

Configure Automox for Single Sign-On

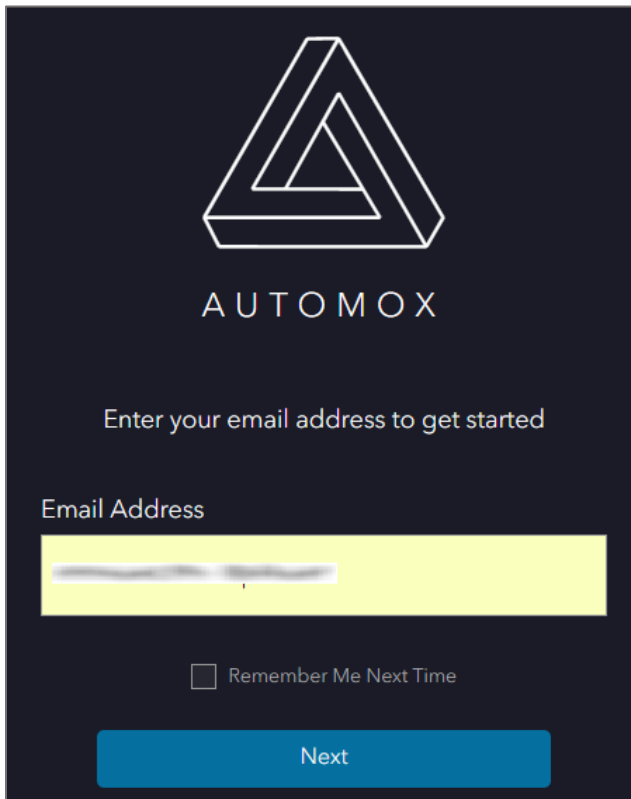
Configuring Automox for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Automox by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

To configure Automox for SSO by using SAML:

1. In a browser, type <https://console.automox.com/login> and press **Enter**.
2. Type your Automox email address and click **Next**.



