK)</p> <p>Body:</p> <pre>{ "name": "syslog-udp-rule", "sourceName": "syslog-udp", "destinationPoolName": "udp-syslog-connectors", "routingPolicy": "WeightedRoundRobin", "enabled": true }</pre>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Routing rule is already disabled: routing rule=[syslog-udp-rule]" }]</pre> <p>Reason: This error occurs when you try to disable a routing rule that is already in the disabled state.</p>

Retrieving a List of Sources

This method displays all the sources.

API Reference	GET /config/sources
Sample Request	URI: GET https://127.0.0.1:8443/config/sources
Sample Response	<p>Success Code: 200 (OK)</p> <p>Body:</p> <pre>[{ "name": "syslog-tcp", "type": "SYSLOG", "protocol": "tcp", "port": 512 }, { "name": "syslog-udp", "type": "SYSLOG", "protocol": "udp", "port": 513 }]</pre>

Retrieving Details of a Source

This method displays details of the selected source.

API Reference	GET /config/sources/source/<name of the source>
Sample Request	URI: GET https://127.0.0.1:8443/config/sources/source/syslog-tcp
Sample Response	<p>Success Code: 200 (OK)</p> <p>Body:</p> <pre>{ "name": "syslog-tcp", "type": "SYSLOG", "protocol": "tcp", "port": 512 }</pre>

Creating a Source

This method adds a new source.

API Reference	POST /config/sources/source
Content-Type	application/json
Sample Request	URI: POST https://127.0.0.1:8443/config/sources/source Body: <pre>{"name": "syslog-tcp", "type": "SYSLOG", "protocol": "tcp", "port": 512}</pre>
Sample Response	Status: 201 (Created) Body: <pre>{"name": "syslog-tcp", "type": "SYSLOG", "protocol": "tcp", "port": 512}</pre>

Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Duplicate name found for Source=[syslog-tcp]" }, { "errorSource": "Configuration", "description": "Duplicate port found from Source=[syslog-tcp]: Port=[512]" }]</pre> <p>Reason: This error occurs when the source already exists and some other source has already used the port provided in the request.</p>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Duplicate port found from Source=[syslog-tcp2]: Port=[512]" }]</pre> <p>Reason: This error occurs when the port mentioned in a new source is already associated with an existing source.</p>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>Can not construct instance of com.arcsight.lb.bean.EndPointType from String value 'syslog': value not one of declared Enum instance names: [FILE, SYSLOG, URI]</pre> <pre>at [Source: org.glassfish.jersey.message.internal.ReaderInterceptorExecutor\$UnCloseableInputStream@160485; line: 2, column: 22] (through reference chain: com.arcsight.lb.bean.AdaptedEndPoint["type"])</pre> <p>Reason: This error occurs when the value of the field <code>type</code> is incorrect.</p>

Deleting a Source

This method deletes the selected source.

API Reference	DELETE /config/sources/source/<name of the source>
Sample Request	URI: DELETE https://127.0.0.1:8443/config/sources/source/syslog-tcp

Sample Response	<p>Status: 200 (OK)</p> <p>Body:</p> <pre>{ "name": "syslog-tcp", "type": "SYSLOG", "protocol": "tcp", "port": 512 }</pre>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "The source=[syslog-tcp] is being referenced by Routing Rule=[[syslog-tcp-rule]]" }]</pre> <p>Reason: This error occurs when the source you are trying to delete is referenced by an existing routing rule.</p>

Retrieving a List of Destinations

This method displays all the destinations.

API Reference	GET /config/destinations
Sample Request	URI: GET https://127.0.0.1:8443/config/destinations

Sample Response	<p>Success Code: 200 (OK)</p> <p>Body:</p> <pre>[{ "name": "syslog-tcp-connector-1", "type": "SYSLOG", "host": "10.0.0.0", "protocol": "tcp", "additionalParameters": { "type": "connector", "properties": { "property": [{ "key": "remote.management.listener.port", "value": "9001" }] } }, "port": 514 }, { "name": "syslog-udp-connector-1", "type": "SYSLOG", "host": "10.0.0.0", "protocol": "udp", "additionalParameters": { "type": "connector", "properties": { "property": [{ "key": "remote.management.listener.port", "value": "9001" }] } }, "port": 514 }</pre>
------------------------	--

	}
]

Retrieving Details of a Destination

This method displays details of the selected destination.

API Reference	GET /config/destinations/destination/<destination-name>
Sample Request	URI: GET https://127.0.0.1:8443/config/destinations/destination/syslog-tcp-connector-1

Sample Response	<p>Status: 200 (OK)</p> <p>Body:</p> <pre>{ "name": "syslog-tcp-connector-1", "type": "SYSLOG", "host": "10.0.0.0", "protocol": "tcp", "additionalParameters": { "type": "connector", "properties": { "property": [{ "key": "remote.management.listener.port", "value": "9001" }] } }, "port": 514 }</pre>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Destination not found, destination=[syslog-tcp-connector-2]" }]</pre> <p>Reason: This error occurs when you try to retrieve a destination that is not present.</p>

Creating a Destination

This method adds a new destination.

API Reference	POST /config/destinations/destination
Content-Type	application/json

Sample Request	URI: POST https://127.0.0.1:8443/config/destinations/destination Body: <pre>{ "name": "syslog-udp-connector-1", "type": "SYSLOG", "host": "10.0.0.0", "protocol": "udp", "additionalParameters": { "type": "connector", "properties": { "property": [{ "key": "remote.management.listener.port", "value": "9001" }] }, "port": 514 } }</pre>
-----------------------	--

Sample Response	<p>Status: 201 (Created)</p> <p>Body:</p> <pre>{ "name": "syslog-udp-connector-1", "type": "SYSLOG", "host": "10.0.0.0", "protocol": "udp", "additionalParameters": { "type": "connector", "properties": { "property": [{ "key": "remote.management.listener.port", "value": "9001" }] } }, "port": 514 }</pre>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Duplicate name found for Destination=[syslog-tcp-connector-1]" }]</pre> <p>Reason: This error occurs when an existing destination is already using the name of the destination in the request.</p>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Duplicate hostname, port and protocol found for Destination=[syslog-tcp-connector-3]: Hostname=[10.0.0.0], Port=[514]" }]</pre> <p>Reason: This error occurs when the combination of hostname, port, and protocol used in a new request is similar to an existing destination.</p>

Deleting a Destination

This method deletes the selected destination.

API Reference	DELETE /config/destinations/destination/<name of the destination to be deleted>
Sample Request	URI: DELETE <code>https://127.0.0.1:8443//config/destinations/destination/syslog-udp-connector-1</code>
Sample Response	Status: 200 (OK) Body: <pre>{ "name": "syslog-udp-connector-1", "type": "SYSLOG", "host": "10.0.0.0", "protocol": "udp", "additionalParameters": { "type": "connector", "properties": { "property": [{ "key": "remote.management.listener.port", "value": "9001" }] } }, "port": 514 }</pre>
Error Code	Status: 400 (Bad Request) Body: <pre>[{ "errorSource": "Configuration", "description": "Destination not found, destination=[syslog-udp-connector-1]" }]</pre> Reason: This error occurs when the destination that you are trying to delete is not present.
Error Code	Status: 400 (Bad Request) Body: <pre>[{ "errorSource": "Configuration", "description": "The destination=[SYSLOG-TCP-CONNECTOR-1] is being referenced by one or more Destination Pools=[[syslog-tcp-connectors]]." }]</pre> Reason: This error occurs when the destination you are trying to delete is present in a destination pool.

Retrieving a List of Destination Pools

This method displays all the destination pools.

API Reference	GET /config/destinationpools
Sample Request	URI: GET <code>https://127.0.0.1:8443/config/destinationpools</code>

Sample Response	Success Code: 200 (OK) Body: <pre>[{ "name": "syslog-tcp-connectors", "destinations": "syslog-tcp-connector-1,syslog-tcp-connector-2" }, { "name": "syslog-tcp-connectors2", "destinations": "syslog-tcp-connector-1" }]</pre>
------------------------	---

Retrieving Details of a Destination Pool

This method displays details of the selected destination.

API Reference	GET /config/destinationpools/destinationpool/<name of the destination pool>
Sample Request	URI: GET https://127.0.0.1:8443//config/destinationpools/destinationpool/tcp-syslog-connectors
Sample Response	Status: 200 (OK) Body: <pre>{ "name": "syslog-tcp-connectors", "destinations": "syslog-tcp-connector-1" }</pre>
Error Code	Status: 400 (Bad Request) Body: <pre>[{ "errorSource": "Configuration", "description": "Destination pool not found, destination pool=[tcp-syslog-connectors-non-existent]" }]</pre> <p>Reason: This error occurs when you try to retrieve a destination pool that is not present.</p>

Creating a Destination Pool

This method adds a new destination pool.

API Reference	POST /config/destinationpools/destinationpool
Content-Type	application/json
Sample Request	URI: POST https://127.0.0.1:8443/config/destinationpools/destinationpool Body: <pre>{ "name": "syslog-udp-connectors", "destinations": "syslog-udp-connector-1" }</pre>
Sample Response	Status: 201 (Created) Body: <pre>{ "name": "syslog-udp-connectors", "destinations": "syslog-udp-connector-1" }</pre>

Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Duplicate name found for Destination Pool=[syslog-tcp-connectors]" }</pre> <p>Reason: This error occurs when the name of the destination pool you are trying to create is already present for some other destination pool.</p>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Undefined or invalid destination found for Destination Pool=[syslog-udp-connectors]: Destination=[syslog-udp-connector-1]" }, { "errorSource": "Configuration", "description": "Found undefined Destination=[syslog-udp-connector-1]" }]</pre> <p>Reason: This error occurs when the destination mentioned in the request is not present.</p>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Destinations in destination pool should be of the same protocol: Destination Pool=[syslog-udp-connectors]" }</pre> <p>Reason: This error occurs when the destinations' protocols present in the request are not same.</p>

Deleting a Destination Pool

This method deletes the selected destination pool.

API Reference	DELETE /config/destinationpools/destinationpool/<name of the destination pool to be deleted>
Sample Request	URI: DELETE <code>https://127.0.0.1:8443/config/destinationpools/destinationpool/syslog-udp-connectors</code>
Sample Response	Status: 200 (OK) Body: <pre>{ "name": "syslog-udp-connectors", "destinations": "syslog-udp-connector-1" }</pre>
Error Code	Status: 400 (Bad Request) Body: <pre>[{ "errorSource": "Configuration", "description": "Destination pool not found, destination pool=[syslog-udp-connectors1]" }]</pre> Reason: This error occurs when you try to delete a destination pool that is not present.

Adding a Destination to a Destination Pool

This method adds a destination to a destination pool.

API Reference	PUT /config/destinationpools/destinationpool/<name of the destination pool>/add/<name of the destination to be deleted>
Sample Request	URI: PUT <code>https://127.0.0.1:8443/config/destinationpools/destinationpool/syslog-tcp-connectors/add/syslog-tcp-connector-2</code>

Sample Response	<p>Status: 200 (OK)</p> <p>Body:</p> <pre>{ "name": "syslog-tcp-connectors", "destinations": "syslog-tcp-connector-1,syslog-tcp-connector-2" }</pre>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Duplicate destination found from the destination pool: destination pool=[syslog-tcp-connectors], destination=[syslog-tcp-connector-1]" }]</pre> <p>Reason: This error occurs when the destination pool already contains the destination you are trying to insert.</p>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "Destinations in destination pool must be of the same protocol: destination pool=[syslog-tcp-connectors], destination=[syslog-udp-connector-1], expected protocol=[tcp]" }]</pre> <p>Reason: This error occurs when the destination you are trying to insert uses a different protocol than that of the existing destination in the same destination pool.</p>
Error Code	<p>Status: 400 (Bad Request)</p> <p>Body:</p> <pre>[{ "errorSource": "Configuration", "description": "No such destination pool found: destination pool=[destination-pool-1]" }]</pre> <p>Reason: This error occurs when the destination pool is not present.</p>

Deleting a Destination From a Destination Pool

This method deletes a destination in a destination pool.

API Reference	DELETE /config/destinationpools/destinationpool/<name of the destination pool>/delete/<name of the destination to be deleted>
Sample Request	URI: DELETE <code>https://127.0.0.1:8443/config/destinationpools/destinationpool/syslog-tcp-connectors/delete/syslog-tcp-connector-1</code>
Sample Response	Status: 200 (OK) Body: <pre>{ "name": "syslog-tcp-connectors", "destinations": "" }</pre>
Error Code	Status: 400 (Bad Request) Body: <pre>[{ "errorSource": "Configuration", "description": "No such destination pool found: destination pool=[destination-pool-1]" }]</pre> Reason: This error occurs when the destination pool is not present.
Error Code	Status: 400 (Bad Request) Body: <pre>[{ "errorSource": "Configuration", "description": "Configuration is not synchronized: destination pool=[syslog-tcp-connectors], destination=[destination-1]" }]</pre> Reason: This error occurs when the destination is not present.

REST API Common Errors

Following are the REST API common errors for Load Balancer:

Error Messages	
1	<ul style="list-style-type: none"> • Status: 401 (Unauthorized) • Body: [{"errorSource": "Configuration", "description": "Operation not supported for non-active primary node"}] • Description: This error occurs when you call REST API using the IP address of the node that was not active during the time of the call.
2	<ul style="list-style-type: none"> • Status: 405 (Method not allowed) • Body: NA • Description: This error occurs when you do not pass the expected method type.
3	<ul style="list-style-type: none"> • Status: 400 (Bad Request) • Body: Unexpected character (''') (code 34)): was expecting comma to separate OBJECT entries at [Source:org.glassfish.jersey.message.internal.ReaderInterceptorExecutor\$UnCloseableInputStream@1a27bdb2; line: 9, column: 10] (through reference chain: com.arcsight.lb.bean.RoutingRule["additionalParameters"]) • Description: This error occurs when a comma is missing between two fields in the JSON object of the request body.
4	<ul style="list-style-type: none"> • Status: 404 (Not Found) • Body: NA • Description: This error occurs when the API name present in the URI is invalid.
5	<ul style="list-style-type: none"> • Status: NA • Body: No response or could not get any response. • Description: This error occurs when the IP address or the hostname or the port number in the URI is not correct.

Load Balancer Troubleshooting

This chapter contains information about troubleshooting for common issues.

Interpreting Logs

Statistics are divided by:

- Routing rule—each rule is on its own line
- Locations—from sources or to destinations
- Metrics—bytes, events, and batches
- Time units—average per second SLC, total SLC, and total since startup

For each routing rule, the combined totals from every source are listed first, followed by the combined totals to every destination, and the individual statistics per destination.

Overall statistics:

```
2015-08-24 08:43:25,556 [INFO][statisticsLogging][com.arcsight.lb.stats.StatLoggingTask][run] - Load  
Balancer statistics {metric=average per second-SLC/SLC/Total}:  
  
2015-08-24 08:43:25,557 [INFO][statisticsLogging][com.arcsight.lb.stats.StatLoggingTask][run] - Routing  
rule=[syslog-tcp-rule-1]: [src=  
(total),bytesRcvd=1636923/16369232/188733127,eventsRcvd=10000/100000/1153000,batchesRcvd=10/  
100/1153], [dest=  
(total),bytesSent=1636923/16369232/196591275,eventsSent=10000/100000/1201000,batchesSent=10/  
100/1201],[dest=tcp-syslog-  
1,bytesSent=818452/8184521/98377554,eventsSent=5000/50000/601000,batchesSent=5/50/601],  
[dest=tcp-syslog-  
2,bytesSent=818471/8184711/98213721,eventsSent=5000/50000/600000,batchesSent=5/50/600]]  
  
2015-08-24 08:43:25,557 [INFO][statisticsLogging][com.arcsight.lb.stats.StatLoggingTask][run] - Routing  
rule=[syslog-tcp-rule-1]: In: EPS=[10000] Bytes/s=[1636923] Out: EPS=[10000] Bytes/s=[1636923]
```

Load Calculators Not Initialized or Destination Monitoring Not Working

Issue: Load calculators are not initialized and destination monitoring is not working, but the certificate import is fine.

```
2015-07-02 12:16:39,266 [ERROR][com.arcsight.lb.b.b][intialize] - Please check the credentials for  
Connector tcp-syslog-connector-12 Error Message ; nested exception is:
```

```
java.net.ConnectException: Connection refused]
```

```
2015-07-02 12:16:39,266 [ERROR][com.arcsight.lb.b.c][initDestinationLoadCalculator] - Failed to initialize  
Load Calculator for the destination [tcp-syslog-connector-12]
```

Answer: This problem can be resolved by:

1. Verifying that connector can be managed remotely by checking the value of `remote.management.enabled` in the `agent.properties` file. This value should be set to `true`.
2. Verifying that the `destination/additionalParameters/properties/property@remote.m anagement.listener.port` matches the value of `remote.management.listener.port`.

Destination Configured with SCP Protocol but File Delivery Fails

Issue: Load Balancer cannot successfully log into the destination host with SCP.

Answer: It may log an exception. There are several possible reason for this error:

- `knownHostsFile` is not specified in the `lbConfig.xml` configuration file.
- `knownHostsFile` is configured, but the host key for this specific host was not found.
- `knownHostsFile` is configured and the host key was found, but the algorithm generated for the host key is neither RSA nor DSA. Currently Load Balancer supports only these two types of algorithms. If the host is configured to use another algorithm in generating a host key, regenerate the host key using one of the accepted algorithms.

Sources Relocated Away from [x] of [y] Destinations in Routing Rule

Issue: "Sources were reallocated away from [x] of [y] destinations in the routing rule [my-routing-rule]. You may wish to add more destinations" displays even though the "There was no incoming data" error message is being displayed.

Answer: The destination overloaded message is triggered by examining the Connector's internal statistics, regardless of the traffic that Load Balancer is sending it. It is therefore possible for a connector to be deemed overloaded even though Load Balancer has not yet sent it any traffic.

Warning Message in Passive or Secondary Node Logs

Issue: When Load Balancer is configured to run in HA mode, it continuously displays the following warning message in passive or secondary node logs:
"VIP is unreachable and will bind the VIP to this host"

Answer: Perform the following steps to stop this warning message:

1. Shut down the Ethernet services for the passive or secondary node by using the following command:
`/sbin/ifdown /etc/sysconfig/network-scripts/ifcfg-ens192:1`
2. Restart the Network Service for the passive or secondary node by using the following command:
`systemctl restart network`

Calculating Loads for Routing

Issue: The metrics used to calculate SmartConnector loads do not represent the actual load of the SmartConnectors, and result in incorrect distribution of events.

Answer: Use a custom expression to set custom load-level calculation expressions for Weighted Round Robin and Aggregation Preferred routing policies, both as a global default and as per-destination overrides.

- For all destinations (excluding those which do not have their own expression,) configure `load.expression.default` in the `globalParameters` block.
- For only a specific destination, configure `load.expression` in the `additionalParameters` block. This overrides `load.expression.default`. Per-destination expressions can be used to favor certain destinations over others. Weaker destinations can be pre-favored to be less utilized by having a large constant value added or multiplied to their load.
- If neither are provided, the existing behavior is used.



Note: To specify a non-integer constant value (for example, 1.5), division must be used (for example, $3/2$), as using a `.` period is prohibited. Otherwise, normal operators and precedence rules apply. Higher return values indicate higher loads. There is no maximum value; values are automatically scaled relative to other load values. Negative values should not be used.

The following case-sensitive variables are available:

Variable Name	Data Type	Description
eps	float	Average events per second over a one-minute period.
queueRate	float	Queue rate over a one-minute period, if file queues are enabled.
queueDropsTotal	float	Total queue drops since the Connector started, if file queues are enabled.
queueDrops	float	Queue drops over a one-minute period, if file queues are enabled. This is calculated locally at the Load Balancer, and may erroneously read 0 if the Connector returns the same counter snapshot multiple times.
cpuLoad	int	Only available for Linux Connectors. The aggregate percentage of CPU time that was not idle, over a one-minute period, as an integer 0-100. (On non-Linux connectors, this will be -1.) *See further notes below.
memUsed	int	The instantaneous amount of memory (in megabytes) used by the heap when statistics were collected. This includes objects eligible for garbage collection, so may be significantly higher than is actually the case.
memTotal	int	The maximum size of the heap (in megabytes).



Note: About the cpuLoad variable:

- This variable is only available for connectors running on Linux. It is only updated every 60 seconds by default, regardless of how often Load Balancer is polling. This is the average level for the entire period of time since the last polling interval. This value may be underreported for virtualized connectors or connectors with heavy disk traffic.
- This variable includes all CPUs (and cores, and hardware threads) added together. For example, if the connector machine has a total of 4 hardware threads (1 socket, 2 cores, with 2 hardware threads per core), and only one hardware thread is at 100% usage while the other 3 are at 0% usage, this will be reported as 25% load. There is no way to distinguish this from all 4 hardware threads being at 25% load.
- To use Linux destinations based solely on CPU load, unless they are dropping events from their queue, use: `cpuLoad + queueDrops * 100`

Appendix

Configuration templates exist for standalone and HA configurations. For more information, see the callouts within the files .

This section includes the following topics:

Sample Configuration File

The following example shows the Load Balancer configuration file configured for syslog load balancing. The template provided by Load Balancer is shown in Appendix.



Note: This is a sample configuration file with passwords obfuscated since it was captured after Load Balancer started.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>

<lbConfiguration>
    <memberHosts ipAddress="10.0.0.0" vipPingPort="9090">
        <memberHost name="primary-node" host="10.0.0.0" port="7701"
isPrimary="false" vipBindCommand="sudo /sbin/ifup /etc/sysconfig/network-
scripts/ifcfg-eth0:1" vipUnbindCommand="sudo /sbin/ifdown
/etc/sysconfig/network-scripts/ifcfg-eth0:1" />
        <memberHost name="secondary-node" host="10.0.0.0" port="7701"
isPrimary="false" vipBindCommand="/sbin/ifup /etc/sysconfig/network-
scripts/ifcfg-eth0:1" vipUnbindCommand="/sbin/ifdown/etc/sysconfig/network-
scripts/ifcfg-eth0:1" />
    </memberHosts>
    <memberIdentity>primary-node</memberIdentity>
    <notification enable="true">
        <enabledNotification>
            <event name="MemberHostUp" message="Member node is up" />
            <event name="MemberHostDown" message="Member node is down" />
            <event name="DestinationUp" message="Destination is up" />
            <event name="DestinationDown" message="Destination is down" />
        </enabledNotification>
        <email>
            <prefix>[Load Balancer]</prefix>
            <recipients>nanjoo.ban@abc.com</recipients>
            <sender>nanjoo.ban@abc.com</sender>
            <smtpServer>englab-mail.arst.usa.abc.com</smtpServer>
        </email>
    </notification>
    <routing>
        <destinationPools>
            <destinationPool name="tcp-syslog-connectors" destinations="tcp-
syslog-1,tcp-syslog-2" />
            <destinationPool name="bc-file-connectors" destinations="bc-
connector-1,bc-connector-2" />
            <destinationPool name="netflow-connectors" destinations="netflow-
connector" />
        </destinationPools>
    </routing>
</lbConfiguration>
```

```
<destinations>
    <destination name="tcp-syslog-1" type="syslog" host="10.0.0.0"
port="8514" protocol="tcp">
        <additionalParameters type="connector">
            <properties>
                <property key="remote.management.listener.port" value="9001"
/>
            </properties>
        </additionalParameters>
    </destination>
    <destination name="tcp-syslog-2" type="syslog" host="10.0.0.0"
port="8514" protocol="tcp">
        <additionalParameters type="connector">
            <properties>
                <property key="remote.management.listener.port" value="9001"
/>
            </properties>
        </additionalParameters>
    </destination>
    <destination name="bc-connector-1" type="file"
path="/opt/ArcSightSmartConnectors/bc-connector/ current/file-feeds"
host="10.0.0.0" protocol="scp" username="admin"
password="OBFUSCATE.1:wAeVeZlW8m4Cq2wLEupkjA==" recursive="false"
flatten="false" passive="false" knownHostsFile="/home/arcsight/.ssh/known_
hosts">
        <additionalParameters type="connector">
            <properties>
                <property key="remote.management.listener.port" value="9001"
/>
            <property key="agent.name" value="bc-connector" />
        </properties>
        </additionalParameters>
    </destination>
    <destination name="bc-connector-2" type="file"
path="/opt/ArcSightSmartConnectors/bc-connector/ current/file-feeds"
host="10.0.0.0" protocol="scp" username="admin"
password="OBFUSCATE.1:wAeVeZlW8m4Cq2wLEupkjA==" recursive="false"
flatten="false" passive="false" knownHostsFile="/home/arcsight/.ssh/known_
hosts">
        <additionalParameters type="connector">
            <properties>
                <property key="remote.management.listener.port" value="9001"
/>
            <property key="agent.name" value="bc-connector" />
        </properties>
        </additionalParameters>
    </destination>
```

```
<destination name="netflow-connector" type="netflow" host="10.0.0.3" port="8515" protocol="udp">
    <additionalParameters type="connector">
        <properties>
            <property key="remote.management.listener.port" value="9001" />
        </properties>
    </additionalParameters>
</destination>
</destinations>
<routingRules>
    <routingRule name="syslog-tcp-rule" sourceName="syslog-tcp" destinationPoolName="tcp-syslogconnectors" routingPolicy="WeightedRoundRobin" enabled="true">
        <additionalParameters type="listener">
            <properties>
                <property key="syslog.address.prepend.mode" value="scan" />
            </properties>
        </additionalParameters>
    </routingRule>
    <routingRule name="bc-file-rule" sourceName="bc-ftp-server" destinationPoolName="bc-file-connectors" routingPolicy="RoundRobin" enabled="true" />
    <routingRule name="netflow-rule" sourceName="netflow-udp" destinationPoolName="netflow-connectors" routingPolicy="RoundRobin" enabled="true" />
</routingRules>
<sources>
    <source name="syslog-tcp" type="syslog" host="10.0.0.0" port="8002" protocol="tcp" />
    <source name="bc-ftp-server" type="file" path="bc-files" host="10.0.0.0" protocol="ftp" username="arcsight" password="OBFUSCATE.1:y05cvjSnFlVybZFBBeOHiQ==" recursive="true" flatten="true" passive="true" localWorkDirectory="/tmp" fileFilter=".log" />
        <source name="netflow-udp" type="netflow" host="10.0.0.1" port="8003" protocol="udp" />
</sources>
</routing>
<statisticsLogging logInterval="60000" />
<webServer httpsPort="8443" certificatePath="loadbalancer.cer" keystorePath="loadbalancer.p12" />
</lbConfiguration>
```

Standalone Mode Configuration File Template

The template files shown in this chapter are used to configure standalone and HA modes for Load Balancer.

```
<?xml version="1.0" encoding="UTF-8"?>
<lbConfiguration>
    <!-- Identify the current host among the memberHosts. -->
    <memberIdentity>primary-node</memberIdentity>

    <!-- Load Balancer can run in standalone mode. -->
    <!-- To run Load Balancer in standalone mode, configure one memberHost. vipAddress and -->
    <!-- vipPingPort cannot be null but it won't be referenced. -->
    <memberHosts vipAddress="10.0.0.0" vipPingPort="9090">
        <!-- 'host' is the host address where Load Balancer is installed and 'port' is internally -->
        <!-- used to communicate with another Load Balancer to detect the health for HA support. -->
        <!-- Standalone mode still requires valid port number to be specified. -->

        <!-- If Load Balancer is running as non-root, add Load Balancer user to sudoer list and -->
        <!-- prefix 'vipBindCommand' and 'vipUnbindCommand' with 'sudo' such as 'sudo /sbin/ifup..'. -->
        <memberHost name="primary-node" host="10.0.0.0" port="6702" isPrimary="true"
vipBindCommand="/sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="/sbin/ifdown
/etc/sysconfig/network-scripts/ifcfg-eth0:1"/>
    </memberHosts>
    <!-- To get an email notification when the Load Balancer member host is down or up, or when -->
    <!-- the destination is down or up, set enable to 'true' and configure the email section. -->
    <notification enable="true">
        <enabledNotification>
            <event name="MemberHostUp" message="Member node is up." />
            <event name="MemberHostDown" message="Member node is down." />
```

```
<event name="DestinationUp" message="Destination is up." />
<event name="DestinationDown" message="Destination is down." />
</enabledNotification>
<email>
    <!-- Create a prefix for the subject line.          -->
    <prefix>[Load Balancer]</prefix>
    <!-- Separate multiple recipients with a space.  -->
    <recipients>jane.doe@abc.com john.doe@abc.com</recipients>
    <sender>admin@abc.com</sender>
    <smtpServer>smtp.abc.com</smtpServer>
</email>
</notification>
<routing>
    <!-- All names in the routing section must be unique. -->
    <destinationPools>
        <destinationPool name="tcp-syslog-connectors" destinations="syslog-connector-1,syslog-
connector-2"/>
        <destinationPool name="udp-syslog-connectors" destinations="syslog-connector-3,syslog-
connector-4"/>
        <destinationPool name="tls-syslog-connectors" destinations="syslog-connector-5,syslog-
connector-6"/>
        <destinationPool name="file-connectors" destinations="file-connector-1,file-connector-2"/>
    </destinationPools>
    <destinations>
        <!-- Examples of configuring TCP connectors as destinations. -->
        <!-- 'host' is the host address where the tcp connector is running and 'port' is connector's
listening      -->
        <!-- port which can be found from agent.properties. 'tcp' corresponds to 'Raw TCP' in
agent.properties.  -->
        <destination name="syslog-connector-1" type="syslog" host="10.0.0.0" port="513"
protocol="tcp">
            <!-- Specify the connection configuration value here with key and matching value. Load
```

```
Balancer need -->
    <!-- the information to perform the connector health check and to obtain the load
information.      -->
    <additionalParameters type="connector">
        <properties>
            <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
                <!-- Prefer to send fewer events to this Connector by counting its CPU load as
twice as busy. -->
            <property key="load.expression" value="cpuLoad * 2"/>
        </properties>
    </additionalParameters>
</destination>
<destination name="syslog-connector-2" type="syslog" host="10.0.0.0" port="513"
protocol="tcp">
    <additionalParameters type="connector">
        <properties>
            <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
        </properties>
    </additionalParameters>
</destination>
<!-- Examples of configuring UDP connectors as destinations. -->
<destination name="syslog-connector-3" type="syslog" host="10.0.0.0" port="514"
protocol="udp">
    <additionalParameters type="connector">
        <properties>
            <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
        </properties>
    </additionalParameters>
</destination>
```

```
<destination name="syslog-connector-4" type="syslog" host="10.0.0.0" port="514"
protocol="udp">
    <additionalParameters type="connector">
        <properties>
            <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
        </properties>
    </additionalParameters>
</destination>
<!-- Examples of configuring TLS connectors as destinations. -->
<!-- As long as the connector is using the same certificate for the TLS syslog transport as
it is for -->
    <!-- remote management, Load Balancer will automatically work with it. -->
    <destination name="syslog-connector-5" type="syslog" host="10.0.0.0" port="515"
protocol="tls">
        <additionalParameters type="connector">
            <properties>
                <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
            </properties>
        </additionalParameters>
</destination>
    <destination name="syslog-connector-6" type="syslog" host="10.0.0.0" port="515"
protocol="tls">
        <additionalParameters type="connector">
            <properties>
                <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
            </properties>
        </additionalParameters>
</destination>
<!-- Examples of configuring file-based connectors as destination.
```

```
-->
    <!-- Supported protocols on the destination side are ftp and scp. Each protocol requires a
different      -->
        <!-- set of configuration values as shown in the examples below. Plaintext passwords are
persisted as      -->
            <!-- encrypted value when Load Balancer starts.
-->
            <!-- In order to use 'scp' protocol, file that has ssh host key should be provided to
'knownHostsFile'. -->
                <!-- Load Balancer does not populate this file automatically. In order to obtain the host
key, ssh to      -->
                    <!-- the destination manually and specify the full path of the system default known_hosts
file or copy      -->
                        <!-- the file to another location and give that path to 'knownHostsFile'.
-->
                        <destination name="file-connector-1" type="file" path="/opt/connector-1/input"
host="10.0.0.0" protocol="scp" username="admin" password="password" knownHostsFile="/root/.ssh/known_
hosts">
                            <!-- Configure the information about this connector before starting Load Balancer.
-->
                            <additionalParameters type="connector">
                                <properties>
                                    <!-- If the destination connector is file-based connector, specify the following
two      -->
                                        <!-- values so that Load Balancer can handshake with the connector.
-->
                                        <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
                                            <property key="agent.name" value="{agent name configured for the destination in
the final stage of agent setup}"/>
                                    </properties>
                                </additionalParameters>
```

```
        </destination>
        <!-- Configure the port if FTP server is configured with a non-default port. Default port 21
is used if not specified. -->
            <!-- 'host' is the host address of FTP server and 'username' and 'password' is the user
credential who has access to -->
                <!-- FTP server. Plaintext password is encrypted and persisted to this file as soon as Load
Balancer starts. -->
                    <destination name="file-connector-2" type="file" host="10.0.0.0" protocol="ftp"
username="admin" password="password" path="landing">
                        <additionalParameters type="connector">
                            <properties>
                                <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
                                <property key="agent.name" value="{agent name configured for the destination in
the final stage of agent setup}"/>
                            </properties>
                        </additionalParameters>
                    </destination>
                </destinations>
                <routingRules>
                    <!-- Supported routing policies are RoundRobin, WeightedRoundRobin, and
AggregationPreferred. -->
                    <routingRule name="syslog-tcp-rule" sourceName="syslog-tcp" destinationPoolName="tcp-syslog-
connectors" routingPolicy="RoundRobin" enabled="true">
                        <additionalParameters type="listener">
                            <properties>
                                <!-- Scan incoming messages to determine if there is a hostname or address
present, and insert one if not. -->
                                <property key="syslog.address.prepend.mode" value="scan"/>
                            </properties>
                        </additionalParameters>
                    </routingRule>
                </routingRules>
            </loadBalancers>
        </loadBalancers>
    </smartConnectors>
</smartConnectors>
```

