Configuring OpenAM

Guide for configuring OpenAM for use with DCDS6.

Table of Contents

- Configuration Changes
  - Add the 'dcds.admin' group:
  - Give the dcds.admin group elevated privileges:
  - Create the "dcdsadmin" user, and make them part of the "dcds.admin" group
  - Remove the 'anonymous' user, and change the demo user's password
  - Enable Email Service
  - Enable User Self Service
  - Set User Session Timeouts
  - Add the CUSTOM-uid header

Prerequisites

- OpenAM Server Setup
- Acquiring OpenAM Packages

Configuration Changes

Add the 'dcds.admin' group:

1. From the OpenAM console, click the Access Control tab.
2. Click the realm name you wish to configure. By default it will be "/ (Top Level Realm)"
3. Click the Subjects tab, then click on the Group tab.
4. Click "New...", and enter "dcds.admin" as the ID then click "OK". You should now see a "dcds.admin" group in the Group table.

Give the dcds.admin group elevated privileges:

1. From the Access Control / (Top Level Realm) screen, click on the Privileges tab, and click on "dcds.admin" in the Privileges table.
2. Check the following privileges
   a. Read and write access to all realm and policy properties
   b. REST calls for reading realms
   c. REST calls for reading subject conditions
   d. REST calls for reading subject attributes
3. Click Save. Your "dcds.admin" group should now have the above privileges. You should see a message saying the Privilege Profile was updated if it worked.
4. Click Back to Privilege(s)

Create the "dcdsadmin" user, and make them part of the "dcds.admin" group

1. Navigate to Access Control / (Top Level Realm), ensure you're on the User tab, and click New....
2. Fill out the following fields: See the tip below regarding encrypting an admin user for use in configuration files.
   a. **ID:** dcdsadmin
   b. **First Name:** DCDS
   c. **Last Name:** Admin
   d. **Full Name:** DCDS Admin
   e. **Password:** (Choose a password)
   f. **Password (confirm):** (Choose a password)
   g. **User Status:** Active

   NOTE: The password for this user will have to undergo an encryption routine so that you can specify this user and password in configuration files. Thus far it has been left as the default testing password, since the encryption tools are outdated.
3. Click OK. You should now see the "DCDS Admin" user in the User table.
4. Click on the DCDS Admin user, then on the Group tab. Select the "dcds.admin(dcds.admin)" entry in the Available column, and click the "Add >" button to apply it to the Selected column. Click Save, and you should see a message saying the Profile was updated.

5. Click Back to Subjects.

> The dcdsadmin user is used by applications that interact with OpenAM, like IWEB and EMAPI. Their configuration files contain encrypted properties for the admin user and the admin password. We have an older build of the user-management-tools application that can encrypt and decrypt strings in the manner OpenAM needs to use them. See OpenAM User/Pass Encryption for details.

Remove the 'anonymous' user, and change the demo user's password

1. Navigate to Access Control / (Top Level Realm), and click the User tab
2. Check the checkbox next to the 'anonymous' user, and click the Delete button
3. Click on the 'demo' user then click the 'Edit' link next to Password. This opens up a change password dialog with the original password box greyed out.
4. Enter a new password and click OK, and close the dialog.

Enable Email Service

1. Navigate to the Email Service configuration; Configuration Global Email Service
2. Complete the configuration using the following settings:
    a. Leave the default Email Message Implementation Class (org.forgerock.openam.services.email.MailServerImpl)
    b. Mail Server Host Name – hostname of corporate SMTP server, or for gmail: smtp.gmail.com
    c. Mail Server Host Port – port SMTP server is running. For gmail: 465
    d. Mail Server Authentication Username – SMTP account username. For gmail: username@gmail.com
    e. Mail Server Authentication Password – SMTP account password
    f. Select SSL if appropriate. For gmail, select SSL.
    g. Email From Address – Address to use as the ‘from’ account. Some SMTP servers do not allow this, for example gmail does not and will use the account credentials for the ‘from’ field.
    h. Email Attribute Name – property representing the user’s email address. Default for OpenAM is ‘mail’
    i. Email Content – content body of email. Leaving it blank will produce an email with just the forgotten password link.
    j. Email Subject – Subject of the email to be sent to users. For example “Reset your DCDS password”
3. Save

Enable User Self Service

User Self Service consists of two functions; user self-registration and forgot password. Only the forgot password functionality is to be enabled.

1. Navigate to the User Self-Service configuration; Configuration Global User Self Service
2. Select the checkbox for Forgot Password for Users.
3. Leave the defaults.
4. Save.

Set User Session Timeouts

The session timeout is the time before a token becomes invalid; the default is 30 minutes and should be increased to prevent user session interruption.

1. Navigate to the Session Configuration; Configuration Global Session
2. Under Dynamic Attributes, set Maximum Session Time and Maximum Idle Time. The time is in minutes, so if a 24 hour session limit is desired, set this field to “1440”
3. Click Save

Add the CUSTOM-uid header

NOTE: Configure after setting up the agent

1. Navigate to Access Control / (Top Level Realm), and click the Agents tab
2. Click on the Agent you configured for the API
3. Click on the Application tab
4. Scroll down to the Profile Attributes section

a. Profile Attribute Fetch Mode : HTTP_HEADER
b. New Value : uid
c. Custom Value : CUSTOM-uid
d. Click Add

5. Click Save

> The username associated with the token making the request is passed to the API in the header. This provides further security as the user is validated to ensure he/she has permissions to request or post information to the API.