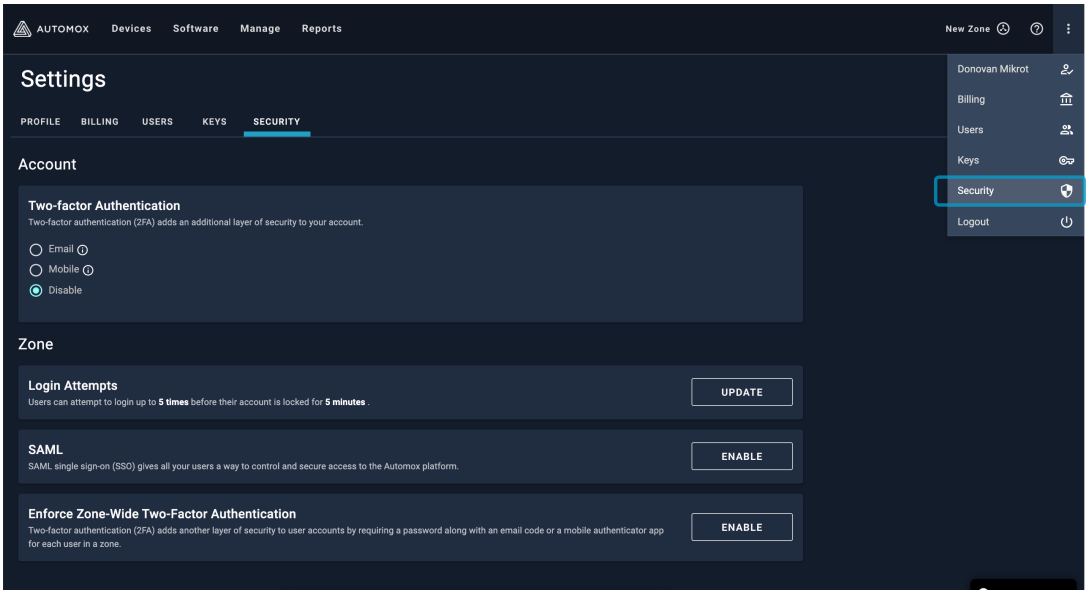
Security

You can manage security-related tasks for accounts and zones from the **Settings > Security** page.

> The term "organization" is now "zone". For more information, refer to Global Zone Management.



Account

The account refers to the individual user account. From the **Settings > Security** tab, you can configure authentication for your account.

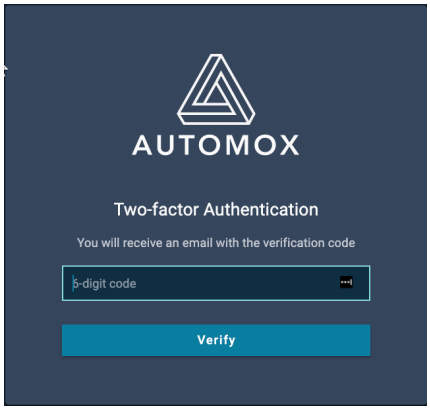
> To access Settings, go to the menu (⋮) in the upper right of the console.

You can disable authentication and just keep the default setting, which requires only an email address and password. You can enable email or mobile authentication, as described in this section.
Note: If 2FA is enforced for the zone, you cannot disable authentication.

Enabling Email Two-factor Authentication

You can enable email two-factor authentication (2FA) for your account.

1. Select **Email** from the Two-factor Authentication section.
2. The next time you log in to the Automox console using your email address and password, you will also need to enter the verification code that was sent to your email address.

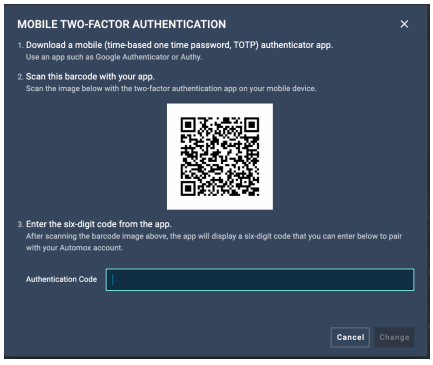


3. To disable this feature, click **Disable** from the same Security > Account page.

Enabling Mobile Two-factor Authentication

You can enable mobile two-factor authentication (2FA) using Google Authenticator, Authy, or other mobile app.

