Learn More About Claims and Claims Mapping

Abstract

This document provides information about the claims, claims mapping and claims based identity process.

October 2022

Revisions

Date	Description
October 2022	Initial release

Acknowledgments

Author: D M Vinod Kumar

Support: NA

Other: NA

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

This document may contain certain words that are not consistent with Dell's current language guidelines. Dell plans to update the document over subsequent future releases to revise these words accordingly.

This document may contain language from third party content that is not under Dell's control and is not consistent with Dell's current guidelines for Dell's own content. When such third-party content is updated by the relevant third parties, this document will be revised accordingly.

Table of contents

Executive summary

Note: This section is required for Reference Architectures, Best Practices guides, and Technical White Papers. It is optional for Deployment and Configuration guides.

The executive summary includes a problem statement and the Dell Technologies solution that is detailed in the remainder of the paper. It should include key findings and information that gives the reader insight as to why they would be interested in this solution.

1 What is Claims?

Claims can contain information about the user, roles, or permissions, useful to build flexible authorization model. In authentication, we usually think of claims as assertions about a user, as asserted by the Identity Provider. For example, a claim list can have the user’s name, user’s e-mail, user’s age, user's authorization for an action.

2 Claims-Based Identity Process

The claims-based identity mechanism can be used to build authentication and authorization process in an application. Claims-based identity depends on trust relationships being established between those making the claims and any relying parties. The following figure illustrates a SP initiated SSO and IdP initiated SSO.

SP Initiated SSO:

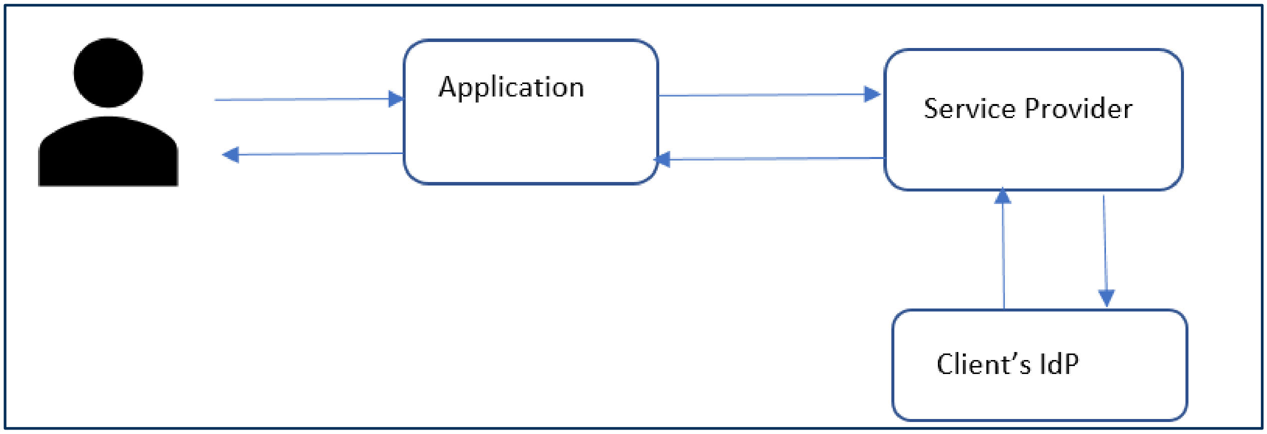


Figure 1 SP Initiated SSO

Service Provider (SP) initiated SSO starts when a user tries to access an application at the service provider end but hasn't yet authenticated from IdP. A user may have visited the site directly. Once the SP sees that the user does not have any browser session active, it will redirect them to the Identity Provider (IdP) asking for authentication request.

1. Process of SP Initiated SSO:

   a. User is trying to access an application.
   b. Application sends a request to the service provider.
   c. The request is redirected to the Client's IdP. The Client's IdP authenticates the request. For more information on how authentication works, refer to the topic: **How does SP Initiated Authentication Work?**
   d. After authentication is successful, the IdP sends the claims in response.
   e. Application validates the user, and the user is granted access.

