Micro Focus Security ArcSight SmartConnectors

SmartConnector for Google Cloud

Configuration Guide

Document Release Date: February 2022
Software Release Date: February 2022

Legal Notices

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

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

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

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

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

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

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

SmartConnector for Google Cloud Platform

This guide provides information about Google Cloud Connector that collects events from Google Cloud Platform.

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 SmartConnectors.

Additional Documentation

The ArcSight SmartConnectors documentation library includes the following resources:

- *Installation Guide for ArcSight SmartConnectors*, which provides detailed information about installing SmartConnectors.
- *Configuration Guides for ArcSight SmartConnectors*, which provides information about configuring SmartConnectorss to collect events from different sources.
- *Release Notes for ArcSight SmartConnectors*, which provides information about the latest release

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 Documentation-Feedback@microfocus.com.

For specific product issues, contact Micro Focus Customer Care.

Product Overview

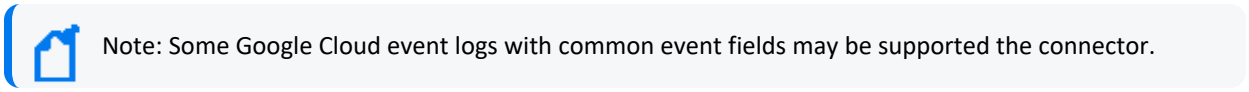
Google Cloud Platform is a suite of public cloud computing services offered by Google. The platform includes a range of hosted services for compute, storage and application development that run on Google hardware. Google Cloud Platform services can be accessed by software developers, cloud administrators, and other enterprises IT professionals over the public internet or through a dedicated network connection.

The following services are currently supported by the SmartConnector for Google Cloud:

- **Pub/Sub** is an asynchronous messaging service that decouples services that produce events from services that process events.

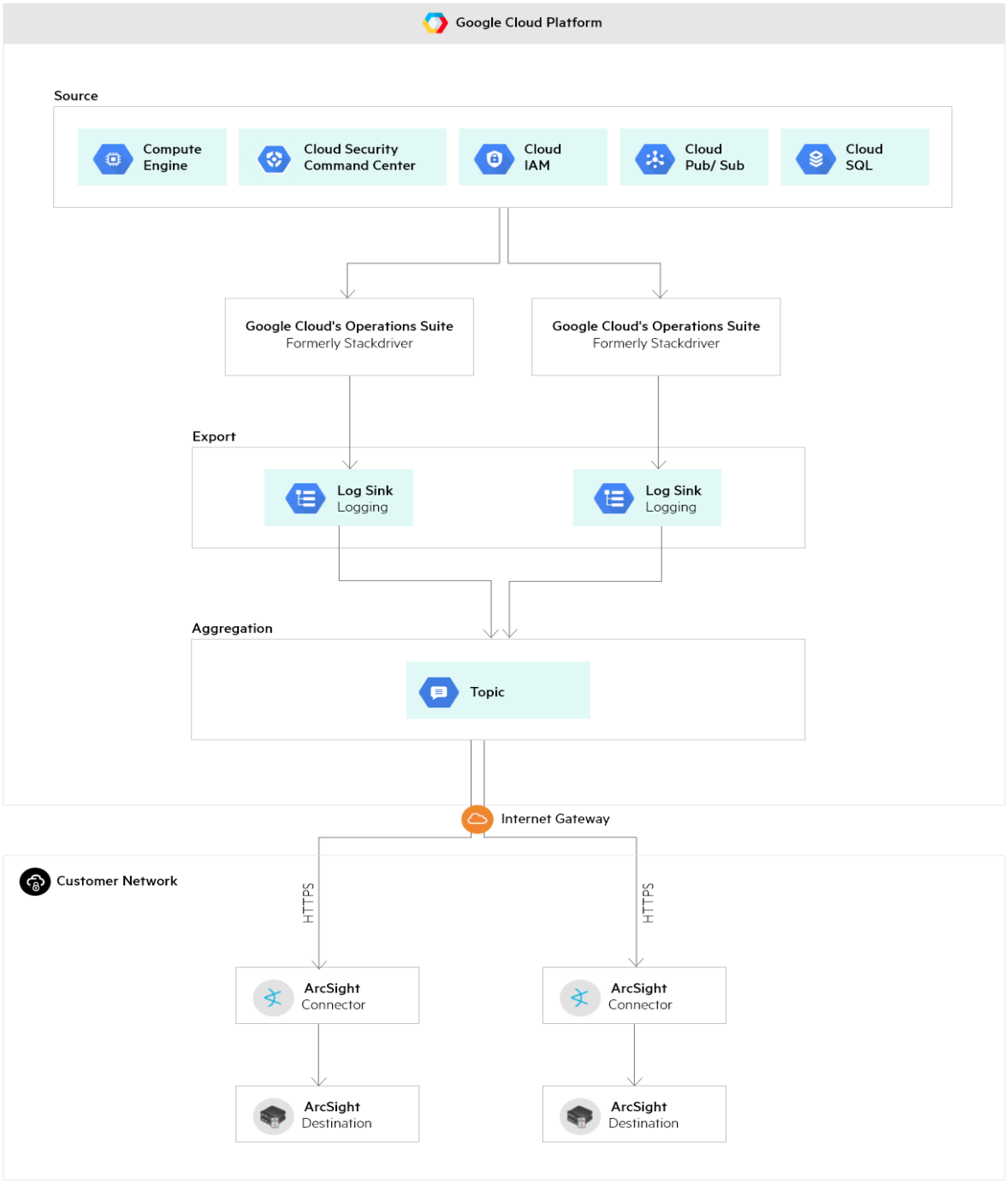
  You can use Pub/Sub as messaging-oriented middleware or event ingestion and delivery for streaming analytics pipelines.

