

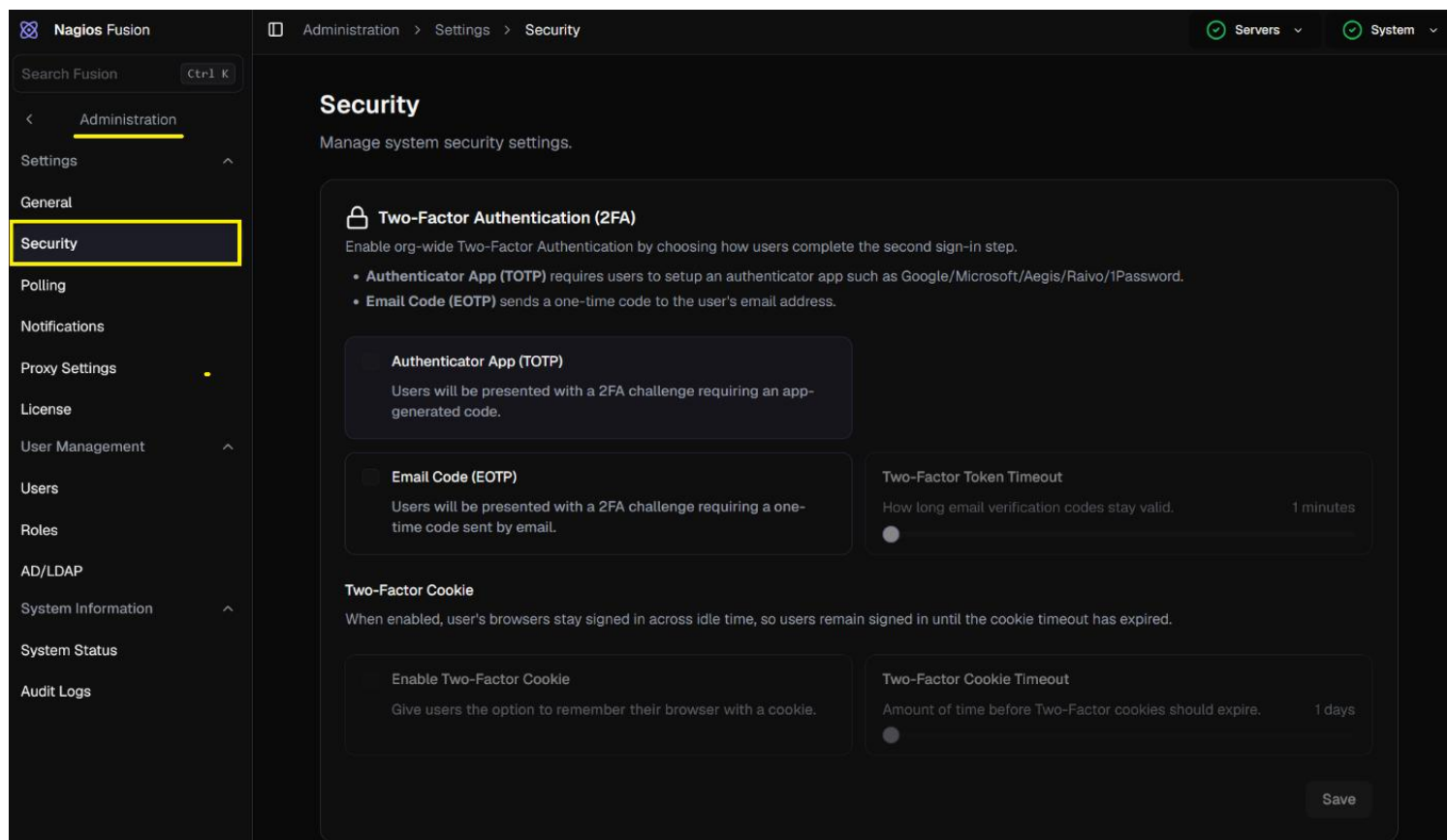
How To Use Two-Factor Authentication In Nagios Fusion 2026R2

Purpose

This document describes how to manage two-factor authentication (2FA) in Nagios Fusion 2026R2+. 2FA can be enabled using an authenticator app or an email code to require a second verification step after password entry for all Fusion users, enhancing security.