2. How does SP Initiated Authentication Work?

   Suppose a user initiates the authentication process by clicking on a login button within the application. The application will generate a request ID and send those values along with the SAML authentication request to the Identity Provider via the browser.

   The application will store the request ID. When the Identity Provider returns a SAML response it will include the request ID provided by the application. The application will then check those values against the stored values to ensure a match.

IdP Initiated SSP:

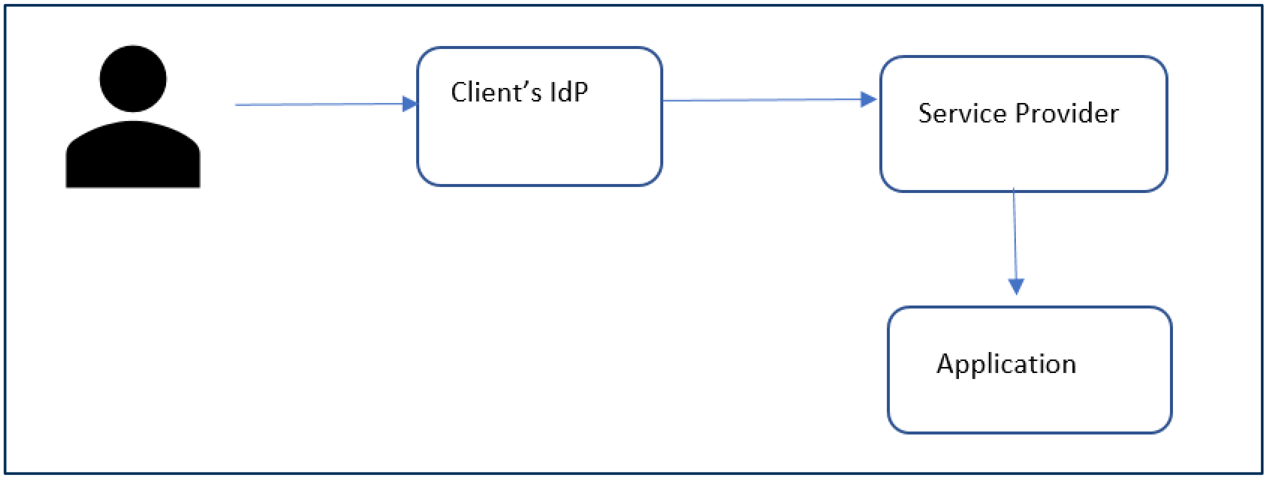


Figure 2 IdP Initiated SSO

Identity provider (IdP) initiated SSO involves the user clicking on a button in the IdP and then being forwarded to a SP along with a SAML message containing an assertion. This flow would typically be initiated by a page within the IdP that shows a list of all available SPs that a user can login to.

1. Process of IdP Initiated SSO:

   a. User will send a request to the Client's IdP for authentication. For more information on how authentication works, refer to the topic: **How does IdP Initiated Authentication Work?**
   b. After successful authentication, the user will post the claims to the service provider.
   c. The application validates the user and access is granted to the user.

2. How does IdP Initiated Authentication Work?

   Suppose a user successfully logs into their Identity Provider, they navigate to the dashboard which displays a variety of Service Providers the user can access, and they click on the desired Service Provider.

   The Identity Provider then creates an SSO response and a SAML 2.0 Assertion which contains authentication details and information about the user. The Service Provider receives the SSO response from the Identity Provider via the browser, validates the SAML 2.0 Assertion, and generates a session for the user.