  Pub/Sub offers durable message storage and real-time message delivery with high availability and consistent performance at scale. Pub/Sub servers run in all Google Cloud regions around the world.
- **IAM** lets you grant granular access to specific Google Cloud resources and helps prevent access to other resources. IAM enables you to adopt the least privileged security principle, stating that nobody should have more permissions than needed.



Understanding Data Collection

The following diagram provides a high-level overview of how the ArcSight SmartConnector for Google Cloud collects the Google Cloud Platform events.



Google Cloud Platform Permissions

Role	Permissions	Description
Create Custom Role For example: ArcSight_ CustomRole	• pubsub.subscriptions.consume • pubsub.subscriptions.get • pubsub.topics.get	These are the minimum roles required to retrieve the events.

Note: While creating the Service Account under **Grant this service account access to project** section, click **Select Role** drop down menu, select the **Custom Role** created above and continue with the installation.

Creating a Service Account Key

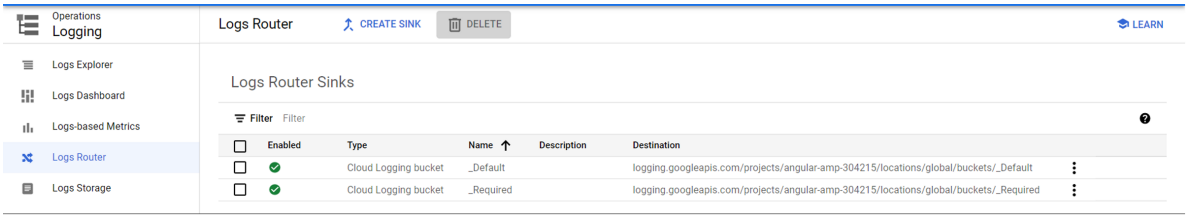
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google.

To create a new service account:

1. Go to **IAM & Admin** > **Service Accounts**.
2. Click **Create Service Account**.
3. Enter the **Service Account Details** and click **Done**.

   The account is successfully created.
4. **Click Actions** > **Create Key**.
5. Choose **JSON** as the export option and click **Create**.

   The service key file is downloaded, and you will use it to access cloud resources.



Configuring Log Retrieval

Creating a Topic

1. Go to the **Pub/Sub** resource.
2. On the left pane, click **Topics**.
3. Click **Create Topic**.
4. Enter a unique topic Id and click **Create Topic**.

   The topic is successfully created as well as its subscription.

Creating a Log Router

1. Go to **Operations** > **Logging** > **Log Router**.
2. Click **Create Sink**.
3. Enter the sink name and a description.
4. Choose the sink destination.
   a. Select the **Cloud Pub/Sub** topic as your sink service.
   b. Select the topic previously created.
5. Write a valid log query to filter out the events that are redirected to the topic.
6. If you want to create an exclusion filter, click **Create Sink** and the newly generated log is routed to the topic.