```
        <routingRule name="syslog-udp-rule" sourceName="syslog-udp" destinationPoolName="udp-syslog-connectors" routingPolicy="WeightedRoundRobin" enabled="true"/>
        <routingRule name="syslog-tls-rule" sourceName="syslog-tls" destinationPoolName="tls-syslog-connectors" routingPolicy="AggregationPreferred" enabled="true"/>
        <routingRule name="file-routing-rule" sourceName="file-watcher" destinationPoolName="file-connectors" routingPolicy="RoundRobin" enabled="true"/>
    </routingRules>
    <sources>
        <!-- When the source is syslog type, set 'type' to 'syslog' and configure the protocol accordingly. -->
        <!-- Supported protocols are 'udp', 'tcp', and 'tls'. 'port' is the listening port on Load Balancer -->
        <!-- and source syslog server should be configured to send the events to this port.
-->
        <source name="syslog-tcp" type="syslog" port="513" protocol="tcp"/>
        <source name="syslog-udp" type="syslog" port="514" protocol="udp"/>
        <source name="syslog-tls" type="syslog" port="515" protocol="tls"/>
        <!-- 'file' type source can be used with the file based connector and Load Balancer
downloads -->
        <!-- the files from FTP server and distribute them to the defined destinations in
destination pool. -->
        <!-- Supported protocol is 'ftp' and 'host' is the host address where FTP server is running.
-->
        <!-- It assumes a default FTP port 21. If other port is configured, add 'port' attribute
port and -->
        <!-- specify the port number. 'path' should a relative path to FTP root directory.
-->
        <!-- Specify the credential for one who has a permission in accessing files from FTP server
with -->
        <!-- a full permission since files will need to moved to another directory or deleted after
-->
        <!-- the file is downloaded. When 'moveToDirectory' is configured, the downloaded file will
```

```
be      -->
        <!-- to a specified directory or when the value is empty, file will be deleted afterwards.
-->
        <!-- If the specified path is located under 'path', be sure to give the path as hidden
directory -->
        <!-- starting with '.'. Otherwise it will attempt to download the files from the directory
again   -->
        <!-- since it will recursively look for sub-directories. To disable recursive lookup, set
false to -->
        <!-- 'recursive' attribute.
-->
        <!-- User credential who has access to FTP server and path should be specified in 'username'
and    -->
        <!-- 'password'. Plaintext password will be converted as encrypted value as soon as Load
Balancer -->
        <!-- starts.
-->
        <!-- 'localWorkDirectory' is where the file is temporarily kept before the file is sent to
one of  -->
        <!-- the destinations. This is required value and it assumes that the directory exists
already.  -->
        <source name="file-watcher" type="file" host="10.0.0.0" protocol="ftp" path="landingzone"
username="admin" password="password" fileFilter=".*log" moveToDirectory=".done" recursive="true"
passive="false" localWorkDirectory="/tmp" />
    </sources>
</routing>
<!-- logInterval is in milliseconds. -->
<statisticsLogging logInterval="60000"/>
<!-- WebServer must be configured for all nodes listed as member hosts in Load Balancer. -->
>
<webServer httpsPort="8443"/>
<!-- Uncomment and configure this section in order to customize the configuration. -->
```

```
>      <!-- Refer to the configuration guide for the details. -->
>
<!-- globalParameters>
<properties>
    <property key="batch.buffersize" value="512000" />
    <property key="load.expression.default" value="cpuLoad"/>
</properties>
</globalParameters -->
</lbConfiguration>
```

HA Mode Configuration File Template

```
<?xml version="1.0" encoding="UTF-8"?>
<lbConfiguration>
    <!-- Identify the current host among the memberHosts. -->
    <memberIdentity>primary-node</memberIdentity>

    <!-- Load Balancer can run in HA mode: two hosts can run primary-secondary or peer. -->
    <!-- (1) To run Load Balancer as primary-secondary, configure two memberHosts and -->
    <!-- for one of the hosts, and set isPrimary to 'true'. -->
    <!-- (2) To run Load Balancer as peer, configure two memberHosts and set isPrimary to -->
    <!-- 'false' for both. -->
    <!-- 'vipAddress' is the virtual IP address that will be shared between two member hosts to -->
    <!-- handle seamless failover of member host. 'vipPingPort' is internally used to check if -->
    <!-- VIP address is still bound to one of the member hosts for continuous event collection. -->
    <!-- Specify any unused port to 'vipPingPort'. -->
    <memberHosts vipAddress="10.0.0.0" vipPingPort="9090">
        <!-- 'host' is the host address where Load Balancer is installed and 'port' is internally -->
        <!-- used to communicate with another Load Balancer to detect the health for HA support. -->
        <!-- If Load Balancer is running as non-root, add Load Balancer user to sudoer list and -->
        <!-- prefix 'vipBindCommand' and 'vipUnbindCommand' with 'sudo' such as 'sudo /sbin/ifup..'. -->
        <memberHost name="primary-node" host="10.0.0.0" port="6702" isPrimary="true"
vipBindCommand="/sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="/sbin/ifdown
/etc/sysconfig/network-scripts/ifcfg-eth0:1"/>
        <memberHost name="secondary-node" host="10.0.0.0" port="6702" isPrimary="false"
vipBindCommand="/sbin/ifup /etc/sysconfig/network-scripts/ifcfg-eth0:1" vipUnbindCommand="/sbin/ifdown
/etc/sysconfig/network-scripts/ifcfg-eth0:1"/>
    </memberHosts>
    <!-- To get an email notification when the Load Balancer member host is down or up, or when -->
    <!-- the destination is down or up, set enable to 'true' and configure the email section. -->
    <notification enable="true">
```

```
<enabledNotification>
    <event name="MemberHostUp" message="Member node is up." />
    <event name="MemberHostDown" message="Member node is down." />
    <event name="DestinationUp" message="Destination is up." />
    <event name="DestinationDown" message="Destination is down." />
</enabledNotification>
<email>
    <!-- Create a prefix for the subject line.          -->
    <prefix>[Load Balancer]</prefix>
    <!-- Separate multiple recipients with a space.  -->
    <recipients>jane.doe@abc.com john.doe@abc.com</recipients>
    <sender>admin@abc.com</sender>
    <smtpServer>smtp.abc.com</smtpServer>
</email>
</notification>
<routing>
    <!-- All names in the routing section must be unique. -->
    <destinationPools>
        <destinationPool name="tcp-syslog-connectors" destinations="syslog-connector-1,syslog-
connector-2"/>
        <destinationPool name="udp-syslog-connectors" destinations="syslog-connector-3,syslog-
connector-4"/>
        <destinationPool name="tls-syslog-connectors" destinations="syslog-connector-5,syslog-
connector-6"/>
        <destinationPool name="file-connectors" destinations="file-connector-1,file-connector-2"/>
    </destinationPools>
    <destinations>
        <!-- Examples of configuring TCP connectors as destinations. -->
        <!-- 'host' is the host address where the tcp connector is running and 'port' is connector's
listening   -->
        <!-- port which can be found from agent.properties. 'tcp' corresponds to 'Raw TCP' in
agent.properties.  -->
    </destinations>
</routing>
```

```
        <destination name="syslog-connector-1" type="syslog" host="10.0.0.0" port="513"
protocol="tcp">
            <!-- Specify the connection configuration value here with key and matching value. Load
Balancer need -->
            <!-- the information to perform the connector health check and to obtain the load
information.      -->
            <additionalParameters type="connector">
                <properties>
                    <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
                    <!-- Prefer to send fewer events to this Connector by counting its CPU load as
twice as busy. -->
                    <property key="load.expression" value="cpuLoad * 2"/>
                </properties>
            </additionalParameters>
        </destination>
        <destination name="syslog-connector-2" type="syslog" host="10.0.0.0" port="513"
protocol="tcp">
            <additionalParameters type="connector">
                <properties>
                    <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
                </properties>
            </additionalParameters>
        </destination>
        <!-- Examples of configuring UDP connectors as destinations. -->
        <destination name="syslog-connector-3" type="syslog" host="10.0.0.0" port="514"
protocol="udp">
            <additionalParameters type="connector">
                <properties>
                    <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
                </properties>
            </additionalParameters>
        </destination>
    </destinations>

```

```
        </properties>
    </additionalParameters>
</destination>
<destination name="syslog-connector-4" type="syslog" host="10.0.0.0" port="514"
protocol="udp">
    <additionalParameters type="connector">
        <properties>
            <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
        </properties>
    </additionalParameters>
</destination>
<!-- Examples of configuring TLS connectors as destinations. --&gt;
<!-- As long as the connector is using the same certificate for the TLS syslog transport as
it is for --&gt;
<!-- remote management, Load Balancer will automatically work with it. --&gt;
&lt;destination name="syslog-connector-5" type="syslog" host="10.0.0.0" port="515"
protocol="tls"&gt;
    &lt;additionalParameters type="connector"&gt;
        &lt;properties&gt;
            &lt;property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/&gt;
        &lt;/properties&gt;
    &lt;/additionalParameters&gt;
&lt;/destination&gt;
&lt;destination name="syslog-connector-6" type="syslog" host="10.0.0.0" port="515"
protocol="tls"&gt;
    &lt;additionalParameters type="connector"&gt;
        &lt;properties&gt;
            &lt;property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/&gt;
        &lt;/properties&gt;</pre>
```

```
        </additionalParameters>
    </destination>
    <!-- Examples of configuring file-based connectors as destination.
-->
    <!-- Supported protocols on the destination side are ftp and scp. Each protocol requires a
different      -->
        <!-- set of configuration values as shown in the examples below. Plaintext passwords are
persisted as      -->
            <!-- encrypted value when Load Balancer starts.
-->
            <!-- In order to use 'scp' protocol, file that has ssh host key should be provided to
'knownHostsFile'. -->
                <!-- Load Balancer does not populate this file automatically. In order to obtain the host
key, ssh to      -->
                    <!-- the destination manually and specify the full path of the system default known_hosts
file or copy      -->
                        <!-- the file to another location and give that path to 'knownHostsFile'.
-->
                        <destination name="file-connector-1" type="file" path="/opt/connector-1/input"
host="10.0.0.0" protocol="scp" username="admin" password="password" knownHostsFile="/root/.ssh/known_
hosts">
                            <!-- Configure the information about this connector before starting Load Balancer.
-->
                            <additionalParameters type="connector">
                                <properties>
                                    <!-- If the destination connector is file-based connector, specify the following
two      -->
                                        <!-- values so that Load Balancer can handshake with the connector.
-->
                                        <property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/>
                                        <property key="agent.name" value="{agent name configured for the destination in
```

```
the final stage of agent setup}"/>
    </properties>
</additionalParameters>
</destination>
<!-- Configure the port if FTP server is configured with a non-default port. Default port 21
is used if not specified. --&gt;
<!-- 'host' is the host address of FTP server and 'username' and 'password' is the user
credential who has access to --&gt;
<!-- FTP server. Plaintext password is encrypted and persisted to this file as soon as Load
Balancer starts. --&gt;
&lt;destination name="file-connector-2" type="file" host="10.0.0.0" protocol="ftp"
username="admin" password="password" path="landing"&gt;
    &lt;additionalParameters type="connector"&gt;
        &lt;properties&gt;
            &lt;property key="remote.management.listener.port" value="
{remote.management.listener.port from agent.properties}"/&gt;
            &lt;property key="agent.name" value="{agent name configured for the destination in
the final stage of agent setup}"/&gt;
        &lt;/properties&gt;
    &lt;/additionalParameters&gt;
&lt;/destination&gt;
&lt;/destinations&gt;
&lt;routingRules&gt;
    <!-- Supported routing policies are RoundRobin, WeightedRoundRobin, and
AggregationPreferred. --&gt;
    &lt;routingRule name="syslog-tcp-rule" sourceName="syslog-tcp" destinationPoolName="tcp-syslog-
connectors" routingPolicy="RoundRobin" enabled="true"&gt;
        &lt;additionalParameters type="listener"&gt;
            &lt;properties&gt;
                <!-- Scan incoming messages to determine if there is a hostname or address
present, and insert one if not. --&gt;
                &lt;property key="syslog.address.prepend.mode" value="scan"/&gt;
            &lt;/properties&gt;
        &lt;/additionalParameters&gt;
    &lt;/routingRule&gt;
&lt;/routingRules&gt;</pre>
```

```
        </properties>
    </additionalParameters>
</routingRule>
<routingRule name="syslog-udp-rule" sourceName="syslog-udp" destinationPoolName="udp-syslog-connectors" routingPolicy="WeightedRoundRobin" enabled="true"/>
<routingRule name="syslog-tls-rule" sourceName="syslog-tls" destinationPoolName="tls-syslog-connectors" routingPolicy="AggregationPreferred" enabled="true"/>
<routingRule name="file-routing-rule" sourceName="file-watcher" destinationPoolName="file-connectors" routingPolicy="RoundRobin" enabled="true"/>
</routingRules>
<sources>
    <!-- When the source is syslog type, set 'type' to 'syslog' and configure the protocol accordingly. -->
    <!-- Supported protocols are 'udp', 'tcp', and 'tls'. 'port' is the listening port on Load Balancer -->
        <!-- and source syslog server should be configured to send the events to this port.
-->
        <source name="syslog-tcp" type="syslog" port="513" protocol="tcp"/>
        <source name="syslog-udp" type="syslog" port="514" protocol="udp"/>
        <source name="syslog-tls" type="syslog" port="515" protocol="tls"/>
        <!-- 'file' type source can be used with the file based connector and Load Balancer
downloads -->
            <!-- the files from FTP server and distribute them to the defined destinations in
destination pool. -->
            <!-- Supported protocol is 'ftp' and 'host' is the host address where FTP server is running.
-->
            <!-- It assumes a default FTP port 21. If other port is configured, add 'port' attribute
port and -->
                <!-- specify the port number. 'path' should a relative path to FTP root directory.
-->
                <!-- Specify the credential for one who has a permission in accessing files from FTP server
with -->
```

```
        <!-- a full permission since files will need to moved to another directory or deleted after
-->
        <!-- the file is downloaded. When 'moveToDirectory' is configured, the downloaded file will
be      -->
        <!-- to a specified directory or when the value is empty, file will be deleted afterwards.
-->
        <!-- If the specified path is located under 'path', be sure to give the path as hidden
directory -->
        <!-- starting with '.'. Otherwise it will attempt to download the files from the directory
again   -->
        <!-- since it will recursively look for sub-directories. To disable recursive lookup, set
false to  -->
        <!-- 'recursive' attribute.
-->
        <!-- User credential who has access to FTP server and path should be specified in 'username'
and     -->
        <!-- 'password'. Plaintext password will be converted as encrypted value as soon as Load
Balancer -->
        <!-- starts.
-->
        <!-- 'localWorkDirectory' is where the file is temporarily kept before the file is sent to
one of   -->
        <!-- the destinations. This is required value and it assumes that the directory exists
already.  -->
        <source name="file-watcher" type="file" host="10.0.0.0" protocol="ftp" path="landingzone"
username="admin" password="password" fileFilter=".log" moveToDirectory=".done" recursive="true"
passive="false" localWorkDirectory="/tmp" />
    </sources>
</routing>
<!-- logInterval is in milliseconds. -->
<statisticsLogging logInterval="60000"/>
<!-- WebServer must be configured for all nodes listed as member hosts in Load Balancer. -->
```

