

Configuring Workstars

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

Prerequisite

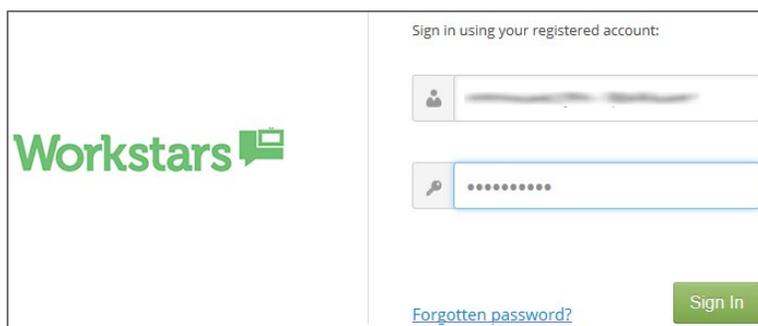
Browser Requirements: Internet Explorer 11 and above

To configure Workstars for SSO by using SAML:

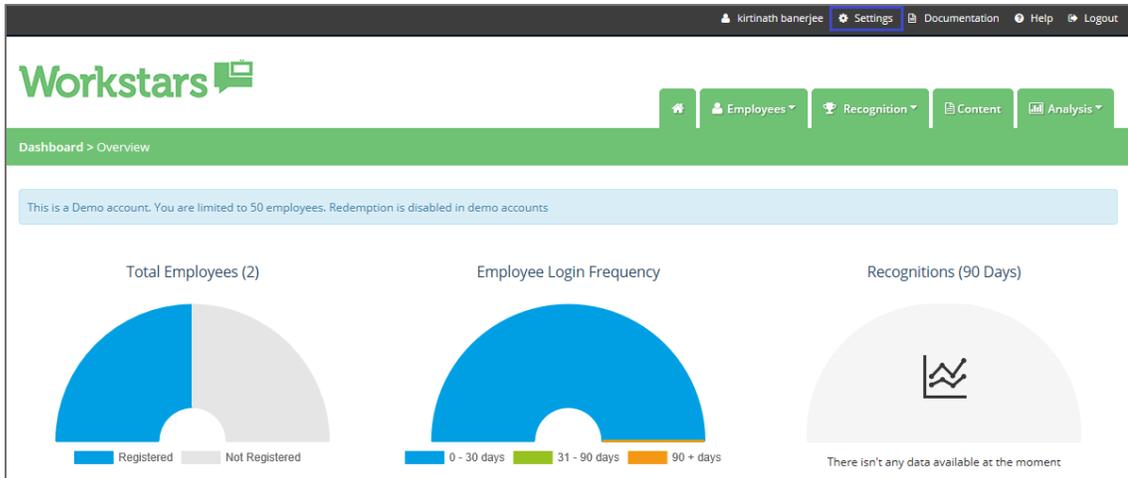
1. Contact the Workstars support team to enable SSO.

Note: The support team will create an admin account and provide the logon link and credentials.

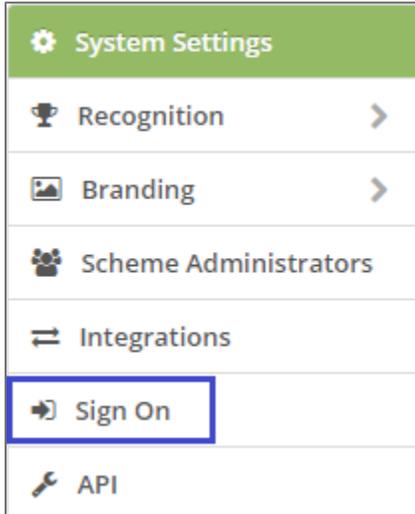
2. In a browser, type <https://<customer domain>.workstars.com/admin/login> and press **Enter**.
3. Type your Workstars admin account credentials (**Email** and **Password**) and click **Sign In**.



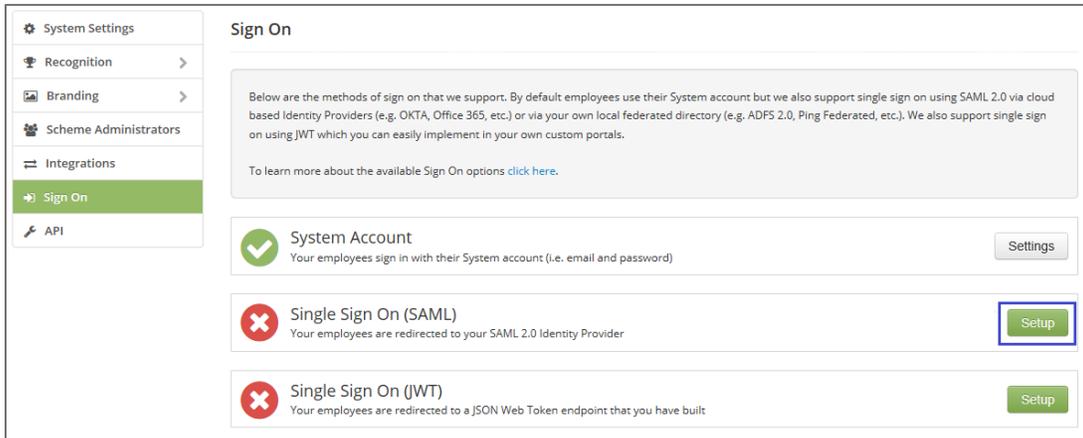
4. Click **Settings** present at the top of the page.



