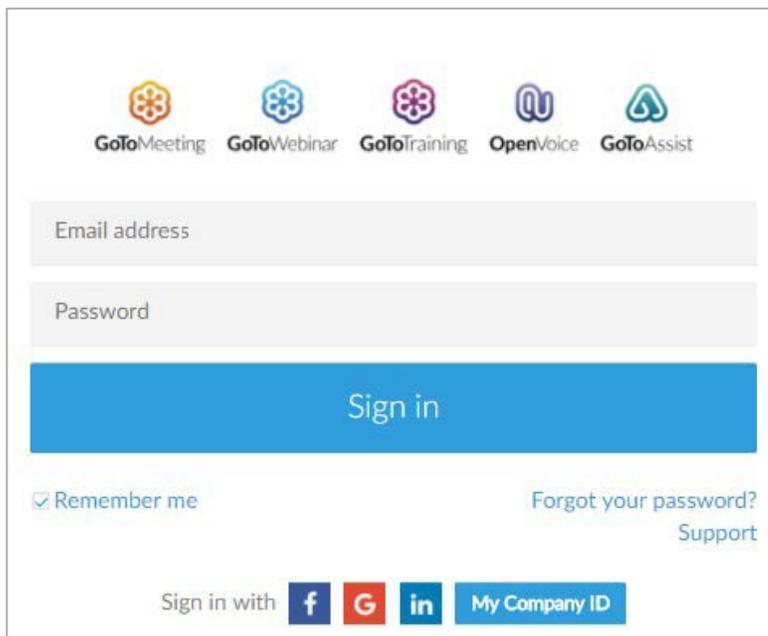


Configuring GoToMeeting

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

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

1. In a browser, type <https://organization.logmeininc.com> and press Enter.
2. Log on to your GoToMeeting account.



The screenshot shows the GoToMeeting login interface. At the top, there are five logos: GoToMeeting (orange), GoToWebinar (blue), GoToTraining (purple), OpenVoice (blue), and GoToAssist (green). Below the logos are two input fields: "Email address" and "Password". A large blue "Sign in" button is positioned below the password field. Underneath the button, there is a checked checkbox labeled "Remember me" and a link for "Forgot your password?". At the bottom, there is a "Sign in with" section featuring icons for Facebook, Google, LinkedIn, and a "My Company ID" button. A "Support" link is also visible at the bottom right.

3. On the home page, in the **Email** tab you can add a domain.
4. In the **Identity provider** tab, specify the following details:

- i. **How would you like to configure your SAML IDP?** – click **Manual**.

Note: You can click the appropriate option to configure automatically using a metadata URL, by uploading a SAML metadata file, or manually with sign-in and sign-out URLs, an identity provider ID and by uploading verification certificate.

- ii. **Sign-in page url** - type the IdP URL followed by /saml/login. For example:
https://<customerFQDN>/saml/login
- iii. **Sign-in binding** – click the appropriate sign-in binding option. By default, GoToMeeting uses **REDIRECT**.
- iv. **Sign-out page url (optional)** -type the log-out URL.
- v. **Sign-out binding** – click the appropriate sign-in binding option. By default, GoToMeeting uses **REDIRECT**.

- vi. **Identity Provider Entity ID** – type a unique IdP entity ID.

vii. **Verification certificate** – paste the IDP certificate.

To obtain your IdP certificate, follow the steps below:

- i. Remotely access your NetScaler instance using PuTTY.
- ii. Navigate to /nsconfig/ssl folder (using shell command `cd /nsconfig/ssl`) and press Enter.
- iii. Type `cat <certificate-name>` and press Enter.

```
root@pers:~# cd /nsconfig/ssl
root@pers:~# cat /nsconfig/ssl/sslcert.pem
-----BEGIN CERTIFICATE-----
MIIClzCCAkCgAwIBAgIGAWHYpNi8MA0GCSqGSIb3DQEBBQUAMIGuMQswCOYDVQQGEwJVUzETMBEG
A1IqAgEBBQAwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
4BBAQwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
f2EwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
N1EwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
FAEwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
cjEwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
rkEwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
pCEwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
pamEwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
N4EwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
7xEwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
h8iEwYzEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEwLjEw
jPrC4ydcewMxqGdFFSQ/LHWUPGvGlpHzj47MzcN0EbdVrVmKF61e4/fTkVz3ST3U=
-----END CERTIFICATE-----
root@pers:~#
```

- iv. Copy the text from -----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----
- v. Paste the text in a text editor and save the file in an appropriate format such as <your company name>.pem

5. Select the **My identity provider has been updated with the new domain** check box.
6. Click **Save Configuration**.

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