

Multi-Factor Authentication using TOTP

Definition
<p>Multi-Factor Authentication (MFA) is a security best practice that adds an extra layer of protection on top of a username and password combination. By requiring an additional authentication code from a trusted device, MFA safeguards access to a user's account even if the password is compromised.</p> <p>There are various authentication methods to implement MFA. The Time-based One-Time Password (TOTP) algorithm is a popular and secure method that automatically generates an authentication code which changes after a certain period of time.</p> <p>TOTP has been adopted as Internet Engineering Task Force standard RFC 6238.</p>

New Feature
This is a new feature in Joget Workflow v6.

- [Configuring Multi-Factor Authentication in the Security Enhanced Directory Manager](#)
- [Activating Multi-Factor Authentication as a User](#)
- [Deactivating Multi-Factor Authentication](#)

Configuring Multi-Factor Authentication in the Security Enhanced Directory Manager

1. As an administrator in Joget Workflow **Settings > Directory Manager**, choose the [Security Enhanced Directory Manager](#) and select **Time-based One-time Password (TOTP) Authenticator** for the **Multi Factor Authenticator** property.


[blocked URL](#)
2. Once the TOTP Authenticator has been enabled, users will be able to enable MFA individually in their user profile.

Activating Multi-Factor Authentication as a User

1. As a user, download and install a TOTP compatible mobile app. For example, on Android and iOS, you can use [Google Authenticator](#) or [Microsoft Authenticator](#).

[blocked URL](#)
2. In your Joget Workflow profile page, click on the **Activate** button in the **Time-based One-time Password (TOTP) Authenticator** property at the bottom of the form.
3. A popup dialog will appear showing the **secret key** and a **barcode**.

[blocked URL](#)
4. Using the TOTP mobile app, scan the **barcode** or key in the **secret key**. The TOTP mobile app will create a new account.

 Save the secret key in a safe place, in case you need to reactivate your account e.g. in case of a lost device.

5. Key in the current generated code displayed in the TOTP mobile app into the **Password** field and click on **Submit**. If the code is valid, MFA is will be activated.

[blocked URL](#)
6. On subsequent logins, you will be prompted for a TOTP code password.

Deactivating Multi-Factor Authentication

1. As a user, you can disable MFA by clicking on the **Deactivate** button in your user profile.
2. Administrators can also disable MFA for a specific user by selecting the user under [Setup Users](#) and clicking on the **Deactivate MFA** button.