Identity Reporting

This guide describes basic usage of ForgeRock Identity Reporting, including overviews and instructions for management and generation of reports and other administrative tasks occurring within the Reporting Dashboard.

This guide is written for ForgeRock Identity Reporting administrators performing actions as part of the reporting process.

Installation

Install ForgeRock Identity Reporting.

Reporting Interface

Learn about the ForgeRock Identity Reporting interface.

Data Sources

Learn about the ForgeRock Identity Reporting data sources.

Report Definitions

Learn about the ForgeRock Identity Reporting report definitions.

Report Schedules

Learn about the ForgeRock Identity Reporting report schedules.

Report Configuration

Learn about the ForgeRock Identity Reporting report configuration.

GDPR

Learn about the ForgeRock Identity Reporting GDPR compliance.

Installation

The following chapter provides details about the Identity Reporting installation.

Provided files

The installer is provided in the `identity-reporting-7.1.0.zip` archive on the ForgeRock BackStage Downloads site. The top-level directory contains the following files and directories:

- **install.sh**. Linux installer.
- **install.bat**: Windows installer.
- **install.groovy**: Common installer, invoked by both Linux and Windows installers.
- **install.properties**: Properties file used in place of interactive input with the installers.
- **openidm**: Files to be installed in the IDM home directory. These files include configuration files, scripts, workflows, user interface configuration and file fragments injected into existing files.
- **legal-notices**: Legal notes and third party license information.

Installation instructions

1. Unzip the `identity-reporting-7.1.0.zip` to a temporary directory then navigate to the directory that was unzipped.
2. Run the following command to initiate the installer:

```
For Windows:
install.bat [--properties filename | -p filename]
```

```
For Linux:
./install.sh [--properties filename | -p filename]
```

The command can be run with the following optional argument:

- **`-properties or –p <location/of/properties/file>`**. Provides a properties file for script input. If no properties file is specified, the user must input the following properties at run time.

The following input is used for the installer:

- **openidm_location**: File location of IDM home directory.
- **project_location**: File location of IDM project directory.
- **installer_location**: File location of unzipped installer.

> NOTE
>
> Names are those found in the properties file. If a properties file is not used, equivalent input is gathered directly from the installer.

The installer prints updates to the console until it successfully completes.

Clustered environment

Currently, the installer script can only be run once per environment. In a clustered environment, manual steps need to be completed to copy artifacts to subsequent nodes once the installer has been run on the first node. The following needs to be replicated on each node after the first:

1. Copy the following files from the installer zip into the IDM installation directory:
    a. Everything in the `/IDR/openidm/script` directory, copied into the `script` directory of the installation.
    b. Everything in the `/IDR/openidm/conf` directory, copied into the `conf` directory of the installation.
    c. All jar files under `/IDR/openidm/bundle` directory, copied into the `bundle` directory of the installation.
    d. All jar files under the `/IDR/openidm/bundle/X.x/` directory corresponding to the version of IDM, copied to the bundle directory of the installation
    e. The entire `/IDR/openidm/reporting` directory, copied into the IDM installation directory.
2. Copy the following files from the first node’s IDM installation directory:

    - `openidm/script/access.js`

Post-installation instructions

After installation steps are complete, it is recommended that the installer ZIP and the created installation folders and files be removed from the server.

IDM/AM Integration for 7.x

If installing ForgeRock Identity Reporting into an IDM environment configured to authenticate through ForgeRock Access Management (AM), you must configure an OAuth client in AM for the reporting context.

NOTE

AM and IDM must be on version 7.x or higher.

To start, refer to the Configure OAuth clients section of the ForgeRock Identity Platform.

In step 5 of the section, instructions are given to configure a client for the end-user UI. For Identity Reporting, please repeat those steps with the following adjustments:

- **Client ID**. `identity-reporting-ui`
- **Core**. Redirect URIs: `[IDM domain]/reporting/appAuthHelperRedirect.html`
- **Advanced**. Subject Type: `Public`

Reporting interface

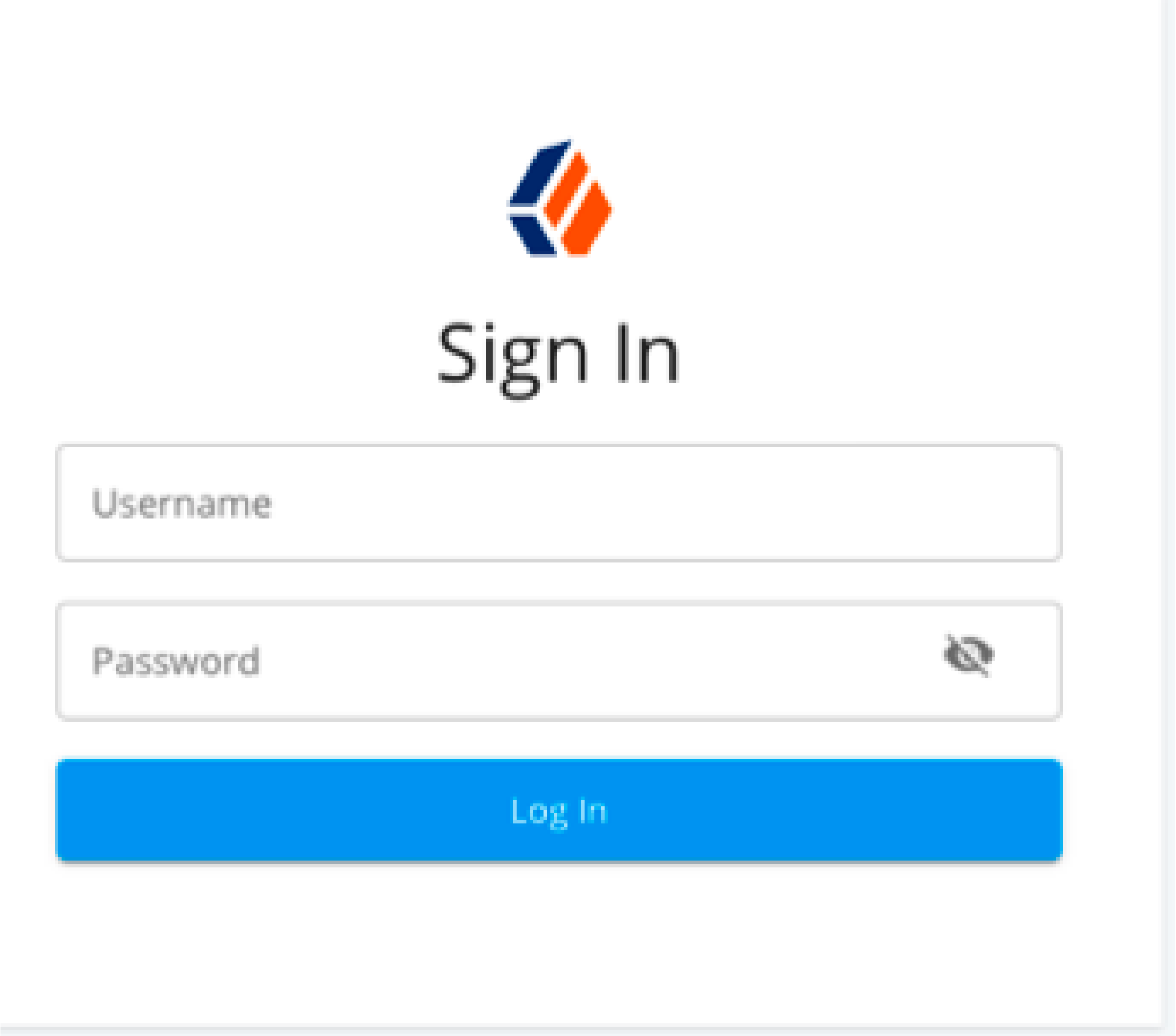
The ForgeRock Identity Reporting interface consists of the sections listed below. The **Report Definitions** tab is available to any ForgeRock Identity Management authorized end user. The other three sections are available to users with the `reporting administrator` role.

1. **Report Definitions**
2. **Report Schedules**
3. **Data Sources**
4. **Configuration**

Logging on to the reporting interface

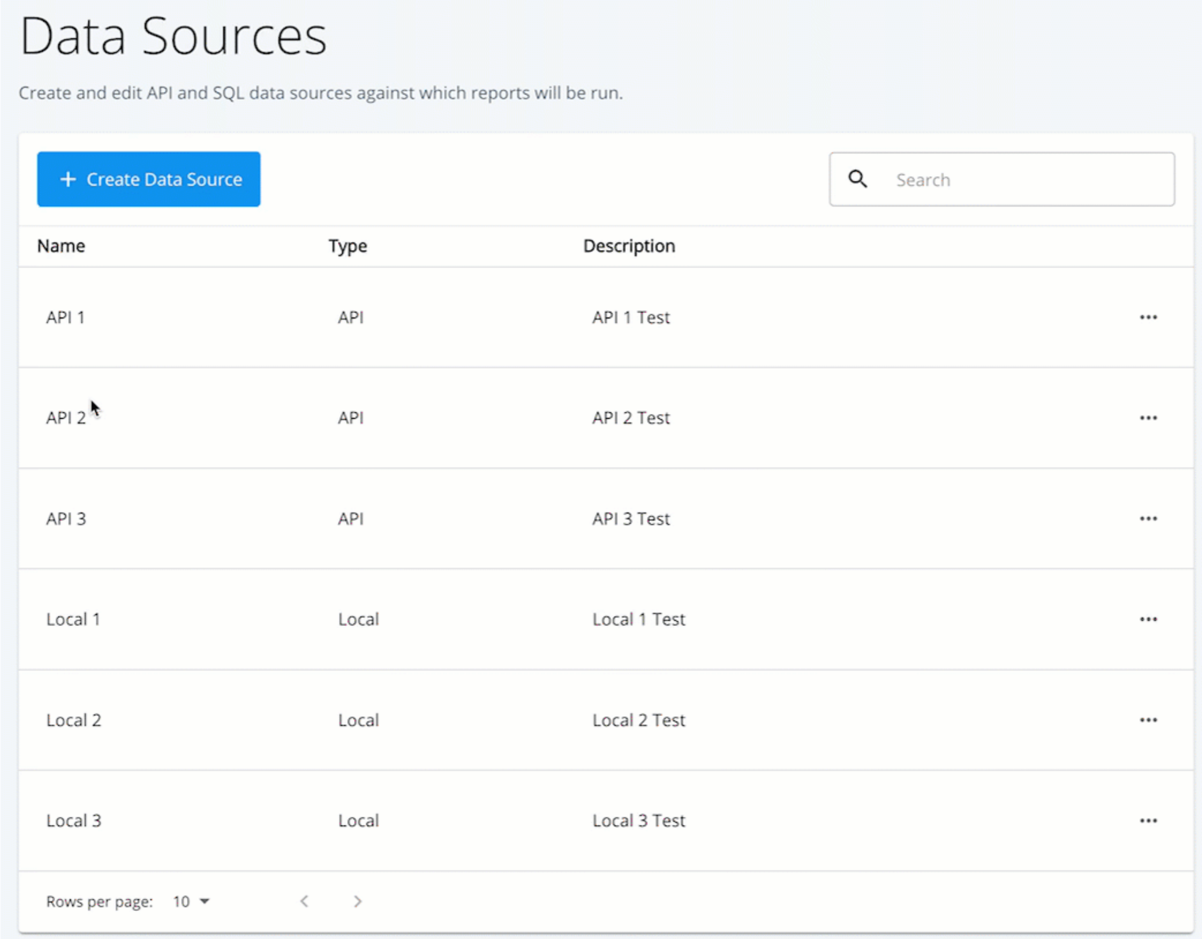
Log in to reporting interface directly as an administrator by navigating to the default URL context: http://<HOSTNAME>:<PORT>/reporting (The host and port reference IDM's URL).

