
Micro Focus Security ArcSight SmartConnectors

SmartConnector for Okta Configuration Guide

Document Release Date: December 3, 2020

Software Release Date: December 3, 2020



Legal Notices

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

<https://www.microfocus.com>

Copyright Notice

© Copyright 2020 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.

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:

[ArcSight Product Documentation on the Micro Focus Security Community](#)

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://community.softwaregrp.com/t5/ArcSight-Product-Documentation/ct-p/productdocs

Revision History

Date	Description
12/03/2020	First edition of this guide

Contents

SmartConnector for Okta	5
Overview	5
Prerequisites	5
Configuration	5
Configuring the Connector for Event Collection	5
Configuring the Appliance/ArcSight Management Center	5
Prepare to Install Connector	6
Install Core Software	6
Set Global Parameters (optional)	7
Select Connector and Add Parameter Information	9
Select a Destination	11
Complete Installation and Configuration	11
Upgrading the SmartConnector from the Connector Appliance/ArcMC	11
Run the SmartConnector	12
Device Event Mapping to ArcSight Fields	13
Okta Mappings to ArcSight Fields - JSON Parser	13
Send Documentation Feedback	15

SmartConnector for Okta

The Arcsight Okta configuration guide provides information to install the SmartConnector for Okta and configuring the connector for event collection.

Overview

Okta is an enterprise-grade identity and access management service, which helps any person connect with any application, device, or technology. It enables users to securely access any application or device at any time. Although Okta is built for cloud-environments, it is compatible with many on-premise devices as well.

Identity and access management services address authentication, authorization, and access control. It is also about the access that resources might have and how the enabled functions perform.

Prerequisites

- Okta login credentials.

Configuration

Configuring the Connector for Event Collection

Complete the following procedure to enable the connector to access Okta log data:

1. Open a browser, then specify the hostname and port for the proxy server.
You will be redirected to the Okta login page.
2. Log in to Okta using your Okta credentials.
For more information about the events logged by Okta, see the [Okta Documentation](#).

Configuring the Appliance/ArcSight Management Center

Run restutil to Obtain a Refresh Token

Before configuring the SmartConnector for Okta on the Connector Appliance / ArcMC, obtain a refresh token. This token is required to configure the connector. It enables the connector to access Okta log data. To obtain a refresh token, use the REST FlexConnector Configuration Support Tool (restutil) and perform the following steps:

1. Install the SmartConnector package on a host machine where you can access a web browser.
2. Navigate to `$ARCSIGHT_HOME\current\bin`.
3. To retrieve a refresh token, invoke the tool with the following command:

```
arcsight restutil boxtoken <-proxy >
```

For example: `arcsight restutil boxtoken -proxy
proxy.location.microfocus.com:8080`

A web browser launches and prompts you to log into Okta.

4. Enter your Okta user name and password.
5. Click through to access Okta.

The refresh token string displays in the command line window.

6. Copy the string into the Refresh Token field while configuring the connector.

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
- Credentials to log in to Okta

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 the [Micro Focus Security Community](#) website.

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

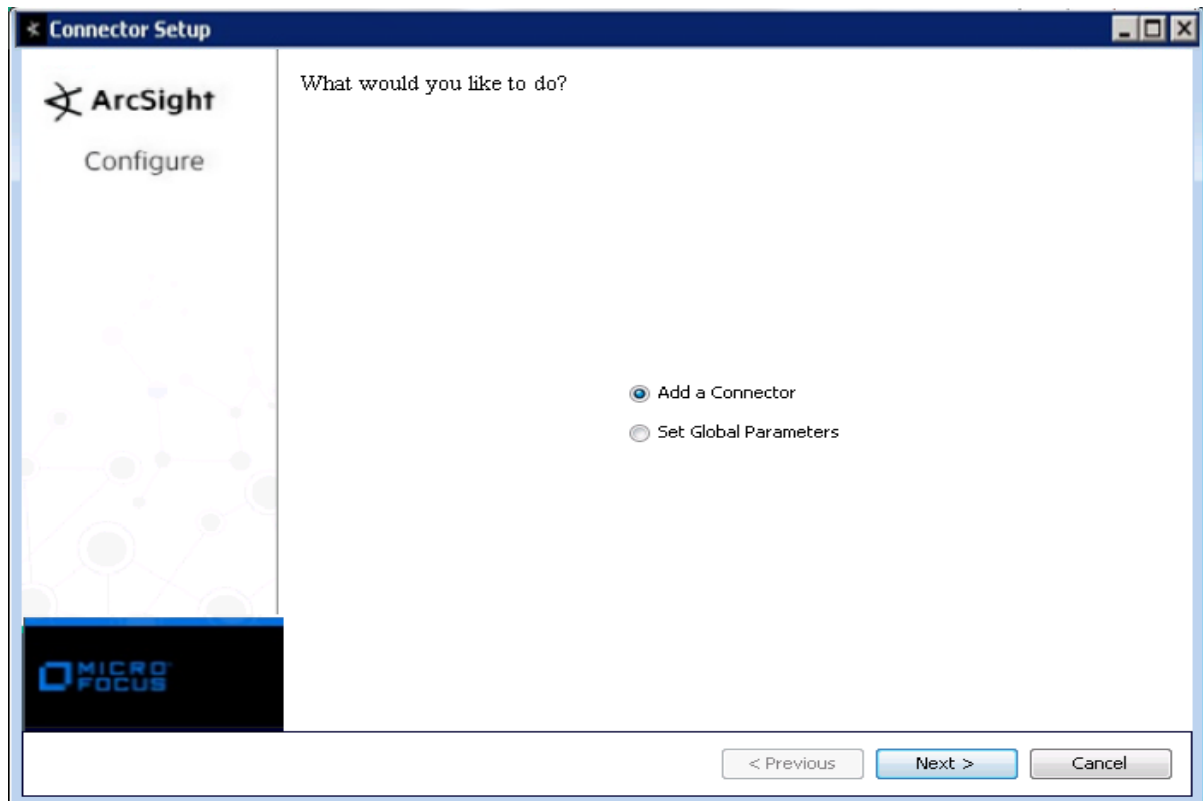
Choose Install Folder

Choose Shortcut Folder

Pre-Installation Summary

Installing...

