One Identity Starling Two-Factor Authentication

Administration Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Starling Two-Factor Authentication Administration Guide
Updated - August 2018

Contents

What you can do with One Identity Starling Two-Factor Authentication

If your organization wants to enable two-factor authentication on a product, you can purchase Starling Two-Factor Authentication subscription. When your organization purchases the subscription, a subscription gets created and you receive an invitation to access Starling Two-Factor Authentication Dashboard.

To configure Starling Two-Factor Authentication in your product, you have to provide the subscription key that is available on the Starling Two-Factor Authentication Dashboard or, join your product to a Starling account. For more information on configuring Starling Two-Factor Authentication in your product, see the relevant section in the documentation set of your product.

On Starling Two-Factor Authentication Dashboard, you can do the following:

- Add or delete collaborators (Administrators and Helpdesk users)
- Manage the user status of the service
- Monitor the service usage statistics
- View the license details and subscription details
- View and change the subscription key
- Modify the user authentication settings
- Customize the token appearance on the Starling 2FA app

Logging in to Starling Two-Factor Authentication dashboard

To log in to the dashboard:

1. Log in to Starling account. If you are logging in to the Starling account for the first time, do one of the following:
   - If you have a Starling account, when a subscription is created for you, you will receive a Starling invitation email. Click the link in the email and log in to the Starling account.
   - If you do not have a Starling account, when a subscription is created for you, you will get a Starling Sign-up email to complete a registration process to create a Starling account. Complete the registration and log in using the credentials that you have provided during registration. For account creation details, see the **One Identity Starling User Guide**.
2. Under **My Services**, click **Two-Factor Authentication**.

   Starling Two-Factor Authentication Dashboard is displayed.

3

Managing subscription

The **Dashboard** tab displays the details of Starling Two-Factor Authentication service usage statistics for the current month, license details, subscription details and the subscription key. These details help in tracking and managing the subscription.

Starling 2FA services can be used either by joining a client product to Starling using the Join functionality or, by using a subscription key. This depends on the version of the client product that is being used.

NOTE: Please refer the appropriate version of the client product documentation, for the configuration steps.

Stand-alone Subscription

Customers can buy stand-alone subscriptions depending on the number of user licenses required. Number of users using the services is dependent on the number of licenses purchased.

One Identity Hybrid Subscription

Customers using other One Identity products can use Hybrid subscription, to subscribe to Starling 2FA services. Contact your sales representative for more information.

Service usage statistics

Service usage statistics section displays the details of the service usage for the current month such as number of users using the service, phone calls, SMS and authentications. It also provides a graphical representation of the service usage.

License details

License details related to both the subscriptions (stand-alone and hybrid) are detailed below.

Stand-Alone Subscription

Different parameters related to stand-alone subscription are mentioned in the table below.

ITEM NAME	TOOLTIP TEXT
Licensed users	Number of users licensed under your stand-alone subscription.
Consumed user licenses	Number of consumed user licenses under your stand-alone subscription. If you have purchased a hybrid subscription, this value may be initially inaccurate and will be automatically updated as your users start using the hybrid subscription.
Created	Creation date of your stand-alone subscription.
Expires	Expiration date of your stand-alone subscription. If you have an active hybrid subscription you can use it, once your stand-alone subscription expires.
Hybrid subscription	If you have a valid standalone subscription, set to **NO**.

One Identity Hybrid Subscription

Different parameters related to hybrid subscription are mentioned in the table below.

ITEM NAME	TOOLTIP TEXT
Hybrid subscription	Indicates whether you have purchased a hybrid subscription.
Hybrid subscription expires	Expiration date of your hybrid subscription. If you have an active stand-alone subscription you can continue to use it once your hybrid subscription expires.
Hybrid subscription users	Number of users using Starling 2FA as part of the hybrid subscription.
License Status	Indicates whether the license is valid or invalid

Subscription details

Subscription details section displays the Subscription Id and Subscription name.

Subscription key

Subscription key section displays the subscription key allotted to you when a new subscription is created for you. You can use this key to configure your software that uses Starling Two-Factor Authentication. If the subscription key is used by unauthorized users or used inappropriately, the Administrator can change the subscription key. After the new key is created, the current key will be valid only for next 24 hours.

Managing collaborators

The **Collaborators** tab displays all the collaborators and their roles assigned by the Administrators. Collaborators are users who are assigned with certain roles. They manage the administrative and general tasks in Starling Two-Factor Authentication. Collaborators can log in to Dashboard and perform the tasks as per the roles assigned to them.

Collaborators are categorized into three: Helpdesk user, Administrator, and Primary Administrator. A Helpdesk user performs general tasks, whereas Administrators and Primary Administrators perform administrative tasks.

The tasks initiated by an Administrator require approval from at least one other Administrator. Any Administrator other than the one who initiated the action can approve or cancel a request. The Administrator who initiated the action can resend the approval email.

A Primary Administrator can perform the tasks of a Helpdesk user and Administrator without any approval.

