**opentext**™

# ArcSight SmartConnectors

Software Version: 8.4.3

# Configuration Guide for Microsoft IIS Multiple Site File SmartConnector

## Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

## Copyright Notice

## Trademark Notices

## Documentation Updates

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

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

# Contents

# Configuration Guidefor 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 os 1048576 bytes. If this attribute is set to a value less than 1048576 bytes, the default value is implicitly7 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 **W3SVC**X, 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. |

| 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 configuredfor 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 |
| | - If the local log file is at C:\inetpub\logs\LogFiles\W3SVC1, then set agents[0].logfilehome =C\:\\inetpub\\logs\\LogFiles |
| 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.

**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 08/072015, 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 |

| 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 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 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!