```
>      <webServer httpsPort="8443"/>
>      <!-- Uncomment and configure this section in order to customize the configuration. -->
>      <!-- Refer to the configuration guide for the details. -->
>      <!-- globalParameters>
>          <properties>
>              <property key="batch.buffersize" value="512000" />
>              <property key="load.expression.default" value="cpuLoad"/>
>          </properties>
>      </globalParameters -->
</lbConfiguration>
```

Publication Status

Released: February 2025

Updated: February 2025

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 Load Balancer (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:

ArcSight Customer Support - Help with SmartConnector and Parser Updates

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 home page of this Help 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

ArcSight Customer Support - Help with SmartConnector and Parser Updates	4
About SmartConnectors and Event Parsers	4
Supporting Minor Parser Updates and Overrides	4
Supporting Device Version Updates	5
Supporting Un-Obfuscated Parsers	5
Supporting New Device Connectors	6
Send Documentation Feedback	7

ArcSight Customer Support - Help with SmartConnector and Parser Updates

About SmartConnectors and Event Parsers

The integration of device event-feeds in to ArcSight relies on the availability of a suitable SmartConnector (or FlexConnector) to both acquire and parse/normalize the raw device events in to the ArcSight schema. ArcSight SmartConnectors exist for the most common source devices and will have been tested, certified and documented against a given range of device versions. The SmartConnector release process follows a split monthly/quarterly cycle, whereby updates to parsing of many connectors are released each month and new features or support for completely new source devices requiring code-changes occur within the quarterly release.

As new versions of each device become available, existing parsing support might:

- Work perfectly well due to little or no change in the event format itself (even though not yet formally certified)
- Prove incomplete or suboptimal, possibly matched against an incorrect parser for a different source device
- Fail entirely to match the new format of the source events, resulting in ‘unparsed event’ alerts being generated
- Require a new mechanism entirely to acquire the events ready for parsing, resulting in no events being retrieved at all

Furthermore, parsing support even for device versions already certified by ArcSight may not prove optimal for all use-cases and would also require update to the associated connector parser to better meet a specific customer requirement.

Supporting Minor Parser Updates and Overrides

The majority of parsing requirements fall into the category of ‘device version-updates’ and typically require only minor changes to reinstate proper normalization. In order to streamline and hasten the update of the connectors, we have initiated a revised process via our Support organization who will now accept requests for connector device version-updates and, dependent upon the scope of work required as well as the availability of sample raw device events, may be able to devise and provide a ‘parser override’ before the next monthly or quarterly release. Previously, such requests fell under the ‘Enhancement Request’ process that is driven instead through the ArcSight Idea Exchange portal.

Thus, where sub-optimal or failed parsing is observed for either an existing certified device version, or else an updated version of an existing supported device, do the following:

- Check the available documentation to determine whether a more recent SmartConnector release is expected to support your device/version and upgrade the connector version accordingly. Otherwise,
- Raise a case with Support requesting a parser update
- State to Support the precise name, sub-component (where relevant) and version of the device that is no longer being parsed as expected.
- Acquire and provide Support with a set of sample events (wherever possible), that no longer parse correctly – highlighting the parsing deficiencies where not already self-evident
- Provide any relevant context, such as device version that last parsed correctly or other relevant data that may assist the triage process.

Once the prerequisite data points have been captured, Support will first attempt to reproduce the reported parsing behavior, before then engaging our development team to determine the scope of work required to correct or enhance the current parsing. Support will keep you informed of progress through the support-case and, where a parser override can be devised before the next release cycle, will share that with you for validation within your environment. Once validated, the parser changes will be automatically rolled-up in to the next parser AUP release.

Supporting Device Version Updates

Where the changes instead require more significant investigation, it may not be possible to provide an interim parser override. In this case, a formal request will be raised internally on your behalf and targeted for a future release. Support will let you know the outcome.

ArcSight recommends that our customers to work closely with their IT Ops team to preempt the upgrade of any source devices that feed ArcSight and review the latest SmartConnector Configuration Guide for each device to check whether or not the new device version has already been certified by ArcSight and thus avoid or mitigate any delay before updated parsing support can be made available. Given sufficient time before the roll-out of a new device version, it would therefore be appropriate to post a new ‘idea’ on the ArcSight Idea Exchange portal for triage by our Product Management team and potential inclusion in to the usual release-cycle. However, we understand that this preemptive approach is not always possible and hence have introduced the revised process described above to help our customers restore full visibility of their security events as soon as practicable.

Supporting Un-Obfuscated Parsers

Should you decide to develop an updated parser or override the out-of-the-box provided parser, we are pleased to announce that, as of the v8.0 SmartConnector release (July 2020),

each release will include an unobfuscated/plaintext copy of the entire set of ArcSight parser files, which will provide a valuable starting-point for further parser development.

Supporting New Device Connectors

Finally, the ArcSight Idea Exchange portal remains the appropriate route for support requests for devices for which no SmartConnector is yet available. Please do not forget our FlexConnector SDK – available as part of your ArcSight entitlement – should you have the ability in-house to devise your own custom parsers, or to engage our Professional Services organization for more substantial parser development.

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 Customer Support - Help with SmartConnector and Parser Updates
(SmartConnectors)**

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

Recommendations for Windows Event Log Collection

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

Recommendations for Windows Event Log Collection	4
Overview	5
Microsoft Windows Event Log - Native (WiNC)	5
Windows Event Log SmartConnector (WiSC)	5
Windows Event Log Collection Best Practices	6
Option 1: Use WiNC SmartConnector as a Log Aggregator	6
Option 2: Use WiNC in a WEC or WEF Environment	6
Useful References	7
Send Documentation Feedback	8

Recommendations for Windows Event Log Collection

Over the years, OpenText has released multiple SmartConnectors to collect event logs from Microsoft Windows OS and Microsoft Active Directory environments.

A short summary and deployment considerations are provided in this document.

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

At this time, we *only* recommend using the WiNC SmartConnector for production environments, because of the limitations with WiSC options that are listed below.

Microsoft Windows Event Log - Native (WiNC)

WiNC is a next-generation SmartConnector that supports native event log collection, using the .NET framework.

Pros:

- It is scalable.
- It provides high performance event log collection.

Cons:

- It can only be deployed on Windows Server operating systems.

Windows Event Log SmartConnector (WiSC)

WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. We have experienced the following issues.

- **High CPU utilization on the monitored Windows host (log endpoint)**

High CPU utilization has been detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average).

- **WinRM inherent EPS limitations**

Given the circumstances with WinRM, the event rate has a limit of around 140 EPS (sustained). Therefore, we do not recommend the use of the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates.

Windows Event Log Collection Best Practices

Use the Windows Native Connector (WiNC) SmartConnector, as detailed below.

Windows Native Connector is our recommended deployment option, while we are investigating a long-term solution to have a SmartConnector running on Linux operating systems.

Option 1: Use WiNC SmartConnector as a Log Aggregator

WiNC SmartConnector is a high-performance SmartConnector that can handle large EPS volumes. See the “*SmartConnector for Microsoft Windows Event Log – Native ‘Configuration Guide’*” for detailed implementation steps.

Option 2: Use WiNC in a WEC or WEF Environment

Windows Event Collection (WEC) and Windows Event Forwarding (WEF) are native Microsoft technologies that support Windows event log collection in a Windows environment.

WiNC SmartConnector is capable of collecting “Forwarded Events or Other WEC Logs from Local Or Remote Hosts”. As such, you may consider deploying a suitable Windows Event Forwarding architecture for your organization.

WiNC can be deployed in the following ways:

- Directly on WEF aggregation point (WEC Server)
- Remotely on another Windows Server, to connect and collect forwarded events from one or many WEC Server(s).

As a result, the footprint of the ArcSight WiNC SmartConnector can be optimized depending on your architectural goals.

Useful References

For more information on using WiNC in a WEF environment, please check the following document:

[Collecting Windows Event Logs Using Windows Event Forwarding](#)

For more information on Windows Event Forwarding, please check the following documents:

[Windows Event Collector](#)

[Use Windows Event Forwarding to help with intrusion detection](#)

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 Recommendations for Windows Event Log Collection (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!

Micro Focus Security ArcSight SmartConnectors

Software Version: 8.4.2

SmartConnector Release Notes

Document Release Date: July 2023

Software Release Date: July 2023



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2010 - 2023 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.

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

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://www.microfocus.com/documentation/arcsight/

Contents

Release Highlights	5
What's New	6
New SmartConnectors and Modules	6
Cloud Updates	6
Security Updates	7
Version Updates	7
Platform Support	8
SmartConnector Enhancements	9
Software Fixes	10
Event Categorization Updates	13
SmartConnector Parser Support Policy	14
Installing SmartConnectors	15
System Requirements	15
Downloading the SmartConnector 8.4.2 Installation Packages	15
Upgrading to 8.4.2	16
Deleting Older Vulnerable Libraries after Upgrading a Connector	17
Known Issues	20
Connector End-of-Life Notices	27
SmartConnector End of Support Announcements	27
SmartConnectors No Longer Supported	27
Publication Status	29
Send Documentation Feedback	30

Release Highlights

The SmartConnector 8.4.2 release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Support for a new SmartConnector named ServiceNow
- Support for a new SmartConnector named Microsoft Azure Event Hub
- Support for the Apache Tomcat File logs for version 10.1.2
- Support for IBM Security Access Manager Syslog logs for version 10.0.1
- Support for Cisco IronPort Web Security Syslog AsyncOS 12.0.1
- Support for Microsoft Server SharePoint DB 2019
- Support for Check Point Syslog R81.40 modules
- Support for Rocky Linux 8.6 as the installation platform
- Support for Citrix NetScaler 13.0.0
- Support for Linux Kernel-based Virtual Machine (KVM) 9.0
- Support for Microsoft Windows Hyper-V logs
- Support for Red Hat Enterprise Linux (RHEL) 9.0 and 9.1 logs for the Linux Audit File, Linux Audit Syslog, UNIX Login/Logout File, and UNIX OS Syslog connectors
- Support for the Microsoft Windows Server 2019 and Microsoft Windows Server 2022 events for Microsoft ADFS
- Upgrade of Zulu OpenJDK to 8u372
- Upgrade of Tomcat version to 9.0.74
- Updates of ArcSight Event Content-Categorization till May 2023. These updates are now a monthly release.

For detailed information, see "[What's New](#)" on the next page.

The Connector Team has worked tirelessly, and in a few cases, have enjoyed the benefits of partnering with some of the customers to overcome some of the issues. The extra effort from the customer success and support teams, and especially customers, in helping the team understand and reproduce some difficult situations in order to improve the SmartConnectors is duly appreciated.

Additionally, the [ArcSight Idea Exchange portal](#), will be updated with affected entries and monitored to help, prioritize, and plan new features for next release.

What's New

SmartConnector 8.4.2 incorporates the following SmartConnector releases, and content and categorization updates:

- [SmartConnector 8.4.1 Patch 1](#)
- [Event Content-Categorization updates May 2023](#)

New SmartConnectors and Modules

New SmartConnectors/ Application Module	Description
Microsoft Azure Event Hub	<p>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. The Microsoft Azure Event Hub SmartConnector helps you monitor the activities on Microsoft Azure Cloud services. The Microsoft Azure Event Hub SmartConnector is a better alternative version of Microsoft Azure Monitor Event Hub Connector, which can be deployed on both cloud and off cloud, to monitor the activities on Microsoft Azure Cloud services. It provides the following benefits:</p> <ul style="list-style-type: none">• Overall cost reduction• Better performance• More log type support• No deployment complexity <p>For more information, see Configuration Guide for Microsoft Azure Event Hub SmartConnector.</p>
ServiceNow	<p>The SmartConnector for ServiceNow retrieves events from ServiceNow, normalizes the events, and then sends them to the configured destinations.</p> <p>For more information, see Configuration Guide for SmartConnector for ServiceNow.</p>

Cloud Updates

None at this time.

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	<p>Upgraded Zulu OpenJDK to 8u372.</p> <p>The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade:</p> <ul style="list-style-type: none"> • CVE-2023-21930 • CVE-2023-21954 • CVE-2023-21967 • CVE-2023-21939 • CVE-2023-21937 • CVE-2023-21938 • CVE-2023-21968
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.74.

Version Updates

Application Module Version Updates	Description
Apache Tomcat File	Added support for the Apache Tomcat File logs for version 10.1.2.
IBM Security Access Manager Syslog	Added support for IBM Security Access Manager Syslog logs for version 10.0.1.
<ul style="list-style-type: none"> • Linux Audit File • Linux Audit Syslog • UNIX Login/Logout File • UNIX OS Syslog 	Added support for Red Hat Enterprise Linux (RHEL) 9.0 and 9.1.

Application Module Version Updates	Description
Microsoft Windows Event Log - Native	<p>Added support for the following Microsoft Windows Server 2019 and Microsoft Windows Server 2022 events for Microsoft ADFS.</p> <ul style="list-style-type: none"> • Event 105 • Event 111 • Event 221 • Event 227 • Event 298 • Event 352 • Event 397 • Event 575 • Event 1000
<ul style="list-style-type: none"> • UNIX Login/Logout File • UNIX OS Syslog 	Added support for Linux Kernel-based Virtual Machine (KVM) 9.0.
WiNC on Connector Hosting Appliance	Added support for Red Hat Enterprise Linux Server (RHEL) 7.9.

Platform Support

Application Module Platform Support	Description
All SmartConnectors and Load Balancer	Added support for Rocky Linux 8.6.

For details about hardware, software or platform, and SmartConnector requirements, refer to [Technical Requirements for SmartConnectors](#).

SmartConnector Enhancements

Application Module Enhancements	Description
All SmartConnectors	<p>Added support for Default AWS Credentials Provider for the Amazon S3 destination to use the Default Credential Provider Chain.</p> <p>For more information about the Default AWS Credentials Provider parameter, see Amazon S3 Parameters.</p>
All SmartConnectors with Microsoft Event hubs destination	<p>Added support for Certificate and Client secret based authentication to authenticate Microsoft Azure Event Hub. Azure Event hub access using connection string having SharedAccessKey information have been deprecated in this release.</p> <p>When configuring the Kafka FlexConnector, if the source type is selected as Azure Event Hub, then the Microsoft Event hub destination needs to be reconfigured to use any one of the authentication mechanisms.</p> <p>For more information about the destination parameter details, see Installation and User Guide for SmartConnector.</p> <p>For more information about Azure Event Hub, see Configuration Guide for Microsoft Azure Event Hub.</p>
ArcSight Threat Acceleration Program (ATAP)	<p>ATAP connector, previously known as Galaxy Threat Acceleration Program (GTAP) is now available with the latest security fixes.</p>
Developer's Guide to FlexConnector for Kafka	<p>Added support for Certificate and Client secret based authentication to authenticate Microsoft Azure Event Hub. Azure Event hub access using connection string having SharedAccessKey information have been deprecated in this release.</p> <p>When configuring the Kafka FlexConnector, if the source type is selected as Azure Event Hub, then the Microsoft Event hub destination needs to be reconfigured to use any one of the authentication mechanisms.</p> <p>For more information about the destination parameter details, see Installation and User Guide for SmartConnector.</p> <p>For more information about Azure Event Hub, see Configuration Guide for Microsoft Azure Event Hub.</p>

Application Module Enhancements	Description
Microsoft 365 Defender	<p>Added support for the Certificate-based authentication method for the Microsoft 365 Defender SmartConnector. The connector will make the access token request with the Client Certificate and the same can be used for pulling the APIs.</p> <p>For more information, see the Configuration Guide for Microsoft 365 Defender.</p>
Microsoft Message Trace REST API	<p>Added support for the OAuth2-Client Credentials authentication type to secure REST APIs to collect events from Microsoft Office 365 Message Trace REST API.</p> <p>For more information, see parameter details in the Configuration Guide for Message Trace Rest API Connector.</p>
Microsoft SharePoint Server DB	<p>Added support for Microsoft Server SharePoint DB 2019.</p> <p>Added support for the following events:</p> <ul style="list-style-type: none"> • Event 1 • Event 10
Microsoft Windows Event Log - Native	<p>Added support for Microsoft Windows Hyper V logs.</p> <p>For more information about configuring the Microsoft Windows Hyper V log source, see Microsoft Windows Hyper V.</p> <p>For more information about supported event mappings, see Event Mappings for Microsoft Windows Hyper V.</p>

Software Fixes

The following issues are fixed in the 8.4.2 release:

Application Modules Software Fixes	Description
All SmartConnectors	<p>The runagentsetup was throwing errors after changing the remote management password from the Command Line (CLI) as the password in <code>connector_config.xml</code> was not getting updated with new password.. Only default credentials must be used for remote management password of the smartconnector.</p> <p>Fix: The issue is resolved by changing the remote management password of the connector by adding <code>remote.management.password=new password</code> to <code>agent.properties</code> and then running the <code>runagentsetup</code>.</p>
All SmartConnectors	<p>The connector was sending failover event agent:051 to only the first instance of failover of primary ESM and not for every failover event.</p> <p>Fix: This issue was fixed by removing a condition in the code, that was set to send the failover event only on the first occurrence.</p>
All SmartConnectors (Syslog files)	<p>After restarting, the connector stops reading the events from the log files from the last position to which it was saved. The connector was only reading the events from the end of the file.</p> <p>Fix: The issue has been fixed, as now the connector will start reading the log files from the point where it stopped.</p>
ArcSight Common Event Format REST	<p>A few minutes after the ArcSight Common Event Format REST connector starts receiving events from the Qualys API, the vm_scan_since parameter in the eventsurl property of the <code>agent.properties</code> file gets automatically updated. This results in the href field in the URL of the API being empty, which, in turn, leads to the connector not receiving events anymore.</p> <p>Fix: The issue has been fixed by updating the value of the vm_scan_since parameter to the timestamp of the URL of the API.</p>
	<p>The ArcSight Common Event Format REST connector polls the Digital Shadows API endpoint frequently in a minute, thus reaching the API's call rate limit. This results in the locking of the API key.</p> <p>Fix: The issue has been fixed by introducing a new property called maxqueriesperminute in the <code>RestApiConstants.java</code> file. This property specifies the maximum number of times per minute that the connector can poll the API. The default value of the property is 60. When the API polling count reaches the maxqueriesperminute value in a minute, then, for the remaining seconds of that minute, the polling is paused.</p>

Application Modules Software Fixes	Description
Check Point Syslog	<p>The Check Point Syslog connector was unable to parse the logs for the Application Control and Smart Defense modules, because a new key resource was introduced in the logs.</p> <p>Fix: The base regex of the Check Point Syslog parser file has been modified to provide support for the resource key in the Application Control and Smart Defense modules of Check Point logs.</p>
Cisco IOS Syslog	<p>The Cisco IOS Syslog connector was unable to retrieve the value of the hostname field.</p> <p>Fix: The parser file has been modified to retrieve the value of the hostname field.</p>
Cisco IronPort Web Security Appliance Syslog	<p>The logs of Cisco IronPort Web Security Syslog AsyncOS version 12.0.1 were not being parsed.</p> <p>Fix: Added support for Cisco IronPort Web Security Syslog AsyncOS 12.0.1.</p>
Citrix NetScaler Syslog	<p>The timestamp of citrix netscaler events for the following modules was not getting converted from GMT to PST:</p> <ul style="list-style-type: none"> • SSLVPN HTTPREQUEST • AAATM HTTPREQUEST <p>Fix: The issue has been fixed by making changes in the regex of SSLVPN HTTPREQUEST and AAATM HTTPREQUEST modules to adjust the time.</p>
Citrix NetScaler Syslog	<p>The Citrix NetScaler Syslog connector was unable to parse some of the events for Citrix NetScaler Version 13.0.0.</p> <p>Fix: Added support for Citrix NetScaler 13.0.0.</p>
Fortinet Fortigate Syslog	<p>The Fortinet Key_value parser for Fortinet Fortigate Syslog was using the date and time field for the Device Receipt Time field.</p> <p>Fix: The issue is fixed by making changes in parser to prioritize eventtime or log time timestamp over date and time for the Device Receipt Time field.</p>
Juniper Firewall ScreenOS Syslog	<p>The Source and Destination fields in the system-warning-00518 module logs from Juniper ScreenOS were not being parsed.</p> <p>Fix: An existing sub-message for the system-warning-00518 module has been modified to handle the parsing issue for Juniper ScreenOS logs.</p>

Application Modules Software Fixes	Description
Microsoft Windows Event Log - Native	<p>The Microsoft Windows Event Log - Native connector was unable to parse Event ID 411 correctly, due to the presence of multiple addresses in %5. It was resulting in the Source Address field to remain empty.</p> <p>Fix: The Source Address field is now being populated with the first of the two addresses, while both addresses are being stored in Device Custom String 3.</p>
Oracle Unified Audit Trail DB	<p>After applying the fix for the ORA-22835 error, the following error is displayed: ORA-01401: inserted value too large for column. This error occurs because the size of the text fields provided in the fix for the ORA-22835 error is too large (4000).</p> <p>Fix: To fix this issue, the Oracle admin must reduce the size of the text fields by replacing all instances of "4000" with "2000" in the fix provided for the ORA-22835 error.</p> <p>For more information, refer to the Troubleshooting section of the <i>Configuration Guide for Oracle Unified Audit Trail DB SmartConnector</i>.</p>
Tenable Nessus .nessus File	<p>The Tenable Nessus .nessus File connector was unable to process events from long reports in the .nessus format from a Nessus source device. When the connector was configured to use ESM as a destination, it was displaying 'byte array size too long' error. This error caused the connector to prevent the other Nessus reports from being processed.</p> <p>Fix: The issue was occurring because of lengthy Nessus report values that were being compared with the 'Short.MAX' value of Java. This resulted in throwing an exception.</p> <p>The issue has been resolved now, as the incoming value is truncated to the maximum size allowed in the 'writeString' method of 'PrimitiveOutputStream.java'.</p>

Event Categorization Updates

For more information, see [Release Notes for ArcSight Content AUP -Categorization Updates 2023](#).

SmartConnector Parser Support Policy

Inline with the documents [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#), [Technical Requirements for SmartConnectors](#), the note at the top of the [SmartConnector Grand List \(A-Z\) documentation](#) page, we would like to take this opportunity to clarify what is meant by Connector Support.

As mentioned in the note on the [SmartConnector Grand List \(A-Z\) documentation](#) page:

The device versions currently documented as **certified** are versions that have been tested by ArcSight Quality Assurance. For device releases that fall in between certified major versions, it has been our experience that vendors typically do not make significant changes to the event generation mechanism.

Oftentimes, there are few, if any, significant changes even between major versions to the event logs. Therefore, we consider all device releases to be supported, with the understanding that major version releases may not work as expected, depending on the types of changes made to that major version.

Where possible, minor adjustments can be accommodated by parser overrides as needed. For example, Extreme Networks Dragon Export Tool versions 7.4 and 8.2 have been certified; Dragon Export Tool version 7.5 is also supported, as well as versions 8.3 or 9.0 should they be released.

In other words, if we have a SmartConnector with any certified version of a device, that device is supported regardless of version as long as the version in question is supported by the vendor.

In the situations where parser overrides cannot provide adequate functionality to support a new major or minor version of a device release, the Support Team will elevate the issue to the appropriate development teams.

Please be aware that the development team may not have immediate access to the updated device and logs. Support will request that you attach the unparsed or improperly parsed logs to your support ticket.

Please also note that we have a log anonymization/sanitization tool that you can use to remove sensitive information from logs we would need you to submit.

We may also request a conference call with you to help clarify or expedite any issues, especially if the device's connection and logging methods have changed.

For details as to the need to collect logs or possible vendor changes to devices, please see [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#).

Installing SmartConnectors

For information about installing SmartConnector, see the [Installing SmartConnectors](#) section in Installation Guide for ArcSight SmartConnectors.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to [Technical Requirements for SmartConnectors](#).

Downloading the SmartConnector 8.4.2 Installation Packages

You can download the SmartConnector installation packages for your platform from the [Software Licenses and Downloads \(SLD\)](#). The installation packages include their respective signature files for validating that the downloaded software is authentic and has not been tampered with by a third party.

File Name	Description
ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-8.4.2.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.2.xxxx.0-Collectors-Linux64.bin	This is the 64-bit Collector installer for Linux.
ArcSight-8.4.2.xxxx.0-Collectors-Win64.exe	This is the 64-bit Collector installer for Windows.
ArcSight8.4.2.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.2.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.2.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.2.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.2.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.2.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.2.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.

ArcSight-8.4.2.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.2.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.2.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.2.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.2.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.2.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.2.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.
ArcSightSmartConnectorLoadBalancer-opensource-8.4.2.xxxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.2.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.2.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading to 8.4.2



Important: If you use any of the SmartConnectors listed in the [Software Fixes](#) section, note that installing the updated SmartConnector can impact your created content.

Verifying Your Upgrade 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.

For information and instructions, see [Verifying Micro Focus Signatures with gpg or rpm](#).



Note: If a Parser Override was provided, determine whether the Bug or Feature Request number is included in the Fixed or Enhancements section. If the number is not listed, do not upgrade the Connector. You can test the upgrade in a STAGE (staging) environment to ensure it works as expected before you upgrade your environment PROD (production)

Upgrading SmartConnector to 8.4.2

You can upgrade a SmartConnector to implement the newly introduced features, mapping improvements and overall functionality of a SmartConnector. You can upgrade connectors either locally or remotely. Connectors automatically determine their upgrade status when they start.

For information and instructions, see [Upgrading SmartConnectors](#).

Upgrading Load Balancer to 8.4.2

For information about upgrading Load Balancer to 8.4.2, see [Upgrading Load Balancer](#).

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.



Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:



Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command: `cd Xxxxx/lib/agent`

3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`
5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
6. Run the following command: `cd Xxxxx/lib/agent/axis`
7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Open the `Xxxxx\lib\agent` folder.
3. Search for **log4j** and delete all the entries.
4. Open the `Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\` folder.
5. Search for **log4j** and delete all the entries.
6. Open the `Xxxxx\lib\agent\axis` folder.
7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm -rf X8444`)

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Delete the **Xxxxx** folder manually.

Known Issues

This section includes legacy issues from the ArcSight Installer.

Application Module	Description
All SmartConnectors	<p>SmartConnector or Collector remote connections fail due to low entropy</p> <p>All SmartConnectors or Collectors remote connections go through SSL and they depend on the Operating System random number pool (entropy pool) to generate private keys for secure communication. When the entropy pool is less than the ideal lower limit of 1000, the keys are not generated, communication cannot be established and the SmartConnector or Collector does not start. In cloud hosted Linux instances, the entropy pool value can be less than 1000.</p> <p>Workaround:</p> <p>To ensure that the entropy value is at the desired level:</p> <ol style="list-style-type: none"> 1. Install the rng-tools package: <code>sudo yum install -y rng-tools</code> 2. Add the following line to the /etc/sysconfig/rngd file: <code>EXTRAOPTIONS="-r /dev/urandom"</code> 3. Check the entropy availability in the system: <code>cat /proc/sys/kernel/random/entropy_avail</code> 4. Start the rngd package as root user: <code>service rngd start</code> 5. Enable the rngd service to start at the system start-up: <code>systemctl enable rngd.service</code> <code>systemctl start rngd.service</code> 6. Ensure that the rngd package is always running (even after a reboot) as root user: <code>chkconfig --level 345 rngd on</code> 7. Check the entropy availability in the system, after starting the rngd service: <code>cat /proc/sys/kernel/random/entropy_avail</code>
	<p>Unable to install connector because of missing packages</p> <p>Workaround:</p> <p>Ensure that the following packages are installed:</p> <ol style="list-style-type: none"> 1. <code>yum install -y unzip</code> 2. <code>yum install -y fontconfig \ dejavu-sans-fonts</code>

All SmartConnectors installed on Solaris	<p>When upgrading SmartConnectors on Solaris, a timeout error is displayed</p> <p>Workaround:</p> <ul style="list-style-type: none"> • If the Solaris connector is already installed as a standalone, locally upgrade to 8.2.0. • If the Solaris Connector is installed as a service: <ol style="list-style-type: none"> a. Stop the service. b. Go to HOME/current/bin and execute <code>./runagentsetup</code>. c. Uninstall the service in Global Parameters and exit the wizard. d. Perform a local upgrade to 8.2.0. e. Install the Connector as a service and exit the wizard. f. Start the service.
	<p>Connector logs show Fatal Exception error: Unable to find requested property 'transport.cef kafka.extra.prod.props'</p> <p>This message does not impact the performance or the functionality of the Connector.</p> <p>Workaround:</p> <p>If you are using a map file with an expression set in the <code><connector_install_location>\counterintelligence</code> location and the connector runs out of memory, add the following property to <code>agent.properties</code> as a workaround: <code>parser.operation.result.cache.enabled=false</code></p> <p>If this problem happens with Windows Event Log Native, and the above workaround does not completely solve the problem, reduce the value of the eventprocessorthreadcount Native connector parameter. You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your environment. Example:</p> <pre>agents[0].eventprocessorthreadcount=5 or agents[0].eventprocessorthreadcount=1, etc..</pre> <p>where 0 is the index of the Microsoft Windows Event Log - Native connector in the container.</p>
All File SmartConnectors	<p>When adding a log into a log file using the vi text editor, events are not sent to ESM</p> <p>Arcsight file connectors do not read events if the files are edited using the vi editor on Linux platforms.</p> <p>Workaround:</p> <p>Use the cat command to append data:</p> <p>Syntax:</p> <pre>cat >> log_file_name [Enter] "your logs" ctrl+c</pre>

Google Cloud SmartConnector	<p>The Google SmartConnector cannot authenticate tokens with Google API</p> <p>The following error is displayed when the connector is used from ArcMc with the One-Click feature:</p> <pre>{ "error" : "invalid_grant", "error_description" : "Invalid JWT: Token must be a short-lived token (60 minutes) and in a reasonable timeframe. Check your iat and exp values in the JWT claim." }</pre> <p>Workaround:</p> <p>The common cause is that the clock in the machine from which you are executing your task is not in sync with the Network Time Protocol (NTP). Match the connector time with the current time.</p>
--------------------------------	--

ArcMC Managed SmartConnectors	<p>SmartConnectors cannot be bulk-upgraded on a Linux server</p> <p>Workaround:</p> <p>Before performing a SmartConnector bulk upgrade from ArcMC on any Linux server including an ArcMC appliance, install the rng-tools on the corresponding Linux OS.</p> <p> Note: This procedure is not required if the connector is upgraded on a Windows server or if only one connector is upgraded per Linux server.</p> <p>To install and configure the rng-tools package after a fresh install, follow the steps mentioned for SmartConnector or Collector remote connections fail due to low entropy.</p> <p>One-Click installation fails on RHEL 8.1 or later, CentOS 8.1 or later, and SUSE 15 or later through ArcMC 2.9.4</p> <p>This issue might occur in other ArcMC versions.</p> <p>Workaround:</p> <p>Pre-requisites for instant connector or collector deployment:</p> <ul style="list-style-type: none">• Python2• Libselinux-python <p> Note: If the SmartConnector Linux machine does not have Python pre-installed, proceed with manual installation.</p> <p>To manually install Python:</p> <p>Apply these changes to the target Linux host (the VM where the connector or collector will be deployed):</p> <ol style="list-style-type: none">1. Install python2 by the following command: <code>sudo yum install -y python2</code>2. Create a symlink by the following command: <code>sudo ln -s /usr/bin/python2 /usr/bin/python</code>3. Install the libselinux-python package by the following command: <code>sudo yum install -y libselinux-python</code> <p> Note: If the yum command fails when installing libselinux-python, the rpm can be downloaded from: http://mirror.centos.org/centos/8/AppStream/x86_64/os/Packages/libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm</p>
-------------------------------	---

IBM Big Fix REST API	<p>Connector installation fails when the client properties file is auto populated incorrectly</p> <p>While installing the IBM Big Fix API connector through ArcMC, it populates the following incorrect path on the client properties file: "E:\depot\candidate\connector\GA\main\system\agent\config\bigfix_api\relevancequeryfile.properties". When the client properties file is auto populated incorrectly, the connector installation fails.</p> <p>Workaround:</p> <p>Set the following path manually:</p> <pre>\$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties</pre>
McAfee ePolicy Orchestrator DB	<p>Connector installation issue in FIPS mode</p> <p>Unable to install the McAfee ePolicy Orchestrator DB SmartConnector in FIPS Mode.</p> <p>Workaround:</p> <p>You must install the SmartConnector in non-FIPS mode only.</p>
Microsoft Message Trace REST API	<p>Issues with ArcMC upgrade behaviour in the Message Trace REST API connector</p> <p>Unable to upgrade the Message Trace Rest API Connector through ArcMC.</p> <p>Workaround:</p> <p>You can upgrade the Message Trace REST API Connector either using ESM or locally.</p>
Microsoft Windows Event Log (WiSC)	<p>WiSC SmartConnector issues</p> <p>WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. It has the following issues:</p> <ul style="list-style-type: none"> • Issue #1: High CPU utilization on the monitored Windows host (log endpoint) High CPU utilization is detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average). • Issue #2: WinRM inherent EPS limitations WinRM has an event rate limit of around 140 EPS (sustained). Therefore, it is not recommended to use the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates. <p>Workaround:</p> <p>To mitigate these issues, use the Microsoft Windows Event Log - Native. For more information, see the Technical Note on WinRM-related Issues.</p>

Known Issues

Microsoft Windows Event log - Native	<p>The Microsoft Windows Event Log - Native SmartConnector 8.4 is unable to receive events on Windows Server 2012 R2</p> <p>The communication between winc-agent (.NET component) and the SmartConnector (Java component) does not support TLS.</p> <p>Workaround:</p> <p>Because of the cipher suite support limitations in Microsoft Windows, the SmartConnectors 8.4 running on Window Server 2012 R2 must use 'Raw TCP' instead of the TLS protocol.</p> <p>To use 'Raw TCP', perform the following steps after installing the SmartConnector:</p> <ol style="list-style-type: none"> 1. Open the <ARCSIGHT HOME>/current/user/agent/agent.properties file. 2. Change the parameter value from agents[0].communicationprotocol=TLS to agents [0].communicationprotocol=Raw TCP 3. Restart the SmartConnector.
Microsoft Azure Monitor Event Hub	<p>Azure Event Hub debug mode issue</p> <p>Enable the Azure Event Hub Debug Mode for function apps for support purposes. Enabling it for normal operation can cause parsing and mapping errors.</p> <p>Workaround:</p> <p>To configure the debug mode:</p> <ol style="list-style-type: none"> 1. Go to Azure portal > Function app > Configuration. 2. Set the DebugMode application value to False. 3. Restart the Function App.