1. Download a TFA mobile app such as Google Authenticator or Authy.
2. Install the app and open it.
3. From the Automox console, go to Settings > Security and select **Mobile** from the Two-factor Authentication section.
4. From the Mobile Two-factor Authentication window, you must scan the QR code with your mobile device to pair it with the Automox console.
5. Enter the code that appears. Depending on the mobile app you are using, you might need to enter a second code.



Resetting mobile two-factor authentication

> If you lose access to the mobile authentication method, contact the Zone Administrator to regain access to the user account.

Disabling Two-factor Authentication

To disable either email or mobile two-factor authentication, click **Disable** from the Security > Settings

page.

> **Note**: When two-factor authentication is enabled for the entire zone, you can switch between email and mobile authentication, but you cannot disable two-factor authentication. See Enforce Zone-Wide Two-factor Authentication.

Zone

Only Zone Administrators have permission to configure the following zone security settings:

- Login Attempt Settings
- SAML
- Enforce Zone-Wide Two-Factor Authentication

Login Attempt Settings

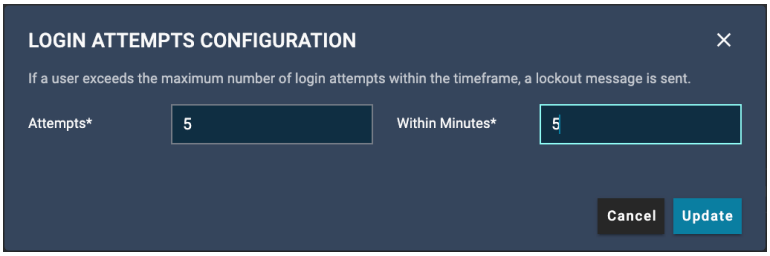
You can set the number of login attempts to the Automox platform that a user can make within a time frame before the account is locked.

1. Click **Update** to open the Login Attempts Configuration dialog box.
2. You can set the following:

   a. Enter the maximum number of login attempts a user can make within a set time frame.

   b. Enter a time frame in minutes. If the user exceeds the allowed number of login attempts during this time frame, the account is locked.
3. Click **Update.**

In this example, the user can attempt to login 5 times within a time frame of 5 minutes. If the user exceeds the number of attempts within the 5-minute time frame, the account is locked.



For assistance, contact Automox Support (support@automox.com).

SAML-based Single Sign-on (SSO)

You can enable SAML-based single sign-on (SSO) for all of your Automox users. Automox supports SAML-authentication through Microsoft Azure.

Note:

- It is not possible to have SAML and Zone-Wide Two-Factor Authentication enabled at the same time.
- When SAML-based SSO is enabled, you can no longer sign in using email address and password.

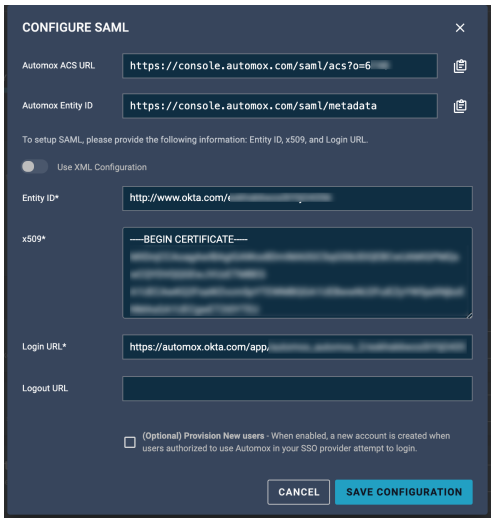
Security Assertion Markup Language (SAML) is a standard for exchanging authentication data between an identity provider and a service provider. With SAML, users can use corporate credentials at a single point of authentication. There are two types of authentication flows. Automox-to-IDP and IDP-to-Automox.