The administrator can add a collaborator by performing the below procedure:

1. From the **Collaborators** page, click **Add**. The **Add Collaborators** dialog box opens.
2. Select a value from the **Role** drop-down menu.
3. Enter appropriate values in the following fields:
    - First Name
    - Last Name
    - Email ID
4. Click **Add**. An invitation is sent as an email to the mentioned email ID if the Starling account is not present. Invited collaborators are marked as **Invited** in the **Collaborators** page.

NOTE: You can cancel or resend an invitation that was sent to an invited collaborator from the **Collaborators** page.

The following table lists the various tasks that each collaborator role can perform.

Table 1: Collaborator roles and tasks

Tasks	Helpdesk user	Administrator	Primary Administrator
Log in to Dashboard	Yes	Yes	Yes
Create, manage, and delete users, who use two-factor authentication	Yes	Yes	Yes
Run health check for the Starling 2FA app installed on the user's device	Yes	Yes	Yes
Generate temporary response code	Yes	Yes	Yes
View and change subscription key	No	Yes	Yes
Add new Administrators and Helpdesk users	No	Yes	Yes
Delete Administrator and Helpdesk users	No	Yes	Yes
Change the role	No	Yes	Yes
Change subscription settings	No	Yes	Yes

5

Managing approvals

The **Approvals** tab displays all the approval requests received from other Administrators for administrative actions that require an approval from another Administrator. In such cases, the Administrators receive an approval email or receive an approval link in the **Approvals** tab.

To complete an approval for an administrative action, do one of the following:

- Click the link in the approval email and approve the action.
- Access the **Approvals** section on the Dashboard and approve or cancel the request.

6

Managing user accounts

The **Users** tab displays all the users who have subscribed for Starling Two-Factor Authentication for two-factor authentication. You can manage the user accounts by performing the following user management tasks:

- **Creating new user account**: When a new user requires two-factor authentication security for his application, you can click **Add** and create a new user account. The user account must be created checking the license capacity of the subscription.
- **Disabling and enabling the user account**: When a user's phone is lost or is defective, you can click **Disable** and disable the user account as a security measure. When the phone is available and functional, you can click **Enable** and activate the disabled account.
- **Deleting and restoring the user account**: When a user is not using Starling Two-Factor Authentication, you can click **Delete** to delete the user account. When you delete a user, the account is immediately suspended and marked for deletion. Except **Restore** option, all other options are not available for the deleted users. You can click **Restore** and restore the user account from the Users pane in the 2FA Dashboard within 30 days period. After 30 days, the account is permanently deleted.
- **Generating a temporary response code**: When a user's phone is inaccessible, you can click **Temporary response** and provide the user a temporary response code for two-factor authentication. The code is valid for 15 minutes.
- **Performing heath check**: You can click Health check and verify whether the Starling 2FA app on the user's device is working properly or not.
- **Displaying list of users**: Select an option from the **State** drop-down menu. Click one of these options **All**, **Active**, **Disabled**, or **Deleted** to display list of users for the respective category.

Customizing settings

The **Settings** tab displays all the user authentication settings and the options to customize the token UI. You can set the User authentication settings and customize the token UI as per the requirement.

Customizing user authentication

The **General** tab displays the options to configure user authentication methods and to send installation instructions to install Starling 2FA app for authentication.

If the **Installation instructions** option is set to ON, when a new user is added to the subscription, the user receives an SMS with instructions to install Starling 2FA app.

You can configure the required methods for two-factor authentication on this tab. The following are the available options:

- Push notifications

  NOTE: If the option is already enabled, it is not displayed. If the option is not enabled, you can enable it. If enabled, you cannot disable the option.

- SMS
- Phone call
- Interactive phone calls

To enable an option, set the option to **ON**.

Customizing token UI

The **Token UI** tab allows you to customize the appearance of the token user interface on Starling 2FA app. You can customize the images for main logo, menu logo and specify

colors for the token.

NOTE: The logo images must be in PNG format and the file size must not exceed 128 KB. The dimensions of main logo must not exceed 588 X 214 pixels. The dimensions of menu logo must not exceed 81 X 81 pixels.

You can also configure a token name to display on the Starling 2FA app. By default, **Starling 2FA** is displayed as the token name on the app. You can set a token name which is not more that 30 characters in the **Token name** field.

When the customization is complete, the Starling 2FA app reflects the changes made on the Dashboard.

Starling 2FA application

Starling 2FA application, for mobile and Chrome store is used to generate one-time passwords (OTP) and receive push notification requests.

The Starling 2FA application is available for the following platforms:

For Chrome:

https://chrome.google.com/webstore/detail/starling-2fa/khnikiidjicifceeiommikcipipmcngk

For Android

https://play.google.com/store/apps/details?id=com.starling.twofactor

For iOS:

https://itunes.apple.com/app/starling-2fa/id1205700916

When users install the app, they register with a mobile phone number that serves as their unique ID. Users can install the app on different devices and register with the same phone number in order to be able to have a backup device in case the primary device is inaccessible.

To generate OTP through Starling 2FA application:

1. If the user is provisioned in a Starling 2FA subscriptions they will see the token for that subscription in the app. Click the token to get the token response.
2. The users must copy the token response to log-in to the client application.

Use push notifications:

The user can either approve or deny a push notification request from Starling 2FA application.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product