Two-factor Authentication

How Two Factor Authentication works:

Access via a web browser:

- **Step 1**: User logs in with their Username and Password
- **Step 2**: If the entered password is correct, the user will receive a unique and random one-time password. (via SMS/Voice call or QR Code as per TFA configuration)
- **Step 3**: Provide the one-time password (OTP) in the browser. If correct, access to the account is granted.

Access via POP/ IMAP or Active Sync protocols:

- **Step 1**: The user generates a unique Application-specific Password for each external application used.
- **Step 2**: During the configuration of the Zoho account in the application, provide the 12 digits Application-specific Password, instead of the regular password.
- **Step 3**: Upon successful validation, you will be able to access your account.

Given that application-specific passwords never expire, you will not be required to update the password in your application, even if your web password expires. You can revoke an application-specific password from the TFA settings to remove access for a particular application. Apart from that, during password reset a user can revoke an application-specific password by revoking auth tokens.

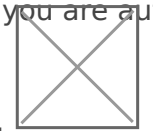
Via Zoho Mail Apps for iOS and Android (Apps created and published by Zoho):

Zoho Mail provides mobile applications (iOS and Android) to access your Zoho Mail and Streams with its full set of features from smartphones. You can directly login to your account via these apps without application-specific passwords. And when two-factor authentication is enabled, all you need to provide is the one-time password.

- **Step 1**: User logs in with Username and Password.
- **Step 2**: User gets a secure code via SMS/ Voice call or QR Code app linked with the account during set up.
- **Step 3**: The user provides the secure code in the mobile app, to access the account.

Enable two-factor authentication for your organization

When you enable TFA to your organization, all the users part of your organization will be required to provide the additional security code to login and access their account. To enable TFA for your organization,

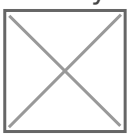
1. Login to Zoho Mail Admin Console
2. Navigate to **Security and Compliance** in the left pane.
3. Under Security, go to **TFA** and toggle it to ON
4. Re-authenticate and verify your identity to perform this action, as this step is necessary to confirm that you are authorized to make changes to the security settings of your organization. 

After the administrator enables TFA, the users will be prompted to choose their preferred TFA method, the next time they log in. If you want to disable TFA to the entire organization, you can follow the same steps and toggle it off

For information on the mode of TFA, refer to this help page.

Enable/ Disable TFA for Specific Users:

The administrator can enable or disable the TFA status for users from the Control Panel.

1. Login to Zoho Mail Admin Console
2. Navigate to **Users** in the left pane and click the user you would like to enable or disable TFA.
3. Go to Security settings, click TFA, and toggle it off
4. To proceed with this action, you will need to re-authenticate your session to verify your identity for security purposes.


?Reset TFA for specific users

The administrator can reset the TFA for users, in case they lost the mobile device or do not have access to the mobile device they used at the time of TFA activation. To reset the TFA of a user,

1. Login to Zoho Mail Admin Console
2. Navigate to **Users** in the left pane and click the user you would like to reset TFA.
3. Go to Security settings, click TFA, and click **Reset TFA**.
4. You'll be prompted to re-authenticate your session to verify your identity for security reasons.

Once reset, the user can set up their TFA mode afresh during sign-in.

