

```

<?xml version="1.0" encoding="UTF-8"?><rss version="2.0"
  xmlns:content="http://purl.org/rss/1.0/modules/content/"
  xmlns:wfw="http://wellformedweb.org/CommentAPI/"
  xmlns:dc="http://purl.org/dc/elements/1.1/"
  xmlns:atom="http://www.w3.org/2005/Atom"
  xmlns:sy="http://purl.org/rss/1.0/modules/syndication/"
  xmlns:slash="http://purl.org/rss/1.0/modules/slash/"

  xmlns:georss="http://www.georss.org/georss"
  xmlns:geo="http://www.w3.org/2003/01/geo/wgs84_pos#"
>

<channel>
  <title>2fa - GitHub Changelog</title>
  <atom:link href="https://github.blog/changelog/label/2fa/feed/" rel="self"
type="application/rss+xml" />
  <link>https://github.blog/changelog/label/2fa/</link>
  <description>Updates, ideas, and inspiration from GitHub to help
developers build and design software.</description>
  <lastBuildDate>Thu, 20 Jun 2024 16:28:31 +0000</lastBuildDate>
  <language>en-US</language>
  <sy:updatePeriod>
hourly    </sy:updatePeriod>
  <sy:updateFrequency>
1        </sy:updateFrequency>
  <generator>https://wordpress.org/?v=6.6.1</generator>

<image>
  <url>https://github.blog/wp-content/uploads/2019/01/cropped-github-
favicon-512.png?fit=32%2C32</url>
  <title>2fa - GitHub Changelog</title>
  <link>https://github.blog/changelog/label/2fa/</link>
  <width>32</width>
  <height>32</height>
</image>
<site xmlns="com-wordpress:feed-additions:1">153214340</site>    <item>
  <title>2FA security checkup experience is now improved</title>
  <link>https://github.blog/changelog/2024-06-20-2fa-security-checkup-
experience-is-now-improved</link>

  <dc:creator><![CDATA[Allison]]></dc:creator>
  <pubDate>Thu, 20 Jun 2024 16:28:31 +0000</pubDate>
  <guid
isPermaLink="false">https://github.blog/changelog/2024-06-20-auto-draft</guid>

  <description><![CDATA[<p>GitHub is committed to a
secure software ecosystem and requires most developers who contribute code on
GitHub.com to enable one or more forms of two-factor authentication (2FA).To
ensure that all&#8230;</p>
<p>The post <a href="https://github.blog/changelog/2024-06-20-2fa-security-
checkup-experience-is-now-improved">2FA security checkup experience is now
improved</a> appeared first on <a href="https://github.blog">The GitHub
Blog</a>.</p>
]]></description>

  <content:encoded><![
CDATA[<p>GitHub is committed to a secure software ecosystem and requires most
developers who contribute code on GitHub.com to enable one or more forms of two-
factor authentication (2FA).To ensure that all users stay up to date with their
account security configurations, we are now improving the checkup experience
using various global banners that guide users to review and update their
settings on a more regular basis.</p>
<p>These banners replace the security checkup interstitials that were previously
displayed every 3 months for 2FA users. Each banner calls out the specific
security configuration that needs attention (ex: user only having a single

```

verified email), and will also include a quick link to the corresponding settings page to modify the required settings.

To learn more about the 2FA program, see our April 2024 blog post about [how GitHub is securing millions of developers using 2FA](https://github.blog/2024-04-24-securing-millions-of-developers-through-2fa/), as well as the [About the mandatory 2FA program](https://docs.github.com/en/authentication/securing-your-account-with-two-factor-authentication-2fa/about-mandatory-two-factor-authentication); documentation.

