Identity Reporting 1.1 Identity Reporting

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Refer to https://docs.pingidentity.com for the most current product documentation.

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 Dashboard

Learn about the ForgeRock Identity Reporting dashboard.

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

Report Configuration

Learn about the ForgeRock Identity

Reporting report schedules.

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-1.1.3.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 that can be 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 that will be injected into existing files.

Installation Instructions

1. Unzip the `identity-reporting-1.1.3.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.
- **openidm_url**: URL where IDM can be reached. This will often be *localhost*.
- **openidm_version**: The version of IDM. This will either be 6.5 or 7.0.
- **openidm_admin**: User ID for the user with the `openidm-admin` role.
- **openidm_admin_password**: Password for the `openidm-admin` role.
- **create_local_ds**: Create a datasource for the IDM database. Note: IDM must be running if this is set to `yes`.

NOTE

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

The installer will print 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`
3. Delete or move the following file from the IDM installation directory:
    - `openidm/bundle/httpclient-osgi-4.x.x.jar`

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 that is 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 section 2.1.2 of the ForgeRock Platform Setup Guide found at the following url: https://backstage.forgerock.com/docs/platform/7/platform-setup-guide/#proc-auth-clients

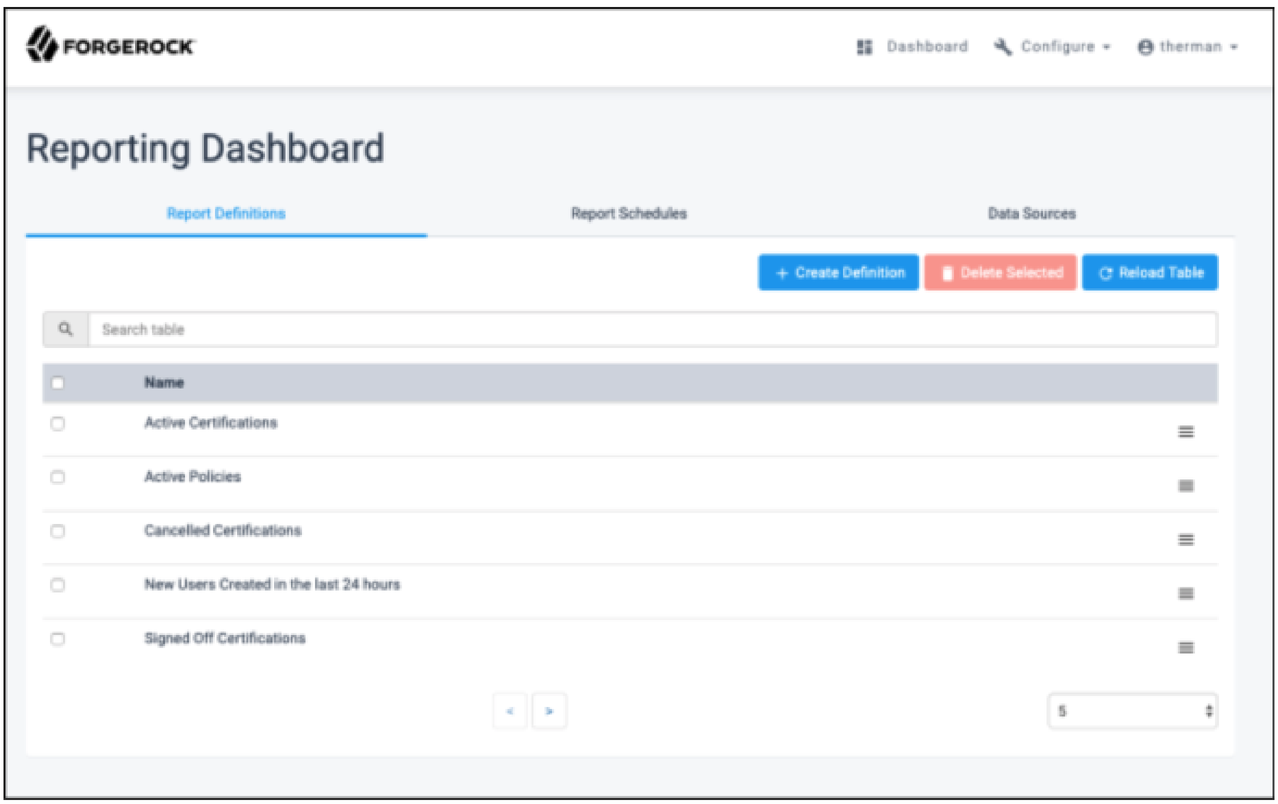
In step 5 of the section, instructions are given to configure a client for the end-user UI. For Identity Reporting, please repeat those steps with the following adjustments:

