How to Set Up Single Sign-On

Abstract

This document provides instructions on how to setup Single Sign-On (SSO) experience.

December 2023

Revisions

Date	Description
December 2023	Revision 4

Acknowledgments

Author: Vedam Venkateshwara

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. [10/27/2022]

Table of contents

Rev	risions	2
Ack	nowledgments	2
Tab	le of contents	3
Exe	cutive summary	4
1	Setting Up the Single Sign-On (SSO) Experience for your Organization's identity Provider	5
2	Managing Identity Administrator	21

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.

4

The service provider or Dell identity group invites IAM expert. IAM expert receives an invitation email with a link to validate his credentials. For more information, refer to the Topic 1: **Sign In and Verify your Account** of <u>Email Invitation</u> document.

After your account is verified, you will be redirected to the External Federation Portal.

If the page **Manage Domain** appears, then follow **Section 1** of <u>Domain Management</u> document or else follow Step 1 of this document.

To enable an SSO experience for the user, perform the following steps:

1. Click Create IdP Group.

	🖉 Michael 🗸
< Back to dashboard	
Welcome John Smith!	
You have been invited to configure SSO for the domain coke.com. To verify domain ownership, you can create a new idP group.	
① This invitation will be valid for 30 days.	
Requested Domain Date Requested coke.com 11 January 2022	
Need technical support? Please reach out to your regional Dell customer technical support teams.	



5

- 2. Perform the following:
 - a. In the IdP Group Name field, enter the name of the IdP Group.
 - b. Click Create IdP Group.

D¢	XLT echnologies	🖉 Michael 🗸
	< Back to dashboard	
	Welcome John Smith!	
	You have been invited to configure SSO for the domain coke.com.	
	To verify domain ownership, you can create a new idP group.	
	() This invitation will be valid for Create IdP Group	
	Requested Do IdP Group Name coke.com Enter a IdP group name	
	Cancel Create IdP Group	
	Need technical support? Please reach out to your regional Dell customer technical support teams.	

Figure 2 IdP Group Name

3. You will be redirected to the Manage Domain page as shown below. You can choose to either verify the primary domain or go to the dashboard by clicking on the "Back to Dashboard" button. To know more on how to verify a domain, refer **Section 2** of <u>Domain Management</u> document.

	🖉 Michael	×
Back to dashboard A second secon		
Manage Domain	Learn how to add and verify domain 🖸	
All the domains added to this organization are listed here. Click Verify Domain to confirm the domain ownership. Only verified domain will be associated with the IdP. The Delete button will be disabled if the domain is associated with an IdP. If you want to enable the Delete button, dissociate the domain from that IdP.		
coke.com Verify Domain	Assosiated to	
▲ Warning: To add a new domain you should verify your invited domain first.	×	
+ Add Domain		
Need Help? You can always reach us by email on dci.developerexperience@dell.com. We'll get back to you shortly!		

Figure 3 Verify Domain

4. Click Register IdP for SSO

D≪LL Technologies		🧟 🧟 Michael 🗸
Currently viewing: IdP Group 1 Switch IdP group		Invite and Requests
Single Sign-On (SSO) Setup	Manage Domain	Manage Administrator
Let's start setting up the Single Sign-On experience for your organization's Identity Important! Ensure that you perform the following steps before setting up the IdP \sim	y provider (IdP).	
 In case of SAML and OIDC, go to manage domain to add or verify email domain. Prior to the SSO being active, the email domain need In case of SAML and OIDC, set up Dell Identity as a relaying party under your Identity provider by downloading the SAML service prov Redirect URI. This step is required for the registration of an IdP. Make sure that you have access to IdP metadata from your Identity provider. This information is necessary since you need the config In the case of SAML, look for the list of Dell applications that support IdP-Initiated SSO in Supported applications. 	eds to be connected to the vider metadata file or cop iguration details for the Id	e IdP. oying the OIDC IP registration.
① You should be able to test SSO connection before activiating it for your organization's domains. Learn More		
Register IdP for SSO Learn how to set up SSO		
Need technical support? Please reach out to your regional Dell customer technical support teams	IS.	

Figure 4 Register IdP for SSO

- 5. In the **Select Domain** Tab, perform the following:
 - a. In the **SSO Configuration Name** field, enter the name for the SSO configuration record.
 - Select the Domain Name associated with the IdP.
 If you cannot find the domain you want, then click Manage Domain. For more information on adding a domain, refer to the Step 2.a of <u>Domain Management</u> document.
 - c. Click Next.