Load Balancer	<p>Load Balancer arc_connlb service does not start and displays an error message</p> <p>When you upgrade Load Balancer while the services are still running, after the successful upgrade, the Load Balancer arc_connlb service does not start and displays an error message in the lb.out.wrapper.log even after you start the arc_connlb service manually.</p> <p>Workaround: When you upgrade Load Balancer while the services are still running, the system displays a notification message to stop all the programs before continuing with the upgrade. However, it does not mention the specific services you need to stop. Perform the following steps to fix this issue:</p> <ol style="list-style-type: none">1. After you install Load Balancer as a service, before you upgrade, stop the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb stop</code> or <code>service arc_connlb stop</code>2. After Load Balancer is successfully upgraded, start the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb start</code> or <code>service arc_connlb start</code>
---------------	---

Connector End-of-Life Notices



Note: For information about connector end-of-life status, refer to [Connector End-of-Life Notices](#) on the [ArcSight SmartConnector 8.4 Documentation](#) page.

SmartConnector End of Support Announcements

SmartConnector	End of Support Date	Details
Connectors in Transformation Hub (CTH) and Collectors	11/2025	The CTH and Collectors are supported in this release and are deprecated as of 8.4. CTH functionality and Collectors will be removed in an upcoming release, by March 31, 2024. CTH and Collectors will have limited support for customers already using these components until the end of support date for the ArcSight Connector 8.4.0 release.

SmartConnectors No Longer Supported

SmartConnector	End of Support Date	Details
Model Import Connector for Malware Information Sharing Platform (MISP)	06/2023	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Model Import Connector for Micro Focus Security ArcSight Reputation Security Monitor Plus (RepSM Plus)	10/2022	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Microsoft Windows Event Log – Unified Connector (WUC)	12/2021	Lack of customer demand.
Microsoft Forefront Threat Management Gateway (TMG) 2010	04/2020	End of support by vendor.
Windows Server 2008 R2	01/2020	End of support by vendor.

SmartConnector Release Notes
Connector End-of-Life Notices

Checkpoint Syslog	12/2019	The vendor no longer supports version R77.30. Therefore, we offer limited support. Fixes and improvements are no longer provided for this version.
Solsoft Policy Serve	11/2019	Lack of customer demand.
Oracle Audit DB version 9	08/2019	End of support by vendor.
All 32-bit SmartConnectors	04/2018	Supported only 64-bit SmartConnectors.
Symantec Endpoint Protection DB – SEP version 1	02/2018	End of support by vendor.
Solaris 10 Premier support	01/2018	End of support by vendor.

Publication Status

Released: July 2023

Updated: July 2023

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 Release Notes (SmartConnectors 8.4.2)

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!



ArcSight SmartConnectors

Software Version: 8.4.3

SmartConnector Release Notes

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

Release Highlights	4
What's New	5
New SmartConnectors and Modules	6
Cloud Updates	7
Security Updates	8
Version Updates	8
Platform Support	8
SmartConnector Enhancements	9
Software Fixes	9
Event Categorization Updates	11
SmartConnector Parser Support Policy	13
Installing SmartConnectors	14
System Requirements	14
Downloading the SmartConnector 8.4.3 Installation Packages	14
Upgrading SmartConnectors	16
Upgrading to 8.4.3	16
Deleting Older Vulnerable Libraries after Upgrading a Connector	16
Known Issues	19
Connector End-of-Life Notices	27
SmartConnector End of Support Announcements	27
SmartConnectors No Longer Supported	27
Send Documentation Feedback	29

Release Highlights

The SmartConnector 8.4.3 release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Created a new [SmartConnector for Mulesoft Audit](#)
- Created a new [SmartConnector for Terraform Cloud](#)
- Created a new [SmartConnector for Trellix ePolicy Orchestrator DB](#)
- Added Amazon Security Lake log source for the Amazon S3 SmartConnector
- Certified RHEL versions 8.8, 9.0, 9.1, and 9.2 as installation platforms
- Certified Rocky Linux 8.8 as installation platform
- Certified F5 BIG-IP Syslog version 14.1.5
- Certified Tenable Nessus .nessus File version 10.4.0
- Certified Fortinet Fortigate Syslog version 6.2.0
- Certified Cisco ISE Syslog version 3.1
- Certified IBM eServer iSeries Audit Journal File V5R3 Type 5 version 7.4
- Certified Microsoft DHCP File logs for Microsoft Windows Server 2019
- Certified Microsoft DNS Trace Log Multiple Server File for Microsoft Windows Server 2022
- Upgraded Zulu OpenJDK to 8u382
- Upgraded Tomcat version to 9.0.76

For detailed information, see "[What's New](#)" on the next page.

The Connector Team has worked tirelessly, and in a few cases, have enjoyed the benefits of partnering with some of the customers to overcome some of the issues. The extra effort from the customer success and support teams, and especially customers, in helping the team understand and reproduce some difficult situations in order to improve the SmartConnectors is duly appreciated.

Additionally, the [ArcSight Idea Exchange portal](#), will be updated with affected entries and monitored to help, prioritize, and plan new features for next release.

What's New

SmartConnector 8.4.3 incorporates the following SmartConnector and content and categorization updates:

- [New SmartConnectors and Modules](#)
- [Cloud Updates](#)
- [Security Updates](#)
- [Version Updates](#)
- [Platform Support](#)
- [SmartConnector Enhancements](#)
- [Software Fixes](#)
- [Event Categorization Updates](#)

New SmartConnectors and Modules

New SmartConnectors/ Application Module	Description
Mulesoft Audit	<p>SmartConnector for Mulesoft Audit Logs aims at retrieving the audit logs through the Audit logging query API. Mulesoft is a platform that gives IT administrators the tools to automate everything in their organization. This includes integrating data and systems and automating workflows and processes. It creates high-quality digital experiences, all on a single, easy-to-use platform. With the unique approach offered by Mulesoft, IT creates the digital building blocks that can be used as required, with all the right security, governance, and compliance measures built in.</p> <p>For information about installing and configuring Mulesoft Audit SmartConnector, see Configuration Guide for SmartConnector for Mulesoft Audit.</p>
Terraform Cloud	<p>Terraform Cloud enables infrastructure automation for provisioning, compliance, and management of any cloud, data center, and service.</p> <p>The Audit Trails API provides access to a continuous flow of audit events that detail modifications made to application entities (such as workspaces, runs, etc.) associated with a Terraform Cloud organization.</p> <p>Access to audit trails requires a paid subscription, which is included in the Terraform Cloud for a Business (TFCB) upgrade package. For more information, refer to the Terraform Cloud pricing page.</p> <p>For information about installing and configuring the Terraform Cloud SmartConnector, see Configuration Guide for SmartConnector for Terraform Cloud.</p>

New SmartConnectors/ Application Module	Description
Trellix ePolicy Orchestrator DB	<p>The Trellix Endpoint Security (ENS) protect and empower your workforce with an integrated security framework that protects every endpoint. Endpoint Security intercepts threats, monitors overall system health, and reports detection and status information. Client software is installed on each system to perform these tasks.</p> <p>The Trellix Endpoint Security connector is installed on the client computers to connect to the Trellix DB where it gathers and reports the overall system health, reports detection and status information. Install one or more Endpoint Security modules on client systems, manage detections, and configure settings that determine how product features work.</p> <p>For information about installing and configuring Trellix SmartConnector, see Configuration Guide for SmartConnector for Trellix ePolicy Orchestrator DB.</p>

Cloud Updates

Application Module	Description
Amazon S3	<p>Added support for Amazon Security Lake log source.</p> <p>Amazon Security Lake Integration automates the collection of security-related log and event data from integrated AWS services and third-party services.</p> <p>The Amazon S3 SmartConnector collects and parses the Open Cybersecurity Schema Framework (OCSF) logs that are stored in an Amazon S3 bucket by Amazon Security Lake.</p> <p>For more information, see Amazon Security Lake in Configuration Guide for Amazon S3 SmartConnector.</p>

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	<p>Upgraded Zulu OpenJDK to 8u382.</p> <p>The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade:</p> <ul style="list-style-type: none"> • CVE-2023-22043 • CVE-2023-22045 • CVE-2023-22049
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.76.

Version Updates

Application Module Version Updates	Description
Cisco ISE Syslog	Added support for Cisco ISE Syslog version 3.1 logs.
F5 BIG-IP Syslog	Added support for Cisco ISE Syslog version 14.1.5 logs.
Fortinet Fortigate Syslog	Added support for Fortinet Fortigate Syslog version 6.2.0 logs.
IBM eServer iSeries Audit Journal File	Added support for IBM eServer iSeries Audit Journal File for V5R3 Type 5 version 7.4.
Microsoft DHCP File	Added support for the Microsoft DHCP File logs for Microsoft Windows Server 2019.
Microsoft DNS Trace Log Multiple Server File	Added support for Microsoft DNS Trace Log Multiple Server File for Microsoft Windows Server 2022.
Tenable Nessus .nessus File	Added support for Tenable Nessus .nessus File for version 10.4.0.

Platform Support

Application Module Platform Support	Description
All SmartConnectors and Load Balancer	Added platform support for RHEL 8.8, 9.0, 9.1, and 9.2.
All SmartConnectors and Load Balancer	Added support for Rocky Linux 8.8.

For details about hardware, software or platform, and SmartConnector requirements, refer to the [Compatibility Matrix of SmartConnector section](#) of the [Technical Requirements for SmartConnectors](#).

SmartConnector Enhancements

Application Module Enhancements	Description
All SmartConnectors	<p>Added a new property named remote.management.listener.client.ip.allow. This property is used to accommodate IPv4 addresses and is designated for ArcMc instances, which allows precise control over the access of the connector for the specific addresses.</p> <p>Note: The remote.management.listener.client.ip.allow property does not support hostnames.</p> <p>For more information, see Remotely Managing Software-Based Connectors in Installation and User Guide for SmartConnector.</p>

Software Fixes

The following issues are fixed in the 8.4.3 release:

Application Modules Software Fixes	Description
All SmartConnectors	<p>The connector could not be added as a host to ArcMC when using the the FQDN with 8.4.1 p3 and above.</p> <p>Fix: The issue has been fixed now.</p>
ArcSight Common Event Format File	<p>When the connector sent some events containing the dpriv field to the ESM destination, the Target User Privileges column for each of the events was not updated correctly in ESM. Instead, the Target User Privileges column was updated with a fixed value for all events.</p> <p>Fix: The ESM export now displays the correct values in the Target User Privileges column for all events.</p>
AWS Security Hub	<p>The AWS Security Hub connector was unable to parse the JSON format logs that contained line feed characters such as \n, because the logs were fragmented into multiple lines.</p> <p>Fix: The approach for parsing JSON logs has been changed to ensure that all occurrences of \n are removed. This effectively prevents the logs from being split into multiple lines.</p>

Application Modules Software Fixes	Description
Linux Audit Syslog	<p>The connector was unable to merge and parse RHEL 8.3 logs by using the event merging function.</p> <p>Fix: The parser file has been modified to enhance the support for RHEL 8.3 event logs.</p>
McAfee ePolicy Orchestrator DB	<p>The devicecustomIPV6address field is being populated with an IPv4 value instead of IPv6 value. This issue occurs because, for security reasons, the value of the ThreatsourceIPV6 field is a hash code present in the raw logs and the devicecustomIPV6address field is mapped to the ThreatsourceIPV6 field.</p> <p>Fix: Because the hash code cannot be directly converted to an IPv6 value and all the devicecustomstrings are already populated, the hash code is displayed as is in the SourceIPV6Address and DestinationIPV6Address fields, indicating that.</p>
	<p>The McAfee ePolicy Orchestrator DB 8.0 connector was unable to capture and accurately map the SourceDescription field to the corresponding ArcSight field.</p> <p>Fix: The endpoint security parser file has been updated to capture the SourceDescription field and to subsequently enable its mapping to a new ArcSight data field named SourceDescription.</p>
Microsoft Azure Event Hub	<p>The Microsoft Azure Event Hub connector presently limits the length of the rawEvent field for Defender for Endpoint. This results in the truncation of the field value if it's length exceeds the limit.</p> <p>Fix: A fix has been implemented to avoid the rawEvent field truncation.</p>
	<p>The Microsoft Azure Event Hub Connector was omitting the backslash character \ from the output field values.</p> <p>Fix: This issue has been resolved by populating the backslashes.</p>
Microsoft DNS Trace Log Multiple Server File	<p>The connector was not able to parse and process the event logs after upgrading it from 8.4.0 to 8.4.1. It was showing start and end file processing with no cache or errors.</p> <p>Fix: Added framework code to handle the parsing issue of the events.</p>

Application Modules Software Fixes	Description
Microsoft Windows Event Log - Native	<p>When the Microsoft Windows Event Log - Native connector was configured with the Windows Event Forwarder (WEF) mode, it was unable to receive events forwarded to a Windows Event Collector (WEC) host causing the WiNC agent to crash. The connector was facing issues because of the Microsoft Windows Server 2022 changes.</p> <p>Fix: Now, the Microsoft Windows Event Log - Native connector receives events that are forwarded to a Windows Event Collector (WEC) host.</p>
MS Windows Event Log – Native SmartConnector (WiSC)	<p>The WiSC connector 8.4 was unable to receive events from remote hosts and was throwing a Java exception.</p> <p>Fix: The "Apache CXF Runtime" and "jaxb-impl" jar files and their dependencies have been upgraded to the compatible versions.</p>
Tenable Nessus .nessus File	<p>The connector was aggregating the vulnerabilities using the hostname, as there was no option to reconfigure the connector to aggregate the vulnerabilities while using IP address. This happens if the .nessus file does not contain hostname information but contains only IP for some assets in the file.</p> <p>Fix: A new property useIP has been added to <code>agent.properties</code>, which by default is false. If this property is set to true it will reconfigure the connector to aggregate the vulnerabilities using IP address. Based on this property, the vulnerabilities will be mapped using either hostname or IP.</p>

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the 8.4.3 release:

- Cisco ISE 1
- IBM X-Force XPU 4212.12221
- Juniper IDP Content Version 3622, 3614, and 3604
- McAfee Network Security Manager 11.10.8.1, 11.10.7.1, and 11.10.6.1
- Microsoft SharePoint 2010
- Microsoft Windows
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0

- Sourcefire SEU 31470, and 2983
- Symantec Network Security 7100 1659, 7100 1639, and 7100 1621
- TippingPoint SMS IPS DV9814, DV9807, and DV9800
- UNIX syslog

For more information, see [Event Content-Categorization updates August 2023](#) in the [Release Notes for ArcSight Content AUP -Categorization Updates 2023](#).

SmartConnector Parser Support Policy

Inline with the documents [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#), [Technical Requirements for SmartConnectors](#), the note at the top of the [SmartConnector Grand List \(A-Z\) documentation](#) page, we would like to take this opportunity to clarify what is meant by Connector Support.

As mentioned in the note on the [SmartConnector Grand List \(A-Z\) documentation](#) page:

The device versions currently documented as **certified** are versions that have been tested by ArcSight Quality Assurance. For device releases that fall in between certified major versions, it has been our experience that vendors typically do not make significant changes to the event generation mechanism.

Oftentimes, there are few, if any, significant changes even between major versions to the event logs. Therefore, we consider all device releases to be supported, with the understanding that major version releases may not work as expected, depending on the types of changes made to that major version.

Where possible, minor adjustments can be accommodated by parser overrides as needed. For example, Extreme Networks Dragon Export Tool versions 7.4 and 8.2 have been certified; Dragon Export Tool version 7.5 is also supported, as well as versions 8.3 or 9.0 should they be released.

In other words, if we have a SmartConnector with any certified version of a device, that device is supported regardless of version as long as the version in question is supported by the vendor.

In the situations where parser overrides cannot provide adequate functionality to support a new major or minor version of a device release, the Support Team will elevate the issue to the appropriate development teams.

Please be aware that the development team may not have immediate access to the updated device and logs. Support will request that you attach the unparsed or improperly parsed logs to your support ticket.

Please also note that we have a log anonymization/sanitization tool that you can use to remove sensitive information from logs we would need you to submit.

We may also request a conference call with you to help clarify or expedite any issues, especially if the device's connection and logging methods have changed.

For details as to the need to collect logs or possible vendor changes to devices, please see [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#).

Installing SmartConnectors

For information about installing SmartConnector, see the [Installing SmartConnectors](#) section in Installation Guide for ArcSight SmartConnectors.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to [Technical Requirements for SmartConnectors](#).

Downloading the SmartConnector 8.4.3 Installation Packages

You can download the SmartConnector installation packages for your platform from the [Software Licenses and Downloads \(SLD\)](#). The installation packages include their respective signature files for validating that the downloaded software is authentic and has not been tampered with by a third party.

File Name	Description
ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-8.4.3.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.3.xxxx.0-Collectors-Linux64.bin	This is the 64-bit Collector installer for Linux.
ArcSight-8.4.3.xxxx.0-Collectors-Win64.exe	This is the 64-bit Collector installer for Windows.
ArcSight8.4.3.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.3.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.3.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.3.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.3.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.3.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.3.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.

SmartConnector Release Notes

Installing SmartConnectors

ArcSight-8.4.3.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.3.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.3.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.3.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.3.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.3.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.3.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.
ArcSightSmartConnectorLoadBalancer-opensource-8.4.3.xxxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.3.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.3.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading SmartConnectors

Upgrading to 8.4.3



Important: If you use any of the SmartConnectors listed in the [Software Fixes](#) section, note that installing the updated SmartConnector can impact your created content.

Verifying Your Upgrade Files

OpenText provides a digital public key for you to verify that the signed software you received is indeed from OpenText and has not been manipulated in any way by a third party.

For information and instructions, see [Verifying Micro Focus Signatures with gpg or rpm](#).



Note: If a Parser Override was provided, determine whether the Bug or Feature Request number is included in the Fixed or Enhancements section. If the number is not listed, do not upgrade the Connector. You can test the upgrade in a STAGE (staging) environment to ensure it works as expected before you upgrade your environment PROD (production)

Upgrading SmartConnector to 8.4.3

You can upgrade a SmartConnector to implement the newly introduced features, mapping improvements and overall functionality of a SmartConnector. You can upgrade connectors either locally or remotely. Connectors automatically determine their upgrade status when they start.

For information and instructions, see [Upgrading SmartConnectors](#).

Upgrading Load Balancer to 8.4.3

For information about upgrading Load Balancer to 8.4.3, see [Upgrading Load Balancer](#).

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.



Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:



Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command: `cd Xxxxx/lib/agent`
3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`
5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
6. Run the following command: `cd Xxxxx/lib/agent/axis`
7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Open the `Xxxxx\lib\agent` folder.
3. Search for **log4j** and delete all the entries.
4. Open the `Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\` folder.
5. Search for **log4j** and delete all the entries.

6. Open the **Xxxxx\lib\agent\axis** folder.
7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm -rf X8444`)

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Delete the **Xxxxx** folder manually.

Known Issues

This section includes legacy issues from the ArcSight Installer.

Application Module	Description
All SmartConnectors	<p>SmartConnector or Collector remote connections fail due to low entropy</p> <p>Note: The CTH and Collectors are supported in this release and are deprecated as of 8.4. CTH functionality and Collectors will be removed in an upcoming release, by March 31, 2024</p> <p>All SmartConnectors or Collectors remote connections go through SSL and they depend on the Operating System random number pool (entropy pool) to generate private keys for secure communication. When the entropy pool is less than the ideal lower limit of 1000, the keys are not generated, communication cannot be established and the SmartConnector or Collector does not start. In cloud hosted Linux instances, the entropy pool value can be less than 1000.</p> <p>Workaround:</p> <p>To ensure that the entropy value is at the desired level:</p> <ol style="list-style-type: none"> 1. Install the rng-tools package: <code>sudo yum install -y rng-tools</code> 2. Add the following line to the /etc/sysconfig/rngd file: <code>EXTRAOPTIONS="-r /dev/urandom"</code> 3. Check the entropy availability in the system: <code>cat /proc/sys/kernel/random/entropy_avail</code> 4. Start the rngd package as root user: <code>service rngd start</code> 5. Enable the rngd service to start at the system start-up: <code>systemctl enable rngd.service</code> <code>systemctl start rngd.service</code> 6. Ensure that the rngd package is always running (even after a reboot) as root user: <code>chkconfig --level 345 rngd on</code> 7. Check the entropy availability in the system, after starting the rngd service: <code>cat /proc/sys/kernel/random/entropy_avail</code>
	<p>Unable to install connector because of missing packages</p> <p>Workaround:</p> <p>Ensure that the following packages are installed:</p> <ol style="list-style-type: none"> 1. <code>yum install -y unzip</code> 2. <code>yum install -y fontconfig \ dejavu-sans-fonts</code>

All SmartConnectors installed on Solaris	<p>When upgrading SmartConnectors on Solaris, a timeout error is displayed</p> <p>Workaround:</p> <ul style="list-style-type: none"> • If the Solaris connector is already installed as a standalone, locally upgrade to 8.2.0. • If the Solaris Connector is installed as a service: <ol style="list-style-type: none"> a. Stop the service. b. Go to HOME/current/bin and execute <code>./runagentsetup</code>. c. Uninstall the service in Global Parameters and exit the wizard. d. Perform a local upgrade to 8.2.0. e. Install the Connector as a service and exit the wizard. f. Start the service.
	<p>Connector logs show Fatal Exception error: Unable to find requested property 'transport.cef kafka.extra.prod.props'</p> <p>This message does not impact the performance or the functionality of the Connector.</p> <p>Workaround:</p> <p>If you are using a map file with an expression set in the <code><connector_install_location>\counterintelligence</code> location and the connector runs out of memory, add the following property to <code>agent.properties</code> as a workaround: <code>parser.operation.result.cache.enabled=false</code></p> <p>If this problem happens with Windows Event Log Native, and the above workaround does not completely solve the problem, reduce the value of the eventprocessorthreadcount Native connector parameter. You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your environment. Example:</p> <pre>agents[0].eventprocessorthreadcount=5 or agents[0].eventprocessorthreadcount=1, etc..</pre> <p>where 0 is the index of the Microsoft Windows Event Log - Native connector in the container.</p>
All File SmartConnectors	<p>When adding a log into a log file using the vi text editor, events are not sent to ESM</p> <p>Arcsight file connectors do not read events if the files are edited using the vi editor on Linux platforms.</p> <p>Workaround:</p> <p>Use the cat command to append data:</p> <p>Syntax:</p> <pre>cat >> log_file_name [Enter] "your logs" ctrl+c</pre>

Google Cloud SmartConnector	<p>The Google SmartConnector cannot authenticate tokens with Google API</p> <p>The following error is displayed when the connector is used from ArcMc with the One-Click feature:</p> <pre>{ "error" : "invalid_grant", "error_description" : "Invalid JWT: Token must be a short-lived token (60 minutes) and in a reasonable timeframe. Check your iat and exp values in the JWT claim." }</pre> <p>Workaround:</p> <p>The common cause is that the clock in the machine from which you are executing your task is not in sync with the Network Time Protocol (NTP). Match the connector time with the current time.</p>
--------------------------------	--

ArcMC Managed SmartConnectors	<p>SmartConnectors cannot be bulk-upgraded on a Linux server</p> <p>Workaround:</p> <p>Before performing a SmartConnector bulk upgrade from ArcMC on any Linux server including an ArcMC appliance, install the rng-tools on the corresponding Linux OS.</p> <p> Note: This procedure is not required if the connector is upgraded on a Windows server or if only one connector is upgraded per Linux server.</p> <p>To install and configure the rng-tools package after a fresh install, follow the steps mentioned for SmartConnector or Collector remote connections fail due to low entropy.</p> <p>One-Click installation fails on RHEL 8.1 or later, CentOS 8.1 or later, and SUSE 15 or later through ArcMC 2.9.4</p> <p>This issue might occur in other ArcMC versions.</p> <p>Workaround:</p> <p>Pre-requisites for instant connector or collector deployment:</p> <ul style="list-style-type: none">• Python2• Libselinux-python <p> Note: If the SmartConnector Linux machine does not have Python pre-installed, proceed with manual installation.</p> <p>To manually install Python:</p> <p>Apply these changes to the target Linux host (the VM where the connector or collector will be deployed):</p> <ol style="list-style-type: none">1. Install python2 by the following command: <code>sudo yum install -y python2</code>2. Create a symlink by the following command: <code>sudo ln -s /usr/bin/python2 /usr/bin/python</code>3. Install the libselinux-python package by the following command: <code>sudo yum install -y libselinux-python</code> <p> Note: If the yum command fails when installing libselinux-python, the rpm can be downloaded from: http://mirror.centos.org/centos/8/AppStream/x86_64/os/Packages/libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm</p>
-------------------------------	---

IBM Big Fix REST API	<p>Connector installation fails when the client properties file is auto populated incorrectly</p> <p>While installing the IBM Big Fix API connector through ArcMC, it populates the following incorrect path on the client properties file: "E:\depot\candidate\connector\GA\main\system\agent\config\bigfix_api\relevancequeryfile.properties". When the client properties file is auto populated incorrectly, the connector installation fails.</p> <p>Workaround:</p> <p>Set the following path manually:</p> <pre>\$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties</pre>
Microsoft Message Trace REST API	<p>Issues with ArcMC upgrade behaviour in the Message Trace REST API connector</p> <p>Unable to upgrade the Message Trace Rest API Connector through ArcMC.</p> <p>Workaround:</p> <p>You can upgrade the Message Trace REST API Connector either using ESM or locally.</p>
Microsoft Windows Event Log (WiSC)	<p>WiSC SmartConnector issues</p> <p>WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. It has the following issues:</p> <ul style="list-style-type: none"> • Issue #1: High CPU utilization on the monitored Windows host (log endpoint) High CPU utilization is detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average). • Issue #2: WinRM inherent EPS limitations WinRM has an event rate limit of around 140 EPS (sustained). Therefore, it is not recommended to use the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates. <p>Workaround:</p> <p>To mitigate these issues, use the Microsoft Windows Event Log - Native. For more information, see the Technical Note on WinRM-related Issues.</p>

Known Issues

Microsoft Windows Event log - Native	<p>The Microsoft Windows Event Log - Native SmartConnector 8.4 is unable to receive events on Windows Server 2012 R2</p> <p>The communication between winc-agent (.NET component) and the SmartConnector (Java component) does not support TLS.</p> <p>Workaround:</p> <p>Because of the cipher suite support limitations in Microsoft Windows, the SmartConnectors 8.4 running on Window Server 2012 R2 must use 'Raw TCP' instead of the TLS protocol.</p> <p>To use 'Raw TCP', perform the following steps after installing the SmartConnector:</p> <ol style="list-style-type: none"> 1. Open the <ARCSIGHT HOME>/current/user/agent/agent.properties file. 2. Change the parameter value from agents[0].communicationprotocol=TLS to agents [0].communicationprotocol=Raw TCP 3. Restart the SmartConnector.
Microsoft Azure Monitor Event Hub	<p>Azure Event Hub debug mode issue</p> <p>Enable the Azure Event Hub Debug Mode for function apps for support purposes. Enabling it for normal operation can cause parsing and mapping errors.</p> <p>Workaround:</p> <p>To configure the debug mode:</p> <ol style="list-style-type: none"> 1. Go to Azure portal > Function app > Configuration. 2. Set the DebugMode application value to False. 3. Restart the Function App.

Load Balancer	<p>Load Balancer arc_connlb service does not start and displays an error message</p> <p>When you upgrade Load Balancer while the services are still running, after the successful upgrade, the Load Balancer arc_connlb service does not start and displays an error message in the lb.out.wrapper.log even after you start the arc_connlb service manually.</p> <p>Workaround: When you upgrade Load Balancer while the services are still running, the system displays a notification message to stop all the programs before continuing with the upgrade. However, it does not mention the specific services you need to stop. Perform the following steps to fix this issue:</p> <ol style="list-style-type: none">1. After you install Load Balancer as a service, before you upgrade, stop the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb stop</code> or <code>service arc_connlb stop</code>2. After Load Balancer is successfully upgraded, start the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb start</code> or <code>service arc_connlb start</code>
---------------	---

Trellix ePolicy Orchestrator DB	<p>Reregistration of the Trellix Orchestrator DB type connector fails with ESM as the destination</p> <p>When you re-register the Trellix Orchestrator DB type connector with ESM as the destination, the reregistration fails and the connector displays an error (null) message,</p> <p>Workaround:</p> <p>Perform the following steps for re-registering the connector on ESM using ArcMC:</p> <ol style="list-style-type: none">1. Enable the remote management mode in the connector using runagentsetup script, with port range of 9001-9010.2. Navigate to Node Management > View all nodes in ArcMC.3. Enter the Location and provide a name for the location, and then click Next.4. Specify the location of your computer as the host, and then click Add.5. Enter the Type of the SmartConnector.6. Enter the user and password as User:connector_user and Password:change_me and click Add and Import certificate.7. Navigate to Node management > View all nodes.8. Click Connectors > Connector > Destinations.9. Click Next > Re-register destination.10. Click Failed destination.11. Enter the user and password for ESM and click Next.12. Click Yes > Done. <p>The connector is now linked to ESM with a new name.</p> <p>Error is displayed while importing the parameters of the Trellix Orchestrator DB type connector</p> <p>While installing the Trellix Orchestrator DB type connector, if you import its parameters instead of manually specifying them on the screen, an error message is displayed and the installation is terminated.</p> <p>Workaround:</p> <p>While installing the connector, manually specify the parameters instead of importing them.</p>
---------------------------------	---

Connector End-of-Life Notices



Note: For information about connector end-of-life status, refer to [Connector End-of-Life Notices](#) on the [ArcSight SmartConnector 8.4 Documentation](#) page.

SmartConnector End of Support Announcements

SmartConnector	End of Support Date	Details
Connectors in Transformation Hub (CTH) and Collectors	11/2025	The CTH and Collectors are supported in this release and are deprecated as of 8.4. CTH functionality and Collectors will be removed in an upcoming release, by March 31, 2024. CTH and Collectors will have limited support for customers already using these components until the end of support date for the ArcSight Connector 8.4.0 release.

SmartConnectors No Longer Supported

SmartConnector	End of Support Date	Details
Model Import Connector for Malware Information Sharing Platform (MISP)	06/2023	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Model Import Connector for Micro Focus Security ArcSight Reputation Security Monitor Plus (RepSM Plus)	10/2022	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Microsoft Windows Event Log – Unified Connector (WUC)	12/2021	Lack of customer demand.
Microsoft Forefront Threat Management Gateway (TMG) 2010	04/2020	End of support by vendor.
Windows Server 2008 R2	01/2020	End of support by vendor.

SmartConnector Release Notes
Connector End-of-Life Notices

Checkpoint Syslog	12/2019	The vendor no longer supports version R77.30. Therefore, we offer limited support. Fixes and improvements are no longer provided for this version.
Solsoft Policy Serve	11/2019	Lack of customer demand.
Oracle Audit DB version 9	08/2019	End of support by vendor.
All 32-bit SmartConnectors	04/2018	Supported only 64-bit SmartConnectors.
Symantec Endpoint Protection DB – SEP version 1	02/2018	End of support by vendor.
Solaris 10 Premier support	01/2018	End of support by vendor.

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 Release Notes (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 24.1

SmartConnector 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 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

Release Highlights	4
What's New	5
New SmartConnectors and Modules	5
Cloud Updates	6
Security Updates	7
Version Updates	7
Platform Support	7
SmartConnector Enhancements	8
Software Fixes	9
Event Categorization Updates	11
SmartConnector Parser Support Policy	12
Installing SmartConnectors	13
System Requirements	13
Downloading the SmartConnector Installation Packages	13
Upgrading SmartConnectors	16
Upgrading to CE 24.1 (v8.4.4)	16
Deleting Older Vulnerable Libraries after Upgrading a Connector	16
Known Issues	19
Connector End-of-Life Notices	27
SmartConnector End of Support Announcements	27
SmartConnectors No Longer Supported	27
Send Documentation Feedback	29

Release Highlights

The SmartConnector CE 24.1 (v8.4.4) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Rebranded both the documents and products to OpenText
- New [SmartConnector for GitHub Enterprise Audit Log](#)
- Support for the following new device sources:
 - [VMware Carbon Black EDR](#)
 - [CyberArk Privileged Access Security version 11.3](#)
 - [OpenText Network Detection & Response \(Bricata\)](#)
- Certified version 9.2 for Red Hat Enterprise Linux (RHEL) logs for the Linux Audit File, Linux Audit Syslog, UNIX Login/Logout File, and UNIX OS Syslog connectors
- Support for the following Trellix Endpoint Security modules:
 - SolidCore 8.3
 - Threat Intelligence Exchange Server 4.0
 - Trellix Security for SharePoint 3.5
- Certified version 9.2 for Rocky Linux as the installation platform
- Support for registration URL for the **ArcSight SaaS** destination
- Certified version 15.1 for Juniper JUNOS Syslog
- Certified version 7200-05 for IBM AIX Audit Syslog
- Certified version(s) 8.5.161.0 and 8.3.14.0 for Cisco Wireless LAN Controller Syslog
- Certified version 5 v2.72 for HPE Integrated Lights-Out Syslog
- Upgrade of Zulu OpenJDK to 8u392
- Upgrade of Tomcat version to 9.0.82

For detailed information, see "[What's New](#)" on the next page.

The Connector Team has worked tirelessly, and in a few cases, have enjoyed the benefits of partnering with some of the customers to overcome some of the issues. The extra effort from the customer success and support teams, and especially customers, in helping the team understand and reproduce some difficult situations in order to improve the SmartConnectors is duly appreciated.

Additionally, the [ArcSight Idea Exchange portal](#), will be updated with affected entries and monitored to help, prioritize, and plan new features for next release.

What's New

SmartConnector CE 24.1 incorporates the following SmartConnector and content and categorization updates:

- [New SmartConnectors and Modules](#)
- [Cloud Updates](#)
- [Security Updates](#)
- [Version Updates](#)
- [Platform Support](#)
- [SmartConnector Enhancements](#)
- [Software Fixes](#)
- [Event Categorization Updates](#)

New SmartConnectors and Modules

New SmartConnectors/ Application Module	Description
CyberArk Privileged Access Security	<p>SmartConnector for CyberArk Privileged Access Security collects the CEF formatted logs and parse them to the desired destination. The key agent in this facility is syslog connector. It receives messages and routes them to their destination based on configuration information provided in the /etc/syslog.conf file.</p> <p>The CyberArk's Privileged Access Security (PAS) solution is a full life-cycle solution for managing the most privileged accounts and SSH Keys in the enterprise. It enables organizations to secure, provision, manage, control, and monitor all activities associated with all types of privileged identities.</p> <p>For more information, see Configuration Guide for CyberArk Privileged Access Security SmartConnector.</p>
GitHub Enterprise Audit Log	<p>SmartConnector for GitHub Enterprise Audit Log retrieves audit trail events through the GitHub Rest API, normalizes the events, and then sends them to the configured destinations.</p> <p>For more information, see Configuration Guide for GitHub Enterprise Audit Log SmartConnector.</p>

New SmartConnectors/ Application Module	Description
OpenText Network Detection & Response (Bricata)	<p>SmartConnector for OpenText Network Detection & Response (Bricata) collects the logs from Bricata and leads the next generation of advanced network detection and response solutions for the enterprise. With fusing detection, forensic analysis and proactive threat hunting, OpenText NDR empowers high-performance enterprise security teams with total visibility into network traffic and also empowers security teams to effectively defend against known threats and to illuminate those otherwise unseen.</p> <p>For more information, see Configuration Guide for OpenText Network Detection & Response (Bricata) SmartConnector.</p>
VMware Carbon Black EDR	<p>SmartConnector for VMware Carbon Black EDR collects the CEF formatted logs and parse them to the desired destination. The key agent in this facility is syslog connector. It receives messages and routes them to their destination based on configuration information provided in the <code>/etc/syslog.conf</code> file. VMware Carbon Black EDR is an incident response and threat hunting solution designed for Security Operations Center teams with offline environments or on-premises requirements.</p> <p>Carbon Black EDR continuously records and stores endpoint activity data so security professionals can hunt threats in real time and visualize the complete attack kill chain, using the VMware Carbon Black Cloud's aggregated threat intelligence.</p> <p>For more information, see Configuration Guide for VMware Carbon Black EDR SmartConnector.</p>