Finding Security Settings

To configure 2FA, navigate to **Adminstrating > Settings > Security**.



How To Use Two-Factor Authentication In Nagios Fusion 2026R2

Configuring 2FA

First, choose your 2FA method by clicking the target checkbox.

The screenshot shows the 'Two-Factor Authentication (2FA)' configuration page. At the top, there's a lock icon and the title 'Two-Factor Authentication (2FA)'. Below it, a description states: 'Enable org-wide Two-Factor Authentication by choosing how users complete the second sign-in step.' Two methods are listed: 'Authenticator App (TOTP)' and 'Email Code (EOTP)'. The 'Authenticator App (TOTP)' option is selected, indicated by a checked checkbox. Below the methods, there are two sections: 'Two-Factor Token Timeout' and 'Two-Factor Cookie'. The 'Two-Factor Token Timeout' section has a slider set to '1 minutes'. The 'Two-Factor Cookie' section has a checkbox for 'Enable Two-Factor Cookie' which is unchecked, and a slider for 'Two-Factor Cookie Timeout' set to '1 days'. At the bottom right, there are 'Cancel' and 'Save' buttons. The 'Save' button is highlighted with a yellow box.

Two-Factor Authentication (2FA)

Enable org-wide Two-Factor Authentication by choosing how users complete the second sign-in step.

- **Authenticator App (TOTP)** requires users to setup an authenticator app such as Google/Microsoft/Aegis/Raivo/1Password.
- **Email Code (EOTP)** sends a one-time code to the user's email address.

☒ **Authenticator App (TOTP)**
Users will be presented with a 2FA challenge requiring an app-generated code.

☐ **Email Code (EOTP)**
Users will be presented with a 2FA challenge requiring a one-time code sent by email.

Two-Factor Token Timeout
How long email verification codes stay valid. 1 minutes

Two-Factor Cookie
When enabled, user's browsers stay signed in across idle time, so users remain signed in until the cookie timeout has expired.

☐ **Enable Two-Factor Cookie**
Give users the option to remember their browser with a cookie.

Two-Factor Cookie Timeout
Amount of time before Two-Factor cookies should expire. 1 days

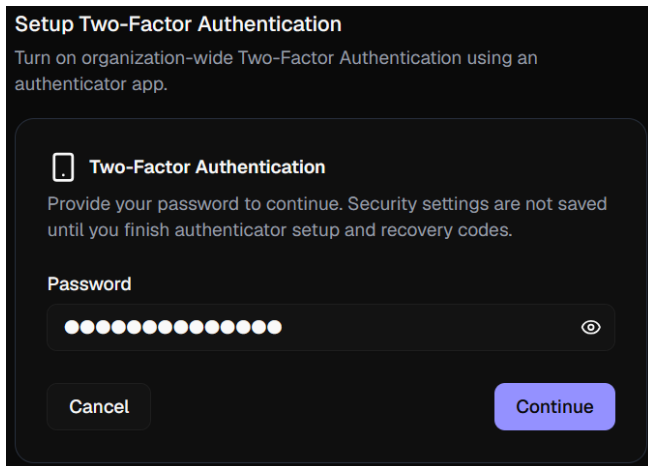
Cancel Save

- [Authenticator App \(TOTP\)](#)
- [Email Code](#)

How To Use Two-Factor Authentication In Nagios Fusion 2026R2

Authenticator App

Once you click Save, you will be brought to a new screen where you will enter your current user password, then click **Continue**.



Setup Two-Factor Authentication
Turn on organization-wide Two-Factor Authentication using an authenticator app.

Two-Factor Authentication
Provide your password to continue. Security settings are not saved until you finish authenticator setup and recovery codes.