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 Micro Focus SecureData solutions to provide encryption. See the Micro Focus SecureData Architecture Guide for more information.	
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.
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 "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 **Okta** and click **Next**.
3. Enter the required SmartConnector parameters to configure the SmartConnector, then click Next.

Parameter	Description
Proxy Host	Enter the proxy host IP address or name. This value is required for proxy configuration in order to access Okta host.
Proxy Port	Enter the proxy port. This value is required for proxy configuration.
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.
Event URL	

Parameter	Description
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.
Client ID	This value is provided by the vendor when you register an application
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
Redirect URI	You configure this when you register an application. This is the URL to which the vendor sends the authorization code
Scope	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.
Reauthenticate	If this is set to TRUE, user is required to authenticate when connector starts.
Time Stamp Format	yyyy-MM-dd'T'HH:mm:ss.SSS'Z'
State	An arbitrary alphanumeric string that the authorization server will reproduce when redirecting the user-agent back to the client.
Limit Events	Specifies the number of results.

If a proxy is not required to access the internet, leave the proxy fields in blank and click **Next**.

A web browser window is automatically launched by the connector so that you can log in to Okta.

When the connector launches the web browser window, it attempts to use the default web browser configured in your system. If the default web browser does not launch, it immediately tries launching in other web browsers (Firefox, Google Chrome, Internet Explorer, Konqueror, or Mozilla). Verify that you have one of these web browsers configured in your system.

Also, ensure that the proxy settings in your web browsers are configured correctly so that you can access the internet through your web browser. The Okta authorization endpoint has a lifetime of 10 minutes. To log in, enter your Okta user name and password and click through to access Okta.

After logging in to Okta , continue to the connector configuration. The next page of the connector installation and configuration wizard is displayed automatically. To continue the connector configuration, be sure to return to the installation and configuration wizard window.

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.

Upgrading the SmartConnector from the Connector Appliance/ArcMC

To upgrade a container to the get the latest version of the SmartConnector for Okta:

1. Download the upgrade files for the connector or the remote Connector Appliance from the ArcSight Customer Support site at softwaresupport.softwaregrp.com to the computer that you use to connect to the browser-based interface.
 2. Log in to the browser-based interface.
 3. Click **SetupConfiguration > Administration > Repositories**.
 4. Upload the connector AUP build that contains the latest version of the connector.
 5. In the Connector Appliance, click **Manage**.
 6. Click the **Containers** tab.
 7. Select the container you want to upgrade.
 8. Click **Upgrade**. Click **Next** to upgrade the container.
 9. Select the AUP version and click **Next**.
 10. Select the container you have upgraded and then select **Add New Connector**.
 11. Select the Okta connector and click **Next**.
 12. Enter the parameter values for the connector, including the Refresh Token. See the Configuration Guide for the SmartConnector for Okta for details about parameters. See [Run restutil to Obtain a Refresh Token for ArcSight Management Center](#). Click **Next**.
 13. Select the destination. Click **Next**.
 14. Enter the destination parameters. Click **Next**.
 15. Enter connector details. Click **Next**.
- The connector is added to the container.

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.

Okta Mappings to ArcSight Fields - JSON Parser

ArcSight ESM Field	Device-Specific Field
Device Event Class ID	eventType
Device Product	'OKTA'
Device Receipt Time	__safeToDate(published,"yyyy-MM-dd'T'HH:mm:ss.SSSX")
Device Vendor	'IAM'
External ID	uuid
File ID	One of (source_folder_id, source_item_id)
File Name	One of (source_item_name, source_folder_name)
File Type	One of (source_item_type, one of (source_folder_id, 'folder'))
Name	__ifThenElse(displayMessage,"null",__concatenate(eventType," ",outcome_result),__concatenate(displayMessage," ",__toLowerCase(outcome_result)))
Source Address	Client/ipAddress
Reason	Outcome/reason
Event Outcome	Outcome/result
Device Event Category	eventType
Device Severity	severity
Request Url	debugContext/debugData/url
Request Client Application	client/userAgent/rawUserAgent
Device Action	__regexToken(eventType,"(?:[a-z]+\.\.)(.*)")
Device Custom String 2	transaction/type
Device Custom String 2 Label	'Transaction Type'

ArcSight ESM Field	Device-Specific Field
DeviceCustomString3	__oneOf(debugContext/debugData/signOnMode, debugContext/debugData/appname)
Device Custom String 3 Label	'SignOnModeType/AppName'
Device Custom String 4	__oneOf(debugContext/debugData/requestId, debugContext/debugData/jobId)
Device Custom String 4 Label	'Request/Job Id'
Device Custom String 5	debugContext/debugData/threatSuspected
Device Custom String 5 Label	'Threat Suspected'
Device Version	Version
Flex String 2	authenticationContext/authenticationProvider
Flex String 2 Label	'Authentication Provider'

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 8.1.0)

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!