- In the left panel, click **Sign On** under **System Settings**.



- Click **Setup** in the **Single Sign On (SAML)** tile.



- In the **Single Sign On (SAML) – Settings** page, enter the values for the following fields:

Field Name	Description
Identity Provider	Citrix
Identity Provider Entity ID	URL given by your IdP that will be used to identify themselves in the authorization process
X509 Certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate----- Note: The IdP Certificate is provided by Citrix and can be accessed from the link below: https://ssb4.mgmt.netscalergatewaydev.net/idp/saml/templatetest/idp_metadata.xml
SAML SSO URL	IdP logon URL

Remote Logout URL	IdP logout URL
Name ID	Email ID of the user

Single Sign On (SAML) - Settings

To update the settings for your 'Identity Provider' please enter them below and press confirm. Please be aware that these changes will be applied immediately. If you would like to change to an alternative 'Identity Provider' please disable Single Sign On using SAML and run the setup again.

Identity Provider  NetScaler

Identity Provider Entity ID  [Redacted]

x509 Certificate  -----BEGIN CERTIFICATE-----
[Redacted]

SAML SSO URL  https:// [Redacted]

Remote Logout URL  [Redacted]

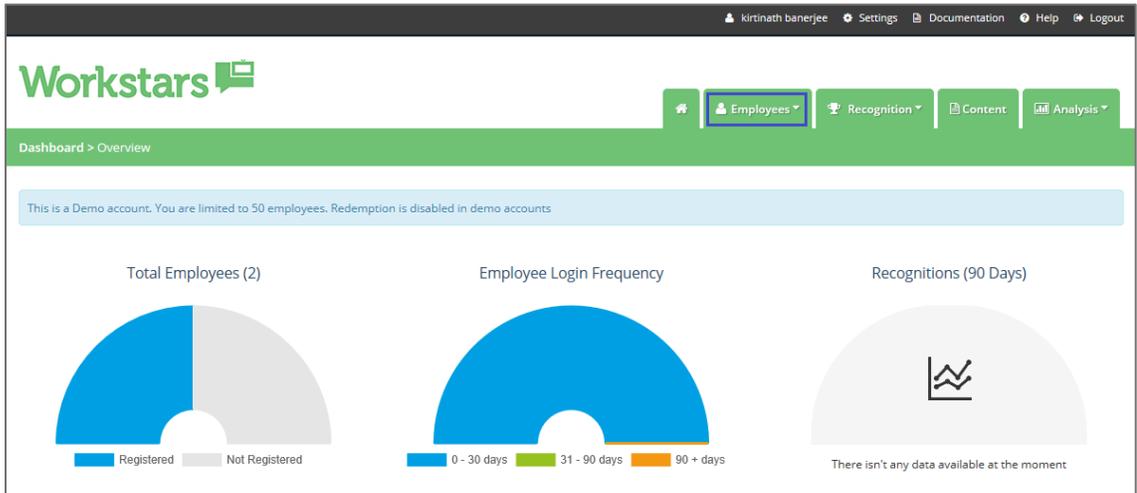
Name ID  Email (Default) 

IP Ranges  [Redacted]

8. Click **Confirm**.

9. Click **Enable**.

10. To add a user, click the **Employees** icon and select **Employees** from the drop-down list.



11. In the **Employees** page, click the **Add Employee** button.

The screenshot shows the 'Employees' page with an 'Add Employee' button in the top right corner. Below the button is a table with the following data:

Employee ID	Name	Reporting Group	Status	Added	Registered	Action
[Redacted]	[Redacted]	[Redacted]	Active	13/08/2018	13/08/2018	Manage
[Redacted]	[Redacted]	[Redacted]	Active	10/08/2018	-	Manage

12. Enter the employee ID, forename, and surname under **Add Employee**.

The screenshot shows the 'Add Employee' form with the following input fields:

- Employee ID
- Forename
- Surname

13. Enter the employee position details under **Position Details**.

Field Name	Description
Job Title	Employee's job title.
Reporting Group	Select Director from the drop-down list.
Manager	Enter admin username.
Is Director	Click the Yes radio button.
Is Manager	Click the Yes radio button.
Start Date	Employee start date.
Employee Type	Select Employee from the drop-down list.

Position Details

These details relate to how and where the employee works within your organisation.

Job Title ?

Reporting Group ?

Manager ?

Is Director ? No Yes

Is Manager ? No Yes

Start Date ?

Employee Type

14. Enter the employee's email address under **Contact Details**.

Contact Details

Details on how your other scheme administrators can contact the employee

Email ?

15. Click **Add Employee**.

A verification mail will be sent to the registered email address. Added user needs to verify from that link.