Integrating Bitwarden SSO / SCIM with Microsoft Entra ID **Using SAML 2.0**

With Trusted Devices Encryption and Domain Verification

1.1 Select Enterprise applications:

SSO Identifier: bw-saml Enterprise App: bw-saml-az

D bitwarden

X



Create Enterprise Application

Azure Portal: go to Microsoft Entra ID

https://bitwarden.com/help/about-sso/ https://bitwarden.com/help/about-scim/ https://bitwarden.com/help/domain-verification/ https://bitwarden.com/help/about-trusted-devices/ https://bitwarden.com/help/sami-microsoft-entra-id/

1.4 Give this application a unique name:



1.2 Select the New application button:



3

Enable Sign-On

Prepare your AZ app to



Configure Bitwarden Settings and Azure SAML Configuration

In your Bitwarden instance, navigate to your organization's Settings → Single sign-on screen.	On Azu	ıre → Edit I	Basic SAML Configu	uration.		
Single sign-on 🛛 🖷 📵	Basic SAML Configuration			+		
Use the require single sign on authentication policy to require all members to log in with SSO.	🔚 Sav	e 🔗 Got fe	eedback?			
Once set up, your configuration will be saved and members will be able to authenticate using their identity Proviner configuration	Identifi The uniq	er (Entity ID) * ue ID that identif	fies your application to Microsofi	t Entra ID. This value must be unique across all applications in	n your	
SSO Identifier (requires) bitwarden-sami	Microsof	ft Entra tenant. Th	ne default identifier will be the au	idience of the SAML response for IDP-initiated SSO. Default		
Provide this ID to your members to login with SSO. To bypass this step, set up Domain verification	https:	//sso.bitwarden.c	om/saml2/9c44474c-f7a6-477d-	aa31-b07d0188d60a 🗸 🖉 🛈	1	
Member decryption options O Master password Trusted devices Once authenticated, members will decrypt vault data using a key stored on their device. The single organization policy.550 required policy, and account recovery administration policy with automatic enrollment will turn on	Reply L	JRL (Assertion	Consumer Service URL) * e application expects to receive	• the authentication token. This is also referred to as the "Asse	rtion	
Type SAML 2.0	Consume https://	//sso.bitwarden.ci	om/saml2/9c44474c-f7a6-477d-	Index Default	i i	
	Add reply URL					
SAML service provider configuration Set a unique SP entity ID	Sign on URL (Optional) Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL					
Generate an identifier that is unique to your organization SP entity ID	for your https://	for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on. https://vault.bitwarden.com/#/sso ✓				
https://sso.bitwarden.com/sam12/9c44474c-f7a6-477d-aa31-b07d0188d60a	Relay S	tate (Optional) 0			
https://sso.bitwarden.com/sami2/9c4474c-f7a6-477d-aa31-b07d0188d60a	The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.					
Assertion consumer service (ACS) URL https://sso.bitwarden.com/sami2/964474c.f7a6-477d-aa31-b07d0188d60arAcs	Enter a	relay state				
Name ID format Unspecified	Logout	Url (Optional))			
Outbound signing algorithm	This URL is used to send the SAML logout response back to the application. Enter a logout url					
Integr/www.ws.org.2001/04XIII038-III076915a-518236						
If IdP Wants Authin Requests Signed	Set up	o Single Sigr	n-On with SAML	mproves security, reliability, and end user experiences and is	easier to	
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	impleme more.	ent. Choose SAM	L single sign-on whenever possi	ble for existing applications that do not use OpenID Connec	t or OAuth. Lean	
Expect signed assertions Validate certificates	Read th	e configuration g	guide 🖉 for help integrating bw	-saml-az.		