2.1 Types of Claims

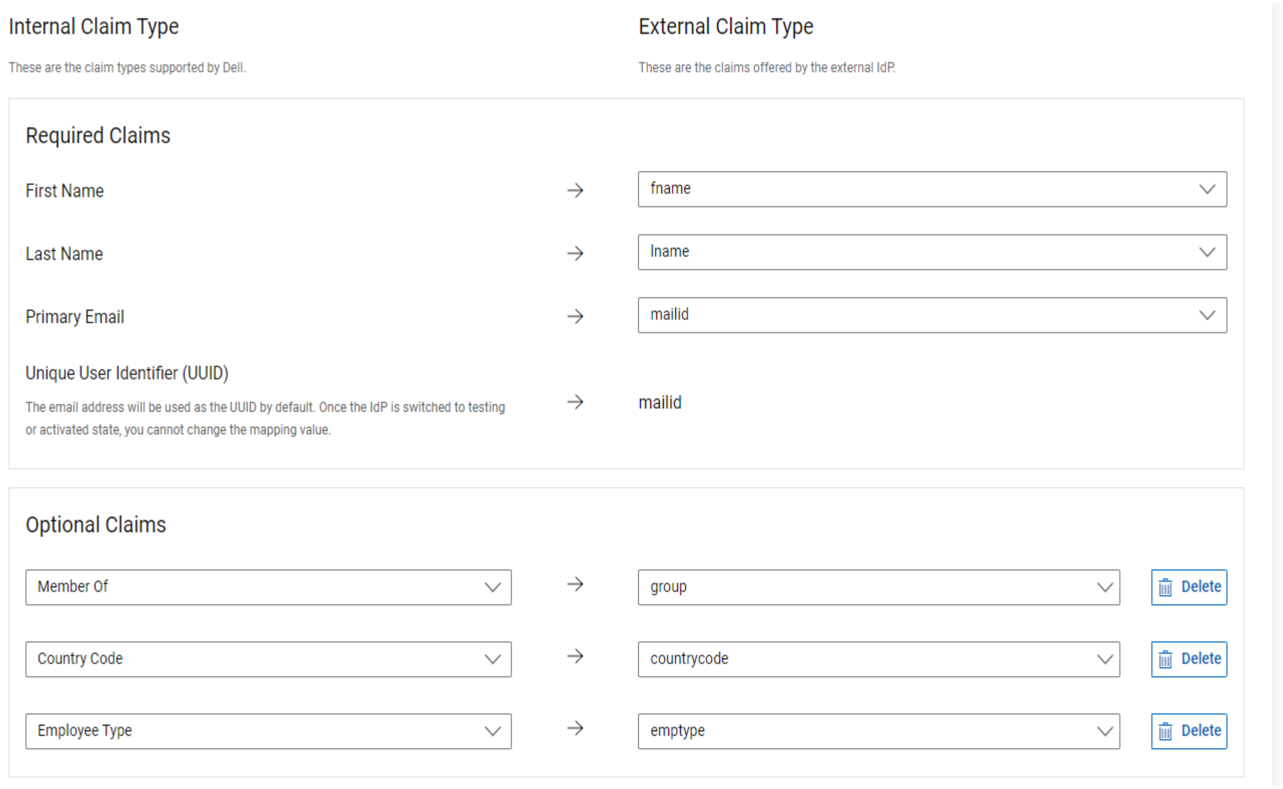
Internal Claims and External Claims are the two types of claims. Internal claims are supported by Dell. External claims are the claims offered by external IdP. The required claims section consists of Primary Email, First Name, Last Name and Unique User Identifier (UUID).

Note: The email address will be used as the UUID by default. Once the IdP has been registered, the mapping value cannot be changed.

The Optional Claims section consists of Country Code, Member Of and Employee Type. You must select the appropriate claim list from the drop-down to map the required claims and optional claims. In case the user has uploaded a IDP meta data file then the External Claims will be read from the meta data file and will be pre populated in the external claims dropdown.

2.2 Claims Mapping

We have Internal Claims and External Claims as shown in the below image for example.



Internal Claim Type

These are the claim types supported by Dell.

External Claim Type

These are the claims offered by the external IdP.

