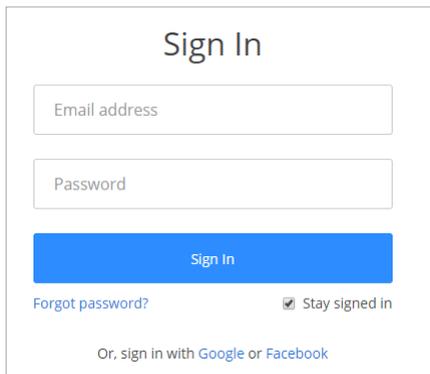


Configuring Zoom

Configuring Zoom for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Zoom using their enterprise credentials.

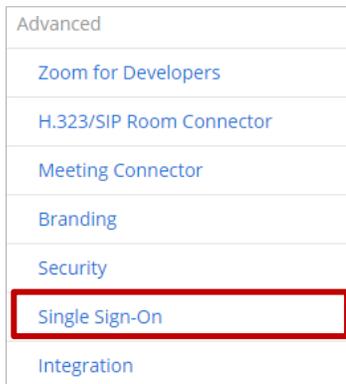
To configure Zoom for single sign on through SAML, follow the steps below:

1. In a browser, type <https://zoom.us/signin> and press enter.
2. Log on to your Zoom account.



The image shows the Zoom Sign In page. It features a title "Sign In" at the top. Below the title are two input fields: "Email address" and "Password". A blue "Sign In" button is positioned below the password field. Underneath the button, there is a link for "Forgot password?" and a checkbox labeled "Stay signed in" which is checked. At the bottom of the form, there is a text link that says "Or, sign in with Google or Facebook".

3. On the **My Profile** page, in the left pane, under **Advanced** section, click **Single Sign-On**.



The image shows a vertical list of menu items under the "Advanced" section of the Zoom My Profile page. The items are: "Zoom for Developers", "H.323/SIP Room Connector", "Meeting Connector", "Branding", "Security", "Single Sign-On", and "Integration". The "Single Sign-On" item is highlighted with a red rectangular border.

4. In the **SAML** tab, copy the URL that the **Vanity URL** box displays. This URL is required for NetScaler configurations.

5. In the **Sign-in Page URL** box, enter the IdP URL of your NetScaler app: https:// <Netscaler Gateway FQDN>/saml/login
6. In the **Sign-out Page URL** box, enter https:< Netscaler Gateway FQDN >.com/cgi/tmlogout.
7. In the **Identity provider certificate** box, you must paste the Identity provider certificate.
8. 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 between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

```

root@pers:~# cd /nsconfig/ssl
root@pers:~# cat certificate-name.pem
-----BEGIN CERTIFICATE-----
MIIClzCCAkCgAwIBAgIGAWhYpNi8MA0GCSqGSIb3DQEEBQUAMIGuMQswCQYDVQQGEwJKVUzETMBEG
A1IqNDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1
4BNDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1NDk1
f2MDExMDEyMDEzMDE0MDE1MDE2MDE3MDE4MDE5MDE6MDE7MDE8MDE9MDE0MDE1MDE2MDE3MDE4
N1MRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYwMRYw
FAaWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1aWR1
cjBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkqBgkq
rk7aff7aff7aff7aff7aff7aff7aff7aff7aff7aff7aff7aff7aff7aff7aff7aff7aff7aff7aff
bC5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ5OyZ
oaFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3kFF3k
N+H99ZH99ZH99ZH99ZH99ZH99ZH99ZH99ZH99ZH99ZH99ZH99ZH99ZH99ZH99ZH99ZH99ZH99
7xhr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8ihr8i
jPrC4ydcewMxqGdFFSQ/LHWUPGvGlpHzj47MzcN0EbdVrVmKF61e4/fTkVz3ST3U=
-----END CERTIFICATE-----
root@pers:~#

```

9. Copy the URL displayed by the **Service Provider (SP) Entity ID** box.

Service Provider (SP) Entity ID:

If your identity provider(idp) prefers a URN-based entity ID for a Service Provider(SP), please use the default value: [ctxnsqa.zoom.us](#).
Otherwise, if your idp prefers a URL-based entity ID for a Service Provider(SP), please select [https://ctxnsqa.zoom.us](#).

10. In the **Issuer (IDP Entity ID)** box, type a unique issuer ID and click **Save Changes**.

Issuer (IDP Entity ID):

Binding: HTTP-POST HTTP-Redirect

Security: Sign SAML request
 Support encrypted assertions
 Enforce automatic logout after user has been logged in for

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