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

Reporting Dashboard

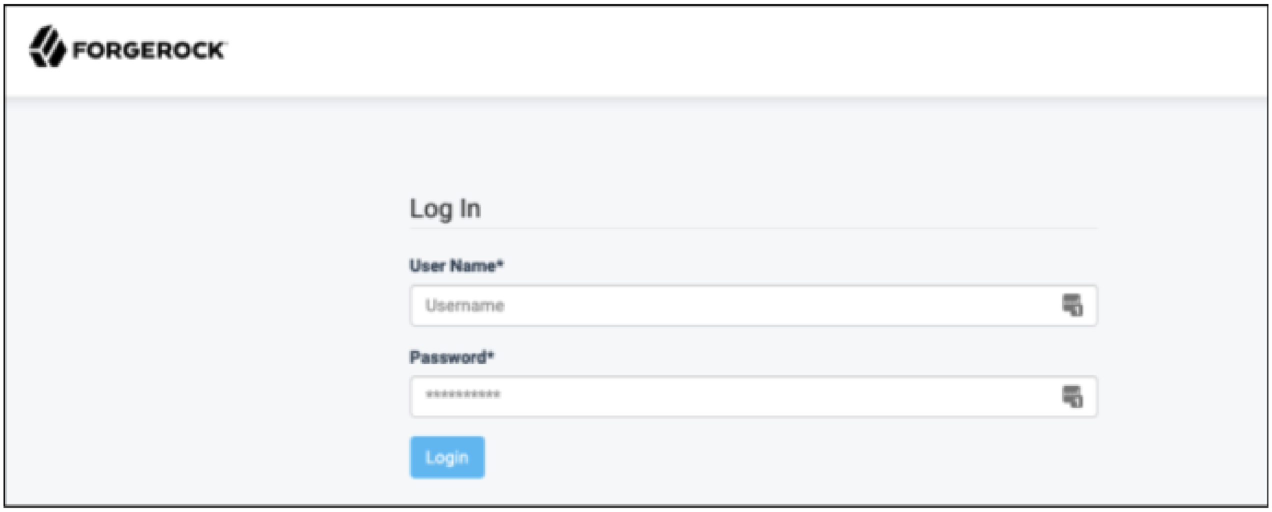
The Reporting Dashboard details the following options for configuration to the administrator:

- **Report Definitions**
- **Report Schedules**
- **Data Sources**
- **Configuration**