Automox-to-IDP

The Automox-to-IDP authentication flow allows users to provide their email address from the Automox console login page, and be redirected to their configured Identity Provider (IDP) for authentication before being redirected back to the Automox console as the expected user.

For Automox-to-IDP, follow these steps:

1. From the Settings > Security tab in your Automox console, go to the SAML tile.
2. Click **Enable**. This will disable 2FA, if enabled.
3. In the Configure SAML window, enter the following information that is provided by your Identity Provider:
    - Entity ID
    - x509
    - Login URL
4. Click **Save Configuration**.

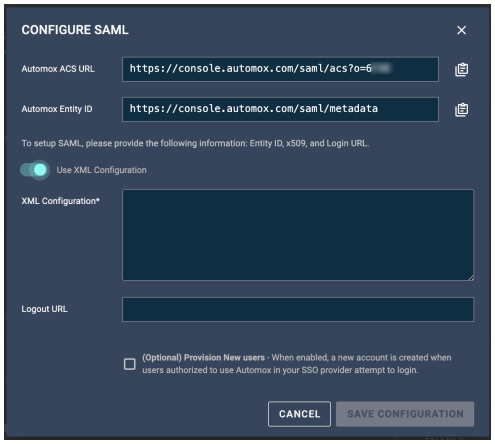


IDP-to-Automox

The IDP-to-Automox authentication flow allows users to log into the Automox console directly from their IDP dashboard. This is a common flow in organizations that utilize more than one SSO-enabled

service.For IDP-to-Automox, follow these steps:

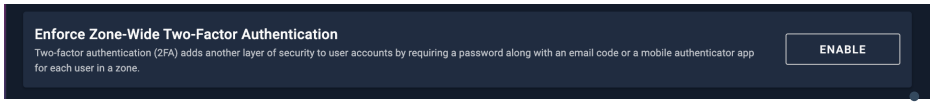
1. From the Settings > Security tab in your Automox console, go to the **SAML** tile.
2. Click **Enable**. This will disable 2FA, if enabled.
3. In the Configure SAML window, switch on **Use XML Configuration**.
4. Enter the XML Configuration information and click **Save Configuration**.



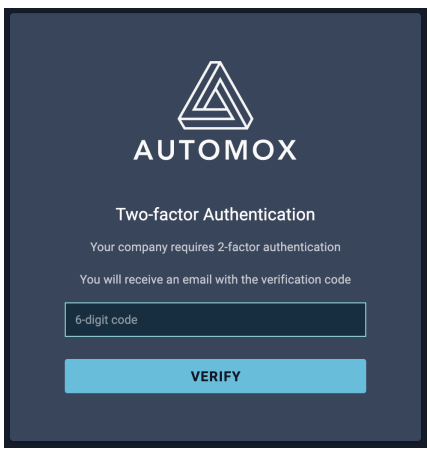
Enforce Zone-Wide Two-factor Authentication

To ensure all users in a zone are on the same level of security for compliance, a zone administrator can enforce two-factor authentication (2FA) for all users.

- From the Settings > Security tab, go to **Enforce Zone-Wide Two-factor Authentication** and click **Enable**.



- If a user does not have 2FA enabled already and 2FA is enforced, the user is redirected to the verification code page. A message explains that 2FA has been enabled at a zone level. The user is instructed to check the associated email account for the verification code.



- A user can switch to mobile authentication, if desired, from the Settings > Security > Accounts section. This is described in Enabling Mobile Two-factor Authentication. At this time it is not possible for an administrator to enforce mobile 2FA.
- When an administrator resets 2FA for a user account (Resetting a User Account), this always resets it back to verification by email.

Refer also to User Accounts for details about enabling and disabling 2FA for user accounts.