## **Configuring Slack**

Users can securely log on to Slack using their enterprise credentials. To configure Slack for single sign on through SAML, follow the steps below:

1. In a browser, type https://<your-organization>.slack.com and press Enter.

**Note**: For example, if the URL is <u>https://myserver.slack.com</u>, you must replace <yourorganization> with myserver.

2. Log on to your Slack account.

Sign in to charge	
Enter your <b>email address</b> and <b>password</b> .	
you@example.com	
password	
Sign in	

3. On the home page, in the upper left corner, click your workspace name.



4. Click Administration > Workspace Settings.



5. Click **Authentication** > **Configure** next to SAML authentication.

Setting	gs & Permiss	ions		Import/Export Data →
djust workspac	e-wide settings and	preferences here for ctx	ans. You can also manage me	embers and roles.
Settings	Permissions	Authentication	Attachments	Access Logs
Slack suppo below, or lea	rts a number of singl arn more about using e an authentica	e sign-on (SSO) services s single sign-on with Slac tion method	. Get started with setting up ck.	your workspace's SSO
G Go	ogle Apps authen t members sign in wit	<b>tication</b> th a Google account.		Configure
	ML authentication	ı		2

6. To turn the test mode on to test and then save the configuration, click **Configure** next to **Configure SAML Authentication**.



The test button appears indicating that the test mode is turned on.

7. In the **Configure SAML Authentication** section, specify the following information

nter your SAML 2.0 Endpoint. his is where you go when you try o login.	https://u_l_l_saml/login
Custom SAML Instructions	
dentity Provider Issuer	
The IdP Entity ID for the service you use.	Slack_2

- i. **SAML 2.0 Endpoint (HTTP)** type the log in URL.
- ii. Identity Provider Issuer type IDP Entity ID.
- iii. Public Certificate paste the identity provider certificate

To upload your IdP certificate, follow the steps below:

- i. Remotely access your NetScaler instance using PuTTY.
- ii. Navigate to /nsconfig/ssl folder (cd /nsconfig/ssl) and press Enter.
- iii. Type cat certificate-name.pem and press Enter.
  - Note: This is your SAML IdP signing certificate.
- iv. Copy the text from -----BEGIN CERTIFICATE----- to-----END CERTIFICATE-----.

1					NAME OF TAXABLE PARTY.	VTF
B	BORDER AT \$1. 2 100	I THE REAL PROPERTY.	Company States Stores			ND
2	and a state of the	1 1 11 11 11		and the second second		MDE
1		A COLUMN TWO IS NOT	and the state of			MR
A				and the second sec	Carlot and Desired	aWE
1		No. No. of Concession,	A MARY MANA			Bg]
k	A REAL PROPERTY.			No. of Concession, Name		7a1
C	10.00 B 10.00	State State				501
a	the second second	the state of the second state		Company of the local division of	Anna a start	FE
+ Harden Street Street	and the second second	and the second second second	ALC: NO. OF	and the second second second	State of Long State of Long	H99
x	and the Party of the local		in the second second	THE OWNER WATCHING		hr

8. In the **Advanced Options** section, select the **Sign** checkbox.

Advanced Options		close
Sign AuthnRequest	- We will use this public key to sign our requests	
	BEGIN CERTIFICATE MIJ V	
	BAY p	
2	CXN J Bgn h	
	bmh V BAll 3	
	388 M	
	/m0	
	910 X 72E 5	
	Pro di VVC Q	
	UP2/Zj295awYC4sCljQYnWq2N/d0uYH8m0iFzqLcINUG8xOkV/tX1Hvj9c5rmlnJ	

The SP Signing Certificate appears. Copy and paste the value (end-to-end encryption key) in a notepad file and save the file in .pem format. For example: slack-sp.pem.

9. **AuthnContextClassRef** displays the following value by default: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

AuthnContextClassRef	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransp
5	The RequestedAuthnContext we will send in requests to your IdP. Don't see a value you need here? Let us know!
Service Provider Issuer	2 https://slack.com
	The SP Entity ID you would like us to send. By default, this is https://slack.com.
Choose how the SAML response	e from your IDP is signed. You must choose at least one option.
Responses Signed 3	
Assertions Signed	

- In the Service Provider Issuer box, type <u>https://slack.com</u>.
  Note: If you change the Service Provider Issuer name, ensure that you note it.
- 11. To specify how the SAML response from your IdP is signed, select the check boxes named **Responses Signed** and **Assertions Signed**.

12. In the **Settings** area, define if the users can edit their profile information such as email address and display name. You can also define if SSO authentication must be optional or required.



13. In the **Customize** area you can type a label for the Sign in button.

	Customize		
	Sign In Button Label	Button Pre	view
2	Custom Label	ୈ	Sign in with SAML
	Do you have a nickname for your SSO system? Add it to the Sign In Button!		your Sign In Button will look like.

14. <u>To test the configuration, click **Test Configuration**</u>.

Test and Save	
Test Configuration	Save Configuration
This will only test your changes.	Emails will be sent to workspace members who have not set up SSO for their Slack accounts.

If the configuration is appropriate, a confirmation message appears.



15. Click Save Configuration.

You have completed the required configuration on the service provider which is in this case – Slack.