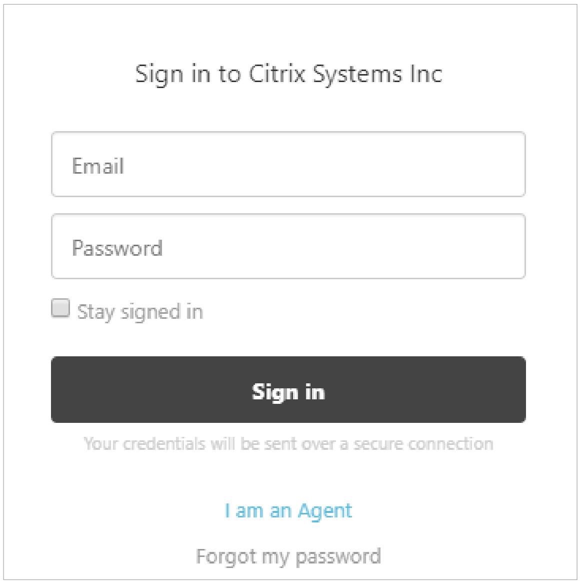
Configuring Zendesk

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

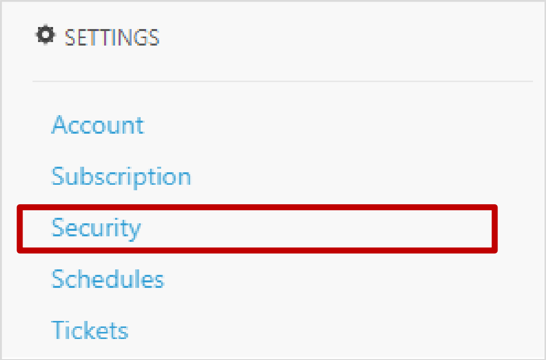
1. In a browser, type https://<customer>.zendesk.com and press enter.
2. Log on to your Zendesk account as an administrator.



