FORGEROCK®

ForgeRock Identity Cloud Guide
/ Web Agents 5.8

Latest update: 5.8.2.1

,'

,'

Copyright © 2020-2021 ForgeRock AS.

Abstract

Instructions for configuring Web Agents with the ForgeRock Identity Cloud.

Table of Contents

Preface

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.

Example Installation for This Guide

Unless otherwise stated, examples assume the following installation:

- Web Agents are installed on http://www.example.com:80 in the `alpha` realm. For more information, see "*Installing Web Agents*" in the *User Guide*.

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

  Find the value of the following properties:

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

  - The URL of the Access Management component of the ForgeRock 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.

Chapter 1

About Web 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 Web 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 an agent, and the Web Agents's interaction with ForgeRock Identity Cloud to enforce resource-based policies.

Clients

6 | 1 Request to protected resource

Web server

Agent modules

2

4

Native shared
libraries

5

3

Web
resources

Access
Management

Agent profile

Services

Authentication

Authorization

...

Customer Domain

ForgeRock Cloud Domain
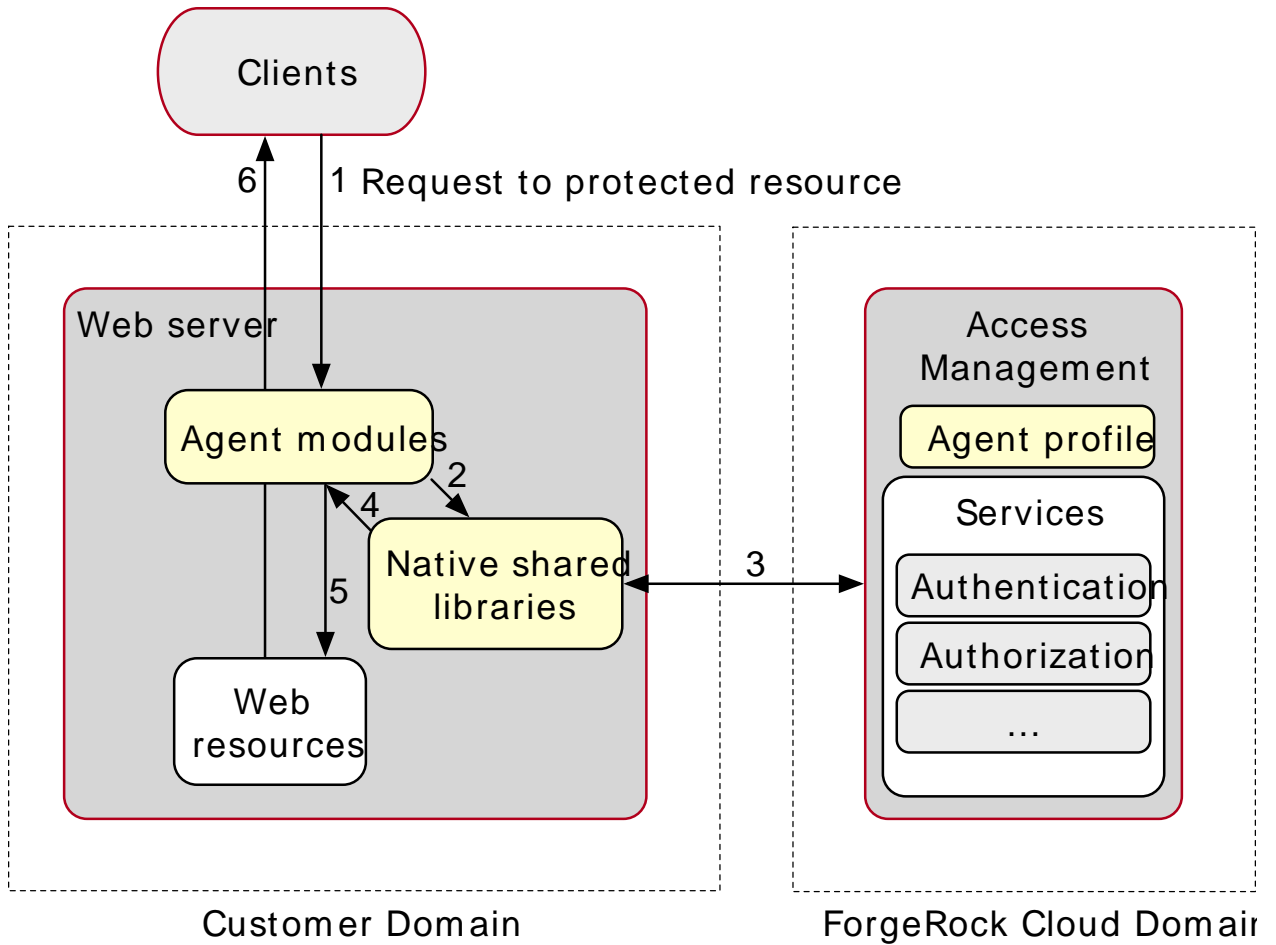
For information about the ForgeRock Identity Cloud, see the ForgeRock Identity Cloud Docs.

Chapter 2
Enforce Policies From ForgeRock Identity Cloud

This example sets up ForgeRock Identity Cloud as a policy decision point for requests processed by Web Agents. For more information about Web Agents, 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 ForgeRock 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, click ⚙ Realm Settings, 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 at the top of the screen, click ⚙ Realm Settings, and switch to the `alpha` realm.

   b. Add an agent:

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

- Agent ID: `web-agent`

- Agent URL: `http://www.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. Add a policy to protect a web page:

i. Click 🔍 Authorization > Policy Sets, and add a new policy set with the following values:

- Id: `PEP`

- Resource Types: `URL`

ii. 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.

iii. On the Actions tab, add actions to allow HTTP `GET` and `POST`.

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

3. Set up Web Agents:

a. Create a text file containing the agent profile password:

   Linux

```
$ echo password > /tmp/pwd.txt
$ chmod 400 /tmp/pwd.txt
```

Windows

```
C:\> echo password > pwd.txt
```

b. Using "*Installing Web Agents*" in the *User Guide*, install an 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://www.example.com:80`

- Agent Profile name: `web-agent`

- Agent realm/organization name: `/alpha`

- Agent Profile password source: `/tmp/pwd.txt`

c. Restart Web Agents; for example:

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

4. Test the setup:

a. In a new browser, go to http://www.example.com:80. The Identity Cloud login page is displayed.

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