



ArcSight SmartConnectors

Software Version: 8.4.3

Configuration Guide for Okta 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

Configuration Guide for Okta SmartConnector	4
Overview	5
Prerequisites	5
Configuration	5
Creating Okta API Tokens	5
Enabling the okta.logs.read Scope	5
Installing the SmartConnector	6
Preparing to Install Connector	6
Installing and Configuring the SmartConnector by Using the Wizard	6
Upgrading the Okta Connector	8
Upgrading the Okta Connector from Connector Appliance or ArcMC	8
Upgrading the Okta Connector from ESM	9
Upgrading the Okta Connector Locally	9
Device Event Mapping to ArcSight Fields	9
Okta Mappings to ArcSight Fields - JSON Parser	10
Troubleshooting	12
API Token Authentication Error	12
Send Documentation Feedback	13

Configuration Guide for Okta SmartConnector

The Configuration Guide for Arcsight SmartConnector provides information to install the SmartConnector for Okta and to configure the connector for event collection.

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](#).

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 to log in to Okta organization with the administrator level privileges. You must at least have "Read Only Administrator" permission so that the account is authenticated to generate API Token.
- The application requires `logs.read` permission/scope.

Configuration

Creating Okta API Tokens

For information about creating API Token, refer to the [Create Okta API tokens](#) section from Okta Documentation help.

Enabling the `okta.logs.read` Scope

Perform the following steps to grant consent for the **okta.logs.read** scope:

1. Log in to your Okta account as a user with the administrator privileges.
2. In the Admin Console, go to **Applications > Applications**.
3. Go to **Status > Active** and click the application you created.
4. Click the **Okta API Scopes** tab.



Important: To view the **Okta API Scopes** tab, you must have the administrator level privileges for your Okta account credentials. See [Prerequisites](#).

5. In the **Consent** table, click **Grant** for the **okta.logs.read** scope.
The consent is successfully granted to **okta.logs.read**.

Installing the SmartConnector

Preparing to Install Connector

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:

- Local access to the machine where you want to install the SmartConnector.
- Credentials to log in to Okta.

Installing and Configuring the SmartConnector by Using the Wizard

The installation steps described in this section are specific to the Okta Connector. For detailed installation steps or for manual installation steps, see [SmartConnector Installation and User Guide](#).

To install and configure the Okta 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 **Okta REST API** as the type of connector, then click **Next**.
5. Enter the following SmartConnector parameter values, then click **Next**:

ot Connector Setup

opentext
ArcSight

Configure

Enter the parameter details

Proxy Host

Proxy Port

Proxy User Name

Proxy Password

Event URL

Time Stamp Format

API Token

Limit Events

< Previous

Next >

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 proxy configuration to access Okta host.
Proxy Port	(Optional) If proxy is enabled for your machine, the port number of the proxy server required for proxy configuration.
Proxy User Name	(Optional) If proxy is enabled for your machine, the user name for the proxy server. This value is optional for additional proxy authentication. If you enter the proxy user name, you must provide the proxy password. Specify this value only if proxy needs access to internet.
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.
Event URL	The URL of the vendor to which the request for the events will be made.

Parameter	Description
Time Stamp Format	yyyy-MM-dd'T'HH:mm:ss.SSS'Z'
API Token	Enter the API Token to authenticate with Okta APIs. To create Okta API Token, see "Creating Okta API Tokens" on page 5 .
Limit Events	The number of results.

6. Select a destination and configure parameters.
7. Specify a name for the connector.
8. 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.
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.

Upgrading the Okta Connector

- ["Upgrading the Okta Connector from Connector Appliance or ArcMC" below](#)
- ["Upgrading the Okta Connector from ESM" on the next page](#)
- ["Upgrading the Okta Connector Locally" on the next page](#)

Upgrading the Okta Connector from Connector Appliance or ArcMC

To upgrade to 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 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**, then 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 **API Token**. Click **Next**.



Note: When you upgrade the Okta connector from ArcMc, you must update the **API Token** parameter. To obtain a API Token, see ["Creating Okta API Tokens" on page 5](#).

13. Select the destination and click **Next**.
14. Enter the destination parameters and click **Next**.
15. Enter connector details and click **Next**.

The connector is added to the container.

Upgrading the Okta Connector from ESM

For more information, see [Upgrading Connectors from ESM](#).



Note: When you upgrade the Okta connector from ESM, you must upgrade the connector first and then reconfigure the connector by providing the correct API Token value.

Upgrading the Okta Connector Locally

For more information, see [Upgrading Connectors Locally](#).



Note: When you upgrade the Okta connector locally, you must chose the **Modify Connector** option and configure the API Token value, then complete the upgrade.

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 Receipt Time	<code>__safeToDate(published,"yyyy-MM-dd'T'HH:mm:ss.SSSX")</code>
Device Product	<code>'OKTA'</code>
Device Severity	<code>severity</code>
Device Action	<code>__regexToken(eventType,"(?:[a-z]+\\.)(.*)")</code>
Device Custom String 2	<code>transaction/type</code>
Device Custom String 2 Label	<code>'Transaction Type'</code>
Device Custom String 3	<code>__oneOf(debugContext/debugData/signOnMode, debugContext/debugData/appname)</code>
Device Custom String 3 Label	<code>'SignOnModeType/AppName'</code>
Device Custom String 4	<code>__oneOf(debugContext/debugData/requestId, debugContext/debugData/jobId)</code>
Device Custom String 4 Label	<code>'Request/Job Id'</code>
Device Custom String 5	<code>debugContext/debugData/threatSuspected</code>
Device Custom String 5 Label	<code>'Threat Suspected'</code>
Device Event Category	<code>eventType</code>
Device Event Class ID	<code>eventType</code>
Device Vendor	<code>'IAM'</code>
Device Version	<code>Version</code>
Event Outcome	<code>Outcome/result</code>
External ID	<code>uuid</code>
File ID	<code>One of (source_folder_id, source_item_id)</code>
File Name	<code>One of (source_item_name, source_folder_name)</code>
File Type	<code>One of (source_item_type, one of (source_folder_id, 'folder'))</code>
Flex String 2	<code>authenticationContext/authenticationProvider</code>
Flex String 2 Label	<code>'Authentication Provider'</code>

ArcSight ESM Field	Device-Specific Field
Name	<code>__ifThenElse(displayMessage,"null",__concatenate(eventType," ",outcome_result),__concatenate(displayMessage," ",__toLowerCase(outcome_result)))</code>
Reason	Outcome/reason
Request Client Application	client/userAgent/rawUserAgent
Request Url	debugContext/debugData/url
Source Address	Client/ipAddress

Troubleshooting

API Token Authentication Error

API tokens are valid for 30 days and automatically renew every time they are used with an API request.

When the API Token has been inactive for more than 30 days, it is revoked and cannot be used again. To get the new API Token, refer to the [Create Okta API tokens](#) section from Okta Documentation help.

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 Okta 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!