Password

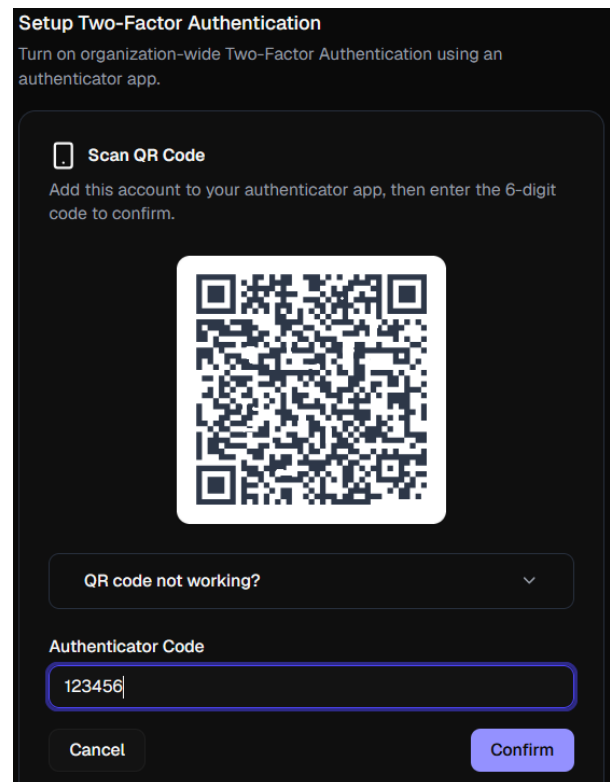
●●●●●●●●●●●●●●●●

Cancel Continue

On the next screen you will find a QR code which you can scan with your Authenticator app.

Scan the QR code, then enter your code in the **Authenticator Code** field, and click **Confirm**.

If you're having trouble scanning the QR code, you can get a setup key in the **QR code not working?** dropdown.



Setup Two-Factor Authentication
Turn on organization-wide Two-Factor Authentication using an authenticator app.

Scan QR Code
Add this account to your authenticator app, then enter the 6-digit code to confirm.



QR code not working? ▾

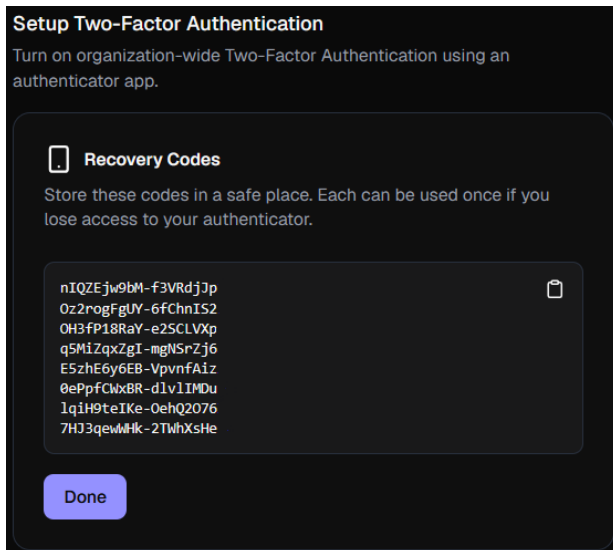
Authenticator Code

123456

Cancel Confirm

How To Use Two-Factor Authentication In Nagios Fusion 2026R2

You will now be presented with several Recovery codes which can be used once each if you lose access to your authenticator.



Store these in a safe place, then click **Done** to finalize setup.

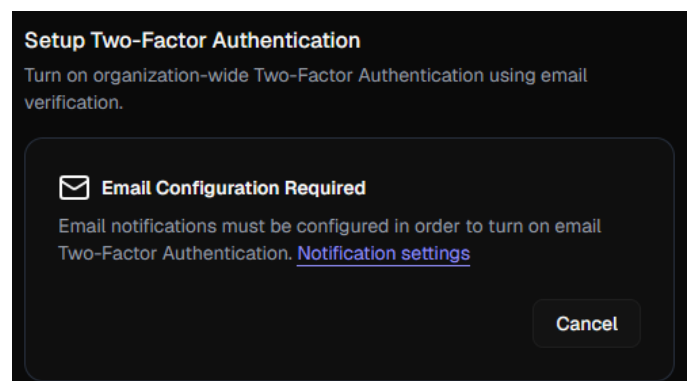
After setup is completed, all other users will need to set up the authenticator app as well next time they log in, as will new users you create going forward when they first access the Fusion web interface.