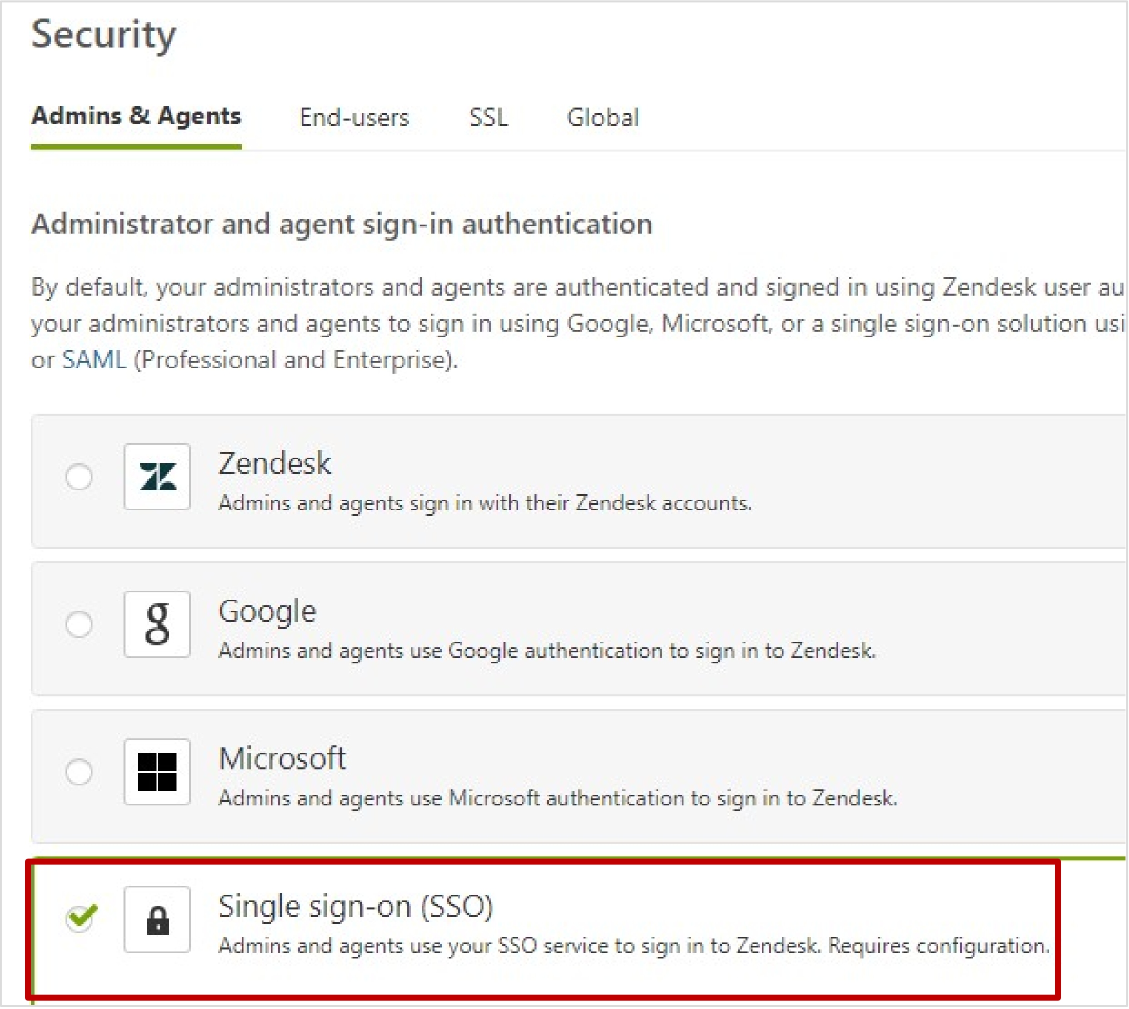
Sign in to Citrix Systems Inc

Your credentials will be sent over a secure connection

3. On the **Support** page, in the left pane, click the **Admin** icon ⚙.
4. In the **Setting** section, click **Security**.



5. In the **Security** area, to enable single sign on for administrators and agents, in the **Admin & Agents** section, click **Single sign-on (SSO)**.



Administrator and agent sign-in authentication

By default, your administrators and agents are authenticated and signed in using Zendesk user au your administrators and agents to sign in using Google, Microsoft, or a single sign-on solution usi or SAML (Professional and Enterprise).

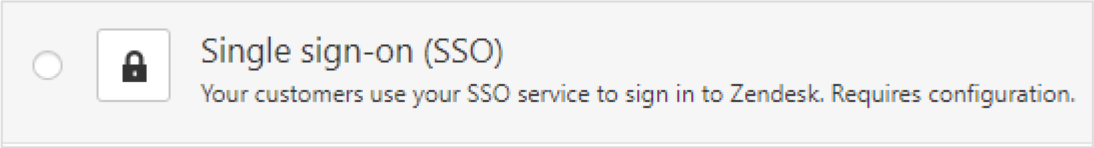
○ Zendesk
Admins and agents sign in with their Zendesk accounts.

○ Google
Admins and agents use Google authentication to sign in to Zendesk.

○ Microsoft
Admins and agents use Microsoft authentication to sign in to Zendesk.

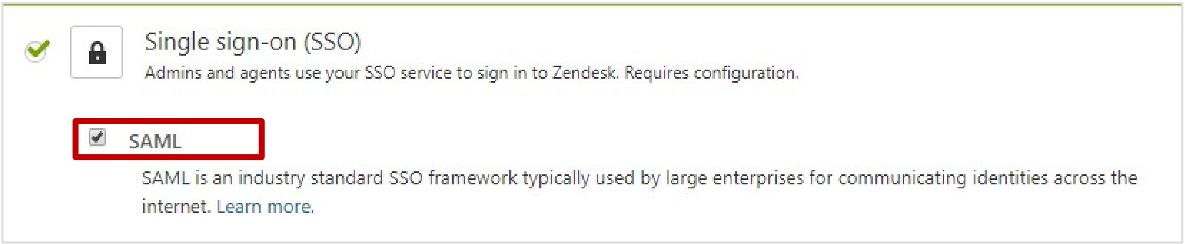
✓ Single sign-on (SSO)
Admins and agents use your SSO service to sign in to Zendesk. Requires configuration.

6. To enable single sign on for end users, in the **End-users** section, click **Single sign-on (SSO)**.



○ Single sign-on (SSO)
Your customers use your SSO service to sign in to Zendesk. Requires configuration.

