Micro Focus Security ArcSight SmartConnectors

Software Version: 8.3.0

SmartConnector for Okta 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

Configuration Guide for SmartConnector for Okta 5
Overview 5
Prerequisites 5
Configuration 6
Creating an OIDC Application when Grant Type is Password 6
Creating an OIDC Application when Grant Type is Authorization Code 7
Assigning a User to the Native or Web Application 8
Enabling the okta.logs.read Scope 8
Configuring the Appliance or ArcSight Management Center 8
Installing the SmartConnector 10
Preparing to Install Connector 10
Installing and Configuring the SmartConnector by Using the Wizard 10
Upgrading the Okta Connector from Connector Appliance or ArcMC 13
Device Event Mapping to ArcSight Fields 15
Okta Mappings to ArcSight Fields - JSON Parser 15
Troubleshooting 17
Refresh Token Authentication Error 17

Send Documentation Feedback 18

Configuration Guide for SmartConnector for Okta

The Configuration Guide for Arcsight SmartConnector provides information to install the SmartConnector for Okta and to configure 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 to log in to Okta organization with the administrator level privileges (at least "Read Only Administrator" permission) so that the account is authenticated to generate refresh token and access token.
- The application requires `logs.read permission/scope`.
- Ensure that the platform on which you want to install the connector must support UI options. The installation does not support Command Line Interface (CLI) platforms when the grant type is selected as **Authorization Code**.

Configuration

Creating an OIDC Application when Grant Type is Password

Perform the following steps to create an OIDC Application when Grant Type is Password:

1. Log in to your Okta account as a user with the administrator privileges.
2. In the Admin Console, go to **Applications** > **Applications**.
3. Click **Create App Integration**.
4. Select **OIDC - OpenID Connect** as the **Sign-in Method**.
5. Select **Native Application** as the **Application Type**, then click **Next**.
   The **New Native App Integration** page appears.
6. In **General Settings**, in the **App integration name** field, specify the appropriate name of your native application.
7. For **Grant type**, select the following check boxes available under **Client acting on behalf of a user**:
   - Refresh Token
   - Resource Owner Password
8. The **Sign-in redirect URIs** and **Sign-out redirect URIs(Optional)** parameters can be skipped or left as default.
9. In **Assignments**, select **Skip group assignment for now** as the **Controlled access**.
10. Click **Save**.

    It displays the message "Application created successfully". The created app appears in the **Applications** page.
11. On the native application page you created, in the **Client Credentials** section, click **Edit** and select **Use Client Authentication** for **Client authentication**, then click **Save**.
    The **Client secret** id is available.

    > **Important**: Ensure that **Refresh token behavior** is selected as **Use persistent token** and **User Consent** is selected as **Require consent**.
12. Copy the **Client ID** and **Client secret** to use them during the Okta connector installation.

For more information about creating a native application that uses **Password** based Grant Type, refer to the Set up your app section from Okta Documentation help .

Note: Multi Factor Authentication (MFA) must be disabled before you select the Grant Type as **Password**.

Creating an OIDC Application when Grant Type is Authorization Code

Perform the following steps to create an OpenID Connect (OIDC) application you want to integrate with Okta:

1. Log in to your Okta account as a user with the administrator privileges.
2. In the Admin Console, go to **Applications** > **Applications**.
3. Click **Create App Integration**.
4. Select **OIDC - OpenID Connect** as the **Sign-in Method**.
5. Select **Web Application** as the **Application Type**, then click **Next**.
   The **New Web App Integration** page appears.
6. In **General Settings**, in the **App integration name** field, specify the appropriate name of your web application.
7. For **Grant type**, select the following check boxes available under **Client acting on behalf of a user**:
   - Authorization Code (This check box is selected by default.)
   - Refresh Token
   - Implicit (Hybrid)
8. In **Sign-in redirect URIs**, you can keep the following default URI as is, or modify it if required:

   `http://localhost:8080/authorization-code/callback`.

   Note: The **Sign-in redirect URI** is the input for the Redirect URI parameter during the connector installation.
9. The **Sign-out redirect URIs(Optional)** and **Base URIs(Optional)** parameters can be skipped or left as default.
10. In **Assignments**, select **Skip group assignment for now** as the **Controlled access**.
11. Click **Save**.

    It displays the message "Application created successfully". The created app appears in the **Applications** page.
    For information about creating new web app integrations, see Create an OIDC app integration using AIW from Okta documentation.

Assigning a User to the Native or Web Application

Perform the following steps to assign an administrator user (with the Read Only Administrator" permission) to the created native application or web application:

1. Open the native application or web application you created.
2. Click the **Assignments** tab.
3. Click **Assign** > **Assign to People**. The "Assign <application name> to People" window appears.
4. Search for the administrator user you want to assign the application to and click **Assign**. The "Assign <application name> to People" window appears with the selected user details.
5. Click **Save and Go Back**. The selected user is assigned to your application.
6. Click **Done**.