Creating a Log Router for Topics Located in a Different Project

1. Go to **Operations** > **Logging** > **Log Router**.
2. Click **Create Sink**.
3. Enter the sink name and a description.
4. Choose the sink destination.
   a. Select a fully qualified topic name.
   b. Prepend **pubsub.googleapis.com** to it.

      The format is

pubsub.googleapis.com/projects/PROJECT_NAME/topics/TOPIC_NAME

for example

pubsub.googleapis.com/projects/angular-amp-304215/topics/ArcSight-Topic

5. Write a valid log query to filter out the events that are redirected to the topic.
6. If you want to create an exclusion filter, click **Create Sink** and the newly generated log is routed to the topic.

Installing 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 Micro Focus SSO and Protect 724 sites.

1. Download the SmartConnector executable for your operating system from the Micro Focus SSO site.
2. Start the SmartConnector installation and configuration wizard by running the executable.

   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...

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:

Parameters	Settings
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 Micro Focus SecureData solutions to provide encryption. For more information, refer to the *Micro Focus SecureData Architecture* guide.	
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 Micro Focus 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.

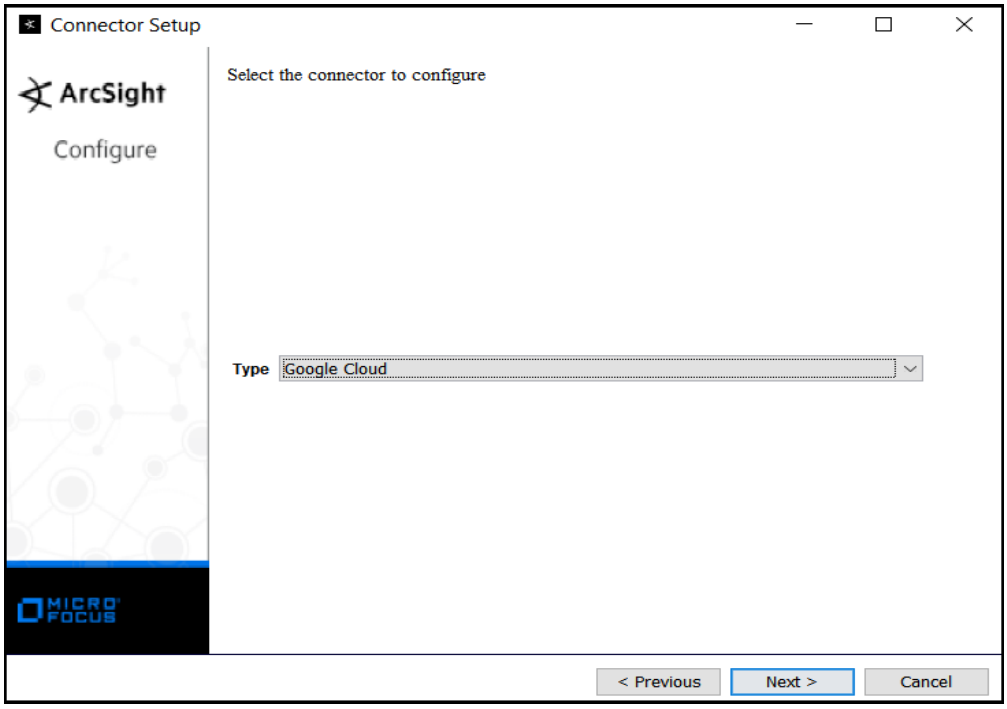
Parameters	Settings
Format Preserving Identity	The Micro Focus SecureData client software allows client applications to protect and access data based on key names. This key name is referred to as the identity. Enter the user identity configured for Micro Focus SecureData.
Format Preserving Secret	Enter the secret configured for Micro Focus SecureData to use for encryption.
Event Fields to Encrypted	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.