The post [2FA security checkup experience is now improved](https://github.blog/changelog/2024-06-20-2fa-security-checkup-experience-is-now-improved) appeared first on [The GitHub Blog](https://github.blog).

```
<post-id xmlns="com-wordpress:feed-additions:1">78578</post-id>
</item>
<item>
  <title>Enabling reactive 2FA requirements for release
creation</title>
  <link>https://github.blog/changelog/2023-10-31-enabling-reactive-
2fa-requirements-for-release-creation</link>

  <dc:creator><![CDATA[Kevin Duck]]></dc:creator>
  <pubDate>Tue, 31 Oct 2023 19:54:40 +0000</pubDate>
  <guid
isPermaLink="false">https://github.blog/changelog/2023-10-31-enabling-reactive-
2fa-requirements-for-release-creation</guid>

  <description><![CDATA[<p>Enabling reactive 2FA
requirements for release creation</p>
<p>The post <a href="https://github.blog/changelog/2023-10-31-enabling-reactive-
2fa-requirements-for-release-creation">Enabling reactive 2FA requirements for
release creation</a> appeared first on <a href="https://github.blog">The GitHub
Blog</a>.</p>
]]></description>

  <content:encoded><![
CDATA[<p>Users who are not part of the <a href="https://github.blog/2023-03-09-
raising-the-bar-for-software-security-github-2fa-begins-march-13/">mandatory 2FA
program</a> will now be added to it within 24 hours of creating their first <a
href="https://docs.github.com/en/repositories/releasing-projects-on-github/
managing-releases-in-a-repository">release</a>. In August we expanded the 2FA
requirement to include most GitHub.com users that had created a release. Those
groups have now completed their 2FA enrollment, but additional developers have
since created their first release. They will be added to the 2FA program in the
coming days, as will more users over time as they create releases. </p>
<p>Enterprise or organization administrators can learn more about their
users' current 2FA requirements by visiting the <a
href="https://github.blog/changelog/2023-07-31-2fa-requirement-status-on-the-
people-pages/">People page</a> for their enterprise or organization.</p>
<p>To learn more about the 2FA program, see our <a
href="https://github.blog/2023-03-09-raising-the-bar-for-software-security-
github-2fa-begins-march-13/">May 2023 blog post</a>, as well as the <a
href="https://docs.github.com/en/authentication/securing-your-account-with-two-
factor-authentication-2fa/about-mandatory-two-factor-
authentication">About the mandatory 2FA program</a>;
documentation</a>.</p>
<p>The post <a href="https://github.blog/changelog/2023-10-31-enabling-reactive-
2fa-requirements-for-release-creation">Enabling reactive 2FA requirements for
release creation</a> appeared first on <a href="https://github.blog">The GitHub
Blog</a>.</p>
]]></content:encoded>
```

```

        <post-id xmlns="com-wordpress:feed-additions:1">75179</post-id>
    </item>
    <item>
        <title>Passkeys are Generally Available</title>
        <link>https://github.blog/changelog/2023-09-21-passkeys-are-
generally-available</link>

        <dc:creator><![CDATA[Kevin Duck]]></dc:creator>
        <pubDate>Thu, 21 Sep 2023 16:01:56 +0000</pubDate>
        <guid
isPermaLink="false">https://github.blog/changelog/2023-09-21-passkeys-are-
generally-available</guid>

        <description><![CDATA[<p>Passkeys are Generally
Available</p>
<p>The post <a href="https://github.blog/changelog/2023-09-21-passkeys-are-
generally-available">Passkeys are Generally Available</a> appeared first on <a
href="https://github.blog">The GitHub Blog</a>.</p>
]]></description>

        <content:encoded><![
CDATA[<p>Passkeys are a replacement for passwords when signing in, providing
higher security, ease-of-use, and loss-protection. They are now <a
href="https://github.blog/2023-09-21-passkeys-are-generally-
available/">generally available on GitHub.com</a> for all users. By using a
passkey you no longer need to enter a password, or even your username, when you
sign in &#8211; nor do you need to perform 2FA, if you have 2FA enabled on your
account. This is because passkeys validate your identity, as well as possession
of a device, so they count as two authentication factors in one. Once enrolled,
you can register a brand new passkey and upgrade many security keys to
passkeys.</p>
<p align="center"></p>
<p>To learn more, check out our documentation <a
href="https://docs.github.com/en/authentication/authenticating-with-a-passkey/
about-passkeys">"About passkeys"</a>, as well as <a
href="https://gh.io/passkeys-beta-blog">this previous blog post from the
passkeys beta announcement</a>. If you have any feedback, please drop us a note
in our <a href="https://gh.io/passkey-feedback">public discussion</a> &#8211;
we&#039;re excited for this advance in account security, and would love to
understand how we can make it better for you.</p>
<p>The post <a href="https://github.blog/changelog/2023-09-21-passkeys-are-
generally-available">Passkeys are Generally Available</a> appeared first on <a
href="https://github.blog">The GitHub Blog</a>.</p>
]]></content:encoded>

        <post-id xmlns="com-wordpress:feed-additions:1">74211</post-id>
    </item>
    <item>
        <title>New 2FA account recovery options via password reset
flow</title>
        <link>https://github.blog/changelog/2023-09-07-new-2fa-account-