Cloud Updates

None at this time.

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	<p>Upgraded Zulu OpenJDK to 8u392.</p> <p>The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade:</p> <ul style="list-style-type: none"> • CVE-2023-22067 • CVE-2023-22081
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.82.

Version Updates

Application Module Version Updates	Description
Cisco Wireless LAN Controller Syslog	Certified version(s) 8.5.161.0 and 8.3.14.0 for Cisco Wireless LAN Controller Syslog logs.
Juniper JUNOS Syslog	Certified version 15.1 for Juniper JUNOS Syslog logs.
IBM AIX Audit Syslog	Certified version 7200-05 for IBM AIX Audit Syslog logs.
<ul style="list-style-type: none"> • Linux Audit File • Linux Audit Syslog • UNIX Login/Logout File • UNIX OS Syslog 	Certified version 9.2 for Red Hat Enterprise Linux (RHEL).
HPE Integrated Lights-Out Syslog	Certified version 5 v2.72 for HPE Integrated Lights-Out Syslog logs.

Platform Support

Application Module Platform Support	Description
All SmartConnectors and Load Balancer	Added support for Rocky Linux 9.2.

For details about hardware, software or platform, and SmartConnector requirements, refer to the [Compatibility Matrix of SmartConnector section](#) of the [Technical Requirements for SmartConnectors](#).

SmartConnector Enhancements

Application Module Enhancements	Description
All SmartConnectors	<p>Added support for registration URL for the ArcSight SaaS destination.</p> <p>If ArcSight SaaS is configured as a destination, all security events are sent in the Avro format to Amazon MSK that is managed by ArcSight's SaaS offering.</p> <p>For more information about the destinations parameters to be selected during installation, see ArcSight SaaS.</p>
All SmartConnectors	<p>The CEF 1.2 schema has now been updated with the following new CEF fields:</p> <p>Note: The ParserVersion and ParserIdentifier parameters are applicable only for CEF Version 1.0.</p> <ul style="list-style-type: none"> • ParserVersion <p>This field contains the release timestamp (YY-MM-DD) of the parser file that processed the events. The release timestamp is updated as and when any new enhancement is done to the content of the parser.</p> <ul style="list-style-type: none"> • ParserIdentifier <p>This field contains a unique ID assigned to each of the parser file. The agent:049 event containing this specific unique ID can be used to extract information such as the name of the parser file, signature of the parser file, and to determine whether it is an overridden parser file and so on.</p> <p>For information about the agent:049 event, see SmartConnector Audit Events.</p> <p>Note: The agent:049 event generation is currently set to disabled. This will be enabled when the Avro based destinations are supported.</p> <p>For more information, see ArcSight Common Event Format (CEF) Implementation Standard.</p>
Trellix ePolicy Orchestrator DB	<p>Added support for the following Trellix Endpoint Security modules:</p> <ul style="list-style-type: none"> • SolidCore 8.3 • Threat Intelligence Exchange Server 4.0 • Trellix Security for SharePoint 3.5

Software Fixes

The following issues are fixed in the CE 24.1 release:

Application Modules Software Fixes	Description
All SmartConnectors	<p>While receiving IPAddress instead of a hostname, or vice-versa, the connector was interpreting the events as two separate events. Because of this, the connector was sending duplicate agent:043 as Connector device status signals for the same device.</p> <p>Fix: This issue has been fixed as now the connector will send only one message if it is able to resolve the hostname and IPAddress issue.</p>
All SmartConnectors	<p>After upgrading the connector through ArcMC, the uninstall variable file of the Connectors which is installvariables.properties, was not getting updated. The value of the PRODUCT_VERSION_NUMBER property remained same as the base version even after upgrading the connector.</p> <p>Fix: The issue has now been fixed as the value of the PRODUCT_VERSION_NUMBER property under ArcsightHome/uninstallerData/installvariables.properties will get updated from the base version to the current version after upgrading the connector.</p>
All SmartConnectors managed by containerized ArcMC	<p>Connector required a manual restart for the events to display the custom zones in the ESM Active Channels after the network zone information was pushed from ArcMC</p> <p>Fix: This issue has been fixed by implementing a listener for this event, ensuring that network zones are updated automatically without the need for a manual restart of a Connector.</p>
Cisco ASA Syslog	<p>The Cisco PIX event type 302303 for Cisco ASA Syslog connector was not being parsed.</p> <p>Fix: The issue has been resolved by modifying the regex.</p>
Cisco ISE Syslog	<p>The Cisco ISE Syslog connector was unable to parse the Cisco ISE (Identity Services Engine) service logs for CISE_PROFILER, as it was encountering the number format exceptions. This happened because the delimiter in CISE_PROFILER was \, instead of ,.</p> <p>Fix: The issue has been resolved by retrieving the required data and excluding the special characters.</p>

Application Modules Software Fixes	Description
Infoblox NIOS Syslog	<p>Infoblox 8.5.2 device events were not getting parsed and the vendor and product names were erroneously getting labeled as UNIX.</p> <p>Fix: A code fix has been provided to ensure the successful parsing of Infoblox 8.5.2 events. Consequently, the corrected values for device Vendor and Product are now recognized as Infoblox and NIOS, respectively.</p>
Windows Event Log SmartConnector (WiSC)	<p>While reconfiguring the Windows Event Log SmartConnector (WiSC) by modifying the default connector parameter values, it throws an error leading to a deadlock. Whereas, while installing the connector with the default parameter values, it is getting through.</p> <p>Fix: This issue has now been fixed.</p>
Fortinet Fortigate Syslog	<p>The Fortinet Fortigate Syslog connector was parsing the bandwidth field value as an integer instead of long. This resulted in the incorrect mapping in the destination and an error message was displayed in the agent.log file.</p> <p>Fix: This issue has been resolved by changing the data type of the bandwidth field from integer to long while parsing.</p> <p>This change was required only for CEF 1.0 because it was working fine with CEF 0.1.</p>
	<p>The eventtime value of the Fortinet Fortigate Syslog connector was provided in nanoseconds. But the Fortigate parser was converting the epoch time from seconds. This resulted in incorrect field values for the Device Receipt Time and End Time.</p> <p>Fix: The issue has been resolved by updating the field value for the Device Receipt Time in the Fortigate parser. It now derives the date and time information present within the log that ensures the accuracy of the field value. And, the field value for End Time now depends on the Device Receipt Time for populating the accurate value.</p>
F5 BIG-IP Syslog	<p>Both F5 Big IP and UNIX/ UNIX-like systems have the id value as systemd because of which it was fetching the same value for the device vendor and device product that is F5 Big IP.</p> <p>Fix: The issue has been resolved by modifying the base regex to ensure that logs from F5 Big IP with systemd as the id value receives the accurate device vendor and device product values, that identifies as F5 Big IP. Similarly, logs from Unix/ Unix-like systems with systemd as the id value is now assigned the accurate device vendor and device product values, categorizing them as Unix.</p> <p>The F5 big events for F5 BIG-IP Syslog connector was not being parsed.</p> <p>Fix: Added regex to handle the parsing issue of the events.</p>

Application Modules Software Fixes	Description
Microsoft Azure Event Hub	<p>The Microsoft Azure Event Hub connector was observing a casting exception while trying to write IPv4 address into custom string in the primaryIPv4Address field for Resource Event Logs.</p> <p>Fix: This issue has now been fixed.</p>
	<p>The Microsoft Azure Event Hub connector was unable to process certain events for Defender for Cloud.</p> <p>Fix: The issue has been resolved by modifying the log processing capability to handle the format of the unparsed events.</p>
Microsoft IIS File	<p>The Microsoft IIS File connector was locking and not releasing the previously created log files.</p> <p>Fix: The issue has now been fixed.</p>
Microsoft 365 Defender	<p>The endTime and startTime fields of the Microsoft 365 Defender connector were always being populated as 01/01/2023.</p> <p>Fix: This issue has now been fixed.</p>

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the CE 24.1 release:

- Cisco ISE
- F-Secure Anti-Virus 5.5
- Juniper IDP Content Version 3652
- McAfee Network Security Manager 11.10.11.1
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 2983
- Symantec Network Security 7100 1729
- TippingPoint SMS IPS DV9849
- Trellix SolidCore 8.3
- Trellix Security for SharePoint 3.5
- Trellix Threat Intelligence Exchange 4.0

For more information, see [Event Content-Categorization updates November 2023](#) in the [Release Notes for ArcSight Content AUP - Categorization Updates 2023](#).

SmartConnector Parser Support Policy

Inline with the documents [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#), [Technical Requirements for SmartConnectors](#), the note at the top of the [SmartConnector Grand List \(A-Z\) documentation](#) page, we would like to take this opportunity to clarify what is meant by Connector Support.

As mentioned in the note on the [SmartConnector Grand List \(A-Z\) documentation](#) page:

The device versions currently documented as **certified** are versions that have been tested by ArcSight Quality Assurance. For device releases that fall in between certified major versions, it has been our experience that vendors typically do not make significant changes to the event generation mechanism.

Oftentimes, there are few, if any, significant changes even between major versions to the event logs. Therefore, we consider all device releases to be supported, with the understanding that major version releases may not work as expected, depending on the types of changes made to that major version.

Where possible, minor adjustments can be accommodated by parser overrides as needed. For example, Extreme Networks Dragon Export Tool versions 7.4 and 8.2 have been certified; Dragon Export Tool version 7.5 is also supported, as well as versions 8.3 or 9.0 should they be released.

In other words, if we have a SmartConnector with any certified version of a device, that device is supported regardless of version as long as the version in question is supported by the vendor.

In the situations where parser overrides cannot provide adequate functionality to support a new major or minor version of a device release, the Support Team will elevate the issue to the appropriate development teams.

Please be aware that the development team may not have immediate access to the updated device and logs. Support will request that you attach the unparsed or improperly parsed logs to your support ticket.

Please also note that we have a log anonymization/sanitization tool that you can use to remove sensitive information from logs we would need you to submit.

We may also request a conference call with you to help clarify or expedite any issues, especially if the device's connection and logging methods have changed.

For details as to the need to collect logs or possible vendor changes to devices, please see [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#).

Installing SmartConnectors

For information about installing SmartConnector, see the [Installing SmartConnectors](#) section in Installation Guide for ArcSight SmartConnectors.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to [Technical Requirements for SmartConnectors](#).

Downloading the SmartConnector Installation Packages

You can download the SmartConnector installation packages for your platform from the [Software Licenses and Downloads \(SLD\)](#). The installation packages include their respective signature files for validating that the downloaded software is authentic and has not been tampered with by a third party.

Signature Verification Procedure

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 more information and instructions on validating the downloaded software, visit the [OpenText Code Signing site](#). 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.

SmartConnector CE 24.1 (v8.4.4) Installers

File Name	Description
ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-8.4.4.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.4.xxxx.0-Collectors-Linux64.bin	This is the 64-bit Collector installer for Linux.
ArcSight-8.4.4.xxxx.0-Collectors-Win64.exe	This is the 64-bit Collector installer for Windows.
ArcSight-8.4.4.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.4.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.4.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.4.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.4.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.4.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.4.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.
ArcSight-8.4.4.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.4.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.4.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.4.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.4.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.4.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.

SmartConnector Release Notes

Installing SmartConnectors

ArcSightSmartConnectorLoadBalancer-8.4.4.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.
ArcSightSmartConnectorLoadBalancer-opensource-8.4.4.xxxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.4.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.4.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading SmartConnectors

Upgrading to CE 24.1 (v8.4.4)



Important: If you use any of the SmartConnectors listed in the [Software Fixes](#) section, note that installing the updated SmartConnector can impact your created content.

Verifying Your Upgrade Files

For information and instructions, see "[Signature Verification Procedure](#)" on page 13.

Upgrading SmartConnector to CE 24.1 (v8.4.4)

You can upgrade a SmartConnector to implement the newly introduced features, mapping improvements and overall functionality of a SmartConnector. You can upgrade connectors either locally or remotely. Connectors automatically determine their upgrade status when they start.

For information and instructions, see [Upgrading SmartConnectors](#).

Upgrading Load Balancer to CE 24.1 (v8.4.4)

For information about upgrading Load Balancer to CE 24.1, see [Upgrading Load Balancer](#).

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.



Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:



Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command: `cd Xxxxx/lib/agent`

3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`

5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

6. Run the following command: `cd Xxxxx/lib/agent/axis`

7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Open the `Xxxxx\lib\agent` folder.

3. Search for **log4j** and delete all the entries.

4. Open the `Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\` folder.

5. Search for **log4j** and delete all the entries.

6. Open the `Xxxxx\lib\agent\axis` folder.

7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm -rf X8444`)

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Delete the **Xxxxx** folder manually.

Known Issues

This section includes legacy issues from the ArcSight Installer.

Application Module	Description
All SmartConnectors	<p>SmartConnector or Collector remote connections fail due to low entropy</p> <p>Note: The CTH and Collectors are supported in this release and are deprecated as of 8.4. CTH functionality and Collectors will be removed in an upcoming release, by March 31, 2024</p> <p>All SmartConnectors or Collectors remote connections go through SSL and they depend on the Operating System random number pool (entropy pool) to generate private keys for secure communication. When the entropy pool is less than the ideal lower limit of 1000, the keys are not generated, communication cannot be established and the SmartConnector or Collector does not start. In cloud hosted Linux instances, the entropy pool value can be less than 1000.</p> <p>Workaround:</p> <p>To ensure that the entropy value is at the desired level:</p> <ol style="list-style-type: none"> 1. Install the rng-tools package: <code>sudo yum install -y rng-tools</code> 2. Add the following line to the /etc/sysconfig/rngd file: <code>EXTRAOPTIONS="-r /dev/urandom"</code> 3. Check the entropy availability in the system: <code>cat /proc/sys/kernel/random/entropy_avail</code> 4. Start the rngd package as root user: <code>service rngd start</code> 5. Enable the rngd service to start at the system start-up: <code>systemctl enable rngd.service</code> <code>systemctl start rngd.service</code> 6. Ensure that the rngd package is always running (even after a reboot) as root user: <code>chkconfig --level 345 rngd on</code> 7. Check the entropy availability in the system, after starting the rngd service: <code>cat /proc/sys/kernel/random/entropy_avail</code>
	<p>Unable to install connector because of missing packages</p> <p>Workaround:</p> <p>Ensure that the following packages are installed:</p> <ol style="list-style-type: none"> 1. <code>yum install -y unzip</code> 2. <code>yum install -y fontconfig \ dejavu-sans-fonts</code>

All SmartConnectors installed on Solaris	<p>When upgrading SmartConnectors on Solaris, a timeout error is displayed</p> <p>Workaround:</p> <ul style="list-style-type: none"> • If the Solaris connector is already installed as a standalone, locally upgrade to 8.2.0. • If the Solaris Connector is installed as a service: <ol style="list-style-type: none"> a. Stop the service. b. Go to HOME/current/bin and execute ./runagentsetup. c. Uninstall the service in Global Parameters and exit the wizard. d. Perform a local upgrade to 8.2.0. e. Install the Connector as a service and exit the wizard. f. Start the service.
	<p>Connector logs show Fatal Exception error: Unable to find requested property 'transport.cef kafka.extra.prod.props'</p> <p>This message does not impact the performance or the functionality of the Connector.</p> <p>Workaround:</p> <p>If you are using a map file with an expression set in the <connector_install_location>\counterintelligence location and the connector runs out of memory, add the following property to agent.properties as a workaround: parser.operation.result.cache.enabled=false</p> <p>If this problem happens with Windows Event Log Native, and the above workaround does not completely solve the problem, reduce the value of the eventprocessorthreadcount Native connector parameter. You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your environment. Example:</p> <pre>agents[0].eventprocessorthreadcount=5 or agents[0].eventprocessorthreadcount=1, etc..</pre> <p>where 0 is the index of the Microsoft Windows Event Log - Native connector in the container.</p>
All File SmartConnectors	<p>When adding a log into a log file using the vi text editor, events are not sent to ESM</p> <p>Arcsight file connectors do not read events if the files are edited using the vi editor on Linux platforms.</p> <p>Workaround:</p> <p>Use the cat command to append data:</p> <p>Syntax:</p> <pre>cat >> log_file_name [Enter] "your logs" ctrl+c</pre>

Google Cloud SmartConnector	<p>The Google SmartConnector cannot authenticate tokens with Google API</p> <p>The following error is displayed when the connector is used from ArcMc with the One-Click feature:</p> <pre>{ "error" : "invalid_grant", "error_description" : "Invalid JWT: Token must be a short-lived token (60 minutes) and in a reasonable timeframe. Check your iat and exp values in the JWT claim." }</pre> <p>Workaround:</p> <p>The common cause is that the clock in the machine from which you are executing your task is not in sync with the Network Time Protocol (NTP). Match the connector time with the current time.</p>
--------------------------------	--

ArcMC Managed SmartConnectors	<p>SmartConnectors cannot be bulk-upgraded on a Linux server</p> <p>Workaround:</p> <p>Before performing a SmartConnector bulk upgrade from ArcMC on any Linux server including an ArcMC appliance, install the rng-tools on the corresponding Linux OS.</p> <p> Note: This procedure is not required if the connector is upgraded on a Windows server or if only one connector is upgraded per Linux server.</p> <p>To install and configure the rng-tools package after a fresh install, follow the steps mentioned for SmartConnector or Collector remote connections fail due to low entropy.</p> <p>One-Click installation fails on RHEL 8.1 or later, CentOS 8.1 or later, and SUSE 15 or later through ArcMC 2.9.4</p> <p>This issue might occur in other ArcMC versions.</p> <p>Workaround:</p> <p>Pre-requisites for instant connector or collector deployment:</p> <ul style="list-style-type: none">• Python2• Libselinux-python <p> Note: If the SmartConnector Linux machine does not have Python pre-installed, proceed with manual installation.</p> <p>To manually install Python:</p> <p>Apply these changes to the target Linux host (the VM where the connector or collector will be deployed):</p> <ol style="list-style-type: none">1. Install python2 by the following command: <code>sudo yum install -y python2</code>2. Create a symlink by the following command: <code>sudo ln -s /usr/bin/python2 /usr/bin/python</code>3. Install the libselinux-python package by the following command: <code>sudo yum install -y libselinux-python</code> <p> Note: If the yum command fails when installing libselinux-python, the rpm can be downloaded from: http://mirror.centos.org/centos/8/AppStream/x86_64/os/Packages/libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm</p>
-------------------------------	---

Known Issues

CyberArk Privileged Access Security	<p>Issues are encountered when parsing the CyberArk logs in Common Event Format (CEF)</p> <p>The issue occurs because the CyberArk logs do not contain a pipe symbol (' ') in the header section, after the name field. This results in mapping discrepancies across all the fields in some cases or issues in the event.name field in other cases. This parsing anomaly hinders the accurate extraction and representation of information from the logs.</p> <p>Workaround</p> <p>To address this issue, request modifications to the log formatas described in the ArcSight Common Event Format (CEF) Implementation Standard document, to ensure that the header section contains the pipe symbol (' ') after the name field.</p>
IBM Big Fix REST API	<p>Connector installation fails when the client properties file is auto populated incorrectly</p> <p>While installing the IBM Big Fix API connector through ArcMC, it populates the following incorrect path on the client properties file: "E:\depot\candidate\connector\GA\main\system\agent\config\bigfix_api\relevancequeryfile.properties". When the client properties file is auto populated incorrectly, the connector installation fails.</p> <p>Workaround:</p> <p>Set the following path manually:</p> <pre>\$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties</pre>
Microsoft Message Trace REST API	<p>Issues with ArcMC upgrade behaviour in the Message Trace REST API connector</p> <p>Unable to upgrade the Message Trace Rest API Connector through ArcMC.</p> <p>Workaround:</p> <p>You can upgrade the Message Trace REST API Connector either using ESM or locally.</p>
Microsoft Windows Event Log (WiSC)	<p>WiSC SmartConnector issues</p> <p>WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. it has the following issues:</p> <ul style="list-style-type: none"> Issue #1: High CPU utilization on the monitored Windows host (log endpoint) High CPU utilization is detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average). Issue #2: WinRM inherent EPS limitations WinRM has an event rate limit of around 140 EPS (sustained). Therefore, it is not recommended to use the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates. <p>Workaround:</p> <p>To mitigate these issues, use the Microsoft Windows Event Log - Native. For more information, see the Technical Note on WinRM-related Issues.</p>

Known Issues

Microsoft Windows Event log - Native	<p>The Microsoft Windows Event Log - Native SmartConnector 8.4 is unable to receive events on Windows Server 2012 R2</p> <p>The communication between winc-agent (.NET component) and the SmartConnector (Java component) does not support TLS.</p> <p>Workaround:</p> <p>Because of the cipher suite support limitations in Microsoft Windows, the SmartConnectors 8.4 running on Window Server 2012 R2 must use 'Raw TCP' instead of the TLS protocol.</p> <p>To use 'Raw TCP', perform the following steps after installing the SmartConnector:</p> <ol style="list-style-type: none"> 1. Open the <ARCSIGHT HOME>/current/user/agent/agent.properties file. 2. Change the parameter value from agents[0].communicationprotocol=TLS to agents [0].communicationprotocol=Raw TCP 3. Restart the SmartConnector.
Microsoft Azure Monitor Event Hub	<p>Azure Event Hub debug mode issue</p> <p>Enable the Azure Event Hub Debug Mode for function apps for support purposes. Enabling it for normal operation can cause parsing and mapping errors.</p> <p>Workaround:</p> <p>To configure the debug mode:</p> <ol style="list-style-type: none"> 1. Go to Azure portal > Function app > Configuration. 2. Set the DebugMode application value to False. 3. Restart the Function App.

Load Balancer	<p>Load Balancer arc_connlb service does not start and displays an error message</p> <p>When you upgrade Load Balancer while the services are still running, after the successful upgrade, the Load Balancer arc_connlb service does not start and displays an error message in the lb.out.wrapper.log even after you start the arc_connlb service manually.</p> <p>Workaround: When you upgrade Load Balancer while the services are still running, the system displays a notification message to stop all the programs before continuing with the upgrade. However, it does not mention the specific services you need to stop. Perform the following steps to fix this issue:</p> <ol style="list-style-type: none">1. After you install Load Balancer as a service, before you upgrade, stop the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb stop</code> or <code>service arc_connlb stop</code>2. After Load Balancer is successfully upgraded, start the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb start</code> or <code>service arc_connlb start</code>
---------------	---

Trellix ePolicy Orchestrator DB	<p>Reregistration of the Trellix Orchestrator DB type connector fails with ESM as the destination</p> <p>When you re-register the Trellix Orchestrator DB type connector with ESM as the destination, the reregistration fails and the connector displays an error (null) message,</p> <p>Workaround:</p> <p>Perform the following steps for re-registering the connector on ESM using ArcMC:</p> <ol style="list-style-type: none">1. Enable the remote management mode in the connector using runagentsetup script, with port range of 9001-9010.2. Navigate to Node Management > View all nodes in ArcMC.3. Enter the Location and provide a name for the location, and then click Next.4. Specify the location of your computer as the host, and then click Add.5. Enter the Type of the SmartConnector.6. Enter the user and password as User:connector_user and Password:change_me and click Add and Import certificate.7. Navigate to Node management > View all nodes.8. Click Connectors > Connector > Destinations.9. Click Next > Re-register destination.10. Click Failed destination.11. Enter the user and password for ESM and click Next.12. Click Yes > Done. <p>The connector is now linked to ESM with a new name.</p> <p>Error is displayed while importing the parameters of the Trellix Orchestrator DB type connector</p> <p>While installing the Trellix Orchestrator DB type connector, if you import its parameters instead of manually specifying them on the screen, an error message is displayed and the installation is terminated.</p> <p>Workaround:</p> <p>While installing the connector, manually specify the parameters instead of importing them.</p>
---------------------------------	---

Connector End-of-Life Notices



Note: For information about connector end-of-life status, refer to [Connector End-of-Life Notices](#) on the [ArcSight SmartConnector 24.1 Documentation](#) page.

SmartConnector End of Support Announcements

SmartConnector	End of Support Date	Details
Connectors in Transformation Hub (CTH) and Collectors	11/2025	The CTH and Collectors are supported in this release and are deprecated as of 8.4. CTH functionality and Collectors will be removed in an upcoming release, by March 31, 2024. CTH and Collectors will have limited support for customers already using these components until the end of support date for the ArcSight Connector 8.4.0 release.

SmartConnectors No Longer Supported

SmartConnector	End of Support Date	Details
Model Import Connector for Malware Information Sharing Platform (MISP)	06/2023	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Model Import Connector for Micro Focus Security ArcSight Reputation Security Monitor Plus (RepSM Plus)	10/2022	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Microsoft Windows Event Log – Unified Connector (WUC)	12/2021	Lack of customer demand.
Microsoft Forefront Threat Management Gateway (TMG) 2010	04/2020	End of support by vendor.
Windows Server 2008 R2	01/2020	End of support by vendor.

SmartConnector Release Notes
Connector End-of-Life Notices

Checkpoint Syslog	12/2019	The vendor no longer supports version R77.30. Therefore, we offer limited support. Fixes and improvements are no longer provided for this version.
Solsoft Policy Serve	11/2019	Lack of customer demand.
Oracle Audit DB version 9	08/2019	End of support by vendor.
All 32-bit SmartConnectors	04/2018	Supported only 64-bit SmartConnectors.
Symantec Endpoint Protection DB – SEP version 1	02/2018	End of support by vendor.
Solaris 10 Premier support	01/2018	End of support by vendor.

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 Release Notes (SmartConnectors CE 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: CE 24.2.1

SmartConnector Release Notes

Document Release Date: May 2024

Software Release Date: May 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

Release Notes for ArcSight SmartConnector CE 24.2.1	4
Release Highlights	6
What's New	7
Security Updates	7
Software Fixes	7
Downloading and Applying the Patch	10
Deleting Older Vulnerable Libraries after Upgrading a Connector	10
Send Documentation Feedback	13

Release Notes for ArcSight SmartConnector CE 24.2.1

This Release Notes document describes how to apply this latest release of ArcSight SmartConnector and ArcSight SmartConnector Load Balancer, and provides other information about the most recent changes, known limitations, and software fixes.

SmartConnector is an application that collects log messages from log sources, processes them into ArcSight security events, and transports them to destination consumers for analytic, storage, and compliance reporting.

You can apply SmartConnectors CE 24.2.1 (v8.4.5.P1) to:

- Perform a fresh install of the SmartConnectors.
- Upgrade the SmartConnectors from SmartConnectors CE 24.2 (v8.4.5).

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](#).

Release Highlights

The SmartConnector CE 24.2.1 (v8.4.5.P1) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Upgrade of Zulu OpenJDK to 8u412
- Software fixes for Amazon CloudWatch, Amazon S3, and Check Point Syslog

For detailed information, see "[What's New](#)" on the next page.

The Connector Team has worked tirelessly, and in a few cases, have enjoyed the benefits of partnering with some of the customers to overcome some of the issues. The extra effort from the customer success and support teams, and especially customers, in helping the team understand and reproduce some difficult situations in order to improve the SmartConnectors is duly appreciated.

Additionally, the [ArcSight Idea Exchange portal](#), will be updated with affected entries and monitored to help, prioritize, and plan new features for next release.

What's New

SmartConnectors CE 24.2.1 (v8.4.5.P1) incorporates the following SmartConnector updates:

- [Security Updates](#)
- [Software Fixes](#)

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	<p>Upgraded Zulu OpenJDK to 8u412.</p> <p>The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade:</p> <ul style="list-style-type: none">• CVE-2023-41993• CVE-2024-21011• CVE-2024-21068• CVE-2024-21085• CVE-2024-21094• CVE-2024-21003• CVE-2024-21005• CVE-2024-21002• CVE-2024-21004

Software Fixes

The following issues are fixed in the CE 24.2.1 (v8.4.5.P1) release:

Application Modules Software Fixes	Number	Description
Amazon CloudWatch	OCTCR33I889094	<p>The deployment of the Amazon CloudWatch connector failed because AWS Lambda support was discontinued for the Java 8 and Python 2.7 runtimes. Syntax issues also emerged in the heartbeat function's Python code that was originally written in Python 2.</p> <p>Fix: To resolve this issue, the Java runtime has been transitioned from Java 8 to java8.al2, and adjustments have been made to the heartbeat function to comply with the Python 3 syntax.</p>
Amazon S3	OCTCR33I883037	<p>The Amazon S3 connector encountered the following errors:</p> <ul style="list-style-type: none"> Not a CloudTrail log - the connector was displaying this fatal exception while processing digest files in the Amazon S3 bucket for the CloudTrail events when digest files were present in the S3 bucket. [com.arcsight.common.flow.stock.h] [send]No consumer specified for this output connector - the connector was continuously throwing this [ERROR] in the agent.log file. <p>Fix: The following fixes have been implemented to resolve the issues:</p> <ul style="list-style-type: none"> The connector will skip processing the digest files even if they are present in the Amazon S3 bucket without throwing any error. Code changes were made to resolve the underlying issue of incomplete event alignment.

Application Modules Software Fixes	Number	Description
Check Point Syslog	OCTCR33I886016	<p>The Check Point Syslog connector encountered parsing issues for events in which the Name and Device Event Class Id fields were populated with the 0 (Zero) that is derived from the action field of event log.</p> <p>Fix: The mapping regex has been updated so that if the action field value is 0, then the Name and Device Event Class Id field values are mapped to the first field that is not null from the following set of fields:</p> <pre>Action,event_name,malware_action,auth_status,short_desc,description,message_info,activity,subscription_stat_desc,contract_name,rule_name,event_type,, scan direction, all of (one of (ProductName, product), ' ', One of (subscription_stat, 'Event')), 'Scan Summary'</pre>

Downloading and Applying the Patch

Download the appropriate executable for your platform from the [Software Licenses and Downloads \(SLD\)](#).

The 64-bit executable is available for download for Windows and Linux platforms. Only the 64-bit executable is available for Solaris platforms. Users should move to the Solaris 64-bit platform. There is no upgrade path from the Solaris 32-bit image to the Solaris 64-bit image.

For a successful SmartConnector installation, follow the installation procedures documented in the individual SmartConnector configuration guides available on the [ArcSight Documentation website](#).

To apply the patch for:

- SmartConnectors, see [Upgrading SmartConnectors](#).
- Load Balancer, see the [Upgrading Load Balancer](#) section in *Configuration Guide for SmartConnector Load Balancer*.

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.



Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:



Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

SmartConnector Release Notes
Downloading and Applying the Patch

1. Run the following command: `cd $Arcsight_Home`
The following folders will be displayed:
 - **current** (upgraded version of the connector)
 - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Run the following command: `cd Xxxxx/lib/agent`
3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`
5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
6. Run the following command: `cd Xxxxx/lib/agent/axis`
7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to `$Arcsight_Home`.
The following folders will be displayed:
 - **current** (upgraded version of the connector)
 - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Open the `Xxxxx\lib\agent` folder.
3. Search for **log4j** and delete all the entries.
4. Open the `Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\` folder.
5. Search for **log4j** and delete all the entries.
6. Open the `Xxxxx\lib\agent\axis` folder.
7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`
The following folders will be displayed:
 - **current** (upgraded version of the connector)
 - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm -rf X8444`)

SmartConnector Release Notes
Downloading and Applying the Patch

For Windows:

1. Go to \$Arcsight_Home.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Delete the **Xxxxx** folder manually.

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 Release Notes (SmartConnectors CE 24.2.1)

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 24.2

SmartConnector Release Notes

Document Release Date: April 2024

Software Release Date: April 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

Release Highlights	4
What's New	5
New SmartConnectors and Modules	5
Cloud Updates	5
Security Updates	5
Version Updates	6
Platform Support	6
SmartConnector Enhancements	7
Software Fixes	7
Event Categorization Updates	12
SmartConnector Parser Support Policy	14
Installing SmartConnectors	15
System Requirements	15
Downloading the SmartConnector Installation Packages	15
Upgrading SmartConnectors	18
Upgrading to CE 24.2 (8.4.5)	18
Deleting Older Vulnerable Libraries after Upgrading a Connector	18
Known Issues	21
Connector End-of-Life Notices	30
SmartConnector End of Support Announcements	30
SmartConnectors No Longer Supported	30
Send Documentation Feedback	32

Release Highlights

The SmartConnector CE 24.2 (8.4.5) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Certified parser for Cisco IOS Syslog 15.9
- Certified parsers for HPE UX Syslog and HPE UX Audit File version 11.0
- Certified version 8.9 for Rocky Linux as the installation platform
- Certified Red Hat Enterprise Linux (RHEL) version 7.8.0 for UNIX Login/Logout File and UNIX OS Syslog
- Support for the following Trellix Endpoint Security modules:
 - Data Loss Prevention 11.10
 - Data Loss Prevention Incident Events 11.10
 - Advanced Threat Defense and Intelligent Sandbox 5.2
 - Data Loss Prevention Discover 11.10
- Upgrade of Zulu OpenJDK to 8u402
- Upgrade of Tomcat version to 9.0.86
- Upgrade of PostgreSQL JDBC version to 42.4.4

For detailed information, see "[What's New](#)" on the next page.

The Connector Team has worked tirelessly, and in a few cases, have enjoyed the benefits of partnering with some of the customers to overcome some of the issues. The extra effort from the customer success and support teams, and especially customers, in helping the team understand and reproduce some difficult situations in order to improve the SmartConnectors is duly appreciated.

Additionally, the [ArcSight Idea Exchange portal](#), will be updated with affected entries and monitored to help, prioritize, and plan new features for next release.

What's New

SmartConnector CE 24.2 (8.4.5) incorporates the following SmartConnector and content and categorization updates:

- [New SmartConnectors and Modules](#)
- [Cloud Updates](#)
- [Security Updates](#)
- [Version Updates](#)
- [Platform Support](#)
- [SmartConnector Enhancements](#)
- [Software Fixes](#)
- [Event Categorization Updates](#)

New SmartConnectors and Modules

New SmartConnectors/Application Module	Description
Trellix ePolicy Orchestrator DB	Added support for the following Trellix Endpoint Security modules: <ul style="list-style-type: none">• Data Loss Prevention 11.10• Data Loss Prevention Incident Events 11.10• Advanced Threat Defense and Intelligent Sandbox 5.2• Data Loss Prevention Discover 11.10

Cloud Updates

None at this time.

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors	Upgraded PostgreSQL JDBC version to 42.4.4.
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.86.

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	<p>Upgraded Zulu OpenJDK to 8u402.</p> <p>The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade:</p> <ul style="list-style-type: none"> • CVE-2024-20918 • CVE-2024-20952 • CVE-2024-20919 • CVE-2024-20921 • CVE-2024-20926 • CVE-2024-20945 • CVE-2024-20923 • CVE-2024-20925 • CVE-2024-20922

Version Updates

Application Module Version Updates	Description
Cisco IOS Syslog	Certified parser for Cisco IOS Syslog 15.9.
<ul style="list-style-type: none"> • HPE UX Syslog • HPE UX Audit File 	Certified parsers for HPE UX Syslog and HPE UX Audit File version 11.0.
<ul style="list-style-type: none"> • UNIX Login/Logout File • UNIX OS Syslog 	Certified RHEL version 7.8.0 for UNIX Login/Logout File and UNIX OS Syslog logs.

Platform Support

Application Module Platform Support	Description
All SmartConnectors and Load Balancer	Added support for Rocky Linux 8.9.

For details about hardware, software or platform, and SmartConnector requirements, see [Compatibility Matrix of SmartConnector](#) section in the [Technical Requirements for SmartConnectors](#) guide.

SmartConnector Enhancements

Application Module Enhancements	Description
Load Balancer	<p>Added support for the following global properties of Load Balancer:</p> <ul style="list-style-type: none"> • read.timeout • retry.count • retry.delay <p>For more information, see the Configuration Parameters section in the Configuration Guide for SmartConnector Load Balancer.</p>