7

	nologies				Aich
< Back t	to dashboard				
Sing	gle Sign-On (SSC	D) Setup			
Setting	up configuration for SSO exper	rience			
	⊘ Select Domain	Select Protocol	Register IdP	Add User Group	Activate
Provi	de a Display Name				
SSO Coi	nfiguration Name				
XYZ 2	2022				
Enter the r	name for the SSO configuration record				
Linui ulei	name for the 656 configuration record.				
Select Ensure 1 ① Ca	: Domain(s) that atleast one verified domai ant find the domain you are looking xyz.com	in is selected to activate the IdP. g for? To add or verify domain, go to <u>Manage</u>	<u>2 Domain</u>		
Select Ensure 1 ① Ca	: Domain(s) that atleast one verified domai ant find the domain you are looking xyz.com xyz.uk	in is selected to activate the IdP. I for? To add or verify domain, go to <u>Manage</u>	: Domain		
Select Ensure 1 ① Ca	: Domain(s) that atleast one verified domai ant find the domain you are looking xyz.com xyz.uk sub.xyz.com	in is selected to activate the IdP. g for? To add or verify domain, go to <u>Manage</u>	: Domain		
Select Ensure 1 ① Ca	: Domain(s) that atleast one verified domai ant find the domain you are looking xyz.com xyz.uk sub.xyz.com	in is selected to activate the IdP. g for? To add or verify domain, go to <u>Manage</u>	: Domain		Cancel Next



Note: Ensure that at least one domain is selected to activate the IdP.

 In the Select Protocol tab, perform the following: By default, SAML 2.0 is selected. For more information about SAML, click on Learn more about SAML here.

For OIDC, refer Page 17.

a. Select the authentication method.

SP--initiated SSO is selected as the authentication method by default, and it cannot be changed. You can select IdP initiated SSO if your applications are listed in supported applications. For more information on SP-initiated SSO and IdP-initiated SSO, click on Learn more about SP & IdP initiated flow.

- b. Import the Identity Provider Metadata in one of the following ways:
 - Upload IdP metadata: If you have an IdP Metadata file, select Upload IdP Metadata, and click Upload File. Browse to the location where the IdP Metadata XML file is located and click Open. The IdP metadata file is uploaded.
 - SAML Endpoint URL: Enter the URL of the XML file that holds the federation metadata.
 - Manually Enter Values: If you do not have an IdP Metadata file, select Manually Enter Values.
- c. Click **Download SP Metadata (XML)** to download the metadata file and to set up Dell Identity as your Identity provider. For more information, click on **Learn more how to use SP metadata**.
- d. Copy all the SP metadata values and paste it in the respective fields at your IdP.
- e. After setting Dell Identity as your identity provider, click on I have set up SP metadata and have uploaded to my Identity provider check box.
- f. Click Next

