eHealth Framework

How to configure permission assignments for new users

Imprint

InterComponentWare
Altrottstraße 31
69190 Walldorf
Tel.: +49 (0) 6227 385 0
Fax.: +49 (0) 6227 385 199

Contents

1 Overview

When new users are created within the eHF usermanagement module, permissions can be automatically assigned to these new users.

This document describes how to do this. It further motivates the underlying use case, explains where to configure these permission assignments and mentions the default configuration. Finally the document covers the possible configuration options.

Motivation for User Permissions

Typically, an eHF-based application needs to assign permissions to newly created users. Otherwise, a newly created user account would be virtually useless. Therefore, the eHF usermanagement module provides the ability to define an initial set of permissions that are assigned to a user account when it is created. Likewise, the same set of permissions is revoked from the user account, when the user is deleted

Note: If a user is deleted, only the permissions from the default configurations will be revoked. User permissions that have been assigned after creation of his account, will remain unchanged in the system.

2 Tasks

This chapter describes the relevant tasks that are necessary to define the initial permission assignments for a newly created user. First, the set of permissions, called a 'permission profile', must be defined. After that, the permission assignments must be configured for the newly created user .

2.1 Definition of permission profile

In the first step, the initial set of permissions must be defined in a permission profile.

A permission is defined as a target-action pair specifying an operation on one or more protected resources. Typically, protected resources within an eHF-based application are domain object instances, domain object types or method calls. Other resource types like URLs, etc. are also possible.

An action is an operation performed on a target resource. Restrictions are supported as well. For further information on permissions please refer to the *eHF Reference Documentation, chapter 15.3 'Authorization'.*
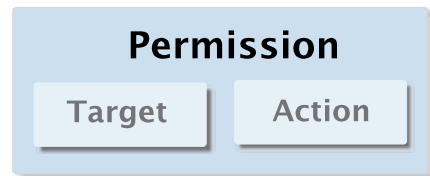
Figure 1: Structure of a permission

Permission profiles are defined in xml files (the name of these files are arbitrary) in the bootstrap resource folder of your assembly. In an eHF assembly, these files are located in `src/main/resources/META-INF/ehf-assembly/bootstrap` . The following code snippet shows the structure of this xml file:

```xml
<?xml version="1.0" encoding="UTF-8"?>
<authorization>
    <namedProfiles>
        <profile>
            <permission>
                <target> ... </target>
                <actions>
                    <action> ... </action>
                    <action> ... </action>
                </actions>
            </permission>
            <permission>
                ...
            </permission>
        </profile>
        <category>...</category>
        <name>...</name>
    </namedProfiles>
    <namedProfiles>
        ...
    </namedProfiles>
    ...
```

```
</authorization>
```

All relevant permissions must be grouped in a permission profile. A permission profile (see XML tag `<namedProfiles>`) is uniquely identified by its name and its category.

In case you need more information, please refer to the *eHF Reference Documentation, chapter 15.3 'Authorization'*.

2.2 Assign permissions to a newly created user

The following steps are necessary to assign permissions to a newly created user:

1. Search for the file `ehf-system-context.xml` in your assembly, located in `src/main/config`.

2. In the file navigate to the configuration of the bean named `profileAssignmentHolders`.

3. If the configuration is not available, add the following code snippet:
   ```xml
   <util:list id="profileAssignmentHolders">

   </util:list>
   ```

4. Verify the configured permission assignments.

5. Configure your required permission assignment for a newly created user by adding the following code snippet for each assignment within the bean configuration named `profileAssignmentHolders`:

   ```xml
       <bean class="com.icw.ehf.usermgnt.security.authr.
   ProfileAssignmentHolder">
           <property name="profileName" value="<name_of_profile>" />
           <property name="profileCategory" value="<name_of_category_of_profile>" />
           <property name="principalSuffix" value="<suffix_of_principal>" />
       </bean>
   ```

   The bean's properties are:

   - `profileName` [mandatory] - name of the profile
   - `profileCategory` [mandatory] - category of the profile
   - `principalSuffix` [optional] - if this property is not set, the profile will be assigned to the default principal of the user, otherwise to a new principal with the name *<name_of_default_principal>_<principalSuffix>*.


> ⚠️ **Important:** Be aware of the fact that the profile used must be defined in your configuration.

---

6. In order to assign more than one permission profile to a principal, you have to define several beans of the class `com.icw.ehf.usermgnt.security.authr.ProfileAssignmentHolder`.

In order to get a better understanding of this configuration, a short description of permission assignments follows below:

A principal represents an identity of a user. A user can have more than one principal. Every principal gets permissions assigned. That means, that a user gets assigned all permissions that are assigned to his principals.
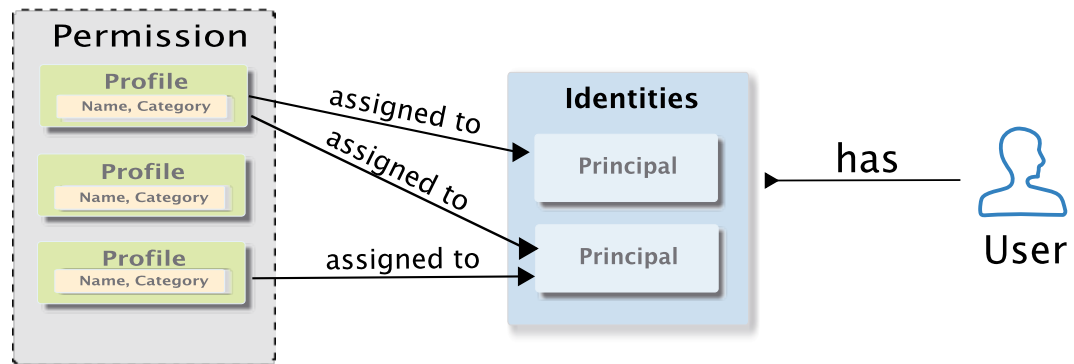
Figure 2: Concept of a permission assignment.

The example configuration in the eHF Assembly

The following code snippet shows an example configuration in the eHF Assembly:

```
<util:list id="profileAssignmentHolders">
    <bean class="com.icw.ehf.usermgnt.security.authr.ProfileAssignmentHolder">
        <property name="profileName" value="OWN-USR" />
        <property name="profileCategory" value="FUNCT" />
    </bean>
    <bean class="com.icw.ehf.usermgnt.security.authr.ProfileAssignmentHolder">
        <property name="profileName" value="OWN-SERVICE-PIN" />
        <property name="profileCategory" value="FUNCT" />
        <property name="principalSuffix" value="SERVICE-PIN" />
    </bean>
</util:list>
```

This configuration specifies the assignment of:

- the permission profile *OWN-USR* to the principal representing the identity of a newly created user.
- the permission profile *OWN-SERVICE-PIN* to the principal with the name `<name_of_the_default_user_principal>_SERVICE-PIN`.