Holder group login

Introduction

In some organizations is necessary to assign roles that affect only a part of the structure, for instance, a department, a division or a country. A **Holder Group** can be defined as a collection of entities (referred to as "holders") that share similar characteristics, roles, permissions, or access requirements. The concept of a Holder Group simplifies the management of identities by enabling administrators to apply policies, assign roles, and manage permissions at the group level rather than individually.

The Soffid federation allows a new way to login, the **Holder group login**. This new way, allows the user to login to applications, Service Provider, indicating with which group the user wants to log in. Soffid will share with the application the roles and permissions according to the selected group.

If you want an application to allow Holder group login, the option Ask for group membership after authentication of the Service Provider must be activated (Yes option selected).

Once the user has logged in using the federation, Soffid will share with the Service Provider application the following information:

- **Holder group**: Group selected by the user when logging in.
- **Roles list**:
  - Roles directly assigned to the user.
  - Roles assigned to the user in compliance with a Role Assignment Rule.
  - Roles assigned in the group selected by the user when logging in.
- **Scope**: the scope will be shared when you try to log in using OpenID-Connect.

How Holder group login works?

1. The user is not logged in to the Identity Provider.

1.1. The user type the user and password into the Identity Provider.

1.2. The Identity Provider validates the user credentials, and requires a 2FA if it is necessary.

1.2.1. If the credentials are not correct, an error message is displayed.

1.2.2. If the credentials are correct, the Identity Provider get a list of all groups to which the user can log in. This list is obtained by selecting all groups, primary and/or

secondary, that have as type one with Rol holder Yes. The groups are not repeated in this list.

1.2.2.1. If there is no group with these characteristics, the Identity Provider automatically logs the user, and shares the data with the Service Provider.

1.2.2.2. If there is only one group with these characteristics, the Identity Provider automatically logs the user into this group, and shares the data with the Service Provider.

1.2.2.3. If there is more than one group, the Identity Provider displays a list of the groups for the user to select which one to log in to. Here the user selects the group and logs in, then Identity Provider shares the updated data with the Service Provider.

2. The user is already logged in to the Identity Provider.

2.1. The user login to a new application, Service Provider.

2.2. The Identity Provider checks if there are any additional adaptive rules required to perform the login.

2.2.1. If the credentials are not correct, an error message is displayed.

2.2.2. If the credentials are correct, the user logs in to the application with the group to which the user was previously logged in. The Identity Provider shares the updated data with the Service Provider, so if there have been any changes in the user's roles, these updates are reflected in the shared data.

Service providers that allow Holder group login

The following Service Providers allow you to configure the login with Holder group

- SAML
- SAML API client
- OpenID-Connect
- CAS client

Revision #19
Created 15 January 2025 10:51:59
Updated 20 January 2025 10:01:50