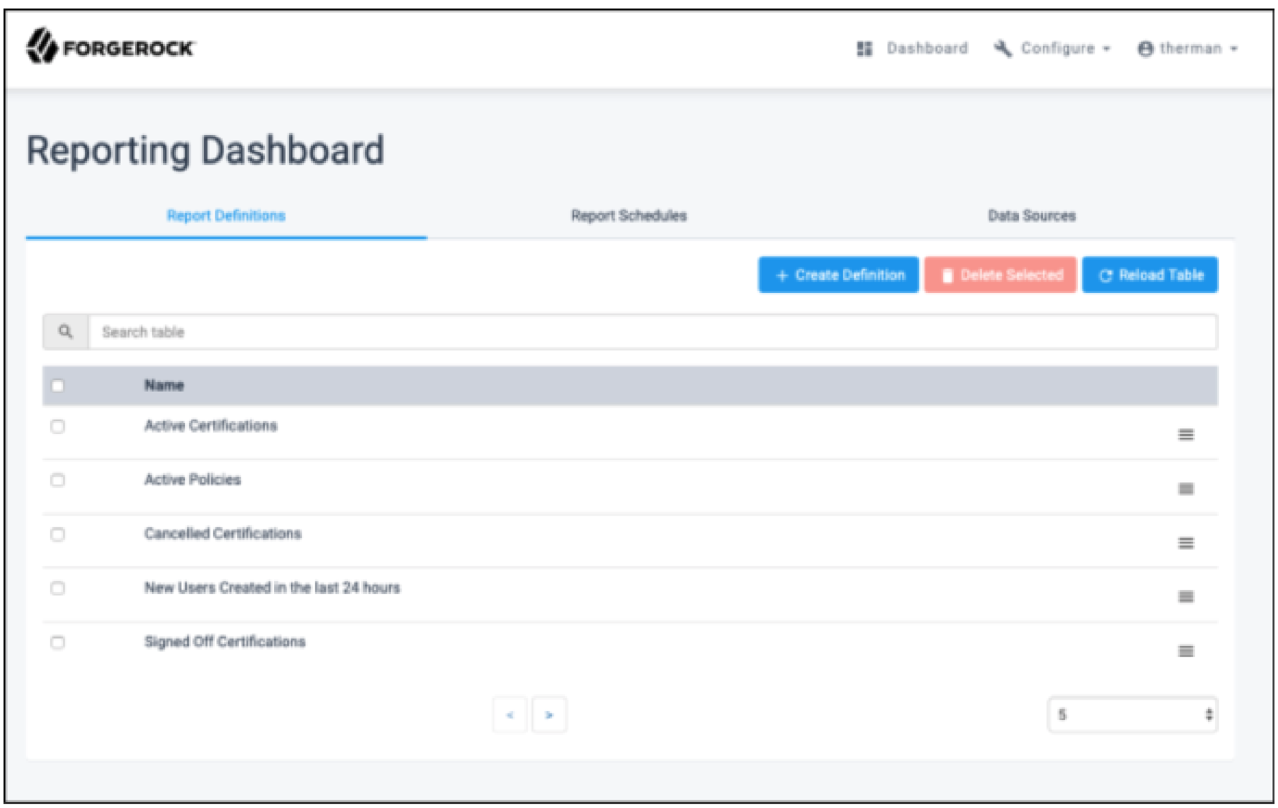
Logging on to the Reporting Dashboard

Log in to Reporting Dashboard directly as an administrator by navigating to the default URL context: http://<HOSTNAME>:<PORT>/reporting.



Tables

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



- **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.

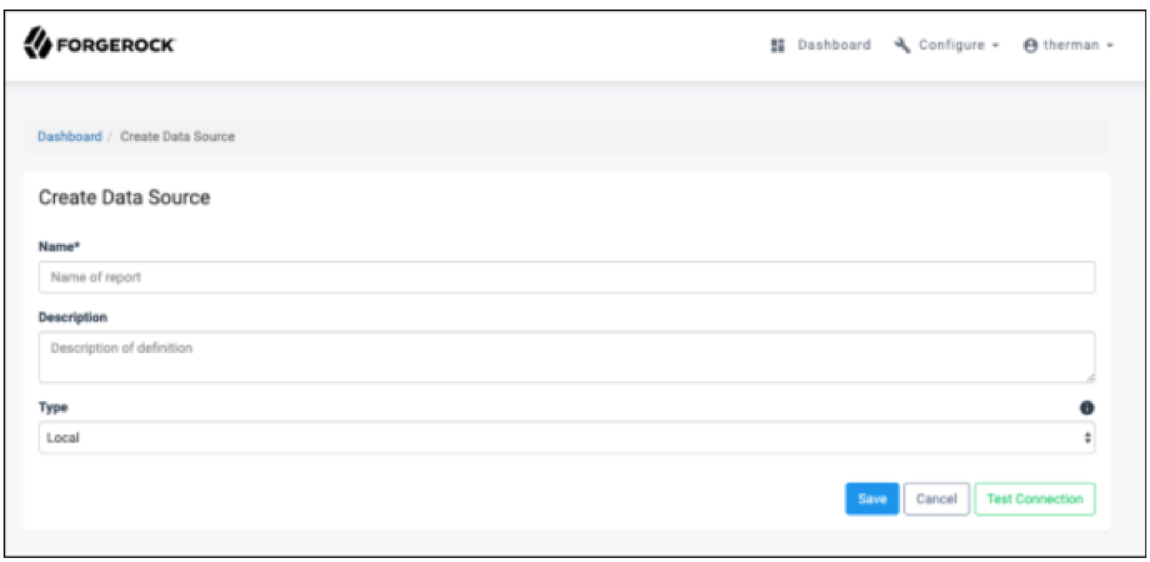
- **Limiting results per page**. (Items per page) Identifies a number of results made visible at a specific time within the table. Values may include 5, 10, 25 or 50.
- **Navigating results**. Allows navigation within the table when results exceed the number specified in the field Items per page.

Data Sources

Data sources are used to specify where reports can retrieve information and any necessary connection details. The Data Sources tab of the dashboard is used for managing these data sources. Current versions of ForgeRock Identity Reporting only support database connections.

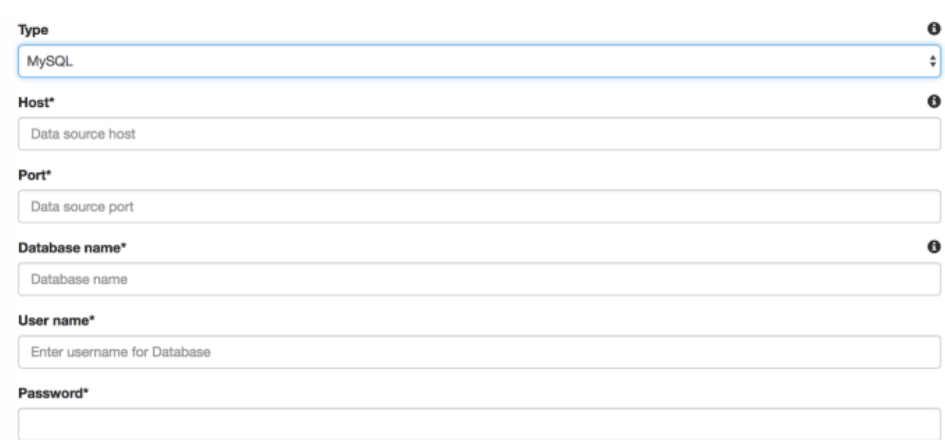
Creating New Data Sources

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



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



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.

