


Was this helpful?  

ForgeRock Identity Cloud guide

ON THIS PAGE

- ForgeRock Identity Cloud guide
 - About this guide
 - Example installation for this guide
 - About Java Agents and the ForgeRock Identity Cloud
 - Enforce policies decisions from ForgeRock Identity Cloud

ForgeRock Identity Cloud guide

ForgeRock Identity Platform serves as the basis for our simple and comprehensive Identity and Access Management solution. For more information, visit <https://www.pingidentity.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 [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` in the `alpha` realm.

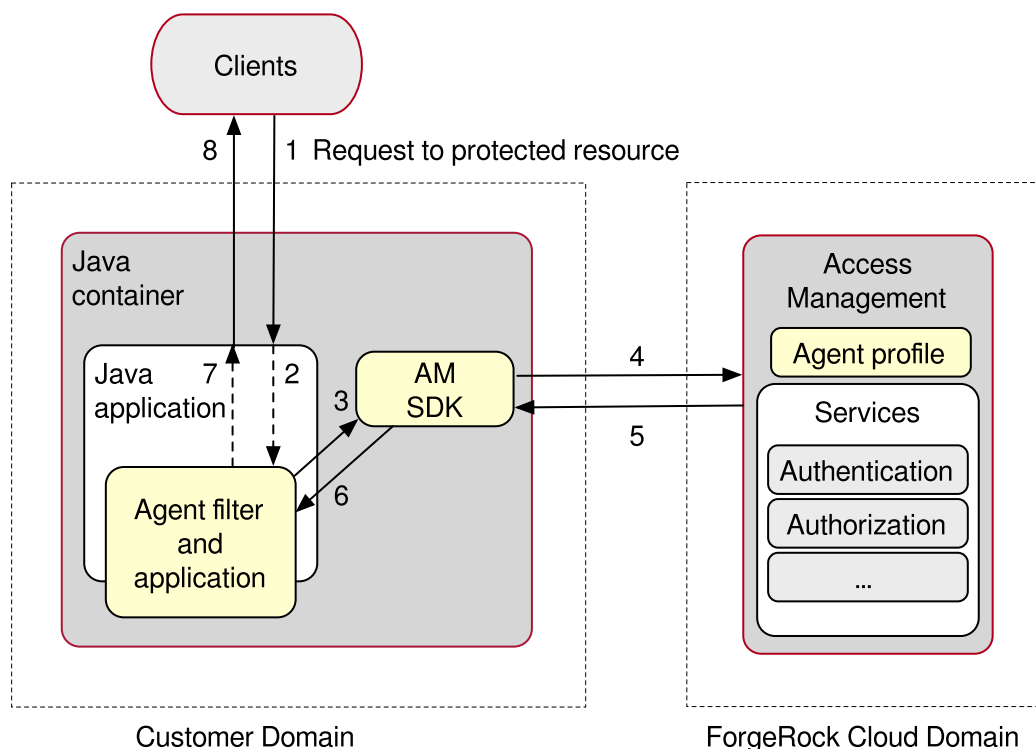
- The root URL of your Identity Cloud. This guide uses `https://tenant.forgeblocks.com`.
- The URL of the Access Management component of the Identity Cloud. This guide uses `https://tenant.forgeblocks.com/am`.
- The realm where you work. This guide uses `alpha`.

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, see the [Identity Cloud](#) docs.

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, see the [User guide](#).

Before you start, use the [Installation guide](#) to install a Java Agent with the following values:

- 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: `/tmp/pwd.txt`

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. [Add a user profile](#) with the following values:
 - **Username** : `demo`
 - **First name** : `demo`
 - **Last name** : `user`
 - **Email Address** : `demo@example.com`
 - **Password** : `Ch4ng3!t`
4. Add a Java Agent profile:
 - a. Go to  **Gateways & Agents** > **New Gateway/Agent**, and a Java Agent with the following values:
 - **Agent ID** : `java-agent`
 - **Password** : `password`
 - **Application URL** : `http://agent.example.com:80/app`
 - b. Click **Done**
5. Add a policy set and policy:
 - a. On the agent profile page, make sure that **Use Policy Authorization** is selected.
 - b. Go to **Policy Set** > **Add**. The AM UI is displayed, on the **New Policy Set** page.
 - c. Add a policy set with the following values:
 - **Id** : `PEP`
 - **Resource Types** : `URL`

d. In the policy set, add a policy with the following values:

- **Name** : PEP-policy
- **Resource Type** : URL
- **Resource pattern** : *://*:*/*
- **Resource value** : *://*:*/*

e. On the **Actions** tab, add actions to allow HTTP GET and POST .

f. On the **Subjects** tab, remove any default subject conditions, add a subject condition for all Authenticated Users .

6. Assign the new policy set to the agent profile:

a. Return to the agent profile page on the Identity Cloud Admin UI, and refresh the page.

b. In **Policy Set**, select PEP to assign the PEP policy set to the agent profile.

7. Test the setup:

a. Log out of Identity Cloud, and clear any cookies.

b. Go to `http://agent.example.com:80/app` . The Identity Cloud login page is displayed.

c. Log in to Identity Cloud as user `demo` , password `Ch4ng3!t` , to access the web page protected by the Java Agent.

Was this helpful?  