bit is divided Single Sign-On (SSO) Setup ieing up configuration for SDD reperiors Setup configuration for SDD reperiors iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	🖉 Mic					logies	Techn
Single Sign-On (SSO) Setup array a configuration for 500 expension						lashboard	Back to
<pre>character control to to 500 expension</pre>) Setup	e Sign-On (SSO)	Sing
<pre>strain protection of the sector barrent of the sector barrent</pre>					ence	configuration for SSD experies	Setting
• is best burnin • is best Photocol Reptor VP Add Yeer Youp Add					ence	configuration for 550 experies	Setting t
Select a Protocol Concert diverse decemple dece	Ictivate	Add User Group Activate	egister IdP	_	⊘ Select Protocol	Select Domain	(
Outcome and configure the external identity provider that you want to enable.						a Protocol	Selec
• Mat 2.0 Control Accention Markup Language 2.0 (SMAL 2.0) is a version of the SMAL standards and accention and administration markup language 2.0 (SMAL 2.0). Control Accention Markup Language 2.0 (SMAL 2.0). Control Accentio				nable.	ntity provider that you want to en	d configure the external identi	Choose
Security Assection Markup Language 2 0 (AML 20) is a veriou of the SAML standard of SAML standard of the SAML standard of SAML standard standard standard standard standard standard standard standard standa		inect (OIDC)	Open ID Con			ML 2.0	0 9
Select the Authentication Method Learn more about SP2 A BP2 Select the Authentication Method Learn more about SP2 A BP2 Select the Service Provider (SP) occurs when a user attempts to access an application at the SP end and the application is not authenticated by the UPA A user may be directly to the sele. Once the SP confirms that the user does not have any active browser sessions, it will redirect them to the UPA and request authenticated by the UPA A user may be inderectly on the sele. Once the SP confirms that the user does not have any active browser sessions, it will redirect them to the UPA and request authenticated by the UPA A user may be inderectly on the sele. Once the SP confirms that the user does not have any active browser sessions, it will redirect them to the UPA and request authenticated by the UPA A user may be inderectly on themse the SP confirms that the user does not have any active browser sessions, it will redirect them to the UPA and request authenticated by the UPA A user may be inderectly on themse the SP confirms that the user does not have any active browser sessions, it will redirect them to the UPA and request authentication. So the SP confident SSO (Cytoronal) A SelectSP worker (Method SSO (Cytoronal) A SelectSP worker (Method SSO (Cytoronal) Confirme the UPA and deployse as is of all available SPs to which a user can togin. Confirme Service Provider Method SSO Download Service Provider Method SSO Download Service Provider Method SSO Download Service Str Mutadata (Method SSO (Cytoronal) Confirme Service Service Str Mutadata (Mutadata SSO (Cytoronal) Confirme Service Service Service Str Mutadata (Mutadata) Confirme Service	JavaScript end-users.	lows clients of all types, including Web-based, mobile, and JavaScr and receive information about authenticated sessions and end-use OIDC [2]	OpenID Connect all clients, to request a	he <u>SAML</u> standard for <u>rity domains</u> .	2.0 (SAML 2.0) is a version of th <u>ization</u> identities between <u>secur</u>	Assertion Markup Language 2. Ing <u>authentication</u> and <u>authoriz</u> re about SAML 2.0 [2]	Security exchan
SP-Initiated SBO The SP-Initiated SBO The SP-Initiated SBO is selected as the authentication method by default, and it cannot be changed. SSD initiated by the Service Provider (SP) occurs when a user attempts to access an application at the SP end and the application is not authenticated by the SP A user may he directly to the site. Once the SP confirms that the user does not have any active browser assisting, it will refired them to the IdP and request authentication. Image: Initiated SSO (Optional) Image: Initiated SSO (Optional) Image: Initiated SSO (Optional) SSO initiated by an identity Provider (IdP) involves the user clicking a button in the IdP which is 10 SSO initiated by an identity Provider (IdP) involves the user clicking a button in the IdP which is 10 SSO initiated by an identity Provider (IdP) involves the user clicking a button in the IdP which is 10 SSO initiated by an identity Provider (IdP) involves the user clicking a button in the IdP which is 10 Download Service Provider Metadata Download Service Provider Metadata Impl/www.defl.com/identity/ Impl/www.defl.com/identity/ Impl/www.defl.com/identity/ Impl/www.defl.com/identity/ Impl/www.defl.com/identity/ Impl/www.defl.com/identity/ Impl/www.defl.com/identity/ImpleOut4-ccit-4218-8367 at TabeOutd802 ImpleOut4002 ImpleOut4-ccit-4218-8367 at TabeOut48002 ImpleOut4002 ImpleOut4-ccit-4218-8367 at TabeOut48002 ImpleOut4000 ImpleOut4-ccit-4218-8367 at TabeOut48002 ImpleOut4000 ImpleOut4-000	P Initiated flow	Learn more about SP & IdP Initiate			bd	e Authentication Method	Select
or							
In the sensitive source selected as the authentication method by default, and it cannot be changed. Sol initiated by the Service Provider (SP) occurs when a user attempts to access an application at the SP end and the application is not authentication. In the site. Once the SP confirms that the user does not have any active browser session, it will reflerent them to the IdP and request authentication. Image: Statistication of the site. Once the SP confirms that the user does not have any active browser session, it will reflerent them to the IdP and request authentication. Solutions that the user does not have any active browser session, it will reflerent them to the IdP and request authentication. Image: Statistication of the SP confirms that the user does not have any active browser session, it will reflerent them to the IdP and request authentication. Solutions the service Provider (PdP) involves the user clicking a button in the IdP which is forwarded to an SP along with a SAML message containing an assertion. This for usually initiated by a page within the IdP that displays a list of all available SPs to which a user can login. Download Service Provider (Pd Hetadata Site and add Dell Identity to your Identity provider as a relaying party. I conclust of Metadata Value Entity ID: http://www.dell.com/identity/ Com/identity/ Gobal/n/396/c004-4cc84 428 4367 at 3be0add802 Comp Enal Address: OCSAuthentication@Dell.com Com/identity/Gobal/n/396/c004-4cc84 428 4367 at 3be0add802 Comp Enal Address: OCSAuthentication@Dell.com Com/identity/Gobal/n/396/c004-4cc84 428 4367 at 3be0add802 Comp Enal Address: OCSAuthentication@Dell.com Com/identity/Gobal/n/396/c004-4cc84 428 4367 at 3be0add802 Comp Enal Address: OCSAuthentication@Dell.com Com/identity/ Gobal/n/396/c004-4cc84 428 4367 at 3be0add802 Comp Enal Address: OCSAuthentication@Dell.com						or-intiated 550	
sob initiated by the Service Provider (SP) occurs when a user attempts to access an application is the SP and the application is not authenticated by the KP. A user may fail directly to the site. Once the SP confirms that the user does not have any active browser essions, it will redirect them to the IdP and request authentication.			d.	ult, and it cannot be char	s the authentication method by defai	ne SP-initiated SSO is selected as t	0
