# Configure QAComplete for Single Sign-On

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

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure QAComplete for SSO by using SAML:

1. In a browser, type https://login.qacomplete.smartbear.com/common/ and press **Enter**.

2. Type your QAComplete admin account credentials (**User Name** and **Password**) and click **SIGN IN**.
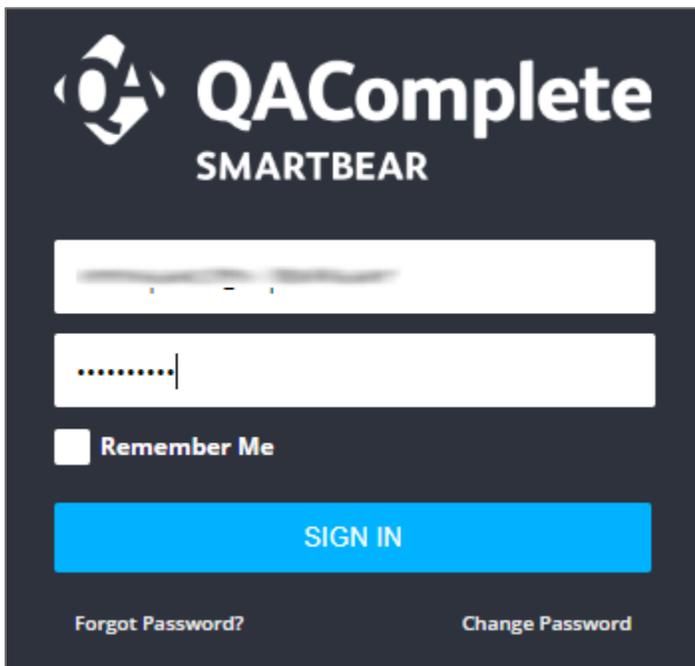
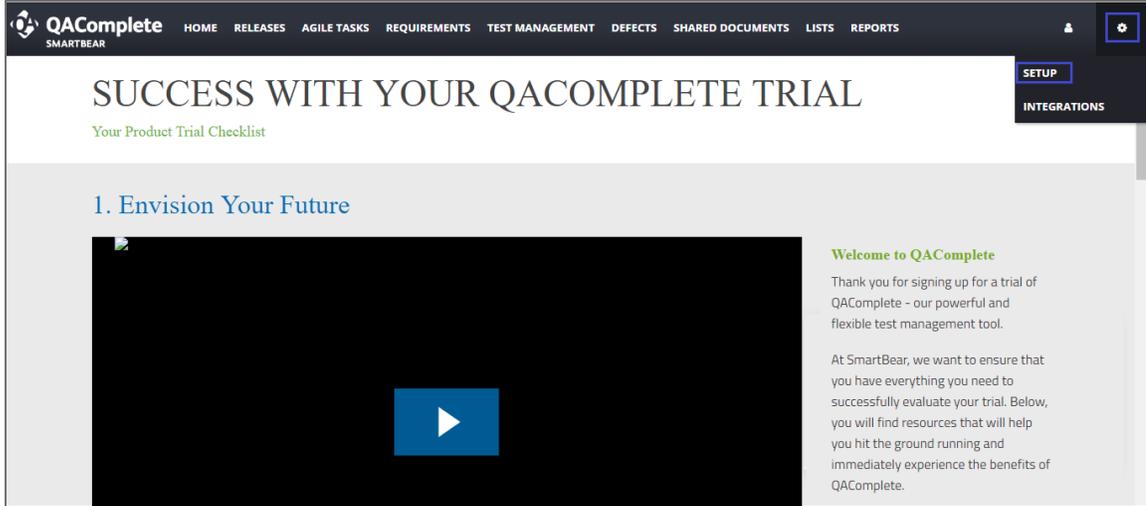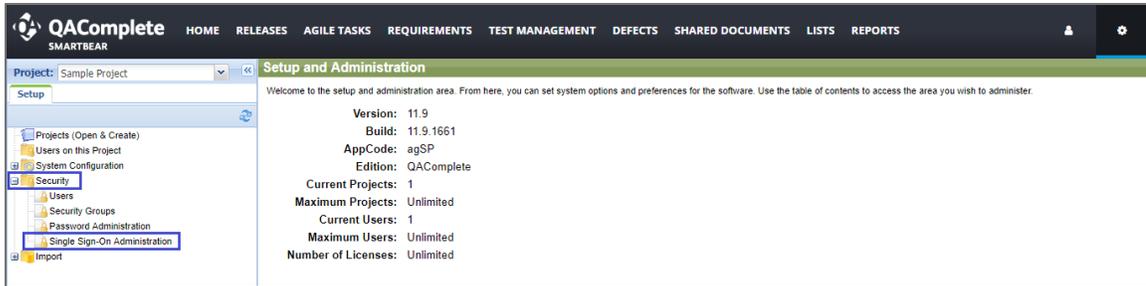3. In the dashboard page, click the Settings icon in the top-right corner and select **SETUP**.

4. In the left pane, click **Security > Single Sign-On Administration**.

5. In the **Single Sign-On Administration** page, select the **Use Single Sign-On** check box and enter the values for the following fields:

Required Information	Description
Identity Provider Single Sign-On URL	IdP logon URL
Identity Provider Issuer	Issuer URL
X.509 Certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with - - - - -Begin Certificate- - - - - and - - - - -End Certificate- - - - - **Note:** The IdP metadata is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app. https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml

Single Sign-On Administration

To enable single sign-on, you should first configure the application in the identity management service. Then enter the information you received and adjust the needed settings:

Domain name: Domain name is your company name used in the application (without spaces, digits and punctuation marks). You can find it on the Settings System Configuration | System Options page. It also can include your department ID.

Identity Provider Single Sign-On URL: Your identity provider will use this URL to log users in. A SAML assertion will be sent to this location with a HTTP post.

Identity Provider Issuer: The unique identifier of the identity provider.

X.509 Certificate: The application will use this certificate to authenticate the identity provider.

Default Project: The users who authenticate for the first time will automatically join this project.

Default Security Group: The users who authenticate for the first time will automatically join this security group.

Default Time Zone: The default time zone for the new user.

Allow Standard (non-SSO) Authentication: Specifies whether the non-administrator users can use the standard QAComplete authentication screen for logging in.

☑ Use Single Sign-On

Single Sign-On Settings

Domain name:	
Login url:	
Identity Provider Single Sign-On URL:	
Identity Provider Issuer:	
X.509 Certificate:	
Default Project:	All Projects ▼
Default Security Group:	Security Administrator ▼
Default Time Zone:	GMT+05.5 New Delhi ▼
Allow Standard (non-SSO) Authentication:	☐

[Save Changes]

6. Finally, click **Save Changes**.