Email Code

Before choosing this option, you'll need set up Notifications. Full details can be found in this guide:

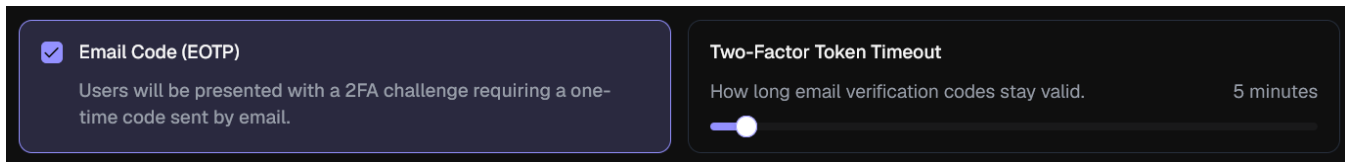
[Understanding Email Sending in Nagios Fusion](#)

If you have not yet done so, you'll see the following notice when you choose the Email Code option and click **Save**:



How To Use Two-Factor Authentication In Nagios Fusion 2026R2

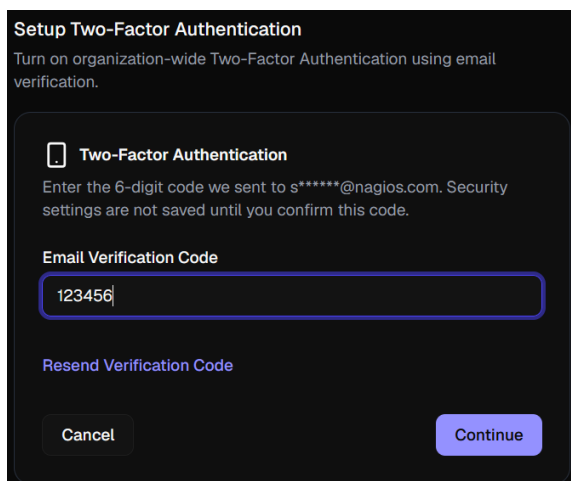
Once your Notification settings are confirmed, check the **Email Code (EOTP)** checkbox, and set your **Two-Factor Token Timeout** to determine how long email verification codes stay valid.



The screenshot shows two configuration panels. The left panel, titled 'Email Code (EOTP)', has a checked checkbox and a description: 'Users will be presented with a 2FA challenge requiring a one-time code sent by email.' The right panel, titled 'Two-Factor Token Timeout', shows a slider set to '5 minutes' with the text 'How long email verification codes stay valid.' below it.

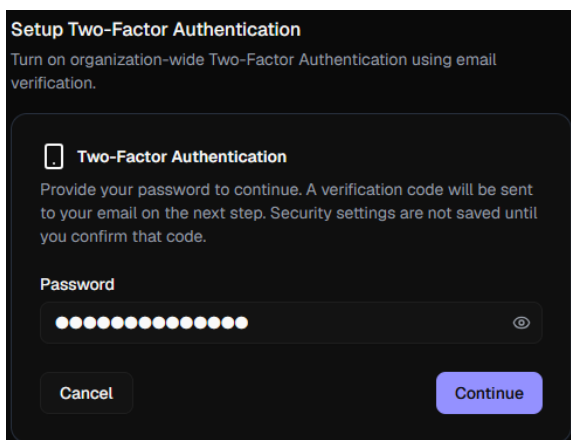
Click **Save** to proceed. This will automatically send a 6-digit code to your user's email address.

In the next section, enter the email code you received in the **Email Verification Code** section, then click **Continue**.



The screenshot shows the 'Setup Two-Factor Authentication' screen. It includes a title, a subtitle 'Turn on organization-wide Two-Factor Authentication using email verification.', and a section titled 'Two-Factor Authentication' with instructions to enter a 6-digit code. Below this is an 'Email Verification Code' input field containing '123456'. There are also links for 'Resend Verification Code', 'Cancel', and 'Continue' buttons.