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. If left blank, the password field will not update and overwrite the existing password; however, if testing the connection, the password field must be filled in.
4. Click **Save** to complete the update.

NOTE

At any point during or after this process, “Test Connection” can be selected and a connection will attempt to be made using any of currently supplied information on the form. It is recommended to test the connection after completing the form and before saving the details.

Deleting Data Sources

Data Sources can be deleted individually or in bulk.

Delete individual data sources:

1. Navigate to the Data Sources tab of the main dashboard.
2. In the table, select the data source to be deleted.
3. Click **Delete**.
4. Select **Yes** to confirm the deletion.

Bulk Deletion is done directly from the Data Sources table in the dashboard.

Run bulk deletion:

1. Navigate to the Data Sources tab of the main dashboard.
2. In the table, locate and select, via the checkboxes on the left, the data sources to be deleted.
3. Select **Delete Selected**.
4. Select **Yes** to confirm the deletion.

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.

Creating New Report Definitions

1. Navigate to the Report Definitions tab of the main dashboard.
2. Select **Create Definition**.
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 will appear in this list for selection.
   - **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 (e.g., [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.

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

Modifying Report Definitions

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

Deleting Report Definitions

Report Definitions can be deleted individually or in bulk.

Delete individual report definitions:

1. Navigate to the Report Definitions tab of the main dashboard.
2. In the table, select the report definition to be modified.
3. Click **Delete**.
4. Select **Yes** to confirm the deletion.

Bulk Deletion is done directly from the Report Definitions table in the dashboard.

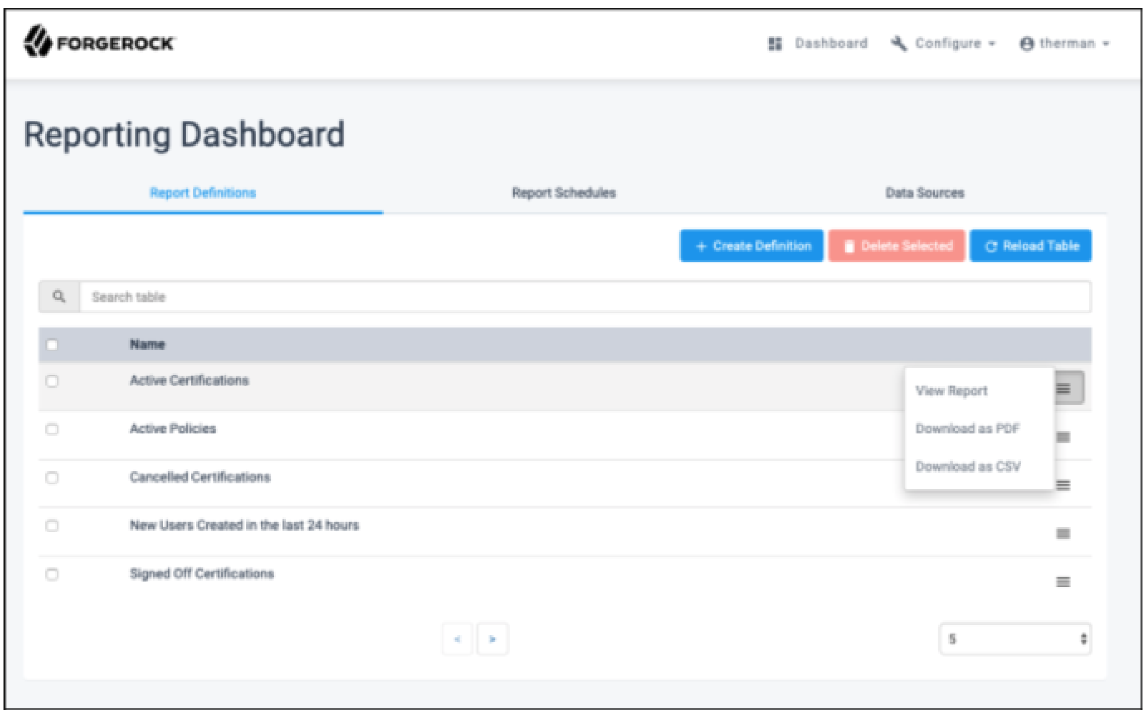
Delete individual report definitions:

1. Navigate to the Report Definitions tab of the main dashboard.
2. In the table, locate and select, via the checkboxes on the left, the report definitions to be deleted.
3. Click **Delete Selected**.
4. Select **Yes** to confirm the deletion.