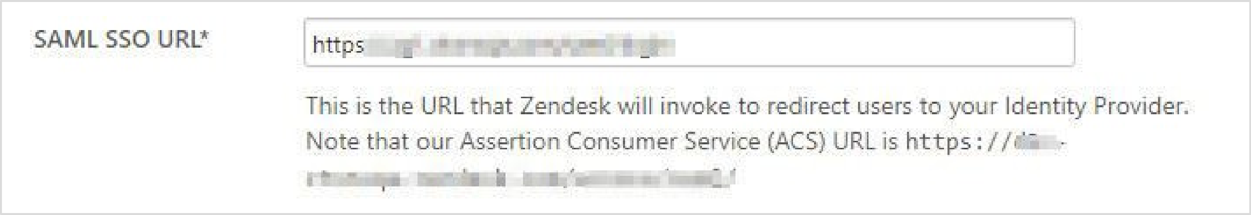
7. Select the **SAML** check box.



✓ Single sign-on (SSO)
Admins and agents use your SSO service to sign in to Zendesk. Requires configuration.

☑ SAML
SAML is an industry standard SSO framework typically used by large enterprises for communicating identities across the internet. Learn more.

8. Enter the SAML SSO URL for example: https://<Netscaler FQDN>/saml/login.

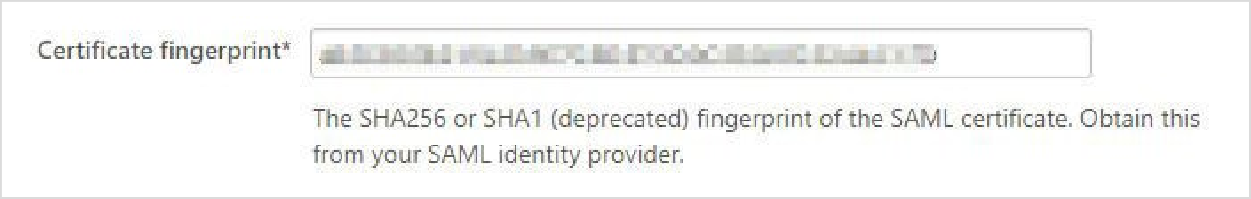


SAML SSO URL*

https [redacted]

This is the URL that Zendesk will invoke to redirect users to your Identity Provider. Note that our Assertion Consumer Service (ACS) URL is https://[redacted]

9. In the **Certificate fingerprint*** box, you must paste the Certificate fingerprint.



Certificate fingerprint*

[redacted]

The SHA256 or SHA1 (deprecated) fingerprint of the SAML certificate. Obtain this from your SAML identity provider.

10. To add fingerprint of the NetScaler IDP SAML Signing certificate, follow the steps below:

    i. Remotely access your NetScaler instance using PuTTY.

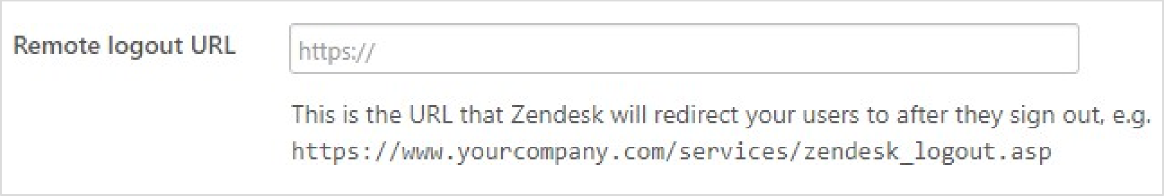
    ii. Log on to Shell by typing Shell.

    iii. Navigate to /nsconfig/ssl folder (cd /nsconfig/ssl) and press Enter.

    iv. Type *openssl x509 -in certificatename shell.pem -fingerprint –noout* and press Enter.

    v. Copy the fingerprint that has been generated and paste that in the **Certificate fingerprint*** box.

11. If you want the users to redirect to a specific site after logging out, in the **Remote logout URL** box, enter the specific URL. For example: www.yourcompany.com/zendesklogout.

