ForgeRock Identity Cloud Guide

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 Identity Cloud without changing the architecture of the agent-based model.

The examples in this document are based on the version of Identity Cloud that was available when Web Agent 5.9 was released. As Identity Cloud evolves, the examples in this document will be updated to reflect the changes.

Example Installation for This Guide

Unless otherwise stated, examples assume the following installation:

- Web Agent is installed on `http://agent.example.com:80` in the `alpha` realm. For more information, see Install Web Agent.

- Identity Cloud is installed with the default configuration described in the Identity Cloud Docs.

Find the value of the following properties:

- The root URL of your Identity Cloud. This guide uses
  `https://tenant.forgeblocks.com:443`.

- The 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 Web Agent and the Identity Cloud

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 Web Agent with the
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
Web Agent, and the agent's interaction with Identity Cloud to enforce resource-based
policies.
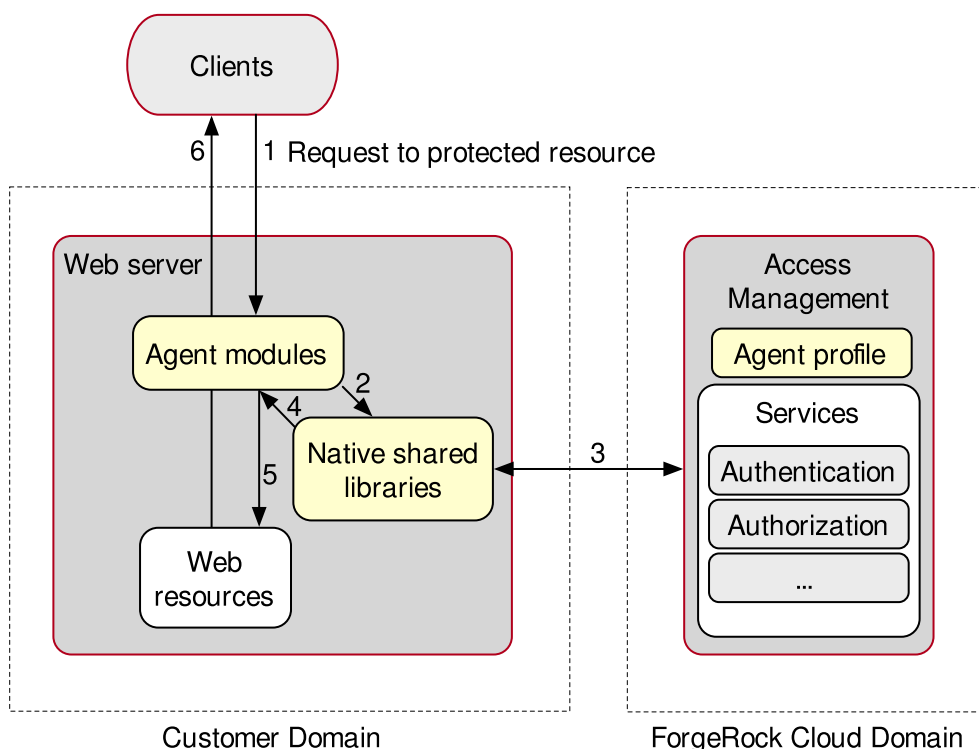
For information about the Identity Cloud, see the Identity Cloud Docs.

Enforce Policies From Identity Cloud

This example sets up Identity Cloud as a policy decision point for requests processed by Web Agent. For more information about Web Agent, see the User Guide.

1. Set up Identity Cloud:

   a. Install Identity Cloud with the default configuration in Example Installation for This Guide, as described in the ForgeRock Identity Cloud Docs.

   b. Log in to the Identity Cloud as an administrator.

   c. Make sure that you are managing the `alpha` realm. If not, click the current realm at the top of the screen, and switch to the `alpha` realm.

   d. In the platform console, go to 🪪 Identities > Manage > Alpha realm - Users, and add a new user with the following values:

      - **Username** : `demo`

      - **First name** : `demo`

      - **Last name** : `user`

      - **Email Address** : `demo@example.com`

      - **Password** : `Ch4ng3!t`

2. Set up Access Management in Identity Cloud:

   a. Go to the alpha realm in the AM console:

      i. In the platform console, click Native Consoles > Access Management. The Access Management console is displayed.

      ii. Make sure that you are managing the `alpha` realm. If not, click the current realm, and switch to the `alpha` realm.

   b. Add a Web Agent:

      i. Click Applications > Agents > Web, and add an agent with the following values:

         - **Agent ID** : `web-agent`

         - **Agent URL** : `http://agent.example.com:80`

         - **Server URL** : `https://tenant.forgeblocks.com:443/am`

         - **Password** : `password`

      ii. On the AM Services tab, set the following values:

         - **AM Conditional Login URL**:
           `|\https://tenant.forgeblocks.com:443/am/oauth2/authorize?realm=/alpha`

           Note the `|` at the start of the URL.

         - **Policy Evaluation Realm** : `/alpha`

- **Policy Set** : PEP

c. Click 🔑 Authorization > Policy Sets, and add a new 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** : `*://*:*/*`

   This policy protects all web pages.

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`.

3. Set up Web Agent:

a. Create a text file for the agent password, and protect it. For example, use commands similar to these, changing the password value and path:

   1. Unix
   2. Windows

```
$ cat > /tmp/pwd.txt
password
CTRL+D

$ chmod 400 /tmp/pwd.txt
```

```
C:> 'password' | Out-File -Encoding ascii pwd.txt
```

   In Windows Explorer, right-click the password file, for example `pwd.txt`, select Read-Only, and then click OK.

b. Using <u>Install Web Agent</u>, install the agent with the following values:

- **Configuration file [/opt/apache/conf/httpd.conf]** : Enter the path to your Apache configuration file.
- **Existing agent.conf file** : Skip the import, or enter the path to your file.
- **OpenAM URL** : `https://tenant.forgeblocks.com:443/am`

- **Agent URL** : `http://agent.example.com:80`
- **Agent Profile name** : `web-agent`
- **Agent realm/organization name** : `/alpha`
- **Agent Profile password source** : `/tmp/pwd.txt`

c. Restart the agent:

```
$ apachectl -k stop
$ apachectl -k start
```

4. Test the setup:

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

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

    c. Log in to Identity Cloud as user `demo`, password `Ch4ng3!t`, to access the agent.