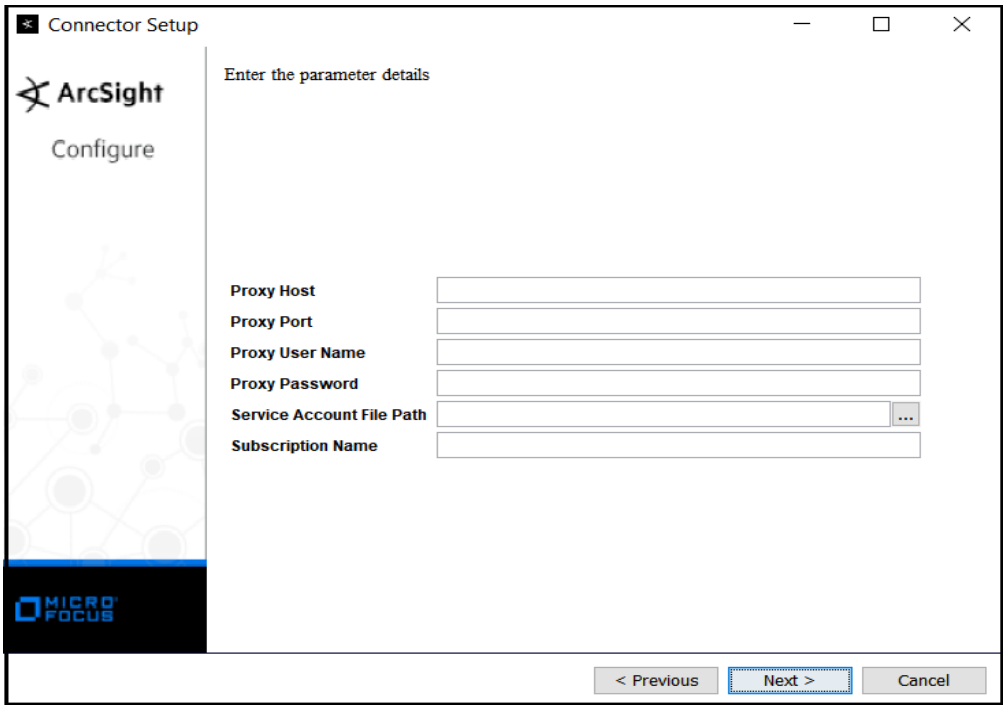
Review the summary of your selections and click **Next**. Click **Continue** to return to proceed with the **Add a Connector** window. Continue the installation procedure with "Select Connector and Add Parameter Information".

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 **Google Cloud** and click **Next**.



3. Enter the required SmartConnector parameters to configure the SmartConnector, then click **Next**.



Parameter	Details
Proxy Host	Enter the proxy host IP address or name.
Proxy Port (Optional)	The proxy port used to access the Internet.
Proxy User Name (Optional)	The proxy user used to access the Internet.
Proxy Password (Optional)	The proxy password used to access the Internet.
Service Account File Path	Service account file path
Subscription Name	PubSub topic subscription name

4. 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*.
5. 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.
6. 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.
7. 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

ArcSight ESM Field	Device-Specific Field
Device Product	protoPayload/serviceName
Device Vendor	Google Cloud
device Receipt Time	timestamp
Device Event Class Id	Last word of the (protoPayload/methodName) + "|" + (success|failure)
Name	protoPayload/methodName
Device Severity	severity
Device Custom String 1	resource/labels/project_id
Device Custom String 2	protoPayload/resourceName
Source User Name	protoPayload/authenticationInfo/principalEmail
Device Custom String 4	protoPayload/authenticationInfo/principalSubject
Device Custom String 5	protoPayload/request/messageRetentionDuration
Device Custom Date 1	protoPayload/requestMetadata/requestAttributes/time
Device Custom Date 2	receiveTimestamp
Device Custom Number 1	protoPayload/request/ackDeadlineSeconds
Source Address	protoPayload/requestMetadata/callerIp
Request Method	protoPayload/methodName
Request Client Application	protoPayload/requestMetadata/callerSuppliedUserAgent
Source Service Name	protoPayload/serviceName
Message	protoPayload/request/role/description
File Permission	protoPayload/serviceData/permissionDelta/addedPermissions
File Id	protoPayload/request/role_id

Troubleshooting

The Google SmartConnector cannot authenticate token with Google API.

The following error is displayed when when the connector is being used from ArcMc with the One-Click feature:

```
{ “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." }
```

Workaround:

The common cause is that the clock from which you are executing your task is not in sync with the NTP (Network Time Protocol). Match the connector time with the current time.

For more information, see troubleshooting.

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 (SmartConnectors 8.3.0)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!