

Configuring Yodeck

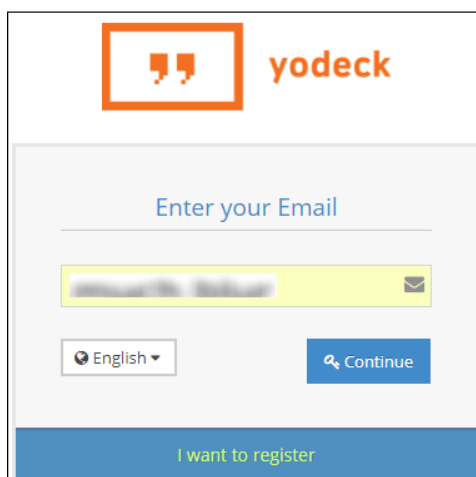
Configuring Yodeck for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on Yodeck by using the enterprise credentials.

Prerequisite

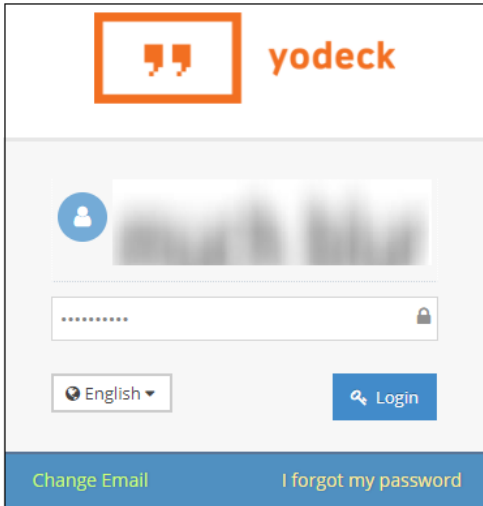
Browser Requirements: Internet Explorer 11 and above

To configure Yodeck for SSO by using SAML:

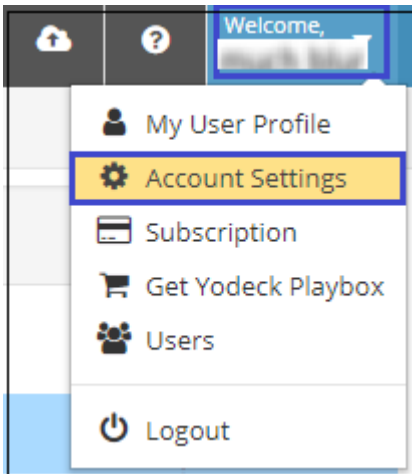
1. In a browser, type <https://yodeck.com> and press **Enter**.
2. On the home page, click **sign in**.
3. Type your Yodeck admin email address and click **Continue**.



4. Type your Yodeck admin password and click **Login**.











5. In the home page, click the user profile that is present at the top-left corner of the screen, and select **Account Settings**.



6. In **Home > Account Settings** page, click the **SSO (Single Sign-On)** tile.


Home > Account Settings

	Account Subscription Upgrade your Yodeck Subscription. All Plans FREE for 1 screen.	Enterprise (Free) - 1 screens	Upgrade for FREE
	Buy a Player or Build one Buy a Yodeck Player and see the magic on your screen, or build one yourself.	\$79 per Player	Buy
	Users Add Users to your Account with different levels of access.	1 Users	Manage
	Workspaces Set up spaces for Content and Monitors, and assign Users with Roles on them.	Enterprise 0 Workspaces	Manage
	Custom Roles Define Roles with custom permissions to reflect your needs.	Enterprise 0 Custom Roles	Manage
	Audit Log Detailed records of activity for all Users within your Account.	Enterprise Enabled	View
	Password Policy Enforce password strength, expiry, and reset options.	Enterprise Disabled	Configure
	SSO (Single Sign On) Set up Single Sign On with your SAML Identity Provider.	Enterprise Disabled	Configure

7. In the **SSO (Single Sign ON)** page, enter the values for the following fields:

Field	Description
Enable SAML	Select ON .
Digest Algorithm	Select sha256 from the drop-down list.
Service Metadata URL	Copy the metadata XML URL provided in IdP configuration.
XML	Browse, 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/template/test/idp_metadata.xml
Identifier, Assertion Consumer Service and Logout Service	Note the Identifier, Assertion Consumer Service and Logout Service as it is required for IdP configuration.
Entity Id, Login URL and Logout URL	Import the XML metadata file. Entity Id, Login URL and Logout URL fields are filled automatically.

SSO (Single Sign On)

Enable SAML ON 

Digest Algorithm

Service Metadata URL

Import From URL
 Import From XML

XML

Identifier

Assertion Consumer Service

Logout Service

Entity Id

Login URL

Logout URL

Use Default NameID
 Use Attribute

8. Finally, click **Save**.