AUTOMOX

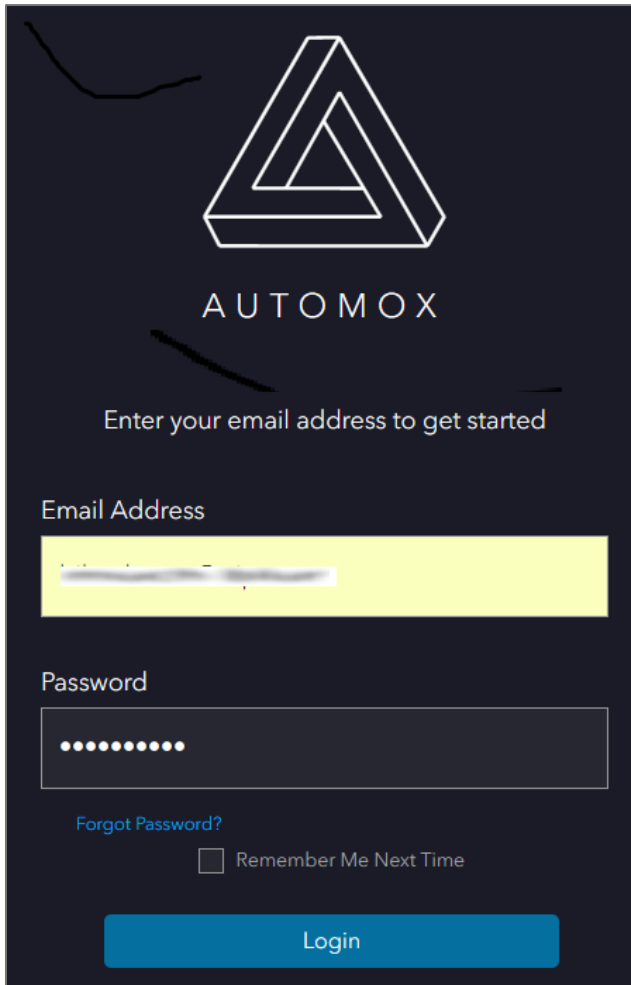
Enter your email address to get started

Email Address

Remember Me Next Time

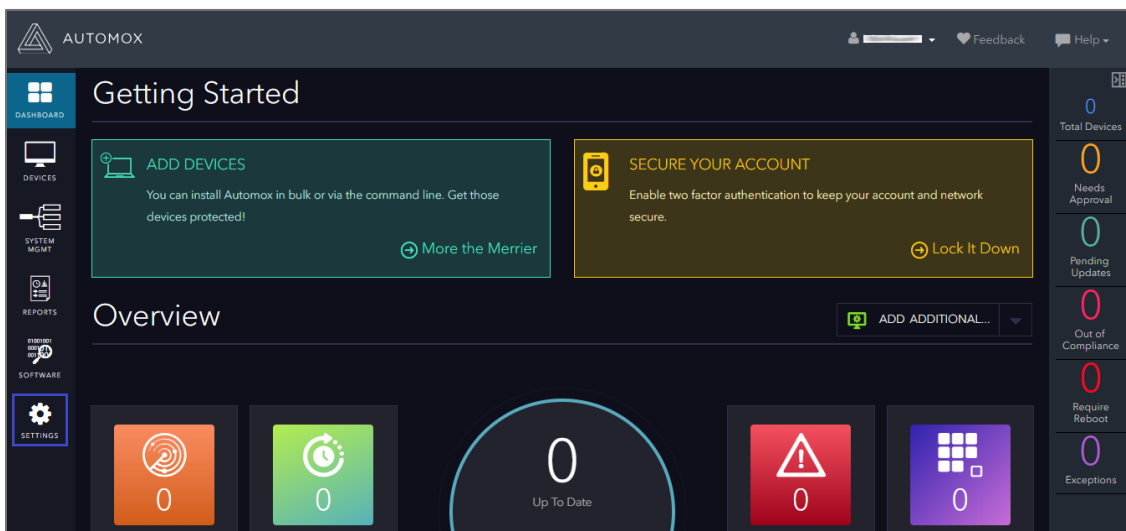
Next

3. Type your Automox password and click **Login**.



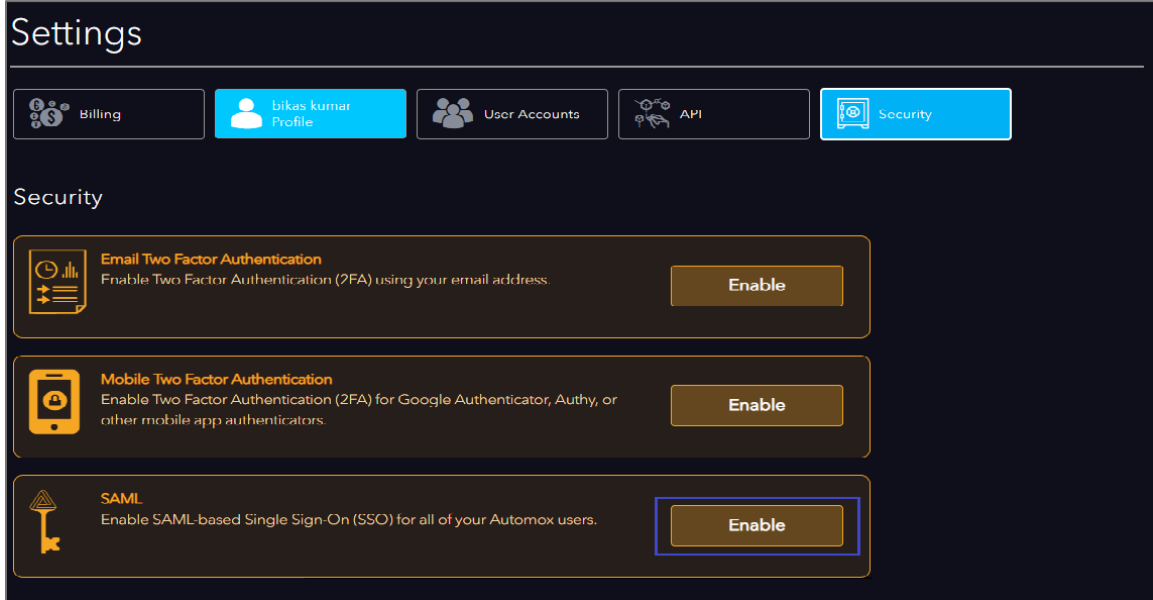
The image shows the Automox login page. At the top center is the Automox logo, a white geometric shape resembling a triangle with a smaller one inside, set against a dark background. Below the logo, the word "AUTOMOX" is written in white capital letters. Underneath, the text "Enter your email address to get started" is displayed. There are two input fields: "Email Address" and "Password". The "Email Address" field is highlighted in yellow. Below the "Password" field, there is a link for "Forgot Password?" and a checkbox labeled "Remember Me Next Time". At the bottom of the form is a blue "Login" button.

4. In the dashboard page, click **Settings** from the left panel.



The image shows the Automox dashboard. The top left corner features the Automox logo and the word "AUTOMOX". The top right corner has a user profile icon, a "Feedback" button, and a "Help" dropdown menu. The main content area is titled "Getting Started" and contains two cards: "ADD DEVICES" (with a "More the Merrier" link) and "SECURE YOUR ACCOUNT" (with a "Lock It Down" link). Below this is an "Overview" section with an "ADD ADDITIONAL..." button. The bottom of the dashboard features a row of five colored tiles: an orange tile with a fingerprint icon and "0", a green tile with a clock icon and "0", a large white circle with "0" and "Up To Date" below it, a red tile with a warning triangle icon and "0", and a purple tile with a grid icon and "0". On the left side, there is a vertical navigation menu with icons for "DASHBOARD", "DEVICES", "SYSTEM MGMT", "REPORTS", "INVENTORY AND COMPLIANCE", "SOFTWARE", and "SETTINGS" (which is highlighted with a blue box). On the right side, there is a vertical status bar with icons and numbers for "Total Devices", "Needs Approval", "Pending Updates", "Out of Compliance", "Require Reboot", and "Exceptions".

- In the **Settings** page, click the **Security** tab.



- Click **Enable** in the **SAML** tile.
- In the pop-up window, enter the values for the following fields:

Field Name	Description
Entity ID	Issuer ID
x509	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. <a href="https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml">https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml
Login URL	IdP logon URL

Automox ACS URL: <https://console.automox.com/saml/acs?o=...>

Automox Entity ID: <https://console.automox.com/saml/metadata>

To setup SAML, please provide the following information: Entity ID, x509, and Login URL. [Toggle XML](#)

Entity ID

x509

```
-----BEGIN CERTIFICATE-----  
[Redacted Certificate Content]  
-----END CERTIFICATE-----
```

Login URL

(Optional) Logout URL

(Optional) Provision New Users - When enabled, a new account will be created when users authorized to use Automox in your SSO provider attempt login.

Note: Note down the **Automox ACS URL** and **Automox Entity ID** for IdP configuration.

8. Finally, click **Save**.