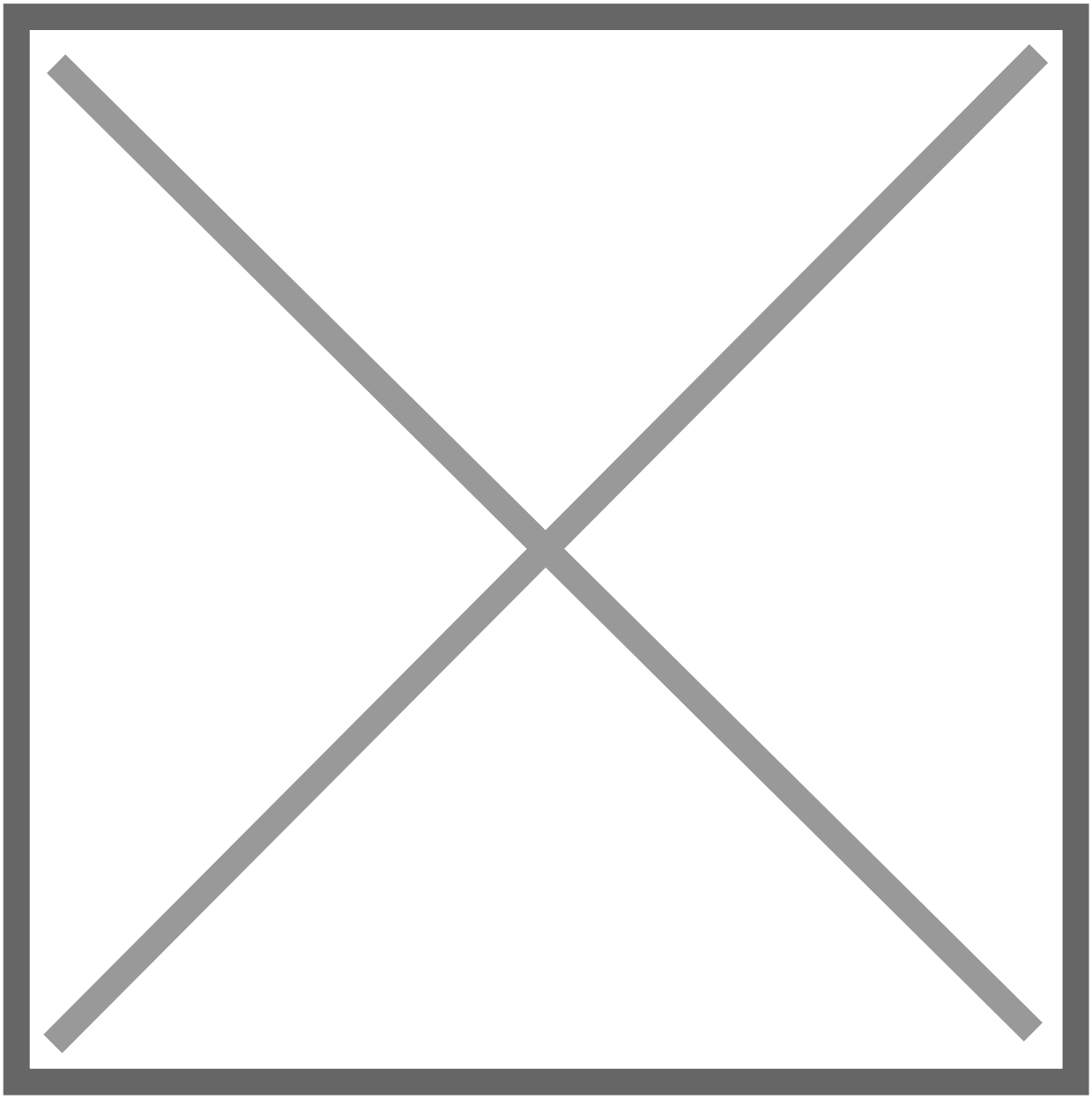
Note:

- Whenever you make any changes to the TFA settings of a specific user or the entire organization, it is mandatory to re-authenticate your session to ensure that only authorized users can perform this sensitive action.
- Re-authentication will be done using the MFA (Multi-Factor Authentication) method configured on your account for security purposes. If you do not have MFA configured for your account, you will be prompted to re-authenticate your session using your account password in a new tab or window, depending on your browser preference.
- For TFA (Two-Factor Authentication) updates, re-authentication is required every five minutes after you verify your identity. During this five-minute window, you can make additional changes without needing to re-verify. However, if you attempt to make a change after this period has elapsed, you will need to verify your identity again.

Generating App-Specific Password

If two-factor authentication is enabled for an account, then the users have to provide the application-specific password when they access their account via POP/IMAP or Active Sync. To generate an app-specific password,

1. Login to Zoho Accounts
2. From the left menu, navigate to **Security** and click **App passwords**
3. Click **Generate New Password**.



4. You will be asked to give a name the name of your application for future reference. Enter the name and click **Generate**.

5. Your password will be generated and it can be used to login from one application.

App Specific Password will be required:

1. To authenticate clients use Zoho Mail as an IMAP/ POP account.
2. To sync your Zoho Calendar with calendar clients using CalDAV.
3. To authenticate clients use Zoho Mail as an IMAP/ POP account for organization users with SAML login.

Note:

- The device-specific password will be displayed only once and will be not be displayed again.
- When providing the password in your email clients, enter it without any spaces.
- You can delete an application-specific password whenever you longer use that device or application or want to revoke access to that application.

Revision #1
Created 8 December 2024 16:55:08 by Sam Brost
Updated 8 December 2024 16:55:53 by Sam Brost