Software Fixes

The following issues are fixed in the CE 24.2 release:

Application Modules Software Fixes	Description
All SmartConnectors	<p>While starting the connector, a fatal exception error that No password has been defined occurred. This error occurred because Remote Management was enabled, and the password for Remote Management was not specified in the properties file.</p> <p>Fix: The issue has been resolved by changing the log level from FATAL to WARN.</p>
All SmartConnectors	<p>After upgrading the Connector on Linux OS, the zipped file of the build of the previously installed Connector failed to preserve the correct file permissions. As a result, the user was unable to execute the old build to roll back to the previously installed version of the Connector.</p> <p>Fix: The previously installed Connector's installation folder has now been Tar.GZipped for Linux OS, enabling it to retain the file permissions after an upgrade. This issue has not been observed for connectors installed on Windows OS.</p>
Amazon S3	<p>The Amazon S3 connector with AWS CloudTrail log was displaying a fatal exception and was unable to parse the timestamp format "yyyy-MM-dd'T'HH:mm:ssZ".</p> <p>Fix: The parser has been modified by adding support for the "yyyy-MM-dd'T'HH:mm:ssZ" timestamp format.</p>
ArcSight FlexConnector JSON Multiple Folder Follower	<p>The ArcSight FlexConnector JSON Multiple Folder Follower connector was unable to parse compressed files, such as .gz.</p> <p>Fix: The issue has now been resolved.</p>

Application Modules Software Fixes	Description
AWS CloudTrail	<p>The AWS CloudTrail connector was displaying a fatal exception and was unable to parse the following timestamp formats: "yyyy-MM-dd'T'HH:mm:ssZ" and "yyyy-MM-dd".</p> <p>Fix: The parser has been modified by adding support for the "yyyy-MM-dd'T'HH:mm:ssZ" and "yyyy-MM-dd" timestamp formats.</p>
Cisco IronPort Email Security Appliance Syslog	<p>The Cisco IronPort Email Security Appliance Syslog connector was experiencing the following issues:</p> <ul style="list-style-type: none"> The Cisco IronPort Email Security Appliance encountered parsing issues with the Device Custom String 6 field when it was parsing logs using the Cisco IronPort Email Security Appliance Syslog connector. The parser also inserted other data apart from the Subject into the Device Custom String 6 field. When there were more than ~125 other lines between the start and the finish events for the message, the Subject that was saved in the Device Custom String 6 gets lost and does not appear in the final aggregated message. <p>Fix: To fix this issue:</p> <ul style="list-style-type: none"> Modified the mapping of the Device Custom String 6 field for the specific events. Now, the non-subject values will appear in the Flex String 2 field. When a message has more than ~125 other lines between the start and the finish events of the message with the same MID, the Subject that was saved in the Device Custom String 6 field will now remain valid and appear in the final aggregated message as expected. <p>Note: Ensure the following for successfully merging the events:</p> <ul style="list-style-type: none"> The Start and Message Finished strings must be present at the beginning and the end, respectively. All the email logs must have the same MID.
Cisco ISE Syslog	<p>The Remote-Address field for the Cisco ISE Syslog connector was not mapped for the CISE_Failed_Attempts event.</p> <p>Fix: The issue has now been resolved by mapping the Remote-Address field to the Source Address field for both CISE_Failed_Attempts and Cisco ISE TACACS Diagnostics events.</p>
Cisco NX-OS Syslog	<p>The events of the ARP-3-DUP_SRC_IP_PROBE module for the CISCO NX-OS Syslog connector were not being parsed.</p> <p>Fix: Modified a sub-message to enable the parsing of the events of the ARP-3-DUP_SRC_IP_PROBE module.</p>
Cisco PIX/ ASA Syslog	<p>The events of the ASA-6-302025 module for the Cisco PIX/ ASA Syslog connector were not being parsed.</p> <p>Fix: Modified sub-messages to enable the parsing of the events of the ASA-6-302025 module.</p>

Application Modules Software Fixes	Description
Cisco PIX/ ASA Syslog	<p>The Cisco PIX/ ASA Syslog connector was not parsing the events properly for the following message IDs:</p> <p>402143, 725006, 302025, 302027, 434004, and 303002.</p> <p>Fix: The parser has been modified to fix the parsing issue of these message IDs.</p>
Citrix NetScaler Syslog	<p>The Citrix NetScaler Syslog connector was incorrectly parsing the timestamp format "DD/MM/YYYY" for the "AAA TM session logged out" events.</p> <p>Fix: The parser has been modified by adding support for the following timestamp formats for the "AAA TM session logged out" events:</p> <ul style="list-style-type: none"> • MM/dd/yyyy:HH:mm:ss z • MM/dd/yyyy:HH:mm:ss • yyyy/MM/dd:HH:mm:ss z • yyyy/MM/dd:HH:mm:ss <p>Note: If users need support for the "dd/MM" format, they must obtain the override parser file from Customer Support.</p>
F5 BIG-IP Syslog	<p>The F5 BIG events for F5 BIG-IP Syslog connector were not being parsed.</p> <p>Fix: Added regex to handle the parsing issue of the events.</p>
F5 BIG-IP Syslog	<p>The source username of F5 BIG-IP logs for the F5 BIG-IP Syslog connector was getting parsed with closed parenthesis.</p> <p>Fix: Modified the regex to parse the source username.</p>
Fortinet Fortigate Syslog	<p>The eventtime field's value of the Fortinet Fortigate Syslog was mapped incorrectly to the Device Receipt Time field in the Fortigate parser. Because the eventtime field value was in nanoseconds for some customers and in seconds for other customers, the value was parsed into an incorrect date time format.</p> <p>In addition, customers were also not able to use the function 'Store Original Time In Flex Date 1' of the connector's destination setting. The function was displaying a random value and taking an incorrect timestamp. Therefore, an aggregation issue was encountered when piping the logs.</p> <p>Fix: This issue has been resolved by considering the first 10 digits of eventtime and converting it using epoch.</p>

Application Modules Software Fixes	Description
IBM WebSphere File	<p>The IBM WebSphere File connector was encountering parsing issues with timestamps in Websphere SystemOut logs.</p> <p>Fix: To fix this issue:</p> <ul style="list-style-type: none"> Added support for the following date formats in the parser: <ul style="list-style-type: none"> M/dd/yy HH:mm:ss:SSS z yyyy/M/dd HH:mm:ss:SSS z Added support for the following Websphere SystemOut message types in the parser: <ul style="list-style-type: none"> FISCSocketClientListener PMRM0003I ConfigFileHelper
<ul style="list-style-type: none"> Linux Audit File Linux Audit Syslog 	<p>For the proctitle type of logs, the value of the proctitle field was assigned to the fileHash field. However, the proctitle field value does not accurately represent the hash of the file, leading to a parsing issue.</p> <p>Fix: The decoded value of the proctitle has been mapped to Device Custom String 1 to resolve the issue.</p>
Load Balancer	<p>Load Balancer was experiencing issues because of an elevated number of threads, leading to a crash.</p> <p>Fix: The following fixes have been implemented to resolve the issue:</p> <ul style="list-style-type: none"> A read timeout has now been implemented on the input stream to prevent blocking of threads after processing all the data. This fix has been applied to those customer environments where the end of the stream or fin packet was not being received. The number of retry attempts for failed messages has now been limited to 5 when the destination is unavailable. However, once the destination becomes available, all new messages are redirected to it.
Load Balancer	<p>Load Balancer was experiencing issues when the Aggregation Preferred routing policy was selected.</p> <p>Fix: The code that obtains the connector's statistics to determine its overload status has been fixed to solve the issue. Load Balancer now retrieves the connector statistics in case of overloading and relocates the events to a source that is away from the connector.</p>
Load Balancer	<p>The HTTP OPTIONS method was enabled for the Load Balancer server.</p> <p>Fix: The issue has been resolved by disabling the HTTP OPTIONS method in the Load Balancer.</p>

Application Modules Software Fixes	Description
Microsoft 365 Defender	<p>The new Microsoft 365 Defender Graph APIs were not parsing the events properly for the following ESM fields:</p> <ul style="list-style-type: none"> • oldFileType • deviceExternalId • destinationHostName • oldFilePermission • sourceUserName • sourceNtDomain • healthStatus <p>Fix: The parser has been modified to fix the parsing issue of these ESM fields.</p>
Microsoft Azure Event Hub	<p>The Microsoft schema for the Microsoft Azure Event Hub connector was changed, resulting in the Azure Diagnostic logs not being parsed.</p> <p>Fix: Code changes were made for the new schema to enable the parsing of the Azure Diagnostic logs.</p>
Microsoft Azure Event Hub	<p>The Azure Event Hub connector encountered the fatal exception error of type mismatch. This error occurred because the durationMS token was set to string instead of long.</p> <p>Fix: The issue has now been resolved by making changes in the parser to convert the value of the durationMS token to the long format. This will now successfully store the value to deviceCustomNumber1.</p>
Microsoft Azure Event Hub	<p>The Microsoft schema for the Microsoft Azure Event Hub connector was changed, resulting in the Azure Activity logs not being parsed.</p> <p>Fix: Code changes were made for the new schema to enable the parsing of the Azure Activity logs.</p>
Microsoft DNS Trace Log Multiple Server File	<p>The Microsoft DNS Trace Log Multiple Server File SmartConnector was receiving the following warning message when the Answer Section or TTL field was empty in the event sent from the DNS server:</p> <pre>[com.arcsight.agent.parsers.operation.regexTokenAsLongOperation] [getResult]No match between string [XID 0x9175 Flags 0x0100 QR 0 (QUESTION) OPCODE 0 (QUERY) AA 0 TC 0 RD 1 RA 0 Z 0 CD 0 AD 0 RCODE 0 (NOERROR) QCOUNT 1 ACOUNT 0 NSCOUNT 0 ARCOUNT 0 QUESTION SECTION: Offset = 0x000c, RR count = 0 Name "(2)uk(2)ng(3)msg (5)teams(9)microsoft(3)com(0)" QTYPE A (1) QCLASS 1 ANSWER SECTION: empty AUTHORITY SECTION: empty ADDITIONAL SECTION: empty] and regex [.*TTL\s+(\d+)\s+.*]</pre> <p>Fix: The parser has been modified to handle the cases when the Answer Section or TTL field is empty and now the exception is not being received in the agent.log file.</p>

Application Modules Software Fixes	Description
Symantec Endpoint Protection Syslog	<p>The following types of events for the Symantec Endpoint Protection Syslog connector were not being parsed:</p> <ul style="list-style-type: none"> Administrator logout Virus found <p>Fix: The parser has been modified to support the parsing of these events.</p>
Syslog NG Daemon	<p>The Syslog NG Daemon SmartConnector was unable to parse the Solaris server events.</p> <p>Fix : The parsers have been modified to support the parsing of Solaris server events for the following message IDs: corntab, sshd, su, ftpd, rlogind, xntpd, syslogd, Had, reboot, /lib/inet/nwamd, vdc, mac, ldap_cachemgr, svc.startd,bash, nfs, iscsadm, llt, cacao_launcher, rexec, AgentFramework, vxvm, hotplugd, explorer, ing, perl, pkgserv, ansible-setup, and ansible-command</p>
Syslog NG Daemon	<p>The numerous events that were previously supported experienced issues with categorization as a result of modifications made to the Device Event Class ID field.</p> <p>Fix: The issue has been resolved by restoring the original value of the Device Event Class ID field for the impacted events.</p>
<ul style="list-style-type: none"> UNIX Login/Logout File UNIX OS Syslog 	<p>The following types of events of RHEL 7.8.0 and 7.5.0 for both the UNIX Login/Logout File and UNIX OS Syslog connectors were not being parsed:</p> <ul style="list-style-type: none"> Start session Close session <p>Fix: Added new sub-messages to enable the parsing of these types of events.</p>
<ul style="list-style-type: none"> UNIX Login/Logout File UNIX OS Syslog 	<p>The following events that are generated in RHEL versions 7.8.0 and 7.5.0 were not getting parsed: sshd, EARL-SW1_DFC3-1-EXCESSIVE_PARITY_ERROR, winbindd, ftpd, journal, DMI-2-NETCONF_SSH_CRITICAL, insights-client, systemd, IIB, setroubleshoot, postfix/sendmail, snmpd, SEL, pendsect, syslog-ng, rhsmd, systemd-logind, SMART_LIC-3-COMM_FAILED, abrt-hook-cpp, abrt-server, internal-sftp, PKI-6-AUTOCERTFAIL,PKI-6-CERT_RENEW_AUTO, sendmail, root, crond, rhnsd, sasauth, sssd, subscription-manager, postfix/local, postfix/pickup, sssd_be, nmbd, su</p> <p>Fix: Added new sub messages and modified the existing ones in the parser.</p>

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the CE 24.2 (8.4.5) release:

- HPE HP-UX
- Juniper IDP Content Version 3676
- McAfee Network Security Manager 11.10.14.1
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1786
- TippingPoint SMS IPS DV9874
- Trellix Data Loss Prevention 11.10

For more information, see [Event Content-Categorization updates February 2024](#) in the [Release Notes for ArcSight Content AUP - Categorization Updates 2024](#).

SmartConnector Parser Support Policy

Inline with the documents [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#), [Technical Requirements for SmartConnectors](#), the note at the top of the [SmartConnector Grand List \(A-Z\) documentation](#) page, we would like to take this opportunity to clarify what is meant by Connector Support.

As mentioned in the note on the [SmartConnector Grand List \(A-Z\) documentation](#) page:

The device versions currently documented as **certified** are versions that have been tested by ArcSight Quality Assurance. For device releases that fall in between certified major versions, it has been our experience that vendors typically do not make significant changes to the event generation mechanism.

Oftentimes, there are few, if any, significant changes even between major versions to the event logs. Therefore, we consider all device releases to be supported, with the understanding that major version releases may not work as expected, depending on the types of changes made to that major version.

Where possible, minor adjustments can be accommodated by parser overrides as needed. For example, Extreme Networks Dragon Export Tool versions 7.4 and 8.2 have been certified; Dragon Export Tool version 7.5 is also supported, as well as versions 8.3 or 9.0 should they be released.

In other words, if we have a SmartConnector with any certified version of a device, that device is supported regardless of version as long as the version in question is supported by the vendor.

In the situations where parser overrides cannot provide adequate functionality to support a new major or minor version of a device release, the Support Team will elevate the issue to the appropriate development teams.

Please be aware that the development team may not have immediate access to the updated device and logs. Support will request that you attach the unparsed or improperly parsed logs to your support ticket.

Please also note that we have a log anonymization/sanitization tool that you can use to remove sensitive information from logs we would need you to submit.

We may also request a conference call with you to help clarify or expedite any issues, especially if the device's connection and logging methods have changed.

For details as to the need to collect logs or possible vendor changes to devices, please see [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#).

Installing SmartConnectors

For information about installing SmartConnector, see the [Installing SmartConnectors](#) section in Installation Guide for ArcSight SmartConnectors.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to [Technical Requirements for SmartConnectors](#).

Downloading the SmartConnector Installation Packages

You can download the SmartConnector installation packages for your platform from the [Software Licenses and Downloads \(SLD\)](#). The installation packages include their respective signature files for validating that the downloaded software is authentic and has not been tampered with by a third party.

Signature Verification Procedure

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 more information and instructions on validating the downloaded software, visit the [OpenText Code Signing site](#). 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.

SmartConnector CE 24.2 (8.4.5) Installers

File Name	Description
ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-8.4.5.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.5.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.5.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.5.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.5.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.5.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.5.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.5.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.
ArcSight-8.4.5.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.5.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.5.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.5.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.5.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.5.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.5.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.

SmartConnector Release Notes

Installing SmartConnectors

ArcSightSmartConnectorLoadBalancer-opensource-8.4.5.xxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.5.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.5.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading SmartConnectors

Upgrading to CE 24.2 (8.4.5)



Important: If you use any of the SmartConnectors listed in the Software Fixes section, note that installing the updated SmartConnector can impact your created content.

Verifying Your Upgrade Files

For information and instructions, see "[Signature Verification Procedure](#)" on page 15.

Upgrading SmartConnector to CE 24.2 (8.4.5)

You can upgrade a SmartConnector to implement the newly introduced features, mapping improvements and overall functionality of a SmartConnector. You can upgrade connectors either locally or remotely. Connectors automatically determine their upgrade status when they start.

For information and instructions, see [Upgrading SmartConnectors](#).

Upgrading Load Balancer to CE 24.2 (8.4.5)

For information about upgrading Load Balancer to CE 24.2 (8.4.5), see [Upgrading Load Balancer](#).

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.



Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:



Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command: `cd Xxxxx/lib/agent`

3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`

5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

6. Run the following command: `cd Xxxxx/lib/agent/axis`

7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Open the `Xxxxx\lib\agent` folder.

3. Search for **log4j** and delete all the entries.

4. Open the `Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\` folder.

5. Search for **log4j** and delete all the entries.

6. Open the `Xxxxx\lib\agent\axis` folder.

7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm -rf X8444`)

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Delete the **Xxxxx** folder manually.

Known Issues

This section includes legacy issues from the ArcSight Installer.

Application Module	Description
Amazon S3	<p>Connector displays an error while processing digest files in the Amazon S3 bucket</p> <p>While processing the CloudTrail events, if digest files are present in the S3 bucket, the connector displays a fatal exception stating, Not a CloudTrail log.</p> <p>Workaround:</p> <p>Disable the digest events from the S3 bucket where the CloudTrail events are streamed, and delete the existing digest events folder.</p>

All SmartConnectors	<p>SmartConnector remote connections fail due to low entropy</p> <p>Note: The CTH is supported in this release and are deprecated as of 8.4. CTH functionality will be removed in an upcoming release, by March 31, 2024</p> <p>All SmartConnectors remote connections go through SSL and they depend on the Operating System random number pool (entropy pool) to generate private keys for secure communication. When the entropy pool is less than the ideal lower limit of 1000, the keys are not generated, communication cannot be established and the SmartConnector does not start. In cloud hosted Linux instances, the entropy pool value can be less than 1000.</p> <p>Workaround:</p> <p>To ensure that the entropy value is at the desired level:</p> <ol style="list-style-type: none">1. Install the rng-tools package: <code>sudo yum install -y rng-tools</code>2. Add the following line to the /etc/sysconfig/rngd file: <code>EXTRAOPTIONS="-r /dev/urandom"</code>3. Check the entropy availability in the system: <code>cat /proc/sys/kernel/random/entropy_avail</code>4. Start the rngd package as root user: <code>service rngd start</code>5. Enable the rngd service to start at the system start-up: <code>systemctl enable rngd.service</code> <code>systemctl start rngd.service</code>6. Ensure that the rngd package is always running (even after a reboot) as root user: <code>chkconfig --level 345 rngd on</code>7. Check the entropy availability in the system, after starting the rngd service: <code>cat /proc/sys/kernel/random/entropy_avail</code> <p>Unable to install connector because of missing packages</p> <p>Workaround:</p> <p>Ensure that the following packages are installed:</p> <ol style="list-style-type: none">1. <code>yum install -y unzip</code>2. <code>yum install -y fontconfig \ dejavu-sans-fonts</code>
---------------------	---

All SmartConnectors installed on Solaris	<p>When upgrading SmartConnectors on Solaris, a timeout error is displayed</p> <p>Workaround:</p> <ul style="list-style-type: none"> • If the Solaris connector is already installed as a standalone, locally upgrade to 8.2.0. • If the Solaris Connector is installed as a service: <ol style="list-style-type: none"> a. Stop the service. b. Go to HOME/current/bin and execute ./runagentsetup. c. Uninstall the service in Global Parameters and exit the wizard. d. Perform a local upgrade to 8.2.0. e. Install the Connector as a service and exit the wizard. f. Start the service.
	<p>Connector logs show Fatal Exception error: Unable to find requested property 'transport.cef kafka.extra.prod.props'</p> <p>This message does not impact the performance or the functionality of the Connector.</p> <p>Workaround:</p> <p>If you are using a map file with an expression set in the <connector_install_location>\counterintelligence location and the connector runs out of memory, add the following property to agent.properties as a workaround:</p> <pre>parser.operation.result.cache.enabled=false</pre> <p>If this problem happens with Windows Event Log Native, and the above workaround does not completely solve the problem, reduce the value of the eventprocessorthreadcount Native connector parameter. You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your environment. Example:</p> <pre>agents[0].eventprocessorthreadcount=5 or agents[0].eventprocessorthreadcount=1, etc..</pre> <p>where 0 is the index of the Microsoft Windows Event Log - Native connector in the container.</p>
All File SmartConnectors	<p>When adding a log into a log file using the vi text editor, events are not sent to ESM</p> <p>Arcsight file connectors do not read events if the files are edited using the vi editor on Linux platforms.</p> <p>Workaround:</p> <p>Use the cat command to append data:</p> <p>Syntax:</p> <pre>cat >> log_file_name [Enter] "your logs" ctrl+c</pre>

Google Cloud SmartConnector	<p>The Google SmartConnector cannot authenticate tokens with Google API</p> <p>The following error is displayed when the connector is used from ArcMc with the One-Click feature:</p> <pre>{ "error" : "invalid_grant", "error_description" : "Invalid JWT: Token must be a short-lived token (60 minutes) and in a reasonable timeframe. Check your iat and exp values in the JWT claim." }</pre> <p>Workaround:</p> <p>The common cause is that the clock in the machine from which you are executing your task is not in sync with the Network Time Protocol (NTP). Match the connector time with the current time.</p>
--------------------------------	--

ArcMC Managed SmartConnectors	<p>SmartConnectors cannot be bulk-upgraded on a Linux server</p> <p>Workaround:</p> <p>Before performing a SmartConnector bulk upgrade from ArcMC on any Linux server including an ArcMC appliance, install the rng-tools on the corresponding Linux OS.</p> <p> Note: This procedure is not required if the connector is upgraded on a Windows server or if only one connector is upgraded per Linux server.</p> <p>To install and configure the rng-tools package after a fresh install, follow the steps mentioned for SmartConnector remote connections fail due to low entropy.</p> <p>One-Click installation fails on RHEL 8.1 or later, CentOS 8.1 or later, and SUSE 15 or later through ArcMC 2.9.4</p> <p>This issue might occur in other ArcMC versions.</p> <p>Workaround:</p> <p>Pre-requisites for instant connector deployment:</p> <ul style="list-style-type: none">• Python2• Libselinux-python <p> Note: If the SmartConnector Linux machine does not have Python pre-installed, proceed with manual installation.</p> <p>To manually install Python:</p> <p>Apply these changes to the target Linux host (the VM where the connector will be deployed):</p> <ol style="list-style-type: none">1. Install python2 by the following command: <code>sudo yum install -y python2</code>2. Create a symlink by the following command: <code>sudo ln -s /usr/bin/python2 /usr/bin/python</code>3. Install the libselinux-python package by the following command: <code>sudo yum install -y libselinux-python</code> <p> Note: If the yum command fails when installing libselinux-python, the rpm can be downloaded from: http://mirror.centos.org/centos/8/AppStream/x86_64/os/Packages/libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm</p>
-------------------------------	--

Known Issues

CyberArk Privileged Access Security	<p>Issues are encountered when parsing the CyberArk logs in Common Event Format (CEF)</p> <p>The issue occurs because the CyberArk logs do not contain a pipe symbol (' ') in the header section, after the name field. This results in mapping discrepancies across all the fields in some cases or issues in the event.name field in other cases. This parsing anomaly hinders the accurate extraction and representation of information from the logs.</p> <p>Workaround</p> <p>To address this issue, request modifications to the log formatas described in the ArcSight Common Event Format (CEF) Implementation Standard document, to ensure that the header section contains the pipe symbol (' ') after the name field.</p>
IBM Big Fix REST API	<p>Connector installation fails when the client properties file is auto populated incorrectly</p> <p>While installing the IBM Big Fix API connector through ArcMC, it populates the following incorrect path on the client properties file: "E:\depot\candidate\connector\GA\main\system\agent\config\bigfix_api\relevancequeryfile.properties". When the client properties file is auto populated incorrectly, the connector installation fails.</p> <p>Workaround:</p> <p>Set the following path manually:</p> <pre>\$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties</pre>
Microsoft 365 Defender	<p>Command Line installation of the Microsoft 365 Defender SmartConnector mandates 'Certificate Path' value for the 'Shared Secret' authentication method</p> <p>While installing the Microsoft 365 Defender SmartConnector from the command line, if the authentication method selected is Shared Secret, the connector installation script treats the optional Certificate Path parameter as mandatory, and therefore does not proceed with the installation if the parameter has no value.</p> <p>Workaround: Install the Microsoft 365 Defender SmartConnector by using the installation wizard. OR</p> <p>You can enter any sample value for the Certificate Path parameter to proceed with the installation.</p>
Microsoft Message Trace REST API	<p>Issues with ArcMC upgrade behaviour in the Message Trace REST API connector</p> <p>Unable to upgrade the Message Trace Rest API Connector through ArcMC.</p> <p>Workaround:</p> <p>You can upgrade the Message Trace REST API Connector either using ESM or locally.</p>

Microsoft Windows Event Log (WiSC)	<p>WiSC SmartConnector issues</p> <p>WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. It has the following issues:</p> <ul style="list-style-type: none"> Issue #1: High CPU utilization on the monitored Windows host (log endpoint) High CPU utilization is detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average). Issue #2: WinRM inherent EPS limitations WinRM has an event rate limit of around 140 EPS (sustained). Therefore, it is not recommended to use the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates. <p>Workaround:</p> <p>To mitigate these issues, use the Microsoft Windows Event Log - Native. For more information, see the Technical Note on WinRM-related Issues.</p>
Microsoft Windows Event log - Native	<p>The Microsoft Windows Event Log - Native SmartConnector 8.4 is unable to receive events on Windows Server 2012 R2</p> <p>The communication between winc-agent (.NET component) and the SmartConnector (Java component) does not support TLS.</p> <p>Workaround:</p> <p>Because of the cipher suite support limitations in Microsoft Windows, the SmartConnectors 8.4 running on Window Server 2012 R2 must use 'Raw TCP' instead of the TLS protocol.</p> <p>To use 'Raw TCP', perform the following steps after installing the SmartConnector:</p> <ol style="list-style-type: none"> Open the <ARCSIGHT HOME>/current/user/agent/agent.properties file. Change the parameter value from agents[0].communicationprotocol=TLS to agents [0].communicationprotocol=Raw TCP Restart the SmartConnector.
Microsoft Azure Monitor Event Hub	<p>Azure Event Hub debug mode issue</p> <p>Enable the Azure Event Hub Debug Mode for function apps for support purposes. Enabling it for normal operation can cause parsing and mapping errors.</p> <p>Workaround:</p> <p>To configure the debug mode:</p> <ol style="list-style-type: none"> Go to Azure portal > Function app > Configuration. Set the DebugMode application value to False. Restart the Function App.

Load Balancer	<p>Load Balancer arc_connlb service does not start and displays an error message</p> <p>When you upgrade Load Balancer while the services are still running, after the successful upgrade, the Load Balancer arc_connlb service does not start and displays an error message in the lb.out.wrapper.log even after you start the arc_connlb service manually.</p> <p>Workaround: When you upgrade Load Balancer while the services are still running, the system displays a notification message to stop all the programs before continuing with the upgrade. However, it does not mention the specific services you need to stop. Perform the following steps to fix this issue:</p> <ol style="list-style-type: none">1. After you install Load Balancer as a service, before you upgrade, stop the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb stop</code> or <code>service arc_connlb stop</code>2. After Load Balancer is successfully upgraded, start the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb start</code> or <code>service arc_connlb start</code>
---------------	---

Trellix ePolicy Orchestrator DB	<p>Reregistration of the Trellix Orchestrator DB type connector fails with ESM as the destination</p> <p>When you re-register the Trellix Orchestrator DB type connector with ESM as the destination, the reregistration fails and the connector displays an error (null) message,</p> <p>Workaround:</p> <p>Perform the following steps for re-registering the connector on ESM using ArcMC:</p> <ol style="list-style-type: none">1. Enable the remote management mode in the connector using runagentsetup script, with port range of 9001-9010.2. Navigate to Node Management > View all nodes in ArcMC.3. Enter the Location and provide a name for the location, and then click Next.4. Specify the location of your computer as the host, and then click Add.5. Enter the Type of the SmartConnector.6. Enter the user and password as User:connector_user and Password:change_me and click Add and Import certificate.7. Navigate to Node management > View all nodes.8. Click Connectors > Connector > Destinations.9. Click Next > Re-register destination.10. Click Failed destination.11. Enter the user and password for ESM and click Next.12. Click Yes > Done. <p>The connector is now linked to ESM with a new name.</p> <p>Error is displayed while importing the parameters of the Trellix Orchestrator DB type connector</p> <p>While installing the Trellix Orchestrator DB type connector, if you import its parameters instead of manually specifying them on the screen, an error message is displayed and the installation is terminated.</p> <p>Workaround:</p> <p>While installing the connector, manually specify the parameters instead of importing them.</p>
---------------------------------	---

Connector End-of-Life Notices



Note: For information about connector end-of-life status, refer to [Connector End-of-Life Notices](#) on the [ArcSight SmartConnector 24.2 Documentation](#) page.

SmartConnector End of Support Announcements

SmartConnector	End of Support Date	Details
Connectors in Transformation Hub (CTH) and Collectors	01/2027	<p>The CTH and Collectors were deprecated with the SmartConnector release of 8.4. Deployment of CTH and Collectors is now removed in CE 24.2.</p> <p>CTH and Collectors will have limited support for customers already using these components until the end of support date for the ArcSight Connector CE 24.1 release, which is Jan 31, 2027.</p>
Microsoft Azure Monitor Event Hub	04/2027	<p>The Microsoft Azure Monitor Event Hub connector has been replaced by the Microsoft Azure Event Hub SmartConnector.</p> <p>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.</p>

SmartConnectors No Longer Supported

SmartConnector	End of Support Date	Details
Model Import Connector for Malware Information Sharing Platform (MISP)	06/2023	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.

SmartConnector Release Notes
Connector End-of-Life Notices

Model Import Connector for Micro Focus Security ArcSight Reputation Security Monitor Plus (RepSM Plus)	10/2022	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Microsoft Windows Event Log – Unified Connector (WUC)	12/2021	Lack of customer demand.
Microsoft Forefront Threat Management Gateway (TMG) 2010	04/2020	End of support by vendor.
Windows Server 2008 R2	01/2020	End of support by vendor.
Checkpoint Syslog	12/2019	The vendor no longer supports version R77.30. Therefore, we offer limited support. Fixes and improvements are no longer provided for this version.
Solsoft Policy Serve	11/2019	Lack of customer demand.
Oracle Audit DB version 9	08/2019	End of support by vendor.
All 32-bit SmartConnectors	04/2018	Supported only 64-bit SmartConnectors.
Symantec Endpoint Protection DB – SEP version 1	02/2018	End of support by vendor.
Solaris 10 Premier support	01/2018	End of support by vendor.

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 Release Notes (SmartConnectors CE 24.2)

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

SmartConnector Release Notes

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

Release Highlights	4
What's New	5
New SmartConnectors and Modules	5
Cloud Updates	6
Security Updates	6
Version Updates	7
Platform Support	7
SmartConnector Enhancements	8
Software Fixes	8
Event Categorization Updates	12
SmartConnector Parser Support Policy	14
Installing SmartConnectors	15
System Requirements	15
Downloading the SmartConnector Installation Packages	15
Upgrading SmartConnectors	18
Upgrading to CE 24.3 (8.4.6)	18
Deleting Older Vulnerable Libraries after Upgrading a Connector	18
Known Issues	21
Connector End-of-Life Notices	32
SmartConnector End of Support Announcements	32
SmartConnectors No Longer Supported	32
Send Documentation Feedback	34

Release Highlights

The SmartConnector CE 24.3 (8.4.6) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- New [SmartConnector for Integrated Dell Remote Access Controller \(iDRAC\) Syslog](#)
- Certified parser for [Cisco IronPort Web Security Appliance Syslog](#) version 12.5.5
- Certified parsers for the [Cisco IronPort Email Security Appliance Syslog \(AMP\)](#) and the [Cisco IronPort Email Security Appliance File \(AMP\)](#) version 14.3.0
- Certified [Microsoft Network Policy Server File](#) for Microsoft Windows Server 2022
- Certified parsers for , [Apache Tomcat File](#), [Apache HTTP Server Error File](#), and [Apache HTTP Server Access Multiple File](#) version 9.0.56
- Certified parser for [RedHat JBoss Security Audit Multiline](#) version 4.3.0 GA_CP03_EAP
- Support for the 'Octet-Counting Framing' mode standard for the RFCs 6587 event formats
- Support for the following [Microsoft Azure Event Hub](#) resource logs modules:
 - App Service HTTP Logs
 - App Service IP Sec Audit Logs
- Added support for the following [Trellix Endpoint Security modules](#):
 - Trellix MOVE Antivirus 4.1
 - McAfee Security for Microsoft Exchange (MSME) 8.8
 - Data Loss Prevention Administrative 11.x
 - Trellix Agent 5.7
- Upgrade of Zulu OpenJDK to 8u412
- Upgrade of Tomcat version to 9.0.89

For detailed information, see "[What's New](#)" on the next page.

The Connector Team has worked tirelessly, and in a few cases, have enjoyed the benefits of partnering with some of our customers to overcome some of the issues. The extra effort from the customer success and support teams, and especially customers, in helping the team understand and reproduce some difficult situations in order to improve the SmartConnectors is duly appreciated.

Additionally, the [ArcSight Idea Exchange portal](#), will be updated with affected entries and monitored to help, prioritize, and plan new features for next release.

What's New

SmartConnector CE 24.3 (8.4.6) incorporates the following SmartConnector and content and categorization updates:

- [New SmartConnectors and Modules](#)
- [Cloud Updates](#)
- [Security Updates](#)
- [Version Updates](#)
- [Platform Support](#)
- [SmartConnector Enhancements](#)
- [Software Fixes](#)
- [Event Categorization Updates](#)

New SmartConnectors and Modules

New SmartConnectors/Application Module	Description
Integrated Dell Remote Access Controller (iDRAC)	<p>The SmartConnector for Integrated Dell Remote Access Controller (iDRAC) Syslog receives logs from iDRAC and converts them to CEF format.</p> <p>iDRAC is a hardware component found in Dell servers. It is a remote management and monitoring tool that allows administrators to manage and monitor Dell servers remotely, even when the server is offline or in a non-operational state.</p> <p>For more information, see Configuration Guide for Integrated Dell Remote Access Controller (iDRAC).</p>
Microsoft Azure Event Hub	<p>Added support for the following Azure Event Hub resource logs modules:</p> <ul style="list-style-type: none">• App Service HTTP Logs• App Service IP Sec Audit Logs <p>For information about the event mappings, see Device Event Mapping to ArcSight Fields in the Configuration Guide for Microsoft Azure Event Hub SmartConnector.</p>

New SmartConnectors/Application Module	Description
Trellix ePolicy Orchestrator DB	<p>Added support for the following Trellix Endpoint Security modules:</p> <ul style="list-style-type: none"> • Trellix MOVE Antivirus 4.1 • McAfee Security for Microsoft Exchange (MSME) 8.8 • Data Loss Prevention Administrative 11.x • Trellix Agent 5.7 <p>For information about the event mappings, see Device Event Mapping to ArcSight Fields in the Configuration Guide for Trellix ePolicy Orchestrator DB SmartConnector.</p>

Cloud Updates

No updates at this time.

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.89.
All SmartConnectors and Load Balancer	<p>Upgraded Zulu OpenJDK to 8u412.</p> <p>The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade:</p> <ul style="list-style-type: none"> • CVE-2023-41993 • CVE-2024-21011 • CVE-2024-21068 • CVE-2024-21085 • CVE-2024-21094 • CVE-2024-21003 • CVE-2024-21005 • CVE-2024-21002 • CVE-2024-21004

Version Updates

Application Module Version Updates	Description
<ul style="list-style-type: none">• Apache Tomcat File• Apache HTTP Server Error File• Apache HTTP Server Access Multiple File	Certified parsers for Apache Tomcat File, Apache HTTP Server Error File, and Apache HTTP Server Access Multiple File version 9.0.56.
<ul style="list-style-type: none">• Cisco IronPort Email Security Appliance Syslog (AMP)• Cisco IronPort Email Security Appliance File (AMP)	Certified parsers for Cisco AMP logs for Cisco IronPort Email Security Appliance Syslog and Cisco IronPort Email Security Appliance File version 14.3.0.
Cisco IronPort Web Security Appliance Syslog	Certified parser for Cisco IronPort Web Security Appliance Syslog version 12.5.5.
JBoss Security Audit File	Certified parser for RedHat JBoss Security Audit Multiline version 4.3.0 GA_CP03_EAP.
Microsoft Network Policy Server File	Added support for Microsoft Network Policy Server File for Microsoft Windows Server 2022.

Platform Support

No updates at this time.

For details about hardware, software or platform, and SmartConnector requirements, see [Compatibility Matrix of SmartConnector](#) section in the [Technical Requirements for SmartConnectors](#) guide.

SmartConnector Enhancements

Application Module Enhancements	Description
All SmartConnectors	All the previous clear text passwords have now been encrypted and the new passwords can be specified in the agent.properties file using the .encrypted property extension.
Syslog NG Daemon	<p>Added support for the Octet-Counting Framing mode standard for the RFCs 6587 event formats.</p> <p>The new property syslog.framing.type is added in the agent.defaults.properties file of the Syslog connectors to support the Octet-counting enabled syslog messages.</p> <p>For more information, see RFC Compliance Support and Installing the SmartConnector to Use the Raw TCP or UDP Protocol in the Configuration Guide for Syslog NG Daemon SmartConnector.</p>

