ForgeRock Identity Cloud guide

ForgeRock® Identity Platform serves as the basis for our simple and comprehensive Identity and Access Management solution. We help our customers deepen their relationships with their customers, and improve the productivity and connectivity of their employees and partners. For more information about ForgeRock and about the platform, see https://www.forgerock.com.

About this guide

This guide is for customers using an agent-based integration model, with ForgeRock Access Management on-premise, or another on-premise access management solution. The guide provides an example of how to transition from on-premise access management to ForgeRock Identity Cloud without changing the architecture of the agent-based model.

The examples in this document are based on an available version of Identity Cloud. As Identity Cloud evolves, the examples in this document will be updated to reflect the changes.

Example installation for this guide

Identity Cloud is described in the ForgeRock Identity Cloud docs.

Find the value of the following properties:

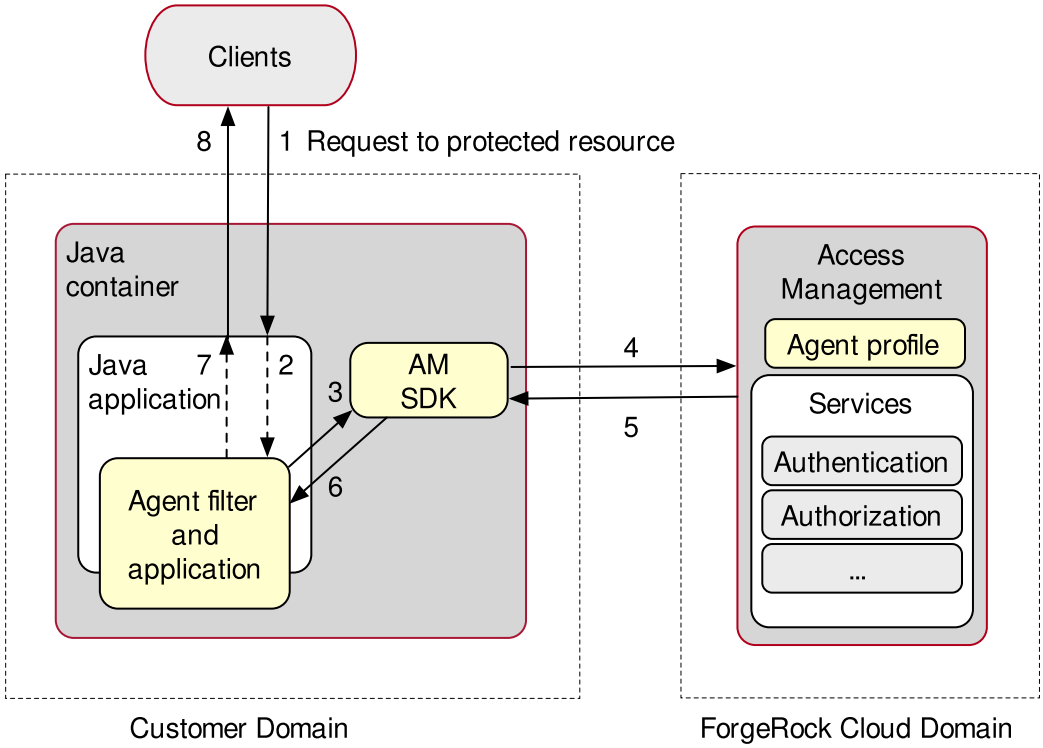
- The agent URL. This guide uses Java Agent installed on `http://agent.example.com:80/app`.
- The root URL of your Identity Cloud. This guide uses `https://tenant.forgeblocks.com:443`.
- The server URL of the Access Management component of the Identity Cloud. This guide uses `https://tenant.forgeblocks.com:443/am`.
- The realm where you work. This guide uses `alpha`.

If you use a different configuration, substitute in the procedures accordingly.