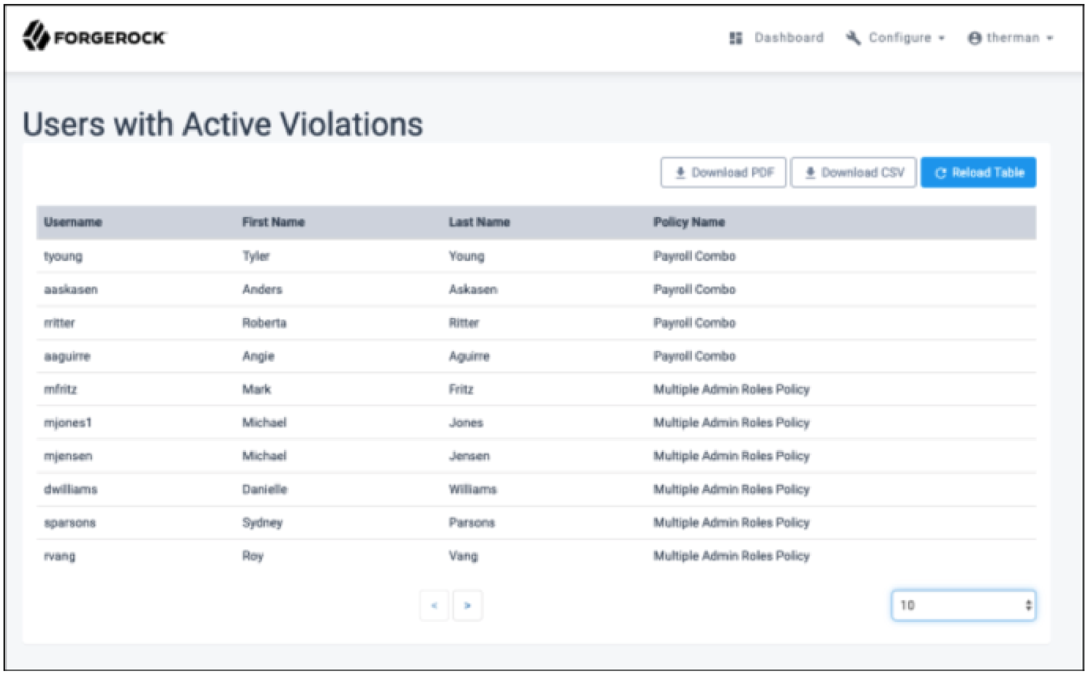
Ad-hoc Report Generation

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:



   a. **View Report**. This will generate 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.



b. **Download as PDF**. This will generate the report in the form of a PDF file to be downloaded to the client machine. If this option is selected, there will be an additional prompt that asks whether the SQL used to generate the report should be included in the PDF.

c. **Download as CSV**. This will generate 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.

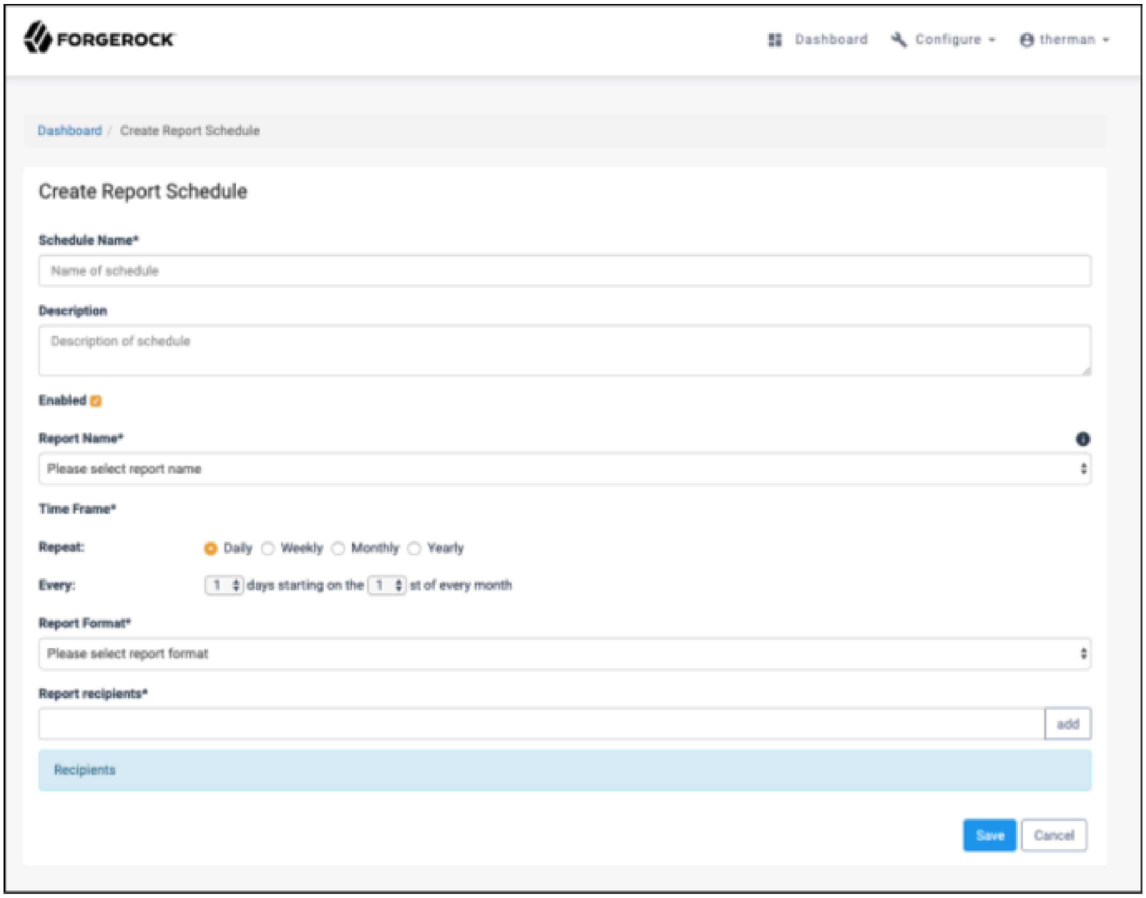
3. After selecting the format of the report, an additional prompt may appear if the report definition contains parameters. This will allow the user that is running the report to enter specific values only for the current execution of the report, without affecting any other users that wish to make use of the same report definition.