```

recovery-options-via-password-reset-flow</link>

<dc:creator><![CDATA[Kevin Duck]]></dc:creator>
<pubDate>Thu, 07 Sep 2023 20:33:28 +0000</pubDate>
<guid

isPermaLink="false">https://github.blog/changelog/2023-09-07-new-2fa-account-recovery-options-via-password-reset-flow</guid>

<description><![CDATA[<p>New 2FA account recovery options via password reset flow</p>
<p>The post New 2FA account recovery options via password reset flow appeared first on The GitHub Blog.</p>
]]></description>

<content:encoded><![CDATA[<p>Users with two-factor authentication enabled can now begin the account recovery process from the password reset flow. Previously, the account password was needed to access 2FA account recovery, but passwords on 2FA-enabled accounts could only be reset with a valid second factor. If you lost your password and all of your second factors, you were locked out because you could not access account recovery. With this change, a user can recover their account as long as they can perform email verification and provide a recovery factor, such as an SSH key, PAT, or previously signed in device.</p>
<p>Once you have performed email verification and provided a recovery factor, your recovery will be manually reviewed by GitHub's support team, who will email you within three business days. If your request is approved, you'll receive a link that lets you disable 2FA on your account. After that, you can reset your password and regain access to your account.</p>
<p>For more information about two-factor authentication, see "About two-factor authentication". For account recovery details, see "Recovering your account if you lose your 2FA credentials".</p>
<p>The post New 2FA account recovery options via password reset flow appeared first on The GitHub Blog.</p>
]]></content:encoded>

<post-id xmlns="com-wordpress:feed-additions:1">74021</post-id>
</item>

<item>
<title>2FA requirement status on the People pages</title>
<link>https://github.blog/changelog/2023-07-31-2fa-requirement-status-on-the-people-pages</link>

<dc:creator><![CDATA[Kevin Duck]]></dc:creator>
<pubDate>Mon, 31 Jul 2023 21:47:29 +0000</pubDate>
<guid

isPermaLink="false">https://github.blog/changelog/2023-07-31-2fa-requirement-status-on-the-people-pages</guid>

<description><![CDATA[<p>2FA requirement status on the People pages</p>
<p>The post 2FA requirement status on the People pages appeared first on The GitHub Blog.</p>
]]></description>

<content:encoded><![CDATA[<p>As part of the two-factor authentication requirement program on GitHub.com, the People pages of enterprises and organizations have been updated to include the 2FA requirement status of members and collaborators. As an administrator, you can see which of your users have not yet enabled 2FA but are required to do so because of an action they have taken in one of your organizations, or elsewhere on GitHub.com.</p><p>A clock icon will appear as a user's 2FA status will show if the user is required to enable 2FA. When the icon is red, they are past the due date for enabling 2FA, and are at risk of being blocked from accessing GitHub.com until they enable it. Clicking the clock icon will display the user's enrollment date.
</p><p>You can filter the UI to show only users who have a pending requirement. Enrollment dates are also now included in the CSV and JSON downloads of enterprise and organization memberships.</p><p>To learn more about the 2fa enrollment program, see our blog post with more details. For information about viewing your members, see the organization and enterprise documentation.</p><p>The post 2FA requirement status on the People pages appeared first on The GitHub Blog.</p>]]</content:encoded>

<post-id xmlns="com-wordpress:feed-additions:1">73452</post-id>
</item>
<item>
<title>Passkeys Public Beta</title>
<link>https://github.blog/changelog/2023-07-12-passkeys-public-beta</link>

<dc:creator><![CDATA[Kevin Duck]]></dc:creator>
<pubDate>Wed, 12 Jul 2023 15:09:38 +0000</pubDate>
<guid
isPermaLink="false">https://github.blog/changelog/2023-07-12-passkeys-public-beta</guid>

<description><![CDATA[<p>Passkeys Public Beta</p><p>The post Passkeys Public Beta appeared first on The GitHub Blog.</p>]]</description>

