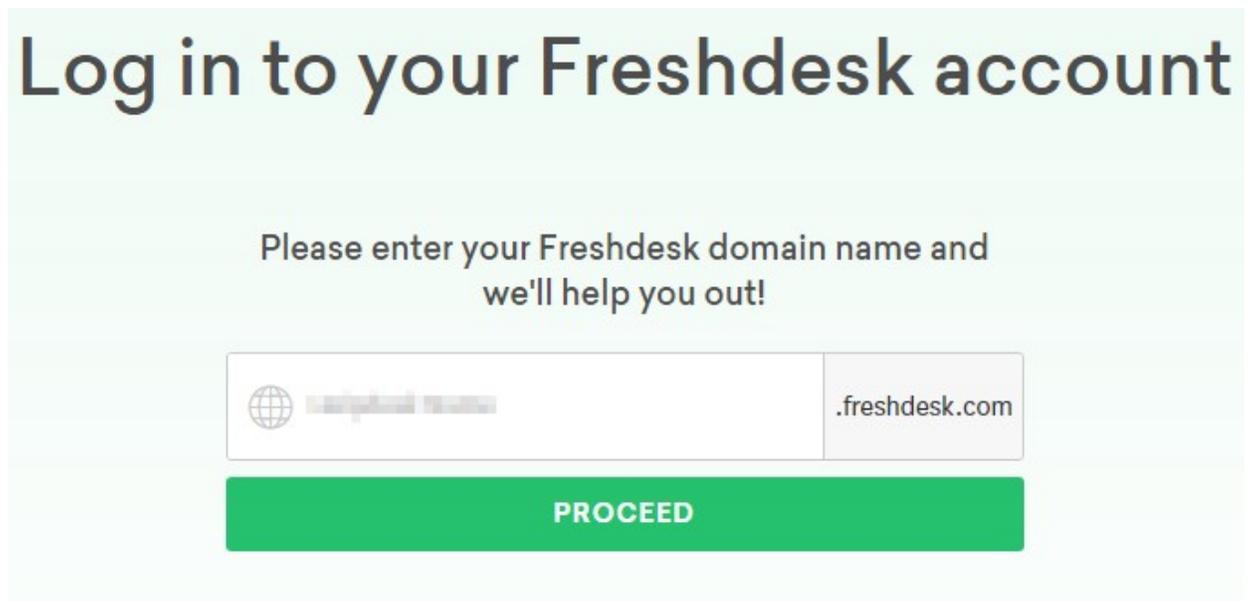


Configuring Freshdesk

Users can securely log on to Freshdesk using their enterprise credentials.

To configure Freshdesk Enterprise for SSO through SAML, follow the steps below:

1. Login to **Freshdesk** as an Admin user.



Log in to your Freshdesk account

Please enter your Freshdesk domain name and we'll help you out!

.freshdesk.com

PROCEED

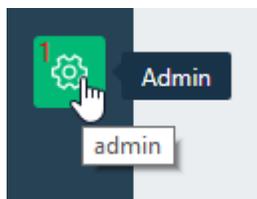
2. Enter your domain name and click on proceed, you will navigate to your domain login page.

Login to the support portal

Enter the details below

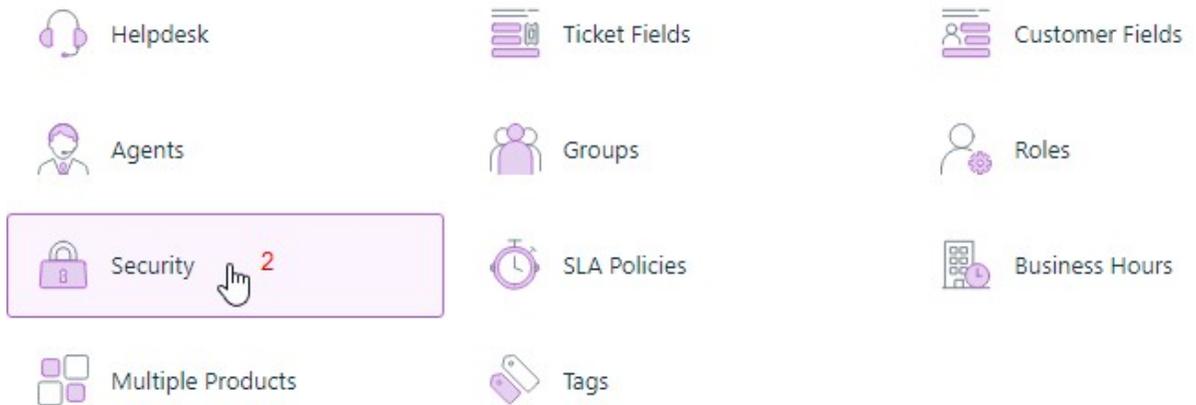
 Remember me on this computer
[Forgot your password?](#)

3. Click on **Admin** tab in left side menu.



4. Admin window will appear, Inside **General Settings** click on **Security**.

General Settings



5. Security window will appear, check on the **Single Sign On (SSO)**, **SAML SSO** and **Secure connection using SSL** buttons and Complete all the field with appropriate values.

Security

3 Single Sign On (SSO)

4 SAML SSO

SAML is an XML standard used for communicating identities between two web applications. You can use it to let large teams access your support portal easily using Single Sign On.

SAML Login URL

Freshdesk will redirect users to this URL to login. You can get this from your SAML Identity Provider.

Logout URL

Optional logout URL to which users will be sent to when they logout of freshdesk.

Security Certificate Fingerprint

Fingerprint (SHA256) of the SAML certificate provided by your SAML Provider. This will be used for encryption / validation

Simple SSO

Single Sign On allows you to use your own application or a centralized Server (like MS Active Directory) to authenticate agents and customers so that they can access Freshdesk without entering a separate username and password.

5 Secure Connection using SSL

Secure Sockets Layer allows you to encrypt data that is transferred to and from Freshdesk

Field Name	Values
SAML Login URL	https://ug1.<customer_domain>.com/saml/login
Logout URL	https://ug1.<customer_domain>.com/cgi/logout
Security Certificate Fingerprint	Generate the fingerprint of your IdP certificate and paste it in this section

- Select the Admin user to send the notification.

Admin Notifications

Send notifications to

Notification will be sent when

- Agent is Added or Deleted

Password Policy

Changes you make to the password policy will be applicable within 8 hours. Your agents will be prompted to update their passwords during this time. If they fail to conform, they will be logged out of the support portal and will be forced to change their passwords the next time they try to log in.

For Agents

Default Advanced

- Minimum of 8 characters
- Cannot contain username

For Contacts

Default Advanced

- Minimum of 8 characters
- Cannot contain username

- Click on **SAVE**.