Or provider tight provider (dP) Involves the user clicking a button in the kP, which is forwarded to an SP along with a SAML message containing an assertion. This is a useful in thated by a page within the kP that displays a list of all available SPs to which a user can login. Download Service Provider Metadata Learn how to use Download Service Provider Metadata Learn how to use a nelsying party. Download Service Provider Metadata Learn how to use Download Service Provider Metadata Learn how to use Download the service provider metadata file and add Dell Identity to your Identity provider as a relaying party. Download Service Provider Metadata Download Service Provider Metadata Download the service provider metadata file and add Dell Identity to your Identity provider as a relaying party. Download Service Provider Metadata Download Service Provider Metadata Download the service provider metadata file and add Dell Identity to your Identity provider as a relaying party. Download Service Provider Metadata Download the service provider metadata file and add Dell Identity () C cay Request Initiator: http://www.pdell.com/identity/global/in/396/f004-4cc8-4218-8367 at 3ba0add802 [Coay Coay care inpauniform@Dell.com [Coay Coay care inpauniform@Dell.com [Coay care inpauniform@Dell.c	have gone	.he application is not authenticated by the IdP. A user may have go am to the IdP and request authentication.	ation at the SP end and t ssions, it will redirect the	npts to access an app ve any active browser	r (SP) occurs when a user attem firms that the user does not hav	tiated by the Service Provider to the site. Once the SP confi	SSO direc
Entry ID: http://www.dell.com/identity/ Copy NameID Format: umcoasis:namest::SAML2:0:nameid-format.persistent Copy Request initiator: https://www-poc.dell.com/identity/global/in/396fc004-4cc8-4218-8367-a13be0add802 Copy Assertion Consumer Service: https://www-poc.dell.com/identity/global/in/396fc004-4cc8-4218-8367-a13be0add802 Copy Email Address: OCSAuthentication@Dell.com Copy Email Address: OCSAuthentication@Dell.com Copy Token Exchange Endpoint: Loremipsumforem@Dell.com Copy I configured the SP metadata and uploaded it to my identity provider. I			relaying party.	our Identity provider as	ta file and add Dell Identity to yo	the service provider metadata)ownloa ⊥
Entry ID: http://www.dell.com/identity/ © copy NameID Format: um:oasis:namest::SAML2:0nameid-format:persistent © copy Request initiator: https://www.poc.dell.com/identity/global/in/396fc004-4cc8-4218-8367-a13be0add802 © copy Assertion Consumer Service: https://www.poc.dell.com/identity/global/in/396fc004-4cc8-4218-8367-a13be0add802 © copy Email Address: OCSAuthentication@Dell.com © copy Copy Token Exchange Endpoint: Loremipsumlorem@Dell.com © copy Copy the endpoint to generate access token to integrate with Dell core APIs.						letadata Value	Copy SF
NamelD Format: um:coasis:names:tc:SAML2:0:nameid/format.persistent [] Copy Request initiator: https://www-poc.dell.com//dentity/global/in/396fc004-4cc8-4218-8367-a13be0add802 [] Copy Assertion Consumer Service: https://www-poc.dell.com//dentity/global/in/396fc004-4cc8-4218-8367-a13be0add802 [] Copy Email Address: OCSAuthenticoation@Dell.com [] Copy Copy Token Exchange Endpoint: Loremipsumforem@Dell.com [] copy Token Exchange Endpoint: Loremipsumforem@Dell.com [] copy @ Copy this endpoint to generate access token to integrate with Dell core APIs.				Сору	http://www.dell.com/identity/	: h	Entity
Request Initiator: https://www.poc.dell.com/identity/global/in/396fc004-4cc8-4218-8367-a13be0add802 Copy Assertion Consumer Service: https://www.poc.dell.com/identity/global/in/396fc004-4cc8-4218-8367-a13be0add802 Copy Email Address: OCSAuthentication@Dell.com Copy Token Exchange Endpoint: Loremipsumforem@Dell.com Opy this endpoint to generate access token to integrate with Dell core APIs. I configured the SP metadata and uploaded it to my identity provider. The following methods are available for importing Identity Provider Metadata. Upload IdP Metadata SAML Endpoint URL Manually Enter Values			Сору	ameid-format:persiste	urn:oasis:names:tc:SAML2:0:na	Format: u	Name
Assertion Consumer Service: https://www.poc.dell.com/identity/global/in/396fc004-4cc8-4218-8367-a13be0add802 Copy Email Address: OCSAuthentication@Dell.com Copy Copy Copy Token Exchange Endpoint: Loremipsumlorem@Dell.com Copy Copy this endpoint to generate access token to integrate with Dell core APis. I configured the SP metadata and uploaded it to my identity provider. The following methods are available for importing Identity Provider Metadata. Upload IdP Metadata SAML Endpoint URL Manually Enter Values 		ladd802 🚺 Copy	4cc8-4218-8367-a13be0	ntity/global/in/396fc0	https://www-poc.dell.com/Iden	Initiator: h	Reque
Email Address: OCSAuthentication@Dell.com Copy Token Exchange Endpoint: Loremipsumlorem@Dell.com Copy Token Exchange Endpoint: Loremipsumlorem@Dell.com Copy Copy Ocspy this endpoint to generate access token to integrate with Dell core APIs. I configured the SP metadata and uploaded it to my identity provider. The following methods are available for importing Identity Provider Metadata. Upload IdP Metadata SAML Endpoint URL Manually Enter Values)add802 🚺 Copy	4cc8-4218-8367-a13be0	ntity/global/in/396fc0	https://www-poc.dell.com/Iden	n Consumer Service: h	Asser
Copy Token Exchange Endpoint: Loremipsumlorem@Dell.com Copy I configured Endpoint to generate access token to integrate with Dell core APIs. I configured the SP metadata and uploaded it to my identity provider. The following methods are available for importing Identity Provider Metadata. Upload IdP Metadata SAML Endpoint URL Manually Enter Values I upload File Only XML files are accepted. P Partner_MBP_Metadata 1 MB Manually Enter Values				🖸 Сору	OCSAuthentication@Dell.com	ddress: 0	Email
Cover Exchange Endpoint: Lorempsumicrengues.com Copy Copy this endpoint to generate access token to integrate with Dell core APIs. Configured the SP metadata and uploaded it to my identity provider. The following methods are available for importing identity Provider Metadata. Upload IdP Metadata SAML Endpoint URL Manually Enter Values Upload File Only XML files are accepted. Protex_MP_Metadata 1108				.		n Exchange Endpoint	Сору То
C Copy this encount to generate access token to integrate with Der Cole APIs. I configured the SP metadata and uploaded it to my identity provider. The following methods are available for importing identity Provider Metadata. Upload IdP Metadata SAML Endpoint URL Manually Enter Values Upload File Only XML files are accepted. P Pather_MB-Metadata 1 MB				Сору	corempsumorem@beil.com	change Endpoint.	TOKEN
I configured the SP metadata and uploaded it to my identity provider. The following methods are available for importing Identity Provider Metadata. Upload IdP Metadata SAML Endpoint URL Manually Enter Values Upload File Only XML files are accepted. Pertner_JBP_Metadata 1 MB				APIS.	ess token to integrate with Dell core i	py this endpoint to generate acces	0.0
The following methods are available for importing Identity Provider Metadata. Upload IdP Metadata SAML Endpoint URL Manually Enter Values				ider.	l uploaded it to my identity provi	figured the SP metadata and u	🗸 I c
Upload IdP Metadata SAML Endpoint URL Manually Enter Values						ing motheral second states in the	Th. 7 "
①r Upload File Only XML files are accepted. Ø Partner_KBP_Metadata 1 MB			es	etadata. Manually Enter V	r Importing Identity Provider Me	ing methods are available for i	UINE follo
Dybad File Only XML files are accepted. Partner_J&P_Metadata 1 M8							_
🖗 Partner, JSP, Metadata 1 1/18					accepted.	Upload File Only XML files are a	1
						tner_ldP_Metadata 1 MB	Ø