If the user does not currently have an active IDM session, they are prompted to log in.



Tables

Throughout the reporting dashboard, information is often displayed in tables with a common set of properties, including the following options:



Data Sources

Create and edit API and SQL data sources against which reports will be run.

Name	Type	Description	
API 1	API	API 1 Test	···
API 2	API	API 2 Test	···
API 3	API	API 3 Test	···
Local 1	Local	Local 1 Test	···
Local 2	Local	Local 2 Test	···
Local 3	Local	Local 3 Test	···

- **Searching**: Allows the administrator to search through results in the list. The filter details all rows where matching values exist and updates results as the value is entered.
- **Sorting**: Selecting a column header sorts information in a table by that column value. This feature is only available when viewing report output tables.

  > NOTE
  >
  > Selecting multiple times adjusts the order from descending to ascending for the field selected.

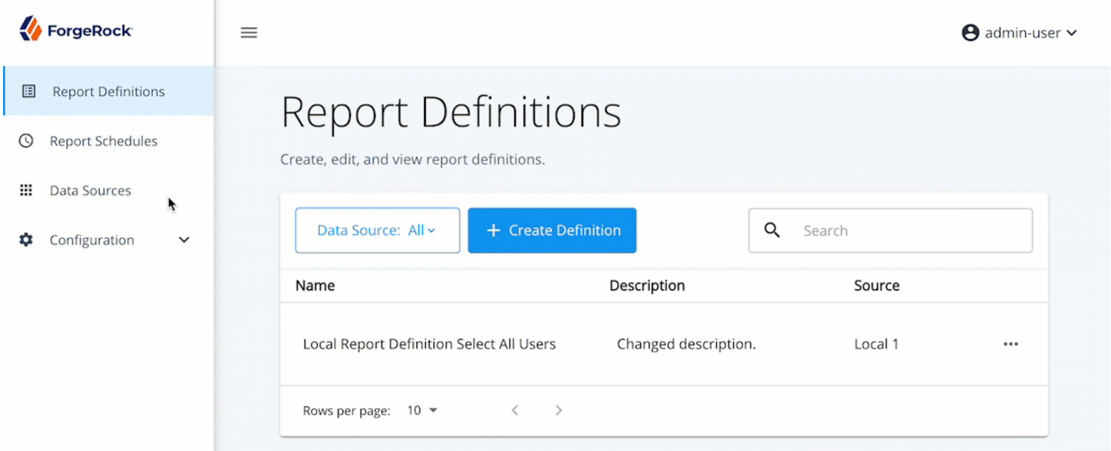
- **Limiting results per page**: (Items per page) Identifies a number of results made visible at a specific time within the table. Values can include `5`, `10`, `25`, or `50`.
- **Navigating results**: Allows navigation within the table when results exceed the number specified in the field Items per page.

Data sources

Data sources are used to specify where the source of information retrieved by report definitions and also include the necessary connection details for that source. ForgeRock Identity Reporting supports database and Application Programming Interface (API) data source types.

Creating new data sources

1. Navigate to the **Data Sources** tab of the main dashboard.
2. Click **Create Data Source**.

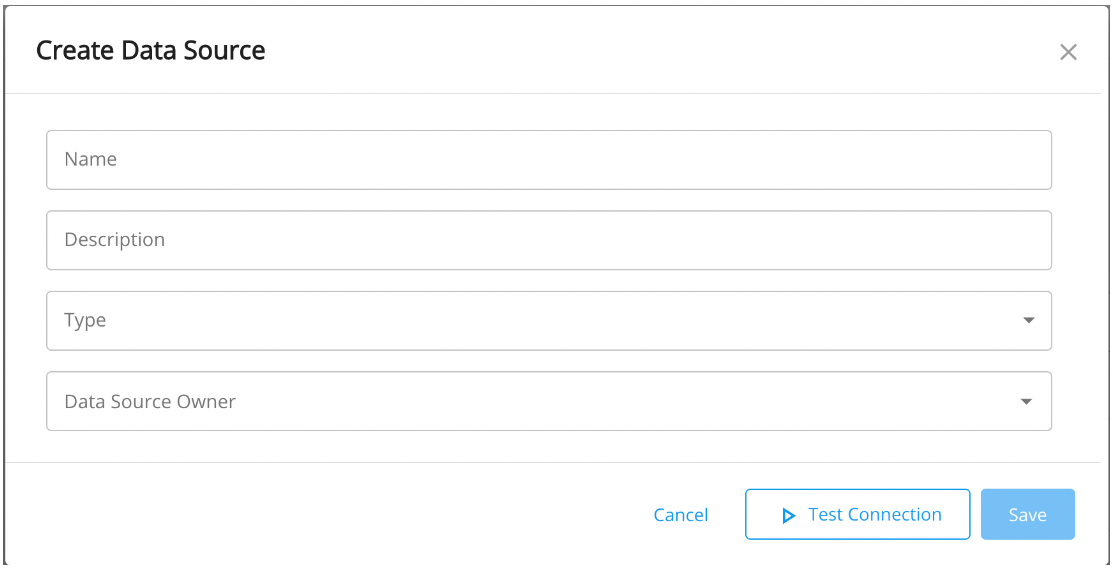


Report Definitions

Create, edit, and view report definitions.

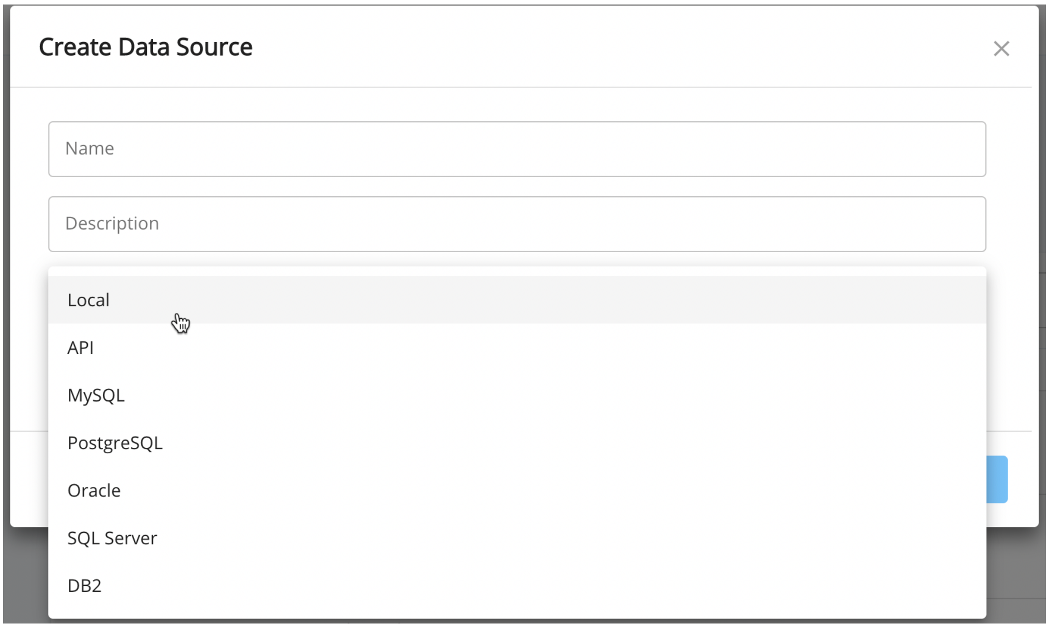
Name	Description	Source
Local Report Definition Select All Users	Changed description.	Local 1

3. On the Create Data Sources page, fill in each of the required fields.


Create Data Source

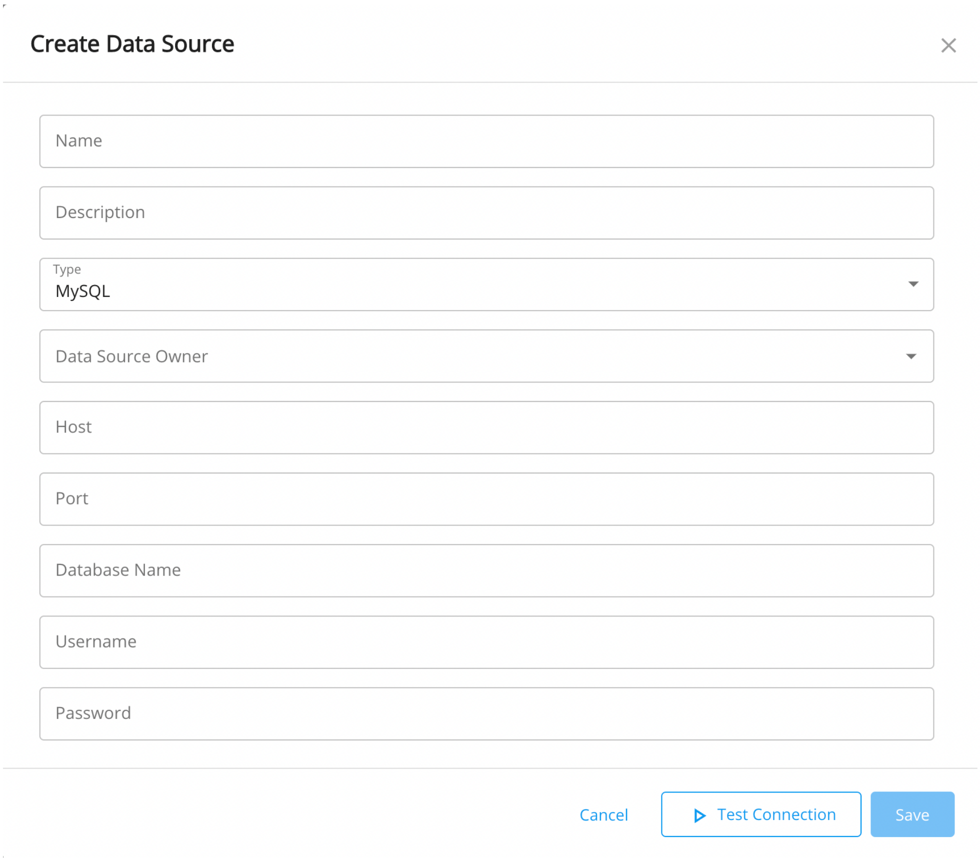
Additional details on the available fields are given below:

- **Name**. (Required) Name of the data source that appears in the table and in the list of available data sources on Report Definition forms.
- **Description**. Provides additional information about the data source and the connection being made.
- **Type**. (Required) Specifies the type of data source, which determines the available connection parameters.



Options are:

- **Local**. The default data source type that uses IDM's local database repository. If Local is selected, no additional parameters are required as the connection details are pulled directly from IDM.
- **MySQL, PostgreSQL, Oracle, SQL Server, DB2**. Data sources that use database-specific jdbc drivers to connect to a remote database.

