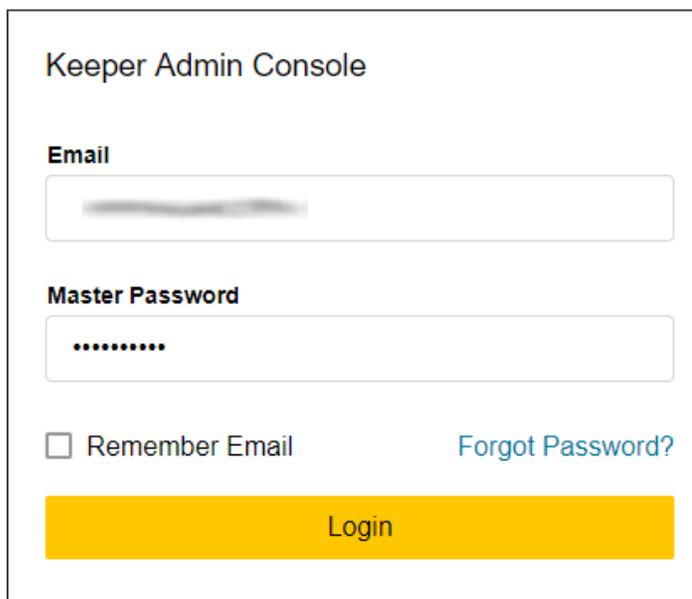# Configuring Keeper Security

Configuring Keeper Security for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Keeper Security by using the enterprise credentials.

Prerequisite

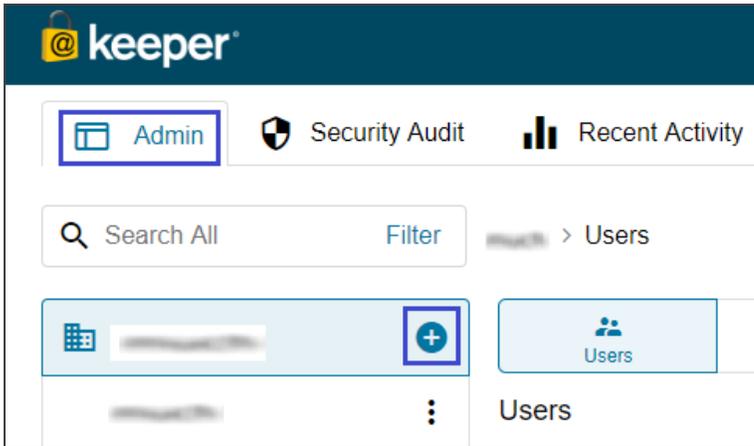Browser Requirements: Internet Explorer 11 and above

To configure Keeper Security for SSO by using SAML:

1. In a browser, type https://keepersecurity.com/en_US/console/#login and press **Enter**.

2. Type your Keeper Security admin account credentials (**Email Address** and **Master Password**) and click **Login**.

3. In the **Admin** tab, click **+** icon present in the left panel to create a node.

4. In the **Add Node** pop-up box, enter the values for the following fields:

Field Name	Description
Node	Select the created node.
Name	Type the name of the user.

5. Click the created node from the left panel. Navigate to **Provisioning > Edit** and enter the values for the following fields:

Field Name	Description
SSO Connect URL	SSO Connect URL
Enterprise Domain	Domain name

Single Sign-On (SAML 2.0) with Keeper SSO Connect   ✕

Provision and authenticate users into their Keeper vault using any SAML 2.0 compatible Identity Provider. Keeper SSO Connect is an on-premise or cloud based service that seamlessly authenticates users into their Keeper vault and dynamically provisions accounts.

SSO Connect URL

https://   /sso-connect/saml/login

Enterprise Domain

New User Provisioning

Users can be provisioned to your Keeper Enterprise account without having to create user accounts in advance. When a new user logs into the organization's SSO solution, their Keeper account is automatically created for them. Alternatively, you may manually invite users through the Admin Console "Users" tab or invite users via the Keeper Bridge.

☑ Enable Just-In-Time Provisioning

Cancel   Save

6. Click **Save.**

7. Select **Download SSO Connect for Windows** for Windows operating system or select **Download SSO Connect for Linux** for Linux operating system.
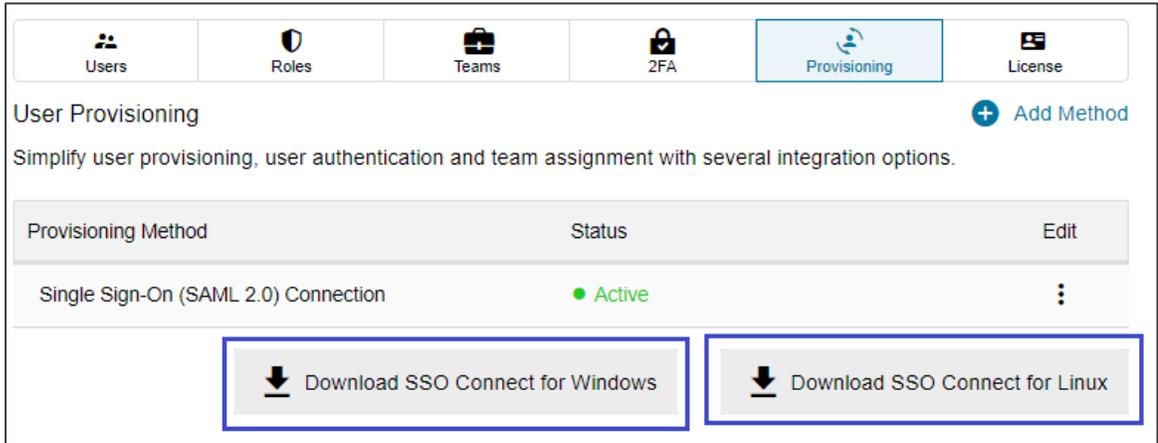
Note 1: Users can select any of the two methods suitable for them to configure SP.
Note 2: Launch the downloaded file for Windows operating system to configure SP.

8. Host Keeper Security instance on your preferred or local VM and run the commands mentioned below:

To	Do this
Upload SSL file	**java –jar SSOConnect.jar –ssl_file<path>**
Upload IdP metadata	**java –jar SSOConnect.jar –saml_file<path>**
Configure SP	**java –jar SSOConnect.jar –c**

Note 1: **<path>** denotes the location of the file.
Note 2: A DNS entry has to be created for public IP through which SP can be accessed.

9. Enter the values for the following fields:

Field Name	Description
Username	Type the admin username
Password	Type the admin password.
Do you wish to configure Hostname, SSL Port, Signing, or Field Mapping? (Y/N)	Type N
Key Store Password	Type the ssl password.

```
[ec2-user@ip-172-31-8-61 SSOConnect]$
[ec2-user@ip-172-31-8-61 SSOConnect]$ java -jar SSOConnect.jar -c
INFO  2018-08-29 09:15:18,751 com.keepersecurity.sso.SsoConnect.<clinit> Using log file
rectory: /home/ec2-user/SSOConnect/
INFO  2018-08-29 09:15:20,712 com.keepersecurity.sso.dagger.AppModule.getBuildProperties
Username:
Password:
To keep the current setting or skip a prompt, leave the line blank
Do you wish to configure Hostname, SSL Port, Signing, or Field Mappings? (Y/N) : N
Information needed to process the ssl key store:
Key Store Password:
```