D&LLTechnologies		< Back		
Select the Authentication Method		Applications S	Supported	
		# If you can't find the an	indication where you need IdP-initiated SSD, contact the	PDC of the application in your IdP Group
The SP-initiated S50 will be a default authenticat	The SP-Initiated SSO will be a default authentication method and it cannot be changed.			
SP-initiated SSO starts when a user tries to acces have any browser session active, it will redirect th	ss an application at the Service Provider(SP) end, but hasn't yet authenti- nem to the IdP asking for the authentication request.	Application	Relay URL/Target URL	Action
		Premier	https://www.dell.com/account	Сору
IdP-Initiated SSO (Optional)				
Select IdP-initiated flow if your application is lister	ed in Supported Applications.			
Identity Provider (IdP) initiated SS0 involves the shows a list of all available SPs that a user can lo	user clicking on a button in the IdP, which is forwarded to a SP along wit \ensuremath{ogin} to			
Download Service Provider Metada	ita			
Download the service provider metadata file and se	etup Dell Identity as a relying party under your identity provider.			
🛓 Download SP Metadata (KML)				
Copy SP Metadata Value				
Entity ID:	https:///divub.defi.com Copy []			
Assertion Consumer Service:	https://idhub.dell.com/sp/ADS.saml2 Copy			
Email Address:	NAM_SSO_Opu@Dell.com			

