



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 `\\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 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 <code>\\MyLogServer\LogShare</code>. 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: <code>systemroot\System32\IISLogFile</code>.</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: <code>\\MyLogServer\LogShare\W3SVC1</code>, then enter it as <code>agents[0].foldertable[0].folder=\\\\MyLogServer\LogShare</code>.• The local log file is at: <code>C:\inetpub\logs\LogFiles\W3SVC1</code>, then enter it as <code>agents[0].foldertable[0].folder=C:\inetpub\logs\LogFiles</code>.
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	<p>Select true or false.</p> <p>If you select true, only the log file with the latest times tamp in a site folder (such as W3SVCX) are processed when connection is initiated. Otherwise, all log files are processed.</p>



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!