<content:encoded><![CDATA[<p>Passkeys are a replacement for passwords when signing in, providing higher security, ease-of-use, and loss-protection. They're now available on GitHub.com as a public beta – see this blog post for more information.</p><p>This public beta is open to all users with a password, regardless of whether you use 2FA. To get started, enable passkeys as a feature preview.</p><p>By using passkeys, you no longer need to enter a password, or even your

username, when you sign in – nor do you need to perform 2FA, if you have 2FA enabled on your account. That's because passkeys validate your identity, as well as possession of a device, so they count as two authentication factors in one.</p>

<p>Once enrolled, you can register a brand new passkey and upgrade many security keys to a passkey. If you're enrolled in the preview, the next time you use an eligible security key you'll be asked to upgrade it.

src="https://github.com/github/docs/assets/1666363/a4fb158f-31f7-4b70-8a92-a7720bf0f7ed"></p>

<p>To learn more, check out this blog post about passkeys, as well as "About passkeys" in our documentation. If you have any feedback, please drop us a note in our public discussion – we're excited for this advance in account security, and would love to understand how we can make it better for you.</p>

<p>The post Passkeys Public Beta appeared first on The GitHub Blog.</p>

]]></content:encoded>

<post-id xmlns="com-wordpress:feed-additions:1">73064</post-id>
</item>

<item>

<title>TOTP codes for 2FA are now single-use</title>

<link>https://github.blog/changelog/2023-06-29-totp-codes-for-2fa-are-now-single-use</link>

<dc:creator><![CDATA[Kevin Duck]]></dc:creator>

<pubDate>Thu, 29 Jun 2023 21:56:12 +0000</pubDate>

<guid

isPermaLink="false">https://github.blog/changelog/2023-06-29-totp-codes-for-2fa-are-now-single-use</guid>

<description><![CDATA[<p>TOTP codes for 2FA are now single-use</p>

<p>The post TOTP codes for 2FA are now single-use appeared first on The GitHub Blog.</p>

]]></description>

<content:encoded><![

CDATA[<p>During two-factor authentication and when entering <code>sudo</code> mode for sensitive actions on GitHub.com, TOTP codes could be successfully used multiple times within their validity window. To improve security, this reuse is no longer allowed on GitHub.com, and will be updated in GHES with version 3.10.</p>

<p>Systems that have attempted to script the login flow, across multiple parallel jobs, may break as a result of this change.</p>

<p>Learn more about two-factor authentication with TOTP.</p>

<p>The post TOTP codes for 2FA are now single-use appeared first on The GitHub Blog.</p>

]]></content:encoded>

```
<post-id xmlns="com-wordpress:feed-additions:1">72803</post-id>
</item>
<item>
  <title>SMS has been removed from the GitHub.com sudo page</title>
  <link>https://github.blog/changelog/2023-06-09-sms-has-been-removed-
from-the-github-com-sudo-page</link>

  <dc:creator><![CDATA[Kevin Duck]]></dc:creator>
  <pubDate>Fri, 09 Jun 2023 17:25:58 +0000</pubDate>
  <guid
isPermaLink="false">https://github.blog/changelog/2023-06-09-sms-has-been-
removed-from-the-github-com-sudo-page</guid>

  <description><![CDATA[<p>SMS has been removed from
the GitHub.com sudo page</p>
<p>The post <a href="https://github.blog/changelog/2023-06-09-sms-has-been-
removed-from-the-github-com-sudo-page">SMS has been removed from the GitHub.com
sudo page</a> appeared first on <a href="https://github.blog">The GitHub
Blog</a>.</p>
]]></description>

  <content:encoded><![
CDATA[<p>The option to use SMS on the <a
href="https://docs.github.com/en/authentication/keeping-your-account-and-data-
secure/sudo-mode">sudo page</a> on GitHub.com has been removed. Users can still
use other 2FA methods as well as their password to pass the sudo check and take
sensitive actions. If your account only has SMS as its 2FA method, you can visit
your security settings to enable additional methods such as security keys and
TOTP, as well as installing the GitHub Mobile app.</p>
<p>To learn more about the GitHub.com sudo prompt, see <a
href="https://docs.github.com/en/authentication/keeping-your-account-and-data-
secure/sudo-mode">"Sudo mode"</a>. For details about setting up
additional 2FA methods, see <a
href="https://docs.github.com/en/authentication/securing-your-account-with-two-
factor-authentication-2fa/configuring-two-factor-
authentication">"Configuring two-factor authentication"</a>.</p>
<p>The post <a href="https://github.blog/changelog/2023-06-09-sms-has-been-
removed-from-the-github-com-sudo-page">SMS has been removed from the GitHub.com
sudo page</a> appeared first on <a href="https://github.blog">The GitHub
Blog</a>.</p>
]]></content:encoded>