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**.

Configuring the Appliance or ArcSight Management Center

You must obtain a refresh token to configure the SmartConnector for Okta on the Connector Appliance or ArcSight Management Center (ArcMC). A refresh token enables the connector to access Okta log data. You must use the REST FlexConnector Configuration Support Tool (RESTUtil) to retrieve a refresh token.

The `restutil` script lets you obtain the dynamic portion of an events URL. Some configuration values of the REST Flex Connector can include a dynamic portion that can be retrieved after running HTTP calls. For example, the Google Apps events URL has the customer id in the path and it can be retrieved via an authorized HTTP GET using the token obtained after the authentication is completed.

Use `restutil` to retrieve the dynamic portion of the events URL after installing core software and before beginning the connector configuration.

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 oktatoken -proxy <-proxy_details> -config <-
   configuration_file_location>
   ```

   For example: `arcsight restutil oktatoken -proxy proxy.location.microfocus.com:8080 -config C:\okta.properties`

   A web browser launches and prompts you to log in to Okta.
4. Enter your username 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.

Installing the SmartConnector

Preparing to Install Connector

Before you install any SmartConnectors, make sure that the Micro Focus 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:

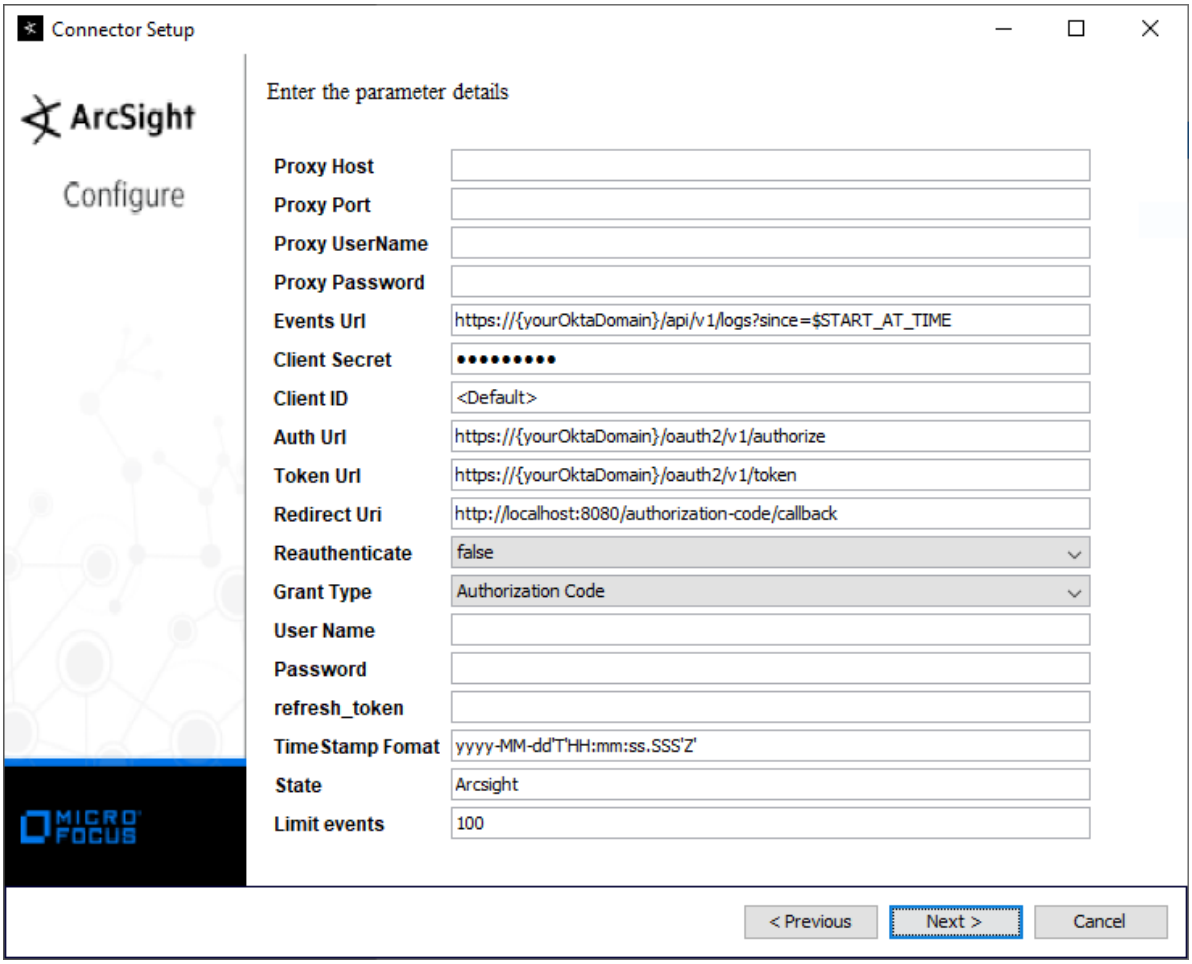
- Local access to the machine where you want to install the SmartConnector.
- Credentials to log in to Okta.

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** as the type of connector, then click **Next**.
5. Enter the following SmartConnector parameter values, then click **Next**:



Parameter	Description
Proxy Host	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	If proxy is enabled for your machine, the port number of the proxy server required for proxy configuration.
Proxy User Name	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	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.
Client Secret	The client secret key generated for your app in the registration portal. This value is also provided by the vendor when you register an application. This value is obfuscated. The values **client_id** and **client_secret** help the vendor to identify an application.

Parameter	Description
Client ID	The client ID generated for your app in the registration portal. This value is provided by the vendor when you register an application.
Auth Url	The URL of the vendor to which the initial request must be made to get an authorization code. For more information, see Okta Documentation help. Leave as default when the Grant type is **Password**. This field is mandatory if the Grant Type is selected as **Authorization Code**. In `https://{yourOktaDomain}/oauth2/v1/authorize`, you must replace {yourOktaDomain} with your appropriate Okta domain. Example: `https://dev-654/oauth2/v1/authorize`
Token Url	The URL of the vendor to which the request for an Access Token will be made. For more information, see Okta Documentation help.
Redirect Uri	You configure this parameter when you register an application. This is the URL to which the vendor sends the authorization code. Leave as default when the Grant type is **Password**. The parameter is mandatory if the Grant Type is selected as **Authorization Code**.
Scope	(Optional) A value for the scope parameter. However, 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 them as a space-separated list of values.
