



ArcSight SmartConnectors

Software Version: CE 24.1

Configuration Guide for GitHub Enterprise Audit Log SmartConnector

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

| | |
|--|----|
| Configuration Guide for GitHub Enterprise Audit Log SmartConnector | 4 |
| Product Overview | 5 |
| Prerequisites | 5 |
| Installing and Configuring the SmartConnector | 6 |
| Installing and Configuring the SmartConnector | 6 |
| Device Event Mapping to ArcSight Fields | 8 |
| Send Documentation Feedback | 10 |

Configuration Guide for GitHub Enterprise Audit Log SmartConnector

The guide provides information on installing and configuring SmartConnector for the GitHub Enterprise Audit Log instance.

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

SmartConnector for GitHub Enterprise Audit Log retrieves the audit log events from the enterprise's activity on Github Enterprise with the help of the GitHub REST API. After retrieving the events, it normalizes them and sends them to the configured destinations.

GitHub is a code hosting platform for version control and collaboration. It is used by millions of developers around the world to host their code, collaborate with others, and build software.

GitHub audit logs are logs of events that occur within a GitHub organization or enterprise. These logs can be used to track user activity, identify potential security threats, and troubleshoot problems.

For detailed information about Audit Logs, see [GitHub Enterprise Cloud Documentaion](#).

Prerequisites

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, see *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 GitHub Enterprise Audit Log SmartConnector, ensure the following:

- You have created the Personal Access Token. For more information and to create the Personal Access Token, see [Creating a personal access token](#).
- You have enabled the **read:audit_log** scope for the Personal Access Token created.

Installing and Configuring the SmartConnector


The following sections provide instructions for installing and configuring the connector.

For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

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. From the **Type** drop-down list, select **GitHub Enterprise Audit Log**, and then click **Next**.
5. Specify the following parameters to configure the SmartConnector, and then click **Next**.

The screenshot shows the 'Connector Setup' window for OpenText ArcSight. The window has a title bar with the OpenText logo and standard window controls. On the left, there is a sidebar with the 'opentext ArcSight' logo and a 'Configure' button. The main area is titled 'Enter the parameter details'. It contains several input fields for configuration: 'Proxy Host', 'Proxy Port', 'Proxy User Name', 'Proxy Password', 'Event URL' (which has a pre-filled URL: 'https://api.github.com/enterprises/<Enterprise Name>/audit-l'), and 'Personal Access Token'. At the bottom right, there are three buttons: '< Previous', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

| Parameter | Description |
|-----------------------|--|
| Proxy Host | (Optional) If proxy is enabled for your machine, the IP address or host name of the proxy server required for the proxy configuration to access the internet. |
| Proxy Port | (Optional) If proxy is enabled for your machine, the port number of the proxy server required for the proxy configuration. |
| Proxy User Name | (Optional) If proxy is enabled for your machine, the user name for the proxy server. Specify this value only if proxy needs access to the Internet. If you enter the proxy user name, you must provide the proxy password. |
| Proxy Password | (Optional) If proxy is enabled for your machine, the password for the proxy server user. Specify this value only if proxy needs access to internet and you have specified a user name for the proxy server. |
| Event URL | <p>The URL from where you need to fetch events.</p> <p>The default value is: <code>https://api.github.com/enterprises/<Enterprise Name>/audit-log</code></p> <p><Enterprise Name> is the name of your enterprise.</p> <p>Example: If your enterprise name is Test123 then the Event URL will be as follows: <code>https://api.github.com/enterprises/Test123/audit-log</code></p> |
| Personal Access Token | <p>Enter the Personal Access Token created to authenticate with the GitHub Enterprise Audit Log APIs. For more information and to create the Personal Access Token, see Creating a personal access token.</p> <div> Important: You must enable the <code>read:audit_log</code> scope while creating the Personal Access Token.</div> |

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.



Important: If you select **Do not import the certificate to connector from destination**, the connector installation will end.

9. Select whether you want to run the connector as a service or in the standalone mode.
10. Complete the installation.
11. [Run the SmartConnector](#).

12. For instructions about upgrading the connector or modifying its parameters, see [SmartConnector Installation and User Guide](#).

Device Event Mapping to ArcSight Fields

This section lists the mappings of the ArcSight data fields to the device-specific event fields. For more information about the ArcSight data fields, see [ArcSight Console User's Guide for ESM](#).

| ArcSight ESM Field | Device-Specific Field |
|------------------------------|-----------------------|
| Device Action | action |
| Device Event Class Id | action |
| Device Custom Number 1 | business_id |
| Device Custom Number 1 Label | business_id |
| Device Custom Number 2 | org_id |
| Device Custom Number 2 Label | org_id |
| Device Custom Number 3 | repo_id |
| Device Custom Number 3 Label | Repo Id |
| Device Custom String 1 | country_code |
| Device Custom String 1 Label | Actor Location |
| Device Custom String 2 | business |
| Device Custom String 2 Label | business |
| Device Custom String 3 | org |
| Device Custom String 3 Label | Organization |
| Device Custom String 4 | public_repo |
| Device Custom String 4 Label | Public Repo |
| Device Custom String 5 | repo |
| Device Custom String 5 Label | repo |
| Device Event Category | operation_type |
| Device Product | Audit Log |
| Device Receipt Time | Created_at |
| Device Vendor | GitHub |

| | |
|----------------------------|------------|
| Request Client Application | User_agent |
| Source Address | actor_ip |
| Source User Id | actor_id |
| Source User Name | actor |

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 GitHub Enterprise Audit Log SmartConnector (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!