Required Claims

First Name → fname

Last Name → lname

Primary Email → mailid

Unique User Identifier (UUID)

The email address will be used as the UUID by default. Once the IdP is switched to testing or activated state, you cannot change the mapping value. → mailid

Optional Claims

Member Of → group

Country Code → countrycode

Employee Type → emptype

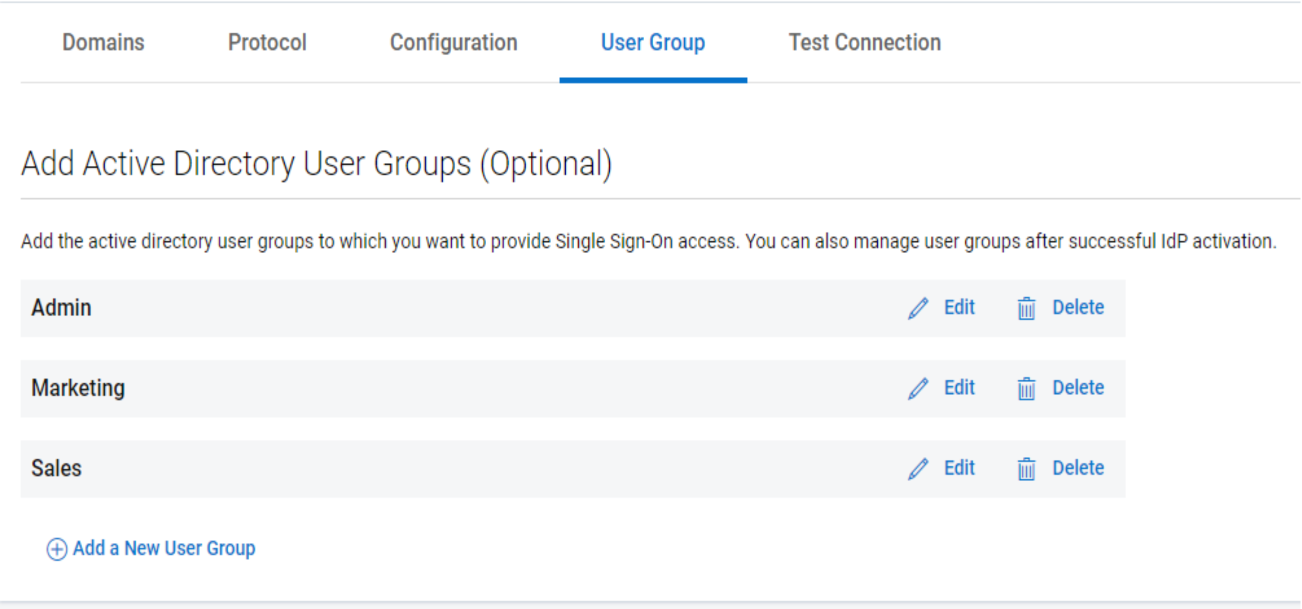
The claim names like First Name, Last Name, Primary Email and Unique User Identifier(UUID) are the required mandatory claims. Member Of, Country Code and Employee Type are the optional claims from Dell's End.

Once the IDP metadata has been uploaded the dropdowns for External Claim Type will be populated with all the possible claim names from the clients IDP. In case the parsing is not successful then these names can be keyed in manually.

Now the user has to map the External Claim Name from his IDP metadata(fname in the above example prepopulated from parsing the IDP metadata) to the Firstname claim on Dell's end.The same needs to be done for the rest of the required claims.

Unique UserIdentifier(UUID) is defaulted to the value selected for Primary Email. But at the time of registration of IDP you can select any other claim as well. Once the IDP has been Registered the user will not have the option to modify the UUID mapping.

The Member Of claim is related to the set of filtered groups to which the user belongs to. In the above example its mapped to a claim named group. After configuring this mapping and registering the IDP the user will be taken to the next screen where he will define the list of filtered groups as shown below.



Add Active Directory User Groups (Optional)

Add the active directory user groups to which you want to provide Single Sign-On access. You can also manage user groups after successful IdP activation.

Admin
Marketing
Sales

Clicking on “Add a New User Group” IAM expert can add the filtered list of AD groups that will be validated and passed as part of the Member Of claim for the user.

Applications after configuring the AD groups here can then define rules for Authorization of the user based on the group that he is Member Of.