One Identity Starling Two-Factor Authentication

Release Notes

25 March 2020

These release notes provide information about the 25 March 2020 Starling Two-Factor Authentication release.

About this release

One Identity Starling Two-Factor Authentication is designed to support non-federated applications and applications that act as an Identity Provider (IdP), to accept a one-time password (OTP) for two-factor authentication. It provides OTP by SMS, phone call or Starling 2FA app. It also supports push notifications, where users receive approval requests on their Starling 2FA app for two-factor authentication. An application that uses Starling Two-Factor Authentication is able to validate OTP and redirect all OTP and push notification management workflows to Starling Two-Factor Authentication. Starling Two-Factor Authentication provides a single interface for two-factor authentication.

Starling Two-Factor Authentication 25 March 2020 is a general release.

New features

New features in the 25 March 2020 release of Starling Two-Factor Authentication:

- There are no new features for this release. See below for information regarding new features in previous releases.

See also:

The following were new features in previous releases of Starling Two-Factor Authentication.

6 November 2019 new features

- Azure Active Directory integration – You can now integrate Azure Active Directory with your Starling Two-Factor Authentication service.

23 October 2019 new features

- Downloads page – A new page has been added that provides access to downloads for the Starling 2FA application and on-premises Starling Two-Factor Authentication components.

11 September 2019 new features

- Minor changes made to the **Dashboard** page – The tiles have been updated to show information pertaining to the current month. The user count information has been removed (both the **Users** tile and corresponding graph data).

28 August 2019 new features

- Desktop application – The Chrome application has been replaced with a desktop application.

31 July 2019 new features

- TOTP hardware token support – The Starling Two-Factor Authentication service now supports TOTP tokens for authentication. This includes DPX file support.

17 July 2019 new features

- Hardware token support – The Starling Two-Factor Authentication service now supports OATH-compliant HOTP tokens for authentication. You can also bulk import users (as long as they are identical to existing users within your client product) in order to assign a hardware token before they begin authenticating.

19 June 2019 new features

- New user interface – The Starling Two-Factor Authentication service has been redesigned to improve your experience and create a more seamless transition as you move between Starling services.
- Mobile compatibility – Some functionalities within Starling Two-Factor Authentication can now be performed from mobile devices.
- Configurable one-time password length – You can now select a character length (6-8) for one-time passwords.

Enhancements

The following is a list of enhancements implemented in the 25 March 2020 Starling Two-Factor Authentication release.

- There were no enhancements. See below for information regarding enhancements in previous releases.

The following enhancements appeared in previous releases of Starling Two-Factor Authentication.

6 November 2019 enhancements

Table 1: General enhancements

Enhancement	Issue ID
Allow updating of name and email when adding an existing user (based on phone number) with updated information.	168308

Deprecated features

The following is a list of features that are no longer supported for Starling Two-Factor Authentication.

- New Azure Active Directory integrations: You can no longer add new Azure Active Directory integrations.

Resolved issues

The following is a list of issues addressed in this release.

- There were no resolved issues. See below for information regarding resolved issues in previous releases.

The following issues were resolved in previous releases of Starling Two-Factor Authentication.

6 November 2019 resolved issues

Table 2: General resolved issues

Resolved Issue	Issue ID
Refresh buttons on the Users and Hardware Tokens pages are not working.	168310
When deleting an organization (and thus all associated users) there is a 30 day delay before the token (and users) are fully deleted. There is no delay to the token deletion if you delete each user individually before deleting the organization.	168449

9 October 2019 resolved issues

Table 3: General resolved issues

Resolved Issue	Issue ID
The Starling 2FA application is missing from the Google Play Store. We have contacted Google about fixing the issue. No other versions of the application are impacted.	167360

11 September 2019 resolved issues

Table 4: General resolved issues

Resolved Issue	Issue ID
Currently unable to save changes to the token name on the **Settings** page.	140462

14 August 2019 resolved issues

Table 5: General resolved issues

Resolved Issue	Issue ID
Leaving the Settings page discards unsaved changes without prompting for confirmation.	113515

3 July 2019 resolved issues

Table 6: General resolved issues

Resolved Issue	Issue ID
Error message stating that an Administrator is unable to remove the last Primary Administrator from Starling Two-Factor Authentication is not appearing. The Primary Administrator is not removed even though the error message does not appear.	115138

26 June 2019 resolved issues

Table 7: General resolved issues

Resolved Issue	Issue ID
Collaborator invites and approval requests randomly failing for Administrators. Workaround: Delete any failed approval and try as a Primary Administrator.	123952
The install link for the Starling Two-Factor Authentication application stopped working.	124117
Approval for a new subscription key failing.	124089

19 June 2019 resolved issues

Table 8: General resolved issues

Resolved Issue	Issue ID
On the **Users** page, you are unable to filter results based on country code.	56525
Canceling out of saved changes when leaving a page may result in a stuck loading dialog. Workaround: Refresh the page (**F5**).	112134

8 May 2019 resolved issues

Table 9: General resolved issues

Resolved Issue	Issue ID
An error page displays if trying to access Starling Two-Factor Authentication subscription from the **Access Summary** page of Starling. The service tile is not impacted.	114465

24 April 2019 resolved issues

Table 10: General resolved issues

Resolved Issue	Issue ID
When you try to open the Starling Two-Factor Authentication service, the following ambiguous error message is displayed: The user account is suspended. This error message means that the subscription has expired.	13629
The **Collaborator** page CUI control (buttons) does not reset after performing an operation on the selected item.	28507
When using the Edge browser, the **Approvals** page incorrectly displays the status of the requests as pending. Attempting to manage approval requests using Edge may result in errors. Workaround: Do not use Edge to view or manage approvals.	28645

14 April 2019 resolved issues

Table 11: General resolved issues

Resolved Issue	Issue ID
On the **Dashboard**, adding a collaborator again with a different role, changes the role of the existing collaborator to a new role. Workaround: Use the **Edit collaborator** window to change the role of a collaborator.	35449

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

Table 12: General known issues

Known Issue	Issue ID
An error might appear when an AAD user first tries to log in to an application protected by Starling 2FA AAD integration. Workaround: Log in to the application again.	169688

System requirements

Before using the 25 March 2020 Starling Two-Factor Authentication release, ensure that your system meets the following minimum hardware and software requirements. For additional requirements, see the *Additional hardware and software requirements* section in the *Starling Two-Factor Authentication Administration Guide*.

Browser requirements

Table 13: Supported desktop browsers

Browser	Minimum OS/Platform	Version
Internet Explorer	Windows 7	11
Google Chrome	Windows 10 Mac OS X Yosemite	Latest

Browser	Minimum OS/Platform	Version
Mozilla Firefox	Windows 8.1	Latest
Microsoft Edge	Windows 10	Latest
Safari	Mac OS X Yosemite	See OS/Platform

Table 14: Supported mobile browsers

Browser	Minimum OS/Platform	Version
Google Chrome	Android	Latest
Safari	iOS	Latest

Product licensing

Use of this software is governed by the Software Transaction Agreement found at http://www.oneidentity.com/legal/sta.aspx and the SaaS Addendum at http://www.oneidentity.com/legal/saas-addendum.aspx. This software does not require an activation or license key to operate.

New service instructions

For information and instructions on adding the Starling Two-Factor Authentication service to a Starling organization, see the *Starling Two-Factor Authentication Administration Guide*.

More resources

Additional information is available from the following:

- Online product documentation
- Starling online community

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section

does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan. It supports bidirectional writing (Arabic and Hebrew). The release supports Complex Script (Central Asia – India, Thailand).

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.