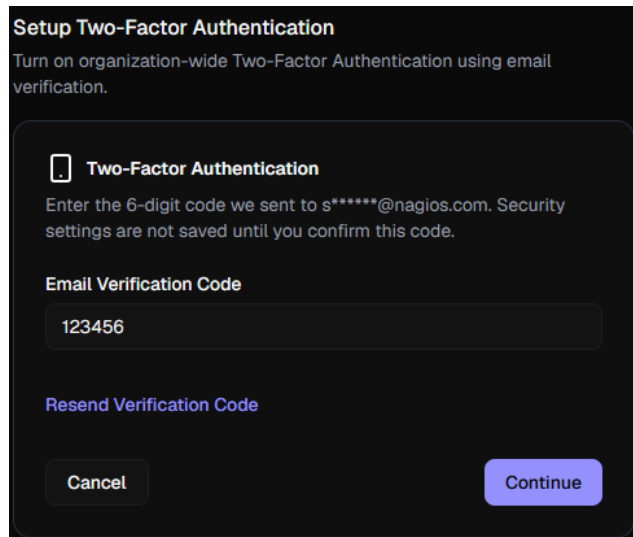
You will now be prompted for your Fusion user password. Enter it, then click **Continue** to proceed.



The screenshot shows the 'Setup Two-Factor Authentication' screen. It includes a title, a subtitle 'Turn on organization-wide Two-Factor Authentication using email verification.', and a section titled 'Two-Factor Authentication' with instructions to provide a password. Below this is a 'Password' input field with masked characters and an eye icon. There are also 'Cancel' and 'Continue' buttons.

How To Use Two-Factor Authentication In Nagios Fusion 2026R2

As a final verification, you will be emailed one more code. Enter the code in the **Email Verification Code** section, then click **Continue** to finish setup.



Setup Two-Factor Authentication
Turn on organization-wide Two-Factor Authentication using email verification.

Two-Factor Authentication
Enter the 6-digit code we sent to s*****@nagios.com. Security settings are not saved until you confirm this code.

Email Verification Code
123456

[Resend Verification Code](#)

[Cancel](#) [Continue](#)

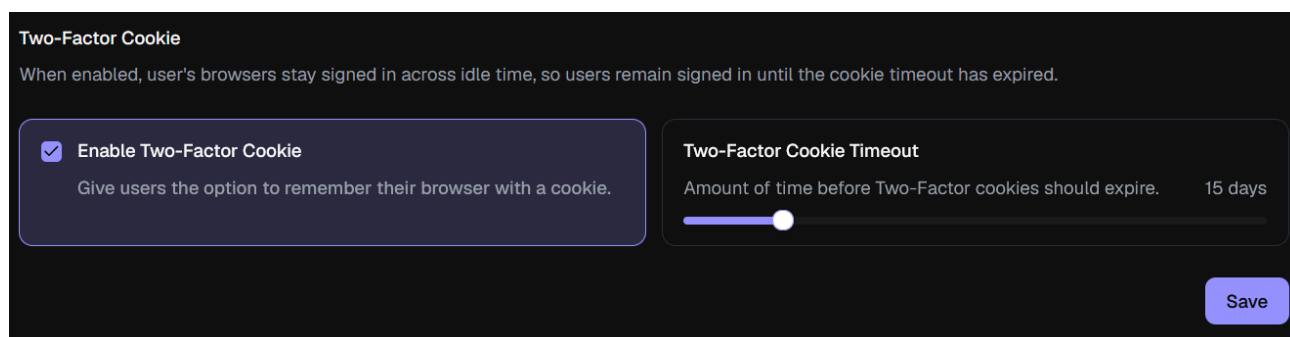
After setup is completed, all users will be emailed and prompted for their code when attempting to login, so it is important to ensure that each Fusion user has a valid email address configured. You can learn more about managing user settings here:

[Managing Users and Roles in Nagios Fusion](#)

Two-Factor Cookie

This optional feature can be used to enable a browser cookie which allows users to log in without needing to enter a 2FA code for a set period of time after each successful 2FA login.