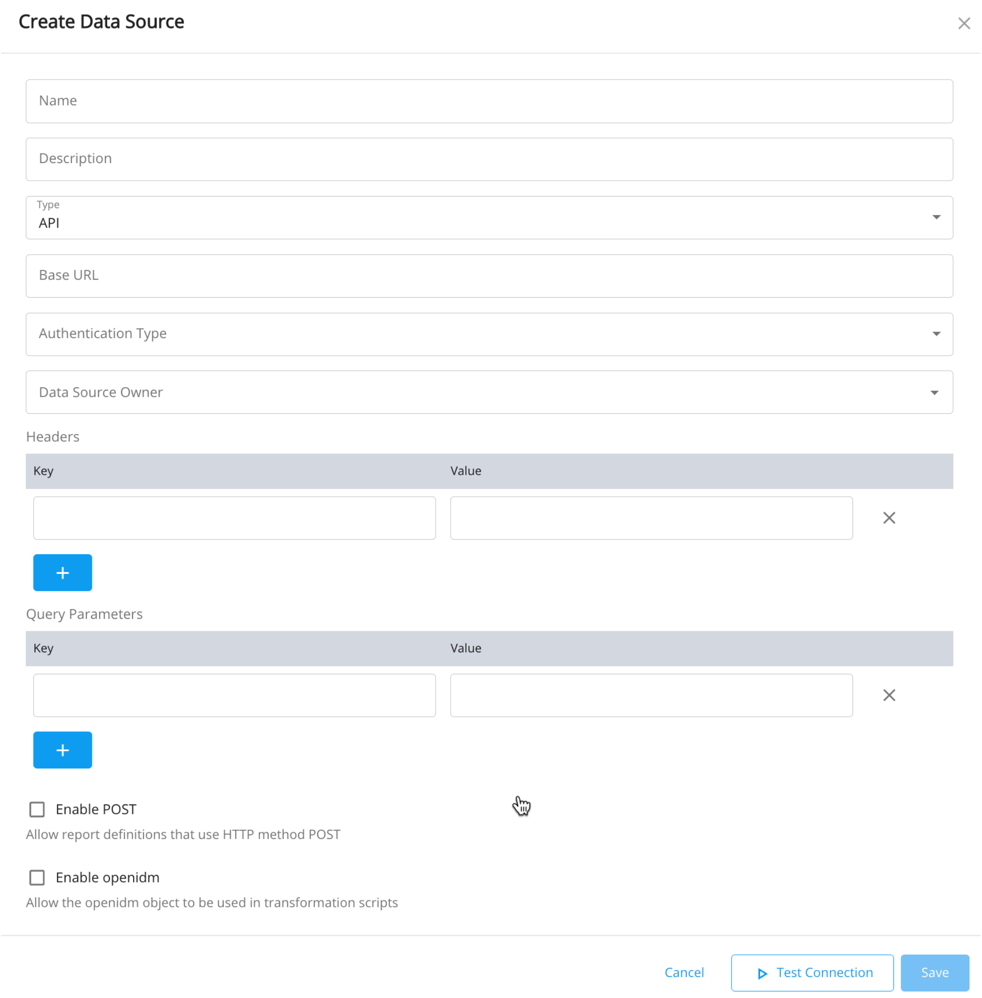


Type: MySQL

When one of these types is selected, the following parameters become available for user input on the form:

- **Host**. (Required) The IP or hostname of the server where the remote database is hosted.
- **Port**. (Required) The port on which the remote database is listening on for incoming connections.
- **Database name**. (Required) The name of the database instance that is being connected with.
- **Username**. (Required) The username of the account with which the connection is being made. It is **highly** recommended to use a service account with **read-only** access.
- **Password**. (Required) The password of the account with which the connection is being made.

- **API**. This data source connects to an available API service, which must be reachable by the IDM deployment on which IDR is installed. Queries can be executed against the specified API to retrieve the desired data.



Create Data Source

Type: API

□ Enable POST

Allow report definitions that use HTTP method POST

□ Enable openidm

Allow the openidm object to be used in transformation scripts

When the API data source type is selected, the following parameters become available for user input on the form:

- **Base URL**. The root path of the API service that the data source connects to. Any report definitions created for this data source extends this path for the desired call.

- **Authentication Type**. There are three API data source authentication types supported by IDR:
    - **None**. No specific authentication method is required in the hyper text transfer protocol (HTTP) call to the service. This applies to unauthentication services as well as those that are header-based, for exaxmple, API keys, as those methods can be handled using the headers information (described below).
    - **Basic**. Basic username and password credentials, **base64 encoded**, and sent as an *Authentication* header.
        - **Authentication Username**. The username to authenticate with.
        - **Authentication Password**. The password to authenticate with.
    - **Bearer**. Authentication through a bearer token, which is retrieved through a separate endpoint call, and is included with each API call that is executed.
        - **Authentication URL**. The full path to the authentication endpoint that must be called to retrieve the bearer token.
        - **Authentication Body**. The full payload that must be sent to the authentication endpoint to retrieve the bearer token.

TIP

When the **Authentication Type** is set to `Bearer`, the field must contain a payload to authenticate in JSON format as follows:

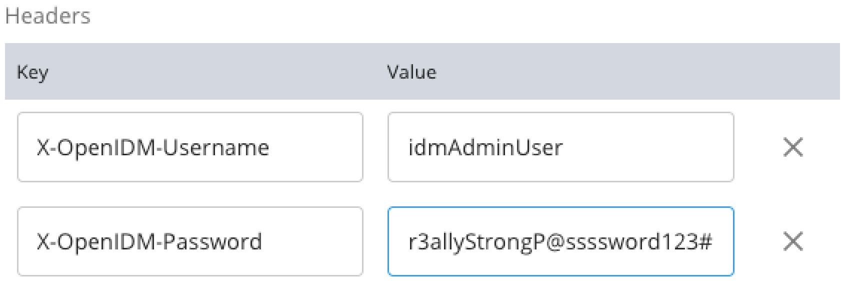
```
{
   "username": "john.doe@forgerock.com",
   "password": "Welcome123"
}
```

- **Headers**. A list of key/value pairs sent as headers with each representation state transfer (REST) call. These headers are included, by default, in every report definition that uses this data source. It can be used for alternate authentication methods, or to define globally used headers in a single place, as opposed to defining headers on every report definition.

TIP

TIP

For example, if you are connecting to IDM from IDR, use the native IDM headers to authenticate.



Headers

Key	Value
X-OpenIDM-Username	idmAdminUser
X-OpenIDM-Password	r3allyStrongP@ssssword123#

- **Query Parameters**. A list of key/value pairs sent as query parameters with each REST call. By default, these parameters are included in every report definition that uses this data source. It can be used to define globally used parameters in a single place, as opposed to defining headers on every report definition.
- **Enable POST**. When selected, report definitions for this data source are allowed to be created with the HTTP method POST. If disabled, only the HTTP method GET will be allowed.
- **Enable openidm**. The IDR report definitions use a transformation script to take the results of an API call and transforms them into a payload that IDR expects. Since these transformation scripts run within the IDM script engine, the `openidm` object can be made available to the report definition. This allows for complex transformations and enrichment of the report data to take place. When this is not selected, transformation scripts that reference the `openidm` object are not accepted and its use is disabled. It is recommended that his option be turned **off** and exposed only in data sources that are available with the proper **authorization** to use it.

4. Once all the necessary fields have been filled in, click `Save` to finish creating the data source.

NOTE

At any point during or after this process, use “Test Connection” and a connection is made using any supplied information on the form. It is recommended to test the connection after completing the form prior to before saving the details.
For API data sources, a field marked *API Endpoint Test Connection* is available in order to provide a complete test endpoint (appended to the Base URL) that IDR can attempt to call to. This field will not persist on the data source.

Modifying data sources

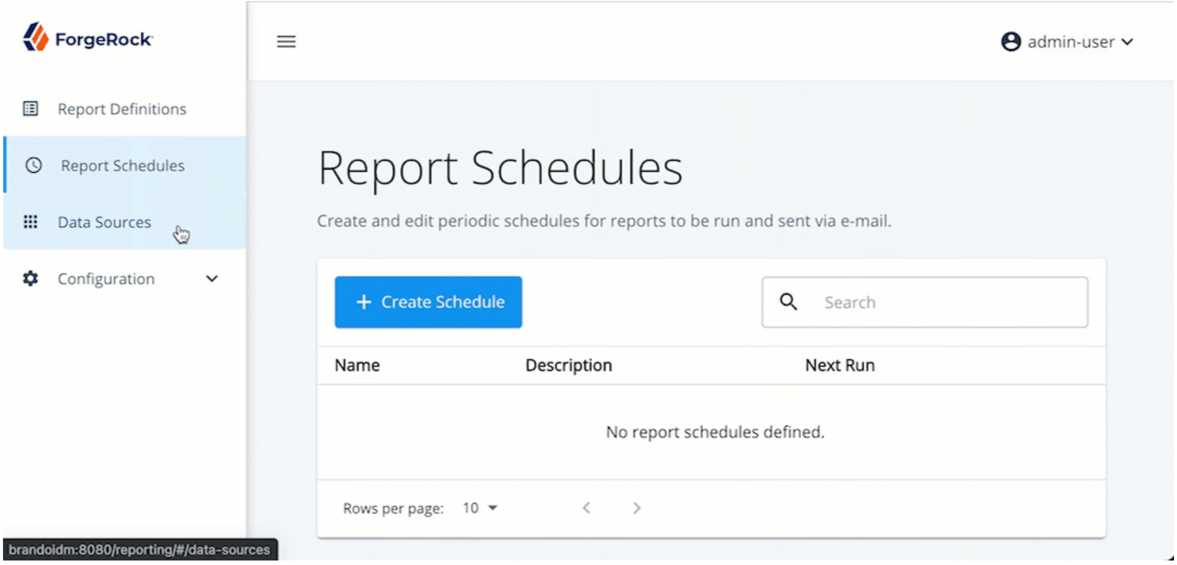
1. Navigate to the **Data Sources** tab of the main dashboard.
2. In the table, select the data source to be modified.
3. Update the fields as necessary. You are unable to edit a Data Source’s type.
4. Click **Save** to complete the update.

> NOTE
>
> A created data source cannot modify its type once it is created. A new data source must be created to do this.

Deleting data sources

Delete individual data sources:

1. Navigate to the **Data Sources** tab of the main dashboard.
2. In the table, click the ellipses to the right of the data source you wish to delete.
3. Click **Delete**.
4. Select **Delete Data Source** to confirm the deletion.



Report Schedules

Create and edit periodic schedules for reports to be run and sent via e-mail.

Name	Description	Next Run

No report schedules defined.

NOTE

NOTE

A data source that currently has existing report definitions cannot be deleted. The administrator of the data source owner must first **delete all existing report definitions** for the specified data source, before the data source itself can be deleted.

Report definitions

Report Definitions contain the specific details of the report to be generated, including any parameters needed and which data source to run the report against. The Report Definitions tab of the dashboard is used for managing these definitions, as well as generating on-demand reports. There must be at least one data source before a report definition can be created.