Figure 7 IdP Initiated SSO

7. In the **Register IdP** tab, all the fields in the Basic SAML information, Endpoints and Certificate section are auto populated if the IdP metadata file is uploaded.

Claim section.

- a. In the Required Claims section, select the appropriate URLs from the drop-down list in the next fields.
- b. If necessary, select the claim list from the drop-down list for Member Of, Country Code, and Employee Type in the Optional Claims section.
- c. Click Register

Note: If any of the IdP Metadata sections contain errors, you will receive an error message. Ensure That you fix the errors before you register your IdP.

Back to dashboard							
Single Sign-On (SS	O) Setup						
Setting up configuration for SSO experience							
⊘ Select Domain	⊘ Select Protocol	⊘ Register IdP		Add User Group	Activate		
AML Configuration							
Basic SAML Information	A claim is information about a user the SAM attribute Statement in a SAM	hat an identity provider includes in	the token t	hey issue for that user. This informa	tion is typically contained in the		
 Endpoints 	Learn more about claims here	. NORACE.					
 Certificate 	Internal Claim Type			External Claim Type			
Claims	DELL supports the following claim ty	pes.		These are the claims offered by	the external IdP;		
	Required Claims						
	Primary Email	\rightarrow	htt	p://www.dell.com/identity/claims/p	rofile/email 🗸 🗸		
	First Name	\rightarrow	htt	p://www.dell.com/identity/claims/p	rofile/firstname 🗸 🗸		
	Last Name	\rightarrow	htt	p://www.dell.com/identity/claims/p	rofile/lastname V		
	Optional Claims						
	Member of	~	\rightarrow	Select	∨ 🗊 Delete		
	Country ode	~	\rightarrow	Select	∼ 🗊 Delete		
	Add Claim						



- The Add User Groups tab is displayed. This is an optional step. If you do not want to update the user group, you can skip Step 7 and click Next. Even after activating the IdP, you can add User Groups.
- 9. In the Add User Groups, perform the following:
 - a. To edit or delete an existing user group, click on the **Edit** or **Delete** icon with the respective user groups.
 - OR

To add new user groups, click on the **Add New User Group** button. Enter the name of the user group in the **Enter a group name** field and click **Save**.

Note: The groups set up will be effective only if the Member Of has been mapped.

Single Sign-On (SS	J) Setup			
etting up configuration for SSO expe	rience			
⊘ Select Domain	Select Protocol	Ø Register IdP	Add User Group	Activate
Add Active Directory User	Groups (Optional)			
dd the active directory user groups	to which you want to provide Single Sign-Or	access. You can also manage ti	ne user groups after successful IdP activation.	
▲ Warning: The new groups will be eff	ective only after mapping the member of claim. C	io to the tab IdP Metadata> <u>Claims</u> to	add the member of claim.	
User Group 1	10	in 前 Delete		
User Group 2	/* Ec	lit 🗊 Delote		
Add a New User Group				
			Cancel	Back Next



b. Click Next.

10. It is recommended to test the IdP connection and perform an end-to-end SSO testing to activate the IdP. This helps in detecting issues or if there is any break in connection. Click **Activate**.

To test the IdP connection,

- a. Click **Test IdP Connection**. This will open an SSO session in a browser window with Dell Identity using your IdP. When prompted, Sign in using your corporate credentials, and the test results will appear on the page.
- b. If the setup is tested successful, navigate to the tab **Test Connection** on the **Single Sign-on Setup page**, and invite a user to test SSO. If the test fails, check the IdP configuration. If you require assistance, please contact the Dell Identity team.

To invite users to Test SSO experience,

- a. Click **Enable Test SSO** to test the SSO experience.
 - Enabling Test SSO generates a unique email address for this IdP.
 - SSO is activated only for the users that are using this unique IdP email address.
- b. Share the unique email address that is generated with trusted users allowed to test the SSO.
- c. Share the application URL with the user to test the SSO.

For SP Initiated SSO, users are required to access their specific application from Dell.com page to test the SSO.