Reauthenticate	If this is set to **True**, then a user is required to authenticate when connector starts.
Grant Type	If selected as **Authorization Code**, then it uses the Auth code flow for authorization. If selected as **Password**, then it uses the Resource Owner Password flow for authorization. For more information, refer to Implement authorization by grant from Okta Documentation help.
User Name	Enter the administrator user name assigned to the respective Okta native application. This field is mandatory if the Grant Type is selected as **Password**.
Password	Enter the administrator password assigned to the respective Okta native application. This field is mandatory if the Grant Type is selected as **Password**.
refresh_token	Enter the refresh token; This is applicable only to users running the SmartConnector in the Connector Appliance/ArcSight Management Center (ArcMC) environment. For more information, see the ArcSight Connector Appliance/ArcSight Management Center Administrator's Guide and "Connector Appliance/ArcSight Management Center Considerations". Other users, leave this field blank.
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 to the client.
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.

For instructions about upgrading the connector or modifying parameters, see SmartConnector Installation and User Guide.

Upgrading the Okta Connector from Connector Appliance or 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 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 **Refresh Token**. To obtain a refresh token, see "Configuring the Appliance or ArcSight Management Center" on page 8. Click **Next**.
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.

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	__safeToDate(published,"yyyy-MM-dd'T'HH:mm:ss.SSSX")
Device Product	‘OKTA'
Device Severity	severity
Device Action	__regexToken(eventType,"(?:[a-z]+\\.)+(.*)")
Device Custom String 2	transaction/type
Device Custom String 2 Label	‘Transaction Type’
Device Custom String 3	__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 Event Category	eventType
Device Event Class ID	eventType
Device Vendor	'IAM'
Device Version	Version
Event Outcome	Outcome/result
External ID	uuid
File ID	One of (source_folder_id, source_item_id)
File Name	One of (source_item_name, source_folder_name)

ArcSight ESM Field	Device-Specific Field
File Type	One of (source_item_type, one of (source_folder_id, 'folder')
Flex String 2	authenticationContext/authenticationProvider
Flex String 2 Label	‘Authentication Provider’
Name	__ifThenElse(displayMessage,"null",__concatenate (eventType," ",outcome_result),__concatenate (displayMessage," ",__toLowerCase(outcome_result)))
Reason	Outcome/reason
Request Client Application	client/userAgent/rawUserAgent
Request Url	debugContext/debugData/url
Source Address	Client/ipAddress

Troubleshooting

Refresh Token Authentication Error

If you cannot refresh the access token, then reconfigure the connector and re-authenticate the user.

To refresh the access token:

1. While setting up the connector, set the `agents[0].reauthenticate_onstartup` parameter to **True** in the `user/agent/agent.properties` file to force a new authentication.
2. Stop the connector, and change the parameter to **False**.
3. Restart the connector after you get the refresh token.

   Note that the refresh token takes from 2 to 3 minutes to be generated.

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 SmartConnector for Okta 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!