Report definition authorization

There are three levels of authorization for the report definitions tab:

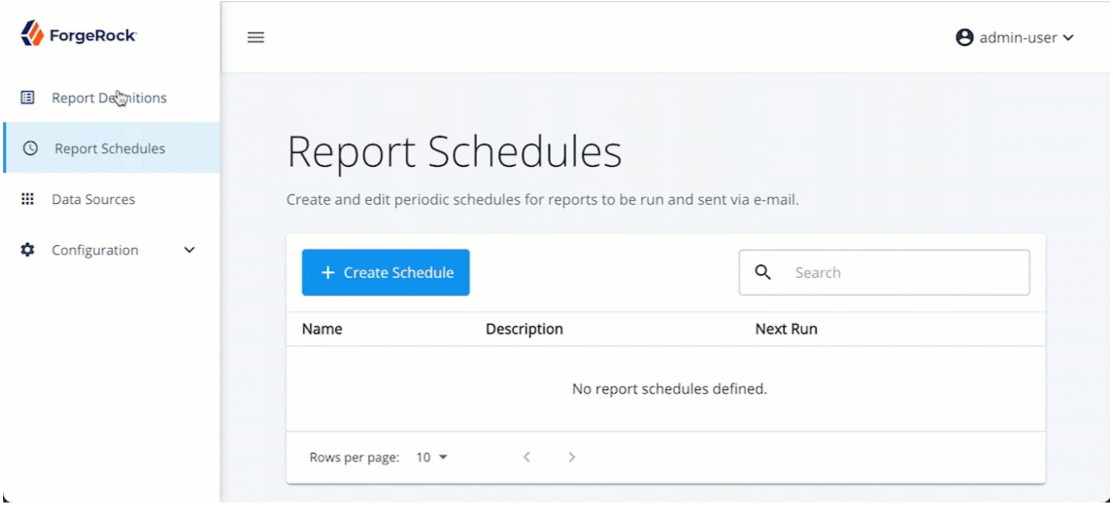
1. **Reporting Administrator**. Users with the *reporting_administrator* internal authorization role have full access to the report definitions tab, and all the definitions within the system. They can create, run, update, or delete any report for any data source.
2. **Data Source Owner**. Users that have an authorization role granted that is also defined on the data source as the owner of that data source have the same create, run, update, or delete privileges as the reporting administrator *only* for the data sources which **they own**. These users will not be able to see report definitions for other data sources, nor are they able to create a new definition for a source they do not own.
3. **Report Viewer**. Users that have an authorization role granted that is also defined on a report definition as the viewer of that data source have the ability to run or view the generated reports for which they are assigned *Viewer*. These users are able to run report definitions for other sources, have no create, update, delete privileges, nor are they able to view the contents of the report definition object itself. The only privilege they have is to view the report contents.

IMPORTANT

Any IDM user with the *openidm-authorized* authorization role has access to the reporting interface and definitions tab. No data will be available to them if they are not granted an authorization role **explicitly** defined on the IDR object.

Creating new report definitions

1. Navigate to the **Report Definitions** tab of the main dashboard.
2. Select **Create Definition**.



Report Schedules

Create and edit periodic schedules for reports to be run and sent via e-mail.

Name	Description	Next Run

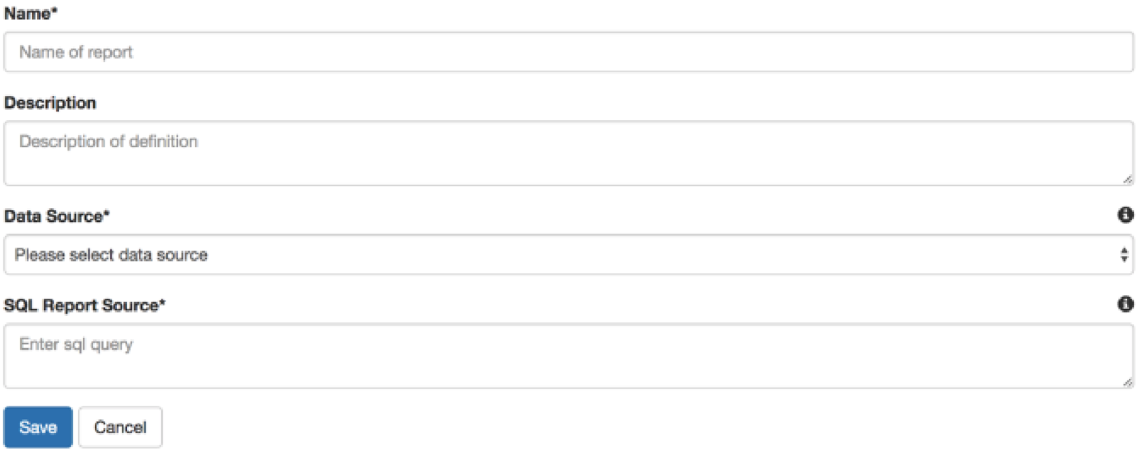
No report schedules defined.

3. On the Create Report Definitions page, fill in each of the required fields. Additional details on the available fields are given below:

- **Name**. (Required) Name of the report definition that appears in the table and in the list of available report definitions on Report Schedule forms.
- **Description**. Provides additional information about the report definition and its purpose.
- **Data Source**. (Required) Name of the data source to run the report against. After a data source has been successfully created, it displays in this list for selection.
- **Report Viewer**. The IDM authorization role that grants a user the ability to run/view the contents of the generated report, including the ability to provide any run time parameters that the report requires. No other privileges are granted from this field. For more information on the report viewer, see Report Definition Authorization.

For reports where SQL is selected under *Data Source*:

- **SQL Report Source**. (Required) SQL Query used to generate the report data. Multiple parameter values can be included by enclosing the parameter names in square brackets; for example *[role_name]*, within the query. Any parameters that are designated in such a way are replaced by user-specified values at the time the report is generated or at the time a schedule is created using this report definition.



Name*

Name of report

Description

Description of definition

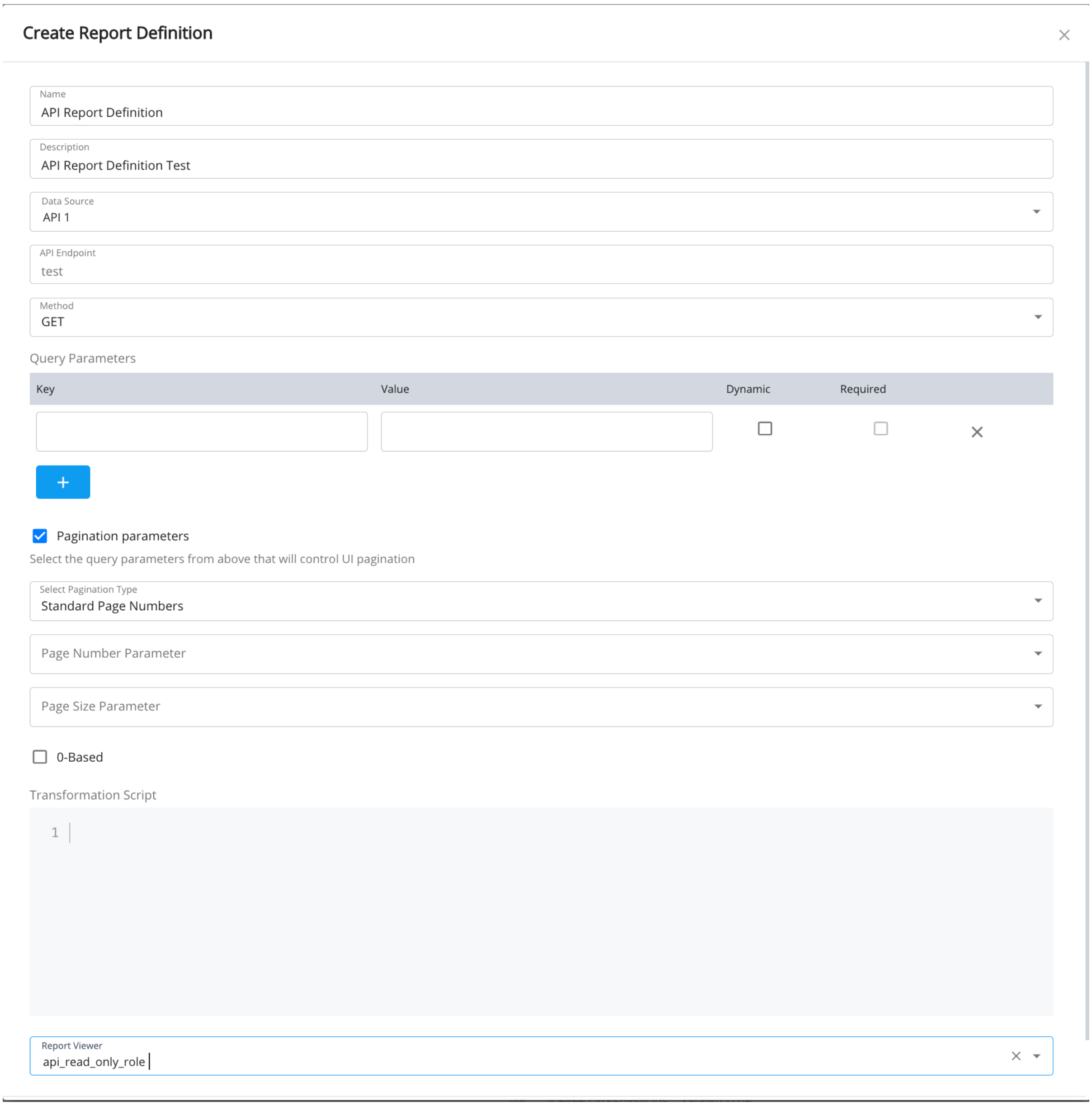
Data Source*

Please select data source

SQL Report Source*

Enter sql query

For reports where API is selected under *Data Source*:



Create Report Definition

Name: API Report Definition

Description: API Report Definition Test

Data Source: API 1

API Endpoint: test

Method: GET

Query Parameters

Key	Value	Dynamic	Required	
		□	□	×

☑ Pagination parameters

Select the query parameters from above that will control UI pagination

Select Pagination Type: Standard Page Numbers

Page Number Parameter

Page Size Parameter

□ 0-Based

Transformation Script

```
1
```

Report Viewer: api_read_only_role

- **API Endpoint**. The specific API endpoint that is called by this report. This value is appended to the **Base URL** defined in the report's data source (which is visible within the form field).

- **Method**. HTTP method of API call, either GET or POST. For data sources that disable POST calls, GET is the only option available.
- **Query Parameters**. Key/value pairs that are used as query parameters when making the API call. Each pair has the ability to be listed as dynamic, meaning the entire value of the key/value pair can be user provided at the report run time. If marked as dynamic, the key/value pair can alse be marked as required, which means that the value *must* be provided in order to generate the report.
- **Pagination Parameters**. For report viewing within the IDR interface, this option allows you to define which specific query parameters among the ones defined in the *Query Parameters* section are used to control pagination. When enabled, the user running the report is not prompted to enter those parameters in the user interface, but instead be inferred upon based on the user interface controls for the page number and page size.

  NOTE

  The options selected here only apply to the out-of-the-box (OOTB) ForgeRock Identity Reporting interface, and does not affect direct API calls or downloaded PDF/CSV reports.

  - **Select Pagination Type**. The type of pagination that the endpoint uses. IDR currently supports page number or page offset pagination types.
  - **Page Size Parameter**. The query parameter that controls the results returned per page.
  - **Page Offset Parameter**. The query parameter that controls the offset value used (when page offset pagination type is selected).
  - **Page Number Parameter**. The query parameter that controls the page number of results to return (when page number pagination type is selected).
  - **0-based**. Page number parameter 0-based. Select **True** if the first page number is 0 as opposed to 1 (when page number pagination type is selected).
- **Request Body**. For definitions with the method POST, a request body must be defined to be sent with the request. The field is used to define the request body content.

  TIP

  For example, the request body could contain the below content:

  ```
  {
    "ownerId": "{{ownerId}}"
  }
  ```

- **Transformation Script**. The transformation script is the snipped of code that takes the results retrieved from the API call defined, and converts the results into the expected data format that IDR can consume. For more information, see Transformation Scripts.

4. Once all the necessary fields have been filled in, click **Save** to finish creating the report definition.

Transformation scripts

Use the transformation script to convert the API report definition’s API call results into the expected IDR report format. IDR uses JavaScript for the scripts.