Report Schedules

Report Schedules are used to define schedules for re-occurring reports or reports that need to be run on a future date. Each schedule will also contain 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**.



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.

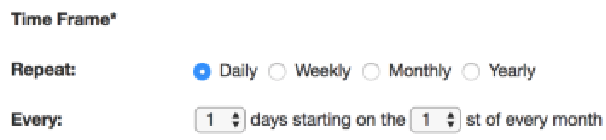
    b. **Description**. Provides additional information about the report schedule and its purpose.

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

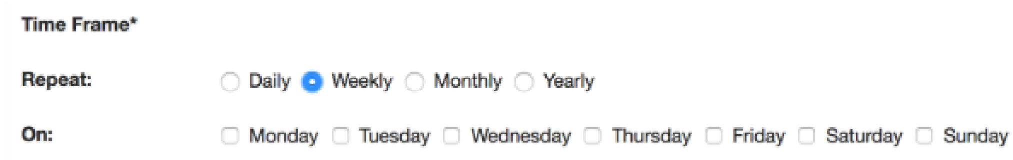
    d. **Report Name**. (Required) Name of report definition that will be run on a scheduled basis. After a report definition has been successfully created, it appears in this list for selection.

    e. **Time Frame**. (Required) Interval at which the schedule should run to generate a report. The options available use CRON standard settings:

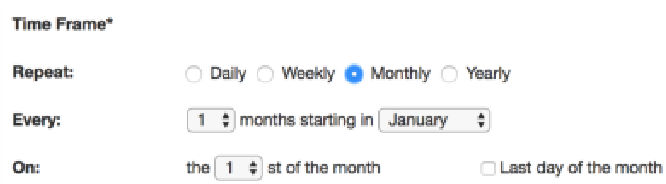
        - **Daily**. Allows the administrator to generate a report every specified number of days, starting on a specified day of the month.



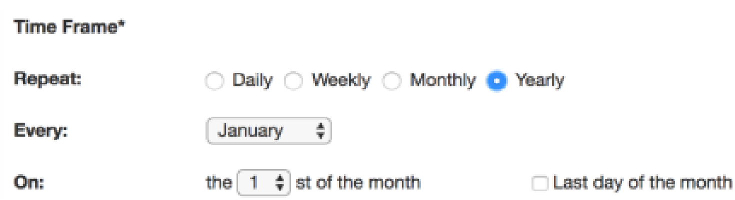
- **Weekly**. Allows the administrator to generate a report on specified days of the week.



- **Monthly**. Allows the administrator to generate a report every specified number of months starting on a specified month. Day of the month for the report generation can also be specified, with `Last day of the month` as an option.



- **Yearly**. Allows the administrator to generate a report every year on the specified day of the specified month. The day of the month for report generation can also be specified, with `Last day of the month` as an option.



f. **Report Format**. (Required) File format of the report that will be attached in the email notification.

g. **Report Recipients**. (Required) List of emails that will receive a notification containing the report when the schedule runs.

Modifying Report Schedules

1. Navigate to the Report Schedules tab of the main dashboard.
2. In the table, select the report scheduled to be modified.
3. Update the fields as necessary.

4. Click **Save**.

Deleting Report Schedules

Report Schedules can be deleted individually or in bulk.