Software Fixes

The following issues are fixed in the CE 24.3 release:

Application Modules Software Fixes	Number	Description
All SmartConnectors	OCTCR33I883014	<p>The connector repeatedly generated an internal event called Event Transport Fail Over with the Device Event Class ID of agent:51, even though no destination failover occurred.</p> <p>Fix: The issue has been fixed to ensure that the internal event is generated only when a destination failover occurs.</p>
All SmartConnectors	OCTCR33I889075	<p>The following warning messages were displayed in the connector's log file because of the duplicate entries in one of the internal configuration files:</p> <pre>[WARN][com.arcsight.agent.cx.b][loadLookUpTable]Duplicate Unique Id [GEMALTO SAFENET PROTECTDB] near tokens [[Gemalto, SafeNet ProtectDB, Content Security]] at line [278] found, ignoring [WARN][com.arcsight.agent.cx.b][loadLookUpTable]Duplicate Unique Id [HP TIPPINGPOINT NEXT GENERATION FIREWALL] near tokens [[HP TippingPoint, Next Generation Firewall, Firewall]] at line [288] found, ignoring</pre> <p>Fix: The issue has been fixed by removing the duplicate entries in the configuration file.</p>
<ul style="list-style-type: none"> • Apache Tomcat File • Apache HTTP Server Error File 	OCTCR33I863046	<p>The events for the following modules of Apache Tomcat File and Apache HTTP Server with version 9.0.56 were not getting parsed:</p> <ul style="list-style-type: none"> • localhost • Catalina • localhost access <p>These modules utilize the Apache Tomcat File and Apache HTTP Server Error File connectors for parsing.</p> <p>Fix: Modified the parser to resolve the issue.</p>

Application Modules Software Fixes	Number	Description
AWS CloudTrail	OCTCR33I871053	<p>When the AWS CloudTrail connector received CloudTrail logs with IPv6 values, the Source Address field remained empty.</p> <p>Fix: Modified the mapping of the Source Address field in the parser to resolve the issue.</p>
AWS Security Hub	OCTCR33I534008	<p>The AWS Security Hub connector was unable to parse the JSON format logs that contained line feed characters such as \n, because the logs were fragmented into multiple lines.</p> <p>Fix: This issue has been fixed.</p>
Cisco IronPort Web Security Appliance Syslog	OCTCR33I685003	<p>The Destination Port field of the Cisco IronPort Web Security Appliance Syslog connector was empty and not being parsed.</p> <p>Fix: To fix this issue:</p> <ul style="list-style-type: none"> Added support for the Cisco IronPort Web Security Appliance Syslog version 12.5.5 logs. Modified the parser for the 12.5.5 version wherein the port number is extracted from the URL and populated in the Destination Port field. Now, the Destination Port field is not empty.
Cisco PIX/ ASA Syslog	OCTCR33I900239	<p>The Cisco PIX/ ASA Syslog SmartConnector was unable to parse events containing the following message IDs:</p> <p>109201, 109202, 109203, 109204, 109205, 109206, 109207, 109208, 109209, 1092010, 1092011, 1092012, and 109213</p> <p>Fix: The parser has been updated with the regex to parse session-based authentication logs of Cisco Secure PIX Firewall with the message ids from 109201 to 109213.</p>

Application Modules Software Fixes	Number	Description
F5 BIG-IP Syslog	OCTCR33I883013	<p>The User Agent value for the tmm module for the F5 BigIP logs was incorrectly mapped to an additional data field of the F5 BIG-IP Syslog connector.</p> <p>Fix: The mapping has been modified to fix this issue. Now, the User Agent value is getting correctly mapped to the Request Client Application field as expected.</p>
Fortinet Fortigate Syslog	OCTCR33I876081	<p>The Fortinet Fortigate Syslog connector was facing parsing issues with the bandwidth token because the values of the bandwidth field were getting mapped to the bytesin and bytesout fields.</p> <p>Fix: The mappings have been modified to fix this issue. Now, the bandwidth field is getting mapped to the additionaldata fields. For more information about the additionaldata fields, see the FortiGate Event Mappings table in Configuration Guide for Fortinet FortiGate Syslog SmartConnector.</p>
Infoblox NIOS Syslog	OCTCR33I901220	<p>The events of the Infoblox NIOS Syslog module were not being parsed</p> <p>Fix: Added new sub-messages to handle the parsing issue.</p>
Microsoft Azure Event Hub	OCTCR33I826024	<p>The Microsoft Azure Event Hub connector encountered the following fatal exception when the events (such as metric data) did not contain the category field:</p> <pre>[ERROR][com.arcsight.agent.ee.f] [getJsonParser]Unable to initialize Json Parser for category [resource], file [u1]</pre> <p>Fix: Added the following warning message in the agent.log file when the category field is not found in the Azure Event Hub logs:</p> <p>"The received events do not match SmartConnector supported log format from Azure Event Hub, Event will be skipped."</p>

Application Modules Software Fixes	Number	Description
Microsoft Azure Event Hub	OCTCR33I883062	<p>Microsoft Azure Event Hub diagnostic logs were not getting parsed.</p> <p>Fix: Added support for the following Azure Event Hub resource logs modules:</p> <ul style="list-style-type: none"> • App Service HTTP Logs • App Service IP Sec Audit Logs <p>For information about the event mappings, see Device Event Mapping to ArcSight Fields in Configuration Guide for Microsoft Azure Event Hub SmartConnector.</p>
Pulse Secure Pulse Connect Secure Syslog	OCTCR33I873076	<p>The Pulse Secure events that are generated from the Pulse Secure device version 9.1R18 were getting parsed as Unix events because of an extra set of square brackets in the message.</p> <p>Fix: Updated the parser containing the regex to enable the parsing of the pulse secure events.</p>
Pulse Secure Pulse Connect Secure Syslog	OCTCR33I647077	<p>The Pulse Secure events that are generated from the Pulse Secure device versions 9.1R14.1 and 9.1R16.2 were not getting parsed.</p> <p>Fix: Updated the parser containing the regex to enable the parsing of the pulse secure events.</p>
Pulse Secure Pulse Connect Secure Syslog	OCTCR33I901108	<p>The Pulse Secure events generated from the Pulse Secure device version 9.1R18.5 were not getting parsed. The parsing issue started where the events were displayed as Unix events and showed only "su failed".</p> <p>Fix: Modified the base regex to parse all the logs of each module of the Pulse Secure device version 9.1R18.5.</p>

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the CE 24.3 (8.4.6) release:



Note: From May 2024 onwards, a new Category named **DDoS** has been introduced under Techniques.

- Fortinet Fortigate 5.2 Content 3.086
- Juniper IDP Content Version 3703
- McAfee Network Security Manager 11.10.14.4
- Microsoft AzureActiveDirectory
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1847
- TippingPoint SMS IPS DV9899

For more information, see [Event Content-Categorization updates May 2024](#) in the [Release Notes for ArcSight Content AUP - Categorization Updates 2024](#).

SmartConnector Parser Support Policy

Inline with the documents [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#), [Technical Requirements for SmartConnectors](#), the note at the top of the [SmartConnector Grand List \(A-Z\) documentation](#) page, we would like to take this opportunity to clarify what is meant by Connector Support.

As mentioned in the note on the [SmartConnector Grand List \(A-Z\) documentation](#) page:

The device versions currently documented as **certified** are versions that have been tested by ArcSight Quality Assurance. For device releases that fall in between certified major versions, it has been our experience that vendors typically do not make significant changes to the event generation mechanism.

Oftentimes, there are few, if any, significant changes even between major versions to the event logs. Therefore, we consider all device releases to be supported, with the understanding that major version releases may not work as expected, depending on the types of changes made to that major version.

Where possible, minor adjustments can be accommodated by parser overrides as needed. For example, Extreme Networks Dragon Export Tool versions 7.4 and 8.2 have been certified; Dragon Export Tool version 7.5 is also supported, as well as versions 8.3 or 9.0 should they be released.

In other words, if we have a SmartConnector with any certified version of a device, that device is supported regardless of version as long as the version in question is supported by the vendor.

In the situations where parser overrides cannot provide adequate functionality to support a new major or minor version of a device release, the Support Team will elevate the issue to the appropriate development teams.

Please be aware that the development team may not have immediate access to the updated device and logs. Support will request that you attach the unparsed or improperly parsed logs to your support ticket.

Please also note that we have a log anonymization/sanitization tool that you can use to remove sensitive information from logs we would need you to submit.

We may also request a conference call with you to help clarify or expedite any issues, especially if the device's connection and logging methods have changed.

For details as to the need to collect logs or possible vendor changes to devices, please see [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#).

Installing SmartConnectors

For information about installing SmartConnector, see the [Installing SmartConnectors](#) section in Installation Guide for ArcSight SmartConnectors.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to [Technical Requirements for SmartConnectors](#).

Downloading the SmartConnector Installation Packages

You can download the SmartConnector installation packages for your platform from the [Software Licenses and Downloads \(SLD\)](#). The installation packages include their respective signature files for validating that the downloaded software is authentic and has not been tampered with by a third party.

Signature Verification Procedure

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 more information and instructions on validating the downloaded software, visit the [OpenText Code Signing site](#). 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.

SmartConnector CE 24.3 (8.4.6) Installers

File Name	Description
ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-8.4.6.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.6.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.6.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.6.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.6.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.6.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.6.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.6.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.
ArcSight-8.4.6.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.6.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.6.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.6.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.6.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.6.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.6.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.

SmartConnector Release Notes

Installing SmartConnectors

ArcSightSmartConnectorLoadBalancer-opensource-8.4.6.xxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.6.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.6.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading SmartConnectors

Upgrading to CE 24.3 (8.4.6)



Important: If you use any of the SmartConnectors listed in the "Software Fixes" section, note that installing the updated SmartConnector can impact your created content.

Verifying Your Upgrade Files

For information and instructions, see "[Signature Verification Procedure](#)" on page 15.

Upgrading SmartConnector to CE 24.3 (8.4.6)

You can upgrade a SmartConnector to implement the newly introduced features, mapping improvements and overall functionality of a SmartConnector. You can upgrade connectors either locally or remotely. Connectors automatically determine their upgrade status when they start.

For information and instructions, see [Upgrading SmartConnectors](#).

Upgrading Load Balancer to CE 24.3 (8.4.6)

For information about upgrading Load Balancer to CE 24.3 (8.4.5), see [Upgrading Load Balancer](#).

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.



Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:



Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command: `cd Xxxxx/lib/agent`

3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`

5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

6. Run the following command: `cd Xxxxx/lib/agent/axis`

7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Open the `Xxxxx\lib\agent` folder.

3. Search for **log4j** and delete all the entries.

4. Open the `Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\` folder.

5. Search for **log4j** and delete all the entries.

6. Open the `Xxxxx\lib\agent\axis` folder.

7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm -rf X8444`)

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Delete the **Xxxxx** folder manually.

Known Issues

This section includes legacy issues from the ArcSight Installer.

Application Module	Description
Microsoft Azure Monitor Event Hub	<p>The certs folder does not get created after deploying the Azure Monitor Event Hub connector</p> <p>After a new deployment of the Azure Monitor Event Hub, the certs folder is not created in the following location:</p> <p>Storage accounts > <Storage account name> > Data Storage > File shares > <function app name> > <function app name>.</p> <p>Workaround</p> <p>To fix this issue:</p> <ol style="list-style-type: none">1. After the deployment of the new connector, go to the newly created storage account.2. In the navigation pane, click Settings > Configuration.3. In the Allow Blob anonymous access option, click Enabled and then click Save.4. Run the DeployFunction.ps1 file again.5. 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. <p>After the deployment process is completed, the certs folder will be created.</p>

All SmartConnectors	<p>SmartConnector Services are not restarting automatically when the server is restarted</p> <p>When the SmartConnector is installed as a service and the sever is restarted, the SmartConnector service does not start automatically even though the Start the service automatically option is set to Yes. This issue is reproducible in RHEL 9.x and Rocky Linux 9.x.</p> <p>Workaround</p> <p>To keep the SmartConnector service running automatically after the server is restarted:</p> <ol style="list-style-type: none">1. Install the chkconfig package as a root user: <code>yum install chkconfig</code> <div style="border-left: 3px solid #0070C0; padding-left: 10px;"><p>Note: You might encounter the error “unpacking rpm package error” when installing the chkconfig package. For more information, see Issue while installing the chkconfig package. Make sure that you read through it all before installing chkconfig.</p></div> <ol style="list-style-type: none">2. Install the SmartConnector as a root user. Ensure that you have set the Start the service automatically option to Yes.3. Run the following command: <code>chcon system_u:object_r:bin_t:s0 /etc/init.d/service_name</code> This command changes the security context of the /etc/init.d/service_name file to system_u:object_r:bin_t:s0. The chcon command is used to change the SELinux security context of a file.
---------------------	---

Issue while installing the chkconfig package

When the **chkconfig** package is installed, it fails with the following error message: “Error unpacking rpm package”

Root Cause

- The **/etc/init.d** directory was created in system during the installation of some third-party applications.
- Later on, when you install the **chkconfig** package, the system attempts to create a symbolic link **/etc/init.d** and point to **/etc/rc.d/init.d**.
- Because the **/etc/init.d/** directory already exists , the installation of the **chkconfig** package fails because the system is unable to create the symbolic link for the installation.

Workaround

Remove the **/etc/init.d** directory or any other '**/etc/rc***' directories (except **rc.d**) or move it to the other location by running either of the following commands:

- `# rm -rf /etc/init.d/`
- `# mv /etc/init.d /tmp/init.d.bk`

	<p>Note: An error occurs if the cleanup is not appropriate. Therefore, the chkconfig package might end up creating a file with the wrong name instead of init.d:</p> <pre>[root@rhel92 ~]# ls -l /etc/ grep init.d drwxr-xr-x. 2 root root 6 Apr 5 12:42 init.d lrwxrwxrwx. 1 root root 11 May 23 2023 init.d;660f733f -> rc.d/init.d <== In such cases, remove the file manually: # rm init.d\;660f733f</pre> <p>Diagnostic Steps</p> <ul style="list-style-type: none"> Check if the content of chkconfig RPM already exists as directories. The links appear as follows: <pre># ll /etc/rc* lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc0.d -> rc.d/rc0.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc1.d -> rc.d/rc1.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc2.d -> rc.d/rc2.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc3.d -> rc.d/rc3.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc4.d -> rc.d/rc4.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc5.d -> rc.d/rc5.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc6.d -> rc.d/rc6.d lrwxrwxrwx. 1 root root 13 Aug 22 2023 /etc/rc.local -> rc.d/rc.local # ll /etc/init.d lrwxrwxrwx. 1 root root 11 May 23 2023 /etc/init.d -> rc.d/init.d</pre> <ul style="list-style-type: none"> Get a strace of the yum command and analyze the strace output: <pre>strace -fttTvy -s 1024 -o /tmp/yum_install_chkconfig.out yum install chkconfig -y</pre> <p>From the strace output, the following error can be found because the /etc/init.d directory already existed and the system was unable to create the symbolic link for the installation:</p> <pre>error: unpacking of archive failed on file /etc/init.d: cpio: File from package already exists as a directory in system</pre>
Amazon S3	<p>Connector displays an error while processing digest files in the Amazon S3 bucket</p> <p>While processing the CloudTrail events, if digest files are present in the S3 bucket, the connector displays a fatal exception stating, Not a CloudTrail log.</p> <p>Workaround:</p> <p>Disable the digest events from the S3 bucket where the CloudTrail events are streamed, and delete the existing digest events folder.</p>

All SmartConnectors	<p>SmartConnector remote connections fail due to low entropy</p> <p>Note: The CTH is supported in this release and are deprecated as of 8.4. CTH functionality will be removed in an upcoming release, by March 31, 2024</p> <p>All SmartConnectors remote connections go through SSL and they depend on the Operating System random number pool (entropy pool) to generate private keys for secure communication. When the entropy pool is less than the ideal lower limit of 1000, the keys are not generated, communication cannot be established and the SmartConnector does not start. In cloud hosted Linux instances, the entropy pool value can be less than 1000.</p> <p>Workaround:</p> <p>To ensure that the entropy value is at the desired level:</p> <ol style="list-style-type: none">1. Install the rng-tools package: <code>sudo yum install -y rng-tools</code>2. Add the following line to the /etc/sysconfig/rngd file: <code>EXTRAOPTIONS="-r /dev/urandom"</code>3. Check the entropy availability in the system: <code>cat /proc/sys/kernel/random/entropy_avail</code>4. Start the rngd package as a root user: <code>service rngd start</code>5. Enable the rngd service to start at the system start-up: <code>systemctl enable rngd.service</code> <code>systemctl start rngd.service</code>6. Ensure that the rngd package is always running (even after a reboot) as root user: <code>chkconfig --level 345 rngd on</code>7. Check the entropy availability in the system, after starting the rngd service: <code>cat /proc/sys/kernel/random/entropy_avail</code> <p>Unable to install connector because of missing packages</p> <p>Workaround:</p> <p>Ensure that the following packages are installed:</p> <ol style="list-style-type: none">1. <code>yum install -y unzip</code>2. <code>yum install -y fontconfig \ dejavu-sans-fonts</code>
---------------------	--

All SmartConnectors installed on Solaris	<p>When upgrading SmartConnectors on Solaris, a timeout error is displayed</p> <p>Workaround:</p> <ul style="list-style-type: none"> • If the Solaris connector is already installed as a standalone, locally upgrade to 8.2.0. • If the Solaris Connector is installed as a service: <ol style="list-style-type: none"> a. Stop the service. b. Go to HOME/current/bin and execute <code>./runagentsetup</code>. c. Uninstall the service in Global Parameters and exit the wizard. d. Perform a local upgrade to 8.2.0. e. Install the Connector as a service and exit the wizard. f. Start the service.
	<p>Connector logs show Fatal Exception error: Unable to find requested property 'transport.cef kafka.extra.prod.props'</p> <p>This message does not impact the performance or the functionality of the Connector.</p> <p>Workaround:</p> <p>If you are using a map file with an expression set in the <code><connector_install_location>\counterintelligence</code> location and the connector runs out of memory, add the following property to <code>agent.properties</code> as a workaround: <code>parser.operation.result.cache.enabled=false</code></p> <p>If this problem happens with Windows Event Log Native, and the above workaround does not completely solve the problem, reduce the value of the eventprocessorthreadcount Native connector parameter. You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your environment. Example:</p> <pre>agents[0].eventprocessorthreadcount=5 or agents[0].eventprocessorthreadcount=1, etc..</pre> <p>where 0 is the index of the Microsoft Windows Event Log - Native connector in the container.</p>
All File SmartConnectors	<p>When adding a log into a log file using the vi text editor, events are not sent to ESM</p> <p>Arcsight file connectors do not read events if the files are edited using the vi editor on Linux platforms.</p> <p>Workaround:</p> <p>Use the cat command to append data:</p> <p>Syntax:</p> <pre>cat >> log_file_name [Enter] "your logs" ctrl+c</pre>

Google Cloud SmartConnector	<p>The Google SmartConnector cannot authenticate tokens with Google API</p> <p>The following error is displayed when the connector is used from ArcMc with the One-Click feature:</p> <pre>{ "error" : "invalid_grant", "error_description" : "Invalid JWT: Token must be a short-lived token (60 minutes) and in a reasonable timeframe. Check your iat and exp values in the JWT claim." }</pre> <p>Workaround:</p> <p>The common cause is that the clock in the machine from which you are executing your task is not in sync with the Network Time Protocol (NTP). Match the connector time with the current time.</p>
--------------------------------	--

ArcMC Managed SmartConnectors	<p>SmartConnectors cannot be bulk-upgraded on a Linux server</p> <p>Workaround:</p> <p>Before performing a SmartConnector bulk upgrade from ArcMC on any Linux server including an ArcMC appliance, install the rng-tools on the corresponding Linux OS.</p> <p> Note: This procedure is not required if the connector is upgraded on a Windows server or if only one connector is upgraded per Linux server.</p> <p>To install and configure the rng-tools package after a fresh install, follow the steps mentioned for SmartConnector remote connections fail due to low entropy.</p> <p>One-Click installation fails on RHEL 8.1 or later, CentOS 8.1 or later, and SUSE 15 or later through ArcMC 2.9.4</p> <p>This issue might occur in other ArcMC versions.</p> <p>Workaround:</p> <p>Pre-requisites for instant connector deployment:</p> <ul style="list-style-type: none">• Python2• Libselinux-python <p> Note: If the SmartConnector Linux machine does not have Python pre-installed, proceed with manual installation.</p> <p>To manually install Python:</p> <p>Apply these changes to the target Linux host (the VM where the connector will be deployed):</p> <ol style="list-style-type: none">1. Install python2 by the following command: <code>sudo yum install -y python2</code>2. Create a symlink by the following command: <code>sudo ln -s /usr/bin/python2 /usr/bin/python</code>3. Install the libselinux-python package by the following command: <code>sudo yum install -y libselinux-python</code> <p> Note: If the yum command fails when installing libselinux-python, the rpm can be downloaded from: http://mirror.centos.org/centos/8/AppStream/x86_64/os/Packages/libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm</p>
-------------------------------	--

Known Issues

CyberArk Privileged Access Security	<p>Issues are encountered when parsing the CyberArk logs in Common Event Format (CEF)</p> <p>The issue occurs because the CyberArk logs do not contain a pipe symbol (' ') in the header section, after the name field. This results in mapping discrepancies across all the fields in some cases or issues in the event.name field in other cases. This parsing anomaly hinders the accurate extraction and representation of information from the logs.</p> <p>Workaround</p> <p>To address this issue, request modifications to the log format as described in the ArcSight Common Event Format (CEF) Implementation Standard document, to ensure that the header section contains the pipe symbol (' ') after the name field.</p>
IBM Big Fix REST API	<p>Connector installation fails when the client properties file is auto populated incorrectly</p> <p>While installing the IBM Big Fix API connector through ArcMC, it populates the following incorrect path on the client properties file:</p> <p>"E:\depot\candidate\connector\GA\main\system\agent\config\bigfix_api\relevancequeryfile.properties". When the client properties file is auto populated incorrectly, the connector installation fails.</p> <p>Workaround:</p> <p>Set the following path manually:</p> <pre>\$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties</pre>
Microsoft 365 Defender	<p>Command Line installation of the Microsoft 365 Defender SmartConnector mandates 'Certificate Path' value for the 'Shared Secret' authentication method</p> <p>While installing the Microsoft 365 Defender SmartConnector from the command line, if the authentication method selected is Shared Secret, the connector installation script treats the optional Certificate Path parameter as mandatory, and therefore does not proceed with the installation if the parameter has no value.</p> <p>Workaround:</p> <p>Install the Microsoft 365 Defender SmartConnector by using the installation wizard.</p> <p>OR</p> <p>You can enter any sample value for the Certificate Path parameter to proceed with the installation.</p>
Microsoft Message Trace REST API	<p>Issues with ArcMC upgrade behaviour in the Message Trace REST API connector</p> <p>Unable to upgrade the Message Trace Rest API Connector through ArcMC.</p> <p>Workaround:</p> <p>You can upgrade the Message Trace REST API Connector either using ESM or locally.</p>

Microsoft Windows Event Log (WiSC)	<p>WiSC SmartConnector issues</p> <p>WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. It has the following issues:</p> <ul style="list-style-type: none"> • Issue #1: High CPU utilization on the monitored Windows host (log endpoint) High CPU utilization is detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average). • Issue #2: WinRM inherent EPS limitations WinRM has an event rate limit of around 140 EPS (sustained). Therefore, it is not recommended to use the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates. <p>Workaround:</p> <p>To mitigate these issues, use the Microsoft Windows Event Log - Native. For more information, see the Technical Note on WinRM-related Issues.</p>
Microsoft Windows Event log - Native	<p>The Microsoft Windows Event Log - Native SmartConnector 8.4 is unable to receive events on Windows Server 2012 R2</p> <p>The communication between winc-agent (.NET component) and the SmartConnector (Java component) does not support TLS.</p> <p>Workaround:</p> <p>Because of the cipher suite support limitations in Microsoft Windows, the SmartConnectors 8.4 running on Window Server 2012 R2 must use 'Raw TCP' instead of the TLS protocol.</p> <p>To use 'Raw TCP', perform the following steps after installing the SmartConnector:</p> <ol style="list-style-type: none"> 1. Open the <ARCSIGHT HOME>/current/user/agent/agent.properties file. 2. Change the parameter value from agents[0].communicationprotocol=TLS to agents [0].communicationprotocol=Raw TCP 3. Restart the SmartConnector.
Microsoft Azure Monitor Event Hub	<p>Azure Event Hub debug mode issue</p> <p>Enable the Azure Event Hub Debug Mode for function apps for support purposes. Enabling it for normal operation can cause parsing and mapping errors.</p> <p>Workaround:</p> <p>To configure the debug mode:</p> <ol style="list-style-type: none"> 1. Go to Azure portal > Function app > Configuration. 2. Set the DebugMode application value to False. 3. Restart the Function App.

Load Balancer	<p>Load Balancer arc_connlb service does not start and displays an error message</p> <p>When you upgrade Load Balancer while the services are still running, after the successful upgrade, the Load Balancer arc_connlb service does not start and displays an error message in the lb.out.wrapper.log even after you start the arc_connlb service manually.</p> <p>Workaround: When you upgrade Load Balancer while the services are still running, the system displays a notification message to stop all the programs before continuing with the upgrade. However, it does not mention the specific services you need to stop.</p> <p>Perform the following steps to fix this issue:</p> <ol style="list-style-type: none">1. After you install Load Balancer as a service, before you upgrade, stop the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb stop</code> or <code>service arc_connlb stop</code>2. After Load Balancer is successfully upgraded, start the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb start</code> or <code>service arc_connlb start</code>
---------------	--

Trellix ePolicy Orchestrator DB	<p>Reregistration of the Trellix Orchestrator DB type connector fails with ESM as the destination</p> <p>When you re-register the Trellix Orchestrator DB type connector with ESM as the destination, the reregistration fails and the connector displays an error (null) message,</p> <p>Workaround:</p> <p>Perform the following steps for re-registering the connector on ESM using ArcMC:</p> <ol style="list-style-type: none">1. Enable the remote management mode in the connector using runagentsetup script, with port range of 9001-9010.2. Navigate to Node Management > View all nodes in ArcMC.3. Enter the Location and provide a name for the location, and then click Next.4. Specify the location of your computer as the host, and then click Add.5. Enter the Type of the SmartConnector.6. Enter the user and password as User:connector_user and Password:change_me and click Add and Import certificate.7. Navigate to Node management > View all nodes.8. Click Connectors > Connector > Destinations.9. Click Next > Re-register destination.10. Click Failed destination.11. Enter the user and password for ESM and click Next.12. Click Yes > Done. <p>The connector is now linked to ESM with a new name.</p> <p>Error is displayed while importing the parameters of the Trellix Orchestrator DB type connector</p> <p>While installing the Trellix Orchestrator DB type connector, if you import its parameters instead of manually specifying them on the screen, an error message is displayed and the installation is terminated.</p> <p>Workaround:</p> <p>While installing the connector, manually specify the parameters instead of importing them.</p>
---------------------------------	---

Connector End-of-Life Notices



Note: For information about connector end-of-life status, refer to [Connector End-of-Life Notices](#) on the [ArcSight SmartConnector 24.3 Documentation](#) page.

SmartConnector End of Support Announcements

SmartConnector	End of Support Date	Details
Connectors in Transformation Hub (CTH) and Collectors	01/2027	<p>The CTH and Collectors were deprecated with the SmartConnector release of 8.4. Deployment of CTH and Collectors is now removed in CE 24.2.</p> <p>CTH and Collectors will have limited support for customers already using these components until the end of support date for the ArcSight Connector CE 24.1 release, which is Jan 31, 2027.</p>
Microsoft Azure Monitor Event Hub	01/2027	<p>The Microsoft Azure Monitor Event Hub connector has been replaced by the Microsoft Azure Event Hub SmartConnector.</p> <p>The Microsoft Azure Monitor Event Hub connector will not be shipped after January 2025. Therefore, it is highly recommended to switch to the Microsoft Azure Event Hub SmartConnector before January 2025.</p>

SmartConnectors No Longer Supported

SmartConnector	End of Support Date	Details
Model Import Connector for Malware Information Sharing Platform (MISP)	06/2023	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.

SmartConnector Release Notes
Connector End-of-Life Notices

Model Import Connector for Micro Focus Security ArcSight Reputation Security Monitor Plus (RepSM Plus)	10/2022	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Microsoft Windows Event Log – Unified Connector (WUC)	12/2021	Lack of customer demand.
Microsoft Forefront Threat Management Gateway (TMG) 2010	04/2020	End of support by vendor.
Windows Server 2008 R2	01/2020	End of support by vendor.
Checkpoint Syslog	12/2019	The vendor no longer supports version R77.30. Therefore, we offer limited support. Fixes and improvements are no longer provided for this version.
Solsoft Policy Serve	11/2019	Lack of customer demand.
Oracle Audit DB version 9	08/2019	End of support by vendor.
All 32-bit SmartConnectors	04/2018	Supported only 64-bit SmartConnectors.
Symantec Endpoint Protection DB – SEP version 1	02/2018	End of support by vendor.
Solaris 10 Premier support	01/2018	End of support by vendor.

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 Release Notes (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: CE 24.4.1

SmartConnector Release Notes

Document Release Date: November 2024

Software Release Date: November 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

Release Notes for ArcSight SmartConnector CE 24.4.1	4
Release Highlights	6
What's New	7
Security Updates	7
Software Fixes	7
Event Categorization Updates	9
Known Issues	11
Downloading and Applying the Patch	12
Deleting Older Vulnerable Libraries after Upgrading a Connector	12
Send Documentation Feedback	15

Release Notes for ArcSight SmartConnector CE 24.4.1

This Release Notes document describes how to apply this latest release of ArcSight SmartConnector and ArcSight SmartConnector Load Balancer, and provides other information about the most recent changes, known limitations, and software fixes.

SmartConnector is an application that collects log messages from log sources, processes them into ArcSight security events, and transports them to destination consumers for analytic, storage, and compliance reporting.

You can apply SmartConnectors CE 24.4.1 (8.4.7.P1) to:

- Perform a fresh install of the SmartConnectors.
- Upgrade the SmartConnectors from SmartConnectors 8.x to any later versions. For example, you can directly upgrade from version 8.2 to 8.4.7.P1.

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](#).

Release Highlights

The SmartConnector CE 24.4.1 (8.4.7.P1) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Upgrade of Zulu OpenJDK to 8u432.
- Software fixes for [Microsoft 365 Defender](#), [Syslog NG Daemon](#), and all SmartConnectors.

For detailed information, see "[What's New](#)" on the next page.

The Connector Team has worked tirelessly, and in a few cases, have enjoyed the benefits of partnering with some of the customers to overcome some of the issues. The extra effort from the customer success and support teams, and especially customers, in helping the team understand and reproduce some difficult situations in order to improve the SmartConnectors is duly appreciated.

Additionally, the [ArcSight Idea Exchange portal](#), will be updated with affected entries and monitored to help, prioritize, and plan new features for next release.

What's New

SmartConnectors CE 24.4.1 (8.4.7.P1) incorporates the following SmartConnector updates:

- [Security Updates](#)
- [Software Fixes](#)
- [Event Categorization Updates](#)

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	<p>Upgraded Zulu OpenJDK to 8u432.</p> <p>The following Common Vulnerabilities and Exposures (CVEs) have been addressed as part of this Zulu OpenJDK upgrade:</p> <ul style="list-style-type: none">• CVE-2023-42950• CVE-2024-25062• CVE-2024-21235• CVE-2024-21208• CVE-2024-21210• CVE-2024-21217

Software Fixes

The following issues are fixed in the CE 24.4.1 (8.4.7.P1) release:

Application Modules Software Fixes	Number	Description
All SmartConnectors	NA	<p>This patch release resolves a known issue wherein custom passwords that are stored in plain text are lost when you upgrade the SmartConnector from version 24.2 (8.4.5) or earlier to version 24.3 (8.4.6) or later and then start the SmartConnector. For more information about this issue, see the Known Issues section in ArcSight SmartConnector Release Notes CE 24.4.</p> <p>Fix: This issue has been resolved. Custom passwords stored in plain text for the keystore, truststore, or remote management are now retained and encrypted during the upgrade process. These passwords are stored in the corresponding property appended with the suffix .encrypted in the agent.properties file.</p> <p>For example:</p> <p>If you have the following property before upgrade: <code>remote.management.ssl.key.password=<custom password in clear text></code></p> <p>After upgrading the SmartConnector to 24.4.1(8.4.7.P1) or later, it will be replaced with the following encrypted password property: <code>remote.management.ssl.key.password.encrypted=<encrypted custom password></code></p> <p>For more information, see the Password Management section in ArcSight SmartConnector Installation Guide</p>
Microsoft 365 Defender	OCTCR33I941067	<p>The Microsoft 365 Defender connector was receiving an incomplete response when the mdeDeviceId field was null.</p> <p>Fix: The logic has been updated to make sure the complete response is returned when the mdeDeviceId field is null.</p>

Application Modules Software Fixes	Number	Description
Microsoft 365 Defender	OCTCR33I941068	<p>The connector was unable to parse the complete JSON object because it encountered multiple instances of the "evidence" objects or attributes in the original JSON result. This resulted in the loss of data.</p> <p>Fix: Added a regex to fix this issue.</p>
Microsoft 365 Defender	OCTCR33I956110	<p>The SmartConnector for Microsoft 365 Defender did not parse all the data related to security for the Graph API alert type.</p> <p>Fix: The issue has been fixed. The following are the fixes:</p> <ul style="list-style-type: none"> The following mappings have been added to the Device Evidence events: lastExternalIpAddress, lastIpAddress, ipInterfaces, loggedOnUsers (accountName and domainName). The parser file has been updated to parse a new event type analysedMessageEvidence. <p>For more information about the Device Evidence events and the new event type, see Configuration Guide for Microsoft 365 Defender SmartConnector</p>
Syslog NG Daemon	NA	<p>The Syslog NG Daemon connector was unable to receive events, encountering multiple instances of the CLOSE_WAIT status over the TCP communication.</p> <p>Fix: The code has been modified to close the TCP connection if a broken pipe error occurs. An additional check has also been implemented to ensure the detection of an invalid connection.</p>

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the CE 24.4.1 (8.4.7.P1) release:



Note: From May 2024 onwards, a new Category named **DDoS** has been introduced under Techniques.

- CISCO Pix 6.3
- Juniper IDP Content Version 3757
- Palo Alto Networks PAN-OS 11.2
- Snort 3.0
- Sourcefire SEU 31470

- Symantec Network Security 7100 1972
- TippingPoint SMS IPS DV9967

For more information, see [Event Content-Categorization updates November 2024](#) in the [Release Notes for ArcSight Content AUP - Categorization Updates 2024](#).

Known Issues

This section contains issues that are identified in 24.4.1 patch release.

Application Module	Description
All SmartConnectors	<p>In the FIPS mode, the connection to a destination failed when different custom passwords were set for the keystore, truststore, and remote management properties.</p> <p>Workaround:</p> <p>Set the same custom password for the keystore, truststore, and remote management files and then update the same password for the corresponding properties in the agent.properties file.</p>

Downloading and Applying the Patch

Download the appropriate executable for your platform from the [Software Licenses and Downloads \(SLD\)](#).

The 64-bit executable is available for download for Windows and Linux platforms. Only the 64-bit executable is available for Solaris platforms. Users should move to the Solaris 64-bit platform. There is no upgrade path from the Solaris 32-bit image to the Solaris 64-bit image.

For a successful SmartConnector installation, follow the installation procedures documented in the individual SmartConnector configuration guides available on the [ArcSight Documentation website](#).

To apply the patch for:

- SmartConnectors, see [Upgrading SmartConnectors](#).
- Load Balancer, see the [Upgrading Load Balancer](#) section in *Configuration Guide for SmartConnector Load Balancer*.

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.



Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:



Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

SmartConnector Release Notes