For IdP Initiated SSO, use the URL generated by your IdP and share the URL with your users to authenticate it with your IdP. On successful authentication, the user is redirected to the application using the relay URL mentioned in the table.

- d. Once Test SSO has been successfully confirmed, click Activate.
 - **Note:** If the user activates the IdP without disabling the test SSO, the test SSO will be automatically disabled.
 - After clicking on Activate, the IdP is activated but the SSO experience will be enabled after 40 minutes.
 - If you click Skip Activation, your IdP will be in 'Pending Activation' state. In case you want to activate your IdP, click Edit IdP and update the required information.

DØ	LLTechnologies					🖉 Michael 🗸		
	< Back to dashboard							
	Single Sign-On (SSO) Setup							
	Setting up configuration for SSO experience							
	⊘ Select Domain	⊘ Select Protocol	⊘ Register IdP	⊘ Add User Group	Ø Activate			
	Almost there! Test the co	onnection before activating t	he IdP					
	(j) You must test the IdP connection a	nd it is recommended to perform an end to end	SSO testing to update or activate the IdP. Th	is helps in detecting issues or if there is any break i	n connection.			
	1. Test IdP Connection					^		
	Test Connection Successful! This will open an SSO session in If the test is successful, a token in Test IdP Connection	IdP is ready to be activated. a browser window with Dell Identity using message with the user claim details will b	your IdP. Sign in with your corporate cr e displayed. If the test is unsuccessful,	edentials and the test result will be dislayed on check your IdP configuration or reachout to t	on the page. he Dell identity team.			
	2. Invite Users to Test SSO Exper	rience (Optional)				^		
	Enable the Test SSO to test the S	SO experience with your business use cas	ses.					
	 Enabling Test SSO generate SSO is activated only for the 	s a unique email address for this IdP. e users that are using this unique IdP email addr	ess.					
	Enable SSO Test							
				Skip Activation	Back	vate		

Figure 10 Activate

11. If you want to disable your registered IdP, click **Disable** on the IdP configuration page. A confirmation message dialog box will appear to confirm if you want to disable your IdP. Click **Yes**. Your registered IdP will be disabled.

Single Sign-On (SSO) Se	tup	⇔ Register a New IdP	🌐 Manage Domain	$\mathcal{E}_{\!\!\Theta}$ Manage Administrator
Important! Ensure that you perform the fol IdP SSO Configuration Learn how to set up SSO 🔀	lowing steps before setting up the IdP \sim			
XYZ 2022	Last modified 11 January 2022	Status Active		Disable Edit IdP
	Do you need assistance? Please reach out to DI Supp	port and we will respond as soon as po	ossible!	

Figure 11 Registered IdP - Disabled

Note: Ensure that at least one domain is selected to activate the IdP.

- In the Select Protocol tab, select OIDC as protocol.
 For more information about OIDC, click on Learn more about OIDC.
 a. There are two ways in which configuration can be enabled
 Well known Endpoint
 Manually Enter Values
 Select either Well known Endpoint or Manually Enter Values,
 b. Enter either Well known Endpoint or Manually Enter Values as per t
 - b. Enter either Well known Endpoint or Manually Enter Values as per the selection.
 - c. Click Next

L lechnologies				2 M	
< Back to dashboard					
Single Sign-On (SS	60) Setup			Service Provider Metadata	
Setting up configuration for SSO exp	perience				
Select Domain	⊘ Select Protocol	Register IdP	Add User Group	Activate	
Select a Protocol					
Choose and configure the external is SAML 2.0	dentity provider that you want to enable.		pen ID Connect (OIDC)		
Security Assertion. Markup Language 2.3 (SAML 2.3) is a version of the <u>SAML</u> standard for exchanging <u>authentication</u> and <u>authorization</u> identifies between <u>security domains</u> .		standard for OpenID ins. clients, t	OpenID Connect allows clients of all types, including Web based, mobile, and JavaScript clients, to request and receive information about authenticated sessions and end-users.		
Learn more 🖸		Learn m	nore 🖸		
The following methods are available	e for importing Identity Provider Metadata.				
The following methods are available Well-known Enpoint O Manua	e for importing Identity Provider Metadata. ally Enter Values				
The following methods are available Well-known Enpoint Well-known Endpoint	e for importing Identity Provider Metadata. ally Enter Values				
The following methods are available Well-known Enpoint Manua Well-known Endpoint https://www.dell.com/dci/fp/oidc	e for importing Identity Provider Metadata. Illy Enter Values /v3/.well-known/openid-configuration				
The following methods are available Well-known Engoint Mell-known Endpoint https://www.dell.com/dcl/fp/oldc	for importing Identity Provider Metadata. Illy Enter Values				

Figure 12 OIDC - Select Protocol

- 2. In the **Register IdP** tab, Issuer and Redirect URI, and all the fields in the Endpoint are auto populated. Basic Information
 - a. Enter Client ID, which you will find on your Identity Provider.
 - b. Enter Client Secret, which you will find on your Identity Provider.
 - c. Copy the **Redirect URI** and configure with your application.