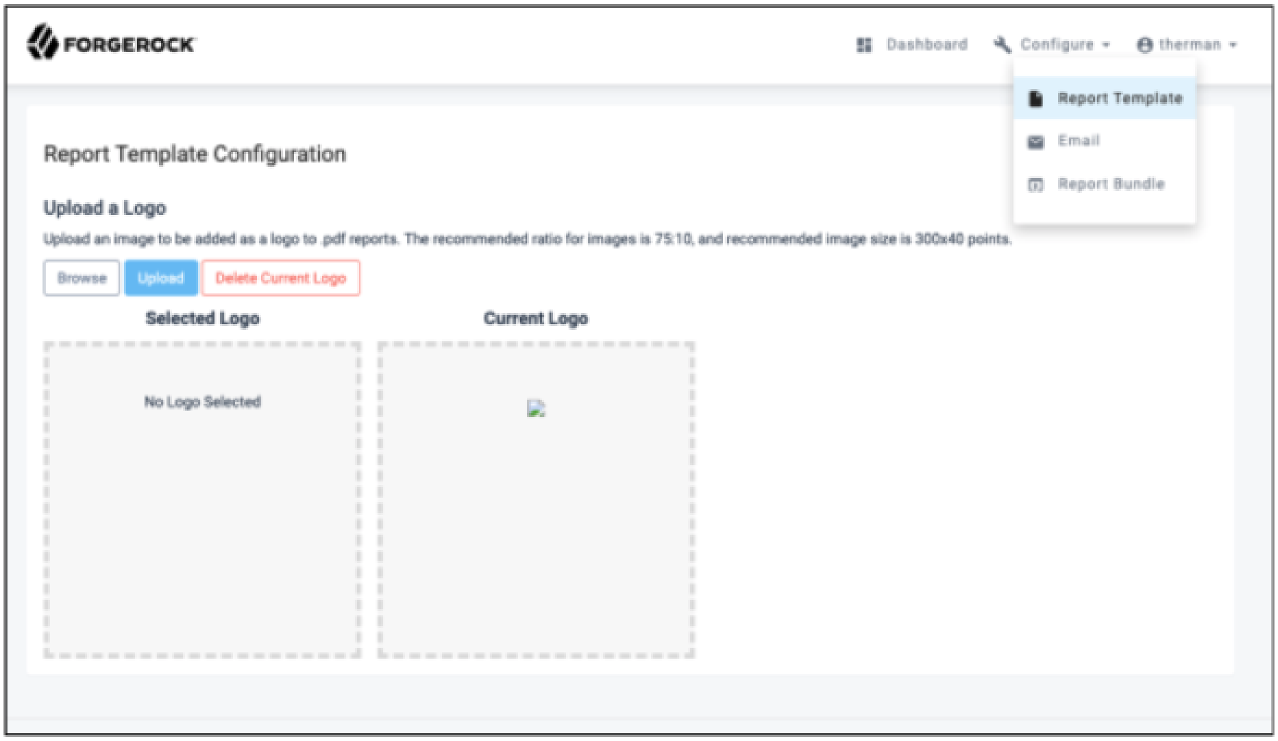
> Delete Individual Report Schedules:
>
> 1. Navigate to the Report Schedules tab of the main dashboard.
> 2. In the table, select the report scheduled to be deleted.
> 3. Click **Delete**.
> 4. Select **Yes** to confirm the deletion.

Bulk Deletion is done directly from the Report Schedules table in the dashboard.

> Delete Bulk Report Schedules:
>
> 1. Navigate to the Report Schedules tab of the main dashboard.
> 2. In the table, locate and select, via the checkboxes on the left, the report schedules to be deleted.
> 3. Click **Delete Selected**.
> 4. Select **Yes** to confirm the deletion.

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.



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:

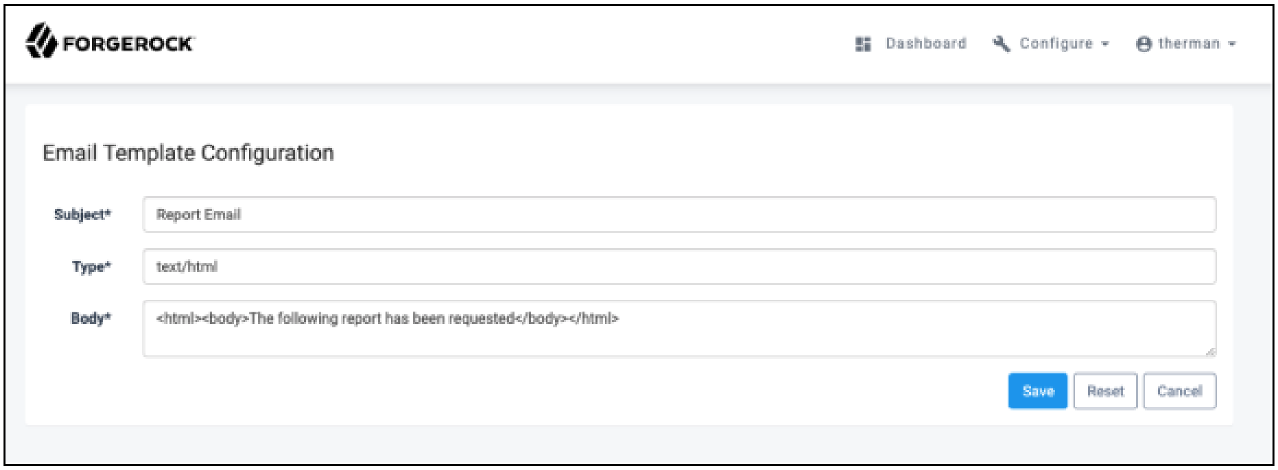
1. At the top of the dashboard page, in the navigation bar, select **Report Template** under Configure menu.
2. Click **Browse** to open the Choose File dialog box and select an image to upload. The supported image formats are jpeg and png.
3. Once a valid image has been selected, it will appear in the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