The script has reference to the following variables:

> - ***response***. The response contents.
> - ***type***. The type of report being generated, either *html*, *csv*, or *pdf*.
> - ***parameterValues***. The dynamic values provided by the call to generate the report, if any.

The script has the ability to execute the necessary logic to manipulate the returned data. However, on completion of the script, it **must** return an object that contains the following two properties (at a minimum) in the expected format"

> - ***columns***. An array of column name strings.
> - ***data***. An array of objects, each of which contains the key/value pairs for the columns defined above.

TIP

TIP

An example transformation script of attributes from IDM, for example, could be the following:

```
 var result = {
   data: [],
   columns: ["Requestee", "Requester", "Items", "Start Date" ]
}

response.result.forEach( function(entry) {
   var row = {};
   row["Requestee"] = entry.requestee.displayName
   row["Requester"] = entry.requester.displayName
   row["Start Date"] = entry.startDate
   row["Items"] = _.map(entry.items, 'displayName').join(', ');
   result.data.push(row);
})

return result;
```

Dynamic report parameters

Both SQL and API report types support dynamic parameters that the user generating the report can submit at run time. You can also define these parameters when you create a schedule using the report definition.

SQL definitions

Parameter values can be defined within the *SQL Source* field, by enclosing the parameter names in square brackets; for example *[role_name]*. All SQL parameters are **required**.

API definitions

Parameter values can be defined by using double curly brace syntax; for example *{{userId}}*, in different places within the report definition.

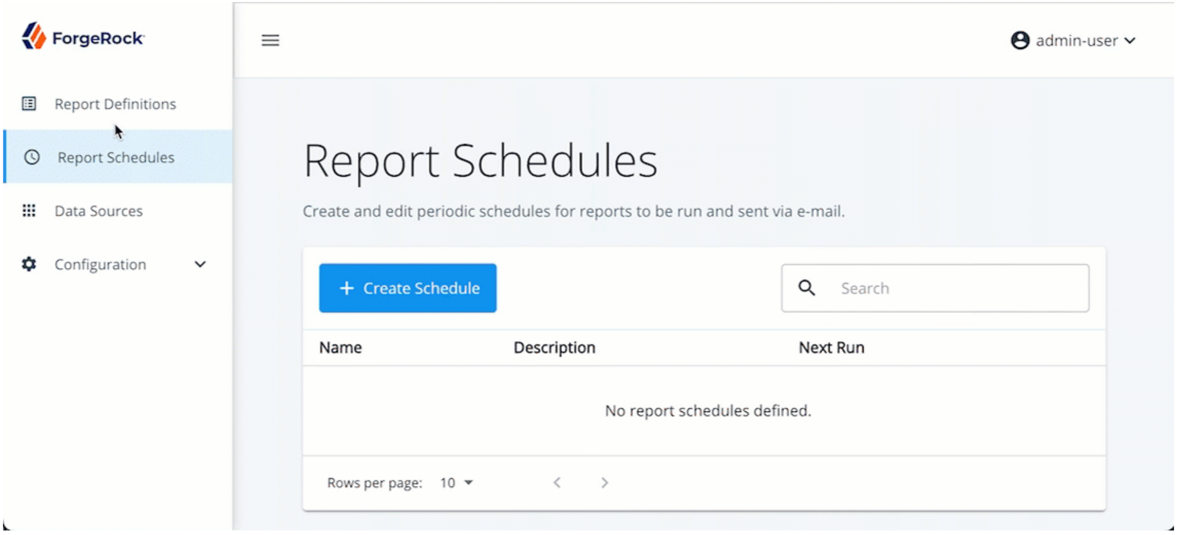
The various places are:

- **API Endpoint**.
- **Request Body**.
- **Query Parameters**.
    - When a parameter is defined as dynamic, no curly brace syntax is required, the value entered when prompted is the entire value.

- When a parameter is not defined as dynamic, the curly brace syntax is used to replace a section of a static value.
    - For example, a *_queryFilter* parameter can have a value of `accountStatus eq '{{accountStatus}}'` and only the marked section are dynamically populated.

Modifying report definitions

1. Navigate to the Report Definitions tab of the main dashboard.
2. In the table, click the ellipses next to the desired report to be modified, and select **Edit**.
3. Update the fields as necessary.
4. Click **Save** to complete the update.



Report Schedules

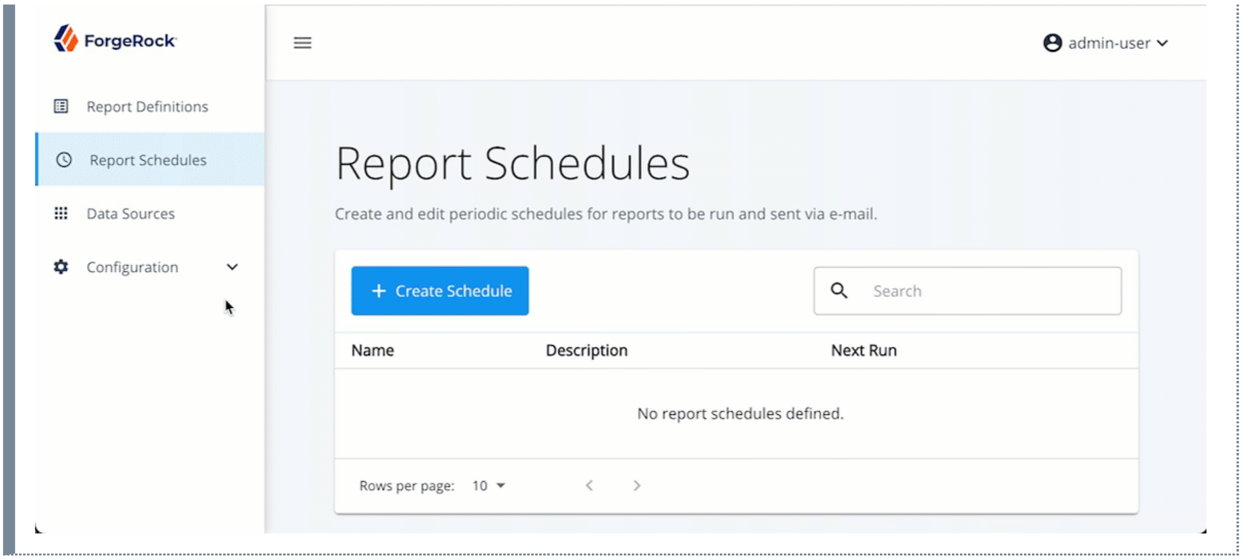
Create and edit periodic schedules for reports to be run and sent via e-mail.

Name	Description	Next Run
No report schedules defined.		

Rows per page: 10

Deleting report definitions

1. Navigate to the Report Definitions tab of the main dashboard.
2. In the table, click the ellipses next to the desired report to be modified, and select **Delete**.
3. Click **Delete Definition**.



Report Schedules

Create and edit periodic schedules for reports to be run and sent via e-mail.

Name	Description	Next Run
	No report schedules defined.	

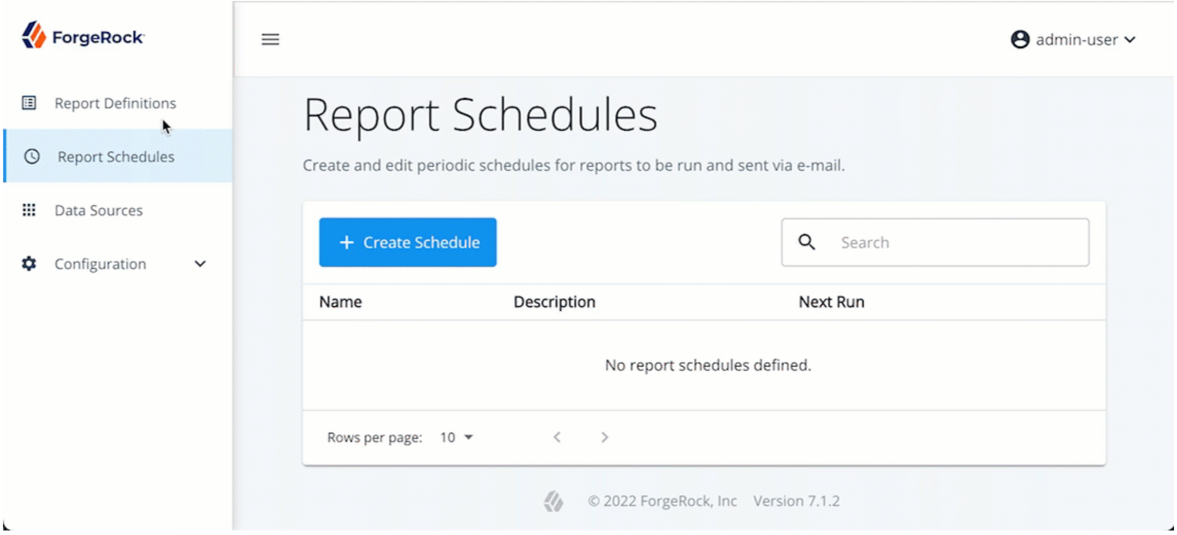
NOTE

Deleting a report definition that currently has existing schedules causes those schedules to be removed from IDR.

Duplicating report definitions

1. Navigate to **Report Definitions** tab of the main dashboard.
2. In the table, click the ellipses next to the desired report to be duplicated.
3. Select **Duplicate**.

Once the report definition has been duplicated, the new duplicated report has the text *copy* appended as a suffix.



Report Schedules

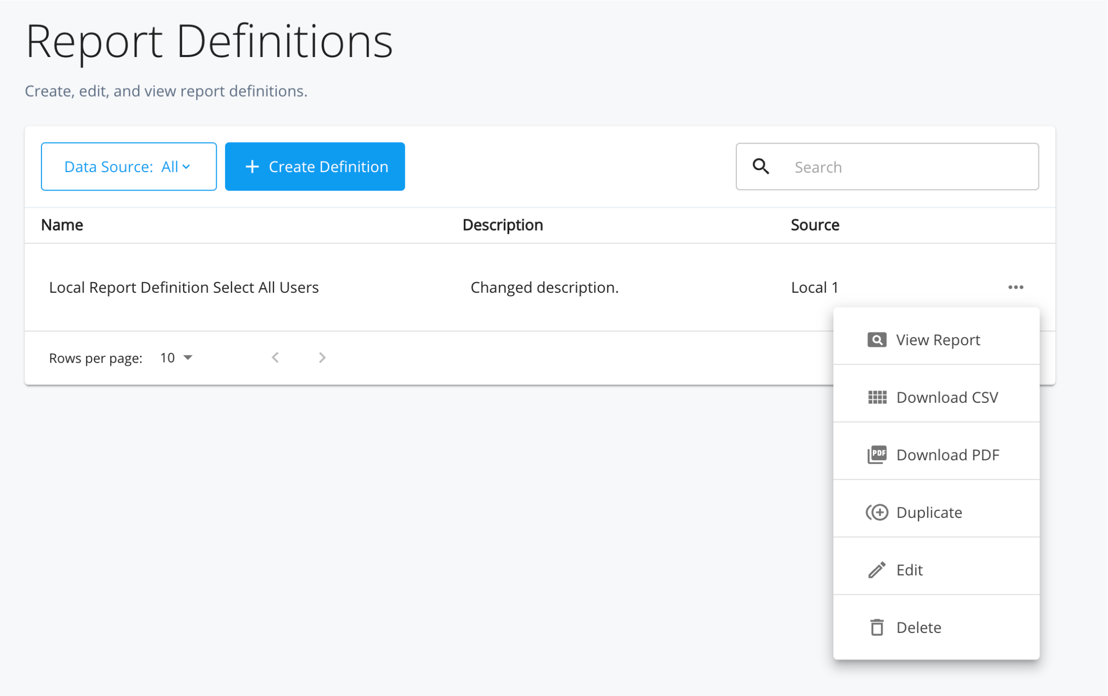
Create and edit periodic schedules for reports to be run and sent via e-mail.