To turn this on, check the **Enable Two-Factor Cookie** checkbox, choose the number of days after which the cookie should expire with the **Two-Factor Cookie Timeout** slider, then click **Save**:



Two-Factor Cookie
When enabled, user's browsers stay signed in across idle time, so users remain signed in until the cookie timeout has expired.

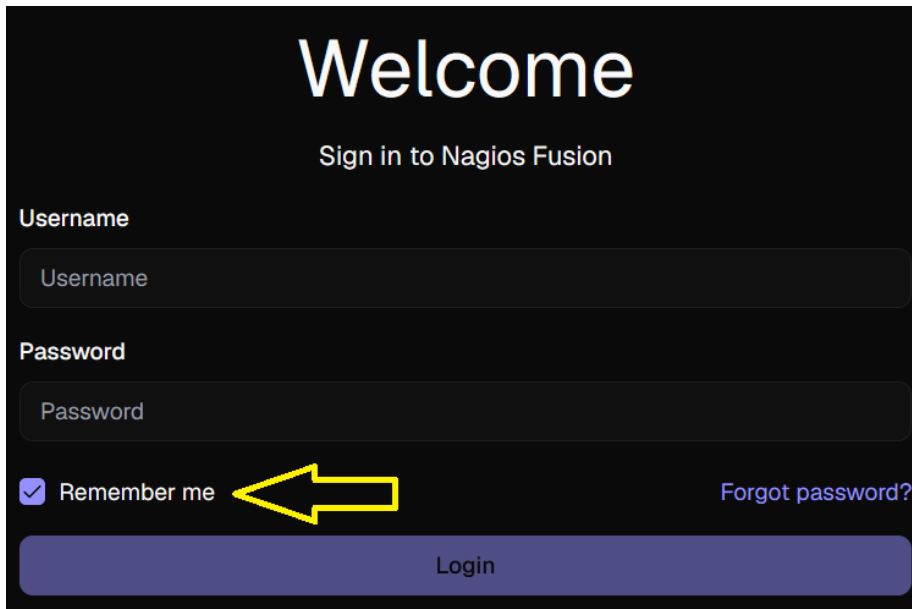
☒ **Enable Two-Factor Cookie**
Give users the option to remember their browser with a cookie.

Two-Factor Cookie Timeout
Amount of time before Two-Factor cookies should expire. 15 days

[Save](#)

How To Use Two-Factor Authentication In Nagios Fusion 2026R2

Once Two-Factor Cookie is enabled administratively, users can check the **Remember me** option on the login page when logging in to leverage the cookie:

A screenshot of the Nagios Fusion login page. The page has a dark background with white text. At the top, it says "Welcome" in a large font, followed by "Sign in to Nagios Fusion" in a smaller font. Below this are two input fields: "Username" and "Password". Under the "Password" field, there is a checkbox labeled "Remember me" which is checked. A yellow arrow points to this checkbox. To the right of the checkbox is a link that says "Forgot password?". At the bottom of the form is a blue "Login" button.

Emergency Deactivate 2FA

In the event that you run into trouble with 2FA and are unable to de-activate it from the user interface by unchecking the active method, Fusion includes a built-in script which can be executed from the command line to deactivate it globally.

To use the script, establish a terminal session with your Nagios Fusion server and run the following commands as root:

```
cd /usr/local/fusion/scripts
./emergency-2fa-off.sh
```

This will de-activate all 2FA methods, as well as Two-Factor Cookie.

All users will now be able to login normally using their user password alone.

How To Use Two-Factor Authentication In Nagios Fusion 2026R2

Finishing Up

This completes the documentation on Using 2FA in Nagios Fusion. If you have additional questions or other support-related questions, please visit the Nagios Support Forum, Nagios Documentation Hub, or Nagios Library:

[Visit Nagios Support Forum](#)

[Visit Documentation Hub](#)

[Visit Nagios Library](#)