Downloading and Applying the Patch

1. Run the following command: `cd $Arcsight_Home`
The following folders will be displayed:
 - **current** (upgraded version of the connector)
 - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Run the following command: `cd Xxxxx/lib/agent`
3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`
5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`
6. Run the following command: `cd Xxxxx/lib/agent/axis`
7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to `$Arcsight_Home`.
The following folders will be displayed:
 - **current** (upgraded version of the connector)
 - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Open the `Xxxxx\lib\agent` folder.
3. Search for **log4j** and delete all the entries.
4. Open the `Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\` folder.
5. Search for **log4j** and delete all the entries.
6. Open the `Xxxxx\lib\agent\axis` folder.
7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`
The following folders will be displayed:
 - **current** (upgraded version of the connector)
 - **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)
2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm -rf X8444`)

SmartConnector Release Notes
Downloading and Applying the Patch

For Windows:

1. Go to \$Arcsight_Home.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Delete the **Xxxxx** folder manually.

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 Release Notes (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

SmartConnector 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 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

Release Highlights	4
What's New	5
New SmartConnectors and Modules	5
Cloud Updates	5
Security Updates	5
Version Updates	6
Platform Support	6
SmartConnector Enhancements	6
Software Fixes	6
Event Categorization Updates	9
SmartConnector Parser Support Policy	11
Installing SmartConnectors	12
System Requirements	12
Downloading the SmartConnector Installation Packages	12
Upgrading SmartConnectors	15
Upgrading to CE 24.4 (8.4.7)	15
Deleting Older Vulnerable Libraries after Upgrading a Connector	15
Known Issues	18
Connector End-of-Life Notices	30
SmartConnector End of Support Announcements	30
SmartConnectors No Longer Supported	31
Send Documentation Feedback	32

Release Highlights

The SmartConnector CE 24.4 (8.4.7) release represents some significant enhancements to our connectors. The most requested improvements are centered around:

- Certified parser for [Amazon S3 Cisco Umbrella Proxy V8 logs](#)
- Certified version 8.10 and 9.4 for Rocky Linux as the installation platform
- Certified version 9.4 for RHEL as the installation platform
- Support for the following [Trellix Endpoint Security \(ENS\) modules](#):
 - Policy Auditor 6.5
 - Rogue System Detection 5.0
- Upgrade of Tomcat version to 9.0.90
- Upgrade of third-party Java Service Wrapper to 3.5.59
- Upgrade of third-party Apache CXF Core jar to cxf-core-3.5.9.jar

For detailed information, see "[What's New](#)" on the next page.

The Connector Team has worked tirelessly, and in a few cases, have enjoyed the benefits of partnering with some of our customers to overcome some of the issues. The extra effort from the customer success and support teams, and especially customers, in helping the team understand and reproduce some difficult situations in order to improve the SmartConnectors is duly appreciated.

Additionally, the [ArcSight Idea Exchange portal](#), will be updated with affected entries and monitored to help, prioritize, and plan new features for next release.

What's New

SmartConnector CE 24.4 (8.4.7) incorporates the following SmartConnector and content and categorization updates:

- [New SmartConnectors and Modules](#)
- [Cloud Updates](#)
- [Security Updates](#)
- [Version Updates](#)
- [Platform Support](#)
- [SmartConnector Enhancements](#)
- [Software Fixes](#)
- [Event Categorization Updates](#)

New SmartConnectors and Modules

New SmartConnectors/Application Module	Description
Trellix ePolicy Orchestrator DB	Added support for the following Trellix Endpoint Security (ENS) modules: <ul style="list-style-type: none">• Policy Auditor 6.5• Rogue System Detection 5.0

Cloud Updates

No updates at this time.

Security Updates

SmartConnector Security Updates Application Module	Description
All SmartConnectors and Load Balancer	Upgraded Tomcat version to 9.0.90.
All SmartConnectors and Load Balancer	Upgraded third-party Java Service Wrapper to 3.5.59.
All SmartConnectors	Upgraded third-party Apache CXF Core jar to cxf-core-3.5.9.jar.

Version Updates

Application Module Version Updates	Description
Amazon S3	Certified parser for Amazon S3 Cisco Umbrella Proxy V8 logs.

Platform Support

Application Module Platform Support	Description
All SmartConnectors and Load Balancer	<ul style="list-style-type: none">Added platform support for RHEL 9.4Added support for Rocky Linux 8.10 and 9.4

For details about hardware, software or platform, and SmartConnector requirements, see [Compatibility Matrix of SmartConnector](#) section in the [Technical Requirements for SmartConnectors](#) guide.

SmartConnector Enhancements

No updates at this time.

Software Fixes

The following issues have been fixed in the CE 24.4 release:

Application Modules Software Fixes	Number	Description
Amazon S3	OCTCR33I886007	<p>Encountered the following fatal exception after upgrading to 8.4.4: [processLine] [java.lang.Exception: Incorrect format, expected [23] tokens, found [24]</p> <p>Fix: Modified the existing parser to resolve the fatal exception.</p>
Cisco ISE Syslog	NA	<p>Cisco ISE version 3.1 TACACS Accounting types of events did not have all the fields mapped to the ArcSight event fields.</p> <p>Fix: Added new conditional mappings to handle the parsing issue of the event values that were not mapped to the ArcSight event fields.</p>
Cisco NX-OS Syslog	OCTCR33I918044	<p>The Cisco NX-OS Syslog SmartConnector was unable to parse events containing the following message: "File does not exist"</p> <p>Fix: Modified the parser to handle the unparsed events.</p>
Cisco PIX/ ASA Syslog	OCTCR33I906171	<p>The Cisco PIX/ ASA Syslog SmartConnector was unable to parse events containing the following message IDs: 430002 and 430003</p> <p>Fix: Added support for the Cisco ASA FTD mappings for these message IDs: 430002 and 430003.</p>
Cisco PIX/ ASA Syslog	NA	<p>The Cisco PIX/ ASA Syslog SmartConnector was unable to parse events containing the following message IDs: 317078, 317077, and 105053</p> <p>Fix: Added support for the Cisco ASA mappings for these message IDs: 317078, 317077, and 105053</p>

Application Modules Software Fixes	Number	Description
F5 BIG-IP Syslog	OCTCR33I904209	<p>The events for F5 Big IP logs for module httpd were not getting parsed.</p> <p>Fix: Modified the base regex and added new submessages to handle the parsing issue.</p>
F5 BIG-IP Syslog	OCTCR33I901155	<p>The Device Severity field was being incorrectly parsed for some of the F5 events.</p> <p>Fix: The hard-coded values have been removed to fix the parsing issue of the Device Severity field.</p>
GitHub Enterprise Audit Log	NA	<p>The Connector was receiving a bad request error from GitHub.</p> <p>Fix: This issue has been fixed.</p> <p>Also, added a new property named github_per_page_count to the agent.properties file for controlling the pagination event count.</p> <p>Changed the default value of this property from 1000 to 100. You can modify this value in the agent.properties file.</p>
Kafka FlexConnector	OCTCR33I943094	<p>The Kafka Flex Connector consumer client was unable to read logs from the LZ4-compressed topics on a Kafka server.</p> <p>Fix: Added support for the LZ4 compression in the Kafka flex connector.</p>

Application Modules Software Fixes	Number	Description
Microsoft Office 365 Management Activity	OCTCR33I918020	<p>The values of Role.DisplayName newValue and Role.DisplayName oldValue were not appearing in their respective ESM fields, DestinationUserPrivileges and SourceUserPrivileges.</p> <p>Fix: Modified the regular expression to correctly parse the values of Role.DisplayName newValue and Role.DisplayName oldValue and mapped them to their respective ESM fields, DestinationUserPrivileges and SourceUserPrivileges.</p>
Syslog NG Daemon	OCTCR33I904092	<p>The syslog parser file was incorrectly parsing the UNIX events as F5 Big IP syslog device.</p> <p>Fix: Modified the base regex for F5 Big IP and added new submessages to handle the parsing issue of the syslog parser file.</p>
UNIX OS Syslog	NA	<p>In the earlier versions, UNIX events of the sshd module were getting parsed successfully with the device vendor as "UNIX". However, in the SmartConnector release CE 24.2 (8.4.5), these events were labeled with the product "IBM" and device vendor as "AIX Audit." This resulted in the categorization fields being parsed as empty.</p> <p>Fix: Modified a submessage to handle the parsing issue of the sshd logs generated by the Syslog connector.</p>

Event Categorization Updates

The following Data Sources with New Signatures and Categorizations are included in the CE 24.4 (8.4.7) release:



Note: From May 2024 onwards, a new Category named **DDoS** has been introduced under Techniques.

- Bricata Alert
- Juniper IDP Content Version 3736
- Palo Alto Networks PAN-OS 10.0.8
- Snort 3.0
- Sourcefire SEU 31470
- Symantec Network Security 7100 1924
- TippingPoint SMS IPS DV9940
- Trellix Rogue System Detection 5.0.7

For more information, see [Event Content-Categorization updates September 2024](#) in the [Release Notes for ArcSight Content AUP - Categorization Updates 2024](#).

SmartConnector Parser Support Policy

Inline with the documents [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#), [Technical Requirements for SmartConnectors](#), the note at the top of the [SmartConnector Grand List \(A-Z\) documentation](#) page, we would like to take this opportunity to clarify what is meant by Connector Support.

As mentioned in the note on the [SmartConnector Grand List \(A-Z\) documentation](#) page:

The device versions currently documented as **certified** are versions that have been tested by ArcSight Quality Assurance. For device releases that fall in between certified major versions, it has been our experience that vendors typically do not make significant changes to the event generation mechanism.

Oftentimes, there are few, if any, significant changes even between major versions to the event logs. Therefore, we consider all device releases to be supported, with the understanding that major version releases may not work as expected, depending on the types of changes made to that major version.

Where possible, minor adjustments can be accommodated by parser overrides as needed. For example, Extreme Networks Dragon Export Tool versions 7.4 and 8.2 have been certified; Dragon Export Tool version 7.5 is also supported, as well as versions 8.3 or 9.0 should they be released.

In other words, if we have a SmartConnector with any certified version of a device, that device is supported regardless of version as long as the version in question is supported by the vendor.

In the situations where parser overrides cannot provide adequate functionality to support a new major or minor version of a device release, the Support Team will elevate the issue to the appropriate development teams.

Please be aware that the development team may not have immediate access to the updated device and logs. Support will request that you attach the unparsed or improperly parsed logs to your support ticket.

Please also note that we have a log anonymization/sanitization tool that you can use to remove sensitive information from logs we would need you to submit.

We may also request a conference call with you to help clarify or expedite any issues, especially if the device's connection and logging methods have changed.

For details as to the need to collect logs or possible vendor changes to devices, please see [ArcSight Customer Support - Help with SmartConnector and Parser Updates](#).

Installing SmartConnectors

For information about installing SmartConnector, see the [Installing SmartConnectors](#) section in Installation Guide for ArcSight SmartConnectors.

System Requirements

For details about hardware, software or platform, and SmartConnector requirements, refer to [Technical Requirements for SmartConnectors](#).

Downloading the SmartConnector Installation Packages

You can download the SmartConnector installation packages for your platform from the [Software Licenses and Downloads \(SLD\)](#). The installation packages include their respective signature files for validating that the downloaded software is authentic and has not been tampered with by a third party.

Signature Verification Procedure

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 more information and instructions on validating the downloaded software, visit the [OpenText Code Signing site](#). 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.

SmartConnector CE 24.4 (8.4.7) Installers

File Name	Description
ARCSIGHT-CONNECTORUNOBFUSCATEDPARSERS-8.4.7.xxxx.0.ZIP	This contains unobfuscated parser files for various devices.
ArcSight-8.4.7.xxxx.0-Connector-Linux.bin	This is the 32-bit Connector installer containing CheckPoint OpSec device support for Linux.
ArcSight-8.4.7.xxxx.0-Connector-Linux64.bin	This is the 64-bit Connector installer for Linux.
ArcSight-8.4.7.xxxx.0-Connector-Solaris64.bin	This is the 64-bit Connector installer for Solaris.
ArcSight-8.4.7.xxxx.0-Connector-SolarisIA64.bin	This is the 64-bit Connector installer for Solaris Intel Architecture.
ArcSight-8.4.7.xxxx.0-Connector-Win.exe	This is the 32-bit Connector installer containing a CheckPoint OpSec device support for Windows.
ArcSight-8.4.7.xxxx.0-Connector-Win64.exe	This is the 64-bit Connector installer for Windows.
ArcSight-8.4.7.xxxx.0-Connectors.aup	This is used to install or upgrade the Connector through ArcMC or ESM.
ArcSight-8.4.7.xxxx.0-opensource.tgz	This file is needed from compliance perspective.
ArcSight-8.4.7.xxxx.0-LoggerToNNMiConnector-Linux64.bin	This is the installer file for NNMi Connector support for Linux.
ArcSight-8.4.7.xxxx.0-LoggerToOmiConnector-Linux64.bin	This is the installer file for Omi Connector support for Linux.
ArcSight-AWS-CloudWatch-Connector-8.4.7.xxxx.0.zip	This contains the installation files for Amazon CloudWatch Connector.
ArcSight-AWS-SecurityHub-Connector-8.4.7.xxxx.0.zip	This contains the installation files for Amazon SecurityHub Connector.
ArcSight-Azure-Monitor-EventHub-Connector-8.4.7.xxxx.0.zip	This contains the installation files for Microsoft Azure Monitor Event Hub Connector.
ArcSightSmartConnectorLoadBalancer-8.4.7.xxxxx.0.bin	This is the installer file for Load Balancer support for Linux.

SmartConnector Release Notes

Installing SmartConnectors

ArcSightSmartConnectorLoadBalancer-opensource-8.4.7.xxxx.0.tgz	This file is needed from compliance perspective.
ArcSight-8.4.7.xxxx.0-GalaxyThreatAccelerationConnector-Linux64.bin	This is the installer file for ArcSight Threat Acceleration Program support for Linux.
ArcSight-8.4.7.xxxx.0-GalaxyThreatAccelerationConnector-Win64.exe	This is the installer file for ArcSight Threat Acceleration Program support for Windows.

Upgrading SmartConnectors

Upgrading to CE 24.4 (8.4.7)



Important: If you use any of the SmartConnectors listed in the "Software Fixes" section, note that installing the updated SmartConnector can impact your created content.

Verifying Your Upgrade Files

For information and instructions, see "[Signature Verification Procedure](#)" on page 12.

Upgrading SmartConnector to CE 24.4 (8.4.7)

You can upgrade a SmartConnector to implement the newly introduced features, mapping improvements and overall functionality of a SmartConnector. You can upgrade connectors either locally or remotely. Connectors automatically determine their upgrade status when they start.

For information and instructions, see [Upgrading SmartConnectors](#).

Upgrading Load Balancer to CE 24.4 (8.4.7)

For information about upgrading Load Balancer to CE 24.4 (8.4.7), see [Upgrading Load Balancer](#).

Deleting Older Vulnerable Libraries after Upgrading a Connector

When you upgrade a Connector from local, ArcMC, or ESM, it creates a backup of the install directory of the existing connector to facilitate rollback in unforeseen scenarios.

Earlier versions of the connector might have libraries that were vulnerable and were upgraded to non-vulnerable later versions. This might require cleaning all vulnerable libraries from the system manually.



Note: Though the vulnerable libraries are present in the backup folder, the active connector instances do not use these files. Whether you delete the vulnerable libraries or not, these static files will not cause any harm.

Perform the following steps to delete the older vulnerable libraries manually:



Note: This disables the rollback ability. However, you can retain the backup of certain configurations, if required.

Option 1 – Delete only the vulnerable libraries

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command: `cd Xxxxx/lib/agent`

3. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

4. Run the following command: `cd Xxxxx/system/agent/web/webapps/axis/WEB-INF/lib/`

5. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

6. Run the following command: `cd Xxxxx/lib/agent/axis`

7. Run the following command to remove the log4j libraries: `rm -rf *log4j*`

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Open the `Xxxxx\lib\agent` folder.

3. Search for **log4j** and delete all the entries.

4. Open the `Xxxxx\system\agent\web\webapps\axis\WEB-INF\lib\` folder.

5. Search for **log4j** and delete all the entries.

6. Open the `Xxxxx\lib\agent\axis` folder.

7. Search for **log4j** and delete all the entries.

Option 2 - Delete the complete backup folder of the existing connector

For Linux:

1. Run the following command: `cd $Arcsight_Home`

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Run the following command to delete the backed up folder: `rm -rf Xxxxx` (for example: `rm -rf X8444`)

For Windows:

1. Go to `$Arcsight_Home`.

The following folders will be displayed:

- **current** (upgraded version of the connector)
- **Xxxxx** (xxxx refers to the build number of connector before upgrade, for example: X8444)

2. Delete the **Xxxxx** folder manually.

Known Issues

This section includes legacy issues from the ArcSight Installer.

Application Module	Description
All SmartConnectors	<p>When upgrading the SmartConnector from version 24.2 (8.4.5) or earlier to version 24.3 (8.4.6) or later, any custom keystore or truststore passwords for remote management are lost when you start the SmartConnector after the upgrade. This issue occurs because the custom passwords that are set in plain text are deleted and replaced with the obfuscated version of the default password.</p> <p>Workaround:</p> <p>After upgrading the SmartConnector, do the following to reset the custom password:</p> <ol style="list-style-type: none"> 1. Open the agent.properties file. 2. Do one of the following: <ul style="list-style-type: none"> • If you have started the SmartConnector after the upgrade, stop the connector, and then edit the file to replace the obfuscated default password with your custom password in plain text that will further be encrypted. For example: Change: <code>remote.management.ssl.key.password.encrypted=OBFUSCATE.4.9.0\:1qCPcLBfJN/VxyAZbkMm1tebkwXzzlVNrzTpqjJdunckB023</code> to <code>remote.management.ssl.key.password.encrypted=<custom password in clear text></code> • If you have not started the SmartConnector after the upgrade, then edit the file to encrypt the plain text custom password. For example: Change: <code>remote.management.ssl.key.password=<custom password in clear text></code> to <code>remote.management.ssl.key.password.encrypted=<custom password in clear text></code> 3. Start the SmartConnector. After starting, the custom password in plain text will be replaced with its encrypted version. <p>Note: After applying the workaround, the encrypted custom password will be retained for future upgrades.</p>

Known Issues

Microsoft Azure Monitor Event Hub	<p>The certs folder does not get created after deploying the Azure Monitor Event Hub connector</p> <p>After a new deployment of the Azure Monitor Event Hub, the certs folder is not created in the following location:</p> <p>Storage accounts > <Storage account name> > Data Storage > File shares > <function app name> > <function app name>.</p> <p>Workaround</p> <p>To fix this issue:</p> <ol style="list-style-type: none">1. After the deployment of the new connector, go to the newly created storage account.2. In the navigation pane, click Settings > Configuration.3. In the Allow Blob anonymous access option, click Enabled and then click Save.4. Run the DeployFunction.ps1 file again.5. 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. <p>After the deployment process is completed, the certs folder will be created.</p>
--	--

All SmartConnectors	<p>SmartConnector Services are not restarting automatically when the server is restarted</p> <p>When the SmartConnector is installed as a service and the sever is restarted, the SmartConnector service does not start automatically even though the Start the service automatically option is set to Yes. This issue is reproducible in RHEL 9.x and Rocky Linux 9.x.</p> <p>Workaround</p> <p>To keep the SmartConnector service running automatically after the server is restarted:</p> <ol style="list-style-type: none">1. Install the chkconfig package as a root user: <code>yum install chkconfig</code> Note: You might encounter the error “unpacking rpm package error” when installing the chkconfig package. For more information, see Issue while installing the chkconfig package. Make sure that you read through it all before installing chkconfig.2. Install the SmartConnector as a root user. Ensure that you have set the Start the service automatically option to Yes.3. Run the following command: <code>chcon system_u:object_r:bin_t:s0 /etc/init.d/service_name</code> This command changes the security context of the <code>/etc/init.d/service_name</code> file to <code>system_u:object_r:bin_t:s0</code>. The chcon command is used to change the SELinux security context of a file. <p>Issue while installing the chkconfig package</p> <p>When the chkconfig package is installed, it fails with the following error message: “Error unpacking rpm package”</p> <p>Root Cause</p> <ul style="list-style-type: none">• The <code>/etc/init.d</code> directory was created in system during the installation of some third-party applications.• Later on, when you install the chkconfig package, the system attempts to create a symbolic link <code>/etc/init.d</code> and point to <code>/etc/rc.d/init.d</code>.• Because the <code>/etc/init.d/</code> directory already exists , the installation of the chkconfig package fails because the system is unable to create the symbolic link for the installation. <p>Workaround</p> <p>Remove the <code>/etc/init.d</code> directory or any other '<code>/etc/rc*</code>' directories (except <code>rc.d</code>) or move it to the other location by running either of the following commands:</p> <ul style="list-style-type: none">• <code># rm -rf /etc/init.d/</code>• <code># mv /etc/init.d /tmp/init.d.bk</code>
---------------------	---

Known Issues

	<p>Note: An error occurs if the cleanup is not appropriate. Therefore, the chkconfig package might end up creating a file with the wrong name instead of init.d:</p> <pre>[root@rhel92 ~]# ls -l /etc/ grep init.d drwxr-xr-x. 2 root root 6 Apr 5 12:42 init.d lrwxrwxrwx. 1 root root 11 May 23 2023 init.d;660f733f -> rc.d/init.d <=</pre> <p>In such cases, remove the file manually:</p> <pre># rm init.d\;660f733f</pre>
Amazon S3	<p>Diagnostic Steps</p> <ul style="list-style-type: none"> Check if the content of chkconfig RPM already exists as directories. The links appear as follows: <pre># ll /etc/rc* lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc0.d -> rc.d/rc0.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc1.d -> rc.d/rc1.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc2.d -> rc.d/rc2.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc3.d -> rc.d/rc3.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc4.d -> rc.d/rc4.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc5.d -> rc.d/rc5.d lrwxrwxrwx. 1 root root 10 May 23 2023 /etc/rc6.d -> rc.d/rc6.d lrwxrwxrwx. 1 root root 13 Aug 22 2023 /etc/rc.local -> rc.d/rc.local # ll /etc/init.d lrwxrwxrwx. 1 root root 11 May 23 2023 /etc/init.d -> rc.d/init.d</pre> <ul style="list-style-type: none"> Get a strace of the yum command and analyze the strace output: <pre>strace -fttVyy -s 1024 -o /tmp/yum_install_chkconfig.out yum install chkconfig -y</pre> <p>From the strace output, the following error can be found because the /etc/init.d directory already existed and the system was unable to create the symbolic link for the installation:</p> <pre>error: unpacking of archive failed on file /etc/init.d: cpio: File from package already exists as a directory in system</pre>

All SmartConnectors	<p>SmartConnector remote connections fail due to low entropy</p> <p>Note: The CTH is supported in this release and are deprecated as of 8.4. CTH functionality will be removed in an upcoming release, by March 31, 2024</p> <p>All SmartConnectors remote connections go through SSL and they depend on the Operating System random number pool (entropy pool) to generate private keys for secure communication. When the entropy pool is less than the ideal lower limit of 1000, the keys are not generated, communication cannot be established and the SmartConnector does not start. In cloud hosted Linux instances, the entropy pool value can be less than 1000.</p> <p>Workaround:</p> <p>To ensure that the entropy value is at the desired level:</p> <ol style="list-style-type: none">1. Install the <code>rng-tools</code> package: <code>sudo yum install -y rng-tools</code>2. Add the following line to the <code>/etc/sysconfig/rngd</code> file: <code>EXTRAOPTIONS="-r /dev/urandom"</code>3. Check the entropy availability in the system: <code>cat /proc/sys/kernel/random/entropy_avail</code>4. Start the <code>rngd</code> package as a root user: <code>service rngd start</code>5. Enable the <code>rngd</code> service to start at the system start-up: <code>systemctl enable rngd.service</code> <code>systemctl start rngd.service</code>6. Ensure that the <code>rngd</code> package is always running (even after a reboot) as root user: <code>chkconfig --level 345 rngd on</code>7. Check the entropy availability in the system, after starting the <code>rngd</code> service: <code>cat /proc/sys/kernel/random/entropy_avail</code> <p>Unable to install connector because of missing packages</p> <p>Workaround:</p> <p>Ensure that the following packages are installed:</p> <ol style="list-style-type: none">1. <code>yum install -y unzip</code>2. <code>yum install -y fontconfig \ dejavu-sans-fonts</code>
---------------------	--

All SmartConne ctors installed on Solaris	<p>When upgrading SmartConnectors on Solaris, a timeout error is displayed</p> <p>Workaround:</p> <ul style="list-style-type: none"> • If the Solaris connector is already installed as a standalone, locally upgrade to 8.2.0. • If the Solaris Connector is installed as a service: <ol style="list-style-type: none"> a. Stop the service. b. Go to HOME/current/bin and execute ./runagentsetup. c. Uninstall the service in Global Parameters and exit the wizard. d. Perform a local upgrade to 8.2.0. e. Install the Connector as a service and exit the wizard. f. Start the service.
	<p>Connector logs show Fatal Exception error: Unable to find requested property 'transport.cefkafka.extra.prod.props'</p> <p>This message does not impact the performance or the functionality of the Connector.</p> <p>Workaround:</p> <p>If you are using a map file with an expression set in the <connector_install_location> \counterintelligence location and the connector runs out of memory, add the following property to agent.properties as a workaround:</p> <pre>parser.operation.result.cache.enabled=false</pre> <p>If this problem happens with Windows Event Log Native, and the above workaround does not completely solve the problem, reduce the value of the eventprocessorthreadcount Native connector parameter. You can try to reduce it successively, down to a minimum value of 1, to see which value works best for your environment. Example:</p> <pre>agents[0].eventprocessorthreadcount=5 or agents[0].eventprocessorthreadcount=1, etc..</pre> <p>where 0 is the index of the Microsoft Windows Event Log - Native connector in the container.</p>
All File SmartConne ctors	<p>When adding a log into a log file using the vi text editor, events are not sent to ESM</p> <p>Arcsight file connectors do not read events if the files are edited using the vi editor on Linux platforms.</p> <p>Workaround:</p> <p>Use the cat command to append data:</p> <p>Syntax:</p> <pre>cat >> log_file_name [Enter] "your logs" ctlr+c</pre>

Known Issues

Google Cloud SmartConne ctor	<p>The Google SmartConnector cannot authenticate tokens with Google API</p> <p>The following error is displayed when the connector is used from ArcMc with the One-Click feature:</p> <pre>{ "error" : "invalid_grant", "error_description" : "Invalid JWT: Token mustbe a short-lived token (60 minutes) and in a reasonable timeframe. Check youriat and exp values in the JWT claim." }</pre> <p>Workaround:</p> <p>The common cause is that the clock in the machine from which you are executing your task is not in sync with the Network Time Protocol (NTP). Match the connector time with the current time.</p>
---------------------------------------	--

ArcMC Managed SmartConnectors	<p>SmartConnectors cannot be bulk-upgraded on a Linux server</p> <p>Workaround:</p> <p>Before performing a SmartConnector bulk upgrade from ArcMC on any Linux server including an ArcMC appliance, install the <code>rng-tools</code> on the corresponding Linux OS.</p> <p>Note: This procedure is not required if the connector is upgraded on a Windows server or if only one connector is upgraded per Linux server.</p> <p>To install and configure the <code>rng-tools</code> package after a fresh install, follow the steps mentioned for SmartConnector remote connections fail due to low entropy.</p> <p>One-Click installation fails on several versions of Linux distributions</p> <p>The following are the Linux distributions where the one-click installation fails through ArcMC 2.9.4:</p> <ul style="list-style-type: none">• RHEL 8.1 or later• CentOS 8.1 or later• SUSE 15 or later <p>However, this issue is not detected in RHEL 9.4, Rocky Linux 9.4, and Rocky Linux 8.10.</p> <p>Workaround:</p> <p>Pre-requisites for instant connector deployment:</p> <ul style="list-style-type: none">• Python2• Libselinux-python <p>Note: If the SmartConnector Linux machine does not have Python pre-installed, proceed with manual installation.</p> <p>To manually install Python:</p> <p>Apply these changes to the target Linux host (the VM where the connector will be deployed):</p> <ol style="list-style-type: none">1. Install python2 by the following command: <code>sudo yum install -y python2</code>2. Create a symlink by the following command: <code>sudo ln -s /usr/bin/python2 /usr/bin/python</code>3. Install the libselinux-python package by the following command: <code>sudo yum install -y libselinux-python</code> <p>Note: If the <code>yum</code> command fails when installing <code>libselinux-python</code>, the <code>rpm</code> can be downloaded from: http://mirror.centos.org/centos/8/AppStream/x86_64/os/Packages/libselinux-python-2.8-6.module_el8.0.0+111+16bc5e61.x86_64.rpm</p>
-------------------------------------	--

Known Issues

CyberArk Privileged Access Security	<p>Issues are encountered when parsing the CyberArk logs in Common Event Format (CEF)</p> <p>The issue occurs because the CyberArk logs do not contain a pipe symbol (' ') in the header section, after the name field. This results in mapping discrepancies across all the fields in some cases or issues in the event.name field in other cases. This parsing anomaly hinders the accurate extraction and representation of information from the logs.</p> <p>Workaround</p> <p>To address this issue, request modifications to the log format as described in the ArcSight Common Event Format (CEF) Implementation Standard document, to ensure that the header section contains the pipe symbol (' ') after the name field.</p>
IBM Big Fix REST API	<p>Connector installation fails when the client properties file is auto populated incorrectly</p> <p>While installing the IBM Big Fix API connector through ArcMC, it populates the following incorrect path on the client properties file:</p> <p>"E:\depot\candidate\connector\GA\main\system\agent\config\bigfix_api\relevancequeryfile.properties". When the client properties file is auto populated incorrectly, the connector installation fails.</p> <p>Workaround:</p> <p>Set the following path manually:</p> <pre>\$ARCSIGHT_HOME/current/system/agent/config/bigfix_api/relevancequeryfile.properties</pre>
Microsoft 365 Defender	<p>Command Line installation of the Microsoft 365 Defender SmartConnector mandates 'Certificate Path' value for the 'Shared Secret' authentication method</p> <p>While installing the Microsoft 365 Defender SmartConnector from the command line, if the authentication method selected is Shared Secret, the connector installation script treats the optional Certificate Path parameter as mandatory, and therefore does not proceed with the installation if the parameter has no value.</p> <p>Workaround:</p> <p>Install the Microsoft 365 Defender SmartConnector by using the installation wizard.</p> <p>OR</p> <p>You can enter any sample value for the Certificate Path parameter to proceed with the installation.</p>
Microsoft Message Trace REST API	<p>Issues with ArcMC upgrade behaviour in the Message Trace REST API connector</p> <p>Unable to upgrade the Message Trace Rest API Connector through ArcMC.</p> <p>Workaround:</p> <p>You can upgrade the Message Trace REST API Connector either using ESM or locally.</p>

Microsoft Windows Event Log (WiSC)	<p>WiSC SmartConnector issues</p> <p>WiSC is a special SmartConnector that can be deployed on supported Linux operating systems. It has the following issues:</p> <ul style="list-style-type: none"> • Issue #1: High CPU utilization on the monitored Windows host (log endpoint) <p>High CPU utilization is detected on the monitored Windows hosts (log endpoints) as a result of the WinRM process taking up to 50% to 70% (on average).</p> <ul style="list-style-type: none"> • Issue #2: WinRM inherent EPS limitations <p>WinRM has an event rate limit of around 140 EPS (sustained). Therefore, it is not recommended to use the WiSC SmartConnector to collect logs from Windows endpoints as they generate higher EPS rates.</p> <p>Workaround:</p> <p>To mitigate these issues, use the Microsoft Windows Event Log - Native. For more information, see the Technical Note on WinRM-related Issues.</p>
Microsoft Windows Event log - Native	<p>The Microsoft Windows Event Log - Native SmartConnector 8.4 is unable to receive events on Windows Server 2012 R2</p> <p>The communication between winc-agent (.NET component) and the SmartConnector (Java component) does not support TLS.</p> <p>Workaround:</p> <p>Because of the cipher suite support limitations in Microsoft Windows, the SmartConnectors 8.4 running on Window Server 2012 R2 must use 'Raw TCP' instead of the TLS protocol.</p> <p>To use 'Raw TCP', perform the following steps after installing the SmartConnector:</p> <ol style="list-style-type: none"> 1. Open the <ARCSIGHT HOME>/current/user/agent/agent.properties file. 2. Change the parameter value from agents[0].communicationprotocol=TLS to agents[0].communicationprotocol=Raw TCP 3. Restart the SmartConnector.
Microsoft Azure Monitor Event Hub	<p>Azure Event Hub debug mode issue</p> <p>Enable the Azure Event Hub Debug Mode for function apps for support purposes. Enabling it for normal operation can cause parsing and mapping errors.</p> <p>Workaround:</p> <p>To configure the debug mode:</p> <ol style="list-style-type: none"> 1. Go to Azure portal > Function app > Configuration. 2. Set the DebugMode application value to False. 3. Restart the Function App.

Load Balancer	<p>Load Balancer arc_connlb service does not start and displays an error message</p> <p>When you upgrade Load Balancer while the services are still running, after the successful upgrade, the Load Balancer arc_connlb service does not start and displays an error message in the lb.out.wrapper.log even after you start the arc_connlb service manually.</p> <p>Workaround: When you upgrade Load Balancer while the services are still running, the system displays a notification message to stop all the programs before continuing with the upgrade. However, it does not mention the specific services you need to stop.</p> <p>Perform the following steps to fix this issue:</p> <ol style="list-style-type: none">1. After you install Load Balancer as a service, before you upgrade, stop the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb stop</code> or <code>service arc_connlb stop</code>2. After Load Balancer is successfully upgraded, start the arc_connlb service by using the following command: <code># /etc/init.d/arc_connlb start</code> or <code>service arc_connlb start</code>
---------------	--

Trellix ePolicy Orchestrato r DB	<p>Reregistration of the Trellix Orchestrator DB type connector fails with ESM as the destination</p> <p>When you re-register the Trellix Orchestrator DB type connector with ESM as the destination, the reregistration fails and the connector displays an error (null) message,</p> <p>Workaround:</p> <p>Perform the following steps for re-registering the connector on ESM using ArcMC:</p> <ol style="list-style-type: none">1. Enable the remote management mode in the connector using runagentsetup script, with port range of 9001-9010.2. Navigate to Node Management > View all nodes in ArcMC.3. Enter the Location and provide a name for the location, and then click Next.4. Specify the location of your computer as the host, and then click Add.5. Enter the Type of the SmartConnector.6. Enter the user and password as User:connector_user and Password:change_me and click Add and Import certificate.7. Navigate to Node management > View all nodes.8. Click Connectors > Connector > Destinations.9. Click Next > Re-register destination.10. Click Failed destination.11. Enter the user and password for ESM and click Next.12. Click Yes > Done. <p>The connector is now linked to ESM with a new name.</p> <p>Error is displayed while importing the parameters of the Trellix Orchestrator DB type connector</p> <p>While installing the Trellix Orchestrator DB type connector, if you import its parameters instead of manually specifying them on the screen, an error message is displayed and the installation is terminated.</p> <p>Workaround:</p> <p>While installing the connector, manually specify the parameters instead of importing them.</p>
---	---

Connector End-of-Life Notices



Note: For information about connector end-of-life status, refer to [Connector End-of-Life Notices](#) on the [ArcSight SmartConnector 24.4 Documentation](#) page.

Starting in ArcSight SmartConnectors version 24.4.0, the 32-bit version of SmartConnectors are no longer Generally Available through the SLD portal and will be deprecated as of October 31, 2024, as there are very few customers who use the 32-bit version.

OpenText will continue to support the 32-bit version of SmartConnectors as part of the regular Product Support Lifecycle in future SmartConnectors releases until OpenText determines that there are no existing customers using it. If you have the need to download the 32-bit SmartConnectors, you can request the Support Team for the binaries.



Note: There will be a change in the file name of 32-bit SmartConnectors to make the “32-bit” identifier more prominent. This is done to ensure that someone does not accidentally download the 32-bit version instead of the 64-bit version.

SmartConnector End of Support Announcements

SmartConnector	End of Support Date	Details
Connectors in Transformation Hub (CTH) and Collectors	01/2027	<p>The CTH and Collectors were deprecated with the SmartConnector release of 8.4. Deployment of CTH and Collectors is now removed in CE 24.2.</p> <p>CTH and Collectors will have limited support for customers already using these components until the end of support date for the ArcSight Connector CE 24.1 release, which is Jan 31, 2027.</p>

Microsoft Azure Monitor Event Hub	01/2027	<p>The Microsoft Azure Monitor Event Hub connector has been replaced by the Microsoft Azure Event Hub SmartConnector.</p> <p>The Microsoft Azure Monitor Event Hub connector will not be shipped after January 2025. Therefore, it is highly recommended to switch to the Microsoft Azure Event Hub SmartConnector before January 2025.</p>
-----------------------------------	---------	--

SmartConnectors No Longer Supported

SmartConnector	End of Support Date	Details
Model Import Connector for Malware Information Sharing Platform (MISP)	06/2023	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Model Import Connector for Micro Focus Security ArcSight Reputation Security Monitor Plus (RepSM Plus)	10/2022	Replaced by the new SmartConnector named - ArcSight Threat Acceleration Program (ATAP), which has enhanced threat intelligence capabilities.
Microsoft Windows Event Log – Unified Connector (WUC)	12/2021	Lack of customer demand.
Microsoft Forefront Threat Management Gateway (TMG) 2010	04/2020	End of support by vendor.
Windows Server 2008 R2	01/2020	End of support by vendor.
Checkpoint Syslog	12/2019	The vendor no longer supports version R77.30. Therefore, we offer limited support. Fixes and improvements are no longer provided for this version.
Solsoft Policy Serve	11/2019	Lack of customer demand.
Oracle Audit DB version 9	08/2019	End of support by vendor.
Symantec Endpoint Protection DB – SEP version 1	02/2018	End of support by vendor.
Solaris 10 Premier support	01/2018	End of support by vendor.

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 Release Notes (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!