

Learn How to Use Service Provider (SP) Metadata

Abstract

This document provides instructions on how to use and download Service Provider (SP) Metadata.

November 2023

Revisions

Date	Description
November 2023	Revision

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.

Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [12/14/2023]

Table of contents

Revisions.....	2
Acknowledgments.....	2
Table of contents	3
Executive summary.....	4
1 What is SP Metadata?.....	5
2 Downloading SP Metadata.....	6

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 SP Metadata?

The Service Provider (SP) metadata .xml file contains services, keys, and URLs defining the SAML endpoints. You can use your IdP's SP metadata file generator to generate the SP metadata XML file. This metadata file is sent to all the IdP's you want to enable single sign-on with. Similarly, each IdP makes its own metadata available to import it into your application.

2 Downloading SP Metadata

To download the service provider metadata file,

1. Click on **Download SP metadata file (XML)**
OR
Click on **Copy SP Metadata URL**

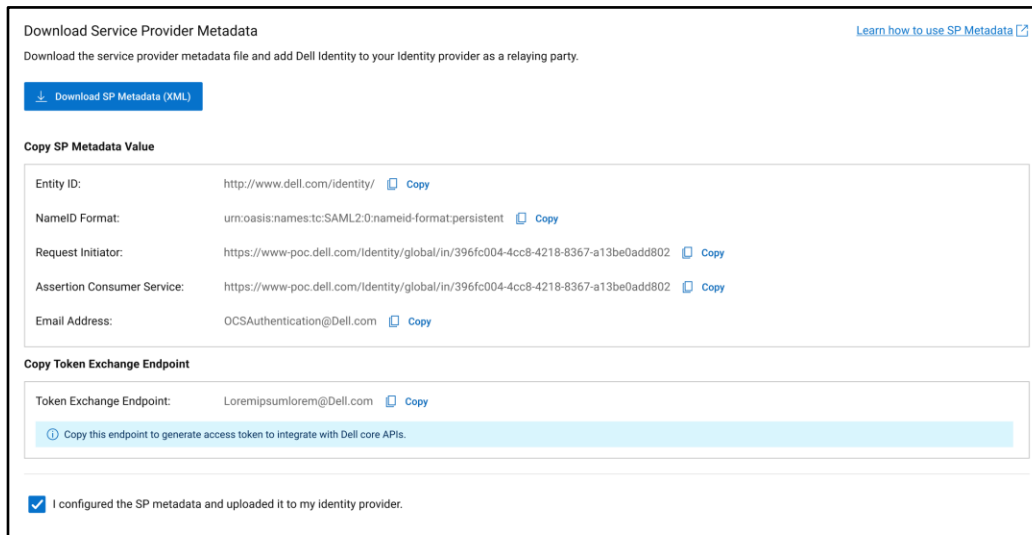


Figure 1 Download SP Metadata

You can copy the following SP metadata values:

a. NameID Format:

SP and IdP use Name Identifiers to pass information about the users. The name identifier must have a specific format so that the service providers can identify the name based on the format that is returned by the IdP. This format can be:

- Unspecified
- emailAddress – e.g., john@company.com
- X509SubjectName – e.g. CN=john,O=Company Ltd.,C=US
- WindowsDomainQualifiedName – e.g., CompanyDomain\John
- Kerberos – e.g., john@realm

A persistent identifier is an opaque service-specific identifier which must include a pseudo-random value and must not be traceable to the actual user. This is a privacy feature.

A transient identifier is an opaque identifier which is temporary.

b. Entity ID:

Entity ID is used to identify entities that provide SAML-based services and looks like a URL.

c. Request Initiator:

This protocol is used to ask that a service provider supporting a federated authentication protocol produce a request for authentication using options or assumptions. It is assumed that the user wields a standard HTTP user agent. The protocol is specified between the user agent and the service provider. Any technical means may be used to cause the user agent to submit a request using this protocol, including static or dynamic links on any web site, client-side scripting, manual entry by a user, etc.

The request initiation protocol consists of a single HTTP [RFC2616] request/response, a normative request followed by an arbitrary response from the service provider. This response may be a request for authentication using a selected protocol (the format of which is left to the definition of that protocol), or it may be a refusal to perform the requested action or any other response the service provider deems appropriate.

In the event of failure, the response must inform the user as to the nature of the problem or prompt for additional information as required. For example, if the request does not identify the identity provider to use, the response could be in the form of a request to a discovery service, per [IdPDisco].

d. Assertion Consumer Service:

Assertion Consumer Service specifies the URL of the Assertion Consumer Service where the Identity Provider sends the response. The value must correspond to the endpoint in the Service Provider metadata.

2. Upload the SP metadata file or paste the SP metadata values in your application.
3. Set up Dell Identity as a relying party under your IdP.
4. Select the **'I have set up the SP Metadata and have uploaded it to my Identity provider'** checkbox and click **Next**.