Name	Description	Next Run
	No report schedules defined.	

Ad-hoc report generation

After Report Definitions have been created, they can immediately be used to generate reports directly from the Report Definitions table using the following steps:

1. Navigate to the Report Definitions tab of the main dashboard.
2. In the table, locate the report definition to generate the report from and select the “action” to bring up a menu containing one of the following options:

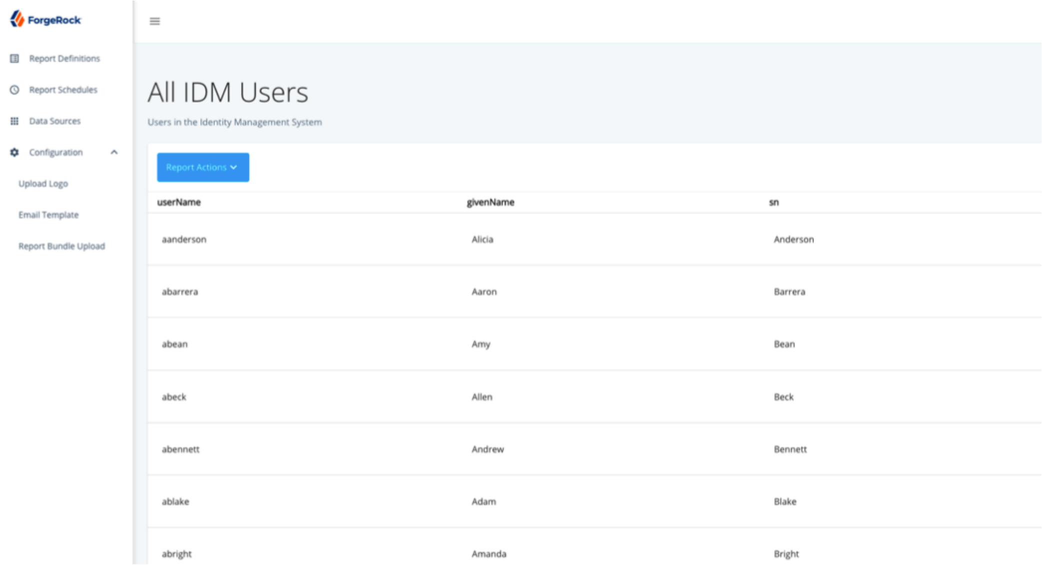


Report Definitions

Create, edit, and view report definitions.

Name	Description	Source
Local Report Definition Select All Users	Changed description.	Local 1

a. **View Report**. Generates the report for viewing directly in ForgeRock Identity Reporting within the browser. The output of the report will be displayed in a table, which the user can sort by individual columns and navigate through multiple pages. After reviewing the output of the report, the user may also download and save a copy of the report in one of the other two formats using the buttons in the top right of the report view.



All IDM Users

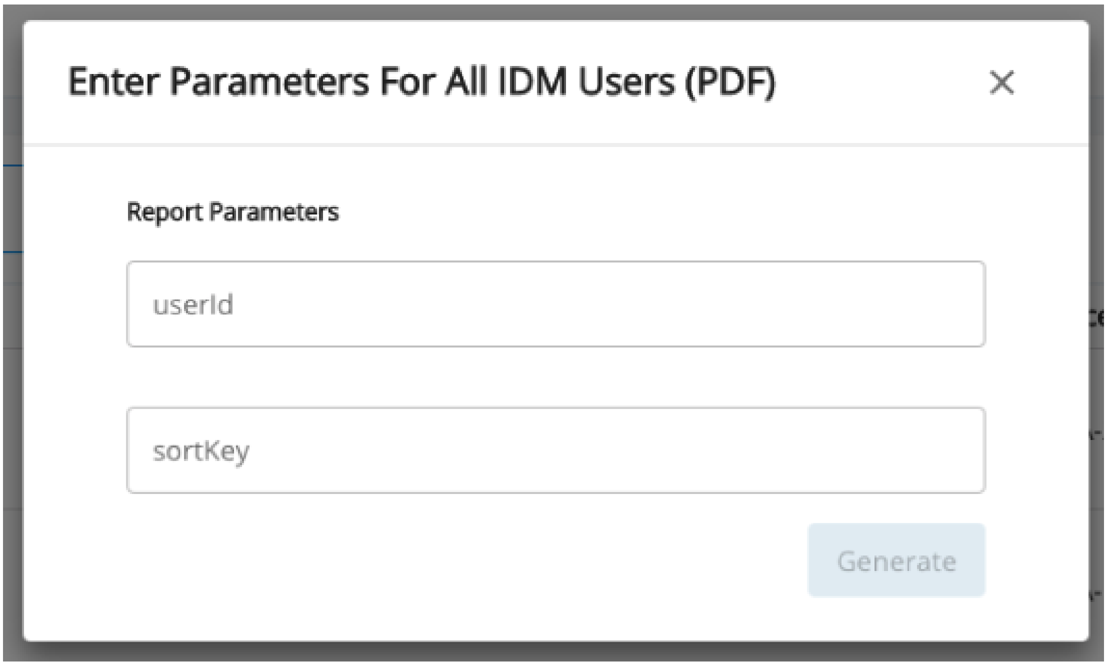
Users in the Identity Management System

userName	givenName	sn
aanderson	Alicia	Anderson
abarrera	Aaron	Barrera
abean	Amy	Bean
abeck	Allen	Beck
abennett	Andrew	Bennett
ablake	Adam	Blake
abright	Amanda	Bright

b. **Download as PDF**. Generates the report in the form of a PDF file to be downloaded to the client machine.

    c. **Download as CSV**. Generates the report in the form of a CSV file to be downloaded to the client machine. This file can then be used for flat-file operations or loaded into spreadsheet software, such as Excel.

3. After selecting the format of the report, an additional prompt may appear if the report definition contains parameters. This allows the user who is running the report to enter specific values only for the current execution of the report, without affecting any other users that wish to make use of the same report definition. The generate button is enabled only when all the required values are provided.



Enter Parameters For All IDM Users (PDF)

Report Parameters

userId

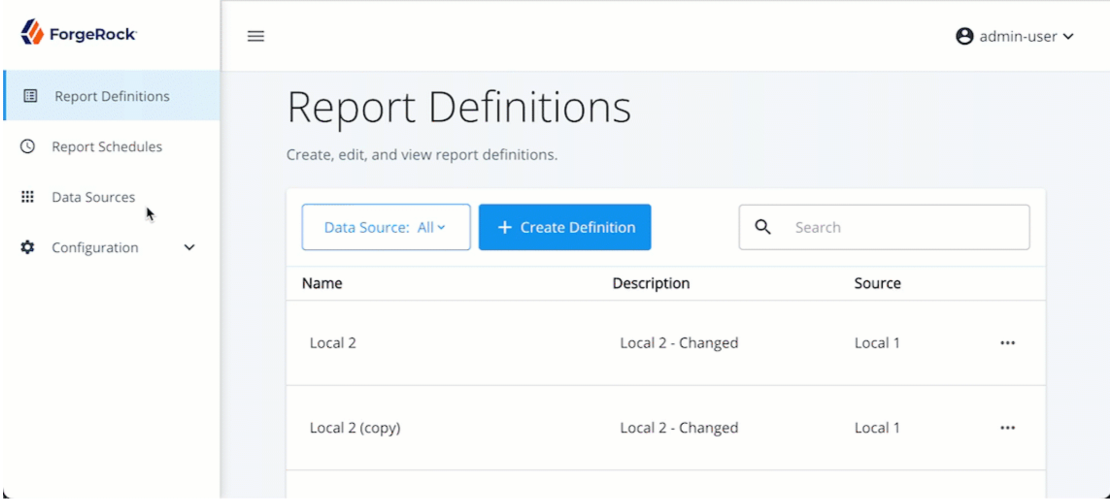
sortKey

Report schedules

Report schedules are used to define schedules for reoccurring reports or reports that need to be run on a future date. Each schedule contains a list of email recipients to which the report will be forwarded. The Report Schedules tab of the dashboard is used for managing these schedules. There must be at least one report definition before a report schedule can be created.

Creating new report schedules

1. Navigate to the **Report Schedules** tab of the main dashboard.
2. Click **Create Schedule**.



Report Definitions

Create, edit, and view report definitions.

Name	Description	Source	
Local 2	Local 2 - Changed	Local 1	•••
Local 2 (copy)	Local 2 - Changed	Local 1	•••

3. On the Create Report Schedule page, fill in each of the required fields. Additional details on the available fields are given below:

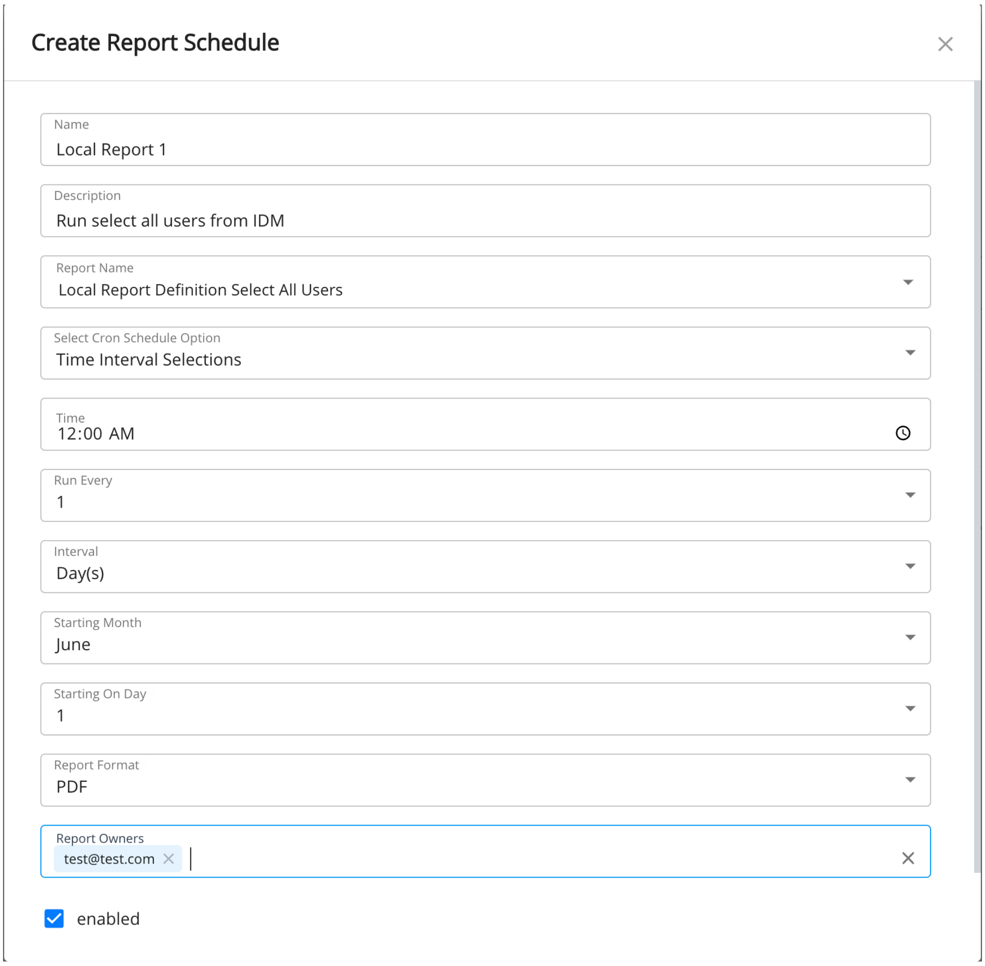
   a. **Schedule Name**: (Required) Name of the report schedule that appears in the table.

   b. **Description**: Provides additional information about the report schedule and its purpose.

   c. **Report Name**: (Required) Name of report definition to be run on a scheduled basis. After a report definition has been successfully created, it appears in this list for selection.

   d. **Select Cron Schedule Option**: (Required) Choose whether to enter schedule time options manually or to provide a cron formatted string.