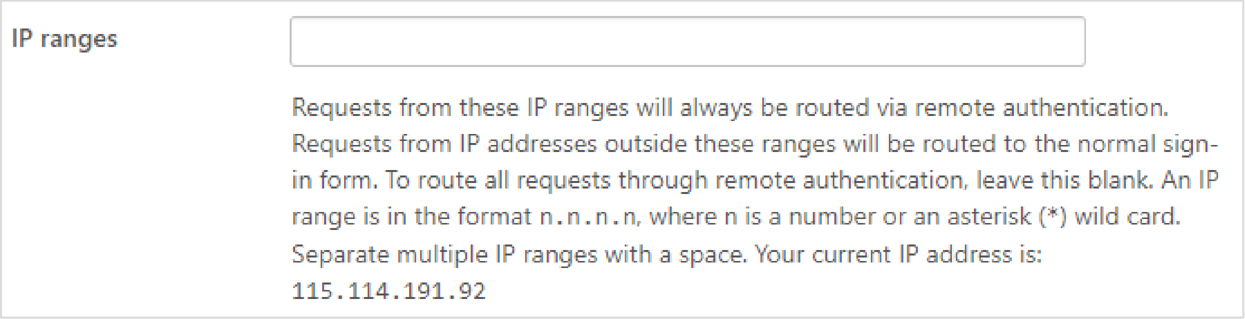


Remote logout URL

https://

This is the URL that Zendesk will redirect your users to after they sign out, e.g. https://www.yourcompany.com/services/zendesk_logout.asp

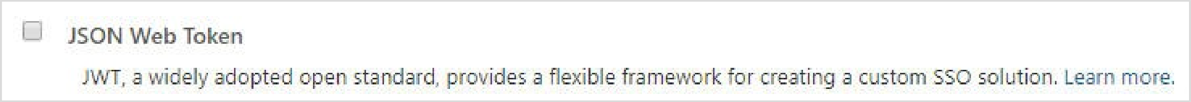
12. Type the IP ranges if required.



IP ranges

Requests from these IP ranges will always be routed via remote authentication. Requests from IP addresses outside these ranges will be routed to the normal sign-in form. To route all requests through remote authentication, leave this blank. An IP range is in the format n.n.n.n, where n is a number or an asterisk (*) wild card. Separate multiple IP ranges with a space. Your current IP address is: 115.114.191.92

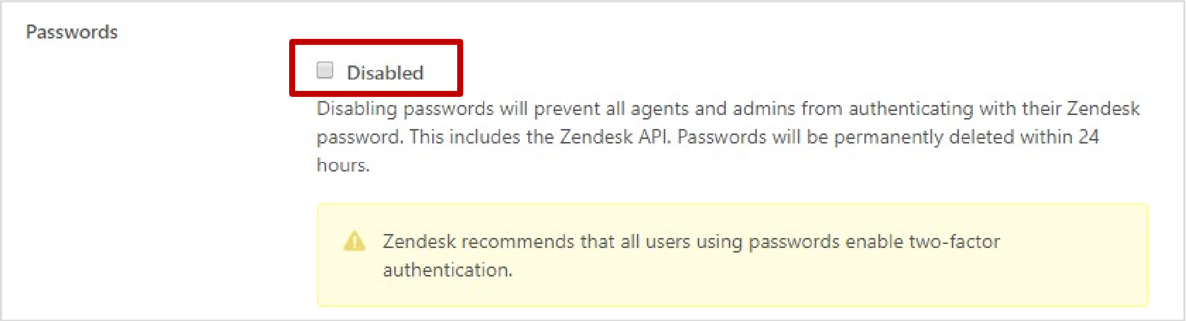
13. Keep the **JSON Web Token** check box unchecked.



□ JSON Web Token

JWT, a widely adopted open standard, provides a flexible framework for creating a custom SSO solution. Learn more.

14. If you don't want to necessitate the agents and administrators to enter passwords, select the **Disabled** check box.



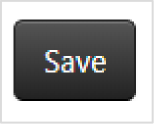
Passwords

□ Disabled

Disabling passwords will prevent all agents and admins from authenticating with their Zendesk password. This includes the Zendesk API. Passwords will be permanently deleted within 24 hours.

⚠ Zendesk recommends that all users using passwords enable two-factor authentication.

15. Click **Save**.



You have completed the required configuration.