Note: Changes to the issuer will update the Redirect URI

LTechnologies				<u></u>	
Back to dashboard					
Single Sign-On (SSO) Setup				
Setting up configuration for SSC) experience				
⊘ Select Domain	 Select Protocol 	Register IdP	Add User Group	Activate	
OpenID Connect Conf	iguration				
🧈 Basic Information	mation Authentication Method				
Endpointe	Broof Kay for Code Exchange	(RKCE)			
 Scopes 	If your application cappat safely st	e (FNGC)			
	<u> </u>				
	Client ID				
	Error the angua public identifier indexed by year thronty Provider for anting up 000 with Dol.				
				1	
	the second beauty and the second seco	the second second second second second second second			
	. The on more of the approximation				
	Issuer				
	Enter your app replayaboe's subsatty URL				
	Redirect URI: https://www.dell.co	om/identity/ 🔲 Copy			
	Please use the redirect URI and con	nfigure DELL as a relying party in your identity prov	vider. Changes to the lasuer will update the Redirect	URI.	
			Gancel	Register	

Figure 13 OIDC - Register IdP - Basic Information

Endpoints

Endpoints are auto populated from the Well Known Endpoints or Manually Entered Values.

C Back to dashboard					
Single Sign-On (SSO) Setup				
Setting up configuration for SS	0 experience				
② Select Domain	Select Protocol	Register IdP	Add User Group	Activate	
OpenID Connect Con	figuration				
 Basic Information 	Endpoints to communicate with the OpenID Connect provider for accessing protected resources.				
 Endpoints Scopes 	Endpoints				
	Authorization Endpoint				
	https://dev-12345678.okta.com/oau	uth2/v1/authorize		1	
	This is the URL to your Schridy Provider's legit sage, to which DELL indirects uses when they attenuit to access a DELL auditation.				
	Authentication Method: O BASIC O POST				
	https://dev-12345678.okta.com/oau	uth2/v1/token			
	This is the LOL which returns second takes. In higher and advest takes				
	Userinfo Endpoint (Optional)				
	This is the URL that returns claims about the auth	enticated user			
	Logout Endpoint (Optional)				
	When upert the out of the DELL prediction that a	un radiociad in this 112			
	Revocation Endpoint (Optional)				
	anoonana sunung di commit di sandi di C				
	Hordens of access tokens or refined bakens can use the URL to notify the identity Provider that a previously abbained reflects or ascess laken is no longer required and must be revolved. https://dev12345678.okta.com/oauth2/v1/keys JSGN Web Key Sets (JWKS) URL				
	Endpoint to request the $key(\mathfrak{a})$ to validate tokers			=	
			Cancel	Back Register	
				the protect	

Figure 14 OIDC - Register IdP - Endpoints

Scopes

a. Some of the predefined scopes are auto populated based on the Well Known Endpoint or Manually Entered Endpoints
b. Enter or Select Claim for UUID

c. Click Register IdP

Back to dashboard				
Single Sign-On (SSO) Setup			
Setting up configuration for SS	O experience			
⊘ Select Domain	Select Protocol	Register IdP	Add User Group	Activate
OpenID Connect Con	figuration			
 Basic Information Endpoints Scopes 	OpenID Connect (OIDC) scopes are used du specific set of user information which is mu Learn more about scopes here Scopes Scopes Address, Phane One or more scope is skeady eilst. Scopes Added Openid Prof/er Phone Unique User Identifier (UUID) Select or enter a claim value. When users log and of the OELL appRicking, Bary are	uring authentication to authorize accer ade available as claim.	ss to a user's details, like name and ema	I. Each scope can be used to request
	Claims (Optional)		-	
	Claims (Optional)	~ →	Enter a claim value	Delata
	Claims (Optional) Address Phone_number Add Claim	~	Enter a claim value	Delete

Figure 15 OIDC - Register IdP - Scopes

For Add User Group and Activate refer to Page 9 – Page 11.

1 Managing Identity Administrator

To invite a new Identity Administrator from dell identity portal, perform the following:

- a. In the IdP configuration page, click Manage Identity Administrator.
- b. Enter your First name, Last name, and Email address.
- c. Click Invite.

The requested user will receive a welcome email along with the steps to be followed. For more information, refer to Topic 1: **Sign In and Verify your Account** of <u>Email Invitation</u> document.