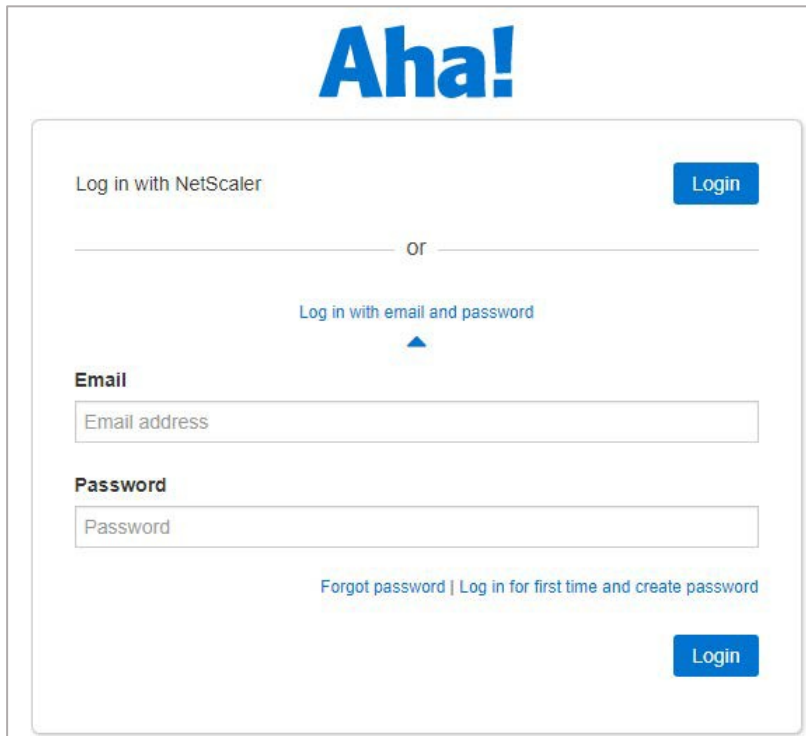


Configuring Aha


Configuring Aha for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Aha using their enterprise credentials.

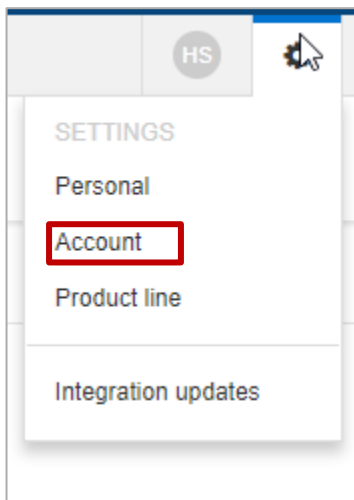
To configure Aha for SSO through SAML, follow the steps below:

1. In a browser, type <https://ctxnsqa.aha.io> and press Enter.
2. Click **Log in with email and password**.
3. Log on to your Aha account.

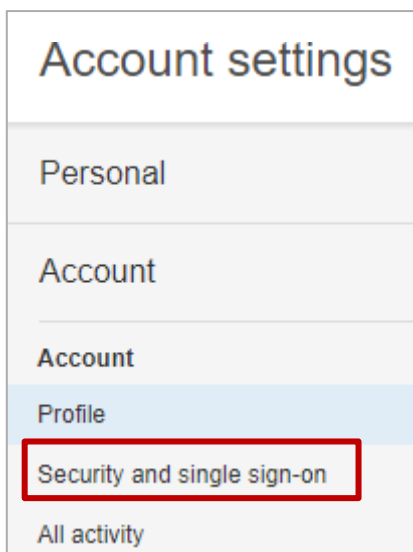


The screenshot displays the Aha! login interface. At the top center is the 'Aha!' logo in blue. Below it, there are two login options. The first is 'Log in with NetScaler' with a blue 'Login' button to its right. A horizontal line with 'or' in the center separates this from the second option, 'Log in with email and password', which is highlighted in blue. Below this option is a small blue upward-pointing triangle. Underneath are two input fields: 'Email' with a placeholder 'Email address' and 'Password' with a placeholder 'Password'. At the bottom of the form, there is a link for 'Forgot password | Log in for first time and create password' and another blue 'Login' button.

4. On the **Home** page, at the upper-right corner, click the SETTINGS icon  and click **Account**.



5. In the left pane, under Account, click **Security and single sign-on**.



6. In the right pane, in the Single sign-on section, specify the following information:

Read how to configure SAML single sign-on on the [support site](#).

1 Name
Give this single sign-on provider a name that will be displayed to users.

2 Configure using Metadata URL Metadata file Manual settings

Single sign-on endpoint 3
The URL for SAML single sign-on at the identity provider.

Certificate fingerprint 4
The fingerprint of the certificate (not the entire certificate) in 00:00:00... format. Separate multiple fingerprints with commas.

SAML consumer URL 5
This is the URL that the identity provider will redirect users to after login.

SAML service provider metadata URL 6
This URL may be required by some identity providers.

SAML entity ID 7
Unique identifier for the service provider (Aha!).

8 Certificate fingerprint algorithm
The algorithm used to generate the certificate fingerprint (default is SHA1).

- i. **Name** – enter the IdP name.
- ii. **Configure using** – click **Manual settings**.
- iii. **Single sign-on endpoint** - enter the NetScaler URL followed by /saml/ login. For example: `https://<customerFQDN>.com/saml/login`
- iv. **Certificate fingerprint** – paste the certificate fingerprint.
To add fingerprint of the NetScaler IDP SAML Signing certificate, follow the steps below:
 - a. Remotely access your NetScaler instance using PuTTY.
 - b. Log on to Shell by typing Shell.
 - c. Navigate to /nsconfig/ssl folder (`cd /nsconfig/ssl`) and press Enter.
 - d. Type `openssl x509 -in certificatename.shell.pem -fingerprint -noout` and press Enter.
 - e. Copy the fingerprint that has been generated and paste that in the Certificate fingerprint box.
- v. **SAML consumer URL** – displays the Assertion Consumer Service URL.
Note: Copy this value to use it while configuring NetScaler for SSO for the Assertion Consumer Service URL field.
- vi. **SAML service provider metadata URL** – displays metadata URL. Access this URL to download an XML file that contains data such as endpoints, supported bindings,

identifier, and public keys required for interaction with SAML-enabled identity or service provider.

- i. **SAML entity ID** – displays the unique identifier that you can use for the SP Entity ID field while configuring NetScaler for SSO.
 - ii. **Certificate fingerprint algorithm** - click the fingerprint algorithm from which you generated the IdP signing certificate fingerprint, in this case SHA1.
7. Click **Save Configuration**.