Modify Email Notification:

1. At the top of the dashboard page, in the navigation bar, select **Email** under the Configure 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

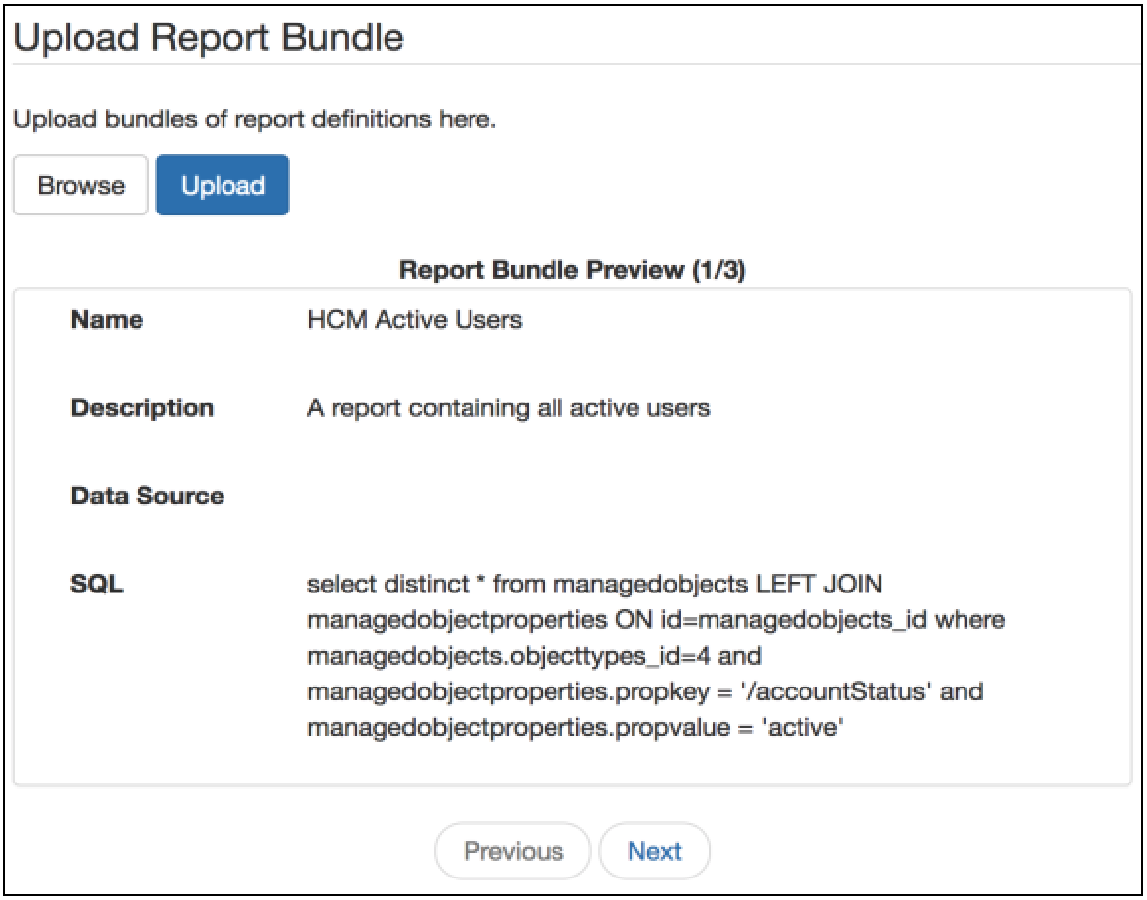
The Report Bundle section of the configuration allows an administrator to import sets of pre-configured report definitions. The following guidelines can be used when creating bundles:

- Report bundles are required to be .json files that contain a “reportDefinitions” array in a JSON string
- The “reportDefinitions” array will contain one or more JSON objects that represent individual report definitions

- Each object can specify all attributes available to a report definition (See Creating New Resource Definitions; however, they require the `name` and `SQL` attributes at a minimum. The `data_source` attribute may also be used to reference data sources that have already been created in the environment.
- If a `data_source` is not specified in the object, the report definition will still be created in the system with an empty data source. This report definition will not generate reports until it has been manually updated and an appropriate data source is selected.

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



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