      - When *Time Interval Selections* is selected:



Create Report Schedule

Name: Local Report 1

Description: Run select all users from IDM

Report Name: Local Report Definition Select All Users

Select Cron Schedule Option: Time Interval Selections

Time: 12:00 AM

Run Every: 1

Interval: Day(s)

Starting Month: June

Starting On Day: 1

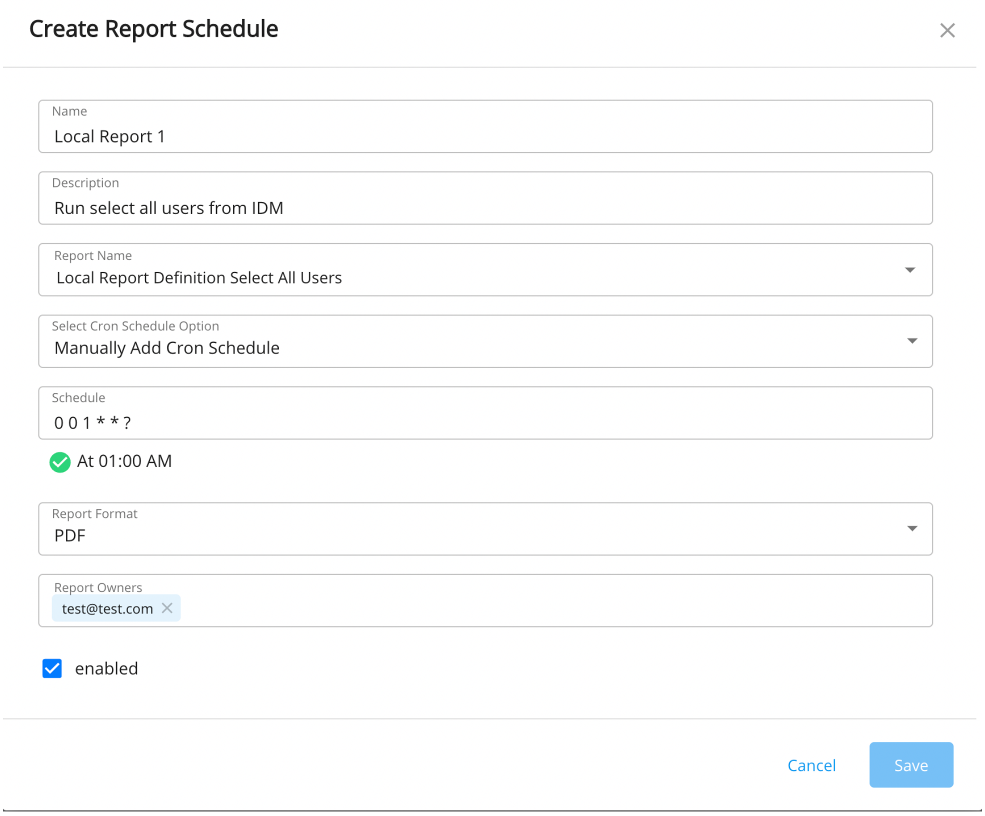
Report Format: PDF

Report Owners: test@test.com

☑ enabled

- **Time**: The time of day the report runs.
- **Run Every**: When choosing day as the interval, chose the number of days in between the runs.
- **Interval**: Time period interval for the report to run selecting days, weeks, or months.
- **Starting Month**: Month of the year the schedule takes effect.
- **Staring Day**: Day of the month the schedule takes effect.
- **Select Months**: When running monthly, select the months of the year the schedule should run.

- When *Manually Add Cron Schedule* is selected:



Create Report Schedule

Name: Local Report 1

Description: Run select all users from IDM

Report Name: Local Report Definition Select All Users

Select Cron Schedule Option: Manually Add Cron Schedule

Schedule: 0 0 1 * * ?

At 01:00 AM

Report Format: PDF

Report Owners: test@test.com

☑ enabled

- **Schedule**: Enter a cron formatted string, which determines the report schedule frequency.

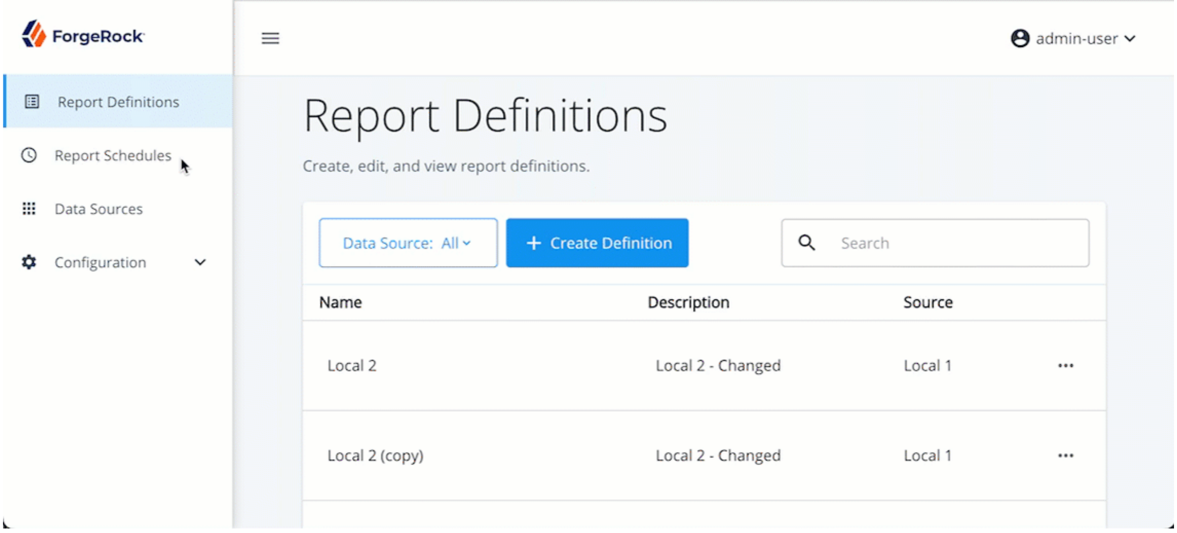
e. **Report Format**: (Required) File format of the report attached in the email notification.

f. **Report Owners**: (Required) List of emails that receive a notification containing the report when the schedule runs.

g. **Enabled**: Determines whether the schedule should run at the designated intervals. While the checkbox remains empty, the schedule does not generate a report or any corresponding notifications.

Modifying report schedules

1. Navigate to the Report Schedules tab of the main dashboard.
2. In the table, click the ellipses of the desired schedule, and select **Edit**.
3. Update the fields as necessary.
4. Click **Save**.



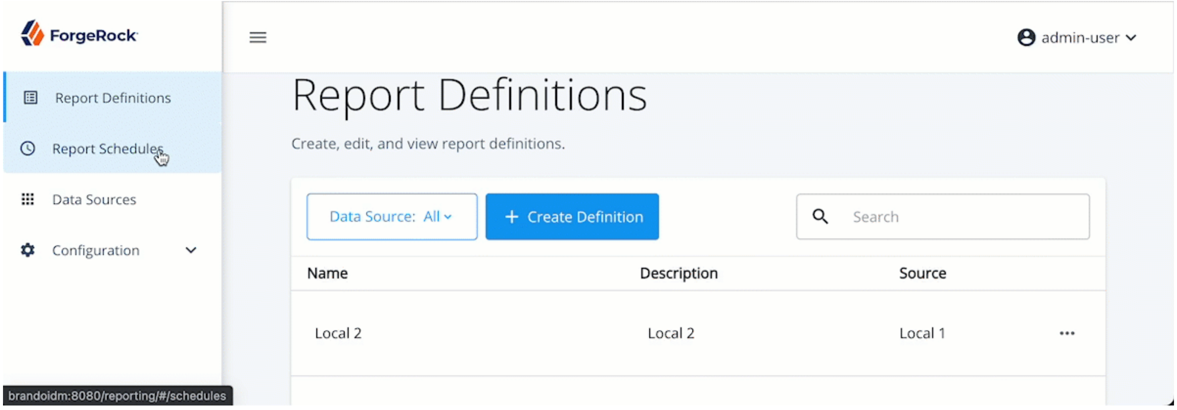
Report Definitions

Create, edit, and view report definitions.

Name	Description	Source	
Local 2	Local 2 - Changed	Local 1	···
Local 2 (copy)	Local 2 - Changed	Local 1	···

Deleting report schedules

1. Navigate to the Report Schedules tab of the main dashboard.
2. In the table, click the ellipses of the desired schedule and select **Delete**.
3. Select **Delete Report Schedule** to confirm the deletion.



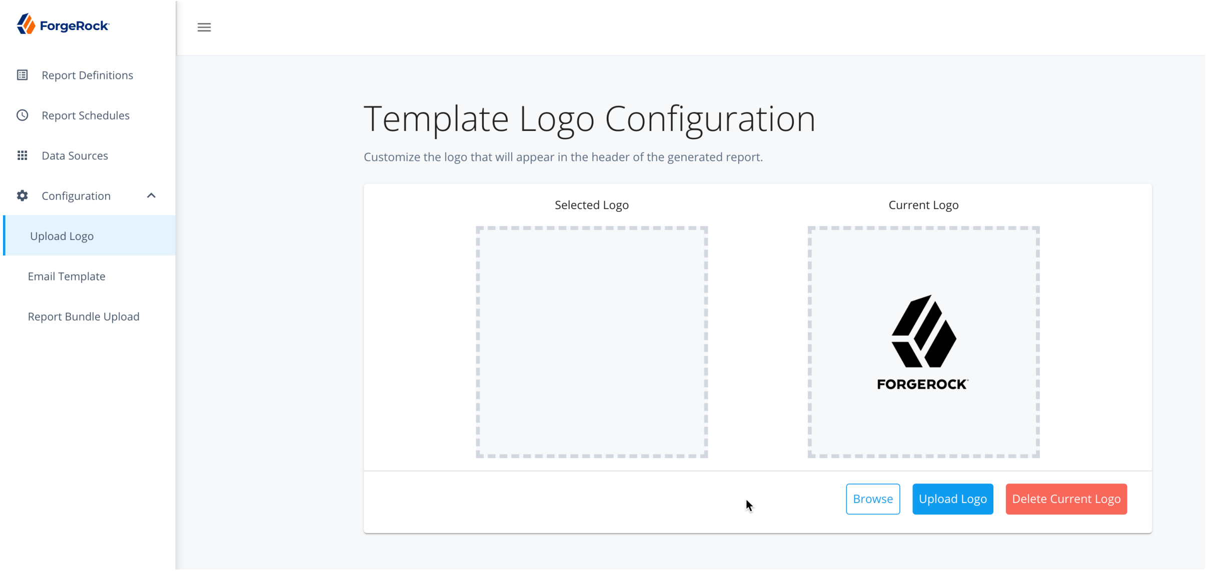
Report Definitions

Create, edit, and view report definitions.