```

```
<post-id xmlns="com-wordpress:feed-additions:1">72339</post-id>
</item>
<item>
  <title>SMS and TOTP can now both be registered 2FA methods</title>
  <link>https://github.blog/changelog/2023-03-02-sms-and-totp-can-now-
both-be-registered-2fa-methods</link>

  <dc:creator><![CDATA[Kevin Duck]]></dc:creator>
  <pubDate>Thu, 02 Mar 2023 19:51:00 +0000</pubDate>
  <guid
isPermaLink="false">https://github.blog/changelog/2023-03-02-sms-and-totp-can-
now-both-be-registered-2fa-methods</guid>

  <description><![CDATA[<p>SMS and TOTP can now both
be registered 2FA methods</p>
<p>The post <a href="https://github.blog/changelog/2023-03-02-sms-and-totp-can-
now-both-be-registered-2fa-methods">SMS and TOTP can now both be registered 2FA
methods</a> appeared first on <a href="https://github.blog">The GitHub
Blog</a>.</p>


```

]]></description>

<content:encoded><!

[CDATA[<p>You can now set up both SMS and an authenticator app (TOTP) for two-factor authentication on your GitHub.com account. Previously these methods were mutually exclusive, and you needed to create a "fallback"; SMS registration that could be used for account recovery.</p>

<p></p>

<p>With this update, we are removing the fallback SMS option, and will migrate all fallback SMS registrations to be standard 2FA methods today. A small set of users had both a primary and fallback SMS registration on their account – they continue to have that fallback SMS registration, and will receive email about it today.</p>

<p>To learn more about setting up 2FA and GitHub's account recovery methods, see "Configuring 2FA" and "Configuring 2fa recovery methods"</p>

<p>The post SMS and TOTP can now both be registered 2FA methods appeared first on The GitHub Blog.</p>

]]></content:encoded>

<post-id xmlns="com-wordpress:feed-additions:1">70454</post-id>

</item>

<item>

<title>Preferred 2FA methods and settings improvements</title>

<link>https://github.blog/changelog/2023-02-22-preferred-2fa-methods-and-settings-improvements</link>

<dc:creator><![CDATA[Kevin Duck]]></dc:creator>

<pubDate>Wed, 22 Feb 2023 20:20:57 +0000</pubDate>

<guid

isPermaLink="false">https://github.blog/changelog/2023-02-22-preferred-2fa-methods-and-settings-improvements</guid>

<description><![CDATA[<p>Preferred 2FA methods and

settings improvements</p>

<p>The post Preferred 2FA methods and settings improvements appeared first on The GitHub Blog.</p>

]]></description>

<content:encoded><!

[CDATA[<p>The <code>Primary</code> field on two-factor authentication methods has been removed, and replaced with a <code>Preferred</code> option. This new option sets your preferred 2FA method for account login and use of the sudo prompt. You can choose between TOTP, SMS, security keys, or GitHub Mobile as your preferred 2FA method.</p>

<p>Additionally, you can now update your 2FA methods inline at https://github.com/settings/security, rather than going through the initial 2FA setup flow again.</p>

<p></p>

<p>With this change, device-specific preferences for 2FA have been removed – each login will always default to your preferred method. If you

previously set a default on one of your devices, your most recent choice has been copied to your account-wide preference. Otherwise, no preference will be set, and GitHub will select from your available second factors in this order: security keys, GitHub Mobile, TOTP, and then SMS.</p>

<p>To learn more, see "Changing your preferred two-factor authentication method"

and "Configuring two-factor authentication".</p>

<p>The post Preferred 2FA methods and settings improvements appeared first on The GitHub Blog.</p>

]]></content:encoded>

<post-id xmlns="com-wordpress:feed-additions:1">70221</post-id>

</item>

</channel>

</rss>