About Java Agents and the ForgeRock Identity Cloud

ForgeRock Identity Cloud simplifies the consumption of ForgeRock as an Identity Platform. However, many organizations have business web applications and APIs deployed across multiple clouds, or on-premise. This guide provides an example of how to use Java Agents with the ForgeRock Identity Cloud, without changing the architecture of the agent-based model.

The following image illustrates the flow of an inbound request to a website, through a Java Agent, and the Java Agent's interaction with ForgeRock Identity Cloud to enforce resource-based policies.



For information, refer to the ForgeRock Identity Cloud docs.

Prepare for installation

For information about installing Java Agent, refer to the Installation guide. This section summarizes considerations for using the agent with Identity Cloud:

- Configure Identity Cloud and set up a policy before you install the agent. When you configure the agent in the Identity Cloud admin UI, you can select the policy.
- For environments with load balancers or reverse proxies, consider the communication between the agent and the Identity Cloud servers, and between the agent and the client. Configure the environment **before** you install the agent.

Example installation for this guide

Unless otherwise stated, the examples in this guide assume the following installation:

- AM server URL: `https://tenant.forgeblocks.com:443/am`
- Agent URL: `http://agent.example.com:80/app`
- Agent profile name: `java-agent`
- Agent profile realm: `/alpha`
- Agent profile password: `/secure-directory/pwd.txt`

Add a demo user in Identity Cloud

Add a user so you can test the examples in this guide.

1. In the Identity Cloud admin UI, select **Identities** > **Manage** > **Alpha realm - Users**.
2. Add a new user with the following values:
    - **Username** : `demo`
    - **First name** : `demo`
    - **Last name** : `user`
    - **Email Address** : `demo@example.com`
    - **Password** : `Ch4ng3!t`

Create a policy set and policy in Identity Cloud

1. In the Identity Cloud admin UI, select **Native Consoles** > **Access Management**. The AM admin UI is displayed.
2. In the AM admin UI, select **Authorization** > **Policy Sets** > **New Policy Set**, and add a policy set with the following values:
    - **Id** : `PEP`
    - **Resource Types** : `URL`
3. In the policy set, add a policy with the following values:
    - **Name** : `PEP-policy`
    - **Resource Type** : `URL`
    - **Resource pattern** : `*://*:*/*`
    - **Resource value** : `*://*:*/*`
4. On the **Actions** tab, add actions to allow HTTP `GET` and `POST`.
5. On the **Subjects** tab, remove any default subject conditions, add a subject condition for all `Authenticated Users`.

Create an agent profile in Identity Cloud

1. In the Identity Cloud admin UI, go to **Gateways & Agents** > **+ New Gateway/Agent**, and add a Java Agent with the following values:
   - **Agent ID** : `java-agent`
   - **Password** : `password`
   - **Application URL** : `http://agent.example.com:80/app`
2. Click **Save Profile** and **Done**.
3. On the agent profile page, select **Use Policy Authorization**, select a policy set to assign to the profile, and then click **Save**.

   If a suitable policy set isn't available, select **Edit advanced settings** to edit or create one.

Enforce policies decisions from ForgeRock Identity Cloud

This example sets up ForgeRock Identity Cloud as a policy decision point for requests processed by Java Agents. For more information about Java Agents, refer to the User guide.

> 1. Using the ForgeRock Identity Cloud docs, log in to Identity Cloud as an administrator.
> 2. Make sure that you are managing the `alpha` realm. If not, switch realms.
> 3. Create a policy set and policy.
> 4. Create an agent profile.
>
>   When a policy set is assigned to the agent profile during creation, the agent uses that policy set. If a suitable policy set isn't available during creation, select **Edit advanced settings** to edit or create one and assign it to the agent profile.
> 5. Test the setup:
>   a. Go to `http://agent.example.com:80/app` . The Identity Cloud login page is displayed.
>   b. Log in to Identity Cloud as user `demo` , password `Ch4ng3!t` , to access the web page protected by the Java Agent.