Name	Description	Source	
Local 2	Local 2	Local 1	···

Configuration

ForgeRock Identity Reporting allows reporting administrators to customize the reporting experience with a few general, system-wide configurations. Administrators also have the option to import report bundles that contain single or multiple report definitions, allowing for simple migration from one environment to the next.



Template Logo Configuration

Customize the logo that will appear in the header of the generated report.

Report template

The report template section of the configuration allows an administrator to view, upload or remove a branding image used for PDF reports. Supported image formats are jpeg and png.

Upload New Logo:

> NOTE
>
> This process overwrites any existing logo with the new image.

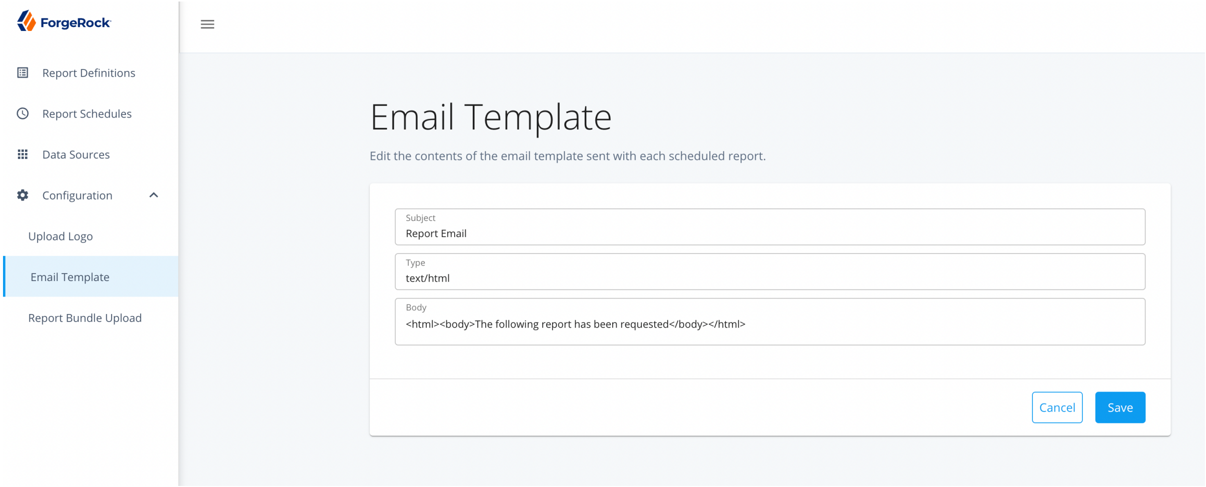
1. At the top of the dashboard page, in the navigation bar, select **Upload Logo** under Configuration menu.
2. Click **Browse** to open the Choose File dialog box and select an image to upload. The supported image formats are jpeg and png.
3. Once a valid image has been selected, it displays in the **Selected Logo** area for validation
4. Click **Upload** to complete the upload process. The new logo displays in the **Current Logo** area.

Delete current logo:

1. At the top of the dashboard page, in the navigation bar, select **Report Template** under the **Configure** menu.
2. Click **Delete Current Logo**. The image disappears from the **Current Logo** area.

Email

The email section of the configuration allows an administrator to modify the contents of the email notification that is sent out with every scheduled report.



Email Template

Edit the contents of the email template sent with each scheduled report.

Subject: Report Email

Type: text/html

Body: <html><body>The following report has been requested</body></html>

Modify email notification:

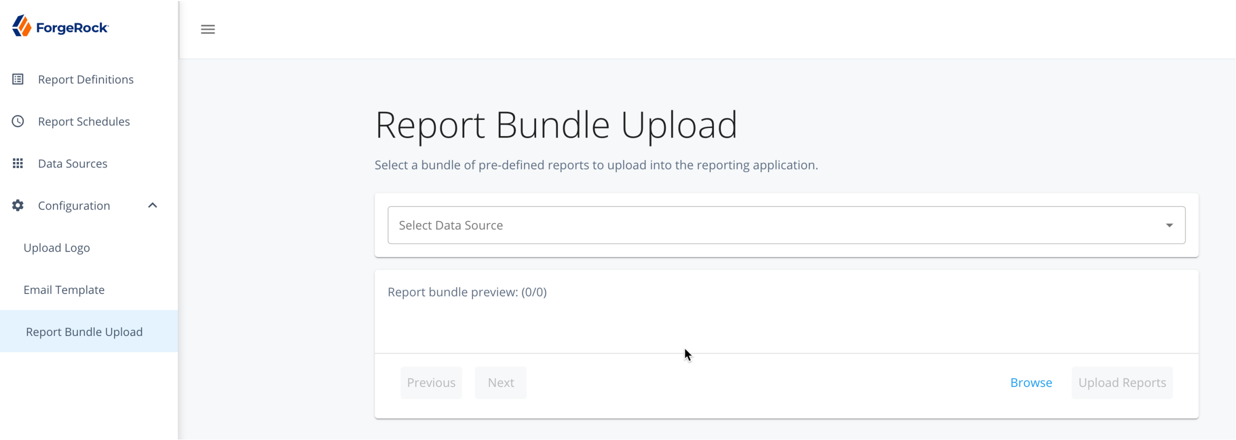
1. At the top of the dashboard page, in the navigation bar, select **Email Template** under the Configuration menu.
2. On the Email Template Configuration page, fill in each of the required fields. Additional details on the available fields are given below:
   - **Subject**: (Required) Subject of email notification.
   - **Type**: (Required) Content-Type of email body can be set to text/HTML or text/plain.
   - **Body**: (Required) Body of email notification.

Report bundle

The report bundle section of the configuration allows an administrator to import sets of pre-configured report definitions. The following guidelines can be used when creating bundles:

- Report bundles are required to be .json files that contain a “reportDefinitions” array in a JSON string
- The “reportDefinitions” array contains one or more JSON objects that represent individual report definitions
- Each object can specify all attributes available to a report definition, as described in Creating New Resource Definitions. All required attributes must be provided at a minimum. The Data Source selection box is available within the interface to allow

you to choose which data source the reports are being uploaded to. To upload reports for multiple data sources, use the API endpoint instead.



Report Bundle Upload

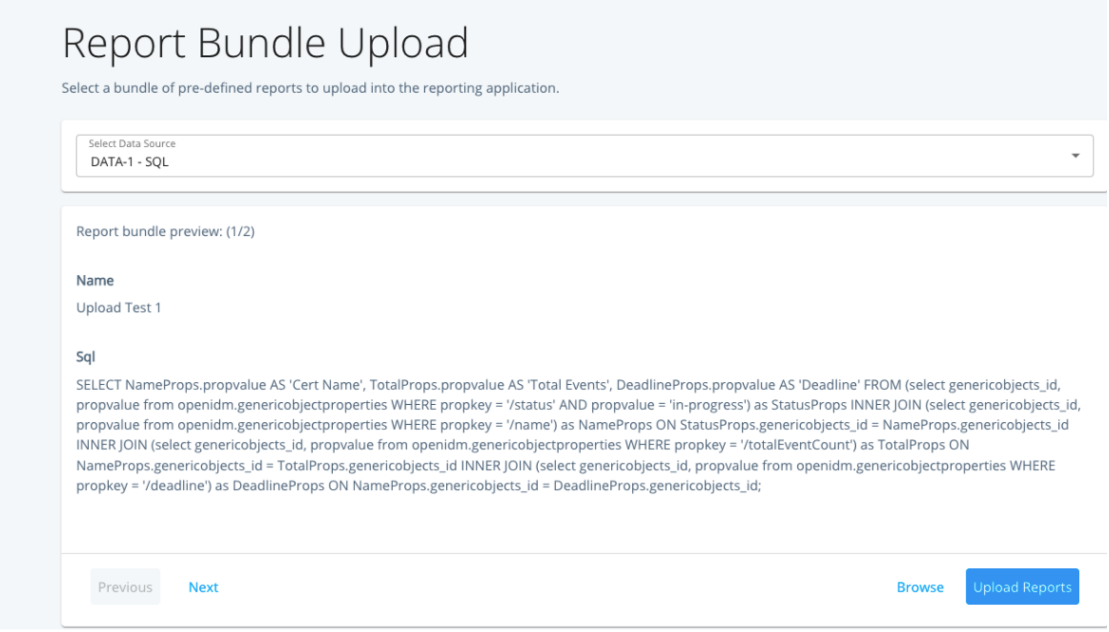
Select a bundle of pre-defined reports to upload into the reporting application.

Select Data Source

Report bundle preview: (0/0)

Upload report bundle:

1. At the top of the dashboard page, in the navigation bar, select **Report Bundle** under Configure
2. Click **Browse** to open the Choose File dialog box and select an image to upload. The bundle must be a .json file and contain valid JSON syntax



Report Bundle Upload

Select a bundle of pre-defined reports to upload into the reporting application.

Select Data Source
DATA-1 - SQL

Report bundle preview: (1/2)

Name
Upload Test 1

Sql
SELECT NameProps.propvalue AS 'Cert Name', TotalProps.propvalue AS 'Total Events', DeadlineProps.propvalue AS 'Deadline' FROM (select genericobjects_id, propvalue from openidm.genericobjectproperties WHERE propkey = '/status' AND propvalue = 'in-progress') as StatusProps INNER JOIN (select genericobjects_id, propvalue from openidm.genericobjectproperties WHERE propkey = '/name') as NameProps ON StatusProps.genericobjects_id = NameProps.genericobjects_id INNER JOIN (select genericobjects_id, propvalue from openidm.genericobjectproperties WHERE propkey = '/totalEventCount') as TotalProps ON NameProps.genericobjects_id = TotalProps.genericobjects_id INNER JOIN (select genericobjects_id, propvalue from openidm.genericobjectproperties WHERE propkey = '/deadline') as DeadlineProps ON NameProps.genericobjects_id = DeadlineProps.genericobjects_id;

3. Once a valid bundle has been selected, contents are loaded into the preview area for validation. The administrator is then able to navigate among multiple report definitions using the **Previous** and **Next** buttons.
4. Click **Upload Reports** to complete the upload process.

GDPR compliance

Due to GDPR regulations, Forgerock has identified the following critical areas that assist in implementing a compliant system. The sections below identify what personal data is captured, where that data is stored when it is stored and who can potentially access the data. It is the implementer's responsibility to scrub personal data as necessary to be considered compliant with GDPR regulations.

What personal data is being stored?

As ForgeRock IDM allows the user schema to be customized and linked to outside resources, it is not feasible to identify all potential Personal Identification Information (PII) that ForgeRock Identity Reporting can access. It is important to know that any application data that contains PII linked to an IDM user is exposed to the ForgeRock Identity Reporting application.

Examples: User Attributes:

- username
- givenName
- sn
- email

Where is personal data stored?

Reports can be exported in XLS or PDF format. Exporting a report is done in memory and leaves no artifacts on the filesystem.

When is the data being stored?

Data is stored when an authorized Identity Reporting user exports a report to XLS or PDF. Exporting a report is done in memory and leaves no artifacts on the filesystem.

Who can access the data?

- ForgeRock Identity Reporting administrators
- IDM Admins
- Individuals who received the exported report
- IT administrators who have access to the filesystem