		Identifier (Entit	onfiguration ty ID)	https://sso.bitwarden.com/saml2/9c44474c-f7a6-477d-aa	C Edit	
SAML identity provider configuration Entity ID (required)		Reply URL (Ass	sertion Consumer Service URL)	31-b07d0188d60a https://sso.bitwarden.com/saml2/9c44474c-f7a6-477d-aa 31-b07d0188d60a/Acs		
https://sts.windows.net/0d3fe087-b3a6-4a28-a29e-1d52bdbb6da1/		Sign on URL Relay State (Op Logout Url (Op	ptional) otional)	https://vault.bitwarden.com/#/sso Optional Optional		
HTTP POST	2					
Single sign-on service URL https://login.microsoftonline.com/0d3fe087-b3a6-4a28-a29e-1d52bdbb6da1/sami2		Attributes & G	Claims	user.givenname	C Edit	
Required if Entity ID is not a URL. Single log-out service URL		surname emailaddress name		user.surname user.mail user.userprincipalname		
		Unique User Identifier		user.userprincipalname		
X509 public certrincate (required) MIIC8DCCAdigAwiBAgiQSrmUtiOXLIdNWwhTKYnOZANBgkqhkiG9w0BAQsFADA0MTiwMAYDVQQDEylNaWNyb3NiZ ngQQXpTuugRwtXZqhdGVkiFNTYgbZXqJawZpY2F0ZTAeEvojNiDAzMDMwMDE2MTZaEvojNizAzMDMwMDE2M	3 SAML Certificate		ates			
TZaMDQxMJwdgvVDaAMTKU IpY3yc23mdCBBenvj2SBGZWBIcm62XWQU INPIENcRp2cpJJYXBIMIBJJABgkphlk 9w0BAQEFAAOCAQ8AMIBCgKCAQEAtQAxtcn:xn57apx5M5917Tm05k6DNzw2t2iMp2 4mWLowbhzUVY3JL3LHTMUpAyirg7ligQMJafEH33x08bD13ydyWemHbDPwMX5xC, leb5p7MH4CK058zXe		Token signing certificate Status Thumbprint		Active	C Edit	
/s1HbVCaaOVzpM/llt3/zjpGetgzCYSIUJbdmLVWqdhNr2ikCYo2MuPW+lC7+Xjk88kdsc1aFeN6sD2DhRFvDhdbPjgv+		Expiration Notification Email App Federation Metadata Uri		3/3/2027, 1:16:16 AM fer@ferqwerty.com		
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256		Certificate (Base64) Certificate (Raw)		Download		
Allow outbound logout requests Sign authentication requests		Federation Metadata XML		Download		
Save		Verification certificates (optional) Required Active Expired		No 0 0	🖉 Edit	
A Verify Domain	4	Set up bw-sar	ml-az			
Once domain's ownership is verified, @bitwarden support accounts will be able	You'll need to configure the application to I		configure the application to link	nk with Microsoft Entra ID.		
to bypass SSO ID step during login.		Microsoft Entra	a Identifier	https://login.microsoftonline.com/0d3fe087-b3a6		
Domain verification		LOGOULORL		https://login.microsoftonline.com/0d3fe087-b3a6		
Verify domain tansarten apport						
Domain name (required)						
Example: regionalized and the separate entries to the separate entries to the serified.	amlaz	Provisionin	g		~	
DNS TXT record DW=6ldzCHidzadwfZCv0r4wBY0m6PQ47mLzhAinQ11mm8	unn-uz	• «	Save X Discard			
Copy and paste the TXT record into your DNS Provider.	riew					
Reverify domain Cancel	ige		Provisioning Mode Automatic		~]	
¢ P 23 U	Isers and groups	4.	and group assignment.	eauon and synchronization of user accounts in fer-bw-sso-saml-scim ba	isea on user	
5 SCIM Provisioning	pression builde, tor		∧ Admin Credentials Admin Credentials			
Accept requests from your identity provider (IdP) for user and group provisioning and de-provisioning.	pieshoot		Microsoft Entra needs the follo data.	wing information to connect to fer-bw-sso-saml-scim's API and synchro	nize user	
SCIM provisioning = 📵			Tenant URL * ③ https://scim.bitwarden.com/vi	2/9c44474c-f7a6-477d-aa31-b07d0188d60a		
Automatically provision users and groups with your preferred identity provider via SCIM provisioning			Secret Token			
Set up your preferred identity provider by configuring the URL and SCIM API Key SCIM 100			Test Connection			
https://scim.bitwarden.com/v2/5044476c17a6.477d-aa31-b07d0188660a			✓ Mappings			
This API key has access to manage users within your organization. It should be kept secret.			\vee Settings			
Save			Provisioning Status () On Off			